



# Instructor Materials

## Chapter 1: A World of Wizard, Heroes, and Criminals



**Cybersecurity Essentials v1.0**

**Cisco Networking Academy®**  
Mind Wide Open™

## Chapter 1: A World of Wizard, Heroes, and Criminals



## Cybersecurity Essentials v1.0

Cisco | Networking Academy®  
Mind Wide Open™



# Chapter 1 - Sections & Objectives

- **1.1 Characteristics of Cybersecurity World**
  - Describe the common characteristics comprising the cybersecurity world
- **1.2 Criminals and Cybersecurity Professionals**
  - Differentiate the characteristics of cyber criminals and heroes
- **1.3 Comparing Cybersecurity Threats**
  - Compare how cybersecurity threats affect individuals, businesses, and organizations
- **1.4 Cybercrime Growth Factors**
  - Analyze the organizations and efforts committed to expanding the cybersecurity workforce

## 1.1 The Cybersecurity World





# The Kingdoms

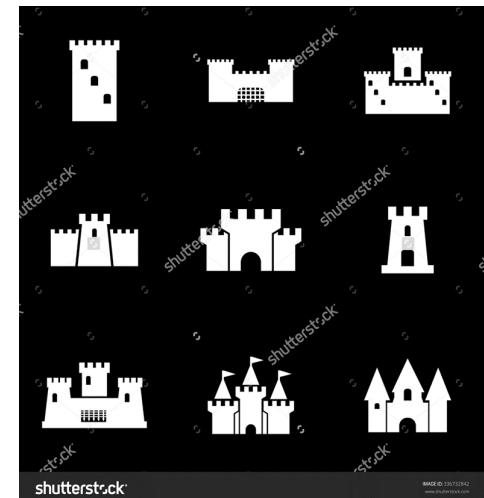
# Overview of the Kingdoms

## ■ Websites and Power of Data

- Great businesses have been created by collecting and harnessing the power of data and data analytics
- These businesses have the responsibility to protect this data from misuse and unauthorized access
- The growth of data has created great opportunities for cybersecurity specialists

## ■ Kingdoms

- Business large and small have recognized the power of big data and data analytics
- Organizations like Google, LinkedIn, Amazon provide important services and opportunity for their customers
- The growth in data collection and analytics poses great risks to individuals and modern life if precautions are not taken to protect sensitive data from criminals or others who have intent to harm





## The Kingdoms

# Overview of the Kingdoms (Cont.)

- Cyber wizards now have the technology to track worldwide weather trends, monitor the oceans, and track the movement and behavior of people, animals and objects in real time.
- New technologies, such as Geospatial Information Systems (GIS) and the Internet of Everything (IoE), have emerged. Each depends on collecting and analyzing tremendous amounts of data.
- This growing collection of data can help people save energy, improve efficiencies, and reduce safety risks.



## 1.2 Cyber Criminals versus Cyber Professionals





# Cybercriminal versus Cyber Heroes

## Cybersecurity Criminals

- **Hackers** – This group of criminals breaks into computers or networks to gain access for various reasons.

**White hat** attackers break into networks or computer systems to discover weaknesses in order to improve the security of these systems.

**Gray hat** attackers are somewhere between white and black hat attackers. The gray hat attackers may find a vulnerability and report it to the owners of the system if that action coincides with their agenda.

**Black hat** attackers are unethical criminals who violate computer and network security for personal gain, or for malicious reasons, such as attacking networks.





# Cybercriminal versus Cyber Heroes

## Cybersecurity Criminals (Cont.)

Criminals come in many different forms. Each have their own motives:

- **Script Kiddies** - Teenagers or hobbyists mostly limited to pranks and vandalism, have little or no skill, often using existing tools or instructions found on the Internet to launch attacks.
- **Vulnerability Brokers** - Grey hat hackers who attempt to discover exploits and report them to vendors, sometimes for prizes or rewards.
- **Hacktivists** - Grey hat hackers who rally and protest against different political and social ideas. Hacktivists publicly protest against organizations or governments by posting articles, videos, leaking sensitive information, and performing distributed denial of service (DDoS) attacks.



## Cybercriminal versus Cyber Heroes

# Cybersecurity Criminals (Cont.)

Criminals come in many different forms. Each have their own motives:

- **Cyber Criminals** - These are black hat hackers who are either self-employed or working for large cybercrime organizations. Each year, cyber criminals are responsible for stealing billions of dollars from consumers and businesses.
- **State Sponsored Hackers** - Depending on a person's perspective, these are either white hat or black hat hackers who steal government secrets, gather intelligence, and sabotage networks. Their targets are foreign governments, terrorist groups, and corporations. Most countries in the world participate to some degree in state-sponsored hacking.



# Cybercriminal versus Cyber Heroes

# Cybersecurity Specialists

Thwarting the cyber criminals is a difficult task, company, government and international organizations have begun to take coordinated actions to limit or fend off cyber criminals. The coordinated actions include:

- **Vulnerability Database:** The National Common Vulnerabilities and Exposures (CVE) database is an example of the development of a national database. The CVE National Database was developed to provide a publicly available database of all known vulnerabilities.  
<http://www.cvedetails.com/>
- **Early Warning Systems:** The Honeynet project is an example of creating Early Warning Systems. The project provides a HoneyMap which displays real-time visualization of attacks.  
<https://www.honeynet.org/node/960>
- **Share Cyber Intelligence:** InfraGard is an example of wide spread sharing of cyber intelligence. The InfraGard program is a partnership between the public and private sector. The participants are dedicated to sharing information and intelligence to prevent hostile cyberattacks.  
<https://www.infragard.org/>



# Cybercriminal versus Cyber Heroes Cybersecurity Specialist (Cont.)

- **ISM Standards:** The ISO 27000 standards are an example of Information Security Management Standards. The standards provide a framework for implementing cybersecurity measures within an organization. <http://www.27000.org/>
- **New Laws:** The ISACA group track law enacted related to cyber security. These laws can address individual privacy to protection of intellectual property. Examples of these laws include: Cybersecurity Act, Federal Exchange Data Breach Notification Act and the Data Accountability and Trust Act.  
<http://www.isaca.org/cyber/pages/cybersecuritylegislation.aspx>

## Tools for Thwarting Cybercrime



## 1.3 Threats to the Kingdom





# Threats to the Kingdom

## Threat Arenas

- The term cyber wizards refers to the innovators and visionaries that build the cyber kingdom
- Cyber wizards possess the insight to recognize the influence of data and harness that power to build great organizations, provide services and protect people from cyberattacks
- Cyber wizards recognize the threat that data poses if used against people
- A cybersecurity threat is the possibility that a harmful event, such as an attack, will occur
- Cyber vulnerability is a weakness that makes a target susceptible to an attack
- Cyber threats are particularly dangerous to certain industries and the type of information they collect and protect



# Threats to the Kingdom Threat Arenas (Cont.)

The following examples are just a few sources of data that can come from established organizations:

- **Personal Information**
- **Medical Records**
- **Education Records**
- **Employment and Financial Records**





# Threats to the Kingdom

## Threat Arenas (Cont.)

Network services like DNS, HTTP and Online Databases are prime targets for cyber criminals.

- Criminals use packet-sniffing tools to capture data streams over a network. Packet sniffers work by monitoring and recording all information coming across a network.
- Criminals can also use rogue devices, such as unsecured Wi-Fi access points.
- Packet forgery (or packet injection) interferes with an established network communication by constructing packets to appear as if they are part of a communication.



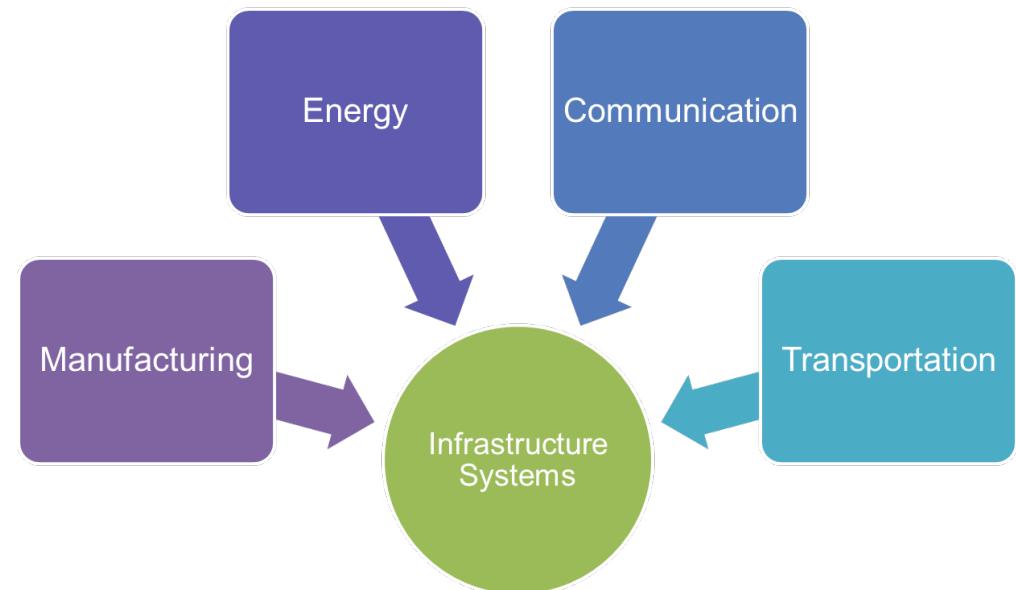


# Threats to the Kingdom

## Threat Arenas (Cont.)

Sectors of the kingdom include:

- Manufacturing
  - Industry Controls
  - Automation
  - SCADA
- Energy Production and Distribution
  - Electrical Distribution and Smart Grid
  - Oil and Gas
- Communication
  - Phone
  - Email
  - Messaging
- Transportation systems
  - Air Travel
  - Rail
  - Over the Road





# Threats to the Kingdom

## Threat Arenas (Cont.)

- On a personal level, everyone needs to safeguard his or her identity, data, and computing devices.
- At the corporate level, it is the employees' responsibility to protect the organization's reputation, data, and customers.
- At the state level, national security and the citizens' safety and well-being are at stake.
- In the U.S., the National Security Agency (NSA) is responsible for intelligence collection and surveillance activities.
- The efforts to protect people's way of life often conflicts with their right to privacy.



## 1.4 The Dark Forces of Cybersecurity





# The Dark Forces of Cybersecurity

## The Spread of the Dark Forces

Attacks can originate from within an organization or from outside of the organization, as shown in the figure.

### Internal Security Threats

- An internal user, such as an employee or contract partner, can accidentally or intentionally
- Internal threats have the potential to cause greater damage than external threats because internal users have direct access to the building and its infrastructure devices. Internal attackers typically have knowledge of the corporate network, its resources, and its confidential data. They may also have knowledge of security countermeasures, policies and higher levels of administrative privileges.

### External Security Threats

- External threats from amateurs or skilled attackers can exploit vulnerabilities in networked devices, or can use social engineering, such as trickery, to gain access.
- External attacks exploit weaknesses or vulnerabilities to gain access to internal resources.



# The Dark Forces of Cybersecurity

## The Spread of the Dark Forces (Cont.)

**Vulnerabilities of Mobile Devices** - In the past, employees typically used company-issued computers connected to a corporate LAN.

- Today, mobile devices such as iPhones, smartphones, tablets, and thousands of other devices, are becoming powerful substitutes for, or additions to, the traditional PC.
- More and more people are using these devices to access enterprise information. Bring Your Own Device (BYOD) is a growing trend.
- The inability to centrally manage and update mobile devices poses a growing threat to organizations that allow employee mobile devices on their networks.

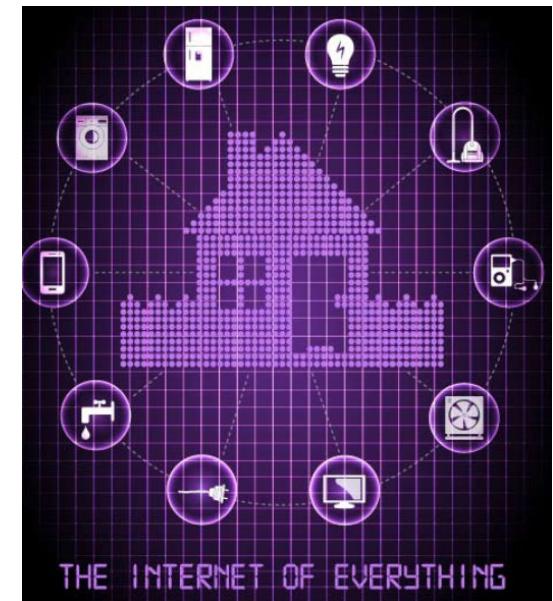




## The Dark Forces of Cybersecurity

# The Spread of the Dark Forces (Cont.)

- **Emergence Internet-of-Things** - The Internet of Things (IoT) is the collection of technologies that enable the connection of various devices to the Internet.
- IoT technologies enable people to connect billions of devices to the Internet. These devices include appliances, locks, motors, and entertainment devices, to name just a few.
- This technology affects the amount of data that needs protection. Users access these devices remotely, which increases the number of networks requiring protection.
- With the emergence of IoT, there is much more data to be managed and secured. All of these connections, plus the expanded storage capacity and storage services offered through the Cloud and virtualization, has led to the exponential growth of data.





# The Dark Forces of Cybersecurity

## The Spread of the Dark Forces (Cont.)

**Impact of Big Data** – Big data is the result of data sets that are large and complex, making traditional data processing applications inadequate. Big data poses both challenges and opportunities based on three dimensions:

- The volume or amount of data
- The velocity or speed of data
- The variety or range of data types and sources

There are numerous examples of big corporate hacks in the news. As a result, enterprise systems require dramatic changes in security product designs and substantial upgrades to technologies and practices. Additionally, governments and industries are introducing more regulations and mandates that require better data protection and security controls to help guard big data.





## The Spread of the Dark Forces

# The Sophistication of the Dark Forces

### Advanced Weapons

- Advanced persistent threat (APT) is a continuous computer hack that occurs under the radar against a specific object. Criminals usually choose an APT for business or political motives.
- Algorithm attacks can track system self-reporting data, like how much energy a computer is using, and use that information to select targets or trigger false alerts. Algorithmic attacks are more devious because they exploit designs used to improve energy savings, decrease system failures, and improve efficiencies.
- Intelligent selection of victims. In the past, attacks would select the low hanging fruit or most vulnerable victims. Many of the most sophisticated attacks will only launch if the attacker can match the signatures of the targeted victim.

### Broader Scope and Cascade Effect

- Federated identity management refers to multiple enterprises that let their users use the same identification credentials gaining access to the networks of all enterprises in the group. The goal of federated identity management is to share identity information automatically across castle boundaries.
- The most common way to protect federated identity is to tie login ability to an authorized device.



## The Spread of the Dark Forces

# The Sophistication of the Dark Forces (Cont.)

### Safety Implications

- There are many safety implication associated with the dark forces of cyber security including emergency call centers in the U.S. are vulnerable to cyberattacks that could shut down 911 networks, jeopardizing public safety.
- A telephone denial of service (TDoS) attack uses phone calls against a target telephone network tying up the system and preventing legitimate calls from getting through.
- The next generation 911 call centers are vulnerable because they use Voice-over-IP (VoIP) systems rather than traditional landlines.

### Heightened Recognition of Cybersecurity Threats

- The defenses against cyberattacks at the start of the cyber era were low. A smart high school student or script kiddie could gain access to systems.
- Now, countries across the world have become more aware of the threat of cyberattacks. The threat posed by cyberattacks now head the list of greatest threats to national and economic security in most countries.

## 1.5 Creating More Heroes





Creating More Heroes

# A Workforce Framework for Cybersecurity

## Addressing the Shortage of Cybersecurity Specialists

- In the U.S., the National Institute of Standards and Technologies (NIST) created a framework for companies and organizations in need of cybersecurity professionals. The framework enables companies to identify the major types of responsibilities, job titles, and workforce skills needed.

## The Seven Categories of Cybersecurity Wizards

The Workforce Framework categorizes cybersecurity work into seven categories.

- **Operate and Maintain** includes providing the support, administration, and maintenance required to ensure IT system performance and security
- **Protect and Defend** includes the identification, analysis, and mitigation of threats to internal systems and networks
- **Investigate** includes the investigation of cyber events and/or cyber crimes involving IT resources
- **Collect and Operate** includes specialized denial and deception operations and the collection of cybersecurity information



Creating More Heroes

# A Workforce Framework for Cybersecurity (Cont.)

- **Analyze** includes highly specialized review and evaluation of incoming cybersecurity information to determine if it is useful for intelligence
- **Oversight and Development** provides for leadership, management, and direction to conduct cybersecurity work effectively
- **Securely Provision** includes conceptualizing, designing, and building secure IT systems

Within each category, there are several specialty areas. The specialty areas then define common types of cybersecurity work.





Creating More Heroes

# Online Cybersecurity Communities

## Professional Organizations

- Cybersecurity specialists must collaborate with professional colleagues frequently. International technology organizations often sponsor workshops and conferences. Visit each site with your class and explore the resources available.

 www.cert.org	 www.sans.org	 www.mitre.org
 www.first.org	 www.infosyssec.org	
 www.isc2.org	 <b>MULTI-STATE</b> Information Sharing & Analysis Center msisac.cisecurity.org	



## Creating More Heroes

# Online Cybersecurity Communities

### Cybersecurity Student Organizations and Competitions

- Cybersecurity specialists must have the same skills as hackers, especially black hat hackers, in order to protect against attacks.
- How can an individual build and practice the skills necessary to become a cybersecurity specialist?
- Student skills competitions are a great way to build cybersecurity knowledge skills and abilities.
- There are many national cybersecurity skills competitions available to cybersecurity students.



SkillsUSA®





## Creating More Heroes

# Cybersecurity Certifications

### Industry Certifications

In a world of cybersecurity threats, there is a great need for skilled and knowledgeable information security professionals. The IT industry established standards for cybersecurity specialists to obtain professional certifications that provide proof of skills, and knowledge level.

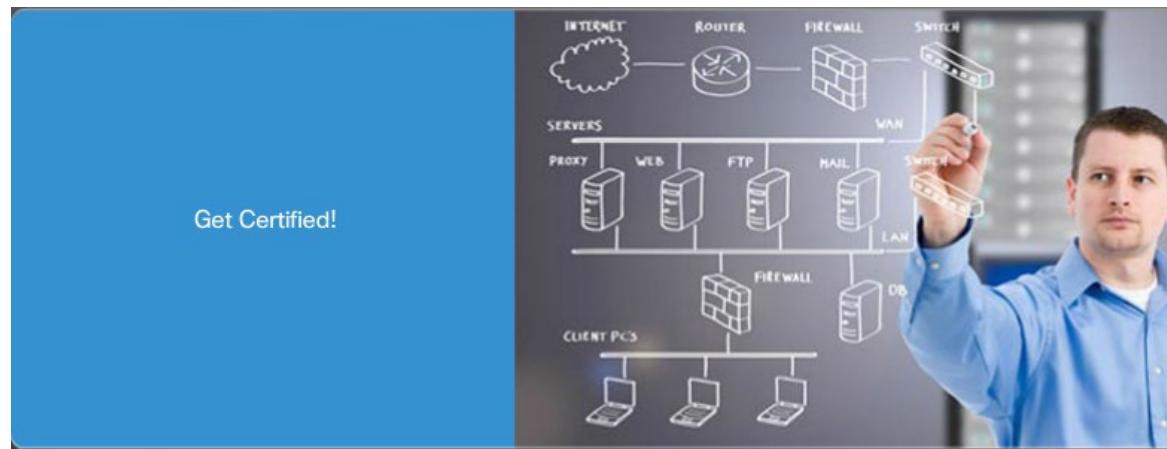
- **CompTIA Security+** - Security+ is a CompTIA-sponsored testing program that certifies the competency of IT administrators in information assurance.
- **EC-Council Certified Ethical Hacker (CEH)** – CEH is an intermediate-level certification asserts that cybersecurity specialists holding this credential possess the skills and knowledge for various hacking practices.
- **SANS GIAC Security Essentials (GSEC)** - The GSEC certification is a good choice for an entry-level credential for cybersecurity specialists who can demonstrate that they understand security terminology and concepts and have the skills and expertise required for “hands-on” security roles. The SANS GIAC program offers a number of additional certifications in the fields of security administration, forensics, and auditing.



Creating More Heroes

# Cybersecurity Certifications (Cont.)

- **(ISC)² Certified Information Systems Security Professional (CISSP)** - The CISSP certification is a vendor-neutral certification for those cybersecurity specialists with a great deal of technical and managerial experience. It is also formally approved by the U.S. Department of Defense (DoD) and is a globally recognized industry certification in the security field.
- **ISACA Certified Information Security Manager (CISM)** - Cyber heroes responsible for managing, developing and overseeing information security systems at the enterprise level or for those developing best security practices can qualify for CISM.





## Creating More Heroes

# Cybersecurity Certifications (Cont.)

**Company Sponsored Certifications** - Another important credential for cybersecurity specialists are company-sponsored certifications. These certifications measure knowledge and competency in installing, configuring, and maintaining vendor products. Cisco and Microsoft are examples of companies with certifications that test knowledge of their products. Click [here](#) to explore the matrix of the Cisco certifications shown in the figure.

**Cisco Certified Network Associate Security (CCNA Security)** - The CCNA Security certification validates that a cybersecurity specialist has the knowledge and skills required to secure Cisco networks.

Cisco Certifications				
	Entry	Associate	Professional	Expert
Architect				CCAr Architect
Cloud		CCNA Cloud	CCNP Cloud	
Collaboration		CCNA Collaboration	CCNP Collaboration	CCIE Collaboration
Data Center		CCNA Data Center	CCNP Data Center	CCIE Data Center
Design	CCENT	CCDA	CCDP	CCDE
Industrial / IoT		CCNA Industrial		
Routing & Switching	CCENT	CCNA Routing & Switching	CCNP Routing & Switching	CCIE Routing & Switching
Security	CCENT	CCNA Security	CCNP Security	CCIE Security
Service Provider		CCNA SP	CCNP SP	CCIE SP
Wireless	CCENT	CCNA Wireless	CCNP Wireless	CCIE Wireless
Other Certifications	Certified Technician			
Specialist	Business	Data Center	Internet of Things	Network Programmability
	Security	Operating System Software	Service Provider	Collaboration



## Creating More Heroes

# Cybersecurity Certifications (Cont.)

### How to Become a Cyber Hero

Heroes must be able to respond to threats as soon as they occur. This means that the working hours can be somewhat unconventional. Cyber heroes also analyze policy, trends, and intelligence to understand how cyber criminals think. Many times, this may involve a large amount of detective work. Here is good advice for becoming a cybersecurity hero:

- **Study:** Learn the basics by completing courses in IT. Be a life-long learner. Cybersecurity is an ever-changing field, and cybersecurity specialists must keep up.
- **Pursue Certifications:** Industry and company sponsored certifications from organizations such as Microsoft and Cisco prove that one possesses the knowledge needed to seek employment as a cybersecurity specialist.
- **Pursue Internships:** Seeking out a security internship as a student can lead to opportunities down the road.
- **Join Professional Organizations:** Join computer security organizations, attend meetings and conferences, and join forums and blogs to gain knowledge from the experts.



## 1.6 Chapter Summary



Cisco | Networking Academy®  
Mind Wide Open™



# Chapter Summary

# Summary

- This chapter explained the structure of the cybersecurity world and the reason it continues to grow with data and information as the prized currency.
- It explored the motivation of cyber criminals.
- It explored the spread of the dark forces due to the ever-expanding technical transformations taking place throughout the world.
- It provided details on how to become a cyber hero to help defeat the cyber criminals that empower the dark forces.
- It surveyed the resources available to help create more heroes.
- It explained that cyber professionals must have the same skills as the cyber criminals.
- If you would like to further explore the concepts in this chapter, please check out the Additional Resources and Activities page in Student Resources.

# Cisco | Networking Academy®

## Mind Wide Open™





# Instructor Materials

## Chapter 2: The Cybersecurity Sorcery Cube



## Cybersecurity Essentials v1.0

**Cisco Networking Academy®**  
Mind Wide Open™



## Chapter 2: The Cybersecurity Sorcery Cube



## Cybersecurity Essentials v1.0

Cisco | Networking Academy®  
Mind Wide Open™



# Chapter 2 - Sections & Objectives

## 2.1 The Cybersecurity Sorcery Cube

Describe the three dimensions of the McCumber Cube.

## 2.2 CIA TRIAD

Describe the principles of confidentiality, integrity, and availability.

## 2.3 States of Data

Differentiate the three states of data.

## 2.4 Cybersecurity Countermeasures

Compare the types of cybersecurity countermeasures.

## 2.5 IT Security Management Framework

Describe the ISO Cybersecurity Model

## 2.1 The Cybersecurity Sorcery Cube



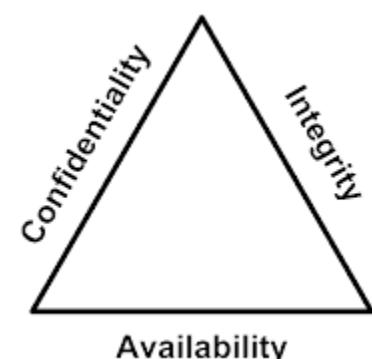


# The Cybersecurity Sorcery Cube

## The Three Dimensions

### The Principles of Security

- The first dimension of the cybersecurity sorcery cube identifies the goals to protect the cyber world. The goals identified in the first dimension are the foundational principles of the cybersecurity world.
- These three principles are confidentiality, integrity and availability.
- The principles provide focus and enable the cyber wizard to prioritize actions in protecting the cyber world.
- Use the acronym CIA to remember these three principles.



### The States of Data

- The cyber world is a world of data; therefore, cyber wizards focus on protecting data. The second dimension of the cybersecurity sorcery cube focuses on the problems of protecting all of the states of data in the cyber world. Data has three possible states:
  - 1) Data at rest or in storage
  - 2) Data in transit
  - 3) Data in process

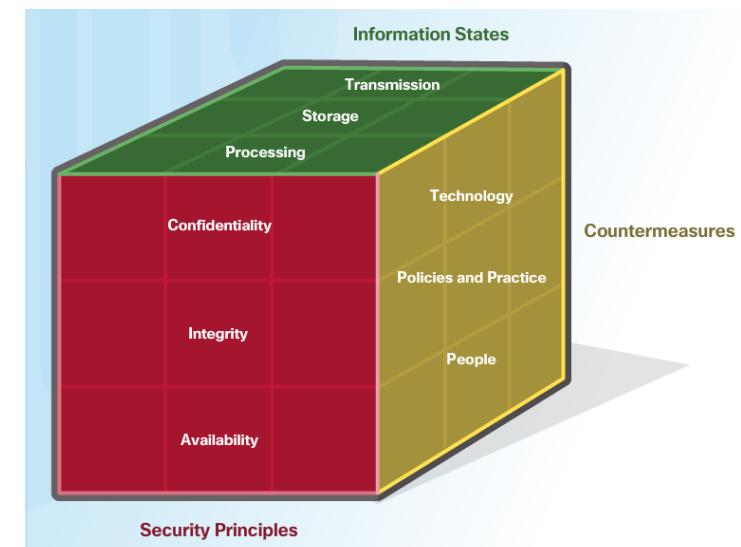


# The Cybersecurity Sorcery Cube

## The Three Dimensions (Cont.)

### Cybersecurity Safeguards

- The third dimension of the cybersecurity sorcery cube defines the types of powers used to protect the cyber world. The sorcery cube identifies the three types of powers:
- **Technologies** - devices, and products available to protect information systems and fend off cyber criminals.
- **Policies and Practices** - procedures, and guidelines that enable the citizens of the cyber world to stay safe and follow good practices.
- **People** - Aware and knowledgeable about their world and the dangers that threaten their world.



## 2.2 CIA TRIAD





# CIA TRIAD

## Confidentiality

### The Principle of Confidentiality

- Confidentiality prevents the disclosure of information to unauthorized people, resources and processes.  
Another term for confidentiality is privacy.
- Organizations need to train employees about best practices in safeguarding sensitive information to protect themselves and the organization from attacks.
- Methods used to ensure confidentiality include data encryption, authentication, and access control.



### Protecting Data Privacy

- Organizations collect a large amount of data and much of this data is not sensitive because it is publicly available, like names and telephone numbers.
- Other data collected, though, is sensitive. Sensitive information is data protected from unauthorized access to safeguard an individual or an organization.



# CIA TRIAD

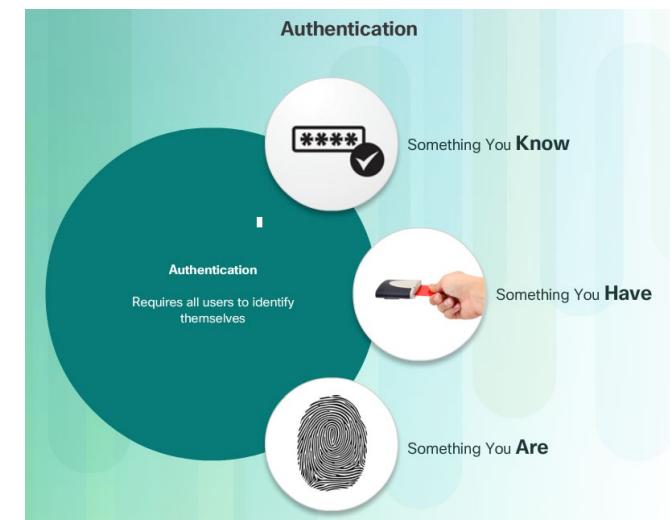
## Confidentiality (Cont.)

### Controlling Access

Access control defines a number of protection schemes that prevent unauthorized access to a computer, network, database, or other data resources. The concepts of AAA involve three security services: Authentication, Authorization and Accounting. **Authentication** verifies the identity of a user to prevent unauthorized access. Users prove their identity with a username or I.D.

**Authorization** services determine which resources users can access, along with the operations that users can perform. Authorization can also control when a user has access to a specific resource.

**Accounting** keeps track of what users do, including what they access, the amount of time they access resources, and any changes made.





## CIA TRIAD

# Confidentiality (Cont.)

Confidentiality and privacy seem interchangeable, but from a legal standpoint, they mean different things.

- Most privacy data is confidential, but not all confidential data is private. Access to confidential information occurs after confirming proper authorization. Financial institutions, hospitals, medical professionals, law firms, and businesses handle confidential information.
- Confidential information has a non-public status. Maintaining confidentiality is more of an ethical duty.
- Privacy is the appropriate use of data. When organizations collect information provided by customers or employees, they should only use that data for its intended purpose.

### U.S. Laws

- Privacy Act of 1974
- Freedom of Information ACT (FOIA)
- Family Education Records and Privacy Act (FERPA)
- U.S. Computer Fraud and Abuse Act (CFAA)
- U.S. Children's Online Privacy Protection Act (COPPA)
- Video Privacy Protection Act (VPPA)
- Health Insurance Portability & Accountability Act
- Gramm-Leach-Bliley Act (GLBA)
- California Senate Bill 1386 (SB 1386)
- U.S. Banking Rules and Regulations
- Payment Card Industry Data Security Standard (PCI DSS)
- Fair Credit Reporting Act (FCRA)



# CIA TRIAD

## Integrity

### Principle of Data Integrity

- Integrity is the accuracy, consistency, and trustworthiness of data during its entire life cycle.
- Another term for integrity is quality.
- Methods used to ensure data integrity include hashing, data validation checks, data consistency checks, and access controls.

### Need for Data Integrity

- The need for data integrity varies based on how an organization uses data. For example, Facebook does not verify the data that a user posts in a profile.
- A bank or financial organization assigns a higher importance to data integrity than Facebook does. Transactions and customer accounts must be accurate.
- Protecting data integrity is a constant challenge for most organizations. Loss of data integrity can render entire data resources unreliable or unusable.

### Integrity Checks

- An integrity check is a way to measure the consistency of a collection of data (a file, a picture, or a record). The integrity check performs a process called a hash function to take a snapshot of data at an instant in time.



## CIA TRIAD

# Availability

Data availability is the principle used to describe the need to maintain availability of information systems and services at all times. Cyberattacks and system failures can prevent access to information systems and services.

- Methods used to ensure availability include system redundancy, system backups, increased system resiliency, equipment maintenance, up-to-date operating systems and software, and plans in place to recover quickly from unforeseen disasters.
- High availability systems typically include three design principles: eliminate single points of failure, provide for reliable crossover, and detect failures as they occur.

Organizations can ensure availability by implementing the following:

1. Equipment maintenance
2. OS and system updates
3. Test backups
4. Plan for disasters
5. Implement new technologies
6. Monitor unusual activity
7. Test to verify availability

## 2.3 States of Data

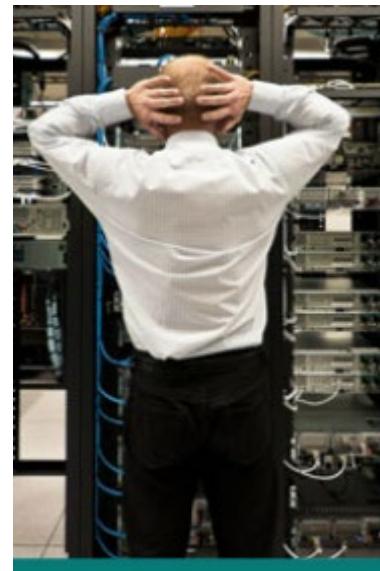




## States of Data

# Data at Rest

- Stored data refers to data at rest. Data at rest means that a type of storage device retains the data when no user or process is using it.
- A storage device can be local (on a computing device) or centralized (on the network). A number of options exist for storing data.
- Direct-attached storage (DAS) is storage connected to a computer. A hard drive or USB flash drive is an example of direct-attached storage.





## States of Data

# Data at Rest (Cont.)

- Redundant array of independent disks (RAID) uses multiple hard drives in an array, which is a method of combining multiple disks so that the operating system sees them as a single disk. RAID provides improved performance and fault tolerance.
- A network attached storage (NAS) device is a storage device connected to a network that allows storage and retrieval of data from a centralized location by authorized network users. NAS devices are flexible and scalable, meaning administrators can increase the capacity as needed.
- A storage area network (SAN) architecture is a network-based storage system. SAN systems connect to the network using high-speed interfaces allowing improved performance and the ability to connect multiple servers to a centralized disk storage repository.





## States of Data

# Data In Transit

Data transmission involves sending information from one device to another. There are numerous methods to transmit information between devices including:

- **Sneaker net** – uses removable media to physically move data from one computer to another
- **Wired networks** – uses cables to transmit data
- **Wireless networks** – uses the airwaves to transmit data

The protection of transmitted data is one of the most challenging jobs of a cybersecurity professional. The greatest challenges are:

- **Protecting data confidentiality** – cyber criminals can capture, save and steal data in-transit.
- **Protecting data integrity** – cyber criminals can intercept and alter data in-transit.
- **Protecting data availability** - cyber criminals can use rogue or unauthorized devices to interrupt data availability.



## States of Data

# Data In Process

The third state of data is data in process. This refers to data during initial input, modification, computation, or output.

- Protection of data integrity starts with the initial input of data.
- Organizations use several methods to collect data, such as manual data entry, scanning forms, file uploads, and data collected from sensors.
- Each of these methods pose potential threats to data integrity.
- Data modification refers to any changes to the original data such as users manually modifying data, programs processing and changing data, and equipment failing resulting in data modification.
- Processes like encoding/decoding, compression/decompression and encryption/decryption are all examples of data modification. Malicious code also results in data corruption.



## 2.4 Cybersecurity Countermeasures





## Cybersecurity Countermeasures

# Technologies

### Software-based Technology Safeguards

- Software safeguards include programs and services that protect operating systems, databases, and other services operating on workstations, portable devices, and servers. There are several software-based technologies used to safeguard an organization's assets.

### Hardware-based Technology Safeguards

- Hardware based technologies are appliances that are installed within the network faculties. They can include: Firewall appliances, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS) and Content filtering systems.





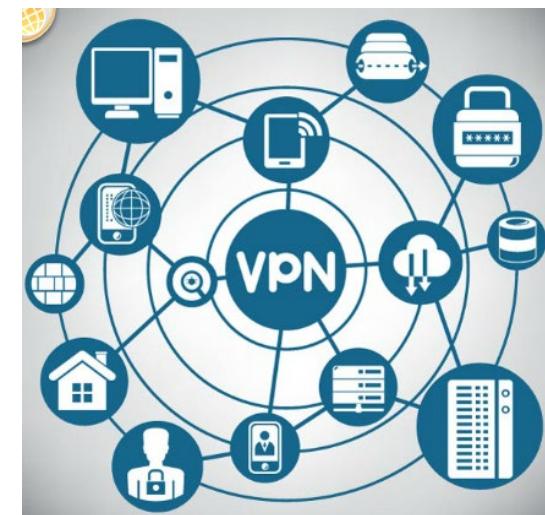
## Cybersecurity Countermeasures

# Technologies

### Network-based Technology Safeguards

Technological countermeasures can also include network-based technologies.

- **Virtual Private Network (VPN)** is a secure virtual network that uses the public network (i.e., the Internet). The security of a VPN lies in the encryption of packet content between the endpoints that define the VPN.
- **Network access control (NAC)** requires a set of checks before allowing a device to connect to a network. Some common checks include up-to-date antivirus software or operating system updates installed.
- **Wireless access point security** includes the implementation of authentication and encryption.





## Cybersecurity Countermeasures

# Technologies

### Cloud-based Technology Safeguards

- Technological countermeasures now also include cloud-based technologies. Cloud-based technologies shift the technology component from the organization to the cloud provider.
- **Software as a Service (SaaS)** allows users to gain access to application software and databases. Cloud providers manage the infrastructure. Users store data on the cloud provider's servers.
- **Infrastructure as a Service (IaaS)** provides virtualized computing resources over the Internet. The provider hosts the hardware, software, servers, and storage components.
- **Virtual security appliances** run inside a virtual environment with a pre-packaged, hardened operating system running on virtualized hardware.





## Cybersecurity Countermeasures

# Implementing Cybersecurity Education and Training

A security awareness program is extremely important for an organization. An employee may not be purposefully malicious but just unaware of what the proper procedures are.

There are several ways to implement a formal training program:

- Make security awareness training a part of the employee's onboarding process
- Tie security awareness to job requirements or performance evaluations
- Conduct in-person training sessions
- Complete online courses

Security awareness should be an ongoing process since new threats and techniques are always on the horizon.





## Cybersecurity Countermeasures

# Cybersecurity Policies and Procedures

- A security **policy** is a set of security objectives for a company that includes rules of behavior for users and administrators and specifies system requirements. These objectives, rules, and requirements collectively ensure the security of a network, the data, and the computer systems within an organization.
- **Standards** help an IT staff maintain consistency in operating the network. Standards provide the technologies that specific users or programs need in addition to any program requirements or criteria that an organization must follow.
- **Guidelines** are a list of suggestions on how to do things more efficiently and securely. They are similar to standards, but are more flexible and are not usually mandatory. Guidelines define how standards are developed and guarantee adherence to general security policies.
- **Procedure** documents are longer and more detailed than standards and guidelines. Procedure documents include implementation details that usually contain step-by-step instructions and graphics.

## 2.5 IT Security Management Framework





## Security Management Framework

# The ISO Model

Security professionals need to secure information from end-to-end within the organization. This is a monumental task, and it is unreasonable to expect one individual to have all of the requisite knowledge.

**The International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC)** developed a comprehensive framework to guide information security management.

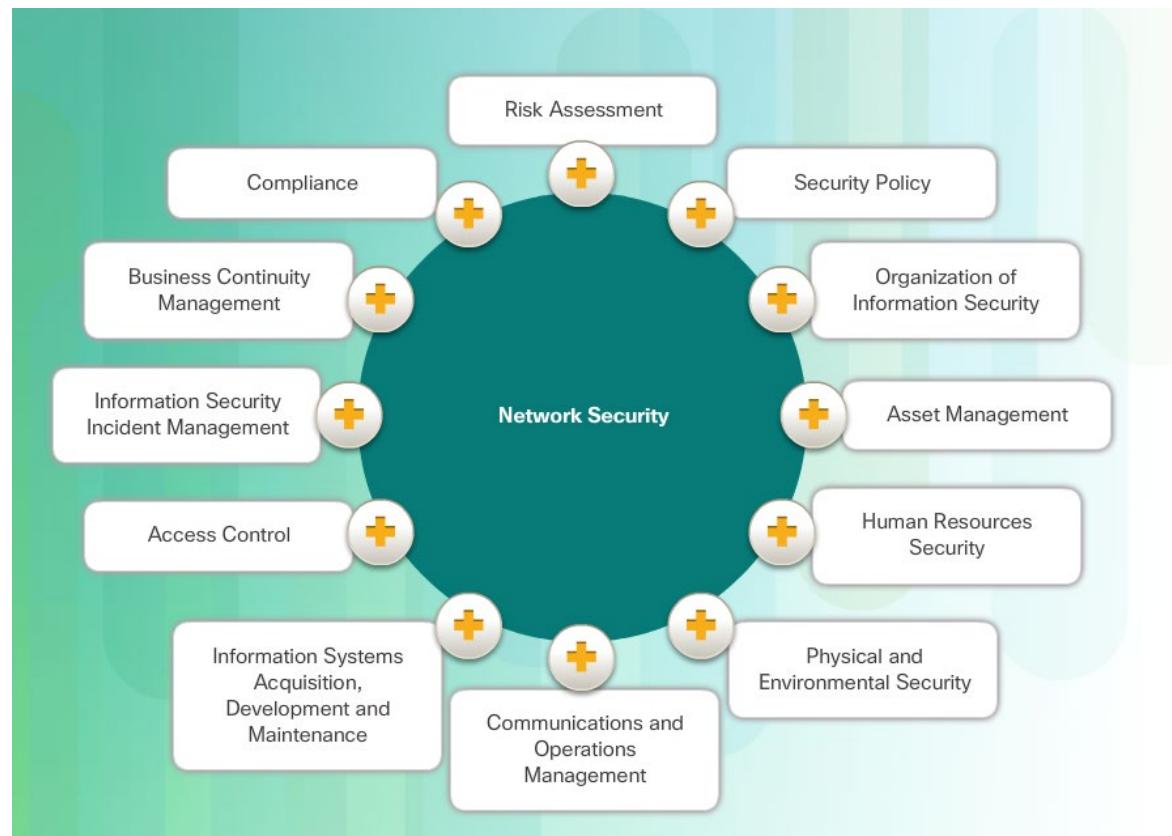
The ISO cybersecurity model is to cybersecurity professionals what the OSI networking model is to network engineers. Both provide a framework for understanding and approaching complex tasks.





# Security Management Framework The ISO Model (Cont.)

ISO/IEC 27000 is an information security standard published in 2005 and revised in 2013. ISO publishes the ISO 27000 standards. Even though the standards are not mandatory, most countries use them as a de facto framework for implementing information security.





## Security Management Framework

# Using the ISO Cybersecurity Model

- The ISO 27000 is a universal framework for every type of organization. In order to use the framework effectively, an organization must narrow down which domains, control objectives, and controls apply to its environment and operations.
- The ISO 27001 control objectives serve as a checklist. The first step an organization takes is to determine if these control objectives are applicable to the organization.

ISO/IEC 27002 Section	Primary Objective		
	Confidentiality	Integrity	Availability
5			
5.1			
5.1.1	√	√	√
5.1.2	√	√	√
6			
6.1			
6.1.1	√	√	√
6.1.2		√	√
6.1.3			√
6.1.4	√		√
6.1.5	√		
6.1.6	√	√	√
6.1.7	√	√	√
6.1.8	√	√	√



## Security Management Framework

# Using the ISO Cybersecurity Model (Cont.)

### The ISO Cybersecurity Model and the States of Data

- Different groups within an organization may be responsible for data in each of the various states.
- For example, the network security group is responsible for data during transmission.
- Programmers and data entry people are responsible for data during processing.
- The hardware and server support specialists are responsible for stored data. The ISO Controls specifically address security objectives for data in each of the three states.

ISO/IEC Controls Provide Direction

ISO/IEC Controls Directly Associated To CIA Principles

ISO/IEC Controls Reviewed to Determine Applicability



## Security Management Framework

# Using the ISO Cybersecurity Model (Cont.)

### The ISO Cybersecurity Model and Safeguards

- The ISO 27001 control objectives relate directly to the organization's cybersecurity policies, procedures and guidelines which upper management determines.
- The ISO 27002 controls provide technical direction. For example, upper management establishes a policy specifying the protection of all data coming in to or out of the organization. Implementing the technology to meet the policy objectives would not involve upper management.
- It is the responsibility of IT professionals to properly implement and configure the equipment used to fulfill the policy directives set by upper management.

ISO/IEC 27000

ISO/IEC 27001

ISO/IEC 27002

## 2.6 Chapter Summary





# Chapter Summary

## Summary

- This chapter discussed the three dimensions of the cybersecurity sorcery cube. The central responsibility of a cybersecurity wizard is to protect an organization's systems and data.
- The chapter explained how each of the three dimensions contributes to that effort.
- The chapter also discussed the ISO cybersecurity model. The model represents an international framework to standardize the management of information systems.
- This chapter explored the twelve domains. The model provides control objectives that guide the high-level design and implementation of a comprehensive information security management system (ISMS).
- The chapter also discussed how security professionals use controls to identify the technologies, devices, and products to protect the organization.
- If you would like to further explore the concepts in this chapter, please check out the Additional Resources and Activities page in Student Resources.

# Cisco | Networking Academy®

## Mind Wide Open™





## Instructor Materials

### Chapter 3: Malware and Malicious Code



**Cybersecurity Essentials v1.0**

**Cisco Networking Academy®**  
Mind Wide Open™

## Chapter 3: Malware and Malicious Code



## Cybersecurity Essentials v1.0



# Chapter 3 - Sections & Objectives

## 3.1 Malware and Malicious Code

Differentiate the types of malware and malicious code.

## 3.2 Trickery

Describe the tactics, techniques and procedures used by cyber criminals.

## 3.3 Attacks

Compare the different methods used in social engineering.

Compare different types of cyberattacks.

## 3.1 Malware and Malicious Code



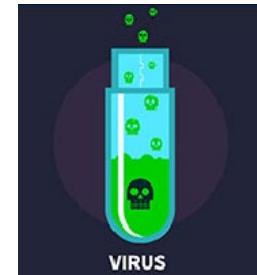


# Malware and Malicious Code

## Types of Malware

Cyber criminals target user's end devices through the installation of malware.

**Viruses** - A virus is malicious executable code attached to another executable file, such as a legitimate program. Most viruses require end-user initiation, and can activate at a specific time or date.



**Worms** - Worms are malicious code that replicates by independently exploiting vulnerabilities in networks. Worms usually slow down networks. Whereas a virus requires a host program to run, worms can run by themselves. Other than the initial infection, worms no longer require user participation.



**Trojan horse** - A Trojan horse is malware that carries out malicious operations under the guise of a desired operation such as playing an online game. This malicious code exploits the privileges of the user that runs it. A Trojan horse differs from a virus because the Trojan binds itself to non-executable files, such as image files, audio files, or games.





## Malware and Malicious Code

# Types of Malware (Cont.)

- **Logic Bomb** - A logic bomb is a malicious program that uses a trigger to awaken the malicious code. For example, triggers can be dates, times, other programs running, or the deletion of a user account. The logic bomb remains inactive until that trigger event happens. Once activated, a logic bomb implements a malicious code that causes harm to a computer.
- **Ransomware** - Ransomware holds a computer system, or the data it contains, captive until the target makes a payment. Ransomware usually works by encrypting data in the computer with a key unknown to the user.
- **Backdoors and Rootkits** - A backdoor or rootkit refers to the program or code introduced by a criminal who has compromised a system. The backdoor bypasses the normal authentication used to access a system. A rootkit modifies the operating system to create a backdoor. Attackers then use the backdoor to access the computer remotely.





## Malware and Malicious Code

# Email and Browser Attacks (Cont.)

Email is a universal service used by billions worldwide.

As one of the most popular services, email has become a major vulnerability to users and organizations.

**Spam** - Spam, also known as junk mail, is unsolicited email. In most cases, spam is a method of advertising. However, spam can send harmful links, malware, or deceptive content.

**Spyware** - Spyware is software that enables a criminal to obtain information about a user's computer activities.

Spyware often includes activity trackers, keystroke collection, and data capture. In an attempt to overcome security measures, spyware often modifies security settings.



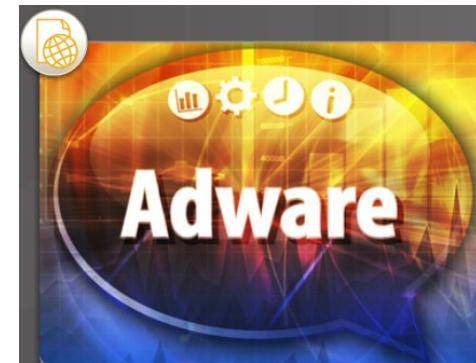


## Malware and Malicious Code

# Email and Browser Attacks (Cont.)

**Adware** - Adware typically displays annoying pop-ups to generate revenue for its authors. The malware may analyze user interests by tracking the websites visited. It can then send pop-up advertising pertinent to those sites.

**Scareware** - Scareware persuades the user to take a specific action based on fear. Scareware forges pop-up windows that resemble operating system dialogue windows.





## Malware and Malicious Code

# Email and Browser Attacks (Cont.)

**Phishing** - Phishing is a form of fraud. Cyber criminals use email, instant messaging, or other social media to try to gather information such as login credentials or account information by masquerading as a reputable entity or person. Phishing occurs when a malicious party sends a fraudulent email disguised as being from a legitimate, trusted source. The message intent is to trick the recipient into installing malware on his or her device or into sharing personal or financial information.

**Spear phishing** - Spear phishing is a highly targeted phishing attack. While phishing and spear phishing both use emails to reach the victims, spear phishing sends customized emails to a specific person.





## Malware and Malicious Code

# Email and Browser Attacks (Cont.)

**Vishing** - Vishing is phishing using voice communication technology. Criminals can spoof calls from legitimate sources using voice over IP (VoIP) technology. Victims may also receive a recorded message that appears legitimate.

**Pharming** - Pharming is the impersonation of a legitimate website in an effort to deceive users into entering their credentials.

**Whaling** - Whaling is a phishing attack that targets high profile targets within an organization such as senior executives.





## Malware and Malicious Code

# Email and Browser Attacks (Cont.)

**Plugins** - The Flash and Shockwave plugins from Adobe enable the development of interesting graphic and cartoon animations that greatly enhance the look and feel of a web page. Plugins display the content developed using the appropriate software.

**SEO Poisoning** - Search engines such as Google work by ranking pages and presenting relevant results based on users' search queries. Depending on the relevancy of web site content, it may appear higher or lower in the search result list. SEO, short for Search Engine Optimization, is a set of techniques used to improve a website's ranking by a search engine. While many legitimate companies specialize in optimizing websites to better position them, SEO poisoning uses SEO to make a malicious website appear higher in search results.

**Browser Hijacker** - A browser hijacker is malware that alters a computer's browser settings to redirect the user to websites paid for by the cyber criminals' customers. Browser hijackers usually install without the user's permission and is usually part of a drive-by download.

## 3.2 Trickery





# Trickery

## The Art of Trickery

**Social Engineering** - Social engineering is a completely non-technical means for a criminal to gather information on a target. Social engineering is an attack that attempts to manipulate individuals into performing actions or divulging confidential information.

Social engineers often rely on people's willingness to be helpful but also prey on people's weaknesses. These are some types of social engineering attacks:

**Pretexting** - This is when an attacker calls an individual and lies to them in an attempt to gain access to privileged data. An example involves an attacker who pretends to need personal or financial data in order to confirm the identity of the recipient.

**Something for Something (Quid pro quo)** - This is when an attacker requests personal information from a party in exchange for something, like a gift.

Hi this is Amy from the help desk. We need to upgrade the software on your computer after work hours. What is your user ID and password? You can change the password tomorrow when you log in.



Social Engineer

Ok, my user ID and password are...



Unsuspecting Employee at XYZ Corporation



## Trickery

# Types of Trickery

**Shoulder Surfing and Dumpster Diving** – refers to picking up PINs, access codes or credit card numbers. An attacker can be in close proximity to his victim or the attacker can use binoculars or closed circuit cameras to shoulder surf.

**Impersonation and Hoaxes** - Impersonation is the action of pretending to be someone else. For example, a recent phone scam targeted taxpayers. A criminal, posing as an IRS employee, told the victims that they owed money to the IRS.

**Piggybacking and Tailgating** - Piggybacking occurs when a criminal tags along with an authorized person to gain entry into a secure location or a restricted area. Tailgating is another term that describes the same practice.

**Online, Email, and Web-based Trickery** - Forwarding hoax emails and other jokes, funny movies, and non-work-related emails at work may violate the company's acceptable use policy and result in disciplinary actions.



### 3.3 Attacks





## Attacks

# Types of Cyber Attacks

**Denial-of-Service (DoS) Attacks** - are a type of network attack. A DoS attack results in some sort of interruption of network services to users, devices, or applications. DoS attacks are a major risk because they can easily interrupt communication and cause significant loss of time and money. These attacks are relatively simple to conduct, even by an unskilled attacker.

**Sniffing** - Sniffing is similar to eavesdropping on someone. It occurs when attackers examine all network traffic as it passes through their NIC, independent of whether or not the traffic is addressed to them or not. Criminals accomplish network sniffing with a software application, hardware device, or a combination of the two.

**Spoofing** - Spoofing is an impersonation attack, and it takes advantage of a trusted relationship between two systems. If two systems accept the authentication accomplished by each other, an individual logged onto one system might not go through an authentication process again to access the other system.



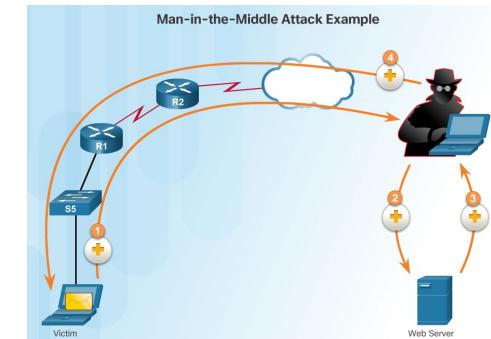
## Attacks

# Types of Cyber Attacks

**Man-in-the-middle** - A criminal performs a man-in-the-middle (MitM) attack by intercepting communications between computers to steal information crossing the network. The criminal can also choose to manipulate messages and relay false information between hosts since the hosts are unaware that a modification to the messages occurred. MitM allows the criminal to take control over a device without the user's knowledge.

**Zero-Day Attacks** - A zero-day attack, sometimes referred to as a zero-day threat, is a computer attack that tries to exploit software vulnerabilities that are unknown or undisclosed by the software vendor. The term zero hour describes the moment when someone discovers the exploit.

**Keyboard Logging** - Keyboard logging is a software program that records or logs the keystrokes of the user of the system. Criminals can implement keystroke loggers through software installed on a computer system or through hardware physically attached to a computer. The criminal configures the key logger software to email the log file. The keystrokes captured in the log file can reveal usernames, passwords, websites visited, and other sensitive information.





## Attacks

# Wireless and Mobile Attacks (Cont.)

### Grayware and SMiShing

- Grayware includes applications that behave in an annoying or undesirable manner. Grayware may not have recognizable malware concealed within, but it still may pose a risk to the user. Grayware is becoming a problem area in mobile security with the popularity of smartphones.
- SMiShing is short for SMS phishing. It uses Short Message Service (SMS) to send fake text messages. The criminals trick the user into visiting a website or calling a phone number. Unsuspecting victims may then provide sensitive information such as credit card information. Visiting a website might result in the user unknowingly downloading malware that infects the device.





## Attacks

# Wireless and Mobile Attacks (Cont.)

**Rogue Access Points** - A rogue access point is a wireless access point installed on a secure network without explicit authorization. A rogue access point can be set up in two ways.

**RF Jamming** - Wireless signals are susceptible to electromagnetic interference (EMI), radio-frequency interference (RFI), and may even be susceptible to lightning strikes or noise from fluorescent lights. Wireless signals are also susceptible to deliberate jamming. Radio frequency (RF) jamming disrupts the transmission of a radio or satellite station so that the signal does not reach the receiving station.

**Bluejacking and Bluesnarfing** - Bluejacking is the term used for sending unauthorized messages to another Bluetooth device. Bluesnarfing occurs when the attacker copies the victim's information from his device. This information can include emails and contact lists.





## Attacks

# Wireless and Mobile Attacks (Cont.)

### WEP and WPA Attacks

**Wired Equivalent Privacy (WEP)** is a security protocol that attempted to provide a wireless local area network (WLAN) with the same level of security as a wired LAN. Since physical security measures help to protect a wired LAN, WEP seeks to provide similar protection for data transmitted over the WLAN with encryption.

- WEP uses a key for encryption.
- There is no provision for key management with WEP, so the number of people sharing the key will continually grow.

**Wi-Fi Protected Access (WPA) and then WPA2** came out as improved protocols to replace WEP. WPA2 does not have the same encryption problems because an attacker cannot recover the key by observing traffic.

- WPA2 is susceptible to attack because cyber criminals can analyze the packets going between the access point and a legitimate user.
- Cyber criminals use a packet sniffer and then run attacks offline on the passphrase.



## Attacks

# Wireless and Mobile Attacks (Cont.)

### Defending Against Wireless and Mobile Device Attacks

There are several steps to take to defend against wireless and mobile device attacks.

- Most WLAN products use default settings. Take advantage of the basic wireless security features such as authentication and encryption by changing the default configuration settings.
- Restrict access point placement with the network by placing these devices outside the firewall or within a demilitarized zone (DMZ) which contains other untrusted devices such as email and web servers.
- WLAN tools such as NetStumbler may discover rogue access points or unauthorized workstations. Develop a guest policy to address the need when legitimate guests need to connect to the Internet while visiting. For authorized employees, utilize a remote access virtual private network (VPN) for WLAN access.



## Attacks

# Application Attacks

**Cross-site scripting (XSS)** - is a vulnerability found in web applications. XSS allows criminals to inject scripts into the web pages viewed by users. This script can contain malicious code. Cross-site scripting has three participants: the criminal, the victim, and the website. The cyber-criminal does not target a victim directly. The criminal exploits vulnerability within a website or web application. Criminals inject client-side scripts into web pages viewed by users, the victims.

**Code Injections Attacks** - One way to store data at a website is to use a database. There are several different types of databases such as a Structured Query Language (SQL) database or an Extensible Markup Language (XML) database. Both XML and SQL injection attacks exploit weaknesses in the program such as not validating database queries properly.

**Buffer Overflow** - A buffer overflow occurs when data goes beyond the limits of a buffer. Buffers are memory areas allocated to an application. By changing data beyond the boundaries of a buffer, the application accesses memory allocated to other processes. This can lead to a system crash, data compromise, or provide escalation of privileges.



## Attacks

# Application Attacks

**Remote Code Executions** vulnerabilities allow a cybercriminal to execute malicious code and take control of a system with the privileges of the user running the application. Remote code execution allows a criminal to execute any command on a target machine.

**ActiveX Controls and Java** controls provide the capability of a plugin to Internet Explorer.

- ActiveX controls are pieces of software installed by users to provide extended capabilities. Third parties write some ActiveX controls and they may be malicious. They can monitor browsing habits, install malware, or log keystrokes. Active X controls also work in other Microsoft applications.
- Java operates through an interpreter, the Java Virtual Machine (JVM). The JVM enables the Java program's functionality. The JVM sandboxes or isolates untrusted code from the rest of the operating system. There are vulnerabilities, which allow untrusted code to go around the restrictions imposed by the sandbox.



## Attacks

# Application Attacks

### Defending Against Application Attacks

- The first line of defense against an application attack is to write solid code.
- Regardless of the language used, or the source of outside input, prudent programming practice is to treat all input from outside a function as hostile.
- Validate all inputs as if they were hostile.
- Keep all software including operating systems and applications up to date, and do not ignore update prompts.
- Not all programs update automatically, so at the very least, always select the manual update option.

## 3.4 Chapter Summary





# Chapter Summary

## Summary

Threats, vulnerabilities, and attacks are the central focus of the cybersecurity wizards.

- This chapter discussed the various cybersecurity attacks that cyber criminals launch.
- The chapter explained the threat of malware and malicious code.
- The chapter discussed the types of trickery involved with social engineering. Maneuvering explained the types of attacks that both wired and wireless networks experience.
- Finally, the chapter discussed the vulnerabilities presented by application attacks.

Understanding the types of possible threats allows an organization to identify the vulnerabilities that make it a target. The organization can then learn how to defend itself against cybersecurity trickery and maneuvering.







## Instructor Materials

### Chapter 4: The Art of Protecting Secrets



**Cybersecurity Essentials v1.0**

**Cisco Networking Academy®**  
Mind Wide Open™



## Chapter 4: The Art of Protecting Secrets



## Cybersecurity Essentials v1.0

Cisco | Networking Academy®  
Mind Wide Open™



# Chapter 4 - Sections & Objectives

## 4.1 Cryptography

Explain how encryption techniques protect confidentiality.

## 4.2 Access Control

Describe access control techniques used to protect confidentiality.

## 4.3 Obscuring Data

Describe the concept of obscuring data.

## 4.1 Cryptography





# Cryptography Overview

Cryptology is the science of making and breaking secret codes. Cryptography is a way to store and transmit data so only the intended recipient can read or process it. Modern cryptography uses computationally secure algorithms to make sure that cyber criminals cannot easily compromise protected information.

The history of cryptography started in diplomatic circles thousands of years ago. Messengers from a king's court took encrypted messages to other courts. Occasionally, other courts not involved in the communication, attempted to steal messages sent to a kingdom they considered an adversary. Not long after, military commanders started using encryption to secure messages.

Each encryption method uses a specific algorithm, called a cipher, to encrypt and decrypt messages. A cipher is a series of well-defined steps used to encrypt and decrypt messages. There are several methods of creating ciphertext:

- Transposition
- Substitution
- One-time pad



# Cryptography Overview (Cont.)

## Two Types of Encryption

There are two classes of encryption algorithms:

- **Symmetric algorithms** - These algorithms use the same pre-shared key, sometimes called a secret key pair, to encrypt and decrypt data. Both the sender and receiver know the pre-shared key before any encrypted communication begins.
- **Asymmetric algorithms** - Asymmetrical encryption algorithms use one key to encrypt data and a different key to decrypt data. One key is public and the other is private. In a public-key encryption system, any person can encrypt a message using the public key of the receiver, and the receiver is the only one that can decrypt it using his private key. Parties exchange secure messages without needing a pre-shared key. Asymmetric algorithms are more complex. These algorithms are resource intensive and slower to execute.



## Cryptography

# Private-Key Encryption

**Symmetrical Encryption Process** - Symmetric algorithms use pre-shared key to encrypt and decrypt data, a method also known as private-key encryption. Numerous encryption systems use symmetric encryption. Some of the common encryption standards that use symmetric encryption include the following:

- **3DES (Triple DES):** Digital Encryption Standard (DES) is a symmetric block cipher with 64-bit block size that uses a 56-bit key. Triple DES encrypts data three times and uses a different key for at least one of the three passes, giving it a cumulative key size of 112-168 bits.
- **IDEA:** The International Data Encryption Algorithm (IDEA) uses 64-bit blocks and 128-bit keys. IDEA performs eight rounds of transformations on each of the 16 blocks that results from dividing each 64-bit block. IDEA was the replacement for DES, and now PGP (Pretty Good Privacy) uses it.
- **AES:** The Advanced Encryption Standard (AES) has a fixed block size of 128-bits with a key size of 128, 192, or 256 bits. The National Institute of Standards and Technology (NIST) approved the AES algorithm in December 2001. The U.S. government uses AES to protect classified information.



# Cryptography

## Public-Key Encryption

**Asymmetrical Encryption Process** - Asymmetric encryption, also called public-key encryption, uses one key for encryption that is different from the key used for decryption. A criminal cannot calculate the decryption key based on knowledge of the encryption key, and vice versa, in any reasonable amount of time. The asymmetric algorithms include:

- **RSA (Rivest\_Shamir-Adleman)** - uses the product of two very large prime numbers with an equal length of between 100 and 200 digits. Browsers use RSA to establish a secure connection.
- **Diffie-Hellman** - provides an electronic exchange method to share the secret key. Secure protocols, such as Secure Sockets Layer (SSL), Transport Layer Security (TLS), Secure Shell (SSH), and Internet Protocol Security (IPsec), use Diffie-Hellman.
- **ElGamal** - uses the U.S. government standard for digital signatures. This algorithm is free to use because no one holds the patent.
- **Elliptic Curve Cryptography (ECC)** - uses elliptic curves as part of the algorithm. In the U.S., the National Security Agency uses ECC for digital signature generation and key exchange.

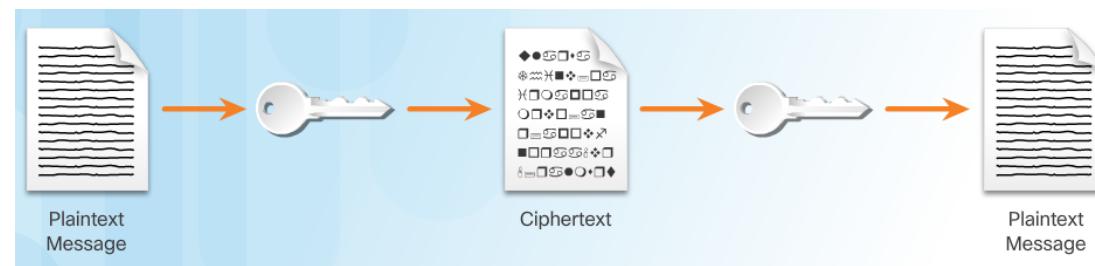


## Cryptography

# Symmetrical versus Asymmetrical Encryption

### Comparing Encryption Types

- It is important to understand the differences between symmetric and asymmetric encryption methods. Symmetric encryption systems are more efficient and can handle more data. However, key management with symmetric encryption systems is more problematic and harder to manage.
- Asymmetric cryptography is more efficient at protecting the confidentiality of small amounts of data, and its size and speed make it more secure for tasks such as electronic key exchange which is a small amount of data rather than encrypting large blocks of data.





## Cryptography

# Symmetrical versus Asymmetrical Encryption

### Application

There are many applications for both symmetric and asymmetric algorithms. A one-time password-generating token is a hardware device that uses cryptography to generate a one-time password. A one-time password is an automatically generated numeric or alphanumeric string of characters that authenticates a user for one transaction of one session only. The number changes every 30 seconds or so. The session password appears on a display and the user enters the password.

- The electronic payment industry uses 3DES.
- Operating systems use DES to protect user files and system data with passwords.
- Most encrypting file systems, such as NTFS, use AES.



## Cryptography

# Symmetrical versus Asymmetrical Encryption

### Application

Four protocols use asymmetric key algorithms:

- Internet Key Exchange (IKE), which is a fundamental component of IPsec Virtual Private Networks (VPNs).
- Secure Socket Layer (SSL), which is a means of implementing cryptography into a web browser.
- Secure Shell (SSH), which is a protocol that provides a secure remote access connection to network devices.
- Pretty Good Privacy (PGP), which is a computer program that provides cryptographic privacy and authentication to increase the security of email communications.



## Cryptography

# Symmetrical versus Asymmetrical Encryption

### Application

A VPN is a private network that uses a public network, usually the Internet, to create a secure communication channel. A VPN connects two endpoints such as two remote offices over the Internet to form the connection.

- VPNs use IPsec. IPsec is a suite of protocols developed to achieve secure services over networks.
- IPsec services allow for authentication, integrity, access control, and confidentiality.
- With IPsec, remote sites can exchange encrypted and verified information.
- Data in use is a growing concern to many organizations. When in use, data no longer has any protection because the user needs to open and change the data.
- System memory holds data in use and it can contain sensitive data such as the encryption key.
- If criminals compromise data in use, they will have access to data at rest and data in motion.

## 4.2 Access Control





## Access Control

# Types of Access Control

**Physical Access Controls** - actual barriers deployed to prevent direct contact with systems. The goal is to prevent unauthorized users from gaining physical access to facilities, equipment, and other organizational assets. Physical access control determines who can enter (or exit), where they can enter (or exit), and when they can enter (or exit).

**Logical Access Controls** - hardware and software solutions used to manage access to resources and systems. These technology-based solutions include tools and protocols that computer systems use for identification, authentication, authorization, and accountability.

**Administrative Access Controls** - policies and procedures defined by organizations to implement and enforce all aspects of controlling unauthorized access. Administrative controls focus on personnel and business practices.





## Access Control

# Access Control Strategies

**Mandatory access control (MAC)** - restricts the actions that a subject can perform on an object. A subject can be a user or a process. An object can be a file, a port, or an input/output device. An authorization rule enforces whether or not a subject can access the object.

**Discretionary access control (DAC)** - DAC grants or restricts object access determined by the object's owner. As the name implies, controls are discretionary because an object owner with certain access permissions can pass on those permissions to another subject.

**Role-based access control (RBAC)** - is based on the role of the subject. Roles are job functions within an organization. Specific roles require permissions to perform certain operations. Users acquire permissions through their role. RBAC can work in combination with DAC or MAC by enforcing the policies of either one.

**Rule-based access control** - uses access control lists (ACLs) to help determine whether to grant access. A series of rules is contained in the ACL, as shown in the figure. The determination of whether to grant access depends on these rules. An example of such a rule is one that states that no employee may have access to the payroll file after hours or on weekends.



# Access Control Identification

Identification enforces the rules established by the authorization policy:

- A subject requests access to a system resource.
- Every time the subject requests access to a resource, the access controls determine whether to grant or deny access.
- Cybersecurity policies determine which identification controls should be used.
- The sensitivity of the information and information systems determine how stringent the controls.
- The increase in data breaches has forced many organizations to strengthen their identification controls.





## Access Control

# Authentication Methods

**What You Know** - Passwords, passphrases, or PINs are all examples of something that the user knows. Passwords are the most popular method used for authentication.

**What You Have** - Smart cards and security key fobs are both examples of something that users have in their possession.

**Who You Are** - A unique physical characteristic, such as a fingerprint, retina, or voice, that identifies a specific user is called biometrics.

**Multi-factor Authentication** - Multi-factor authentication uses at least two methods of verification. A security key fob is a good example. The two factors are something you know, such as a password, and something you have, such as a security key fob.





## Access Control Authorization

Authorization controls what a user can and cannot do on the network after successful authentication:

- After a user proves his or her identity, the system checks to see what network resources the user can access and what the users can do with the resources.
- Authorization uses a set of attributes that describes the user's access to the network.
- The system compares these attributes to the information contained within the authentication database, determines a set of restrictions for that user, and delivers it to the local router where the user is connected.
- Defining authorization rules is the first step in controlling access. An authorization policy establishes these rules.





## Access Control

# Accountability

Accountability traces an action back to a person or process making the change to a system, collects this information, and reports the usage data:

- The organization can use this data for such purposes as auditing or billing.
- The collected data might include the log in time for a user, whether the user log in was a success or failure, or what network resources the user accessed.
- This allows an organization to trace actions, errors, and mistakes during an audit or investigation.
- Implementing accountability consists of technologies, policies, procedures, and education.
- Log files provide detailed information based on the parameters chosen.



## Access Control

# Types of Security Controls

**Preventative Controls** - Prevent means to keep something from happening. Preventative access controls stop unwanted or unauthorized activity from happening.

**Deterrent Controls** - A deterrent is the opposite of a reward. A reward encourages individuals to do the right thing, while a deterrent discourages them from doing the wrong thing. Cybersecurity professionals and organizations use deterrents to limit or mitigate an action or behavior. Deterrents do not always stop these actions.

**Detective Controls** - Detection is the act or process of noticing or discovering something. Access control detections identify different types of unauthorized activity. Detection systems can be very simple, such as a motion detector or security guard. They can also be more complex, such as an intrusion detection system.





## Access Control

# Types of Security Controls

**Corrective Controls** - Corrective counteracts something that is undesirable. Organizations put corrective access controls in place after a system experiences a threat. Corrective controls restore the system back to a state of confidentiality, integrity, and availability. They can also restore systems to normal after unauthorized activity occurs.

**Recovery Controls** - Recovery is a return to a normal state. Recovery access controls restore resources, functions, and capabilities after a violation of a security policy. Recovery controls can repair damage, in addition to stopping any further damage. These controls have more advanced capabilities over corrective access controls.

**Compensative Controls** - Compensate means to make up for something. Compensative access controls provide options to other controls to bolster enforcement in support of a security policy. A compensative control can also be a substitution used in place of a control that is not possible under the circumstances.

## 4.3 Obscuring Data





## Obscuring Data Data Masking

Data Masking is a technology that secures data by replacing sensitive information with a non-sensitive version. The non-sensitive version looks and acts like the original. This means that a business process can use non-sensitive data and there is no need to change the supporting applications or data storage facilities.

In the most common use case, masking limits the propagation of sensitive data within IT systems by distributing surrogate data sets for testing and analysis.

There are data masking techniques that can ensure that data remains meaningful but changed enough to protect it:

- **Substitution** - replaces data with authentic looking values to apply anonymity to the data records.
- **Shuffling** - derives a substitution set from the same column of data that a user wants to mask. This technique works well for financial information in a test database, for example.



## Obscuring Data

# Steganography

Steganography conceals data (the message) in another file such as a graphic, audio, or other text file.

The advantage of steganography over cryptography is that the secret message does not attract any special attention. No one would ever know that a picture actually contained a secret message by viewing the file either electronically or in hardcopy.

There are several components involved in hiding data:

- There is the embedded data, which is the secret message.
- Cover-text (or cover-image or cover-audio) hides the embedded data producing the stego-text (or stego-image or stego-audio).
- A stego-key controls the hiding process.



## Obscuring Data

# Data Obfuscation

**Data obfuscation** - is the use and practice of data masking and steganography techniques in the cybersecurity and cyber intelligence profession:

- Obfuscation is the art of making the message confusing, ambiguous, or harder to understand.
- A system may purposely scramble messages to prevent unauthorized access to sensitive information.
- Software watermarking protects software from unauthorized access or modification.
- Software watermarking inserts a secret message into the program as proof of ownership.
- The secret message is the software watermark. If someone tries to remove the watermark, the result is nonfunctional code.

## 4.4 Chapter Summary





# Chapter Summary

## Summary

- This chapter discussed the principles of cryptology used to secure communications.
- The chapter explained both symmetric and asymmetric encryption algorithms, compared the two algorithms, and provided examples of their use.
- The chapter explained how access control prevents unauthorized access to a building, a room, a system, or a file using identification, authentication, authorization, and accountability. In addition, the chapter also described the different access control models and access control types.
- The chapter concluded by discussing the various ways users mask data. Data obfuscation and steganography are two techniques used to accomplish data masking.

# Cisco | Networking Academy®

Mind Wide Open™





## Instructor Materials

### Chapter 5: The Art of Ensuring Integrity



**Cybersecurity Essentials v1.0**

**Cisco Networking Academy®**  
Mind Wide Open™



## Chapter 5: The Art of Ensuring Integrity



## Cybersecurity Essentials v1.0

Cisco | Networking Academy®  
Mind Wide Open™



# Chapter 5 - Sections & Objectives

## 5.1 Types of Data Integrity Controls

Explain the processes used to ensure integrity.

## 5.2 Digital Signatures

Explain the purpose of digital signatures.

## 5.3 Certificates

Explain the purpose of digital certificates.

## 5.4 Database Integrity Enforcement

Explain the need for database integrity enforcement.

## 5.1 Types of Data Integrity Controls





## Types of Data Integrity Controls

# Hashing Algorithms

- Hashing is a tool that ensures data integrity by taking binary data (the message) and producing a fixed-length representation called the hash value or message digest.
- Hashing is a one-way mathematical function that is relatively easy to compute, but significantly harder to reverse. Grinding coffee beans is a good analogy of a one-way function. It is easy to grind coffee beans, but it is almost impossible to put all of the tiny pieces back together to rebuild the original beans.

A cryptographic hash function has the following properties:

- The input can be any length.
- The output has a fixed length.
- The hash function is one way and is not reversible.
- Two different input values will always result in different hash values.

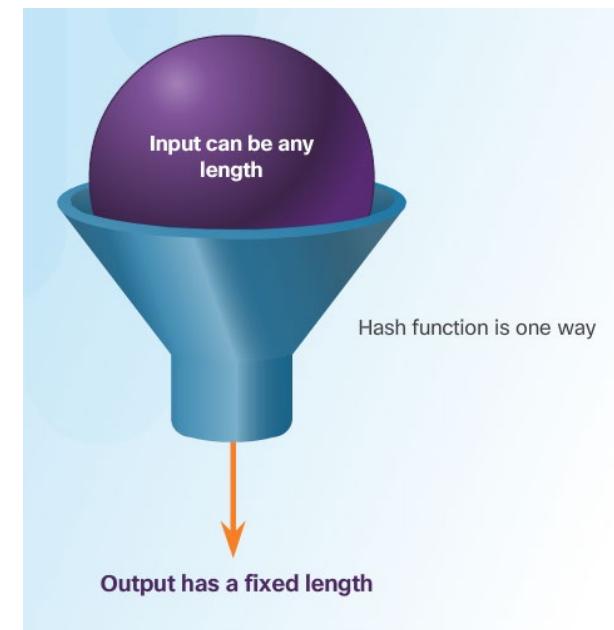


# Types of Data Integrity Controls

## Hashing Algorithms

There are many modern hashing algorithms widely used today. Two of the most popular are MD5 and SHA.

- **Message Digest 5 (MD5) Algorithm** - is a hash algorithm developed by Ron Rivest that produces a 128-bit hash value.
- **Secure Hash Algorithm (SHA)** – was developed by the U.S. National Institute of Standards and Technology (NIST) and can be implemented in different strengths:
  - SHA-224 (224 bit)
  - SHA-256 (256 bit)
  - SHA-384 (384 bit)
  - SHA-512 (512 bit)





# Types of Data Integrity Controls

## Salting

- Salting is used to make hashing more secure. If two users have the same password, they will also have the same password hashes. A salt, which is a random string of characters, is an additional input to the password before hashing.
- This creates a different hash result for the two passwords as shown in the figure. A database stores both the hash and the salt.

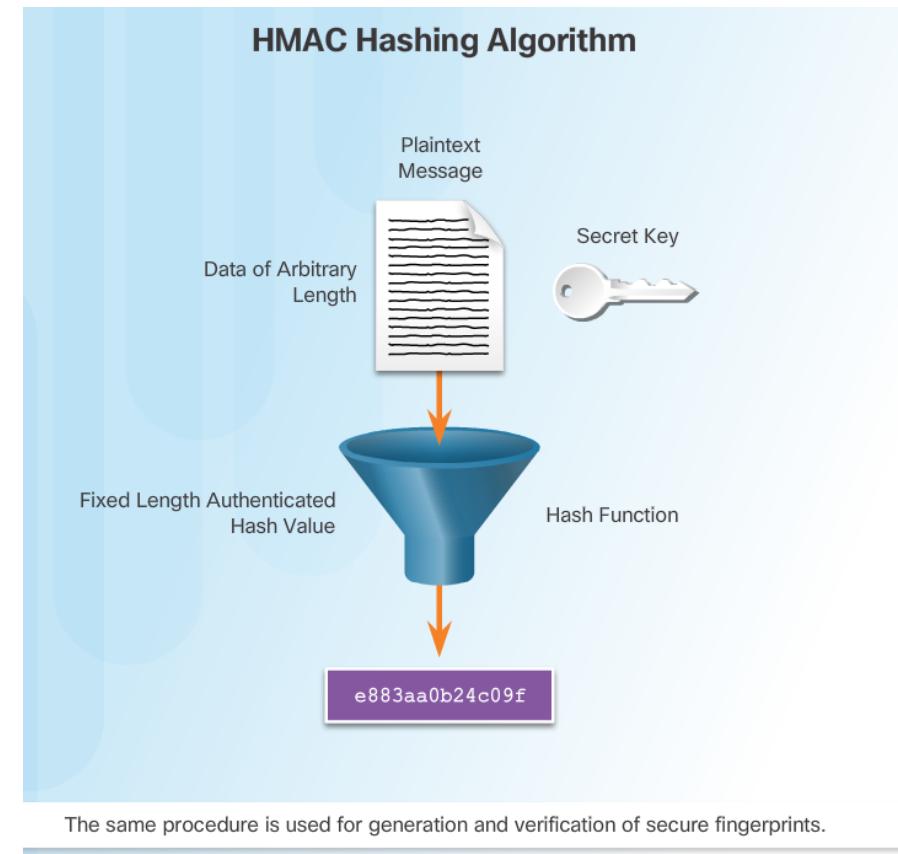
Salt	Hash Value
Hash ("password" + <b>QxLUF1bIAdeQX</b> )	= <b>b3bad1e5324f057753a4b8d7cef293e4</b>
Hash ("password" + <b>R9PeIC7sxQXb8</b> )	= <b>713c7beb54841a26a7c81eb06d6cf066</b>



# Types of Data Integrity Controls

## HMAC

- HMACs strengthens hashing algorithms by using an additional secret key as input to the hash function.
- The use of HMAC goes a step further than just integrity assurance by adding authentication.
- An HMAC uses a specific algorithm that combines a cryptographic hash function with a secret key, as shown in the figure.



## 5.2 Digital Signatures





# Digital Signatures

## Signatures and the Law

- Digital signatures provide the same functionality as handwritten signatures for electronic documents.
- A digital signature is used to determine if someone edits a document after the user signs it.
- A digital signature is a mathematical method used to check the authenticity and integrity of a message, digital document, or software.
- In many countries, digital signatures have the same legal importance as a manually signed document.
- Digital signatures also provide repudiation.

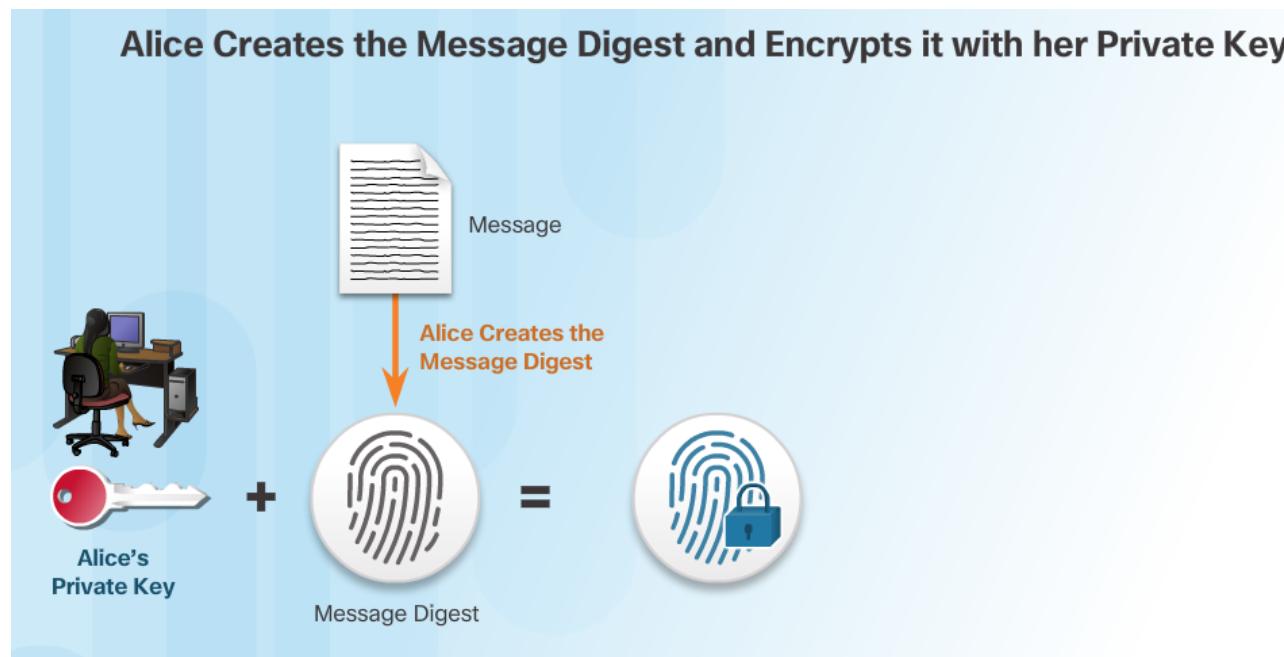




## Digital Signatures

# How Digital Signature Technology Works

Asymmetric cryptography is the basis for digital signatures. A public key algorithm like RSA generates two keys: one private and the other public. The keys are mathematically related.



## 5.3 Certificates



Cisco | Networking Academy®  
Mind Wide Open™



## Certificates

# The Basics of Digital Certificates

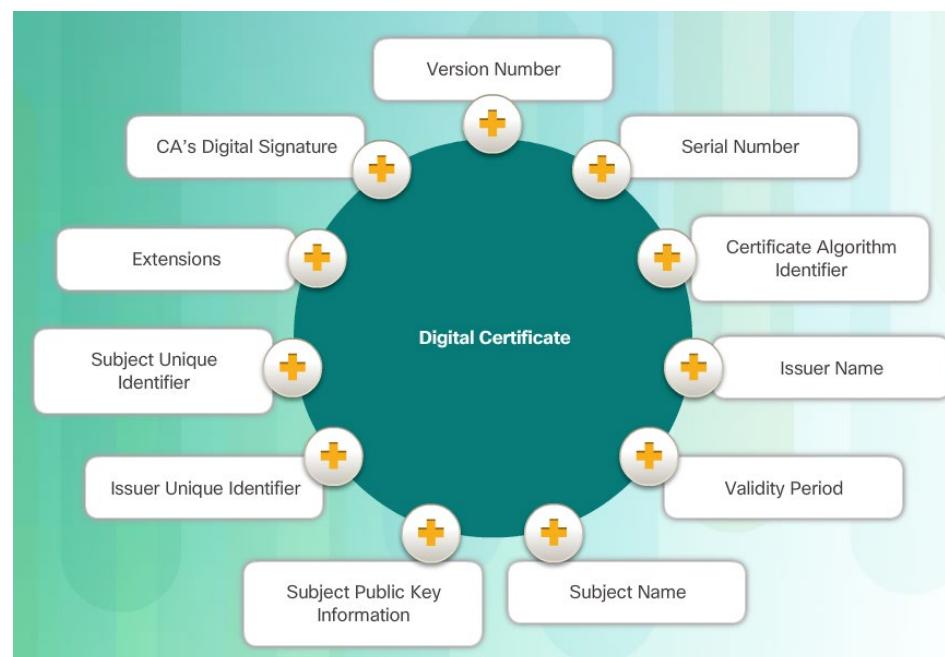
- A digital certificate is equivalent to an electronic passport.
- Digital certificates enable users, hosts, and organizations to exchange information securely over the Internet.
- A digital certificate authenticates and verifies that users sending a message are who they claim to be.
- Digital certificates can also provide confidentiality for the receiver with the means to encrypt a reply.



## Certificates

# Constructing a Digital Certificate

- Digital certificate must follow a standard structure so that any entity can read and understand it regardless of the issuer.
- The X.509 is the standard for construction of digital certificates and the public key infrastructure (PKI) used to manage digital certificates.
- PKI is the policies, roles, and procedures required to create, manage, distribute, use, store, and revoke digital certificates.



## 5.4 Database Integrity Enforcement





# Database Integrity Enforcement

# Database Integrity

- Databases provide an efficient way to store, retrieve, and analyze data.
- As data collection increases and data becomes more sensitive, it is important for cybersecurity professionals to protect the growing number of databases.
- Data integrity refers to the accuracy, consistency, and reliability of data stored in a database.

ID	Company	First Name	Last Name
8	Company H	Elizabeth	Andersen
18	Company R	Catherine	Autier Miconi
3	Company C	Thomas	Axen
17	Company Q	Jean Philippe	Bagel
1	Company A	Anna	Bedecs
12	Company L	John	Edwards



# Database Integrity Enforcement

## Database Integrity (Cont.)

The four database integrity rules or constraints are as follows:

- **Entity Integrity:** All rows must have a unique identifier called a Primary Key.
- **Domain Integrity:** All data stored in a column must follow the same format and definition.
- **Referential Integrity:** Table relationships must remain consistent. Therefore, a user cannot delete a record which is related to another one.
- **User-defined Integrity:** A set of rules defined by a user which does not belong to one of the other categories. For example, a customer places a new order. The user first checks to see if this is a new customer. If it is, the user adds the new customer to the customers table.

ID	Company	First Name	Last Name
8	Company H	Elizabeth	Andersen
18	Company R	Catherine	Autier Miconi
3	Company C	Thomas	Axen
17	Company Q	Jean Philippe	Bagel
1	Company A	Anna	Bedecs
12	Company L	John	Edwards

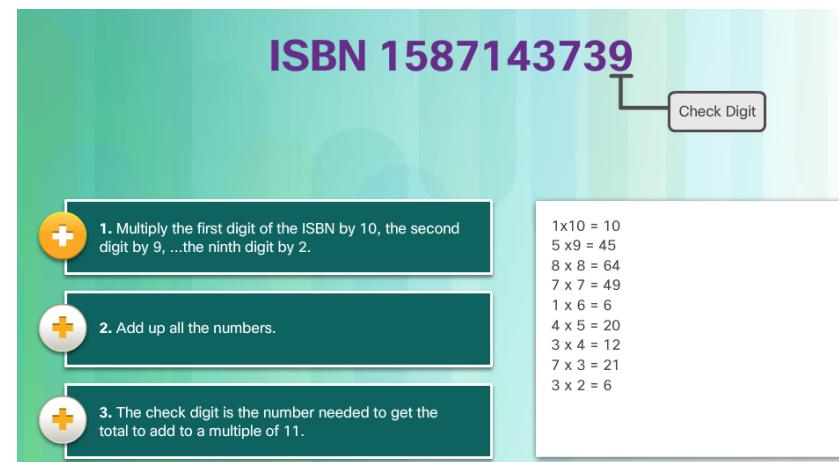


# Database Integrity Enforcement

## Database Validation

A validation rule checks that data falls within the parameters defined by the database designer. A validation rule helps to ensure the completeness, accuracy and consistency of data. The criteria used in a validation rule include the following:

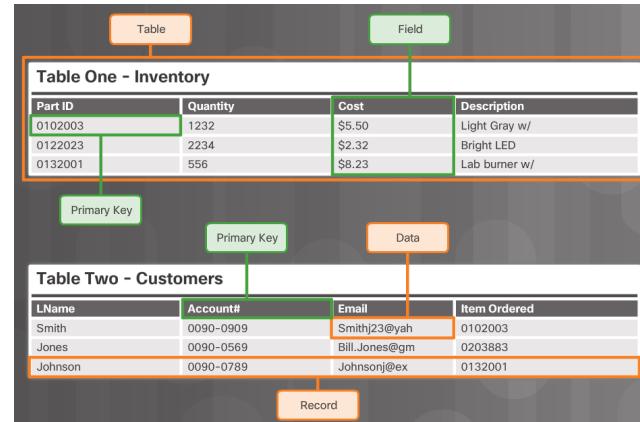
- Size – checks the number of characters in a data item
- Format – checks that the data conforms to a specified format
- Consistency – checks for the consistency of codes in related data items
- Range – checks that data lies within a minimum and maximum value
- Check digit – provides for an extra calculation to generate a check digit for error detection.





# Database Integrity Enforcement

## Database Integrity Requirements



- Maintaining proper filing is critical in maintaining the trustworthiness and usefulness of the data within the database.
- Tables, records, fields, and data within each field make up a database.
- In order to maintain the integrity of the database filing system, users must follow certain rules.
- Entity integrity is an integrity rule, which states that every table must have a primary key and that the column or columns chosen to be the primary key must be unique and not NULL.
- Null in a database signifies missing or unknown values. Entity integrity enables proper organization of data for that record.



# Database Integrity Enforcement

## Database Integrity Requirements (Cont.)

Table One - Inventory			
Part ID	Quantity	Cost	Description
0102003	1232	\$5.50	Light Gray w/
0122023	2234	\$2.32	Bright LED
0132001	556	\$8.23	Lab burner w/

Primary Key

Table Two - Customers			
LName	Account#	Email	Item Ordered
Smith	0090-0909	Smithj23@yahoo	0102003
Jones	0090-0569	Bill.Jones@gm	0203883
Johnson	0090-0789	Johnsonj@ex	0132001

Foreign Key

- Another important integrity check is referential integrity which deals with foreign keys. A foreign key in one table references a primary key in a second table. The primary key for a table uniquely identifies entities (rows) in the table. Referential integrity maintains the integrity of foreign keys.



# Database Integrity Enforcement

## Database Integrity Requirements (Cont.)

SSN 243-27-3361	<ul style="list-style-type: none"><li>Must have nine integers</li><li>Format xxx-xx-xxxx</li><li>Entered or modified by customer only</li><li>Must be validated</li></ul>
Credit Card Number 4539 4769 0728 4479	<ul style="list-style-type: none"><li>Must have sixteen integers</li><li>Format xxxx-xxxx-xxxx-xxxx</li><li>Entered or modified by customer only</li><li>Must be validated</li></ul>
Email Address tortor@ odio.com	<ul style="list-style-type: none"><li>Must have no more than 128 characters</li><li>Format xxxx@xxxx.xxxx</li><li>Entered or modified by customer only</li><li>Validated by email response</li></ul>

- Domain integrity ensures that all the data items in a column fall within a defined set of valid values. Each column in a table has a defined set of values, such as the set of all numbers for credit card numbers, social security numbers, or email addresses. Limiting the value assigned to an instance of that column (an attribute) enforces domain integrity. Domain integrity enforcement can be as simple as choosing the correct data type, length and or format for a column.

## 5.5 Chapter Summary





# Chapter Summary

## Summary

- Chapter five presented the art of integrity which is used to ensure that data remains unchanged by anyone or anything over its entire life cycle.
- The chapter introduced types of data integrity controls including:
  - hashing algorithms
  - password salting
  - keyed-hash message authentication code (HMAC)
- These tools provide a way for cybersecurity specialists to verify the authenticity of messages and documents.
- The chapter concluded with a discussion of database integrity enforcement.
- Having a well-controlled and well-defined data integrity system increases the stability, performance, and maintainability of a database system.

# Cisco | Networking Academy®

## Mind Wide Open™





## Instructor Materials

### Chapter 6: The Realm of Five Nines



**Cybersecurity Essentials v1.0**

**Cisco Networking Academy®**  
Mind Wide Open™



## Chapter 6: The Realm of Five Nines



**Cybersecurity Essentials v1.0**

**Cisco Networking Academy®**  
Mind Wide Open™



# Chapter 6 - Sections & Objectives

## 6.1 High Availability

Explain the concept of high availability.

## 6.2 Measures to Improve Availability

Explain how high availability measures are used to improve availability.

## 6.3 Incident Response

Describe how an incident response plan improves high availability.

## 6.4 Disaster Recovery

Describe how disaster recovery planning plays an important role in implementing high availability.

## 2.1 High Availability





# High Availability The Five Nines

## What is Five Nine?

- Five nines mean that systems and services are available 99.999% of the time. It also means that both planned and unplanned downtime is less than 5.26 minutes per year. High availability refers to a system or component that is continuously operational for a given length of time. To help ensure high availability:
  - Eliminate single points of failure
  - Design for reliability
  - Detect failures as they occur

Availability	Downtime per Year
99%	87 hours 36 mins
99.5%	43 hours 48 mins
99.95%	4 hours 23 mins
99.99%	53 mins
99.999%	5 mins



# High Availability The Five Nines (Cont.)

# **Environments That Require Five Nines**

Although the cost of sustaining high availability may be too costly for some industries, several environments require five nines.

- The finance industry needs to maintain high availability for continuous trading, compliance, and customer trust.
  - Healthcare facilities require high availability to provide around-the-clock care for patients.
  - The public safety industry includes agencies that provide security and services to a community, state, or nation.
  - The retail industry depends on efficient supply chains and the delivery of products to customers. Disruption can be devastating, especially during peak demand times such as holidays.



Finance Industry



## Health Care Facilities



Public Safety



# High Availability The Five Nines (Cont.)

## Threats to Availability

There are many different types of threats to high availability, the threats can range from failure of a mission-critical application to severe storm such as a hurricane or tornado. Threats can also include catastrophic event such as a terrorist attack, building bombing, or building fires.

## Designing a High Availability System

High availability incorporates three major principles to achieve the goal of uninterrupted access to data and services:

- Elimination or reduction of single-points of failure
- System Resiliency
- Fault Tolerance



Finance Industry



Health Care Facilities



Public Safety

## 2.2 Measures to Improve Availability





## Measures to Improve Availability Asset Management

An organization needs to know what hardware and software assets they have in order to protect them. Asset management includes a complete inventory of hardware and software. This means that the organization needs to know all of components that can be subject to security risks, including:

- Every hardware system
- Every operating system
- Every hardware network device
- Every network device operating system
- Every software application
- All firmware
- All language runtime environments
- All individual libraries

Many organizations may choose an automated solution to keep track of assets.



## Measures to Improve Availability

# Asset Management (Cont.)

- **Asset classification** - assigns all resources of an organization into a group based on common characteristics. An organization should apply an asset classification system to documents, data records, data files, and disks.
- **Asset Standardization** - as part of an IT asset management system, an organization specifies the acceptable IT assets that meet its objectives
- **Threat Identification** - The United States Computer Emergency Readiness Team (US-CERT) and the U.S. Department of Homeland Security sponsor a dictionary of common vulnerabilities and exposure (CVE). The CVE identification contains a standard identifier number with a brief description, and references to related vulnerability reports and advisories.
- **Risk Analysis** - is the process of analyzing the dangers posed by natural and human-caused events to the assets of an organization. A user performs an asset identification to help determine which assets to protect.
- **Mitigation** - Mitigation involves reducing the severity of the loss or the likelihood of the loss from occurring. Many technical controls mitigate risk including authentication systems, file permissions, and firewalls.



## Measures to Improve Availability

# Defense in Depth

Defense in depth will not provide an impenetrable cyber shield, but it will help an organization minimize risk by keeping it one step ahead of cyber criminals. To make sure data and information remains available, an organization must create different layers of protection:

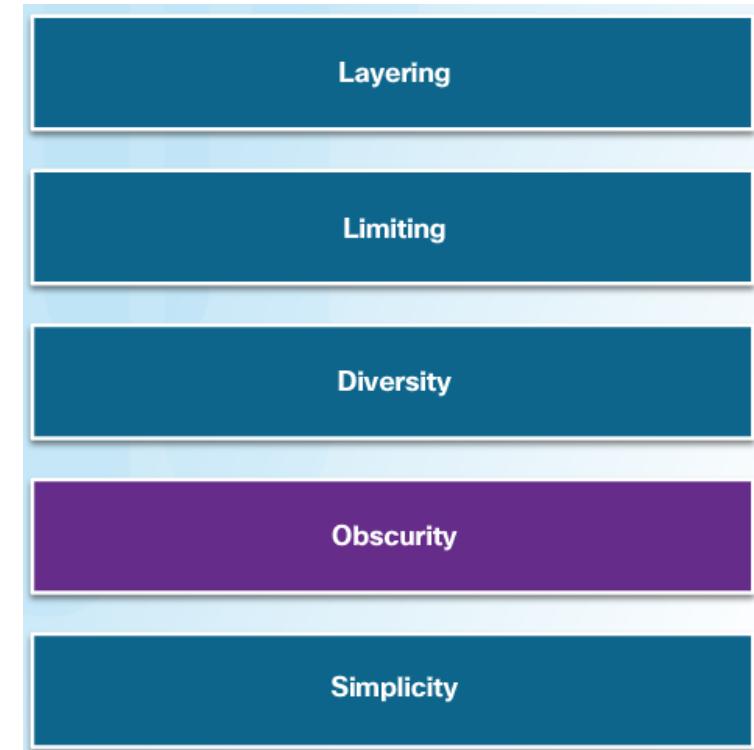
- A **layered** approach provides the most comprehensive protection. If cyber criminals penetrate one layer, they still have to contend with several more layers with each layer being more complicated than the previous one. Layering is creating a barrier of multiple defenses that coordinate together to prevent attacks.
- **Limiting** access to data and information reduces the possibility of a threat. An organization should restrict access so that users only have the level of access required to do their job.



## Measures to Improve Availability

# Defense in Depth

- **Diversity** refers to changing the controls and procedures at different layers. Breaching one layer of security does not compromise the whole system. An organization may use different encryption algorithms or authentication systems to protect data in different states.
- **Obscuring** information can also protect data and information. An organization should not reveal any information that cyber criminals can use to figure out what version of the operating system a server is running or the type of equipment it uses.
- Complexity does not necessarily guarantee security. If the process or technology are too complex, misconfigurations or failure to comply can result. **Simplicity** can actually improve availability.





# Measures to Improve Availability

## Redundancy

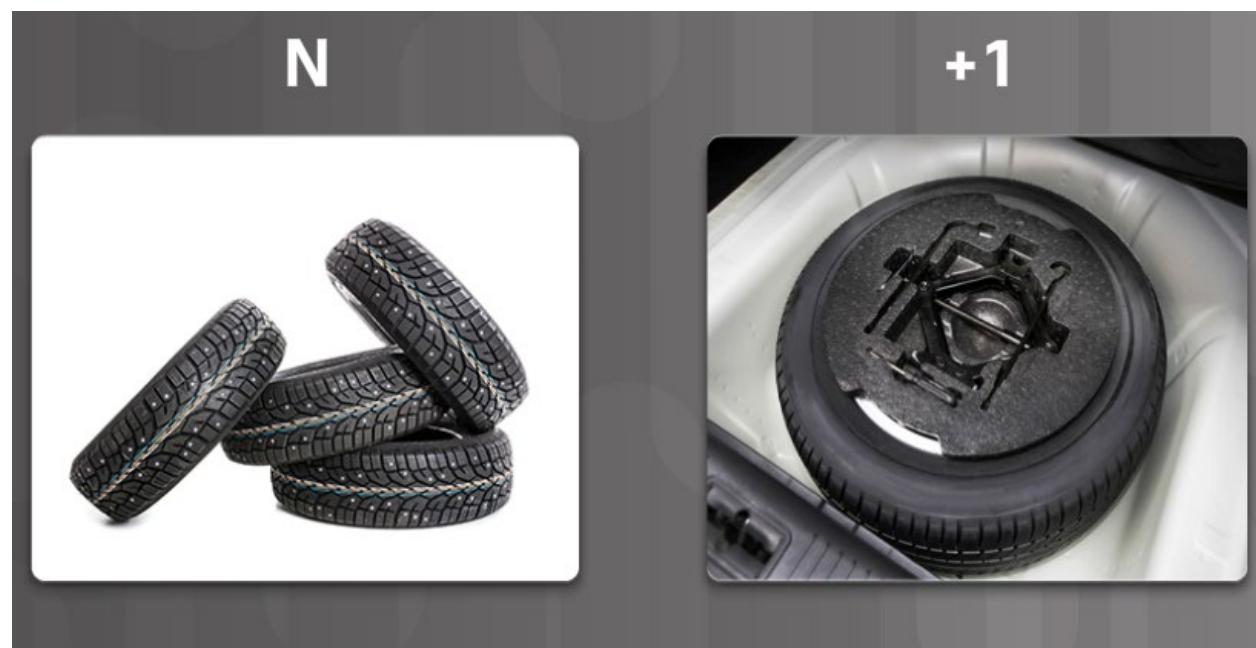
A **single point of failure** must be identified and addressed. A single point of failure can be a specific piece of hardware, a process, a specific piece of data, or even an essential utility.

- Single points of failure are the weak links in the chain that can cause disruption of the organization's operations.
- Generally, the solution to a single point of failure is to modify the critical operation so that it does not rely on a single element.
- The organization can also build redundant components into the critical operation to take over the process should one of these points fail.



## Measures to Improve Availability Redundancy (Cont.)

- **N+1 redundancy** ensures system availability in the event of a component failure.
- Components (N) need to have at least one backup component (+1).
- For example, a car has four tires (N) and a spare tire in the trunk in case of a flat (+1).





## Measures to Improve Availability **Redundancy (Cont.)**

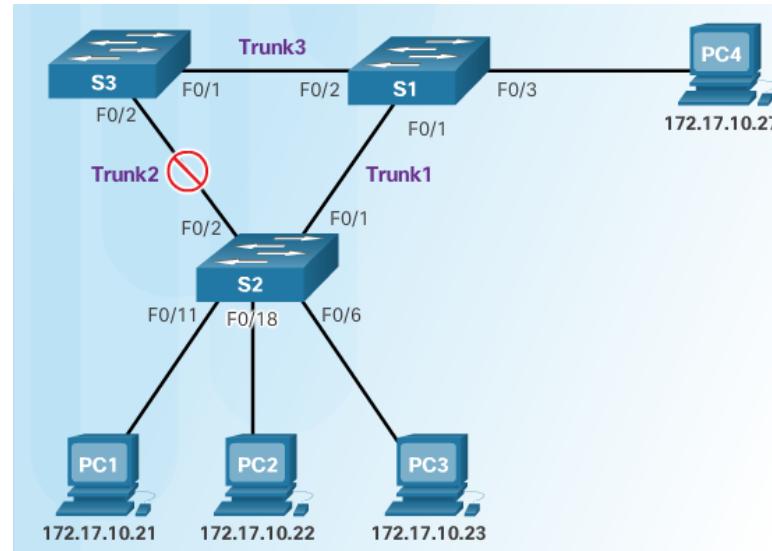
- A **redundant array of independent disks (RAID)** combines multiple physical hard drives into a single logical unit to provide data redundancy and improve performance.
- RAID takes data that is normally stored on a single disk and spreads it out among several drives. If any single disk is lost, the user can recover data from the other disks where the data also resides.
- RAID can also increase the speed of data recovery.
- Using multiple drives makes retrieving requested data faster, instead of relying on just one disk to do the work.
- A RAID solution can be either hardware-based or software-based. The following terms describe how RAID stores data on the various disks:
  - **Parity** - Detects data errors.
  - **Striping** - Writes data across multiple drives.
  - **Mirroring** - Stores duplicate data on a second drive.



# Measures to Improve Availability Redundancy (Cont.)

**Spanning Tree** is a network protocol that provides for redundancy:

- The basic function of STP is to prevent loops on a network when switches interconnect via multiple paths.
- STP ensures that redundant physical links are loop-free. It ensures that there is only one logical path between all destinations on the network.
- STP intentionally blocks redundant paths that could cause a loop.

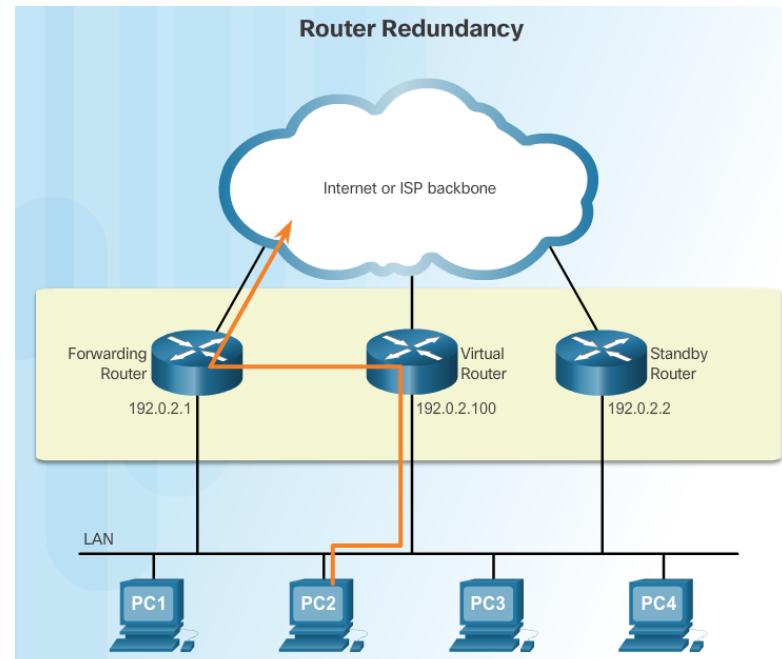




# Measures to Improve Availability Redundancy (Cont.)

The default gateway is typically the router that provides devices access to the rest of the network or to the Internet. If there is only one router serving as the default gateway, it is a single point of failure. Router redundancy involves:

- Choosing to install an additional standby router.
- The ability of a network to dynamically recover from the failure of a router acting as a default gateway is known as first-hop redundancy.





## Measures to Improve Availability **Redundancy (Cont.)**

**Router Redundancy Options** - options available for router redundancy include:

- **Hot Standby Router Protocol (HSRP)** - HSRP provides high network availability by providing first-hop routing redundancy.
- **Virtual Router Redundancy Protocol (VRRP)** - A VRRP router runs the VRRP protocol in conjunction with one or more other routers attached to a LAN. In a VRRP configuration, the elected router is the virtual router master, and the other routers act as backups, in case the virtual router master fails.
- **Gateway Load Balancing Protocol (GLBP)** - GLBP protects data traffic from a failed router or circuit, like HSRP and VRRP, while also allowing load balancing (also called load sharing) between a group of redundant routers.



## Measures to Improve Availability **Redundancy (Cont.)**

**Location Redundancy** - An organization may need to consider location redundancy depending on its needs. The following outlines three forms of location redundancy:

- **Synchronous** - Synchronizes both locations in real time, requires high bandwidth and locations must be close together to reduce latency.
- **Asynchronous Replication** - Not synchronized in real time but close to it, requires less bandwidth and sites can be further apart because latency is less of an issue.
- **Point-in-time-Replication** - Updates the backup data location periodically and is the most bandwidth conservative option because it does not require a constant connection.



## Measures to Improve Availability

# System Resilience

Resiliency defines the methods and configurations used to make a system or network tolerant of failure. Routing protocols provide resiliency. Resilient design is more than just adding redundancy. Resiliency is critical to understand the business needs of the organization, and then incorporate redundancy to create a resilient network.

## 6.3 Incident Response Phases





# Incident Response

## Incident Response Phases

Incident response defines the procedures that an organization follows after an event occurs outside the normal range. When an incident occurs, the organization must know how to respond. Organizations need to develop an incident response plan and put together a Computer Security Incident Response Team (CSIRT) to manage the response. Incident response has consist of four phases:

- 1. Preparation** – planning for potential incidents
- 2. Detection and Analysis** - discovering the incident
- 3. Containment and Eradication, and Recovery** - efforts to immediately contain or eradicate the threat and begin recovery efforts
- 4. Post-Incident Follow-Up** – investigate the cause of the incident and ask questions to better understand the nature of the threat



## Incident Response

# Incident Response Technologies

There are many technologies that are used to implement an incident response:

- **Network Admission Control (NAC)** - allows network access for authorized users with compliant systems. A compliant system meets all of the policy requirements of the organization.
- **Intrusion Detection Systems (IDSs)** - monitor the traffic on a network. IDS systems are passive.
- **Intrusion Prevention Systems** - operates in inline mode. It can detect and immediately address a network problem.
- **NetFlow and IPFIX** - NetFlow is a Cisco IOS technology that provides statistics on packets flowing through a Cisco router or multilayer switch. The Internet Engineering Task Force (IETF) used Cisco's NetFlow Version 9 as the basis for IP Flow Information Export (IPFIX).
- **Advanced Threat Intelligence** - can help organizations detect attacks during one of the stages of the cyberattack (and sometimes before with the right information).

## 2.4 Disaster Recovery





## Disaster Recovery

# Disaster Recovery Planning

**Types of Disasters** - It is critical to keep an organization functioning when a disaster occurs. A disaster includes any natural or human-caused event that damages assets or property and impairs the ability for the organization to continue operating.

- **Natural Disasters** - geological disasters (earthquakes, landslides, volcanoes, and tsunamis), meteorological disasters (hurricanes, tornadoes, snow storms, lightning, and hail), health disasters (widespread illnesses, quarantines, and pandemics) and miscellaneous disasters (fires, floods, solar storms, and avalanches).
- **Human-caused Disasters** - Human-caused disasters - labor events (strikes, walkouts, and slowdowns), social-political events (vandalism, blockades, protests, sabotage, terrorism, and war), materials events (hazardous spills and fires) and utilities disruptions (power failures, communication outages, fuel shortages, and radioactive fallout)



# Disaster Recovery

# Business Continuity Planning

**Need for Business Continuity** - Business continuity is one of the most important concepts in computer security. Even though companies do whatever they can to prevent disasters and loss of data, it is impossible to predict every scenario. It is important for companies to have plans in place that ensure business continuity regardless of what may occur.

**Business Continuity Considerations** - Business continuity controls are more than just backing up data and providing redundant hardware. Business Continuity Considerations should include:

- Documenting configurations
- Establishing alternate communications channels
- Providing power
- Identifying all dependencies for applications and processes
- Understanding how to carry out automated tasks manually



# Disaster Recovery

# Business Continuity Planning

## Business Continuity Best Practices

1. Write a policy that provides guidance to develop the business continuity plan and assigns roles to carry out the tasks.
2. Identify critical systems and processes, and prioritize them based on necessity.
3. Identify vulnerabilities, threats, and calculate risks.
4. Identify and implement controls and countermeasures to reduce risk.
5. Devise methods to bring back critical systems quickly.
6. Write procedures to keep the organization functioning when in a chaotic state.
7. Test the plan.
8. Update the plan regularly.

## 6.5 Chapter Summary





# Chapter Summary

# Summary

- This chapter began by explaining the concept of five nines, a high availability standard that allows for 5.26 minutes of downtime per year.
- The chapter discussed the various approaches that organizations take to ensure system availability.
- Solid system design includes accommodating measures that provide redundancy and resiliency so that an organization can recover quickly and continue operation.
- The chapter also discussed how an organization responds to an incident by establishing procedures that it follows after an event occurs.
- The chapter concluded with a discussion of disaster recovery and business continuity planning.

# Cisco | Networking Academy®

Mind Wide Open™





## Instructor Materials

### Chapter 7: Fortifying the Kingdom



**Cybersecurity Essentials v1.0**

**Cisco Networking Academy®**  
Mind Wide Open™

## Chapter 7: Fortifying the Kingdom



## Cybersecurity Essentials v1.0

Cisco | Networking Academy®  
Mind Wide Open™



# Chapter 7 - Sections & Objectives

## 7.1 Defending Systems and Devices

Describe how cybersecurity domains are used within the CIA triad.

Explain how technologies, processes and procedures protect systems.

## 7.2 Server Hardening

Explain how to protect servers on a network.

## 7.3 Network Hardening

Explain how to implement security measures to protect network devices.

## 7.4 Physical Security

Explain how physical security measures are implemented to protect network equipment.



## 7.1 Defending Systems and Devices



Cisco | Networking Academy®  
Mind Wide Open™



# Defending Systems and Devices

## Host Hardening

**Operating System Security** - The operating system plays a critical role in the operation of a computer system and is the target of many attacks.

- An administrator hardens an operating system by modifying the default configuration to make it more secure to outside threats.
- This process includes the removal of unnecessary programs and services.
- Another critical requirement of hardening operating systems is the application of security patches and updates.

**Antimalware** - Malware includes viruses, worms, Trojan horses, keyloggers, spyware, and adware.

- They all invade privacy, steal information, damage the system, or delete and corrupt data.
- It is important to protect computers and mobile devices using reputable antimalware software.



# Defending Systems and Devices

## Host Hardening (Cont.)

**Patch Management** - Patches are code updates that manufacturers provide to prevent a newly discovered virus or worm from making a successful attack. Manufacturers combine patches and upgrades into a comprehensive update application called a service pack.

**Host-based Firewalls** - A software firewall is a program that runs on a computer to allow or deny traffic between the computer and other connected computers. The software firewall applies a set of rules to data transmissions through inspection and filtering of data packets.

**Host Intrusion Detection Systems** - A host intrusion detection system (HIDS) is software that runs on a host computer that monitors suspicious activity.

**Secure Communications (VPNs)** - When connecting to the local network and sharing files, the communication between computers remains within that network. To communicate and share resources over a network that is not secure, users employ a Virtual Private Network (VPN). A VPN is a private network that connects remote sites or users together over a public network, like the Internet.



# Defending Systems and Devices

## Hardening Wireless and Mobile Devices

**Wired Equivalent Privacy (WEP)** - One of the most important components of modern computing are mobile devices. The majority of devices found on today's networks are laptops, tablets, smart phones and other wireless devices. WEP is one of the first widely used Wi-Fi security standards. The WEP standard provides authentication and encryption protections.

**WPA/WPA2** - The next major improvement to wireless security was the introduction of WPA and WPA2. Wi-Fi Protected Access (WPA) was the computer industry's response to the weakness of the WEP standard. The WPA standard provided several security improvements.

**Mutual Authentication** - The imposter can launch a man-in-the-middle attack which is very difficult to detect and can result in stolen login credentials and transmitted data. To prevent rogue access points, the computer industry developed mutual authentication. Mutual authentication, also called two-way authentication, is a process or technology in which both entities in a communications link authenticate to each other.



# Defending Systems and Devices

## Host Data Protection

**File Access Control** – This consists of permissions that limit folder or file access for an individual or for a group of users.

**File Encryption** – File encryption is a tool used to protect data stored in the form of files. Encryption transforms data using a complicated algorithm to make it unreadable. Software programs can encrypt files, folders, and even entire drives.

**System and Data Backups** - A data backup stores a copy of the information from a computer to removable backup media. Backing up data is one of the most effective ways of protecting against data loss. If the computer hardware fails, the user can restore the data from the backup after the system is again functional.



# Defending Systems and Devices

# Images and Content Control

## Content Screening and Blocking

Content control software restricts the content that a user can access with a web browser over the Internet.

Content control software can block sites that contain certain types of material such as pornography or controversial religious or political content.

## Disk Cloning and Deep Freeze

- Many third-party applications are available to restore a system back to a default state. This allows the administrator to protect the operating system and configuration files for a system.
- Disk cloning copies the contents of the computer's hard disk to an image file.
- Deep Freeze “freezes” the hard drive partition. When a user restarts the system, the system reverts to its frozen configuration. The system does not save any changes that the user makes, so any applications installed or files saved are lost when the system restarts.



# Defending Systems and Devices

## Physical Protection and Workstations

**Security Cables and Locks** - There are several methods of physically protecting computer equipment:

- Use cable locks
- Keep telecommunication rooms locked.
- Use security cages around equipment.

**Logout Timers** - An employee gets up and leaves his computer to take a break. If the employee does not take any action to secure his workstation, any information on that system is vulnerable to an unauthorized user.

**Idle Timeout and Screen Lock** - Employees may or may not log out of their computer when they leave the workplace. Therefore, it is a security best practice to configure an idle timer that will automatically log the user out and lock the screen.

**Login Times** - In some situations, an organization may want employees to log in during specific hours, such as 7 a.m. to 6 p.m. The system blocks logins during the hours that fall outside of the allowed login hours.



# Defending Systems and Devices

## Physical Protection and Workstations

**GPS Tracking** – uses satellites and computers to determine the location of a device. GPS technology is a standard feature on smartphones that provides real-time position tracking. GPS tracking can pinpoint a location within 100 meters.

**Inventory and RFID Tags** - Radio frequency identification (RFID) uses radio waves to identify and track objects. RFID inventory systems use tags attached to all items that an organization wants to track.



## 7.2 Server Hardening





## Server Hardening

# Secure Remote Access

**Managing Remote Access** - Remote access refers to any combination of hardware and software that enables users to access a local internal network remotely.

**Telnet, SSH, and SCP** - Secure Shell (SSH) is a protocol that provides a secure (encrypted) management connection to a remote device.

- **SSH** should replace Telnet for management connections.
- **Telnet** is an older protocol that uses unsecure plaintext transmission of both the login authentication (username and password) and the data transmitted between the communicating devices.
- **Secure copy (SCP)** securely transfers computer files between two remote systems. SCP uses SSH for data transfer (including the authentication element), so SCP ensures the authenticity and confidentiality of the data in transit.



# Server Hardening Administrative Measures

**Securing Ports and Services** - Cyber criminals exploit the services running on a system because they know that most devices run more services or programs than they need. An administrator should look at every service to verify its necessity and evaluate its risk. Remove any unnecessary services.

**Privileged Accounts** - Cyber criminals exploit privileged accounts because they are the most powerful accounts in the organization. Privileged accounts have the credentials to gain access to systems and they provide elevated, unrestricted access. Administrators use these accounts to deploy and manage operating systems, applications, and network devices. These account should be secured or removed to mitigate these risks.

**Group Policies** - In most networks that use Windows computers, an administrator configures Active Directory with Domains on a Windows Server. An administrator configures user account policies such as password policies and lockout policies by adding users to groups and setting policy at a group level.

**Enable Logs and Alerts** - A log records events as they occur on a system. Log entries make up a log file, and a log entry contains all of the information related to a specific event. Logs that relate to computer security have grown in importance.



## Server Hardening

# Physical Protection of Server

**Power** - A critical issue in protecting information systems is electrical power systems and power considerations. A continuous supply of electrical power is critical in today's massive server and data storage facilities.

**Heating, Ventilation, and Air Conditioning (HVAC)** - HVAC systems are critical to the safety of people and information systems in the organization's facilities. When designing modern IT facilities, these systems play a very important role in the overall security. HVAC systems control the ambient environment (temperature, humidity, airflow, and air filtering) and must be planned for and operated along with other data center components such as computing hardware, cabling, data storage, fire protection, physical security systems and power.

**Hardware Monitoring** - Hardware monitoring is often found in large server farms. A server farm is a facility that houses hundreds or thousands of servers for companies.

## 7.3 Network Hardening





# Network Hardening

## Securing Network Devices

**Operation Centers** - The Network Operation Center (NOC) is one or more locations containing the tools that provide administrators with a detailed status of the organization's network. The NOC is ground zero for network troubleshooting, performance monitoring, software distribution and updates, communications management, and device management.

**Switches, Routers, and Network Appliances** - Network devices ship with either no passwords or default passwords.

- **Network switches** are the heart of the modern data communication network. The main threat to network switches are theft, hacking and remote access, attacks against network protocols like ARP/STP or attacks against performance and availability.
- **VLANs** - provide a way to group devices within a LAN and on individual switches. VLANs use logical connections instead of physical connections.



## Network Hardening

# Securing Network Devices (Cont.)

- **Firewalls** - are hardware or software solutions that enforce network security policies. A firewall filters unauthorized or potentially dangerous traffic from entering the network.
- **Routers** - Routers form the backbone of the Internet and communications between different networks. Routers communicate with one another to identify the best possible path to deliver traffic to different networks. Routers use routing protocols to make routing decision.
- **Wireless and Mobile Devices** - Wireless and mobile devices have become the predominant type of devices on most modern networks. They provide mobility and convenience but pose a host of vulnerabilities. These vulnerabilities include theft, hacking and unauthorized remote access, sniffing, man-in-the-middle attacks, and attacks against performance and availability.
- **Network and Routing Services** - Cyber criminals use vulnerable network services to attack a device or to use it as part of the attack. Securing network services ensures that only necessary ports are exposed and available. Network services include; DHCP, DNS, ICMP, Routing Services (RIP-OSPF-ISS), NTP and others.



## Network Hardening

# Voice and Video Equipment

**VoIP Equipment** - uses networks such as the Internet to make and receive phone calls. The equipment required for VoIP includes an Internet connection plus a phone.

**Cameras** - An Internet camera sends and receives data over a LAN and/or the Internet. A user can remotely view live video using a web browser on a wide range of devices including computer systems, laptops, tablets, and smartphones. Cameras come in various forms including the traditional security camera.

**Videoconferencing Equipment** - allows two or more locations to communicate simultaneously using telecommunication technologies. These technologies take advantage of the new high definition video standards. Videoconferencing is now part of normal day-to-day operations in industries like the medical field.

**Network and IoT Sensors** - One of the fastest sectors of information technology is the use of intelligent devices and sensors. The computer industry brands this sector as the Internet of Things (IoT). Businesses and consumers use IoT devices to automate processes, monitor environmental conditions, and alert the user of adverse conditions.

## 7.4 Physical Security





## Physical Security

# Physical Access Control

**Fencing and Barricades** - Physical barriers are the first thing that comes to mind when thinking about physical security. This is the outermost layer of security, and these solutions are the most publicly visible. A perimeter security system typically consists of perimeter fence system, security gate system, bollards, vehicle entry barriers and guard shelters.

**Biometrics** - are the automated methods of recognizing an individual based on a physiological or behavioral characteristic. Biometric authentication systems include measurements of the face, fingerprint, hand geometry, iris, retina, signature, and voice. Biometric technologies can be the foundation of highly secure identification and personal verification solutions.

**Badges and Access Logs** – A badge allows an individual to gain access to an area with automated entry points. An entry point can be a door, a turnstile, a gate, or other barrier. Access badges use various technologies such as a magnetic stripe, barcode, or biometrics. The system logs the transaction for later retrieval. Reports reveal who entered what entry points at what time.



# Physical Security Surveillance

**Guards and Escorts** - All physical access controls including deterrent and detection systems ultimately rely on personnel to intervene and stop the actual attack or intrusion. In highly secure information system facilities, guards control access to the organization's sensitive areas.

**Video and Electronic Surveillance** – This type of surveillance can supplement or in some cases, replace security guards. The benefit of video and electronic surveillance is the ability to monitor areas even when no guards or personnel are present, the ability to record and log surveillance videos and data for long periods, and the ability to incorporate motion detection and notification.

**RFID and Wireless Surveillance** – These types of surveillance are used to manage and locate important information system assets.

## 7.5 Chapter Summary





# Chapter Summary

# Summary

- This chapter discussed the technologies, processes and procedures that cyber wizards use to defend the systems, devices, and data that make up the network infrastructure.
- Host hardening includes securing the operating system, implementing an antivirus solution, and using host-based solutions such as firewalls and intrusion detection systems.
- Server hardening includes managing remote access, securing privileged accounts, and monitoring services.
- Data protection includes file access control and implementing security measures to ensure the confidentiality, integrity, and availability of data.
- Device hardening also involves implementing proven methods of physically securing network devices. Fortifying the kingdom is an on-going process to secure an organization's network infrastructure and requires a constant vigilance to threats against the kingdom.

# Cisco | Networking Academy®

Mind Wide Open™





# Instructor Materials

## Chapter 8: Joining the Order of Cybersecurity Specialist



## Cybersecurity Essentials v1.0

**Cisco Networking Academy®**  
Mind Wide Open™



## Chapter 8: Joining the Order of Cybersecurity Specialist



## Cybersecurity Essentials v1.0

Cisco | Networking Academy®  
Mind Wide Open™



# Chapter 8 - Sections & Objectives

## 8.1 Cybersecurity Domains

Describe resources available to students interested in pursuing a career in cybersecurity.

## 8.2 Understanding the Oath of Membership

Explain how ethics provide guidance.

## 8.3 Next Step

Explain how to take the next step to become a cybersecurity professional.

## 8.1 Cybersecurity Domains





# Cybersecurity Domains

## User Domain

### Common User Threats and Vulnerabilities

- The User Domain includes the users who access the organization's information system.
- Users can be employees, customers, business contractors and other individuals that need access to data.
- Users are often the weakest link in the information security systems and pose a significant threat to the confidentiality, integrity, and availability of the organization's data.

### Managing User Threats

- Conduct security awareness training and user education.
- Enable and automate content filtering and antivirus scanning.
- Disable internal CD drives and USB ports.
- Minimize permissions, restrict access, track and monitor users and enable intrusion detection.



# Cybersecurity Domains

## Device Domain

### Common Threats to Devices

- Unattended workstations, user downloads, unpatched software
- Malware, use of unauthorized media, and violations of the acceptable use policy.

Device Domain Threats	Countermeasure to Manage Threat
Unattended workstations	Establish user account policies for passwords and threshold lockouts
User downloads	Establish access control policies, standards, procedures, and guidelines
Unpatched software	Update and apply security patches according to defined policies, standards, procedures, and guidelines
Malware	Enable an automated antivirus solution to scan systems and update antivirus software
Unauthorized media	Disable internal CD drives and USB ports
Acceptable Use Policy Violation	<ul style="list-style-type: none"><li>▪ Use content filtering</li><li>▪ Use antivirus scanning for downloaded files</li><li>▪ Disable internal CD drives and USB port</li></ul>



# Cybersecurity Domains

## Local Area Network Domain

### Common Threats to the LAN

- Unauthorized LAN access, unauthorized access to systems, applications, wireless networks and data
- Network operating system software vulnerabilities, misconfigurations and failure to perform updates
- Unauthorized network probing and port scanning

LAN Domain Threats	Countermeasure to Manage Threat
Unauthorized LAN access	<ul style="list-style-type: none"><li>▪ Secure wiring closets, data centers, computer rooms</li><li>▪ Define strict access control policies, procedures, and guidelines</li></ul>
Unauthorized access to systems, applications, and data	<ul style="list-style-type: none"><li>▪ Define strict access control policies, procedures, and guidelines</li><li>▪ Restrict access privileges for folders and files based on need</li></ul>
Network operating system software vulnerabilities	<ul style="list-style-type: none"><li>▪ Implement policy to patch and update operating systems</li></ul>
Network operating system unpatched	<ul style="list-style-type: none"><li>▪ Implement policy to patch and update operating systems</li></ul>
Unauthorized access by rogue users	<ul style="list-style-type: none"><li>▪ Require passphrases or authentication for wireless networks</li></ul>
Exploits of data in-transit	<ul style="list-style-type: none"><li>▪ Implement encryption between devices and wireless networks</li></ul>
LAN servers with different hardware or operating systems	<ul style="list-style-type: none"><li>▪ Implement LAN server configuration standards</li></ul>
Unauthorized network probing and port scanning	<ul style="list-style-type: none"><li>▪ Conduct post-configuration penetration tests</li></ul>
Firewall misconfiguration	<ul style="list-style-type: none"><li>▪ Conduct post-configuration penetration tests</li></ul>



## Cybersecurity Domains

# Private Cloud (WAN) Domain

### Common Threats to the Private Cloud:

- Unauthorized network probing, port scanning and access to resources.
- Router, firewall, or network device operating system software vulnerability and misconfiguration.
- Remote users accessing the organization's infrastructure and downloading sensitive data.

Private Cloud Domain Threats	Countermeasure to Manage Threat
Unauthorized network probing and port scanning	<ul style="list-style-type: none"><li>▪ Disable ping, probing, and port scanning</li></ul>
Unauthorized access to resources	<ul style="list-style-type: none"><li>▪ Implement intrusion detection and prevention systems</li></ul>
Router, firewall, or network device operating system software vulnerability	<ul style="list-style-type: none"><li>▪ Update devices with security fixes and patches</li></ul>
Router, firewall, or network device configuration error	<ul style="list-style-type: none"><li>▪ Conduct penetration tests post configuration</li><li>▪ Test inbound and outbound traffic</li></ul>
Remote users download sensitive data	<ul style="list-style-type: none"><li>▪ Implement data classification standard</li><li>▪ Implement file transfer monitoring and scanning</li></ul>



# Cybersecurity Domains

## Public Cloud Domain

### Common Threats to the Public Cloud:

- Data breaches, loss or theft of intellectual property and compromised credentials.
- Federated identity repositories are a high-value target.
- Account hijacking, social engineering attacks and lack of understanding on the part of the organization.

Public Cloud Domain Threats	Countermeasure to Manage Threat
Data breaches	<ul style="list-style-type: none"><li>■ Multifactor authentication</li><li>■ Use of encryption</li><li>■ One-time passwords, phone-based authentication, and smartcards</li></ul>
Loss or theft of intellectual property	<ul style="list-style-type: none"><li>■ Due diligence</li><li>■ Use of encryption</li><li>■ Data backup</li></ul>
Compromised credentials	<ul style="list-style-type: none"><li>■ Multifactor authentication</li><li>■ Use of encryption</li><li>■ One-time passwords, phone-based authentication, and smartcards</li></ul>
Use of federated identity repositories	<ul style="list-style-type: none"><li>■ Multifactor authentication</li><li>■ Implement one-time passwords, phone-based authentication, and smartcards</li></ul>
Account hijacking	<ul style="list-style-type: none"><li>■ Multifactor authentication</li><li>■ Implement one-time passwords, phone-based authentication, and smartcards</li></ul>
Lack of understanding on the part of organization	<ul style="list-style-type: none"><li>■ Due diligence on agreement responsibilities</li></ul>
Social engineering attacks that lure the victim	<ul style="list-style-type: none"><li>■ Security awareness programs</li></ul>
Compliance violations	<ul style="list-style-type: none"><li>■ Due diligence</li><li>■ Policies</li></ul>



# Cybersecurity Domains

## Physical Facilities Domain

### Common Threats to Physical Facilities:

- Natural threats including weather problems, geological hazards, and power interruptions
- Unauthorized access to the facilities, open lobbies, theft, unlocked data center, lack of surveillance
- Social engineering, breach of electronic perimeter defenses

Physical Facilities Domain Threats	Countermeasure to Manage Threat
Natural threats including weather and geological problems	<ul style="list-style-type: none"><li>▪ Develop a disaster recovery plan</li><li>▪ Develop a business continuity plan</li></ul>
Unauthorized access to facilities	<ul style="list-style-type: none"><li>▪ Implement badge encryption for entry access</li></ul>
Power interruptions	<ul style="list-style-type: none"><li>▪ Develop a disaster recovery plan</li></ul>
Social engineering	<ul style="list-style-type: none"><li>▪ Implement badge encryption for entry access</li><li>▪ Conduct security awareness training regularly</li></ul>
Breach of electronic perimeter defenses	<ul style="list-style-type: none"><li>▪ Test building security using both cyber and physical means to covertly gain access</li></ul>
Theft	<ul style="list-style-type: none"><li>▪ Implement an asset tagging system</li><li>▪ Establish policies and procedures for visitors</li></ul>
An open lobby	<ul style="list-style-type: none"><li>▪ Implement badge encryption for entry access</li></ul>
Lack of surveillance	<ul style="list-style-type: none"><li>▪ Implement CCTV coverage of all entrances</li><li>▪ Test building security using both cyber and physical means to covertly gain access</li></ul>
An unlocked data center	<ul style="list-style-type: none"><li>▪ Implement badge encryption for entry access</li></ul>



# Cybersecurity Domains

## Application Domain

### Common Threats to Applications:

- Unauthorized access to data centers, computer rooms, and wiring closets
- Server downtime for maintenance, IT systems down for extended periods
- Network operating system software vulnerability
- Unauthorized access to systems
- Data loss

Application Domain Threats	Countermeasure to Manage Threat
Unauthorized access to data centers, computer rooms, and wiring closets	<ul style="list-style-type: none"><li>▪ Policies, standards, and procedures for staff and visitors</li></ul>
Server downtime for maintenance	<ul style="list-style-type: none"><li>▪ Disaster recovery plan</li><li>▪ Business continuity plan</li></ul>
Network operating system software vulnerability	<ul style="list-style-type: none"><li>▪ Patches and updates completed regularly</li></ul>
Unauthorized access to systems	<ul style="list-style-type: none"><li>▪ Multi-factor authentication</li><li>▪ Monitor log files</li></ul>
Data loss	<ul style="list-style-type: none"><li>▪ Data classification standards</li><li>▪ Backup procedures</li></ul>
Downtime of IT systems for an extended period	<ul style="list-style-type: none"><li>▪ Disaster recovery plan</li><li>▪ Business continuity plan</li></ul>
Software development vulnerabilities	<ul style="list-style-type: none"><li>▪ Conduct software testing prior to launch</li></ul>

## 8.2 Understanding the Oath of Membership





# Understanding the Oath of Membership Ethics and Guiding Principles

## Ethics of a Cybersecurity Specialist

Ethics is the little voice in the background guiding a cybersecurity specialist as to what he should or should not do, regardless of whether it is legal. The organization entrusts the cybersecurity specialist with the most sensitive data and resources. The cybersecurity specialist needs to understand how the law and the organization's interests help to guide ethical decisions.

## Computer Ethics Institute

The Computer Ethics Institute is a resource for identifying, assessing, and responding to ethical issues throughout the information technology industry. CEI was one of the first organizations to recognize the ethical and public policy issues arising from the rapid growth of the information technology field.



# Understanding the Oath of Membership

## Cyber Laws and Liability

### Cybercrime

Laws prohibit undesired behaviors. Unfortunately, the advancements in information system technologies are much faster than the legal system can accommodate. A number of laws and regulations affect cyberspace.

### Cybercrime

A computer may be involved in a cybercrime in a couple of different ways. There is computer-assisted crime, computer-targeted crime, and computer- incidental crime. Child pornography is an example of computer- incidental crime; the computer is a storage device and is not the actual tool used to commit the crime.

### Organizations Created to Fight Cybercrime

There are a number of agencies and organizations out there to aid the fight against cybercrime.



# Understanding the Oath of Membership Cyber Laws and Liability (Cont.)

## Civil, Criminal, and Regulatory Cyber Laws

In the United States, there are three primary sources of laws and regulations: statutory law, administrative law, and common law. All three sources involve computer security. The U.S. Congress established federal administrative agencies and a regulatory framework that includes both civil and criminal penalties for failing to follow the rules.

## Industry Specific Laws

- Gramm-Leach-Bliley Act (GLBA)
- Sarbanes-Oxley Act (SOX)
- Payment Card Industry Data Security Standard (PCI DSS)
- Import/Export Encryption Restrictions

## Security Breach Notification Laws

- Electronic Communications Privacy Act (ECPA)
- Computer Fraud and Abuse Act (1986)



# Understanding the Oath of Membership Cyber Laws and Liability (Cont.)

## Protecting Privacy

- Privacy Act of 1974
- Freedom of Information ACT (FOIA)
- Family Education Records and Privacy Act (FERPA)
- U.S. Computer Fraud and Abuse Act (CFAA)
- U.S. Children's Online Privacy Protection Act (COPPA)
- U.S. Children's Internet Protection Act (CIPA)
- Video Privacy Protection Act (VPPA)
- Health Insurance Portability & Accountability Act
- California Senate Bill 1386 (SB 1386)

## International Laws

- Convention on Cybercrime
- Electronic Privacy Information Center (EPIC)



# Understanding the Oath of Membership

## Cybersecurity Information Websites

**National Vulnerability Database (NVD)** - is a U.S. government repository of standards-based vulnerability management data that uses the Security Content Automation Protocol (SCAP).

**CERT** - The Software Engineering Institute (SEI) at Carnegie Mellon University helps government and industry organizations to develop, operate, and maintain software systems that are innovative, affordable, and trustworthy. It is a Federally Funded Research and Development Center sponsored by the U.S. Department of Defense.

**Internet Storm Center** - provides a free analysis and warning service to Internet users and organizations. It also works with Internet Service Providers to combat malicious cyber criminals. The Internet Storm Center gathers millions of log entries from intrusion detection systems every day using sensors covering 500,000 IP addresses in over 50 countries.

**The Advanced Cyber Security Center (ACSC)** - is a non-profit organization that brings together industry, academia, and government to address advanced cyber threats. The organization shares information on cyber threats, engages in cybersecurity research and development, and creates education programs to promote the cybersecurity profession.



# Understanding the Oath of Membership

## Cybersecurity Weapons

**Vulnerability Scanners** - assess computers, computer systems, networks, or applications for weaknesses. Vulnerability scanners help to automate security auditing by scanning the network for security risks and producing a prioritized list to address weaknesses.

**Penetrating Testing** (or pen testing) - is a method of testing the areas of weaknesses in systems by using various malicious techniques. Pen testing is not the same as vulnerability testing. Vulnerability testing just identifies potential problems. Pen testing involves a cybersecurity specialist who hacks a website, network, or server with the organization's permission to try to gain access to resources without the knowledge of usernames, passwords, or other normal means.

**Packet Analyzers** (or packet sniffers) - intercept and log network traffic. The packet analyzer captures each packet, shows the values of various fields in the packet, and analyzes its content. A sniffer can capture network traffic on both wired and wireless networks.

**Security Tools** - There is no one size fits all when it comes to the best security tools. Much depends on the situation, circumstance, and personal preference. A cybersecurity specialist must know where to go to get sound information.

## 8.3 Next Step



Cisco | Networking Academy®  
Mind Wide Open™



## Next Step

# Exploring the Cybersecurity Profession

### Defining the Roles of Cybersecurity Wizards

The ISO standard defines the role of cybersecurity wizards. The ISO 27000 framework requires:

- A senior manager responsible for IT and ISM (often the audit sponsor)
- Information security professionals and security administrators
- Site/physical security manager and facilities contacts
- HR contact for HR matters such as disciplinary action and training
- Systems and network managers, security architects and other IT professionals

### Job Search Tools

A variety of websites and mobile applications advertise information technology jobs. Each site targets varying job applicants and provides different tools for candidates researching their ideal job position:

- Indeed.com
- CareerBuilder.com
- USAJobs.gov

## 8.4 Chapter Summary

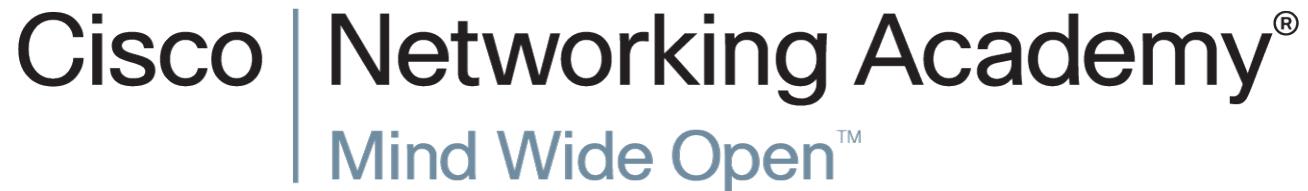




# Chapter Summary

## Summary

- This chapter categorizes the information technology infrastructure created by the advancement of technology into seven domains.
- The chapter discussed the laws that affect technology and cybersecurity requirements.
- Laws such as FISMA, GLBA, and FERPA focus on protecting confidentiality.
- Laws that focus on the protection of integrity include FISMA, SOX, and FERPA, and laws that concern availability include FISMA, GLBA, SOX, and CIPA.
- In addition to the laws in force, the cybersecurity specialist needs to understand how the use of computers and technology affect both individuals and society.
- The chapter also explored the opportunity to become a cybersecurity specialist.
- Finally, this chapter discussed several tools available to cybersecurity specialists.





# CS361C: Information Assurance and Security

## It's a Dangerous (Cyber) World

Dr. Bill Young  
Department of Computer Sciences  
University of Texas at Austin

Last updated: January 26, 2015 at 14:28

# What I'd Like to Discuss

- The scope of the problem
  - Why cyber security is hard
  - Are we at (Cyber) war?
  - What responses are legal and feasible



# From the Headlines

## Silent War, Vanity Fair, July 2013



On the hidden battlefields of history's first known cyber-war, the casualties are piling up. In the U.S., many banks have been hit, and the telecommunications industry seriously damaged, likely in retaliation for several major attacks on Iran.

Washington and Tehran are ramping up their cyber-arsenals, built on a black-market digital arms bazaar, enmeshing such high-tech giants as Microsoft, Google, and Apple.

# From the Headlines

**Iran's supreme leader tells students to prepare for cyber war,**  
rt.com, 2/13/14



Ayatollah Ali Khamenei has delivered a sabre-rattling speech to Iran's 'Revolutionary foster children' (in other words, university students) to prepare for cyber war. The supreme leader has urged his country's students whom he called "cyber war agents" — to prepare for battle.

Israel, Tehran's main adversary in regional politics, has voiced similar statements recently; Major General Aviv Kochavi said that cyber warfare will change the nature of conflict. "Cyber, in my modest opinion, will soon be revealed to be the biggest revolution in warfare, more than gunpowder and the utilization of air power in the last century."

# From the Headlines

## **House Intel Chair Mike Rogers Calls Chinese Cyber Attacks 'Unprecedented'**, ABC News, 2/24/13

House Intelligence Committee Chair Mike Rogers, R-Mich., said it was “beyond a shadow of a doubt” that the Chinese government and military is behind growing cyber attacks against the United States, saying “we are losing” the war to prevent the attacks.



“It is unprecedented,” Rogers added. “This has never happened in the history of the world, where one nation steals the intellectual property to re-purpose it—to illegally compete against the country ... and I’ll tell you, It is as bad as I’ve ever seen it and exponentially getting worse. Why? There’s no consequence for it.”

## Pentagon accuses China of trying to hack US defence networks, The Guardian, 5/7/13



China is using espionage to acquire technology to fuel its military modernisation, the Pentagon has said, for the first time accusing the Chinese of trying to break into US defense computer networks and prompting a firm denial from Beijing.

# From the Headlines

**Cyber security in 2013: How vulnerable to attack is US now?**, Christian Science Monitor, 1/9/13

The phalanx of cyberthreats aimed squarely at Americans' livelihood became startlingly clear in 2012 and appears poised to proliferate in 2013 and beyond.

**That prediction came true:**

2013 was the most historic year ever for cyber attacks. The industry saw several mega attacks that included sophisticated DDoS attack methods. (IT Business Edge, 12/16/13)

Do you think that 2014 was even worse? What's your evidence of that?

# From the Headlines

## **U.S. Not Ready for Cyberwar Hostile Attackers Could Launch, The Daily Beast, 2/21/13**

The Chinese reportedly have been hacking into U.S. infrastructure, and Leon Panetta says future attacks could plunge the U.S. into chaos.



If we are plunged into chaos and suffer more physical destruction than 50 monster hurricanes and economic damage that dwarfs the Great Depression ... Then we will wonder why we failed to guard against what outgoing Defense Secretary Leon Panetta has termed a "cyber-Pearl Harbor."

# The U.S. at Risk?

Experts believe that U.S. is perhaps particularly vulnerable to cyberattack compared to many other countries.

- The U.S. is probably more dependent on technology than any other society on earth.
- Sophisticated attack tools are readily available to anyone on the Internet.
- The openness of U.S. society means critical information and vulnerabilities are accessible.



# The U.S. at Risk?

## More reasons we're vulnerable:

- Much of the U.S. critical infrastructure is accessible on-line.
- Other nation states have much more control over their national communication infrastructure.
- The defense establishment is drowning in data.
- Technology advances rapidly but remains riddled with vulnerabilities.

# How Bad Is It?

**Cyberwarfare greater threat to US than terrorism, say security experts, Al Jazeera America, 1/7/14**



Cyberwarfare is the greatest threat facing the United States — outstripping even terrorism — according to defense, military, and national security leaders in a Defense News poll, a sign that hawkish warning about an imminent 'cyber Pearl Harbor' have been absorbed in defense circles.

45 percent of the 352 industry leaders polled said cyberwarfare is the gravest danger to the U.S., underlining the government's shift in priority—and resources—toward the burgeoning digital arena of warfare.

# The U.S. Government Takes this Seriously

“The Pentagon has concluded that computer sabotage coming from another country can constitute an act of war, a finding that for the first time opens the door for the U.S. to respond using traditional military force.”  
(Wall Street Journal, 5/31/11)



“The Pentagon plans to triple its cybersecurity staff by 2016, U.S. Secretary of Defense Chuck Hagel announced recently. A few days later, FBI Supervisory Special Agent Charles Gilgen said at a conference on cybercrime that his agency’s cyber division plans to hire 1,000 agents and 1,000 analysts in the coming year. Just those two agencies are looking for 6,000 people with cybersecurity skills in the next two years.” (Bloomberg Business, 4/15/14)

# Current Concern

The Obama administration has placed an emphasis on protection of critical infrastructure from cyber attack.

On 2/12/13, the administration released an executive order *Improving Critical Infrastructure Cybersecurity* and Presidential Policy Directive 21: *Critical Infrastructure Security and Resilience*

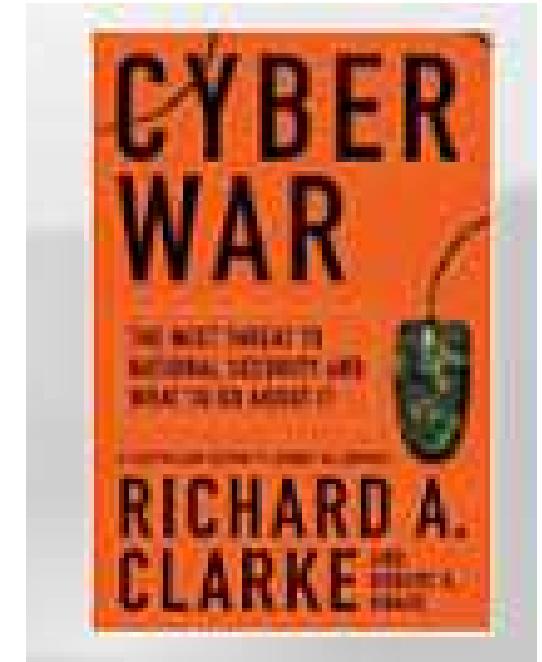
*The Nation's critical infrastructure provides the essential services that underpin American society. Proactive and coordinated efforts are necessary to strengthen and maintain secure, functioning, and resilient critical infrastructure including assets, networks, and systems that are vital to public confidence and the Nation's safety, prosperity, and well-being.*

# But Are We Already at (Cyber) War?

Cyber warfare involves “actions by a nation-state to penetrate another nation’s computers or networks for the purpose of causing damage or disruption.” –Clarke and Knape.

This definition raises as many questions as it addresses:

- Can’t a non-state entity engage in warfare?
- Which computers or networks matter?
- Which actions should qualify as acts of war?
- Is “warfare” even a useful term in this context?
- Why not just make our computers and networks impervious to such attacks?



# Why Are We At Risk?

Arguably, the only way that another nation-state can “penetrate [our] computers or networks for the purpose of causing damage or disruption” is

- ① if they have insider access; or
- ② there are exploitable vulnerabilities that allow them to gain remote access.



So, why not just “harden” our computers and networks to remove the vulnerabilities?

# Why Security is Hard: Target Rich Environment

From the DoD 2010 *Quadrennial Defense Review*:



“On any given day there are as many as 7 million DoD computers and telecommunication tools in use in 88 countries using war-fighting and support applications. The number of potential vulnerabilities, therefore, is staggering.”

That means that there are *lots* of insiders, in addition to the possible vulnerabilities in the software and hardware.

# Is Cyber Security Particularly Hard?

But why is cybersecurity any harder than any other technological problem? Or is it?

*Partial answer:* Most technological problems are concerned with ensuring that something good happens. Security is all about ensuring that *bad things never happen*.



In cybersecurity, you have to defeat an *actively malicious adversary*. Security Guru Ross Anderson characterizes this as “*Programming Satan’s Computer*.”

# Cyber Defense is Asymmetric

The defender has to find and eliminate *all* exploitable vulnerabilities; the attacker only needs to find *one*!

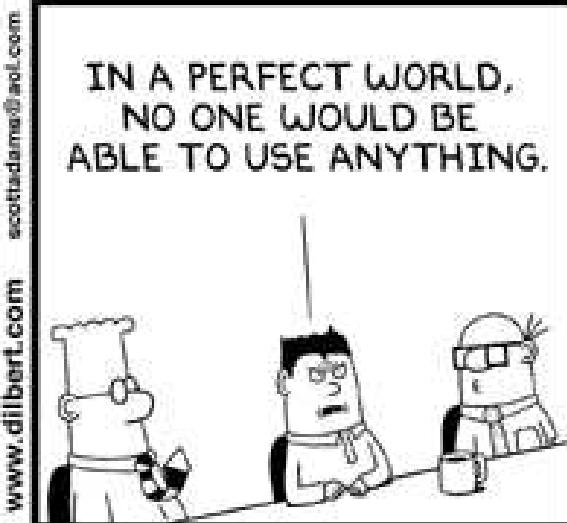


Not only do you have to find “bugs” that make the system behave differently than expected, you have to identify any features of the system that are susceptible to misuse and abuse, *even if your programs behave exactly as you expect them to*.

# Cyber Security is Tough



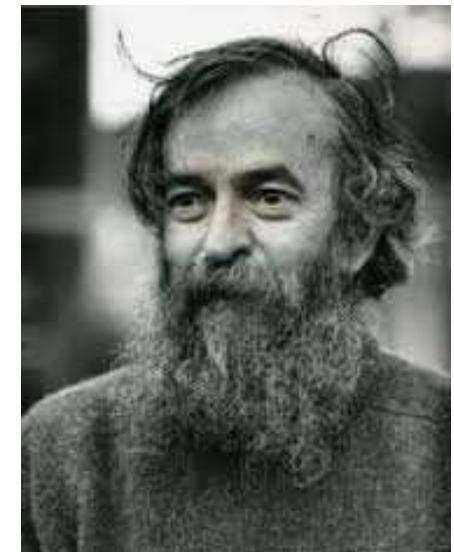
*Perfect security is unachievable in any useful system. We trade-off security with other important goals: functionality, usability, efficiency, time-to-market, and simplicity.*



© Scott Adams, Inc./Dist. by UFS, Inc.

# Is It Getting Better?

“The three golden rules to ensure computer security are: do not own a computer; do not power it on; and do not use it.” –Robert H. Morris (mid 1980's), former chief scientist of the National Computer Security Center



“Unfortunately the only way to really protect [your computer] right now is to turn it off, disconnect it from the Internet, encase it in cement and bury it 100 feet below the ground.” –Prof. Fred Chang (2009), former director of research at NSA

# Some Sobering Facts

- It is *undecidable* whether a given piece of software contains malicious functionality.
- Once PCs are infected they tend to stay infected. The median length of infection is 300 days.
- “More than 5.5 billion attempted attacks were identified in 2011, an increase of 81 percent over 2010, with an unprecedented 403 million unique malware variants that year, a 41 percent leap.” (Symantec Internet Security Threat Report, 2012)



# The Cost of Data Breaches

The Privacy Right's Clearinghouse's *Chronology of Data Breaches* (January, 2012) estimates that more than half a billion sensitive records have been breached since 2005. This is actually a very "conservative estimate."



The Ponemon Institute estimates that the approximate current cost per record compromised is around \$318.

*"A billion here, a billion there, and pretty soon you're talking real money"* (attributed to Sen. Everett Dirksen)

# Security is About Managing Risk

In *Building Secure Software*, Viega and McGraw assert that software and system security is “all about managing risk.” This can be done through:

**Risk acceptance:** some risks are simply tolerated by the organization.

**Risk avoidance:** not performing an activity that would incur risk.

**Risk mitigation:** taking actions to reduce the losses due to a risk.

**Risk transfer:** shift the risk to someone else.

There is generally much more money in a bank than in a convenience store; but which is more likely to be robbed? Why?

# But is it War?

- How real is the threat?
- Is the warfare metaphor a help or a hinderance?
- Are cyberattacks best viewed as crimes, “armed attacks,” both, or something else entirely?
- Is this issue about semantics or substance?
- Does it really matter?



# Why Does it Matter?

Many experts believe that cyber attacks are a serious risk to U.S. national interests today.

America's failure to protect cyberspace is one of the most urgent national security problems facing the new administration that will take office in January 2009. ... It is a battle we are losing. Losing this struggle will wreak serious damage on the economic health and national security of the United States. –CSIS report on *Securing Cyberspace for the 44th Presidency*, Dec. 2008

But others argue the threat is overrated and is largely hype by the security establishment.

*Is it really warfare or is it just crime, that should be dealt with by the criminal justice establishment?*

# Warfare: Cyber and Otherwise

In modern parlance, a shooting war is called *kinetic warfare*, where “kinetics” is concerned with the relationship between the motion of bodies and its causes.

Recall Clarke’s definition of cyber warfare: “actions by a nation-state to penetrate another nation’s computers or networks for the purposes of causing damage or disruption.”

Can activity in cyberspace have kinetic consequences such as property damage and loss of lives? *Does it have to have such consequences to qualify as an act of war?*

## Cyber Combat: Act of War, Wall Street Journal, 5/31/11



“The Pentagon has concluded that computer sabotage coming from another country can constitute an act of war, a finding that for the first time opens the door for the U.S. to respond using traditional military force. ...

One idea gaining momentum at the Pentagon in the notion of 'equivalence.' If a cyber attack produces the death, damage, destruction, or high level disruption that a traditional military attack could cause, it would be a candidate for a 'use of force' consideration.”

# Notable Cyber Campaigns

**First Persian Gulf War (1991):** Iraq's command and control infrastructure is targeted. Radar and missile control network is fragmented and sections of radar coverage are taken offline without central control being aware of the outage.

**Estonia (2007):** Cyberattacks disabled the websites of government ministries, political parties, newspapers, banks, and companies. Russia was suspected of launching the attack in retaliation for the removal of the Bronze Soldier Soviet war memorial in central Tallinn.

**Georgia (2008):** Russia attacked the nation of Georgia in a dispute over the province of South Ossetia. In addition to the military attack, a concerted cyber DoS attack shut down much of Georgia's ability to communicate with the external world.

# What Might an Attack Look Like: Stuxnet



Stuxnet is a Windows computer worm discovered in July 2010 that targets Siemens SCADA (Supervisory Control and Data Acquisition) systems.

In interviews over the past three months in the United States and Europe, experts who have picked apart the computer worm describe it as far more complex and ingenious than anything they had imagined when it began circulating around the world, unexplained, in mid-2009. —New York Times, 1/16/11

# Stuxnet Characteristics

*Stuxnet is the new face of 21st-century warfare: invisible, anonymous, and devastating. ... Stuxnet was the first literal cyber-weapon. America's own critical infrastructure is a sitting target for attacks like this.*  
*(Vanity Fair, April 2011)*

- Stuxnet was the first (known) malware that subverts specific industrial systems.
- Believed to have involved years of effort by skilled hackers to develop and deploy.
- Narrowly targeted, quite possibly at Iran's nuclear centrifuges.
- Widely believed to have been developed by Israel and the U.S.

## Kaspersky Lab Provides Its Insights on Stuxnet Worm, Kaspersky.com, 9/24/10

"I think that this is the turning point, this is the time when we got to a really new world, because in the past there were just cyber-criminals, now I am afraid it is the time of cyber-terrorism, cyber-weapons and cyber-wars."



# Children of Stuxnet

The successors of Stuxnet may be even more sophisticated:

**DuQu:** (Sept. 2011) looks for information that could be useful in attacking industrial control systems.



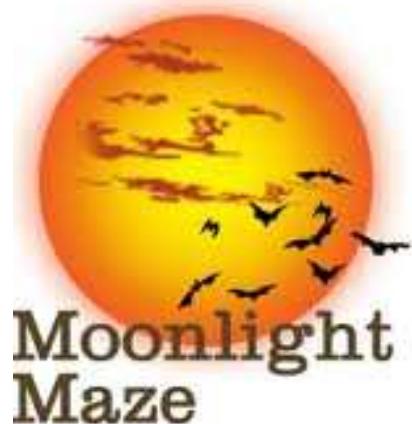
**Flame:** (May 2012) designed for cyber-espionage, targeted government organizations and educational institutions in Iran and elsewhere.

**Gauss:** (Aug. 2012) complex cyber-espionage toolkit designed to steal sensitive data.

*Unlike conventional munitions, could be repurposed and redirected at the sender.*

# Cyber Attacks on the U.S.

The U.S. has already been “attacked” in the sense of cyber espionage.



**Moonlight Maze:** coordinated attacks on U.S. computer systems in 1999, traced to a computer in Moscow. Hackers obtained large stores of data possibly including classified naval codes and information on missile guidance systems.

**Titan Rain:** series of coordinated attacks on U.S. computer systems since 2003. Probably Chinese in origin and probably gathering intelligence; *an estimated 10-20 terabytes of data may have been downloaded.*



*There are undoubtedly others that we don't yet know about.*

# Does This Go Beyond Espionage?

Some security experts warn that a successful possible widespread attack on U.S. computing infrastructure *could largely shut down the U.S. economy for up to 6 months.*

It is estimated that the destruction from a single wave of cyber attacks on U.S. critical infrastructures could exceed \$700 billion USD—the equivalent of 50 major hurricanes hitting U.S. soil at once. (Source: US Cyber Consequences Unit, July 2007)

# CyberAttacks: An Existential Threat?

## **Cyberattacks an 'Existential Threat' to U.S., FBI Says,** Computerworld, 3/24/10

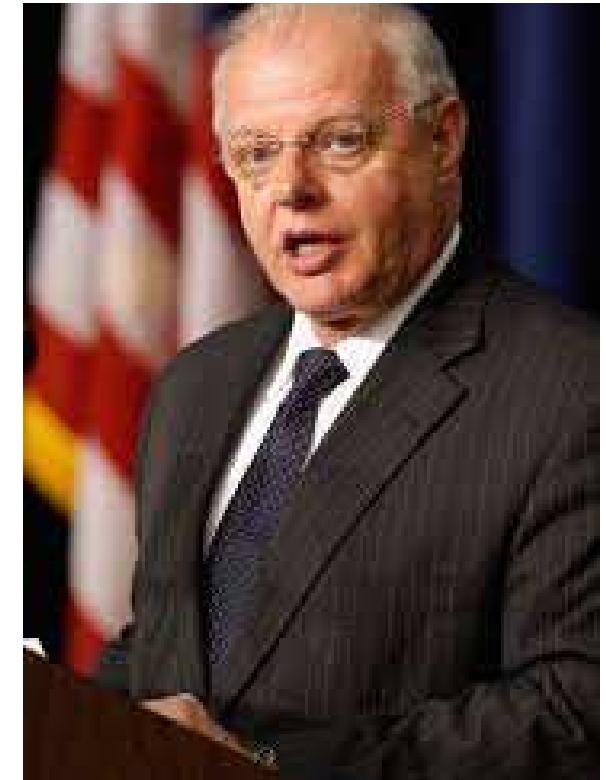


A top FBI official warned today that many cyber-adversaries of the U.S. have the ability to access virtually any computer system, posing a risk that's so great it could "challenge our country's very existence."

According to Steven Chabinsky, deputy assistant director of the FBI's cyber division: "The cyber threat can be an existential threat—meaning it can challenge our country's very existence, or significantly alter our nation's potential."

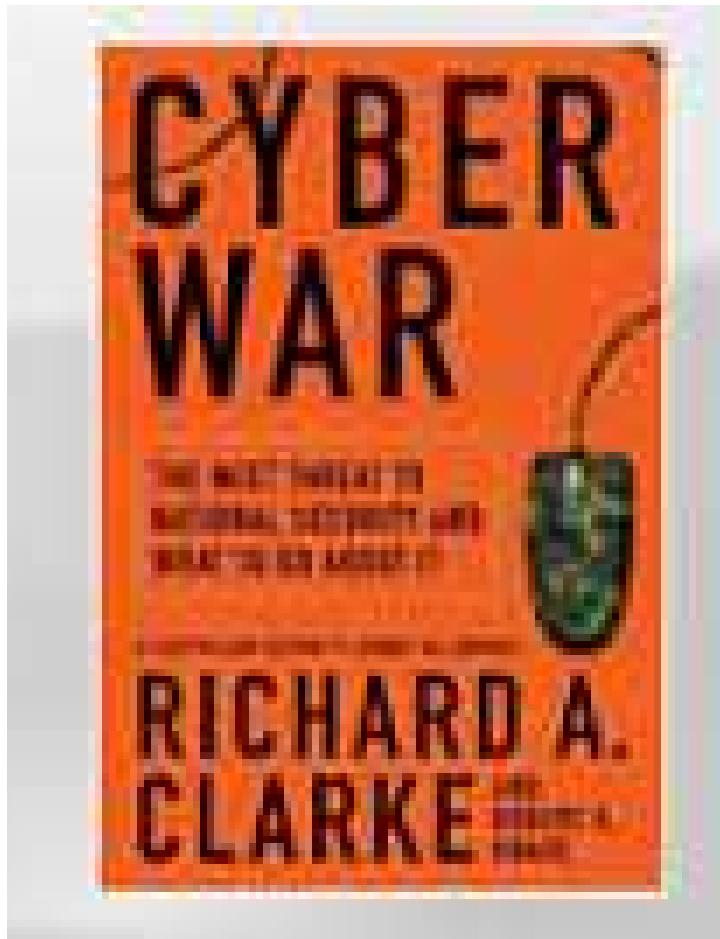
# Not Everyone Agrees

Howard Schmidt, the new cybersecurity czar for the Obama administration, has a short answer for the drumbeat of rhetoric claiming the United States is caught up in a cyberwar that it is losing. “There is no cyberwar. I think that is a terrible metaphor and I think that is a terrible concept,” Schmidt said. “There are no winners in that environment.” (Wired, 3/4/10)



Does Mr. Schmidt think there is no problem? Or just that we're calling it by the wrong name?

# Not Everyone Agrees



The cyberwar rhetoric is dangerous. Its practitioners are artists of exaggeration, who seem to think spinning tall tales is the only way to make bureaucracies move in the right direction. ... Not only does it promote unnecessary fear, it feeds the forces of parochial nationalism and militarism undermining a communications system that has arguably done more to connect the world's citizens than the last 50 years of diplomacy. (Ryan Singel review of Clarke and Knape in Wired, 4/22/10)

# Is a Cyber Attack an Act of War?

There are some serious questions that deserve national and international dialogue.

- How serious would a cyber attack have to be considered an “act of war”?
- What if it were an act by *non-state* actors?
- Would it require *certainty* about who initiated it?
- What degree of control would the offending nation have to exert over such actors?
- Must the response be electronic or could it be a “kinetic”?

# An Act of War?

According to the McAfee *2009 Virtual Criminology Report*:

“When determining whether a cyber attack is an act of cyber war, experts evaluate four key attack attributes:

- **Source:** Was the attack carried out or supported by a nation-state?
- **Consequence:** Did the attack cause harm?
- **Motivation:** Was the attack politically motivated?
- **Sophistication:** Did the attack require customized methods and/or complex planning?”

What do you think of these criteria? Are they precise enough to be useful?

# Cyber Attacks as Armed Attacks

Various international conventions allow a self-defense or “anticipatory self-defense” response to an *armed attack*. But they don’t define “armed attack.”

So, when is a cyber attack “equivalent” to an armed attack?

At least three different analytic frameworks have been proposed:

**Instrument-based:** the damage is such that it previously could only have been caused by a kinetic attack.

**Effects-based:** what are the overall effects of the attack on the victim state.

**Strict liability:** attacks against critical infrastructure qualify because of the potential serious consequences.

Which of these analytic frameworks do you find most reasonable?

# Selecting Targets

In traditional warfare, the targets tend to be *military*, or industrial sites with military value. Maybe it's too obvious, but why is that?

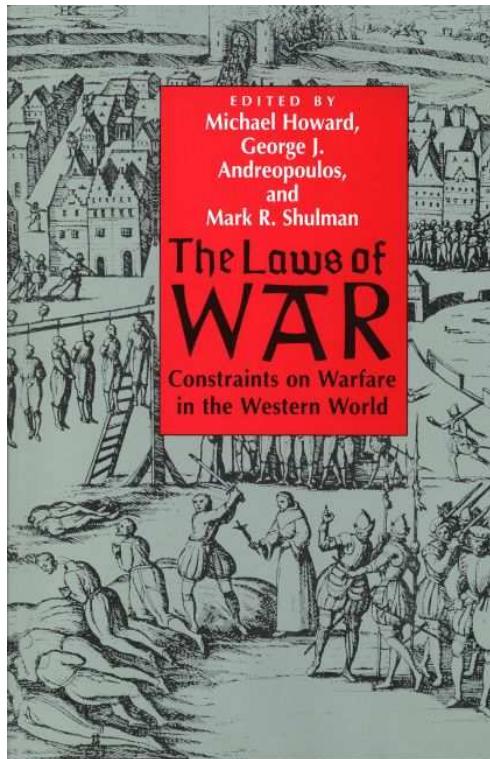
# Selecting Targets

In traditional warfare, the targets tend to be *military*, or industrial sites with military value. Maybe it's too obvious, but why is that?

- ① Military and industrial targets allow the enemy to counterattack, so have high value.
- ② Military assets are likely to be on the defensive perimeter.
- ③ Certain principles (are supposed to) regulate the conduct of states during warfare.

# Selecting Targets

States are supposed to adhere to certain criteria in selecting targets:



- **Distinction:** requires distinguishing combatants from non-combatants and directing actions against military objectives
- **Necessity:** limits force to that “necessary to accomplish a valid military objective”
- **Humanity:** prohibits weapons designed “to cause unnecessary suffering”
- **Proportionality:** protects civilians and property against excessive uses of force

Do these apply to cyberattacks? To responses to cyberattacks?

# Targets

There are good reasons to believe that the choice of targets might be different in cyber vs. kinetic warfare.

- Non-state actors may not feel bound by the conventional laws of war.
- The actors may be in an asymmetric power relationship.
- Non-state actors may be looking for “soft” high-value targets.
- Cyber attacks offer the ability to “skip the battlefield.”

*Systems that people rely upon, from banks to air defense radars, are accessible from cyberspace and can be quickly taken over or knocked out without first defeating a country's traditional defenses. –Clarke and Knape, 31*

# Targets

In a cyberattack, targets could be: *military, civil or private sector.*

If a major cyber conflict between nation-states were to erupt, it is very likely that the private sector would get caught in the crossfire. Most experts agree that critical infrastructure systems—such as the electrical grid, banking and finance, and oil and gas sectors—are vulnerable in many countries. Some nation-states are actively doing reconnaissance to identify specific vulnerabilities. –McAfee report, 3



# Targets



If adversaries intended to attack nations in cyber space, they would select targets which would cause the largest impacts and losses to their opponents with the least effort. It is therefore a very reasonable assumption that adversaries would attack critical infrastructure systems via the Internet. –McAfee report, 16

# Protecting Critical Infrastructure

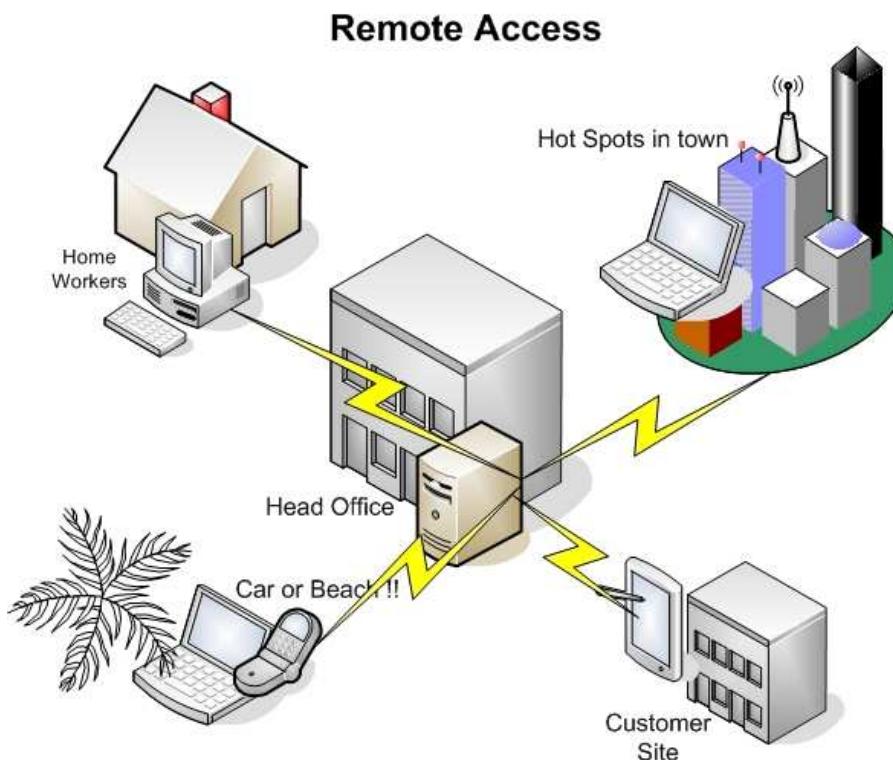
The government takes protection of infrastructure very seriously.  
Presidential Decision Directive (PDD-63) of 1998 states:

- Civilian systems are “essential to the minimum operations of the economy and government”
- Examples: telecommunications, energy, banking, transportation and emergency services

Surely such systems are not vulnerable to cyberattack. Nobody would be dumb enough to make such critical functionality accessible remotely. *Would they?*

# How Vulnerable is Our Infrastructure?

Surely our critical infrastructure is not vulnerable to cyberattack. Nobody would be dumb enough to make such critical functionality accessible remotely. *Would they?*



"I have yet to meet anyone who thinks SCADA systems should be connected to the Internet. But the reality is that SCADA systems need regular updates from a central control, and it is cheaper to do this through an existing Internet connection than to manually move data or build a separate network." –Greg Day, Principal Security Analyst at McAfee

# Non-State Actors

Should a nation-state act against another nation-state in response to actions by a non-state actor?

Did the Afghan government (Taliban) attack the World Trade Center and Pentagon on September 11, 2001?

Did Russia actively organize, encourage and facilitate private hackers participating in the cyber attacks on Georgia and Estonia?

Herb Lin, Senior Scientist of the National Academy of Sciences, said that cyberattacks against the U.S. go up during exam periods in China. *What do you think that's about?*

# Active vs. Passive Defenses

Defenses against cyber attack can be:

**Passive:** taking steps to prevent an attack or to mitigate the damage should an attack occur (access control, secure system design, security administration).

**Active:** electronic measures designed to strike attacking computer systems and shut down an attack midstream (destructive viruses, packet flooding)

Most effective approach is probably a *layered* defense or “*defense in depth*” incorporating both approaches.

But victim states often worry that active defenses may violate the laws of war.

# The Attribution Problem

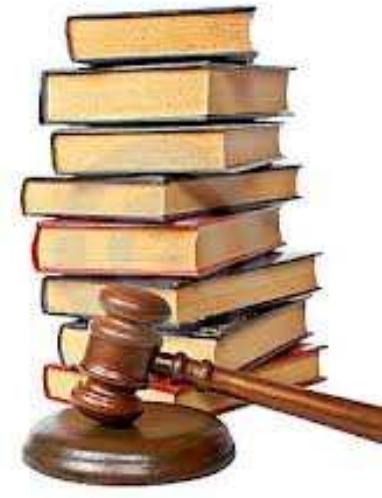
Often it is extremely difficult to determine the source of a cyber attack.



“States find themselves in a ‘response crisis’ during a cyber attack, forced to decide between effective but arguably illegal, active defenses, and the less effective, but legal, passive defenses and criminal laws.” –Carr, *Inside Cyber Warfare*, 47

# The Law of War

How do the laws of war apply to cyber attacks?



Laws of war arose in a conventional context in which:

- it is easy to assess the damage following an attack, and
- it is typically easy to identify the attacker.

“Current international law is not adequate for addressing cyber war. Analogies to environmental law, law of the sea and kinetic war all break down at some point. Answering the question of when to use force in response to a cyber attack needs its own framework.” –Eneken Tikk, legal advisor for the Cooperative Cyber Defence Centre of Excellence in Estonia

# The Prevailing View

According to Lt. Cmd Matt Sklerov (quoted in Carr, 47):

“The prevailing view of states and legal scholars is that states must treat cyber attacks as a criminal matter

- ① out of uncertainty over whether a cyberattack can even qualify as an armed attack, and
- ② because the law of war requires states to attribute an armed attack to a foreign government or its agents before responding with force.”

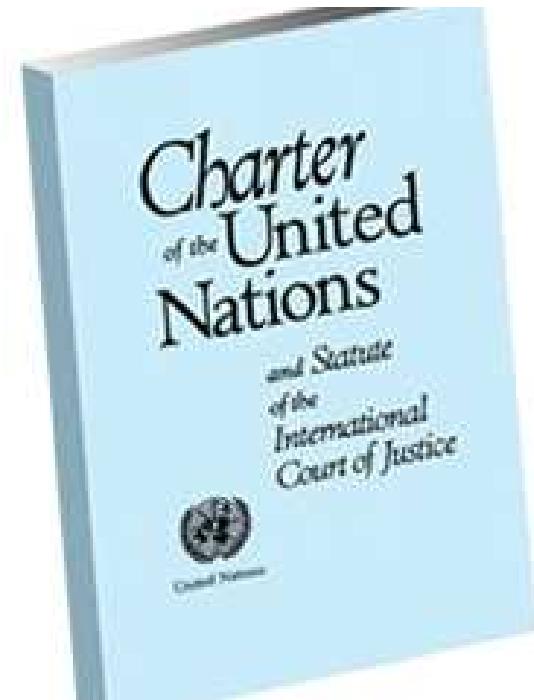
# The Crime-Based Approach

If you treat cyber attacks as a criminal matter, with deterrence from criminal laws and penalties, *how do you force states to comply with international criminal laws?*

- “Several major states, such as China and Russia, allow their attackers to operate with impunity when their attacks target rival states.” (Carr, 47)
- “International legal acts regulating relations arising in the process of combating cyber crimes and cyber terrorism must not contain norms violating such immutable principles of international law as non-interference in the internal affairs of other states, and the sovereignty of the latter.” (Moscow Military Thought, 3/31/97)

# U.N. Charter

The U.N. Charter preserves the right of states to engage in “individual or collective self-defense” in response to an “armed attack.” (Article 51).



However, that begs the question of when a cyber attack should be considered an “armed attack.”

# The Law of War

States have a long-standing duty to prevent non-state actors from using their territory to commit cross-border attacks, including the requirement for states to act against groups generally known to carry out illegal attacks.

Sklerov suggests that duty “should be interpreted to require states to enact and enforce criminal laws to deter cross-border cyber attacks.”

A state which fails to do so could be labeled a *sanctuary state* and sanctioned by the international community.

# The Laws of War

In the cases relating to war crimes in the former Yugoslavia, it was allowed:

*to impute host-state responsibility for the actions of groups of non-state actors when a state exercised “overall control” of the group, even though the state may not have directed the particular act in question. (Prosecutor vs. Tadic)*



# International Agreements



Most directly relevant is the European Convention on Cybercrime, which recognizes the need of states to criminalize cyber attacks and the duty of states to prevent non-state actors on their territory from launching them.

- requires states to establish domestic criminal offenses for most types of cyber attacks
- recognizes the importance of prosecuting attackers
- requires extending jurisdiction to cover a state's territory and actions of citizens regardless of their location.

The Convention has been signed by 26 countries including the U.S.

# Conclusions

- Cyber attacks are a serious threat to the U.S. and other states.
- Cyber warfare may not be a helpful metaphor.
- The nature of the Internet makes cyber attacks powerful, difficult to counter, and difficult to attribute.
- No technical solutions are on the horizon.
- Treaties and legal frameworks have not kept pace with the threat.
- Promising theories and approaches are developing to help the international community cope.



# CS361C: Information Assurance and Security

## Introduction to IA

Bill Young  
Department of Computer Science  
University of Texas at Austin

Last updated: February 2, 2015 at 06:38

# Some Sources

- Andrew Blyth and Gerald L. Kovacich, *Information Assurance: Surviving in the Information Environment*: Springer, 2001.
- Debra S. Herrmann, *Complete Guide to Security and Privacy Metrics*: Auerbach, 2007.
- Douglas J. Landoll, *The Security Risk Assessment Handbook*: Auerbach, 2006.
- Michael E. Whitman and Herbert J. Mattord, *Principles of Information Security*: Thomson, 2009.
- Bel G. Raggad, *Information Security Management: Concepts and Practice*: CRC Press, 2010.

# Thought Experiment

Suppose you visit an e-commerce website such as your bank, stock broker, etc.

Before you type in highly sensitive information, you'd like to have some assurance that your information will be protected. Do you (have such assurance)? How can you know?

What security-relevant things do you want to happen, or not happen when you use such a website?

# Thought Experiment

You might want:

- Privacy of your data
- Protection against phishing
- Integrity of your data
- Authentication
- Authorization
- Confidentiality
- Non-repudiation
- Availability
- What else?

Which of these do you think fall under Information Assurance?

# System Quality

According to ISO/IEC Standard 9126-1 (Software Engineering—Product Quality), the following are all aspects of system quality:

- functionality
  - adequacy
  - interoperability
  - correctness
  - security
- reliability
- usability
- efficiency
- maintainability
- portability

Which of these do you think apply to IA?

# What is Information?

This class is about *Information Assurance*; so what is “information”? How does information differ from data?

# What is Information?

This class is about *Information Assurance*; so what is “information”? How does information differ from data?

*“Information is data endowed with relevance and purpose.*

*Converting data into information thus requires knowledge.*

*Knowledge by definition  
is specialized.” (Blyth  
and Kovacich, p. 17)*



And what characteristics should information possess to be useful?  
It should be: accurate, timely, complete, verifiable, consistent,  
available.

# What is Information?

According to Raggad (pp. 14ff), the following are all distinct conceptual resources:

**Noise**: raw facts with an unknown coding system

**Data**: raw facts with a known coding system

**Information**: processed data

**Knowledge**: accepted facts, principles, or rules of thumb that are useful for specific domains. Knowledge can be the result of inferences and implications produced from simple information facts.

# What is Information Assurance?

What about “assurance”? What does that mean? Assurance from what or to do what? Is it context-dependent?

# What is Information Assurance?

What about “assurance”? What does that mean? Assurance from what or to do what? Is it context-dependent?

According to the U.S. Department of Defense, IA involves:

*Actions taken that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection and reaction capabilities.*

*Information Assurance* (IA) is the study of how to protect your information assets from destruction, degradation, manipulation and exploitation. But also, how to recover should any of those happen. *Notice that it is both proactive and reactive.*

# What is IA? (cont)

According to the DoD definition, these are some aspects of information needing protection:

**Availability:** timely, reliable access to data and information services for authorized users;

**Integrity:** protection against unauthorized modification or destruction of information;

**Confidentiality:** assurance that information is not disclosed to unauthorized persons;

**Authentication:** security measures to establish the validity of a transmission, message, or originator.

**Non-repudiation:** assurance that the sender is provided with proof of a data delivery and recipient is provided with proof of the sender's identity, so that neither can later deny having processed the data.

Is this specifically a military view? Which of these are the most important? How would you decide?

# What is IA?



Information Assurance is such a broad field that there is no universally accepted definition. Researchers often give their own spin to IA, usually reflecting their own concerns.

In these slides, are several different views of IA, including the DoD view (above), Herrmann's view (below), and Blyth and Kovacich's view (below). Be able to compare and contrast these views.

# A Different View of IA

According to Debra Herrmann (*Complete Guide to Security and Privacy Metrics*), IA should be viewed as spanning four security engineering domains:

- physical security
- personnel security
- IT security
- operational security

*The simple truth is that IT security cannot be accomplished in a vacuum, because there are a multitude of dependencies and interactions among all four security engineering domains. (Herrmann, p. 10)*

So threats/risks to IA should be considered along these dimensions as well.

# A Different View of IA

According to Debra Herrmann, IA has four major categories:

- physical security
- personnel security
- IT security
- operational security



Into which of these would you put the following?

- enforcing hard-to-guess passwords
- encrypting your hard drive
- locking sensitive documents in a safe
- stationing a marine guard outside an embassy
- assigning security clearances to staffers
- using SSL for data transfers
- having off-site backup of documents

# Four Security Domains

Quotes from Debra Herrmann, *Complete Guide to Security and Privacy Metrics*:

“*Physical security* refers to the protection of hardware, software, and data against physical threats to reduce or prevent disruptions to operations and services and loss of assets.”

“*Personnel security* is a variety of ongoing measures taken to reduce the likelihood and severity of accidental and intentional alteration, destruction, misappropriation, misuse, misconfiguration, unauthorized distribution, and unavailability of an organization’s logical and physical assets, as the result of action or inaction by insiders and known outsiders, such as business partners.”

# Four Security Domains

“*IT security* is the inherent technical features and functions that collectively contribute to an IT infrastructure achieving and sustaining confidentiality, integrity, availability, accountability, authenticity, and reliability.”

“*Operational security* involves the implementation of standard operational security procedures that define the nature and frequency of the interaction between users, systems, and system resources, the purpose of which is to

- ① achieve and sustain a known secure system state at all times, and
- ② prevent accidental or intentional theft, release, destruction, alteration, misuse, or sabotage of system resources.”

Are these domains purely defensive, or might they be offensive? Compare and contrast Herrmann’s view of IA with the government view outlined before.

# Yet Another Perspective

According to Raggad's taxonomy of information security, a computing environment is made up of five continuously interacting components:



- activities,
  - people,
  - data,
  - technology,
  - networks.

A comprehensive security plan must take all of these into account.  
How do these map onto the previous scheme?

Does protecting a computing environment merely mean protecting these five components?

# Yet Another View: Components of IA

IA includes computer and information security, but more besides. According to Blyth and Kovacich, IA can be thought of as protecting information at three distinct levels:

**physical:** data and data processing activities in physical space;

**information infrastructure:** information and data manipulation abilities in cyberspace;

**perceptual:** knowledge and understanding in human decision space.

# IA Levels: the Physical

The lowest level focus of IA is the physical level: computers, physical networks, telecommunications and supporting systems such as power, facilities and environmental controls. Also at this level are the people who manage the systems.

**Desired Effects:** to affect the technical performance and the capability of physical systems, to disrupt the capabilities of the defender.

**Attacker's Operations:** physical attack and destruction, including: electromagnetic attack, visual spying, intrusion, scavenging and removal, wiretapping, interference, and eavesdropping.

**Defender's Operations:** physical security, OPSEC, TEMPEST.

# IA Levels: Infrastructure

The second level focus of IA is the information structure level. This covers information and data manipulation ability maintained in cyberspace, including: data structures, processes and programs, protocols, data content and databases.

**Desired Effects:** to influence the effectiveness and performance of information functions supporting perception, decision making, and control of physical processes.

**Attacker's Operations:** impersonation, piggybacking, spoofing, network attacks, malware, authorization attacks, active misuse, and denial of service attacks.

**Defender's Operations:** information security technical measures such as: encryption and key management, intrusion detection, anti-virus software, auditing, redundancy, firewalls, policies and standards.

# IA Levels: Perceptual

The third level focus of IA is the perceptual level, also called *social engineering*. This is abstract and concerned with the management of perceptions of the target, particularly those persons making security decisions.

**Desired Effects:** to influence decisions and behaviors.

**Attacker's Operations:** psychological operations such as:

deception, blackmail, bribery and corruption, social engineering, trademark and copyright infringement, defamation, diplomacy, creating distrust.

**Defender's Operations:** personnel security including psychological testing, education, and screening such as biometrics, watermarks, keys, passwords.

Thus, IA includes aspects of:

- COMPSEC: computer security;
- COMSEC: communications and network security;
- ITSEC: (which includes both COMPSEC and COMSEC);
- OPSEC: operations security.

Compare Blyth and Kovacich's view of IA with the government view and Herrmann's views described previously.

*If you entrench yourself behind strong fortifications, you compel the enemy to seek a solution elsewhere.* –Carl von Clausewitz



A recent headline in the AAS read: “The Biggest Threat to Computer Security? Carelessness”

*Principle of Easiest Penetration:* An attacker on any information system will use the simplest means of subverting system security.

# Many IA Failures Don't Involve Technology

In 1996, news of possible signs of life in a Martian meteorite called ALH84001 leaked out ahead of a press conference that had been scheduled by NASA.



*This was partly because a high-ranking White House official told a prostitute about the meteorite, who then sold the information to a tabloid.*

NASA had to scramble to reschedule its press conference to an earlier date to satisfy the growing demand for information from the press and the public.

# The Information Warfare Spin on IA

The flip side of Information Assurance is Information Warfare (IW). In fact, one can think of the offensive part of IW as “information operations,” and the defensive part as information assurance.

- *Type I* involves managing an opponent’s perception through deception and psychological operations. In military circles, this is called *Truth Projection*.
- *Type II* involves denying, destroying, degrading, or distorting the opponent’s information flows to disrupt their ability to carry out or co-ordinate operations.
- *Type III* gathers intelligence by exploiting the opponent’s use of information systems.

IW can be carried out against individuals, corporations, or nations.  
Is hacking IW?

# Nature of the Threat

Necessary for IW, as for any related activity, are *motive*, *means*, and *opportunity*.

In general, the offensive players in the world of IW come in six types:

**Insiders:** consists of employees, former employees and contractors.

**Hackers:** one who gains unauthorized access to or breaks into information systems for thrills, challenge, power, or profit.

**Criminals:** target information that may be of value to them: bank accounts, credit card information, intellectual property, etc.

# Nature of the Threat (cont.)

**Corporations:** actively seek intelligence about competitors or steal trade secrets.

**Governments and agencies:** seek the military, diplomatic, and economic secrets of foreign governments, foreign corporations, and adversaries. May also target domestic adversaries.

**Terrorists:** usually politically motivated and may seek to cause maximal damage to information infrastructure as well as endanger lives and property.

Is there overlap among these categories of actors? Which do you think is the biggest threat? Does it depend on the target?

# Why Does it Matter?

It's a dangerous world out there.

*While experts may disagree on the definition of cyber war, there is significant evidence that nations around the world are developing, testing and in some cases using or encouraging cyber means as a method of obtaining political advantage.* –McAfee *Virtual Criminology Report 2009*

*A plausible worst-case worm could cause \$50 billion or more in direct economic damage by attacking widely used services in Microsoft Windows and carrying a highly destructive payload.”* –Nicholas Weaver and Vern Paxson, 6/14/04

# Why Does it Matter?

*America's failure to protect cyberspace is one of the most urgent national security problems facing the new administration that will take office in January 2009. ... It is a battle we are losing. Losing this struggle will wreak serious damage on the economic health and national security of the United States.* –CSIS report on *Securing Cyberspace for the 44th Presidency*, Dec. 2008

# IA Functional Components

Note that IA is both proactive and reactive involving: *protection, detection, capability restoration, and response.*

- *IA environment protection pillars:* “ensure the availability, integrity, authenticity, confidentiality, and non-repudiation of information”
- *Attack detection:* “timely attack detection and reporting is key to initiating the restoration and response processes.”

# IA Functional Components (2)

- *Capability restoration:*
  - “relies on established procedures and mechanisms for prioritizing restoration of essential functions. Capability restoration may rely on backup or redundant links, information system components, or alternative means of information transfer.”
  - “A post-attack analysis should be conducted to determine the command vulnerabilities and recommended security improvements.”
- *Attack response:* “involves determining actors and their motives, establishing cause and complicity, and may involve appropriate action against perpetrators... contributes ... by removing threats and enhancing deterrence.”

# IA Applies to Info Infrastructure

*If adversaries intended to attack nations in cyber space, they would select targets which would cause the largest impacts and losses to their opponents with the least effort. It is therefore a very reasonable assumption that adversaries would attack critical infrastructure systems via the Internet.* –McAfee Virtual Criminology Report 2009, p. 16

- *Global Information Infrastructure:* “worldwide interconnection of communication networks, computers, databases, and consumer electronics that make vast amounts of information available to users.”
- *National Information Infrastructure:* those within or serving the U.S., for government, commerce and research.
- *Defense Information Infrastructure:* those within or serving the DoD (e.g. nodes on SIPRNET and NIPRNET).

## *Presidential Decision Directive (PDD-63) of 1998*

- Civilian systems are “essential to the minimum operations of the economy and government”
- Examples: telecommunications, energy, banking, transportation and emergency services

Increased vulnerability as:

- information systems have become automated and interlinked;
- information systems are using COTS technology, subject to viruses, worms, etc.

Every federal department CIO is responsible for information assurance.

# Federal Orgs Defining IA

## *Committee on National Security Systems (CNSS)*

- Designation of the National Security Telecommunications and Information Systems Security Committee (NSTISSC), chaired by DoD.
- Establishes federal policy directives on network security.
- Sanctions universities to offer security certification.

## *National Security Agency (NSA)*

- Lead cryptographic organization
- Builds and tests secure systems for classified applications
- Coordinates with industry on security development

## *National Institute of Standards and Technology (NIST)*

- Formerly National Bureau of Standards (NBS)
- Leverages NSA's experience in standardizing cryptosystems for civilian use. E.g. DES, SHA, AES.

# IA Relationship to Computer Security

- IA includes considerations for non-security threats to information systems, such as acts of nature and the process of recovery from incidents.
- IA *emphasizes management, process, and human involvement*, and not merely technology.
- IA deployments may involve multiple disciplines of security:
  - COMPUSEC (Computer security)
  - COMSEC (Communications security), SIGSEC (Signals security) and TRANSEC (transmission security)
  - EMSEC (Emanations security) denying access to information from unintended emanations such as radio and electrical signals
  - OPSEC (Operations security) the processes involved in protecting information

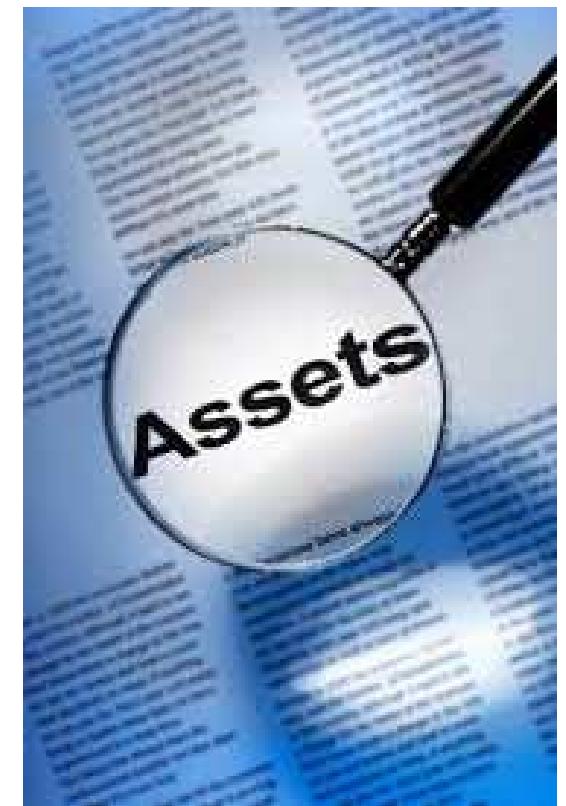
# Some Basic IA Terms

A complete IA glossary can be found at: *National Information Assurance Glossary*,  
[www.cnss.gov/Assets/pdf/cnssi\\_4009.pdf](http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf).

# Assets

An **asset** is the resource being protected, including:

- **physical assets:** devices, computers, people;
- **logical assets:** information, data (in transmission, storage, or processing), and intellectual property;
- **system assets:** any software, hardware, data, administrative, physical, communications, or personnel resource within an information system.



Assets have value so are worth protecting.

# Subjects and Objects

Often a security solution/policy is phrased in terms of the following three categories:

**Objects:** the items being protected by the system (documents, files, directories, databases, transactions, etc.)

**Subjects:** entities (users, processes, etc.) that execute activities and request access to objects.

**Actions:** operations, primitive or complex, that can operate on objects and must be controlled.

For example, in the Unix operating system, processes (subjects) may have permission to perform read, write or execute (actions) on files (objects). In addition, processes can create other processes, create and delete files, etc. Certain processes (running with root permission) can do almost anything. That is one approach to the security problem.

Can an entity be both a subject and an object?

# Attributes

Both subjects and objects have associated *attributes*. The security mechanisms may operate in terms on the attributes and manipulation of the attributes can be used to subvert security.

What are some attributes associated with subjects? With objects?  
How are attributes established/changed?

# Critical Aspects

Information assets (objects) may have critical aspects:

**availability:** authorized users are able to access it;

**accuracy:** the information is free of error and has the value expected;

**authenticity:** the information is genuine;

**confidentiality:** the information has not been disclosed to unauthorized parties;

**integrity:** the information is whole, complete and uncorrupted;

**utility:** the information has value for the intended purpose;

**possession:** the data is under authorized ownership and control.

# Terms: Threat and Threat Actors

A *threat* is a *category* of entities, or a circumstance, that poses a potential danger to an asset (through unauthorized access, destruction, disclosure, modification or denial of service).

- Threats can be categorized by intent: accidental or purposeful (error, fraud, hostile intelligence);
- Threats can be categorized by the kind of entity involved: human (hackers, someone flipping a switch), processing (malicious code, sniffers), natural (flood, earthquake);
- Threats can be categorized by impact: type of asset, consequences.

A *threat actor* is a specific instance of a threat, e.g. a specific hacker, a particular storm, etc.

# Examples of Threats

**Interruption:** an asset becomes unusable, unavailable, or lost.

**Interception:** an unauthorized party gains access to an information asset.

**Modification:** an unauthorized party tampers with an asset.

**Fabrication:** an asset has been counterfeit.

Give examples of each of these.

# Examples of Threats

**Interruption:** an asset becomes unusable, unavailable, or lost.

**Interception:** an unauthorized party gains access to an information asset.

**Modification:** an unauthorized party tampers with an asset.

**Fabrication:** an asset has been counterfeit.

Give examples of each of these.

Examples:

**Interruption:** a denial of service attack on a website

**Interception:** compromise of confidential data, e.g., but packet sniffing

**Modification:** hacking to deface a website

**Fabrication:** spoofing attacks in a network

# Terms: Environments, Enclaves

A *hostile environment* for assets is one that has known threats.

Example: locating an asset in a war zone or a flood zone, or placing an unprotected machine on the Internet.

A *benign environment* is a nonhostile environment that may be protected from external hostile elements by physical, personnel, and procedural countermeasures.

An *enclave* is a collection of computing environments connected by one or more internal networks under the control of a single authority and security policy, including personnel and physical security.

Describe a local enclave here at UT?

# Terms: Vulnerabilities and Exploits

A *vulnerability* is a weakness or fault in a system that exposes information to attack.

- A bug in a computer program is a very common vulnerability in computer security (e.g. buffer overflow situation).
- A procedural failing can subvert technology controls (e.g. a core dump of secure information upon a failure).
- A lack of controls can result in vulnerabilities, if controls are subverted (e.g. Enron financials).

An *exploit* is a method for taking advantage of a known vulnerability.

What's the difference between an exploit and an attack?

# Terms: Vulnerabilities and Exploits

A *dangling vulnerability* is one for which there is no known threat (vulnerability is there but not exploitable).

A *dangling threat* is one that does not pose a danger as there is no vulnerability to exploit (threat is there, but can't do damage).

Can you give examples of these or situations in which they might occur?

# Terms: Attacks, etc.

An **attack** is an attempt to gain access, cause damage to or otherwise compromise information and/or systems that support it.

**Passive attack:** an attack in which the attacker observes interaction with the system.

**Active attack:** an attack in which the attacker directly interacts with the system.

**Unintentional attack:** an attack where there is not a deliberate goal of misuse

## Terms: Attacks, etc. (2)

Attacks have a subject and object.

**Attack subject:** the active entity, usually a threat actor, that interacts with the system.

**Attack object:** the targeted information system asset.

The *attack surface* of an organization/entity is the set of ways in which an adversary can enter the system and potentially cause damage. For example:

*The attack surface of a software environment is the code within a computer system that can be run by unauthenticated users. This includes, but is not limited to: user input fields, protocols, interfaces, and services.*  
*(Wikipedia)*

Mention some ways in which the attack surface can be reduced.

# Terms: Exposure, Compromise

*Exposure* is an instance when the system is vulnerable to attack.

A *compromise* is a situation in which the attacker has succeeded.

An *indicator* is a recognized action—specific, generalized or theoretical—that an adversary (threat actor) might be expected to take in preparation for an attack.

Give an example of an indicator.

# Terms: Consequences

A *consequence* is the outcome of an attack. In a purposeful threat, the threat actor has typically chosen a desired consequence for the attack, and selects the IA objective to target to achieve this.

**Disruption:** targets availability

**Corruption:** targets integrity

**Exploitation:** targets confidentiality

A consequence may cause the information system to lose effectiveness, and may have other costs.

*Inadvertant disclosure* is a type of consequence, involving accidental exposure of information to an agent not authorized access.

# Terms: Countermeasures

*Controls, safeguards* and *countermeasures* are any actions, devices, procedures, techniques and other measures that reduce the vulnerability of an information system. There are many kinds:

- technical
- policy, procedures and practices
- education, training and awareness
- cover and deception (camouflage)
- human intelligence (HUMINT), e.g. disinformation
- monitoring of data and transmissions
- surveillance countermeasures that detect or neutralize sensors, e.g. TEMPEST
- assessments and inspections.

A *security posture* or security profile is the implementation (policy, procedures, technology) of the security effort within an organization.

# Terms: Risk

Viega and McGraw, *Building Secure Software* assert that software and system security is “all about managing risk.” Do you agree? Why or why not?

*Risk* is the possibility that a particular threat will adversely impact an information system by exploiting a particular vulnerability. The assessment of risk must take into account the consequences of an exploit.

*Risk management* is a process for an organization to identify and address the risks in their environment. There are several *risk management frameworks*, and each defines a procedure for an organization to follow.



# Risk Management Framework

One particular risk management procedure (from Viega and McGraw) consists of six steps:

- ① Assess assets
- ② Assess threats
- ③ Assess vulnerabilities
- ④ Assess risks
- ⑤ Prioritize countermeasure options
- ⑥ Make risk management decisions

Thought experiment: try to follow this procedure to manage risks to your material possessions stored at your home or apartment.

# Risk Treatments

Once the risk has been identified and assessed, managing the risk can be done through one of four techniques:

**Risk acceptance:** risks not avoided or transferred are retained by the organization. E.g. sometimes the cost of insurance is greater than the potential loss. Sometimes the loss is improbable, though catastrophic.

**Risk avoidance:** not performing an activity that would incur risk. E.g. disallow remote login.

**Risk mitigation:** taking actions to reduce the losses due to a risk; many technical countermeasures fall into this category.

**Risk transfer:** shift the risk to someone else. E.g. most insurance contracts, home security systems.

# Risk Management

The risk treatments—acceptance, avoidance, mitigation, transfer—are with respect to a *specific risk for a specific party*.

E.g., buying insurance is risk transfer for you, not for the insurance company. For the insurance company, it's risk acceptance. But they may require you to take measures to avoid or mitigate their risk.

There is generally more money in a bank than in a convenience store; but which is more likely to be robbed? Why? Of which risk management technique(s) is this an instance?

# Mitigation versus Avoidance

There is often a confusion about the difference between *risk avoidance* and *risk mitigation*.

Risk avoidance is about preventing the risk from being actualized.  
E.g., not parking in a high crime area.

Risk mitigation is about limiting the damage should the risk be actualized. E.g., having a LoJack or cheap car stereo.

Note the risk in this case is that your car will be broken into.

# Terms: Trust and Assurance

*Trust* is a generic term that implies a mechanism in place to provide a basis for confidence in the reliability/security of the system. Failure of the mechanism may destroy the basis for trust.

*Trust mechanisms* are the security features of a system that provide enforcement of a security policy.

The *trusted computing base* (TCB) is a collection of all the trust mechanisms of a computer system which collectively enforce the policy.

*Assurance* is a measure of confidence that the security features, practices, procedures, and architecture of a system accurately mediates and enforces the security policy.

# Trust Management

The concept of *trust management* provides a unified approach to conceptualizing (parts of) IA. That is, a big part of IA is about controlling interactions among:

- actions
- principals
- policies
- credentials

Various policy management systems have been built with the goal of formalizing and describing these relationships: KeyNote (1999) and Extensible Access Control Markup Language (XACML) (2009).

These provide formal mechanisms for defining policy languages.

Why do you think that trust is a vital component of IA?

# Lifecycle

A *lifecycle* is the process by which an asset is managed from its arrival or creation to its termination or destruction.

Software engineering defines several lifecycle models for the development or acquisition of computer software. In a *waterfall model*, the process is divided into stages performed sequentially:

- Requirements
- Design
- Coding
- Testing
- Deployment
- Production
- Decommission

# Security Systems Lifecycle Management

Security systems lifecycle management is a process by which the project managers for a system will ensure that appropriate information assurance safeguards are incorporated into a system.

The stages leading to acquisition by the government of a secured system might be:

- ① evaluation of sensitivity of the application based on risk analysis
- ② determination of security specifications
- ③ design review and perform system tests to ensure safeguards are adequate, through testing and validation that the product meets specifications
- ④ system certification and accreditation, issuance of a certificate that the system meets the need and can be procured.

# Assurance Requirements

Some indication of various types of lifecycle concerns appear in the Common Criteria “Assurance requirements”, including:

Class APE, ASE: *System Evaluation*.

Class ACM: *Configuration Management*, includes CM automation, capabilities, and scope.

Class ADO: *Delivery and Operations*, includes delivery and installation, and generation and set-up.

Class ADV: *Development*, includes functional specification, low-level design, implementation representation, TSF internals, high-level design, representation correspondence, and security policy modeling.

# Assurance Requirements (2)

Class AGC: *Guidance Documentation*, includes administrator guidance, and user guidance.

Class ALC: *Life Cycle*, includes development security, flaw remediation, tools and techniques, and life cycle definition.

Class ATE: *Tests*, includes test coverage, test depth, functional tests, and independent testing.

Class AVA: *Vulnerability Assessment*, includes covert channel analysis, misuses, strength of functions, and vulnerability analysis.

Class AMA: *Maintenance of Assurance*, includes assurance maintenance plan, component categorization, evidence of assurance maintenance, and security impact analysis.

# CS378: Information Assurance and Security

## IA in the Military

Dr. Bill Young  
Department of Computer Science  
University of Texas at Austin

Last updated: February 6, 2015 at 08:38

# Why Study the Military

Why study IA in military contexts?

# Why Study the Military

## Why study IA in military contexts?

- Excellent case study for both defensive and offensive IA.
- Critically important protection domain that affects all of our lives.
- Historically, that's where IA has been developed.
- Most of the lessons of military IA can be adapted to other IA contexts.
- Others (?)

# IA in the Military

Historically, much of the work in Information Assurance has been contracted/subsidized by the military. Why do you think that is? Why does the government (particularly) care about IA?

# IA in the Military

Historically, much of the work in Information Assurance has been contracted/subsidized by the military. Why do you think that is? Why does the government (particularly) care about IA?

- The stakes are high: national security, national prestige, international advantage.
- IA is part of an intelligent defensive/offensive posture.
- The government has deep pockets and can afford to support broader research than other entities.
- Govt. concern for the national welfare goes well beyond strictly military matters. E.g., Financial losses attributable to malicious hacking, online corporate espionage and other computer crimes have a huge impact on commercial activity in this country.
- Others?

# U.S. DOD IA Emblem



# McAfee Report Findings

McAfee's *Virtual Criminology Report 2009* was focused on cyber warfare. They reported three key findings:

- ① Although there is no commonly accepted definition for cyber war today, we have seen nation-states involved in varying levels of cyber-conflict.
- ② If a major cyber conflict between nation states were to erupt, it is very likely that the private sector would get caught in the crossfire.
- ③ Too much of the debate on policies related to cyber war is happening behind closed doors.

# 1940–1960: IA Prehistory

IA is an outgrowth of (predominately US) military thinking of the role of computers, and more generally, automated info processing in defense.

Initial military uses of computers were cryptography and mathematics

- Electromechanical “Bombe” deciphered Enigma messages.
- ENIAC and later computers were used for computing tables and trajectories.

Most security efforts at that time are focused on physical security and information security on paper and in transmission. *Why do you think that's the case?*

TEMPEST programs were begun to deal with emissions security, i.e., leaking information via electromagnetic emanations.

# 1960–1985: Multi-User Systems

Early systems were single-task, single-user machines. The 1960's saw the development of time-sharing and resource-sharing systems, and multi-processing.

What additional security challenges did this introduce?

# 1960–1985: Multi-User Systems

Military contexts have a specific protection model for document access control.

- Information containers (files) have associated classification levels (CONFIDENTIAL, SECRET, etc.)
- May have additional restrictions (NOFORN, EYES ONLY, etc.).
- Users assigned clearance according to their trustworthiness, job responsibilities.
- Information access may be further compartmented into “need-to-know” categories (CRYPTO, NUCLEAR, etc.).  
Why?

Does this model translate well into the electronic world? Why or why not?

# 1960–1985: Multi-User Systems

Four models of operation were defined for computers handling classified information:

**dedicated:** all users cleared for all information on machine; no need for access control (MILS);

**system-high:** all users cleared, but must obey need-to-know compartments (discretionary access control).

**compartmented:** all users cleared, but must be need-to-know compartments (mandatory access control). System must handle requests across classifications.

**multi-level:** not all users cleared for all information; system enforces access control (MLS).

Multi-level is the most difficult so was not widely deployed.

RAND Report R-609-1, “Security Controls for Computer Systems,” (1970) summarizes best practice.

# 1985–1990: TCSEC

In 1985, the *Trusted Computer Systems Evaluation Criteria* (Orange Book) established a set of criteria by which the government could evaluate secure computer systems.

- Evaluation criteria for DoD purchase of COTS computer products.
- Criteria had four divisions: D (minimal protection) to A (verified protection), with several classes in most divisions (C1, C2, B1, B2).
- Most commercially viable systems did not seek certification.  
*Why do you think that was?*
- Only special purpose network products sought the highest certification levels (A1).

TCSEC was specifically for operating systems. No provisions for evaluating other security-related products.

## TCSEC (2)

TCSEC was superceded by Common Criteria, which we'll discuss later in the semester.

“Rainbow series” of books attempted to apply TCSEC across a wider class of products. ([see “Rainbow series” on Wikipedia](#))

Windows NT Workstation and many Unix-based operating systems achieved C2 rating (very weak, and often used configurations only generally of interest to the military).

Only Trusted XENIX and Multics operating systems obtained B2 rating. No general purpose operating system obtained A1 rating, only special purpose network products (Boeing MLS/LAN, Gemini Trusted Network Processor).

# 1960–1990: Military Networking

Early wide-area networks were based on person-to-person telegram messages, such as AUTODIN, begun in 1962.

ARPANET, for real-time data exchange, establishes first connection in 1969 between two researchers.

Computers on the early ARPANET network at many universities were accessible via dial-up, and these were not particularly secure. (ARPANET's password system was once compromised by two high school students.)

But some threats, such as viruses, were not yet known.

# 1980–present: Networking

Defense networks began to switch to TCP/IP in 1983. ARPANET was terminated in 1990 and replaced for military purposes by:

**NSFNET:** (1985–1995) for research, which became the backbone of the Internet.

**SIPRNET:** network for SECRET communication, has no connection to Internet. (Secret Internet Protocol Router NETwork)

**NIPRNET:** DoD network for unclassified, but sensitive communication, from which user can access Internet. (Non-classified IPR network)

Highly secure military applications may not be connected to any external network. Example: U.S. Navy submarines connect to SIPRNET only when surfaced and in a non-CSI mission phase.

# Nature of the Threat

*Cyber war is not occurring right now but nation-states are definitely in competition. Cyber weapons exist, and we should expect that adversaries might use them.*

*–McAfee Virtual Criminology Report 2009, p. 13*

*America's failure to protect cyberspace is one of the most urgent national security problems facing the new administration that will take office in January 2009. ... It is a battle we are losing. Losing this struggle will wreak serious damage on the economic health and national security of the United States. –CSIS report on Securing Cyberspace for the 44th Presidency, Dec. 2008*

# Information Warfare

In recent years, conventional combat has been augmented (or replaced) by information warfare—attacking the cyber-infrastructure of the adversary.

*In the very near future many conflicts will not take place on the open field of battle, but rather in spaces on the Internet, fought with the aid of information soldiers, that is hackers. This means that a small force of hackers is stronger than the multi-thousand force of the current armed forces.* —Nikolai Kuryanovich, Russian Deputy of the State Duma, March 2006

Thus, a large sponsor/consumer of IA activity is the military establishment.

# Cyber Warfare

The 2009 Virtual Criminology Report from McAfee says that cyber strikes could have a devastating impact on national infrastructure with power grids, water supplies and financial markets all at risk.

In their 2007 report, McAfee reported that approximately 120 countries have been developing ways to use the Internet as a weapon and target financial markets, government computer systems and utilities.

*Beijing is increasingly devoting itself to cyberwarfare. This is a cheap way to counter American dominance in traditional military fields. If the U.S. and China ever jostle with force, Beijing may hit us not with missiles but with cyberinfiltrations that shut down the electric grid, disrupt communications and tinker with the floodgates of dams. –Nicholas Kristof, The New York Times, January 18, 2010*

# Information Operations

Information Operations actions implement Information Warfare.

1998 *Joint Doctrine for Information Operations* defines IO as:  
“actions taken to affect adversary information and information systems while defending one’s own information and information systems.”

## *Offensive Information Operations*

- Target adversary decision makers and control systems
- “May have the greatest impact in peace and the initial stages of a crisis”
- Operations include “hacker brigades” that attempt to infiltrate and compromise adversary’s network-accessible systems

# Information Operations (2)

## *Defensive Information Operations:*

- Integrates and coordinates policies and procedures, operations, personnel, and technology
- Types of operations include:
  - typical information assurance measures
  - operations security (OPSEC)—a process for protecting information that denies an adversary the ability to compromise it
  - physical security—protection of or with physical assets (e.g. perimeters, mechanical defenses)
  - counterdeception—negating an attacker's deception attempt
  - counterpropoganda—exposing attacker's propoganda

# Information Operations Roadmap

In October, 2003, then-Secretary of Defense Donald Rumsfeld issued the *Information Operations Roadmap*, which was initially secret but subsequently released.

Google “Information Operations Roadmap 2003” to see a copy. You’ll note that it’s marked **SECRET/NOFORN**.

The release embarrassed the U.S. government because the document suggested that the U.S. was involved in significant PSYOPS activity, but didn’t distinguish external adversaries from the American public.

The Smith-Mundt Act (1948, amended 1972 and 1998) expressly prohibits the government from propagandizing the American public with information and psychological operations directed at foreign audiences.

# Information in War

Information Warfare (IW) is a key scenario for military IA. What does an attack look like? How do I prepare? How do I respond?

# Information in War

Information Warfare (IW) is a key scenario for military IA. What does an attack look like? How do I prepare? How do I respond?

Military strategist John Boyd came up with a characterization of strategic response to threat called the *OODA Loop*.

**Observe:** sensors transmit information about the attack to the commander.

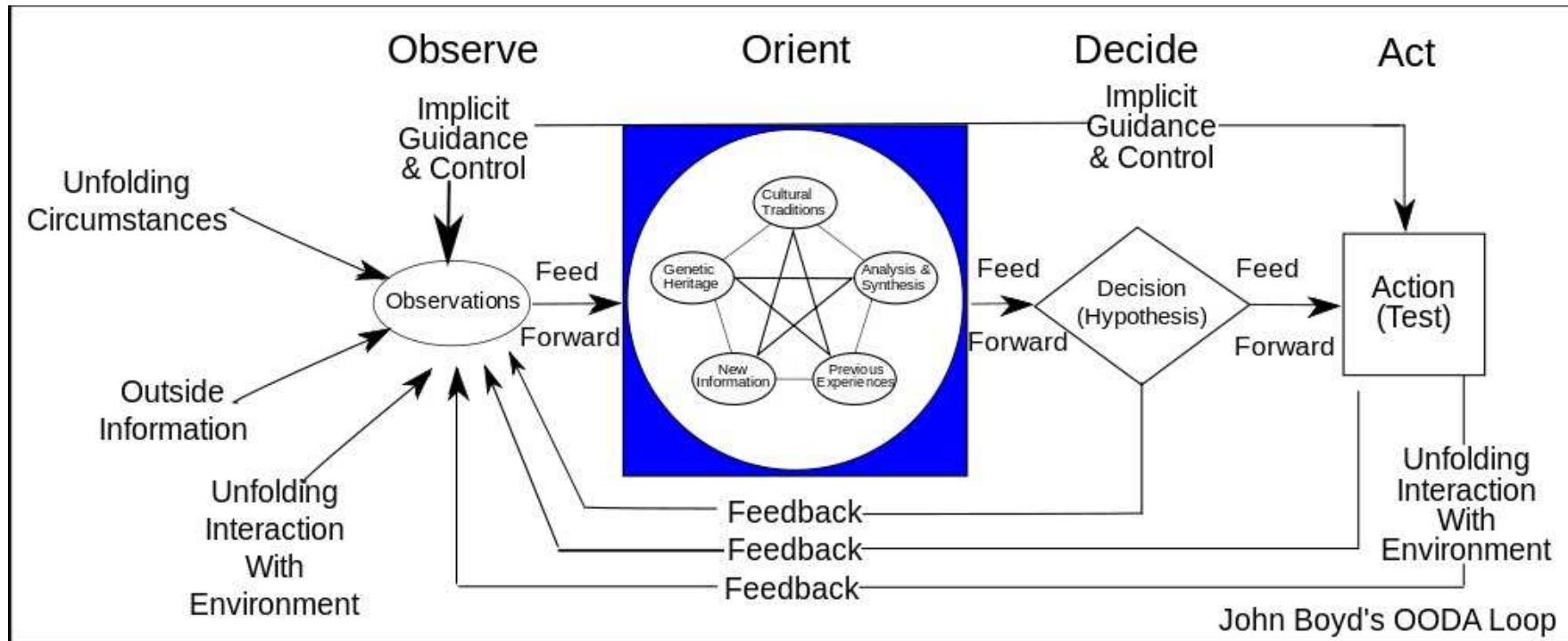
**Orient:** the information is interpreted by the commander.

**Decide:** the commander forms a plan of operation.

**Act:** the plan is carried out.

What do you think are the primary goals of the OODA loop?

# OODA Loop



From the Wikipedia page on OODA Loop.

# OODA Loop

The OODA Loop was originally applied to the combat operations process, but has been adapted for commercial operations and learning processes.

Ideally, an individual or an organization that can process the cycle quickly, observing and responding to unfolding events can gain a strategic advantage by “getting inside” the opponent’s decision cycle.

**Aside:** Boyd's thinking was instrumental in moving the US Air Force from heavy, powerful jet fighters such as the F-4 Phantom to lighter and more responsive jets such as the F-16 Falcon. What is the relationship between OODA and jet fighters?

# The OODA Loop

The OODA Loop provides a framework for formulating/evaluating a response, but must take into account whether one can/will respond.

If A launches an attack on B, what factors are likely to influence B's response?

# The OODA Loop

The OODA Loop provides a framework for formulating/evaluating a response, but must take into account whether one can/will respond.

If A launches an attack on B, what factors are likely to influence B's response?

- *B's perception of the situation:* based on data and resources available and many other factors.
- *B's capacity to act:* resources available to B to make a response.
- *B's will to act:* human factor hardest for A to quantify or affect.

This suggests that an offensive strategy should take these factors into account and attempt to influence them, if possible.

# Influencing the OODA Loop

What types of attack are possible?

# Influencing the OODA Loop

What types of attack are possible?

- *Physical attack*: destruction intended to reduce B's capacity to respond. (Example: D-Day 1944—massive shelling followed by invasion at Normandy beaches)
- *Deception*: reduces B's effectiveness in responding through distortion, concealment and false indications. (D-Day: fake invasion plans and exercises targeting Pas-de-Calais instead of Normandy)
- *Psychological attack*: cause B to become disoriented. (D-Day: dummy paratroopers dropped behind enemy lines)
- *Information attack*: explicitly target B's sensors and information infrastructure. (D-Day: French resistance and special ops teams cut telephone lines)

Remote access need not include physical force or even physical presence. Can warfare exist primarily at the information level?

# Some Information Attacks

*First Persian Gulf War (1991):* Iraq's command and control infrastructure is targeted. Radar and missile control network is fragmented and sections of radar coverage are taken offline without central control being aware of the outage.

*Estonia (2007):* Cyberattacks disabled the websites of government ministries, political parties, newspapers, banks, and companies. Russia was suspected of launching the attack in retaliation for the removal of the Bronze Soldier Soviet war memorial in central Tallinn.

*Georgia (2008):* Russia attacked the nation of Georgia in a dispute over the province of South Ossetia. In addition to the military attack, a concerted cyber DoS attack shut down much of Georgia's ability to communicate with the external world.

## Some Information Attacks (2)

Is the U.S. at risk from cyber attack? Do you think that the U.S. has already been attacked?

## Some Information Attacks (2)

Is the U.S. at risk from cyber attack? Do you think that the U.S. has already been attacked?

*Titan Rain:* series of coordinated attacks on American computer systems since 2003. The attacks were labeled as Chinese in origin, although their precise nature (i.e., state-sponsored espionage, corporate espionage, or random hacker attacks) and their real identities are unknown.

*Moonlight Maze:* series of alleged coordinated attacks on American computer systems in 1999. The attacks were traced to a computer in Moscow but it is not known if that is where they originated. It was claimed, though not certain, that these hackers had obtained large stores of data that might include classified naval codes and information on missile guidance systems.

Credible U.S. security experts suggest that a successful widespread attack on U.S. computing infrastructure could largely shut down the U.S. economy for up to 6 months.

# Objectives of Information Warfare

**Information dominance:** (typically at national level) obtain strategic and battlefield superiority, denying the enemy information or the systems on which to process it.

**Information protection:** (defensive) protect information systems from attack, and recover when attacks occur.

**Information attack:** (offensive)

- ***Disruption (denial of service):*** cause loss of or delay in accessing services
  - Attacks include jamming, physical destruction
  - Targets the *availability* of the information
- ***Corruption:*** change information or services; targets the *integrity* of the information
- ***Exploitation:*** gain access to protected information; targets the *confidentiality* of the information.

# Examples of Information Attacks

- **International context:** information wars between nations (or proxies)
- **Corporate context:** industrial espionage and sabotage
- **Interpersonal context:** impersonation and identity theft
- **Asymmetric contexts:** terrorism and hacking

# CyberWarfare Tactics

According to the Wikipedia article on CyberWarfare, these are the “methods of attack in cyberwarfare,” *ranked from mildest to most severe.*

1. *Cyber espionage:* the act or practice of obtaining secrets from individuals, competitors, rivals, groups, governments and enemies also for military, political, or economic advantage using illegal exploitation methods on internet, networks, software and or computers.
2. *Web vandalism:* attacks that deface web pages, or denial-of-service attacks. This is normally swiftly combated and of little harm.
3. *Propaganda:* political messages can be spread through or to anyone with access to the internet or any device that receives digital transmissions from the Internet to include cell phones, PDAs, etc.

# CyberWarfare Tactics (2)

4. *Gathering data*: classified information that is not handled securely can be intercepted and even modified, making espionage possible from the other side of the world. (Titan Rain and Moonlight Maze)
5. *Distributed Denial-of-Service Attacks*: large numbers of computers controlled by one person launch a DoS attack against systems
6. *Equipment disruption*: Military activities that use computers and satellites for coordination are at risk from this type of attack. Orders and communications can be intercepted or replaced, putting soldiers at risk.

# CyberWarfare Tactics (3)

7. *Attacking critical infrastructure:* Power, water, fuel, communications, commercial and transportation are all vulnerable to a cyber attack.
8. *Compromised/Counterfeit Hardware:* Common hardware used in computers and networks that have malicious software hidden inside the software, firmware or even the microprocessors.

# CyberWarfare Tactics (4)

The Wikipedia article on CyberWarfare ranks these *from mildest to most severe*.

- ① Cyber espionage
- ② Web vandalism
- ③ Propoganda
- ④ Gathering data
- ⑤ Distributed denial-of-service attacks
- ⑥ Equipment disruption
- ⑦ Attacking critical infrastructure
- ⑧ Compromised/counterfeit hardware

Do you agree with this ordering? Could it possibly be that compromised/counterfeit hardware is more of a threat than attacking critical infrastructure?

# CyberWarfare Tactics (5)

According to the Wikipedia article, the most severe attack strategy in CyberWarfare is: Compromised/Counterfeit Hardware. **Is that really a problem? Does it even happen?**

# CyberWarfare Tactics (5)

According to the Wikipedia article, the most severe attack strategy in CyberWarfare is: Compromised/Counterfeit Hardware. **Is that really a problem? Does it even happen?**

December 2009: “A federal grand jury has indicted four people accused of selling counterfeit Cisco Systems Inc. computer hardware through their Colorado-based company.”

How is this relevant to CyberWarfare?

# 2008 DefenseTech Article

From: [defensetech.org/2008/04/01:](http://defensetech.org/2008/04/01/)

*Recent events have raised the concerns about hidden backdoors and malicious code inside of counterfeit hardware all the way down to the integrated circuit level. In fact, a 2005 report by the Pentagon's Defense Science Board addresses this issue. While this report assessed the problem, recent events have now raised the anxiety over cyber sabotage in bogus hardware. In fact, many consider the use of compromised counterfeit hardware as a strategic tactic in cyber warfare. In January of 2008, a joint task force seized \$78 million of counterfeit Cisco networking hardware. This international effort resulted in over 400 seizures of counterfeit networking hardware that was shipped between China, Canada and the United States.*

# The Acquisition Problem

In addition to direct attacks on the national cyberstructure, the U.S. military is a consumer of vast amounts of commercial hardware/software. This is called *acquisition*, *procurement* or *supply chain*. Where do these products come from? How do we know they're reliable? Can we even tell? Is this just a problem for the military?

# The Acquisition Problem

In addition to direct attacks on the national cyberstructure, the U.S. military is a consumer of vast amounts of commercial hardware/software. This is called *acquisition*, *procurement* or *supply chain*. Where do these products come from? How do we know they're reliable? Can we even tell? Is this just a problem for the military?

The trend in government acquisition is toward commercial-off-the-shelf (COTS) products and services.

- (1991) Sec. of Defense Perry announces DoD Strategic Acquisition Initiative mandating a preference for COTS products.
- (1997) Sec. of Defense Cohen launches Defense Acquisition Reform Initiative that accelerated the preference for COTS in defense acquisition.

What do you think motivated this preference for COTS over GOTS or contract developments?

# Advantages of COTS Products

Preference for COTS products aims to obtain the latest technology at reduced cost, with shorter development and refresh cycles, and to leverage commercial investment and commercial best practices.

Do you think this is an effective strategy?

# Advantages of COTS Products

Preference for COTS products aims to obtain the latest technology at reduced cost, with shorter development and refresh cycles, and to leverage commercial investment and commercial best practices.  
Do you think this is an effective strategy?

Experience has shown that COTS products are often more:

- flexible
- scalable
- configurable
- maintainable

than products produced solely for the government

These benefits are exemplified by a reported *ten-fold reduction in price for U.S. Navy submarine sonar and combat systems over a ten year period*, with significantly enhanced capabilities. (Stevens)

# So What's the Downside

How could compromised hardware/software cause problems?

# So What's the Downside

How could compromised hardware/software cause problems?

An adversary intent on damaging U.S. national interests might insert unauthorized or damaging functionality which could be:

**active:** code that

- alters the behavior of critical systems,
- exfiltrates sensitive information,
- modifies programs or data,
- crashes a machine or network

**passive:** e.g., a backdoor to allow a future intruder to bypass the security protections of the system.

# Role of Acquisitions Policy

One of the CSIS recommendations “to make a noticeable improvement in the nations cybersecurity” is:

*Use acquisitions policy to improve security. The federal government is the largest single consumer of information technology products. We recommend that the United States buy only secure products and services; standards and guidelines for secure products should be developed in partnership with industry. (CSIS report, p. 2)*

Well, isn't that the solution to the acquisition problem? Just buy only secure products. So, what's the problem?

# Product Evaluation

*Trust, but verify. – Ronald Reagan*

**Question:** Isn't that what vulnerability scanners are for? Can't we just implement methods to ensure that acquired systems do not contain exploitable vulnerabilities?

# Product Evaluation

*Trust, but verify. – Ronald Reagan*

**Question:** Isn't that what vulnerability scanners are for? Can't we just implement methods to ensure that acquired systems do not contain exploitable vulnerabilities?

**Answer:** Not completely. The problem of detecting arbitrary malicious functionality is *undecidable*—there is no algorithm that can reliably distinguish between malicious and benign code.

# Malicious Software

Ken Thompson (1984 Turing Award lecture) noted that even complete control over source code is not sufficient to ensure the absence of malicious functionality, which can be introduced by the compiler, linker, loader, assembler, microcode, and even hardware.

*You can't trust code that you did not completely create yourself. (Especially code from companies that employ people like me.) No amount of source-level verification or scrutiny will protect you from using untrusted code. [...] As the level of program gets lower, these bugs will be harder and harder to detect. A well-installed microcode bug will be almost impossible to detect. –Ken Thompson*

# But We Can Try

**Example:** The U.S. Army requires that all systems receive a “certificate of networthiness” (CoN) before being deployed on Army networks.

According to the Army’s *Networthiness Certification Program for Information Systems*, networthiness encompasses:

*network security, network impact, compatibility with the total infrastructure, infrastructure requirements, spectrum support, security policy compliance, Foreign Ownership and Influence (FOCI), Joint Technical Architecture-Army (JTA-A) standards compliance, communications and information manpower, training, logistics support, schedule, and funding.*

The Army currently has a backlog of several thousand applications awaiting CoN evaluation by the 3 or so guys working for the Certification Program.

# Some Sobering Facts

- A recent study of 32,000 Websites found that *nearly 97% of sites carry a severe vulnerability.* –Web Application Security Consortium, Sept 2008
- “NSA found that inappropriate or incorrect software security configurations (most often caused by configuration errors at the local base level) were responsible for 80 percent of Air Force vulnerabilities.” –CSIS report on *Securing Cyberspace for the 44th Presidency*, Dec. 2008, p. 55.
- “Some U.S. government computer systems have shown significant security lapses.” –Bagchi, et al., Summer 2005

*But the fact that these statistics are available at all implies that significant classes of vulnerabilities can be detected.*

# There is Some Hope

The fact that a problem is undecidable *doesn't mean that there aren't useful steps that can be taken.*

Most vulnerabilities in software systems were introduced inadvertently rather than maliciously. In many cases, it is impossible to distinguish the two.

*Sufficiently advanced incompetence is indistinguishable from malice.* –Prof. Hovav Shacham

Historically, most vulnerabilities have not been recognized as such until someone discovered a way to exploit them.

*A good attack is one that the engineers never thought of.*  
–security guru Bruce Schneier

# There is Some Hope

The most common approach is *vulnerability scanning*, which seems to be the main approach of the Army currently. Several automated scanners are used by the CoN certifiers:

- **Nessus**: proprietary network scan tool, easily configured with plugins, available for Windows and Unix platforms.
- **Retina**: commercial network monitoring tool (Windows, Unix, others).
- **DISA Gold**: detect, report and remediate vulnerabilities in Windows.

There are many other tools out there. How could you decide what tools are the most appropriate? What factors enter into the decision?

# The Problem

*As we know, there are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns—the ones we don't know we don't know. And if one looks throughout the history of our country and other free countries, it is the latter category that tend to be the difficult ones.* —Donald Rumsfeld, Secy of Defense

Scanners are excellent tools for discovering *known vulnerabilities*, but a sophisticated adversary will craft the attack until it defeats the scanners. Explain.

**Example:** In tests of 36 commercial anti-virus products, fewer than half of the newest malicious software programs were identified. (research by Stuart Staniford of FireEye, Nov. 2008)  
What's the lesson here?

# Vulnerability Scanners

Vulnerability scanning has the following weaknesses:

- Scanners only test for known vulnerabilities; may not be effective against zero-day attacks.
- Only applicable to testable vulnerabilities; some may trigger on specific environmental conditions.
- Report presence/absence of vulnerabilities not potential for damage; e.g., foothold scenarios.
- May be limited to vulnerabilities on individual machines; some require a network of machines to exploit.

Explain zero-day attacks and foothold scenarios. How would you go about countering zero-day attacks?

# Dimensions of the Analysis

There are multiple dimensions in which to evaluate an analysis methodology.

**Objects of analysis:** What artifacts are available to the analyst—code (source, intermediate or object), an executable system, test vectors, etc.?

**Depth of analysis:** How thorough is the analysis carried out with any given tool?

**Required skillset:** What expertise is required to use a given tool effectively?

**Precision and accuracy:** Are specific methods likely to find all and/or only genuine vulnerabilities?

# Depth of Analysis

Another key dimension is how deep is the analysis.

**Black box methods:** take a purely external perspective on the object of analysis without knowledge of the internal details.

**Gray box methods:** apply limited knowledge of the internal working of the object to guide the analysis.

**White box methods:** relies on internal knowledge of the software to guide the analysis.

These categories are typically applied to generation of test cases, but can be applied to any analysis methods. Why would you ever use a more shallow analysis if a deeper analysis is possible?

# Depth of Analysis

Another key dimension is how deep is the analysis.

**Black box methods:** take a purely external perspective on the object of analysis without knowledge of the internal details.

**Gray box methods:** apply limited knowledge of the internal working of the object to guide the analysis.

**White box methods:** relies on internal knowledge of the software to guide the analysis.

These categories are typically applied to generation of test cases, but can be applied to any analysis methods. Why would you ever use a more shallow analysis if a deeper analysis is possible?

Which to use depends crucially on the available time and resources, toolset, artifacts for analysis, etc.

# Precision vs. Accuracy

We say that a vulnerability detection scheme is

**Precise:** if it never reports legitimate functionality as harmful,  
i.e., *no false positives*;

**Accurate:** if it detects all genuine vulnerabilities, i.e., *no false  
negatives*.

It is easy to build a scheme that is either accurate or precise; it's hard to do both simultaneously. Why?

Which is worse: false positives or false negatives? How would you go about estimating the rate of false positives/negatives in your system?

# Base-Rate Fallacy

When searching for events that are relatively rare in a population, even a moderately accurate detection scheme will return a high proportion of false positives.

**Example:** Suppose that only 1% of traffic is attacks and the detection accuracy is 90%. What percentage of raised alarms do you think will be false alarms?

# Base-Rate Fallacy

When searching for events that are relatively rare in a population, even a moderately accurate detection scheme will return a high proportion of false positives.

**Example:** Suppose that only 1% of traffic is attacks and the detection accuracy is 90%. What percentage of raised alarms do you think will be false alarms?

*Approximately 92% of raised alarms will be false alarms.*

What conclusions can you draw from this analysis?

Useful systems often have parameters that can be tuned to adjust the levels of false positives and false negatives depending on the environment and threat profile.

# CS361C: Information Assurance and Security

## IA in Business

Dr. Bill Young  
Department of Computer Science  
University of Texas at Austin

Last updated: February 13, 2015 at 14:24

# Relating IA to Business Needs

IA developed in a military context, but has obvious benefits for commercial enterprises. Like what?

# Relating IA to Business Needs

IA developed in a military context, but has obvious benefits for commercial enterprises. Like what?

- Enabling safe operation of business services
- Safeguarding assets
- Providing for recovery in case of disaster
- Assisting the organization in meeting regulatory requirements
- Obviating embarrassing disclosures of security lapses

Imagine that you are a consultant or IA officer in a business context. Some of you may well have that role in the future.

What are your goals/responsibilities? How does IA in business contexts differ from IA in military contexts?

# Importance of IA

Financial losses attributable to malicious hacking, online corporate espionage and other computer crimes have a huge impact on commercial activity in this country.

The Computer Security Institute estimates total losses due to computer crime of more than \$10 billion annually, mostly from financial fraud and proprietary information theft.

In one survey, 59% of companies reported attacks initiated from the Internet, and 38% reported attacks initiated from internal company computers.

# IA in Business Information Systems

*There is no security on this earth; there is only opportunity.* –Gen. Douglas MacArthur

The traditional emphasis of IA in corporations is in information security, particularly for networks and multi-user systems. However, there are often misconceptions about what is possible. “Perfect security” is impossible to achieve in practice. Why?

# IA in Business Information Systems

*There is no security on this earth; there is only opportunity.* —Gen. Douglas MacArthur

The traditional emphasis of IA in corporations is in information security, particularly for networks and multi-user systems. However, there are often misconceptions about what is possible. “Perfect security” is impossible to achieve in practice. Why?

- Real world systems are remarkably complex.
- Security cannot be just a feature of a product; it is part of a process to manage risk.
- The existence of countermeasures that could provide perfect security would imply that there is no risk—i.e., it has all been mitigated. However, it is likely that some threats and vulnerabilities have not yet been identified.

# Business IA Expectations

*“One of the most difficult achievements in technology is getting the resolve to spend on the possibilities of what if.” –Ron Barrett, Making High Availability Pay for Itself (2009)*

Business planning always involves a tradeoff between cost and benefits. Why?

# Business IA Expectations

*“One of the most difficult achievements in technology is getting the resolve to spend on the possibilities of what if.” –Ron Barrett, Making High Availability Pay for Itself (2009)*

Business planning always involves a tradeoff between cost and benefits. **Why?**

*Business is inherently profit-driven.* Deployment of security infrastructure in a business requires not only that costs must be justified, but that it meets the needs of the organization and users.

*Costs come in various forms.* If the security burden is so high for the users that it interferes with productivity, security functions will be bypassed reducing effectiveness of the system. **Give some examples.**

# Business IA Expectations

*Examples:* A cumbersome login process may have users logged in for weeks at a time. An IDS that gives repeated false alarms will be disconnected.

*“The number one reason for abandoning (on-line) transactions, as stated by survey respondents, was that the process was taking too long (48%). The research revealed people will opt for speed over the risks of maintaining their security online.” (Online Security: A Human Perspective, Oracle Systems, 2010)*

# Why Do Businesses Care?

If security is a cost, what motivates businesses to implement it?

# Why Do Businesses Care?

If security is a cost, what motivates businesses to implement it?

- Potential for loss
- Business reputation
- Competitive advantage
- Legislative and regulatory mandates
- others (?)

# Why Do Businesses Care?

*“Now that the Privacy Rights Clearing House maintains a comprehensive list of all known data breaches since 2005, major breaches live on in infamy long after the incident.”*  
*(Real World Data Loss Prevention Benefits, Sophos report, 2010)*

*“A recent survey reported that computer security is the critical attribute of corporate networks for 78 percent of executives. Another survey reported that security outweighed other concerns by a factor of three as the driving concern for IT improvements.”* (Landoll, The Security Risk Assessment Handbook, 2006)

# Legislation Driving IA

- *Computer Security Act* (1987): minimum security standards for Federal Agencies
- *Family Educational Rights and Privacy Act* (1974): protects student records in education
- *Health Insurance Portability and Accountability Act* (1996): regulates privacy and security in health care
- *Children's Online Privacy Protection Act* (COPPA) (1998): regulates privacy of children's online information
- *Gramm-Leach-Bliley Act* (1999): regulates security and privacy of financial records
- *Government Information Reform Act* (2000): redefines minimal security standards for government systems
- *Sarbanes-Oxley Act* (2002): regulates financial disclosure and audit for publicly held companies
- *North American Electric Reliability Council Cyber Security Standards* (2004): regulates security within electric systems industry

# Regulations and Best Practice

Regulations often define “best practice” within a *particular industry*. Different industries have different standards. Why should that be?

*“The term best practices is commonly used to connote a set of documented strategies, procedures, or methods employed by highly successful organization to effectively achieve results in a particular circumstance.” –The Perfect Online Course by Orellano et al., p. ix.*

# Regulations and Best Practice

*“There is no single definition of the ‘best practices’ for an information security program. ... In fact, the term ‘best practices’ for information security is really a misnomer or even could be considered a myth.” (Landoll)*

Discuss this assertion.

Security safeguards are generally identified as:

**technical:** access control, identification and authentication, encryption, intrusion detection, etc.

**non-technical:** management and operational controls (e.g., security policies), operational procedures, and personnel, physical, and environmental security.

The *Family Educational Rights and Privacy Act* of 1974, is a federal law that pertains to the release of and access to educational records.

FERPA applies to personally identifiable information in educational records.

- student's name
- names of family members
- addresses
- personal identifiers such as social security numbers
- personal characteristics or other information that make the student's identity easily traceable.

*Educational records* are all records that contain information directly related to a student and are maintained by an educational agency or institution, or by a party acting on its behalf.

These do not include:

- sole possession records: only accessible to the maker and used as personal memory aid.
- medical or psychological treatment records that include those maintained by physicians, psychiatrists, and psychologists;
- employment records, provided that employment is not contingent upon being a student;
- law enforcement records;
- records collected about an individual after that person is no longer a student.

# Student Rights under FERPA

Any student has a right to

- inspect and review his or her educational records;
- request to amend his or her educational records;
- have some control over the disclosure of information from his or her educational records.

# Directory Information

UT designates some information as *Directory information* that may be disclosed without the student's permission, including

- Student's name
- Local, permanent, and email addresses
- UT eid public username
- Telephone listing
- Date and place of birth
- Major fields of study
- Dates of attendance
- Enrollment status
- Degrees, awards, and honors received, including selection criteria
- Most recently attended previous educational institution
- Classification
- Expected graduation date
- Certain other.

# Who Can See Your Records

Nondirectory information may not be released without prior written consent from the student. Exceptions include:

- access by appropriate university administrators, faculty members, or staff members who require access to educational records in order to perform their legitimate educational duties;
- officials of other schools in which the student seeks or intends to enroll;
- in connection with a student's application for, or receipt of, financial aid.

Which of the following does FERPA describe: goals, consequences, policies, mechanisms? Keep that question in mind for each of the other legislative mandates.

# Regulations Driving IA: HIPAA

*Health Insurance Portability and Accountability Act (HIPAA)* (1996) establishes safeguards that health care providers must use to protect personal information. The goal is to:

*... improve the portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and healthcare delivery, to promote medical savings accounts, to improve access to long-term care services and coverage, and to simplify the administration of health insurance.*

# Regulations Driving IA: HIPAA

HIPAA is concerned with several issues:

- Addresses the ability to transfer insurance when changing jobs, and maintaining insurance after leaving a job.
- Addresses protecting the privacy of medical records as they are transferred among physicians, hospitals, clinics, pharmacies, and insurance providers.

HIPAA involves two separate rules with fairly specific IA components:

- ① Security Standards Final Rule;
- ② Standards for the Privacy of Individually Identifiable Health Information Final Rule.

In this context, explain the difference between security and privacy.

# HIPAA: Security Standards Rule

Healthcare entities must:

- Ensure the confidentiality, integrity and availability of all “electronic protected health information” they create, receive, maintain, or transmit;
- Protect against anticipated threats or hazards to the security or integrity of such information;
- Protect against anticipated uses or disclosures of info that are not permitted or required;
- Ensure compliance by its workforce with all provisions of the bill.

HIPAA does not mandate specific technical solutions. Is this a good idea or not? Why “anticipated” threats?

# HIPAA Admin Security Safeguards

HIPAA either requires (R) or addresses (A) various specific administrative security safeguards:

- *Security Management*: including risk analysis, risk management, sanction, system activity review.
- *Assigned Security Responsibility*.
- *Workforce Security*: authorization and supervision, clearance, termination procedures.
- *Information Access Management*: isolating clearinghouse functions, access authorization, access establishment and modification.

# HIPAA Admin Security Safeguards (continued)

- *Security Awareness and Training:* reminders, malicious software, log-in monitoring, password management.
- *Security Incident Procedures:* response and reporting.
- *Contingency Planning:* data backup, disaster recovery, emergency mode plan, testing and revision, application and data criticality analysis.
- *Evaluation.*
- *Business Associate Contracts and Other Arrangements.*

# HIPAA Physical Security Safeguards

HIPAA defines certain **physical security** safeguard categories:

- *Facility Access Controls*: contingency operations, facility security plan, access control and validation, maintenance records.
- *Workstation Use*.
- *Workstation Security*.
- *Device and Media Controls*: disposal, media reuse, accountability, data backup and storage.

# HIPAA Technical Security Safeguards

HIPAA also defines certain **technical security** safeguard categories:

- *Access Control*: unique user ID, emergency access procedures, automatic logoff, encryption and decryption.
- *Audit Controls*.
- *Integrity*: mechanism to authenticate electronic protected health info.
- *Person or Entity Authentication*.
- *Transmission Security*: integrity controls, encryption.

# HIPAA Privacy Requirements

The Privacy Rule is less specific than the Security Rule. It demands protection of “individually identifiable health information” defined as:

*Information that is a subset of health information, including demographic information collected from an individual, and (1) is created or received by a health care provider, health plan, employer, or health care clearinghouse, and (2) relates to the past, present, or future physical or mental health, or condition of an individual; the provision of health care to an individual, or the past, present, or future payment for provision of health care to an individual, and (a) that identifies the individual, or (b) with respect to which there is reasonable basis to believe that the individual can be used to identify the individual.*

# HIPAA Privacy Requirements

To disclose information, authorization is required including:

- description of the information
- identification of those authorized to disclose or use
- statement of purpose of the use or disclosure
- expiration date for the authorization
- signature of the individual, parent or guardian
- statement of and procedures for revoking the authorization
- consequences of not signing an authorization
- potential re-disclosure of the info by recipient

Items from a “limited data set” may be disclosed, but must not contain any specific identifying info such as names, SSNs, URLs, etc. *What do you think this “limited data set” provision is about?*

# Other Health Related Mandates

The *Patient's Omnibus Transaction on Mandatory Information Security* is a follow-on to HIPAA and provides additional protection relating to financial reporting and disclosure.

# Other Health Related Mandates

The *Patient's Omnibus Transaction on Mandatory Information Security* is a follow-on to HIPAA and provides additional protection relating to financial reporting and disclosure.

The two together form the HIPAA-POTOMIS suite of regulations.

# Other Health Related Mandates

The *Patient's Omnibus Transaction on Mandatory Information Security* is a follow-on to HIPAA and provides additional protection relating to financial reporting and disclosure.

The two together form the HIPAA-POTOMIS suite of regulations.

*If you haven't figured it out by now, this slide is a joke and can safely be ignored.*

# HITECH Act

*The Health Information Technology for Economic and Clinical Health Act* (HITECH) is Title XIII of the 2009 American Recovery and Reinvestment Act (ARRA). It expands the reach of HIPAA.

Reserves \$22 billion to “advance the use of health information technology” to move toward Obama’s promised e-health records.

- Expands HIPAA data privacy and security requirements to include “business associates” of entities subject to HIPAA.
- Strengthens HIPAA enforcement measure to include civil and criminal penalties.
- Monetary penalties become mandatory for “willful neglect.”

Penalties are funneled back to HHS Office of Civil Rights enforcement, leading some to fear that this may encourage more punitive enforcement.

# Regulations Driving IA: Sarbanes-Oxley

*Sarbanes-Oxley Act (SOX) (2002)* affects all US publicly traded companies.

The rules were designed to: ...protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws ... to protect the interests of investors and further the public interest in the preparation of informative, accurate, and independent audit reports for companies the securities of which are sold to, and held by and for, public investors.



- Congress dramatically increased fines and penalties for fraudulent corporate financial reporting.
- Section 404 requires disclosure of the management's internal controls over financial reporting.
- Provisions apply to all corporations required to file annual reports by U.S. Securities and Exchange Commission.
- CIOs are responsible for the security of the Enterprise Resource Planning (ERP) systems which generate financial reports.
- Does not mandate particular internal control methodology.

In a survey of 217 companies with annual revenues of \$5 billion, average one-time start-up cost was \$4.26 million, or 0.0825 percent of annual revenue.

# Sarbanes-Oxley and IT

The IT community cares for the following two reasons:

- ① Requires certifying the accuracy and attesting to the reliability of financial reports.
- ② Mandates adequate internal controls to ensure the accuracy and reliability of IT systems and operational procedures used to generate financial reports.

A large percentage of these internal controls is expected to relate to the design, development, operation and interaction with information systems. I.e., ensuring data, information, systems, and network integrity.

What does this mean for IT management at a publicly traded company?

# Regulations Driving IA: GLBA

*Financial Services Modernization Act* (1999) (also known as Gramm-Leach-Bliley Act or GLBA) eliminates many of the barriers between banks, brokerage firms, and insurance companies.

Title V of GLBA declares that:

*“each financial institution has ... a continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers’ nonpublic personal information.”*

Nonpublic personal information is defined as:

*“personally identifiable financial information: (i) provided by a consumer to a financial institution; (ii) resulting from any transaction with the consumer or any service performed for the consumer; or (iii) otherwise obtained by the financial institution.”*

# Regulations Driving IA: GLBA

It also requires banks:

- “to insure the security and confidentiality of customer records and information;
- to protect against any anticipated threats or hazards to the security or integrity of such records;
- to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.”

Financial institutions must provide customers with information relating to their privacy policies and procedures (and changes to it). Customers can *opt out* of any disclosures they don't like.

Why “anticipated threats”? Discuss the pros and cons of opt out vs. opt in policies.

# Regulations Driving IA: GLBA

Despite GLBA, a 2003 study found that:

- ① 66 percent of financial institutions surveyed had one or more Web forms that collected personally identifiable information but did not use SSL encryption;
- ② 91 percent of these institutions used weak SSL encryption, such as 40-bit RC4, rather than the 128-bit encryption then recommended by federal bank regulators.

**Upshot:** A regulation is only as good as its enforcement.

Do you think the figures would be a lot better today?

# Regulations Driving IA: FISMA

From Wikipedia:

*The Federal Information Security Management Act of 2002 is a federal law enacted in 2002. ... The act recognized the importance of information security to the economic and national security interests of the United States. The act requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems. ... FISMA has brought attention within the federal government to cybersecurity and explicitly emphasized a “risk-based policy for cost-effective security.”*

# Threats to Business Information

What do you think are the major threats to business information?

# Threats to Business Information

What do you think are the major threats to business information?

- *Human error or failure:* mistakes of authorized users may compromise confidentiality, integrity, availability.
- *Intellectual property compromise:* software piracy, unauthorized duplication violating software licensing. Business Software Alliance ([www.bsa.org](http://www.bsa.org)) active to reduce this.
- *Espionage/trespass:*
  - Industrial espionage: companies gathering competitive information on other companies. May also involve national intelligence services.
  - Shoulder surfing or dumpster diving: opportunistic acquisition of carelessly guarded or discarded information.
  - Hackers: have techniques and tools to locate and target vulnerabilities in order to trespass.

# Threats to Business Information

- *Extortion:*
  - After assets (e.g. credit card numbers) are stolen, blackmailing the target to pay
  - If the target refuses to pay, the assets might be sold to other criminals.
- *Sabotage:*
  - The most common form is web page defacement. 95% of large organizations reported in 2005 “more than 10 incidents” involving the website, though not all were successful attacks.
  - More damaging is damage to infrastructure control systems, for defense, utilities, telecommunications, etc. (In 1996 a juvenile hacker compromised the phone system used by Worcester, MA air traffic control, fire department and '911' system.)

# Other Threats to Information

- *Theft*: loss of electronic assets more difficult to detect than loss of physical assets.
- *Software attacks (malware)*: viruses, worms, trojan horses, DoS attacks, etc.
- *Forces of Nature*:
  - Major disasters: (fire, flood, earthquake, lightning, landslide, tornado, hurricane, tsunami); effects can often be mitigated via insurance and physical design
  - Small-scale attacks: (rodents, electrostatic damage, dust, conductive contamination).

# Other Threats to Information

- *Other Factors:*
  - Quality of service issues:
    - Service providers (power, network connectivity) may experience failure or degradation in quality.
    - Backup services, where available, may not provide same quality of service as normal providers.
  - *Hardware and software failures*
  - *Technology obsolescence:* many organizations still depend on Windows NT or Window 2000, even though these are not actively maintained.

# Business Impact of Computer Insecurity

According to a 2005 CSI/FBI Computer Crime and Security Survey:

- 56% of organizations had known, unauthorized use of computer systems.
- Approximately the same number of incidents resulted from insider threats as from outsiders.
- Top three causes of loss: viruses, unauthorized access, theft of proprietary information
- 97% of organizations use firewalls, 96% use antivirus software, approximately the same percentage as in 2004.
- Actual losses are typically not known, as only 20% of organizations report intrusions.
  - 43% claim reporting to law enforcement would hurt their stock/image
  - 33% claim competitors would use this to their advantage

# Approaches to Business IA

There are several points in an org chart where IA decisions can originate. Organizations typically drive IA decisions in one of two patterns:

**Bottom-up:** IA decisions originate from those closest to the information assets such as system administrators and technologists.

**Top-down:** senior management determines the policies, goals and outcomes for IA projects.

If you were tasked to develop a comprehensive IA program for your company or agency, which approach would you choose (or perhaps some hybrid of the two)?

# Bottom-up Approach to IA

In a *bottom-up* approach, those closest to information assets (system administrators) originate IA decisions.

- In the 1990s as companies attached to the Internet, system administrators often were responsible for identifying the need for security technology, selecting appropriate products, and deploying the products.
- Administrators have in-depth knowledge of the systems being managed, and are most aware of associated vulnerabilities and threats.
- Such IA projects are often funded as one-time special projects or as part of an overall infrastructure cost to the business of having IT services.

# Bottom-up Approach

The bottom-up approach appears most frequently in:

- R&D organizations operating their own unique IT infrastructure
- groups creating or tracking emerging technologies
- small or decentralized organizations.

# Evaluating the Bottom-up Approach

Is the bottom-up approach a viable long-term solution for business-critical information systems?

# Evaluating the Bottom-up Approach

Is the bottom-up approach a viable long-term solution for business-critical information systems?

**No!**

- Solutions may not have buy-in from all involved parties, such as systems' end users.
- Approach likely does not have senior management awareness or participation. Costs and benefits not known to management, so cannot budget for IA.
- In large organizations, different IT teams may select incompatible technologies for solving similar problems.
- Turnover of IT staff may create an unrecognized knowledge gap.

# Top-down Approach to IA

In a *top-down* approach, the IA program is initiated by senior business management, which determines policy, goals and outcomes for IA projects.

Program's processes may flow through organization in several ways:

- ① Each level of management writes increasingly more specific statements on the IA process, and delegates implementation to the level below.
- ② An IA project team may be set up, responsible for implementation and coordinating with each line-of-business.
- ③ A federated approach, such as in multinationals, in which each part of the company chooses an approach to implementation, but may be required to coordinate on selected areas across the organization.

# Success Factors in Top-Down Approach

Top-down projects are often more likely to receive consistent funding, be integrated into organizational culture, and involve all necessary parties for a successful outcome.

The IA program should have a *champion* within senior management.

- Could be Chief Information Officer (CIO), Chief Information Security Officer (CISO), or VP of information technology or network operations.
- Establishes business goals of the program and ensures integration of requirements into budget and planning.
- The champion may also establish an integration roadmap or timeline to ensure that projects move ahead.

IA projects in a top-down approach typically follow a system development lifecycle model. The IA project is thus tracked similarly to other IT projects within the organization.

# Senior Management Involvement

How should you organize IA management within your company?

How does UT do it?

**Chief Information Officer:** establishes IA strategy and communicates with other managers.

**Chief Information Security Officer:** responsible for information security across the organization.

**Chief Technology Officer:** often responsible for special projects, not part of normal IT operations.

**VP for Information Technology:** responsible for IT services.

**VP of Network Operations:** responsible for operating data networks and related servers.

**Other VPs and managers:** may have their own IT infrastructure for line-of-business services.

**Auditors:** certify that the organization has correctly reported, and may validate the IA services that protect the data for such reports.

# IA Project Teams

Possible roles with an IA deployment project:

**Champion:** promotes the project and ensures its visibility to appropriate management.

**Team leader:** manager who tracks the project status and ensures it meets goals.

**Policy specialists:** identify security policies appropriate for the organization.

**Risk assessment specialists:** coordinate risk assessment process used in IA and financial/business risk management.

**Security professionals:** specialists in information security (technical and non-technical).

**System administrators:** responsible for administering the systems and networks being protected.

**End users:** selected users validate that the approach does not disrupt business activities.

**Lead developers:** IA projects may need custom software engineering to integrate with existing systems.

# Data Ownership and Flow

Three roles of data ownership:

- *Data owners* are responsible for the security and use of a particular category of data, and are typically senior managers.
- *Data custodians* are responsible for implementing the security and storage of data, often CISO or system administrators' responsibilities. Backup and recovery is of primary interest to the data custodian.
- *Data users* are the end users who interact with the data in order to fulfill a business function, and are typically integral in maintaining the security of data.

Explain the relationships among these various roles.

# Data Ownership and Flow (2)

Multiple groups fill each role, as data flow throughout the organization.

- The process of creating new data, such as new accounts for customers in a database, is called *provisioning*.
- The authoritative database known to have correct (or best) information and supplies updates is called the *System of Record* database.

# Communities of Interest

A *community of interest* is a group (may be distributed) with similar interests and a common goal within an organization.

*Information Security:* protects the organization's information systems and information from attack.

*Information Technology:*

- Manage IT costs, ease-of-use, timeliness, performance.
- May conflict with information security community as goals are not always aligned.

*Organizational:*

- General management, and the rest of the organization.
- To IT, these are “end users”; to Information Security, these are “subjects.”
- Goals of IT and information security must be aligned with organizational goals.

Describe effects of having multiple communities of interest.

# Other Organizational Roles in IA

A *security office* may be responsible for developing organizational security policies, and implementing certain policies, such as physical site security.

A *telecommunications office* may be responsible for maintaining the security of voice, video and data communications.

The functions of the *INFOSEC Officer* varies, and may include:

- managing an information security team
- reviewing operations which might impact information security (e.g., adding a modem dial-in line).
- performing risk assessments
- compiling documents of best practices for information security

# Other Organizational Roles in IA

In government and contractor organizations:

- The *COMSEC Custodian* is responsible for safeguarding of communications security devices used in discussing classified information and training end users.
- The *OPSEC Manager* is responsible for identifying potential adversaries and their information targets, and developing security countermeasures.

# A Security Systems Development Lifecycle

A security systems development lifecycle is a methodology:

- A methodology is a formal approach to problem solving based on a structured sequence of procedures.
- The lifecycle will have an end goal, as well as intermediate milestones, and a project team will be held accountable to meeting milestones and the end goal.

The process is started by an event or conditions, e.g. responding to a break-in or meeting shareholder/regulatory requirements.

# A Security Systems Development Lifecycle

Often the lifecycle is based on the Waterfall model, and a feasibility analysis at the end of each phase:

- ① Investigation
- ② Analysis
- ③ Logical design
- ④ Physical design
- ⑤ Implementation
- ⑥ Maintenance and change

In some organizations, one or more of these phases may be outsourced. (According to a 2005 survey: 26% outsource up to 20% of security functions; 63% outsource none)

# Phases of Security Systems Development Lifecycle

- *Investigation*

- Specify objectives, constraints and scope of the project, and develop cost-benefit analysis.
- Begin an *enterprise information security policy* document, as well as dictates from management of expected outcomes and budget.
- Organize project teams, determine whether the organization has necessary resources and commitment for success.

- *Analysis*

- Assess the organization, current systems and policies, and functions and interactions of the new system.
- Analyze legal constraints, current threats and countermeasures.
- Begin risk management process.

# Phases of Security Systems Development Lifecycle

- *Logical design*

- Create a system solution for the business need. Select applications, data, and ranges for technology alternatives. The logical design is implementation independent.
- Establish IA policies, including
  - incident response: actions to take when an attack occurs
  - disaster recovery: immediate recovery of information and systems after a loss
  - continuity planning: how business will continue in the event of a loss.

- *Physical design*

- Select specific technologies, perform build-vs-buy tradeoffs and establish success criteria
- Develop *information security blueprint* document and physical security measures
- Present entire solution to management for approval and signoff.

# Phases of Security Systems Development Lifecycle

- *Implementation*

- Create or acquire software and test components.
- Train users and test whole system.
- Provide sponsors with a performance review and acceptance test results.

- *Maintenance and Change*

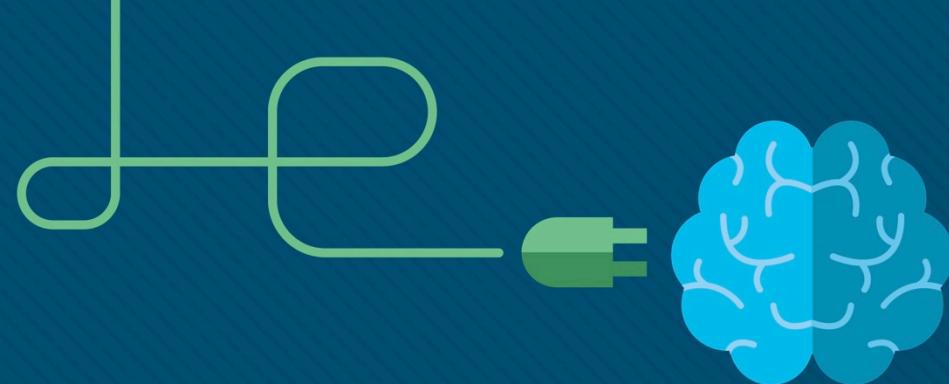
- Support and modify the system as needed for the rest of its life cycle.
- Monitor and validate, upgrade countermeasures, repair and recover as needed.
- Longest and possibly most expensive phase.



# Chapter 1: The Need for Cybersecurity

Instructor Materials

Introduction to Cybersecurity v2.1



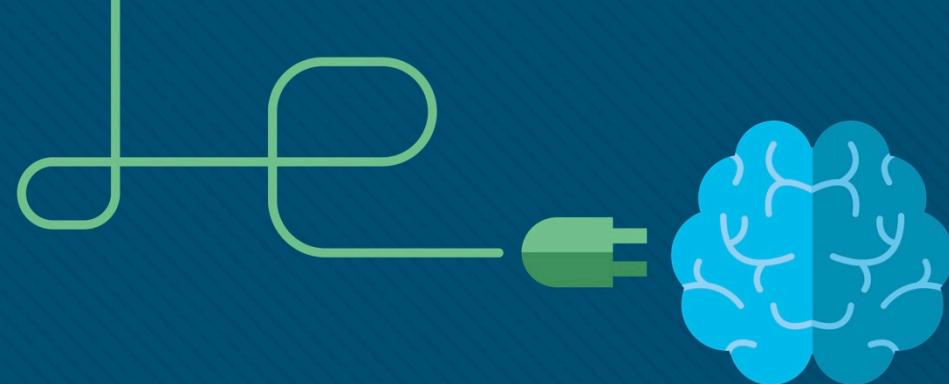
# Chapter 1: The Need for Cybersecurity

**Introduction to Cybersecurity v2.1  
Planning Guide**



# Chapter 1: The Need for Cybersecurity

Introduction to Cybersecurity v2.1



# Chapter 1 - Sections & Objectives

- **1.1 Personal Data**

- Explain the characteristics and value of personal data.
  - Define personal data.
  - Explain why personal data is profitable to hackers.

- **1.2 Organization Data**

- Explain the characteristics and value of data within an organization.
  - Describe types of data used by governments and organizations.
  - Describe the impact of a security breach.

- **1.3 Attackers and Cybersecurity Professionals**

- Explain the characteristics and motives of cyber attackers and the legal and ethical issues for cybersecurity professionals.
  - Describe the characteristics and motives of an attacker.

- **1.4 Cyberwarfare**

- Explain the characteristics and purpose of cyberwarfare.
  - Describe cyberwarfare.



# 1.1 Personal Data

# Introduction to Personal Data

- What is Cybersecurity?
  - Protection of networked system and data from unauthorized use or harm
- Your Online and Offline Identity
  - Offline Identity
    - Your identity that interacts on a regular basis at home, school or work
  - Online Identity
    - Your identity while you are in cyberspace
    - Should only reveal a limited amount of information about you
    - Username or alias
    - Should not include any personal information
    - Should be appropriate and respectful
    - Should not attract unwanted attention



## Personal Data

# Introduction to Personal Data

- Your Data

- Medical Records
  - electronic health records (EHR) – physical, mental, and other personal information
  - prescriptions
- Education Records
  - Grades, test scores, courses taken, awards and degrees rewarded
  - Attendance
  - Disciplinary reports
- Employment and Financial Records
  - Income and expenditures
  - Tax records – paycheck stubs, credit card statements, credit rating and banking statement
  - Past employment and performance



# Introduction to Personal Data

- Where is Your Data?
  - Medical records: doctor's office, insurance company
  - Store loyalty cards
    - Stores compile your purchases
    - Marketing partner uses the profiles for target advertisement
  - Online pictures: friends, strangers may also have a copy
- Your Computer Devices
  - Data storage and your portal to your online data
  - List some example of your computing devices



## Personal Data

# Personal Data as a Target

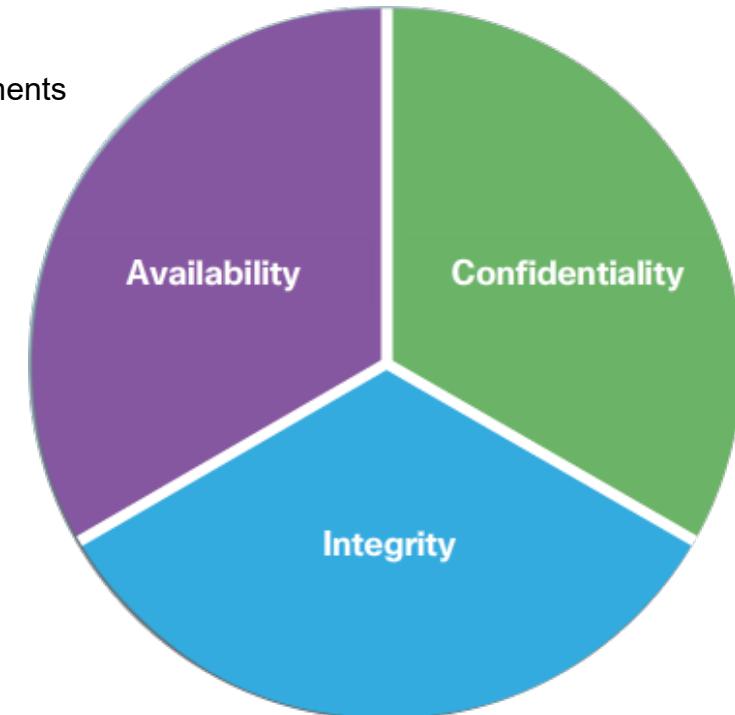
- How do the criminals get your money?
  - Online credentials
    - Gives thieves access to your accounts
  - Creative schemes
    - Trick into wiring money to your friends or family
- Why do they want your identity?
  - Long-term profits
  - Medical benefits
  - File a fake tax return
  - Open credit card accounts
  - Obtain loans



# 1.2 Organizational Data

# Introduction to Organizational Data

- Types of Organizational Data
  - Traditional Data
    - Personnel – application materials, payroll, offer letter, employee agreements
    - Intellectual – patents, trademarks, product plans, trade secrets
    - Financial – income statements, balance sheets, cash flow statements
  - Internet of Things and Big Data
    - IoT – large network of physical objects, such as sensors
    - Big Data – data from the IoT
- Confidentiality, Integrity and Availability
  - Confidentiality – privacy
  - Integrity – accuracy and trustworthiness of the information
  - Availability – information is accessible



## Lab – Compare Data with a Hash



### Lab – Compare Data with a Hash

#### Objectives

Use a hashing program to verify the integrity of data.

#### Background / Scenario

It is important to understand when data has been corrupted or it has been tampered with. A hashing program can be used to verify if data has changed, or if it has remained the same. A hashing program performs a hash function on data or a file, which returns a (usually much shorter) value. There are many different hash functions, some very simple and some very complex. When the same hash is performed on the same data, the value that is returned is always the same. If any change is performed on the data, the hash value returned will be different.

**Note:** You will need installation privileges and some knowledge of the process to install Windows programs.

#### Required Resources

- PC with Internet access

#### Step 1: Create a Text file

- a. Search your computer for the Notepad program and open it.
- b. Type some text in the program.

# The Impact of a Security Breach

- The Consequences of a Security Breach
  - Not feasible to prevent every attack
  - Attackers will always find new ways
  - Ruined reputation, vandalism, theft, revenue lost, damaged intellectual property
- Security Breach Example - LastPass
  - An online password manager
  - Stolen email addresses, password reminders, and authentication hashes
  - Requires email verification or multi-factor authentication when logging in from an unknown device
  - Users should use complex master password, change master password periodically, and beware of phishing attacks



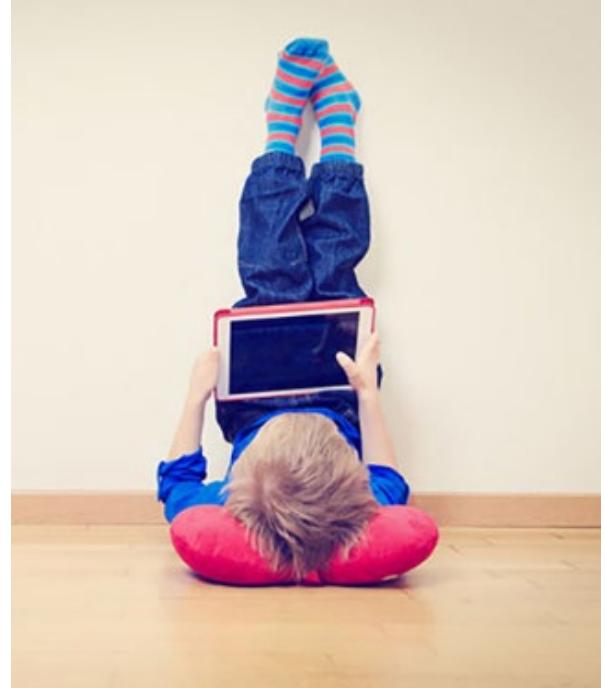
# The Impact of a Security Breach

- Security Breach Example - Vtech

- Vtech is a high tech toy maker for children
- exposed sensitive information including customer names, email addresses, passwords, pictures, and chat logs.
- Vtech did not safeguard information properly
- Hackers can create email accounts, apply for credits, and commit crimes using the children's information
- Hackers can also take over the parents' online accounts

- Security Breach Example - Equifax

- Equifax is a consumer credit reporting agency.
- Attackers exploited a vulnerability in web application software.
- Equifax established a dedicated web site with a new domain name that allowed nefarious parties to create unauthorized websites for phishing scheme



# The Impact of a Security Breach

## Lab – What Was Taken?



### Lab – What was Taken?

#### Objectives

Search for and read about a few recent occurrences of security breaches.

#### Background / Scenario

Security breaches occur when individuals or applications are trying to gain unauthorized access to data, applications, services, or devices. During these breaches, the attackers, whether they are insiders or not, attempt to obtain information that they could use for financial gains or other advantages. In this lab, you will explore a few security breaches to determine what was taken, what exploits were used, and what you can do to protect yourself.

#### Required Resources

- PC or mobile device with Internet access

#### Security Breach Research

- a. Use the two provided links to security breaches from different sectors to fill out the table below.
- b. Search for a few additional interesting breaches and record the findings in the table below.

# 1.3 Attackers and Cybersecurity Professionals

# The Profile of a Cyber Attacker

## Types of Attackers

- Amateurs
  - Script kiddies with little or no skill
  - Using existing tools or instructions found online for attacks
- Hackers - break into computers or networks to gain access
  - White hats – break into system with permission to discover weaknesses so that the security of these systems can be improved
  - Gray hats – compromise systems without permission
  - Black hats - take advantage of any vulnerability for illegal personal, financial or political gain
- Organized Hackers - organizations of cyber criminals, hacktivists, terrorists, and state-sponsored hackers.

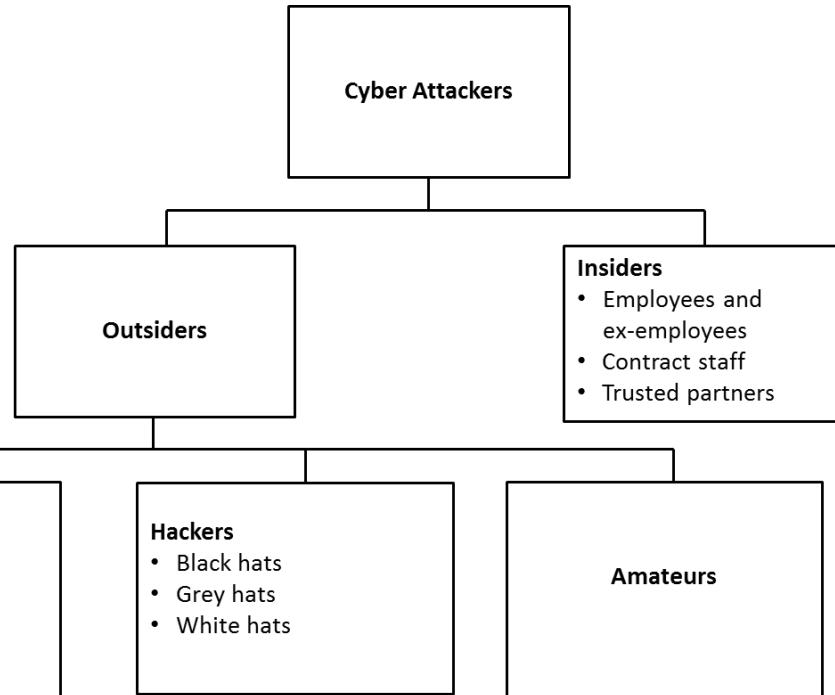


# The Profile of a Cyber Attacker

## Internal and External Threats

### Internal Security Threats

- Can be an employee or contract partner
  - Mishandle confidential data
  - Threaten the operations of internal servers or network infrastructure devices
  - Facilitate outside attacks by connecting infected USB media into the corporate computer system
  - Accidentally invite malware onto the network through malicious email or websites
  - Can cause great damage because of direct access



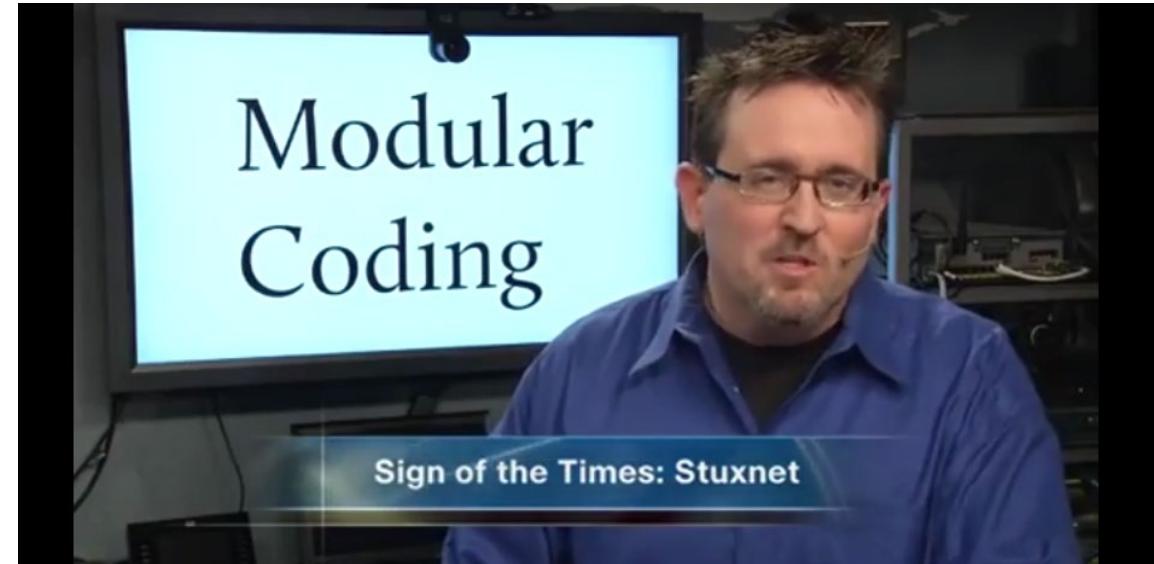
### External Security Threats

- exploit vulnerabilities in network or computing devices
- use social engineering to gain access

# 1.4 Cyberwarfare

# What is Cyberwarfare

- What is Cyberwarfare?
  - Conflict using cyberspace
  - Stuxnet malware
    - Designed to damage Iran's nuclear enrichment plant
    - Used modular coding
    - Used stolen digital certificates



# The Purpose of Cyberwarfare

- Use to gain advantage over adversaries, nations or competitors
  - Can sabotage the infrastructure of other nations
  - Give the attackers the ability to blackmail governmental personnel
  - Citizens may lose confidence in the government's ability to protect them.
  - Affect the citizens' faith in their government without ever physically invading the targeted nation.



# 1.5 Chapter Summary

# Chapter Summary

## Summary

- Define personal data.
- Explain the characteristics and value of personal data.
- Explain the characteristics and value of data within an organization.
- Describe the impact of security breach.
- Describe the characteristics and motives of an attacker.
- Describe the legal and ethical issues facing a cybersecurity professional.
- Explain the characteristics and purpose of cyberwarfare.





# Chapter 2: Attacks, Concepts and Techniques

Instructor Materials

Introduction to Cybersecurity v2.1



# Chapter 2: Attacks, Concepts and Techniques

**Introduction to Cybersecurity v2.1  
Planning Guide**





# Chapter 2: Attacks, Concepts and Techniques

Introduction to Cybersecurity v2.1

# Chapter 2 - Sections & Objectives

- 2.1 Analyzing a Cyberattack

- Explain the characteristics and operation of a cyber attack.
  - Explain how a security vulnerability is exploited.
  - Identify examples of security vulnerabilities.
  - Describe types of malware and their symptoms.
  - Describe methods of infiltration.
  - Describe methods used to deny service.

- 2.2 The Cybersecurity Landscape

- Explain trends in the cyberthreat landscape.
  - Describe a blended attack.
  - Describe the importance of impact reduction.

# 2.1 Analyzing a Cyberattack

# Finding Security Vulnerabilities

- An *exploit* is the term used to describe a program written to take advantage of a known vulnerability.
- An *attack* is the act of using an exploit against a vulnerability.
- Software vulnerability
  - Errors in OS or application code
  - SYNful Knock – Vulnerability in Cisco IOS
    - allows attackers to gain control of the routers
    - monitor network communication
    - infect other network devices.
  - Project Zero – Google formed a permanent team dedicated to finding software vulnerabilities.
- Hardware vulnerability
  - Hardware design flaws
  - Rowhammer - RAM memory exploit allows data to be retrieved from nearby address memory cells.



# Categorizing Security Vulnerabilities

- Buffer Overflow
  - Data is written beyond the limits of a buffer
- Non-validated Input
  - Force programs to behave in an unintended way
- Race Conditions
  - Improperly ordered or timed events
- Weaknesses in Security Practices
  - Protect sensitive data through authentication, authorization, and encryption
- Access-control Problems
  - Access control to physical equipment and resources
  - Security practices



# Types of Malware

- Malware is used to steal data, bypass access controls, cause harm to, or compromise a system.
- Types of Malware
  - **Spyware** - track and spy on the user
  - **Adware** - deliver advertisements, usually comes with spyware
  - **Bot** - automatically perform action
  - **Ransomware** - hold a computer system or the data captive until a payment is made
  - **Scareware** - persuade the user to take a specific action based on fear.



Initial Code Red Worm Infection

# Types of Malware (Cont.)

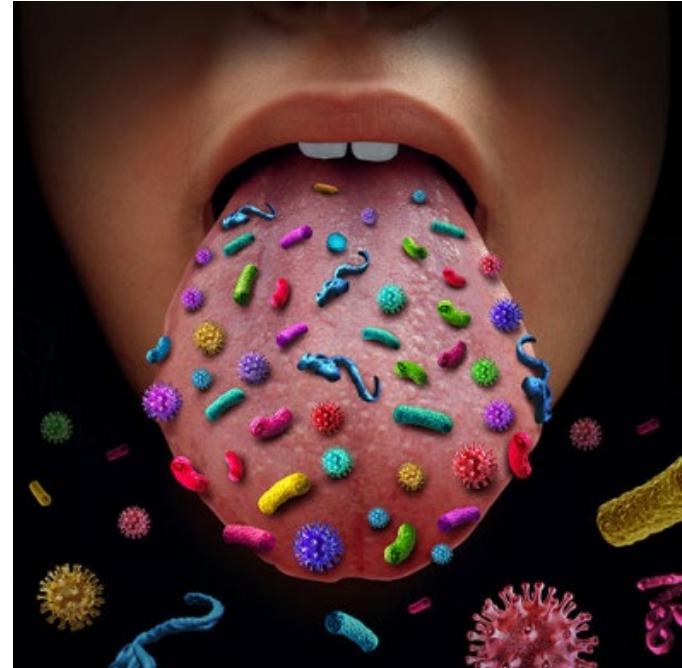
- Types of Malware (Cont.)
  - **Rootkit** - modify the operating system to create a backdoor
  - **Virus** - malicious executable code that is attached to other executable files
  - **Trojan horse** - carries out malicious operations under the guise of a desired operation
  - **Worm** - replicate themselves by independently exploiting vulnerabilities in networks
  - **Man-in-The-Middle or Man-in-The-Mobile** – take control over a device without the user's knowledge



Code Red Worm Infection 19 Hours Later

# Symptoms of Malware

- There is an increase in CPU usage.
- There is a decrease in computer speed.
- The computer freezes or crashes often.
- There is a decrease in Web browsing speed.
- There are unexplainable problems with network connections.
- Files are modified.
- Files are deleted.
- There is a presence of unknown files, programs, or desktop icons.
- There are unknown processes running.
- Programs are turning off or reconfiguring themselves.
- Email is being sent without the user's knowledge or consent.



# Social Engineering

- Social Engineering – manipulation of individual into performing actions or divulging confidential information
  - **Pretexting** - an attacker calls an individual and lies to them in an attempt to gain access to privileged data.
  - **Tailgating** - an attacker quickly follows an authorized person into a secure location.
  - **Something for something (Quid pro quo)** - an attacker requests personal information from a party in exchange for something



# Wi-Fi Password Cracking

- Wi-Fi Password Cracking – Password discovery
  - **Social engineering** - The attacker manipulates a person who knows the password into providing it.
  - **Brute-force attacks** - The attacker tries several possible passwords in an attempt to guess the password.
  - **Network sniffing** - The password maybe discovered by listening and capturing packets send on the network.



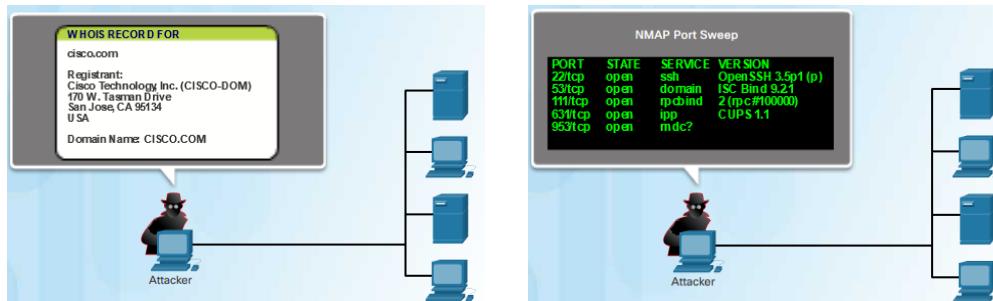
# Phishing

- Phishing
  - malicious party sends a fraudulent email disguised as being from a legitimate, trusted source
  - trick the recipient into installing malware on their device or sharing personal or financial information
- Spear phishing
  - a highly targeted phishing attack



# Vulnerability Exploitation

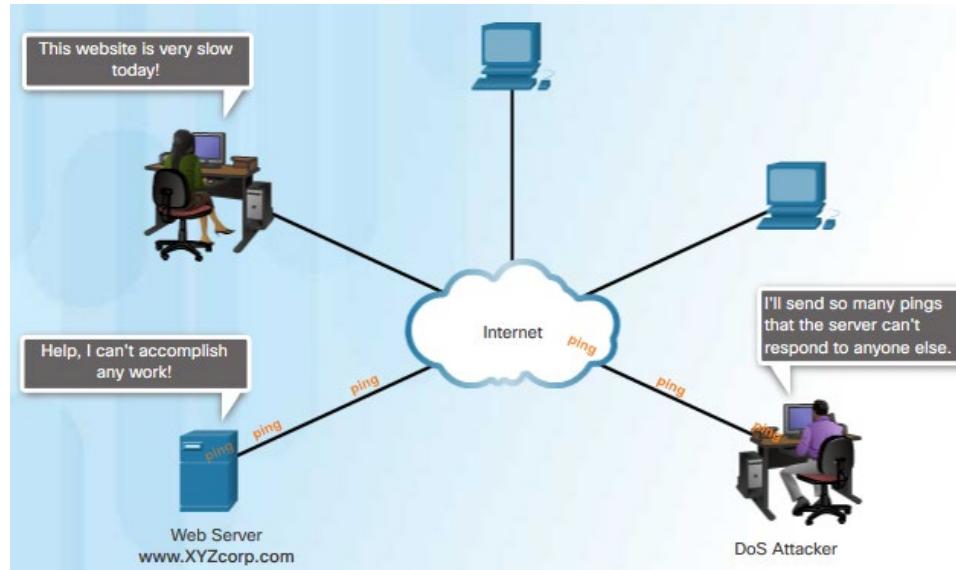
- Vulnerability Exploitation – scan to find vulnerability to exploit
  - **Step 1** - Gather information about the target system using port scanner or social engineering
  - **Step 2** - Determine learned information from step 1
  - **Step 3** - Look for vulnerability
  - **Step 4** - Use a known exploit or write a new exploit
- Advanced Persistent Threats – a multi-phase, long term, stealthy and advanced operation against a specific target
  - usually well-funded
  - deploy customized malware



# Denial of Service

## DoS

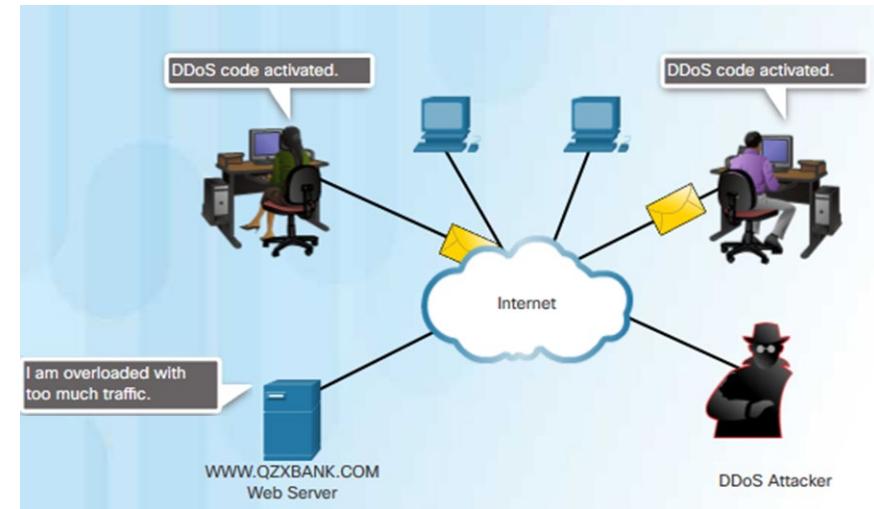
- DoS is a disruption of network services
  - **Overwhelming quantity of traffic** - a network, host, or application is sent an enormous quantity of data at a rate which it cannot handle
  - **Maliciously formatted packets** - maliciously formatted packet is sent to a host or application and the receiver is unable to handle it



# Denial of Service

## DDoS

- Similar to DoS, from multiple, coordinated sources
- Botnet - a network of infected hosts
- Zombie - infected hosts
- The zombies are controlled by handler systems.
- The zombies continues to infect more hosts, creating more zombies.



# SEO Poisoning

- SEO
  - Search Engine Optimization
  - Techniques to improve a website's ranking by a search engine
- SEO Poisoning
  - Increase traffic to malicious websites
  - Force malicious sites to rank higher



# 2.2 The Cybersecurity Landscape

# What is a Blended Attack?

- Uses multiple techniques to compromise a target
- Uses a hybrid of worms, Trojan horses, spyware, keyloggers, spam and phishing schemes
- Common blended attack example
  - spam email messages, instant messages or legitimate websites to distribute links
  - DDoS combined with phishing emails
- Examples: Nimbda, CodeRed, BugBear, Klez, Slammer, Zeus/LICAT, and Conficker



# What is Impact Reduction?

- Communicate the issue
- Be sincere and accountable
- Provide details
- Understand the cause of the breach
- Take steps to avoid another similar breach in the future
- Ensure all systems are clean
- Educate employees, partners and customers



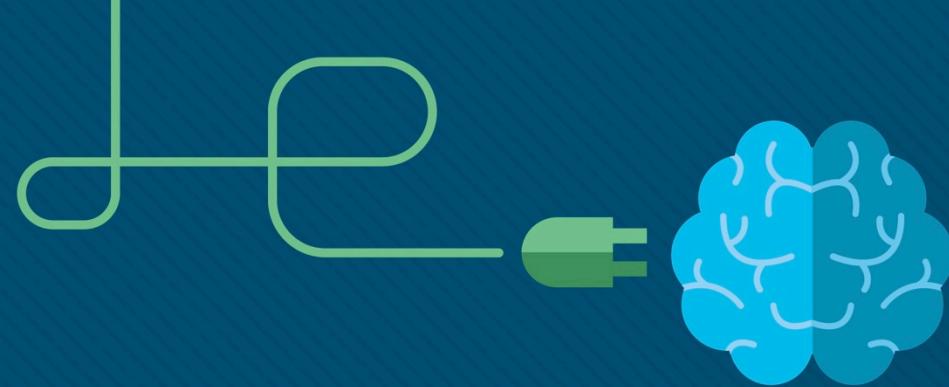
# 2.3 Chapter Summary

# Chapter Summary

## Summary

- Identify examples of security vulnerabilities.
- Explain how a security vulnerability is exploited.
- Describe types of malware and their symptoms, methods of infiltration, methods used to deny service.
- Describe a blended attack and the importance of impact reduction.





# Chapter 3: Protecting Your Data and Privacy

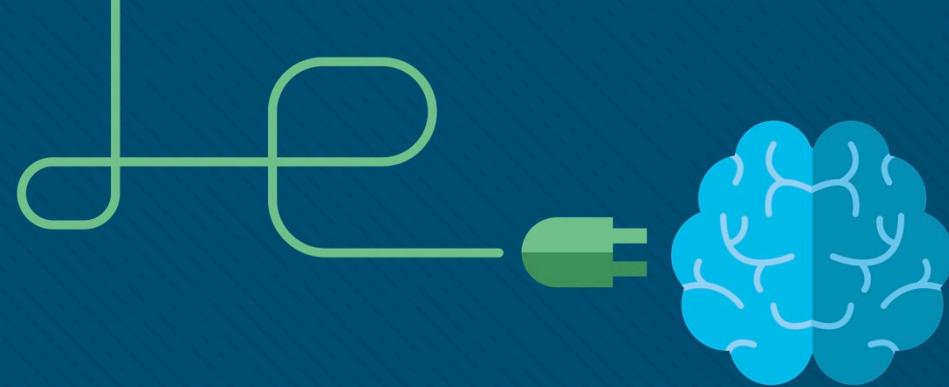
Instructor Materials

Introduction to Cybersecurity v2.1



# Chapter 3: Protecting Your Data and Privacy

**Introduction to Cybersecurity v2.1  
Planning Guide**



# Chapter 3: Protecting Your Data and Privacy

Introduction to Cybersecurity v2.1



# Chapter 3 - Sections & Objectives

- **3.1 Protecting Your Data**

- Explain how to protect devices from threats.
  - Explain how to protect your devices and network.
  - Describe safe procedures for data maintenance.

- **3.2 Safeguarding Your Online Privacy**

- Explain how to safeguard your privacy.
  - Describe strong authentication methods.
  - Describe safe online behaviors.

# 3.1 Protecting Your Data

## Protecting Your Devices and Network

# Protecting Your Computing Devices

- Keep the Firewall On
  - Prevent unauthorized access to your data or computing devices
  - Keep the firewall up to date
- Use Antivirus and Antispyware
  - Prevent unauthorized access to your data or computing devices
  - Only download software from trusted websites
  - Keep the software up to date
- Manage Your Operating System and Browser
  - Set the security settings at medium or higher
  - Update your computer's operating system and browser
  - Download and install the latest software patches and security updates
- Protect All Your Devices
  - Password protect
  - Encrypt the data
  - Only store necessary information
  - IoT devices



# Use Wireless Networks Safely

- Home Wireless Network

- Change the pre-set SSID and default administrative password on your Wi-Fi router.
- Disable SSID broadcast
- Use WPA2 encryption feature
- Be aware of WPA2 protocol security flaw – KRACK
  - Allows intruder to break the encryption between wireless router and clients

- Use caution when using public Wi-Fi hotspots

- Avoid accessing or sending sensitive information
- Use of VPN tunnel can prevent eavesdropping

- Turn off Bluetooth when not in use



# Use Unique Passwords for Each Online Account

- Prevents criminals from accessing all your online accounts using one stolen credentials
- Use password managers to help with remembering passwords
- Tips for choosing a good password:
  - Do not use dictionary words or names in any languages
  - Do not use common misspellings of dictionary words
  - Do not use computer names or account names
  - If possible use special characters, such as ! @ # \$ % ^ & \* ( )
  - Use a password with ten or more characters

OK	Good	Better
allwhitecat	a11whitecat	A11whi7ec@t
Fblogin	1FBLogin	1.FB.L0gin\$
amazonpass	AmazonPa55	Am@z0nPa55
ilikemyschool	ILikeMySchool	!Lik3MySch00l
Hightidenow	HighTideNow	H1gh7id3Now

# Use Passphrase Rather Than a Password

- Tips in choosing a good passphrase:
  - Choose a meaningful statement to you
  - Add special characters, such as ! @ # \$ % ^ & \* ( )
  - The longer the better
  - Avoid common or famous statements, for example, lyrics from a popular song
- Summary of the new NIST guidelines:
  - 8 characters minimum in length, but no more than 64 characters
  - No common, easily guessed passwords, such as password, abc123
  - No composition rules, such as having to include lowercase and uppercase letters and numbers
  - No knowledge-based authentication, such as information from shared secret questions, marketing data, transaction history
  - Improve typing accuracy by allowing the user to see the password while typing
  - All printing characters and spaces are allowed
  - No password hints
  - No periodical or arbitrary password expiration

OK	Thisismypassphrase.
Good	Acatthatlovesdogs.
Better	Acat th@tlov3sd0gs.

# Lab – Create and Store Strong Passwords



Networking  
Academy

## Lab – Create and Store Strong Passwords

### Objectives

Understand the concepts behind a strong password.

**Part 1: Explore the concepts behind creating a strong password.**

**Part 2: Explore the concepts behind securely storing your passwords?**

### Background / Scenario

Passwords are widely used to enforce access to resources. Attackers will use many techniques to learn users' passwords and gain unauthorized access to a resource or data.

To better protect yourself, it is important to understand what makes a strong password and how to store it securely.

### Required Resources

- PC or mobile device with Internet access

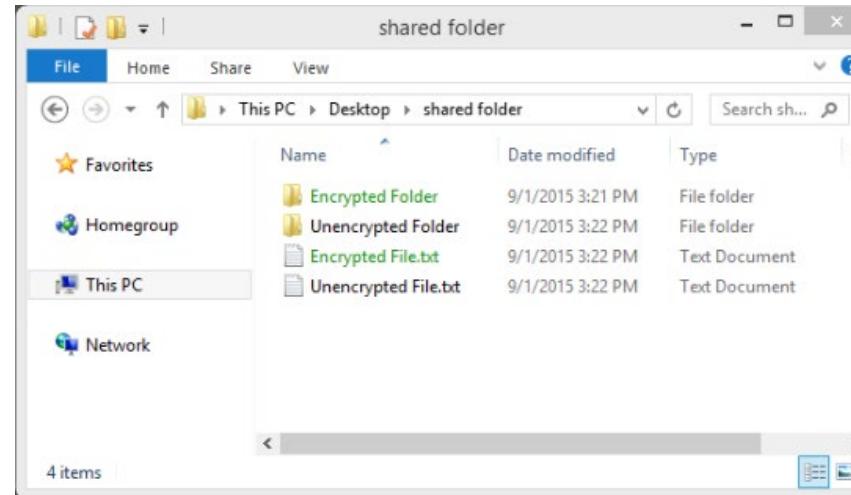
### Part 1: Creating a Strong Password

Strong passwords have four main requirements listed in order of importance:

## Data Maintenance

# Encrypt Your Data

- Encrypted data can only be read with the secret key or password
- Prevent unauthorized users from reading the content
- What is Encryption?
  - process of converting the information into a form where an unauthorized party cannot read it



# Back up Your Data

- Prevent the loss of irreplaceable data
- Need additional storage location for the data
- Copy the data to the backup location regularly and automatically
- Local Backup
  - NAS, external hard drive, CDs/DVDs, thumb drives, or tapes
  - Total control and responsible for the cost and maintenance
- Cloud Storage Service, such as AWS
  - Access to backup as long as you have access to your account
  - may need to be more selective about the data being backed up



# Lab – Back up Data to External Storage



Networking  
Academy

## Lab – Backup Data to External Storage

### Objectives

Backup user data.

**Part 1: Use a local external disk to backup data**

**Part 2: Use a remote disk to backup data**

### Background / Scenario

It is important to establish a backup strategy that includes data recovery of personal files.

While many backup tools are available, this lab focuses on the Microsoft Backup Utility to perform backups to local external disks. In Part 2, this lab uses the Dropbox service to backup data to a remote or cloud-based drive.

### Required Resources

- PC or mobile device with Internet access

## Part 1: Backing Up to a Local External Disk

### Step 1: Getting Started With Backup Tools in Windows

Computer usage and organizational requirements determine how often data must be backed up and the type

# Deleting Your Data Permanently

- Use available tools to delete permanently: SDelete and Secure Empty Trash, for example
- Destroy the storage device to ensure that the data is unrecoverable
- Delete the online versions



# Lab – Who Owns Your Data



## Lab – Who Owns Your Data?

### Objectives

Explore the ownership of your data when that data is not stored in a local system.

**Part 1: Explore the Terms of Service Policy**

**Part 2: Do You Know What You Signed Up For?**

### Background / Scenario

Social media and online storage have become an integral part of many people's lives. Files, photos, and videos are shared between friends and family. Online collaboration and meetings are conducted in the workplace with people who are many miles from each other. The storage of data is no longer limited to just the devices you access locally. The geographical location of storage devices is no longer a limiting factor for storing or backing up data at remote locations.

In this lab, you will explore legal agreements required to use various online services. You will also explore some of the ways you can protect your data.

### Required Resources

- PC or mobile device with Internet access

### Part 1: Explore the Terms of Service Policy

If you are using online services to store data or communicate with your friends or family, you probably entered into an agreement with the provider. The Terms of Service, also known as Terms of Use or Terms and

# 3.2 Safeguarding Your Online Privacy

# Two Factor Authentication

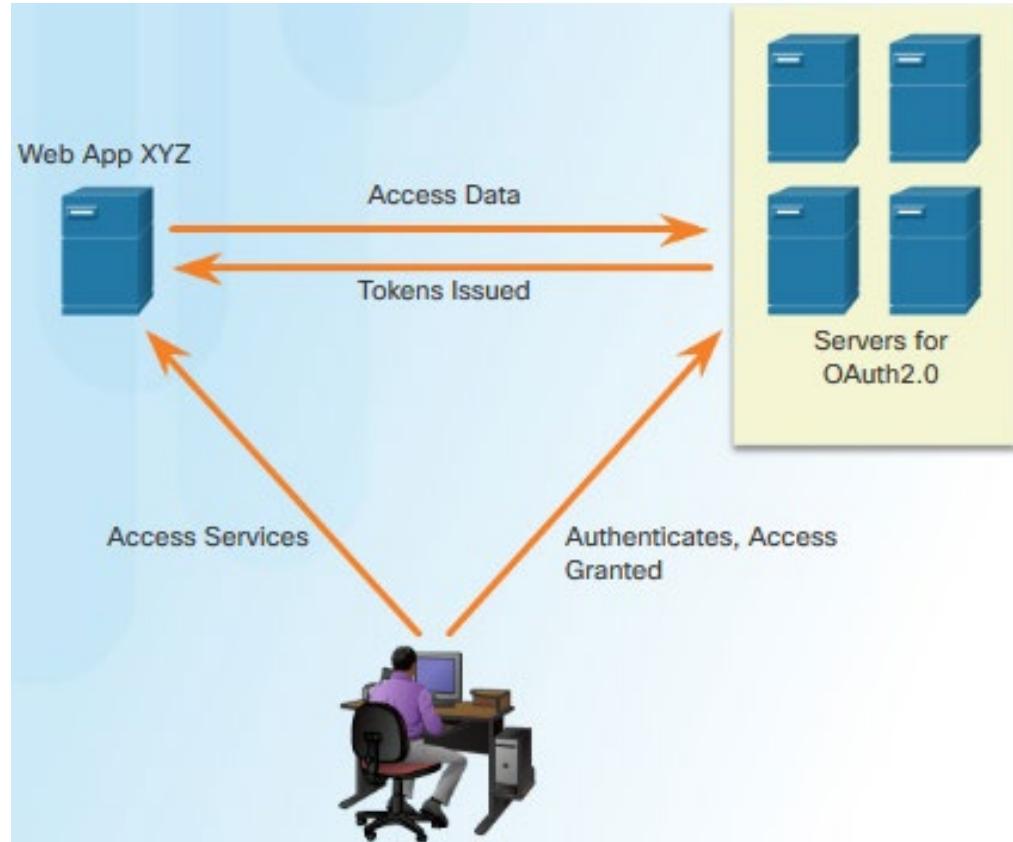
- Popular online services use two factor authentication
- Need Username / password or PIN and a second token for access:
  - **Physical object** - credit card, ATM card, phone, or fob
  - **Biometric scan** - fingerprint, palm print, as well as facial or voice recognition



## Strong Authentication

# OAuth 2.0

- An open standard protocol that allows an end user's credentials to access third party applications without exposing the user's password
- Act as the middle man to decide whether to allow end users access to third party applications.



Sharing Too Much Information?

## Do Not Share Too Much on Social Media

- Share as little information as possible on social media
- Do not share information such as:
  - Birth date
  - Email address
  - Phone number
- Check your social media settings



## Sharing Too Much Information

# Email and Web Browser Privacy

- Email is like sending a postcard.
- Copies of the email can be read by anyone with access.
- The email is passed among different servers
- Use the private browsing mode can prevent other from gathering information about your online activities.
- Private mode on popular browser
  - **Microsoft Internet Explorer:** InPrivate
  - **Google Chrome:** Incognito
  - **Mozilla Firefox:** Private tab / private window
  - **Safari:** Private: Private browsing



# Lab – Discover Your Own Risky Online Behavior



## Lab – Discover Your Own Risky Online Behavior

### Objectives

Explore actions performed online that may compromise your safety or privacy.

### Background / Scenario

The Internet is a hostile environment, and you must be vigilant to ensure your data is not compromised. Attackers are creative and will attempt many different techniques to trick users. This lab helps you identify risky online behavior and provide tips on how to become safer online.

### Part 1: Explore the Terms of Service Policy

Answer the questions below with honesty and take note of how many points each answer gives you. Add all points to a total score and move on to Part 2 for an analysis of your online behavior.

- a. What kind of information do you share with social media sites?
  - 1) Everything; I rely on social media to keep in touch with friends and family. (3 points)
  - 2) Articles and news I find or read (2 points)
  - 3) It depends; I filter out what I share and with whom I share. (1 point)
  - 4) Nothing; I do not use social media. (0 points)

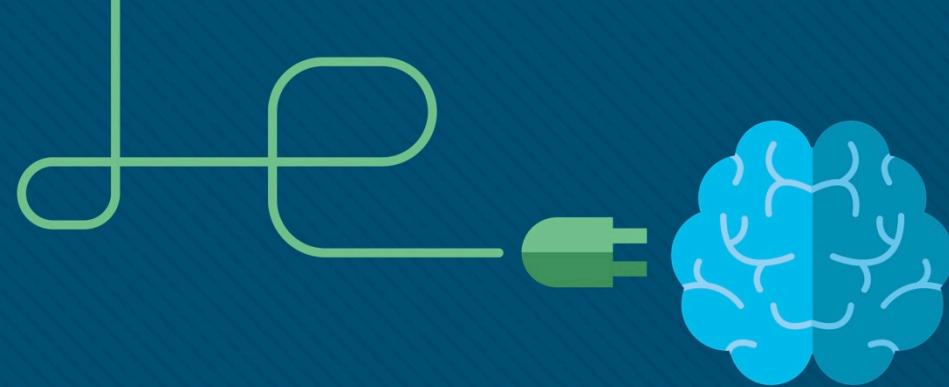
# 3.3 Chapter Summary

## Protecting Your Data and Privacy

# Summary

- Explain how to protect your devices and network from threats.
- Describe safe procedures for data maintenance.
- Explain how to safeguard your privacy by using strong authentication methods and practicing safe online behaviors.





# Chapter 4: Protecting the Organization

Instructor Materials

Introduction to Cybersecurity v2.1



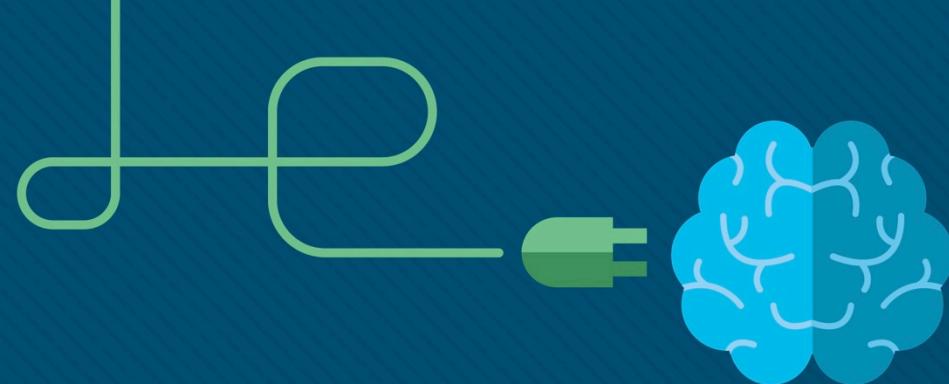
# Chapter 4: Protecting the Organization

**Introduction to Cybersecurity v2.1  
Planning Guide**



# Chapter 4: Protecting the Organization

Introduction to Cybersecurity v2.1



# Chapter 4 - Sections & Objectives

- 4.1 Firewalls

- Explain techniques to protect organizations from cyber attacks.
  - Describe the various types of firewalls.
  - Describe different types of security appliances.
  - Describe different methods of detecting attacks in real time.
  - Describe methods of detecting malware.
  - Describe security best practices for organizations.

- 4.2 Behavior Approach to Cybersecurity

- Explain the behavior-based approach to cybersecurity.
  - Define the term botnet.
  - Define the term kill chain.
  - Define behavior-based security.
  - Explain how NetFlow helps to defend against cyberattacks.

# Chapter 4 - Sections & Objectives (Cont.)

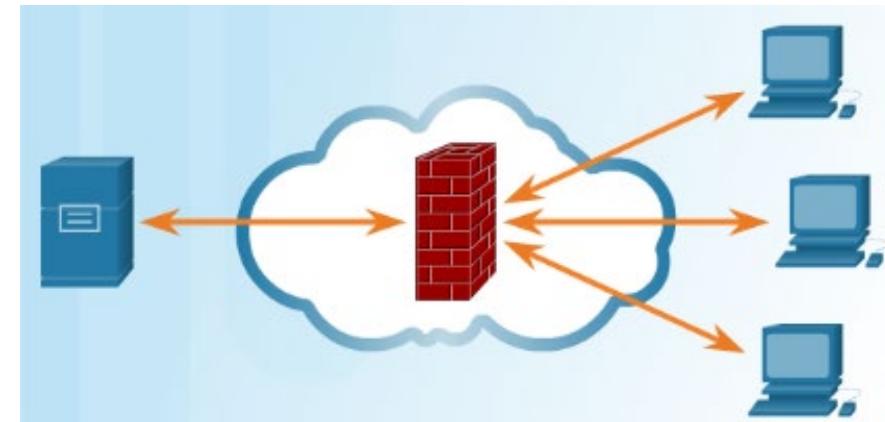
- 4.3 Cisco's Approach to Cybersecurity
  - Explain the Cisco approach to providing cybersecurity.
    - Identify the function of CSIRT within Cisco.
    - Explain the purpose of a security playbook.
    - Identify tools used for incident prevention and detection.
    - Define IDS and IPS.

# 4.1 Firewalls

## Firewalls Types

# Firewall Types

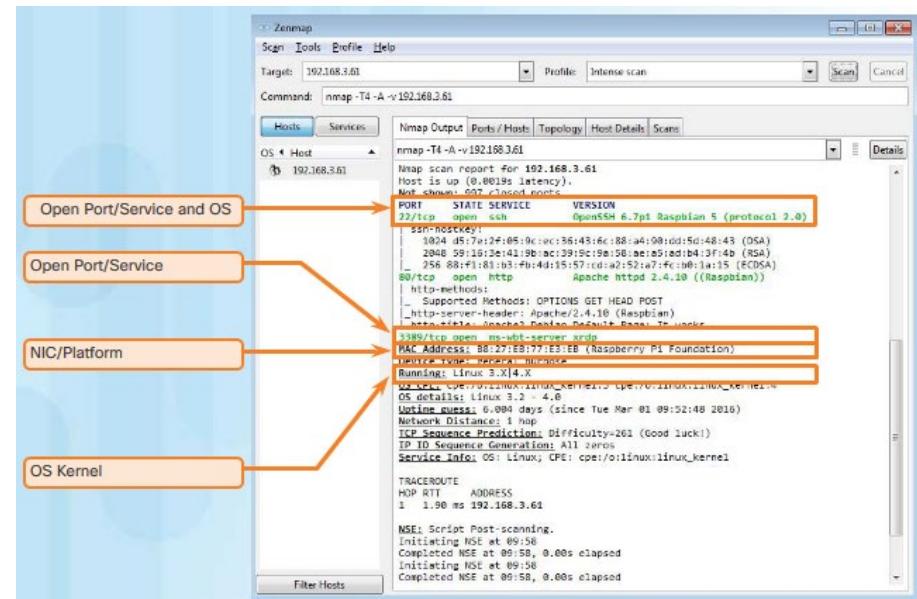
- Control or filter incoming or outgoing communications on a network or device
- Common firewall types
  - **Network Layer Firewall** – source and destination IP addresses
  - **Transport Layer Firewall** – source and destination data ports, connection states
  - **Application Layer Firewall** – application, program or service
  - **Context Aware Application Firewall** – user, device, role, application type, and threat profile
  - **Proxy Server** – web content requests
  - **Reverse Proxy Server** – protect, hide, offload, and distribute access to web servers
  - **Network Address Translation (NAT) Firewall** – hides or masquerades the private addresses of network hosts
  - **Host-based Firewall** – filtering of ports and system service calls on a single computer operating system



## Firewall Types

# Port Scanning

- Process of probing a computer, server or other network host for open ports
- Port numbers are assigned to each running application on a device.
- Reconnaissance tool to identify running OS and services
  - Nmap – A port scanning tool
- Common responses:
  - **Open or Accepted** - a service is listening on the port.
  - **Closed, Denied, or Not Listening** – connections will be denied to the port.
  - **Filtered, Dropped, or Blocked** – no reply from the host.



## Security Appliances

# Security Appliances

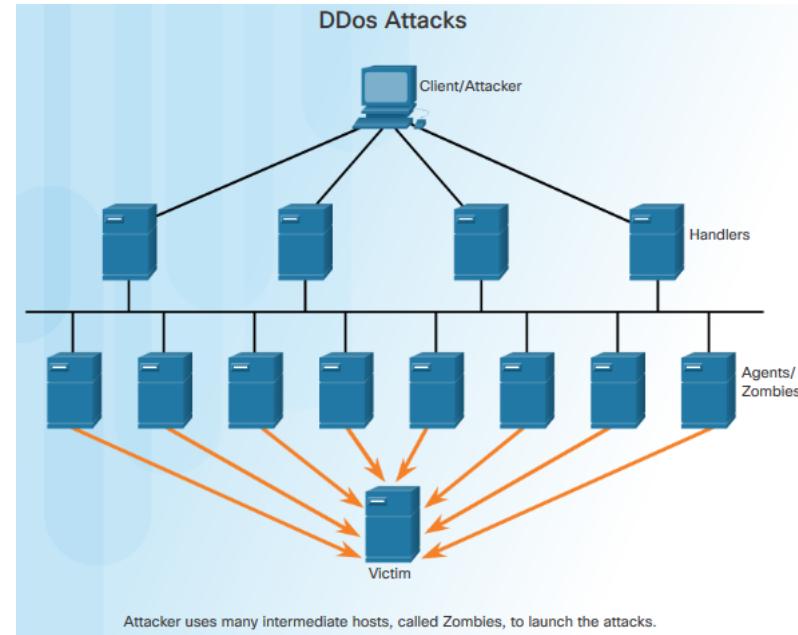
- Security appliances fall into these general categories:

- **Routers** - can have many firewall capabilities: traffic filtering, IPS, encryption, and VPN.
- **Firewalls** – may also have router capability, advanced network management and analytics.
- **IPS** - dedicated to intrusion prevention.
- **VPN** - designed for secure encrypted tunneling.
- **Malware/Antivirus** - Cisco Advanced Malware Protection (AMP) comes in next generation Cisco routers, firewalls, IPS devices, Web and Email Security Appliances and can also be installed as software in host computers.
- **Other Security Devices** – includes web and email security appliances, decryption devices, client access control servers, and security management systems.



# Detecting Attacks in Real Time

- Zero-day attack
  - A hacker exploits a flaw in a piece of software before the creator can fix it.
- **Real Time Scanning from Edge to Endpoint**
  - Actively scanning for attacks using firewall and IDS/IPS network device
  - detection with connections to online global threat centers
  - detect network anomalies using context-based analysis and behavior detection
- **DDoS Attacks and Real Time Response**
  - DDoS, one of the biggest attack threats, can cripple Internet servers and network availability.
  - DDoS originates from hundreds, or thousands of zombie hosts, and the attacks appear as legitimate traffic.



# Detecting Malware

# Protecting Against Malware



# Security Best Practices

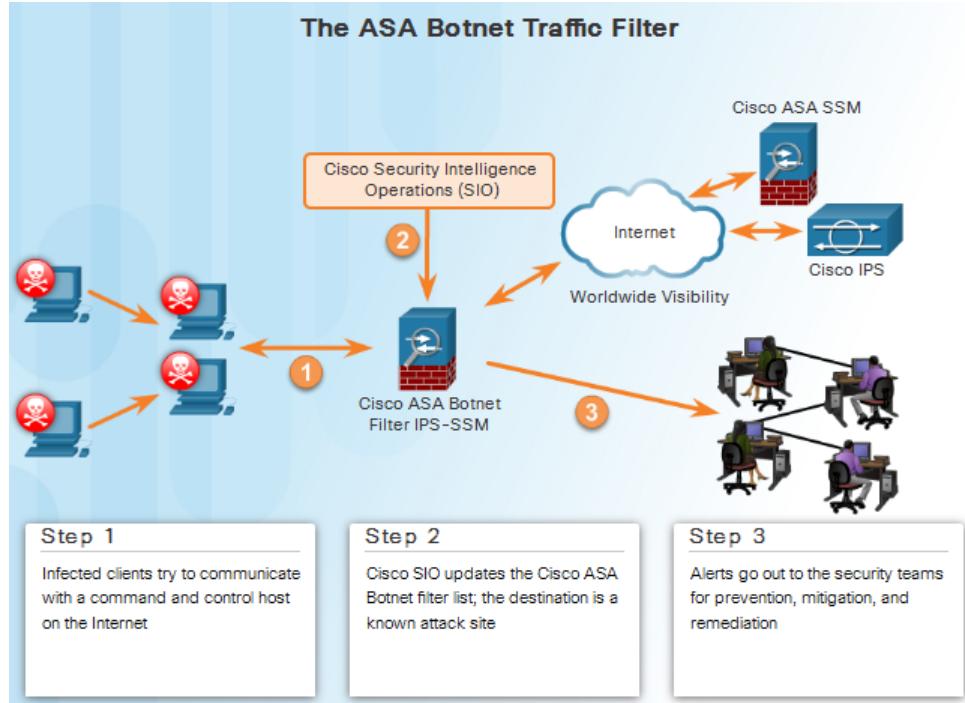
- **Some published Security Best Practices:**
  - **Perform Risk Assessment** – Knowing the value of what you are protecting will help in justifying security expenditures.
  - **Create a Security Policy** – Create a policy that clearly outlines company rules, job duties, and expectations.
  - **Physical Security Measures** – Restrict access to networking closets, server locations, as well as fire suppression.
  - **Human Resource Security Measures** – Employees should be properly researched with background checks.
  - **Perform and Test Backups** – Perform regular backups and test data recovery from backups.
  - **Maintain Security Patches and Updates** – Regularly update server, client, and network device operating systems and programs.
  - **Employ Access Controls** – Configure user roles and privilege levels as well as strong user authentication.
  - **Regularly Test Incident Response** – Employ an incident response team and test emergency response scenarios.
  - **Implement a Network Monitoring, Analytics and Management Tool** - Choose a security monitoring solution that integrates with other technologies.
  - **Implement Network Security Devices** – Use next generation routers, firewalls, and other security appliances.
  - **Implement a Comprehensive Endpoint Security Solution** – Use enterprise level antimalware and antivirus software.
  - **Educate Users** – Educate users and employees in secure procedures.
  - **Encrypt data** – Encrypt all sensitive company data including email.

# 4.2 Behavior Approach to Cybersecurity

# Botnet

## Botnet

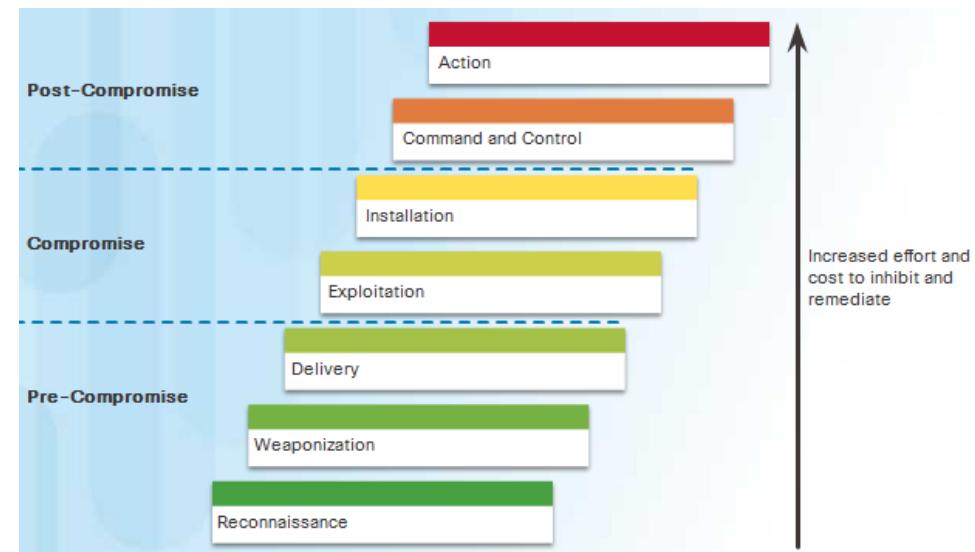
- Botnet
  - A group of bots connect through the Internet
  - Controlled by malicious individuals or groups
- Bot
  - Typically infected by visiting a website, opening an email attachment, or opening an infected media file



## The Kill Chain in Cyberdefense

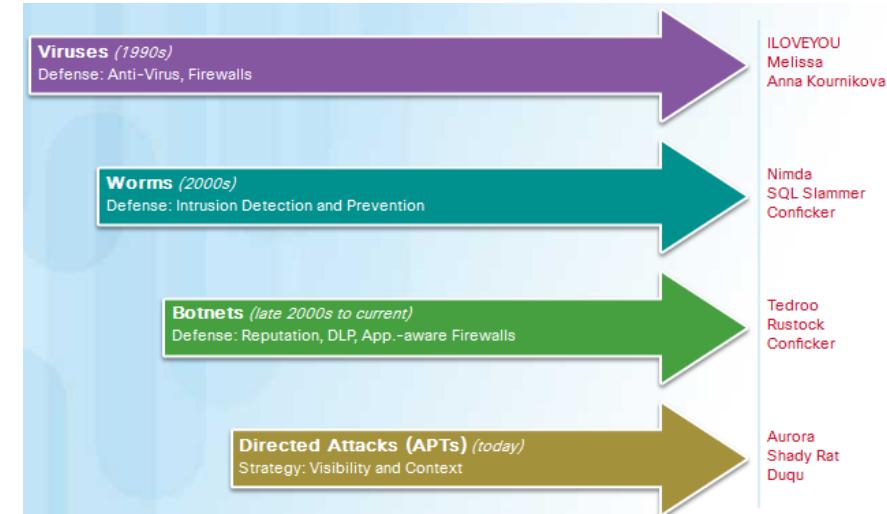
Kill Chain is the stages of an information systems attack.

- 1. Reconnaissance** – Gathers information
- 2. Weaponization** - Creates targeted exploit and malicious payload
- 3. Delivery** - Sends the exploit and malicious payload to the target
- 4. Exploitation** – Executes the exploit
- 5. Installation** - Installs malware and backdoors
- 6. Command and Control** - Remote control from a command and control channel or server.
- 7. Action** – Performs malicious actions or additional attacks on other devices



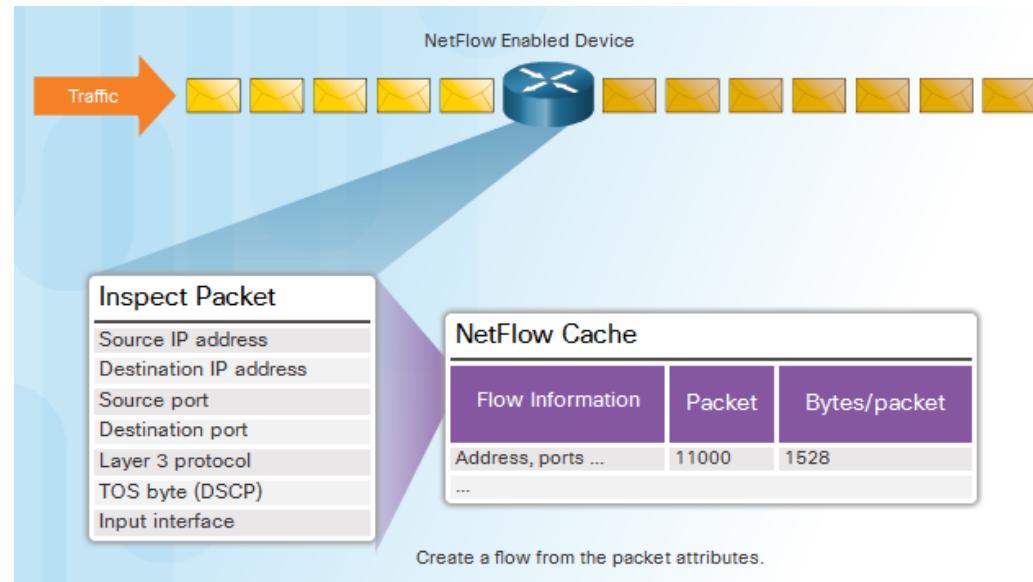
# Behavior-Based Security

- Honeypots
  - Lures the attacker by appealing to the attackers' predictable behavior
  - Captures, logs and analyze the attackers' behavior
  - Administrator can gain more knowledge and build better defense
- Cisco's Cyber Threat Defense Solution Architecture
  - Uses behavior-based detection and indicators
  - Provide greater visibility, context and control



## Netflow

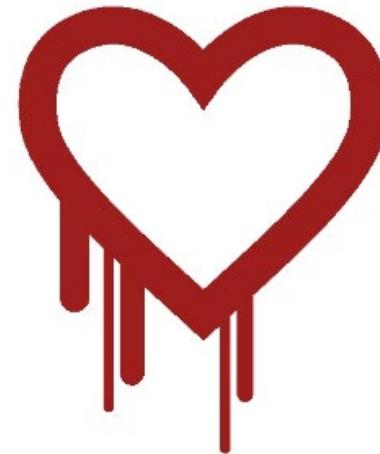
- Gather information about data flowing through a network
- Important components in behavior-based detection and analysis
- Establish baseline behaviors



# 4.3 Cisco's Approach to Cybersecurity

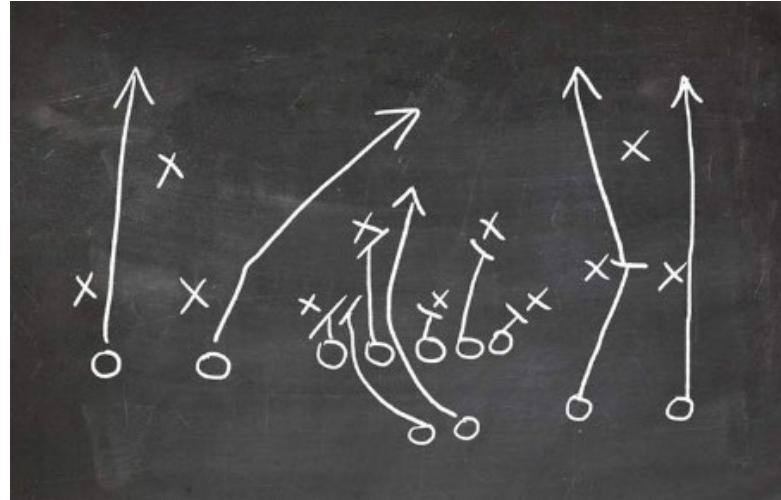
- Computer Security Incident Response Team

- help ensure company, system, and data preservation by performing comprehensive investigations into computer security incidents
- provides proactive threat assessment, mitigation planning, incident trend analysis, and security architecture review



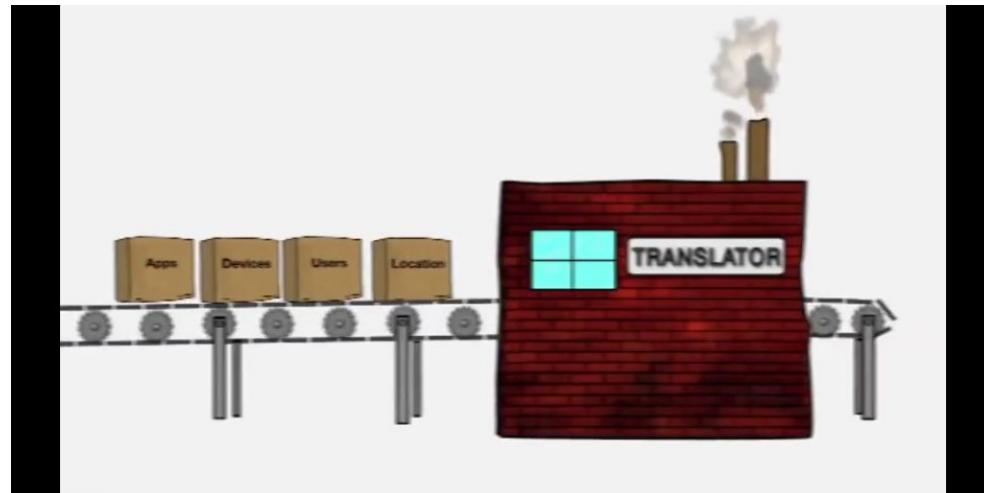
# Security Playbook

- Collection of repeatable queries against security event data sources that lead to incident detection and response
- What does it need to accomplish?
  - Detect malware infected machines.
  - Detect suspicious network activity.
  - Detect irregular authentication attempts.
  - Describe and understand inbound and outbound traffic.
  - Provide summary information including trends, statistics, and counts.
  - Provide usable and quick access to statistics and metrics.
  - Correlate events across all relevant data sources.



# Tools for Incident Prevention and Detection

- SIEM – Security Information and Event Management
  - Software that collects and analyzes security alerts, logs and other real time and historical data from security devices on the network
- DLP – Data Loss Prevention
  - Stops sensitive data from being stolen or escaped from the network
  - Designs to monitor and protect data in three different states
- Cisco Identity Services Engine (Cisco ISE) and TrustSec
  - Uses role-based access control policies



# IDS and IPS

- IDS – Intrusion Detection System
  - Usually placed offline
  - Does not prevent attacks
  - Detect, log, and report
- IPS – Intrusion Prevention System
  - Ability to block or deny traffic based on a positive rule or signature match
- IDS/IPS system
  - Snort
  - Sourcefire (Cisco)

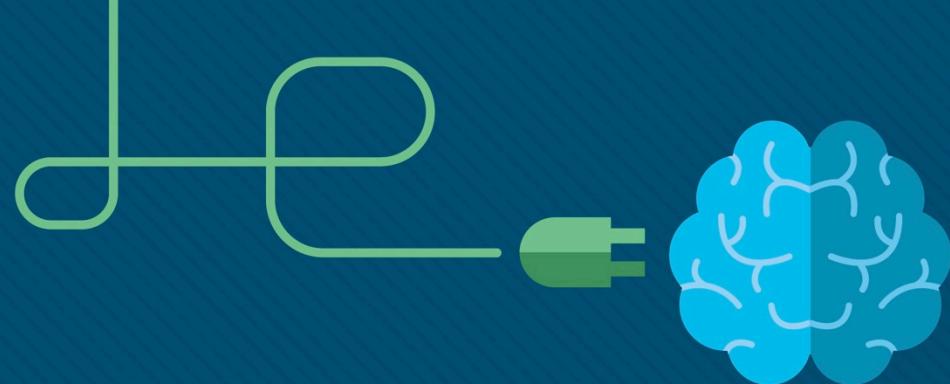


# 4.4 Chapter Summary

# Chapter Summary

- Describe the various types of firewalls and security appliances.
- Describe different methods of detecting malware and attacks in real time.
- Describe security best practices for organizations.
- Define botnet, kill chain, and behavior-based security.
- Explain how Netflow can help defend against cyberattacks.
- Identify the function of CSIRT within Cisco.
- Explain the purpose of a security playbook.
- Identify tools used for incident prevention and detection.
- Define IDS and IPS.





# Chapter 5: Will Your Future Be in Cybersecurity?

Instructor Materials

Introduction to Cybersecurity v2.1



# Chapter 5: Will Your Future Be in Cybersecurity?

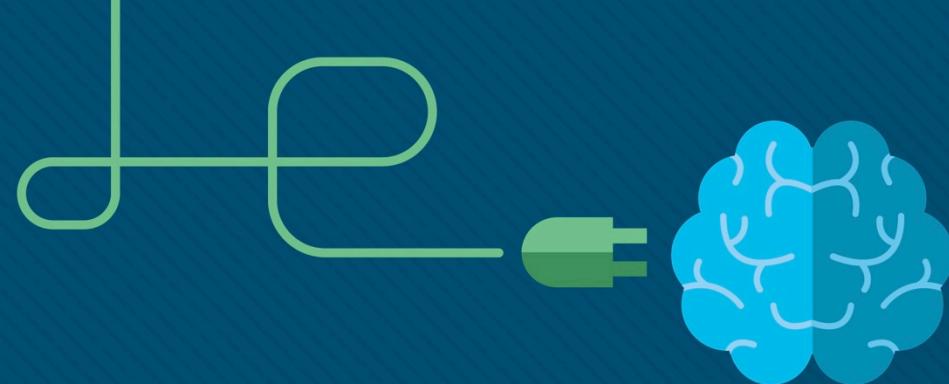
**Introduction to Cybersecurity v2.1  
Planning Guide**





# Chapter 5: Will Your Future Be in Cybersecurity?

Introduction to Cybersecurity v2.1



# Chapter 5 - Sections & Objectives

- 5.1 Cybersecurity Education and Careers
  - Explain the legal and ethical issues facing cybersecurity professionals
    - Describe the legal and ethical issues facing a cybersecurity professional.

# 5.1 Cybersecurity Education and Careers

## Legal Issues in Cybersecurity

- Personal Legal Issues

- Be responsible with your skills

- Corporate Legal Issues

- Businesses are required to abide by the cybersecurity laws.
  - Break the law, you could lose your job and your company could be punished.
  - When you are not sure, you should consult legal department.

- International Law and Cybersecurity

- IMPACT

- global partnership of world governments, industries and academia
  - Improving global capabilities when dealing with cyber threats



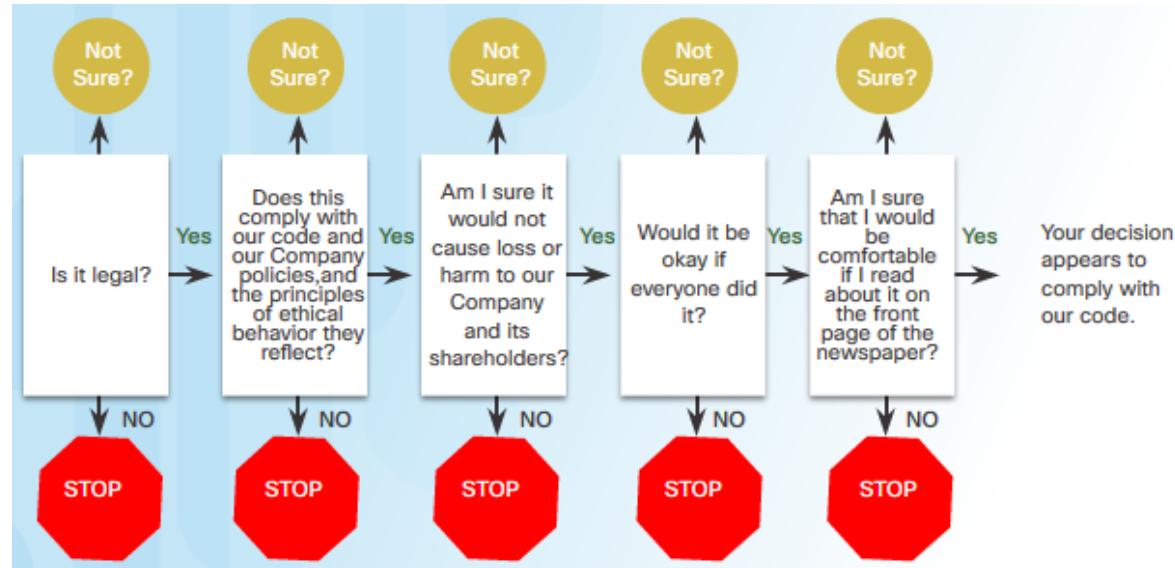
## Ethical Issues in Cybersecurity

- Personal Ethical Issues

- Legal behavior may still be unethical.

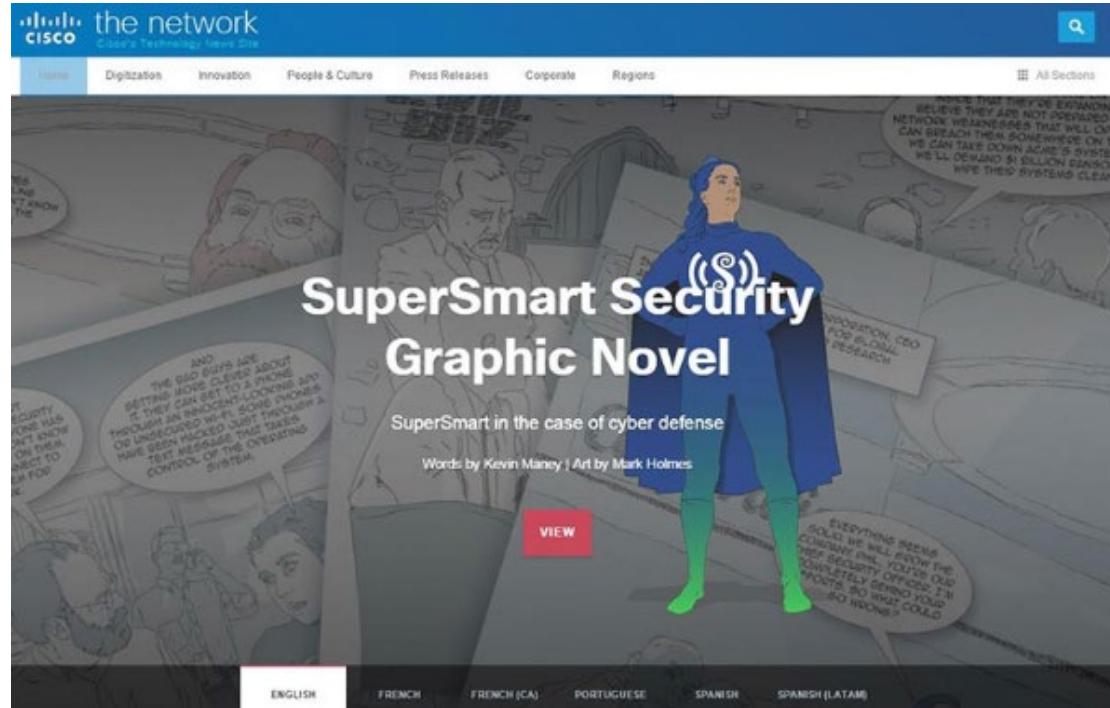
- Corporate Ethical Issues

- Ethics are codes of behavior that are sometimes enforced by laws.
  - Organizations with Published Codes of Ethics:
    - The CyberSecurity Institute (CSI)
    - The Information Systems Security Association (ISSA)
    - The Association of Information Technology Professionals (AITP)



## Cybersecurity Jobs

- Some online job search engine
  - ITJobMatch
  - Monster
  - CareerBuilder
- Different types of cybersecurity jobs
  - Penetration testing / ethical hacker
  - Security administrator
  - Network administrator
  - System administrator



# 5.1 Chapter Summary

# Chapter Summary

- Describe the legal and ethical issues.



# AAA Authentication

Console

Remote Access

# AAA Authentication?

- Authentication, Authorization, and Accounting framework is used to manage the activity of the user to a network that it wants to access by authentication, authorization, and accounting mechanism.

Configure a local user account on R1 and configure authenticate on the console and vty lines using local AAA.

1. Configure a username of admin1 with a secret password of admin1pa55.

- username admin1 secret admin1pa55
- aaa new-model
- aaa authentication login default local
- line con 0
- login authentication default

Check if login in console is working R1

Configure a local user account on R1 and configure authenticate on the console and vty lines using local AAA.

- 2. Configure Local AAA Authentication for vty Lines on R1
  - ip domain-name ccnasecurity.com
  - crypto key generate rsa
  - 1024
  - aaa authentication login SSH-LOGIN local
  - line vty 0 4
  - login authentication SSH-LOGIN
  - transport input ssh
  - end
- Check if SSH is working in the PC

# Configure server-based AAA authentication using TACACS+.

## **Terminal Access Controller Access-Control System**

1. Configure Server-Based AAA Authentication Using TACACS+ on R2.
  - username admin2 secret admin2pa55
2. Verify the TACACS+ Server configuration.
  - complete the information needed by the server
  - client name: R2
  - client IP: 192.168.2.1
  - secret: tacacspa55
  - server type: tacacs
  - user setup (add users to access the router)

# Configure server-based AAA authentication using TACACS+.

## 3. Configure the TACACS+ server specifics on R2.

- tacacs-server host 192.168.2.5
  - tacacs-server key tacacspa55
  - aaa new-model
  - aaa authentication login default group tacacs+ local
  - line con 0
  - login authentication default
- Check if tacacs+ is working on console

# Configure server-based AAA authentication using RADIUS.

## **Remote Authentication Dial-In User Service**

- 1. Configure Server-Based AAA Authentication Using RADIUS on R3
  - username admin2 secret admin2pa55
- 2. Verify the Radius Server configuration.
  - complete the information needed by the server
  - client name: R2
  - client IP: 192.168.3.1
  - secret: tacacspa55
  - server type: radius
  - user setup (add users to access the router)

# Configure server-based AAA authentication using RADIUS.

## 3. Configure the Radius server specifics on R2.

- radius-server host 192.168.3.5
  - radius-server key radiuspa55
  - aaa new-model
  - aaa authentication login default group radius local
  - line con 0
  - login authentication default
- Check if radius is working on console

# ASA Firewall Setup

CISCO ASA Firewall Appliance

# What is a firewall?

- A firewall is a **network security** device that monitors incoming and outgoing network traffic and permits or blocks data **packets** based on a set of security rules. Its purpose is to establish a barrier between your internal network and incoming traffic from external sources (such as the internet) in order to block malicious traffic like viruses and hackers.

# Types of Firewalls

- **Next-generation firewalls (NGFW)** combine traditional firewall technology with additional functionality, such as encrypted traffic inspection, intrusion prevention systems, anti-virus, and more. Most notably, it includes deep packet inspection (DPI). While basic firewalls only look at packet headers, deep packet inspection examines the data within the packet itself, enabling users to more effectively identify, categorize, or stop packets with malicious data. [Learn about Forcepoint NGFW here.](#)
- **Proxy firewalls** filter network traffic at the application level. Unlike basic firewalls, the proxy acts an intermediary between two end systems. The client must send a request to the firewall, where it is then evaluated against a set of security rules and then permitted or blocked. Most notably, proxy firewalls monitor traffic for layer 7 protocols such as HTTP and FTP, and use both stateful and deep packet inspection to detect malicious traffic.

# Types of Firewalls

- **Network address translation (NAT) firewalls** allow multiple devices with independent network addresses to connect to the internet using a single IP address, keeping individual IP addresses hidden. As a result, attackers scanning a network for IP addresses can't capture specific details, providing greater security against attacks. NAT firewalls are similar to proxy firewalls in that they act as an intermediary between a group of computers and outside traffic.
- **Stateful multilayer inspection (SMLI) firewalls** filter packets at the network, transport, and application layers, comparing them against known trusted packets. Like NGFW firewalls, SMLI also examine the entire packet and only allow them to pass if they pass each layer individually. These firewalls examine packets to determine the state of the communication (thus the name) to ensure all initiated communication is only taking place with trusted sources.

# Types of Firewalls

- Packet-filtering Firewalls
- Circuit-level Gateways
- Application-level Gateways (Proxy Firewalls)
- Stateful Multi-layer Inspection (SMLI) Firewalls
- Next-generation Firewalls (NGFW)
- Threat-focused NGFW
- Network Address Translation (NAT) Firewalls
- Cloud Firewalls
- Unified Threat Management (UTM) Firewalls

# What is ASA 5505 Firewall

- Adaptive Security Appliance (ASA)
- The Cisco ASA 5505 is a full-featured firewall for small business, branch, and enterprise teleworker environments. It delivers high-performance firewall, SSL and IPsec VPN, and rich networking services in a modular, immediately operational appliance.
  - Feature: Cisco ASA 5505; Security Plus
  - IPS throughput 2: Up to 75 Mbps with AIP-SSC-5
  - Maximum 3DES/AES VPN Throughput 3: Up to 100 Mbps
  - Stateful inspection throughput (maximum 1): Up to 150 Mbps
- IPsec throughput is **the amount of traffic that can pass through the firewall and the encrypted tunnel to your remote site**. Most good firewalls use hardware encryption so IPsec numbers should approximate the overall throughput of your firewall.

# How to configure internet access on CISCO ASA 5505

- SetUp the Firewall ASA
- Initial Config
  - 1. Check for previous configuration
  - 2. Erase and Reload
  - 3. Enable command (no password, just press enter)
  - 4. Change hostname
  - 5. Enable password (put password)
- Interface Configuration
- Configure Gateway of ASA (OUTSIDE)
  - int g1/1 (pointing to ISP)
  - ip address and subnet mask
  - nameif (name of outside network)
  - security level 0
  - no shut

# Here are a couple of examples of security levels:

- **Security level 0:** This is the lowest security level there is on the ASA and by default it is assigned to the “outside” interface. Since there is no lower security level this means that traffic from the outside is unable to reach any of our interfaces unless we permit it within an access-list.
- **Security level 100:** This is the highest security level on our ASA and by default this is assigned to the “inside” interface. Normally we use this for our “LAN”. Since this is the highest security level, by default it can reach all the other interfaces.
- **Security level 1 – 99:** We can create any other security levels that we want, for example we can use security level 50 for our DMZ. This means that traffic is allowed from our inside network to the DMZ (security level 100 -> 50) and also from the DMZ to the outside (security level 50 -> 0). Traffic from the DMZ however can’t go to the inside (without an access-list) because traffic from security level 50 is not allowed to reach security level 100. You can create as many security levels as you want...

# How to configure internet access on CISCO ASA 5505

- Configure Gateway of ASA (INSIDE)
  - int g1/2 (pointing to LAN)
  - ip address and subnet mask
  - nameif (name of the inside network)
  - security level 100
  - no shut
- You can verify the configuration
  - show int ip brief
  - show run

# How to configure internet access on CISCO ASA 5505

- Creating DHCP server for LAN
  1. Creating the pool
    - dhcp address 192.168.1.10-192.168.1.20 inside
  2. Setup the DNS Server
    - dhcp dns 8.8.8.8
  3. Setup the Default Gateway of the LAN
    - dhcp option 3 ip 192.168.1.1 (default gateway)
  4. Enable the DHCP (inside)LAN
    - dhcp enable inside (to enable dhcp)

# How to configure internet access on CISCO ASA 5505

- Configure the Default Route
  - 1. Enable default route (similar to static routing)
    - route outside 0.0.0.0 0.0.0.0 10.1.1.2
- You can verify the configuration
  - show int ip brief
  - show run

# How to configure internet access on CISCO ASA 5505

## Configure NAT

1. Create Object groups - Objects are reusable components for use in your configuration. The Object Groups feature allows us to classify users, devices, or protocols into groups and apply those groups to access control lists (ACLs).
  - object network INSDE-NET
  - subnet 192.168.1.0 255.255.255.0
2. Setup the NAT
  - nat (inside,outside)dynamic interface

# How to configure internet access on CISCO ASA 5505

## Firewall Permission

1. Create a class-map - The ASA uses class map to identify traffic, IP addresses, Layer 4 protocols, or application protocols.
  - class-map <inspection\_default>
2. Match the class-map to the default-inspection-traffic
  - match default-inspection-traffic
3. Create a global policy
  - policy-map global\_policy
  - class inspection\_default
  - inspect icmp
4. Apply the services to the traffic you are allowing
  - service-policy global\_policy global

# How to configure internet access on CISCO ASA 5505

## Adding Permission to ASA

1. If you want to add permission, use the commands:

- policy-map global\_policy
- class inspection\_default
- inspect <protocol>

protocols:

DNS

HTTP

FTP

ICMP

# Hello!

## Levy Lozada

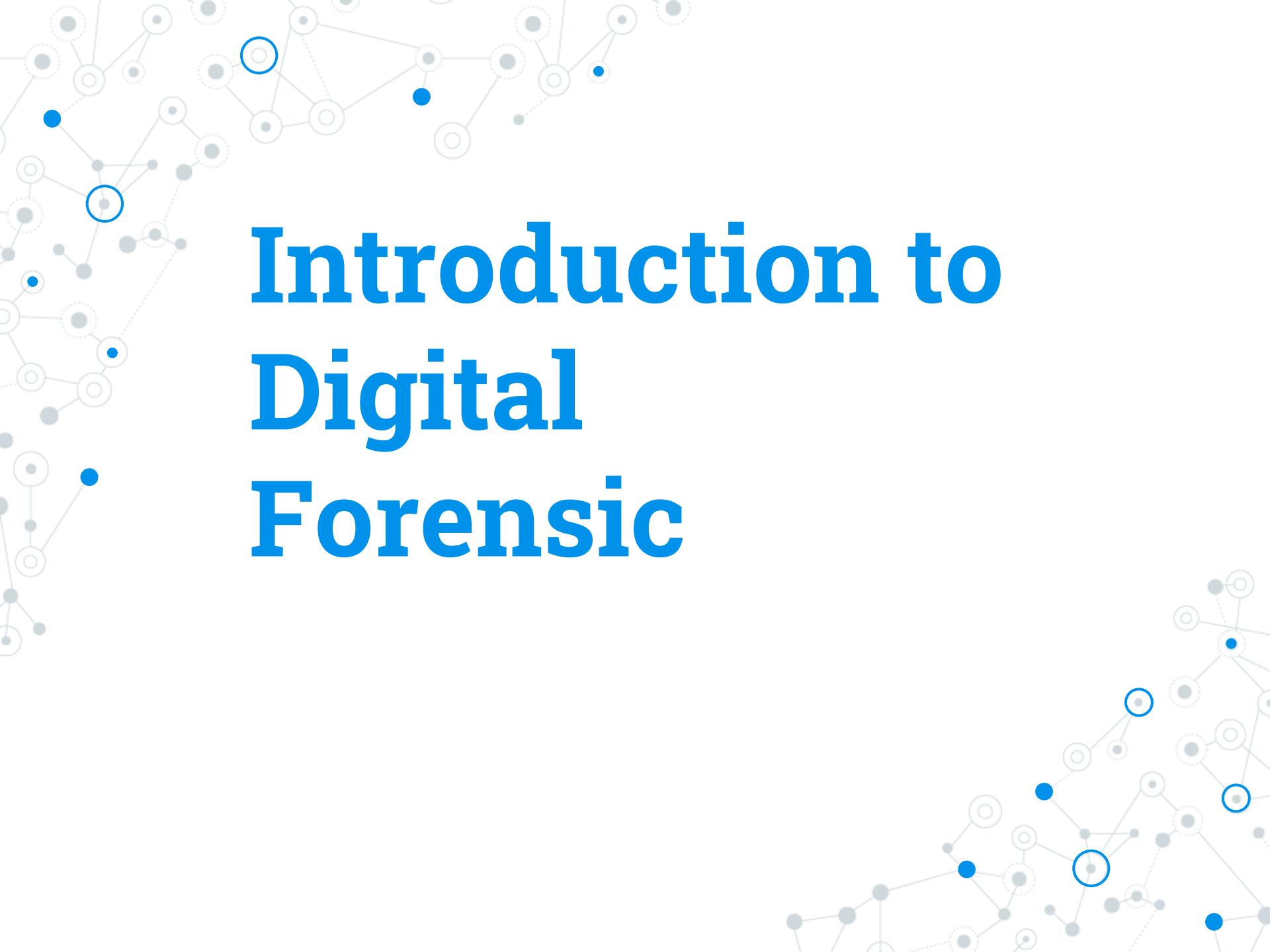
- Police Chief Inspector
- 09189448682
- levylozada@gmail.com



**Microsoft**  
**CERTIFIED**  
Professional

**Microsoft**  
**CERTIFIED**  
Systems Administrator

CompTIA  
**Security+**  
**CERTIFIED**



# Introduction to Digital Forensic

## Course Introduction

### ◎ What you will learn:

- Identification and seizure of electronic evidence
- Digital forensic principles and tools
- Techniques for searching and identifying evidence on digital media pertinent to a case

## Participants Introduction

◎ Please Provide:

- Name
- Position
- Experience in digital forensic
- Course expectation



# Course Schedule

---

Day 1

Modules

- **Course introduction**
  - **Identification and seizure of electronic evidence**
  
  - **Imaging: Forensic acquisition of digital evidence**
  - **Forensic Tools Overview**
  
  - **Hash analysis**
  - **Signature analysis**
- 



# Course Schedule

---

Day 2

Modules

- **Search techniques**
  - **Windows artifacts**
  
  - **Internet artifacts**
  - **Email artifacts**
  
  - **Logical Data storage**
  - **Analysis of Volatile Data**
  
  - **Reporting**
- 





“

*The **more I learn**, the more I learn  
that **I need to learn more**.*

- *unknown*

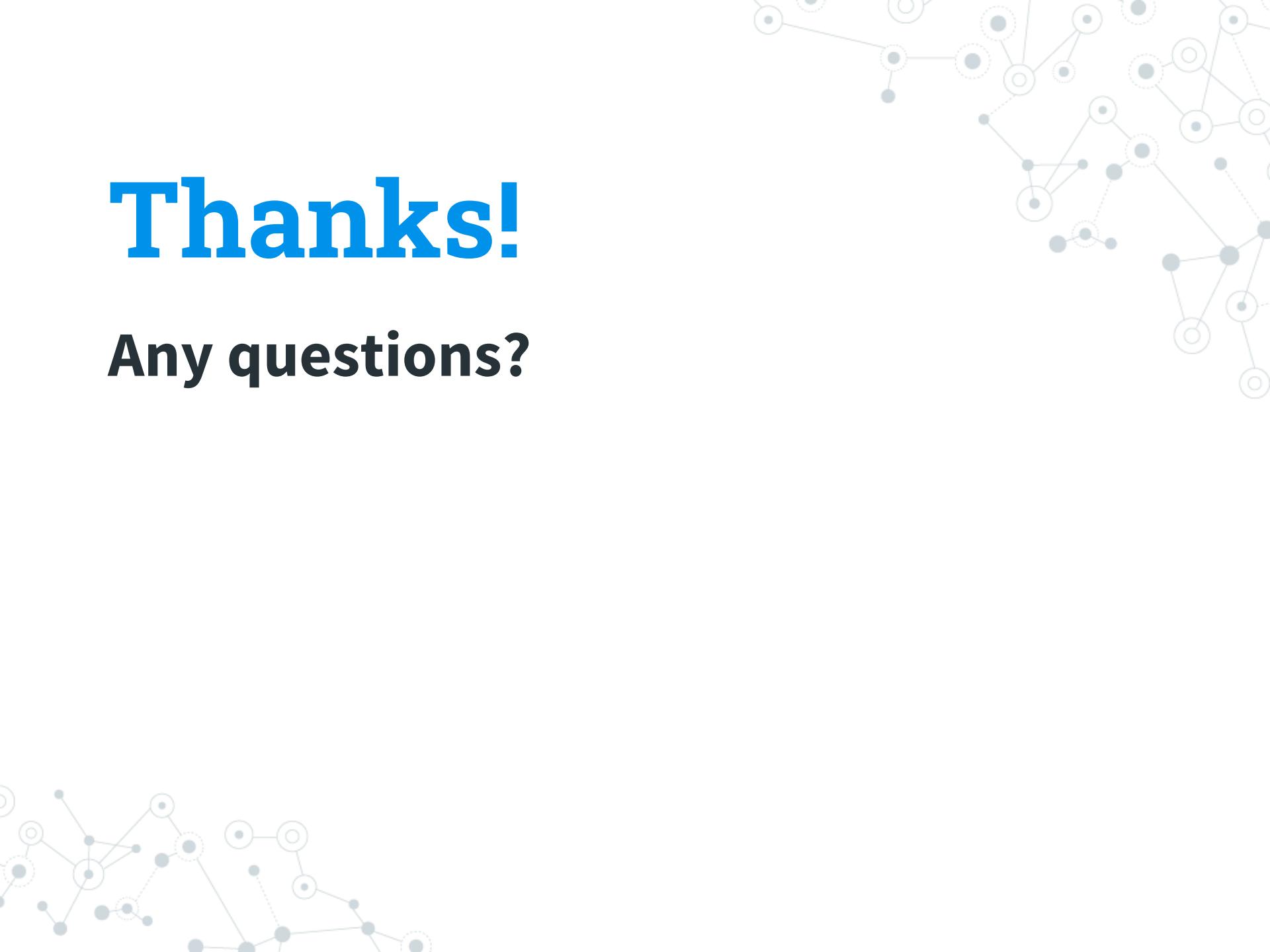
Albert Einstein — 'The more I learn, the more I realize how much I don't know.'

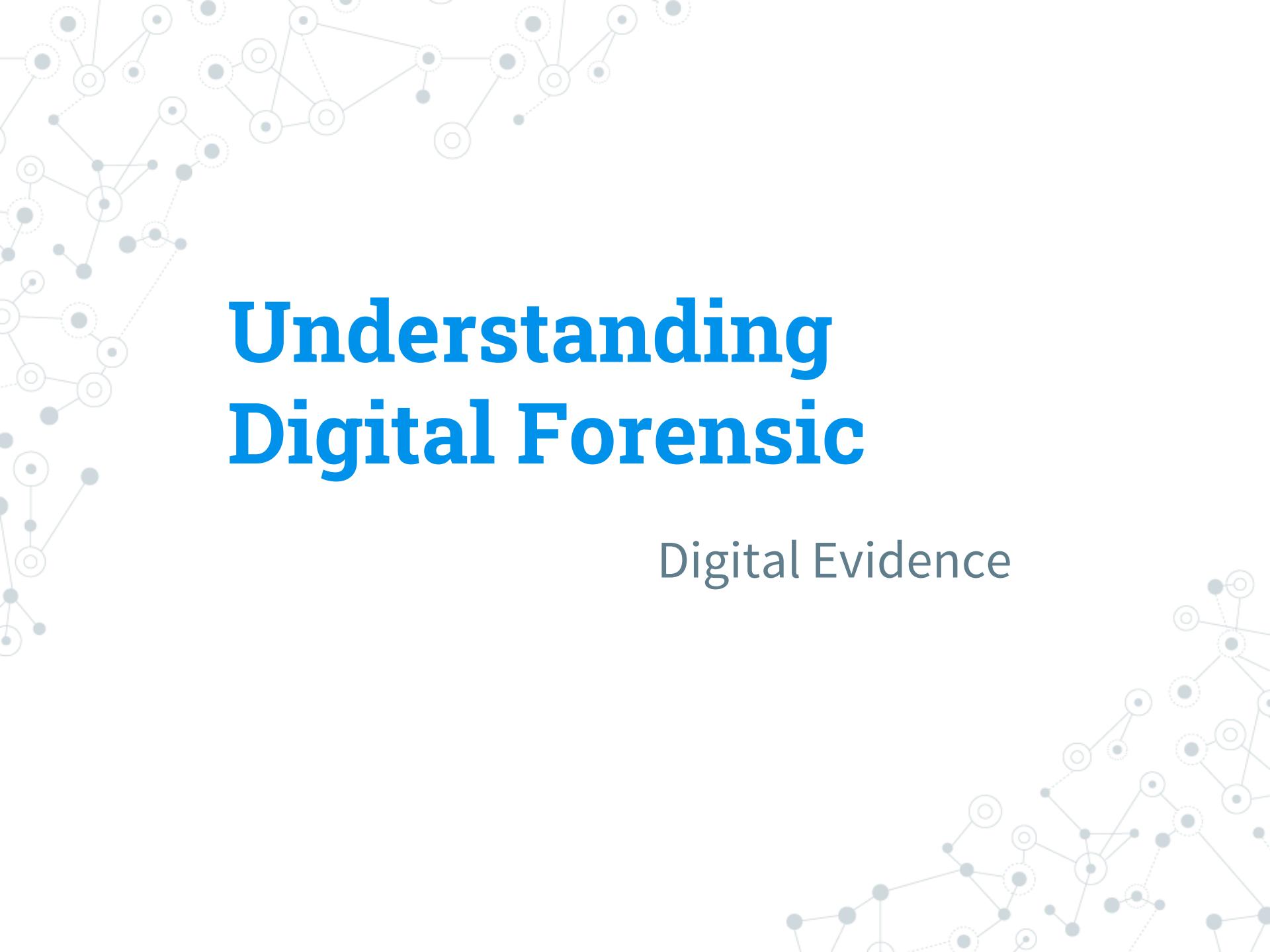
Aristotle — 'The more you know, the more you know you don't know.'

Socrates — 'The more I learn, the more I learn how little I know.'

# Thanks!

Any questions?





# **Understanding Digital Forensic**

Digital Evidence

## What is Digital Forensic?

### ◎ Digital Forensic

- The scientific examination and analysis of data held on or retrieved from computer storage media or network and its presentation in a manner legally acceptable to a Court

## What is Digital Evidence?

### ◎ Digital Evidence

- Refers to digital information that may be used as evidence in a case
- Any information being subject to human intervention or not, that can be extracted from a computer system
- Must be in human-readable format or capable of being interpreted by a person with expertise in the subject

## Digital Forensic Examples

- ◎ Recovering evidence from deliberately formatted hard drive
- ◎ Recovering thousands of deleted emails and chat messages
- ◎ Recovering internet artifacts and file's metadata
- ◎ Performing computer related crime investigation

## Why Digital Forensic

Data as seen by  
**forensic investigator**  
using *sophisticated*  
*forensic tools*.

These data may  
include *deleted*,  
*hidden*, *encrypted*, etc

Data as seen by  
**common users**  
using *windows explorer*, *cmd shell*,  
*web browser*



## Why Digital Forensic?

Any person can gather information from a computer

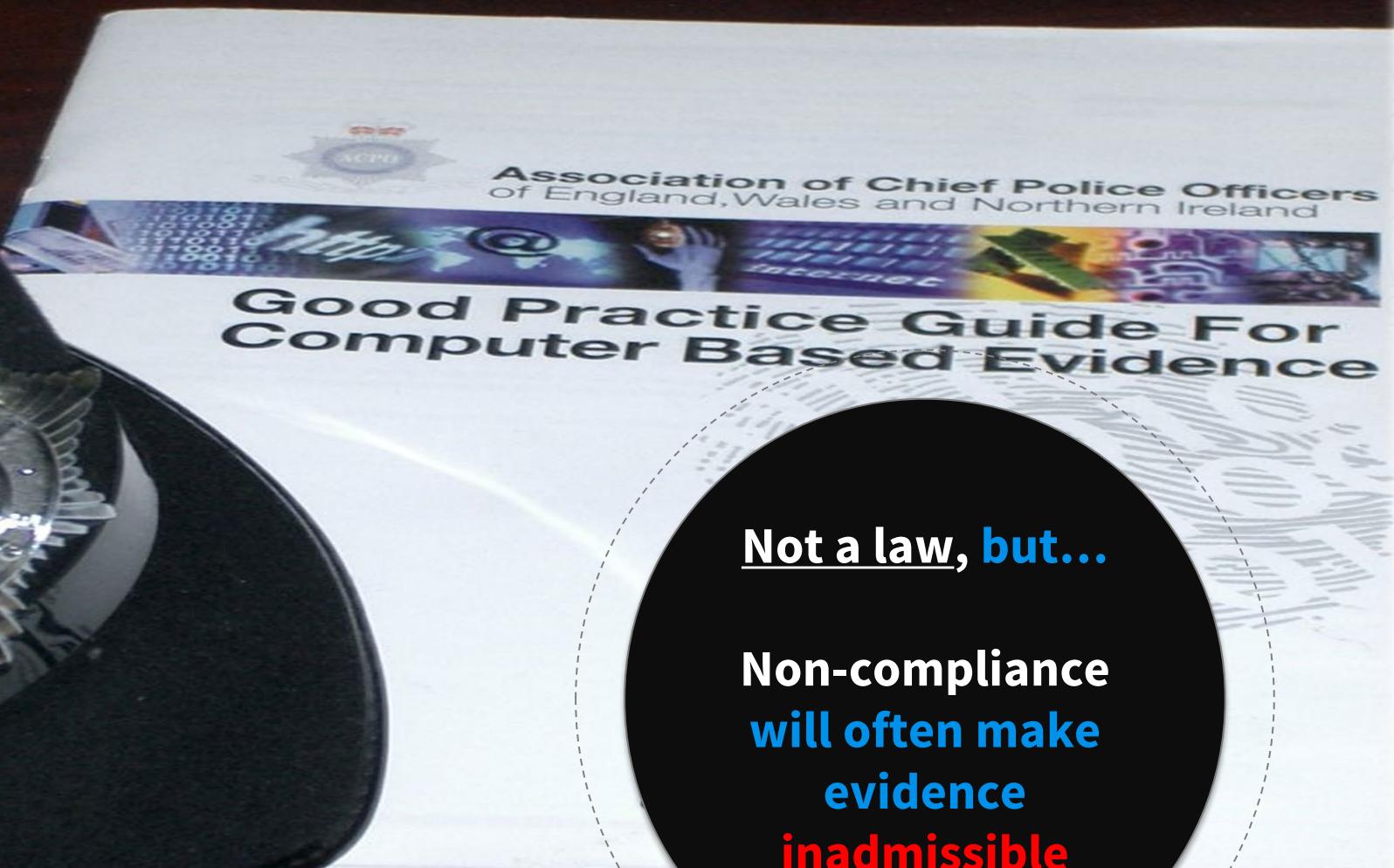
**“ BUT ”**



The Forensic element means it has to be gathered in a manner which makes it reliable to a Court or other body and the information has to become

**“ EVIDENCE ”**





[http://www.7safe.com/electronic\\_evidence/A  
CPO\\_guidelines\\_computer\\_evidence.pdf](http://www.7safe.com/electronic_evidence/A_CPO_guidelines_computer_evidence.pdf)

# ACPO Digital Evidence Principles



## Principle 1 – Primary Rule...

- No action taken by the law enforcement agencies or their agents should change the data held on a computer or other media which may subsequently be relied upon in Court.
- Where possible computer data must be ‘imaged’ and that version be examined.



## Principle 2

- In exceptional circumstances it may be necessary to access the original data held on a target computer.
- However it is imperative that the person doing so is competent and can account for their actions.



## Principle 3

- An audit trail or other record of all processes applied to digital evidence should be created and preserved. An independent third party should be able to examine these processes and achieve the same result.



## Principle 4

- The person in charge of the case has overall responsibility for ensuring that a computer has been correctly examined in accordance with the law and these principles.

# Digital Forensic Process

Identification



Acquisition/  
Imaging



MD5 = ABC123

MD5 = ABC123

Analysis



Reporting



Reports



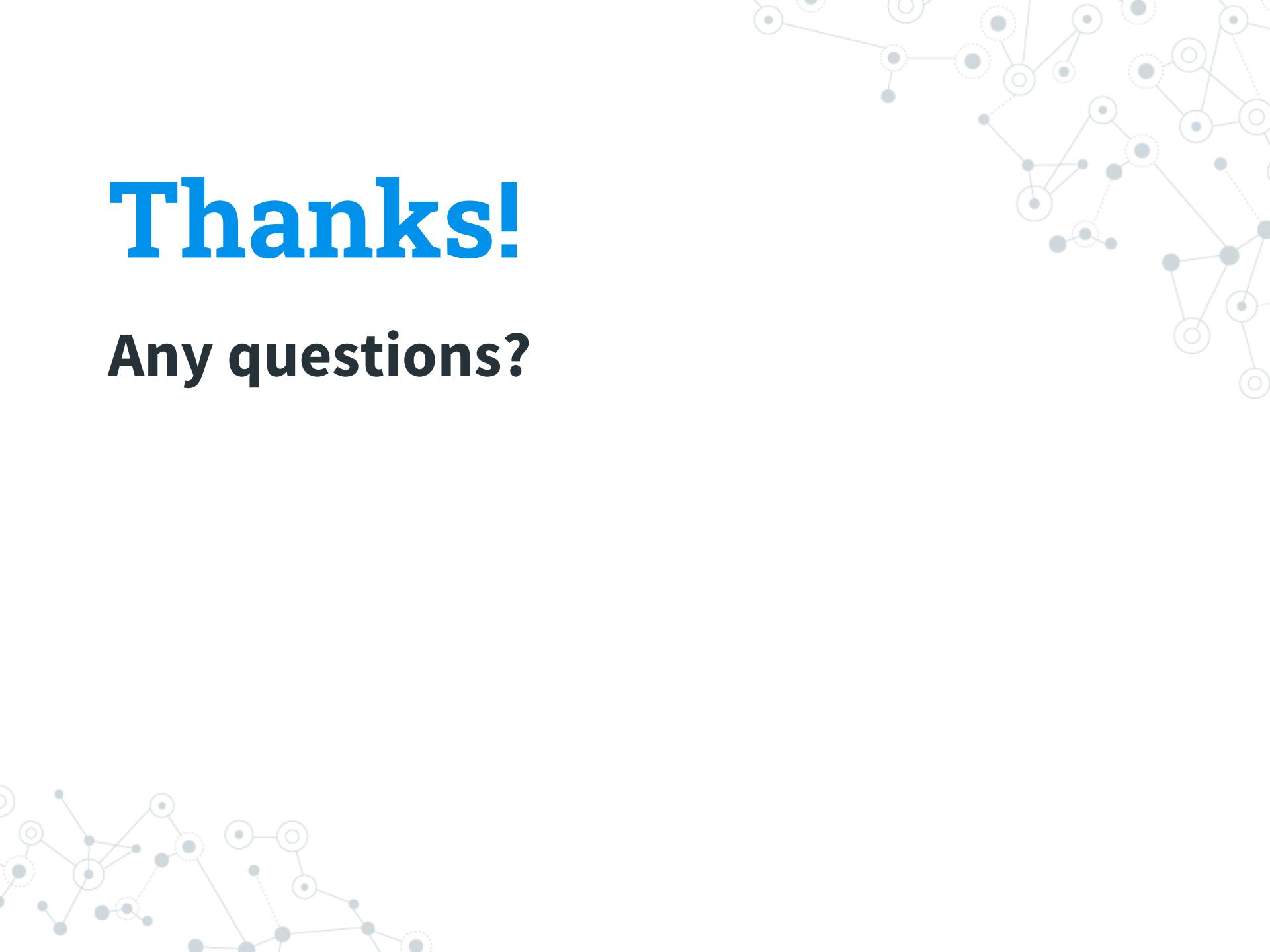
Evidence  
LEFs  
Exports

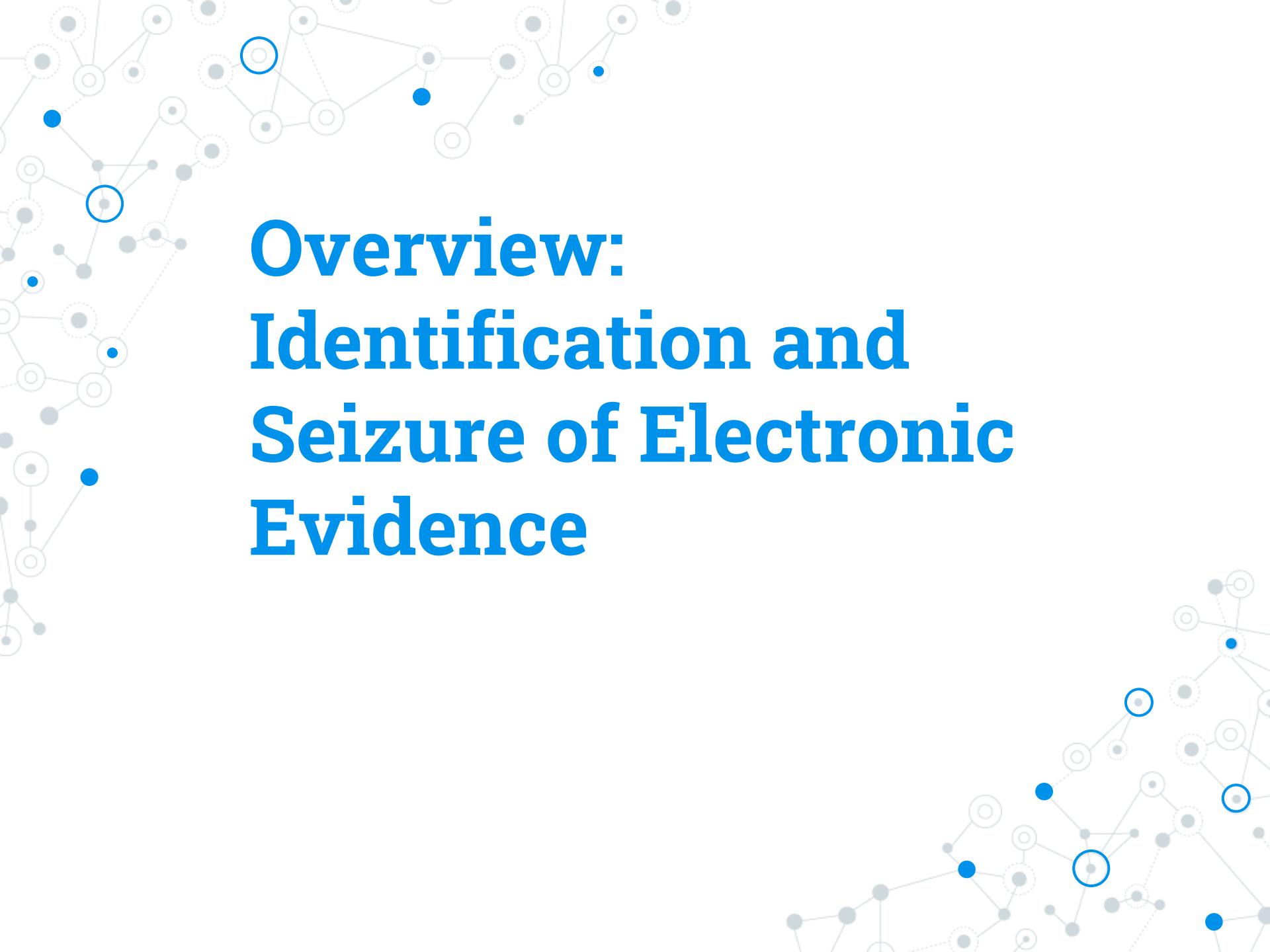
Court  
Presentation



# Thanks!

Any questions?





# **Overview: Identification and Seizure of Electronic Evidence**

## Objective

- ◎ By the end of this module, participants will demonstrate the ability to properly seize electronic evidence.



## Responder's Role

- ◎ Identify all potential electronic evidence at a crime scene
- ◎ Seize the evidence in a manner that supports the investigation and prosecution



## Identification of Electronic Evidence

- ◎ Electronic evidence evolves with advances in technology and market demand
- ◎ Training and awareness by the first responder are critical for identifying evidence



# Computer Hardware



# Computer Software

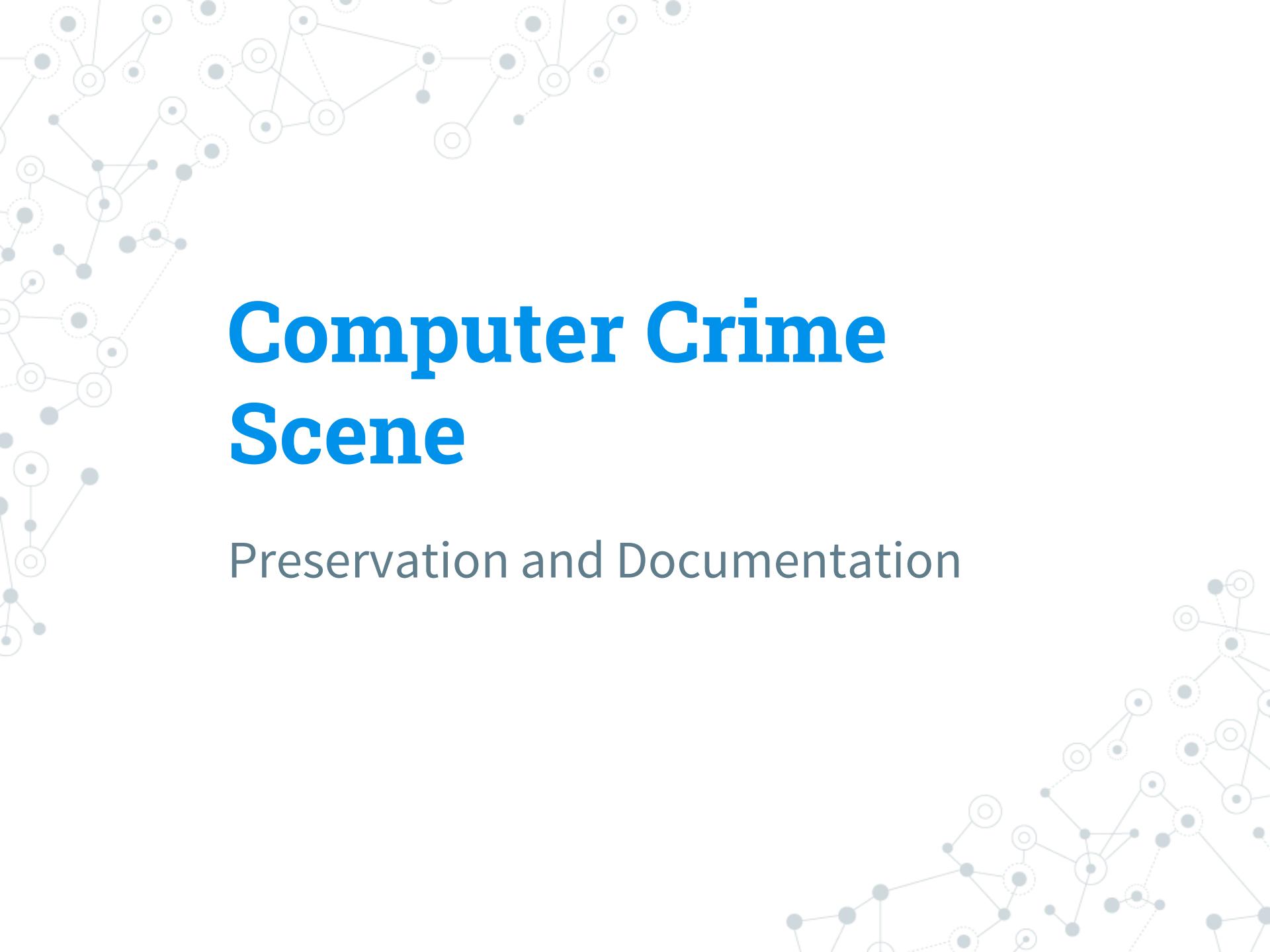


## Where Is the Evidence?

### ◎ Digital Evidence

- Non-volatile data
- Volatile data





# **Computer Crime Scene**

Preservation and Documentation



Traditional  
**Crime Scene**

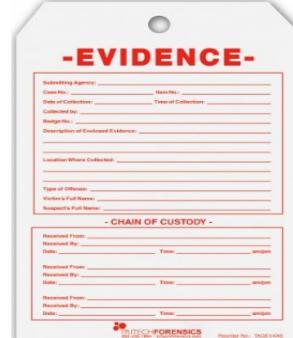
# CRIME SCENE DO NOT CROSS

# CRIME SCENE DO NOT CROSS



## Documentation

- ◎ The first responder must document all steps taken on the scene
- ◎ Documentation:
  - Continues through the investigation
  - Does not stop until case completion



# Windows Task Manager

File Options View Help

Processes Performance App History Startup Users Details Services

Process	Status	1% CPU	37% Memory	0% Disk	0% Network
---------	--------	--------	------------	---------	------------

## Applications (4)

Internet Explorer	0%	125.8 MB	0 MB/s	0 Mbps
Microsoft Word (32 bit)	0.3%	71.6 MB	0 MB/s	0 Mbps
Paint	0%	14.6 MB	0 MB/s	0 Mbps
Windows Task Manager	1.2%	13.3 MB	0 MB/s	0 Mbps

## Background processes (10)

Fast User Switching Utility Service	0%	0.5 MB	0 MB/s	0 Mbps
Media Catalog Object (32 bit)	0%	0 MB	0 MB/s	0 Mbps
Microsoft Windows Search Indexer	0%	0 MB	0 MB/s	0 Mbps
Print driver host for applications	0%	0 MB	0 MB/s	0 Mbps
SMSvcHost.exe	0%	0 MB	0 MB/s	0 Mbps
SMSvcHost.exe	0%	0 MB	0 MB/s	0 Mbps
SMSvcHost.exe	0%	0 MB	0 MB/s	0 Mbps
Spooler SubSystem App	0%	0 MB	0 MB/s	0 Mbps

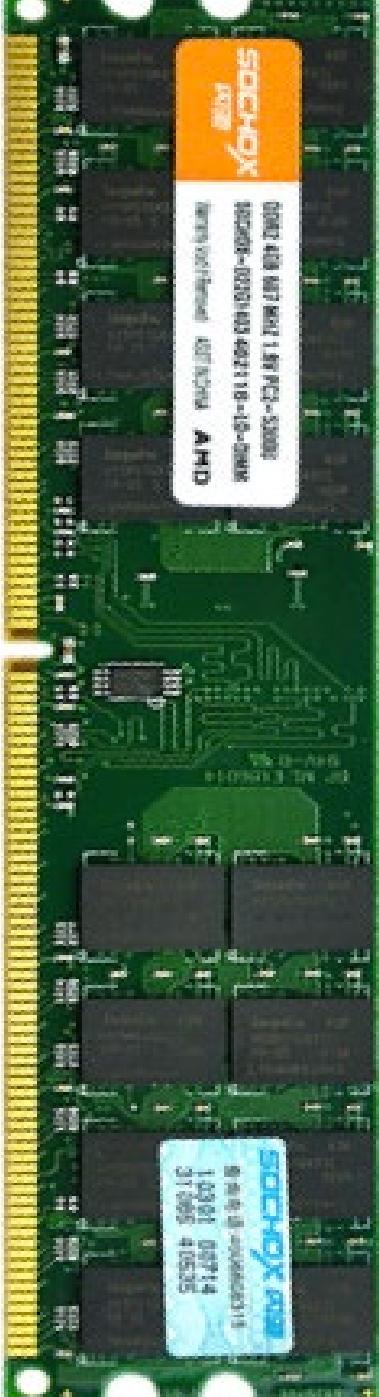
## Windows processes (28)

Client Server Runtime Process
Client Server Runtime Process
Desktop Window Manager

Fewer details

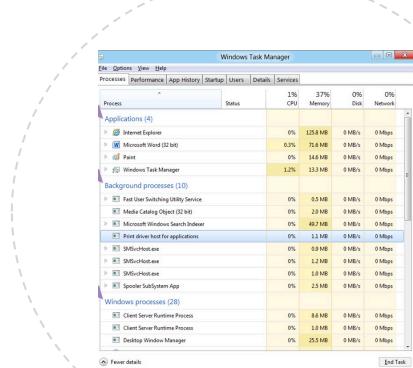
Collection of  
Volatile Data

End Task

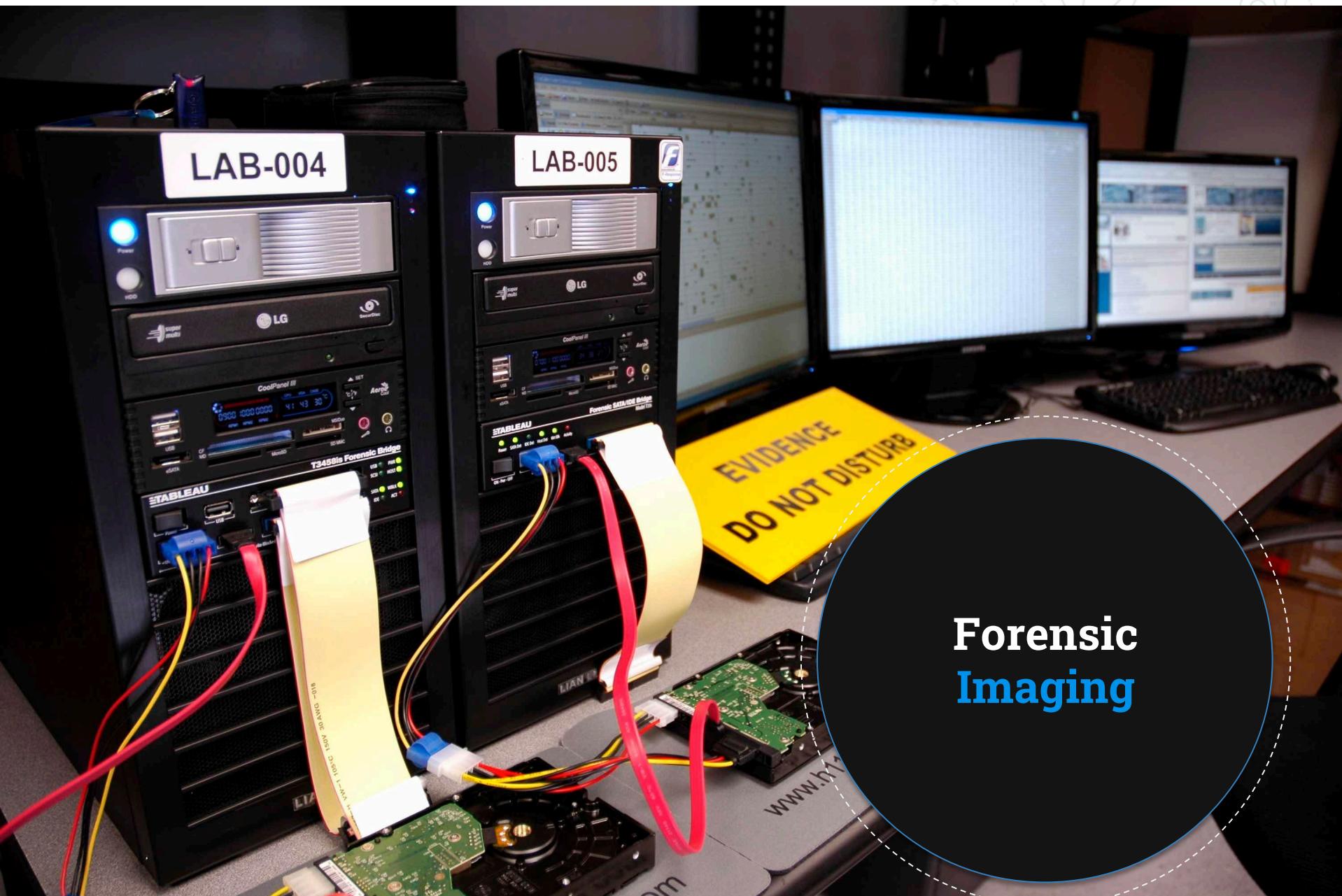


## Collect Volatile Data

- ◎ Resides in temporary storage media and is lost when power is removed
- ◎ Could contain evidence of actions occurring on the system at the exact time of seizure
- ◎ Must be collected quickly at the crime scene using validated tools and proper procedures



# Forensic Imaging



## Forensic Imaging

- ◎ Non-volatile data resides in persistent storage media
- ◎ The first responder must understand legal and technical boundaries
  - Can you legally obtain a forensic copy of source media?
  - Does obtaining a forensic image make sense?
  - If so...which kind? Logical or physical?
  - Do you have the tools to properly obtain the image?



## Process Physical Evidence

◎ Execute “bag and tag” procedures to transport seized items

- Computer hardware
- Collected software
  - Volatile data
  - Triage data
  - Forensic Images collected on-scene



## Troubleshooting

### ◎ The first responder must:

- Have problem solving skills and patience
- Consider:
  - ◎ How to collect physical/digital evidence
  - ◎ The benefit of using a specific tool or technique
  - ◎ How to avoid contaminating evidence



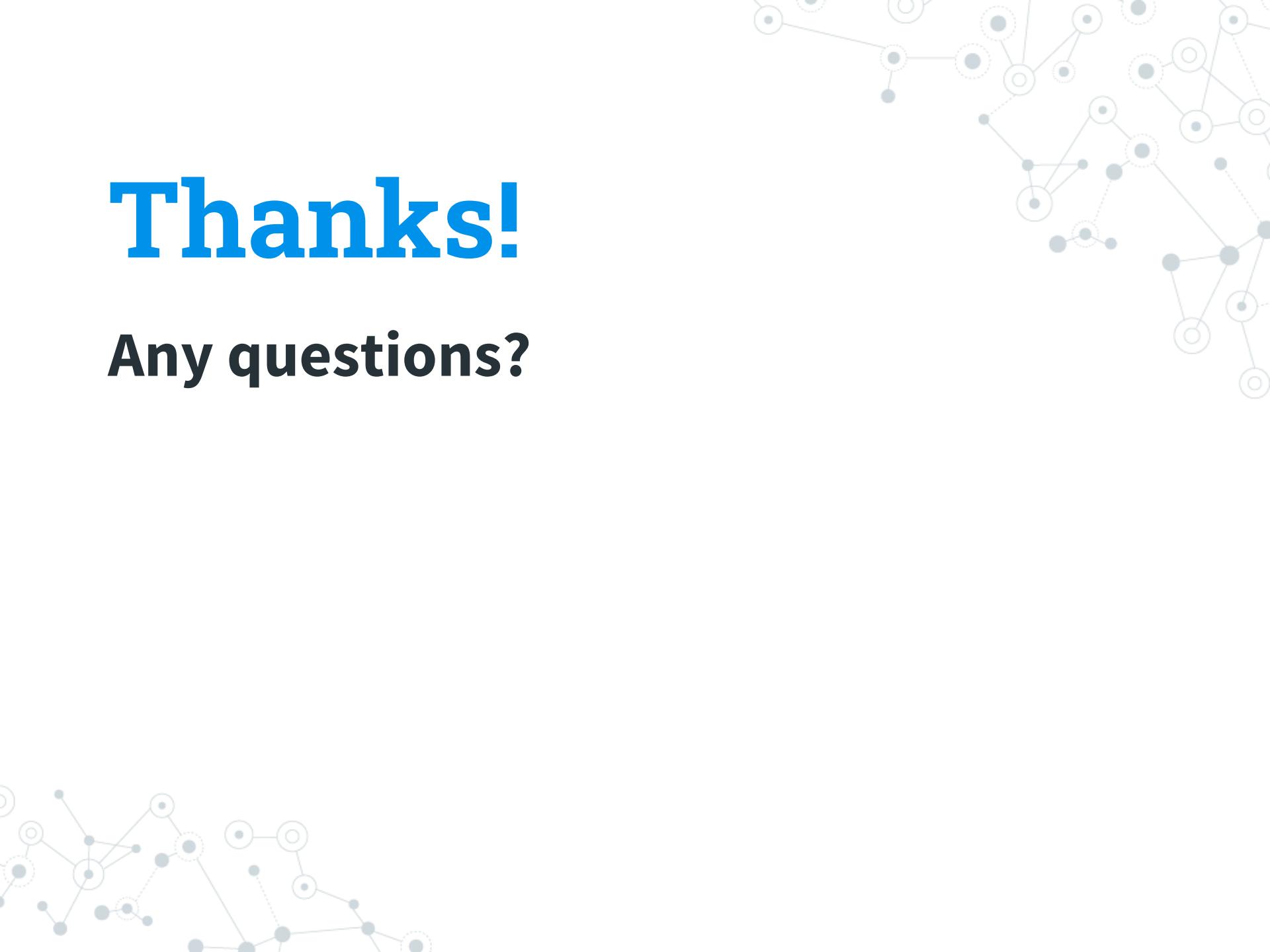
## Summary

- ◎ The proper collection of physical/digital evidence is one of the most important aspects of the digital forensics process
- ◎ If this collection is not done correctly, critical evidence can be lost



# Thanks!

Any questions?





# **Imaging: Forensic**

# **Acquisition of Digital Evidence**

## Objective

- ◎ By the end of this module, participants will be able to create a forensically sound image of digital media consistent with industry best practices



# Digital Forensic Process



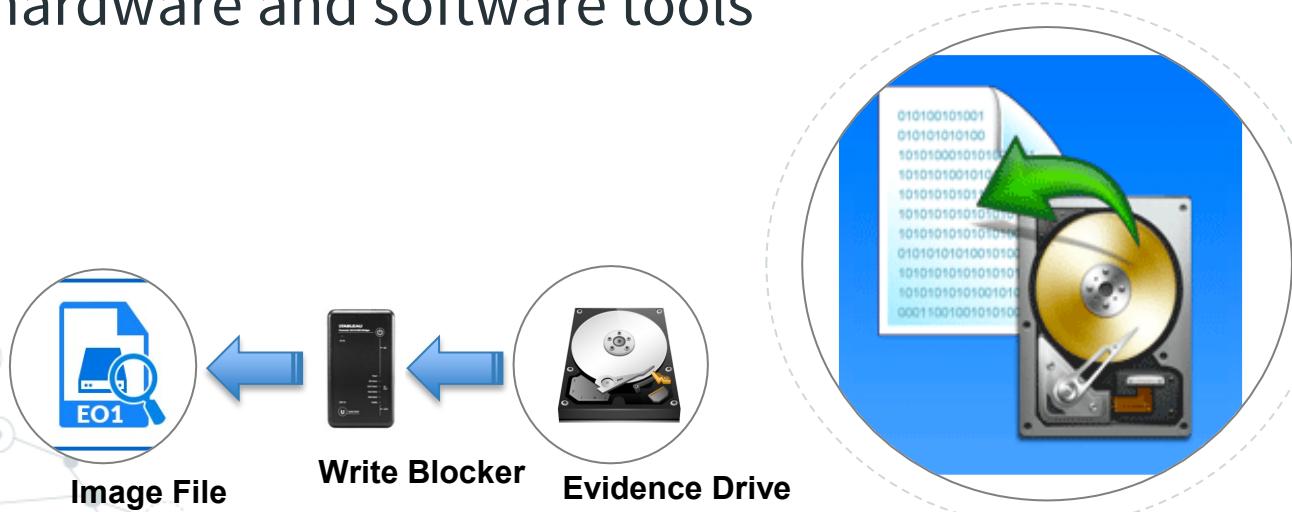
◎ Imaging is the second phase and requires forensically-sound procedures and validated tools



# Digital Forensic Image Acquisition

◎ Forensic image is:

- A verifiable duplicate of all the contents of a storage media or selected files in a form of encapsulated file.
- Acquired by trained digital forensic examiner using validated hardware and software tools



## Hardware-based Imaging Tools

- ◎ Write blocker (physical bridge)
- ◎ Stand-alone imaging device (multifunction tool with dedicated forensic capabilities)



## Software-based Imaging Tools

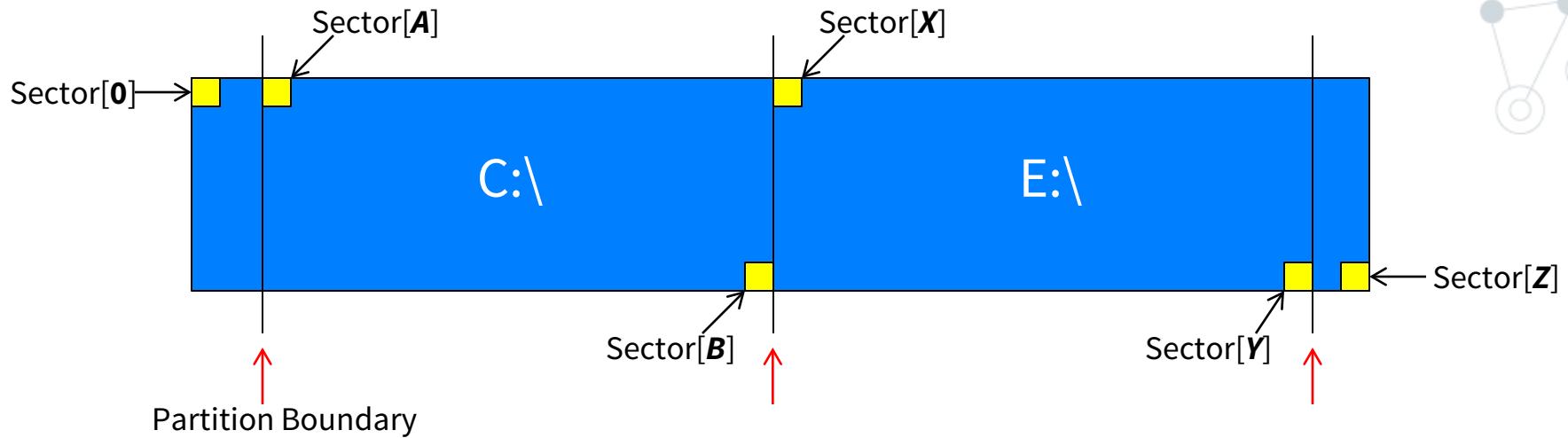
- ◎ Write-blocker: Specialized application
- ◎ Forensic Imager: Multi-function tools that assist with hard drive preparation and duplication, forensic imaging, and verification

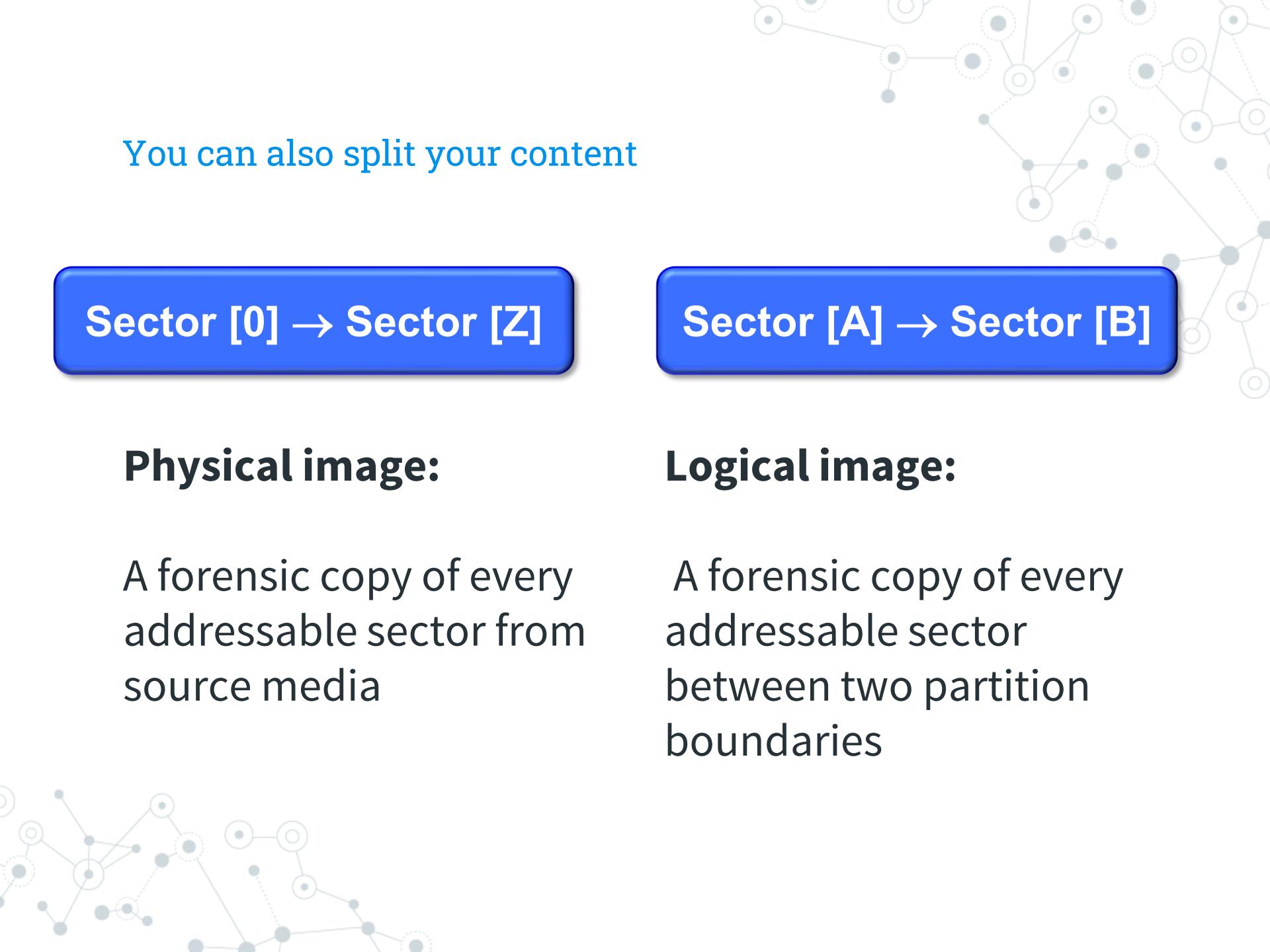


## Imaging Tools Concept



## Imaging a Hard Disk Drive



A faint, light-gray network diagram consisting of numerous small, semi-transparent circles of varying sizes connected by thin gray lines, forming a complex web-like structure.

You can also split your content

**Sector [0] → Sector [Z]**

**Sector [A] → Sector [B]**

## **Physical image:**

A forensic copy of every addressable sector from source media

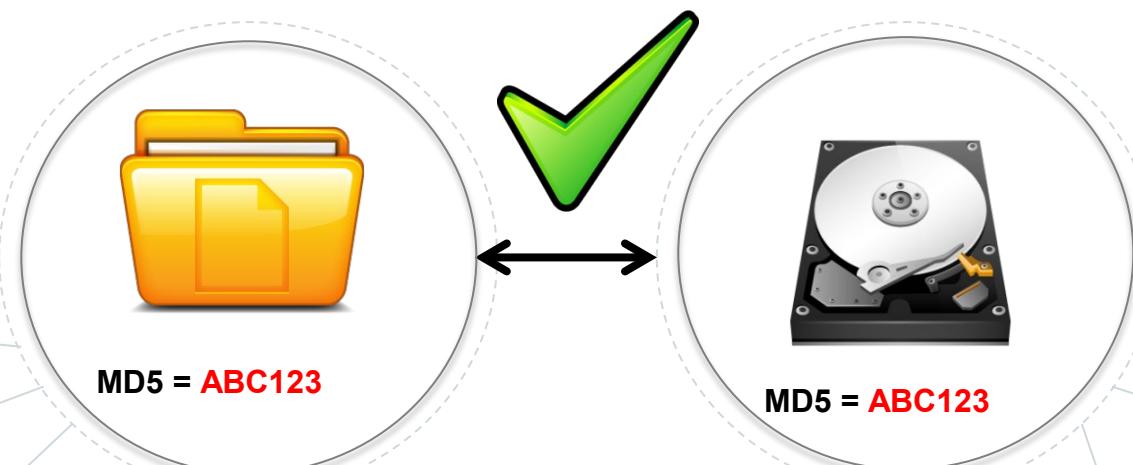
## **Logical image:**

A forensic copy of every addressable sector between two partition boundaries

## Verification of Forensic Image

### ◎ Hash:

- Is a mathematical algorithm
- Produces a unique digital fingerprint
- Verifies that binary content of an acquired forensic image is exactly the same as the source media



## Preparation of Destination Storage Media

- ◎ Verify size requirements of original evidence
- ◎ Select storage media that meets or exceeds capacity of source
- ◎ Sterilize destination media
- ◎ Format storage media

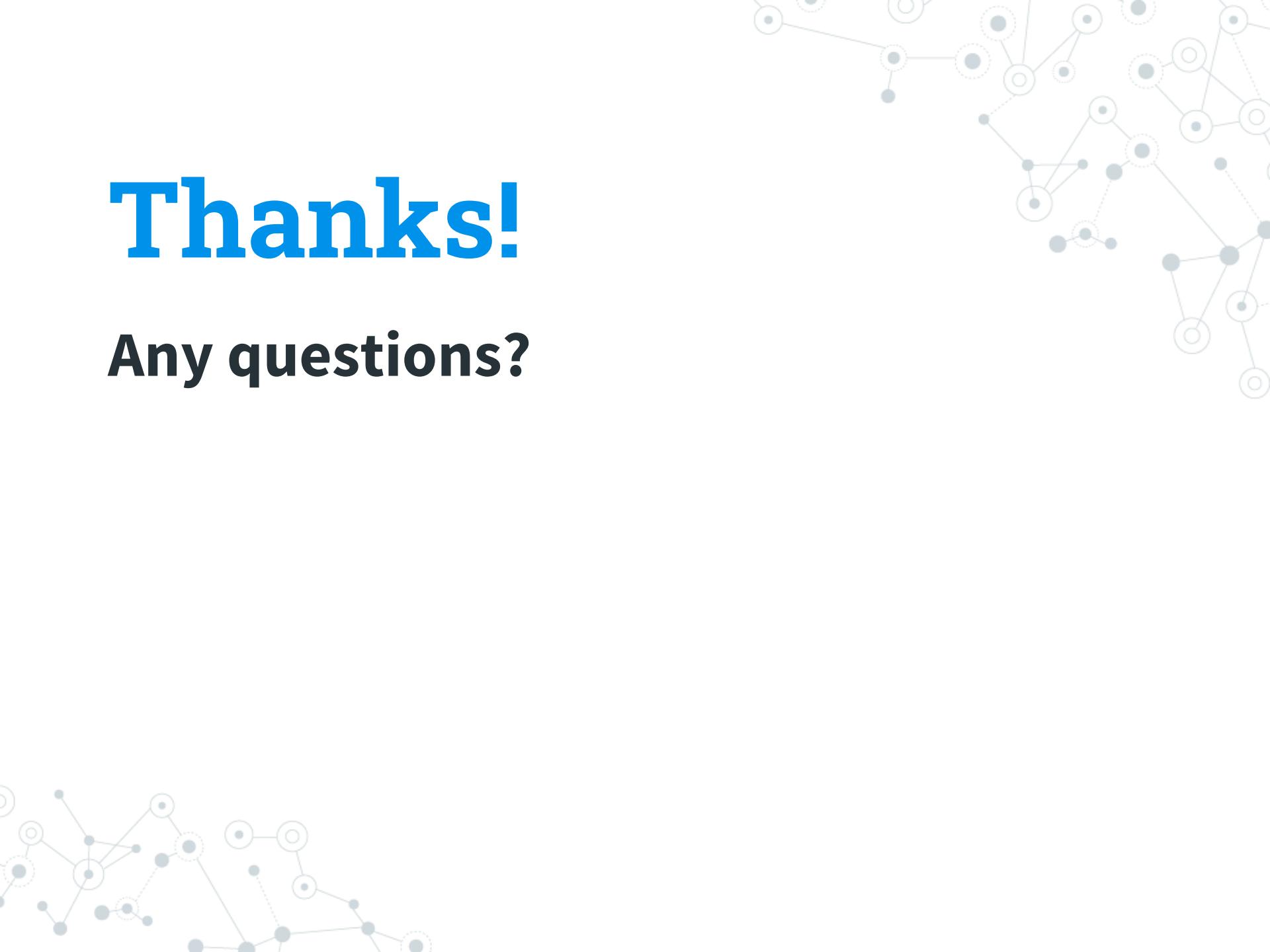


## Summary

- ◎ Forensic Imaging of digital evidence is one of the important phase of digital forensic process to preserve and ensure the integrity of the evidence
- ◎ Digital forensic examiner must follow established forensic procedures when acquiring digital evidence from source media

# Thanks!

Any questions?





# Overview: Digital Forensic Tools

## Objective

- ◎ By the end of this module, participants will be able to use basic features of a forensic tool to examine digital evidence



## Software: Digital Forensic Tool

- ◎ Enables searches within image files
- ◎ Streamlines investigations
- ◎ Includes:
  - **EnCase** by Guidance Software
  - **Forensic Toolkit (FTK)** by Access Data
  - **Autopsy** Open Source





# EnCase

Guidance Software

## Introduction to EnCase

◎ Digital data acquisition tool that enables:

- Email and file system analysis
- Remote imaging and investigations
- Advanced searches
- Remote previewing
- Malicious code discovery



## Introduction to EnCase

◎ Step Action, you will work individually to:

- Install and configure EnCase
- Examine evidence files
- Sort files
- Create bookmarks
- Generate report





# **Forensic Tool Kit**

## **(FTK)**

Access Data

## Introduction to FTK

- ◎ Digital data acquisition tool that:
  - Is similar to EnCase in overall features
  - Uses a different approach to data storage and terminology

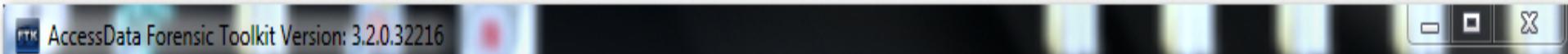


## Introduction to FTK

◎ The facilitators will demonstrate how to

- Log in to the database
- Create a new case
- Manage evidence
- Refine results
- Generate a report

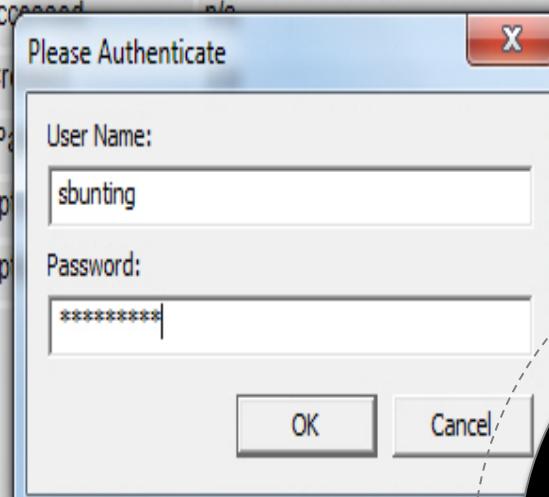




File Database Case Tools Manage Help

Cases

Name	Date Modified	Case ID	n/a
		Case Owner	n/a
		Reference	n/a
		Date Modified	n/a
		Date Accessed	n/a
		Date Created	n/a
		Case Path	n/a
		Description	sbunting
		Description	n/a
		n/a	n/a



**Log in to  
Database**

File Database Case Tools Manage Help

Cases

Name

New...

Open

Assign Users...

Backup

Restore

Delete

Copy Previous Case...

Refresh Case List

F5

Case ID	n/a
Case Owner	n/a
Reference	n/a
Date Modified	n/a
Date Accessed	n/a
Date Created	n/a
Case Path	n/a
Description	n/a
Description	n/a
n/a	n/a

Create a  
New Case



File Database Case Tools Manage Help

Cases

Name

FTK New Case Options

Owner: sbunting

Case Name: FTK Overview

Reference:

Description: FTK Overview

Description File:

Case Folder Directory: C:\FTKCases

Field Mode

Open the case

[Detailed Options...](#)

[OK](#)

Description

n/a

New Case  
Options

File Database Case Tools Manage Help

Manage Evidence



Display Name	State
EnCaseOverview.E01	+

Path: I:\evidencefile\EnCaseOverview.E01

ID / Name: Overview Evidence File

Description:

Evidence Group:

Time Zone: America/New\_York

Field Mode

Add

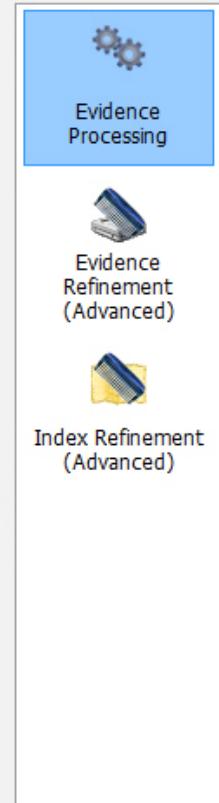
Remove

Description

n/a

Manage  
Evidence

## Refinement Options

**Evidence Processing**

## Generate File Hashes (flag duplicates)

- MD5 Hash
- SHA-1 Hash
- SHA-256 Hash
- Fuzzy Hash

- Flag Duplicate Files
- KFF

[Fuzzy Hash Options...](#) Expand Compound Files

Takes extra time to expand files like email boxes, zips and OLE documents.

[Expansion Options...](#) File Signature Analysis Flag Bad Extensions Entropy Test dtSearch® Text Index Create Thumbnails for Graphics HTML File Listing Data Carve Meta Carve Optical Character Recognition Explicit Image Detection Registry Reports Send Email Alert on Job Completion CSV File Listing[Carving Options...](#)[OCR Options...](#)[EID Options...](#)[RSR Directory...](#)[Reset](#)[OK](#)[Cancel](#)

n/a

n/a

n/a

n/a

n/a

n/a

# Refinement Options

File Database Case Tools Manage Help

FTK Data Processing Status: 3.2.0.32216

File

- [-] Add Evidence Jobs
  - [... EnCaseOverview.E01 (Processing)]
- [-] Additional Analysis Jobs
- [-] Live Search Jobs
- [-] Other Jobs

Add Evidence Progress

Overall: 

Discovered: 11451

Processed: 5419 

Indexed: 471 

Process State: Processing

Evidence Item

Name: EnCaseOverview.E01

Path: I:\evidencefile\EnCaseOverview.E01

Process Manager: localhost

Job Folder...

Remove when finished

Messages

Type	Message
INFO	[1:39 PM 6/29/2012] Using engine localhost
INFO	[1:39 PM 6/29/2012] Database preparation started
INFO	[1:39 PM 6/29/2012] Database preparation finished
INFO	[1:39 PM 6/29/2012] Processing started
INFO	[1:39 PM 6/29/2012] Indexing started

Data  
Processing  
Status

File Edit View Evidence Filter Tools Manage Help

Filter: -unfiltered- Filter Manager...

Explore Overview Email Graphics Bookmarks Live Search Index Search Volatile

Evidence Items

- + Dropbox
- + Favorites
- + Links
- + Local Settings
- + Music
- + My Documents
- + NetHood
- + Pictures
- + PrintHood
- + Recent
- + Saved Games
- + Searches
- + SendTo
- + Start Menu
- + Templates
- + Videos
- + Windows
- + [unallocated space]

File Content  
Hex Text Filtered Natural



File Content Properties Hex Interpreter

File List

<input type="checkbox"/>	Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created
<input type="checkbox"/>	\$130		15355		EnCaseOverview.E01/P...	Index ...	4096 B	4096 B	D124B...	533645...	149781...	2/2/2017
<input type="checkbox"/>	desktop.ini		15356	ini	EnCaseOverview.E01/P...	Text	504 B	504 B	29EAE...	D62CC...	888569...	2/2/2017
<input type="checkbox"/>	SkipjackBest01.jpg		15357	jpg	EnCaseOverview.E01/P...	JPEG E...	1332 KB	1330 KB	52F80B...	BBB05...	1BC2E...	2/3/2017
<input type="checkbox"/>	SkipjackBest01.jpg.FileS...		81358		EnCaseOverview.E01/P...	Slack S...	1484 B	1484 B	n/a	n/a	n/a	n/a
<input type="checkbox"/>	SkipjackBest02.jpg		15358	jpg	EnCaseOverview.E01/P...	JPEG E...	1744 KB	1740 KB	423921...	992D9...	AD4DA...	2/3/2017
<input type="checkbox"/>	SkipjackBest02.jpg.FileS...		81359		EnCaseOverview.E01/P...	Slack S...	3500 B	3500 B	n/a	n/a	n/a	n/a
<input type="checkbox"/>	SkipjackBest04.jpg		15359	jpg	EnCaseOverview.E01/P...	JPEG E...	1392 KB	1388 KB	3E63D...	46D71...	BE06F7...	2/3/2017
<input type="checkbox"/>	SkipjackBest04.jpg.FileS...		81360		EnCaseOverview.E01/P...	Slack S...	3967 B	3967 B	n/a	n/a	n/a	n/a

FTK  
Explore Tab



File Edit View Evidence Filter Tools Manage Help

Filter: -unfiltered- Filter Manager...

Explore Overview Email Graphics Bookmarks Live Search Index Search Volatile

Case Overview

File Content

Hex Text Filtered Natural

- + Evidence Groups ( 292,187 / 292,187 )
- + File Items
- + .ext File Extension ( 152,940 / 152,940 )
- + File Category ( 292,187 / 292,187 )
- + File Status
- + Email Status
- + Labels ( 0 / 0 )
- + Bookmarks

File List



Explore Overview Email Graphics Bookmarks

### Case Overview

- + Evidence Groups ( 292,187 / 292,187 )
- + File Items
- + .ext File Extension ( 152,940 / 152,940 )
- + File Category ( 292,187 / 292,187 )
- + File Status
- + Email Status
- + Labels ( 0 / 0 )
- + Bookmarks



Loaded: 0 Filtered: 0 Total: 0 Highlighted: 0 Checked: 0 Total LSize: 0

Ready

Overview Tab Filter: [None]

- + Email Status
- + Email Archives
- + Email by Date
- + Email Addresses
  - + Senders [From] (0 / 0)
  - + Recipients [To, CC, BCC] (0 / 0)
- Email (33 / 33)
- + MIME (8 / 8)
- + Outlook PST (2 / 2)

## File List

<input checked="" type="checkbox"/>	Subject	Name	To	From	CC	BCC	Submit ...	Deliver...	Unread	Unsent	Has Att...	Created	Accessed
<input type="checkbox"/>	Changes to Go...	49053654-0000...	G3tR00...	Google ...			2/21/2...				False	6/18/2012 5:47...	6/18/2012 5:47...
<input type="checkbox"/>	Re: Special file ...	4D064DB7-0000...	"Susie ...	Johny ...			2/2/20...				False	2/2/2012 5:12...	2/2/2012 5:12...
<input checked="" type="checkbox"/>	Re: Special file ...	56B254CA-0000...	"Susie ...	Johny ...			2/3/20...				False	2/3/2012 11:09...	2/3/2012 11:09...
<input type="checkbox"/>	Get 16 GB of Dr...	5AF12CE4-0000...	g3tR00t...	Dropbo...			4/4/20...				False	6/18/2012 5:47...	6/18/2012 5:47...
<input type="checkbox"/>	Changes to Go...	65F70325-0000...	G3tR00...	Google ...			2/21/2...				False	6/18/2012 5:47...	6/18/2012 5:47...

Loaded: 23 | Filtered: 23 | Total: 23 | Highlighted: 1 | Checked: 0 | Total LSize: 97.41 KB

## File Content

Hex Text Filtered Natural



## Re: Special file attached

**From:** Johny User <g3tR00tn0w@gmail.com>  
**To:** "Susie User" <youg0tr00t@gmail.com>  
**Subject:** Re: Special file attached  
**Sent:** Fri, 3 Feb 2012 11:08:50 -0500

Suzie,

I just went into the company's supposedly secured and classified data storage, only is wasn't to secure. Now that's a surprise I know!

Anyway, I found some satellite imagery that I know we can get some money for if we sell it.

I put the sat pictures in that new dropbox, but since I'm not yet familiar with it enough to trust it, I put them on a USB drive also. I won't have any problem walking out of here with that little device.

File Content Properties Hex Interpreter

EnCaseOverview.E01/Partition 2/NONAME [NTFS]/[root]/Users/user.DC/AppData/Local/Microsoft/Windows Live Mail/Gmail (G3tR 9b3/[Gmail]/Sent Mail/56B254CA-00000002.eml

Ready

Email Tab Filter: Email Files\_Attachments

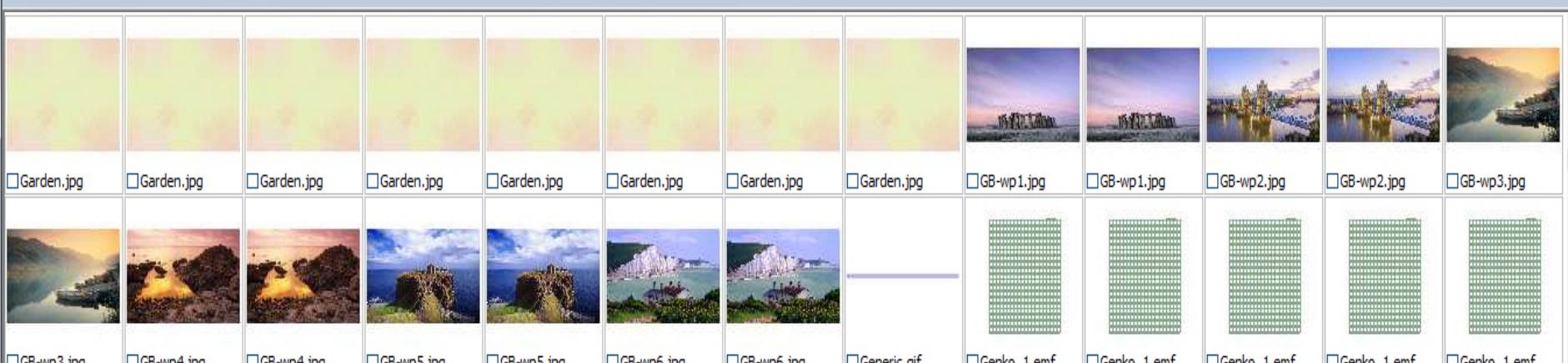
FTK  
Email Tab

File Edit View Evidence Filter Tools Manage Help

Filter: -unfiltered -

Explore Overview Email Graphics Bookmarks Live Search Index Search Volatile

Thumbnails



Loaded: 6,882

Filtered: 6,882

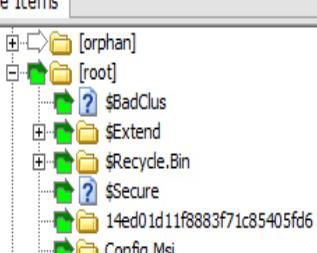
Total: 260,524

Highlighted: 0 Checked: 0

Total LSize: 248.0 MB

 Show Tooltip

Evidence Items



File Content

 Hex  Text  Filtered  Natural

 File Content  Properties  Hex Interpreter

# FTK Graphics Tab

File List

<input type="checkbox"/>	Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created
<input type="checkbox"/>	\$RK9H2EP.jpg		1164	jpg	EnCaseOverview.E01/P...	JPEG E...	5904 KB	5902 KB	BBDC4...	36D58...	36F30...	2/3/20...
<input type="checkbox"/>	(120DPI)alertIcon.png		3209	png	EnCaseOverview.E01/P...	PNG	4096 B	652 B	3FAB6...	E5A0F...	DFCE1...	6/10/200...
<input type="checkbox"/>	(120DPI)alertIcon.png		11269	png	EnCaseOverview.E01/P...	PNG	4096 B	652 B	3FAB6...	E5A0F...	DFCE1...	6/10/2009 3...
<input type="checkbox"/>	(120DPI)alertIcon.png		101931	png	EnCaseOverview.E01/P...	PNG	4096 B	652 B	3FAB6...	E5A0F...	DFCE1...	6/10/2009 4:5...
<input type="checkbox"/>	(120DPI)alertIcon.png		164997	png	EnCaseOverview.E01/P...	PNG	4096 B	652 B	3FAB6...	E5A0F...	DFCE1...	6/10/2009 5:38...
<input type="checkbox"/>	(120DPI)grayStateIcon...		3210	nnn	EnCaseOverview.E01/P...	PNG	429 B	429 B	A03FF...	CD7D4...	918460...	7/13/2009 5:47...

Loaded: 6,882

Filtered: 6,882

Total: 260,524

Highlighted: 0 Checked: 0

Total LSize: 248.0 MB

Ready

Graphics Tab Filter: Graphic Files

File Edit View Evidence Filter Tools Manage Help

Filter: -unfiltered- Filter Manager...

Explore Overview Email Graphics Bookmarks Live Search Index Search Volatile

Bookmarks

- Bookmarks
  - sbunting
    - Significant Image
  - Shared

Bookmark Information

Bookmark Name:

Significant Image

Creator Name:

sbunting

Related Comment:

File Comment:

Selection Comment:

Selection(s):

File Content

Hex Text Filtered Natural



# FTK Bookmarks Tab

File Content Properties Hex Interpreter

File List

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Create
GB-wp5.jpg		20255	jpg	EnCaseOverview.E01\P...	JPEG E...	628.0 KB	624.3 KB	BFEA7...	EAA06...	650A0...	7/14/200...

Loaded: 1 Filtered: 1 Total: 1 Highlighted: 1 Checked: 1 Total LSize: 624.3 KB

EnCaseOverview.E01/Partition 2/NONAME [NTFS]/[root]/Windows/Globalization/MCT/MCT-GB/Wallpaper/GB-wp5.jpg

Ready

Bookmarks Tab Filter: [None]

Text Pattern Hex

Add Clear Export Import

ANSI  Unicode  Other Code Pages Select...  Case Sensitive

Search Terms Type Code Pages

Max Hits Per File: 200 Search Filter: -unfiltered- Search

File Content

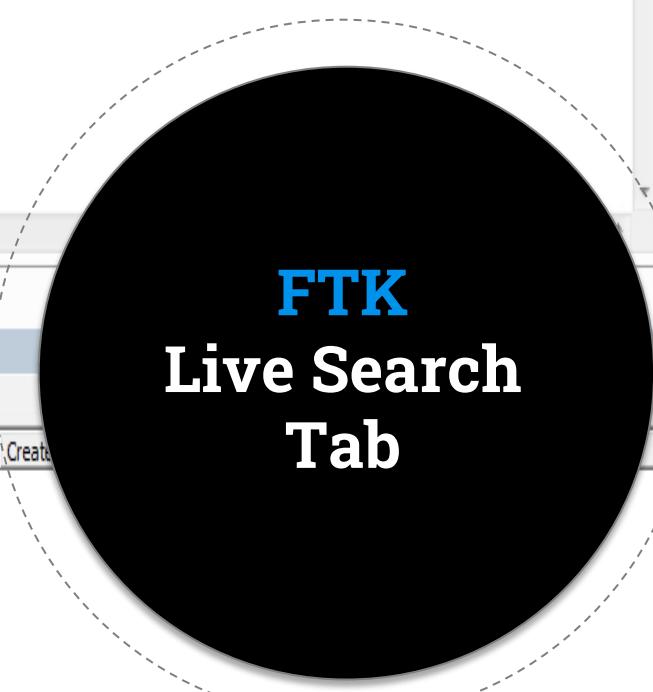
Hex Text Filtered Natural

File Content Properties Hex Interpreter

File List

Display Time Zone: Eastern Daylight Time (From local machine)

Name Label Item # Ext Path Category P-Size L-Size MD5 SHA1 SHA256 Created



FTK  
Live Search  
Tab

File Edit View Evidence Filter Tools Manage Help

Filter: -unfiltered- Filter Manager...

Explore Overview Email Graphics Bookmarks Live Search Index Search Volatile

dtSearch® Index

Terms

Add

Indexed Words Total Hits

Search Criteria

Operators

And

Or

Terms

All

Selected

Accumulate Results

Search Terms

Total Hits

Clear

Import...

Export...

Options...

File Content

Hex Text Filtered Natural

Hit # of

Prev

Next

Go to:

Go

File Content Properties Hex Interpreter

File List

Name Label Item # Ext Path

Category P-Size L-Size MD5 SHA1 SHA256 Create

Normal

Display Time Zone: Eastern Daylight Time (From local machine)

Name  Label  Item #  Ext  Path  Category  P-Size  L-Size  MD5  SHA1  SHA256  Create

Loaded: 0 Filtered: 0

Total: 0

Highlighted: 0

Checked: 1

Total LSize: 0

Ready

Index Search Tab Filter: [None]

FTK  
Index Search  
Tab

File Edit View Evidence Filter Tools Manage Help

Filter: -unfiltered -

Filter Manager...



Explore Overview Email Graphics Bookmarks Live Search Index Search Volatile



## Report Options

- Report Outline
- Case Information
- Bookmarks
- Graphics
- File Paths
- File Properties
- Registry Selections

Import...  
Export...

- Shared
- sbunting
- Significant Image

### Filter

Bookmark: Significant Image

Include email attachments

Export files & include links

Include thumbnail for each object

#### Thumbnail Arrangement

Number of thumbnails per row

Include all thumbnails at end of each bookmark section

Group all file paths at the end of thumbnails

Sort Options...

Apply these settings

# Report Options

Loaded: 0 Filtered: 0 Total: 0 Highlighted: 0 Checked: 1 Total LSize: 0

Ready

Index Search Tab Filter: [None]

**FTK**  
CASE REPORT

- Case Summary
- Case Information
- File Overview
- Evidence List
- Bookmarks
- sbunting
- Significant Image**
- Thumbnails
- Graphics
- Page 1
- File Paths
- File Properties
- Selected Registry Types

6/29/2012

Page 1 of 1

**Bookmark: Significant Image****Comments:****Creator:** sbunting**File Count:** 1**Files****File Comments:**

<b>Thumbnail</b>	1
<b>Name</b>	GB-wp5.jpg
<b>Physical Size</b>	643072 B
<b>Logical Size</b>	639243 B
<b>Created Date</b>	7/14/2009 3:26:29 AM (2009-07-14 07:26:29 UTC)
<b>Modified Date</b>	7/14/2009 3:26:29 AM (2009-07-14 07:26:29 UTC)
<b>Accessed Date</b>	7/14/2009 3:26:29 AM (2009-07-14 07:26:29 UTC)
<b>Path</b>	EnCaseOverview.E01/Partition 2/NONAME [NTFS]/[root]/Windows/Global/
<b>Exported as</b>	<a href="#">files\GB-wp5.jpg</a>



6/29/2012

Page 1 of 1

The  
Report

# Autopsy

Open Source

## Introduction to Autopsy

- ◎ Digital data acquisition tool that:
  - Is also similar to EnCase in overall features
  - Email and file system analysis
  - Advanced searches
  - File type identification
  - Data carving



## Introduction to Autopsy

◎ Step Action, you will work individually to:

- Install Autopsy
- Create new case
- Examine evidence files
- Sort files
- Create bookmarks
- Generate reports





What forensic tool features  
would most benefit my  
investigations?

## Summary

◎ You should now be familiar with using forensic tools to:

- Create a case
- Add and verify evidence
- Adjust time zone offsets
- Process, navigate through, and bookmark evidence
- Create reports from your findings

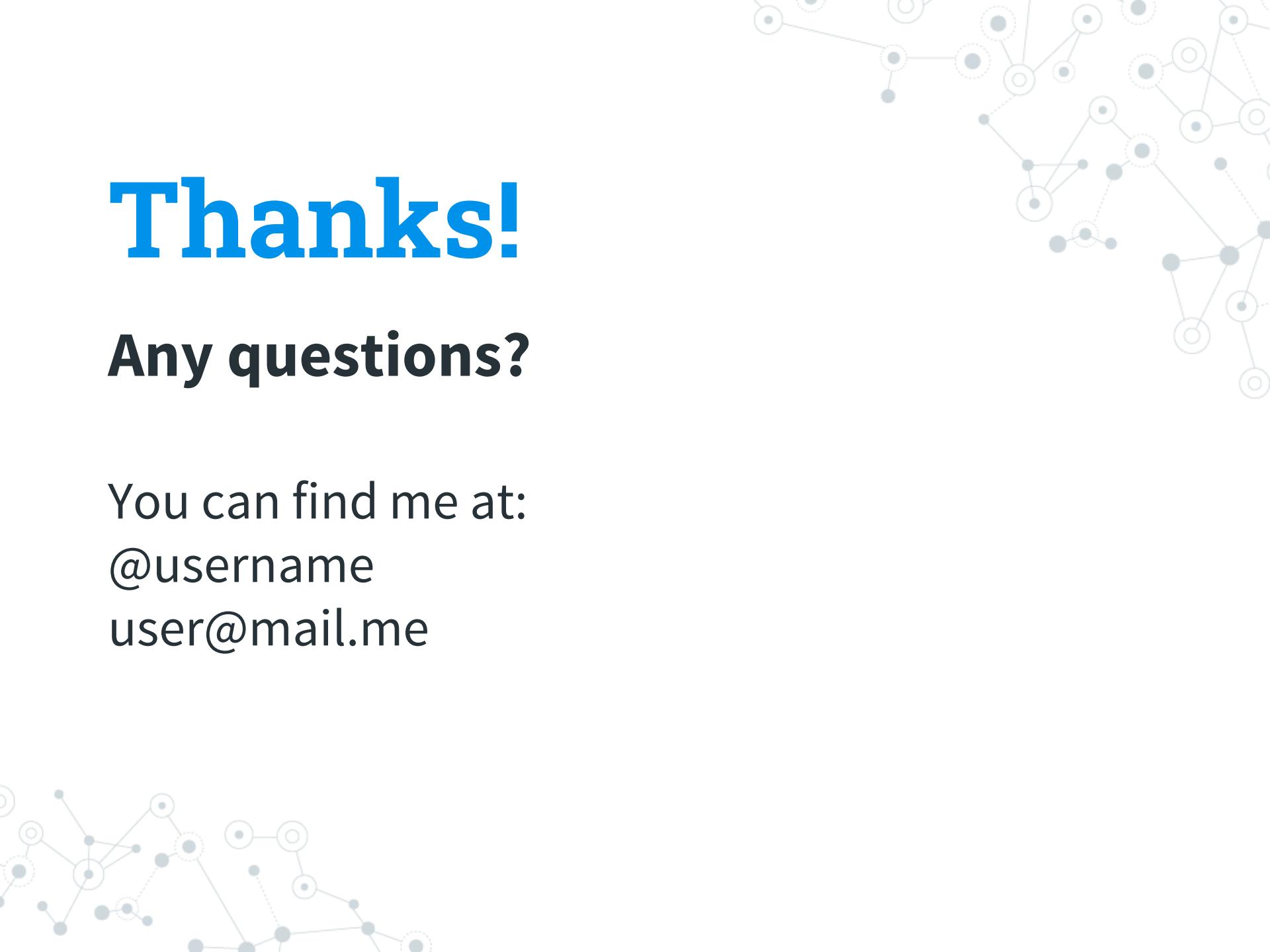
# Thanks!

## Any questions?

You can find me at:

@username

user@mail.me



# Hash Analysis

## Objective

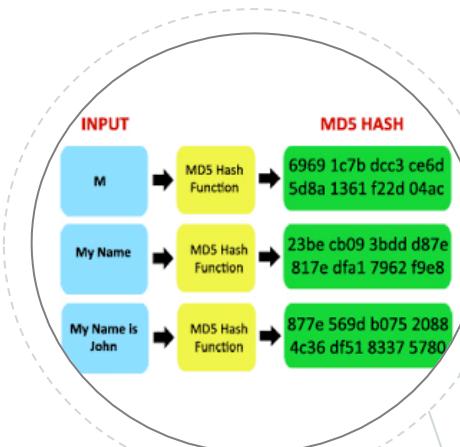
- ◎ By the end of the module, participants will be able to use a hash set to identify known trusted and malicious files



## Hash Definition

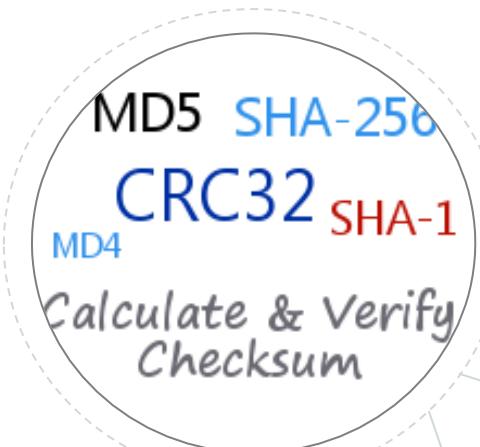
### ◎ Hashes:

- Calculations or algorithms that result in unique value for each file or stream of data to which the calculation is applied



## Hash Algorithm

- ◎ The two key forensics hash algorithms are:
  - **Message Digest 5** (128-bit value)
  - **Secure Hash Algorithm 1** (160-bit value)
- ◎ Two files with the same hash value are statistically likely to contain the same data



# Hash Uses

## Use

Verify evidence file acquisitions

Identify known good files

Identify known bad files

## Process

Compare acquisition and verification hash values

Compare file hashes to libraries of known files

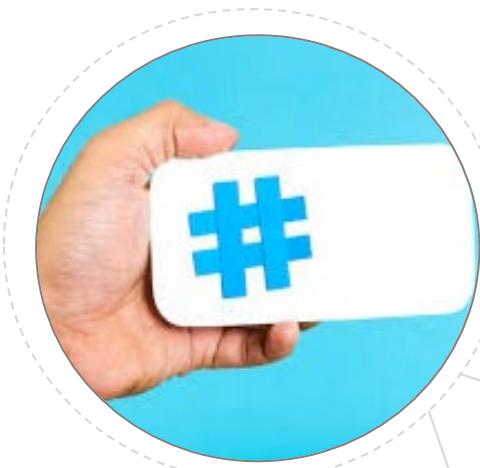
Compare file hashes to tables of known hashes



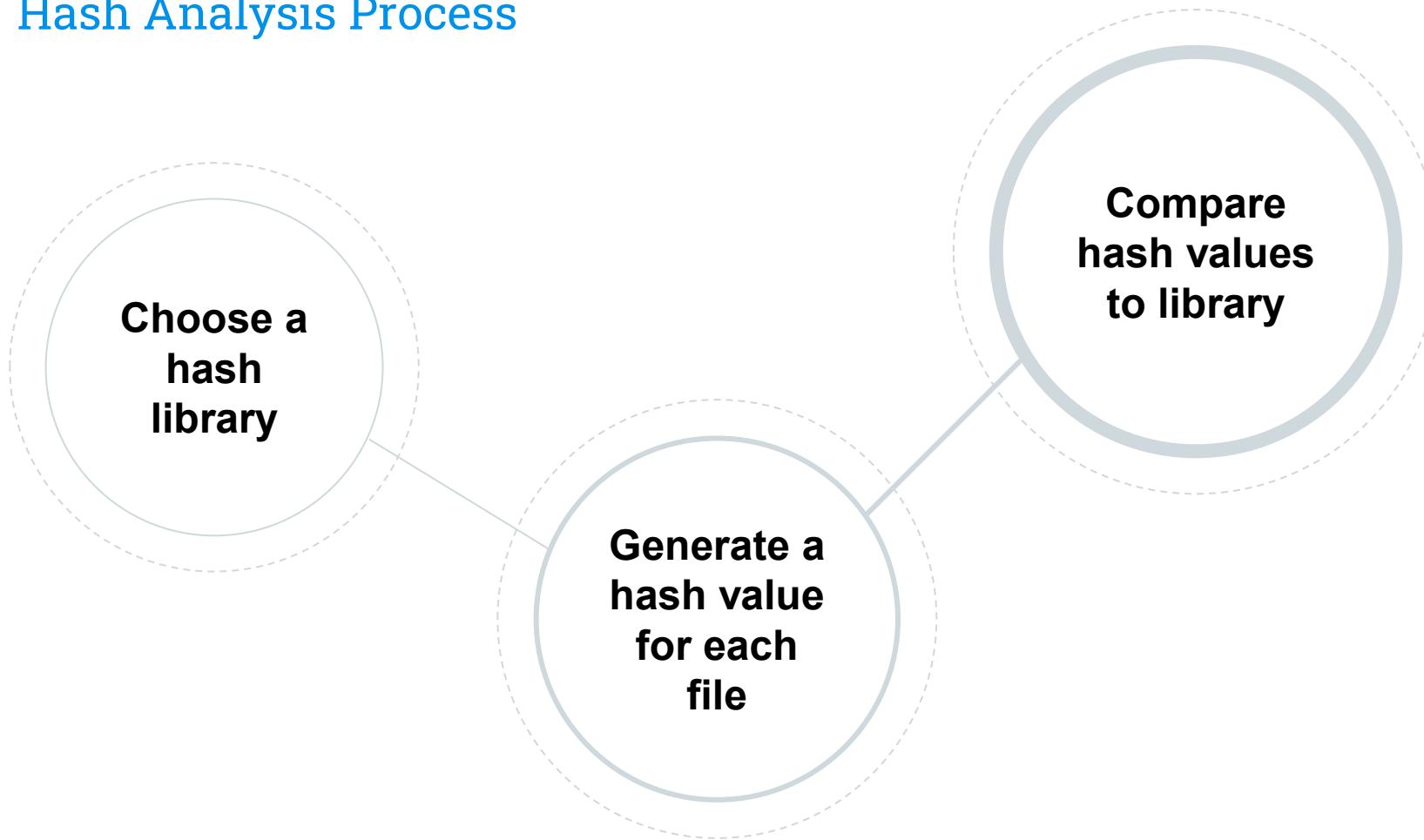
## Hash Sets and Hash Libraries

◎ **Hash Set:** A collection of hash values with similar traits

◎ **Hash Library:** A collection of hash sets



## Hash Analysis Process



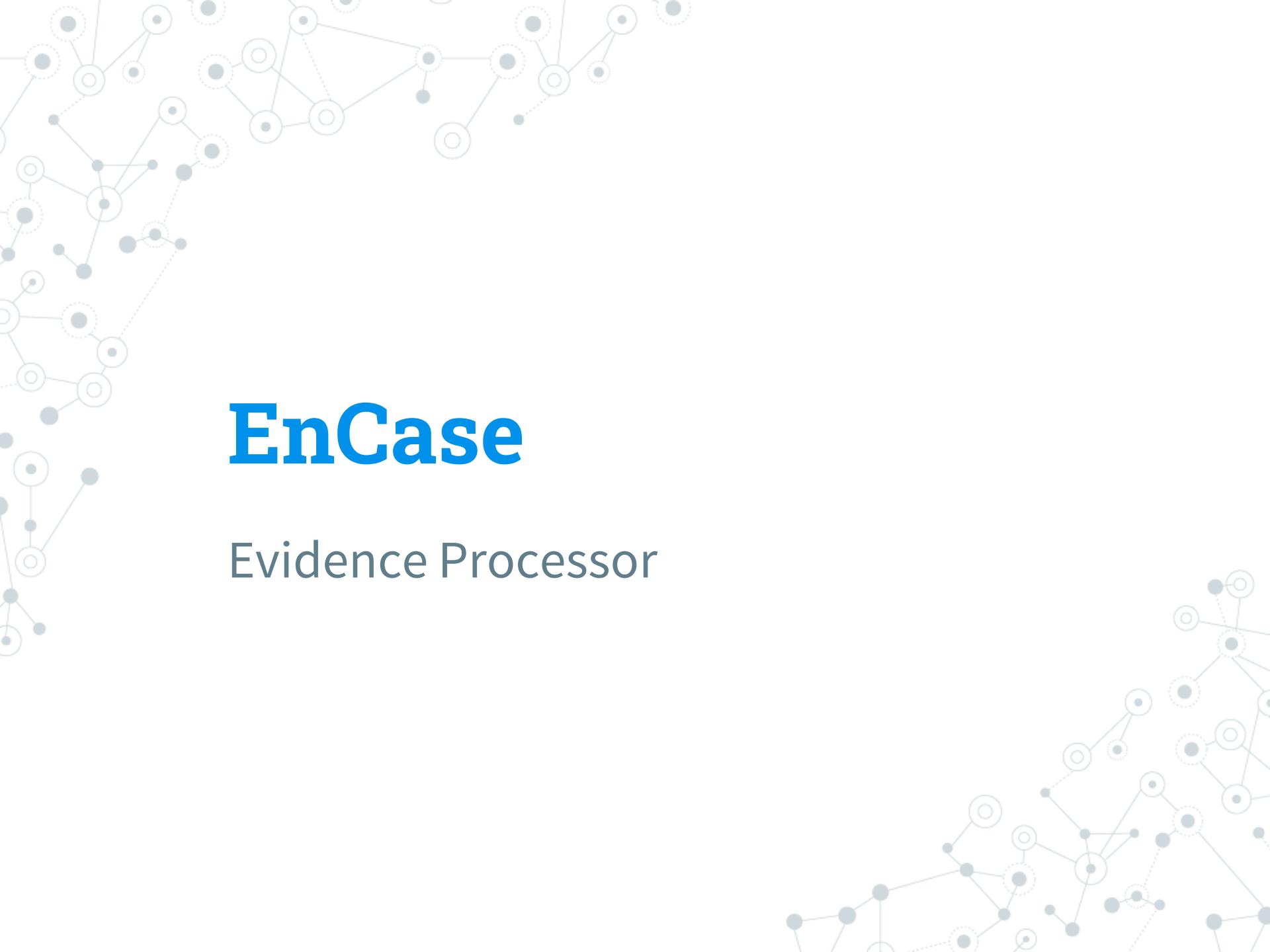
## Sources of Hash Sets

- ◎ Forensic software vendors
- ◎ U.S. National Institutes of Standards and Technology/National Software Reference Library
- ◎ Specialized collections
- ◎ Collections created by examiners/agencies



## Known vs Unknown Files

- ◎ Known files can be good or bad
- ◎ Most files will be unknown
- ◎ A forensic examiner must be capable of creating hash sets for local use



# EnCase

## Evidence Processor

## EnCase Evidence Processor

- ◎ Hashing occurs during evidence processing with EnCase 7
- ◎ EnCase Evidence Processor (EEP) provides hash analysis for files in the selected evidence items

EnCase Forensic

Case (ATACyber) View Tools EnScript Add Evidence

Home Evidence Records Case Info Items

Viewing (Evidence) Split Mode Process Evidence Open Remove Rescan Update Paths

Table Timeline

Selected 0/1

Name Primary Path Evidence Paths

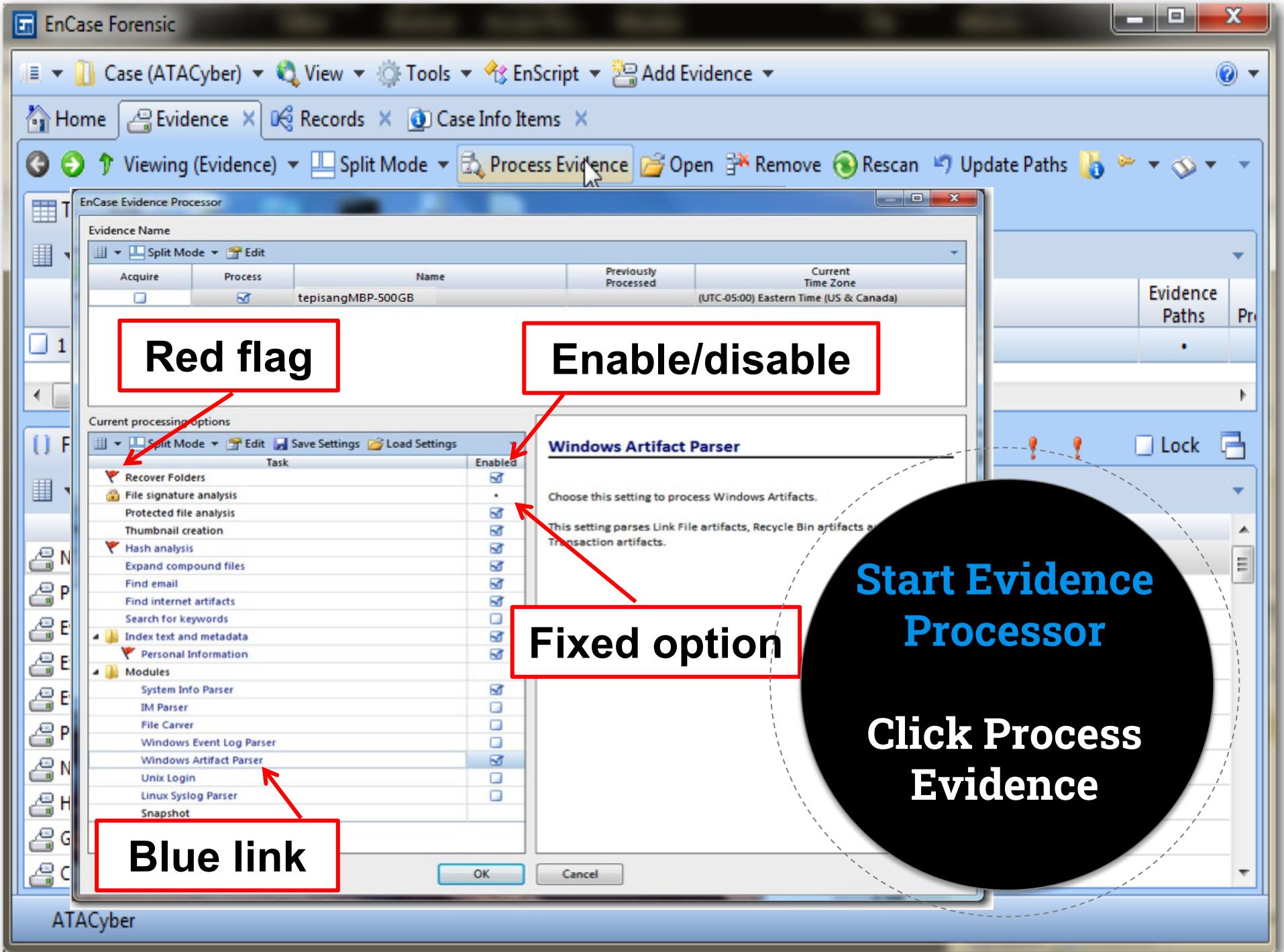
1 tepisangMBP-500GB E:\Cases\ATACyber\Evidence\tepisangMBP-500GB\tepisangMBP-500GB.E01

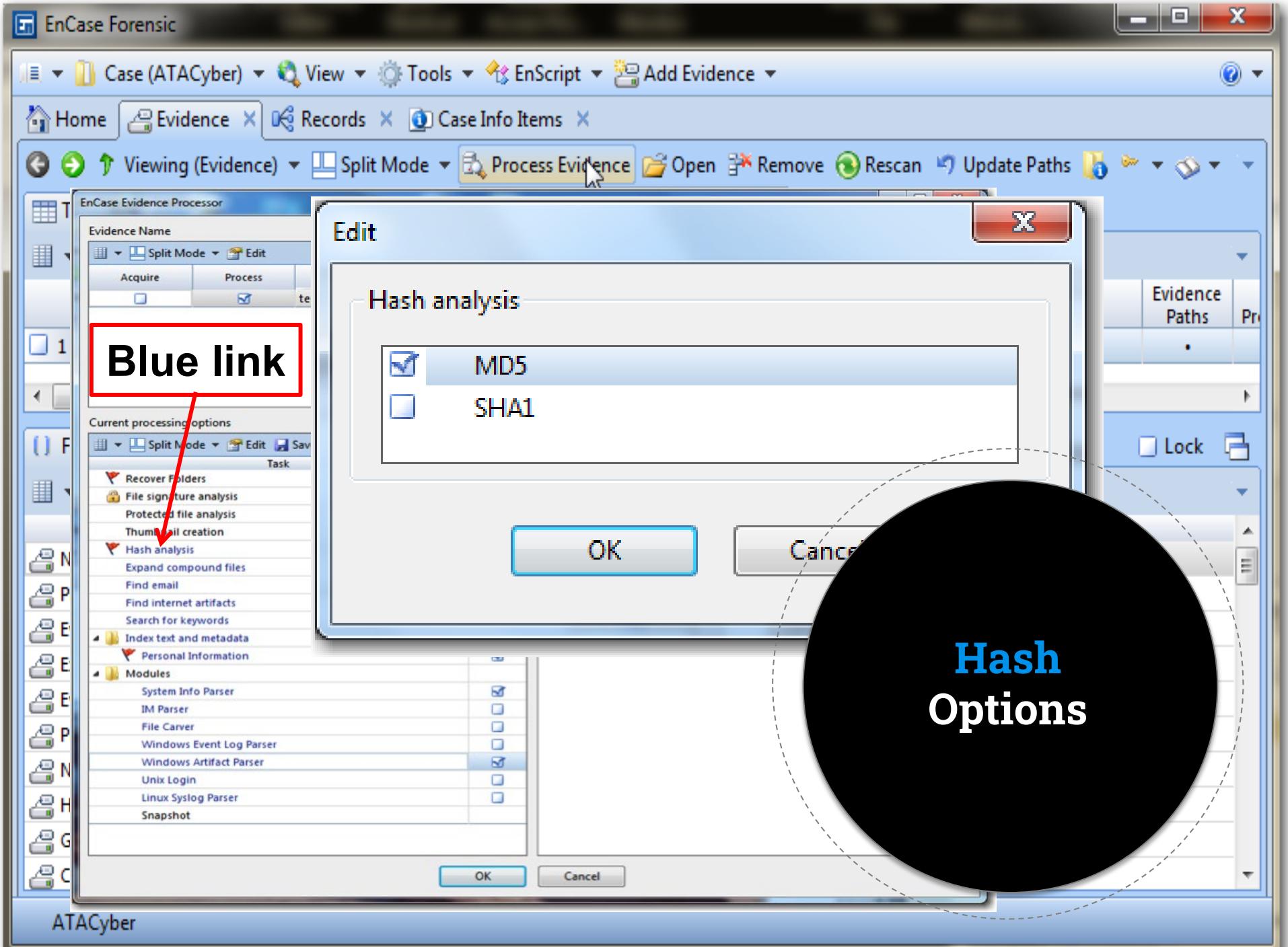
Fields Report Evidence Paths Extra Paths Evidence Processor Logs Lock

Name	Value
Name	tepisangMBP-500GB
Primary Path	E:\Cases\ATACyber\Evidence\tepisangMBP-500GB\tepisangMBP-500GB.E01
Evidence Paths	.
Extra Paths	
Evidence Processor Logs	.
Processing Status	Processed
Not Found	
Has Index	.
GUID	66f1fc3742a04f0dab6b18688b89837f
Credentials	

Start Evidence Processor

Click Process Evidence





EnCase Forensic

Case (ATACyber) View Tools EnScript Add Evidence

Home Reports Evidence Records

Viewing (Entry) Split Mode Condition

Entries ATA\_Cyber\_FilesToHash

Table Timeline Gallery

Selected 2/3

	Name	File Created	Last Accessed	Entry Modified
<input checked="" type="checkbox"/> 1	IMG_0713.mov	08/16/12 05:40:24 AM	08/16/12 02:25:56 PM	08/29/12 10:02:56 AM
<input checked="" type="checkbox"/> 2	thegoods.xlsx		02:25:56 PM	08/29/12 10:02:55 AM

Copy Ctrl-C

Bookmark

Go to file

Find Related

Entries

Acquire

Device

Open With

Copy Files...

Copy Folders...

View File Structure

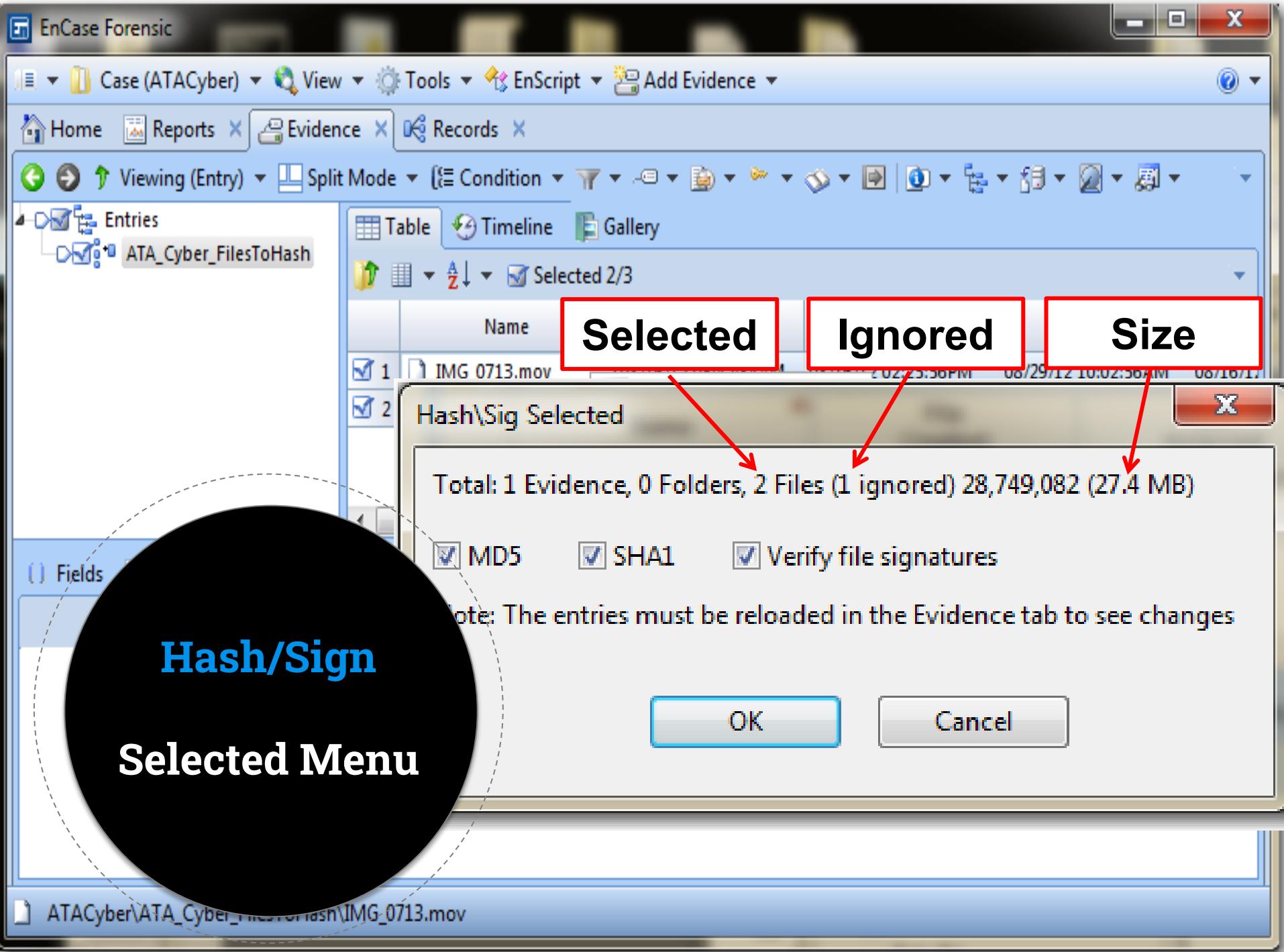
Add to hash library...

Hash\Sig Selected... **Hash\Sig Selected...**

Go To Overwriting File

**Hash Single or Selected Files**

ATACyber\ATA\_Cyber\_FilesToHash\IMG\_0713.mov



EnCase Forensic

Case (ATACyber) View Tools EnScript Add Evidence

Home Reports Evidence Records

Zoom In Zoom Out 100%

BROWSE

Evidence Records

REPORT

Reports Bookmarks Report Templates

CASE

Case Info Items Options Hash Libraries Save Close

Home screen

Evidence in the case  
Processed data, such as email and internet artifacts

Reports created from report templates  
A bookmark  
A template for a report

Information about a case  
Case options and settings  
Change hash libraries settings  
Save this case to disk  
Close this case

Open Hash Libraries



ATACyber\ATA\_Cyber\_FilesToHash\IMG\_0713.mov

EnCase Forensic

Case (ATACyber) View Tools EnScript Add Evidence

Home Reports Evidence Records

Zoom In Zoom Out 100%

BROWSE Evidence Record

REPORT Report Bookmarks Report

CASE Case In Options Hash Library Save Close

Hash Libraries

Hash Library Info

Name Enable Hash library path

Name	Enable	Hash library path
Primary	<input checked="" type="checkbox"/>	C:\Program Files\EnCase7\Hash Libraries\NSRL
Secondary	<input checked="" type="checkbox"/>	C:\Program Files\EnCase7\Hash Libraries\Hash Library #1

Existing hash sets

	Name	Enable	Category	Hash Set Tags
1	CyberScrub Privacy Suite 5.1 with 1 Yr ...	<input checked="" type="checkbox"/>		
2	CyberScrub Privacy Suite 5.1 with 1 Yr ...	<input checked="" type="checkbox"/>		
3	CyberScrub Privacy Suite 5.1 with 1 Yr ...	<input checked="" type="checkbox"/>		
4	CyberScrub Privacy Suite 5.1 with 1 Yr ...	<input checked="" type="checkbox"/>		
5	AntiVirus for Handhelds	<input checked="" type="checkbox"/>		
6	AntiVirus for Handhelds	<input checked="" type="checkbox"/>		
7	AntiVirus for Handhelds	<input checked="" type="checkbox"/>		
8	AntiVirus for Handhelds	<input checked="" type="checkbox"/>		
9	DVD Copy 6	<input checked="" type="checkbox"/>		
10	DVD Copy 6	<input checked="" type="checkbox"/>		
11	DVD Copy 6	<input checked="" type="checkbox"/>		
12	DVD Copy 6	<input checked="" type="checkbox"/>		
13	Reader Rabbit Personalized Math Age...	<input checked="" type="checkbox"/>		
14	Reader Rabbit Personalized Math Age...	<input checked="" type="checkbox"/>		
15	Reader Rabbit Personalized Math Age...	<input checked="" type="checkbox"/>		
16	Reader Rabbit Personalized Math Age...	<input checked="" type="checkbox"/>		
17	Reader Rabbits Math 1	<input checked="" type="checkbox"/>		
18	Reader Rabbits Math 1	<input checked="" type="checkbox"/>		
19	Reader Rabbits Math 1	<input checked="" type="checkbox"/>		
20	Reader Rabbits Math 1	<input checked="" type="checkbox"/>		
21	SupportNotes	<input checked="" type="checkbox"/>		
22	SupportNotes	<input checked="" type="checkbox"/>		

Help

Hash library name  
Primary

Hash library path  
C:\Program Files\EnCase7\Hash Libraries\NSRL

Primary Library Enabled

ATACyber\ATA\_Cyber\_FilesToHash\IMG\_0713.mov

EnCase Forensic

Case (ATACyber) View Tools EnScript Add Evidence

Home Reports Evidence Records

Zoom In Zoom Out 100%

BROWSE

Evidence Record

REPORT

Report Bookmarks Report

CASE

Case In Options Hash Library Save Close

Hash Libraries

Hash Library Info

Name Enable Hash library path

Primary	<input checked="" type="checkbox"/>	C:\Program Files\EnCase7\Hash Libraries\NSRL
Secondary	<input checked="" type="checkbox"/>	C:\Program Files\EnCase7\Hash Libraries\Hash Library #1

Existing hash sets

	Name	Enable	Category	Hash Set Tags
608	CP ZZFB1_KP	<input checked="" type="checkbox"/>	Notable	
609	Adult Porn MAB0002	<input checked="" type="checkbox"/>	Notable	Adult Porn Violates AUP
610	SCP Child Abuse Images 32HQ R v Tat...	<input checked="" type="checkbox"/>	Notable	Child Porn
611	CP HTCU 168	<input checked="" type="checkbox"/>	Notable	Child Porn
612	CP HTCU 175	<input checked="" type="checkbox"/>	Notable	Child Porn
613	CP HTCU 177	<input checked="" type="checkbox"/>	Notable	Child Porn
614	CP HTCU 195	<input checked="" type="checkbox"/>	Notable	Child Porn
615	CP HTCU 201	<input checked="" type="checkbox"/>	Notable	Child Porn
616	CP HTCU 211	<input checked="" type="checkbox"/>	Notable	Child Porn
617	CP HTCU 215	<input checked="" type="checkbox"/>	Notable	Child Porn
618	CP HTCU 229	<input checked="" type="checkbox"/>	Notable	Child Porn
619	CP HTCU 253	<input checked="" type="checkbox"/>	Notable	Child Porn
620	CP HTCU 264	<input checked="" type="checkbox"/>	Notable	Child Porn
621	CP HTCU 280	<input checked="" type="checkbox"/>	Notable	Child Porn
622	CP HTCU 61	<input checked="" type="checkbox"/>	Notable	Child Porn
623	CP ZZ known Child Porn	<input checked="" type="checkbox"/>	Notable	Child Porn
624	CP ZZ00002 Identified Child Porn	<input checked="" type="checkbox"/>	Notable	Child Porn
625	CP ZZ00009 Known Child Pornography	<input checked="" type="checkbox"/>	Notable	Child Porn
626	Sarah Phishing Email	<input checked="" type="checkbox"/>	Notable	Malware
627	PWDump	<input checked="" type="checkbox"/>	Notable	Security Hacking
628	Ziata!Shareware	<input checked="" type="checkbox"/>	Notable	Security Hacking
629	Ziata!	<input checked="" type="checkbox"/>	Notable	Security Hacking

Help

Hash library name Secondary  
Hash library path C:\Program Files\EnCase7\Hash Libraries\Hash Library #1

Secondary Library Enabled

ATACyber\ATA\_Cyber\_FilesToHash\IMG\_0713.mov

EnCase Forensic

Case (ATACyber) View Tools EnScript Add Evidence

Home Reports Evidence Records

Viewing (Entry) Split Mode Condition

Entries ATA\_Cyber\_FilesToHash

Table Timeline Gallery

Selected 2/3

Name Hash Sets MD5 File Type

IMG\_0713.mov 10750aae3013e6e7dafc3d8bb26f31fbe

thegoods.xlsx b4f1cc5e25f9c195b

Copy Ctrl-C

Bookmark

Go to file

Find Related

Entries

Acquire

Device

Open With

Copy Files...

Copy Folders...

View File Structure

Add to hash library... **Hash\Sig Selected...**

Go To Overwriting File

Fields Decode

Creating Hash Sets From the Selected Files

ATACyber\ATA\_Cyber\_FilesToHash\IMG\_0713.mov

Case Backup

The screenshot shows the EnCase Forensic interface. A red box highlights the 'Entries' node under the 'ATA\_Cyber\_FilesToHash' folder in the left pane. A red arrow points from this box to the text 'Blue check'. In the center, a table lists two selected files: 'IMG\_0713.mov' and 'thegoods.xlsx'. A context menu is open over the second file, with 'Entries' selected. A secondary context menu is open under 'Entries', with 'Add to hash library...' highlighted and a cursor over it. A large black circle with a dashed border covers the bottom-left portion of the interface, containing the text 'Creating Hash Sets From the Selected Files'.

EnCase Forensic

Case (ATACyber) View Tools EnScript Add Evidence

Home Reports Evidence Records

Viewing (Entry) Split Mode Condition

Entries ATA\_Cyber\_FilesToHash

**Hash Library Type**

Selecting Secondary Library for New Hash Set

Add to hash library

Hash library type: Primary, Secondary, Other

Hash library path: C:\Program Files\EnCase7\Hash Libraries\NSRL

Name	Category	Hash Set Tags	Count
1 Canvas			10,938
2 Gallery			200,229
3 Decimals Made Easy			122
4 Microsoft Office XP Small Business			8,485
5 Microsoft Office XP			6,972
6 Microsoft Office XP			6,362
7 Microsoft Licensing			9,555
8 Office XP			7,828
9 Publisher Deluxe with Photo Editing			13,533
10 Office XP - for Students and Teachers			8,585
11 Office XP			10,964
12 Office XP 2002			6,356
Office XP			9,904
Office XP Small Business			8,458
Applications Microsoft Office Family			8,855
Linux Developers Resource			8,321
Linux Developer's Resource			26,191
Lotus1-2-3 for Unix			197
300,000 Corel Gallery			352,512
Delphi Studio Companion Tools			2,390

Default Fields: Name, Logical Size, MD5, SHA1

Fields:

- File Ext
- Item Type
- Category
- Signature Analysis
- Signature Tag
- Protected
- Last Accessed
- File Created
- Last Written
- Code Page
- Item Path
- Description
- Entry Modified
- File Deleted
- GUID

OK Cancel

ATACyber\ATA\_Cyber\_FilesToHash\IMG\_0713.mov Case Backup

EnCase Forensic

Case (ATACyber) View Tools EnScript Add Evidence

Home Reports Evidence Records

Viewing (Entry) Split Mode Condition

Entries ATA\_Cyber\_FilesToHash

Table Timeline Gallery

Add to hash library

Hash library type: Secondary Hash library path: C:\Program Files\EnCase7\Hash Libraries\Hash Library #1

Existing hash sets:

	Name	Hash Set Tags
1	-eXML	Notable Security Hacking
2	1-800- translation Directory	Notable Security Hacking
3	A Bluebox dialer	Notable Security Hacking
4	A NAP-PA file	Notable Security Hacking
5	A Unix tutorial	Notable Security Hacking
6	A4Proxy Management software	Notable Security Hacking
7	Adult Porn MAB0002	Notable Adult Porn Violates AUP
8	AerialReconPhotosFromTerrGroupMe...	Notable Security Hacking

**Create New Hash Set**

**Right click, New Hash Set**

ATACyber\ATA\_Cyber\_FilesToHash\IMG\_0713.mov Case Backup

EnCase Forensic

Case (ATACyber) View Tools EnScript Add Evidence

Home Reports Evidence Records

Viewing (Entry) Split Mode Condition

Entries ATA\_Cyber\_FilesToHash

Table Timeline Gallery

Selected 2/3

Create Hash Set

Hash library path  
C:\Program Files\EnCase7\Hash Libraries\Hash Library #1

Existing hash sets

	Name	Category	Hash Set Tags	Count
1	-eXML	Notable	Security Hacking	15
2	1-800- translation Directory	Notable	Security Hacking	2
3	A Bluebox dialer and wardialer	Notable	Security Hacking	11
4	A NAP-PA file about VAX-VMS machines	Notable	Security Hacking	2
5	A Unix tutorial	Notable	Security Hacking	
6	A4Proxy Management Software	Notable	Security Hacking	
7	Adult Porn MAB0002	Notable	Adult Porn Violates AUP	
8	AerialReconPhotosFromTerrGroupMember	Notable	Security Hacking	

Hash Set Name  
ATACyberNatashaFiles

Hash Set Category  
Notable

Hash Set Tags  
ATACyber

OK Cancel

File Type

d8bb26f31fbe

c5e25f9c195b

Create New Hash Set

ATACyber\ATA\_Cyber\_FilesToHash\IMG\_0713.mov

Case Backup

EnCase Forensic

Case (ATACyber) View Tools EnScript Add Evidence

Home Reports Evidence Records

Viewing (Entry) Split Mode Condition

Entries ATA\_Cyber\_FilesToHash

Add to hash library

Hash library type Secondary Hash library path C:\Program Files\EnCase7\Hash Libraries\Hash Library #1

Existing hash sets

	Name	Category	Hash Set Tags	Count
687	ZZ Child Porn FBI_KP	Notable		3,622
688	ZZ known Child Porn	Notable		6
689	ZZ Operation Ore -Landslide	Notable		5,738
690	ZZ Suspect Child Porn -Case 228	Notable		194
691	ZZ00000, suspected child porn	Notable		28
692	ZZ00001 Suspected child porn	Notable		6,038
693	ZZ00002 Identified Child Porn	Notable		12
694	ZZ00003 Suspected child porn	Notable		1,052
695	ZZ00004 Identified Child Porn	Notable		81
696	ZZ00005 Suspected Child Porn	Notable		147
697	ZZ00006 Suspected Child Porn	Notable		3,430
698	ZZ00007a Suspected KP Movies	Notable		107
699	ZZ00007b Suspected KP (US Federal)	Notable		375
700	ZZ00007c Suspected KP (Alabama 13A...)	Notable		3,685
701	ZZ00008 Suspected Child Pornography...	Notable		6,696
702	ZZ00009 Known Child Pornography	Notable		44
703	Sarah Phishing Email	Malware	ATACyber	20
704	ATACyberNatashaFiles	Notable	ATACyber	0

Select the New Set

OK Cancel

MD5

File Type
afc3d8bb26f31fbe
4f1cc5e25f9c195b

Check the Newly Created Hash Set to Add Hashes

ATACyber\ATA\_Cyber\_FilesToHash\IMG\_0713.mov

Case Backup

EnCase Forensic

Case (ATACyber) View Tools EnScript Add Evidence

Home Reports Evidence Records

Zoom In Zoom Out 100%

BROWSE Evidence Record

REPORT Report Bookmarks Report

CASE Case Options Hash Library Save Close

Hash Libraries

Hash Library Info

Split Mode Edit Change hash library Manage hash library

Name	Enable	Hash library path
Primary	<input type="checkbox"/>	
Secondary	<input checked="" type="checkbox"/>	C:\Program Files\EnCase7\Hash Libraries\Hash Library #1

Existing hash sets

Name	Enable	Category	Hash Set Tags
685 Suspected Child Porn (DE UDPD Towe...	<input checked="" type="checkbox"/>	Notable	
686 Suspected Child Porn1 (AL 13A-12-192)	<input checked="" type="checkbox"/>	Notable	
687 ZZ Child Porn FBI_KP	<input checked="" type="checkbox"/>	Notable	
688 ZZ known Child Porn	<input checked="" type="checkbox"/>	Notable	
689 ZZ Operation Ore -Landslide	<input checked="" type="checkbox"/>	Notable	
690 ZZ Suspect Child Porn -Case 228	<input checked="" type="checkbox"/>	Notable	
691 ZZ00000, suspected child porn	<input checked="" type="checkbox"/>	Notable	
692 ZZ00001 Suspected child porn	<input checked="" type="checkbox"/>	Notable	
693 ZZ00002 Identified Child Porn	<input checked="" type="checkbox"/>	Notable	
694 ZZ00003 Suspected child porn	<input checked="" type="checkbox"/>	Notable	
695 ZZ00004 Identified Child Porn	<input checked="" type="checkbox"/>	Notable	
696 ZZ00005 Suspected Child Porn	<input checked="" type="checkbox"/>	Notable	
697 ZZ00006 Suspected Child Porn	<input checked="" type="checkbox"/>	Notable	
698 ZZ00007a Suspected KP Movies	<input checked="" type="checkbox"/>	Notable	
699 ZZ00007b Suspected KP (US Federal)	<input checked="" type="checkbox"/>	Notable	
700 ZZ00007c Suspected KP (Alabama 13A...	<input checked="" type="checkbox"/>	Notable	
701 ZZ00008 Suspected Child Pornograph...	<input checked="" type="checkbox"/>	Notable	
702 ZZ00009 Known Child Pornography	<input checked="" type="checkbox"/>	Notable	
703 Sarah Phishing Email	<input checked="" type="checkbox"/>	Notable	Malware
704 ATACyberNatashaFiles	<input checked="" type="checkbox"/>	Notable	ATACyber

Help

Hash library name: Secondary  
Hash library path: C:\Program Files\EnCase7\Hash Libraries\Hash Library #1

Select the Newly Created Hash Set To Enable in Hash Library

OK Cancel

ATACyber\ATA\_Cyber\_FilesToHash\IMG\_0713.mov

EnCase Forensic

Case (ATACyber) View Tools EnScript Add Evidence

Home Reports Evidence Records

Viewing (Entry) Split Mode Condition Filter Tags

Entries ATA\_Cyber\_FilesToHash

Table Timeline Gallery

Selected 2/3

	Name	Hash Sets	MD5	File Type
1	IMG_0713.mov	.	10750ae3013e6e7dafc3d8bb26f31fbe	
2	thegoods.xlsx	.	098945a3eb398e4b4f1cc5e25f9c195b	

Boolean indicator

Fields Report Text Hex Decode Doc Transcript Picture

Selected 0/1 Split Mode Browse Data

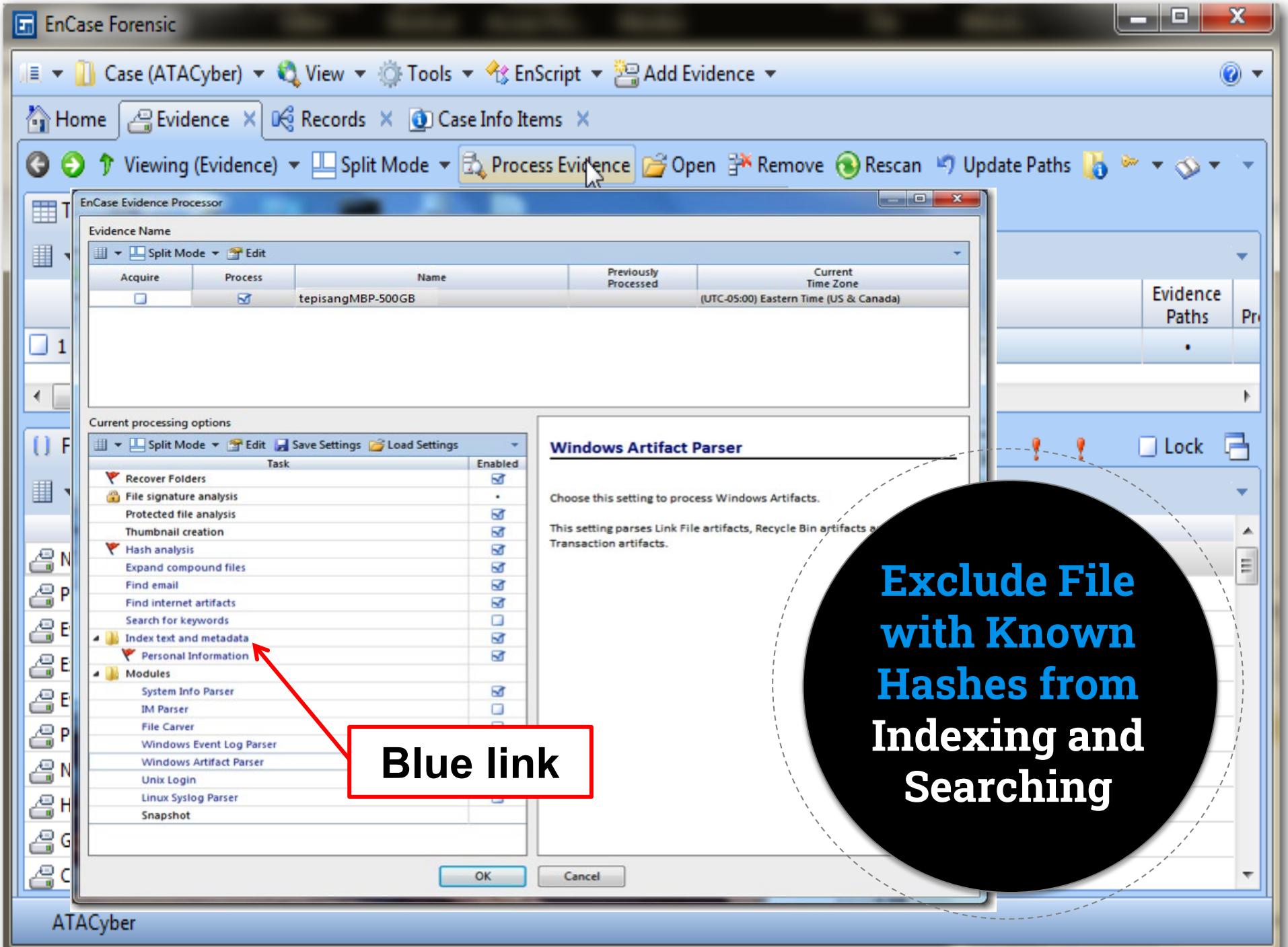
	Name	Category	Hash Set Tags	Hash Items	
1	ATACyberNatashaFiles	Notable	ATACyber	.	C:\Program\file...

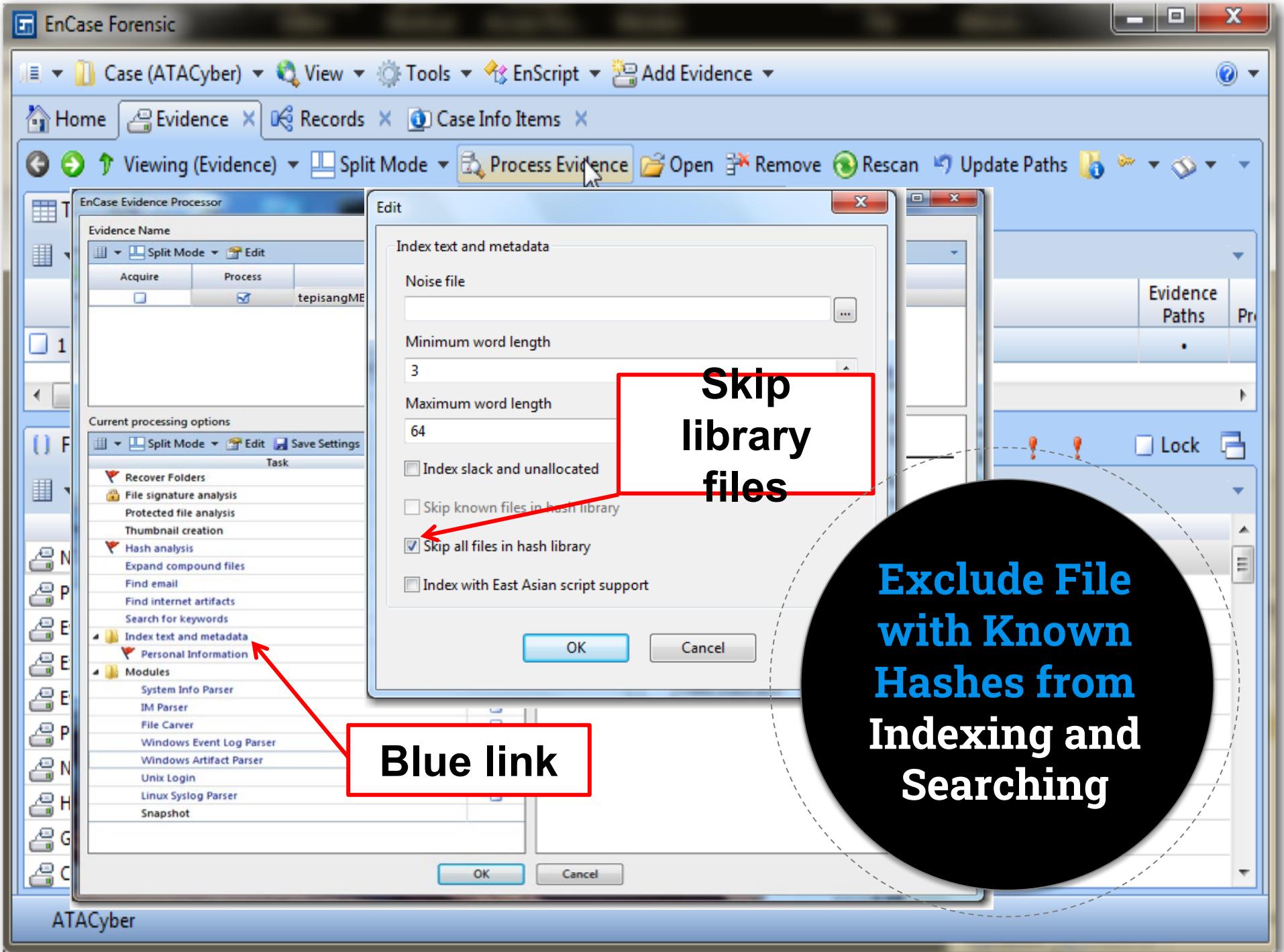
ATACyber\ATA\_Cyber\_FilesToHash\IMG\_0713.mov

Hash Sets Created and Visible

## Using Hash Sets

- ◎ Exclude files with known hashes from indexing and searching to save time
- ◎ Locate files within hash categories using filters or conditions





Case (ATACyber) View Tools EnScript Add Evidence

Home Reports Evidence Records

Viewing (Entry) Split Mode Condition Filter Tags Review Package Raw Se

**Entries**

- tepisangMBP-500GB
  - C
    - EFI
  - 1 Macintosh HD
    - Macintosh HD
  - D
    - DE

**Filter by Hash Category**

Table

1 tepis

Filter menu

Filter1  
FileName  
Find Entries by Date and Size  
**Find Entries by Hash Category**  
Find Entries by Signature  
Find Files based on Category or Extension  
Archives from Entries  
Documents from Entries  
Multimedia from Entries  
Pictures from Entries  
Protected Files from Entries

---

Run...

---

New Filter...  
Edit...

## FTK Hash Analysis Features

- ◎ FTK uses the term Known File Filter (KFF)
- ◎ Hashing occurs during pre-processing
- ◎ Results can be seen using KFF filter feature

FTK AccessData Forensic Toolkit Version: 4.0.2.33 Database: localhost Case: Hashing

File Edit View Evidence Filter Tools Manage Help

Filter: - unfiltered - Filter Manager...

Refinement Options

**Evidence Processing**

Generate File Hashes (flag duplicates)

MD5 Hash  Flag Duplicate Files  
 SHA-1 Hash  KFF  
 SHA-256 Hash  
 Fuzzy Hash  Match Fuzzy Hash Library  
  
 Expand Compound Files  Expansion Options...  
Takes extra time to expand files like email boxes, zips and OLE documents.

File Signature Analysis  
 Flag Bad Extensions  
 Entropy Test  
 dtSearch® Text Index  
 Create Thumbnails for Graphics  
 HTML File Listing  
 Data Carve  
 Meta Carve  
 Optical Character Recognition  
 Explicit Image Detection  
 Registry Reports  
 Include Deleted Files  
 Cerberus Analysis  
 Send Email Alert on Job Completion  
 Decrypt Credant Files

CSV File Listing  Carving Options...  
 OCR Options...  EID Options...  
C:\Program Files\AccessData\RSR Templates ...  
  
 Cerberus Options...  
 Credant Server Settings...  
  
Reset

OK Cancel

DellLaptop\JohnyUser.E01/Partition 2/NONAME [NTFS]/[root]/Windows/winsxs/amd64\_microsoft-windows-m..factory-safehandler\_31bf385ba0304e35\_6.1.7600.1.../handsafe.reg

Ready Overview Tab Filter: [None]

FTK Evidence Processing Options

FTK AccessData Forensic Toolkit Version: 4.0.2.33 Database: localhost Case: Hashing

File Edit View Evidence Filter Tools Manage Help

Filter: - unfiltered - Filter Manager... |

Explore Overview Email Graphics Bookmarks Live Search Index Search Volatile

KFF Admin

Defined Groups

Name	Status
<input checked="" type="checkbox"/> AD_Alert	Alert
<input checked="" type="checkbox"/> AD_Ignore	Ignore

New Edit Delete

Defined Sets

Name	Status	Source V
CyberScrub Privacy Suite 5.1 wi...	Alert	National
AntiVirus for Handhelds 6534	Ignore	National
DVD Copy 6.9540	Ignore	National
(AOL) 1099 Hours Free for 50 Da...	Ignore	National
(AOL) 1175 Hours Free! for 50 Da...	Ignore	National
...for Always IN-2000 Adapter 5428	Ignore	National
.eXML 18	Ignore	National
.mac Internet Essentials from App		National
.NET Framework 2784		National
.NET Framework 3,515		National
.NET Framework 4,148		National
.NET Framework Rem		National
.NET Framework S		National
.NET Framework S		National
.NET Framework		National

FTK Known File Filter (KFF) Administration Menu

Loaded: 84 Filtered: 84 Total: 84 Highlighted: 1 Checked: 0 Total LSize: 32.68 MB

DellLaptopJohnyUser.E01/Partition 2/NONAME [NTFS]/[root]/Windows/winsxs/amd64\_microsoft-windows-m..factory-safehandler\_31bf385ba0304e35\_6.1.7600.1.../handsafe.reg

Ready Overview Tab Filter: [None]

File Edit View Evidence Filter Tools Manage Help

Filter: - unfiltered - Filter Manager...  

Explore Overview Email Graphics Bookmarks Live Search Index Search Volatile



Case Overview

-  Encrypted Files ( 109 / 109 )
-  Flagged Ignore ( 0 / 0 )
-  Flagged Privileged ( 0 / 0 )
-  From Recycle Bin ( 224 / 224 )
-  KFF Alert Files ( 84 / 84 )
-  KFF Ignorable ( 0 / 0 )
-  OCR Graphics ( 0 / 0 )
-  OLE Subitems ( 0 / 0 )

File Content

Hex Text Filtered Natural

REGEDIT4

[HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\DataFactory]

[HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\DataFactory\HandlerInfo1]

File List



<input checked="" type="checkbox"/>	Name	Label	Item #	Type	Owner	Category	P-Size
<input type="checkbox"/>	handsafe.reg		4730	reg	DellLaptopJohnyUser.E...	Text	588 B
<input type="checkbox"/>	handler.reg		101166	reg	DellLaptopJohnyUser.E...	Text	518 B
<input checked="" type="checkbox"/>	handsafe.reg		101477	reg	DellLaptopJohnyUser.E...	Text	588 B
<input type="checkbox"/>	handler.reg		152756	reg	DellLaptopJohnyUser.E...	Text	518 B
<input type="checkbox"/>	handsafe.reg		154042	reg	DellLaptopJohnyUser.E...	Text	518 B
<input type="checkbox"/>	AcroSign.prc		4322	prc	DellLaptopJohnyUser.E...	Unknown	1 B
<input type="checkbox"/>	AdobePiStd.otf		4429	otf	DellLaptopJohnyUser.E...	Unknown	88 B
<input type="checkbox"/>	SY_____.pfm		4443	pfm	DellLaptopJohnyUser.E...	Unknown	672 B
<input type="checkbox"/>	zx_____.pfm		4444	pfm	DellLaptopJohnyUser.E...	Unknown	683 B
<input type="checkbox"/>	zv_____.nfm		4445	nfm	DellLaptopJohnyUser.E...	Unknown	684 B

View results



FTK Known  
File Filter  
(KFF)  
Alert Files

Loaded: 84

Filtered: 84

Total: 84

Highlighted: 1

Checked: 0

Total LSize: 32.68 MB

DellLaptopJohnyUser.E01/Partition 2/NONAME [NTFS]/[root]/Windows/winsxs/amd64\_microsoft-windows-m..factory-safehandler\_31bf385ba0304e35\_6.1.7600.1.../handsafe.reg

Ready

Overview Tab Filter: [None]

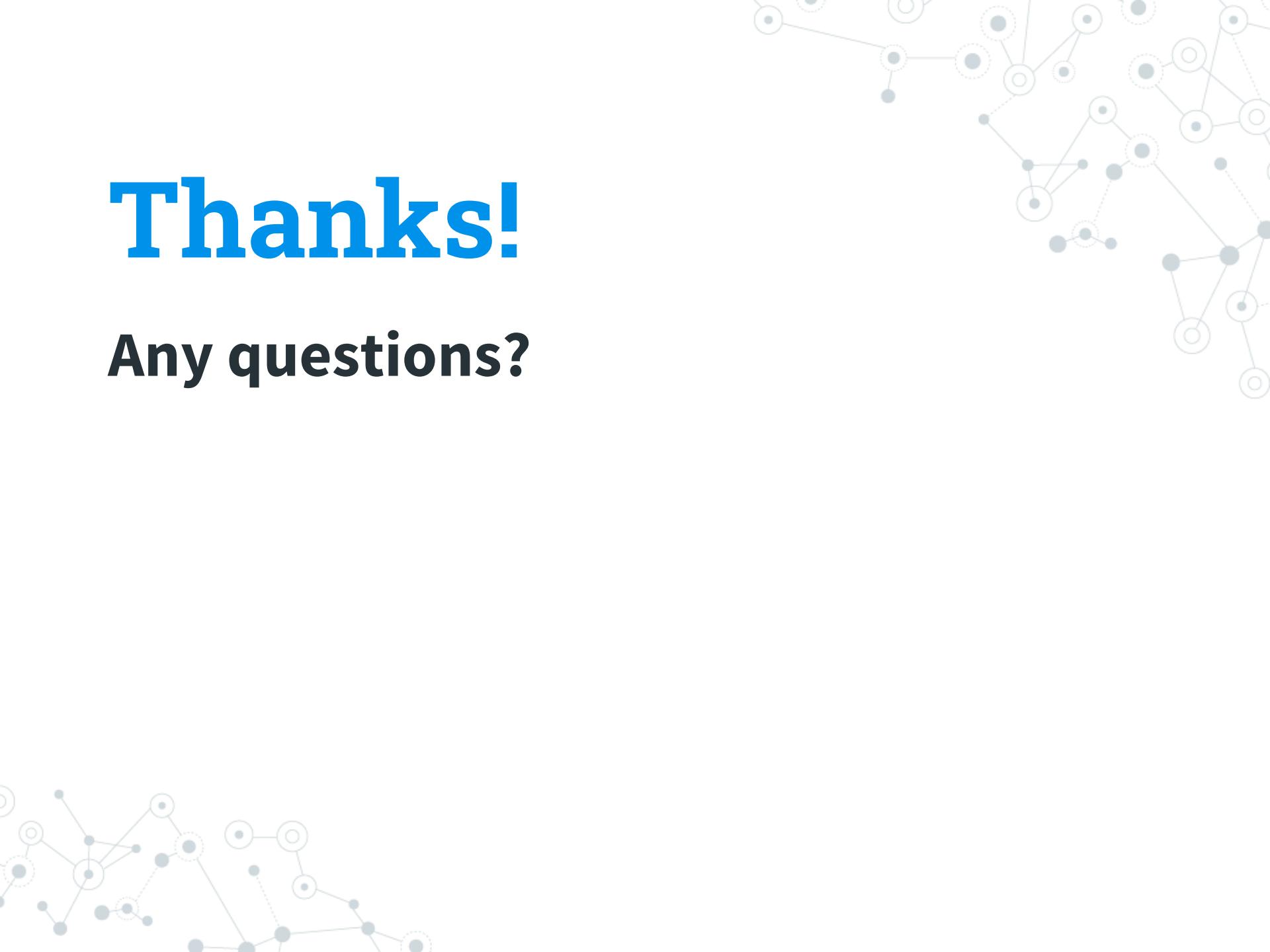
## Summary

◎ You should now be familiar with:

- Identifying available sources of hash sets
- Creating hash sets
- Identifying known files using hash sets

# Thanks!

Any questions?

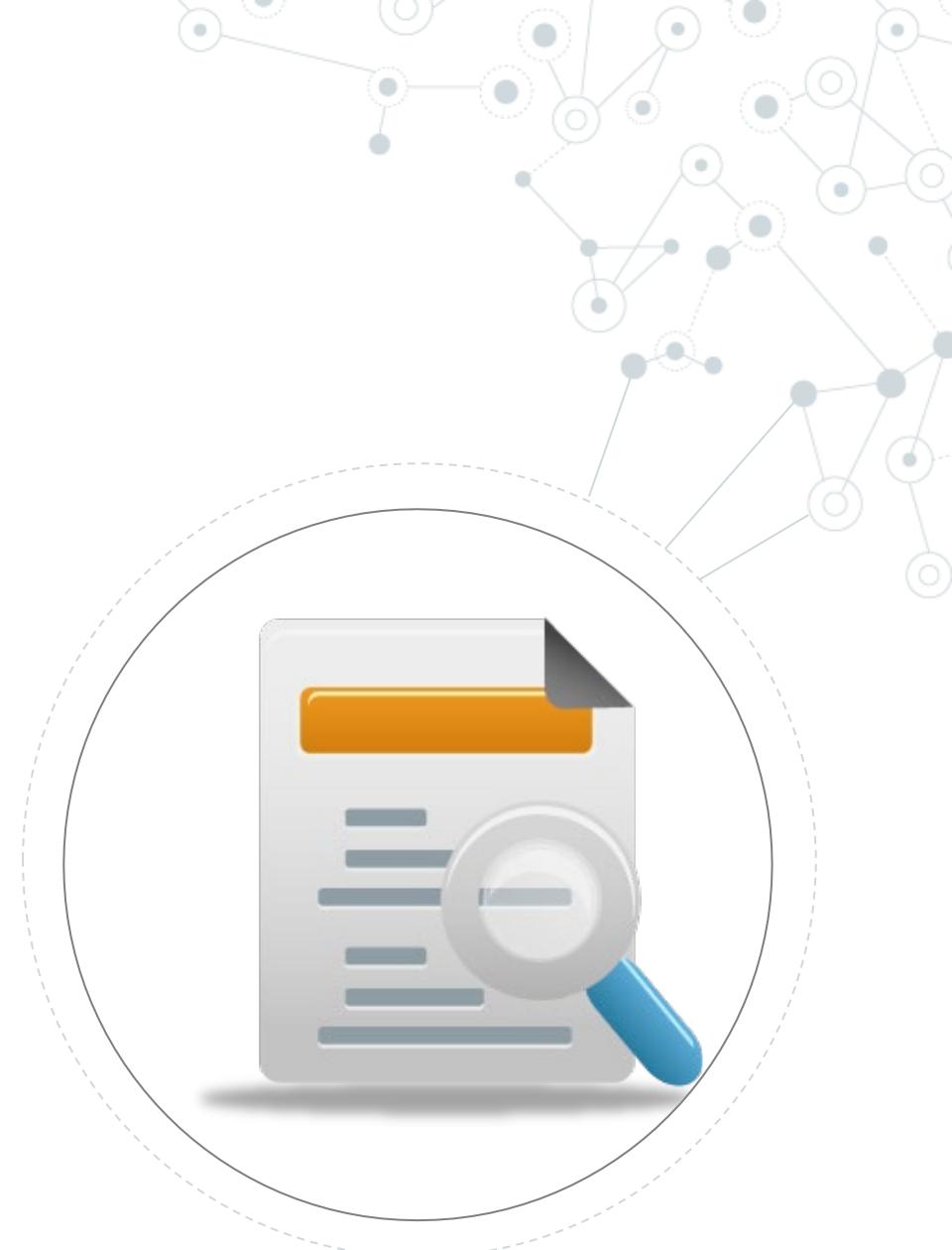




# File Signature Analysis

## Objective

- ◎ By the end of this module, participants will be able to search digital evidence for changes in file extensions



## File Types Overview

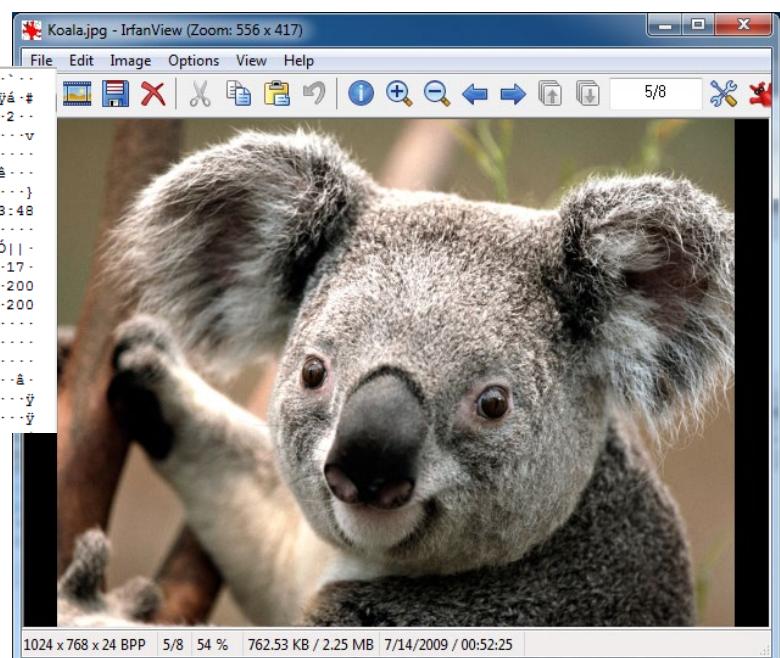
- ◎ Files are accessed by applications and identified by their *type* (header and extension)
- ◎ The Windows environment binds a file to an application using its *extension*



## File Header

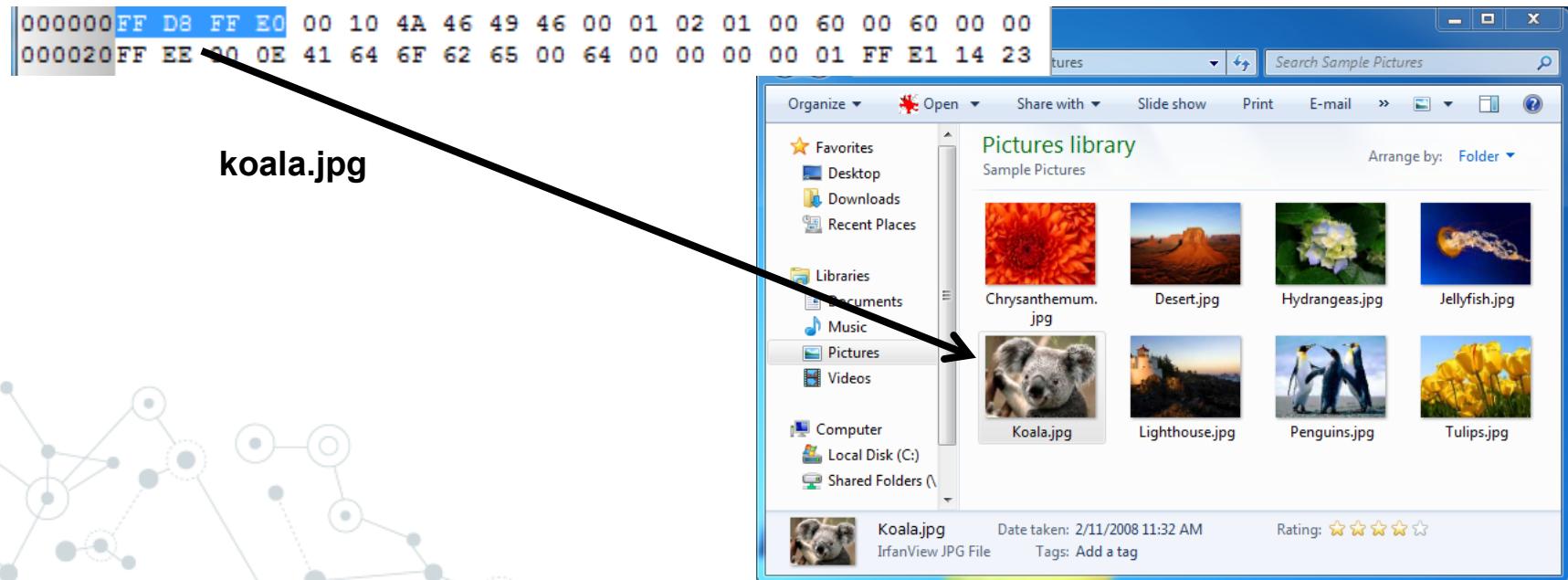
- ◎ Digital signature that applications use to uniquely identify files of a specific type
- ◎ Typically located in the *header* (or first few bytes of the file)

```
000000 FF D8 FF E0 00 10 4A 46 49 46 00 01 02 01 00 60 00 60 00 00  
000020 F0 00 0E 41 64 6F 62 65 00 64 00 00 00 00 01 FF E1 14 23  
000040 08 69 66 00 00 4D 4D 00 2A 00 00 00 07 01 32 00 02  
000060 00 00 14 00 00 00 62 01 3B 00 02 00 00 00 07 00 00 76  
000080 47 46 00 03 00 00 00 01 00 04 00 00 47 49 00 03 00 00 01  
000100 00 3F 00 00 9C 9D 00 01 00 00 00 0E 00 00 00 EA 1C 00 07  
000120 00 00 07 F4 00 00 00 00 87 69 00 04 00 00 00 01 00 00 7D  
000140 00 00 E7 32 30 30 39 3A 30 33 3A 31 32 20 31 33 3A 34 38  
000160 3A 32 38 00 43 6F 72 62 69 73 00 00 05 90 03 00 02 00 00  
000180 14 00 00 BF 90 04 00 02 00 00 00 14 00 00 00 D3 92 91 00  
000200 02 00 00 03 31 37 00 00 92 92 00 02 00 00 00 03 31 37 00  
000220 00 EA 1C 00 07 00 00 07 B4 00 00 00 00 00 00 00 32 30 30  
000240 38 3A 30 32 3A 31 31 20 31 31 3A 33 32 3A 34 33 00 32 30 30  
000260 38 3A 30 32 3A 31 31 20 31 31 3A 33 32 3A 34 33 00 00 05 01  
000280 03 00 03 00 00 00 01 00 06 00 00 01 1A 00 05 00 00 01 00  
000300 00 01 29 01 1B 00 05 00 00 00 01 00 00 01 31 02 01 00 04 00  
000320 00 00 01 00 00 01 39 02 02 00 04 00 00 00 01 00 00 12 E2 00  
000340 00 00 00 00 00 00 48 00 00 00 01 00 00 00 48 00 00 00 01 FF  
000360 D8 FF E0 00 10 4A 46 49 46 00 01 01 00 00 01 00 01 00 FF
```



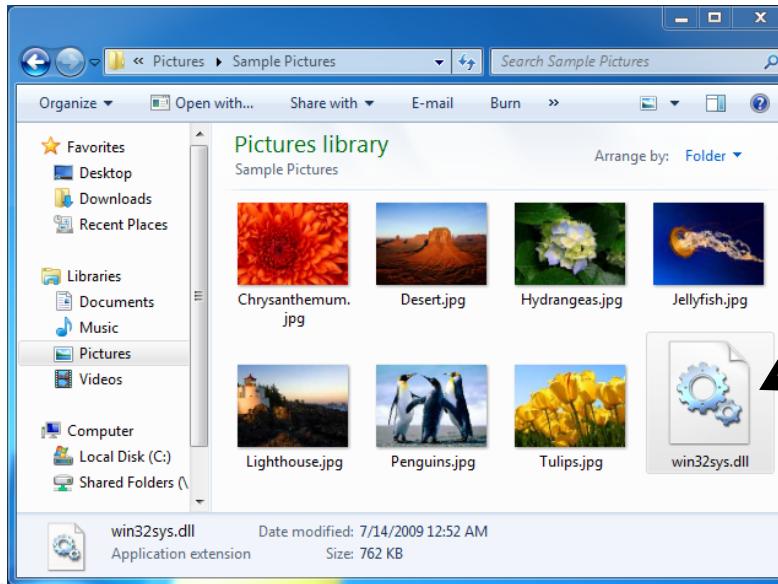
## File Extension

- ◎ Part of the filename that is also typically used to identify the file's type
  - The file header and extension should match
  - Example: koala.jpg → JPEG picture file



## Investigative Consideration

- ◎ Windows relies on the extension—NOT the header
- ◎ Data can be hidden by changing the filename and extension
  - Example: koala.jpg → **win32sys.dll**
  - Binary content of koala.jpg remains the same
  - Windows will now treat the file as a dynamically linked library



## Investigative Software

### ◎ Digital forensics software:

- Analyzes file headers to correctly identify data

win32sys.dll  $\leftarrow \rightarrow$  JPG Header = MISMATCH!!

- Installs with a default set of common file signatures
- Allows examiners to create customized signature searches

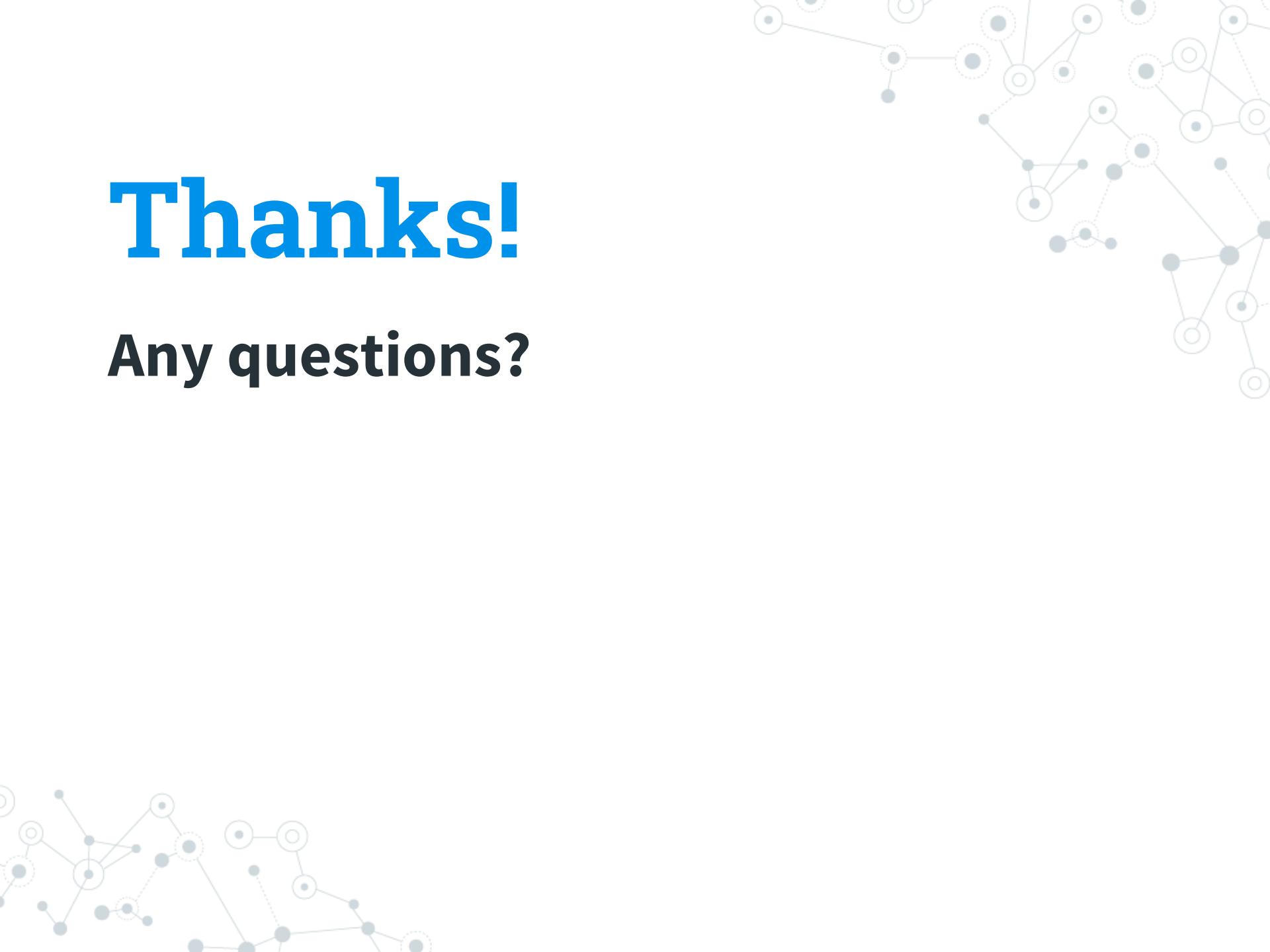
## Summary

### ◎ File signature analysis:

- Is a critical component of digital forensics
- Quickly identifies files that might have been intentionally hidden
- Can decrease the data set for analysis

# Thanks!

Any questions?

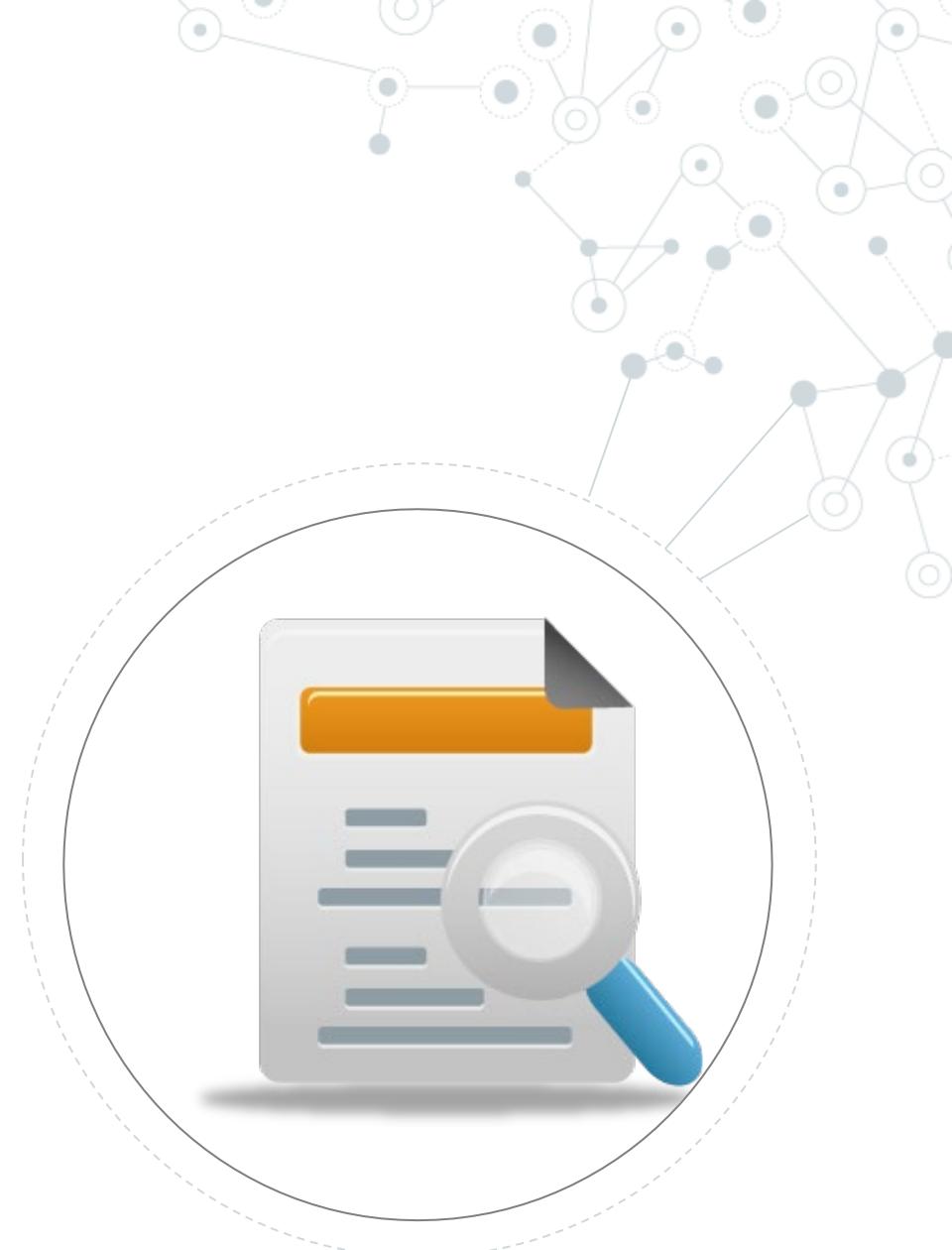




# Search Techniques

## Objective

- ◎ By the end of this module, participants will be able to perform keyword searches



# American Standard Code for Information Interchange (ASCII)

- ◎ A character-encoding scheme originally based on U.S. English
- ◎ Uses 8 bits per characters
- ◎ Is limited to 256 character codes

# ASCII Table Overview

- ◎ The ASCII table consists of the codes for:
  - Characters (Codes 0-127)
  - Decimal values (Codes 128-255)
- ◎ It contains characters found in the Latin alphabet and other characters

# ASCII Table

REGULAR ASCII CHART (character codes 0 – 127)

000d	00h	\	(nul)	016d	10h	►	(dle)	032d	20h	□	048d	30h	0	064d	40h	©	080d	50h	P	096d	60h	‘	112d	70h	p
001d	01h	◎	(soh)	017d	11h	◀	(dc1)	033d	21h	!	049d	31h	1	065d	41h	A	081d	51h	Q	097d	61h	a	113d	71h	q
002d	02h	●	(stx)	018d	12h	‡	(dc2)	034d	22h	”	050d	32h	2	066d	42h	B	082d	52h	R	098d	62h	b	114d	72h	r
003d	03h	▼	(etx)	019d	13h	#!	(dc3)	035d	23h	#	051d	33h	3	067d	43h	C	083d	53h	S	099d	63h	c	115d	73h	s
004d	04h	◆	(eot)	020d	14h	¶	(dc4)	036d	24h	\$	052d	34h	4	068d	44h	D	084d	54h	T	100d	64h	d	116d	74h	t
005d	05h	▲	(enq)	021d	15h	§	(nak)	037d	25h	%	053d	35h	5	069d	45h	E	085d	55h	U	101d	65h	e	117d	75h	u
006d	06h	◆	(ack)	022d	16h	-	(syn)	038d	26h	&	054d	36h	6	070d	46h	F	086d	56h	V	102d	66h	f	118d	76h	v
007d	07h	.	(bel)	023d	17h	‡	(etb)	039d	27h	'	055d	37h	7	071d	47h	G	087d	57h	W	103d	67h	g	119d	77h	w
008d	08h	■	(bs)	024d	18h	†	(can)	040d	28h	(	056d	38h	8	072d	48h	H	088d	58h	X	104d	68h	h	120d	78h	x
009d	09h		(tab)	025d	19h	↓	(em)	041d	29h	)	057d	39h	9	073d	49h	I	089d	59h	Y	105d	69h	i	121d	79h	y
010d	0Ah	■■	(lf)	026d	1Ah		(eof)	042d	2Ah	*	058d	3Ah	:	074d	4Ah	J	090d	5Ah	Z	106d	6Ah	j	122d	7Ah	z
011d	0Bh	σ	(vt)	027d	1Bh	-	(esc)	043d	2Bh	+	059d	3Bh	;	075d	4Bh	K	091d	5Bh	[	107d	6Bh	k	123d	7Bh	{
012d	0Ch		(np)	028d	1Ch	L	(fs)	044d	2Ch	,	060d	3Ch	<	076d	4Ch	L	092d	5Ch	\	108d	6Ch	l	124d	7Ch	
013d	0Dh	›	(cr)	029d	1Dh	--	(gs)	045d	2Dh	-	061d	3Dh	=	077d	4Dh	M	093d	5Dh	]	109d	6Dh	m	125d	7Dh	}
014d	0Eh	¤	(so)	030d	1Eh	▲	(rs)	046d	2Eh	.	062d	3Eh	>	078d	4Eh	N	094d	5Eh	~	110d	6Eh	n	126d	7Eh	-
015d	0Fh	◦	(si)	031d	1Fh	▼	(us)	047d	2Fh	/	063d	3Fh	?	079d	4Fh	O	095d	5Fh	_	111d	6Fh	o	127d	7Fh	□

EXTENDED ASCII CHART (character codes 128 – 255) LATIN1/CP1252

128d	80h	€	144d	90h		160d	A0h	\	176d	B0h	°	192d	C0h	À	208d	D0h	Ð	224d	E0h	à	240d	F0h	ð
129d	81h	145d	91h	‘	161d	A1h	í	177d	B1h	±	193d	C1h	Á	209d	D1h	Ñ	225d	E1h	á	241d	F1h	ñ	
130d	82h	,	146d	92h	’	162d	A2h	¢	178d	B2h	²	194d	C2h	Â	210d	D2h	Ô	226d	E2h	â	242d	F2h	ô
131d	83h	ƒ	147d	93h	“	163d	A3h	£	179d	B3h	³	195d	C3h	Ã	211d	D3h	Õ	227d	E3h	ã	243d	F3h	õ
132d	84h	„	148d	94h	”	164d	A4h	¤	180d	B4h	·	196d	C4h	À	212d	D4h	Ø	228d	E4h	ä	244d	F4h	ö
133d	85h	...	149d	95h	•	165d	A5h	¥	181d	B5h	µ	197d	C5h	Å	213d	D5h	Ø	229d	E5h	å	245d	F5h	ö
134d	86h	†	150d	96h	-	166d	A6h	:	182d	B6h	¶	198d	C6h	È	214d	D6h	Ø	230d	E6h	æ	246d	F6h	ø
135d	87h	‡	151d	97h	--	167d	A7h	§	183d	B7h	·	199d	C7h	Ҫ	215d	D7h	×	231d	E7h	ç	247d	F7h	+
136d	88h	-	152d	98h	-	168d	A8h	-	184d	B8h	¸	200d	C8h	È	216d	D8h	Ø	232d	E8h	è	248d	F8h	ø
137d	89h	‰	153d	99h	™	169d	A9h	©	185d	B9h	¹	201d	C9h	É	217d	D9h	Ù	233d	E9h	ë	249d	F9h	ù
138d	8Ah	Ś	154d	9Ah	Ś	170d	AAh	⌐	186d	BAh	⌐	202d	CAA	È	218d	DAA	Ù	234d	EAh	ë	250d	FAh	ú
139d	8Bh	<	155d	9Bh	>	171d	ABh	⌐	187d	BBh	⌐	203d	CBA	È	219d	DBh	Ø	235d	EBh	ë	251d	FBh	ú
140d	8Ch	Œ	156d	9Ch	Œ	172d	ACH	⌐	188d	BCH	⌐	204d	CCA	Î	220d	DCH	Ù	236d	ECh	í	252d	FCh	ü
141d	8Dh		157d	9Dh		173d	ADh		189d	BDh	⌐	205d	CDA	Î	221d	DDh	Ý	237d	EDh	í	253d	FDh	ý
142d	8Eh	Ž	158d	9Eh	Ž	174d	AEh	®	190d	BEh	⌐	206d	CEA	Î	222d	DEh	Þ	238d	EEh	í	254d	FEh	þ
143d	8Fh		159d	9Fh	ÿ	175d	AFh	-	191d	BFh	⌐	207d	CFA	Î	223d	DFA	Ù	239d	EFh	í	255d	FFh	ÿ



# Unicode

- ◎ Initially, telegraph and computers used only English/Latin characters
- ◎ When other languages were required, ASCII character codes were insufficient

# Unicode

- ◎ **Uses a unique two-byte number for every character**
- ◎ **Can define more than 65,000 characters, allowing the computer to display any world language**

Case (EnCaseOverview) View Tools EnScript Add Evidence

Home

Reports

Evidence

Search

Records



Viewing (Entry)



Table Timeline

Gallery



Selected 0/55

MALAY

Ngày 152004, khởi EUV

Russian

ભારત મેં સુપ્રીમHINDI

બરિએક તુલનાનાકોર્પોરેશન

ઉર્જાકાળેકોર્પોરેશન

Comp and lang docs

System info

Plain Text

ASCII

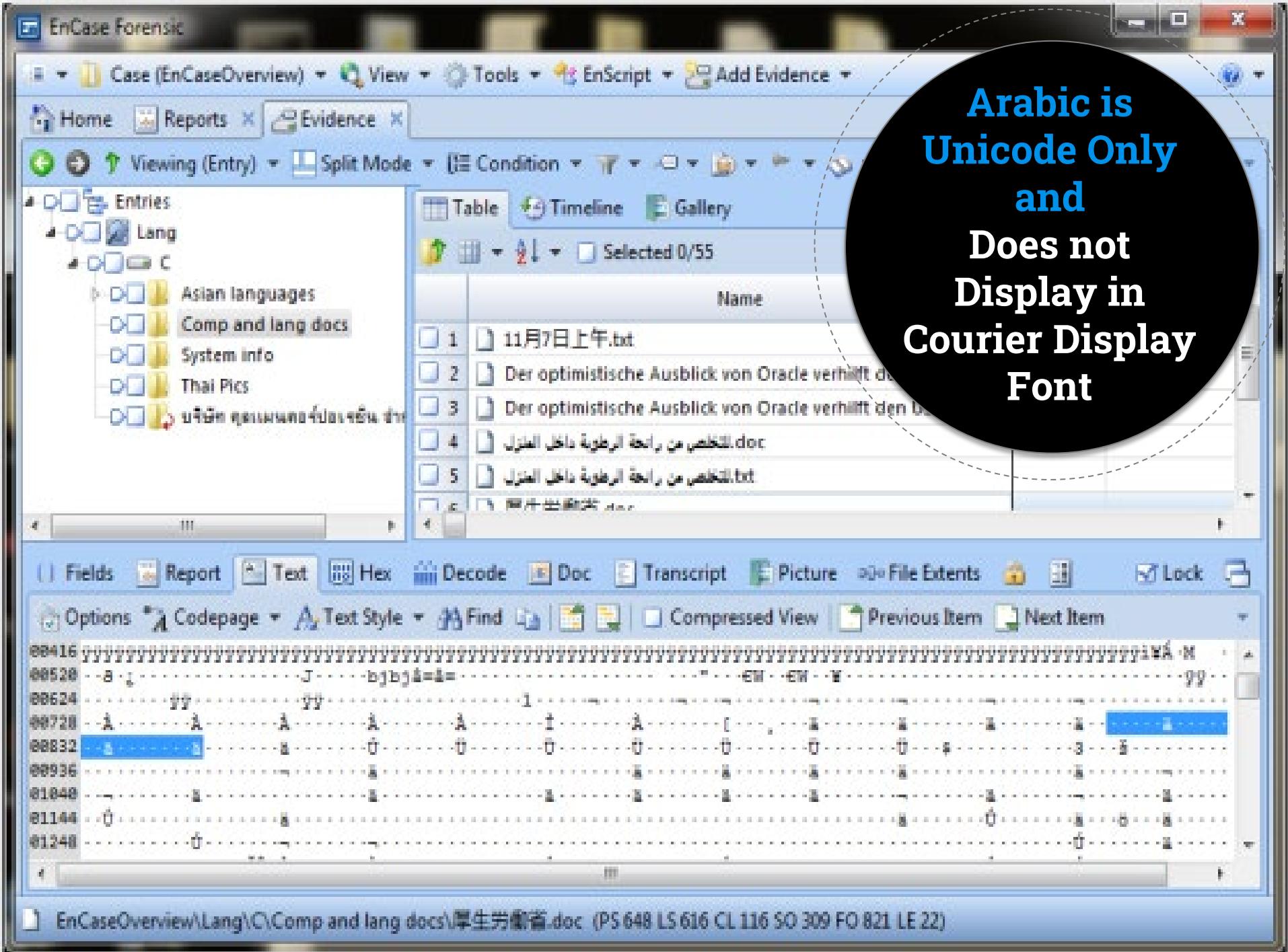
Name

- |   |  |
|---|--|
| 2 | Der optimistische Ausblick von Oracle verhilft den US-Börsen zu kräftigen Gewinne... |
| 3 | Der optimistische Ausblick von Oracle verhilft den US-Börsen zu kräftigen Gewinne... |
| 4 | اللخصر من رائحة الرطوبة داخل المنزل.doc  |

Fields Report Text Hex Decode Doc Transcript Lock

Options Codepage Text Style Find Compressed View Previous Item

01512	00 00 1E 02 00 00 00 00 00 1E 02 00 00 00 00 00 02 00 D9	.....
01533	00 00 00 44 65 72 20 6F 70 74 69 6D 69 73 74 69 73 63 68 65 20	...Der optimistische
01554	41 75 73 62 6C 69 63 6B 20 76 6F 6E 20 4F 72 61 63 6C 65 20 76	Ausblick von Oracle v
01575	65 72 68 69 6C 66 74 20 64 65 6E 20 55 53 2D 42 F6 72 73 65 6E	erhilft den US-Börsen
01596	20 7A 75 20 6B 72 E4 66 74 69 67 65 6E 20 47 65 77 69 6E 6E 65	zu kräftigen Gewinne
01617	6E 2E 20 4F 72 61 63 6C 65 20 FC 62 65 72 6C 61 67 65 72 65 20	n. Oracle überlagerte
01638	64 69 65 20 61 6E 68 61 6C 74 65 6E 64 65 20 46 75 72 63 68 74	die anhaltende Furcht



**Arabic is  
Unicode Only  
and  
Does not  
Display in  
Courier Display  
Font**

EnCase Forensic

Case (EnCaseOverview) View Tools EnScript Add Evidence

Home Reports Evidence Search Records

Viewing (Entry)

MALAY Ngày 152004, khởi EUV Russian ભારત મેં સુપ્રીમ HINDI ປະເທດ ຖະແນນຄອર່ປ່ອເຮົ້າ ວິຊາວາໂທລະໂປຣເກມພິໄຕ Comp and lang docs System info

Table Timeline Gallery Selected 0/55

Name

2 Der optimistische Ausblick von Oracle verhilft den US.txt  
3 Der optimistische Ausblick von Oracle verhilft den US.txt  
4 التخلص من رائحة الرطوبة داخل المنزل.doc

Fields Report Text Hex Decode Doc Transcript Lock

Options Codepage Text Style Find Compressed View Previous Item

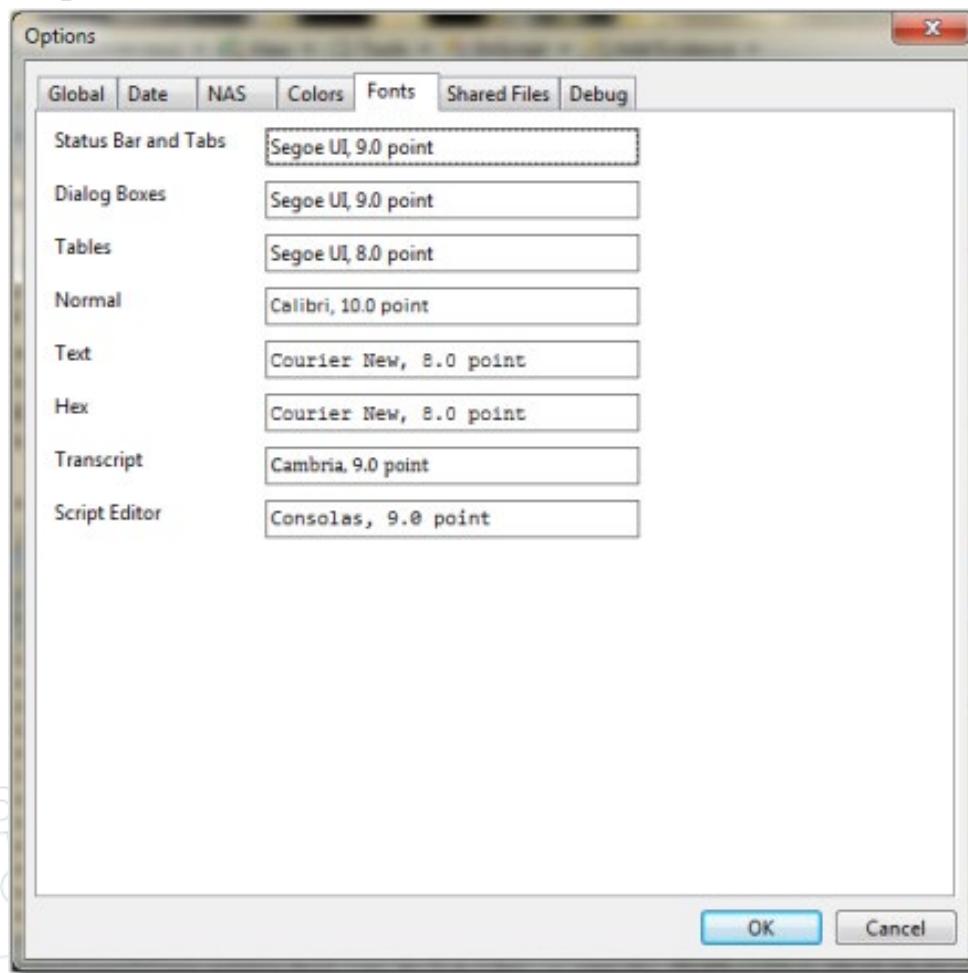
0000	FF FE	44 00 65 00 72 00 20 00 6E 00 70 00 74 00 69 00 6D 00 69	Der optimistische Ausblick von Oracle verhilft den US.txt
0021	00 73 00 74 00 69 00 73 00 63 00 68 00 65 00 20 00 41 00 75 00	Der optimistische Ausblick von Oracle verhilft den US.txt	
0042	73 00 62 00 6C 00 69 00 63 00 6B 00 20 00 76 00 6F 00 6E 00 20	التخلص من رائحة الرطوبة داخل المنزل.doc	
0063	00 4F 00 72 00 61 00 63 00 6C 00 65 00 20 00 76 00 65 00 72 00		
0084	68 00 69 00 6C 00 66 00 74 00 20 00 64 00 65 00 6E 00 20 00 55		
0105	00 53 00 2D 00 42 00 F6 00 72 00 73 00 65 00 6E 00 20 00 7A 00		
0126	75 00 20 00 6B 00 72 00 E4 00 66 00 74 00 69 00 67 00 65 00 6E		

EnCaseOverview\Lang\C...\Der optimistische Ausblick von Oracle verhilft den US.txt (PS 595 LS 563 CL 103 SO 2 FO 2 LE 34)

Same Characters in Unicode

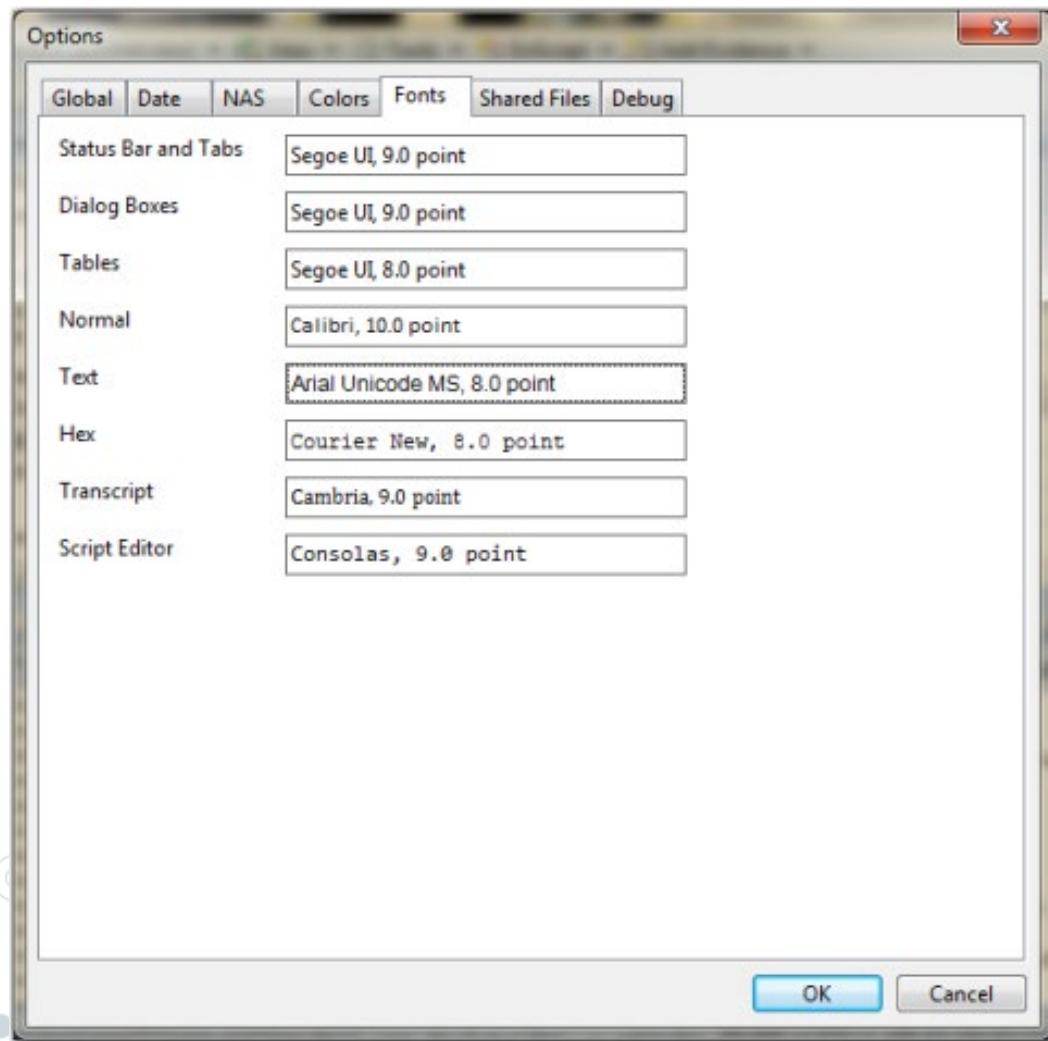
# Modifying the Display Font

◎ To display Unicode fonts, go to:  
**Tools > Options > Fonts**



# Changing the Font

## ◎ Select Arial Unicode MS Font



EnCase Forensic

Case (EnCaseOverview) View Tools EnScript Add Evidence

Home Reports Evidence Search Records

Viewing (Entry)

MALAY Ngày 152004, khởi EUV Russian ભારત મેં સુપ્રીમ HINDI ພັບຊາດ ຖະແນນຄອરໍປ່ອເຮົ້າ ວິວຂາວໂທອດໂປຣເກຣມໄຟ້

Comp and lang docs System info

Fields Report Text Options Codepage

Codepage

016500631  
016800647  
017100629  
017400633  
017700648  
018000643  
018300648  
018600020  
018900627

Unicode Western European (Windows)  
Outlook Compressible Encryption  
Unicode (Big-Endian)  
Unicode (UTF-8)

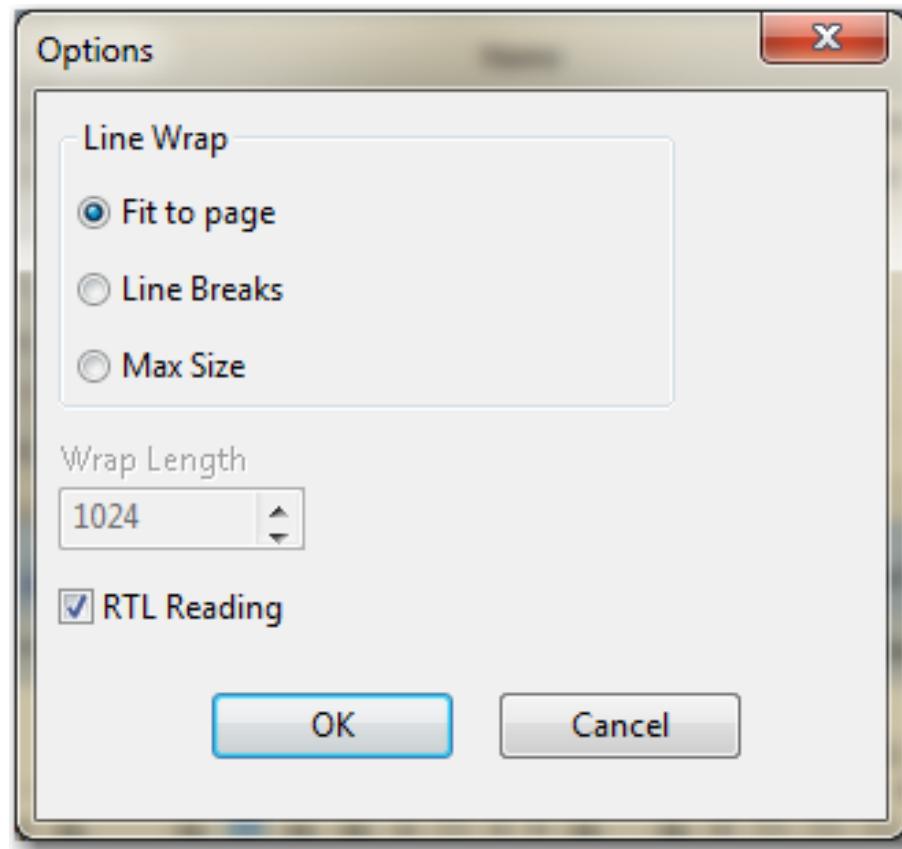
Code Pages...

EnCaseOverview\Lang\C...\Der 2 FO 2 LE 34)

# Changing Code page

# Changing Reading Direction

◎ On Options Menu, Check RTL Reading



Arabic  
Displayed

Correctly

EnCase Forensic

Case (EnCaseOverview) View Tools EnScript Add Evidence

Home Reports Evidence

Viewing (Entry) Split Mode

Entries Lang C Asian languages Comp and lang docs System info Thai Pics

Table Timeline Gallery

Selected 0/55

Name

1 11月7日上午.txt  
2 Der optimistische Ausblick von Oracle verhilft den US-Markt zu einem weiteren Anstieg.  
3 Der optimistische Ausblick von Oracle verhilft den US-Markt zu einem weiteren Anstieg.  
4 التخلص من رائحة الرطوبة داخل المنزل.doc  
5 التخلص من رائحة الرطوبة داخل المنزل.txt

Fields Report Text Hex Decode Doc Transcript Picture Lock

Codepage Text Style Find Compressed View Previous Item Next Item

莫 - موصى المطبخ يمكن ان تظهر رائحة الرطوبة داخل المنزل سهولة والاختبار وجود الرطوبة يمكن المصق قطعة من ورق (الالماسوم) على الحاطن في الماء الذي زال عنه الطلع مع تركها لمدة يوم فانا ظهر البال على سطح الورق فان هذه المنطقة تعانى وجود الرطوبة العالية بسبب تكثيف الرطوبة

EnCaseOverview\Lang\C\Comp and lang docs\التخلص من رائحة الرطوبة داخل المنزل.doc (PS 604 LS 572 CL 105 SO 432 FO 944 LE 270)

# EnCase

## Search Techniques

# Conducting an Index Search

- ◎ To create the index:
  - Run the EnCase Evidence Processor
  - Enable the *Index text and metadata* feature
  - Index personal information (optional)

# Searching and Viewing

## Results

EnCase Forensic

Case (ATACyber) View Tools EnScript Add Evidence

Home Reports Evidence Records Results Search

Viewing (Search) Split Mode Condition Filter Searches Tags Review

Index Tags Keywords Summary Find

Field Patterns Find

skimmer

	Word	Hits	Items
1	skimmer	3,407	264
2	skimmer%20devices&tc=none&iso=...	11	7
3	skimmer%20devices&tc=none&iso=...	3	2
4	skimmer%20devices&tc=none&iso=...	1	1
5	skimmer's	5	5
6	skimmer-install.gif	1	1

Fields Report Text Hex Decode Doc Transcript Picture Review Lock

Zoom In Zoom Out 100% Previous Item Next Item

From: Marco Tepisang <[marco.tepisang@gmail.com](mailto:marco.tepisang@gmail.com)>  
To: Natasha Bunting <[natashabunting@me.com](mailto:natashabunting@me.com)>; Jabari Pearson <[justjabari75@gmail.com](mailto:justjabari75@gmail.com)>  
<[justjabari75@gmail.com](mailto:justjabari75@gmail.com)>  
Sent: 08/15/12 11:55:50AM  
Subject: remember this guy?

This was one of the guys on our team when we were hot and heavy in Brazil...I cant remember his name but he is the one that got Jabari and I in the ATM game!! I guess we wont be seeing him for awhile!!

<http://consumerist.com/2009/09/video-guy-installing-skimmer-on-atm.html>

ATACyber/Sent/remember this guy?

# Proximity Searches

- ◎ Keyword1 w/35 Keyword2 or keywords in quotes
- ◎ Boolean logic
- ◎ Stemming and fuzzy searches
- ◎ Pattern searches

The screenshot shows the EnCase Forensic interface. On the left, there's a search bar with the query "skimmer w/5 atm". Two red boxes highlight this search bar and the results table below it. The results table has columns for Word, Hits, and Items. It shows two entries: "1 atm" with 11,871 hits and 1 item, and "2 atm&a" with 1 hit and 1 item. Below the table, an email message is displayed. The subject is "Re: remember this guy?". The body of the email reads:  
Tristan Williams...  
It was just a matter of time before that moron got bagged. Look at the date of the video upload though...he's probably been convicted already and rotting. No sympathy here!  
  
On Wed, Aug 15, 2012 at 11:55 AM, Marco Tepisang <marco.tepisang@gmail.com> wrote:  
This was one of the guys on our team when we were hot and heavy in Brazil...I cant remember his name but he is the one that got Jabari and I in the ATM game!! I guess we wont be seeing him for awhile!!  
  
<http://consumerist.com/2009/09/video-guy-installing-skimmer-on-atm.html> [http://consumerist.com/2009/09/video-guy-installing-skimmer...]

EnCase Forensic

Case (ATACyber) View Tools EnScript Add Evidence

Home Reports Evidence Records Results Search

Viewing (Entry) Split Mode Condition Filter Tags Review Package

MSOCache PerLogs Program Files Program Files (x) ProgramData Recovery System Volume! Users All Users Default Default User Marco Public Video Windows

Table Timeline Gallery

Selected 14252/579174

	Name	Hash Sets
1	AppData	db3096c4...
2	Application Data	ab9a6395...
3	Contacts	e6d077b0...
4	Cookies	ab9a6395...
5	Desktop	6070957e4...
6	Documents	431cd15d9231989bc9c26da1f1d1f1b36...
7	Downloads	57123185bbfe06c3d98d84cd0699ed7a...
8	Dropbox	1d3a0cf7@af42a78d...
9	Favorites	0db71026785...

New Raw Search Selected...

Fields Report Text Hex Decode Doc Transcript Picture File/Ext

Find Compressed View Previous Item Next Item Fit To Page

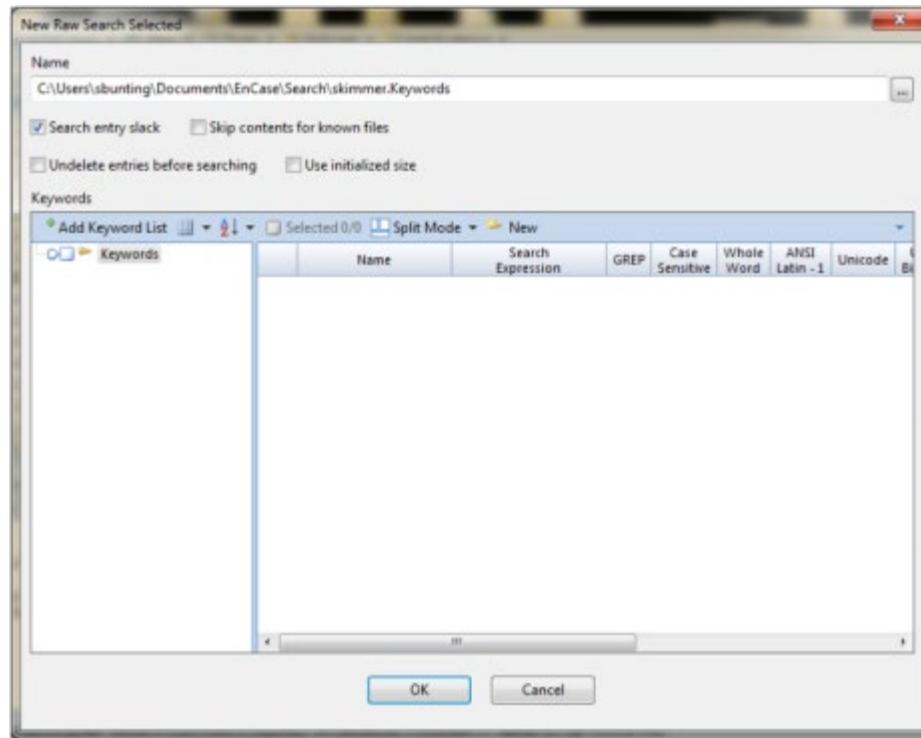
Localing h R E 15@ P@ P@ P@ LocalLow E 'P E UDXr Dr [x] Roaming

ATACyber\episangMBP-500GB\Users\Marco\AppData (PS 494300144 LS 6292464 CL 786558 SO 328 TO 0 LE 775)

New Raw  
Search  
Selected  
  
To Conduct  
Live Search

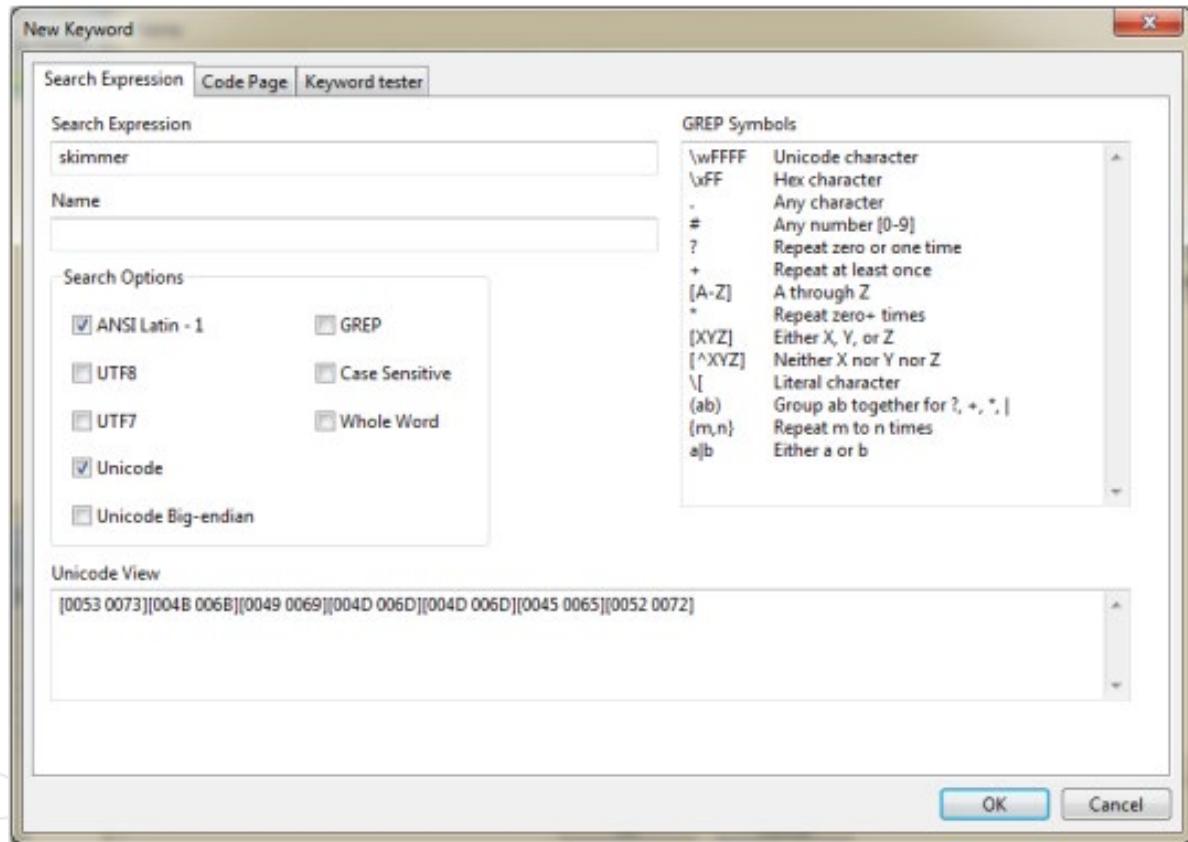
# Creating a New Keyword

- ◎ On the New Raw Search Selected Menu:
  - Name the search
  - Select the path for storage
  - Click New in the keywords toolbar



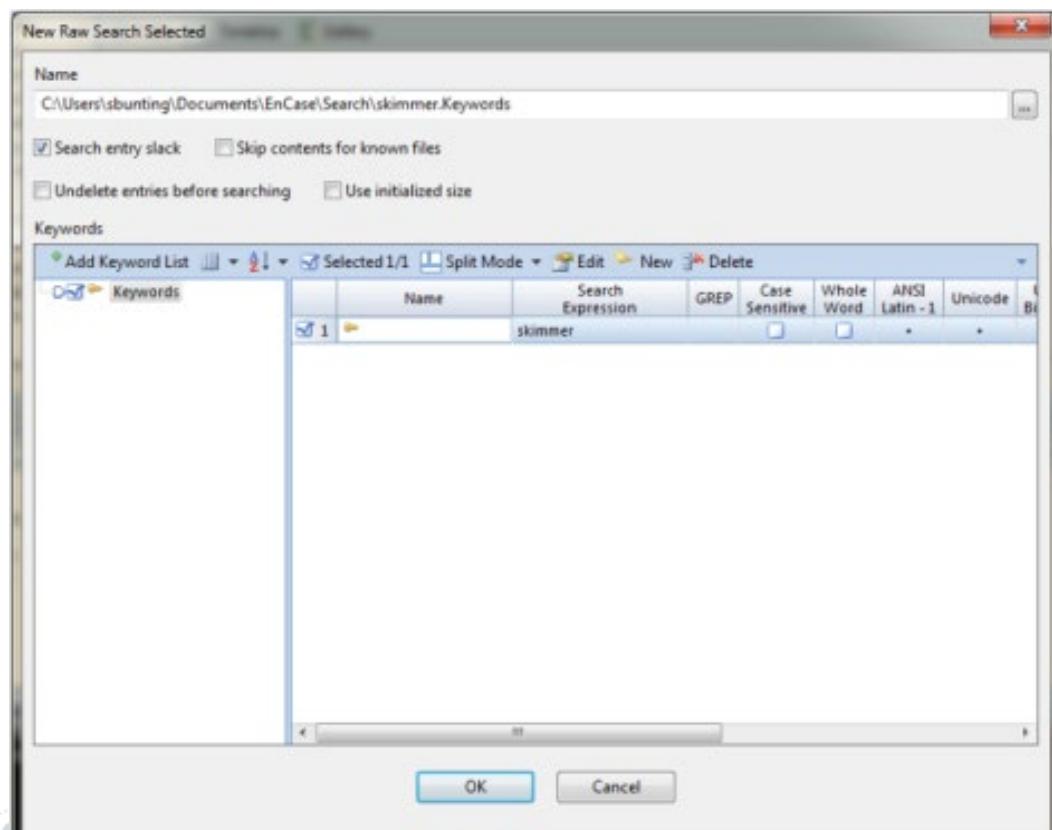
# Keyword Search Expression

- ◎ On the New Keyword Menu:
  - Type the keyword under Search Expression
  - Select the Unicode search option



# Running the Search

- ◎ Verify the file name, path, and search options
- ◎ Click OK to start the search
- ◎ Monitor the progress bar



# Viewing the Results

## ATM Skimmers, Part II

Easily the most-viewed post at [krebsonsecurity.com](#) so far has been the entry on a cleverly disguised ATM skimmer found attached to a Citibank ATM in California in late December. Last week, I had a chance to chat with Rick Doten, chief scientist at Lockheed Martin's [Center for Cyber Security Innovation](#). Doten has built an impressive slide deck on ATM fraud attacks, and pictured below are some of the more interesting images he uses in his presentations.

According to Doten, the U.S. Secret Service estimates that annual losses from ATM fraud totaled about \$1 billion in 2008, or about \$350,000 each day. Card skimming, where the fraudster affixes a bogus card reader on top of the real reader, accounts for more than 80

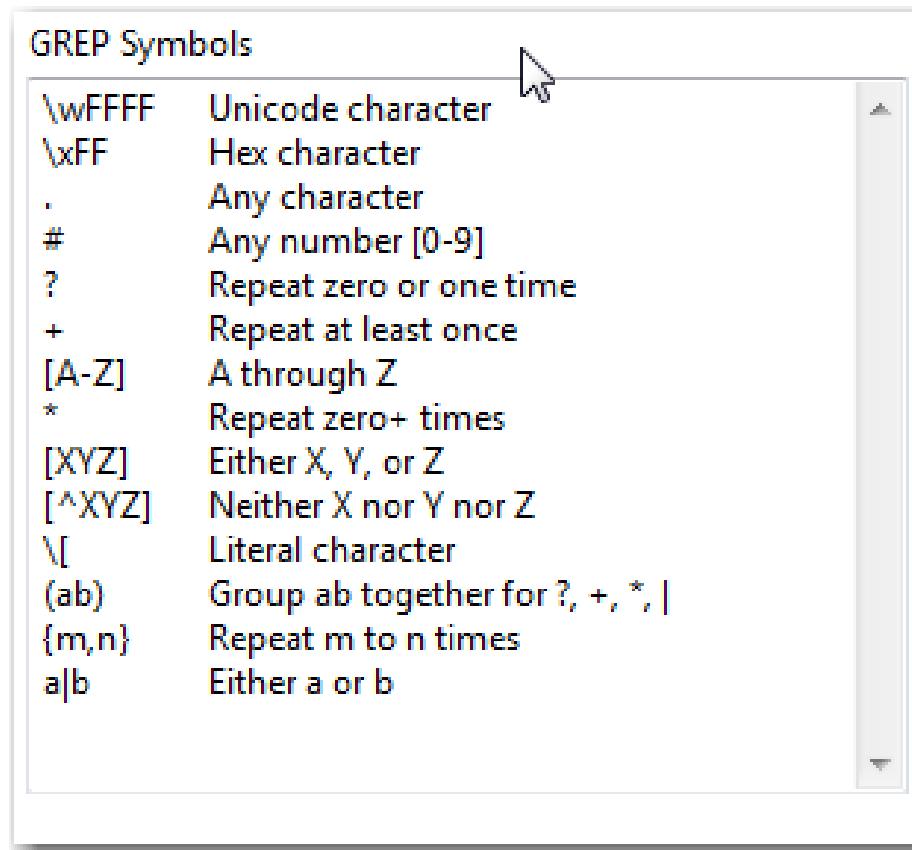
ATACyber\episangMBP-500GB\E\Users\Marco\Dropbox\dropbox.cache\2...\ATM Skimmers, Part II — Krebs on Security (deleted 501acc02-1eaa4-7b8a2d86).html

# GREP Search

- ⦿ **Global Regular Expression Parser (GREP):**
- Searches for plain text with regular expressions
- Matches strings of text against characters, words, numbers, patterns, wildcards, etc.

# GREP Symbols

- From the New Keyword Menu, select GREP symbols to combine with text and numbers

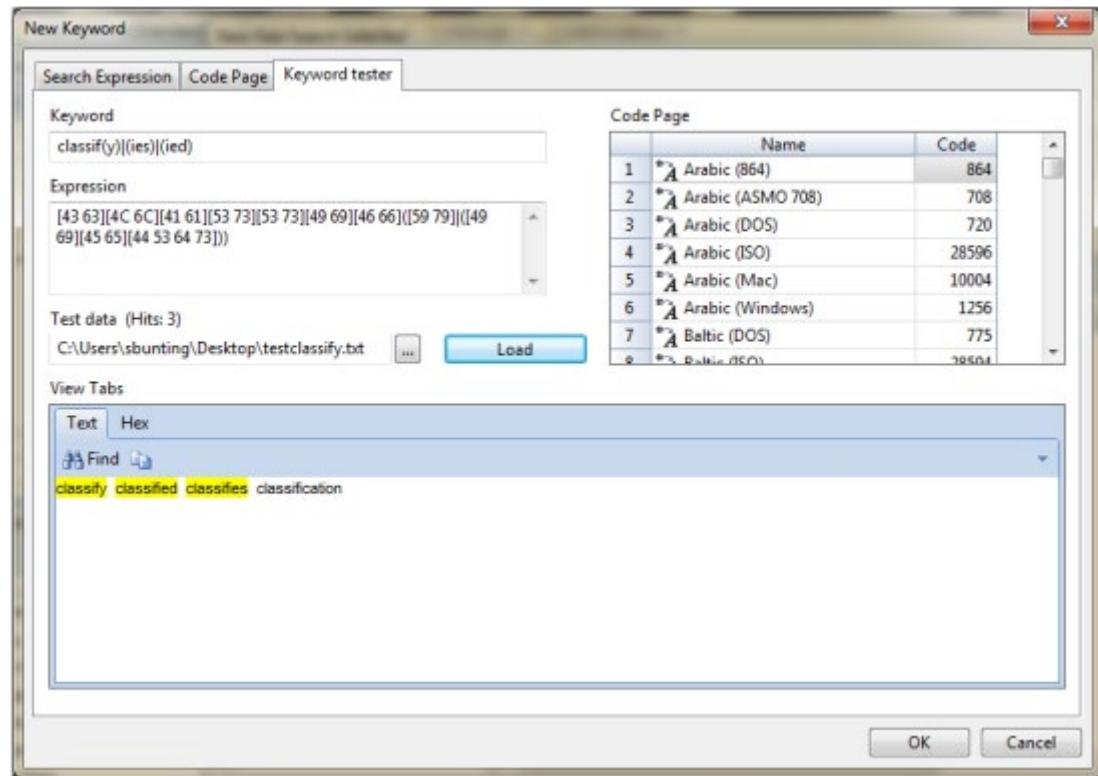


# GREP Examples

GREP Search	Results
re[ae]d	<b>Will find read or reed</b>
reads?	<b>Will find read or reads</b>
classif(y) (ied) (ies)	<b>Will find classify or classified or classifies</b>

# Using the Keyword Tester

- ◎ On the New Keyword menu, go to the keyword tester tab
- ◎ Test the GREP search on a list you created



# Data Carving

- ◎ Locates files, primarily in unallocated spaces, based on file signature (header)
- ◎ Can be:
  - Used against RAM dumps, swap files, and hibernation files
  - Performed manually or automated

# EnCase Forensic

Case (ATACyber) View Tools

Home Reports File Types Evid

Viewing (File Type) Split Mode

Table

Selected 0/818 Edit New

	Name	Extensio
434	InstallShield Uninstall Script	isu
435	Ricoh Camera	j6i
436	Java Archive	jar
437	Compressed Java Archive	jar
438	Java Source	jav;java
439	JPEG	je;im;jif;jif
440	JetFax	jet
441	Corel JPEG	jff
442	Microsoft Scheduler Job O...	job
443	JPEG Image Non-Standard	jpg;jpeg;jpe
444	JPEG Image Uncommon	jpg;jpeg;jpe
445	JPEG Image Standard	jpg;jpeg;jpe
446	Java Script	js

Edit "JPEG Image Standard"

Options Header Footer

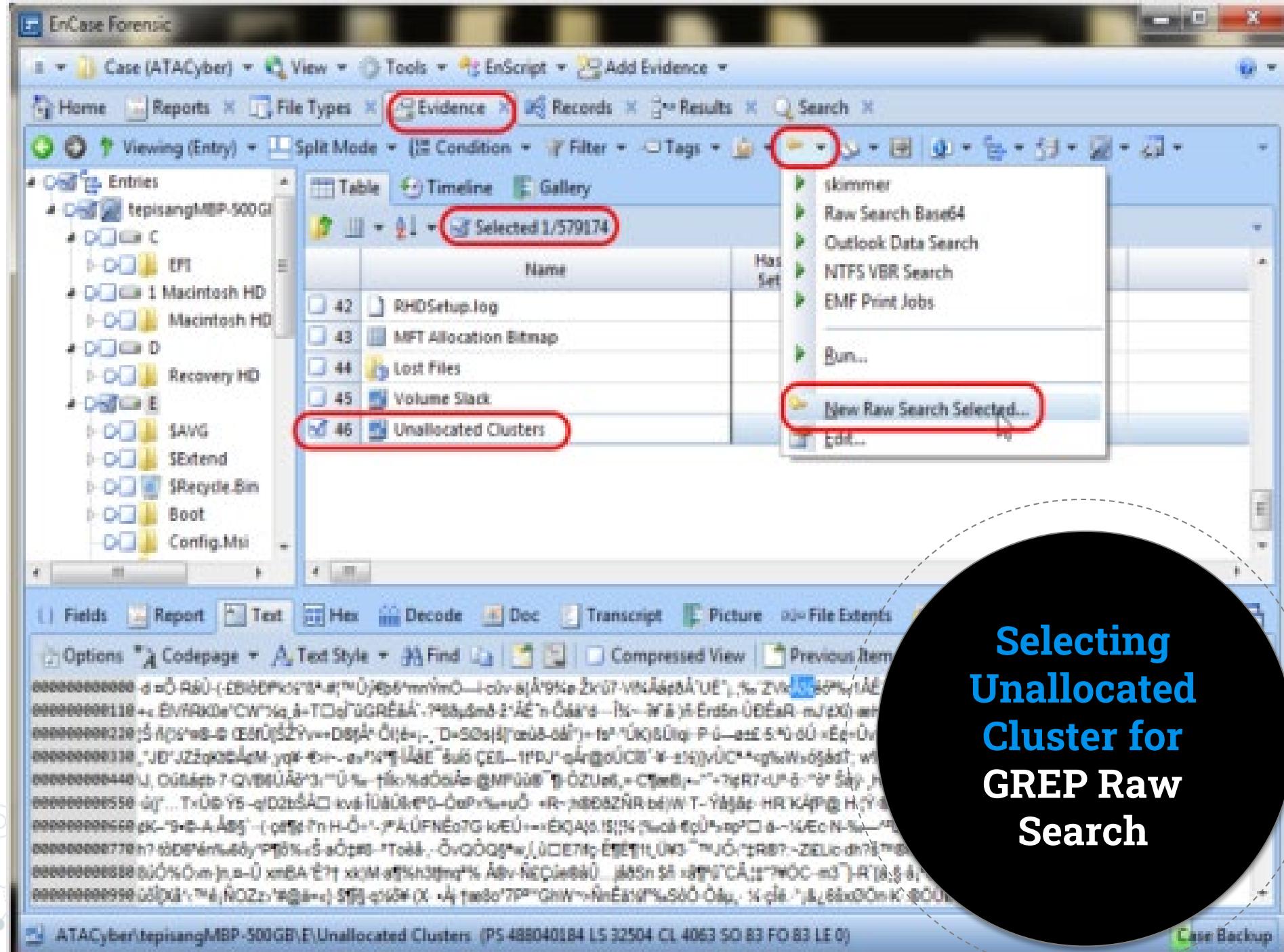
Search Expression: `(xFF\xD8\xFF|\xE0\xEE)`

Search Options:

- GREP
- Case Sensitive

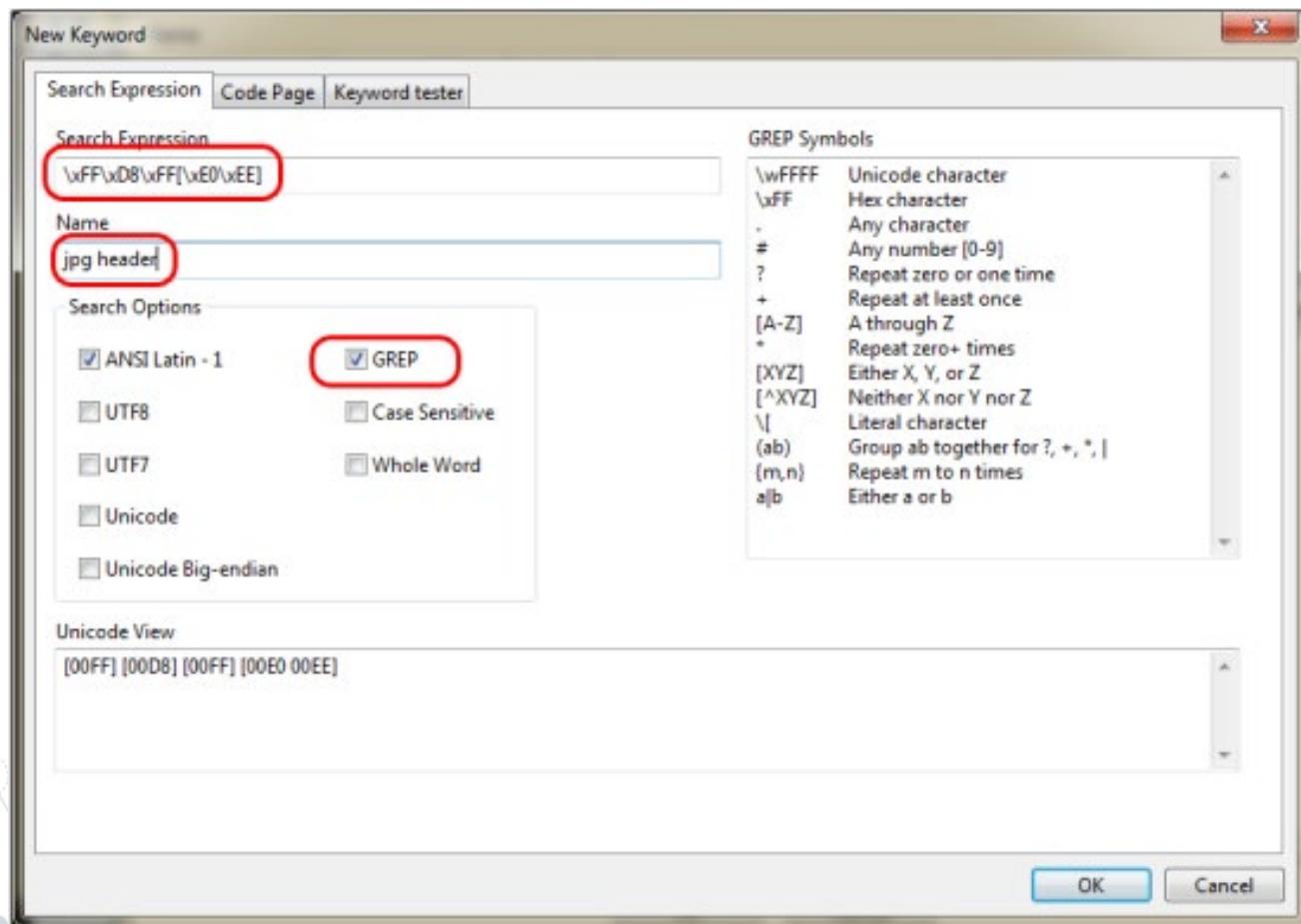
View: [FF] [D8] [FF] [E0 EE]

**Manual Data Carving**  
**From File Types View, Copy JPG Header**



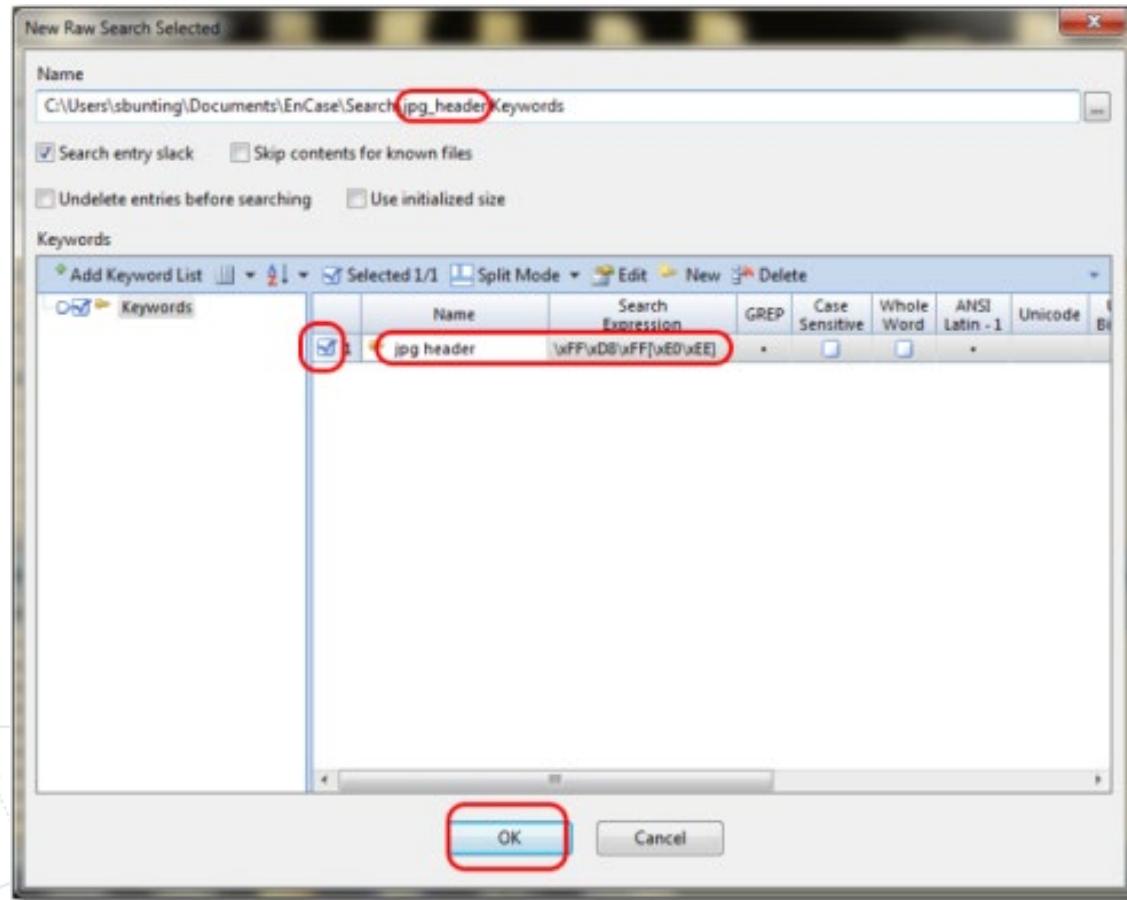
# Creating the GREP Keyword

- From the New Keyword Menu, paste the JPG header



# Running the Search

- ④ On the New Raw Search Selected menu, name the search file and path, then click OK



EnCase Forensic

Case (ATACyber) View Tools EnScript Add Evidence

Home Reports File Types Evidence Records Results Search

Viewing (Entry) Split Mode Condition Filter Tags

Disk Entries

39 bootmgr 383,700

40 BOOTSECT.BAK 8,192

41 pagefile.sys 8,294,977,536

42 RHDSetup.log 2,060

43 MFT Allocation Bitmap 14,112

44 Lost Files 0

45 Volume Stack 3,584

46 Unallocated Clusters 194,194,874,368

Name Logical Size

Table Timeline Gallery

Selected 1/579174

Fields Report Test Hex Decode Doc Transcript Picture File Extents Permissions Lock

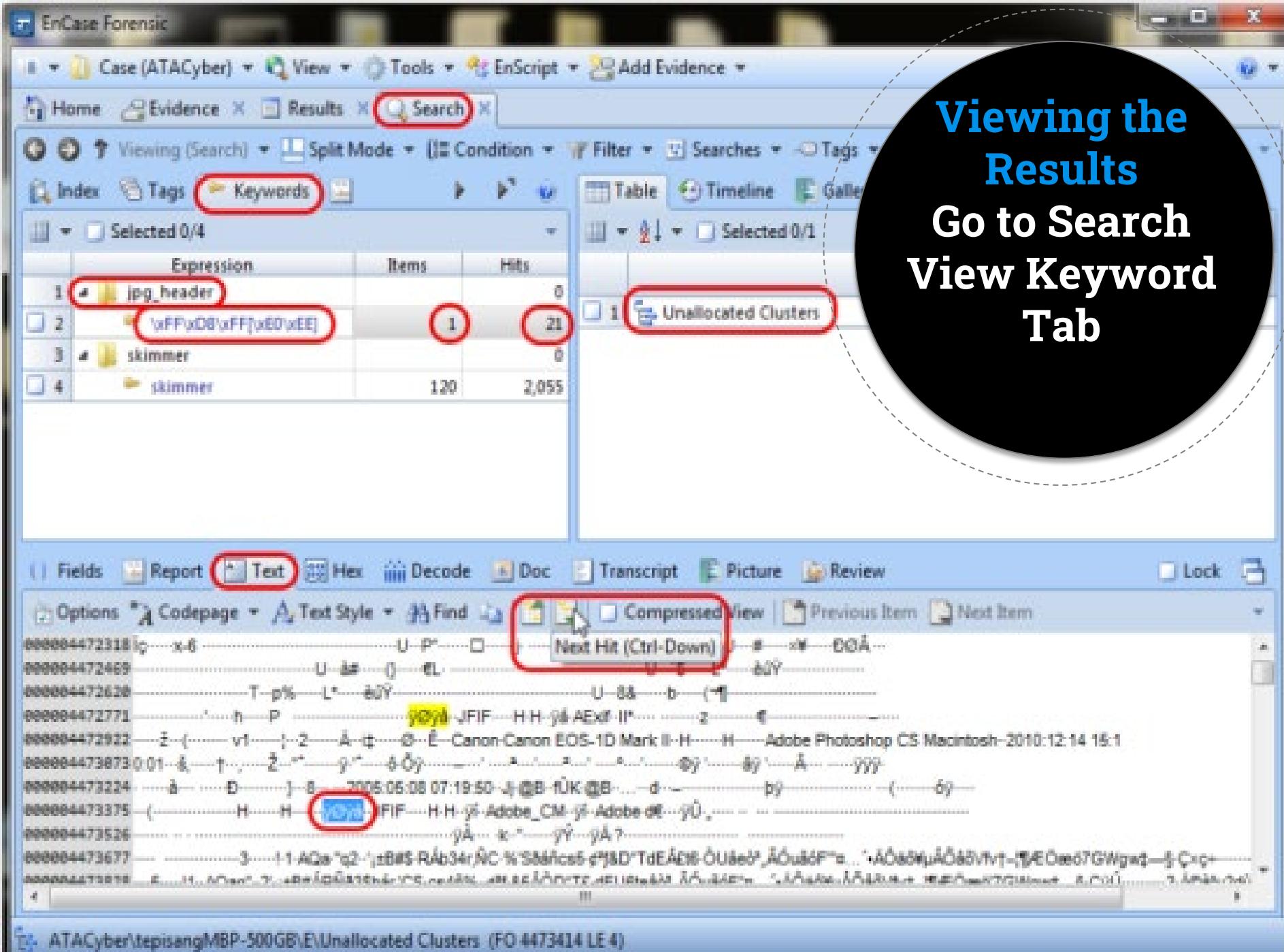
Options Codepage Text Style Find Compressed View Previous Item Next Item

Searching 20 Hits

ATAcyber/tepisangMBP-500GB/E(Unallocated Clusters) (PS 488040184 LS 32504 CL 4063 SO 83 PO 83 LE 0)

Searching 20 Hits

# Monitor the Search Progress Bar



# Viewing the Results

## Go to Search View Keyword Tab

EnCase Forensic

Case (ATACyber) View Tools EnScript Add Evidence

Home Evidence Results Search Bookmarks

Viewing (Search) Split Mode Condition Filter Searches

Index Tags Keywords

Selected 0/4

	Expression	Items	Hits
1	jpg_header		0
2	\xFF\xD8\xF...	1	21
3	skimmer		0
4	skimmer	120	2,055

Table Timeline

Selected 0/1

1 Unallocated Clusters

Fields Report Text Hex Decode Doc Transcript Picture Review Lock

Zoom In Zoom Out 100%

View Types

- Text
- Picture
- Picture
- Base64 Encoded Picture
- UUE Encoded Picture
- Integers
- Dates
- Windows



ATACyber\tepisan\MBP-500GB\E\Unallocated Clusters (FO 4473414 LE 4)

Decode and View Results  
Decode Tab,  
Choose Picture Type

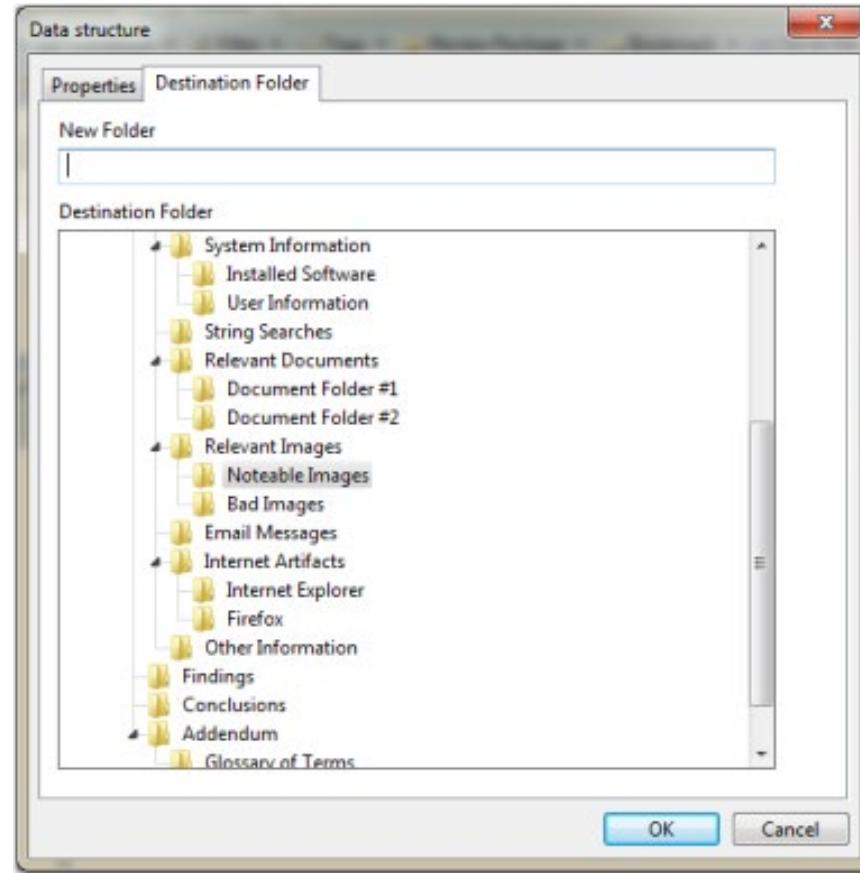
**Bookmark the Results,  
Right-click the Picture,  
Bookmark it as Data Structure**

-  Note...
- 
-  Single item... Ctrl-B
-  Selected items... Ctrl-Shift-B
-  Folder...
- 
-  Table view...
-  Raw text...
-  Data structure... Ctrl-B
- 
-  Transcript text...

-  Zoom In Ctrl-Num +
-  Zoom Out Ctrl-Num -
-  100% Enter
- 
-  Open...
-  Copy Ctrl-C
-  Save As...
- 
-  Save Results...
-  Bookmark
-  Go to file
-  Find Related

# Select the Destination

- ◎ Go to the Data Structure menu destination tab
- ◎ Under Relevant Images, choose Notable Images



EnCase Forensic

Case (ATACyber) View Tools EnScript Add Evidence

Home Reports Evidence Results Search Bookmarks

Examination Report

Go to template Go to bookmark Edit bookmark Zoom In Zoom Out 100%

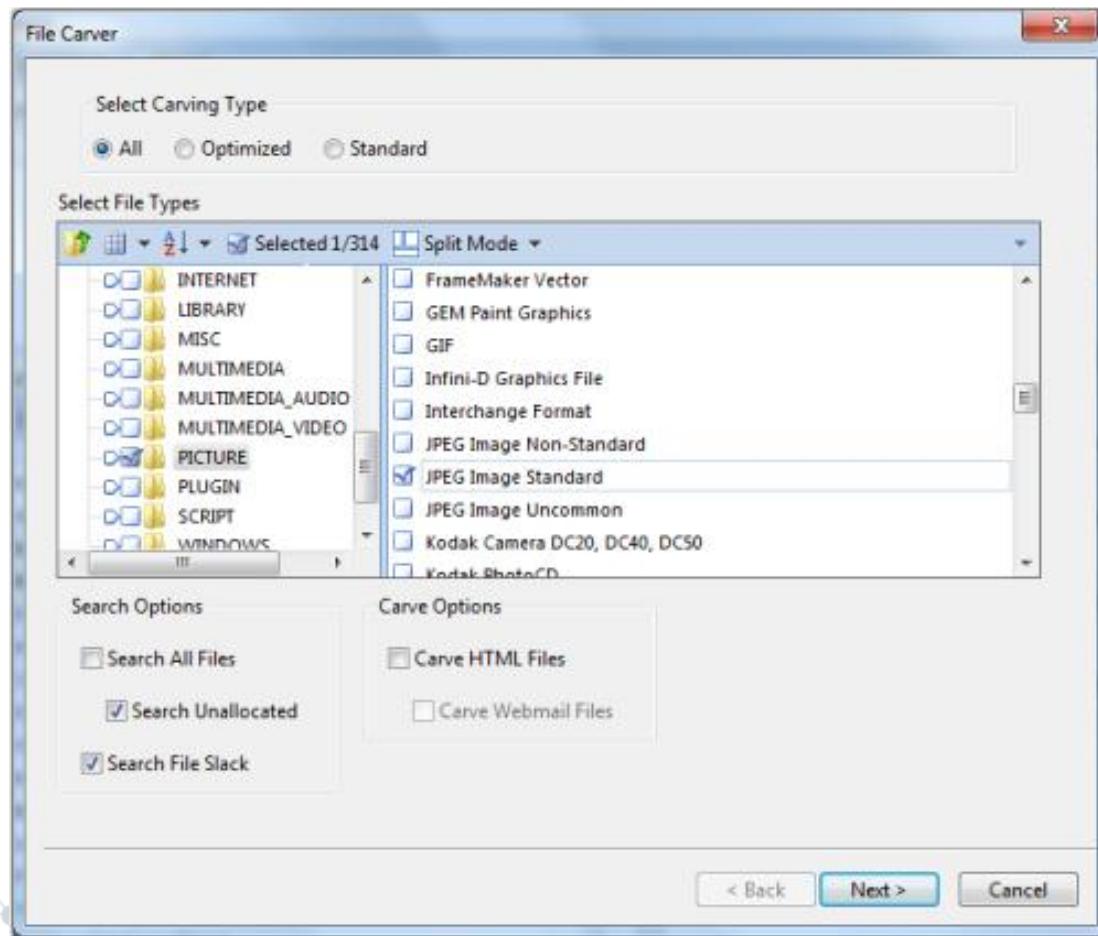
- ⊕ Digital Movies  
Computer generated animation or "digital movies" come in various standard formats, such as MOV and AVI files.
- ⊕ Relevant Images  
The following images were discovered during the examination and are potentially relevant to this case.
- 1] Unallocated Clusters

ATACyber\episang\MBP-500GB\Unallocated Clusters (FO 4473414 LE 4)

# View the Report

# Automated File Carver

- ◎ Easier than the manual method
- ◎ Select options, click OK, and view the results



# FTK

## Search Techniques

# FTK Searching Features

- ◎ **FTK supports:**
- **Indexed searches**
- **Raw searches, including regular expressions**
- **Data carving through its evidence processing feature set**
- **Unicode character sets**

AccessData Forensic Toolkit Version 1.00.02708 Standard - Search Case FTK Case View

File Edit View Evidence Filter Tools Manage Help

Filter - unfiltered Filter Manager...

Explore Overview Email Graphics Bookmarks Live Search Index Search Volume

Search Results

Index Terms Options

Indexed Words Total Hits Total Hits Options

File Content Options

File Content Properties Hex Interpreter

File List Display Time Zone: Eastern Daylight Time (From local machine)

File List Options

File List Options

Used 0 Filtered 0 Total 1 Highlighted 1 Checked 1 Total Used 0

Index Search Tab Filter: [None]

# FTK Index Searching

File Edit View Evidence Filter Tools Manage Help

Digitized by srujanika@gmail.com

1 / 1



Explore Overview Find Graphs Bookmarks Live Search Index Search Help

Text Editor Help

1

100% User-Defined Fields

**Sample Name**      **Type**      **Order Ref#**

Price/Hip/Pair Filter:  Search Filter:

File Content

Worlde | Fazit | Planen | Testen

File Content Properties File Interpreter

10

File Edit View Insert Tools Window Help

- Docker Time Zone: Eastern Daylight Time - (From local machine)

Index	Page	Line	Text	Ex.	Text	Category	Page	Line	Text	Ex.	Text	Category	Page
-------	------	------	------	-----	------	----------	------	------	------	-----	------	----------	------

Digitized by srujanika@gmail.com

Digitized by srujanika@gmail.com

[Logout](#)

1

10

Trunk 8

1

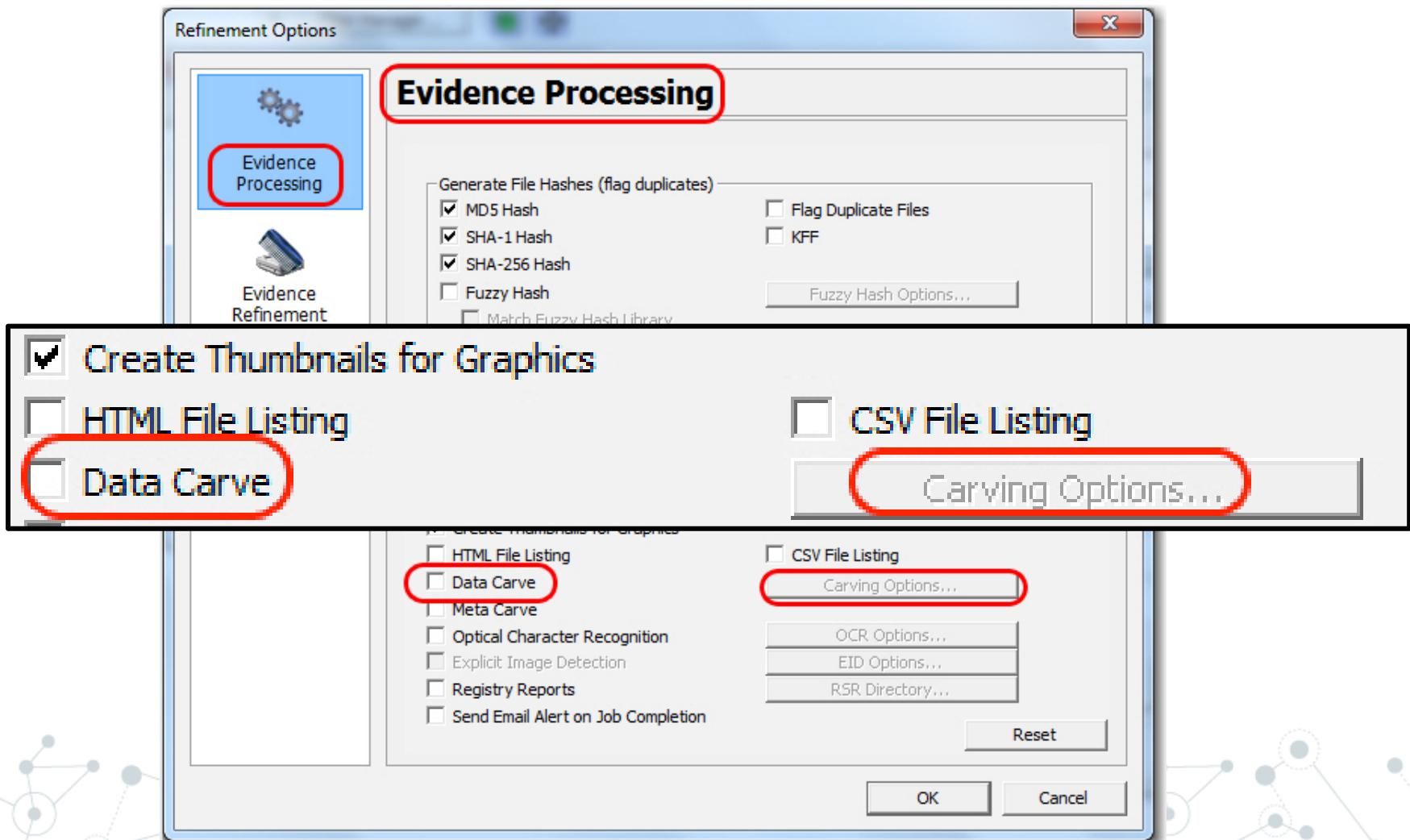
Digitized

Table 1

1

| Use Search Tab Filter: [None]

## FTK Data Carving Feature

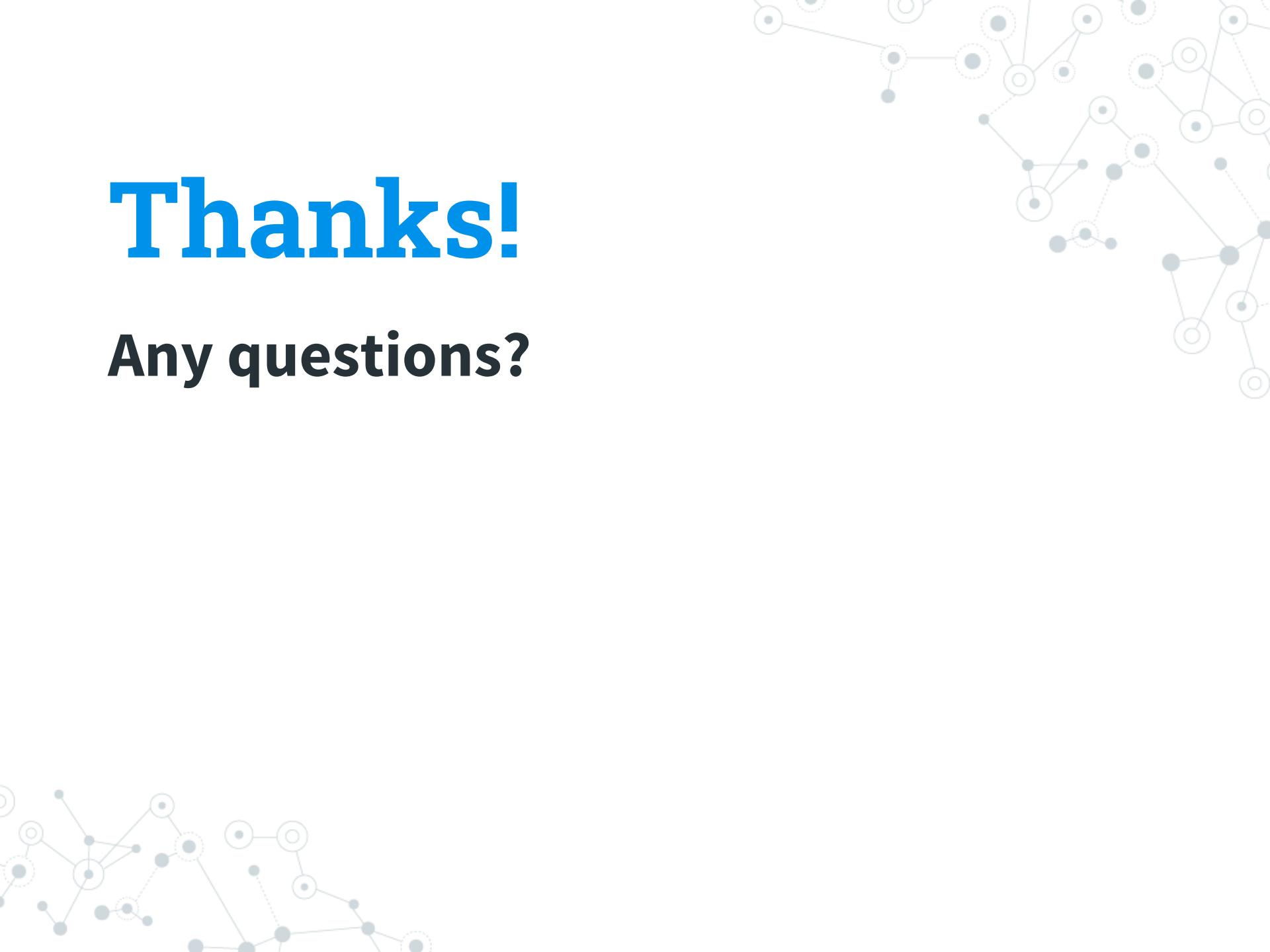


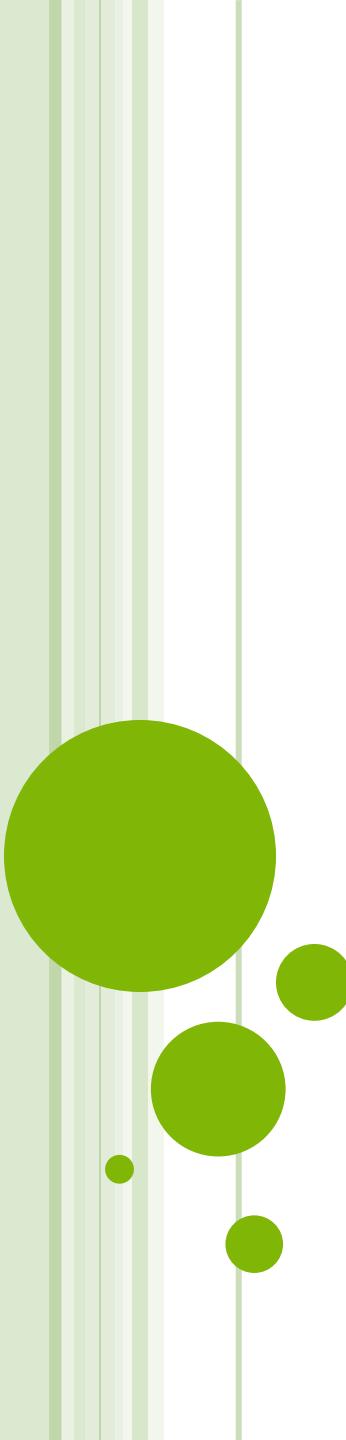
# Summary

- ⦿ You should now be familiar with:
  - ⦿ Storage and search of ASCII and Unicode text
  - ⦿ Types of keyword searches
  - ⦿ Index, live or raw keyword, and GREP searches
  - ⦿ Data carving based on file signatures
  - ⦿ Foreign language views and searches

# Thanks!

Any questions?





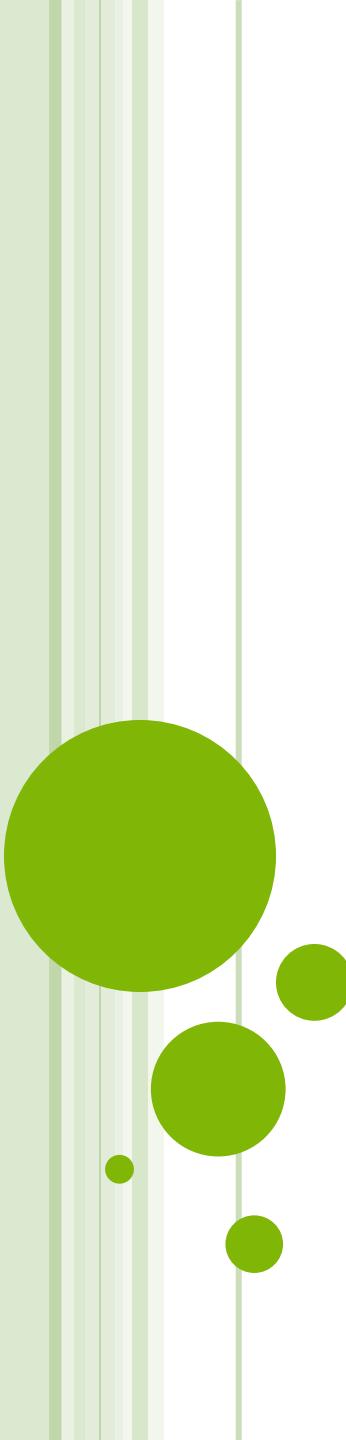
# WINDOWS ARTIFACTS FORENSIC

## OBJECTIVE

---

- By the end of this module, participants will be able to analyze artifacts common to windows 7 operating system.





## WHAT IS AN OPERATING SYSTEM ?

# WHAT IS AN OPERATING SYSTEM?

---



- The largest and most important application
- An interface between applications, hardware, and users
- Support for many hardware configurations



# WINDOWS OPERATING SYSTEM

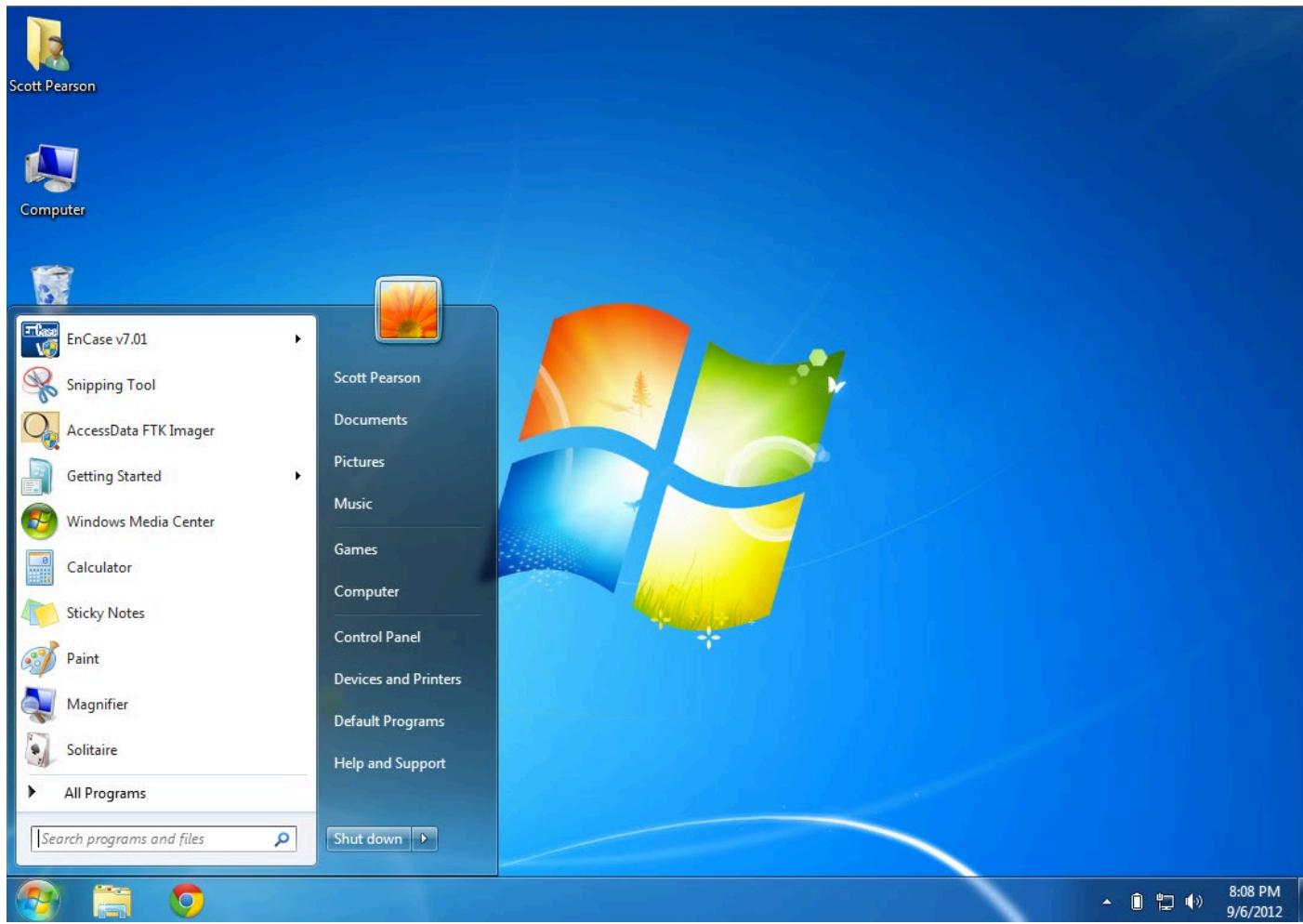
---



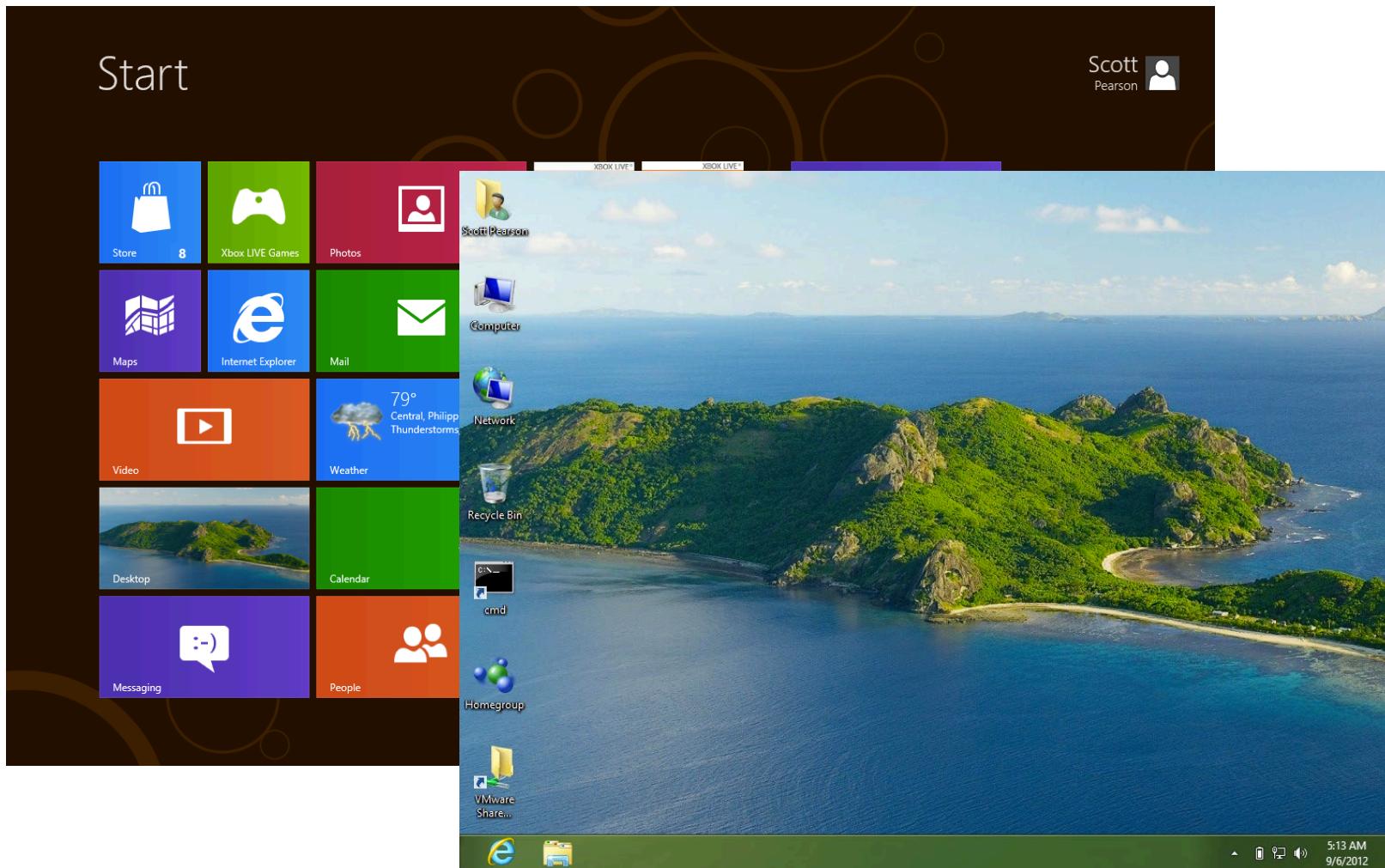
- Microsoft Windows is the most prevalent and widely used operating system
- Examiners must be aware of how Windows is used and where pertinent artifacts could be stored

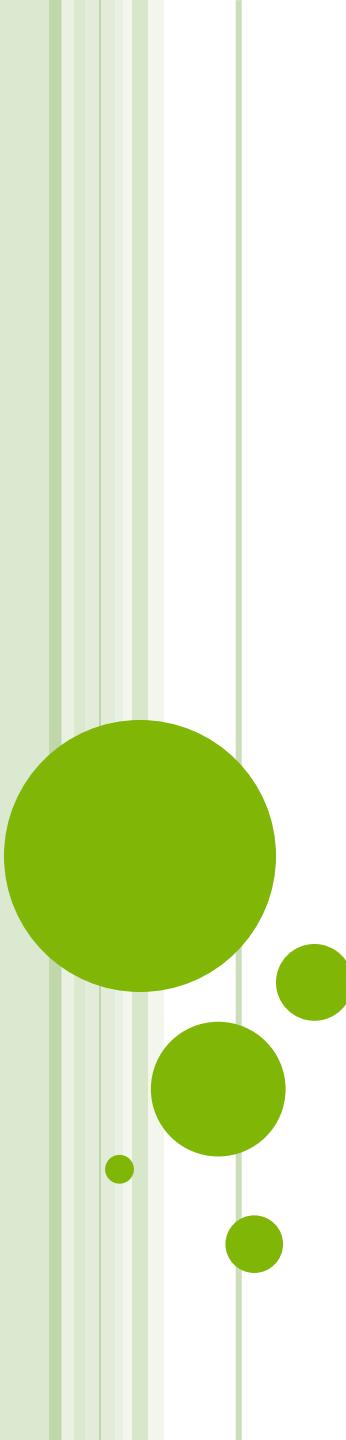


# WINDOWS 7 DESKTOP



# WINDOWS 8 DESKTOP





## COMMON WINDOWS ARTIFACTS

# WINDOWS EVENT LOGS

---



- An event is a notable incident that generates a log entry or user notification
- An event log:
  - Is a collection of events categorized by function
  - Provides a historical reference

C:/Windows/System32/Winevt/Logs



# WINDOWS EVENT LOGS

The screenshot shows the Windows Event Viewer interface. On the left, the navigation pane displays 'Event Viewer (Local)', 'Custom Views', 'Windows Logs' (with 'Application' selected), 'Security', 'Setup', 'System', 'Forwarded Events', 'Applications and Services', and 'Subscriptions'. The main area, titled 'Application 1,766 Events', lists events with columns for Level, Date and Time, Source, Event ID, and Task Category. An event from 'Application Error' on 02-08-2010 at 14:33:49 is highlighted. The details pane for this event shows the error message: 'Faulting application ALMon.exe, version 3.31.87.216, time stamp 0x4aa0f806, faulting module RPCRT4.dll, version 6.0.6002.18024, time stamp 0x49f05bcc, exception code 0xc0000005, fault offset 0x000b21c1, process id 0xc64, application start time 0x01cb327747846643.' Below this, the event properties are listed: Log Name: Application, Source: Application Error, Event ID: 1000, Level: Error, User: N/A, OpCode: , Logged: 02-08-2010 14:33:49, Task Category: (100), Keywords: Classic, Computer: 2ua7180d9q.hou150.che. The right-hand Actions pane includes options like Open Saved Log..., Create Custom View..., Import Custom View..., Clear Log..., Filter Current Log..., Properties, Find..., Save Events As..., Attach a Task To this Log..., View, Refresh, Help, Event Properties, Attach Task To This Event..., Copy, Save Selected Events..., Refresh, and Help.

From Event viewer expand the "Windows logs" and select System or Application to view the system or Application error. It will show the details of the error and by selecting the error will show the complete details of the error in the right side bottom screen, even you can check the online help by selecting the "Event Log Online Help"

Level	Date and Time	Source	Event ID	Task Categ...
Information	02-08-2010 14:34:03	MsiInstaller	1042	None
Information	02-08-2010 14:34:03	MsiInstaller	1035	None
Information	02-08-2010 14:34:03	MsiInstaller	11728	None
Error	02-08-2010 14:33:49	Application Error	1000	(100)
Information	02-08-2010 14:33:45	RestartManager	10001	None
Information	02-08-2010 14:33:47	MsiInstaller	1040	None

Event 1000, Application Error

General Details

Faulting application ALMon.exe, version 3.31.87.216, time stamp 0x4aa0f806, faulting module RPCRT4.dll, version 6.0.6002.18024, time stamp 0x49f05bcc, exception code 0xc0000005, fault offset 0x000b21c1, process id 0xc64, application start time 0x01cb327747846643.

Log Name: Application  
Source: Application Error  
Event ID: 1000  
Level: Error  
User: N/A  
OpCode:  
More Information: [Event Log Online Help](#)

Actions

- Application
- Open Saved Log...
- Create Custom View...
- Import Custom View...
- Clear Log...
- Filter Current Log...
- Properties
- Find...
- Save Events As...
- Attach a Task To this Log...
- View
- Refresh
- Help
- Event 1000, Application Error
- Event Properties
- Attach Task To This Event...
- Copy
- Save Selected Events...
- Refresh
- Help

# WINDOWS USER PROFILE

---

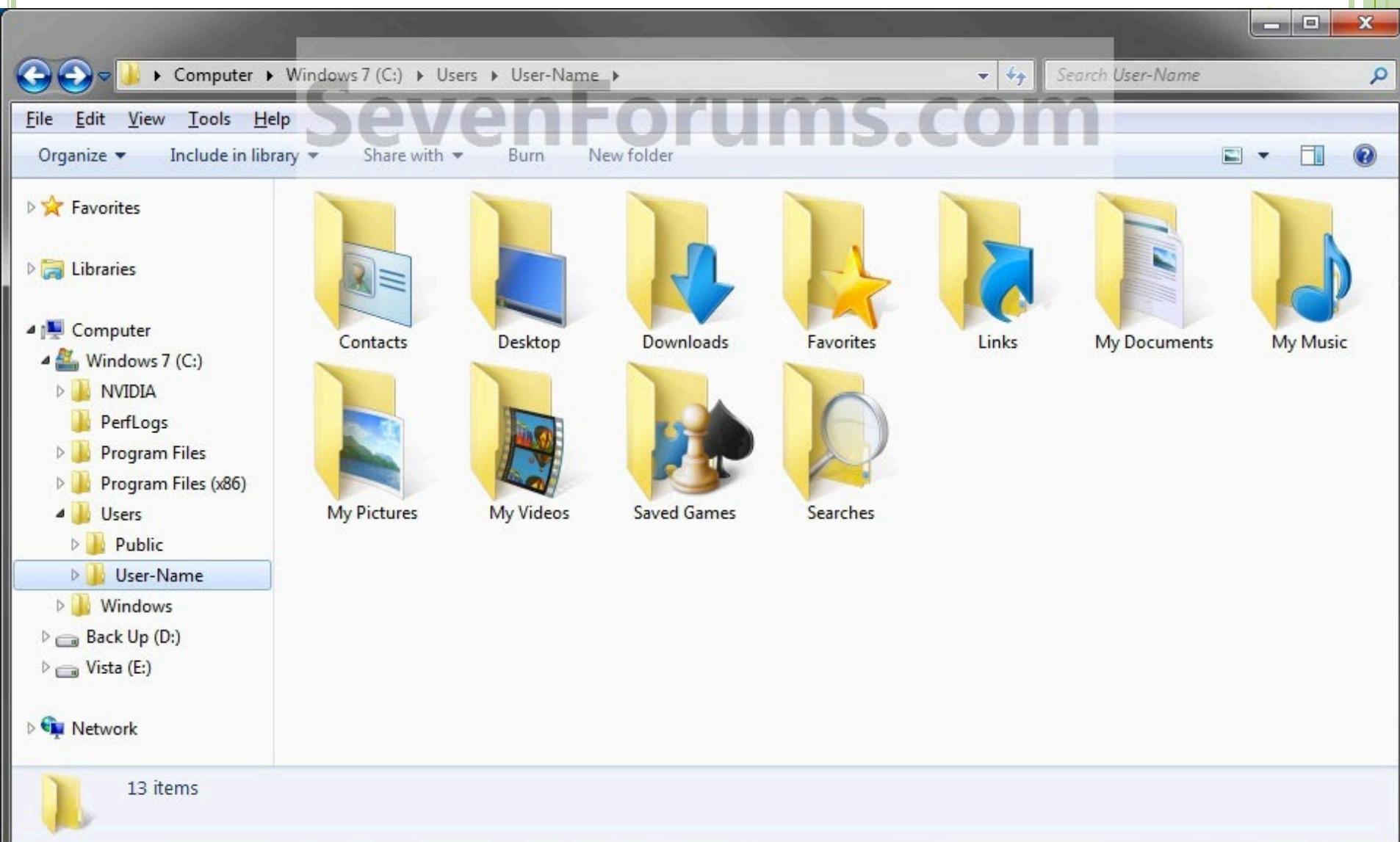


- The user profile is a default collection of folders to store user-generated data
- Every user with a Windows account has their own user profile

**Windows 7 location → C:\Users\<UserID>**



# WINDOWS USER PROFILE



# TEMPORARY INTERNET FILES

---

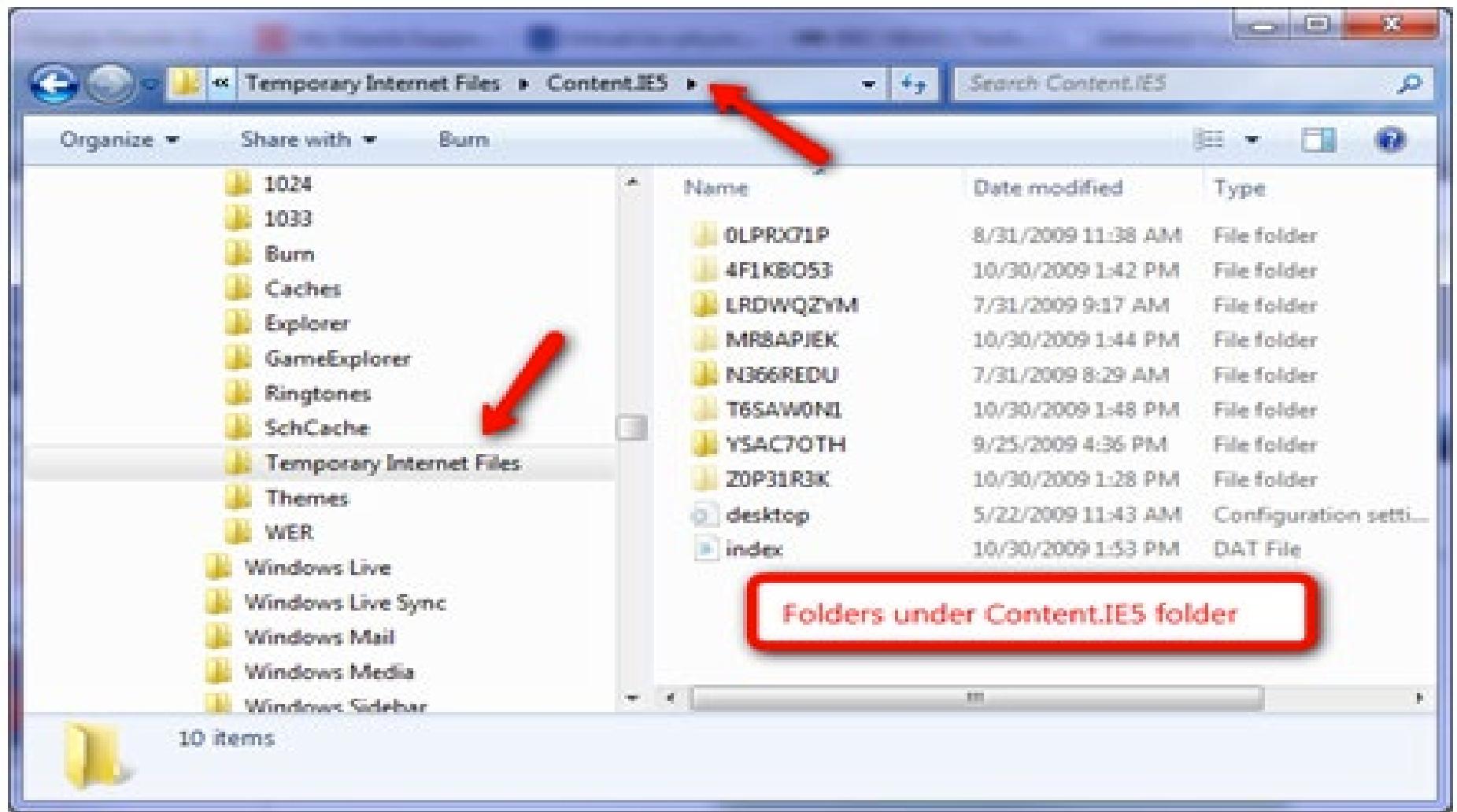


- Serves as the browser cache,
  - Cache pages and other multimedia content, such as video and audio files, from websites visited by the user.
- This allows websites to load more quickly the next time they are visited.

**%userprofile%\AppData\Local\Microsoft\Windows\Temporary Internet Files**



# TEMPORARY INTERNET FILES



# RECENT ITEMS FOLDER AND LINK FILES

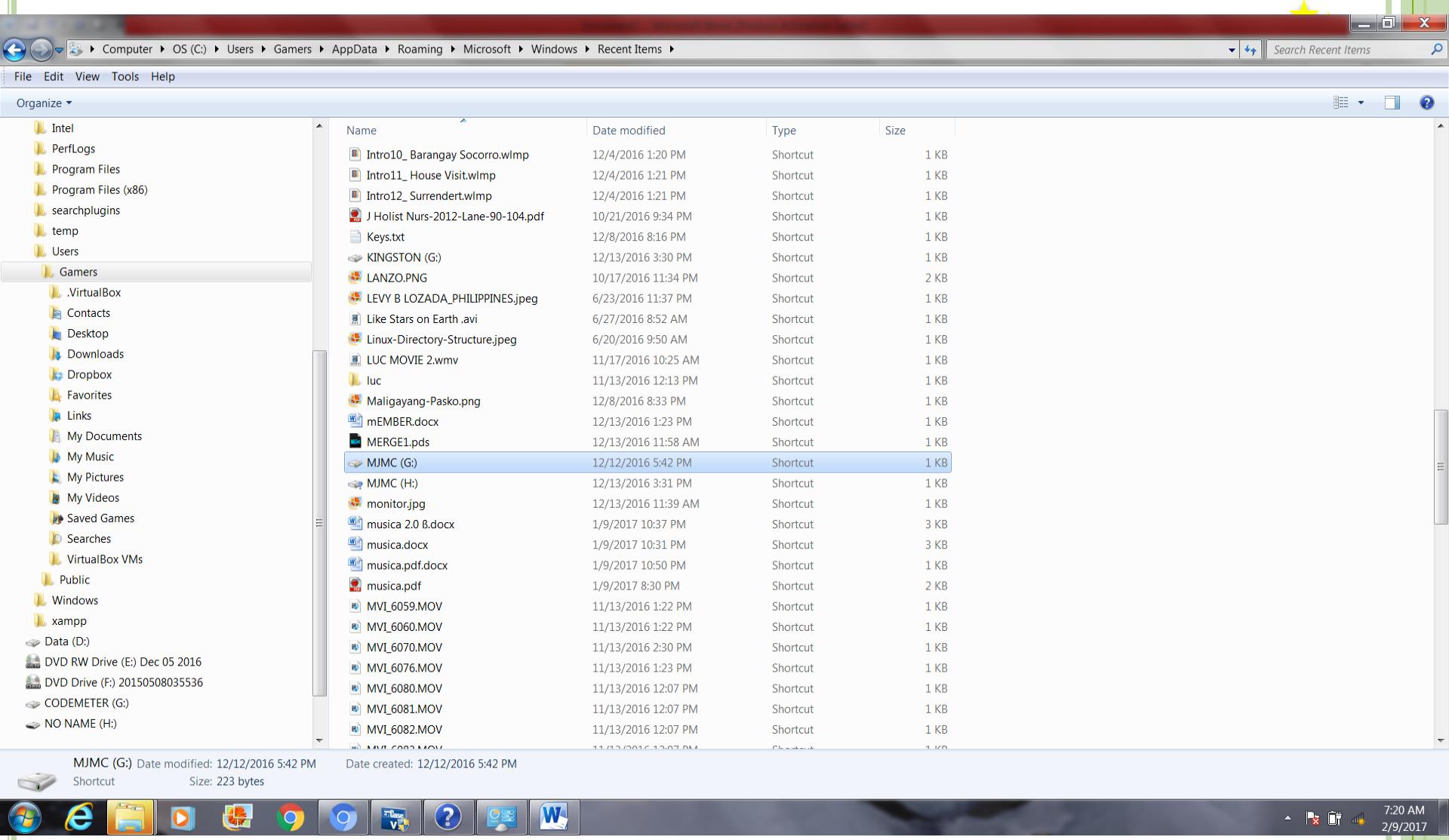
---



- **Recent Items:**
  - The Recent Items folder is used by Windows to record what documents have been opened.
- **Link Files:**
  - Is a shortcut to a file stored within the file system
  - Provides quick access to commonly used files
  - May contain valuable clues to the actual location and/or prior existence of files on the computer



# RECENT ITEMS FOLDER AND LINK FILES



# RECYCLE BIN

---



- Is temporary storage for deleted files
- Will not contain files deleted from devices with removable storage
- Is unique to every Windows user



\\$Recycle.Bin\%SID%,

- %SID% is the SID of the user that performed the deletion.



# RECYCLE BIN

---



- Recycle bin files can:
  - Be restored to their original file system location
  - Be emptied from the file system
  - Provide clues about files the user tried to remove



`\$Recycle.Bin\%SID%`,

- `%SID%` is the SID of the user that performed the deletion.



# RECYCLE BIN

Recycle Bin ▾ Search Recycle Bin

File Edit View Tools Help

Organize ▾ Empty the Recycle Bin Restore all items

Favorites

- Desktop
- Downloads
- Dropbox
- Recent Places

Libraries

- Documents
- Music
- Pictures
- Videos

Homegroup

Computer

- OS (C:)
- Data (D:)
- DVD RW Drive (E): Dec 05 2016
- DVD Drive (F): 20150508035536
- CODEMETER (G:)

Network

18CM-The-Avengers-2-Superman-V-font-b-Batman-b-font-Superhero-Action-Figure-font-b.jpg

- 59B.wmv
- 59B1.wmv
- 20161113\_113044.jpg
- Book1.xlsx
- bookreporttemplate(edit) (4) (1).docx
- EBP Appraisal Form.pdf
- EXTREMELY POWERFUL Pure Clean Positive Energy ↴ Reiki Zen Meditation Music ↴ Healing Music Therap... [Low, 360p].mp4
- Full Chakra Healing ~ Spa Music w Binaural Beats + Isochronic Tones (ZEN, REIKI) [Low, 360p].mp4
- GROUP 2
- IMG\_6056.JPG
- IMG\_6071.JPG
- MVL\_4528.MOV
- MVL\_4528.THM
- MVL\_4856.MOV
- MVL\_4856.THM
- MVI\_6062.MOV
- MVI\_6062.THM
- MVI\_6067.MOV
- MVI\_6067.THM
- MVI\_6082.MOV
- MVI\_6082.THM
- MVI\_6087.MOV
- MVI\_6087.THM
- PATIENT CARE AND HYGIENE.PNG
- PDG Bato Dela Rosa Explain how 'Oplan Tokhang' conducted by the PNP..mp4
- project tokhang.avi
- The Physical Examination Assessment \_ Module 5 \_ The Physical Examination Assessment \_ Nursing Studies - The Physical Examination \_ ALISON.p...
- tokhang
- winzip.exe

30 items

8:49 AM 2/9/2017

# INSTALLED APPLICATIONS

---



- Allow the users to interact with the computer system
- Generate specific types of output
- Leave unique footprints that can assist the examiner to understand how the system was used



# VOLUME SHADOW COPY

Computer > OS (C:) > Program Files >

File Edit View Tools Help

Organize ▾ Include in library ▾ Share with ▾ Burn New folder

Favorites

- Desktop
- Downloads
- Dropbox
- Recent Places

Libraries

- Documents
- Music
- Pictures
- Videos

Homegroup

Computer

- OS (C:)
  - 3DVisionVideoSample
  - AsusVibeData
  - Intel
  - PerfLogs
  - Program Files
    - Program Files (x86)
    - searchplugins
    - temp
  - Users
  - Windows
  - xampp
- Data (D:)
- DVD RW Drive (E) Dec 05 2016
- DVD Drive (F) 20150508035536
- CODEMETER (G:)

45 items

Name	Date modified	Type	Size
ASUS	1/4/2011 9:40 AM	File folder	
ATKGFNEX	11/9/2015 11:59 PM	File folder	
Bonjour	8/28/2016 5:04 PM	File folder	
Cellebrite Mobile Synchronization	4/9/2014 10:39 AM	File folder	
CodeMeter	4/22/2014 1:54 PM	File folder	
Common Files	12/12/2016 5:33 PM	File folder	
Creative	1/4/2011 9:42 AM	File folder	
CyberLink	12/12/2016 5:50 PM	File folder	
DIFX	4/9/2014 9:22 AM	File folder	
DVD Maker	9/5/2016 9:05 PM	File folder	
EnCase6.19.7	6/5/2014 9:13 AM	File folder	
EnCase7	2/9/2017 7:36 AM	File folder	
EnCase7.07	2/8/2017 10:41 PM	File folder	
EnCase7.10.05	2/8/2017 10:45 PM	File folder	
Epson Software	7/8/2013 10:32 AM	File folder	
Google	1/4/2011 9:16 AM	File folder	
HP	8/31/2016 10:09 PM	File folder	
Internet Explorer	5/29/2013 5:55 AM	File folder	
iPod	8/28/2016 5:08 PM	File folder	
iTunes	8/28/2016 5:08 PM	File folder	
Microsoft Games	7/14/2009 3:45 PM	File folder	
Microsoft Office	4/13/2013 11:37 A...	File folder	
Microsoft Silverlight	9/5/2016 8:41 PM	File folder	
MSBuild	7/14/2009 1:32 PM	File folder	
NewBlue	12/12/2016 5:51 PM	File folder	
NVIDIA Corporation	1/4/2011 9:33 AM	File folder	
Oracle	11/27/2013 3:06 PM	File folder	
P4G	1/4/2011 9:39 AM	File folder	
proDAD	12/12/2016 5:50 PM	File folder	

Search Program Files

8:45 AM 2/9/2017

# VOLUME SHADOW SERVICE (VSS)

---



- Creates a snapshot image of application data on a volume
- Enables reliable backups even while the system is actively running
- Enables examiners to access previous versions of files



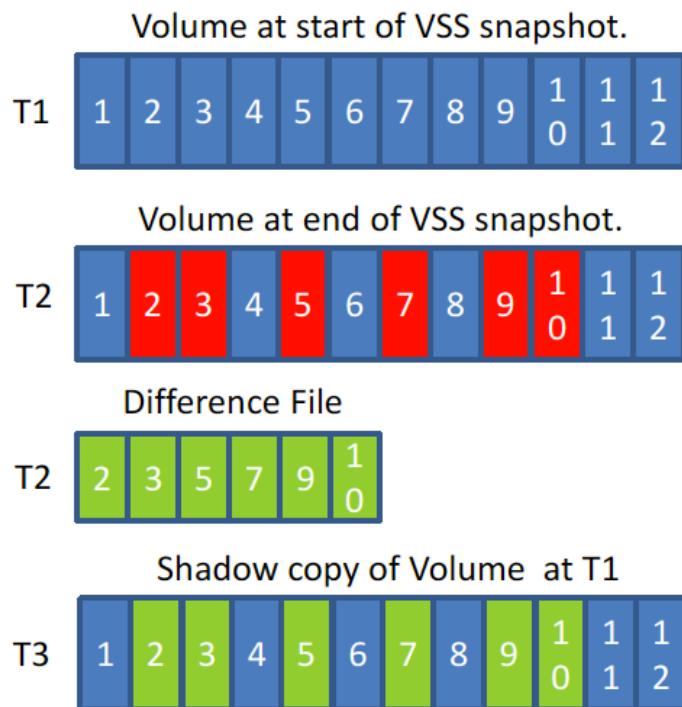
# VOLUME SHADOW COPY

---

- Volume shadow copies are bit level differential backups of a volume.
  - -16 KB blocks.
  - -Copy on write.
  - -Volume Shadow copy files are “difference” files.



# VOLUME SHADOW COPY



- ***Copy on Write:*** Before a block is written to, it is saved to the difference file.
- When a Shadow Copy is read, the “volume” consists of the live, unchanged blocks, and the saved blocks from the difference file.



# VOLUME SHADOW COPY

Computer > OS (C:) > Users > Gamers >

File Edit View Tools Help

Organize Open Include in library Share with Burn New folder

Favorites

- Desktop
- Downloads
- Dropbox
- Recent Places

Libraries

- Documents
- Music
- Pictures
- Videos

Homegroup

Computer

- OS (C:)
- 3DVisionVideoSample
- AsusVibeData
- Intel
- PerfLogs
- Program Files
- Program Files (x86)
- searchplugins
- temp
- Users
- Windows
- xampp

Data (D:)

- DVD RW Drive (E) Dec 05 2016
- DVD Drive (F) 20150508035536

Desktop Date modified: 2/8/2017 11:20 PM

File folder

Name Date modified Type Size

.VirtualBox	8/29/2016 10:01 AM	File folder	
Contacts	9/5/2016 9:22 PM	File folder	
Desktop	2/8/2017 11:20 PM	File folder	
Downloads	12/12/2016 7:01 PM	File folder	
Dropbox	9/12/2016 12:12 PM	File folder	
Favorites	9/5/2016 9:22 PM	File folder	
Links	9/5/2016 9:22 PM	File folder	
My Documents	1/9/2017 10:51 PM	File folder	
My Music	9/5/2016 9:22 PM	File folder	
My Pictures	9/5/2016 9:22 PM	File folder	
My Videos	11/17/2016 10:44 AM	File folder	
Saved Games	9/5/2016 9:22 PM	File folder	
Searches	9/5/2016 9:22 PM	File folder	
VirtualBox VMs	9/30/2014 8:18 AM	File folder	

Desktop Properties

General Sharing Security Location Previous Versions

Previous versions come from restore points or from Windows Backup. [How do I use previous versions?](#)

Folder versions:

Name	Date modified
Today (2)	
Desktop	2/9/2017 9:30 AM
Desktop	2/9/2017 9:18 AM
Yesterday (2)	
Desktop	2/8/2017 11:15 PM
Desktop	2/8/2017 11:14 PM

Open Copy... Restore... OK Cancel Apply

9:33 AM 2/9/2017

# VOLUME SHADOW COPY

EnCase Forensic

Case (WinArtifacts) View Tools EnScript Add Evidence

Home Evidence

Viewing (Entry) Split Mode Condition Filter Review Package Raw Search Selected Bookmark Go to file Find Related Entries Acquire Process Device Open With

Selected 2/500002

	Name	File Ext	File Created	Logical Size	Tag	Category
<input type="checkbox"/> 1	SPP		04/12/13 07:12:36 AM	4,096		Folder
<input type="checkbox"/> 2	MountPointManagerRemoteDatabase		04/12/13 01:48:40 PM	0		Unknown
<input type="checkbox"/> 3	tracking.log	log	04/12/13 01:50:42 PM	30,720		Application Data
<input type="checkbox"/> 4	Syscache.hve	hve	04/12/13 01:50:46 PM	19,136,512		None
<input type="checkbox"/> 5	Syscache.hve.LOG1	LOG1	04/12/13 01:50:46 PM	262,144		None
<input type="checkbox"/> 6	Syscache.hve.LOG2	LOG2	04/12/13 01:50:46 PM	0		None
<input type="checkbox"/> 7	Windows Backup		06/10/14 02:29:51 PM	152		Folder
<input type="checkbox"/> 8	WindowsImageBackup		07/23/15 11:20:52 AM	272		Folder
<input type="checkbox"/> 9	{9868ad38-6cf3-11e6-a264-0025d3ae8c1e}\{3808876b-c176-4e48-b7ae-04046e6cc752}		08/29/16 10:37:17 AM	1,912,602,624		Unknown
<input type="checkbox"/> 10	\{3808876b-c176-4e48-b7ae-04046e6cc752\}		08/29/16 10:37:17 AM	65,536		Unknown
<input type="checkbox"/> 11	\{3808876b-c176-4e48-b7ae-04046e6cc752\}		02/08/17 11:14:36 PM	65,536		Unknown
<input type="checkbox"/> 12	\{d6de7e48-ee04-11e6-879a-0025d3ae8c1e\}\{3808876b-c176-4e48-b7ae-04046e6cc752\}		02/08/17 11:14:36 PM	40,353,792		Unknown
<input type="checkbox"/> 13	\{d6de7e4d-ee04-11e6-879a-0025d3ae8c1e\}\{3808876b-c176-4e48-b7ae-04046e6cc752\}		02/08/17 11:15:14 PM	218,447,872		Unknown
<input checked="" type="checkbox"/> 14	\{d6de7e89-ee04-11e6-879a-0025d3ae8c1e\}\{3808876b-c176-4e48-b7ae-04046e6cc752\}		02/09/17 09:18:55 AM	153,927,680		Unknown
<input checked="" type="checkbox"/> 15	\{acbb4667-eee6-11e6-ab82-485b39118403\}\{3808876b-c176-4e48-b7ae-04046e6cc752\}		02/09/17 09:30:38 AM	369,098,752		Unknown

Fields Report Text Hex Decode Doc Transcript Picture Console File Extents Permissions Hash Sets Attributes Lock

Name	Value
s Name	\{d6de7e89-ee04-11e6-879a-0025d3ae8c1e\}\{3808876b-c176-4e48-b7ae-04046e6cc752\}
s Tag	
s File Ext	
i Logical Size	153,927,680
i Category	Unknown
i Signature Analysis	
s File Type	
s Protected	
i Protection complexity	

WinArtifacts\0\Device\Volume Information\{d6de7e89-ee04-11e6-879a-0025d3ae8c1e\}\{3808876b-c176-4e48-b7ae-04046e6cc752

9:39 AM 2/9/2017

# WINDOWS PREFETCH

---



- Boosts performance by preloading data into RAM based on cache history
- Provides clues about frequently-used applications and when they were last used

Location = C:\Windows\Prefetch  
.PF extension

NTOSBOOT-B00DFAAD.PF



# WINDOWS PREFETCH

Computer > OS (C:) > Windows > Prefetch >

File Edit View Tools Help

Organize Open Burn New folder

inf L2Schemas LiveKernelReports Log Logs Media Microsoft.NET Migration Minidump ModemLogs Offline Web Pages Panther PCHEALTH Performance PLA PolicyDefinitions Prefetch pss pt-PT Registration rescache Resources SchCache schemas security ServiceProfiles servicing Setup ShellNew SoftwareDistribution Speech

Name	Date modified	Type	Size
NTOSBOOT-B00DFAAD(pf)	2/8/2017 9:46 PM	PF File	4,501 KB
OSPPSVC.EXE-E53D3CC0.pf	2/9/2017 10:17 AM	PF File	58 KB
PfSvPerfStats.bin	2/9/2017 9:28 AM	PF File	1 KB
PRESENTATIONFONTCACHE.EXE-73BEC...	2/9/2017 9:29 AM	PF File	61 KB
REGEDIT.EXE-90FEEA06.pf	2/9/2017 9:28 AM	PF File	26 KB
RICHVIDEO.EXE-CF2CB9D7.pf	2/9/2017 9:28 AM	PF File	17 KB
RICHVIDEO64.EXE-AD5B2CEE.pf	2/9/2017 9:28 AM	PF File	13 KB
RSTRUI.EXE-2D50C58D.pf	2/9/2017 9:28 AM	PF File	47 KB
RUNDLL32.EXE-84EA5F2A.pf	12/12/2016 5:21 PM	PF File	0 KB
RUNDLL32.EXE-DE9673F9.pf	2/9/2017 9:27 AM	PF File	11 KB
SDCLT.EXE-E10B972A.pf	2/9/2017 9:14 AM	PF File	39 KB
SEARCHFILTERHOST.EXE-77482212.pf	2/9/2017 10:16 AM	PF File	17 KB
SEARCHPROTOCOLHOST.EXE-0CB8CADE...	2/9/2017 10:15 AM	PF File	15 KB
SETUP.EXE-84C9614B.pf	12/12/2016 5:21 PM	PF File	0 KB
SMARTLOGON.EXE-8F794AF5.pf	2/9/2017 6:20 AM	PF File	33 KB
SPLWOW64.EXE-297C4568.pf	2/9/2017 10:10 AM	PF File	23 KB
SPPSVC.EXE-B0F8131B.pf	2/9/2017 9:28 AM	PF File	54 KB
SVCHOST.EXE-05F624AB.pf	2/9/2017 9:29 AM	PF File	11 KB
SVCHOST.EXE-7AC6742A.pf	2/9/2017 9:07 AM	PF File	17 KB
SVCHOST.EXE-7CFEDEA3.pf	2/9/2017 9:28 AM	PF File	18 KB
SVCHOST.EXE-80F4A784.pf	2/9/2017 8:49 AM	PF File	20 KB
SVCHOST.EXE-E2C2633A.pf	2/9/2017 10:07 AM	PF File	24 KB
SYSTEMPROPERTIESADVANCED.EXE-68C...	2/9/2017 9:28 AM	PF File	33 KB
SYSTEMPROPERTIESPROTECTION.EX-64B...	2/9/2017 9:18 AM	PF File	52 KB
TASKENG.EXE-48D4E289.pf	2/9/2017 10:13 AM	PF File	21 KB
TASKHOST.EXE-7238F31D.pf	2/9/2017 10:12 AM	PF File	58 KB
TASKSCHEDULER.EXE-C2198582.pf	12/12/2016 5:22 PM	PF File	0 KB
TRUSTEDINSTALLER.FXE-3CC531E5.nf	2/9/2017 9:15 AM	PF File	313 KB

NTOSBOOT-B00DFAAD(pf) Date modified: 2/8/2017 9:46 PM  
PF File Date created: 4/11/2013 10:51 PM Size: 4.39 MB

10:23 AM 2/9/2017

# WINDOWS REGISTRY

---



- Is a database of operating system, installed application, and user configuration settings
- Provides valuable clues about how the computer system was used since installation time

**The location of these registry hives are as follows:**

- \* HKEY\_LOCAL\_MACHINE \SYSTEM : \system32\config\system<sup>[1]</sup>HKEY\_LOCAL\_MACHINE \SAM : \system32\config\sam<sup>[1]</sup>HKEY\_LOCAL\_MACHINE \SECURITY : \system32\config\security<sup>[1]</sup>HKEY\_LOCAL\_MACHINE \SOFTWARE : \system32\config\software<sup>[1]</sup>
- \* HKEY\_USERS \UserProfile : \winnt\profiles\username<sup>[1]</sup>HKEY\_USERS.DEFAULT : \system32\config\default



# WINDOWS REGISTRY

The screenshot shows a Windows File Explorer window with the following details:

**Path:** Computer > OS (C:) > Windows > System32 > config

**File Explorer Options:** File, Edit, View, Tools, Help, Organize, Open, Burn, New folder.

**Search Bar:** Search config

**Table Headers:** Name, Date modified, Type, Size

**Table Data:**

Name	Date modified	Type	Size
Journal	7/14/2009 10:34 A...	File folder	
RegBack	2/8/2017 10:17 PM	File folder	
systemprofile	7/29/2009 1:04 PM	File folder	
TxR	7/1/2013 1:26 PM	File folder	
BCD-Template	7/29/2009 2:03 PM	File	28 KB
COMPONENTS	2/9/2017 9:37 AM	File	105,984 KB
DEFAULT	2/9/2017 9:30 AM	File	512 KB
SAM	2/9/2017 9:26 AM	File	256 KB
SECURITY	2/9/2017 9:26 AM	File	256 KB
SOFTWARE	2/9/2017 9:41 AM	File	75,520 KB
SYSTEM	2/9/2017 10:00 AM	File	36,608 KB

**Status Bar:** 4 items selected Date modified: 2/9/2017 9:26 AM Date created: 7/14/2009 10:34 AM Size: 110 MB

**Taskbar:** Icons for File Explorer, Internet Explorer, File Manager, Media Player, Google Chrome, Microsoft Edge, and File Explorer.

**System Tray:** Icons for Network, Battery, Volume, and Date/Time (10:09 AM, 2/9/2017).

# WINDOWS REGISTRY

Registry Editor

File Edit View Favorites Help

Computer

- ▷ HKEY\_CLASSES\_ROOT
- ▷ HKEY\_CURRENT\_USER
- ▷ HKEY\_LOCAL\_MACHINE
  - ▷ BCD00000000
  - ▷ HARDWARE
  - ▷ SAM
  - ▷ SECURITY
  - ▷ SOFTWARE
  - ▷ SYSTEM
- ▷ HKEY\_USERS
  - ▷ .DEFAULT
  - ▷ S-1-5-18
  - ▷ S-1-5-19
  - ▷ S-1-5-20
  - ▷ S-1-5-21-4256024279-3213672507-2442315628-1000
  - ▷ S-1-5-21-4256024279-3213672507-2442315628-1000\_Classes
- ▷ HKEY\_CURRENT\_CONFIG

Name	Type	Data
ab (Default)	REG_SZ	(value not set)

Computer\HKEY\_LOCAL\_MACHINE\SYSTEM

10:20 AM  
2/9/2017

# WINDOWS REGISTRY

EnCase Forensic

Case (WinArtifacts) View Tools EnScript Add Evidence

Home Evidence

Viewing (Entry) Split Mode Condition Filter Review Package Raw Search Selected Bookmark Go to file Find Related Entries Acquire Process Device Open With

Selected 6/500002

	Name	File Ext	File Created	Logical Size	Tag	Category	Signature Analysis
1	SYSTEM		07/14/09 10:34:08 AM	37,486,592	Unknown		
2	SECURITY		07/14/09 10:34:08 AM	262,144	Unknown		
3	SAM		07/14/09 10:34:08 AM	262,144	Unknown		
4	SOFTWARE		07/14/09 10:34:08 AM	77,332,480	Unknown		
5	COMPONENTS(acbb4651-ee66-11e6-ab82-485b39118403).TM.blf	blf	02/09/17 09:27:08 AM	65,536	None		
6	COMPONENTS(acbb4651-ee66-11e6-ab82-485b39118403).TMContainer000000000000...regtrans-ms		02/09/17 09:27:08 AM	524,288	None		
7	COMPONENTS(acbb4651-ee66-11e6-ab82-485b39118403).TMContainer000000000000...regtrans-ms		02/09/17 09:27:08 AM	524,288	None		
8	COMPONENTS(acbb4650-ee66-11e6-ab82-485b39118403).TxR.blf	blf	02/09/17 09:27:09 AM	65,536	None		
9	COMPONENTS(acbb4650-ee66-11e6-ab82-485b39118403).TxR.0.regtrans-ms	regtrans-ms	02/09/17 09:27:09 AM	1,048,576	None		
10	COMPONENTS(acbb4650-ee66-11e6-ab82-485b39118403).TxR.1.regtrans-ms	regtrans-ms	02/09/17 09:27:09 AM	1,048,576	None		
11	COMPONENTS(acbb4650-ee66-11e6-ab82-485b39118403).TxR.2.regtrans-ms	regtrans-ms	02/09/17 09:27:09 AM	1,048,576	None		
12	BCD-Template		07/14/09 01:32:39 PM	28,672	Unknown		
13	BCD-Template.LOG	LOG	07/14/09 01:38:35 PM	25,600	Application Data		
14	COMPONENTS		07/14/09 10:34:08 AM	108,527,616	Unknown		
15	COMPONENTS.LOG	LOG	07/14/09 03:12:16 PM	1,024	Application Data		
16	COMPONENTS.LOG1	LOG1	07/14/09 10:34:08 AM	262,144	None		
17	COMPONENTS(016888b9-6c6f-11de-8d1d-001e0bcd3ec).TM.blf	blf	07/14/09 12:54:56 PM	65,536	None		
18	TxR		07/14/09 11:20:10 AM	4,096	Folder		
19	DEFAULT		07/14/09 10:24:00 AM	524,288	Unknown		

Fields Report Text Hex Decode Doc Transcript Picture Console File Extents Permissions Hash Sets Attributes Lock

Name	Value
s Name	SOFTWARE
s Tag	
s File Ext	
i Logical Size	77,332,480
i Category	Unknown
i Signature Analysis	
s File Type	
s Protected	
i Protection complexity	
Last Accessed	02/09/17 09:25:25 AM
File Created	07/14/09 10:34:08 AM
Last Written	02/09/17 09:35:45 AM
b Is Picture	NO
b Is Indexed	NO

WinArtifacts(0)\Windows\System32\config\SOFTWARE Creating cache files

10:44 AM 2/9/2017

END

---



Thank you  
and  
Good day ...



# Email Artifacts

## Objective

◎ By the end of this module, participants will be able to search emails using industry-standard tools for forensic investigations



# Introduction to Email

- ◎ Internet-based applications have changed how people communicate
- ◎ Traditional communication methods have been enhanced
  - Contact anyone at anytime, anywhere in the world – in real time
  - Instant sharing of files

# What Is Email?

- ◎ Internet-based application enabling users to send and receive messages with guaranteed delivery
- ◎ Messages can be accessed from many devices
  - Cell phones
  - Tablets
  - Computer systems



# Client-Based Versus Web-Based Email

Client-Based	Web-Based
<ul style="list-style-type: none"><li>• Installed by the Operating System</li><li>• Configured according to the user's preferences and server settings</li></ul>	<ul style="list-style-type: none"><li>• Are typically accessed via an Internet browser</li><li>• Store user content on a remote server</li></ul>

# How Does Email Work?

- ◎ Messages are sent and received over the Internet to an email address using specific network protocols
- ◎ Delivery to recipient is guaranteed



# Host and Domain

## Host:

- A member given access to use network resources

[mmouse@gmail.com](mailto:mmouse@gmail.com)

## Domain:

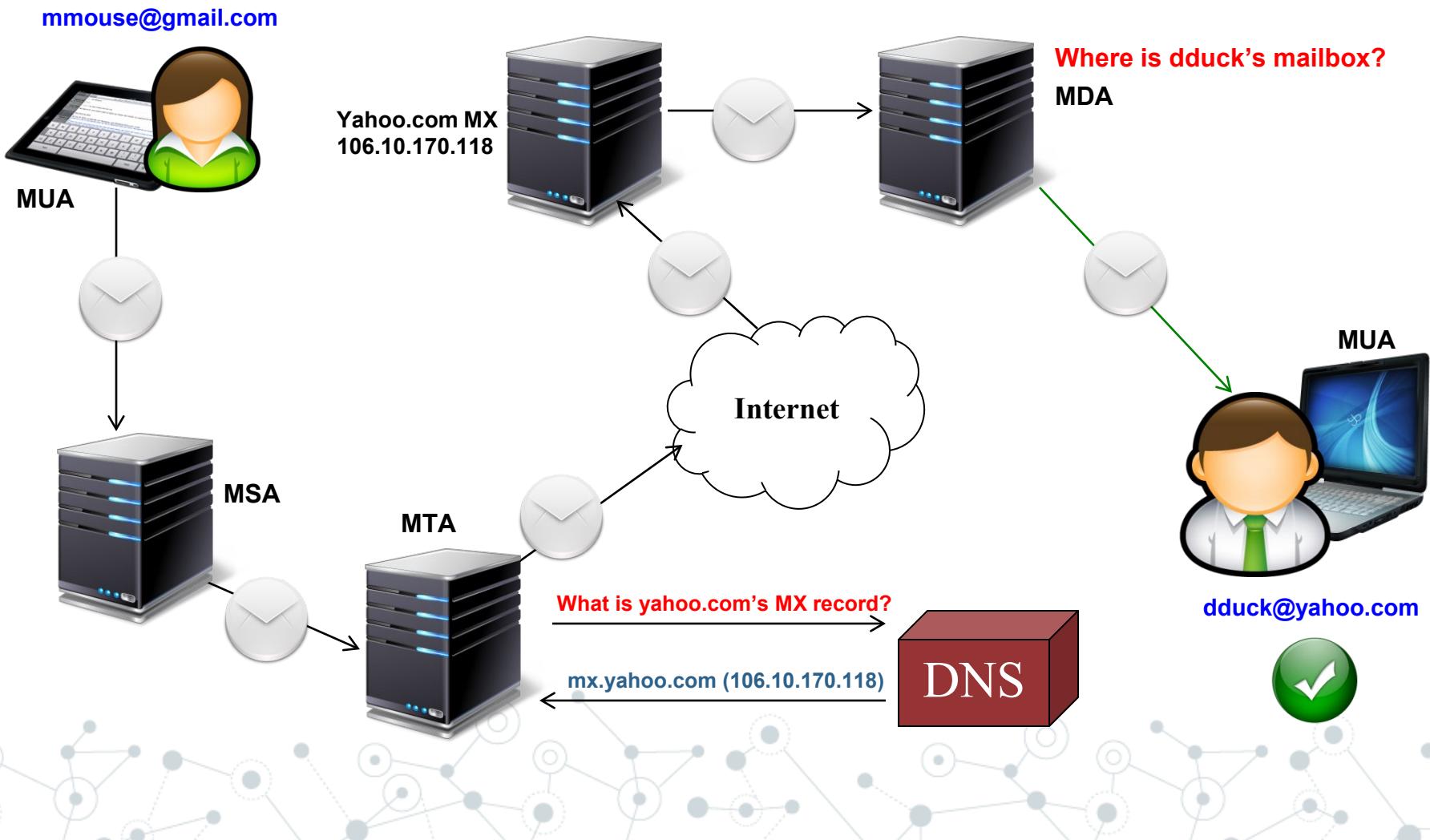
- Collection of shared network resources

# Internet Protocols

- ◎ Simple Mail Transfer Protocol (SMTP)
- ◎ Post Office Protocol (POP)
- ◎ Internet Message Access Protocol (IMAP)
- ◎ Hyper Text Transfer Protocol (HTTP)

## Email Delivery

From: mmouse@gmail.com  
To: dduck@yahoo.com



# Client-Based Email Applications

◎ Installed on Internet-capable devices

- Microsoft Outlook
- Mozilla Thunderbird

- Apple Mail (Macintosh OS X)

◎ User email data stored and managed in locally accessible databases

- Contacts
- Inbox
- Sent Items



# Locating Email Artifacts: MS Outlook

◎ Proprietary database format → Personal Storage Table (\*.pst extension)

- Contacts
- Messages
- Calendar

◎ MS Outlook 2010 database default location →  
C:\Users\<username>\Documents\Outlook  
Files



# Locating Email Artifacts: Thunderbird

- ◎ User data stored in open database format → MBOX
- ◎ Email messages stored in plaintext in one file
  - Inbox
  - Sent Mail
- ◎ Mozilla Thunderbird database default location →  
C:\Users\<username>\AppData\Roaming\Thunderbird\Profiles\\*.default\

# Web-Based Email Applications

◎ Email content is accessed via an installed Internet browser on device → Webmail

- Google Mail (Gmail)
- Windows Live Mail (Hotmail)

- Yahoo! Mail

◎ User data is maintained at the server level

- Inbox/Sent Items

- Contacts

- Trash



# Locating Email Artifacts: Webmail

- ◎ Some artifacts can be recovered
  - Temporary Internet Files
  - Pagefile.sys / Hiberfil.sys
  - NTFS metadata (\$MFT, \$LOGFILE)
  - Registry

# Email Message Headers

- ◎ Detail journey of message from sender to recipient
  - Could provide clues on network identity of sender
  - Google Mail (when accessed via the browser) **hides** senders' network identity
- ◎ Stored as header of original email message
- ◎ Typically manually accessed by user/analyst
- Hidden by most email clients

# Analyzing Email Message Header

## Recipient's email address



```
Delivered-To: spearson47@gmail.com
Received: by 10.60.42.104 with SMTP id n8csp11154oel;
          Wed, 4 Jul 2012 00:17:29 -0700 (PDT)
Received: by 10.68.234.104 with SMTP id ud8mr15438560pbc.163.1341386249321;
          Wed, 04 Jul 2012 00:17:29 -0700 (PDT)
Return-Path: <kfamily_r@yahoo.cn>
Received: from mail.jkgroupbd.com (mail.jkgroupbd.com. [203.76.153.242])
          by mx.google.com with ESMTP id ms9si28256705pbb.132.2012.07.04.00.16.40;
          Wed, 04 Jul 2012 00:17:29 -0700 (PDT)
Received-SPF: neutral (google.com: 203.76.153.242 is neither permitted nor denied by best
guess record for domain of kfamily_r@yahoo.cn) client-ip=203.76.153.242;
Authentication-Results: mx.google.com; spf=neutral (google.com: 203.76.153.242 is neither
permitted nor denied by best guess record for domain of kfamily_r@yahoo.cn)
smtp.mail=kfamily_r@yahoo.cn
Received: by mail.jkgroupbd.com (Postfix, from userid 48)
          id AA8A12EE8204; Wed, 4 Jul 2012 04:27:50 +0600 (BDT)
Received: from 213.136.113.78
          (SquirrelMail authenticated user marketing)
          by 203.76.153.242 with HTTP;
          Wed, 4 Jul 2012 04:27:50 +0600 (BDT)
Message-ID: <>39060.213.136.113.78.1341354470.squirrel@203.76.153.242>
Date: Wed, 4 Jul 2012 04:27:50 +0600 (BDT)
Subject: From Raphael Kamara
From: "Raphael Kamara" <kfamily_r@yahoo.cn>
Reply-To: rfamily_r@yahoo.cn
User-Agent: SquirrelMail/1.4.8-5.el5.centos.13
MIME-Version: 1.0
Content-Type: text/plain; charset=iso-8859-1
Content-Transfer-Encoding: 8bit
X-Priority: 3 (Normal)
Importance: Normal
To: undisclosed-recipients:;
```

**Received  
tags show  
each hop**



**Could be sender's actual IP address  
→ \*traceable to ISP**

# Summary

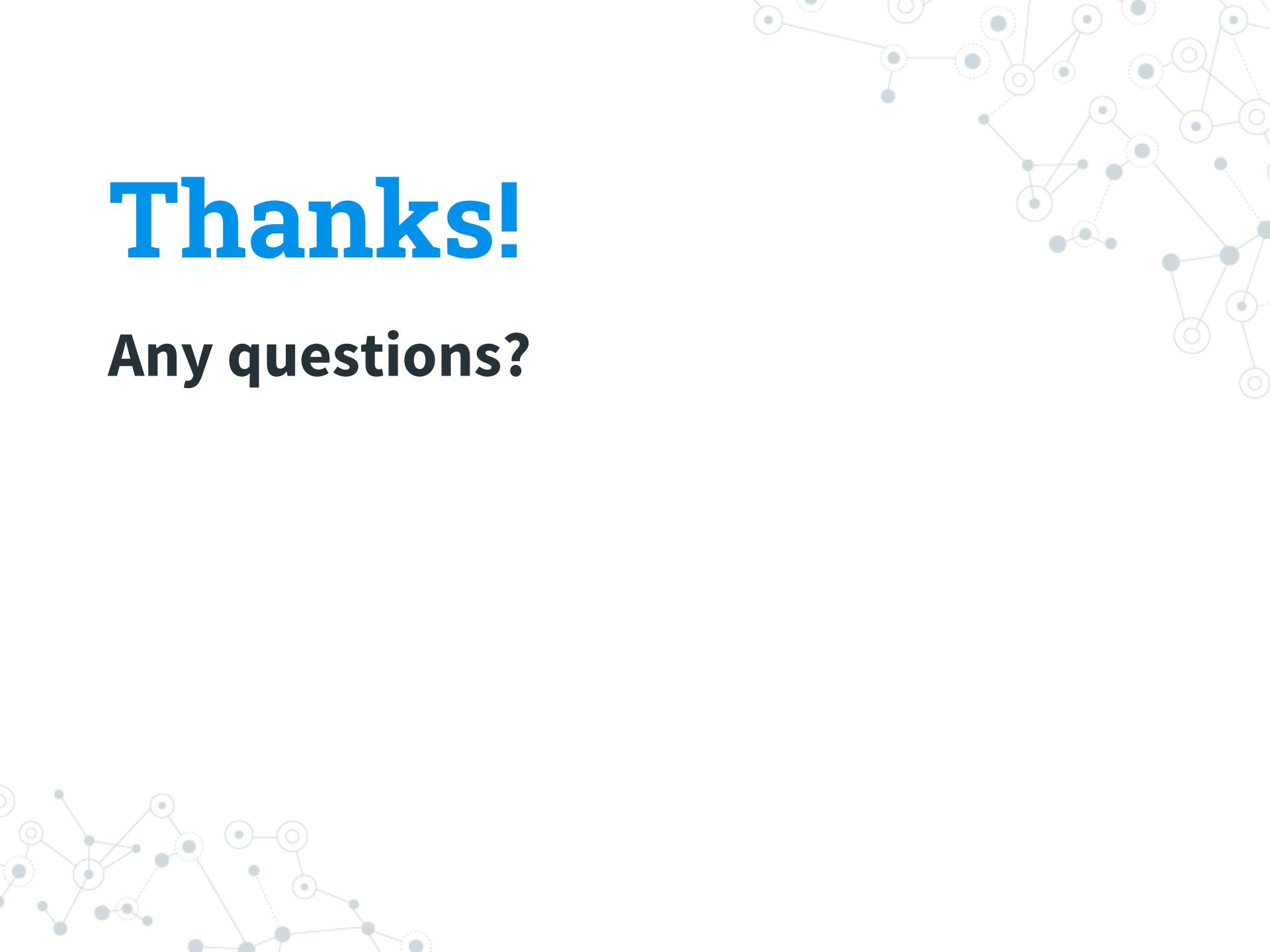
◎ You should now be able to

- Access different types of mail files
- Sort mail using defined fields
- Filter mail types by keyword
- Analyze an email header



# Thanks!

Any questions?





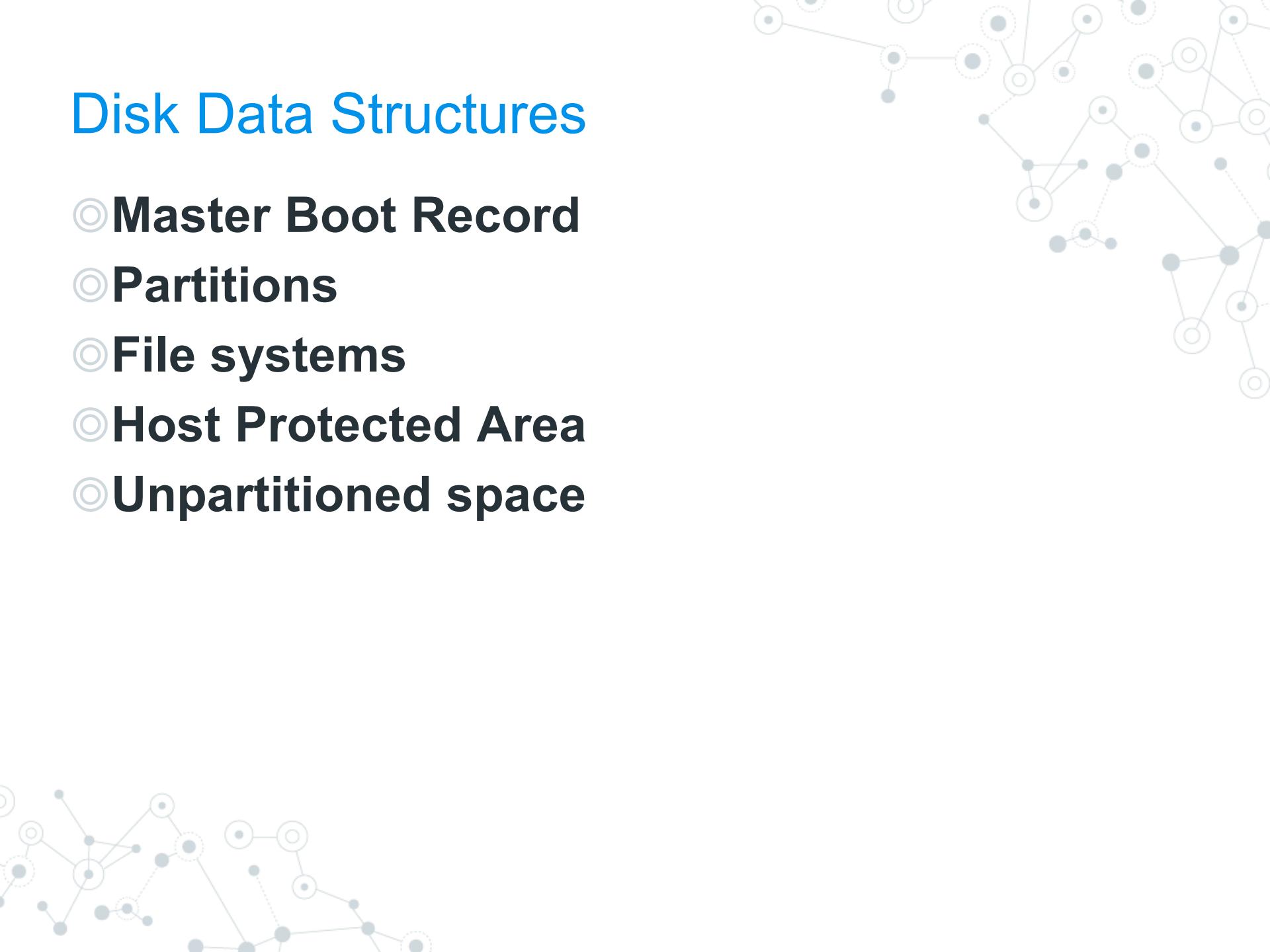
# Logical Data Storage

# Objective

**By the end of this module you will be able to analyze digital evidence using file system functions**

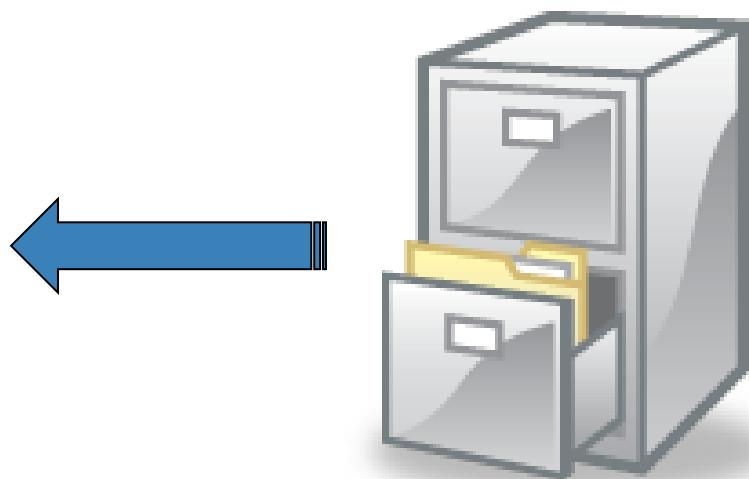
# Disk Data Structures

- ◎ Master Boot Record
- ◎ Partitions
- ◎ File systems
- ◎ Host Protected Area
- ◎ Unpartitioned space



# File System

- ◎ Tool for users to store data within a disk volume in an organized structure of files and directories



# File System Tracking

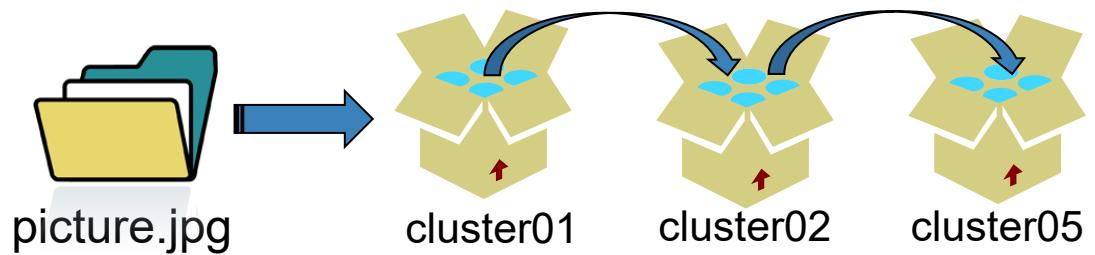
- ◎ Allocated space – Data clusters that contain active files
- ◎ Unallocated space – Data clusters that do not contain active files and are ready to contain new files from the file system

# Partitions

- ◎ Collection of consecutive sectors addressable by a single file system contained within that partition
- ◎ Hard disk can be separated into multiple partitions

# Clusters

- ◎ **Smallest data unit to store a file or directory**
- ◎ **Rules**
- **Clusters are a fixed size**
- **Only one file can be stored in a cluster**
- **Use as many clusters as needed to store a file**
- **Clusters do not have to be contiguous**



## Clusters: Example 1

File System							
0	1	2	3	4	5	6	7
8	9	10	11	12	13	14	15



## Clusters: Example 2

### File System

0	1	2	3	4	5	6	7
8	9	10	11	12	13	14	15

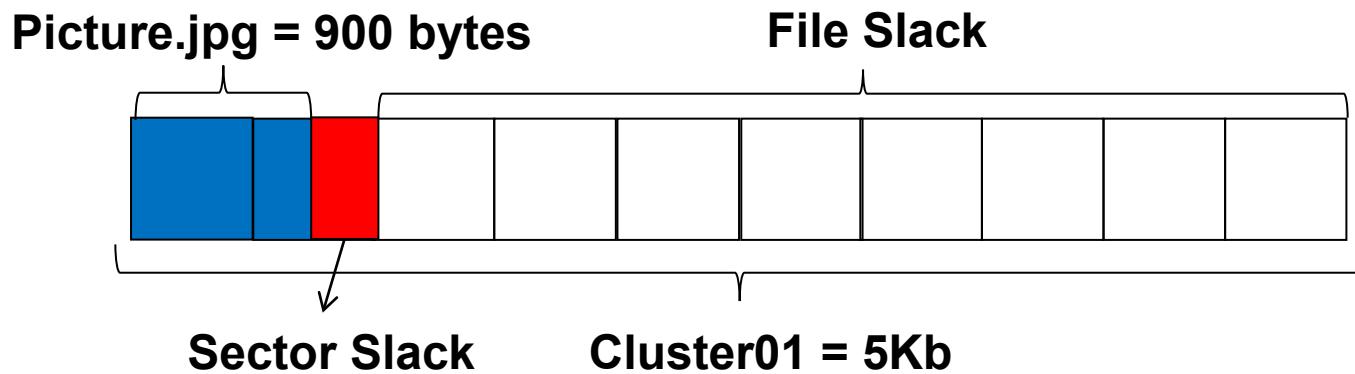
# Slack Space

## ◎ Sector slack or RAM slack

- Data located between the end of the logical file and the end of the last sector of the file

## ◎ File slack

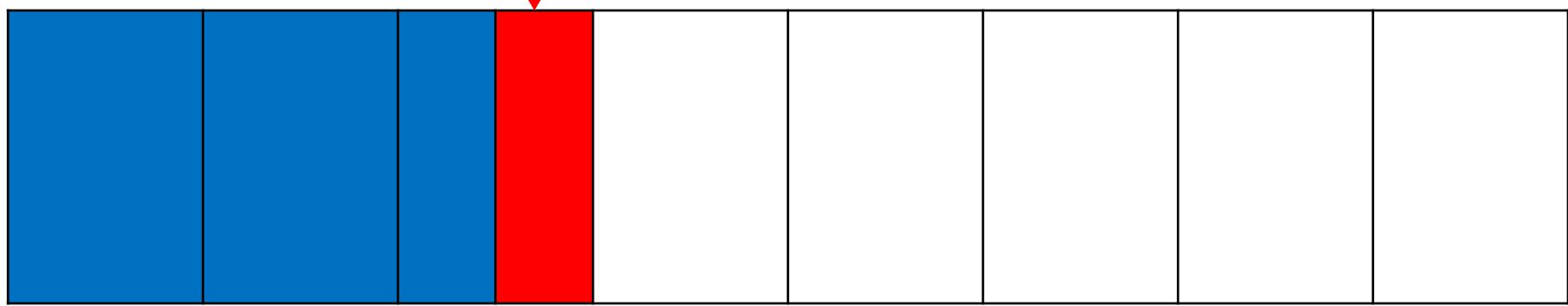
- Data between the last sector of the file and the end of the cluster



Sector Slack

Bank Account # ← RAM

Sector[3]

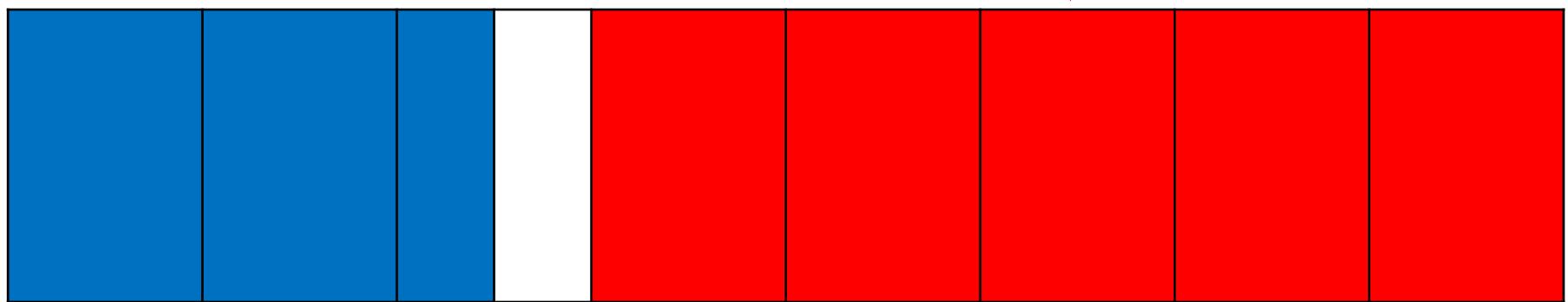
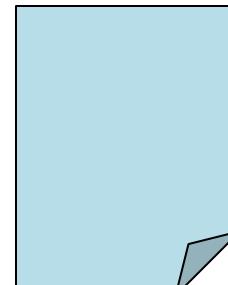


Cluster[2]

File Slack

Sector[3]

myfinances.doc



Cluster[2]

## File Slack

2)  
Name confirm[9].htm  
File Type Web Page  
Is Deleted NO  
Last Accessed 12/14/11 11:39:47AM  
File Created 12/14/11 11:39:47AM  
Last Written 12/14/11 11:39:47AM  
Entry Modified 12/14/11 11:39:47AM  
Hash Value 0673186a8b4c0e73fdb452d3f4e29f39  
Full Path 02072012-54\_Focus Direct Case\001\_Seagate  
500GB\_Sn.Z2A2T6SN\C\Documents and Settings\ikano\Local Settings\Temporary Internet  
Files\Content.IE5\45ENGP6B\confirm[9].htm  
Comment

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
<html>
<head>
<title>DSL Extreme</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
</head>
<body bgcolor="#808080">
<br>
<br>
<br>
<table width="75%" border="1" align="center" cellpadding="0" cellspacing="0">
<tr>
<td height="35" bgcolor="#CACACA"><div align="center"><b><font size="3" face="Arial, Helvetica, sans-serif">Ticket# 4717741&nbsp;has been created. <a href=".../ipnum-app/ipnum-edit.asp?custid=259738&dsl_phone=5624301548">Click Here</a> to continue. </font></b></div></td>
</tr>
</table>
</body>
</html>
-----
-----
-----
(818) 836-1826
CID-104-305-580
3987 HERITAGE OAK CT
SIMI VALLEY CA 93063
--8663472422 2
-----
Corporation for Supportive Housing
104-413-674
800 S FIGUEROA ST
SUIT 810
LOS ANGELES
CA
90017
257183
CBN: 2124614310 ext. 3
-----
Home Organisers, Inc
UN-homeorganisers
PW-99signut99
dslextreme@homeorganisers.com
```

# File Allocation Table (FAT) System

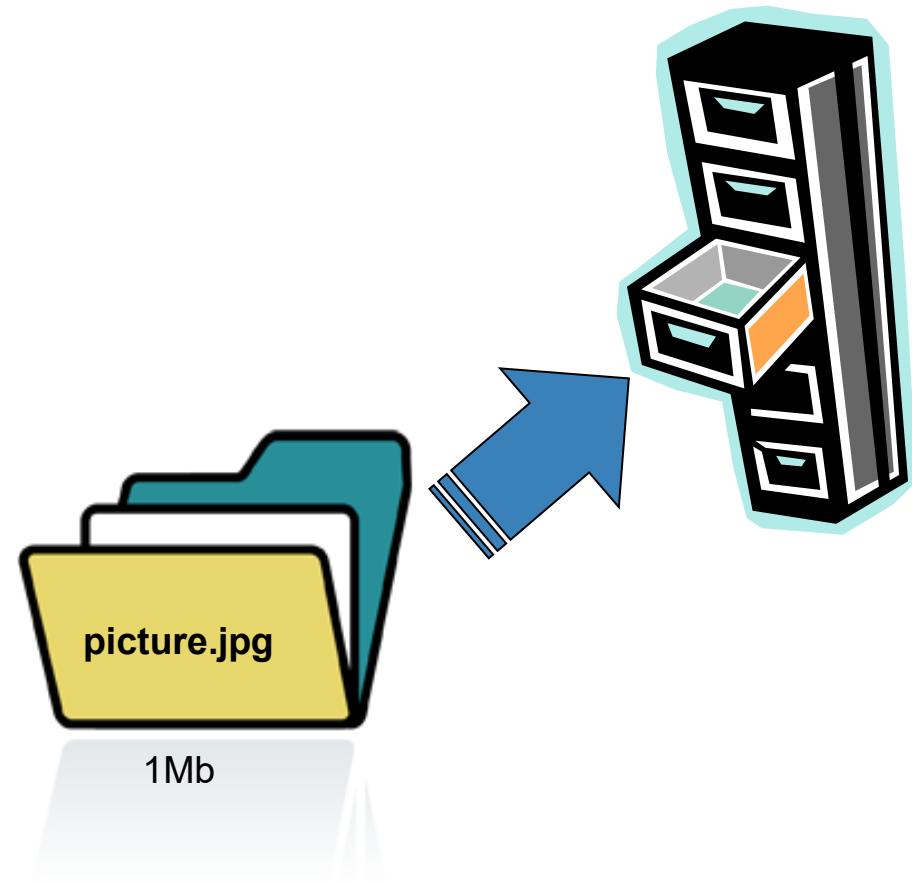
- ◎ Supported by most operating systems, such as
  - Microsoft Windows
  - UNIX
  - Linux
  - OS X
- ◎ Used in most flash media storage devices

# FAT Concepts

- ◎ Tracks clusters used to store file content
- ◎ Consists of two main structures
  - Directory entry
  - File allocation table
- ◎ Has three versions (FAT12, FAT16, FAT32)

# FAT Data Structures: Directory Entry

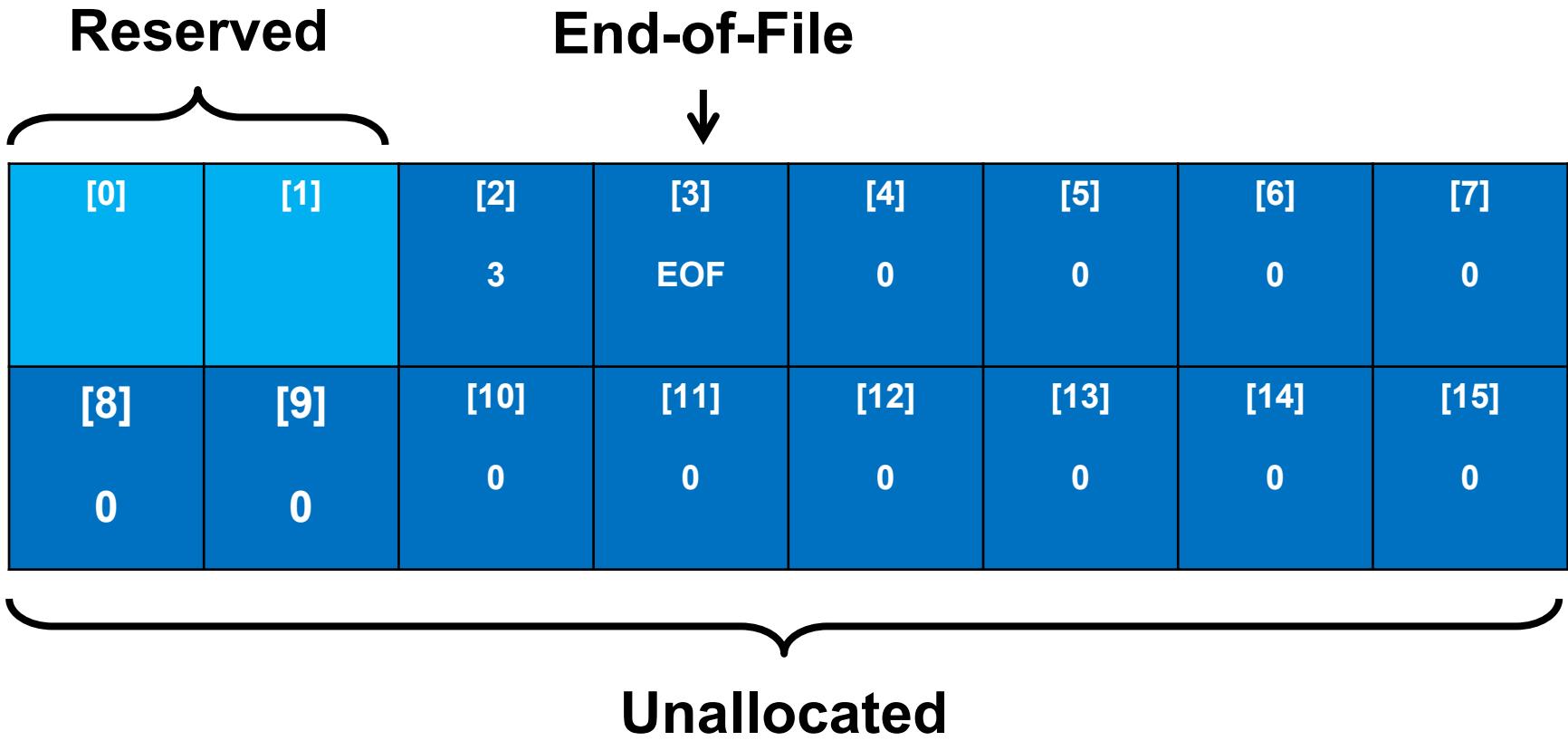
- ◎ Every file and directory has a 32-byte entry
  - Name of file or directory
  - Size (bytes)
  - Beginning cluster address
  - Metadata
    - MAC time stamps



# FAT Data Structures: File Allocation Table

- ◎ Tracks status of clusters
  - Allocated – currently in use by a file
  - Unallocated – not in use; free to store data
  - Bad clusters – cannot be used to store data
- ◎ Tracks location and sequence of clusters used to store file content larger than one cluster

## FAT Data Structures: Example



# Accessing and Retrieving Files

- ◎ A file is initially accessed using its filename and file path
- ◎ The file system retrieves the file contents using the starting cluster address and file size until it reaches the EOF marker assigned in FAT

# Deleting Files

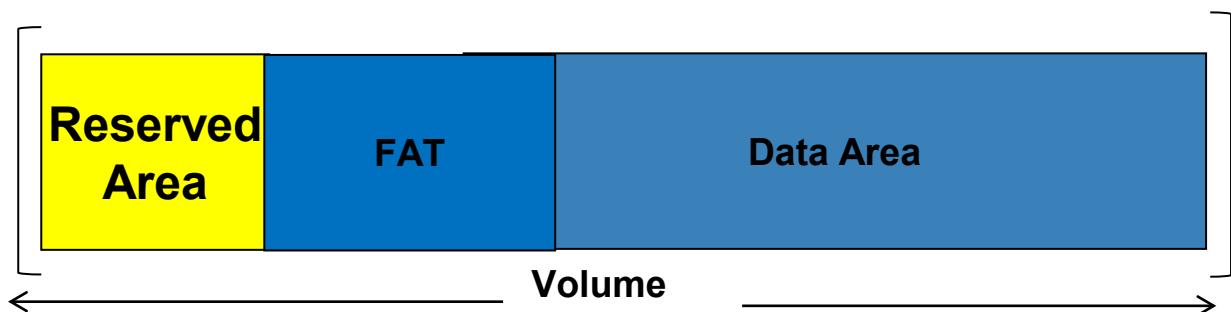
- ◎ The file's directory entry is changed to modify only the first character in its file name to an underscore ( \_ )
- ◎ The clusters allocated for the file's content are marked with zeros

# Recovering Deleted Files from FAT

- ◎ The directory entry still contains information
- ◎ Deleted files can be fully recovered if stored in
  - One cluster that was not overwritten, or
  - Multiple clusters that are
    - Contiguous
    - Not allocated to new files

# FAT Layout

- ◎ Reserved area: Volume boot record
- ◎ File allocation table
- ◎ Data area
- Directory entries
- Content of files and directories



## New Technology File System (NTFS)

### ◎ Supported in

- Windows NT, 2000, XP, Vista, 7
- OS X (read-only)
- UNIX/Linux variants (newer kernels)

### ◎ Successor to FAT

- Stronger file access security
- Faster performance
- More robust

# NTFS Concepts

- ◎ Tracks clusters used to store file content
- ◎ Is contained in system metadata files stored in the data area of the volume

# NTFS System Metadata Files: \$Boot

## ◎ \$Boot

- Contains the **volume boot record**
  - Cluster size
  - Total number of sectors in the volume
  - Starting cluster address of \$MFT
  - Location of Boot code (if bootable partition)
- Very similar to the FAT VBR

# NTFS System Metadata Files: \$MFT

## ◎ \$MFT (Master File Table)

- Record entry for every file and/or directory in volume
  - File name
  - Addresses of all clusters allocated to contain file contents; cluster runs tracked
  - MAC time stamps; file owner
- Small files (<480 bytes) can be stored in MFT record

# NTFS System Metadata Files: \$Bitmap

## • \$Bitmap

- Database that keeps track of each cluster in the volume using bits
  - [0] – cluster is available; unallocated
  - [1] – cluster is allocated to a file
  - Cluster runs are not tracked

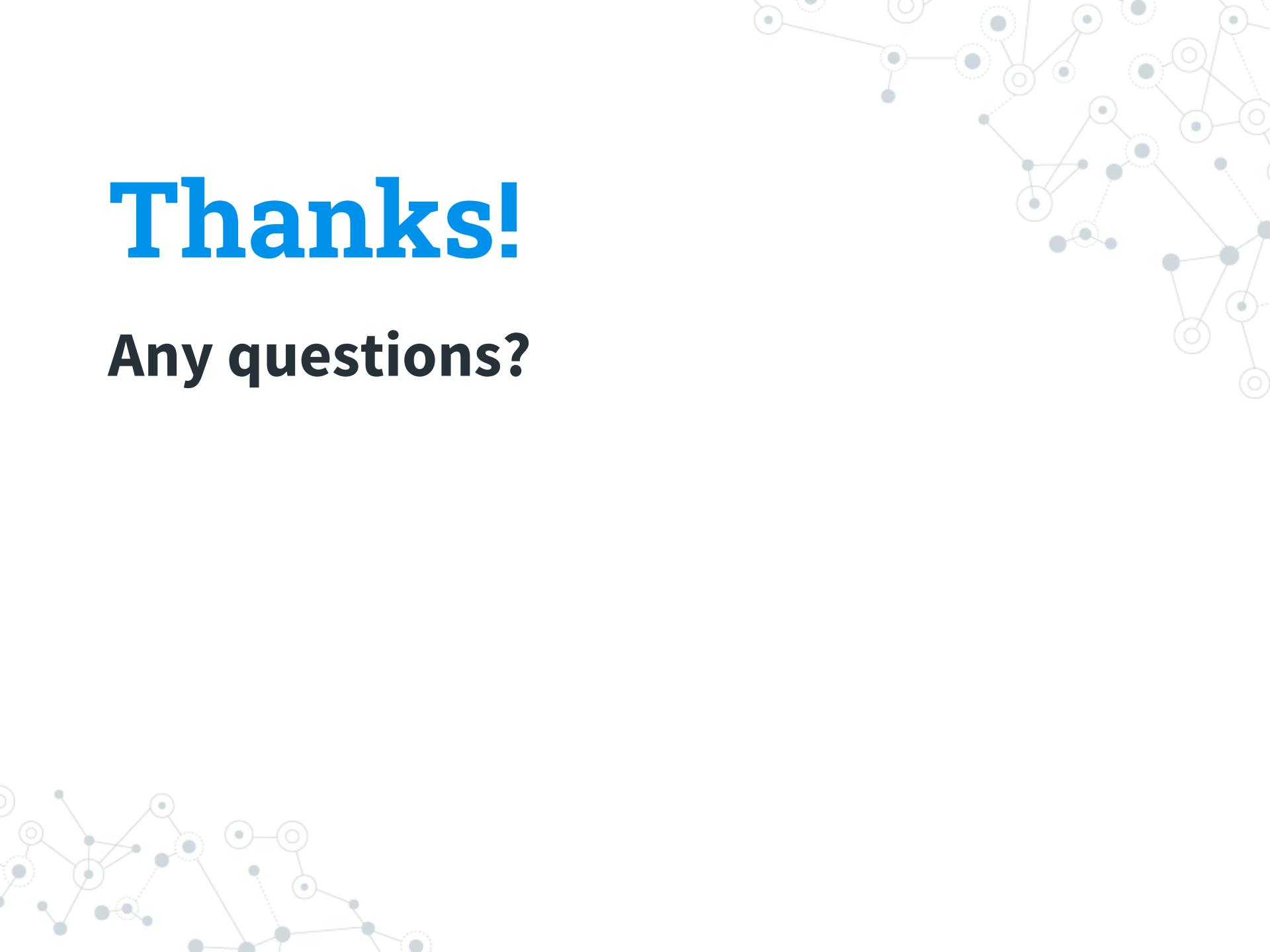
# Summary

You should now be able to

- ◎ Examine logical data structures
- ◎ Distinguish characteristics of FAT and NTFS
- ◎ Identify the file systems used in a storage device
- ◎ Recover deleted files, folders, and partitions

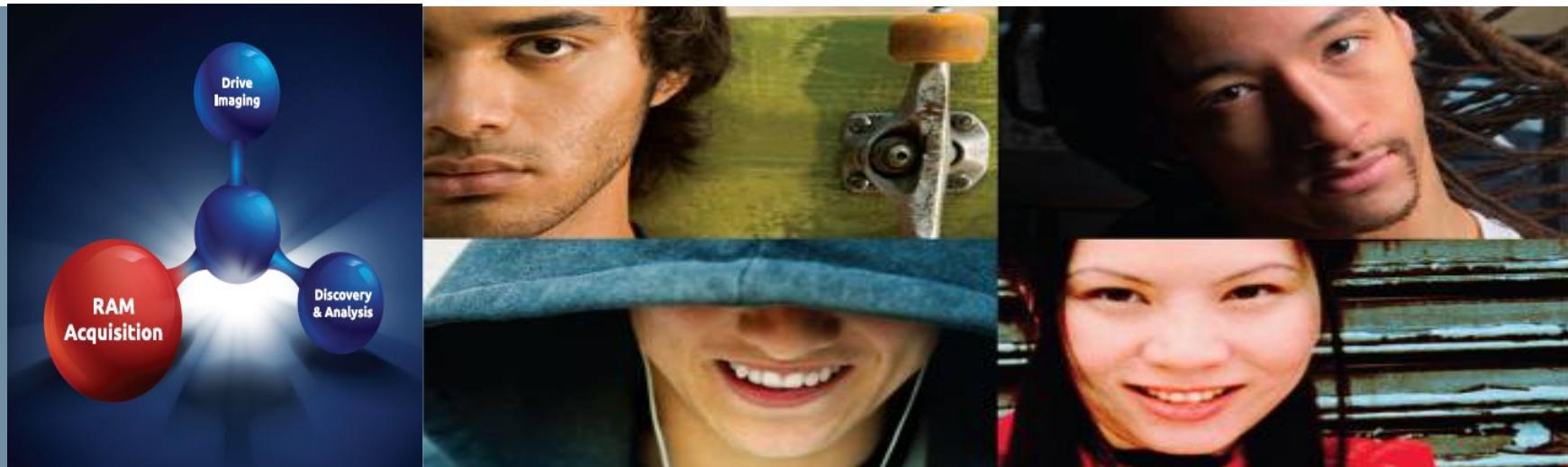
# Thanks!

Any questions?





# Computer Forensics Process



**Godwin S. Monserate**

19/09/2022

# Objectives of the Session(1)



- **Sources of Evidence**



- **Acquire evidence using forensic techniques**



- **Use of forensic tools**

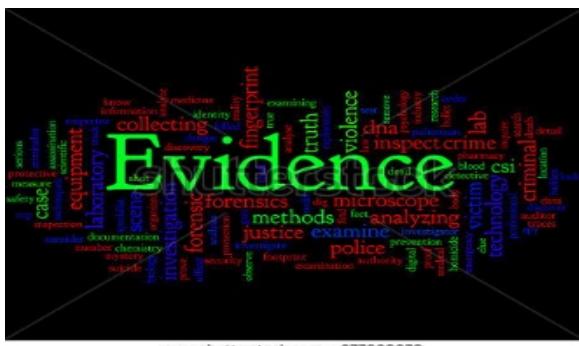


- **Digital evidence analysis**

# Objectives of the Session(2)



- **Solving a Case**



- **Apply and use forensic techniques**

# Digital Forensics

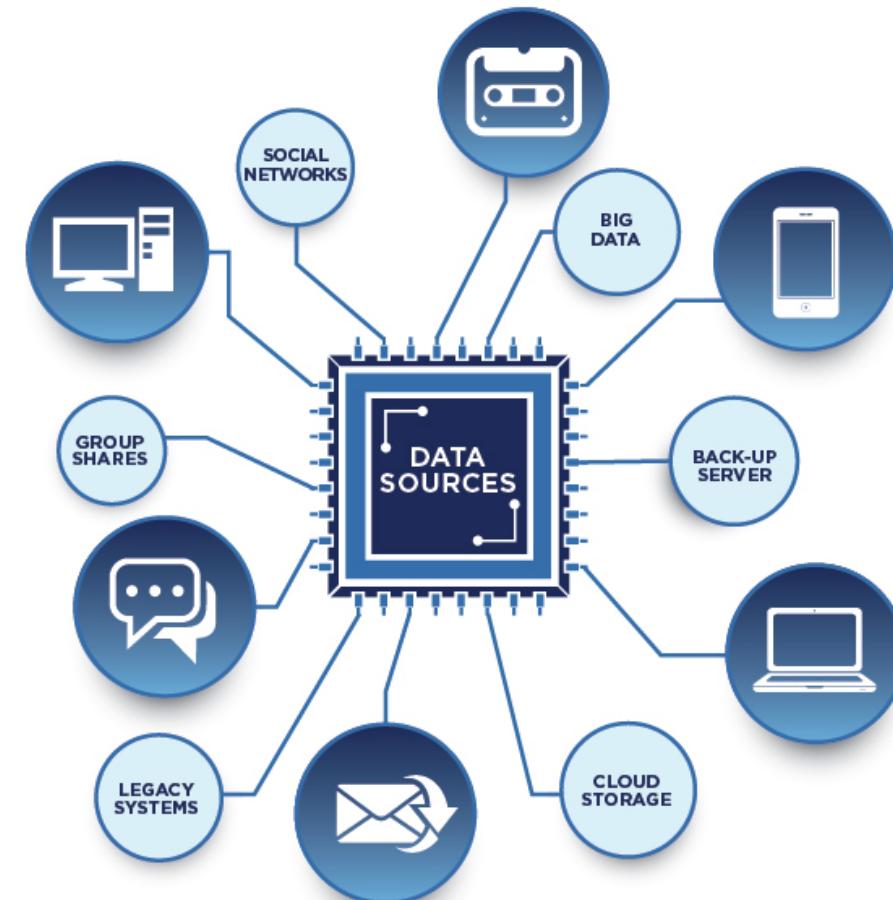


19/09/2022

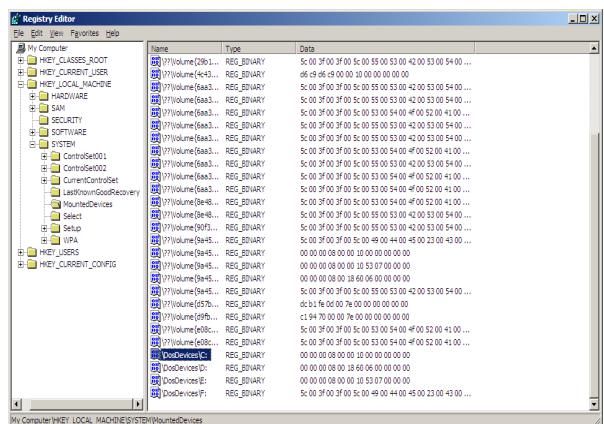
- Also known as Computer Forensics
- Considered to be the use of analytical and investigative techniques to **identify**, **collect**, **examine** and **preserve** evidence/information which is magnetically stored or encoded
- The objectives are:
  - Main objective is to **find** the **criminal** which is directly or indirectly related to cyber world
  - To **find out** **digital evidences**
  - **Presenting** evidences in a manner that leads to **legal action** of the criminal in the court of law

# Digital Evidences

- Any **data** that is recorded or preserved on any **medium** in or by a **computer system** or other similar **device**, that can be **read** or understand by a person or a computer system or other similar device.
- Information and data of value to an investigation that is stored on, received, or transmitted by an electronic device.
- In the legal world, **Evidence** is **EVERYTHING**
- **Evidence** is used to establish **facts**



# Types of Digital Evidence



## ■ Persistent Data

Data that remains intact when the computer is turned off.

E.g. hard drives, disk drives and removable storage devices(such as USB drives or flash drives)

## ■ Volatile Data

Data that would be lost if the computer is turned off.

E.g. deleted files, computer history, the computer's registry, temporary files and web browsing history.



# Sources of Evidence

- Computers
- External hard drives
- CD's and DVD's
- Thumb drives
- Floppy disks
- Cell phones
- Voice over IP phones
- Answering machines
- iPods
- Electronic game devices
- Digital video recorders
- Digital cameras
- PDAs
- GPSs
- Routers
- Switches
- Wireless access points



# Forensic Phases:

- Acquisition
- Identification
- Evaluation
- Presentation



# Computer Forensics Process(1)

## Computer Forensics

### ◎ Identification

- Identify Evidence
- Identify type of information available
- Determine how best to retrieve it



# Handling Digital Evidence at the Scene(1)

- First responders may follow the steps listed below to guide their handling of digital evidence at an electronic crime scene:
  - Recognize, identify, seize and secure all digital evidence at the scene.
  - Document the entire scene and the specific location of the evidence found.
  - Collect, label, and preserve the digital evidence
  - Package and transport digital evidence in a secure manner



- **Before collecting evidence at a crime scene, first responders should ensure that –**
  - Legal authority exists to seize evidence.
  - The scene has been secured and documented.
  - Appropriate personal protective equipment is used.



# First thing to be done at the crime scene

- When seizing a stand alone computer at the crime scene:
  - If the computer is “POWERED OFF”, do not turn it ON(turning it “OFF” could activate lockout feature)
  - If the computer is “POWERED ON”, do not turn it OFF and do not allow any suspect or associate to touch it(turning it “ON” could alter evidence on device)

# Tools and Materials for Collecting Digital Evidence

- Aside from tools for processing crime scenes in general, first responders should have the following items in their digital evidence collection toolkit:
  - Cameras(photo and video)
  - Cardboard boxes
  - Notepads
  - Gloves
  - Evidence inventory logs
  - Evidence tape
  - Evidence stickers, labels, or tags
  - Crime scene tape
  - Antistatic bags
  - Permanent markers
  - Nonmagnetic tools



## Acquisition/Preservation(2)

- Taking images of the drives/partition belonged to the identified system.
- Physically or remotely obtaining possession of the computer and external physical storage devices.
- Imaging is a bit for bit copy of the original evidence.
- It is much different than a simple copy and paste, because it maintains file structure present on the disk.
- Imaging can be time consuming process for a digital investigation, it is a step that cannot be avoided.
- Reasons why digital evidence needs to be imaged.
  - Most important reason is to uphold the integrity of the original media that was seized from the crime scene or suspect
  - Allows investigator to add multiple evidence items to a single analysis tool
  - Allows investigator to process all of the digital evidence for a case at one time, which will speed up the analysis process



# Number of Images Needed

- While the process of imaging can be different depending on the examiner or office procedure, the number of images should be a standard that is maintained for most investigations.
- Recommended is a two image standard.
- The first image that is created is considered the backup image.
- The backup image is an image that is used to create any additional images that are needed.
- When not in use, the backup image should be kept in a secure location to avoid outside manipulation of the evidence.
- From the backup images a second image is created, which is referred to as the working image. The working image is what will be analyzed by the examiner.



# Ways of Imaging/Mirroring

## ■ Hardware Imaging/Mirroring

- There are hardware duplicators that take a hard drive and mirror it on another hard drive.
- One of their big advantages is the speed and the safety.
- Example, the Logicube places the capturing disk (the destination) within the encasing and connects the suspect drive at the outside, preventing the most important mistake that the forensics examiner can make, namely to write in the wrong direction and destroy the evidence.



## ■ Software Based Forensics Duplication

- A number of software products are available that create qualified forensics duplicates.

UNIX dd - The dd utility in UNIX is certified to make forensic duplicates. dd is a UNIX tool, so the original drive needs to be mounted in UNIX. Raw dd duplicates need to be verified with a hashing (signatures), but there are specialized version of dd or scripts that include the verification.

EnCase is a very expensive, but very impressive Windows based Forensics suite that includes the making of qualified forensics duplicates

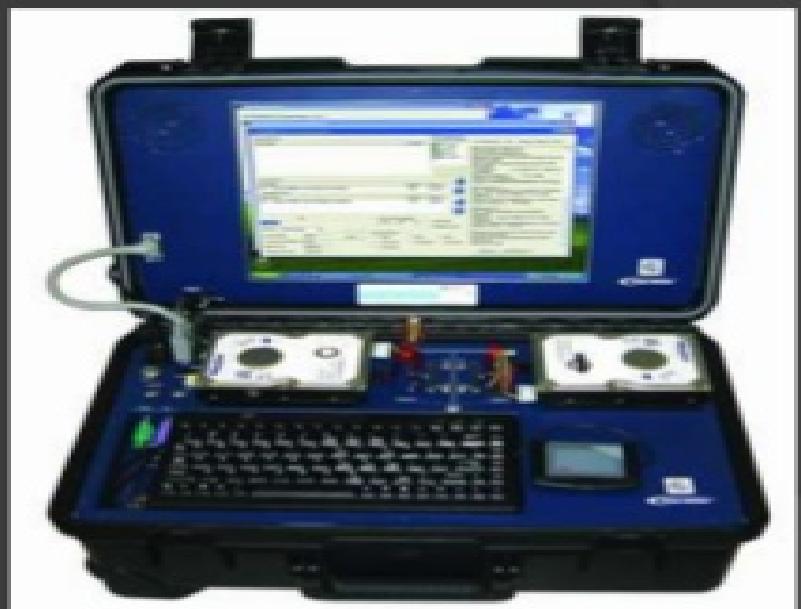
**UNIX®**



# Computer Forensics

## ○ Preservation

- Preserve evidence with least amount of change possible
- Must be able to account for any change
- Chain of custody



# 3 Different Types of Imaging Process

- Disk to disk imaging is used when the investigator needs an exact duplicate or clone of the original storage media.
  - Integrity of the original can be maintained throughout the course of the investigation
- Disk to file imaging is much like disk to disk imaging.
  - Main difference it that instead of a clone of the original a single file is created that represents the original media.
  - If multiple items are seized from a scene it is possible to image multiple pieces of evidence at one time. This allows the examiner to set up the imaging process and step away.
  - Multiple file formats that can be used in Disk to File Imaging
    - dd
      - This format is a raw data format. Native to Linux/Unix
      - Very beneficial because many free tools are linux/unix based.
      - Every bit (0 or 1) that is on the original media is stored in the file.
      - If the original is a 20 GB hard drive, the result will be a 20 GB dd file.
- Files to File imaging is same thing as disk to file imaging except the input is files instead of an entire disk. This type of imaging is mainly used when the scope is limited or the disk has extremely large capacity such as a RAID setup. Files to file imaging is rarely used, but it is essential for the examiner to understand when it should be used.

# FORMAT



# 3 Different Types of Imaging Process

- Multiple file formats that can be used in Disk to File Imaging
  - dd
    - This format is a raw data format. Native to Linux/Unix
    - Very beneficial because many free tools are linux/unix based.
    - Every bit (0 or 1) that is on the original media is stored in the file.
    - If the original is a 20 GB hard drive, the result will be a 20 GB dd file.
  - e01
    - A file format that was created by the developer of the commercial forensics tool Encase.
    - While the format was developed by the developers of Encase, it can be interpreted by other commercial tools.
    - Main benefit of E01 over DD is that the image file is compressed in a manner that is forensically sound.
    - Allows the examiner to save space on the destination storage media.

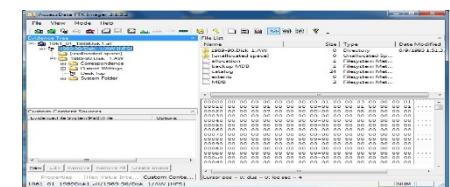
**FORMAT**



# 2 Categories of Software Imagers

- Imagers that use a command line interface.
  - The most common command line interface is DD or data dump.
  - Most command line interfaces used today are linux based.
  - There are multiple versions of DD, some of which include the hashing function, such as DCFLDD.
  - The benefit of command line tools is that the user will usually have more control over the tool.
- Imagers that use a graphical style interface.
  - The graphical interface is much easier to use than command line.
  - Most commercial software imagers on the market will include a graphical style interface.
  - Example is FTK Imager by Access- Data.
  - Like most commercial software imagers FTK Imager supports multiple formats, has hashing capabilities, and generates an imaging report.
  - Like other forms of imaging it is essential that an examiner practice with the tools that he or she is going to use to ensure that they fully understand the capability and procedure of the tools they are using.

```
bash-3.2$ sudo lsof | grep times
Found 2 items, totaling 20.0K
---Linux
times: /lib/timex/ 0r /lib/timex/, act /lib/times/ Linus Torvalds, the author
of Linux. Nobody in the hacker culture has been so readily recognized
by first name alone since Ken Thompson.
---QML/Linux English-English Dictionary
---Linux
/1em/ or /1em/*/, act /lib/times/ Linus Torvalds, the author of Linux. Nobody in the hacker culture has been a
recently recognized by first name alone since Ken Thompson.
Dictionary File 2387
The file contains 986 entries.
QML/Linux English-English Dictionary 16694
Basic English-English Dictionary 16694
Enter word or phrase(s)
Enter word or phrase(s)
bash-3.2$
```

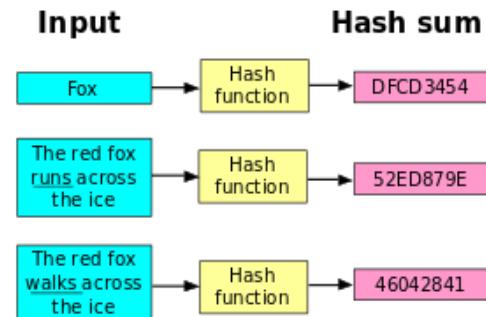


# Commercial vs Open-Source Tools

- Some advantages Commercial tools have over Open-Source tools:
  - Better Documentation
  - Commercial Level Support
  - Slick GUI (Graphical User Interface), user-friendly
  - In some cases, complete report generation which is accepted in court of law
- However, for anything a commercial forensics application can do, there are open-source applications which can do the same thing.

# Authentication

- Important to continue proper documentation throughout the entire investigation process.
- Digital evidence can easily change.
- Authentication, supported by proper documentation, can ensure that the evidence does not change once it was acquired and can ensure that the examination machine did not manipulate the original media.
- To provide proper authentication, verification takes place using hashing algorithms on both evidence and images.
- Hardware write blockers will prevent any change to the original media.



# Create Proof of Non-Alteration( Hashing)

- For this reason, it is common practice to calculate **cryptographic hash** of an evidence file and to record that hash elsewhere, usually in an investigator's notebook, so that one can establish at a later point in time that the evidence has not been modified since the hash was calculated.
- Hashing is a one-way function that computes a fixed length output from a variable input.
- Any change in the input results in a completely different output due to the avalanche effect.
- The **input** of a hashing function can be **any digital stream of data**.
- This can **range** from individual **files** to **large storage devices**.
- The only limitation is that the device must be able to be read by a computer. Items such as cell phones may require some type of data cable or specialized software.



String:

md5

Treat multiple lines as separate strings

MD5 Hash:

b1946ac92492d2347c6235b4d2611184

# Create Proof of Non-Alteration( Hashing)

- The output of a hashing function is usually represented in **hex or base 16**.
- This hash value can be looked at as a **digital fingerprint**.
- A **benefit** of using hash values to compare files is that there is no way to reverse from the **hash to digital media**.
- This **helps** maintain the **integrity** of the evidence while comparing it to other known files or devices.
- There are many different known hashing algorithms.
- The ones that are used the most for digital forensics today are MD5, SHA 1, and SHA 256.
- The MD5 hash algorithm returns a 128 bit output.
- The SHA 1 hash algorithm returns a 160 bit output. The SHA 256 hash algorithm returns a 256 bit output.

String:  
hello

md5

Treat multiple lines as separate strings

MD5 Hash:  
b1946ac92492d2347c6235b4d2611184



# Chain of Custody

- “Chain of Custody” is a fancy way of saying “The ability to demonstrate who has had access to the digital information being used as evidence”.
- Special measures should be taken when conducting a forensic investigation if it is desired for the results to be used in a court of law.
- One of the most important measures is to assure that the evidence has been accurately collected and that there is a clear chain of custody from the scene of the crime to the investigator – and ultimately to the court of law.





# Forensic Techniques

- **Cross-drive analysis:**

- forensic technique that correlates information found on multiple hard drives.
- can be used to perform anomaly detection.

- **Live analysis:**

- The examination of computers from within the operating system using custom forensics to extract evidence.

# Forensic Techniques

- **Deleted files:**

- recovery of deleted files
- Use of forensic software tools for recovering or carving out deleted data.

- **Example of Software Tools:**

- EnCase
- WinHex
- ProDiscover
- S-tool

# Forensic Techniques

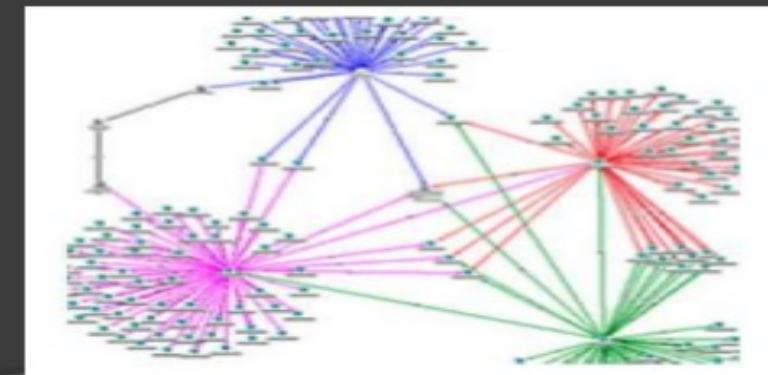
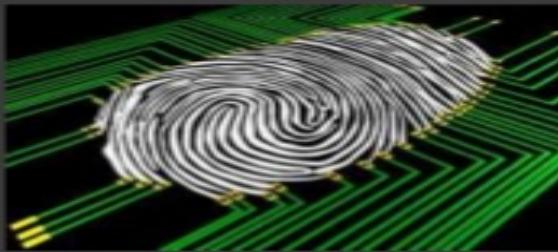
- **Steganography:**

- concealing a message, image, or file within another message, image, or file.
- detection of steganographically encoded packages is called steganalysis.
- the simplest method to detect modified files is to compare them to known originals.

# Computer Forensics Process(3)

## Computer Forensics

- ⦿ Analysis
  - Extract
  - Process
  - Interpret



# Computer Forensics Process(3)

- The third stage is Analysis.
- Analysis is the examination of all digital evidence that has been acquired and authenticated.
- The analysis process will be dictated by the examiner and types of digital evidence.
- In most situations the analysis will require specialized tools and skills. The tools require be both software and hardware based.
- The goal of the analysis stage is to identify all evidence contained in the digital device and report the results.
- Each examiner will have their own approach to analysis.
- A collection of tools that you are comfortable with is important.
- There are both commercial and open source tools available.



# Computer Forensics Process(3)

- There are two leading commercial manufacturers of computer forensics software today.
- They are AccessData and Guidance Software. In addition to commercial software there are free options such as Linux and other free tools.
- Free tools should only be used for examination by someone who has tested and practiced with the tool.
- The next logical step refers to when you are done with an investigation.
- How do you know that you have found all the evidence related to the case? Do you need to look at every file?
- What if you can't find anything?



# Computer Forensics Process(3)

- It is unreasonable to assume that you can look at every bit of data on the disk.
- Depending on your workload and policies, you want to at least look at most of the disk.
- The goal is to determine three things.
  - What is present on the disk?
  - What is the most likely and supported reason that information is present or absent?
  - Are there any plausible alternative explanations? Use the data to rule them out.

# Computer Forensics Process(4)

The final step is to prepare a report that details both your procedure and your findings. Reporting is covered in Advanced Comp Forensic.

## Computer Forensics

### ○Presentation

- Evidence will be accepted in court on:-
  - Manner of presentation
  - Qualifications of the presenter
  - Credibility of the processes used to preserve and analyze evidence
  - If you can duplicate the process



# COMPUTER FORENSIC REQUIREMENTS

- Hardware
  - Familiarity with all internal and external devices/components of a computer
  - Thorough understanding of hard drives and settings
  - Understanding motherboards and the various chipsets used
  - Power connections
  - Memory
- BIOS
  - Understanding how the BIOS works
  - Familiarity with the various settings and limitations of the BIOS

# COMPUTER FORENSIC REQUIREMENTS

- Operation Systems
  - Windows 3.1/95/98/ME/NT/2000/2003/XP
  - DOS
  - UNIX
  - LINUX
- Software
  - Familiarity with most popular software packages such as MS Office
- Forensic Tools
  - Familiarity with computer forensic techniques and the software packages that could be used



# COLLECTING EVIDENCE

- Make Exact copies of all hard drives & disks using computer software
  - ⇒ Date and Time stamped on each file; used for timeline
- Protect the Computer system
  - ⇒ Avoid deletion, damage, viruses and corruption
- Discover files
  - ⇒ Normal Files
  - ⇒ Deleted Files
  - ⇒ Password Protected Files
  - ⇒ Hidden Files
  - ⇒ Encrypted Files
- Reveal all contents of hidden files used by application and operating system
- Access contents of password protected files if legally able to do so
- Analyze data
- Print out analysis
  - ⇒ Computer System
  - ⇒ All Files and data
  - ⇒ Overall opinion
- Provide expert consultation/testimony



# Conclusion

This field will enable crucial electronic evidence to be found, whether it was lost, deleted, damaged, or hidden, and used to prosecute individuals that believe they have successfully beaten the system.





Thank  
you

[ 23 ]



# CREATING A DIGITAL FORENSIC LABORATORY



**Godwin S. Monserate**

**Cisco Networking Academy®**  
**Mind Wide Open™**

# CREATING A DIGITAL FORENSIC LABORATORY



- Creating a digital forensic laboratory is a responsible step. The effectiveness of the laboratory depends on what software, hardware and equipment will be purchased.



# A FORENSIC WORKSTATION

- Choosing a workstation configuration is an important step. The effectiveness of digital examiners depends on the way the workstation is configured.
- However, we want to pay special attention to one point: the workstation should work as quietly as possible. Imagine an open space where several powerful computers are installed, each of which makes a noise like a server. The employees' headache and poor health are guaranteed. Silent workstation performance is achieved by using low-noise fans and passive cooling systems.
- Do not use top hardware. The idea to buy the most expensive processor, memory, motherboard for your new workstation is not the best one.

- This configuration is optimal today:

OS: Windows 10 Pro 64-bit  
CPU (2): E5-2660 v4 (14 core)  
RAM: 64 GB DDR-42133 ECC  
OS Drive: 1 TB SSD  
Temp/Cache/DB Drive: 256 GB SSD  
Data Drive: 8 TB 7200rpm  
RAID Drives: 5 × 4 TB 7200rpm  
Video Card: GeForce GTX 1080



# A FORENSIC WORKSTATION

- It is recommended to use two or more monitors for each workstation.
- The most effective work is achieved when a digital examiner uses two workstations in its work.
- Use Storages to store cases, forensic images, etc. Storages with a volume of 100-150 TB proved to be quite effective.
- Use 10Gbit Net Cards. They will allow you to transfer data from the workstation to storages quickly.



# FORENSIC SOFTWARE

- It's a good idea to have as more different forensic software in the digital laboratory.
- This will allow a forensic examiner to make cases as quickly and efficiently as possible. Also, this makes it possible to recheck the results of the research effectively.
- However, if you have a limited budget, we recommend buying this software:
- Windows 10 Pro, Office 365
- Antivirus software, X-ways Forensic
- AXIOM (Magnet Forensics)
- The rest of the tools can be purchased as the laboratory develops.





# FORENSIC SOFTWARE

- Also, a lot of research can be done using freeware tools.
- Sometimes these tools outperform functionality of commercial tools.

Tarantula	Cellebrite	Oxygen Forensic	X-Ways Forensic	Encase Forensic	AccessData FTK	AccessData Triage	SMART (asrdata.com)	MacQuisition	Forensic Assistant	Belkasoft	PeerLab	NetAnalysis	Recovery My Files

Igor Mikhaylov  
Computer, Cell Phone & Chip-Off Forensics  
[linkedin.com/in/igormikhaylovcf](http://linkedin.com/in/igormikhaylovcf)



# CASE MANAGEMENT SOFTWARE

- The digital forensic laboratory in a government organization, for example in the police department, then most likely they have their own case management software and then your task is just to add a new laboratory to the network of existing ones.
- In other cases, you can use free and chargeable CRM systems. Besides, some CRM systems can be adapted to your management needs.
- Ex. **Kirjuri** (Kirjuri is a web application for managing cases and physical forensic evidence items.)
- Lima Forensic Case Management of all the specialized tools.



# VIDEO FORENSICS

- Use a separate workstation for the production of video forensics cases.  
The following forensic tools are recommended for this task:
  - **DVR Examiner**
  - **Amped FIVE**
  - **Elecard**
- Very good results of recovering deleted videos can be obtained using **X-ways Forensic**.



# MOBILE FORENSICS

- We recommend using a separate workstation to carry out mobile forensics research.
- There are a lot of tools for mobile forensics. That is why it is difficult for a beginner to understand what they need to carry out this research effectively. Using the following mobile forensic tools will help you achieve your objective:
  - UFED 4PC (with CHINEX, UFED Camera Kit)



Cellebrite UFED Touch



# MOBILE FORENSICS

- **Oxygen Forensics DETECTIVE**

- Oxygen Forensic Detective is an all-in-one forensic software platform built to extract, decode, and analyze data from multiple digital sources: mobile and IoT devices, device backups, UICC and media cards, drones, and cloud services. Oxygen Forensic® Detective can also find and extract a vast range of artifacts, system files as well as credentials from Windows, macOS, and Linux machines.

- **XRY**

- **XRY** is a **digital forensics** and mobile device **forensics** product by the Swedish company Micro Systemation used to analyze and recover information from mobile devices such as mobile phones, smartphones, GPS navigation tools and tablet computers. It consists of a hardware device with which to connect phones to a PC and software to extract the data.

- **Elcomsoft Mobile Forensic Bundle**

- includes a number of tools to acquire and analyze evidence from a number of mobile platforms. Physical and logical acquisition of iOS devices Extract evidence from 64-bit iOS devices with or without a jailbreak.

# MOBILE FORENSICS



- **SP Flash tool to retrieve data from MTK based phones.**

SP flash tool is an application which mainly helps you to flash Stock ROM, Custom recovery and fixing in some extreme cases (firmware update, Flash recovery, unbrick bricked Android device etc.).

SmartPhone FlashTool is working with MediaTek Android smartphones (MTK based) You can  
Download SPFlashTool from our  
downloading section.

# MOBILE DATA RECOVERY

- Use flashers for JTAG research:
  - Easy Z3x JTAG BOX
  - Octoplus Box
  - Samsung anyway S101
- For Chip-off we recommend using:
  - VISUAL NAND RECONSTRUCTOR (STARTER KIT, Rusolut)
  - SMARTPHONE KIT (Rusolut)
  - CHINESE SMARTPHONE KIT (Rusolut)
  - NuProg-E UFS/EMMC Programmer
  - IN-UFS-Socket BGA Opentop
  - N-UFS-065-BGA095-115130-02O BGA Opentop
  - N-UFS-050-FBGA153-115130-02O BGA Opentop
- Use Weller WHA 300 Hot Air Reworking Station or Ersa HR100 Hybrid Rework system for disordering chips.





# CLOUD FORENSICS

- Use the following tools for Cloud forensics:
  - UFED Cloud Analyzer
  - Oxygen Forensics DETECTIVE
  - Elcomsoft Cloud eXplorer



# DATA RECOVERY (HARD DRIVES, FLASH DRIVES, MEMORY CARDS)

- Use a separate workstation for the production of Data recovery. You will need special hardware and tools for data recovery:
  - PC-3000 Express Professional System (Acelab)
  - Data Extractor Express (Acelab)
  - PC-3000 Flash (Acelab)



# DATA RECOVERY (HARD DRIVES, FLASH DRIVES, MEMORY CARDS)

- Hardware and tools for data recovery:

PC-3000 Express Professional System (Acelab)

is the fastest, most efficient and most powerful hardware-software solution for recovering data from damaged HDDs based on SATA (Serial ATA) or PATA (IDE) interfaces for numerous vendors



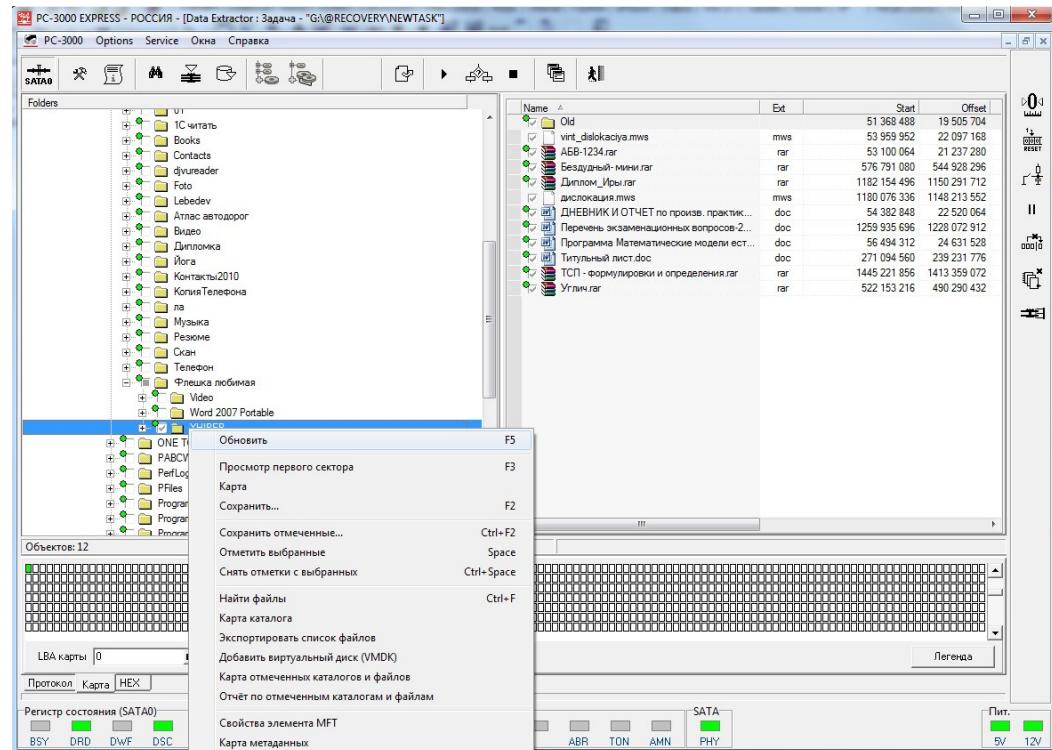


# DATA RECOVERY (HARD DRIVES, FLASH DRIVES, MEMORY CARDS)

Data Extractor Express (Acelab)

PC-3000 Flash (Acelab)

The **Data Extractor Express** is a specialized software product functioning in tandem with the PC-3000 Express hardware-software product.





# FURNITURE

- Many people believe that it is enough to buy ordinary office desks and chairs to equip a digital forensic lab
- Tables must have abrasion resistant coatings.
- Office chairs should be as convenient as possible.
- The table where the electronic equipment is assembled and disassembled should be equipped with an antistatic mat and an antistatic bracelet.





# Digital Forensics



# What Is Digital Forensics?

- Digital forensic science is a branch of forensic science that focuses on the recovery and investigation of material found in digital devices related to cybercrime.
- The term digital forensics was first used as a synonym for computer forensics. Since then, it has expanded to cover the investigation of any devices that can store digital data.
- The first computer crime was reported in 1978, followed by the Florida computers act, it wasn't until the 1990s that it became a recognized term. It was only in the early 21st century that national policies on digital forensics emerged.
- Digital forensics is the process of identifying, preserving, analyzing, and documenting digital evidence. This is done in order to present evidence in a court of law when required.



# What Is Digital Forensics?

- “Digital forensics is the process of uncovering and interpreting electronic data. The goal of the process is to preserve any evidence in its most original form while performing a structured investigation by collecting, identifying, and validating the digital information to reconstruct past events.
- The context is most often for the usage of data in a court of law, though digital forensics can be used in other instances.”

-Techopedia

# Steps of Digital Forensics

## Steps of Digital Forensics

In order for digital evidence to be accepted in a court of law, it must be handled in a very specific way so that there is no opportunity for cyber criminals to tamper with the evidence.

### 3. Analysis

Next, reconstruct fragments of data and draw conclusions based on the evidence found.

### 1. Identification

First, find the evidence, noting where it is stored.

### 2. Preservation

Next, isolate, secure, and preserve the data. This includes preventing people from possibly tampering with the evidence.

### 4. Documentation

Following that, create a record of all the data to recreate the crime scene.

### 5. Presentation

Lastly, summarize and draw a conclusion.

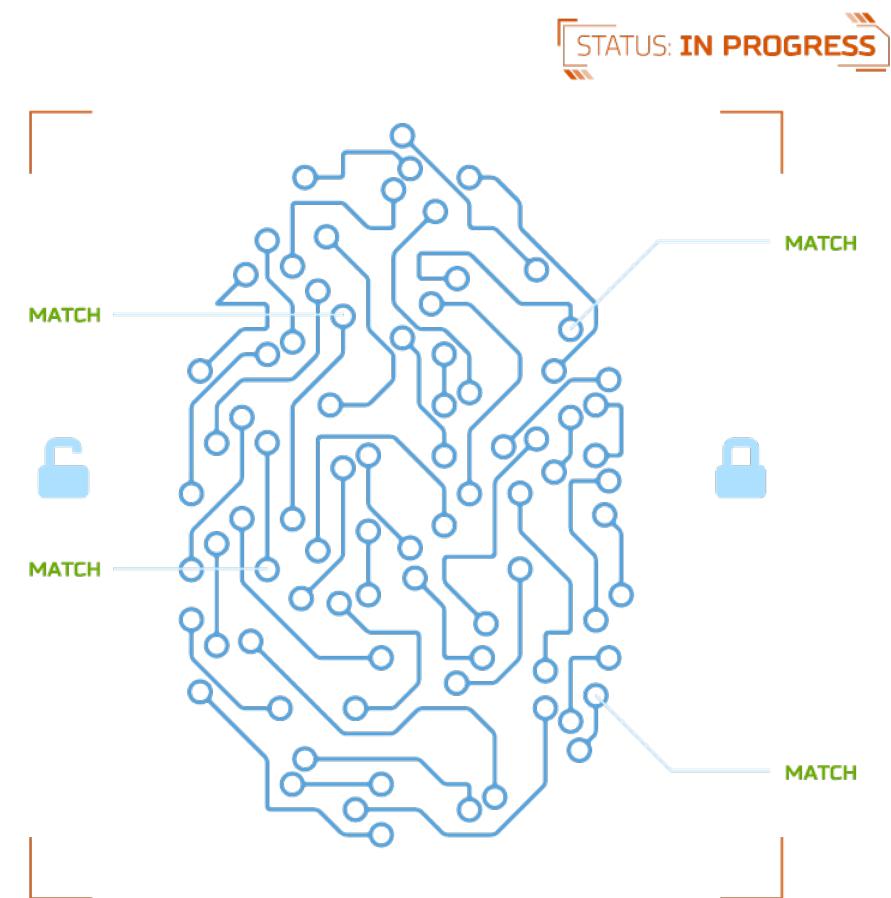
# When Is Digital Forensics Used in a Business Setting?

- For businesses, Digital Forensics is an important part of the Incident Response process.
- Forensic Investigators identify and record details of a criminal incident as evidence to be used for law enforcement.
- Rules and regulations surrounding this process are often instrumental in proving innocence or guilt in a court of law.



# Who Is a Digital Forensics Investigator?

- A Digital Forensics Investigator is someone who has a desire to follow the evidence and solve a crime virtually.
- Imagine a security breach happens at a company, resulting in stolen data.
- Under those circumstances, a digital forensic investigator's role is to recover data like documents, photos, and emails from computer hard drives and other data storage devices, such as zip and flash drives, with deleted, damaged, or otherwise manipulated.





# How Is Digital Forensics Used in an Investigation?

- Digital footprint is the information about a person on the system, such as the webpages they have visited, when they were active, and what device they were using. By following the digital footprints, the investigator will retrieve the data critical to solving the crime case. To name a few –Matt Baker, in 2010, Krenar Lusha, in 2009, and more cases were solved with the help of digital forensics.
- Cyber forensic investigators are experts in investigating encrypted data using various types of software and tools. There are many upcoming techniques that investigators use depending on the type of cybercrime they are dealing with.
- Cyber investigators' tasks include recovering deleted files, cracking passwords, and finding the source of the security breach. Once collected, the evidence is then stored and translated to make it presentable before the court of law or for police to examine further.

**THE BASICS**

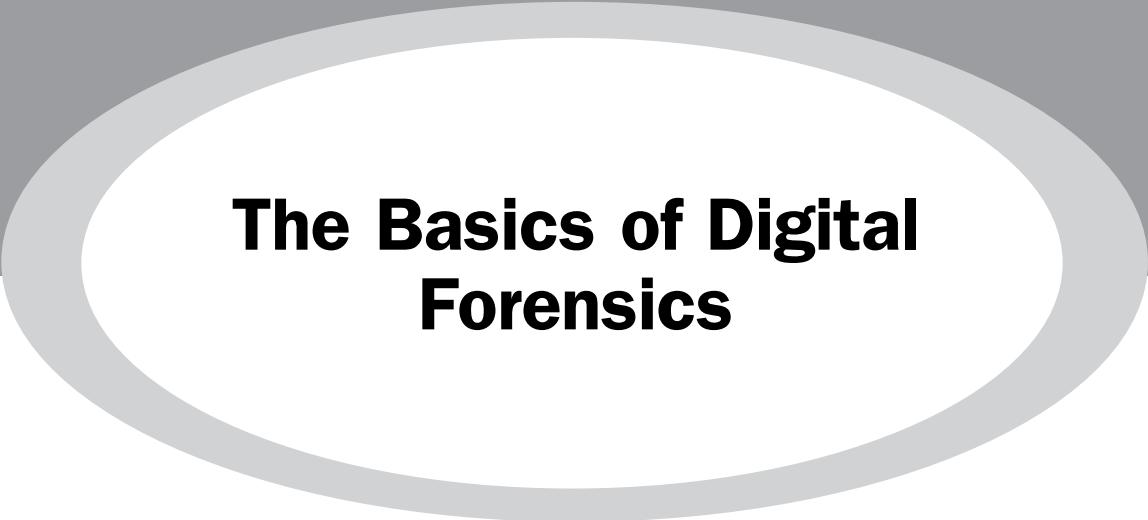
SYNTHESIS

# **THE BASICS OF DIGITAL FORENSICS**

The Primer for Getting Started  
in Digital Forensics

**John Sammons**





# **The Basics of Digital Forensics**

This page intentionally left blank

# **The Basics of Digital Forensics**

**The Primer for Getting Started  
in Digital Forensics**

**John Sammons**

*Technical Editor*

Jonathan Rajewski



AMSTERDAM • BOSTON • HEIDELBERG • LONDON  
NEW YORK • OXFORD • PARIS • SAN DIEGO  
SAN FRANCISCO • SINGAPORE • SYDNEY • TOKYO

Syngress is an imprint of Elsevier

**SYNGRESS®**

**Acquiring Editor:** Chris Katsaropoulos  
**Development Editor:** Heather Scherer  
**Project Manager:** Danielle S. Miller  
**Designer:** Alisa Andreola

Syngress is an imprint of Elsevier  
225 Wyman Street, Waltham, MA 02451, USA

© 2012 Elsevier, Inc. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or any information storage and retrieval system, without permission in writing from the publisher. Details on how to seek permission, further information about the Publisher's permissions policies and our arrangements with organizations such as the Copyright Clearance Center and the Copyright Licensing Agency, can be found at our website: [www.elsevier.com/permissions](http://www.elsevier.com/permissions).

This book and the individual contributions contained in it are protected under copyright by the Publisher (other than as may be noted herein).

#### Notices

Knowledge and best practice in this field are constantly changing. As new research and experience broaden our understanding, changes in research methods or professional practices, may become necessary.

Practitioners and researchers must always rely on their own experience and knowledge in evaluating and using any information or methods described herein. In using such information or methods they should be mindful of their own safety and the safety of others, including parties for whom they have a professional responsibility.

To the fullest extent of the law, neither the Publisher nor the authors, contributors, or editors, assume any liability for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products, instructions, or ideas contained in the material herein.

#### Library of Congress Cataloging-in-Publication Data

Sammons, John.

The basics of digital forensics : the primer for getting started in digital forensics / John Sammons.

p. cm.

ISBN 978-1-59749-661-2

1. Computer crimes—Investigation. I. Title.

HV8079.C65S35 2012

363.25'968—dc23

2011047052

#### British Library Cataloguing-in-Publication Data

A catalogue record for this book is available from the British Library.

For information on all Syngress publications  
visit our website at: [www.syngress.com](http://www.syngress.com)

*Typeset by:* diacriTech, Chennai, India

Printed in the United States of America

12 13 14 15 10 9 8 7 6 5 4 3 2 1

Working together to grow  
libraries in developing countries

[www.elsevier.com](http://www.elsevier.com) | [www.bookaid.org](http://www.bookaid.org) | [www.sabre.org](http://www.sabre.org)

ELSEVIER

BOOK AID  
International

Sabre Foundation

# Dedication

v

For Lora, Abby, and Rae for making me a truly  
blessed and lucky man.

To my mother Juanita, and my grandmother Grace.  
For the many sacrifices you made and  
the example you set ... I miss you.

This page intentionally left blank

# Contents

PREFACE .....	xv
ACKNOWLEDGMENTS .....	xix
ABOUT THE AUTHOR .....	xxi
ABOUT THE TECHNICAL EDITOR .....	xxiii
<b>CHAPTER 1 Introduction .....</b>	<b>1</b>
Introduction .....	1
What Is Forensic Science? .....	2
What Is Digital Forensics? .....	2
Uses of Digital Forensics .....	3
Criminal Investigations .....	3
Civil Litigation .....	4
Intelligence .....	5
Administrative Matters .....	6
Locard's Exchange Principle .....	7
Scientific Method .....	7
Organizations of Note .....	7
Scientific Working Group on Digital Evidence .....	8
American Academy of Forensic Sciences .....	8
American Society of Crime Laboratory Directors/	
Laboratory Accreditation Board .....	9
National Institute of Standards and Technology (NIST) .....	9
American Society for Testing and Materials (ASTM) .....	9
Role of the Forensic Examiner in the Judicial System .....	10
The CSI Effect .....	10
Summary .....	10
References .....	11
<b>CHAPTER 2 Key Technical Concepts .....</b>	<b>13</b>
Introduction .....	13
Bits, Bytes, and Numbering Schemes .....	13
Hexadecimal .....	14
Binary to Text: ASCII and Unicode .....	14

File Extensions and File Signatures .....	15
Storage and Memory .....	16
Magnetic Disks .....	17
Flash Memory .....	18
Optical Storage .....	18
Volatile versus Nonvolatile Memory .....	18
Computing Environments .....	19
Cloud Computing .....	19
Data Types .....	20
Active Data .....	20
Latent Data .....	21
Archival Data .....	21
File Systems .....	21
Allocated and Unallocated Space .....	22
Data Persistence .....	22
How Magnetic Hard Drives Store Data .....	23
Page File (or Swap Space) .....	25
Basic Computer Function—Putting it All Together .....	26
Summary .....	27
References .....	27
<b>CHAPTER 3 Labs and Tools .....</b>	<b>29</b>
Introduction .....	29
Forensic Laboratories .....	29
Virtual Labs .....	30
Lab Security .....	30
Evidence Storage .....	31
Policies and Procedures .....	32
Quality Assurance .....	32
Tool Validation .....	33
Documentation .....	34
Digital Forensic Tools .....	35
Tool Selection .....	36
Hardware .....	36
Software .....	39
Accreditation .....	40
Accreditation versus Certification .....	42
Summary .....	43
References .....	43

<b>CHAPTER 4 Collecting Evidence .....</b>	<b>45</b>
Introduction .....	45
Crime Scenes and Collecting Evidence .....	46
Removable Media .....	46
Cell Phones .....	47
Order of Volatility .....	49
Documenting the Scene .....	49
Photography .....	50
Notes .....	51
Chain of Custody .....	52
Marking Evidence .....	52
Cloning .....	52
Purpose of Cloning .....	54
The Cloning Process .....	54
Forensically Clean Media .....	55
Forensic Image Formats .....	55
Risks and Challenges .....	55
Value in eDiscovery .....	56
Live System versus Dead System .....	56
Live Acquisition Concerns .....	56
Advantage of Live Collection .....	57
Principles of Live Collection .....	58
Conducting and Documenting a Live Collection .....	58
Hashing .....	59
Types of Hashing Algorithms .....	59
Hashing Example .....	59
Uses of Hashing .....	60
Final Report .....	61
Summary .....	61
References .....	62
<b>CHAPTER 5 Windows System Artifacts .....</b>	<b>65</b>
Introduction .....	65
Deleted Data .....	66
Hibernation File (Hiberfile.sys) .....	66
Sleep .....	67
Hibernation .....	67
Hybrid Sleep .....	67
Registry .....	67
Registry Structure .....	68

Attribution .....	69
External Drives .....	70
Print Spooling .....	70
Recycle Bin .....	70
Metadata .....	72
Removing Metadata .....	74
Thumbnail Cache .....	75
Most Recently Used (MRU) .....	76
Restore Points and Shadow Copy .....	76
Restore Points .....	76
Shadow Copies .....	77
Prefetch .....	78
Link Files .....	78
Installed Programs .....	79
Summary .....	79
References .....	80
 <b>CHAPTER 6 Antiforensics .....</b>	<b>81</b>
Introduction .....	81
Hiding Data .....	83
Encryption .....	83
What Is Encryption? .....	83
Early Encryption .....	84
Algorithms .....	85
Key Space .....	86
Some Common Types of Encryption .....	86
Breaking Passwords .....	88
Password Attacks .....	89
Brute Force Attacks .....	89
Password Reset .....	90
Dictionary Attack .....	90
Steganography .....	92
Data Destruction .....	94
Drive Wiping .....	94
Summary .....	100
References .....	100
 <b>CHAPTER 7 Legal .....</b>	<b>103</b>
Introduction .....	103
The Fourth Amendment .....	104

Criminal Law—Searches without a Warrant .....	104
Reasonable Expectation of Privacy .....	104
Private Searches .....	105
E-mail .....	105
The Electronic Communications Privacy Act (ECPA) .....	105
Exceptions to the Search Warrant Requirement .....	105
Searching with a Warrant .....	108
Seize the Hardware or Just the Information? .....	109
Particularity .....	109
Establishing Need for Off-Site Analysis .....	109
Stored Communications Act .....	110
Electronic Discovery (eDiscovery) .....	111
Duty to Preserve .....	111
Private Searches in the Workplace .....	112
Expert Testimony .....	113
Summary .....	114
References .....	115
<b>CHAPTER 8 Internet and E-Mail .....</b>	<b>117</b>
Introduction .....	117
Internet Overview .....	117
Peer-to-Peer (P2P) .....	119
The INDEX.DAT File .....	120
Web Browsers—Internet Explorer .....	120
Cookies .....	120
Temporary Internet Files, a.k.a. web Cache .....	121
Internet History .....	122
Internet Explorer Artifacts in the Registry .....	123
Chat Clients .....	124
Internet Relay Chat (IRC) .....	125
ICQ “I Seek You” .....	125
E-Mail .....	126
Accessing E-mail .....	126
E-mail Protocols .....	126
E-mail as Evidence .....	126
E-mail—Covering the Trail .....	127
Tracing E-mail .....	127
Reading E-mail Headers .....	128
Social Networking Sites .....	129
Summary .....	129
References .....	130

<b>CHAPTER 9 Network Forensics .....</b>	<b>131</b>
Introduction .....	131
Social Engineering .....	132
Network Fundamentals .....	132
Network Types .....	133
Network Security Tools .....	135
Network Attacks .....	135
Incident Response .....	137
Network Evidence and Investigations .....	139
Network Investigation Challenges .....	141
Summary .....	141
References .....	142
<b>CHAPTER 10 Mobile Device Forensics .....</b>	<b>145</b>
Introduction .....	145
Cellular Networks .....	146
Cellular Network Components .....	147
Types of Cellular Networks .....	148
Operating Systems .....	149
Cell Phone Evidence .....	150
Call Detail Records .....	151
Collecting and Handling Cell Phone Evidence .....	152
Subscriber Identity Modules .....	154
Cell Phone Acquisition: Physical and Logical .....	155
Cell Phone Forensic Tools .....	155
Global Positioning Systems (GPS) .....	157
Summary .....	161
References .....	161
<b>CHAPTER 11 Looking Ahead: Challenges and Concerns .....</b>	<b>163</b>
Introduction .....	163
Standards and Controls .....	164
Cloud Forensics (Finding/Identifying Potential Evidence Stored in the Cloud) .....	165
What Is Cloud Computing? .....	165
The Benefits of the Cloud .....	166
Cloud Forensics and Legal Concerns .....	166
Solid State Drives (SSD) .....	167
How Solid State Drives Store Data .....	167
The Problem: Taking out the Trash .....	168

Speed of Change .....	169
Summary .....	170
References .....	171
INDEX .....	173

This page intentionally left blank

Seal Team Six tore the hard drives from Osama bin Laden's computers. Some of Michael Jackson's final words were captured on an iPhone. Google searches for chloroform played a central role in the trial of Casey Anthony. This list could go on and on. Digital forensics is used to keep us safe, to ensure justice is done and company and taxpayer resources aren't abused. This book is your first step into the world of digital forensics. Welcome!

Digital forensics is used in a number of arenas, not just in catching identity thieves and Internet predators. For example, it's being used on the battlefields of Afghanistan to gather intelligence. The rapid exploitation of information pulled from cell phones and other devices is helping our troops identify and eliminate terrorists and insurgents.

It's being used in the multibillion-dollar world of civil litigation. Gone are the days when opposing parties exchanged boxes of paper memos, letters, and reports as part of the litigation process. Today, those documents are written in 1s and 0s rather than ink. They are stored on hard drives and backup tapes rather than in filing cabinets.

Digital forensics helps combat the massive surge in cybercrime. Identity thieves, child pornographers, and "old school" criminals are all using and leveraging technology to facilitate their illegal activities.

Finally, it's being used in the workplace to help protect both companies and government entities from the misuse of their computer systems.

## INTENDED AUDIENCE

As the title suggests, this is a beginner's book. The only assumption is that you have a fundamental understanding or familiarity of computers and other digital devices. If you have a moderate or advanced understanding of digital forensics, this book may not be for you. As part of Syngress's "Basics" series, I wrote this book more as a broad introduction to the subject rather than an all-encompassing tome. I've tried to use as much "plain English" as possible, making it (hopefully) an easier read.

I'd like to emphasize that this is an introductory book that is deliberately limited in length. Given that, there is much that couldn't be covered in depth or even covered at all. Each chapter could be a book all by itself. There are many wonderful books out there that can help further your understanding. I sincerely hope you don't stop here.

## **ORGANIZATION OF THIS BOOK**

The book is organized in a fairly straightforward way. Each chapter covers a specific type of technology and begins with a basic explanation of the technology involved. This is a necessity in order to really understand the forensic material that follows.

To help reinforce the material, the book also contains stories from the field, case examples, and Q and A with a cryptanalyst as well as a specialist in cell phone forensics.

### **Chapter 1 – Introduction**

What exactly is digital forensics? [Chapter 1](#) seeks to define digital forensics and examine how it's being used. From the battlefield to the boardroom to the courtroom, digital forensics is playing a bigger and bigger role.

### **Chapter 2 – Key Technical Concepts**

Understanding how computers create and store digital information is a perquisite for the study of digital forensics. It is this understanding that enables us to answer questions like "How was that artifact created?" and "Was that generated by the computer itself, or was it a result of some user action?" We'll look at binary, how data are stored, storage media, and more.

### **Chapter 3 – Labs and Tools**

In "Labs and Tools," we look at the digital forensic environment and hardware and software that are used on a regular basis. We will also examine standards used to accredit labs and validate tools. Those standards are explored along with quality assurance, which is the bedrock of any forensic operation. Quality assurance seeks to ensure that results generated by the forensic examination are accurate.

### **Chapter 4 – Collecting Evidence**

How the digital evidence is handled will play a major role in getting that evidence admitted into court. [Chapter 4](#) covers fundamental forensically sound practices that you can use to collect the evidence and establish a chain of custody.

### **Chapter 5 – Windows System Artifacts**

The overwhelming odds are that you have a Windows-based computer on your desk, in your briefcase, or both. It's a Windows world. (No disrespect, Mac people. I'm one of you.) With over a 90% market share, it clearly represents the bulk of our work. [Chapter 5](#) looks at many of the common Windows artifacts and how they are created.

## Chapter 6 – Antiforensics

The word is out. Digital forensics is not the secret it once was. Recovering digital evidence, deleted files, and the like is now common place. It's regularly seen on such shows as NCIS and CSI. The response has been significant. There are now many tools and techniques out there that are used to hide or destroy data. These are examined in [Chapter 6](#).

## Chapter 7 – Legal

Although a “forensic” science, the legal aspects of digital forensics can’t be divorced from the technical. In all but certain military/intelligence applications, the legal authority to search is a perquisite for a digital forensics examination. [Chapter 7](#) examines the Fourth Amendment, as well as reasonable expectations of privacy, private searches, searching with and without a warrant, and the Stored Communications Act.

## Chapter 8 – Internet and E-Mail

Social networks, e-mail, chat logs, and Internet history represent some of the best evidence we can find on a computer. How does this technology work? Where is this evidence located? These are just a few of the questions we’ll answer in [Chapter 8](#).

## Chapter 9 – Network Forensics

We can find a network almost anywhere, from small home networks to huge corporate ones. Like computers and cell phones, we must first understand how things work. To that end, [Chapter 9](#) begins with networking basics. Next, we start looking at how networks are attacked and what role digital forensics plays in not only the response, but how perpetrators can be traced.

## Chapter 10 – Mobile Device Forensics

Small-scale mobile devices such as cell phones and GPS units are everywhere. These devices are in many respects pocket computers. They have a huge potential to store evidence. Digital forensics must be as proficient with these devices as they are desktop computers. We’ll look at the underlying technology powering cell phones and GPS units as well as the potential evidence they could contain.

## Chapter 11 – Looking Ahead: Challenges and Concerns

There are two “game-changing” technologies that are upon us that will have a huge impact on not only the technical aspect of digital forensics but the legal piece as well. The technology driving solid state hard drives negates much of the traditional “bread and butter” of digital forensics. That is our ability to recover deleted data. As of today, there is no answer to this problem.

Cloud computing creates another major hurdle. In the cloud, data are stored in a complex virtual environment that could physically be located anywhere in the world. This creates two problems; from a technical standpoint, there is an alarming lack of forensic tools that work in this environment. Deleted files are also nearly impossible to recover. Legally, it's a nightmare. With data potentially being scattered across the globe, the legal procedures and standards vary wildly. Although steps are being taken to mitigate this legal dilemma, the situation still persists today.

Being in its infancy, the digital forensics community still has work to do regarding how it conducts its business, especially in relation to the other more traditional disciplines. [Chapter 11](#) will explore this issue.

# Acknowledgments

Although my name may be on the cover, this book would not have been possible without the help and support of many people. First, I'd like to thank my family, particularly my wife Lora, and my two girls, Abby and Rae. Their patience, understanding, and willingness to "pick up my slack" while I wrote was invaluable. Thank you, ladies.

Next I'd like to thank Nick Drehel, Rob Attoe, Lt. Lannie Hilboldt, Chris Vance, and Nephi Allred for sharing their expertise and experiences. I have no doubt their contributions made this a better book.

My Chair, Dr. Mike Little, and my Dean, Dr. Charles Somerville, also helped make this book a reality. It would have been impossible for me to write this book and still do my "day job" without their support and assistance. Thank you, gentlemen.

I'd like to thank my Editor, Heather Scherer, and my Tech Editor, Jonathan Rajewski, for keeping me on task and on point. Danielle Miller, my Project Manager at Syngress, deserves my thanks as well for putting up with my last minute editing.

Many thanks go to Jennifer Rehme and Jonathan Sisson. Jennifer, as my GA, helped keep me afloat during the semester handling much of my grading and research for this book and other projects. Jonathan, a digital forensics student here at Marshall, created most of the graphics for this book. I have no doubt that each will be wildly successful and real contributors to the forensic science community. I wish you both nothing but continued success after graduation.

Finally, I'd like to thank Angelina Ward for giving me this opportunity.

This page intentionally left blank

# About the Author

xxi



**John Sammons** is an Assistant Professor at Marshall University in Huntington, West Virginia. John teaches digital forensics, electronic discovery, information security and technology in the Department of Integrated Science and Technology. He is also the founder and Director of the Appalachian Institute of Digital Evidence. AIDE is a non-profit organization that provides research and training for digital evidence professionals including attorneys, judges, law enforcement and information security practitioners in the private sector.

Prior to joining the faculty at Marshall, John co-founded Second Creek Technologies, a digital forensics and electronic discovery firm. While at Second Creek, John served as the Managing Partner and CEO. John is a contract instructor for AccessData and is certified by them as both an instructor and examiner. He is a former Huntington Police officer and currently serves as an investigator for the Cabell County (WV) Prosecutors Office. As an investigator, he focuses on Internet crimes against children and child pornography. John is a member of the FBI WV Cybercrime Task Force. John routinely provides training for the legal and law enforcement communities in the areas of digital forensics and electronic discovery. He is an Associate Member of the American Academy of Forensic Sciences, the High Technology Crime Investigation Association, the Southern Criminal Justice Association, and Infragard.

This page intentionally left blank

# About the Technical Editor

xxiii

**Jonathan Rajewski** (EnCe, CCE, CISSP, CFE, CSI, SANS Lethal Forensicator) is an Assistant Professor in the Computer & Digital Forensic program at Champlain College. Aside from his teaching responsibilities he is member of the Vermont Internet Crimes Task Force serving law enforcement and governmental entities. He is also a Director and Principle Investigator with the Senator Patrick Leahy Center for Digital Investigation. In his prior life he was a Global Senior Digital Forensic Consultant with Protiviti. He was recently honored as 2011 Digital Forensic Examiner of the Year by [www.forensic4cast.com](http://www.forensic4cast.com).

His high degree of professionalism, passion, and experience in the detection and prevention of white-collar crime complements his ability to teach, manage, and conduct digital forensic investigations. Jonathan has a keen ability to articulate very technical topics and present in such way that's understandable to both experienced and nontechnical audiences. Jonathan is also the author of the 2011->future Undergraduate Digital Forensic curriculum at Champlain College.

Jonathan has served many high profile confidential clients and has worked alongside many governmental and corporate teams. Jonathan holds a B.S. in Economic Crime Investigation from Hilbert College and an M.S. in Managing Innovation & Information Technology from Champlain College. Jonathan resides in Vermont with his family.

This page intentionally left blank

# CHAPTER 1

# Introduction

1

## Information in This Chapter:

- What Is Forensic Science?
- What Is Digital Forensics?
- Uses of Digital Forensics
- Role of the Forensic Examiner in the Judicial System

“Each betrayal begins with trust.”

— “Farmhouse” by the band Phish

## INTRODUCTION

Your computer will betray you. This is a lesson that many CEO's, criminals, politicians, and ordinary citizens have learned the hard way. You are leaving a trail, albeit a digital one; it's a trail nonetheless. Like a coating of fresh snow, these 1s and 0s capture our “footprints” as we go about our daily life.

Cell phone records, ATM transactions, web searches, e-mails, and text messages are a few of the footprints we leave. As a society, our heavy use of technology means that we are literally drowning in electronically stored information. And the tide keeps rolling in. Don't believe me? Check out these numbers from the research company IDC:

- The digital universe (all the digital information in the world) will reach 1.2 million petabytes in 2010. That's up by 62% from 2009.

If you can't get your head around a petabyte, maybe this will help:

“One petabyte is equal to: 20 million, four-drawer filing cabinets filled with text or 13.3 years of HD-TV video.”

(Mozy, 2009)

The impact of our growing digital dependence is being felt in many domains, not the least of which is the legal system. Everyday, digital evidence is finding

its way into the world's courts. This is definitely not your father's litigation. Gone are the days when records were strictly paper. This new form of evidence presents some very significant challenges to our legal system. Digital evidence is considerably different from paper documents and can't be handled in the same way. Change, therefore, is inevitable. But the legal system doesn't turn on a dime. In fact, it's about as nimble as the Titanic. It's struggling now to catch-up with the blinding speed of technology.

Criminal, civil, and administrative proceedings often focus on digital evidence, which is foreign to many of the key players, including attorneys and judges. We all know folks who don't check their own e-mail or even know how to surf the Internet. Some lawyers, judges, businesspeople, and cops fit squarely into that category as well. Unfortunately for those people, this blissful ignorance is no longer an option.

Where law-abiding society goes, the bad guys will be very close behind (if not slightly ahead). They have joined us on our laptops, cell phones, iPads, and the Internet. Criminals will always follow the money and leverage any tools, including technology, that can aid in the commission of their crimes.

Although forensic science has been around for years, digital forensics is still in its infancy. It's still finding its place among the other more established forensic disciplines, such as DNA and toxicology. As a discipline, it is where DNA was many years ago. Standards and best practices are still being developed.

Digital forensics can't be done without getting under the hood and getting your hands dirty, so to speak. It all starts with the 1's and 0's. This binary language underpins not only the function of the computer but how it stores data as well. We need to understand how these 1's and 0's are converted into the text, images, and videos we routinely consume and produce on our computers.

## **WHAT IS FORENSIC SCIENCE?**

Let's start by examining what it's not. It certainly isn't Humvees, sunglasses, and expensive suits. It isn't done without lots of paperwork, and it's never wrapped up in sixty minutes (with or without commercials). Now that we know what it isn't, let's examine what it is. Simply put, **forensics** is the application of science to solve a legal problem. In forensics, the law and science are forever integrated. Neither can be applied without paying homage to the other. The best scientific evidence in the world is worthless if it's inadmissible in a court of law.

## **WHAT IS DIGITAL FORENSICS?**

There are many ways to define digital forensics. In *Forensic Magazine*, Ken Zatyko defined digital forensics this way:

"The application of computer science and investigative procedures for a legal purpose involving the analysis of digital evidence after proper

search authority, chain of custody, validation with mathematics, use of validated tools, repeatability, reporting, and possible expert presentation.”

(Zatyko, 2007)

Digital forensics encompasses much more than just laptop and desktop computers. Mobile devices, networks, and “cloud” systems are very much within the scope of the discipline. It also includes the analysis of images, videos, and audio (in both analog and digital format). The focus of this kind of analysis is generally authenticity, comparison, and enhancement.

## USES OF DIGITAL FORENSICS

Digital forensics can be used in a variety of settings, including criminal investigations, civil litigation, intelligence, and administrative matters.

### Criminal Investigations

When you mention digital forensics in the context of a criminal investigation, people tend to think first in terms of child pornography and identity theft. Although those investigations certainly focus on digital evidence, they are by no means the only two. In today's digital world, electronic evidence can be found in almost any criminal investigation conducted. Homicide, sexual assault, robbery, and burglary are just a few of the many examples of “analog” crimes that can leave digital evidence.

One of the major struggles in law enforcement is to change the paradigm of the police and get them to think of and seek out digital evidence. Everyday digital devices such as cell phones and gaming consoles can hold a treasure trove of evidence. Unfortunately, none of that evidence will ever see a courtroom if it's not first recognized and collected. As time moves on and our law enforcement agencies are replenished with “younger blood,” this will become less and less of a problem.

#### *BIND. TORTURE. KILL.*

The case of Dennis Rader, better known as the BTK killer, is a great example of the critical role digital forensics can play in a criminal investigation. This case had national attention and, thanks to digital forensics, was solved thirty years later. To all that knew him before his arrest, Dennis Rader was a family man, church member, and dedicated public servant. What they didn't know was that he was also an accomplished serial killer. Dennis Rader, known as Bind, Torture, Kill (BTK), murdered ten people in Kansas from 1974 to 1991. Rader managed to avoid capture for over thirty years until technology betrayed him.

After years of silence, Rader sent a letter to the Wichita *Eagle* newspaper declaring that he was responsible for the 1986 killing of a young mother. The letter was received by the *Eagle* on March 19, 2004. After conferring with the FBI's Behavioral Analysis Unit, the police decided to attempt to communicate with BTK through the media.

In January 2005, Rader left a note for police, hidden in a cereal box, in the back of a pickup truck belonging to a Home Depot employee. In the note, he said:

“Can I communicate with Floppy and not be traced to a computer. Be honest. Under Miscellaneous Section, 494, (Rex, it will be OK), run it for a few days in case I’m out of town-etc. I will try a floppy for a test run some time in the near future-February or March.”

The police did the only thing they could. They lied. As directed, they responded (via an ad in the *Eagle*) on January 28. The ad read “Rex, it will be ok, Contact me PO Box 1st four ref.numbers at 67202.”

On February 16, a manila envelope arrived at KSAS, the Fox affiliate in Wichita. Inside was a purple floppy disc from BTK. The disc contained a file named “Test A.rtf.” (The .rtf extension stands for “Rich Text File”). A forensic exam of the file struck gold. The file’s metadata (the data about the data) gave investigators the leads they had been waiting over thirty years for. Aside from the “Date Created” (Thursday, February 10, 2005 6:05:34 PM) and the “Date Modified” (Monday, February 14, 2005 2:47:44 PM) were the “Title” (Christ Lutheran Church) and “Last Saved By:” (Dennis).

Armed with this information, investigators quickly logged on to the Christ Lutheran Church web site. There they found that Dennis Rader was the president of the church’s Congregation Council. The noose was tightening, but it wasn’t tight enough. Investigators turned to DNA to make the case airtight. Detectives went on to obtain a DNA sample from Rader’s daughter and compared it to DNA from BTK. The results proved that BTK was her father. On February 25, three days after the DNA sample arrived at the lab, Rader was arrested, sealing the fate of BTK. He is currently serving ten consecutive life sentences (*Wichita Eagle*).

## Civil Litigation

The use of digital forensics in civil cases is big business. In 2011, the estimated total worth of the electronic discovery market is somewhere north of \$780 million (Global EDD Group). As part of a process known as **Electronic Discovery (eDiscovery)**, digital forensics has become a major component of much high dollar litigation. eDiscovery “refers to any process in which electronic data is sought, located, secured, and searched with the intent of using it as evidence in a civil or criminal legal case” (TechTarget, 2005).

In a civil case, both parties are generally entitled to examine the evidence that will be used against them prior to trial. This legal process is known as “discovery.” Previously, discovery was largely a paper-based exercise, with each party exchanging reports, letters, and memos; however, the introduction of digital forensics and eDiscovery has greatly changed this practice.

The proliferation of the computer has rendered that practice nearly extinct. Today, parties no longer talk about filing cabinets, ledgers, and memos; they talk about hard drives, spreadsheets, and file types. Some paper-based materials may

come into play, but it's more the exception than the rule. Seeing the evidentiary landscape rapidly changing, the courts have begun to modify the rules of evidence. The rules of evidence, be they state or federal rules, govern how digital evidence can be admitted during civil litigation. The Federal Rules of Civil Procedure were changed in December 2006 to specifically address how electronically stored information is to be handled in these cases.

Digital evidence can quickly become the focal point of a case, no matter what kind of legal proceeding it's used in. The legal system and all its players are struggling to deal with this new reality.

## Intelligence

Terrorists and foreign governments, the purview of our intelligence agencies, have also joined the digital age. Terrorists have been using information technology to communicate, recruit, and plan attacks. In Iraq and Afghanistan, our armed forces are exploiting intelligence collected from digital devices brought straight from the battlefield. This process is known as **DOMEX (Document and Media Exploitation)**. DOMEX is paying large dividends, providing actionable intelligence to support the soldiers on the ground (U.S. Army).

### MOUSSAOUI

It's well documented that the 9-11 hijackers sought out and received flight training in order to facilitate the deadliest terrorist attack ever on U.S. soil. Digital forensics played a role in the investigation of this aspect of the attack.

On August 16, 2001, Zacarias Moussaoui was arrested by INS agents in Eagan, Minnesota, for overstaying his visa. Agents also seized a laptop and floppy disk. After obtaining a search warrant, the FBI searched these two items on September 11, 2001. During the analysis, they found evidence of a Hotmail account ([pilotz123@hotmail.com](mailto:pilotz123@hotmail.com)) used by Moussaoui. He used this account to send e-mail to the flight school as well as other aviation organizations.

For those not familiar with Hotmail accounts, it's a free e-mail service offered by Microsoft, similar to Gmail and Yahoo!. They're quite easy to get and only require basic subscriber information. This information is essentially meaningless, because none of the information is verified. During the exam of Moussaoui's e-mail, agents were also able to analyze the Internet protocol connection logs. One of the IP addresses identified was assigned to "PC11" in a computer lab at the University of Oklahoma.

The investigation further showed that Moussaoui and the rest of the nineteen hijackers made extensive use of computers at a variety of Kinko's store locations in other cities. Agents arrived at the Kinko's in Eagan hoping to uncover evidence. They were disappointed to learn that this specific Kinko's makes a practice of erasing the drives on their rental computers every day. Now forty-four days after Moussaoui's visit, the agents felt the odds of recovering any evidence would be somewhere between slim and none. They didn't bother examining the Kinko's computer. The Eagan store isn't alone. Other locations make a routine practice

of erasing or reimaging the rental computers as well. This is done periodically, some as soon as twenty-four hours, others as long as thirty days. The drives are erased to improve the performance and reliability of the computers as well as to protect the privacy of its customers (Lawler, 2002).

## **Administrative Matters**

Digital evidence can also be valuable for incidents other than litigation and matters of national security. Violations of policy and procedure often involve some type of electronically stored information, for example, an employee operating a personal side business, using company computers while on company time. That may not constitute a violation of the law, but it may warrant an investigation by the company.

### *THE SECURITIES AND EXCHANGE COMMISSION (SEC)*

In 2008, while the economy was in the beginning of its historic downward spiral, the Securities and Exchange Commission (SEC) should have been policing Wall Street. Instead, many of them were spending hours of their days watching pornography. Computer forensics played heavily in this administrative investigation.

In August 2007, the SEC's Office of the Inspector General (OIG) officially opened an investigation into the potential misuse of governmental computers. The OIG was alerted to a potential problem after firewall logs identified several users that had received access denials for Internet pornography. The SEC firewall was configured to block and log this kind of traffic. The logs showed that this employee attempted to visit sites such as [www.thefetishvault.com](http://www.thefetishvault.com), [www.bondagetemple.com](http://www.bondagetemple.com), [www.rape-cartoons.com](http://www.rape-cartoons.com), and [www.pornobaron.com](http://www.pornobaron.com).

On September 5, 2007, the OIG notified the Regional Director that one of his employees was the focus of an investigation regarding the misuse of their government computer. On September 19 this same employee reported that her laptop hard drive suddenly crashed. She was issued a replacement drive and went back to work. A forensic analysis of her hard drive found 592 pornographic images (in her temporary Internet files) along with evidence that she had attempted to bypass the SEC's Internet filters.

The scope of this investigation eventually expanded considerably, identifying several more employees or contractors that were viewing pornography on their governmental computers while at work.

After further investigation, the OIG found that:

- A Regional Staff Accountant received over sixteen thousand access denials for pornographic web sites in a single month.
- A Senior Counsel for the Division of Enforcement accessed pornography from his SEC laptop computer on multiple occasions. His hard drive contained 775 pornographic images.
- A Senior Attorney at Headquarters downloaded so much pornography that he literally ran out of disk space.

The report went on to list the policies that prohibited these behaviors. It says in part:

"SECR 24-4.3 TK IIIC, provides that '[m]isuse or inappropriate personal use of government office equipment includes the creation, download, viewing, storage, copying, or transmission of materials related to gambling, weapons, terrorist activities, and any other illegal activities or activities otherwise prohibited etc' id at 3. The cover memorandum to SEC employees accompanying SECR 24-4.3 states that employees are prohibited from "accessing materials related to illegal or prohibited activities, including sexually explicit materials."

In the end, as this was not considered to be a crime, the entire matter was referred to the SEC administration for disposition (U.S. Securities and Exchange Commission).

## LOCARD'S EXCHANGE PRINCIPLE

Locard's exchange principle says that in the physical world, when perpetrators enter or leave a crime scene, they will leave something behind and take something with them. Examples include DNA, latent prints, hair, and fibers ([Saferstein, 2006](#)).

The same holds true in digital forensics. Registry keys and log files can serve as the digital equivalent to hair and fiber ([Carvey, 2005](#)). Like DNA, our ability to detect and analyze these artifacts relies heavily on the technology available at the time. Look at the numerous cold cases that are being solved as a result of the significant advances in DNA science. Viewing a device or incident through the "lens" of Locard's principle can be very helpful in locating and interpreting not only physical but digital evidence as well.

## SCIENTIFIC METHOD

As an emerging discipline in forensic science, digital forensics is undergoing some expected growing pains. As of today, digital forensics lacks the vast foundation and long-term track record set by forensic DNA. DNA is now considered by many to be the "gold standard" of the forensic sciences. Digital forensics simply lacks the years of development, testing, refining, and legal challenges DNA has undergone since its inception.

Plotting the course forward are several organizations that are looked on to establish the protocols, standards, and procedures that will push digital forensics ahead. The following sections provide more information on these important organizations.

## ORGANIZATIONS OF NOTE

There are several organizations that make significant contributions to the discipline of digital forensics year in and year out. These organizations not only set standards and establish best practices, they provide leadership as well. Examiners

should be familiar with these entities, the roles they play, and the contributions they make. As professionals, it's our responsibility to participate in one or more of these organizations.

## **Scientific Working Group on Digital Evidence**

<http://www.swgde.org/>

Standards and techniques are an essential part of valid and accurate forensic science. They are its foundation, its core. Along with other federal agencies, the FBI has supported the formation and efforts of a wide range of Scientific Working Groups (SWGs) and Technical Working Groups (TWGs) (Federal Bureau of Investigation). These collaborative groups draw their members from "forensic, industrial, commercial, academic and in some cases international communities" (Federal Bureau of Investigation). Some examples include the Scientific Working Group for DNA Analysis Methods (SWGDAM) and the Scientific Working Group for Firearms and Toolmarks (SWGUN). Digital evidence has now joined the party with the formation of SWGDE.

Formed in 1998, the **Scientific Working Group on Digital Evidence (SWGDE)** is made up of "federal government agency, state or local law enforcement agency involved in the digital and multi-media forensic profession" (Scientific Working Group on Digital Evidence).

The mission of SWGDE is as follows: "Brings together organizations actively engaged in the field of digital and multimedia evidence to foster communication and cooperation as well as ensuring quality and consistency within the forensic community" (Scientific Working Group on Digital Evidence).

## **American Academy of Forensic Sciences**

<http://www.aafs.org/>

The **American Academy of Forensic Sciences (AAFS)** is considered the premier forensic organization in the world. Members of the Academy work for the National Institute of Standards and Technology (NIST) and National Academy of Sciences (NAS). The directors of most federal crime labs are members of AAFS. Members of AAFS are also active in the various Scientific Working Groups including SWGDE. The Academy plays a critical role in developing consensus standards of practice for the forensic community.

The Forensic Science Education Programs Accreditation Commission (FEPAC) was a creation of AAFS to ensure quality forensic science education and background for future forensic scientists.

The AAFS has approximately six thousand members and is divided into "eleven sections spanning the forensic enterprise." The Academy comprises "physicians, attorneys, dentists, toxicologists, physical anthropologists, document examiners, psychiatrists, physicists, engineers, criminalists, educators, digital evidence experts, and others" (American Academy of Forensic Sciences).

The Digital & Multimedia Sciences section represents digital forensics. As of November 3, 2010, the Digital Evidence section had 103 members. Despite the name, the reach of the AAFS is truly global, representing over sixty countries around the world (American Academy of Forensic Sciences).

### **American Society of Crime Laboratory Directors/Laboratory Accreditation Board**

<http://www.ascld-lab.org/index.htm>

ASCLD/LAB (pronounced as-clad lab). The ASCLD is to forensic laboratories what Underwriters Labs is to household products. ASCLD/LAB is the “oldest and most well known crime/forensic laboratory accrediting body in the world.” ASCLD/LAB accredited labs are the “gold standard” in the world of forensics. A lab becomes accredited only after successfully meeting all of the standards and requirements set forth in the ASCLD/LAB accreditation manual. These requirements and standards cover every aspect of a lab’s operation and must be strictly followed. Adherence to these standards must be thoroughly and completely documented (American Society of Crime Laboratory Directors/Laboratory Accreditation Board).

### **National Institute of Standards and Technology (NIST)**

<http://www.nist.gov/itl/ssd/computerforensics.cfm>

National Institute of Standards and Technology (NIST) was founded in 1901 and is a part of the U.S. Department of Commerce. It was the first federal physical science research laboratory. Some of NIST’s areas of focus include bioscience and health, chemistry, physics, math, quality, and information technology (National Institute of Standards and Technology).

NIST is heavily involved in digital forensics. Some of the programs and projects include:

- National Initiative Cyber Security Education (NICE)—A national cyber-security education program teaching sound cyber practices that will improve the country’s security.
- National Software References Library—A collection of known software file signatures that can be used by examiners to quickly exclude files that have no investigative value. This would include things like operating system files. This can really reduce the time spent on an examination.
- Computer Forensic Tool Testing—Intended to develop testing methodologies and standards for forensic hardware and software.

(National Institute of Standards and Technology)

### **American Society for Testing and Materials (ASTM)**

<http://www.astm.org/Standards/E2763.htm>

Another major player in the development of standards is ASTM. ASTM is a global organization that has developed approximately twelve thousand standards that

are used to “improve product quality, enhance safety, facilitate market access and trade, and build consumer confidence.” ASTM, founded in 1898, comprises about 30,000 members broken into 141 committees. The Forensics Sciences committee, known as E30, is further divided into several subcommittees. The Digital and Multimedia Evidence subcommittee is known as E30.12 (ASTM).

## **ROLE OF THE FORENSIC EXAMINER IN THE JUDICIAL SYSTEM**

The digital forensics practitioner most often plays the role of an expert witness. What makes them different than nonexpert witnesses? Other witnesses can only testify to what they did or saw. They are generally limited to those areas and not permitted to render an opinion. Experts, by contrast, can and often do give their opinion. What makes someone an “expert?” In the legal sense, it’s someone who can assist the judge or jury to understand and interpret evidence they may be unfamiliar with. To be considered an expert in a court of law, one doesn’t have to possess an advanced academic degree. An expert simply must know more about a particular subject than the average lay person. Under the legal definition, a doctor, scientist, baker, or garbage collector could be qualified as an expert witness in a court of law. Individuals are qualified as experts by the court based on their training, experience, education, and so on (Saferstein, 2011).

What separates a qualified expert from a truly effective one? It is their ability to communicate with the judge and jury. They must be effective teachers. The vast majority of society lacks technical understanding to fully grasp this kind of testimony without at least some explanation. Digital forensic examiners must carry out their duties without bias. Lastly, a digital forensics examiner must go where the evidence takes them without any preconceived notions.

### **The CSI Effect**

It seems that everyone either does or has watched one or more versions of the popular TV series *CSI*. These shows and others like it tend to convince jurors that some form of forensic science can solve any case. In other words, they now *expect* it. These unreasonable expectations can lead to incorrect verdicts. The jury could acquit a guilty defendant simply because no scientific evidence was presented, the presumption being that if the defendant was guilty, there would be some kind of scientific evidence to prove it (Saferstein, 2011).

## **SUMMARY**

In this chapter we looked at what forensic science, particularly digital forensics, is and is not. Forensic sciences aren’t the fast-paced crime-solving dramas that we watch on television, but a scientific method of collection, investigation and analysis used to solve some kind of legal problem. Digital forensics isn’t limited to computers. It encompasses any kind of electronic device that can

store data. These devices include cell phones, tablets, and GPS units just to name a few.

Digital forensics is applicable well beyond criminal investigations. It's used routinely in civil litigation, national and military intelligence matters as well as the private sector.

There are multiple organizations that help establish the standards and best practices used in digital forensics. These organizations include the American Academy of Forensic Sciences, the Scientific Working Group on Digital Evidence, and ASTM.

As a practitioner, communication skills are extremely important. You will spend a significant amount of time explaining your findings to police officers, attorneys, and clients. Most important, you must be able to explain these things to judges and juries. All of these stakeholders must be able to understand your methods and findings. Like all scientific evidence, digital evidence can be quite confusing and overwhelming. With this kind of testimony, it's very easy to lose people. Losing a judge or jury in a trial can have disastrous consequences such as having your findings ignored or misunderstood.

## References

- American Academy of Forensic Sciences. (n.d.). *About AAFS*. Retrieved February 4, 2011, from: <http://www.aafs.org/about-aafs>
- ASTM. (n.d.). *ABOUT: ASTM*. Retrieved February 23, 2011, from: <http://www.astm.org/ABOUT/aboutASTM.html>
- ASTM. (n.d.). *E30*. Retrieved February 23, 2011, from: <http://www.astm.org/COMMIT/SUBCOMMIT/E30.htm>
- ASTM. (n.d.). *Overview: ABOUT: ASTM*. Retrieved February 23, 2011, from: <http://www.astm.org/ABOUT/overview.html>
- Carvey, H. (2005, January 27). *Locard's Exchange Principle in the Digital World: Windows Incident Response*. Retrieved February 23, 2011, from: <http://windowsir.blogspot.com/2005/01/locards-exchange-principle-in-digital.html>
- Federal Bureau of Investigation. (n.d.). *Scientific Working Groups: Federal Bureau of Investigation*. Retrieved February 19, 2011, from: <http://www.fbi.gov/about-us/lab/swgs>
- Lawler, B. A. (2002, September 4). *Government's Response to Court's Order on Computer and Email Evidence*. Retrieved September 13, 2011, from FindLaw.com: [news.findlaw.com/hdocs/docs/moussaoui/usmoussaoui90402grsp.pdf](http://news.findlaw.com/hdocs/docs/moussaoui/usmoussaoui90402grsp.pdf)
- McKendrick, J. (2010, May 12). *Size of the Data Universe: 1.2 Zettabytes and Growing Fast*: ZDNet. Retrieved February 23, 2011, from: <http://www.zdnet.com/blog/service-oriented/size-of-the-data-universe-12-zettabytes-and-growing-fast/4750>
- Regional Computer Forensics Laboratory. (n.d.). *RCFL: Regional Computer Forensics Laboratory*. Retrieved February 4, 2011, from: <http://www.rcfl.gov/>
- Saferstein, R. (2006). *Criminalistics: An Introduction to Forensic Science* (College Edition). Upper Saddle River, New Jersey: Prentice Hall.
- Scientific Working Group on Digital Evidence. (n.d.). *Scientific Working Group on Digital Evidence—About Us*. Retrieved February 4, 2011, from: <http://www.swgde.org>
- Stuart, J., Nordby, J. J., & Bell, S. (2009). *Forensic Science: An Introduction to Scientific and Investigative Techniques*. February 20, 2009 (3rd ed.). Boca Raton, FL: CRC Press.

- U.S. Army. (n.d.). *Document and Media Exploitation (DOMEX): 2010 Army Posture Statement*. Retrieved February 23, 2011, from: [https://secureweb2.hqda.pentagon.mil/vdas\\_armyposurstatement/2010/information\\_papers/Document\\_and\\_Media\\_Exploitation\\_%28DOMEX%29.asp](https://secureweb2.hqda.pentagon.mil/vdas_armyposurstatement/2010/information_papers/Document_and_Media_Exploitation_%28DOMEX%29.asp)
- U.S. Department of Justice. (2009). *RCFL Annual Report for Fiscal Year 2009*. Washington, DC: U.S. Department of Justice.
- Zatyko, K. (n.d.). *Commentary: Defining Digital Forensics*. Retrieved February 19, 2011, from: <http://www.forensicmag.com/node/128>

# CHAPTER 2

# Key Technical Concepts

13

## Information in This Chapter:

- Basic Computer Operation
- Bits & Bytes
- File Extensions and File Signatures
- How Computers Store Data
- Random Access Memory
- Volatility of Data
- The Difference Between Computer Environments
- Active, Latent, and Archival Data
- The Difference Between Allocated and Unallocated Space
- Computer File Systems

## INTRODUCTION

Intimate knowledge of the inner workings of a computer is critical for the digital forensics practitioner. It's this knowledge that permits us to conduct a thorough examination of the evidence and render an accurate opinion. Simply put, we can't do our job without it. Not all processes and hardware hold the same value forensically. Memory and storage play a major role in almost any examination. The processor or CPU, by contrast, plays little if any role. This chapter takes a broad look at some of the technical details of basic computing. Its focus will be on the major areas that impact an investigation. There is no substitute for the mastery of this material. Our responsibilities as an expert witness include explaining technical subject matter in a way that the average person is able to understand.

## BITS, BYTES, AND NUMBERING SCHEMES

To the computer, things are pretty black and white. It's all about the 1s and 0s. Computers use a language called **binary**. In binary, there are only two possible outcomes: a 1 or a 0. Each 1 or 0 is called a bit. In mathematical terms, binary is classified as a base 2 numbering system. In comparison, we use a base 10 numeral system known as **decimal**. Decimal uses numerals 0–9. To speed things up,

computers work with larger collections of bits. These larger chunks of data are called **bytes**. A byte is made up of eight bits. It looks like this: 01101001.

How do bytes relate to letters and numbers? Each letter, number, space, and special character is represented by a single byte. For example, using the ASCII character set 01000001 represents an uppercase "A," while a lowercase "a" is 01100001.

Let's do a little experiment so that you can see this in action. Open a new text document (using a plain text editor, not a word processing application like MS Word) on your computer and type the phrase "Marshall University Digital Forensics." Now, count all the letters and spaces. Next, save and close the new text file to your desktop. Right click on the file and select properties. What's the file size? It should be 26 bytes, which is also the exact number of letters and spaces.

To get a broader perspective, let's look at all of the binary necessary to represent our sample phrase "Marshall University Digital Forensics":

```
010011010110001011100100111001101101000011000010110  
11000110110000100000010101010110110011010010111011  
0011001010111001001110011011010010111010001111001001  
0000001000100011010010110011101101001011101000110000  
101101100001000000100011001101110111001001100101011  
0111001110011011010010110001101110011
```

At first glance, that's a little tough to read, no doubt. Fortunately, there is a shorthand that we can use to make this more readable. This shorthand is called **hexadecimal**.

## Hexadecimal

Hexadecimal, or hex, is a base 16 system that is an expedient way to express binary numbers. Hex is expressed using the numerals 0–9 and the letters A–F. An uppercase "M" is expressed as 4D in hexadecimal. A lowercase "a" is 61. Quite often you will see a hexadecimal number expressed with the prefix 0x. This prefix or the suffix "h" is used to designate or identify it as a hexadecimal or base 16 number. Here is the same phrase (Marshall University Digital Forensics) expressed in hexadecimal:

```
4d 61 72 73 68 61 6D 6C 20 55 6E 69 76 65 72 73 69 74 79  
20 44 69 67 69 74 61 6D 20 46 6F 72 65 6E 73 69 63 73
```

If you look closer, you'll see the number "20" repeated throughout the string. The number "20" in hex represents a space.

## Binary to Text: ASCII and Unicode

So how do these 1s and 0s end up as As and Bs? Computers use encoding schemes to convert binary into something humans can read. There are two

encoding schemes we need to be concerned with, ASCII and Unicode. ASCII, the American Standard Code for Information Interchange, is the encoding scheme used for the English language. ASCII defines 128 characters, of which only 94 are actually printable. The rest are control characters used for spacing and processing. In contrast, **Unicode** is intended to represent all of the world's languages and consists of thousands of characters ([Unicode Inc., 2010](#)).

So, how is this relevant to digital forensics? In many instances, examiners must look at the data at the "bit" and "byte" level to find, extract, and interpret the evidence. This is most evident in a process called **file carving**. File carving is done to locate and mine out files from amorphous blobs of data, like the unallocated space (also known as drive-free space). The first step in the file carving process is to identify the potential file. Normally, the file is identified by the header, if it has one. Once the footer is found, the file can be extracted through a simple copy and paste as long as it is continuous. A fragmented file is far more difficult to recover ([Casey, 2011](#)). Having the ability to interpret binary and hex makes file carving possible.

## FILE EXTENSIONS AND FILE SIGNATURES

Fundamentally, **files** are strings or sequences of bits and bytes. Identifying a file can be done in a couple of different ways. **File extensions** are the most common. As users, we usually identify the file type by the file extension, if the system is configured. An operating system can be set such that file extensions are hidden. File extensions are the suffixes added to the end of a computer file name, indicating its format. Examples would include .docx and .pptx (for the latest versions of Microsoft Word and PowerPoint, respectively).

For our purposes, a file extension isn't the most reliable way to identify it. The file extension is very easily changed, requiring only a mouse click and a couple of key-strokes. You can try this yourself. In Windows, simply right click on the file name and rename it, changing the extension. Let's say we change the extension of a Word file to that of an image, JPEG for example. This is easily accomplished. On a Windows machine, simply click, slight pause, click again. On a Mac, it's click + Return. What happens when we try to open that file? Nothing. It won't open. Change it back and it opens right up.

Some people will attempt to take advantage of this ability to change file extensions as a way to conceal data, hiding them in plain sight. Forensically, this approach is not very effective. Forensic tools identify files based on the header, not the file extension. Many tools will even separate out those files whose header does not match the extension, making them easily discovered. This comparison is generally known as **file signature analysis**. [Figures 2.1 and 2.2](#) illustrate what happens when a file extension is changed.



## FIGURE 2.1

Here we've changed the file extension on "Smoking Gun.docx" to .mp3. Note that the icon has changed. Graphic courtesy of Jonathan Sisson.

Hex	Text	Filtered	Natural
410	OB BB 02 15 ED FF D9 D8-CF BC 3C E7 E4 15 6A 86		» » .iyüÜÜİüççä .j-
420	6D D4 3C 09 B4 97 85 34-0D 9F 2A 19 1E 28 39 81		mö< .. .4 .. * .. (9-
430	FD 8E F1 00 DB 75 24 46-6D 7A 9F 73 6D E9 11 BE		ý .. ñ .. ÜüsFmz .. smé .. k
440	81 C3 E8 98 43 FD 02 3D-09 09 FE 36 0B E8 6D 6F		.Äé .. Cý .. - .p6 .. émo
450	35 EB C5 F6 93 59 AF 9F-1C 71 F1 31 12 73 74 FF		Seäö .. Y- .. -qñ1 .. stý
460	8F 65 E3 36 96 2D 65 04-BB 1B 0C 1B B7 30 EC F6		-eä6 .. -e .. » .. -0iö
470	31 68 BE 70 FA 07 50 4B-07 08 8E C9 65 35 2F 02		lhkpü .. PK .. -ÉeS .. -
480	00 00 5E 07 00 00 50 4B-03 04 14 00 08 08 08 00		- .. ^ .. PK .. - ..
490	F7 6E 51 3F 00 00 00 00-00 00 00 00 00 00 00 00 00		=nQ? .. - ..
4a0	11 00 00 00 77 6F 72 64-2E 64 6F 63 75 6D 65 6E		...word/document
4b0	74 2E 78 6D 6C ED 56 4D-8F 9B 30 10 BD F7 57 10		t.xml iVM .. -0 .. M-W ..
4c0	DF B3 7C 94 AD B6 28 B0-87 92 56 95 DA 55 A4 A4		B .. 1 .. -g .. -V .. ÜUmn ..
4d0	BD 22 C7 18 B0 82 3F 64-4F 60 D3 5F 5F 3B 40 B2		W .. Ç .. -?d0 .. Ö .. _ .. ;@ ..
4e0	2B B5 55 54 F5 D0 03 17-CF 0C E3 F7 9E 6D 2C CF		+pÜTüD .. -I .. -ä .. -m .. I
4f0	AC 1E 9F 79 EB 75 54 1B-26 45 8A C2 BB 00 79 54		- .. -yëüT .. -E .. Ä .. -yT
500	10 59 32 51 A7 E8 DB EE-E3 F2 01 79 06 B0 28 71		-Y2QSeÜiäö .. y .. (q

**FIGURE 22**

FIGURE 2-1 Here is the hexadecimal view of "Smoking Gun.mp3." Note the highlighted file header showing this is actually a Word document. Graphic courtesy of Jonathan Sisson.

## STORAGE AND MEMORY

Where and how data are stored and written is one of the major fundamental concepts that must be learned. There is more than one way to write data. Today, data are generally created in three different ways: **electromagnetism**, **microscopic electrical transistors (flash)**, and **reflecting light** (CDs, DVDs, etc). Storage locations inside a computer serve different purposes. Some are for the short term, used to temporarily hold the data that the computer is using at the moment. The other is for more permanent, long-term keeping.

## Magnetic Disks

Most drives in today's computers read and write data magnetically. They will render each particle either magnetized or not magnetized. If the particle is magnetized, it's read as a 1. If not, it's read as a 0. The drives themselves are usually made up of aluminum platters coated with a magnetic material. These platters spin at very high speeds. The platters spin in the neighborhood of 7,000 rpm to 15,000 rpm. The speed could even be greater for high-end drives. These heavy-duty drives are typically found in servers or professional grade workstations. From a forensic standpoint, faster drive speeds can result in faster acquisitions.

Let's look at the major parts of a standard hard drive. The platters revolve around a small rod called a spindle. The data are physically written to the platter using a read/write head attached to an actuator arm, which is powered by the actuator itself. The actuator arm moves the head across the platter(s), reading and writing data. The read/write head floats on a cushion of air. The read/write head, as it's called, is barely floating above the platter surface, at a height less than the diameter of a human hair. These devices are really pretty amazing. [Figure 2.3](#) shows



**FIGURE 2.3**  
The inside of a typical magnetic drive.

us the inside of a typical magnetic drive. We can clearly see the platters, actuator arm, and the read/write head.

### Flash Memory

**Flash memory** is used in a wide range of devices. Thumb drives and memory cards provide reliable storage in a very portable package, allowing us to take more pictures and take our files on the road. Unlike other kinds of memory, flash memory retains our data even without electricity. Flash is made up of **transistors**. Each transistor is either carrying an electric charge or it isn't. When the transistor is charged, it is read as a "1"; without a charge it's read as a "0."

**Flash based hard drives** are starting to become more and more common. Unlike magnetic drives, flash drives are solid state, meaning that they have no moving parts. They are often referred to as an SSD or "**Solid State Drive**." They offer several significant advantages including increased speed, less susceptibility to shock, and lower power consumption.

SSDs will play a major role in computing and digital forensics going forward. Although these devices offer improved performance, they also present a major challenge to digital forensics. We'll take a deeper look at the momentous challenge presented by SSDs in [Chapter 11](#).

### Optical Storage

**Optical media** read and write data using a laser light along with a reflective material incorporated into optical discs. Optical discs are made of a polycarbonate base covered by a thin layer of aluminum. The disc is then coated with a clear acrylic material for protective purposes. During the manufacturing process, the disc's surface is embossed with tiny bumps. This series of bumps form one long, single, spiral track. A laser projects a highly focused beam of light onto the track. The light is reflected differently from the bumps and the spaces in between, called "**lands**." This change in reflectivity is what the system reads as binary (Brain). The most common types of optical storage media include CDs, DVDs, and Blu-ray discs (Brain).

### Volatile versus Nonvolatile Memory

**Memory** and **storage** are two terms that are somewhat synonymous when it comes to computers. They both refer to internal places where data are kept. Memory is used for the short-term storage, while storage is more permanent. No matter what you call it, there is a significant difference between the two, especially from a forensic perspective. That difference lies in the data's volatility. Data in RAM exist only as long as power is supplied. Once the power is removed (i.e., the machine is turned off), the data start to disappear. This behavior makes this kind of memory volatile. In contrast, files saved on your hard drive remain even after the computer is powered down, making it nonvolatile ([Cooper, 2004](#)).

RAM stores all the data that are currently being worked on by the Central Processing Unit (CPU). Data are fed from the RAM to the CPU, where they are executed. Traditionally, forensic analysis of a computer focused on the hard drive, as much of the evidence can be found there. Today, we're finding that's not always the case. Some instant messaging applications, for example, don't write to the hard drive unless the logging feature is turned on. AOL Instant Messenger and MSN fall into that category. So, if logging is off (which it is by default), the only evidence will be found in RAM while the machine is running.

## COMPUTING ENVIRONMENTS

Not all computing "environments" are created equal. There are substantial differences between them. We can encounter individual computers, networks of various sizes, or even more complex systems. These disparities will have a significant impact on your collection process, where you look for data, the tools you will use, and the level of complexity required. An accurate clarification of the environment is useful to have right from the start of an investigation, even before you respond to a scene. Environments can be broken down into four categories: stand-alone, networked, mainframe, and the cloud.

A stand-alone computer is one that is not connected to another computer. These are the easiest to deal with and investigate. Possible locations for evidence are reasonably confined. Stand-alone systems are routinely encountered in residences such as apartments and houses.

A networked computer is connected to at least one other computer and potentially many, many others. This escalates the complexity as well as the places evidence could be found. We now can see files and artifacts normally found on the local machine spread out to servers or other machines. This environment introduces a variety of variables into the equation. Even though networks are more commonly found in a business setting, they are found more and more in homes.

Unlike a stand-alone machine, a **mainframe system** centralizes all of the computing power into one location. Processors, storage, and applications can all be located and controlled from a single location.

### Cloud Computing

You may not be familiar with the term "**cloud computing**," but if you use Gmail, Facebook, or Twitter, you're already using it. Cloud computing is a hot topic these days, garnering much attention from both the IT and business communities. This "new" model of computing is very similar in many respects to the mainframe systems of old. Like the mainframe, the computing resources are moved from the local machine to some other centralized place.

The cloud model presents some very interesting features that make it attractive to businesses, especially from a cost perspective. The cloud offers software along with computing infrastructure and platforms on an elastic, pay-per-use model. This affords companies the luxury of only paying for what they use.

Technology behemoths such as Microsoft, Google, and Amazon are just three of the companies that are jumping on the bandwagon offering cloud services. Cloud services include **Infrastructure as a Service (IaaS)**, **Platform as a Service (PaaS)**, and **Software as a Service (SaaS)**. All of these are delivered over the Internet. In the cloud, customers only pay for the resources they actually use, just like the way we pay for our water and electricity.

### *IaaS*

With IaaS, organizations outsource their hardware needs to a service provider. This would include everyday hardware needs such as servers, storage, and the like. The associated costs for running and maintaining the hardware are paid by the provider.

### *PaaS*

Programmers develop their software to function in specific computing environments (operating system, services, etc.). PaaS gives developers the ability to rent the environment (hardware, operating systems, storage, servers, etc.) on an “as-needed” basis. PaaS provides excellent flexibility in that the operating system can be modified or upgraded frequently.

### *SaaS*

In the cloud, SaaS provides applications on demand to customers over the Internet. These applications are hosted and maintained by the service provider.

The cloud represents a huge challenge to the digital forensic community, from both a technical and a legal standpoint. Technically, the cloud presents a very complicated, virtualized environment that frustrates if not downright negates many routine forensic procedures. Legally, it can be a jurisdictional nightmare. In the cloud, data know no bounds. The evidence can literally be in the next state or a foreign country halfway around the globe. We'll look closer at the cloud and its impact on forensics in [Chapter 11](#).

## DATA TYPES

Data can be lumped into three broad categories: active, latent, and archival. Looking at data in this way helps in clarifying their location, how they're accounted for by the file system, how they can be accessed by the user, and so on. It also helps to narrow down the cost and effort required to recover the data in question.

### Active Data

Active data are the data that we use every day on our computers. The operating system “sees” and tracks these files. You can locate these files using Windows Explorer. These are the files that reside in the allocated space of the drive. These data can be acquired with standard forensic cloning techniques.

## Latent Data

Data that has been deleted or partially overwritten are classified as **latent**. These files are no longer tracked by the operating system and are therefore “invisible” to the average user. Go looking for one of these files with Windows Explorer and you won’t find it. A bit stream or forensic image is required to collect these data.

## Archival Data

**Archival data**, or backups, can take many forms. External hard drives, DVDs, and backup tapes are just a few examples. Acquisition of archival data can range from simple to extremely complex. The type and age of the backup media are major factors in determining the complexity of the process.

Backup tapes can present some very big challenges, especially if they were made with software or hardware that is no longer in production. Tapes are created using specific pieces of hardware and software. These same tools will be needed to restore the data into a form that can be understood and manipulated. Where it gets really exciting is when the hardware and software are no longer in production. It could be an older version of the software is no longer available or the company is no longer in business. This is known as **legacy data**. What do you do if you no longer have and can’t get access to the necessary tools to restore the data? Sometimes eBay can save the day.

# FILE SYSTEMS

With all the millions or billions of files floating around inside our computers, there has to be some way to keep things neat and tidy. This indispensable function is the responsibility of the **file system**. The file system tracks the drive’s free space as well as the location of each file. The free space, also known as unallocated space, is either empty or the file that previously occupied that location has been deleted.

There are many different types of file systems. Some of the most commonly encountered by forensic examiners include FAT, NTFS, and HFS+. Let’s take a closer look:

**File Allocation Table (FAT)** is the oldest of the common files system. It comes in four flavors: FAT12, FAT16, FAT32, and FATX. Although not used in the latest operating systems, it can often be found in flash media and the like.

**The New Technology File System (NTFS)** is the system used currently by Windows 7, Vista, XP, and Windows Server. It’s much more powerful than FAT and capable of performing many more functions. For example, “NTFS can automatically recover some disk-related errors, which FAT32 cannot,” it provides better support for larger hard drives, and better security through permissions and encryption (Microsoft Corporation).

Hierarchical File System (HFS+) and its relatives HFS and HFSX are used in Apple products. HFS+ is the upgraded successor to HFS. This newer version offers several improvements including improved use of disk space, cross-platform compatibility, and international-friendly file names ([Apple, Inc., 2004](#)).

## ALLOCATED AND UNALLOCATED SPACE

Before we get much further, it's time we talk about how the computer views the space on a hard drive. Generally speaking, the file system categorizes all of the space on the hard drive in one of two ways. The space is either **allocated** or **unallocated** (there are a few exceptions; see the side bar on Host Protected Areas). Put another way, either the space is being used or it's not. Windows can't see data in this unallocated space. To the Operating System, files located in unallocated space are essentially invisible. It's important, however, to understand that "not used" does not always mean "empty."

### MORE ADVANCED

#### **Host Protected Area (HPA) and Device Configuration Overlays (DCO)**

**Host Protected Areas** (HPAs) and **Device Configuration Overlays** (DCOs) refer to hidden areas on a hard drive that are often difficult to detect. These areas are created by manufacturers that can be "accessed, modified, and written to by end users using specific open source and freely available tools, allowing data to be stored and/or hidden in these areas" ([Gupta, Hoeschele, & Rogers, 2006](#)). HPAs can contain diagnostic tools, an operating system for recovery purposes, and so on. It's rare that the HPA is used by suspects to conceal data.

## Data Persistence

Like a telemarketer, data on a hard drive are pretty persistent. It's not as easy to get rid of as you may think. Deleted files will sit there until they're overwritten with more data. You might be asking yourself, "So how long does that take?" The answer is, it depends (which, by the way, is one of the most popular answers in digital forensics). With the massive amount of storage space available on today's hard drives, a file stands a good chance of never being overwritten. Your bachelor (or bachelorette) party pictures could remain on your hard drive for a long, long time. Just keep that in mind before you run for public office.

Remember, the file system's job is to keep track of all files and storage space. The file system keeps things nice and orderly. Think of a file system as an index in the back of a book. When looking up a particular subject, we flip through the index until we find the term we're looking for. Our handy index then gives us the page number and off we go. The file system works basically the same way. Using the book analogy again, deleting a file would be akin to removing the entry from the book's index. Although our subject is no longer referenced in the index, the page and all its content are still in the book, intact and untouched.

You may be surprised to know that when you save your file, it's not necessarily stored in one place. In fact, your spreadsheet could be scattered all over the platter(s) of your hard drive. Strange, huh? You would think as orderly as computers are, that wouldn't be the case.

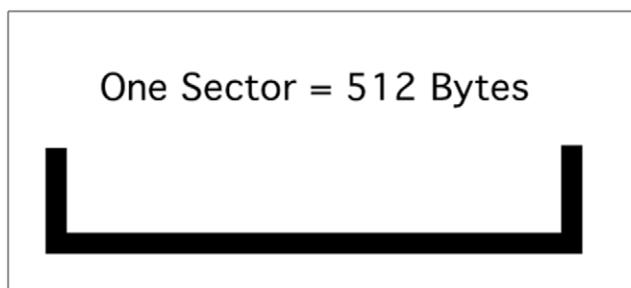
The file system's job is to keep track of these separate clusters so they can be reassembled the next time you open that file. Have you ever "defragged" your hard drive? If you have, you were simply moving these disparate pieces as close together as possible. Moving them closer together speeds things up for your computer. The closer they are, the faster they can be put together and made available to you. Some crooked individuals may attempt to destroy data using the defragging process. In [Chapter 6](#), we'll see how that may or may not be effective.

Files that are overwritten are generally considered to be unrecoverable. But all is not lost (pardon the pun). Like many rules in life, there are exceptions and this is one of those. It is possible that the new file assigned to that space won't need all of it. If that's the case, the original file is only *partially overwritten*. The piece that remains *can* be recovered and could contain information we can use. This remaining space is called **slack space**. Before we take a little closer look at slack space, we're going to have to get a little more technical. So, get your "nerd on" and follow along.

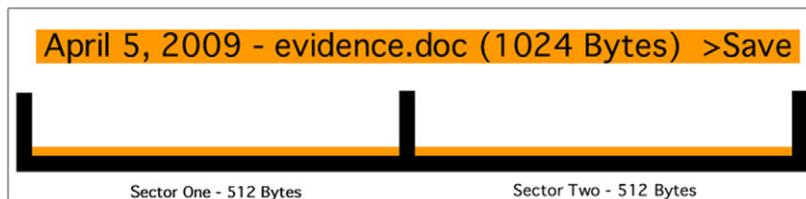
## HOW MAGNETIC HARD DRIVES STORE DATA

We need to understand how the computer stores your files. Computers store your data in defined spaces called **sectors**. Think of sectors as the smallest container a computer can use to store information. Each sector holds up to 512 bytes of data as illustrated in [Figure 2.4](#). It can hold less, but it can't hold more.

While a sector is the smallest container, a computer's operating system only stores data as clusters. Suppose we save our master criminal plan to our hard drive. We'll call it "evidence.doc." It just so happens to be 1024 bytes in size (convenient, isn't it?). Our computer would assign that file to two separate sectors, as shown in [Figure 2.5](#).

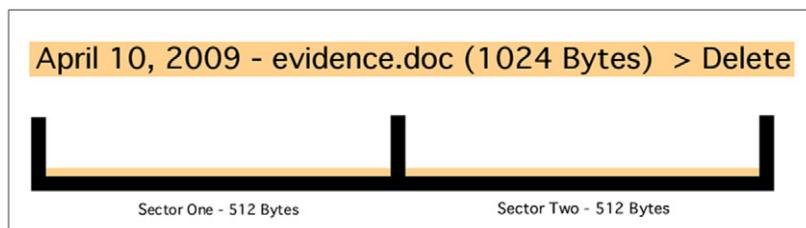


**FIGURE 2.4**  
One sector.

**FIGURE 2.5**

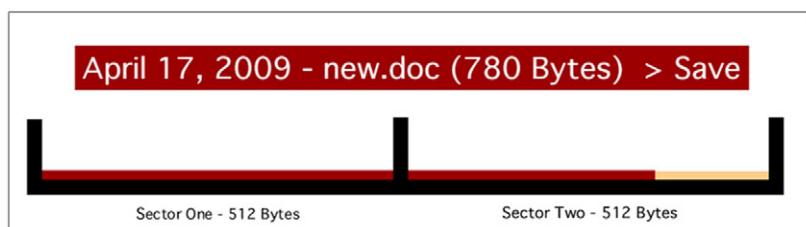
Two sectors with one file called evidence.doc.

After watching Abby and McGee work their magic on NCIS, we start to have second thoughts. We decide it's probably better not to have that file on our computer. So we hit the delete key, sending the file to the recycle bin. With a sly grin we empty the recycle bin, content in the knowledge that evidence.doc is now residing in digital oblivion. [Figure 2.6](#) depicts our two sectors after the recycle bin has been emptied.

**FIGURE 2.6**

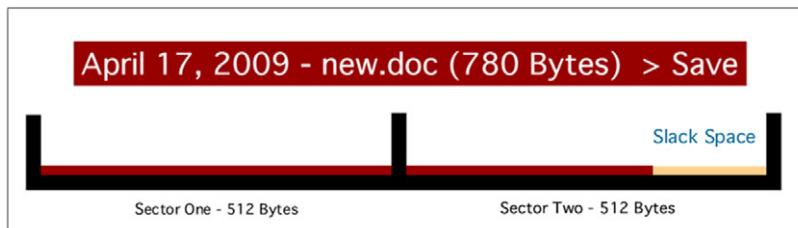
Deleted file, "evidence.doc." Note that it still occupies the original two sectors.

Two days later, we save another file to our drive. We'll call this one "new.doc." It's only 780 bytes. How many sectors will be assigned to this new document? Two you say? Excellent! You are correct. Remember that a 512 byte sector is the smallest "bucket" the computer can store data in. This file is 780 bytes so it's bigger than one sector but won't quite fill a second. (See [Figure 2.7](#).)

**FIGURE 2.7**

"new.doc" is saved over "evidence.doc," overwriting the majority of the original file. Files that are overwritten are unrecoverable.

Our computer, acting solely on its own, decides to place this new file in the same two sectors originally occupied by our first file, evidence.doc. The first 780 bytes of our original file have been overwritten. Some quick math tells us that 244 bytes of our original file are still there. Those 244 remaining bytes comprise the slack space. The slack space, depicted in [Figure 2.8](#) is the difference between the space that is assigned and the space that is actually used.



**FIGURE 2.8**

Note the slack space. This fragment of data can be recovered.

Out of the slack space we can recover fragments of the previous file. It may not be useful. But then again, it just might. It could be part of an incriminating spreadsheet, e-mail, or picture. These fragments could contain just enough of an e-mail to identify the sender or the sender's IP address. A partial picture of the victim could link them to the suspect. Slack space can't be accessed by the user or the operating system. As such, this evidence exists unbeknown to the suspect.

## ADDITIONAL RESOURCES

### How Hard Drives Work

Scott Moulton, from [MyHardDriveDied.com](http://MyHardDriveDied.com), has some excellent presentations on magnetic and solid-state drives. His delivery isn't boring or overly technical. The visuals are outstanding. His web site has videos of his presentations. They are well worth the time.

<http://myharddrivedied.com/presentations-resources>

## Page File (or Swap Space)

The hard drive is used to store your data and applications when they aren't being used. Relatively speaking, this is the slowest component of the three we're discussing. Being the "slow poke" that the hard drive is, it just can't keep up with the blazing speed of the CPU. So, all the data and instructions must be fed to the CPU from the RAM. Otherwise it might be easier to use a stone tablet and chisel. Okay, maybe not, but you get the idea.

Few people can get on their computer and only open one application. It's like the Lay's potato chip ads from several years ago. You can't open just one. Let's say you've got Word, Outlook, and Firefox up and running. Inside Firefox, you've got three separate tabs open. If you keep opening applications or using programs such as Adobe Photoshop that need a great deal of the computer's memory, you'll eventually see your computer slow down. You'll also likely hear your hard drive start to spin. At this point, you'll start to use your computer's virtual memory.

This **virtual memory** is called the page file or swap space. The **page file** isn't a function that is used on a consistent basis. The page file is used when we have exhausted all of the computer's main memory. The main memory is called RAM. RAM stands for Random Access Memory. The RAM holds everything your computer is working on at the moment. All of the data and instructions (programs, etc.) must move from the main memory to the CPU, where they're processed. Every computer comes with a certain amount of RAM. It's not an endless supply and can eventually run out. When the RAM does run out, the computer is going to have to start moving some things around. To alleviate this situation, the computer will swap data in and out of the RAM, writing data to the page file to free up room in the RAM ([Casey, 2009](#)). The great thing about the page file is that it can contain files and file fragments that no longer exist anywhere else on the drive. Even suspects that are successful in deleting and overwriting their files will overlook the swap space, leaving this evidence for later recovery.

So what's in it for us? It could be plenty. Let's connect all the dots and you'll see:

1. Data will stay on a hard drive until they're overwritten.
2. The page file isn't used consistently, so some data may linger there for quite some time.
3. The page file will contain data that were at one point in the RAM. That could be just about anything. We could even find passwords written in the clear.

## BASIC COMPUTER FUNCTION—PUTTING IT ALL TOGETHER

Let's take a very broad look at what's going on "under the hood" of our computers as we go about some common tasks. Our example data, say a Word document, begin on the hard drive where we saved it the day before. Our file was stored on the hard drive as a series of 1s and 0s. Typically, files will have a specific structure or format. The start of the file is called the "**header**." The end of the file is known as the "**footer**." All of the bytes in between represent the remainder of the file. Technically speaking, a file header is considered a form of metadata ("data about the data"). The header, like the extension, is used to identify the file type. However, unlike the extension, the header is much harder to change and is generally inaccessible to most users.

When the file is saved or written to the hard drive, it's not necessarily saved to contiguous clusters as one might expect. These separate pieces of the file could

be on different sides of a platter or on different platters altogether. When we double click on the file to open it, the computer gets the locations of all the sectors allocated to the file from the file system and recreates your file.

To work on the file, it must be loaded into the computer's main memory, also known as RAM. From here, the file is fed into the central processing unit (CPU) as we're working with it.

A filing cabinet, desk, and worker are used as a common analogy to help explain this process. The filing cabinet symbolizes the hard drive. The desk represents the RAM. Finally, the worker at the desk represents the CPU. The filing cabinet, like the hard drive, stores our files when we aren't using them. Just like in the real world, we can't work on any of our documents from the filing cabinet until we move them to the desk. The worker (CPU) can't work on our documents until they are relocated from the filing cabinet to the desk.

## SUMMARY

In [Chapter 2](#) we took a closer look at how computers store data in different forms including magnetic, optical, flash, and others. Each of these storage methods is different and those differences have forensic implications. Computers operate with both memory and storage. While they sound similar, their intended purposes are distinctly different. Memory holds the data that the computer is actively working on at the moment. It's volatile, meaning that it holds data as long as it has power. When power is removed, the data begins to go away. The RAM in your computer is used for memory.

In contrast, storage is used for the long-term storing of data. Storage is considered non-volatile because the data remains even if the device loses power. Your hard drive is an example of storage.

A computer's file system is at the heart of how it saves and retrieves data. File systems keep track of the various pieces of data that must be found and reconstituted in order to open a file. There are multiple file systems in use today, each with their own way doing things.

Not all computing environments are the same. Some are relatively simple, others much more complex. Stand-Alone computers, networks, and the cloud were covered in this chapter.

As forensic examiners, we must have command of this material so that we can explain it to the average person. It is these "average people" that make up our juries.

## References

- Apple, Inc. (2004, March 5). *Technical Note TN1150 HFS Plus Volume Format*. Retrieved August 10, 2011, from: <http://developer.apple.com/library/mac/#technotes/tn/tn1150.html>
- Casey, E. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*. Waltham, MA: Academic Press.

- Casey, E. (2009). *Handbook of Digital Forensics and Investigation*. Burlington, MA: Academic Press.
- Cooper, B. (2004, August). *What Is the Difference Between Memory and Storage?* Retrieved August 10, 2011, from: <http://searchstorage.techtarget.com/answer/What-is-the-difference-between-memory-and-storage>
- Dale, N. (2009). *Computer Science Illuminated, Fourth Edition*. Sudbury, MA: Jones and Bartlett.
- Gupta, M. R., Hoeschele, M. D., & Rogers, M. K. (2006). Hidden Disk Areas: HPA and DCO. *International Journal of Digital Evidence*, 5 (1).
- Microsoft Corporation. (n.d.). *Comparing NTFS and FAT File Systems*. Retrieved August 10, 2011, from: <http://windows.microsoft.com/en-US/windows-vista/Comparing-NTFS-and-FAT-file-systems>
- SearchStorage.com. (2000, December). *Optical Media*. Retrieved August 10, 2011, from: <http://searchstorage.techtarget.com/definition/optical-media>
- Unicode Inc. (2010, September 17). *What Is Unicode?* Retrieved August 10, 2011, from: <http://www.unicode.org/standard/WhatIsUnicode.html>

# CHAPTER 3

## Labs and Tools

29

### Information in This Chapter:

- The Role and Organization of Forensic Laboratories
- The Purpose of Policies & Procedures in Forensic Laboratories
- The Role of Quality Assurance in Forensics
- Digital Forensic Hardware and Software
- Accreditation versus Certification

## INTRODUCTION

In this chapter we will explore the different types of laboratory setups as well as the hardware and software tools in common use. We'll also take a look at Standard Operating Procedures and Quality Assurance, two critical components of an effective digital forensic lab. Obtaining and maintaining laboratory accreditation, although time-consuming and expensive, greatly improves a lab's performance and the quality of its findings. Examiner certification ensures that the skill of the labs meets a minimum level. At the end of the day, these elements come together to ensure that only valid and reliable results are produced and that justice is served.

## FORENSIC LABORATORIES

Forensic labs are scattered throughout the United States and closely follow the jurisdictional lines of law enforcement (local, county, state, and federal) ([James & Nordby, 2009](#)). The majority of these facilities are run by a law enforcement agency. The FBI's crime laboratory in Quantico, Virginia, has the distinction of being the largest lab in the world ([Saferstein, 2006](#)).

Not all computer forensic examinations are conducted in what would be considered a traditional laboratory setting. Many agencies conduct them locally at their departments if they have the necessary equipment and trained personnel on hand.

Digital forensics isn't cheap, so not every agency can afford to train and equip their own examiners. One way to meet this ever-growing demand is the **Regional Computer Forensic Laboratory (RCFL)** program started by the FBI. The RCFL program runs sixteen facilities throughout the United States. They provide digital forensic services and training to all levels of law enforcement. Each RCFL is staffed and managed by a partnership of local, state, and federal law enforcement agencies.

The RCFL program is a great success, and making a significant dent in the backlog of digital forensic examinations across the country. During fiscal year 2010, RCFLs nationwide performed 6,564 forensic examinations and processed a whopping 3,086 terabytes of data. To put that in context, the 2010 Annual Report explains it this way; "One single terabyte is equivalent to 1,024 gigabytes or approximately 1,000 copies of the Encyclopedia Britannica." Doing the math, that's about 3,086,000 encyclopedias. The RCFLs process a wide variety of digital devices and media including smartphones, hard drives, GPS (Global Positioning System) units, and flash drives. In 2010, RCFL examiners helped convict rapists, terrorists, and crooked politicians ([Federal Bureau of Investigation, 2010](#)).

## Virtual Labs

Digital labs don't have to be confined to a single location. Today's technology makes it possible to run a "virtual" lab with the examiners and the central evidence repository located in geographically separate locations. This arrangement has several advantages including cost savings, greater access to more resources (tools and storage for example), access to diverse and greater expertise, and reduction of unnecessary duplication of resources (Craiger).

This virtual arrangement allows for distinct role-based access. For example, full access could be granted to examiners and laboratory management. Prosecutors, investigators, and defense attorneys would have restricted access. This restricted access would limit what those folks could see and what they could do (read only, etc.) ([Whitcomb](#)).

There are some considerable concerns with this approach:

- 1. Security**—The security of the system must be robust enough to maintain the level of evidence integrity required by the courts. Otherwise there could be catastrophic consequences, such as rendering evidence from multiple cases inadmissible.
- 2. Performance**—For this scheme to work, connectivity must be both speedy and reliable. No connection or a slow connection will quickly impact the organization's ability to function.
- 3. Cost**—Startup costs in particular are substantial and potentially beyond what many agencies can afford ([Whitcomb](#)).

## Lab Security

Lab security is always a major concern. Access to the evidence and facilities must be strictly managed. Strict security plays a key role in maintaining the integrity of

the digital evidence that passes through the laboratory. Only authorized, vetted personnel should have access to critical areas such as examination stations and evidence storage. Unauthorized individuals are usually kept out using doors and other physical barriers along with access controls such as keys, swipe cards, and access codes. Digital solutions such as swipe cards and access codes offer an advantage over older methods such as keys. Electronic means provide a ready-made audit trail that can be used in support of the chain of custody. Security is further enhanced with alarm systems and the like.

Unauthorized access isn't the only threat to the evidence. The risk of fire, flooding, and other natural disasters also must be addressed.

The chain of custody continues at the lab, as does the paperwork. In the lab, the evidence must be signed in and out of the evidence storage area for examinations and court. This log must be completed each and every time the evidence is removed or returned to the evidence room or vault. This checkout and check-in process can be done the old-fashioned way with pen and paper or electronically with scanners and bar codes.

Just like in the field, network access to evidence in the lab is also a concern. This is true for both the Internet and the lab's own computers. Best practice tells us that the machine used to perform the examination should not be connected to the Internet. Removing this connection removes that argument that the evidence was somehow compromised by someone or something (malware for example) via the Internet. Virtual labs will need to be able to articulate how the integrity of their evidence is maintained, given the nature of their operation.

Malware (viruses, worms, and the like) could be hiding on any evidence drive brought in for examination. Connecting it in some manner to the internal network poses a major risk to not only the lab's computers but evidence from other cases as well. To mitigate the risk, these drives should be scanned for viruses by at least one antivirus tool prior to examination.

## Evidence Storage

When the evidence is not actively being examined, it must be stored in a secure location with limited access. One of the best solutions is a data safe. These safes come in multiple sizes and are specifically designed to protect digital evidence from theft and fire. Some types of digital media are very vulnerable to heat (tape, for example). A data safe is able to keep the media at an acceptable temperature long enough (hopefully) for the fire to be extinguished.

Evidence storage locations must be kept locked at all times when not actively being used. A log or audit trail should also be maintained detailing who entered, when they entered, and what they removed or returned.

Access to evidence storage and other sensitive areas can be controlled by a variety of means including pass codes and key cards. Electronic controls have some distinct advantages over keys. One significant advantage is the ability to log each

and every time an individual accesses a restricted area. This audit trail can be very helpful in monitoring and verifying the chain of custody.

## POLICIES AND PROCEDURES

How the lab handles evidence, conducts examinations, keeps records, and secures its facility should not be left to chance or the whims of any one individual. These tasks should be governed by policies and **Standard Operating Procedures (SOPs)**. SOPs are documents that detail, among other things, how common forensic examinations should be performed. The art in writing SOPs lies in finding the right balance between being too narrow or overly broad. If too specific, the SOP will lack the flexibility needed to address any unusual conditions that may arise. In digital forensics, these situations occur far more often than we'd like. If too broad, they can be ineffective in keeping things consistent and ensuring the integrity of the evidence.

There are inherent dangers in not following your organization's policies and SOPs. Odds are that questions on your organization's policies and SOPs will come up during cross-examination should the case go to court.

## QUALITY ASSURANCE

In the early 1980s, the Ford Motor Company told us told us that "Quality is Job 1." You may not believe that today in regard to Ford, but it's most assuredly true in regard to forensic science.

**Quality assurance (QA)** is a bedrock principle that underpins every discipline in forensic science. As such, every lab should have a QA program. Quality assurance is defined as "a well-documented system of protocols used to assure the accuracy and reliability of analytical results" ([James & Nordby, 2009](#)). A good QA program will cover a wide array of subjects including peer reviews of reports, evidence handling, case documentation, training of lab personnel, and more ([James & Nordby, 2009](#)).

The review process can be divided into two discrete types: a technical review and an administrative review.

- The technical review, conducted by a separate examiner, focuses on the results and conclusions. The central question in a technical review is "Are the results reported by the original examiner supported by the evidence in the case?"
- In contrast, the focus of an administrative review is ensuring that all of the paperwork is present and has been completed correctly.

An examiner's competency must be confirmed and documented on a regular basis. In the forensic community, this is known as proficiency testing. In a proficiency test, examiners must demonstrate their competence with mock evidence. There are four types of proficiency tests:

1. **Open test**—the analyst(s) and technical support personnel are aware they are being tested.

- 2. Blind test**—the analyst(s) and technical support personnel are not aware they are being tested.
- 3. Internal test**—conducted by the agency itself.
- 4. External test**—conducted by an agency independent of the agency being tested. (Scientific Working Groups on Digital Evidence and Imaging Technology, 2011).

These tests may be conducted in-house, with other lab personnel. These results must be documented because at some point, the analyst's skills and abilities may be called into question during a court proceeding. This documentation will be critical should that happen.

The case of Glen Woodall, although concerning DNA, is a powerful example of the need for quality assurance. On July 8, 1997, Glen Woodall was convicted of the brutal sexual assault of two women by a Cabell County, West Virginia, jury. He was summarily sentenced to two life terms with an additional sentence of 203 to 335 years in prison (The DNA Initiative). The arrest and conviction of Woodall brought some much needed closure to both of the victims and peace to the community as a whole. Unfortunately for the victims and community, the relief didn't last long.

The forensic scientist in this case was West Virginia State Police serologist Fred Zain. After an investigation into Zain's work in both West Virginia and Texas, he was charged with perjury and tampering with evidence (Chan, 1994). During the investigation it was found that Woodall was innocent, and that he, too, was a victim. After serving four years in a West Virginia prison, Woodall was released and awarded \$1 million from the state for his wrongful imprisonment.

What the panel found was extremely disturbing. They discovered that Zain "fabricated or altered evidence and lied about academic qualifications under oath." That's not all. The panel also found that his supervisors may have been culpable as well, overlooking or hiding complaints about his performance (Chan, 1994).

In 2011, twenty-four years later, the real suspect was arrested and eventually convicted of the crimes of which Woodall was originally found guilty. On April 1, Donald Good was sentenced to over two hundred years in prison (WSAZ, 2011). Cases like this hammer home the need for effective quality assurance programs in all forensic sciences.

## Tool Validation

Our tools, be they hardware or software, must function as they are designed. Each and every tool must be validated before it's used on an actual case. A validation process clearly demonstrates that the tool is working properly, is reliable, and yields accurate results. We can't simply accept the manufacturer's word for it; assumptions aren't permitted.

The validation process is another one of those things that has to be committed to paper. To do otherwise will put any evidence found in real jeopardy of being excluded.

## Documentation

The importance of complete and accurate documentation can't be overstated. The old saying "if you didn't write it down, it didn't happen" are truly words to live by in this industry. There are different types of documentation and reports used throughout the entire forensic process. These should be spelled out in the labs' or agencies' SOP and policy manuals. Submission forms, chain of custody records, examiner's notes, and the examiner's final report form the crux of the required documentation.

Normally, all the paperwork associated with a specific case is collected into a case file. The case file will contain all of the documentation pertaining to the case, including paperwork generated by the examiner and others. Usually they include case submission forms, requests for assistance, examiners' notes, crime scene reports, case reports, copy of the search authority, chain of custody, and so on ([National Institute of Justice, 2004](#)).

### FORMS

Preprinted forms are widely used in both the field and the lab. They help guide personnel through the process and ensure that a high level of quality is maintained. Forms ensure all the necessary information is captured in a uniform manner. Typically, forms are used to describe the evidence in detail (make, model, serial number, etc.), document the chain of custody, request an examination, and so on.

### EXAMINER NOTES

Examiner's notes cover most, if not all, of the examiner's actions and observations along with corresponding dates. They must be detailed enough to enable another examiner to duplicate the process used during the examination. Things typically recorded here include:

- Discussions with key players including prosecutors and investigators.
- Irregularities found and associated actions taken.
- Operating systems, versions, and patch state.
- Passwords.
- Any changes made to the system by lab personnel and of law enforcement. ([National Institute of Justice, 2004](#))

If you've ever worked in the legal system, then you know that the wheels of justice can turn very, very slowly. This applies to both criminal and civil cases. It can be months or even years before a case ever gets to trial. By the time you have to testify, you may only be able to recall few, if any, facts of the case. The case documentation, and your notes in particular, will prove a great tool to refresh your recollection.

### EXAMINER'S FINAL REPORT

The **examiner's final report** is the formal document that is delivered to prosecutors, investigators, opposing counsel, and so on at or near the end of an investigation. These reports typically consist of:

- Identity of the reporting agency.
- The case identification number/submission number.
- Identity of the submitting person and case investigator.
- Dates of receipt and report
- Detailed description of the evidence items submitted including serial numbers, makes, models, and so on.
- Identity of the examiner.
- Description of the steps taken during the examination process.
- Results and conclusions. ([National Institute of Justice, 2004](#))

When drafting the final examiner's report, it's critical to take into account the intended audience, which is primarily laypeople. The lawyers, investigators, judges, and clients will most likely have little to no technical background. All too often these reports are filled with technical jargon and details that only serve to frustrate and confuse the majority of its intended audience. These reports should be comprehensible to a nontechnical audience. Jargon and acronyms should be kept to an absolute minimum.

Two major sections of the examiner's report are the summary and the details of the findings. The summary is a brief description of the results of the examination. The end users of our reports find this feature useful, especially in light of the massive caseload and amount of information they are typically dealing with. The findings included here should be supported and explained in the detailed findings.

The detailed findings provide the substance of the report. They provide the details of the examination, steps taken, results, and so on. Typically you may find details relating to:

- Files directly pertaining to the request.
- Files that support the findings.
- Email, web cache, chat logs, and so on.
- Keyword searches.
- Evidence of ownership of the device. ([National Institute of Justice, 2004](#))

A glossary is a helpful addition to an examiner's report. Anything we can do to help our intended audience wade through any unfamiliar jargon and acronyms is always a good thing. Conveying our findings in a way that can be understood is our responsibility as forensic professionals.

## DIGITAL FORENSIC TOOLS

Digital forensic tools make our work much more efficient or even possible. There are tools for specific purposes as well as tools with broader functionality.

They can come in the form of both hardware or software. They can be commercial tools that must be purchased or they can be open source that are freely available. There are advantages and disadvantages to all. Keep in mind, no single tool does everything or does everything exceedingly well. As such, it's a good practice to have multiple tools available. Using multiple tools is also a great way to validate your findings. The same results, with two different tools, significantly increase the reliability of the evidence.

### Tool Selection

The digital forensic tool market boasts a large number of products, with more rolling out all the time. How does an examiner know which tools are reliable and which ones are not? How should these tools be validated? The National Institute of Standards and Technology (NIST) and the National Institute of Justice (NIJ) have taken a big step in helping to answer these and other questions.

NIST has launched the Computer Forensic Tool Testing Project (CFTT), which establishes a "methodology for testing computer forensic software tools by development of general tool specifications, test procedures, test criteria, test sets, and test hardware" (National Institute of Standards and Technology).

Let's explore what this looks like. This is an excerpt from the NIST test of a Tableau brand hardware **write blocking device (HWB)**, summarizing some of the test criteria and results:

"An HWB device shall not transmit a command to a protected storage device that modifies the data on the storage device."

"For all test cases run, the device always blocked any commands that would have changed user or operating system data stored on a protected drive."

"An HWB device shall return the data requested by a read operation."

"For all test cases run, the device always allowed commands to read the protected drive." ([National Institute of Justice, 2009](#))

Each tool, be it hardware or software, must be validated before it is used on casework as well as anytime it is modified or updated. For an example, like other software you're familiar with, our forensic software gets updated on a regular basis. After each update, the tool should be validated again. Validation also proves useful in court, supporting the validity of the tool's results.

### Hardware

There are many hardware tools out there designed and built specifically for digital forensics. Some of these tools include cloning devices, cell phone acquisition devices, write blockers, portable storage devices, adapters, cables, and more.

As you might expect, digital forensics is heavily dependent on an assortment of hardware such as PCs, servers, write blockers, cell phone kits, cables, and so on. [Figure 3.1](#) shows a well-equipped digital forensic workstation.

**FIGURE 3.1**

One of the workstations in the West Virginia State Police Digital Forensics Lab located at the Marshall University Forensic Science Center. (Courtesy of Cpl. Bob Boggs).

Computers are the backbone of any digital forensics lab. So as an examiner you will need the best computer workstation you can afford. Digital forensic exams require quite a bit of computing power. These jobs can tax even the best systems and crush those that don't measure up. A good exam machine has multiple, multi-core processors, as much RAM as you can get (the more the better), and large, fast hard drives. Forensic software manufacturers provide detailed lists of minimum and suggested hardware requirements. Straying below the minimums is done at your own risk. To get a better understanding, let's look at the minimum and recommended system requirements (as of press time) for AccessData's Forensic Tool Kit (FTK).

AccessData's FTK comprises four distinct components and or applications. They are:

1. Oracle Database
2. FTK Client User Interface (UI)
3. Client-side Processing Engine
4. Distributed Processing Engine

The minimums and recommended specifications will vary with each component, but suffice it to say that you can never have too much RAM or computing power. For example, on a machine running the Oracle database, the FTK user interface and the primary processing engine, AccessData recommends the requirements shown in [Table 3.1](#).

**Table 3.1 Basic Recommended Requirement (AccessData Group, LLC, 2011)**

	Minimum	Recommended
Processor	Intel® i7 or AMD equivalent	Intel® i9 Dual Quad Core Xeon, i7 Nehalem or AMD equivalent
RAM	12GB (DDR3) 8GB (DDR2)	12GB (DDR3) 8GB (DDR2)
Operating System	Vista, 2008, Windows 7 (64 bit)	Vista, 2008, Windows 7 (64 bit)

Some components may be installed on separate machines. The minimum and recommended requirements will change depending on which configuration is used.

Examiners frequently sift through massive amounts of data. As such, digital forensics labs need to have the capacity to store voluminous amounts of data. In browsing the PCs for sale on [bestbuy.com](http://bestbuy.com), the majority of them have between 500 GB and 699 GB of hard drive space. Multiterabyte drives are also available. With numbers like these and caseloads ever increasing, it's easy to see that storage is a major concern.

Digital forensics is no longer a "PC centric" endeavor. Small-scale devices such as cell phones and GPS units are pouring into labs across the country. These devices require different hardware from that used on laptops and desktops. Cellebrite's UFED supports over three thousand phones (Cellebrite Mobile Synchronization LTD). Paraben Corporation, a competitor of Cellebrite, boasts support for more than four thousand phones, PDAs, and GPS units (Paraben Corporation). When dealing with cell phones, having the proper cable is critical. Unlike PCs, mobile devices lack much of the standardization with regard to connectors and cables. Labs need to have a wide selection of cables on hand to cope with the vast array of handsets that walk through the doors. Fortunately, the manufacturers of mobile phone forensic hardware provide many of the required cables.

Several companies make hardware cloning devices. If you recall, a forensic clone is a "bit stream" copy of a particular piece of media such as a hard drive. These tools can really speed up the process, cloning multiple drives at once. They can also provide write protection, hash authentication, drive wiping, an audit trail, and more.

#### OTHER EQUIPMENT

The hardware and software we discussed earlier are not the only equipment needed. Crime scene kits are very useful outside the lab. These kits are preloaded with all of the supplies an examiner would need in the field to collect digital evidence. Kits contain standard items such as pens, digital camera, forensically

clean storage media, evidence bags, evidence tape, report forms, permanent markers, and the like.

## Software

There is a wide array of digital forensic software products on the market today. Some are general tools that serve a variety of functions. Others are more focused, serving a fairly limited purpose. These applications tend to focus on a very specific type of evidence, e-mail or Internet, for example.

When selecting software, a choice needs to be made between going with open source tools or a commercially produced product. There are advantages and disadvantages to both. Factors such as cost, functionality, capabilities, and support are some of the criteria that can be used to make this decision.

### ADDITIONAL RESOURCES

#### Open Source Tools

Cory Altheide and Harlan Carvey's book *Digital Forensics With Open Source Tools* is an excellent reference for those practitioners using these applications.

One of the more popular open source tools is SIFT, or the SANS Investigative Forensic Toolkit. SIFT Workstation is a powerful, free, open source tool. It's built on the Linux Ubuntu operating system. This tool is capable of file carving as well as analyzing file systems, web history, recycle bin, and more. It can also analyze network traffic and volatile memory. It can also generate a timeline, which can be immensely helpful during an investigation. SIFT supports the following file systems:

- Windows (MSDOS, FAT, VFAT, NTFS)
- MAC (HFS)
- Solaris (UFS)
- Linux (EXT2/3/4)

(The SANS Institute)

As for commercial tools, two of the most popular general software tools are Forensic Toolkit (FTK®) from AccessData and EnCase® from Guidance Software. Both are excellent and can make exams easier and more efficient. These applications have "Swiss Army knife"-like capabilities. They perform a multitude of tasks, including:

- Searching
- E-mail analysis
- Sorting
- Reporting
- Password cracking

The search tools in these products are particularly powerful, and give examiners the capability to drill down to precisely the information they are looking for. Here is a quick list of some of the information that can be searched for:

- E-mail addresses
- Names
- Phone numbers
- Keywords
- Web addresses
- File types
- Date ranges

As helpful as these tools can be, they do have some limitations. The reality is that no single tool does it all. For that reason, budget permitting, labs need to have a variety of tools available.

More and more specialty tools are coming on the market. These tools focus on one aspect of digital evidence such as e-mail or web-based evidence. These can bring some additional capabilities to the table that some multipurpose tools don't.

### ALERT!

#### Dependence on the Tools

GUI-based forensic tools can become a crutch. “Push-button” tools can make exams much more efficient, but they don't relieve the examiner of his or her responsibility to understand what's going on beneath the surface. Examiners need to understand not only what the tool is doing, but also how the artifact in question is created to begin with.

Some of the forensic tools that an examiner may use are listed in [Table 3.2](#). Many of these companies offer video tutorials or demonstrations of their products. These can be a great source of additional information. They are typically available from their web site or on YouTube. This is in no way meant as an endorsement of a specific tool. These are only a representative sampling of the many tools that are available.

## ACCREDITATION

Accreditation is an endorsement of a crime lab's policies and procedures, the way it does business, if you will ([James & Nordby, 2009](#)). The American Society of Crime Laboratory Directors/Laboratory Accreditation Board (ASCLD/LAB) is recognized as a world leader in the accreditation of forensic laboratories. Despite the name, ASCLD/LAB grants accreditation to labs both inside and outside the United States, which it has been doing since 1982 (Barbara).

**Table 3.2**

**Some hardware and software tools that may be found in a digital forensics laboratory**

Tool	Use	URL
Forensic Toolkit Access Data Group, LLC	Multipurpose tool (acquisition, verification, searching, reporting, wiping, etc.)	<a href="http://accessdata.com">http://accessdata.com</a>
EnCase Guidance Software, Inc.	Multipurpose tool (acquisition, verification, searching, reporting, wiping, etc.)	<a href="http://www.guidancesoftware.com">http://www.guidancesoftware.com</a>
SMART & SMART for Linux ASR Data, Data Acquisition and Analysis, LLC	Multipurpose tool (acquisition, verification, searching, reporting, wiping, etc.)	<a href="http://www.asrdata.com/forensic-software/">http://www.asrdata.com/forensic-software/</a>
X-Ways Forensics X-Ways Software Technology AG	Multipurpose tool (acquisition, verification, searching, reporting, wiping, etc.)	<a href="http://www.x-ways.net/forensics/">http://www.x-ways.net/forensics/</a>
Helix3 Pro e-fense, Inc.	Multipurpose tool (acquisition, verification, searching, reporting, wiping, etc.)	<a href="http://www.e-fense.com/products.php">http://www.e-fense.com/products.php</a>
Softblock, Macquisition, Blacklight BlackBag Technologies, Inc.	Multiple Macintosh forensic tools	<a href="https://www.blackbagtech.com/forensics.html">https://www.blackbagtech.com/forensics.html</a>
Mac Marshall Architecture Technology Corporation	Multiple Macintosh forensic tools	<a href="http://www.macmarshall.com/">http://www.macmarshall.com/</a>
Raptor Forward Discovery, Inc.	Linux-based acquisition and preview tool	<a href="http://www.forwarddiscovery.com/Raptor">http://www.forwarddiscovery.com/Raptor</a>
Dossier Logicube, Inc.	Hardware acquisition	<a href="http://www.logicube.com/">http://www.logicube.com/</a>
Forensic hardware tools Tableau	Write blockers, bridges, storage, acquisition	<a href="http://www.tableau.com/">http://www.tableau.com/</a>
Wiebetech	Storage, write blockers, etc.	<a href="http://www.wiebotech.com/home.php">http://www.wiebotech.com/home.php</a>

Based in Garner, North Carolina, ASCLD/LAB has accredited a total of 385 crime laboratories, 17 of those being outside the United States (American Society of Crime Laboratory Directors/Laboratory Accreditation Board).

According to ASCLD/LAB, they have four objectives. They are to:

1. improve the quality of laboratory services provided to the criminal justice system.
2. develop and maintain criteria that may be used by a laboratory to assess its level of performance and to strengthen its operation.

3. provide an independent, impartial, and objective system by which laboratories can benefit from a total operational review.
4. offer to the general public and to users of laboratory services a means of identifying those laboratories that have demonstrated that they meet established standards (American Society of Crime Laboratory Directors/Laboratory Accreditation Board).

Think of ASCLD/LAB as the “Good Housekeeping Seal of Approval” for forensic science. The earning and maintaining an ASCLD/LAB accreditation is no easy chore. It requires an unbelievable amount of time, planning, documentation, and money. Nothing is taken for granted. Every standard met must be backed up with extensive, detailed documentation.

ASCLD/LAB offers two accreditation programs. The first is the legacy program and the second is the international program. The legacy program is the first program instituted by ASCLD/LAB. As you might expect, there are differences between the two programs as well as some common ground. A major difference is the number of criteria that must be met under each program. The international program has considerably more standards to meet than the legacy program. Labs seeking accreditation under the international program are required to fulfill the relevant requirements to demonstrate conformance to the applicable requirements of both the ISO/IEC 17025:1999(E) General Requirements for the Competence of Testing and Calibration Laboratories and the ASCLD/LAB-International Supplemental Requirements for the Accreditation of Forensic Science Testing and Calibration Laboratories.

While accreditation is highly desirable, it's not mandatory. Non-accredited labs can and do successfully process evidence. The reality is that obtaining and maintaining an accredited forensic lab is both a cash and labor-intensive proposition. The kind of staffing and funding commitment required is tough to secure and frankly is not an option for everyone.

#### **THE AMERICAN SOCIETY FOR TESTING AND MATERIALS (ASTM)**

In addition to ASCLD/LAB, ASTM International also provides standards for the various disciplines within the forensic sciences, including digital forensics. ASTM International was formerly known as the **American Society for Testing and Materials**. It was founded in 1898 by engineers and chemists of the Pennsylvania Railroad. The standards are developed by subject matter experts that are members of ASTM (ASTM International).

#### **Accreditation versus Certification**

These terms may seem interchangeable; however, in the context of a forensic laboratory, they are not. As described earlier, accreditation refers to the laboratory, whereas certification pertains to the individual examiners. Certification normally requires an examiner to pass a written or practical test(s).

The Scientific Working Group on Digital Evidence (SWGDE) issued a paper addressing the certification of digital forensic practitioners. SWGDE asserts that any digital forensic certification must address the following core competencies, at a minimum:

1. Pre-examination procedures and legal issues
2. Media assessment and analysis
3. Data recovery
4. Specific analysis of recovered data
5. Documentation and reporting
6. Presentation of findings ([Scientific Working Group on Digital Evidence, 2010](#))

## SUMMARY

The forensic laboratory plays a critical role in our justice system. Well presented forensic evidence can be very, very persuasive to a jury. Many, many cases turn on the forensic evidence itself or the lack thereof. The forensic laboratory therefore plays a pivotal role in the search for justice.

Quality must be a priority in every forensic laboratory and to every forensic professional. Digital forensics is no different. Quality is achieved through the strict adherence to established quality standards as part of an overall quality assurance program. Accreditation of a digital forensics laboratory is one way to ensure conformance to these standards. The recognized world leader in accreditation of forensic labs is ASCLD/LAB. Standards for digital forensics are drafted by the ASTM.

Accreditation and certification are not synonymous. The primary difference is that accreditation pertains to the physical lab where certification applies to the personnel conducting the examinations. Not only should examiners be tested to demonstrate that they are "functioning properly," so to should their tools. Only tools that have been tested and proven reliable should be used when processing a case. This testing procedure is known as validation.

Digital forensic practitioners use both software and hardware tools in their work. No one single tool does everything or does it well. Most labs will have a variety of tools at their disposal to give them the broad capability they need given the wide array of technology they see coming in the door for analysis.

## References

- About: American Society of Crime Laboratory Directors/Laboratory Accreditation Board.* (n.d.). Retrieved June 4, 2011, from: [http://www.asclab.org/about\\_us/aboutoverview.html](http://www.asclab.org/about_us/aboutoverview.html)
- AccessData Group, LLC. (2011, February). *Downloads: AccessData*. Retrieved August 24, 2011, from: [http://accessdata.com/downloads/media/FTK\\_3x\\_System\\_Specifications\\_Guide.pdf](http://accessdata.com/downloads/media/FTK_3x_System_Specifications_Guide.pdf)
- American Society of Crime Laboratory Directors/Laboratory Accreditation Board. (n.d.). *Did You Know: American Society of Crime Laboratory Directors/Laboratory Accreditation Board*. Retrieved June 4, 2011, from: [http://www.asclab.org/largest\\_accreditation.html](http://www.asclab.org/largest_accreditation.html)

- American Society of Crime Laboratory Directors/Laboratory Accreditation Board. (n.d.). *Objectives: American Society of Crime Laboratory Directors/Laboratory Accreditation Board*. Retrieved June 4, 2011, from: [http://www.asclab.org/about\\_us/objectives.html](http://www.asclab.org/about_us/objectives.html)
- Barbara, J. J. (n.d.). *Digital Evidence Accreditation*. Retrieved August 25, 2011, from: <http://www.forensicmag.com/article/digital-evidence-accreditation?page=0,3>
- Barbara, J. J. (n.d.). *Digital Evidence Accreditation: Forensic Magazine*. Retrieved June 4, 2011, from: <http://www.forensicmag.com/article/digital-evidence-accreditation>
- Brunty, J. (2011, March 2). *Validation of Forensic Tools and Software: A Quick Guide for the Digital Forensic Examiner*. Retrieved August 24, 2011, from: <http://www.dfinews.com/article/validation-forensic-tools-and-software-quick-guide-digital-forensic-examiner?page=0,2>
- Carrier, B. B. (2002, October). *Papers: Digital-evidence.org*. Retrieved August 24, 2011, from: [http://www.digital-evidence.org/papers/opensrc\\_legal.pdf](http://www.digital-evidence.org/papers/opensrc_legal.pdf)
- Chan, S. (1994, August 21). *Scores of Convictions Reviewed as Chemist Faces Perjury Accusations*. Retrieved from LATimes.com: [http://articles.latimes.com/1994-08-21/news/mn-29449\\_1\\_lab-tests-fred-zain-double-murder](http://articles.latimes.com/1994-08-21/news/mn-29449_1_lab-tests-fred-zain-double-murder) (Accessed 21.08.94).
- Federal Bureau of Investigation. (2010). *Regional Computer Forensics Laboratory Annual Report Fiscal Year 2010*. Washington, DC: U.S. Department of Justice.
- James, S., & Nordby, J. J. (2009). *Forensic Science: An Introduction to Scientific and Investigative Techniques, Third Edition*. Boca Raton, FL: CRC Press.
- National Institute of Justice. (2004). *Forensic Examination of Digital Evidence: A Guide for Law Enforcement*. Washington, DC: U.S. Department of Justice.
- National Institute of Justice. (2009). *Test Results for Hardware Write Block Device: T4 Forensic SCSI Bridge (FireWire Interface)*. U.S. Department of Justice, Office of Justice Programs. Washington, DC: National Institute of Justice.
- National Institute of Standards and Technology. (n.d.). *Computer Forensics Tool Testing Project Web Site: National Institute of Standards and Technology*. Retrieved June 6, 2011, from: <http://www.cftt.nist.gov/index.html>
- Saferstein, R. (2006). *Criminalistics: An Introduction to Forensic Science (College Edition) (9th ed.)*. Upper Saddle River, NJ: Prentice Hall.
- Scientific Working Group on Digital Evidence. (2010, May 15). *Minimum Requirements for Quality Assurance in the Processing of Digital and Multimedia Evidence*. Retrieved August 24, 2011, from: <http://www.swgde.org/documents/current-documents/>
- Whitcomb, C. A. (n.d.). *Virtual Digital Forensics Lab*. Largo, FL: National Center for Forensic Science.
- WSAZ. (2011, April 1). *UPDATE: Donald Good Receives Two Life Sentences in Mall Rape Case*. Retrieved from WSAZ.com: [http://www.wsaz.com/news/headlines/UPDATE\\_Judge\\_OHanlon\\_Will\\_Preside\\_Over\\_Huntington\\_Mall\\_Rape\\_Case.html](http://www.wsaz.com/news/headlines/UPDATE_Judge_OHanlon_Will_Preside_Over_Huntington_Mall_Rape_Case.html) (Accessed 17.11.11).

# CHAPTER 4

# Collecting Evidence

45

## Information in This Chapter:

- Introduction to Crime Scenes
- Documenting the Scene and the Evidence
- Establishing and Maintaining the Chain of Custody
- Forensic Cloning of Evidence
- Dealing with Live Systems and Dead Systems
- Using Hashing to Verify the Integrity of Evidence
- Drafting the Examiner's Final Report

## INTRODUCTION

That “smoking gun” you discovered will never get to a jury unless it’s been properly collected and accounted for starting at the scene. As important as it is, you’ll never see it done right on TV cop shows. Nothing kills the excitement faster than three solid hours of paperwork. In the real world, it’s those three solid hours of paperwork that get your evidence into court. It all starts at the crime scene. Just locating the evidence can be tough. Especially with stamp-sized (or smaller) memory cards and the like. They could be hidden in an almost limitless number of places.

At the scene, examiners could be confronted with a variety of devices and storage media. They could find one or more running computers and wireless devices like cell phones. Together, they present some unique challenges for the investigator.

Actions during the collection process must be well documented. Notes, photos, video, and sketches record our actions and refresh our recollections. As digital evidence is extremely volatile, preservation is paramount. If at all possible, a forensic image or clone is made of the suspect media. The exam is conducted on the clone (which is an exact bit for bit copy) rather than the original.

## CRIME SCENES AND COLLECTING EVIDENCE

From a practical standpoint, not all scenes involving digital evidence are created or treated equally. Digital evidence has been the focus of criminal, civil, and administrative proceedings. There are distinct differences in how the scene and the evidence may be handled and documented for these proceedings. Some cases, like a homicide, will require painstaking documentation. Others, like a civil dispute, will necessitate a somewhat less intense response. While acknowledging these subtle differences, there are certain core principles and protocols that will remain consistent.

After it's deemed safe, job one at a digital crime scene, or any other, is securing the evidence. The scene and its evidence must be protected from accidental or intentional compromise. Securing a traditional crime scene entails limiting physical access by those folks that don't have a legitimate reason to be there. Nosy neighbors, the news media, and police supervisors are typical crime scene trespassers. Securing a traditional scene is accomplished by stringing crime scene tape, posting guards, or simply asking people to leave.

In contrast, a scene with digital evidence presents an entirely new dimension of access. Most computers and digital devices are connected to the Internet, cellular, or other kinds of networks. It's this connection that permits remote access and puts the evidence at risk. Computers and wireless devices must be made inaccessible as soon as you're sure that no volatile data would be lost ([Association of Chief Police Officers, 2011](#)). For computers, it may be a matter of removing the Ethernet cable or unplugging a wireless modem or router. With wireless devices such as cell phones, we must take steps to isolate the phone from network signals.

### Removable Media

If legally permissible (such as with a warrant), we want to search anywhere that could contain a piece of storage media. Considering today's "stamp-sized" memory cards, this piece of evidence could be hidden almost anywhere such as in books, wallets, hat bands, etc.

Despite their small size, memory cards can hold a ton of potential evidence such as child pornography or stolen credit card numbers. Let's break it down. A quick check of [Amazon.com](#) shows that you can buy a 64 gigabyte memory card for around \$120. Gigabytes (GB) are pretty abstract for most of us. Instead of using a standard unit of data storage, we'll use an example that is less conventional yet more relatable.

We're going to convert the 64 GB memory card into our own unit of measure, which we will call "Potters"—Harry "Potters," to be exact. Picture a set of all seven books in the Harry Potter series. In rough numbers, each GB contains

about 109 complete sets. With some simple math, we find that our 64 GB memory card can hold approximately seven thousand complete sets of books on something about the size of a postage stamp! Think about the amount of evidence that could be pulled from just one memory card.

#### REMOVABLE STORAGE MEDIA

Removable storage media include things like DVDs, external hard drives, thumb drives, and memory cards.

We're not just interested in the devices and storage media at the scene; the surrounding area and items are also worth a look. For example, books and manuals can give investigators clues as to the skill level of the target and what kind of technology they may be up against. Perhaps the biggest payoff is an alert to the possible use of encryption. Discarded packaging in the trash could also be helpful. Any forensic examiner would tell you that avoiding encryption is definitely worth the trouble.

### Cell Phones

Almost everyone has a cell phone these days. As such, they often contain some very valuable evidence. Text messages, e-mail, call logs, and contacts are examples of what you can recover. These items can be used to show intent, determine the last person to come in contact with a murder victim, establish alibis, determine approximate locations, and more.

As with other electronic devices, our first mandate is to make no changes to the device or its storage media. Therefore, interacting with the phone should be avoided unless absolutely necessary. Cell phones are particularly vulnerable because they can be wiped by the cell provider or even by the owner themselves. This functionality is intended to protect your data should you lose your phone or have it stolen. Apple's "Find My Phone" app is one notable example. We must address this concern by isolating or shielding the phone as soon as possible.

You have a few options to get this done:

- Turn the phone off. The concern with this approach is the same as a PC. The phone may be password-protected. Once powered down, the code may be necessary to access the phone. If possible, it may be best to isolate the phone in a Faraday bag or arson can and leave it powered on. It can then be transported to the lab to be examined in a shielded room, and so on.
- Place the phone in special containers that shield the phone from wireless signals. Empty paint cans and Faraday bags are two of the more typical choices. Both of these items are effective at safeguarding the phone from cell signals. (See [Figure 4.1](#).)



**FIGURE 4.1**  
A Faraday bag and cell phone.

### ALERT!

#### Protecting Cell Phones from Network Signals

It's essential to isolate a live cell phone from the network. If not, it can receive calls, text messages, or even commands to delete all the data. A **Faraday bag** is one way to prevent a network signal from reaching the phone. A Faraday bag is made of "some type of conducting material or mesh" that repels these signals. The function of the bag is based on the work of Michael Faraday, an English scientist who specialized in electromagnetism (Microsoft Corporation).

### ALERT!

#### Power

Power is a concern whenever you seize a cell phone. If the phone is on, it will continuously try to connect to a tower, draining the battery. If the phone is off, you should also seize the power cables. Lab personnel may very well need to recharge the device in order to complete their exam.

Failing to remove connectivity to these devices not only risks destruction of the evidence; it can raise serious concerns about its integrity as well. A competent attorney could successfully argue that this evidence is untrustworthy and should be excluded.

After securing the evidence, a survey of the scene will give investigators an accurate sense of what's ahead. Several questions need to be answered:

- What kinds of devices are present?
- How many devices are we dealing with?
- Are any of the devices running?
- What tools will be needed?
- Do we have the necessary expertise on hand?

Once these questions are answered, the real work begins.

## Order of Volatility

It's a good idea to prioritize the evidence to be collected. Generally, we want to start with the most volatile evidence first. In computer parlance, this is known as the **order of volatility**. This descending list works from the most volatile (RAM) to the least volatile (archived data). The order of volatility is:

1. CPU, cache, and register content
2. Routing table, ARP cache, process table, kernel statistics
3. Memory
4. Temporary file system/swap space
5. Data on hard disk
6. Remotely logged data
7. Data contained on archival media ([Henry, 2009](#))

## DOCUMENTING THE SCENE

There is an old tried and true saying in law enforcement: "*If you don't write it down, it didn't happen.*" These are words of wisdom indeed. Regardless of the situation, any time evidence is collected, documentation is a vitally important part of the process. There are several different types of documentation. The most common in terms of digital forensics are photographs and written notes; video is also an option for documenting evidence.

This documentation process begins the moment investigators arrive at the scene. Typically, we start by noting the date and time of our arrival along with all the people at the scene. The remainder of our notes consists of detailed descriptions of the evidence we collect, its location, the names of who discovered and collected it, and how it was collected. It's also a good idea to note the item's condition, especially if there is visible damage.

Accurately and precisely describing the evidence is of critical importance. A piece of digital evidence is described by type, make, model, serial number, or other similar descriptors. It's also important to note whether a device is on or off or if it's connected to other devices (such as printers) or a network (like the Internet). Virtually everything we see, find, and do should be documented.

While we're talking about peripheral connections, it is good practice to label each so that the entire system can be reconstructed in the lab should that become necessary.

After the scene and evidence are secure, our attention can turn to the documentation as well as identifying and collecting potential sources of evidence. Before anything is done, it's prudent to do a walk-through to survey the scene, pinpointing the type and number of devices as well as resources that will be needed.

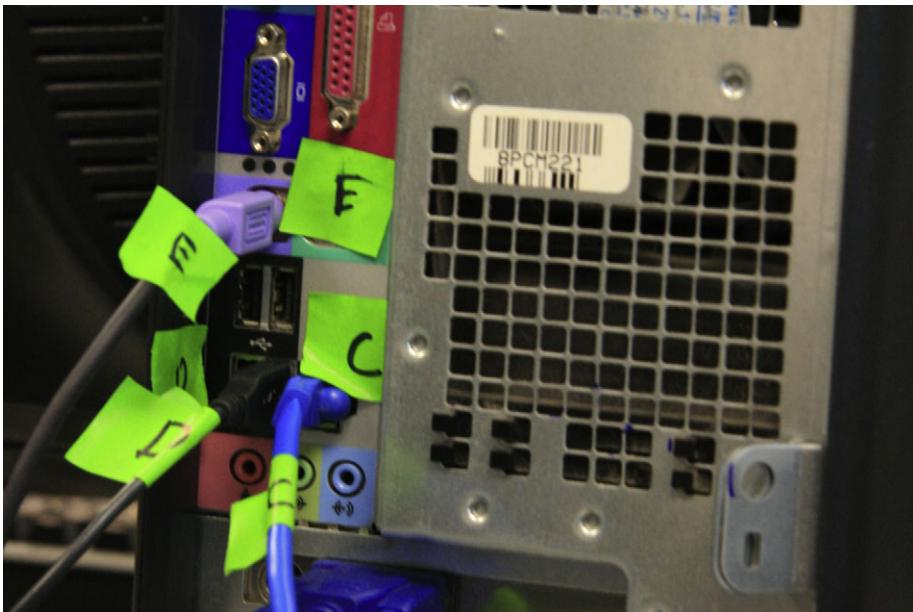
## Photography

Next, the entire scene should be photographed. Photos should be taken of the scene before anything is disturbed, including the evidence. It's helpful to think of the photos as telling a story. Remember, at some point, you may have to walk a judge or jury through this scene weeks, months, or even years later.

Start with a broad perspective, perhaps the outside of the house or office being investigated. After the overall scene has been photographed, we can then focus on each individual piece of evidence. Long-, medium-, and close-range photos show the item in the context of its surroundings. The photos of each item should clearly show the condition of the item as it was found. We need to pay particular attention to and capture things like identifying information such as serial numbers, damage, and connections. Connection examples could include networks and peripherals such as printers and scanners. It's very important to keep in mind that this is likely the only chance we'll get to capture the scene. So, when in doubt shoot more, not less.

You've probably seen photos with both the evidence item and a ruler of some sort. This is done to give some perspective to the item. It gives us an idea as to the size of that particular piece of evidence. Remember, we want to record the scene before it's disturbed or altered in any way so inserting anything into the scene with that item (like a ruler) can qualify as alteration. If it is necessary to show the size of the piece of evidence, it's a good idea to take a picture without the ruler first, then one with the ruler.

Photographs are used to depict the scene and the evidence exactly as we find them to help supplement our notes. They don't replace them. Notes capture our personal observations that won't be recorded in a photo. They are used to refresh our recollections when we go to court. Photos are a great aid to help us tell our story to the judge and jury. They really are worth a thousand words.

**FIGURE 4.2**

Marked cables from the back of a PC. Labels are placed on both ends of a cable to help document how what was connected to the PC at the time it was collected.

## Notes

As we photograph the evidence, we'll also be taking detailed notes of our actions along with any potential evidence we find. There is no set standard for note-taking. It's really up to the individual on how they want to document things. Chronological order is a common method. You would want to note things such as the time you arrived, who was present at the scene, who took what action, who found and collected which piece of evidence, and so on.

Never lose sight of the fact that you will be relying on these photos, notes, and reports months or years later when you prepare for court. With that in mind, you will want more detail rather than less. Memories fade, cases run together, and details get blurry. They should also be legible for the same reason. If cost is a concern, keep in mind that digital photos are cheap. You can fit a lot of photos on today's memory cards.

What you write in those notes matters to other people involved in the case, especially if they end up being turned over to the opposition. Under certain legal requirements, your notes could become discoverable and made available to the opposing side. This can happen if you take your notes with you to the witness stand. With that in mind, it's important not to draw conclusions or speculate based on your initial observations. You could very well end up eating those words and losing the case. It's best to keep those notes focused on what

you do and observe at the scene. Saving the interpretations and conclusions until after the analysis is a much better approach.

## CHAIN OF CUSTODY

Before a piece of evidence gets in front of a jury, it must first meet a series of strict legal requirements. One of those is a well-documented chain of custody. A computer taken in as evidence makes many stops on its road to trial. It's collected, logged in at the lab, stored, checked out for analysis, checked back in for storage, and so on. Each of these stops must be noted, tracking each and every time the evidence item changes hands or locations. Without this detailed accounting, the evidence will be deemed untrustworthy and inadmissible. It's this detailed trail that makes up the chain of custody.

## Marking Evidence

The first "link" in the chain of custody in any case is the person collecting the evidence. Civil cases may differ a bit in that IT staff or others may hold the distinction of being the first link. The evidence is marked as it is collected. Typically, evidence items are marked with initials, dates, and possibly case numbers. Permanent markers are best to ensure the markings aren't smudged or removed altogether. Apart from documenting the chain of custody, these marks help authenticate the item should it be introduced in court. The person who collected the item may be asked to identify it from the witness stand. What needs to be proved is that the item presented is the same one that was collected. These marks make this identification a near sure thing. (See Figure 4.3.)

Items small enough are normally sealed in a bag with tamper-proof evidence tape. The seal is then initialed and dated. The bags are usually made of paper, plastic, or special anti-static material. The anti-static material bags are used for electronics because this material helps protect the sensitive electronics found on hard drives from being damaged by static electricity.

## CLONING

A forensic clone is an exact, bit for bit copy of a hard drive. It's also known as a bit stream image. In other words, every bit (1 or 0) is duplicated on a separate, forensically clean piece of media, such as a hard drive. Why go to all that trouble? Why not just copy and paste the files? The reasons are significant. First, copying and pasting only gets the active data. That is, data that are accessible to the user. These are the files and folders that users interact with, such as a Microsoft Word document. Second, it does NOT get the data in the unallocated space, including deleted and partially overwritten files. Third, it doesn't capture the file system data. All of this would result in an ineffective and incomplete forensic exam.

**FIGURE 4.3**

A marked piece of evidence, sealed in an evidence bag. (Photo courtesy of Marshall University.)

We will want to make a forensic clone of the suspect's hard drive(s) as soon as we reasonably can. Cloning a drive can be a pretty time-consuming process, and for that reason it usually makes more sense to do the cloning in the lab as opposed to at the scene. Cloning in the lab eliminates the need to be on scene for what could be hours. It also provides a much more stable environment, affording us better control of the process.

Before we take a computer off premises, we must have the legal authority to do so. In a criminal case, this request and the rationale behind it should be part of the search warrant application. In civil cases, this provision can be negotiated by the parties or ordered by a judge.

Although taking the hardware back to the lab is routine in criminal cases, the cloning may have to be done at the scene in a civil case. Most civil cases with digital evidence focus on business computers. A business computer sitting in a lab isn't generating any revenue, which tends to get business folks understandably cranky. If the hard drive in a business computer can't be replaced, then the machine is often cloned and put right back into service.

### Purpose of Cloning

We know from earlier chapters that digital evidence is extremely volatile. As such, you never want to conduct your examination on the original evidence unless there are exigent circumstances or there is no other option available. Exigent circumstances could include situations in which a child is missing. Sometimes there are no tools or techniques available to solve the problem at hand.

Examining the clone affords us the chance at a "mulligan" should something go wrong. If possible, the original drive should be preserved in a safe place and only brought out to reimagine if needed.

Hard drives are susceptible to failure. Having two clones gives you one to examine and one to fall back on. Ideally, all examinations are done on a clone as opposed to the original.

Sometimes that isn't an option, especially in a business setting when the machine and drive must be returned to service. In the eyes of the court, a properly authenticated forensic clone is as good as the original.

### The Cloning Process

Cloning a hard drive should be a pretty straightforward process, at least in theory. Typically, you will clone one hard drive to another. The suspect's drive is known as the source drive and the drive you are cloning to is called the destination drive. The destination drive must be at least as large (if not slightly larger) than our source drive. Although it is not always possible, knowing the size of the source in advance is pretty handy. Bringing the right size drive will save a lot of time and aggravation.

The drive we want to clone (the source) is normally removed from the computer. It's then connected via cable to a cloning device of some kind or to another computer. It's **critical** to have some type of write blocking in place before starting the process. A write block is a crucial piece of hardware or software that is used to safeguard the original evidence during the cloning process. The hardware write block is placed between the cloning device (PC, laptop, or standalone hardware) and the source. The write block prevents any data from being written to the original evidence drive. Using this kind of device eliminates the possibility of inadvertently compromising the evidence. Remember, the hardware write blocking device goes in between the source drive and the cloning platform.

There is a little prep work involved in making a clone. The destination drive must be forensically cleaned prior to cloning a suspect's drive to it. Most if

not all forensic imaging tools will generate some type of paper trail, proving that this cleaning has taken place. This paperwork becomes part of the case file.

Once the connections are made, the process is started with the press of a couple of buttons or clicks of a mouse. When complete, a short report should be generated by the tool indicating whether or not the cloning was successful. Cloning is successful when the hash values (think “digital fingerprint”) for the source and clone match. We’ll dig deeper into hash values in just a bit.

## Forensically Clean Media

A forensically clean drive is one that can be proven to be devoid of any data at the time the clone is made. Being sterile is another way of looking at it. It is important to prove the drive is clean because comingled data is inadmissible data. Drives can be cleaned with the same devices used to make the clones. The cleaning process overwrites the entire hard drive with a particular pattern of data such as 111111111111 (Casey, 2011).

## Forensic Image Formats

The end result of the cloning process is a forensic image of the source hard drive. Our finished clone can come in a few different formats. The file extension is the most visible indicator of the file format. Some of the most common forensic image formats include:

- EnCase (Extension .E01)
- Raw dd (Extension .001)
- AccessData Custom Content Image (Extension .AD1)

There are differences in the formats, but they are all forensically sound. Some, like DD, are open source, while others, like AD1, are proprietary. Choosing one format over the other can simply be a matter of preference. Most forensic examination tools will read and write multiple image formats.

In addition to being forensically sound, the other major consideration is that the tools to be used can read the image. The documentation with the tool should provide this information. Compatibility is a concern. This is especially true when exchanging image files between examiners.

## Risks and Challenges

The biggest risk during the cloning process is in writing to the source or evidence drive. Any writes to the evidence will compromise its integrity and jeopardize its admissibility. Getting a functioning write-blocking device or software in place will keep this from happening. Proper cloning should be pretty boring. Any time it gets exciting, you’ve got problems. What can ratchet up the adrenaline? Bad sectors and damaged or malfunctioning drives come to mind. A corrupt boot sector or a failing motor can also create complications.

## Value in eDiscovery

The Sedona Conference, the leading think tank on electronic discovery, defines eDiscovery as: "The process of identifying, preserving, collecting, preparing, reviewing, and producing electronically stored information ("ESI") in the context of the legal process" ([Sedona Conference, 2010](#)).

Forensic cloning provides some additional value in the eDiscovery process. Preservation of potentially relevant data is paramount in electronic discovery. Parties that fail to preserve evidence can face some very stiff punishment. Forensic cloning is one option available to preserve some kinds of media such as hard drives and removable media such as flash drives. It serves as the "gold standard" of data preservation in that it preserves all of the data on a piece of media, not just the active data. The down side of cloning is that it can be expensive and just not practical in all situations.

### ALERT!

#### Sanctions in Electronic Discovery

Take the case of *E.I. du Pont de Nemours v. Kolon Industries* (2011). In this case, the jury awarded \$919 million to DuPont in an eye-popping verdict. Earlier in the case, the court determined that Kolon had destroyed e-mails and other potentially relevant data connecting it to the theft of trade secrets. As a result of that determination, the judge instructed the jury that Kolon (both executives and employees) deleted important evidence even though they had a duty to preserve it. Kolon's suffering may not end there. DuPont plans on requesting \$50 million in punitive damages plus \$30 million more for attorney fees (Favro, 2011).

## LIVE SYSTEM VERSUS DEAD SYSTEM

Up to now, we've been talking about "dead" or powered off machines. What happens when we come across a running computer? At the moment there is no consensus on the answer. A growing debate exists in the digital forensics community about how to handle a "live" or running machine. The "old school" solution is simply to pull the plug, instantly removing power to the computer. Today, that approach is garnering second thoughts. There are compelling reasons not to pull the power on a running computer. Next, we'll look at the reasons both for and against this somewhat controversial method.

## Live Acquisition Concerns

On the plus side, pulling the plug eliminates the need to interact with the running machine. Interacting with a running computer, in any way, causes changes to the system. Any change to a piece of evidence is bad and can cause major problems from a legal standpoint. These alterations can call the integrity of

the evidence into question. Even when a machine is just sitting powered on, things are changing. When a person interacts with a running machine, even more things are changing. Knowing that change is a forensic faux pas; it's easy to see why pulling the plug is an attractive option. On a side note, these changes may have no impact on the artifacts relevant to the case. But the system is changing nonetheless.

We are now starting to second-guess this approach, recognizing that pulling the plug has some significant downsides.

For starters, yanking the plug means that any evidence in RAM will be under real threat of destruction. Data in RAM start to dissipate or fade when power is removed. There is a technique that can be used to preserve data in memory after the power is off, but it's not yet been widely adopted. (See the sidebar.)

## MORE ADVANCED

### Preserving Evidence in RAM

It's widely thought that data in RAM vanish when the power is turned off. That's really not true. Research by Princeton University has shown that data in RAM fade rather than disappear. This dissipation can be further slowed if the RAM is cooled to -58 deg Fahrenheit (-50 Celsius). This cooling will give examiners more time to collect this volatile data. To see this technique in action, see the video here: <http://www.youtube.com/watch?v=JDaicPlgn9U>.

Second, is encryption. The system or files may be unencrypted while the machine is powered on. Abruptly pulling the plug could return it to an encrypted state, potentially putting that evidence out of reach for good. Avoiding encryption is a good idea any time.

Third, a sudden loss of power could damage the data, rendering them unreadable. Fourth, some evidence may not get recorded on the drive unless and until the computer is properly shut down.

The old school solution of pulling the plug is not the only option on the table these days. There are now tools and techniques that will capture volatile memory from a live machine in a forensically sound manner. With these advances, it's time to start recognizing the advantages of live collection.

## Advantage of Live Collection

Until fairly recently, pulling the plug was the only real option. Capturing data in a running computer's main memory (RAM) wasn't a realistic option. The potential solutions that existed just weren't practical to be used in the field. In contrast, present-day examiners do have some forensically sound alternatives. There are several commercial and open source tools that can be used to collect these

volatile data. Unlike the older lab-bound approaches, these tools are very simple to use—so simple, in fact, that they are being marketed to nontechnical folks like most first responders. First responders could include patrol officers and IT staff among others. While these tools do simplify the process, they still require training for proper use.

### Principles of Live Collection

Doing a live collection is not a rudimentary task. The following is an example of one approach.

After coming across a running computer at the scene, a couple of questions will need to be answered right from the start. Is the potential evidence to be recovered truly worth the time and effort? In some instances, the answer may be “no.” In cases involving malware, RAM is vitally important. In others, such as a clear-cut possession of child pornography, RAM will likely have little value. Second, are the necessary resources available? To successfully capture the evidence in memory will require some specialized tools and training. Without these key ingredients, it could be best to punt and simply pull the plug. The risk of compromising the evidence may simply be too great. It’s important to be able to recognize when you are in over your head and when you should call for help.

When interacting with a live machine, it’s best to always choose the least invasive approach possible. This will require thinking before you click. Haste is not your friend in this situation. As mentioned earlier, we want to collect the most volatile information first.

#### ALERT!

##### Evidence in RAM

A computer’s **volatile memory** (RAM) can contain some very valuable evidence, including running processes, executed console commands, passwords in clear text, unencrypted data, instant messages, Internet Protocol addresses, and Trojan horse(s) ([Shipley & Reeve, 2006](#)).

### Conducting and Documenting a Live Collection

Now comes the tricky part. It’s time to get focused. Once you start, you should work uninterrupted until the process is complete. To do otherwise only invites mistakes. Before getting underway, gather everything you will need: report forms, pens, memory capture tools, and so on. Every interaction with the computer will need to be noted. You could use an action/response approach (“I did this ... The computer did that.”).

If the desktop isn’t visible, you can move the mouse slightly to wake it up. If that fails to bring up the desktop, pressing a single key should solve the

problem. You should of course document which key was depressed in your notes. Now that you can see the desktop, the first thing to note is the date and time as it appears on the computer. Next, record the icons and running applications. You don't want to stop there. Documenting the running processes could help identify any malware that is in residence on the computer. The running processes can be documented by accessing the task manager. Why would that matter? One of the more popular defenses, especially in child pornography cases, is to claim that the contraband images were deposited by an unknown third party by way of a Trojan.

Now it's time to use a validated memory capture tool to collect that volatile evidence in the RAM. After this step is complete, the process ends with proper shutdown. The proper shutdown allows any running application a chance to write any artifacts to the disk, allowing us to recover them later.

## HASHING

How do we know our clone is an exact duplicate of the evidence drive? The answer comes in the form of a hash value. A hash is a unique value generated by a cryptographic hashing algorithm. **Hash values (functions)** are used in a variety of ways including cryptography and evidence integrity. Hash values are commonly referred to as a "digital fingerprint" or "digital DNA." Any change to the hard drive, even by a single bit, will result in a radically different hash value. Therefore, any tampering or manipulation of the evidence is readily detectable.

### Types of Hashing Algorithms

There are multiple types of hashing algorithms. The term algorithm may strike fear in the hearts of the mathematically challenged. Never fear. We won't be getting into any higher-level math here, but we will get comfortable with some of the basic concepts and terms. The most common hash functions used in digital forensics are Message Digest 5 (MD5), and Secure Hashing Algorithm (SHA) 1 and 2.

### Hashing Example

Let's hash a short phrase to demonstrate what happens with only a minor change. Apologies up front to any Baltimore or Cleveland fans. For this exercise, we'll use SHA1.

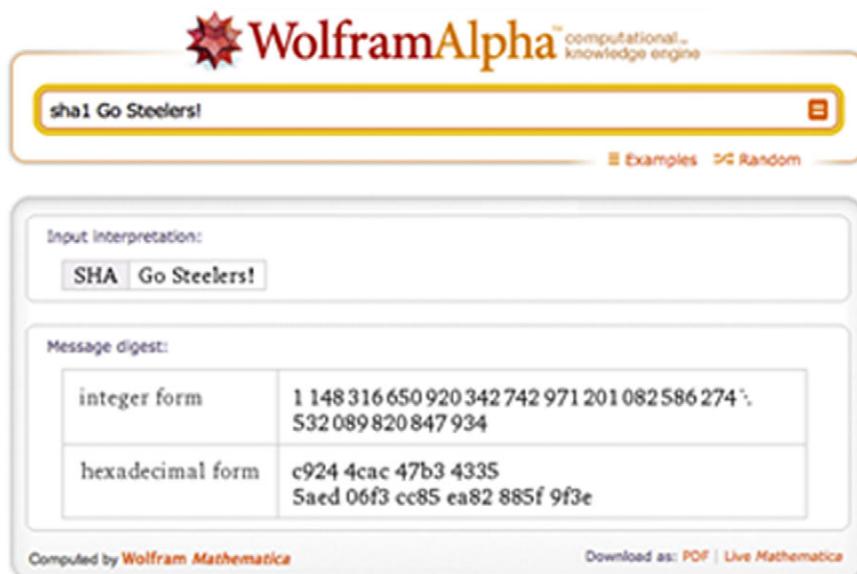
Phrase - Go Steelers!

SHA1 - c924 4cac 47b3 4335 5aed 06f3 cc85 ea82 885f 9f3e

Now let's make one small alteration, changing the "S" from upper case to lower case. When we rehash, we get this:

Phrase - Go steelers!

SHA 1 - 1a10 ffd1 db12 c88f 88e6 b070 561f 6124 f632 26ec



**FIGURE 4.4**  
WolframAlpha results.

Note the drastic change in the resulting hash values. Here they are stacked for an easier comparison:

c924 4cac 47b3 4335 5aed 06f3 cc85 ea82 885f 9f3e  
1a10 ffd1 db12 c88f 88e6 b070 561f 6124 f632 26ec

As you can see, small changes make a big difference. If you'd like to try this yourself, it's easy to do. Go to <http://www.wolframalpha.com> and enter the hash function you would like to use (MD5, SHA1, etc.), followed by a space and then the phrase Go Steelers! (See Figure 4.4.)

### Uses of Hashing

Hash values can be used throughout the digital forensic process. They can be used after the cloning process to verify that the clone is indeed an exact duplicate. They can also be used as an integrity check at any point it is needed. Examiners often have to exchange forensic images with the examiner on the opposing side. A hash value is sent along with the image so that it can be compared with the original. This comparison verifies that the image is a bit for bit copy of the original.

The relevant hash values that were generated and recorded throughout the case should be kept and included with the final report. These digital fingerprints are crucial to demonstrating the integrity of the evidence and ultimately getting them before the jury.

## FINAL REPORT

At the conclusion of the analysis, the examiner will generate a final report detailing what was done, what was found, and their findings. Ideally, final reports need to be crafted with the intended audience in mind. In reality, far too many final reports read like the owner's manual for the space shuttle. Not only can these reports be difficult to read, they can be downright intimidating.

Because they are often filled with jargon and code, these reports aren't very useful to non-technical reader's such as judges, attorneys and juries. It is important to remember that these people must be able to comprehend information contained in your report. Even the best, most compelling evidence can be ignored if the jury can't understand it.

The major forensic tools, such as EnCase and FTK, have very robust reporting features, generating quite a bit of customizable information. However, as helpful as these reports are, they are just not adequate to stand on their own. They are difficult for most non-technical readers to understand. This information should be included in the final report, but they should not serve as the lone piece of documentation for the entire examination.

The best reports will consist of much more than the standard report generated with the tool alone. The final report should include a detailed narrative of all the actions taken by the examiner, starting at the scene if they were present. The examination should be documented with sufficient detail so that the procedure can be duplicated by another examiner.

A digital forensic report written in plain English is both much appreciated and much more effective (can I get an "Amen" from the lawyers out there?).

## SUMMARY

As we discussed in this chapter, the first step in the collection process is to secure both the scene and the evidence. If the device containing the evidence is a cell phone, you will need to isolate the phone from the network signal to prevent evidence from being destroyed.

Photographs are an excellent way to document the evidence and the scene. You will photograph the entire scene (e.g., the entire room, not just the computer on the desk). You must ensure that the chain of custody is fully documented and that the evidence is properly marked.

Preservation of the evidence is critical. Capturing a forensic image or clone eliminates the need to examine the original evidence. Examining the original could lead to the evidence being excluded.

Cloning the device will produce an exact, bit-for-bit copy of the original evidence. Hash values are used to verify that the cloned evidence is identical to the original. These hash values, such as MD5 or SHA1, are often likened to "Digital DNA" or a "Digital Fingerprint." We discussed the differences between

live and dead acquisitions and the benefits and challenges of each. The final report should include detail about the scene, the collection process, the analysis, and the what conclusions, if any, were reached. It's critical that the final report be understandable to a nontechnical audience.

## References

- About: American Society of Crime Laboratory Directors/Laboratory Accreditation Board.* (n.d.). Retrieved June 4, 2011, from: [http://www.asclab.org/about\\_us/aboutoverview.html](http://www.asclab.org/about_us/aboutoverview.html)
- AccessData Group, LLC. (2011, February). *Downloads: AccessData*. Retrieved August 24, 2011, from: [http://accessdata.com/downloads/media/FTK\\_3x\\_System\\_Specifications\\_Guide.pdf](http://accessdata.com/downloads/media/FTK_3x_System_Specifications_Guide.pdf)
- American Society of Crime Laboratory Directors Laboratory Accreditation Board. (n.d.). *ASCLD/LAB Guiding Principles of Professional Responsibility for Crime Laboratories and Forensic Scientists*. Retrieved September 3, 2011, from: [http://www.asclab.org/about\\_us/guidingprinciples.html](http://www.asclab.org/about_us/guidingprinciples.html)
- American Society of Crime Laboratory Directors/Laboratory Accreditation Board. (n.d.). *Did You Know: American Society of Crime Laboratory Directors/Laboratory Accreditation Board*. Retrieved June 4, 2011, from: [http://www.asclab.org/largest\\_accreditation.html](http://www.asclab.org/largest_accreditation.html)
- American Society of Crime Laboratory Directors/Laboratory Accreditation Board. (n.d.). *Objectives: American Society of Crime Laboratory Directors/Laboratory Accreditation Board*. Retrieved June 4, 2011, from: [http://www.asclab.org/about\\_us/objectives.html](http://www.asclab.org/about_us/objectives.html)
- Association of Chief Police Officers. (2011). *Good Practice Guide for Computer-Based Electronic Evidence*. Cambridge, MA: 7Safe.
- ASTM International. (n.d.). *ASTM Overview*. Retrieved October 1, 2011, from: <http://www.astm.org/ABOUT/overview.html>
- Barbara, J. J. (n.d.). *Digital Evidence Accreditation*. Retrieved August 25, 2011, from: <http://www.forensicmag.com/article/digital-evidence-accreditation?page=0,3>
- Barbara, J. J. (n.d.). *Digital Evidence Accreditation: Forensic Magazine*. Retrieved June 4, 2011, from: <http://www.forensicmag.com/article/digital-evidence-accreditation>
- Barbara, J. J. (n.d.). *Triage a Computer*. Retrieved June 14, 2011, from: <http://www.forensicmag.com/article/triage-computer>
- Brunty, J. (2011, March 2). *Validation of Forensic Tools and Software: A Quick Guide for the Digital Forensic Examiner*. Retrieved August 24, 2011, from: <http://www.dfinews.com/article/validation-forensic-tools-and-software-quick-guide-digital-forensic-examiner?page=0,2>
- Carrier, B. B. (2002, October). *Papers: Digital-evidence.org*. Retrieved August 24, 2011, from: [http://www.digital-evidence.org/papers/opensrc\\_legal.pdf](http://www.digital-evidence.org/papers/opensrc_legal.pdf)
- Carvey, H. (2009). *Windows Forensic Analysis DVD Toolkit* (2nd ed.). Burlington, MA: Syngress.
- Casey, E. (2009). *Handbook of Digital Forensics and Investigation*. Burlington, MA: Academic Press.
- Casey, E. (2011). *Digital Evidence and Computer Crime, 3rd ed.: Forensic Science, Computers, and the Internet*. Waltham, MA: Academic Press.
- Cellebrite Mobile Synchronization LTD. (n.d.). *UFED Physical Pro*. Retrieved October 2, 2011, from: <http://www.cellebrite.com/forensic-products/forensic-products/ufed-physical-pro.html>
- Chan, S. (1994, August 21). *Scores of Convictions Reviewed as Chemist Faces Perjury Accusations: Forensics*. Retrieved September 27, 2011, from: [http://articles.latimes.com/1994-08-21/news/mn-29449\\_1\\_lab-tests-fred-zain-double-murder](http://articles.latimes.com/1994-08-21/news/mn-29449_1_lab-tests-fred-zain-double-murder)
- Craiger, P. J. (n.d.). *Virtual Digital Evidence Laboratory*. Retrieved September 16, 2011, from: <http://www.ncfs.org/VDEL.Craiger.Report.NIJ.final.pdf>

- DNA Initiative, The. (n.d.). *Glen Woodall (Huntington, West Virginia)*. Retrieved September 27, 2011, from: [http://www.dna.gov/postconviction/convicted\\_exonerated/woodall](http://www.dna.gov/postconviction/convicted_exonerated/woodall)
- EC-Council. (2009). *Computer Forensics: Investigation Procedures and Response*. Clifton Park, NY: Cengage Learning.
- Favro, P. (2011, September 15) *Breaking News: \$919 Million Verdict for DuPont in Trade Secret Theft and eDiscovery Sanctions Case*. E-Discovery blog: <http://www.clearwellsystems.com/e-discovery-blog/>
- Federal Bureau of Investigation. (2010). *Regional Computer Forensics Laboratory Annual Report Fiscal Year 2010*. Washington, DC: U.S. Department of Justice.
- Henry, P. (2009, September 12). *Best Practices in Digital Evidence Collection*. Retrieved October 15, 2011, from: <http://computer-forensics.sans.org/blog/2009/09/12/best-practices-in-digital-evidence-collection/>
- James, S., & Nordby, J. J. (2009). *Forensic Science: An Introduction to Scientific and Investigative Techniques* (3rd ed.). Boca Raton, FL: CRC Press.
- Microsoft Corporation. (n.d.). *Encarta: Michael Faraday*. Retrieved June 13, 2011, from: <http://www.webcitation.org/5kwc3quLs>
- National Institute of Justice. (n.d.). *Collecting Digital Evidence Flowchart: National Institute of Justice*. Retrieved June 14, 2011, from: <http://www.nij.gov/publications/ercrime-guide-219941/ch5-evidence-collection/collecting-digital-evidence-flowchart.htm>
- National Institute of Justice. (n.d.). *Digital Evidence and Forensics: National Institute of Justice*. Retrieved June 14, 2011, from: <http://www.nij.gov/nij/topics/forensics/evidence/digital/welcome.htm>
- National Institute of Justice. (2004). *Forensic Examination of Digital Evidence: A Guide for Law Enforcement*. Washington, DC: U.S. Department of Justice Office of Justice Programs.
- National Institute of Justice. (2008). *Electronic Crime Scene Investigation: A Guide for First Responders* (2nd ed.). Washington, DC: U.S. Department of Justice.
- National Institute of Justice. (2009a). *Electronic Crime Scene Investigation: An On-the-Scene Reference for First Responders*. Washington, DC: U.S. Department of Justice.
- National Institute of Justice. (2009b). *Test Results for Hardware Write Block Device: T4 Forensic SCSI Bridge (FireWire Interface)*. U.S. Department of Justice, Office of Justice Programs. Washington, DC: National Institute of Justice.
- National Institute of Standards & Technology. (n.d.). *CFTT Project Overview*. Retrieved September 30, 2011, from.gov: [http://www.cftt.nist.gov/project\\_overview.htm](http://www.cftt.nist.gov/project_overview.htm)
- National Institute of Standards and Technology. (n.d.). *Computer Forensics Tool Testing Project Web Site: National Institute of Standards and Technology*. Retrieved June 6, 2011, from: <http://www.cftt.nist.gov/index.html>
- Paraben Corporation. (n.d.). *Device Seizure v4.5*. Retrieved October 2, 2011, from: <http://www.paraben.com/device-seizure.html>
- Phillip, A., Cowen, D., & Davis, C. (2009). *Hacking Exposed Computer Forensics: Computer Forensics Secrets & Solutions*. New York: McGraw-Hill.
- Princeton University Center for Information Technology Policy. (2008, February 21). *Lest We Remember: Cold Boot Attacks on Encryption Keys*. Retrieved October 19, 2011, from: <http://www.youtube.com/watch?v=JDaicPlgn9U>
- Saferstein, R. (2006). *Criminalistics: An Introduction to Forensic Science (College Edition)* (9th ed.). Upper Saddle River, NJ: Prentice Hall.
- Scientific Working Group on Digital Evidence. (2009, January 15). *SWGDE Recommended Guidelines for Validation Testing v1.1*. Retrieved September 19, 2011, from: <http://www.swgde.org/documents/current-documents/>

- Scientific Working Group on Digital Evidence. (2010a, May 15). *Minimum Requirements for Quality Assurance in the Processing of Digital and Multimedia Evidence*. Retrieved August 24, 2011, from: <http://www.swgde.org/documents/current-documents/>
- Sedona Conference. (2010, September). *The Sedona Conference Glossary: E-Discovery & Digital Information Management* (3rd ed.). Retrieved October 21, 2011, from: [http://www.thesedonaconference.org/publications\\_html](http://www.thesedonaconference.org/publications_html)
- Shipley, T. G. (n.d.). *Collection of Evidence from the Internet: Part 1*. Retrieved June 14, 2011, from: <http://www.dfinews.com/article/collection-evidence-internet-part-1?page=0,1>
- Shipley, T. G. (n.d.). *Collection of Evidence from the Internet: Part 2*. Retrieved June 14, 2011, from: <http://www.dfinews.com/article/collection-evidence-internet-part-2>
- Shipley, T. G., & Reeve, H. R. (2006). *Collecting Evidence from a Running Computer: A Technical and Legal Primer for the Justice Community*. Search Group, Incorporated. Sacramento, CA: Search Group, Incorporated.
- Warrington, D. (n.d.). *Crime Scene 101: Locating and Documenting Evidence*. Retrieved June 14, 2011, from: <http://www.forensicmag.com/article/crime-scene-101-locating-and-documenting-evidence>
- Whitcomb, C. (n.d.). *A Virtual Digital Forensics Lab*. Retrieved September 28, 2011, from: <http://www.ascld.org/files/digital%20VDEL%20Craiger%20ASCLD%20cmw.pdf>
- WSAZ. (2011, April 1). *UPDATE: Donald Good Receives Two Life Sentences in Mail Rape Case*. Retrieved September 27, 2011, from: <http://www.wsaz.com/news/headlines/105522183.html>

## CHAPTER 5

# Windows System Artifacts

65

### Information in This Chapter:

- Finding Deleted Data
- Hibernation Files
- Examining the Windows Registry
- Print Spooling Evidence
- Recycle Bin Operation
- Metadata: What It Is and How It's Used
- Thumbnail Images as Evidence
- Most Recently Used Lists: How They're Created and Their Forensic Value
- Working with Restore Points and Shadow Copies
- Examining Prefetch and Link Files

## INTRODUCTION

Many say that the eyes are the window to the soul, but for the forensic examiner, Windows can be the “soul” of the computer. The odds are high that examiners will encounter the Windows operating system more times than not when conducting an investigation. The good news for us is that we can use Windows itself as a tool to recover data and track the footprints left behind by the user. Because of this, it is imperative that examiners have an extensive understanding of the Windows operating system and all of its functions.

Love it or hate it, it’s a Windows world. With about 90% ([Brodkin, 2011](#)) of the desktop market share, a forensic examiner will face a Windows machine the majority of the time. Getting cozy with Windows is an absolute necessity in this line of work. In the course of using Windows and its multitude of compatible applications, users will leave artifacts or footprints scattered throughout the machine. As you can imagine, this is pretty handy from an investigative perspective. These artifacts are often located in unfamiliar or “hard to reach” places. Even a savvy individual, bent on covering their tracks, can miss some of these buried forensic treasures.

The forensic challenge is to identify, preserve, collect, and interpret this evidence correctly. In this chapter, we'll take a closer look at many of these artifacts, their purpose, and their forensic significance.

## DELETED DATA

For the average user, hitting the delete key provides a satisfying sense of security. With the click of a mouse, we think our data are forever obliterated, never again to see the light of day. Think again. We know from [Chapter 2](#) that, contrary to what many folks believe, hitting the delete key doesn't do anything to the data itself. The file hasn't gone anywhere. "Deleting" a file only tells the computer that the space occupied by that file is available if the computer needs it. The **deleted data** will remain until another file is written over it. This can take quite some time, if it's done at all.

### MORE ADVANCED

#### File Carving

The unallocated space on a hard drive can contain valuable evidence. Extracting this data is no simple task. The process is known as file carving and can be done manually or with the help of a tool. As you might imagine, tools can greatly speed up the process. Files are identified in the unallocated space by certain unique characteristics. File headers and footers are common examples of these characteristics or signatures. Headers and footers can be used to identify the file as well as marking its beginning and end.

*Allocated space* refers to the data that the computer is using and keeping tabs on. These are all the files that we can see and open in Windows. The computer's file system monitors these files and records a variety of information about them. For example, the file system tracks and records the date and time a particular file was last modified, accessed, and created. We'll revisit this kind of information when we talk about metadata later in this chapter.

## HIBERNATION FILE (HIBERFILE.SYS)

Computers sometimes need their rest and can nap just like we do. Through this "cybernap" process, more potential evidence can be generated, depending on how "deep" the PC goes to sleep. "Deep sleep" modes like hibernation and hybrid sleep save data to the hard drive as opposed to just holding it in RAM (like "sleep"). As we know, data written to the drive itself are more persistent and can be recovered. It's possible that files deleted by a suspect could still be found here. How? Let's say that the suspect is working on an incriminating document on Monday. She has to step away for awhile to make a phone call. She puts the laptop into **hibernation** mode, which

causes the computer to save everything she is doing to the hard drive. When she returns forty-five minutes later and brings the laptop back up, everything is just like she left it, including the incriminating document. Generally, a computer can go into three different modes or states when it sleeps. Those modes are: sleep, hibernation, and hybrid sleep. (Microsoft Corporation). The different modes are intended to conserve power and can vary from laptop to desktop.

## Sleep

Sleep mode is intended to conserve energy but is also intended to get the computer back into operation as quickly as possible. Microsoft compares this state to "pausing a DVD player" (Microsoft Corporation; TechTarget). Here, a small amount of power is continuously applied to the RAM, keeping those data intact. Remember, RAM is considered volatile memory, meaning that the data disappear when power is removed. Sleep mode doesn't do much for us forensically because all the data remain in the RAM.

## Hibernation

Hibernation is also a power-saving mode but is intended for laptops rather than desktops. It is here that we start to see some potential investigative benefit. In this mode, all of the data in RAM are written to the hard drive, which, as we know, is much harder to get rid of.

## Hybrid Sleep

As the name implies, hybrid sleep is a blend of the previous two modes and is intended mainly for desktops. It keeps a minimal amount of power applied to your RAM (preserving your data and applications) and writes the data to disk.

Like the page file, suspects bent on destroying evidence can overlook these hibernation files. Pedophiles or corporate crooks will often attempt to avoid detection by deleting or destroying evidence on their hard drive as the investigation closes in around them. These hibernation files, unknown to most users, are often missed during these last minute "delete-a-thons."

## REGISTRY

The Windows Registry plays a crucial role in the operation of a PC. Microsoft's TechNet defines the registry as "simply a database for configuration files." You could also describe it as the computer's central nervous system. In that context, you can see just how critical the registry is to the Windows computer.

The registry keeps track of user and system configuration and preferences, which is no simple task. From a forensic standpoint, it can provide an abundance of potential evidence. Many of the artifacts we look for are kept in the

registry. Some of the potential evidence could include search terms, programs that were run or installed, web addresses, files that have been recently opened, and so on.

## **Registry Structure**

The registry is set up in a tree structure similar to the directories, folders, and files you're used to working with in Windows. The registry is broken into four tiers or levels.

Inspecting the registry is something that is done in nearly every forensic examination. Looking at the registry requires a tool that can translate this information into something we can understand. Two of the major multipurpose forensic tools, EnCase and FTK, do just that.

As a key repository of critical system information, the registry could contain quite a bit of evidence. As an added bonus, the Registry can also hold the information we need to break any encrypted files we find.

### *FROM THE CASE FILES: THE WINDOWS REGISTRY*

The Windows Registry helped law enforcement officials in Houston, Texas crack a credit card case. In this case, the suspect's stolen credit card numbers were used to purchase items from the Internet. The two suspects in this case, a married couple, were arrested after a controlled drop of merchandise ordered from the Internet. Examination of the computer's NTUSER.DAT, Registry, and Protected Storage System Provider information, found a listing of multiple other names, addresses, and credit card numbers that where being used online to purchase items. After further investigation, investigators discovered that these too were being used illegally without the owners consent.

The information recovered from the registry was enough to obtain additional search warrants. These extra searches netted the arrest of 22 individuals and lead to the recovery of over \$100,000 of illegally purchased merchandise. Ultimately, all of the suspects plead guilty to organized crime charges and were sentenced to jail time.

### *FROM THE CASE FILES: THE WINDOWS REGISTRY AND USBSTOR*

In a small town outside of Austin, Texas, guests at a local hotel called police after observing an individual at the hotel who was roaming mostly naked and appearing somewhat intoxicated. When the police arrived, they found the individual and determined he was staying at the hotel. They accompanied him back to his room and were surprised by what they found. When the door opened, they discovered another individual in the room and a picture of child pornography being projected on the wall. The projector was attached to a laptop. Two external hard drives were found lying next to the laptop. The unexpected occupant said that the laptop was his but that the two external

drives belonged to the other gentlemen and had never been connected to his laptop. All of the equipment was seized and sent for examination. Forensic clones were made of the laptop and both external drives. The initial examination of the external drives found both still images and movies of child pornography.

Next, examiners wanted to determine if either of those drives had ever been connected to the laptop. The system registry file of the laptop was searched for entries in the USBStor key. Listings for external hard drives were discovered along with the hardware serial numbers from both external hard drives.

Next, examiners sought to validate their results. Using a lab computer system with a clean installation of Windows, they connected the defendants external drives to the lab system. A write blocker was connected between the drives and the system to prevent any changes or modifications to the clones of the external drives.

The lab computer's system registry file was then examined and the USBStor keys showed the same external hard drive listings as the suspect's with matching hardware serial numbers. These results proved that the suspect's external hard drives had in fact been hooked to the laptop at one time. The suspect was eventually convicted of possession of child pornography.

## Attribution

Digital forensics can be used to answer many questions, such as, *what terms were searched using Google?* We can find that. *Did Bob type those terms?* Houston, we've got a problem. Unfortunately, we can rarely put someone's sticky fingers on the keyboard when a particular artifact is created. We may need to uncover other evidence in order to connect those dots.

Tracking something back to a specific user account or identifying the registered owner of the system is a much easier task. A single PC can have multiple user accounts set up on the machine. In a technical sense, user accounts establish what that specific user can and can't do on the computer (Microsoft Corporation). A PC will set up two accounts by default, the administrator and a guest account. Other accounts may be created, but they are not required. The administrator has all rights and privileges on the machine. They can do anything. A guest account (which doesn't require any login) generally has less authority.

For example, a family PC could have separate accounts for mom, dad, and each of the kids. Each of these accounts could be password-protected.

Each account on the machine is assigned a unique number called a security identifier or SID. Many actions on the computer are associated with, and tracked by, a specific SID. It's through the SID that we can tie an account to some particular action or event.

## External Drives

Information has value, sometimes substantial value. They don't keep the formula for Coke under lock and key for grins. Theft of intellectual property is a huge concern. One way that would-be thieves could easily smuggle data out of an organization is by way of one of these external storage devices, such as a thumb drive. As a result, examiners are often asked to determine whether any such device has been attached to a computer.

These devices can take a variety forms such as thumb drives or external hard drives. In addition to stealing information, these devices can also be used to inject a virus or store child pornography. Whether or not such a device was attached can be determined by data contained in the registry. The registry records this kind of information with a significant amount of detail. It tells us both the vendor and the serial number of the device.

## PRINT SPOOLING

In some investigations, a suspect's printing activities may be relevant. As you might expect, printing can also leave some tracks for us to follow. You've probably noticed that there's a bit of a delay after you click Print. This delay is an indication of a process called **spooling**. Essentially, spooling temporarily stores the print job until it can be printed at a time that is more convenient for the printer (TechTarget). During this spooling procedure, Windows creates a pair of complementary files. One is the Enhanced Meta File (EMF) which is an image of document to be printed. The other is the spool file which contains information about the print job itself.

There is one of each for every print job. What kind of information can we recover from the spool file? The spool file (.spl) tells us things like the printer name, computer name as well as the user account that sent the job to the printer. Either or both of these files may have evidentiary value. The problem is they don't stick around long. In fact, they are normally deleted automatically after the print job is finished. However, there are a few exceptions.

The first exception occurs if there is some kind of problem and the document didn't print. The second is that the computer that is initiating the print job may be set up to retain a copy. Some companies may find this setup appealing if they have some reason to hang onto a copy.

Spool and EMF files can be used to directly connect targets to their crimes. Copies of extortion letters, forged contracts, stolen client lists, and maps to body dump sites are but a few pieces of evidentiary gold potentially mined from their computers.

## RECYCLE BIN

The "trash can" has been a familiar presence on our computer desktops starting with the early Macintosh systems. It's a really good idea, especially from the casual user's perspective. Users may not understand sectors and bytes, but most everyone "gets" the trash can. Sometimes, though, the trash can "gets" them. This is especially true when they count on the trash can to erase their evidence. They assume

that their incriminating data have disappeared into a digital “Bermuda Triangle,” never again to see the light of day. Unlike Amelia Earhart, that’s definitely not the case. Using forensic tools such as Forensic Toolkit and EnCase, we can quite often bring those files back in mint condition.

## ALERT!

### Recycle Bin Function

Here’s a quick question. Where is a file moved when it’s deleted? I bet some of you said the recycle bin. That would make the most sense. I mean, that’s where we put the unwanted files, right? But it would also be wrong. When you delete a file, it’s moved to … wait for it … nowhere. The file itself stays exactly where it was. It’s a common notion that when deleted, the file is actually picked up and moved to the **recycle bin**. That’s not the case.

Unwanted files can be moved to the recycle bin a few different ways. They can be moved from a menu item or by dragging and dropping the file to the recycle bin. Finally, you can right-click on an item and choose Delete. The benefit of putting files into the recycle bin is that we can dig through it and pull our files back out. I’ve worked in places where digging through office trash can be a pretty hazardous undertaking. Fortunately, things aren’t nearly as dicey on our computers. As long as our files are still “in the can,” we can get them back. However, emptying the recycle bin (i.e., “taking out the trash”) makes recovery pretty much impossible for the average user.

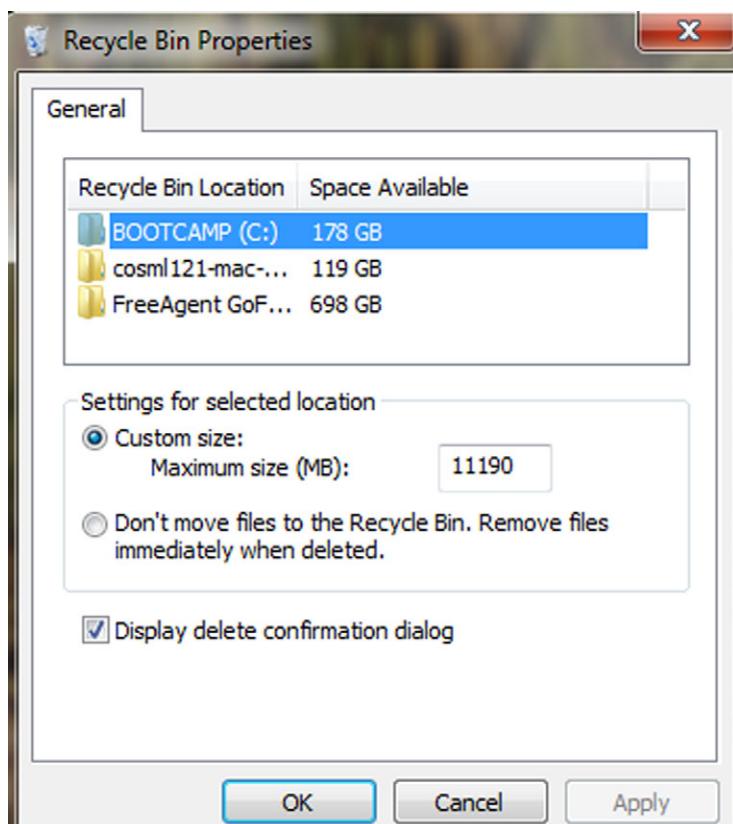
Not everything that’s deleted passes through the recycle bin. A user can actually bypass the bin altogether. Bypassing can be done a couple of ways. First, if you press Shift+Delete, the file will go straight to unallocated space without ever going through the recycle bin. You can also configure your machine to bypass the recycle bin altogether. Your deleted files won’t even brush the sides of the recycle bin.

The recycle bin is obviously one of the first places that examiners look for potential evidence. The first instinct suspects have is to get rid of any and every incriminating file on their computer. Not fully understanding how their computer works, they put all their faith in the recycle bin. Now you know that’s a bad move. Lucky for us, many folks still don’t recognize how misplaced their faith is. As a result, the recycle bin is a great place to look for all kinds of potentially incriminating files.

## MORE ADVANCED

### Recycle Bin Bypass

If an examiner suspects that the system has been set to bypass the recycle bin, the first thing they would check would be the registry. The “NukeOnDelete” value would be set to “1” indicating that this function had been switched on. (See [Figure 5.1](#).)

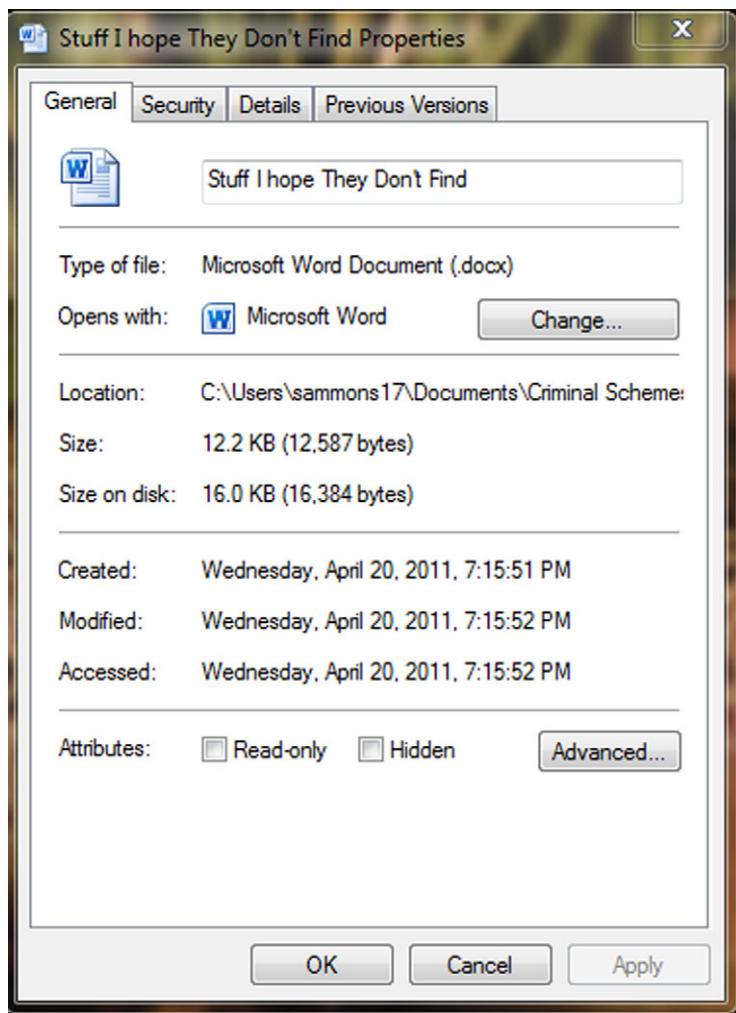


**FIGURE 5.1**  
The recycle bin bypass option.

## METADATA

Metadata is most often defined as data about data. Odds are you've come across metadata at some point. You may not have known that's what you were looking at. There are two flavors of metadata if you will: application and file system. Remember, the file system keeps track of our files and folders as well as some information about them. File system metadata include the date and time a file or folder was created, accessed, or modified. If you right-click on a file and choose "Properties," you can see these date/time stamps as shown in Figure 5.2.

Although this information can prove quite valuable to an investigation, we must keep in mind that all these date/time stamps may not be what they seem. One problem is that the system's clock can be changed by the user. Time zone differences can also cause some issues. Let's take a little closer look at the created, accessed, and modified date/time stamps.

**FIGURE 5.2**

Metadata information as seen after right-clicking on the file and choosing “Properties.” Note the created, modified, and accessed dates and times.

**Created**—The created date/time stamp frequently indicates when a file or folder was created on a particular piece of media, such as a hard drive (Casey, 2009). How the file got there makes a difference. By and large, a file can be saved, copied, cut and pasted, or dragged and dropped.

**Modified**—The modified date and time are set when a file is altered in any way and then saved (Casey, 2009).

**Accessed**—This date/time stamp is updated whenever a file is accessed by the file system. Accessed does not mean the same thing as opened. You may be asking

how a file can be accessed without being opened, and that's a good question. You see, the computer itself can interact with the files. Antivirus scans and other preset events are just two examples of this automated interaction.

### ALERT!

#### Date and Time Stamps

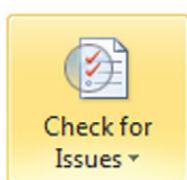
System date and time stamps should NOT be taken simply at face value. These settings are readily accessible and can be easily changed. Determining an accurate timeline can be further complicated if the case involves more than one time zone. Just because the metadata say a file was created at a certain date and time doesn't necessarily make it so.

Applications themselves can create and store metadata as well. Like the file system, they can track the created, accessed, and modified dates and times. But it doesn't stop there. They can also track a variety of application-specific attributes as well. Examples could include the name of the author, the name of the company or organization, and the computer name, just to name a few (Casey, 2009).

### Removing Metadata

Although metadata used to be one of our best-kept secrets, it's not any more. The criminals aren't the only ones taking notice. Corporations, law firms, and private citizens are just some of the folks concerned about metadata and the information contained therein. These legitimate concerns are being addressed by actually removing the metadata prior to sharing those files with other folks. Many tools exist for just that purpose. For example, law firms routinely scrub the metadata from all of their outbound documents, like those transmitted via e-mail. For the privacy-minded individual, the newer versions of Microsoft Word have the ability to detect and remove metadata. (See Figures 5.3 and 5.4.)

Recovered metadata can be used to refute claims by a suspect that they had no knowledge of a file's existence. It's tough to claim you didn't know it was there



#### Prepare for Sharing

Before sharing this file, be aware that it contains:

- Document properties, author's name and related dates
- Footers
- Custom XML data
- Content that people with disabilities are unable to read

**FIGURE 5.3**

Menu item to choose scrubbing inside of Microsoft Word 2010.

- 
- Document Properties and Personal Information**  
Inspects for hidden metadata or personal information saved with the document.
- 

**FIGURE 5.4**

The option to scan for metadata in Microsoft Word 2010.

when you not only opened the file but you changed or deleted the file as well. These dates and times can also be used to construct timelines in a case.

#### *FROM THE CASE FILES: METADATA*

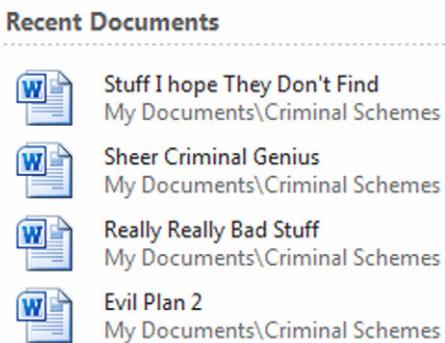
Metadata can help investigators identify all the suspects in a case and recover more evidence. Take this case from Houston, Texas regarding the production of counterfeit credit cards. The suspects in this case used “skimmed” card information in their card production process. Credit card “skimming” is when thieves grab the data from the magnetic strip on the back of credit and debit cards. This often occurs during a legitimate transaction, such as when you use your card to pay for dinner.

After identifying their prime suspect, police arrested him and searched his computer. In the end, the search of the computer was disappointing. The search only found one Microsoft Word document that contained “skimmed” information. Furthermore, the search of the residence found no skimmer hardware and there was no skimming software located on the computer. Not exactly the treasure trove they had hoped to find.

The exam didn’t stop there. Further examination of the Word document hit pay dirt. A review of the metadata revealed the author of the document, a female. Further investigation found that she was the suspect’s girlfriend and that she worked as a waitress in a neighboring town. This information gave investigators the probable cause needed to obtain a second search warrant for her apartment. During the second search, the skimmer (the piece of hardware used to extract the data from the magnetic strip) was recovered. The examination of the computer found not only the skimming software, but additional lists of debit cards and related information. Fortunately, this information was seized before it could be used. Both suspects were eventually found guilty.

## **THUMBNAIL CACHE**

To make it easier to browse the pictures on your computer, Windows creates smaller versions of your photos called **thumbnails**. Thumbnails are just miniaturized versions of their larger counterparts. These miniatures are created automatically by Windows when the user chooses “Thumbnail” view when using Windows Explorer. Windows creates a couple of different kinds of thumbnail files, depending on the version being used. Windows XP creates a file called thumbs.db. Microsoft Vista and Windows 7 create a similar file called thumbcache.db.

**FIGURE 5.5**

An Example of an MRU in Microsoft Word 2010.

Most users are completely unaware that these files even exist. The cool thing about these files is that they remain even after the original images have been deleted. Even if we don't recover the original image, thumbnails can serve as the next best evidence. Their mere existence tells us that those pictures existed at one point on the system.

## MOST RECENTLY USED (MRU)

Windows tries to make our lives, at least on our computers, as pleasant as possible. They may not always succeed, but their hearts are in the right place. The **Most Recently Used (MRU)** list is one such example of Microsoft thinking of us. The MRU are links that serve as shortcuts to applications or files that have recently been used. You can see these in action by clicking on the Windows Start button through the file menu on many applications. (See [Figure 5.5](#).)

## RESTORE POINTS AND SHADOW COPY

Do you ever wish you could go back in time? We're not there yet, but lucky for us, Windows is. There may come a time when it's just easier (or necessary) for our computers to revert back to an earlier point in time when everything was working just fine. In Windows, these are called **restore points (RP)**, and they serve as time travel machines for our computers.

### Restore Points

Restore points are snapshots of key system settings and configuration at a specific moment in time (Microsoft Corporation). These snapshots can be used to return the system to working order. Restore points are created in different ways. They can be created by the system automatically before major system events, like installing software. They can be scheduled at regular intervals, such as weekly.

Finally, they can be created manually by a user. The restore point feature is on by default, and one snapshot is automatically produced every day.

Before you start looking around for your restore points, you should know that Microsoft has taken steps to keep them from your prying eyes. They are normally hidden from the user.

These RPs have metadata (data about the data) associated with them. This information could be valuable in determining the point in time when this snapshot was taken. If the RP contains evidence, this can tell us exactly when that data existed on the system in question.

Digging through the restore points may reveal evidentiary gems that don't exist anywhere else. For the average person trying to conceal information from investigators, restore points are likely not the first place they would start destroying evidence. Obviously, that works in our favor.

#### *FROM THE CASE FILES: INTERNET HISTORY & RESTORE POINTS*

A defendant accused of possessing child pornography claimed that he had visited the site in question on only one occasion, and that was only by accident. To refute this claim, examiners turned to the restore points for the previous two months. Examination of each of the registry files found in the various restore points told a significantly different story. The evidence showed that not only had multiple child pornography sites been visited, but the URLs had been typed directly into the address bar of the browser, destroying his claim that the site was visited by accident. Confronted with this new evidence, the defendant quickly accepted a plea deal.

### **Shadow Copies**

Shadow copies provide the source data for restore points. Like the restore point, shadow files are another artifact that could very well be worth a look. We can use them to demonstrate how a particular file has been changed over time. They can likewise hold copies of files that have been deleted ([Larson, 2010](#)).

#### *FROM THE CASE FILES: RESTORE POINTS, SHADOW COPIES, AND ANTI-FORENSICS*

Officers from the Texas OAG (Office of the Attorney General) Cyber Unit, responding to a tip, served a search warrant at the suspect's residence. The OAG Cyber Unit obtained the search warrant after they were alerted that the suspect was uploading child pornography to the Internet. When the officers served the search warrant, they found the house unoccupied. Officers called the suspect letting him know they were in his home and that he should come home immediately and meet with them. When the suspect arrived, officers interviewed the suspect and searched his vehicle. Inside the car was a laptop computer.

All items seized were taken to the OAG offices for forensic examination. During the exam of the suspect's laptop, an alarming discovery was made. It appeared

the suspect, on the drive home to meet the officers, used a wiping tool to get rid of not only incriminating images but the Internet history from his laptop. While the initial exam found no child pornography on the laptop, other compelling evidence was recovered.

For example, the examiner was able to recover logs from the wiping program itself showing that it had indeed been run. That wasn't all. Since the operating system was Windows Vista, the examiner decided to check the shadow copies found on the machine. Remember, these Shadow Copies (or System Restore Points) are essentially snap shots of data at a given point in time.

Next, the forensic image (clone) of the suspect's laptop was loaded into a virtual environment. This enabled the examiner to see the computer system as the suspect saw it. The examiner exported out the restore points from the suspect's laptop, then imported those same files into his forensic tool. This process allowed the examiner to use his tools to extract images and other information from the suspect's system restore points. This procedure hit pay dirt. More than 3000 images of child pornography were recovered. In addition, log files were found showing searches and downloads of those same files. When it was all said and done, the suspect plead guilty and is currently serving 10 years in a Texas state prison.

## PREFETCH

Speed kills. Or in the case of computers, it's that *lack* of speed that kills. Developers at Microsoft know this and work hard to squeeze every millisecond out of the system. Prefetching is one of the ways they try to speed up the system.

Prefetch files can show that an application was indeed installed and run on the system at one time. Take, for example, a wiping application such as "Evidence Eliminator." Programs like this are designed to completely destroy selected data on a hard drive. Although we may not be able to recover the original evidence, the mere presence of "Evidence Eliminator" can prove to be almost as damning as the original files themselves. Stay tuned for more discussion on "Evidence Eliminator."

## LINK FILES

We all love shortcuts. They help us avoid road construction and steer clear of traffic jams. They save us time and make our travels easier, at least in theory. Microsoft Windows also like shortcuts. It likes them a lot.

Link files are simply shortcuts. They point to other files. Link files can be created by us, or more often by the computer. You may have created a shortcut on your desktop to your favorite program or folder. The computer itself creates them in several different places. You've likely seen and used these link files before. Take Microsoft Word, for example. If you look under the File menu, you'll see an option called "recent." The items in that list are link files, or shortcuts, created by the computer.

Link files have their own date and time stamps showing when they were created and last used. The existence of a link file can be important. It can be used to show that someone actually opened the file in question. It can also be used to refute the assertion that a file or folder never existed. Link files can also contain the full file path, even if the storage device is no longer connected, like a thumb drive.

## Installed Programs

Software that is or has been installed on the questioned computer could also be of interest. This is especially true if the same application has now been removed after some relevant point in time (i.e., when the suspect became aware of a potential investigation). There are multiple locations on the drive to look for these artifacts. The program folder is a great place to start. Link and prefetch files are two other locations that could also bear fruit.

## SUMMARY

The computer records a tremendous amount of information unbeknownst to the vast majority of users. These artifacts come in a variety of forms and can be found throughout the system. For example, it's possible to identify external storage devices, like thumb drives, that have been attached to the system. Items moved to the Windows Recycle Bin can tell us when they were deleted and by which account.

Even if a file has been deleted or overwritten, copies of the file could still exist on the drive in multiple forms. These often-overlooked copies are generated by print jobs and hibernation functions as well as restore points. These files can also be found in the swap space, a specific portion of a hard drive that is used when the system is out of RAM.

One major takeaway from this chapter is that valuable evidence of specific files, actions, or events can be recorded in multiple locations. As such, truly getting rid of it can be a highly technical process beyond the reach of most crooks.

Even deleting data and defragging your hard drive don't get rid of it. The computer stores data in a way that permits fragments of older files to be carved out for further analysis. The partial files removed from the slack space could contain just enough information to become a useful piece of evidence. Attribution is a major challenge in digital forensics. Saying with absolute certainty that a specific individual was responsible for a given artifact is often impossible. Identifying the account is often the best that can be done.

The system and the applications we use generate data about data. This information, known as metadata, can tell us when the file was created, accessed, modified, and deleted. Knowing what software has been installed and run could be relevant to an investigation. Drive wiping software, for example, could be of particular interest. The Windows Registry and the prefetching function are two sources of this potentially relevant information.

## References

- Bard, J. (n.d.). *The Windows Registry*. Retrieved May 2, 2011, from: <http://technet.microsoft.com/en-us/library/cc751049.aspx>
- Brodkin, J. (n.d.). *Windows on Verge of Dropping Below 90% Market Share*. Retrieved May 2, 2011, from: <http://www.networkworld.com/news/2011/011311-windows-on-verge-of-dropping.html>
- Casey, E. (2009). *Handbook of Digital Forensics and Investigation*. Burlington, MA: Academic Press.
- Gupta, M. R., Hoeschele, M. D., & Rogers, M. K. (2006). Hidden Disk Areas: HPA and DCO. *International Journal of Digital Evidence*, 1–8.
- Larson, T. (2010, July 8). *Windows 7: Current Events in the World of Windows Forensics*. Retrieved May 3, 2011, from: <http://computer-forensics.sans.org/summit-archives/2010/files/12-larson-windows7-forensics.pdf>
- Microsoft Corporation. (n.d.). *How the Recycle Bin Stores Files*. Retrieved May 2, 2011, from: <http://support.microsoft.com/kb/136517>
- Microsoft Corporation. (n.d.). *Sleep and Hibernation: Frequently Asked Questions*. Retrieved May 2, 2011, from: <http://windows.microsoft.com/en-US/windows7/Sleep-and-hibernation-frequently-asked-questions>
- Microsoft Corporation. (n.d.). *System Restore: Frequently Asked Questions*. Retrieved May 2, 2011, from: <http://windows.microsoft.com/en-US/windows-vista/System-Restore-frequently-asked-questions>
- Microsoft Corporation. (n.d.). *User Accounts Overview: Microsoft Corporation*. Retrieved May 2, 2011, from: [http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/usercpl\\_overview.mspx?mfr=true](http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/usercpl_overview.mspx?mfr=true)
- Phillip, A., Cowen, D., & Davis, C. (2009). *Hacking Exposed Computer Forensics: Computer Forensics Secrets & Solutions*. New York: McGraw-Hill.
- TechTarget. (n.d.). *Spool: Whatis.com*. Retrieved May 2, 2011, from: [http://whatis.techtarget.com/definition/0,,sid9\\_gci214229,00.html](http://whatis.techtarget.com/definition/0,,sid9_gci214229,00.html)

# CHAPTER 6

# Antiforensics

81

## Information in This Chapter:

- Introduction of Encryption Technology and the Threat It Poses
- Attacks Used to Break Encryption
- Techniques Used to Hide and Destroy Data

## INTRODUCTION

Computer examinations and the resulting evidence make regular appearances in police blotters all across the country. To counter these relatively new forensic advances, antiforensic tools and techniques are cropping up in significant numbers. They are being used by criminals, terrorists, and corporate executives alike. In February 2011, Valerie Caproni, the General Counsel for the FBI, addressed the House Subcommittee on Crime, Terrorism, and Homeland Security. Regarding encryption and the threat it represents, she told the subcommittee, “As the gap between authority and capability widens, the government is increasingly unable to collect valuable evidence in cases ranging from child exploitation and pornography to organized crime and drug trafficking to terrorism and espionage—evidence that a court has authorized the government to collect. This gap poses a growing threat to public safety” ([Caproni, 2011](#)).

There are many definitions for the term *antiforensics*. John Barbara defines it this way “an approach to manipulate, erase, or obfuscate digital data or to make its examination difficult, time consuming, or virtually impossible” ([Barbara, 2008](#)).

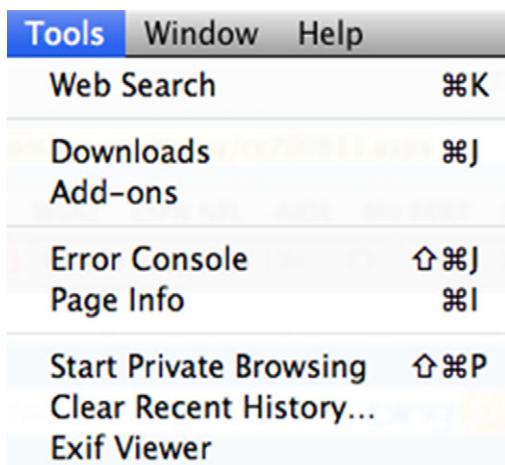
There’s even a web site devoted to the subject, and they’re not the least bit subtle about their objectives. [Anti-Forensics.com](#) is a “community dedicated to the research and sharing of methods, tools, and information that can be used to frustrate computer forensic investigations and forensic examiners.” It goes on to describe the web site’s purpose, saying, “A major goal of some anti-forensics

software, and the focus of [Anti-Forensics.com](#), is to make the analysis and examination of digital evidence as difficult, confusing, and time consuming as possible” ([What Is Anti-Forensics.com?](#)).

The use of antiforensics techniques is not limited to terrorists and pedophiles. Corporate executives have put them to use as well, using these tools and techniques to hide or destroy incriminating e-mails, financial records, and so on. Even everyday applications such as web browsers have features that could be used to obstruct a forensic examination—clearing the Internet history, for example. Most newer browsers come with a “private browsing” mode that doesn’t record things such as web sites visited and searches. In the latest version of Firefox, running in private mode will no longer save visited pages, form and search bar entries, passwords, download list entries, cookies, and web cache files ([Mozilla Foundation, 2011](#)). See [Figure 6.1](#).

In this chapter we’re going to take a look at several techniques used to hide or destroy digital evidence. As you’ll see, some of these techniques are highly effective when used properly. Other techniques have little or no impact on a forensic examination. Even using one of the commercially available drive wiping tools is no guarantee that the data will truly disappear.

From an investigative perspective, it’s important to know that there are legitimate uses of these antiforensic tools and techniques. Proving the intent, therefore, is critical. Suspects could assert that the wiping application was used only to protect their privacy or they used the defragmentation utility to improve performance. That’s possible. However, that defense gets a little tougher to swallow if the tool was only used once and that was three hours after the target became aware of the investigation.



**FIGURE 6.1**

The “Start Private Browsing” menu option in Firefox 6.0. Also note the option to “Clear Recent History.”

## HIDING DATA

Hiding techniques range from the simple to the very complex. Changing file names and extensions, burying files deep within seemingly unrelated directories, hiding files within files, and **encryption** are some of the most common hiding techniques. It's the last two techniques that can cause digital forensics practitioners to lose sleep at night.

### Encryption

We all have secrets. Companies, governments, and individuals share this universal truth. The Colonel's recipe for fried chicken, our bank account numbers, and the Army's plans for war are just a few examples of information that needs to be kept from under wraps. Before our world became such a wired one, keeping this material safe was, in many respects, a lot less complicated.

The legitimate use of encryption has enabled us to enjoy many of the Internet services that we now take for granted. For example, encryption used in e-commerce permits us to buy our favorite books and book our summer vacation. It keeps our businesses running and our country safe. These modern conveniences, however, are not without a cost. Encryption is a double-edged sword with serious consequences when used by criminals, terrorists, unfriendly nations, and crooked CEOs alike.

Today, we have less direct control over these secrets as they travel over the Internet or fly through the air on a wireless network. It is encryption that provides us with both the mechanism and confidence to store and transmit our most sensitive digital information. In this book, however, the focus is on the darker side of this technology and the threat that it poses. Its value is certainly not lost on many people with bad intentions. Take terrorists, for example; despite their seemingly low-tech lifestyle, they are embracing technology including encryption.

"To a greater and greater degree, terrorist groups, including Hezbollah, Hamas, and bin Laden's al Qaida group, are using computerized files, e-mail, and encryption to support their operations," wrote then-CIA Director George Tenet last March to the Senate Foreign Relations Committee. Ramzi Yousef, the architect of the 1993 World Trade Center bombing, is one of those terrorists putting encryption to use. Yousef saved detailed plans to destroy U.S. airliners encrypted on his laptop ([Dick, 2001](#)). If done properly, encryption can keep examiners at bay until hell freezes over, literally.

### What Is Encryption?

Encryption is the conversion of data into a form, called **cipher text**, which cannot be easily understood by unauthorized people ([Bauchie, Hazen, Lund, Oakley, & Rundatz, 2000](#)). Encryption starts with plain text. **Plain text** is the original,

unencrypted message. The plain text message is in the clear and can be read by anyone. A cryptographic algorithm is then applied to the plain text, producing cipher text. Cipher text is basically a scrambled version of plain text that is unintelligible. The algorithm is the method used to encrypt the message. The key is data used to encrypt and decrypt the information. A password or passphrase is commonly used as the key.

### Early Encryption

Encryption itself isn't a by-product of computer technology alone. It's been around for thousands of years in one form or another. One of the earliest and best-known encryption schemes is the Caesar Cipher. The Caesar Cipher is a shift cipher and encrypts the data by replacing the original letters with those "x" number of characters ahead in the alphabet. For example, using the Caesar Cipher and a key of five, an "A" would become an "F." [Table 6.1](#) shows the entire alphabet both as plain text and as cipher text after the same cipher has been applied. Note that each letter has been shifted five spaces below its original position.

Now let's encrypt "forensics" using the Caesar Cipher with a key of eight. [Table 6.2](#) shows us the conversion of plain text to cipher text.

This simple process is still employed today. It's frequently used to obfuscate computer code. At first glance, it appears that the terms encryption and obfuscate are interchangeable. They are similar enough to sometimes be confused, but the differences are significant enough to merit clarification. Obfuscation and encryption are both intended to make things harder to understand. Obfuscation, however, is used to protect computer code, rather than the data itself ([Tyma, 2003](#)). Obfuscation also protects code from reverse engineering. Encryption can't be used in this way because it would render the code totally unreadable to the computer.

ROT13 is a modern version of the Caesar Cipher in use today for obfuscation. In ROT13, letters are shifted 13 positions. In this scheme, an "A" becomes an

**Table 6.1** The Alphabet with Simple Encryption (Caesar Cipher).  
The Key in This Example is Five

Plain text	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Cipher text	F G H I J K L M N O P Q R S T U V W X Y Z A B C D E

**Table 6.2** Shows a Letter by Letter Conversion Using the Caesar Cipher and a Key of Eight

Plain text	F	O	R	E	N	S	I	C	S
Cipher text	N	W	Z	M	V	A	Q	K	A

**Table 6.3** The Opening of Lincoln's Gettysburg Address Encrypted Using ROT13

Fourscore	and	seven	years	ago	our	fathers	brought	forth	on	this
Sbhefpber	naq	frira	lnef	ntb	bhe	snguref	oebhtug	sbegu	ba	guvf
<b>continent</b>	a	<b>new</b>	<b>nation</b>	<b>conceived</b>	in	<b>liberty</b>	and	<b>dedicated</b>		
pbagvarag	n	arj	angvba	pbaprvirq	va	yvoregl	naq	qrqvpngrq		
<b>to</b>	<b>the</b>	<b>proposition</b>		<b>that</b>	<b>all</b>	<b>men</b>	<b>are</b>	<b>created</b>	<b>equal</b>	
gb	gur	cebcbfvgvba		gung	nyy	zra	ner	perngrq	rdhny	

"N," and so on. Table 6.3 shows an excerpt from Lincoln's Gettysburg Address after ROT13 has been applied.

## Algorithms

For the mathematically challenged, like myself, just the word *algorithm* can cause some anxiety. The algorithms we use to send our credit card numbers across the Internet are exponentially more complex than the cipher Julius used in Rome. Although algorithms are complicated and well beyond the scope of this book, we can still get a handle on their basic use and functionality. Put simply, an algorithm is just a set of instructions used to accomplish a certain task. As an example, we can create an algorithm for sending an e-mail about an upcoming meeting.

1. Go to office.
2. Turn on computer
3. Open Microsoft Outlook
4. Click "New Email"
5. Fill in the "To" information
6. Type "Meeting" in the subject line
7. Type the body of the message
8. Press send

Fundamentally, there are two types of encryption algorithms: symmetrical and asymmetrical. **Symmetrical encryption** uses the same key to encrypt and decrypt the data. In contrast, **asymmetrical encryption** uses two separate and distinct keys.

There are many encryption algorithms in use today serving a variety of purposes. You may have already heard of some of them. AES, TripleDES, Blowfish, and RSA are just a few.

### ALGORITHMS: IT'S NO SECRET

It may come as a surprise, but the algorithms themselves are open and well published. Why in the world would they put this information out there? It sure seems counterintuitive. Believe it or not, the answer is security. Best practice in cryptography states that the security of algorithms should be "independent of their secrecy" (Schneier, 2002).

This fundamental cryptographic principle has been around for quite some time. In 1883 Auguste Kerckhoffs, a Dutch linguist and cryptographer, said that in any truly effective crypto system, the key should be the only secret. Any system that relies on the secrecy of the algorithm is less secure ([Schneier, 2002](#)).

"The #1 lesson I've learned from my work at AccessData is 'you cannot trust closed-source crypto.' You have no idea if it is secure or not," said Nephi Allred, a cryptanalyst with AccessData. "I've reverse-engineered a lot of applications in my time: some good, some bad. While there are some good closed-source apps and some bad open-source apps (actually very few), the best apps are invariably open-source and the worst are invariably closed-source. Personally, I would never trust my own data to a closed source application" said Allred.

## Key Space

**Key space** is a metric that is often discussed when talking about the strength of a particular encryption scheme. The key space or key length has a direct impact on our ability to break the encryption, particularly with a brute force attack. A brute force attack tries to break the password by attempting every possible key combination until the right one is found.

This is where this gets particularly troubling when you consider all the possible key permutations and how long it would take to "guess" the password. An encryption scheme with a 128-bit key would have roughly 340,282,366,920, 938,000,000,000,000,000,000,000 possible key combinations. How long would that take a computer to guess the password? Crunching some rough numbers will give us an idea. Using one computer, guessing 500,000 passwords per second would break that key in about 21,580,566,141,612,000,000, 000,000,000 years. Let's crank up the number of computers guessing passwords to 1000. That gets us to a much more "manageable" wait time of only 21,580, 566,141612,000,000,000,000 years. Remember these numbers represent rough estimates; the truth is that they can be much higher depending on the algorithm used. Complex encryption schemes such as Pretty Good Privacy (PGP) can radically drop the number of attempts per second to only a few hundred ([Schneier, 2007](#)).

## Some Common Types of Encryption

With privacy being such a major concern, encryption tools are now included with some versions of the newer operating systems including Windows 7 and Apple OS X. These tools are **BitLocker** and **FileVault**, respectively. These encryption schemes can be applied selectively, only encrypting certain files or folders. They can also be used to encrypt an entire drive. This is known as full or whole disk encryption.

Full disk encryption (FDE) has some noteworthy advantages. We know from previous chapters that operating systems in their course of normal operation will

leave artifacts scattered across the drive. Take swap space, for example. Even though we encrypt an entire folder containing our sensitive files, remnants (or the entire file) could be located in the swap space. Full disk encryption takes care of these data “leaks.” The term *full disk encryption* is a little misleading. It doesn’t really encrypt the entire disk. In order to run BitLocker, there must be two partitions (sections) on the hard drive: one, known as the “operating system volume,” and the other, which contains the files to boot the machine, system tools, and so on. The operating system volume contains everything else including the vast majority of the items of most interest to us ([Microsoft Corporation, 2009](#)).

As they say, there is no free lunch. FDE has some drawbacks as well. Performance will likely suffer as the data are being encrypted and decrypted. This encryption/decryption is done “on the fly,” meaning that it occurs just before the data are saved or loaded into RAM. Passwords and keys are another concern. Recovering your data is dependent on having the proper authentication. If you lose or forget your password, you will very likely never get your data back. Encryption cuts both ways.

### ENCRYPTING FILE SYSTEM (EFS)

**Encrypting File System (EFS)** is used to encrypt files and folders. EFS is simple to use, using nothing more than a check box in a file’s properties. It is “not fully supported on Windows 7 Starter, Windows 7 Home Basic, and Windows 7 Home Premium” ([Microsoft Corporation](#)). EFS uses the Windows username and password as part of the encryption algorithm. EFS is a feature of the New Technology File System (NTFS), not the Windows operating system ([Microsoft Corporation](#)).

### BITLOCKER

Unlike EFS, BitLocker can be used to encrypt an entire hard drive, whereas BitLocker To Go is used to encrypt removable media such as a USB drive ([Microsoft Corporation](#)). BitLocker isn’t available in all versions of Windows. Currently it’s only available on the Windows 7 Ultimate systems ([Microsoft Corporation](#)). BitLocker doesn’t usually function alone. It normally works in conjunction with a piece of hardware called a **Trusted Platform Module (TPM)**. The TPM is a microchip on the motherboard of a laptop or PC that is intended to deliver cryptographic functions ([Microsoft Corporation](#)). The TPM generates and encrypts keys that can only be decrypted by the TPM. If configured to work without the TPM, then the required keys are stored on a USB thumb drive.

BitLocker encryption is pretty stout, making decryption doubtful without the key.

Encountering a running BitLockered machine affords an examiner an excellent opportunity to recover data without having to defeat the BitLocker encryption. Files stored in a BitLocker protected area of the hard drive are decrypted when they are requested by the system ([Microsoft Corporation, 2009](#)). Any time you can avoid going toe to toe with encryption is a good thing.

When dealing with a running computer, recognizing the presence of BitLocker could make all the difference in a case. That running BitLockered machine may very well represent the only chance you would have to recover any evidence from that computer.

#### *APPLE FILEVAULT*

Apple's latest version of OS X, Lion, comes with FileVault 2. FileVault2 uses 128 bit, AES encryption. With FileVault 2 you can encrypt the content of your entire drive. Apple gives customers the chance to store their recovery key with them. Passwords stored with Apple could be retrievable with the proper legal search authority ([Apple, Inc., 2011](#)).

#### *TRUECRYPT*

TrueCrypt is a free, open source software that provides on-the-fly-encryption functionality. In on-the-fly encryption, the data are automatically encrypted and decrypted as they are saved and opened. All of this is done behind the scenes without any user involvement. TrueCrypt also is capable of providing full disk encryption. This includes file names, folder names, as well as the contents of every file. It also includes those files that can contain sensitive data that the system creates on its own. These files include things like log files, swap files, and registry entries. Decryption requires the correct password and or key file(s). TrueCrypt supports Windows, Mac, and Linux operating systems ([TrueCrypt Developers Association, 2011](#)). TrueCrypt can use multiple encryption algorithms including AES, Serpent, Twofish, or some combination of these three. The key space is 256 bits.

### **Breaking Passwords**

Breaking passwords, or cryptanalysis, can be daunting or practically impossible. In order to give us the best chance for success, we'll need to use any advantage we can get. There are multiple ways to break passwords; some are technical, some are not. Sometimes it's as simple as asking. Options include **brute force attacks**, **dictionary attacks**, and **resetting passwords**. They can all yield positive results. We'll dig into these attacks more in an upcoming section.

The good news is that it's not all gloom and doom. In most cases, we are still dealing with people, and they represent the weakest point in this entire process. Humans can be both lazy and careless, giving us the chance we need to crack the encryption. Far too many people use simple passwords that are easy to break. Some of the best include "password," "letmein," or the ever-popular "123." Birthdays, pet names, or the name of our favorite sports team are also used routinely. Memorizing long random passwords is not easy or convenient for the majority of us. Even if a strong password is used, oftentimes it is written down on a Post-It note and stuck to the monitor. Furthermore, encryption keys can be left unsecured and subject to compromise.

People, being creatures of habit, quite often reuse at least a portion of their passwords. We can exploit this behavior to our advantage. If we can get one password, many times we can get them all. "Sometimes if we can go in and find one of those passwords, or two or three, I can start to figure out that in every password, you use the No. 3," said Stuart Van Buren, a U.S. Secret Service agent ([Homeland Security Newswire, 2011](#)).

What exactly qualifies as a strong password? According to Microsoft, a strong password uses a variety of letters, numbers, punctuation, and symbols, and has a minimum length of fourteen characters (Microsoft Corporation).

Examiners may get lucky and find the password in the swap space on the hard drive. Capturing the RAM of a running machine can also help in breaking passwords. You've probably entered a password on a web site at one time or another. As you entered your password, dots appeared, concealing the text as you type. What you may not realize is that the actual password is recorded in RAM. Failing to grab the RAM from a running machine could truly be a missed opportunity.

When the need arises, we have special tools available to us that can break passwords through a variety of attacks. These tools can break some simple passwords in less than a second. One of the leading tools of this type is the Password Recovery Toolkit (PRTK) from AccessData, the Utah-based computer forensic software company. Other tools include John the Ripper and Cain and Abel.

## PASSWORD ATTACKS

Passwords can be attacked and broken in multiple ways, but avoiding encryption is always preferable to having to attack passwords. There are tools and techniques we can use to increase our chances of success. One thing working in our favor is the vulnerability that humans bring to the table. Long random strings of letters, numbers, and characters make for excellent passwords. Unfortunately, they are also tough for people to remember. As such, most passwords are based on actual words, recognizable patterns, or both.

### Brute Force Attacks

A brute force attack is just what it sounds like. We are using as much computing power as we can muster to guess the correct password. The more computers (or, more precisely, central processing units) we can throw at it, the faster we can break it. As you'll see, "faster" is a relative term when it comes to breaking passwords. Products are available now that harness otherwise idle computers and use them against the encrypted file, folder, or drive. This is known as a distributed attack since the computational burden is spread among multiple computers. Some agencies are getting quite creative in breaking encryption.

The digital forensic folks with the U.S. Immigration and Customs Enforcement Cybercrime Center are using networked Sony PS3 gaming consoles to attack passwords. This approach leverages the power of these devices as well as their

cost-effectiveness. “Bad guys are encrypting their stuff now, so we need a methodology of hacking on that to try to break passwords,” said Claude E. Davenport, an agent in the U.S. Immigration and Customs Enforcement Cyber Crimes Center. “The Playstation 3—its processing component—is perfect for large-scale library attacks” ([Wawro, 2009](#)).

## Password Reset

Sometimes we will go after the software rather than the password. Some applications have vulnerabilities that can be exploited to simply reset the password, giving us the access we need. Unfortunately, the password reset isn’t widely effective, working only on a relatively small number of applications. In instances where it becomes necessary to bypass Windows system passwords, bootable CDs can get the job done. They do this by overwriting data in the Security Account Manager, or SAM for short. Elcomsoft’s System Recovery tool is one of many products that fill this need (Elcomsoft Co. Ltd.).

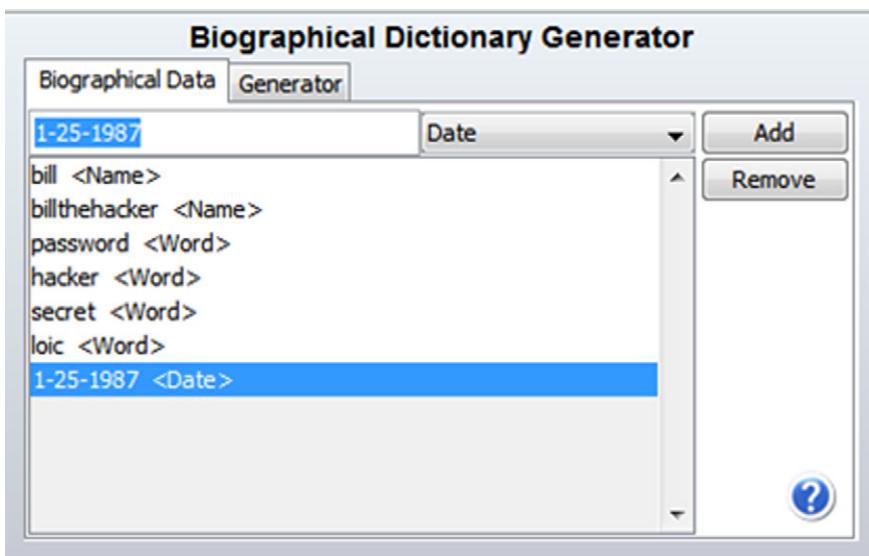
## Dictionary Attack

A dictionary attack is more precise, using words and phrases that can be collected from multiple sources. For example, a forensic application can create an index of all the words found on a suspect’s hard drive. These words would come from both the allocated and unallocated space. Other dictionary sources could be terms commonly used in certain criminal circles such as child pornography or narcotics trafficking. Dictionaries can also contain words from specific sources such as web sites.

Intelligence, the background information on our suspect or target, can really increase our chances of success. This information can be used to build a dictionary of potential passwords. Gathering this information starts at the scene. We are not solely interested in the digital devices alone, but photos, books, etc. We want to know the name of our subject’s children and pets. We want to know their hobbies and interests. The terms and words associated with these interests could provide clues to the suspect’s password. For example, if the suspect is a huge Lord of the Rings (LOTR) fan, we can employ a tool that will index (record the content) of a web site devoted to LOTR. The tool will grab names and places such as Aragorn and Rivendell. These terms can then be used to create custom dictionaries that can help unlock the password.

Let’s look at creating a custom dictionary based on biographical information on our suspect, Bill Thehacker. We’ll be using AccessData’s Password Recovery Toolkit. We enter a total of seven bits of information including names, birth date, and some keywords related to Bill. (See [Figure 6.2](#).)

From the seven words in [Figure 6.2](#), the tool then generates over twenty-six hundred permutations, a sampling of which is shown in [Table 6.4](#). Note the combinations of terms with a multitude of prefixes and suffixes.



**FIGURE 6.2**  
Biographical Dictionary Generator in PRTK.

**Table 6.4** A Sampling of the Over Twenty-six Hundred Keywords Generated from Our Original List of Seven

1	b25billthehacker	251987secret
25	billthehacker251b	251987 secret
1987	billthehacker125b	secret1987h
1251987	b251billthehacker	h1987secret
billbill	b125billthehacker	secret198725h
bill bill	25billthehacker1b	secret251987h
bill-bill	25b1billthehacker	h198725secret
bill_bill	1billthehacker25b	h251987secret
billb	1b25billthehacker	1987secret25h
bill b	billthehacker1b25	1987h25secret
bill-b	b1billthehacker25	25secret1987h
bill_b	billthehacker25b1	25h1987secret
billbillthehacker	b25billthehacker1	secret25h1987
bill billthehacker	billthehacker25bill	h25secret1987
bill-billthehacker	bill25billthehacker	secret1987h25
bill_billthehacker	billthehacker251bill	h1987secret25
billb	billthehacker125bill	secret1987
bill b	bill251billthehacker	secret 1987
bill-b	bill125billthehacker	1987secret
bill_b	25billthehacker1bill	1987 secret
	25bill1billthehacker	

The screenshot shows the AccessData Dictionary Import Utility interface. The title bar reads "AccessData Dictionary Import Utility". Below it is a menu bar with "Dictionary", "Tools", and "Help". The main window is titled "Dictionary Browser" and shows a list of files under the heading "Desktop". The table has four columns: "Name", "Type", "Word Count", and "Modification Date". The entries are:

Name	Type	Word Count	Modification Date
AntiFoernsic 2	???	-	Aug 28, 2011 0:40 PM
AntiForensics	???	-	Aug 26, 2011 0:29 PM
Book Dictionary.xml	GD/A...	-	Aug 29, 2011 2:46 PM
Book Registry	???	-	Aug 28, 2011 10:47 AM
New folder	???	-	Aug 16, 2011 7:52 PM
UserAssist	???	-	Aug 26, 2011 1:18 PM
Yahoo! Group	???	-	Aug 16, 2011 7:51 PM
Yahoo! Unencrypted -- JJS	???	-	Aug 16, 2011 7:52 PM
[en] Book Dictionary-en-c.adf	ADF	2676	Aug 29, 2011 2:46 PM
[en] Book Dictionary-en-u.adf	ADF	2676	Aug 29, 2011 2:46 PM

**FIGURE 6.3**

The final word count generated by our seven original entries.

### ADDITIONAL RESOURCES

#### Encryption

Bruce Schneier is a well-respected author and cryptographer who regularly publishes on encryption and security-related issues. He is the author of several books as well as the Blowfish Encryption Algorithm. His book *Secrets & Lies: Digital Security in a Networked World* is both fascinating and highly readable. He also publishes a blog and the Crypto-Gram Newsletter. A visit to his web site, <http://www.schneier.com/>, is highly recommended.

## STEGANOGRAPHY

Steganography, or stego for short, is another and very effective way to conceal data. The word steganography comes from the Greek words “Stegos” meaning covered and “Graphie” meaning writing. Its exact roots equate to covered writing. [SearchSecurity.com](#) defines steganography as “the hiding of a secret message within an ordinary message and the extraction of it at its destination” ([TechTarget, 2000](#)).

There are two files composing the finished stego file. The file that contains the secret message is called the **carrier file**. Carrier files can be image files, video files, audio files, and word processing documents, just to name a few. The embedded secret document is called the **payload**. The underlying concept behind steganography is fairly straightforward. Let’s start with the carrier files.

These file types are used because they have a significant amount of redundant data, also known as “noise.” The redundant data are replaced with the data composing the hidden message. Payload files don’t necessarily have to be text based. An image file can be inserted into another image file. There are multiple variants or combinations that are possible.

Steganography applications are widely available on the Internet, and many are free. Backbone Security, a company that makes one of the more popular steg detection tools, has cataloged more than 960 separate steganography applications available for download on the internet ([Backbone Security.com, 2011](#)).

What makes stego such a concern? First, it’s very difficult to detect. Second, once discovered it’s very tough, if not impossible, to extract the payload without knowing the steg application and password used to create it.

Before his demise at the hands of Seal Team Six, Osama Bin Laden and his colleagues made extensive use of steganography to communicate. Stego files were posted in sports chat rooms and pornographic bulletin boards ([Kelley, 2005](#)).

Detecting the use of steganography is pretty tough. One of the most popular tools is Stego Suite™ from the Steganography Analysis and Research Center (SARC). The current version identifies over five hundred known steganography applications and has the ability to crack and extract payloads from carrier files (Wetstone Technologies, Inc.).

In June 2010, The FBI arrested ten Russian spies who had been in the United States for roughly a decade. These spies made extensive use of steganography as they passed secret messages to the SVR, the Russian intelligence service ([CBS News, 2010](#)). A criminal complaint in the case, filed in the Southern District of New York, provided some insight into the use of steganography by the Russians. In the complaint, Special Agent Maria Ricci said in part:

“In addition, and among other things, a number of the Boston Conspirators’ Electronic Messages appear directly to concern communication by means of steganography. For example, one message, dated December 15, 2004, discussed the process of ‘decrypt[ing]’ messages embedded in images; another message, dated February 22, 2005, discussed ‘decypher [ing] [sic]’ data embedded in images. Similarly, on or about October 3, 2004, law enforcement agents, acting pursuant to a judicial order, intercepted aural communications taking place inside the Boston townhouse. Tracey Lee Ann Foley, the defendant, was heard saying to Donald Howard Heathfield, the defendant: ‘Can we attach two files containing messages or not? Let’s say four pictures ....’ Based on my training, experience, and participation in this investigation, I believe that this was a reference to conveying messages by means of steganography—placing ‘files containing messages’ in ‘pictures.’ On or about March 7, 2010, law-enforcement agents, acting pursuant to a judicial order, intercepted aural communications taking place inside the Boston townhouse. As a

final example, in or about March 2010, Foley and Heathfield were heard discussing Foley's use of steganography and the schedule of her communications with Moscow Center"

(*United States of America v. Christopher R. Metso, 2010*)

## DATA DESTRUCTION

Sometimes hiding data isn't enough, and perpetrators try to destroy the data instead. Actually destroying the data is a little more complicated than many people think. The uninitiated may simply hit the delete key, assuming that the data no longer exist. As we've seen, this approach is not effective because the "deleted" data remain on the media and are easily recovered. In contrast, many drive wiping tools can be very effective. Using utilities such as these can leave telltale signs of their use, providing substantial evidence even without the original data in question.

**Data destruction** can be accomplished or attempted in several ways. Some of them are better than others. **Drive wiping** software is commercially available and can be effective in destroying potential evidence. Much of its effectiveness rests with the quality of the software, how it is used, and the number of "wipes" that are made. Defragmenting or reformatting a drive is frequently attempted, but often delivers limited results.

### Drive Wiping

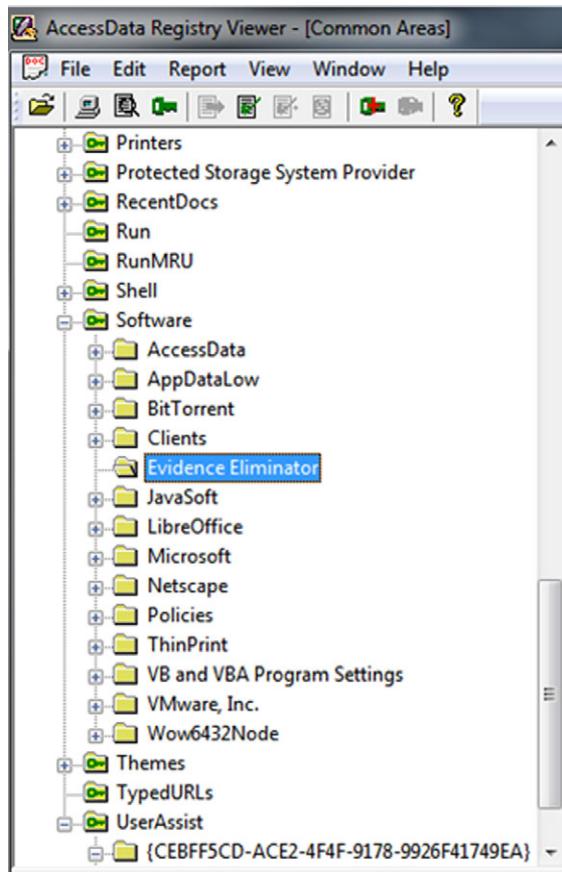
Drive wiping utilities are used to overwrite data on a hard drive in such a way as to make them unrecoverable. Most of these applications are promoted and/or intended to keep personal or corporate information private. Both are noble causes indeed. Unfortunately, these same utilities can be used for other, less honorable purposes. Examples of these tools include "Darik's Boot and Nuke," "DiskWipe," "CBL Data Shredder," "Webroot Window Washer," and "Evidence Eliminator."

Using these tools is not an "all or none" proposition. They can be somewhat surgical in their application, wiping only specified files while leaving others untouched. Operating system files, for example, could be left intact. They can target specific files and folders as well as potentially incriminating system values like those found in the Windows Registry.

These tools do have a legitimate use and are available at many technology stores such as Best Buy. Privacy is a major concern for everyone, and wiping utilities can help. If we want to donate our old computers we certainly don't want our e-mails and other personal information going with it to Goodwill.

Using these tools is no guarantee that the data can't be recovered. Success depends largely on the quality of the tool and the skills of the user.

From an evidentiary or investigative perspective, the presence or use of these applications can serve as the next best thing to the original evidence. Suspects may find it hard to explain why "Evidence Eliminator" software was installed

**FIGURE 6.4**

Note the presence of “Evidence Eliminator” in the Windows Registry software key.

and run on their computer the day before their computer was searched. Figure 6.4 shows the entry for “Evidence Eliminator” in the software key in the Windows Registry. This is an indicator that this software was installed on the machine.

Wiping utilities can leave telltale signs of their use. When looking at the drive at the bit level, a distinct repeating pattern of data may be seen. This is completely different from what would normally be found on a hard drive in everyday use. (See Figure 6.5.)

Evidence of their use can be found elsewhere on the drive. Figure 6.6 shows signs of Evidence Eliminator being opened on that machine.

Some operating systems, Apple OSX Lion for example, ship with a drive wiping utility installed. Called Secure Erase, this utility offers multiple options for data destruction. (See Figure 6.7.)

File Content	
	Hex Text Filtered Natural
09740	09 00 00 00 80 00 00 00-0D 00 00 00 00 00 00 00 00 00
09750	16 3F 04 9D 03 00 00 00 00-00 00 00 00 00 00 00 00 00
09760	00 00 00 00 EF BE AD DE-69 65 63 6F 6D 70 61 74
09770	3A 61 6E 6E 2D 6B 61 74-65 2E 6A 70 00 BE AD DE
09780	DF BE 00 00 E1 80 80 00-00 00 00 00 00 BE AD DE
09790	EF BE AD DE EF BE AD DE-EF BE AD DE EF BE AD DE
097a0	EF BE AD DE EF BE AD DE-EF BE AD DE EF BE AD DE
097b0	EF BE AD DE EF BE AD DE-EF BE AD DE EF BE AD DE
097c0	EF BE AD DE EF BE AD DE-EF BE AD DE EF BE AD DE
097d0	EF BE AD DE EF BE AD DE-EF BE AD DE EF BE AD DE
097e0	EF BE AD DE EF BE AD DE-EF BE AD DE EF BE AD DE
097f0	EF BE AD DE EF BE AD DE-EF BE AD DE EF BE AD DE
09800	55 52 4C 20 02 00 00 00-00 00 00 00 00 00 00 00 00 00
09810	0F C0 5E 4B 03 61 CC 01-00 00 00 00 00 00 00 00 00 00
09820	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00 00 00
09830	60 00 00 00 68 00 00 00-FE 00 10 10 00 00 00 00 00 00
09840	09 00 00 00 80 00 00 00-0D 00 00 00 00 00 00 00 00 00
09850	16 3F 04 9D 03 00 00 00-00 00 00 00 00 00 00 00 00 00
Sel start = 38796, len = 116; dus = 2797459; log sec = 22379675; phy sec = 22381723	

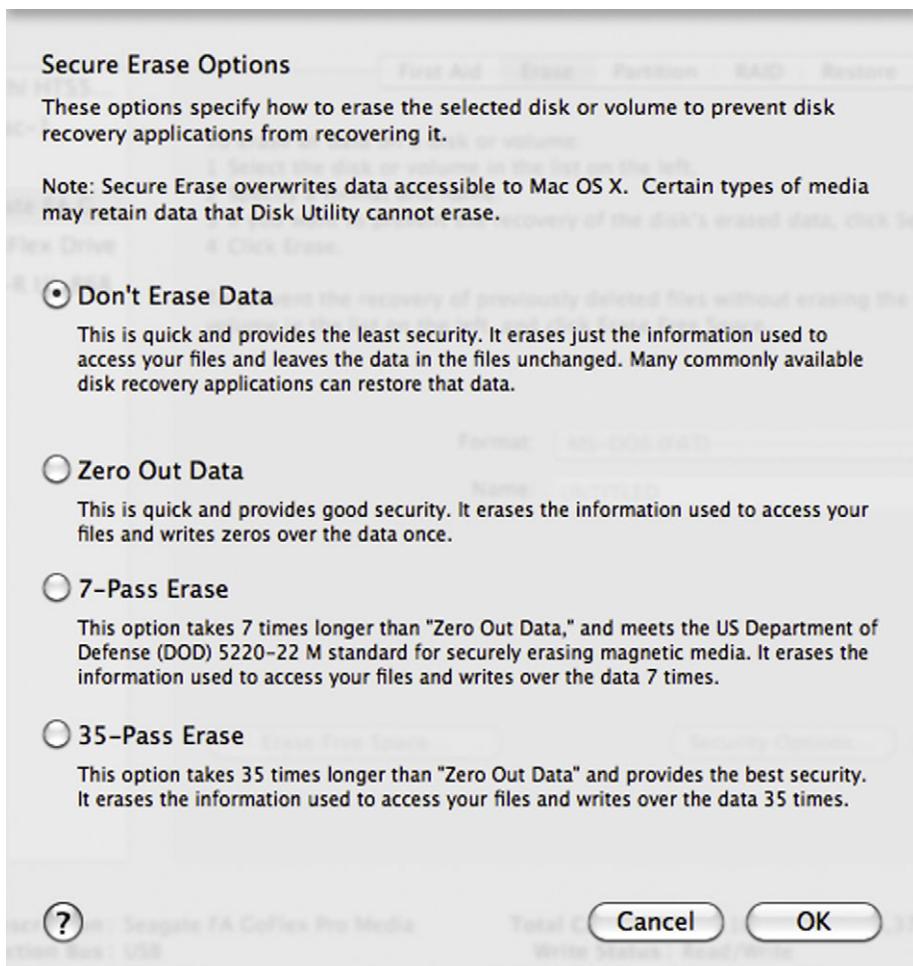
**FIGURE 6.5**

Note the distinct repeating pattern of hexadecimal numbers. This pattern is unusual and may be an indication that a wiping utility was used.

000	5B 00 5D 00 44 00 65 00-6D 00 6F 00 6E 00 6F 00	[.] -D-e-m-o-n-o-
010	69 00 64 00 2E 00 6D 00-65 00 5B 00 5D 00 2D 00	i-d..-m-e-[.]--
020	45 00 76 00 69 00 64 00-65 00 6E 00 63 00 65 00	E-v-i-d-e-n-c-e-
030	5F 00 45 00 6C 00 69 00-6D 00 69 00 6E 00 61 00	-E-l-i-m-i-n-a-
040	74 00 6F 00 72 00 5F 00-39 00 35 00 30 00 32 00	t-o-r-_-9-5-0-2-
050	37 00 35 00 38 00 2E 00-30 00 32 00 31 00 36 00	7-5-8..-0-2-1-6-
060	2E 00 74 00 6F 00 72 00-72 00 65 00 6E 00 74 00	.-t-o-r-r-e-n-t-
070	00 00 DA 00 32 00 00 00-00 00 00 00 00 00 00 00 00	..Ú-2-----
080	5B 5D 44 65 6D 6F 6E 6F-69 64 2E 6D 65 5B 5D 2D	[] Demonoid.me[]-
090	45 76 69 64 65 6E 63 65-5F 45 6C 69 6D 69 6E 61	Evidence_Elimina
0a0	74 6F 72 5F 39 35 30 32-37 35 38 2E 30 32 31 36	tor_9502758.0216
0b0	2E 6C 6E 6B 00 00 96 00-08 00 04 00 EF BE 00 00	.lnk-----i%..
0c0	00 00 00 00 00 00 2A 00-00 00 00 00 00 00 00 00 00 00	.....*.....

**FIGURE 6.6**

Shows signs in the MRU that the program Evidence Eliminator has been opened on this machine.

**FIGURE 6.7**

Secure Erase options from Apple OS X. Note the array of options, particularly the number of passes over the data.

## MORE ADVANCED

### Defragmentation as Antiforensic Technique

Defragmentation or “Defragging” as it’s commonly called is often done to improve computer performance. Defragging is the process of moving clusters as close together as possible in order to speed the system up. This procedure involves moving data from one location on the drive to another. As such, data can be overwritten in the process. These overwritten (destroyed) data may have had some evidentiary value.

(Continued)

(Continued)

The defragmentation process can occur in three ways; it can be user scheduled, manually initiated by the user, or done automatically by the operating system ([Casey, 2009](#)).

There are a few different ways you can attempt to determine whether a drive has been recently defragmented. One way is to boot the drive image in Windows and look at the amount of file fragmentation. Drives in regular use normally show a significant amount of file fragmentation. Drives that show otherwise, without a plausible explanation, would be suspect.

### **Q & A With Nephi Allred, Cryptanalyst with AccessData, the Maker of Password Recovery Toolkit (PRTK).**

By now it should be clear that encryption is a major concern to the digital forensics community. As such, we must be prepared to deal with encrypted data. Decryption tools are one weapon we can bring to the fight. One of the premier decryption tools on the market is Password Recovery Toolkit (PRTK) from AccessData. In the Q&A below, we get a closer look inside PRTK and the encryption it aims to break. PRTK is widely used worldwide by law enforcement, intelligence agencies, and private corporations such as large financial institutions. U.S. users include the FBI, CIA, and Secret Service, just to name a few.

**[Q]** About how many passwords per second does PRTK guess on a “standard” machine?

**[A]** Allred: We get this question a lot. It’s impossible to answer as it stands because the question itself has an implicit assumption, which is wrong. Namely: all password schemes are not the same. It’s a bit like asking how fast animals can go. Which animal? Every program or application or other system that uses passwords does it differently. The way they do it makes all the difference in the world in how much computation is required to test a password.

For example, a “typical” machine might guess two million passwords per second trying to crack an Office 97 file, while the same machine might only guess five hundred passwords per second cracking an Office 2010 file.

And of course the answer also depends on what you mean by a “typical” machine (and that changes as time goes on, too).

**[Q]** PRTK guesses passwords in a certain order to improve the speed and efficiency. Can you talk a little about how that works and why it’s important?

**[A]** Allred: Not all passwords are created equal. In the space of all possible passwords, some are more likely to be used by humans than others. (For example, “Br1tn3y” is much more likely to be used than “H\*i3)-aV.K=TyG7”). So if you are trying to guess passwords, you will be faster and more successful on average if you guess the more probable passwords first.

Of course which passwords are more probable is not always easy to determine, and certainly varies from person to person. PRTK defines a default ordering of passwords that we have tried to make as effective as possible, given what is known about how people tend to choose passwords. But an investigator often has specific knowledge about a suspect and can use that to make a password ordering more tailored to that individual. This is why PRTK gives its users a great deal of password space customization. For example, rather than going with the

default, you can specify that a job first try all the passwords in a (possibly customized) dictionary, then all of those words in reverse order, then all of those words with “123,” “4eva,” or “asdf” appended. And lots more.

- [Q] I know that PRTK also relies on identified patterns of passwords (roots and appendages). What are those based on and how does that work?
- [A] Allred: Based on various password lists that we've obtained over the years (some from clients of ours, others freely available), we've tried to make password “rules” that generate passwords that people actually use in real life. At this point, this is still more an art than a science. That is, there is no deep statistical analysis going on (yet)—mostly we eyeball the lists and look for patterns. For example, a lot of passwords seem to end with “1”. So one of our password rules is “Dictionary followed by common suffixes” (and “1” is one of those common suffixes).
- [Q] Do you know just how effective PRTK is in breaking passwords?
- [A] Allred: Again, this varies widely over the kinds of files and suspects. I don't have any numbers for you, unfortunately. You should probably talk to people who use PRTK (or DNA) on real cases.
- It's worth noting that not all attacks PRTK does are password guessing attacks. Some crypto systems have flaws that allow their passwords to be recovered instantly, with no “guessing” involved. For example, PRTK can instantly recover the master password on the “Whisper32” password manager. This was not uncommon in applications a decade ago, but these days it's becoming much more rare as software developers become more crypto savvy.
- [Q] Is there anything that slows down the decryption process? Can you talk about that and why that is?
- [A] Allred: Yes, there is. These days, most developers of password using applications are aware of tools like PRTK, and they will use measures to slow down password guessing attacks. As I explained in #1, the speed at which we can guess passwords all depends on how the application uses the password. An application could deliberately choose a very slow password-to-key methodology. It might hash the password ten thousand times, for example, instead of just one, while transforming the password into a key. (This is a simplification, but you get the idea). This forces the password-guessing tool to also hash the password ten thousand times per password guessed, which leads to many fewer passwords per second.
- [Q] How is encryption changing? What do you see is the next “big thing” in cryptography? What challenges do you see ahead?
- [A] Allred: Cryptography is a big subject, and I'm hardly an expert in any of the cutting edges of new research. But in the arena of password based encryption, things are changing.
- It's not exactly a new insight, but people are becoming more and more aware that passwords as a security device are often inadequate. What we'll use instead of them (or, more likely, in addition to them) is not yet entirely clear, but encryption providers are trying new things.
- For example, several applications, like TrueCrypt, allow users to enhance their password with “key files.” A key file can be any file, and it is used to scramble a password before use. This means that to run a successful password-guessing attack, PRTK needs to have any and all key files used. It may not be easy for the investigator to figure out what key files were used, if any.

## SUMMARY

Antiforensic tools and techniques can have a significant impact on a forensic examination of a computer. To frustrate examiners, subjects generally attempt to either hide the incriminating data in some fashion, or try to destroy it altogether. Encryption is one of the most common and potentially potent forms of data hiding. Powerful encryption is available free on the Internet and included with some versions of both Microsoft and Apple operating systems. These tools can make it practically impossible to recover the encrypted data.

Should encryption be encountered, it can be attacked in different ways. In a brute force attack, every possible password is tried until the right one is found. This is the slowest and least desirable of all the attacks. Increasing the processing power used in an attack can reduce the time needed to break the password. Some password-protected applications have vulnerabilities that can be exploited. These vulnerabilities can allow us to reset the password to one of our choosing.

Dictionaries can be created and used to break passwords. These can range from standard dictionaries to custom ones based on information specific to the target. Pet names, hobbies, interests, and birth dates are just some of the details that can compose a custom dictionary.

Messages or data can be hidden within other files. In a process known as steganography, files (called payloads) are inserted into other files such as pictures or movies (called carrier files). Steganography can be very difficult to detect. If it is detected, it can also prove tough to extract the message from the carrier file.

A subject may choose to destroy the data with a commercially available drive wiping tool. The effectiveness of these tools is far from foolproof. Incriminating data can still be recovered even after the tool has been used. Even if data have been successfully deleted, the software can leave behind telltale signs of their use. Proof of their use can be potent evidence as well.

## References

- AntiForensics Community. (n.d.). *About AntiForensics: AntiForensics*. Retrieved May 13, 2011, from: <http://www.antiforensics.com/>
- Apple, Inc. (2011, July 26). OS X Lion: *About FileVault 2*. Retrieved August 14, 2011, from: <http://support.apple.com/kb/HT4790>
- Backbone Security.com. (2011, April 26). *Backbone's Digital Steganography Database Exceeds 925 Applications*. Retrieved August 14, 2011, from: [http://www.sarc-wv.com/news/press\\_releases/2011/safdb\\_v39.aspx](http://www.sarc-wv.com/news/press_releases/2011/safdb_v39.aspx)
- Barbara, J. (2008, December 01). *Anti-Digital Forensics, The Next Challenge: Part 1*. Retrieved August 15, 2011, from: <http://www.forensicmag.com/article/anti-digital-forensics-next-challenge-part-1>
- Bauchie, R., Hazen, F., Lund, J., Oakley, G., & Rundatz, F. (2000, July). *Encryption*. Retrieved August 17, 2011, from: <http://searchsecurity.techtarget.com/definition/encryption>
- Berghel, H. (2011, February 17). Hiding Data, Forensics, and Anti-forensics. *Communications of the ACM*, 15–20.

- Caproni, V. (2011, February 17). *Going Dark: Lawful Electronic Surveillance in the Face of New Technologies*. Retrieved August 15, 2011, from: <http://www.fbi.gov/news/testimony/going-dark-lawful-electronic-surveillance-in-the-face-of-new-technologies>
- Casey, E. (2009). *Handbook of Digital Forensics and Investigation*. Burlington, MA: Academic Press.
- Casey, E. (2011). *Digital Evidence and Computer Crime, 3rd ed.: Forensic Science, Computers, and the Internet*. Waltham, MA: Academic Press.
- CBS News. (2010, June 29). *FBI: 10 Russian Spies Arrested in U.S.* Retrieved September 11, 2011, from: <http://www.cbsnews.com/stories/2010/06/28/world/main6627393.shtml>
- Dick, Ronald, L., (2001, April 5). *Issue of Intrusions into Government Computer Networks*, Retrieved August 14, 2011, from: <http://www.fbi.gov/news/testimony/issue-of-intrusions-into-government-computer-networks>
- Elcomsoft Co. Ltd. (n.d.). *System & Security Software*. Retrieved August 27, 2011, from: <http://www.elcomsoft.com/esr.html#forgot%20administrator%20password>
- Geiger, M. (2005). Evaluating Commercial Counter-Forensic Software. DFRWS. New Orleans.
- Gupta, M. R., Hoeschele, M. D., & Rogers, M. K. (2006). Hidden Disk Areas: HPA, and DCO. *International Journal of Digital Evidence*, 1–8.
- Homeland Security Newswire. (2011, March 18). *Feds Forced to Get Creative to Bypass Encryption*. Retrieved August 14, 2011, from: <http://www.homelandsecuritynewswire.com/feds-forced-get-creative-bypass-encryption>
- HowStuffWorks, Inc. (n.d.). *What Is a Computer Algorithm?* Retrieved August 17, 2011, from: <http://computer.howstuffworks.com/question717.htm>
- Kelley, J. (2005, February 5). *Terrorist Instructions Hidden Online*. Retrieved August 14, 2011, from: <http://www.usatoday.com/life/cyber/tech/2001-02-05-binladen-side.htm>
- Microsoft Corporation. (n.d.). *BitLocker Drive Encryption Overview*. Retrieved June 20, 2011, from: <http://windows.microsoft.com/en-US/windows-vista/BitLocker-Drive-Encryption-Overview>
- Microsoft Corporation. (n.d.). *Compare Windows*. Retrieved June 20, 2011, from: <http://windows.microsoft.com/en-US/windows7/products/compare>
- Microsoft Corporation. (n.d.). *Create Strong Passwords*. Retrieved August 13, 2011, from: <http://www.microsoft.com/security/online-privacy/passwords-create.aspx>
- Microsoft Corporation. (n.d.). *The Encrypting File System*. Retrieved September 11, 2011, from: <http://technet.microsoft.com/en-us/library/cc700811.aspx>
- Microsoft Corporation. (n.d.). *Unique Technology for Enterprise Customers*. Retrieved August 27, 2011, from: <http://www.microsoft.com/windows/enterprise/products/windows-7/features.aspx#bitlocker>
- Microsoft Corporation. (n.d.). *What Is Encrypting File System (EFS)?* Retrieved June 20, 2011, from: <http://windows.microsoft.com/en-US/windows7/What-is-Encrypting-File-System-EFS>
- Microsoft Corporation. (n.d.). *Windows BitLocker Drive Encryption Step-by-Step Guide: Microsoft Corporation*. Retrieved May 13, 2011, from: <http://technet.microsoft.com/en-us/library/cc766295%28WS.10%29.aspx>
- Microsoft Corporation. (2009, July 10). *Windows BitLocker Drive Encryption Frequently Asked Questions*. Retrieved August 18, 2011, from: [http://technet.microsoft.com/enus/library/cc766200%28WS.10%29.aspx#BKMK\\_EntireDisk](http://technet.microsoft.com/enus/library/cc766200%28WS.10%29.aspx#BKMK_EntireDisk) Microsoft.
- Mozilla Foundation. (n.d.). *Private Browsing*. Retrieved August 27, 2011, from: [http://support.mozilla.com/enUS/kb/Private%20Browsing#w\\_what-does-private-browsing-not-save](http://support.mozilla.com/enUS/kb/Private%20Browsing#w_what-does-private-browsing-not-save)
- Phillip, A., Cowen, D., & Davis, C. (2009). *Hacking Exposed Computer Forensics: Computer Forensics Secrets & Solutions*. New York: McGraw-Hill.
- Rogers, M. (2005). *Anti-Forensics*. Lockheed Martin. San Diego.
- Schneier, B. (2002, May 15). *Crypto-Gram Newsletter*. Retrieved June 20, 2011, from: <http://www.schneier.com/crypto-gram-0205.html#1>

- Schneier, B. (2007, January 15). *Secure Passwords Keep You Safer*. Retrieved August 25, 2011, from: <http://www.schneier.com/essay-148.html>
- Strickland, J. (n.d.). *How Stuff Works: How Computer Forensics Works*. Retrieved May 13, 2011, from: <http://computer.howstuffworks.com/computer-forensic3.htm>
- Symantec Corporation. (n.d.). *PGP Encryption Products*. Retrieved May 13, 2011, from: <http://www.symantec.com/business/theme.jsp?themeid=pgp>
- Symantec Corporation. (n.d.). *Whole Disk Encryption: Symantec Corporation*. Retrieved May 13, 2011, from: <http://www.symantec.com/business/whole-disk-encryption>
- TechTarget. (2000, December). *Steganography*. Retrieved August 15, 2011, from: <http://searchsecurity.techtarget.com/definition/steganography>
- TrueCrypt Developers Association. (2011, July 11). *System Encryption*. Retrieved August 14, 2011, from: <http://www.truecrypt.org/docs/?s=version-history>
- TrueCrypt Developers Association. (n.d.). *Documentation: TrueCrypt Developers Association*. Retrieved May 13, 2011, from: <http://www.truecrypt.org/docs/>
- Tyma, P. (2003, April 8). *Encryption, Hashing, and Obfuscation*. Retrieved June 20, 2011, from: <http://www.zdnet.com/news/encryption-hashing-and-obfuscation/128604>
- United States of America v. Christopher R. Metsos, et al.* (2010, June 1). Southern District, New York.
- Vijayan, J. (2008, February 4). *Updated Encryption Tool for al-Qaeda Backers Improves on First Version, Researcher Says*. Computerworld. Retrieved May 13, 2011, from: [http://www.computerworld.com/s/article/9060939/Updated\\_encryption\\_tool\\_for\\_al\\_Qaeda\\_backers\\_improves\\_on\\_first\\_version\\_researcher\\_says](http://www.computerworld.com/s/article/9060939/Updated_encryption_tool_for_al_Qaeda_backers_improves_on_first_version_researcher_says).
- Wawro, A. (2009, November 19). *US Government Using PS3s to Crack Encryption, Catch Paedophiles*. Retrieved August 17, 2011, from: <http://www.computerworlduk.com/news/security/17680/us-government-using-ps3s-to-crack-encryption-catch-paedophiles/>
- Wetstone Technologies, Inc. (n.d.). *Stego Suite™—Discover the Hidden*. Retrieved August 18, 2011, from: <http://www.wetstonetech.com/product/stego-suite/>
- What Is Anti-Forensics.com?* (n.d.). Retrieved August 14, 2011, from: <http://www.anti-forensics.com/about-anti-forensics>

# CHAPTER 7

# Legal

103

## Information in This Chapter:

- The Legal Aspects of Digital Forensics
- The Fourth Amendment and Its Impact on Digital Forensics
- Electronic Discovery
- Duty to Preserve Potential Digital Evidence in Civil Cases
- Private Searches and Establishing the Need for Off-Site Analysis
- Overview of The Electronic Communications Privacy Act
- Searching Digital Evidence With & Without a Search Warrant

## INTRODUCTION

No discussion on digital forensic fundamentals can be complete without including the legal aspects of the discipline. The legal community has been playing a perpetual game of catch-up with technology since the very beginning. With computer and other technologies becoming so intertwined in our work and private lives, it was inevitable that electronic data would find its way into the courts. It's not just the child pornographers and identity thieves; digital evidence plays a huge role in civil litigation as well.

With these newfangled technologies came new criminal behaviors that necessitated new statutes outlawing them. Some of these are simply old crimes with a new twist. In this instance, the technology just facilitated the crime in an up-to-date, more efficient way.

Search authority is the very first step in the digital forensic process. The authority itself can take many forms, depending on which venue you're working in at the time.

Whether it be a civil or criminal case, having valid search authority is a requirement. In fact, it's the first step in the digital forensic process. In this chapter, we'll examine the fundamental legal issues in both criminal and civil litigation.

## THE FOURTH AMENDMENT

The Fourth Amendment serves as the “litmus test” for all governmental searches and seizures. Any evidence deemed to be seized in violation of the Fourth Amendment is inadmissible in a court of law. Americans have had a long distaste for governmental intrusion into their private lives. Before the American Revolution, British soldiers, operating under Writs of Assistance, routinely invaded the homes of citizens without cause. The Fourth Amendment to the Constitution was crafted with this travesty in mind. The Fourth Amendment says: “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized” (FindLaw).

## CRIMINAL LAW—SEARCHES WITHOUT A WARRANT

There are two key questions that must be answered from the beginning. First, did the government act? Second, did that action violate the individual’s reasonable expectation of privacy? If the answer to the first question is “no,” then the Fourth Amendment doesn’t apply. It only covers searches by the government (or its agents), not private citizens.

For Fourth Amendment purposes, a person becomes an agent of the government if they are acting at the request of law enforcement. Under that scenario, it would be no different than if the police officer conducted the search.

### Reasonable Expectation of Privacy

What exactly is a “reasonable expectation of privacy”? That’s a great question with no easy answer. There is no clear cut rule or test that would help us define it. Much of the interpretation centers on what society as a whole would consider as being reasonable. For example, a person would reasonably have a greater expectation of privacy on their personal computer than they would at a public library. As a rule of thumb, you can consider the computer as a closed container. If the officer lacks the authority to open a desk drawer or box, then the same would be true with a computer ([Executive Office for United States Attorneys, 2009](#)).

If the person has a reasonable expectation of privacy, then the government must first obtain a search warrant, or the search would have to meet one of the documented exceptions to the warrant requirement.

What about individual files? Should they be seen as separate, closed containers? It seems that courts aren’t sure either. Rulings have been handed down supporting both positions. In ([United States v. Slanina, 2002](#)), the Fifth Circuit ruled that when a proper search is conducted on a portion of a disk, defendants no longer have a reasonable expectation of privacy in regards to other files.

In contrast, the Tenth Circuit took the opposite stance saying “[b]ecause computers can hold so much information touching on many different areas of a person’s life, there is greater potential for the ‘intermingling’ of documents and a consequent invasion of privacy when police execute a search for evidence on a computer” ([United States v. Walser, 2001](#)).

Information that an individual knowingly exposes to others is not protected by the Fourth Amendment. Examples here could include public computers such as those in a classroom or “shared drives” on a network ([Executive Office for United States Attorneys, 2009](#)).

## Private Searches

Private searches are not afforded Fourth Amendment protection unless the search is done at the request of the government or with their knowledge or involvement. Take the Geek Squad at Best Buy, for example. Let’s say that someone gives them permission to work on their home computer and in the process they find child pornography images on their machine. The images found by the repair technician would be admissible as long as they were not searching at the request of the government, thereby acting as their agent.

## E-mail

By and large, an individual maintains their Fourth Amendment protections when an e-mail is being transmitted, but would lose those protections when it reaches its final destination. E-mail is viewed in a similar fashion as regular “snail mail.” The legal interception of an individual’s e-mail or other electronic communication is something that is tightly controlled. Known as the Wiretap Act, Title III of the Omnibus Crime Control and Safe Streets Act of 1968 prohibits unauthorized monitoring and lists the procedures needed to obtain a warrant for wiretapping ([U.S. Department of Justice, Office of Justice Programs, 2010](#)).

## The Electronic Communications Privacy Act (ECPA)

The purpose of the ECPA was to ban a third party from intercepting and/or disclosing electronic communication without prior authorization. This federal statute was passed originally in 1968 as an amendment to the Wiretap Act of 1968. The ECPA underwent its first change in 1994 when it was amended by the Communications Assistance to Law Enforcement Act, also known as CALEA. It was modified once again after the 9/11 attacks by the USA Patriot Act. The Patriot Act was authorized again in 2006 ([TechTarget, 2005](#)).

## Exceptions to the Search Warrant Requirement

There are several well-known exceptions to the search warrant requirement. A warrantless search is valid with **consent** as long as the person giving the consent is authorized and the consent is truly voluntary. The voluntariness of the

consent is judged on the totality of the circumstances. The Supreme Court recognized age, education, intelligence, and the physical and mental condition of the person giving consent as important factors to consider. Other considerations would be whether the person was under arrest at the time of consent and whether the person had been advised of his right to refuse consent. If the validity of the search relies on consent, the burden is on the government to prove it was indeed given voluntarily.

Consent may be revoked at anytime. The search must cease immediately when the consent is withdrawn. So what happens if the suspect has second thoughts after his computer has been collected and taken to the lab for processing? The same standard applies (almost). The search must stop when they revoke their consent. That said, courts have said that this does NOT apply to forensic clones. In other words, although the original must be returned, any clones that have been made do not. Defendants do not have a reasonable expectation of privacy with a forensic clone ([United States v. Megahed, 2009](#)). For this very reason, cloning a drive sooner rather than later is a very wise move.

The scope of a consent search is sometimes at issue in a criminal case. If they give you consent to search the house, does that include closed containers and computers? Well, that depends on the particular details of the situation. Courts will again apply the "reasonableness" standard in making a determination. What would a reasonable person have understood the scope to be under those conditions?

The party granting consent may set forth restrictions on the search. Should that be the case, officers must abide with this request. To do otherwise could very well result in the suppression of any evidence recovered.

### MORE ADVANCED

#### Consent Forms

In searches that hinge on consent, it often comes down to one side's word over the other. What exactly was said, how it was said, and what the suspect understood at the time could all be scrutinized. A well-crafted consent-to-search form will go a long way in countering any attack on the search. The form should include details specifically relating to digital evidence. The form should seek permission to search not just computers but any storage media including cell phones, manuals, printers, and more. The form should ask for permission to take these items from the location for offsite examination ([Executive Office for United States Attorneys, 2009](#)).

In the end, it's important to remember that consent searches can be highly nuanced and heavily dependent on the facts or circumstances that arise during that specific incident. While searching without a warrant is sometimes a necessity, the best practice is to get a search warrant whenever possible. Your case will rest on much more solid ground with a warrant than without.

**Third parties** can sometimes consent to the search of private property. Roommates, spouses, and parents are just a few of the examples. Normally, if a device is shared, all parties have the authority to provide consent to search its common areas. In this situation, none of them would have a reasonable expectation of privacy in the common areas since it's shared with other people. The notion of common areas is significant. Areas such as those that are password protected would not qualify as a common area. The third party would likely not have the authority to consent to its search. However, if the suspect has shared the password with the third party, then this constraint no longer applies. The suspect's reasonable expectation of privacy has been greatly diminished.

It's foreseeable that in the end, the third party in question really didn't have the authority to consent. This is not necessarily a deal breaker as far as the admissibility is concerned. Officers in the field can only do what a reasonable person would do when determining a third party's legal ability to provide consent. If the suspect is present at the scene, a third party is not permitted to grant consent.

Spouses, under normal circumstances, can consent to the search of common areas. Parents may or may not be able to provide consent to search a child's property. If the child in question is less than eighteen years of age, parents are generally permitted to give consent. If the child is over eighteen, then it gets a bit more complicated. Factors that will impact this determination include the child's age, whether or not they pay rent, and what steps (if any) they have taken to restrict access.

Technicians are often in the position of uncovering evidence during the course of their work. The courts have been split when deciding if the technician has the authority to consent. Officers may recreate the technician's search or observe them retrace their steps. They may not, however, expand the technician's search or direct them to look deeper. Should a technician locate evidence, their findings are normally used as the basis for a search warrant.

**Exigent circumstances** arise from time to time requiring the immediate seizure and possible search of a digital device. This is generally permitted under one of these three conditions: the evidence is under immanent threat of destruction, a threat puts law enforcement or the public in general in danger, and when the suspect is expected to escape before a search warrant can be acquired. This exception may apply to the seizure of an item or device, but not automatically the search of it. Once the item has been seized (secured), the exigency may no longer exist, thus requiring a search warrant to continue.

Officers have the right to charge suspects with evidence they see if they are legally permitted to be where they are, and if the item is immediately apparent to be incriminating. This is known as the **plain view** doctrine. This situation typically arises in a digital forensic context when an examiner is analyzing a drive for evidence of one crime and finds evidence of a completely different one. For instance, an examiner searching a hard drive for photos of stolen artwork comes across images of child pornography. At this juncture, the search should

cease until a separate warrant pertaining to the possession of child pornography can be obtained.

Border searches and searches by probation and parole officers are afforded much more latitude than those conducted by police officers. From the court's perspective, individuals entering the country can be searched with probable cause or even reasonable suspicion. The court recognizes the government's need to secure the border from contraband and like material. Those individuals on probation or parole have less of an expectation of privacy than other citizens. For example, sex offenders may be prohibited from using the Internet during their supervised release. This stipulation would permit the parole or probation officer the authority to search the offender's computer at any time to ensure compliance. There is even some case law permitting this type of search without these specific conditions in place.

Employees in the workplace may or may not possess a reasonable expectation of privacy on their work computers. This expectation will vary depending on the facts including whether or not the employee is a government employee. Normally, officers can search an employee's computer without a warrant if the employer or another coworker (with shared authority) gives permission. Government employees are looked at a bit differently. That's not to say that employers can't search the employee's system; it just means that the search must be "work-related, justified at their inception, and permissible in scope" ([Executive Office for United States Attorneys, 2009](#)).

## SEARCHING WITH A WARRANT

Absent one of the well-defined exceptions described here, police officers must have a search warrant before searching someone's private property, including their computer.

A search warrant is an order that is obtained by a law enforcement officer from a judge, granting them permission to search a specific place and seize specific persons or things.

A judge will issue the warrant when he or she believes that there is probable cause that a crime was committed and that the people or things specified in the warrant will be found at that location. The Supreme Court said that probable cause is established when there is "a fair probability that contraband or evidence of a crime will be found in a particular place" ([Illinois v. Gates, 1983](#)). Another way to look at it is more likely than not the items or persons to be seized will be found at that specific location. Mathematically, this would equate to a probability of 51 percent.

When applying for a warrant, it's helpful to determine the role of the computer in the crime. The computer can be considered contraband if it contains child pornography or is stolen property. The computer can also be used to store evidence, such as incriminating documents. Finally, the computer can serve as a tool or instrumentality of the crime. This is the case when the computer is used to hack into a company's network, for example.

## Seize the Hardware or Just the Information?

We know from the Fourth Amendment that a search warrant must “particularly describe the place to be searched and the person or things to be seized.” To effectively meet that requirement, we first need to understand what precisely we need to seize. In short, is it the hardware or the information held by the hardware? If the computer is contraband, evidence, or fruits or instrumentalities of a crime, then we need to establish probable cause to seize the hardware. Otherwise, our focus is on the information alone.

### Particularity

Courts frown heavily on overly broad affidavits that lack the particularity mandated by the Fourth Amendment. Affidavits should make it clear what items can be seized and what can’t. “Particularly” describing things that you likely have never seen may seem like an impossible task. It’s really not. Serial numbers and the like are not required.

Here is some sample language that could be used:

“Any and all personal computer(s)/computing system(s) located at the residence of (INSERT ADDRESS HERE), to include input and output devices, electronic storage media, computer tapes, scanners, disks, diskettes, optical storage devices, printers, monitors, central processing units, and all associated storage media for electronic data, together with all other computer-related operating equipment and materials.”

Describing the information can be done in a somewhat similar fashion. Although we probably don’t know the file names, for example, it’s quite possible that we would know the suspect’s name, the time period, and the specific crime that’s being investigated. The courts are looking for some type of limiting language. Asking for “any and all files” on a suspect’s hard drive stands a very good chance of being deemed overly broad, resulting in the suppression of any evidence found.

## Establishing Need for Off-Site Analysis

The forensic analysis of a hard drive can be a very time-consuming process. For a variety of reasons, this is best done at the lab or police station. For all intents and purposes, doing this at the scene contemporaneously with the search should not be the first option. As such, the search warrant affidavit should spell out in clear terms the logic and need for this practice. Reasons can include the amount of time and data involved and potential use of antiforensic techniques as well as the need to perform this task under the more controlled conditions (like those found in the lab). This is one way to make this point in an affidavit:

“Computer storage devices (like hard disks or CD-ROMs) can store the equivalent of millions of pages of information. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file names. This may require searching authorities to

peruse all the stored data to determine which particular files are evidence or instrumentalities of crime. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical and invasive to attempt this kind of data search on-site.

Technical requirements. Searching computer systems for criminal evidence sometimes requires highly technical processes requiring expert skill and properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert is qualified to analyze the system and its data. In any event, however, data search processes are exacting scientific procedures designed to protect the integrity of the evidence and to recover even “hidden,” erased, compressed, password-protected, or encrypted files. Because computer evidence is vulnerable to inadvertent or intentional modification or destruction (both from external sources or from destructive code imbedded in the system as a “booby trap”), a controlled environment may be necessary to complete an accurate analysis.” ([Executive Office for United States Attorneys, 2009](#))

### Stored Communications Act

The **Stored Communications Act** (SCA), enacted in 1986, provides statutory privacy protection for customers of network service providers. The SCA controls how the government can access stored account information from entities such as Internet Service Providers (ISPs). This account information typically includes e-mail as well as subscriber and billing information. Specifically, the SCA lays out the process state and federal law enforcement officers must adhere to in order to force disclosure of these records by the provider.

The SCA seeks to codify the type of information sought, the privacy expectations associated with it, and the legal instrument required for the government to access it. The SCA breaks down service providers into two separate and distinct groups: “electronic communication service” providers and those organizations that provide “remote computing services.” Understanding these differences is essential to deciphering the SCA and its legal requirements.

According to the SCA, specifically 18 U.S.C. § 2510(15), an **electronic communication service (ECS)** provider is “any service which provides to users thereof the ability to send or receive wire or electronic communications.” ECS examples would include companies that deliver telephone and e-mail services ([Executive Office for United States Attorneys, 2009](#)). America Online comes to mind, as does Hotmail. It may surprise you to know that any company, no matter what its focus, can qualify as an ECS.

Title 18 U.S.C. § 2711(2) defines a **remote computing service (RCS)** as “the provision to the public of computer storage or processing services by means of an electronic communications system.” Put another way, an RCS is provided

by an “off-site computer that stores or processes data for a customer” ([Executive Office for United States Attorneys, 2009](#)).

The SCA also addresses the variety of information these providers store. This can include basic subscriber information like name, address, and credit card number. Other potential information includes logs and opened, unopened, draft, and sent e-mails.

## ELECTRONIC DISCOVERY (eDiscovery)

Digital evidence is alive and well in civil cases. Parties involved in litigation need to review all of the potentially relevant data as well as any data that may have to be disclosed to the opposing party. Common means of discovery include interrogatories, depositions, and requests for document production ([Sedona Conference, 2007](#)). Electronically stored information (ESI) presents some challenges that paper records do not. For example, ESI is easily modified, volatile, and easily duplicated and dispersed. As such, the rules of evidence for both state and federal courts are changing to specifically address ESI.

The ([Sedona Conference, 2007](#)) defines eDiscovery as “The process of collecting, preparing, reviewing, and producing electronically stored information (“ESI”) in the context of the legal process” ([Sedona Conference, 2007](#))

### Duty to Preserve

Evidence that was once confined to paper memos and filing cabinets is now found in Microsoft Word documents and back-up tapes. Digital evidence is significantly different from the paper-based evidence so many lawyers were accustomed to dealing with. For example, digital evidence is far more volatile and easier to alter or destroy. Volume is another key difference. There can be such a mind-boggling amount of data in a case that it can cost millions of dollars just to produce and review them.

In December 2006, the federal courts took the first substantive step in addressing and dealing with digital evidence, changing the Rules of Civil Procedure. These rule changes mandate that opposing attorneys work together to deal with the **electronically stored information (ESI)** in the case very early in the process. Addressing ESI early in a case reduces costs, time, and the chance of relevant evidence being overlooked. Not all lawyers and judges have embraced these changes. Like many folks, some lawyers and judges are very uncomfortable with technology, even going as far as to have someone else check and then print their e-mail.

*Zubalake v. USB Warburg* was a series of landmark electronic discovery cases. Judge Shira Scheindlin’s rulings addressed many of the fundamental concerns in cases that involve ESI. Some of the concerns included the duty to preserve electronic data, a lawyer’s duty to oversee their client’s compliance with these guidelines, data sampling, cost shifting, and sanctions.

The **duty to preserve** potentially relevant data begins when there is a “reasonable anticipation of litigation.” Failing to recognize this trigger and take action

can result in **spoliation** of the evidence and potentially severe sanctions to boot. Like other legal standards addressed in this chapter, defining a reasonable anticipation of litigation can be difficult, quite difficult in fact. The duty to preserve is not just caused by the arrival of a subpoena. It's very likely that the duty kicked in well before that time. It's a very fact-specific determination that will vary from case to case. The firing of a disgruntled employee could be enough to trigger it; likewise, so could an accusation of sexual harassment by an employee against his or her supervisor.

Judge Scheindlin also addressed a lawyer's duty to oversee their client's attempts to identify, preserve, collect, and produce potentially relevant evidence. She said, in part, "[c]ounsel must take affirmative steps to monitor compliance so that all sources of discoverable information are identified and searched." Furthermore, she said that attorneys should draft and distribute a "litigation hold" that directs a company and its employees to protect the relevant data and ensure they're not destroyed or compromised in any way.

**Data sampling** is a way to test a large collection of ESI for the "existence or frequency of relevant information" ([Sedona Conference, 2007](#)). The volume of potentially relevant data can be staggering, especially in a large corporate environment. Data sampling is one of the best ways to save time and reduce costs during the eDiscovery process.

The costs incurred during the eDiscovery process can be massive, rising into hundreds of thousands or even millions of dollars. Typically, in traditional discovery, the producing party bears the cost of production. Under certain conditions, the costs of production may be shifted to the requesting party. In the *Zubulake* case, Judge Scheindlin addressed this concern and devised a seven-factor test to be used to determine if cost shifting is warranted.

The seven factors are "(1) the extent to which the request is specifically tailored to discover relevant information; (2) the availability of such information from other sources; (3) the total cost of production compared to the amount in controversy; (4) the total cost of production compared to the resources available to each party; (5) the relative ability of each party to control costs and its incentive to do so; (6) the importance of the issue at stake in the litigation and; (7) the relative benefits to the parties of obtaining the information" (*Zubulake v. UBS Warburg, 2003*).

### Private Searches in the Workplace

It's not uncommon for work computers to be the subject of a search for criminal, civil, or administrative actions. From the private side, employers have a fair bit of latitude to search an individual's company computer. A company computer use policy that clearly spells out that work computers, e-mail, and so on are for work purposes only and that they may be searched at any time is an accepted best practice. For Fourth Amendment purposes (law enforcement or their agents), a work computer can be searched with consent of a supervisor or another employee as long as they have common authority over the area to

be searched. It is also important to note that federal privacy statutes and the Stored Communications Act may come into play as well.

In the end, consult with the prosecuting attorney or corporate/in-house counsel for guidance. Getting their input can help ensure that the case is on the strongest legal footing ([Executive Office for United States Attorneys, 2009](#))

### ALERT!

#### International eDiscovery

With the cloud environment and data regularly flying across borders, international electronic discovery is becoming an issue. Not every country has the same views on privacy or the same legal standards and procedures for discovery. As a result, gaining access to data in a foreign country is very complex. The Sedona Conference's *Framework for Analysis of Cross-Border Discovery Conflicts: A Practical Guide to Navigating the Competing Currents of International Data Privacy and e-Discovery* is an excellent introduction to the complexities involved in international eDiscovery. You can download it for free from <http://www.thesedonaconference.org/>.

## EXPERT TESTIMONY

As a digital forensic examiner, you must be prepared to testify in court as an expert witness as to your findings and procedures. What's the difference between a witness and an expert witness? A major difference is that a qualified expert witness can give an opinion, but a "regular" witness can't.

Determining whether or not an individual is an expert is a matter for the court to decide. An expert doesn't have to have a Ph.D or other lofty credentials. FindLaw defines an expert as someone "who by virtue of special knowledge, skill, training, or experience is qualified to provide testimony to aid the factfinder in matters that exceed the common knowledge of ordinary people" (FindLaw).

Under this definition, bakers, tailors, accountants, medical doctors, and school bus drivers could be qualified as an expert. Certainly credentials help, but they are not a requirement.

There are two cases that form the foundation for the admissibility of expert testimony. The first is a 1923 case, *United States v. Frye*. The *Frye* (1923) case centered on the admissibility of new lie-detection technology. Out of this case came what became known as the "Frye Test." The test said that "the results of scientific tests or procedures are admissible as evidence only when the tests or procedures have gained general acceptance in the particular field to which they belong" (*United States v. Frye*, 1923).

Eventually, the Frye Test fell by the wayside. In *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579 (1993), the U.S. Supreme Court ruled that the

Federal Rules of Evidence superseded the Frye Test. Merrell Dow Pharmaceuticals Inc. was sued by plaintiffs who claimed that their drug, Bendectin, had caused significant birth defects. The lower court granted Merrell Dow's request for summary citing that the scientific evidence presented by the plaintiff had not yet gained approval within the scientific community. The Supreme Court agreed.

In *Daubert* (1993), the Court said that the admissibility should be evaluated on "whether the testimony's underlying reasoning or methodology is scientifically valid and properly can be applied to the facts at issue. Many considerations will bear on the inquiry, including whether the theory or technique in question can be (and has been) tested, whether it has been subjected to peer review and publication, its known or potential error rate and the existence and maintenance of standards controlling its operation, and whether it has attracted widespread acceptance within a relevant scientific community" (*Daubert*, 1993).

Understanding this groundwork will help the examiner better comprehend the admissibility of their testimony within the context of the law.

### ADDITIONAL RESOURCES

#### Expert Testimony

Fred Smith and Rebecca Bace's book on expert testimony, *A Guide to Forensic Testimony: The Art and Practice of Presenting Testimony as an Expert Technical Witness*, contains a tremendous amount of practical information. One of the best aspects of the book is that it is written for information technology experts. The book covers the topic well and is quite "readable."

### SUMMARY

Proper search authority is a necessary first step in the forensic examination process. Evidence collected without it is very likely to be excluded. The Fourth Amendment to the U.S. Constitution protects citizens from unreasonable searches and seizures. The protections afforded by the Fourth Amendment only cover actions by the government. It does not apply to private citizens acting on their own. Law enforcement can search and seize digital evidence with and without a search warrant. Searches with a warrant are always better, from a legal standpoint, than searches without one. That said, exigent circumstances can and do arise that would permit officers to do otherwise.

On the private side, supervisors and employers will likely have broad authority to search company computers, especially if the employee read and signed a computer usage agreement clearly stating that the company computers, e-mail, and so on could be searched at any time.

Consulting with the appropriate legal counsel before searching or seizing digital evidence is never a bad idea. If you have questions or concerns, they should always be raised in advance.

## References

- Casey, E. (2011). *Digital evidence and computer crime, 3rd ed.: Forensic science, computers, and the Internet*. Waltham, MA: Academic Press.
- Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579 (1993).
- Executive Office for United States Attorneys. (2007). *Prosecuting computer crime*. Office of Legal Education. Washington, DC: United States Department of Justice.
- Executive Office for United States Attorneys. (2009). *Searching and seizing computers and obtaining electronic evidence in criminal investigations*. Office of Legal Education. Washington, DC: United States Department of Justice.
- Frye v. United States, .293 F. 1013 ( D.C. Cir 1923).
- FindLaw. (n.d.). *Fourth Amendment—Search and Seizure*. Retrieved October 4, 2011, from: <http://caselaw.lp.findlaw.com/data/constitution/amendment04/>
- Goldfoot, J. (2011). The physical computer and the Fourth Amendment. *Berkley Journal of Criminal Law*, 16(1), 112–167.
- Illinois v. Gates, 462 U.S. 213, 238, (1983).
- Kerr, O. S. (2005a). Digital evidence and the new criminal procedure. *Columbia Law Review*, 105(1), 279–318.
- Kerr, O. S. (2005b). Searches and seizures in a digital world. *Harvard Law Review*, 119(2), 532–585.
- Kroll OnTrack, Inc. (n.d.). *Zubulake v. UBS Warburg*. Retrieved October 10, 2011, from: <http://www.krollontrack.co.uk/zubulake/>
- McCullagh, D. (2007, December 14). *Judge: Man Can't Be Forced to Divulge Encryption Passphrase*. Retrieved October 3, 2011, from: [http://news.cnet.com/8301-13578\\_3-9834495-38.html](http://news.cnet.com/8301-13578_3-9834495-38.html)
- Scheindlin, S., & Capra, D. J. (2008). *Electronic discovery and digital evidence: Cases and materials*. Eagan, MN: Thomson West.
- Sedona Conference. (2007). *The Sedona Conference glossary: E-Discovery & digital information management* (2nd ed.). Sedona, AZ: Sedona Conference.
- TechTarget. (2005, December). *Electronic Discovery*. Retrieved November 6, 2011, from Search Financial Security. TechTarget.com: <http://searchfinancialsecurity.techtarget.com/definition/electronic-discovery>.
- U.S. Department of Justice, Office of Justice Programs. (2010). *Privacy and Civil Liberties*. Retrieved October 10, 2011, from: <http://it.ojp.gov/default.aspx?area=privacy&page=1284#contentTop>
- United States v. Megahed, 2009 WL 722481, at \*3 (M.D. Fla. Mar. 18, 2009).
- United States v. Slanina, 283 F.3d 670, 680 (5th Cir. 2002).
- United States v. Walser, 275 F.3d 981, 986 (10th Cir. 2001).
- Zubulake v. UBS Warburg, 217 F.R.D. 309 (S.D.N.Y. 2003).

This page intentionally left blank

## CHAPTER 8

# Internet and E-Mail

117

### Information in This Chapter:

- Overview of the Internet and How it Works
- How Web Browsers Work and the Evidence They Can Create
- E-Mail Function & Forensics
- Chat and Social Networking Evidence

## INTRODUCTION

In the beginning, the Internet was a little-known tool used by a few academics and the military. Today, it's a tool truly for the masses. We can order pizza, pay bills, look up a phone number, and take a class. For many of us, it is hard to imagine life without it. For examiners, its use can leave significant pieces of evidence. Web browsing, chat, e-mail, and social networking are just some of the technologies that we must understand how they're used, how they work, and where they leave traces.

## INTERNET OVERVIEW

We'll begin with a quick introduction to the technology involved in getting your favorite web page to appear on your computer screen. Perhaps the best way is to track the process from start to finish. It all begins when someone enters a web address or **URL** (Uniform Resource Locator) into the address bar of a **browser**. A URL comprises three parts: the host, the domain name, and the file name. Let's use <http://www.digitalforensics.com> as an example.

In our example, "http" or **Hypertext Transfer Protocol (HTTP)** is the protocol used on the Internet to browse and interact with web sites and the like. A protocol is nothing more than an agreed-upon way for devices to communicate with

one another. Next is the **domain name**, “digital forensics.” Last is the **Top Level Domain (TLD)**, “.com.” It’s called a TLD because it is at the top of the hierarchy that makes up the Internet’s domain name system. Other TLDs include .org, .edu, and .net, just to name a few.

The browser, using the HTTP protocol, sends a “get” request to the web server hosting [www.digitalforensics.com](http://www.digitalforensics.com). A browser is an application that is used to view and access content on the Internet. There are several browsers to choose from: the most common are Microsoft’s Internet Explorer, Mozilla’s Firefox, and Google’s Chrome.

After hitting enter, the first order of business is to convert the domain name into an **IP (Internet Protocol)** address. The Internet functions with IP addresses. It can’t do anything with the domain name itself. The domain name is for us, making it easier to remember. A **Domain Name Server (DNS)** is responsible for mapping domain names to specific IP addresses. After the DNS makes the conversion, the request is then sent on to the server hosting the web site. After receiving the request, the server returns the requested web page and associated content.

A web page comprises several components. The first is the **HTML (Hypertext Markup Language)** document. This contains quite a bit of information including directions for how the page should be rendered (displayed) by the browser, content, and more. It also contains file names for subcomponents of the web page such as images. It’s important to note that HTML is not a programming language.

There are two types of web pages: static and dynamic. A static web page is one that is prebuilt. Its content, layout, etc., are predetermined. A dynamic page, however, is built “on the fly.” It doesn’t exist until it’s called. The page is built from different pieces drawn from databases. Amazon is a great example of a dynamic web site. My page will very likely be different from your page. The books and so on that appear on my page are based on my shopping and buying habits. All this information is stored in a database(s) along with the things like the book images, descriptions, and so on. When I logon to Amazon, the server sends the items that are standard for everyone (like the Amazon logo) along with the content targeted to me.

When interacting with a web site, it’s important to understand where certain things are occurring. This can be especially important to know from a forensics perspective because it can tell you where you should be looking for a given artifact. Actions can occur on either the client-side or the server-side. JavaScript (no relation to the Java the programming language) is a client-side technology. It’s used for things such as roll-overs on a navigation bar. The code that makes that work is downloaded and run on the local machine. Server-side actions are just the opposite and are used when there is a need to send information to another computer (like my custom content at Amazon).

## ADDITIONAL RESOURCES

### Web Technology

Today's web is a complex place using many different technologies to make it run. Understanding how these work, even at a rudimentary level, will be very helpful. The w3 Schools web site is a great source of introductory material on many of these technologies. The site includes reference material, lessons, quizzes, tutorials, and more.

<http://www.w3schools.com/>

Determining the ownership and host of a particular domain name can become relevant in a criminal or civil case. A search query known as a "whois" can help you identify some of the individuals and/or companies associated with a given domain name. A whois search can tell you the registrant, when the domain was created, the administrative contact, and the technical contact. The contact information typically provides a name, address, and phone number. Most if not all domain name registrars now offer private registration. Any whois search for a domain name with private registration will typically get the registrar's contact information, rather than the actual owner (Network Solutions, LLC). If you'd like to give this a try, visit one of the sites offering the whois service. Network Solutions is one: <http://www.networksolutions.com/whois/index.jsp>.

## Peer-to-Peer (P2P)

P2P is used primarily as a means to share files. A major portion of the traffic on a P2P network is pirated music and movies as well as child pornography. P2P differs from a client/server network in that computers on a P2P network can serve both roles (client and server). **Gnutella** is one of the major systems or architectures used in P2P networks.

## MORE ADVANCED

### Gnutella Requests

On a P2P network, what stops a file request from just propagating forever? There is actually a built-in mechanism in the information packets. In each packet, there is a Time To Live (TTL) value that is set to decrease by one every time it is delivered to another node on the network. Once that number hits 0, the packet is stopped.

To get started with a P2P network, users must first download and install a P2P client such as KaZaA, Frostwire, GigaTribe or eMule. Typically, users then create a "shared" directory containing files they want to make available to others.

To find files of interest to download, users normally enter search term(s) for the file or files he wants. If the search is successful, the software returns a list of computers that have the requested file(s). Lastly, the files are downloaded to a directory of the user's choosing or to the default location specified by the client. P2P networks use HTTP to transfer files.

Nodes on a Gnutella fall into two categories. Nodes that have the required bandwidth as well as the uptime (time on the network) are classified as Ultra-peers. Those that don't are known as leafs. Ultra-peers perform some additional duties such as searching, indexing, and facilitating connections.

### The INDEX.DAT File

The INDEX.DAT is a binary, container-like file that is used by Microsoft's Internet Explorer (MSIE). The INDEX.DAT file holds quite a bit of value for forensic examiners. There are multiple INDEX.DAT files on a system. The INDEX.DAT tracks several pieces of information regarding the URLs visited, the number of visits, and so on. These files are hidden from the user and must be viewed using a tool of some sort. Both FTK and EnCase are able to decipher INDEX.DAT files. MSIE has three directories: History, Cookies, and Temporary Internet Files. INDEX.DAT files are used to track the information and contents of each directory ([Casey, 2009](#)).

## WEB BROWSERS—INTERNET EXPLORER

Web browsers are an indispensable part of the overall computing experience and serve as our "vehicles" on the "Information Superhighway" known as the World Wide Web. Although there are multiple browsers on the market, Microsoft's Internet Explorer is far and away the most widely used. Other browsers (for the PC) also getting some traction are Mozilla's Firefox and Google's Chrome. On Macintosh computers, Safari is king, with Firefox getting some use here as well. At their foundation, these applications function in much the same way. For instance, all of them utilize some sort of caching system. They also have mechanisms to deal with cookies, Internet history, typed URLs, bookmarks, and more. They differ in the details. Space does not permit an exhaustive look at all the browsers and the details of their inner workings. Instead, we'll focus on some of the common functions as they are in MSIE, the overwhelming market leader.

### Cookies

A cookie is a small text file that is deposited on a user's computer by a web server. Cookies can serve a variety of purposes. They can be used to track sessions as well as remember a user's preferences for a particular web site. [Amazon.com](#) is a great example. When you return to the site you are normally

greeted with a “Hello, Susan” as well as customized recommendations based on your buying and browsing history. That level of individualization is made possible through cookies.

Cookies can provide valuable evidence and are tracked in a single INDEX.DAT file. They can contain Uniform Resource Locators (URLs), dates and times, user names, and more. Deciphering a cookie can be a challenge, as they aren’t normally written in the clear. Fortunately for us, tools are available to get this done. It’s critical to note that the existence of a web address in a cookie is not necessarily proof that the suspect actually visited the site ([Casey, 2009](#)).

### Temporary Internet Files, a.k.a. web Cache

We are an impatient lot. As such, speed is vital to a user’s Internet experience. Today, web browsing is expected to be nearly indistinguishable from the applications running on our own machines. web cache is one way that the browser makers shave some time off the download times. Cache speeds things along by reusing web page components like images, saving time from having to download objects more than once.

Microsoft’s browser, Internet Explorer, refers to web cache as **Temporary Internet Files (TIF)**. In Microsoft Internet Explorer, TIF is organized into sub-folders bearing a random eight-character name. They are organized using a collection of INDEX.DAT files. Each file in TIF has a corresponding date and time value associated with it. This includes a “last-checked” time, which is used by the browser to determine if a newer version exists on the server. If so, then it will download the newer version.

Users can view their TIF anytime using Windows Explorer. Inside the TIF folder users will see a listing of its contents. Each item in the list will display an icon showing file type, file name, and the associated URL. It’s important to understand that in this instance, what the user sees is a virtualized representation of the content. The actual items are kept in the TIF subdirectories. The only file that is actually kept here is the INDEX.DAT that keeps tabs on where the files are located inside the various subdirectories.

Webmail evidence can also be found in TIF. Hotmail, AOL, and Yahoo! can all leave messages and/or inbox information that can prove useful. These items can be recognized by the file names. Here are some examples:

- Outlook web Access Messages—Read[#].htm
- AOL Messages—Msgview[#].htm
- Hotmail messages—getmsg[#].htm
- Yahoo!—ShowLetter[#].htm
- Outlook web Access Inbox—Main[#].htm
- AOL Inbox—Msclist[#].htm
- Hotmail Inbox—HoTMail[#].htm
- Yahoo!—ShowFolder.htm

## MORE ADVANCED

### Caching and HTTPS

If you've ever bought anything on the Internet or done any online banking, then odds are that you've used the HTTPS protocol. HTTPS is not just used for electronic commerce. It's also used for secure web-based e-mail.

HTTPS is a secure version of the HTTP protocol we use on the Internet. By default, and for security reasons, MSIE does not cache any HTTPS web pages. This is important to note, especially if you are investigating a case that might involve some sort of HTTPS web traffic. If so, then you may not find any remnants of this activity in cache.

web cache can be used to determine both culpability and intent. Much of what's in web cache will be thumbnails (those small images) along with bits and pieces of web pages.

Image size can impact a case, particularly those involving child pornography. If the suspect images are comprised entirely of small, cache-like images, then some prosecutors may be reluctant to file charges. The issue then becomes intent. Those images could have been downloaded automatically, without his consent. Images of such a small size can make for a much weaker case. Larger images, those not commonly found as part of a web page, are harder to explain away.

### Internet History

Microsoft's Internet Explorer, the reigning king of browsers, keeps multiple historic user records. History is used to prevent a user from having to retype URLs into the address bar of the browser. The index.dat files track other details as well. For example, it tracks the number of times the site is visited, and the name of the file. The Internet history is organized in multiple folders and index.dat files. There are three folders: Daily, Weekly, and Cumulative.

These folders use a naming convention based on a set prefix followed by a date range. For example, a folder covering the Internet history from October 1, 2011, to October 8, 2011, would look like this:

MSHist012011100120111008  
MSHist01 – Folder name/prefix  
2011 – Year (start)  
1001 – Date (start)  
2011 – Date (end)  
1008 – Date (end)

People who have something to hide will often clear their history on a frequent basis. This can be done manually by the user or automatically by the system. By default, the history is set to clear every twenty days. The user can change this to

clear much faster than that. Using a tool that can read the registry, you can view this information here:

NTUSERS\Software\Microsoft\Windows\CurrentVersion\Internet Settings\URL History

## MORE ADVANCED

### The NTUSER.DAT File

The **NTUSER.DAT** file contains preference settings and individual information for each user profile. Browser history is part of this information. There is one NTUSER.DAT for each user profile on the system. Although technically a registry file, the NTUSER.DAT is located in the user folder. Note that we're talking about user "profiles" and not "users." Putting a specific person on the keyboard is a very difficult if not impossible determination to make. Just because a person has a profile on the machine does not mean their fingers were on the keyboard at any given moment.

If this value is set less than the default of twenty days, this can be used to show the defendant took proactive steps to remove potentially incriminating evidence.

## Internet Explorer Artifacts in the Registry

As part of its everyday function, MSIE deposits artifacts in the registry. These items are stored particularly in the NTUSER.DAT hive. Here we can see if the browser stores passwords, the default search engine, the default search provider, and more.

The registry can also tell us what URLs have been typed right into the browser's address bar. These are listed from 1 to 25 with the lowest number being the most recent. Only twenty-five entries can be kept at a time. The entries are purged on a first in, first out basis. [Figure 8.1](#) shows you what they look like through a forensic tool.

Name	Type	Data
ab url1	REG_SZ	http://www.google.com/
ab url2	REG_SZ	http://www.filesredder.com/
ab url3	REG_SZ	http://www.wikileaks.org/
ab url4	REG_SZ	http://hackernews.com/
ab url5	REG_SZ	http://www.hacker.com/
ab url6	REG_SZ	http://www.hacer.com/

**FIGURE 8.1**

Typed URLs as found in the Windows Registry. Graphic courtesy of Jonathan Sisson.

Here is the file path to this registry artifact:

NTUSER\Software\Microsoft\Internet Explorer\Typed URLs

Remember, the registry is not human-readable in its native form. To examine it you will need an appropriate tool. Some of these tools include Microsoft's RegEdit, Harlan Carvey's RegRipper, and AccessData's Registry Viewer.

## Chat Clients

Chat applications are both popular and numerous. They are used for instant text-based communication. Popular applications include AOL Instant Messenger (AIM), Yahoo! Messenger, Windows Live Messenger, Trillian, Digsby, and many more. These clients can be used either to commit or to facilitate a variety of crimes. Pedophiles use these tools to solicit sex from minors or to distribute child pornography. Buyers and sellers use them to negotiate the sale and transfer of narcotics. The list can go on and on. Function varies from client to client as do the artifacts they leave behind. Function and residual evidence can also vary from version to version. It's difficult to keep up with the rapid pace at which these clients change. Changes can result in artifacts moving or disappearing. Rather than get "down in the weeds" with each application and version, we'll talk in broad terms of what kind of artifacts are possible and how they can be used as evidence.

Not unlike other software, chat client will leave artifacts of its installation. Paths and directories may vary somewhat. The presence or absence of these files and folders may help in proving or disproving that a specific client was used to communicate with a victim or accomplice.

Chat programs maintain a contact or "buddy" list. This list of screen names can be used to link individuals together, particularly if the other parties' screen names appear in the logs or on the drive. Screen names are often nonsensical, like "football-fan7878," and can require some effort to connect them with a specific person. Entering screen names as part of your keyword search can also be very helpful. To complicate matters further, users can have multiple screen names. Many times these alternate identities assume a parent-child relationship with the primary identity.

Users can also choose to block people, preventing them from communicating with them. If this function is available, then this setting should be tracked somewhere, potentially leaving relevant artifacts. Often clients will also maintain a list of recent chats.

Other preferences that are under user control include embedding the date time in the chat, selecting a custom icon or image, and enabling or disabling logging. Logging can serve as a tremendous source of evidence if it's enabled.

Normally, logging is turned off by default, requiring the user to activate that function. Logs typically record the chat conversations and/or other related information like connection details, etc. Even if logging is turned off, the user can manually save that particular chat session should they need to. A major difference between having logging turned on and manually saving a session log is the location where

the resulting file is saved. Auto-saved logs will normally go to a default location, whereas a destination will need to be selected for a manually saved log.

Another preference setting of interest involves the automatic acceptance of video calls, file transfers, real-time instant messages, and so on. By default, many of these features are disabled. This setting and the subsequent functionality can be used to prove that an image wasn't downloaded without consent. A suspect will have an uphill slog trying to get a jury to believe that they "had no idea" they were downloading child pornography through their chat client when the settings prove that they had to agree to accept it.

Some chat/IM clients are now allowing users to associate a cell phone (or more than one) with their account. This allows them to have IM messages forwarded to their mobile phone. In this situation, the cell number together with the account information could be used to help connect that person to a particular screen name.

## Internet Relay Chat (IRC)

Commercial chat clients like Yahoo! and AOL are quite popular and in wide use. There are two other chat clients that are well worth exploring. These tools are arguably better suited for criminal activity. **Internet Relay Chat** or IRC is one such tool. IRC is a large chat network that has little to no oversight as it is under the control of no one single entity. It affords its user near total anonymity because there is no formal registration process. IRC is also free to use. The IRC network comprises many smaller networks such as Undernet, IRCnet, and EFnet, just to name a few ([Casey, 2011](#)). IRC users create their own chat rooms or "channels." IRC attracts criminals with a wide range of interests looking to trade information or contraband. Network intrusion, identity theft, and child pornography represent some of the main criminal interests found on IRC.

IRC boasts some other features that make it attractive for criminals. Direct Client Connection (DCC) allows two users to connect directly from one machine to the other. In this mode the communication is totally private. This private traffic even avoids network servers, leaving no evidence for investigators to find.

## ICQ “I Seek You”

ICQ is the second chat tool that warrants a closer look. ICQ came on the scene in 1996.

These numbers from ICQ give you an idea of just how popular this chat client is:

- Over 42 million active users
- Over 425 million downloads
- Over 1.1 billion messages sent and received every day
- The average ICQ user is connected more than five hours per day
- 47% female and 53% male
- 80% of users between the ages of thirteen and twenty-nine
- Available in sixteen languages (ICQ)

Unlike IRC, ICQ does have a registration process. Users that register are assigned a User Identification Number or UIIN. Communication on ICQ maintains a high level of privacy. One must be invited to be included into a conversation. ICQ does route traffic through centralized servers so some artifacts may exist there if that server can be found.

## E-MAIL

Of all the potential sources of digital evidence, e-mail is one of the best. People often draft and send e-mail that they assume will never be read by anyone other than the intended recipient. As such, these often candid exchanges can (and have) come back to haunt the parties involved. It's also persistent, residing in multiple locations, thus making it harder to get rid of.

### Accessing E-mail

E-mail is accessed and managed in one of two ways. The first is web-based e-mail such as Google's Gmail or Microsoft's Hotmail. These tools function through a web browser. The second is through an e-mail application (client). E-mail clients are specialized programs designed specifically for working with e-mail. Some applications also manage calendars, tasks, contacts, and more. Outlook and Windows Live Mail by Microsoft are two of the most popular e-mail clients on Windows systems. Outlook, the more robust of the two, is used primarily in the workplace or by power users. Windows Live Mail and its predecessor Outlook Express have much more limited functionality.

Outlook stores data in either a .pst or .ost file. Windows Live Mail and Outlook Express use .dbx. Getting at the individual messages from inside these containers is a concern, but much less so now that several current tools handle these file types natively. Individual e-mail messages (.msg files) can be exported out and given to investigators or attorneys for review.

### E-mail Protocols

E-mail uses multiple protocols to send and receive e-mail. Some of them are:

- **Simple Mail Transfer Protocol (SMTP)**—Used by e-mail clients to send e-mail and by servers to both send and receive.
- **Post Office Protocol (POP)**—Used by e-mail clients to receive e-mail messages.
- **Internet Message Access Protocol (IMAP)**—Two-way communication protocol used by clients to access e-mail on a server.

### E-mail as Evidence

E-mail is widely used and people tend to be uninhibited in their messages, saying things they may never say otherwise. Thus, e-mail can provide us with a wealth of potential evidence. Some of those things include:

- Communications relevant to the case
- E-mail addresses
- IP Addresses
- Dates and times

When investigating e-mail, it's important to realize that it could be found in a number of places. These include: the suspect's machine, any recipient's machine, company server or backup media, smartphone, service provider, and any server that the message may have passed through on its way to its final destination. Like most web based evidence, time is still a factor. Collecting that evidence sooner rather than later will give you a better chance of success.

The main components of an e-mail are the header, the body, and potentially attachments. Every e-mail message that's sent has a **header**. The header records information as the e-mail travels from the sender to the receiver. Think of it as a passport of sorts. At every stop (server) along the way, information is added to the header. The **body** of the e-mail is the message itself. Finally, any attachments are added. These include things such as images and user-created files such as documents, spreadsheets, and so on. Keeping the attachments connected with an associated e-mail message is very important from an evidentiary perspective.

### E-mail—Covering the Trail

Especially savvy suspects may take steps to prevent someone from tracing the message back to them. For example, they could forge an e-mail (make it appear to be from someone else) or remove or modify the headers. Suspects could also create a phony e-mail account.

There is free software available on the Internet that enables users to "spoof" an e-mail. **Spoofing** is the act of making an e-mail look as though it actually came from someone else or from a different location. There are services available that will remail (forward) messages, stripping out the identifying information prior to transmission. This is known as anonymous remailing. Many of these companies don't keep logs, further ensuring the privacy of their users.

#### ALERT!

##### Shared E-mail Accounts

E-mail can be used to communicate even without being sent. This is done by creating an anonymous account, Yahoo! for example, and sharing the login information. Users then simply create messages and deposit them in the "Drafts" folder for others to read. Once the message is read it can be deleted. These accounts can be for one-time use, making it nearly impossible to trace or monitor. This is a popular practice among terrorists. "One-time anonymous accounts are extremely difficult to monitor," said Richard Clarke, former U.S. counterterrorism czar.

<http://www.pbs.org/wgbh/pages/frontline/shows/front/special/techsidebar.html>

### Tracing E-mail

Tracing an e-mail message is heavily reliant on logs. As we learned earlier, each server along the e-mail's path adds information to the message's header.

One of those bits of information is the **Message ID**. The message ID is a unique number assigned to the message by the e-mail server. Correlating the message ID with the server's logs is solid evidence that the message was received and sent by that particular machine. Again, the providers may purge those logs on a regular basis if they even keep them at all. Foreign providers will likely be very tough to deal with, making collection of this evidence that much harder.

### Reading E-mail Headers

The e-mail header provides a record of the path the message took from sender to receiver (assuming steps weren't taken to alter or remove it). E-mail headers should be read from the bottom to the top. Below is a sample e-mail header from a message I may have sent to legendary Steeler linebacker Jack Lambert.

Delivered-To: [Lambert58@gmail.com](mailto:Lambert58@gmail.com)  
Received: by 11.48.31.1 with SMTP1 id c2ct279nzg; Fri, 25 Oct 2011  
22:38:23 -0800 (PST)  
Return-Path:  
  
Received: from [mail.emailprovider.com](mailto:mail.emailprovider.com) ([mail.myisp.com](http://mail.myisp.com) [12.34.567.890]) by  
[mx.gmail.com](mailto:mx.gmail.com) with SMTP id f27se846431anc.2011.10.25.22.38.19; Fri, 25 Oct  
2011 22:38:23 -0800 (PST)  
  
Message-ID: <[20111025233819.47097.mail@mail.myisp.com](mailto:20111025233819.47097.mail@mail.myisp.com)>  
  
Received: from [12.34.567.890] by [mail.myisp.com](mailto:mail.myisp.com) via HTTP; Fri, 25 Oct 2011  
22:38:19 PST  
  
Date: Fri, 25 Oct 2011 22:38:19 -0800 (PST)  
From: John Sammons  
Subject: Super Bowl  
To: Jack Lambert  
  
Delivered-To: [Lambert58@gmail.com](mailto:Lambert58@gmail.com)  
  
The message recipient  
Message-ID: <[20111025233819.47097.mail@mail.myisp.com](mailto:20111025233819.47097.mail@mail.myisp.com)>  
  
Received: from [12.34.567.890] by [mail.myisp.com](mailto:mail.myisp.com) via HTTP; Fri, 25 Oct 2011  
22:38:19 PST  
  
This is the record of the message being sent through Jack Lambert's email provider,  
[mail.myisp.com](mailto:mail.myisp.com).  
  
Delivered-To: [Lambert58@gmail.com](mailto:Lambert58@gmail.com)  
  
Received: by 11.48.31.1 with SMTP1 id c2ct279nzg; Fri, 25 Oct 2011 22:38:23  
-0800 (PST)  
Return-Path:  
  
Received: from [mail.emailprovider.com](mailto:mail.emailprovider.com) ([mail.myisp.com](http://mail.myisp.com) [12.34.567.890]) by  
[mx.gmail.com](mailto:mx.gmail.com) with SMTP id f27se846431anc.2011.10.25.22.38.19; Fri, 25 Oct  
2011 22:38:23 -0800 (PST)

Finally, the message is transmitted from my email provider to Jack's Gmail account, [Lambert58@Gmail.com](mailto:Lambert58@Gmail.com)

Note the message ID, [20111025233819.47097.mail@mail.myisp.com](mailto:20111025233819.47097.mail@mail.myisp.com). Remember, this is a unique number assigned by an e-mail server (Google, 2011).

## SOCIAL NETWORKING SITES

E-mail and social media have at least one thing in common. There seems to be almost nothing that people won't send, post, or tweet. The fact that everyone seems to be on Facebook, Twitter, or some flavor of social media is not lost on law enforcement or prospective employers for that matter. Both groups routinely look to social media to learn more about suspects and prospective employees.

Social media evidence can be found in several places including the suspect's computer, smartphone, and the provider's network. Getting evidence from the provider will require relatively quick action along with a subpoena or search warrant. Remember, the provider only retains this information for a certain amount of time. At some point, the data you need will be purged without some legal intervention. All things considered, collecting the evidence from the provider might yield the best results.

Recovering evidence on the local machine can be a challenge. The page file (or swap space) is one location that could bear fruit. INDEX.DAT files also hold promise. Multiple artifacts can be found here. The confirmation e-mail (sent when the account is created) is found in the History.IE5\Index.dat file. The user's Facebook profile can be found on the local machine in a file named profile[#].htm. This is located in the Content.IE5 directories. The History.IE Index.dat file can hold Facebook friend searches.

### ADDITIONAL RESOURCES

#### **Casey Anthony Trial Testimony**

The Casey Anthony trial garnered media attention across the country. Anthony was charged with murdering her young daughter Caylee. Digital forensics played a central role in the case, particularly regarding the searches for certain keywords such as "chloroform." The trial testimony in this case by computer forensic examiner Sgt. Kevin Stenger provides some insight expert testimony on browser forensics (Firefox in this instance).

<http://www.myfoxorlando.com/dpp/news/060811-kevin-stenger-testifies>

## SUMMARY

The Internet functions in large part due to two protocols, specifically HTTP and TCP/IP. Another very common technology in wide use is HTML or Hyper-text Markup Language. HTML is one of the primary languages used to construct web pages. In digital forensics, evidence can be found within this code so it

behooves us as examiners to be able navigate through it to locate any existing evidence.

We also looked at how web pages are found and sent to browsers using Uniform Resource Locators (URLs) and Domain Name Servers (DNS).

Peer-to-Peer (P2P) networks can be used to share not only pirated music and movies, but contraband such as child pornography as well.

Chapter 8 also looked at several artifacts generated from Internet and e-mail usage. This includes such things as INDEX.DAT records, Temporary Internet Files (TIF), the NTUSER.DAT file, cookies, and e-mail headers. Tracing an e-mail back to its origin is no easy feat as the identifying information can be forged or removed.

Chat clients and their associated logs are worth examining if found on a computer. Remember, logging may not be turned on by default.

IRC and ICQ are two modes of Internet communication that can't be ignored. These are two of the most popular ways for criminals (and others concerned with private communication) to help cover their trail.

Social networking is used worldwide today by a massive number of people. Social networking evidence can be found locally and remotely on the provider's network.

## References

- Casey, E. (2009). *Handbook of Digital Forensics and Investigation*. Burlington, MA: Academic Press.
- Casey, E. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*. Waltham, MA: Academic Press.
- E.I. du Pont de Nemours and Company v. Kolon Industries, Inc.*, 2011 U.S. Dist. LEXIS 45888 (E.D. Va. April 27, 2011).
- Google. (2011, September 21). *Reading Full Email Headers*. Retrieved October 24, 2011, from: <http://mail.google.com/support/bin/answer.py?hl=en&answer=29436>
- Network Solutions, LLC. (n.d.). *WHOIS Behind That Domain Name?* Retrieved October 13, 2011, from: <http://www.networksolutions.com/whois/index.jsp>
- Refsnes Data. (n.d.). *HTML Introduction*. Retrieved October 13, 2011, from: [http://www.w3schools.com/html/html\\_intro.asp](http://www.w3schools.com/html/html_intro.asp)

# CHAPTER 9

# Network Forensics

131

## Information in This Chapter:

- Networking Fundamentals
- Types of Networks
- Network Security Tools
- Network Attacks
- Incident Response
- Network Evidence & Investigations

## INTRODUCTION

It seems like hardly a day goes by that a major company or government entity isn't reporting a significant network intrusion of some kind. Take Fidelity National Information Services Inc. (FIS), for example. The Jacksonville processor of prepaid credit cards reported that an international criminal enterprise stole \$13 million in a single day during 2011. They disclosed the theft in their first-quarter earnings statement released on May 3, 2011. The hackers executed a highly planned and well-coordinated operation involving ATMs from around the world along with stolen prepaid credit cards (Krebs). FIS is just one of many victims of crimes like this.

What began as a subculture motivated simply by overcoming the challenge hacking presented has now evolved into a much more sinister and significant threat, so much so that it's now a critical matter of national security. So much of the nation's critical infrastructure is reliant upon digital networks and devices. There is certainly no shortage of high-profile targets. These include governmental agencies, the power grid, and the financial and health care industries. This threat now comprises nation-states, organized criminal enterprises, terrorists, as well as individuals.

The private sector bears a significant portion of the responsibility in defending these networks. So, how does digital forensics figure into all this? Digital forensics can play a couple of roles:

Network investigations have some inherent hurdles that don't come into play in an investigation focusing on a stand-alone computer. Unlike a single machine,

data (evidence) could be spread across multiple machines or devices. To further complicate things, they could also be spread across a geographically expansive area. The sheer amount of data that could be involved presents another challenge. Depending on the size of the organization and its network, the volume of data could reach truly astronomical proportions.

Hackers have many attack options at their disposal when it comes to attacking a network. The attacks can be quite sophisticated or astoundingly simple. Some attacks rely on vulnerabilities in the technology; others rely on the weaknesses found in people. Software is one example of a weakness in the technology. Flaws in the software are found in the underlying code. These flaws are identified by software developers, security professionals, or others. Hackers then develop exploits to take advantage of the vulnerability. Hopefully, the software developer will take notice and fix the issue sooner rather than later. These normally come in the form of a “patch.” This is a constant struggle that never seems to end.

Human weakness also contributes to a hacker’s success in a number of ways. First, people are inclined to use weak passwords. They tend to be either too short or too predictable. For example, they use the names of their pets or children or they use actual words that can be found in the dictionary. Finally, even if the password was strong, they could leave the password written down very near the computer. Second, unsuspecting users can fall prey to a **social engineering** attack.

### Social Engineering

In a social engineering attack, an authorized user is persuaded by an unauthorized individual into divulging sensitive information. Common attacks include hackers posing as employees, customers, or security consultants.

These various attacks can also be conducted in combination, leveraging the vulnerabilities of both the technology and the people who control it.

## NETWORK FUNDAMENTALS

Networking or linking computers together has some distinct advantages. Sharing resources and collaboration are just two such benefits.

A network has some basic necessities that are required regardless of its size or purpose. The first is some type of connection between computers or devices. This connection can be a physical one (such as via an Ethernet cable) or wireless. Next, the network must have an established way to communicate. This common language, or set of rules, is known as a protocol. **Transmission Control Protocol/Internet Protocol (TCP/IP)** is a very commonly used network protocol and is also the one used on the Internet.

To lay the foundation, we’ll start by defining and identifying the various types of networks in common use today. By far, the most common type of network

encountered in a commercial setting is client/server. In a **client/server network**, each computer on the network is assigned one of these two roles. Clients are utilized by end-users, such as the workstation on your desk. These machines request files, services, and information from servers. Servers, by contrast, store and provide files, services, and information to multiple clients. In essence, you can have one server sharing files with hundreds of clients. They have much more control on the network. Servers tend to function in specific role(s). File servers, e-mail servers, and print servers are but a few examples.

The other network configuration commonly in use is known as **peer-to-peer (P2P)**. As the name suggests, all machines on the network can/do function as both clients and servers. P2P networks are seldom used in a commercial setting. File sharing is the predominant use of P2P networks. Music, movies, and software are some of the more commonly shared files. Unfortunately, P2P is also a major conduit for not only pirated music, video, and software, but child pornography as well. This is a major problem not only in the United States but worldwide as well.

Now that we have a basic understanding of how networks are organized, let's take a look at how these networks can be classified.

## Network Types

The **Local Area Network** or LAN is generally considered the smallest office network. It comprises computers and devices in a single office or building. The **Wide Area Network (WAN)** is larger, sometimes significantly so. A WAN consists of LANs at different locations. The WAN can be spread across great distances. Other network types include **MANs (Metropolitan Area Network)**, **PANs (Personal Area Networks)**, **CANs (Campus Area Networks)**, and **GANs (Global Area Networks)**.

In contrast to the Internet is an intranet. A company's intranet is private, and access to it is limited. Intranets are routinely used for file sharing, communication, and so on. An intranet functions like the Internet, using web browsers and typically the same protocol (TCP/IP).

On a network that uses the TCP/IP protocol, each computer or device on the network has a unique identifier or address known as an **IP address**. An IP address is used to deliver messages and data to its proper destination, functioning much like a street address. There are two versions of IP addressing we need to be concerned with: version 4 and version 6. IPv4 is being phased out because of the relatively small number of addresses when compared to the staggering numbers of devices and computers on the Internet. We're simply running out of addresses. IPv4 offers in the neighborhood of about four billion different IP addresses. It is being replaced by IPv6. IPv6, by contrast, provides for all intents and purposes a limitless number of addresses (Microsoft Corporation).

An IPv4 address is made up of four numbers that are separated by periods. Each of these four numbers, called octets, can range from 0 to 255. A typical IPv4 address would look like this: 198.122.55.16. An IPv6 address would look like this:

2008:0eb3:29a2:0000:0000:8c1d:0967:7256.

As a comparison, if you wrote an IPv6 address using IPv4 notation, it would look like this:

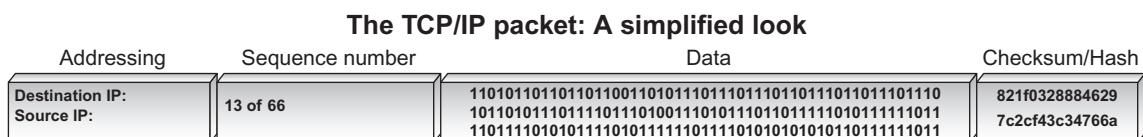
65535.65535.65535.65535.65535.65535.65535.65535 (Nikkel, 2007)

IP addresses can be static or dynamic. A static address is normally fixed and doesn't change. In contrast, a dynamic address changes on a regular basis. For example, certain Internet Service Providers (ISPs) use dynamic IP addressing. Here, each time you log on, the network assigns you an IP address from a pool of addresses that are currently unassigned. This enables a provider to service a large number of customers within the fixed number of IP addresses that they control. This works because not all of their subscribers will be online at any given time.

Data on a network can travel in different ways. **Packet switching** is used on the Internet and many other networks. Packet switching breaks the data into small chunks called packets. These packets then travel the network to their final destination using IP addressing.

Each packet is structured in a uniform manner. Individual packets are comprised of three parts; the header, payload, and footer. The header contains the addressing information, identifying the sender and receiver's IP address. Next, the packet identifies itself relative to the total number of packets. Something like "I'm packet 26 out 234." Then comes the payload itself. Finally, the packet is concluded with a footer or trailer. The trailer tells the receiver that this is the end of the packet. It also conducts a cyclical redundancy check (CRC). The CRC is a sum of all the ones in the packet. If the numbers don't match, the receiving computer will automatically resend the request. It's used to verify the integrity of the packet. [Figure 9.1](#) depicts the organization of a TCP/IP packet.

Networks routinely consist of hardware beyond just computers and servers. These devices are also important from an investigative perspective in that they can contain valuable evidence.



**FIGURE 9.1**

A typical IP packet. Illustration courtesy of Jonathan Sisson.

A gateway is a network point that acts as an entrance to another network (TechTarget, 2000). A bridge, by contrast, is used to connect two networks using the same protocol. Routers direct data, using the IP address, on the network to their final destination.

## NETWORK SECURITY TOOLS

Regarding security, the best (and most realistic) approach is to prepare in terms of "when" there is an intrusion as opposed to "if" there is an intrusion. Working on the assumption that you will be able to keep each and every committed hacker out is just not realistic. Does that mean organizations should only take minimal measures to protect their networks, focusing more resources on response rather than prevention? Absolutely not. A robust perimeter defense should always be employed, the scope of which is normally dictated by the available budget and personnel needed to run it.

Fortunately, there are many hardware and software tools available that can help protect our networks. These tools not only serve to prevent a successful attack, they can also contain information of investigative value. Let's examine a couple of these tools.

A **firewall** is "a set of related programs, located at a network gateway server, that protects the resources of a private network from users from other networks" (TechTarget, 2000). The firewall acts as a filter for both inbound and outbound network traffic. It decides whether or not to allow the traffic to pass after carefully examining the network packets.

The purpose of an **Intrusion Detection System (IDS)** is to detect attacks from both outside and inside an organization. The IDS typically monitors a network looking for a pattern of recognized network attacks as well as unusual system and user actions and activity (TechTarget, 2000). Snort is a well-known open-source network intrusion detection system (**NIDS**). Snort operates as a sniffer, watching the network in real time and firing off alerts should a potential problem be identified (TechTarget, 2002).

## NETWORK ATTACKS

There are many different ways to hack and/or attack a network. These attacks change at something akin to "warp" speed, resulting in a constant strain on the security industry. Below are just some of the attacks in use today.

**Distributed Denial of Service (DDoS)**—This attack uses massive numbers of compromised computers to attack a lone system. The attacking computers overwhelm the target with huge numbers of messages and requests. The target simply can't deal with this large volume of inbound traffic and eventually buckles, shutting down. The "army" of attacking computers are known as a "botnet," comprising individual compromised systems called "zombies."

**Identity Spoofing (IP Spoofing)**—An attacker can forge or “spoof” a valid or “known” IP addresses to gain access to a targeted network.

**Man-In-The-Middle-Attack**—In this attack, the hacker inserts himself between you and the person or entity you are communicating with. Your communications can then be monitored, altered, or deleted. This can also enable the attacker to impersonate you.

**Social Engineering**—Social engineering is one of the most effective attacks at the hacker’s disposal. Social engineering is often described as obtaining protected information by way of a “trick” or a “con.” TechTarget defines social engineering this way: “a term that describes a non-technical kind of intrusion that relies heavily on human interaction and often involves tricking other people to break normal security procedures” ([TechTarget, 2001](#)). Legendary hacker Kevin Mitnick made wide use of this technique with tremendous success ([Mitnick, 2011](#)).

Here is just one of many such examples of Mitnick’s success: Mitnick calls up the network operations center of a cell phone company during a snowstorm. After befriending one of the operators, he asks them: “I left my SecureID card on my desk. Will you fetch it for me?” Of course, the network operators are too busy to do that, so they do the next best thing: They read it to him over the phone, giving him access to their network. Once inside, Mitnick steals source code belonging to the company. In this instance, Mitnick was able to “prove” his identity by telling the network operators his office number, the department where he worked, and the name of his supervisor—all information that the attacker had gleaned from previous phone calls to the company ([Garfinkel, 2002](#)).

In 2011, Verizon Business, the United States Secret Service (USSS), and the Dutch National High Tech Crime Unit (NHTCU) issued an interesting joint report after analyzing some eight hundred security incidents. These incidents were investigated by one or more of these organizations. As part of their report, they identified the most common hacking methods used in these incidents. These include:

- Exploitation of backdoor or command/control channel.
- Exploitation of default or guessable credentials.
- Brute force and dictionary attacks.
- Footprinting and fingerprinting.
- Use of stolen login credentials.

Some, like exploiting default passwords or the use of stolen credentials, are pretty self-explanatory. Others, like the command/control channel exploit and footprinting bear a little further explanation. Exploiting a command and control channel or backdoor allows an attacker to avoid security countermeasures. This enables the attacker to avoid detection. **Footprinting** or **fingerprinting** is an automated process by an attacker to scan for open ports or services ([Verizon Business Global LLC & United States Secret Service, 2011](#)).

Network security must focus on threats not only outside the firewall, but behind it as well. Internal attacks, such as those launched by disgruntled employees, can be devastating. Lets take a look at two such attacks.

**ALERT!****Inside Threat**

It's important to recognize the fact that threats come from not only outside of an organization, but inside as well. Preventative measures must account for both possibilities. An inside threat has a significant advantage in that it can bypass much of the security measures that are in place.

An application developer, who lost his IT sector job as a result of company downsizing, expressed his displeasure at being laid off just prior to the Christmas holidays by launching a systematic attack on his former employer's computer network. Three weeks following his termination, the insider used the username and password of one of his former coworkers to gain remote access to the network and modify several of the company's Web pages, changing text and inserting pornographic images. He also sent each of the company's customers an e-mail message advising that the web site had been hacked. Each e-mail message also contained that customer's usernames and passwords for the web site. An investigation was initiated, but it failed to identify the insider as the perpetrator. A month and a half later, he again remotely accessed the network, executed a script to reset all network passwords, and changed four thousand pricing records to reflect bogus information. This former employee ultimately was identified as the perpetrator and prosecuted. He was sentenced to serve five months in prison and two years on supervised probation, and ordered to pay \$48,600 restitution to his former employer (Keeney, Cappelli, Kowalski, Moore, Shimeall, & Rogers, 2005).

A system administrator, angered by his diminished role in a thriving defense manufacturing firm whose computer network he alone had developed and managed, centralized the software that supported the company's manufacturing processes on a single server, and then intimidated a coworker into giving him the only backup tapes for that software. Following the system administrator's termination for inappropriate and abusive treatment of his coworkers, a logic bomb previously planted by the insider detonated, deleting the only remaining copy of the critical software from the company's server (Keeney, Cappelli, Kowalski, Moore, Shimeall, & Rogers, 2005). The company estimated the cost of damage in excess of \$10 million, which led to the layoff of some eighty employees (Keeney, Cappelli, Kowalski, Moore, Shimeall, & Rogers, 2005).

## INCIDENT RESPONSE

Organizations have to be able to respond when the breach occurs. Having a plan along with the tools and personnel to effectively respond can go a long way in mitigating the damage.

The National Institute of Standards and Technology (NIST) outlined the incident response life cycle in their *Computer Security Incident Handling Guide*. We can use this to walk us through an incident from beginning to end. The phases are: preparation,

prevention, detection and analysis containment, eradication and recovery, and postincident activity ([Scarfone, Grance, & Masone, 2008](#)).

**Preparation**—Preparation is key for organizations to respond quickly and effectively to any network security event. There are many steps an entity can take during the preparation phase. Planning is obviously one such step. A network's defenses should also be assessed and tested at regular intervals in order to identify vulnerabilities.

Proactive measures must be taken to prevent intrusions. Some of the preventative actions that can be taken include patching systems (keeping software up-to-date), host security (hardening individual computers), network security (securing the perimeter of the network), and conducting user awareness and training. Finally, having well-thought-out policies, procedures, and guidelines adds significantly to an organization's preparedness.

**Detection and Analysis**—Detecting a security incident presents a significant challenge. Today's sophisticated attacks can mask themselves as "normal" network activity. Vigilance and a painstaking attention to detail are needed by network security personnel in order to improve their odds of catching an attack. It also helps them reach a proper conclusion after conducting their analysis. It's a well-known fact that Intrusion Detection Systems produce large numbers of false positives. As such, the security team must be capable of accurately sifting through data. What does an attack look like? That can be a little tough to describe. To better identify suspicious activity, it's best to get an accurate picture of what is "normal" network traffic or activity is for the organization. Some of the potential signs of an attack include antivirus software alerts, abnormally slow Internet connectivity, and abnormalities in network traffic.

**Containment, Eradication, and Recovery**—When a breach occurs, it must be controlled in order to minimize its impact. Left unchecked, the fallout from an attack could grow exponentially. How to contain the incident varies based on the type of incident being faced. Some containment options include shutting down the compromised system, disconnecting it from the network, or disabling some functionality. Once the attack has been identified and contained, steps could be required to remove any potentially dangerous components such as malicious code or compromised accounts.

**Postincident Activity**—Unfortunately, this valuable step is often overlooked. A postincident review represents a missed opportunity for the organization as a whole and its personnel to improve. A typical postincident review seeks to answer questions such as:

- What did we get right?
- What did we get wrong?
- Are our policies and procedures adequate and effective?
- Do we have the necessary resources to effectively respond?
- What, if anything, would we do differently?

Responding to a security breach effectively requires diverse skill sets. As part of an incident response plan, an organization should form a computer Incident Response Team. This multidisciplinary team should bring all of the skills necessary to manage the incident to the table. Some of the skills needed to respond include representatives from management, information security, IT support, legal, public affairs/media relations, and others (Scarfone, Grance, & Masone, 2008). Someone with digital forensics capabilities should be part of the team. Many times digital forensics resources do not exist within the company itself. In these instances this function would have to be outsourced. If this is indeed the situation, this resource should be identified well in advance of an actual incident.

## NETWORK EVIDENCE AND INVESTIGATIONS

A hacker's attack typically follows a path both to and through the targeted network. As such, the potential exists to locate evidence all along the route. "Tracking" the intruder, therefore, is a critical step in the process of finding and identifying them. It is to our advantage to identify, follow, and examine as much of this trail as we can.

Our examination should include as many of the in-between or intermediary devices as possible. These intermediary devices, such as routers and servers, can hold valuable information and shouldn't be overlooked. Routers can be both an evidentiary source as well as a target for hackers. As a critical part of a network, they often serve as a valuable goal for hackers. If they can compromise a router, they can gain a significant foothold. A challenge with routers as a source of evidence is their volatility. You may recall from [Chapter 2](#) that volatile memory requires constant electrical power to maintain its contents. Unplugging or rebooting the device will likely result in a loss of potential evidence. This will in all likelihood require a "live" examination of the device while it's running. The best advice is to handle with care and treat it as you would any other piece of volatile memory.

Digital evidence is digital evidence, regardless of its source. The fundamental principles and procedures of preservation and collection still apply.

### LOG FILES

Many devices and computers in a network generate logs of events and activities. As such, log files serve as a primary source of evidence in network investigations. There are several different types of log files. Some of the logs of interest include authentication, application, operating system, and the firewall log. An **authentication log** identifies the account (and IP address) connected to a particular event.

**Application logs** record the date and time as well as the application identifier. The date/time stamps indicate when the application was started and how long it was used. **Operating system** logs track system reboots as well as the use of different devices. The operating system logs are useful in recognizing patterns of activity as well as anomalies (unusual occurrences) in the network.

Device logs such as those generated by routers and firewalls are also worth examining. We'll look at router logs more in just a second (Vacca & Rudolph, 2011).

There are some things to keep in mind with log files. Log files can change or disappear pretty rapidly. They can be purged at regular intervals to help keep storage space free. There's also a good chance that not all of the relevant logs will be in your possession. Attacks that originate outside of your organization will pass through devices under the control of a third party, such as an Internet Service Provider (ISP). These logs may have to be subpoenaed, which can take some time. ISPs won't likely hang onto these logs forever. They likely have document retention and destruction policies in place controlling what gets kept and for how long. Lacking a clear need or reason to keep it, those logs will be destroyed.

The router logs can contain much information of interest. Some of the things we can uncover are:

- Requested Uniform Resource Locators (URLs)
- Server Name
- Server IP Address
- Client's URL
- Client IP Address
- Who logged in and when

When attempting to collect evidence from a router, it's very important to minimize any interaction. Instead of accessing the router through the network itself, it's a better option to go through the router's console. Remember, our objective is to observe and record what we find, not to alter or change anything. To that end, we should avoid any command that could potentially modify any of the data. A configuration command, for example, is one that should be avoided. The "show" command is a much better option. Here are a couple of examples of "show" commands:

```
>(router name)#show clock detail—Displays the system time  
>(router name)#show users—Displays the users that have access to the router
```

### ***N*EWORK INVESTIGATIVE *T*OOLS**

The actual traffic (packets) moving on the network can hold some valuable clues. There are several tools, called "sniffers," available that can capture and analyze network traffic. Some of these tools include:

- Wireshark ([www.wireshark.org](http://www.wireshark.org))
- NetIntercept (<http://www.niksun.com/product.php?id=16>)
- NetWitness Investigator (<http://www.netwitness.com/products-services/investigator>)
- Snort (<http://www.snort.org/>)

Capturing network traffic can yield some great clues. For instance, we can determine what files have been stolen, what commands were executed, as well as any malicious payload that was delivered. From a legal perspective, it's important

to realize that monitoring network traffic in certain instances can be considered wiretapping (Casey, 2009).

## Network Investigation Challenges

Identifying the responsible hacker is by no stretch a simple task. There are many impediments along the way that can keep the attacker's identity hidden. The suspect can "spoof" his or her real IP address, potentially sending investigators on a wild goose chase. Along the same lines, the hacker can channel his or her attack through many intermediate servers scattered across the globe.

Logs can be a great source of evidence, but only if they are actually there for us to examine. Sometimes the logging function is disabled to start with, meaning that no logs were even generated. Time presents another concern. If the breach is discovered too late, then there is a significant chance that any logs maintained by an outside entity (an ISP, for example) will be destroyed pursuant to their retention and destruction policy. Hackers can also intentionally delete relevant logs during their attack, effectively covering their tracks. Lastly, jurisdiction can create a substantial obstacle. The attacker's trail can literally traverse state, national, and international boundaries. Different legal jurisdictions, especially international ones, can have wildly different requirements for obtaining this sort of information. Different countries may also have very different views of cybercrime in general, which can result in a lack of cooperation (Morris, 2005).

### ADDITIONAL RESOURCES

#### Training and Research

Training and research are a must in the world of digital forensics. Established in 1989, the SANS Institute is one of the leading institutions meeting this critical need. They offer a wide array of courses and resources covering both information security and digital forensics. In addition, they offer many certifications that are accepted throughout the industry. They also have a strong presence on Twitter.

<http://www.sans.org/>

<http://computer-forensics.sans.org/blog>

@SANSInstitute

@sansforensics

## SUMMARY

Network security should be a huge concern to all of us. Our networks and PCs are under near constant attack from lone hackers, organized criminals, and foreign countries. Cybercrime, cyberwar, and cyberterrorism are major problems threatening not only our countries and companies, but our personal computers as well. Networks represent a far greater challenge, from a forensic standpoint.

They vary wildly in size and complexity. There are several tools to help us protect our critical network infrastructure, including firewalls and intrusion detection systems. Smart organizations plan ahead for security breaches, enabling them to respond efficiently and effectively, minimizing the damage and increasing the odds that they can identify the perpetrator(s).

## References

- Bowden, M. (2011). *Worm: The First Digital World War*. New York: Atlantic Monthly Press.
- Casey, E. (2009). *Handbook of Digital Forensics and Investigation*. Burlington, MA: Academic Press.
- Casey, E. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*. Waltham, MA: Academic Press.
- Conrad, E., Misenar, S., & Feldman, J. (2010). *CISSP Study Guide*. Burlington, MA: Elsevier.
- Garfinkel, S. (2002, October 7). *Kevin Mitnick and Anti-Social Engineering*. Retrieved November 9, 2011, from CSOOnline.com: <http://www.csoonline.com/article/217395/kevin-mitnick-and-anti-social-engineering>
- Hadnagy, C. (2011). *Social Engineering: The Art of Human Hacking*. Indianapolis: Wiley.
- Krebs, B. (n.d.). *Coordinated ATM Heist Nets Thieves \$13M*. Retrieved September 19, 2011, from: <http://krebsonsecurity.com/2011/08/coordinated-atm-heist-nets-thieves-13m/>
- Keeney, M., Kowalski, E., Cappelli, D., Moore, A., Shimeall, T., and Rogers, S. (2005, May). *Insider threat study: Computer sabotage in critical infrastructure sectors*. United States Secret Service and CERT program. Report available at <http://www.secretservice.gov>
- Maggiore, P. D., & Doherty, J. (2003). *Cisco Networking Simplified*. Indianapolis: Cisco Press.
- McClure, S., Scambray, J., & Kurtz, G. (2009). *Hacking Exposed: Network Security Secrets and Solutions*. New York: McGraw-Hill.
- Microsoft Corporation. (n.d.). *IPv6*. Retrieved September 17, 2011, from: <http://technet.microsoft.com/en-us/network/bb530961.aspx>
- Mitnick, K. (2011). *Ghost in the Wires: My Adventures as the World's Most Wanted Hacker*. New York: Little, Brown and Company.
- Morris, D. A. (2005, May 3). *Tracking a Computer Hacker*. Retrieved September 19, 2011, from: [http://www.justice.gov/criminal/cybercrime/usamay2001\\_2.htm](http://www.justice.gov/criminal/cybercrime/usamay2001_2.htm)
- Nikkel, B. J. (2007). *An Introduction to Investigating IPv6 Networks*. Digital Investigation: The International Journal of Digital Forensics and Incident Response Vol. 4, No. 2. Oxford, England: Elsevier.
- Poulsen, K. (2011). *Kingpin: How One Hacker Took Over the Billion-Dollar Cybercrime Underground*. New York: Crown.
- Powell, S., Kraus, R., & Borkin, M. (2010). *Seven Deadliest Network Attacks*. Burlington, MA: Syngress.
- Scaphone, K., Grance, T., & Masone, K. (2008). *Computer Security Incident Handling Guide*. National Institute of Standards and Technology, Computer Security Division. Gaithersburg, TN: National Institute of Standards & Technology.
- TechTarget. (2000, August). *Intrusion Detection (ID)*. Retrieved September 17, 2011, from: <http://searchmidmarketsecurity.techtarget.com/definition/intrusion-detection>
- TechTarget. (2000, October). *Firewall*. Retrieved September 17, 2011, from: <http://searchsecurity.techtarget.com/definition/firewall>
- TechTarget. (2001, March). *Social Engineering*. Retrieved September 18, 2011, from: <http://searchsecurity.techtarget.com/definition/social-engineering>

- TechTarget. (2002, January). *Snort*. Retrieved September 17, 2011, from: <http://searchmidmarketsecurity.techtarget.com/definition/Snort>
- Vacca, J. R., & Rudolph, K. (2011). *System Forensics, Investigation, and Response*. Sudbury, MA: Jones and Bartlett Learning.
- Verizon Business Global LLC, & United States Secret Service. (2011). *2011 Data Breach Investigations Report*. Ashburn New York: Verizon Business Global LLC.

This page intentionally left blank

## CHAPTER 10

# Mobile Device Forensics

145

### Information in This Chapter:

- Cellular Networks and How They Work
- Overview of Cell Phone Operating Systems
- Potential Evidence Found on Cell Phones
- Collecting and Handling Cell Phones as Evidence
- Cell Phone Forensic Tools
- Global Positioning System Function and Potential Evidence

## INTRODUCTION

The phones riding on our hips and sitting in our pockets are true marvels of technology. These “mini-computers” are capable of delivering much of the same functionality that was once the lone province of desktops and laptops. We can browse the Internet, send and receive e-mail, shoot pictures and videos, and plot our location on a map, just to name a few of the possibilities.

Cell phones and other mobile devices can make a case airtight. Just ask Boise, Idaho’s Dan Kincaid. When the Boise police arrested Kincaid for burglary, they also seized and searched his Blackberry cell phone. It paid off. His e-mail contained several messages that would eventually help convince him to plead guilty. After being spotted, Kincaid e-mailed his girlfriend saying “Just trying to find a way out of this neighborhood without getting caught.” “Dogs bark if I’m between or behind houses ...” He went on to write, “Cops know I have a blue shirt on. ... I need to get out of here before they find me” ([Shachtmann, 2006](#)).

At their core, today’s smart phones are fundamentally computers with radios attached to them. There is an ever-evolving world of cell phone hardware with no slowdown in sight. Like their larger cousins, these small-scale devices can create artifacts that can be recovered and used as evidence.

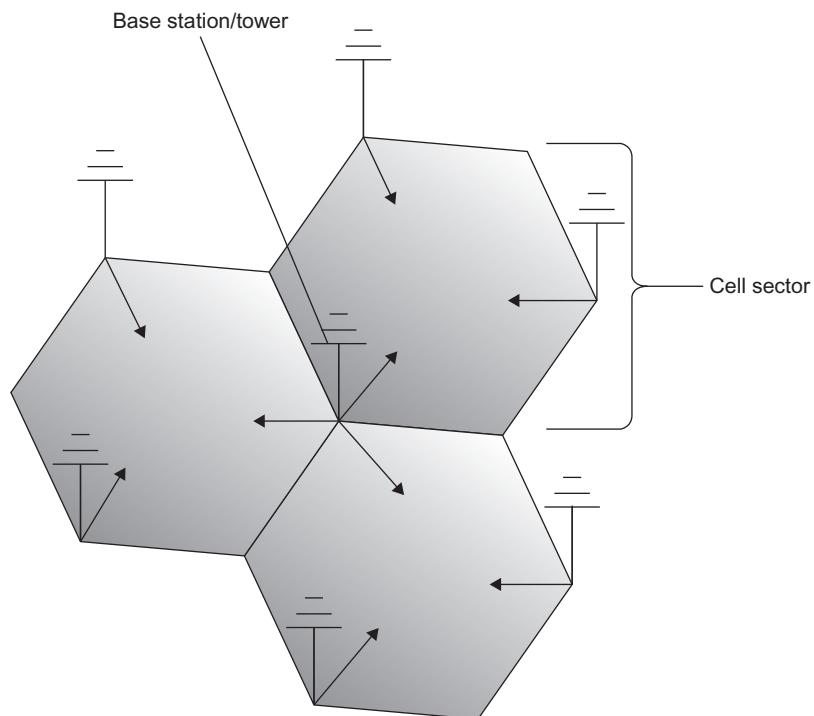
Cellular phones and other mobile devices present yet another challenge for examiners. Walk into any cell phone store and you’ll be confronted with a vast array of cell phone makes, models, and operating systems. The various devices

in turn support many different services and applications. To further complicate things, there is not an established hardware interface. You've likely run across this issue one time or another when you upgraded your phone. Odds are when you got a new phone you had to get a new charger and data cables as well. Keeping pace with the cabling, operating systems, and so on is quite a challenge. The good news is that this seems to be getting better, with many phones now including a mini-USB in their handsets.

## CELLULAR NETWORKS

Evidence can be located not just in the phone or memory card, but on the network itself. As examiners we need to understand the basic operation of cellular networks and the location(s) of any potential evidence.

As the name implies, each cellular network comprises individual cells. Each cell uses a predetermined range of frequencies to provide service to a distinct geographic area. The size and shape of each cell vary. In fact, they can vary wildly. They can cover a few city blocks in an urban environment to over a couple of hundred square miles in the country. The type of terrain, particularly obstructions, is the limiting factor; see [Figure 10.1](#).



**FIGURE 10.1**

The layout of a typical cellular network. (Illustration by Jonathan Sisson.)

The strength of the radio signal emitted from each cell is closely controlled. This is done purposefully to limit its range. By limiting the range, providers can reuse the relatively limited number of frequencies they have to work with.

Each cell has a base station that consists of an antenna (or mast) along with the related radio equipment. Together, they are known as a **cell site**. These cell sites deliver coverage to the individual cells. You've probably seen these large towers along the interstate for example or smaller ones on rooftops in more urban locations. Normally, each cell tower will have three panels per side. The middle panel is usually the transmitter, with the other two being receivers. The receiver panels constantly listen for incoming radio signals.

It may surprise you to know that the cell sites are not located in the center of each cell. They are actually located at the junction of multiple cells, facilitating service as subscribers move from cell to cell.

## Cellular Network Components

It takes quite a bit of infrastructure to get your phone call from that remote location back to your office downtown. Forensically speaking, each of these components could potentially provide information relevant to an investigation.

A **Base Station** consists of the antennas and related equipment.

A **Base Station Controller (BSC)** regulates the signals between base stations. This function is critical as phones move from place to place.

The **Mobile Switching Center (MSC)** processes calls within the network. As a key piece of the wireless network, the MSC holds a tremendous amount of possible evidence. It also coordinates calls between different wireless networks as well as land lines. The MSC handles SMS messages as well. The call detail records and logs are found here.

The **Visitor Location Register (VLR)** is a database that is linked to a MSC. All mobile devices currently being controlled by that MSC are recorded in the VLR. **Interworking Functions** serve as doorways outside data networks such as the Internet.

Information about individual subscribers is collected in the **Home Location Register (HLR)**. This information includes subscriber identification, billing, and the services they receive, along with the current location of the device. The HLR also stores encryption keys. The HLR supports the **Authentication Center (AuC)**, which is used to control access to the network. The AuC screens connections, blocking unauthorized users ([Jansen & Ayers, 2007](#)).

Text or SMS messages are the responsibility of the **Short Message Service Center (SMSC)**. Messages may be recovered from the SMSC, but there is no hard and fast rule dictating how long these messages must be kept by individual providers. It is up to the individual provider to determine how long that information is kept ([Jansen & Ayers, 2007](#)).

It's important to note that your cell phone is regularly communicating with the nearest cellular antennae, even if you're not talking on it. When you turn on your cell phone, it automatically begins searching for the nearest cell site. Once the antenna is found, the phone then transmits identification data so that the network can verify who you are and whether or not you have authorized access. This information would include things like the cell phone number along with the name of your service provider.

As you drive, your "connection" to the network must be transferred from cell tower to cell tower. This transfer is known as a "handoff." The handoff is made as the signal strength begins to fade. Not all handoffs are handled the same way. For instance, GSM (Global System for Mobile Communication) and Code Division Multiple Access (CDMA) for networks handle them differently. A GSM network uses what is known as a hard handoff. Here, the phone can only attach to one tower at a time. The conversation is separated from the current tower and passed to the new one. The phone will then switch to the new tower's frequency. In contrast, CDMA handoffs are considered "soft" handoffs. Here a phone can connect to multiple towers at once, utilizing the tower with the strongest signal.

Records showing when a certain phone is connected to a specific tower can be used to put someone (or more precisely their phone) in the vicinity of a crime or to establish an alibi.

Once your call hits the cell tower it's then transferred to the **Mobile Switching Center (MSC)**. If the call is destined for a phone that is out of the network, the MSC will pass the call to the **Public Switched Telephone Network (PSTN)**. The PSTN will then direct the call to its intended recipient.

We've all experienced dropped calls or a loss of signal at one time or another. One of the potential causes is dead spots. Dead spots can be caused by a gap in the cell coverage or obstructions to the signal. Cell phones are heavily dependent on having a clear and unobstructed (or very close to it) path to the cell tower. Obstructions can be tall buildings, mountains, and large trees.

Cell phones support two kinds of messaging services, **Short Message Service (SMS)** and **Multimedia Messaging Service (MMS)**. SMS are what we normally refer to as text messages. We get the name Short Message from the limitation of the maximum size of each message. SMS messages have a maximum length of 160 characters. MMS offers improved functionality over SMS. MMS messages aren't limited to 160 characters.

## Types of Cellular Networks

Cellular networks can be differentiated or defined in how they transmit data. These transmission schemes include **Code Division Multiple Access (CDMA)**, **Global System for Mobile Communications (GSM)**, and **Integrated Digitally Enhanced Network (iDEN)**.

### CODE DIVISION MULTIPLE ACCESS (CDMA)

CDMA was originally a military technology that was eventually released for use by the public. CDMA uses spread spectrum technology to transmit data. This technology permits several phones to send and receive through a single channel. Each part of these separate conversations is labeled with a specific digital code. The carriers that use CDMA technology include Sprint, Verizon, Alltel, and NEXTEL. CDMA phones typically do not utilize SIM cards. CDMA networks use an **Electronic Serial Number (ESN)** to identify individual handsets (Barbara, 2010).

### GLOBAL SYSTEM FOR MOBILE COMMUNICATION (GSM)

As the name suggests, GSM phones can be used internationally. GSM uses **Time Division Multiple Access (TDMA)** technology. Worldwide, GSM is the most widely used transmission mode. Unlike CDMA, GSM phones use SIM cards. GSM carriers include AT&T, Verizon, T-Mobile, and Cellular One. The **International Mobile Equipment Identity (IMEI)** is used to identify handsets (Barbara, 2011).

### INTEGRATED DIGITALLY ENHANCED NETWORK (iDEN)

iDEN, or Integrated Digitally Enhanced Network, provides two-way radio-like functionality, also known as "Push to Talk." Like GSM phones, they also utilize SIM cards. iDEN carriers include NEXTEL, Sprint, and Boostmobile.

### PREPAID CELL PHONES

At their core, prepaid phones operate like other cell phones in that they use radios to transmit data and must connect to a network. The difference with prepaid phones is that they create some significant investigative hurdles, particularly when trying to identify the subscriber. For one, they can be paid for completely with cash, essentially leaving little to nothing in the way of a paper trail. This makes identifying the purchaser much harder.

Like other cell phones, however, we can identify the area where the phone is being used as well as the calls that are sent and received. With prepaid phones, the information we're looking for will be held by two entities. The phone provider will hold any subscriber information, and the network provider will maintain the call detail records.

## OPERATING SYSTEMS

A phone's operating system (OS) has a significant impact on any forensic examination. The OS determines what artifacts are created and how they are stored. Modern cell phone operating systems include Symbian, Apple iOS, Windows CE and Windows Mobile, Google's Android, and Blackberry OS.

Originally, the Symbian OS was a product of a partnership between Nokia, Ericsson, Motorola, and Psion. Sony Ericsson rolled out the first Symbian-run phone in 2000. In 2008, Nokia bought the rights to the OS. Nokia recently made

Symbian open source. It's used today in Nokia and Sony Ericsson handsets (Barbara, 2010b).

**Blackberrys** were first introduced in 1999 by the Canadian company Research In Motion (RIM). Businesses and governmental entities are heavy Blackberry users. Blackberry phones synchronize with Novell's GroupWise and Microsoft's Exchange. As such, they are quite proficient in handling e-mail, calendars, and the like. The Blackberry OS supports multitasking as well as a variety of applications. This operating system is proprietary, and versions are specific to each carrier. That means that the Verizon version of a specific phone would be different than the AT&T edition (Barbara, 2010b).

**Android** is an open-source OS that is currently developed by Open Handset Alliance. In 2005, Google acquired the Android OS from Android, Inc. In 2007, the Open Handset Alliance was formed and has been developing the OS ever since. The Open Handset Alliance "is a group of 84 technology and mobile companies who have come together to accelerate innovation in mobile and offer consumers a richer, less expensive, and better mobile experience" ([Open Handset Alliance, 2007](#)). Some of the members include Sprint, T-Mobile, LG Electronics, Inc., Kyocera, Motorola, Google, and eBay. Thousands of third-party apps are available to augment Android's core functionality. Android is found on handsets produced by Motorola, Sony Ericsson, and HTC (Barbara, 2010b).

Apple's popular **iOS** can be found not only on the iPhone but also on other mobile devices such as the iPad and the iPod touch. iOS is based on Apple's Mac OS X, which is used on their laptops and desktops. iPhones make heavy use of third-party apps that are purchased/downloaded from the Apple App Store.

Windows Mobile is Microsoft's OS developed for the smart phone and mobile device market. Like its competitors, Windows Mobile also supports a huge array of apps.

## CELL PHONE EVIDENCE

Now that we've looked at how cell phones and networks function, we can look at some of the information they hold that may qualify as evidence. It's important not to focus on one source, as relevant evidence can be found in multiple locations within the handset and the network.

[Table 10.1](#) lists some of the potential evidentiary items found in modern smartphones.

**Table 10.1 Potential Smart Phone Evidence**

Call History	Text Messages	E-mail
Pictures & Video	Deleted Text Messages	Browser History
Contacts	Location Information GPS	Chat Sessions
Calendar	Voice Memo	Documents

The Personal Identification Number (PIN) is used to secure the handset. Three consecutive, unsuccessful attempts to enter the correct PIN will result in the user being locked out. The Personal Unlock Key (PUK) will be needed to unlock the SIM after this lockout has occurred. Typically, a PUK can only be supplied by the provider of the SIM card (Barbara, 2010).

You have probably noticed when typing an e-mail or text on your phone that many times the phone will complete words for you. This is called **predictive text**. Predictive text was developed to make texting easier on phones that lacked a full QWERTY keyboard. Those phones use three letters per key, forcing the user to "scroll" through the multiple letter options before selecting one. With predictive texting technology, the device attempts to predict the word most likely intended by the user. These guesses are based on a database dictionary containing thousands of words, names, abbreviations, slang, and so on (Mobile-phone-directory.org, 2009).

What is most interesting, from a forensic perspective is that these systems are capable of learning. Words, abbreviations, slang, and the like entered by the user is assimilated into the database. E-mail addresses and URLs can also be stored. If this database is recovered, it can produce some interesting evidence. For example, pedophiles could have routinely entered common abbreviations for child pornography (CP). A drug trafficker could routinely enter slang or a code word for their product when texting a buyer.

Several companies produce this technology. Some examples are Tegic Communication's, T9 ([www.T9.com](http://www.T9.com)), Motorola's iTap, and ZiCorp's eZiText (Kessler, 2011).

## Call Detail Records

**Call detail records (CDR)** are normally used by the provider to troubleshoot and improve the networks performance. The CDR is also valuable to examiners. They can show us:

- Date/time the call started and ended.
- Who made the call and who was called.
- How long the call lasted.
- Whether the call was incoming or outgoing.
- The originating and terminating towers.

Although the CDRs can tell you a lot, what they cannot tell you is who actually made the call.

You get what you ask for; therefore it is important to understand the difference between the CDR and the subscriber information. Subscriber information and the call detail records are not the same. Typical subscriber information would include things such as the name, address, and telephone. Other items included with subscriber information are account numbers, e-mail addresses, services, payment mechanisms, and so on.

Every service provider keeps all of these records for a predetermined period of time. The time period is spelled out in their data retention policies.

The retention period is also not uniform across all of the data types. For example, some carriers may keep SMS data for only seven to fourteen days. By contrast, cell sector information could be kept a year or longer. The takeaway here is that you don't have an unlimited amount of time to file the necessary paperwork to ensure that the records you seek won't get purged.

Carriers generally maintain meticulous records of subscribers and their activities for billing and other purposes. This stockpile of information can be enormously helpful during an investigation. These carrier records can tell us the subscriber's name, address, additional phone numbers, Social Security number, and so on. The credit information on file can give investigators billing addresses, credit card numbers, and more.

The **call detail records** describe the specifics of each incoming and outgoing call. These should not be confused with toll records. Toll records refer to land-line information rather than mobile phones. When asking for the call detail records, you must specify a date range. It's a wise practice to pad your request with a day or two on both ends.

The call detail records, when combined with the physical addresses of the towers, can show us the call's origination and termination locations. These records also show the cell sites that were used, the length of the call, the time the call began, the numbers dialed by the target phone, and so on ([Jansens & Ayers, 2007](#)).

The billing records do not represent a complete list of the inbound and outbound calls. The call logs will include data that have not yet made it into the billing system.

Information kept by the carriers will likely have a short, predetermined shelf life. Each carrier has some discretion on how these data are preserved and how long they're stored. This is usually described in the company's retention policies. In light of this practice, the legal paperwork should be generated and served sooner rather than later. This will help to ensure that your evidence won't get purged before it can be preserved and collected.

Cell phones can be located (with varying degrees of accuracy) by a few different means. **Triangulation** is one of the better-known methods. In triangulation, the phone's approximate location is determined using its distance from three different towers. The distance is calculated by determining the signal delay from the phone (or handset) to the three towers. A **directional antenna** can also be used for this purpose. Again, the signal delay is used to determine the distance, but this time only two towers are needed since they are able to also determine the direction. Finally, the location can be determined via GPS using latitude and longitude.

## Collecting and Handling Cell Phone Evidence

Because cell phone data are not unlike other forms of digital evidence, the fundamental principles in handling digital evidence apply to cell phones as well. Job one when dealing with cell phones is isolating it from the network. Isolating

**FIGURE 10.2**

A Faraday bag and cell phone.

the phone is imperative. Aside from the danger of being remotely wiped (by the suspect or carrier), any inbound calls, messages, or e-mails could overwrite any potential evidence. We can effectively isolate the phone using a Faraday or arson can. A Faraday bag, shown in Figure 10.2, is a special container constructed with conductive material that effectively blocks radio signals. An arson can is really nothing more than a clean, empty paint can. These containers can be found in hardware or home improvement stores.

If the phone is on when you recover it, leave it on. If there will be a significant delay in getting the phone to the lab, then you may want to consider turning it off. This is done to ensure that the battery doesn't completely drain. If it does, you run the risk of locking the phone. If the phone is protected with a PIN, turning the phone off will result in the phone being locked when it's turned back on.

Isolating the phone with the power on creates some concerns regarding the battery life. Remember, while the phone is on it will continually attempt to connect to the network, further draining the battery. A dead battery could also trigger the security function, locking up the phone.

If the phone is off, we can remove the battery as well as remove and initial the SIM card. We'll also want to photograph the phone, front and back. During this process, we'll want to pay particular attention to the identifying numbers

underneath the battery (the IMEI, ESN/MEID). We'll also want to isolate the phone from the network, just like a powered on phone.

Before conducting a forensic exam, it's important to identify the make and model of the handset you're dealing with. This information can help you get a full understanding of the phone's functions, features, and capabilities. The make and model of the phone can be typically found under the phone's battery. This same information can also be found in the phone's file system.

Like computers, we only want to access or examine the original evidence as an absolute last resort. Ideally, a forensic tool should be used to first acquire the data, giving the examiner a copy to work with. In the end however, a manual examination may be the only alternative. Should this be necessary, you will have to articulate your reasoning behind taking this course of action. Detailed documentation will be very helpful in accounting for your interaction with the device and establishing the integrity of any evidence that was recovered. Documenting a manual examination typically relies heavily on photographs as opposed to the digital evidence itself. In this instance, the examiner painstakingly navigates through the phone, taking photographs of the screens as he or she goes.

Voicemail is another potential source of evidence that shouldn't be overlooked. Typically, in order to access the voicemail, you will need the password-reset code from the carrier. When collecting voicemail evidence, there are a couple of options. The carrier can simply provide you with an access code or they can deliver you a copy of the data itself. This detail should be worked out early on with the provider, especially if you prefer one method or format to another.

At the scene, you should be on the lookout for additional handsets, SIM cards, and the related power and data cables. The power cable will help the lab ensure that the volatile memory is left intact until it can be properly collected and examined. Don't forget, while the phone is on, it will continually seek to connect with the network, rapidly draining the battery.

## Subscriber Identity Modules

**Subscriber Identity Modules (SIMs)** can be valuable evidence all by themselves. They store a vast amount of information and should be collected and analyzed.

The SIM contains a couple of numbers that will be of particular interest. The first is the **International Mobile Subscriber Identity (IMSI)**. The second is the **Integrated Circuit Card Identifier (ICC-ID)**. The IMSI is used to identify the subscriber's account information and services. The ICC-ID is the serial number of the SIM card itself. The SIM can contain:

- Subscriber Identification (IMSI)
- Service Provider
- Card Identity (ICC-ID)

- Language Preferences
- Phone Location When Powered Off
- User Stored Phone Numbers
- Numbers Dialed by the User
- SMS Text Messages (Potentially)
- Deleted SMS Text Messages (Potentially)

The SIM cards contain several individual components including a processor (CPU), RAM, Flash-based non-volatile memory, and a crypto-chip. They are used in all phones but are present in GSM, iDEN, and Blackberry handsets.

A **Personal Identification Number (PIN)** may be in place to protect the SIM data. PINs are four to eight digits in length. As an added layer of security, only three attempts may be made to enter the correct PIN. After the third unsuccessful attempt, the data can only be accessed with an eight-digit Pin Unblocking Key (PUK) along with a new PIN. Attempts to enter the PUK are also limited. After 10 failed attempts, many SIM cards will permanently deny access with a PUK.

### Cell Phone Acquisition: Physical and Logical

The data on a cell phone can be acquired in one of two ways: physically or logically. A physical acquisition captures all of the data on a physical piece of storage media. This is a bit-for-bit copy, like the clone of a hard drive. This acquisition method captures the deleted information as well. In contrast, a logical acquisition captures only the files and folders without any of the deleted data. Data can be collected using nonforensic tools such as those used to synchronize or back up the data on the cell phone ([Jansen & Ayers, 2007](#)). While this process is similar to the one used to acquire a hard drive, there is one important difference. In this instance no write blocking device is used. The phone must be able to interact with the phone's hardware and software.

A manual examination entails interacting with the device via the keypad or touch screen. Although examining or interacting with the original evidence is never our first choice, sometimes it may be the only option. For example, in cases where time is of the essence, it may be necessary to forgo proper forensic procedures. Those situations may include locating a missing child or preventing an imminent violent act of some sort. In other situations, it may not be possible to even mine the data or extract them in a way that would preserve their integrity. This could happen in cases where forensic tools and techniques hadn't caught up with the latest technology.

## CELL PHONE FORENSIC TOOLS

As you might suspect, there are many, many different tools available to forensically examine a phone. These tools can come in the form of hardware or software. One of the realties is that not all of these tools support all cell phones. To further complicate matters, two tools that actually support a given phone may not read and recover the same information.



**FIGURE 10.3**  
A Cellebrite UFED.

What follows is a sampling of the available tools for cell phone forensics. A close examination of the function and features shows that no single tool does it all. One glaring difference is the number of phones that are supported. Budget permitting, most labs will have multiple tools available to increase their capabilities. [Figure 10.3](#) shows a Cellebrite UFED device.

**BitPim** is a robust open-source application that was not built for forensic purposes. BitPim is designed to work with CDMA phones that are produced by several vendors, including LG and Samsung among others. BitPim can recover data such as the phonebook, calendar, wallpapers, ring tones, and file system (<http://www.bitpim.org/>).

**Oxygen Forensic Suite** is a forensic program specifically designed for cell phones. It's a tool that supports more than twenty-three hundred devices. It extracts data such as phonebook, SIM card data, contact lists, caller groups, call logs, standard and custom SMS/MMS/e-mail folders, deleted SMS messages, calendars, photos, videos, JAVA applications, and GPS locations (<http://www.oxygen-forensic.com/en/>).

**Paraben Corporation** offers several hardware and software products targeted to mobile device forensics. In addition to cell phones, their tools also support GPS devices such as those from Garmin (<http://www.paraben.com/handheld-forensics.html>).

**AccessData's MPE+** supports over thirty-five hundred phones. It's an on-scene, mobile forensic recovery tool that can collect call history, messages, photos, voicemail, videos, calendars, and events. It can analyze and correlate multiple

phones and computers using the same interface. (<http://accessdata.com/products/computer-forensics/mobile-phone-examiner>).

The Cellebrite UFED (Universal Forensic Extraction Device) is a stand-alone, self-contained hardware device used to extract Phonebook, images, videos, SMS, MMS, call history, and much more. It supports over twenty-five hundred phones and is designed to extract information on scene. It also has a SIM card reader and cloner. As an interesting aside, Cellebrite devices (the nonforensic version) can be found in many cell phone stores. They're used to transfer a customer's data from one device to another. (<http://www.cellebrite.com/forensic-products/forensic-products.html?loc=seg>).

EnCase Smartphone Examiner is an EnCase tool designed to review and collect data from smartphones and tablet devices. It collects data from Blackberries, iTune backups, and SD cards. Once the information is collected, it is easily imported into the EnCase Forensic suite for continued investigation (<http://www.guidancesoftware.com/encase-smartphone-examiner.htm>).

So, what do you do if none of these tools will retrieve the information you're looking for? If that's the case, it's time to consider going "old school" and simply using a still or video camera. Although this would not be the first choice, it's better than coming away empty-handed.

## GLOBAL POSITIONING SYSTEMS (GPS)

Like cell phones, Global Positioning Systems (GPS) can be a tremendous source of evidence. They can be used to pinpoint the location of suspects as well as the criminal acts themselves (if the device was active and in their possession at the time the crime was committed). They can also be used to show where suspects intended to go. Some GPS units can provide a great deal more evidence, including mobile phone logs, SMS messages, and images. Given these capabilities along with large storage capacities, examining these devices is well worth the time.

The GPS was originally produced for military use but was eventually shared with everyone. There are twenty-seven GPS satellites in the GPS system. Only twenty-four are in use at a time. The remaining three are held in reserve in case one of the primary satellites goes down. A GPS receiver calculates its position through a mathematical process known as trilateration (Brian & Harris, 2011).

Not all GPS units are the same. Some are feature rich, whereas others are pretty basic. We can separate GPS devices into four categories: simple, smart, hybrid, and connected. Simple units are designed to get users from one point to another. Most simple units can store **trackpoints**, waypoints, and **track logs**. Other features may be present depending on the make and model (LeMere, 2011).

Smart units can be broken down into automotive and USB mass storage devices. These units typically have 2GB of storage at a minimum along with an SD card. They provide the same base functionality as the simple systems. In addition, they can play MP3s, view pictures, and save favorite places.

Hybrid GPS units are feature rich and can provide a great deal of evidence. Hybrid devices possess the same features as smart devices plus some. Most notably, these devices provide hands-free access to your mobile phones via Bluetooth. This ability to interact with the cell phone can provide a secondary source of much of the data found on the phone. This would include call logs, an address book, as well as the MAC address of up to ten of the last phones that have connected to the unit. Finally, SMS messages can also be recovered ([LeMere, 2011](#)).

A connected unit provides hybrid features and the ability to get real-time information including Google searches and traffic information. These units have GSM radios along with SIM cards. This functionality is subscription based and as such, we may be able to obtain the subscriber information associated with the account.

GPS data can be grouped into two categories: system data and user data. System data will provide us with trackpoints and a track log. Track points are a record of where the unit has been. They are automatically created by the system. Trackpoints can't be altered by the user. By default, the system determines the interval at which they are recorded. Users can however modify this setting, changing the time or distance interval. The **track log** is a comprehensive list of all trackpoints. This list is intended to help users retrace their path ([LeMere, 2011](#)).

**Waypoints** are part of the user-created data. When interpreting a waypoint, you need to keep in mind what they represent. Unlike a trackpoint, waypoints don't always indicate the physical locations where the unit has been. They can be places the user intends to visit. The user can enter these locations based on the address, the actual coordinates, or from a list of Points of Interest (POI) supplied by the GPS unit manufacturer.

GPS devices are similar in many respects to cellular phones and are handled in much the same way. They can have volatile memory that may need to be preserved. When powered on, these units are constantly interacting with the satellites above. This interaction can cause complications from a forensic perspective, potentially causing relevant evidence to be overwritten or compromising its integrity.

GPS devices are cropping up in many different places. Taxi cabs, delivery trucks, and more are frequently being outfitted with GPS units. One such example of a GPS unit assisting investigators is the case of Las Vegas dancer Debbie Flores-Narvaez. The brutal December 2010 murder showed the value of GPS evidence. Police were able to locate her dismembered remains using GPS data from a U-Haul truck. The suspect, Jason "Blu" Griffith, apparently transported her remains in the truck and was unaware that the truck was equipped with GPS. Police obtained the GPS data and used them to retrace Griffith's movements, leading to her body.

Evidence in the case also included text messages. The victim's mother, Elise Narvaez, said that her daughter sent her this text message on December 1, 2010: "In case there is ever an emergency with me, contact Blu Griffith in Vegas. My ex-boyfriend. Not my best friend" ([Hartenstein & Sheridan, 2010](#)).

### Q&A with Christopher Vance

Christopher Vance is a Digital Forensic Specialist assisting the West Virginia State Police Digital Forensics Unit. In the Q&A here, he shares some of his insights from the trenches.

- [Q] What do you see as the biggest forensic challenges when dealing with cell phones?
- [A] Vance: The single biggest challenge when dealing with cell phone forensics is that there are thousands of phones, each with different operating systems. There is such a wide variety when dealing with mobile devices it is impossible to be well versed in every single operating structure. It is a constant learning process by trial and error and validation.
- [Q] What advice would you give a new examiner wanting to learn more about cell phones?
- [A] Vance: There's a lot of training opportunities out there, especially for law enforcement. However, even with the best of trainings, it's absolutely key to get your hands on some devices and try it for yourself.
- [Q] How important is continuing education?
- [A] Vance: In this field, it's probably the most important thing there is.
- [Q] How are you seeing cell phones used in the commission of crimes?
- [A] Vance: Depending on the type of case, there's a variety of ways they're being used. However, the biggest pieces of evidence usually trace back to the SMS/MMS messages, stored images, and Call Logs. From drug trafficking, to solicitation, to murder, these always seem to be the biggest key to the case if the evidence exists on the handset.
- [Q] Can you talk a little about the general process you follow when conducting an examination?
- [A] Vance: The two largest keys are Isolation and Validation. The first step is always to isolate your device from its network and keep it that way until the case is completed. Then using a variety of tools and processes (as there is no "super tool" that works on every device) I will collect the data. After the data are collected, I attempt to validate the data either by using multiple tools, hash values, or even visual validation while checking the data against what the phone is saying.
- [Q] What other mobile devices are you seeing brought to the lab? What kind of evidence are you recovering from those?
- [A] Vance: The two biggest mobile devices outside of cell phones are iPod Touch devices and Tablets. Seeing as these devices can run the same operating systems as their cell phone counterparts, we can usually pull about the same. In most cases, it's usually chat logs from third-party applications installed on the devices, i.e., Skype, TextNow, Yahoo!, etc.
- [Q] From your perspective, what does the future hold for cell phone forensics?
- [A] Vance: Hopefully the "dumb-phone" will either die or become assimilated. If the major **smartphone** operating systems can take over the forefront and standardize the market a little, it will make analysts' and engineers' jobs much easier. It's my opinion that one day we'll talk about mobile device operating systems the same way we mention the "big three" of Mac, Windows, and Linux.
- [Q] Can you talk a little about the tools you use?
- [A] Vance: I use a lot of tools to get the job done. There's not one tool that will hit every phone every time and pull all the data. It just does not exist. In our lab we

use the Cellebrite UFED Physical Pro, AccessData's Mobile Phone Examiner+, Paraben Corporation's Device Seizure, viaForensic's viaExtract, LogicCube's CellDek, Flasher Boxes, and a handful of other niche tools that are used from time to time.

**[Q]** Do you have a couple of "war stories" you can share?

**[A]** Vance: There have been a couple of cases I've worked where mobile device evidence has proven to be the smoking gun. Recently, in a murder investigation, there were multiple messages on a phone from the suspect to victim not only informing the victim the suspect was planning on murdering her but even saying when and how the crime would take place.

After the crime, the suspect even used the victim's phone to send out messages to other individuals confessing his guilt. In a solicitation case, we had a single iPod Touch, which we found evidence of not just one crime in the chat logs, but several victims of the same crime all by a single individual. I've even had cases where the individuals will store their entire Child Pornography libraries on the memory in their phones.

**[Q]** Are there misconceptions you would like to shoot down?

**[A]** Vance: Mainly what we refer to as the "CSI Effect." The job is never as fast or as glamorous as the TV shows make it out to be. In many cases, our job is sometimes as much an art as a science. When dealing with mobile devices, the memory that we have to analyze is so small and dynamic that it is much harder for us to recover deleted data in many cases. However, it's not impossible.

**[Q]** How would you compare and contrast the evidence you're finding on phones to that which is typically found on computers?

**[A]** Vance: The data actually play hand in hand. There have been many cases where we can see a chat log start on a computer and then carry over to a mobile device. A lot of times we still see the same types of data, mainly communications and user generated media. It is a lot easier to recover deleted information from a computer than it is a cell phone, however.

**[Q]** How big a role has geolocation data played in your investigations?

**[A]** Vance: There are so many issues with geolocation data that they haven't played a huge role to date. There have been investigations where we have found images with GPS data embedded to assist the investigators. The GPS "tracking" debates<sup>1</sup> of earlier this year were by and large unnecessary. While the GPS data can assist a case, it would take serious validation to make sure that the records you had were exactly what you were looking for. Just because you have geolocation points is not a 100 percent indicator your individual is in that exact point and location.

**[Q]** Anything else you would like to add?

**[A]** Vance: Cell Phone or Mobile Forensics is becoming its own specialization within the digital forensics field. I can easily see that this new wave of technology will one day replace our older machines in the same way the "Cloud" threatens to do.

---

<sup>1</sup> Researchers discovered that the iPhone or 3G iPad—anything with 3G data access—are logging location data to a file called consolidated.db with latitude and longitude coordinates and a timestamp.

## SUMMARY

Our mobile technology allows us to check e-mail, browse the Internet, plot out a road trip, and instantly access other people in our lives. Many people can't remember when or even imagine how they made it through the day without their smartphone. The advent of this technology has created both sources of evidence and challenges for forensic examiners.

In Chapter 10, we covered a wide range of topics on mobile devices, particularly cellular phones and GPS units. Cell networks are comprised of several components including base stations, Mobile Switching Centers, Visitor Location Registers, and others. There are different types of cell networks, each with their own unique characteristics. Code Division Multiple Access (CDMA), Global System for Mobile Communications (GSM), and Integrated Digitally Enhanced Network (iDEN) are the most common.

Like computers, there is more than one operating system used by cell phones. Windows Mobile, iOS, Android, and Symbian were covered in Chapter 10. Cell phones can contain vast amounts of digital evidence including e-mail, call logs, text messages, images, videos, and more.

Records maintained by the carrier can also be valuable during an investigation particularly the Call Detail Records. These records can provide us with dates, times, phone numbers, as well as the originating and terminating towers used during a call. The tower information can help us determine the general vicinity in which the phone has been used.

How cell phone evidence is collected and preserved is critically important. The first priority in dealing with any mobile device is to isolate it from the network. A powered on device that isn't isolated is a major problem. In this state, evidence can be changed, overwritten, or destroyed. Keep in mind that certain cell phones can be wiped remotely by the suspect or the carrier. Isolating a cell phone can be done using a Faraday bag or an arson can. While Subscriber Identity Modules or SIM cards contain data worth examining, it's important to remember that not all phones will have them.

GPS or Global Positioning Systems are in wide use today and function as another source of digital evidence. There are different types of GPS units including simple, smart, hybrid, and connected. Waypoints, trackpoints, and track logs are some of the data recorded by the units that we can use. These artifacts can tell us where the unit has been and where a user intended to go.

## References

- Barbara, J. J. (2010, October 17). *Understanding the World of Cellular Telephones: Part 1*. Retrieved November 13, 2011, from Forensicmag.com: <http://www.forensicmag.com/article/understanding-world-cellular-telephones-part-1?page=0,1>
- Barbara, J. J. (n.d.). *SIM Forensics: Part 1*. Retrieved September 19, 2011, from: <http://www.forensicmag.com/article/sim-forensics-part-1>

- Barbara, J. J. (n.d.). *Sim Forensics: Part 2*. Retrieved September 19, 2011, from: <http://www.forensicmag.com/article/sim-forensics-part-2>
- Barbara, J. J. (n.d.). *SIM Forensics: Part 3*. Retrieved September 18, 2011, from: <http://www.forensicmag.com/article/sim-forensics-part-3>
- Barbara, J. J. (n.d.). *Understanding the World of Cellular Telephones: Part 1*. Retrieved September 21, 2011, from: <http://www.forensicmag.com/article/understanding-world-cellular-telephones-part-1>
- Barbara, J. J. (n.d.). *Understanding the World of Cellular Telephones: Part 2*. Retrieved September 21, 2011, from: <http://www.forensicmag.com/article/understanding-world-cellular-telephones-part-2>
- Barbara, J. J. (n.d.). *Understanding The World of Cellular Telephones: Part 3*. Retrieved September 21, 2011, from: <http://www.forensicmag.com/article/understanding-world-cellular-telephones-part-3>
- BitPim. (n.d.). *BitPim*. Retrieved September 22, 2011, from: <http://www.bitpim.org/>
- Brian, M., & Harris, T. (n.d.). *How GPS Receivers Work*. Retrieved September 14, 2011, from: <http://electronics.howstuffworks.com/gadgets/travel/gps.htm>
- Casey, E. (2009). *Handbook of Digital Forensics and Investigation*. Burlington, MA: Academic Press.
- Casey, E. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*. Waltham, MA: Academic Press.
- Hartenstein, M., & Sheridan, M. (2010, December 21). *Missing Vegas Showgirl Debbie Flores-Narvaez was Pregnant, Beaten by her ex, According to Police*. Retrieved September 25, 2011, from: [http://articles.nydailynews.com/2010-12-21/news/27085062\\_1\\_license-plates-cell-phone-police](http://articles.nydailynews.com/2010-12-21/news/27085062_1_license-plates-cell-phone-police)
- Hoog, A. (2010, April 30). *An Introduction to Android Forensics*. Retrieved September 2011, 2011, from: <http://www.dfinews.com/article/introduction-android-forensics?page=0,0>
- Hoog, A. (2011). *Android forensics: Investigation, Analysis and Mobile Security for Google Android*. Waltham, MA: Elsevier.
- Jansen, W., & Ayers, R. (2007). *Guidelines on Cell Phone Forensics*. Gaithersburg, TN: National Institute of Standards and Technology.
- Kessler, G. C. (2011, June). *Cell Phone Analysis: Technology, Tools, and Processes*. Retrieved September 12, 2011, from: [http://www.garykessler.net/presentations/CellPhone\\_201106\\_ICAC-sanitized.pdf](http://www.garykessler.net/presentations/CellPhone_201106_ICAC-sanitized.pdf)
- LeMere, B. (n.d.). *Enhancing Investigations with GPS Evidence*. Retrieved September 15, 2011, from: <http://www.forensicmag.com/article/enhancing-investigations-gps-evidence>
- LeMere, B. (2011, April 25). *Enhancing Investigations with GPS Evidence*. Retrieved September 15, 2011, from: <http://www.forensicmag.com/article/enhancing-investigations-gps-evidence>
- Mobile-phone-directory.org. (n.d.). *Predictive Text Input*. Retrieved September 17, 2011, from: [http://www.mobile-phone-directory.org/Glossary/P/Predictive\\_Text\\_Input.html](http://www.mobile-phone-directory.org/Glossary/P/Predictive_Text_Input.html)
- Morrissey, S. (2010). *iOS forensic analysis: for iPhone, iPad, and iPod Touch*. New York: Apress.
- Open Handset Alliance. (2007, November). *FAQ*. Retrieved September 19, 2011, from: [http://www.openhandsetalliance.com/oha\\_faq.html](http://www.openhandsetalliance.com/oha_faq.html)
- Shachtman, N. (2006, May 3). *Fighting Crime With Cellphones' Clues*. Retrieved September 19, 2011, from: <http://www.nytimes.com/2006/05/03/technology/techspecial3/03cops.html>

## CHAPTER 11

# Looking Ahead: Challenges and Concerns

163

### Information in This Chapter:

- Standards and Controls
- Cloud Forensics
- Solid State Drives
- Speed of Change

## INTRODUCTION

Digital forensics is still in its infancy. It is very much a work in progress given its relatively short existence as well as the rapid rate of technological change. This work in progress status is likely to carry on for quite some time. This situation results in many challenges and controversies that the legal and forensic communities must wrestle with. The challenges are many. One such challenge is wrestling with emerging and potentially “game changing” technology. Another is reaching a consensus with the forensic science community at large, particularly when it comes to established best practices.

Digital forensics is causing a massive collision if you will, between two seemingly unyielding forces: the legal system and forensic communities that operate at a relatively slow and deliberate pace versus the blinding speed of technology. Neither is built for speed. There are good reasons for that. The stakes are far too high to admit forensic evidence that hasn’t been proven reliable. This proven reliability takes time and can’t be achieved over night.

Two technologies, cloud computing and solid state hard drives, present “game changing” challenges. As it stands, digital evidence in either of these environments could very well be unrecoverable for either technical or legal reasons (or both). These technologies are in use today and represent a problem to which there is no easy answer. How all of these challenges will be met has yet to be seen.

## STANDARDS AND CONTROLS

Standards and controls are a fundamental part of scientific analysis, including forensic science. A **standard** is “a prepared sample that has known properties that is used as a control during forensic analyses” (Barbara, 2007).

A **control** is defined as “a test performed in parallel with experimental samples that is designed to demonstrate that a procedure is working correctly and the results are valid” (Barbara, 2007). In essence, a control is simply a sample that provides a known result.

That may hold true for serology, chemistry, toxicology, and the like, but its relevance to digital forensics is a matter of dispute. More traditional forensic scientists are taking the stance that standards and controls are essential for all forensic disciplines, including digital and multimedia forensics. One of the major digital forensic bodies, the Scientific Working Group on Digital Evidence (SWGDE), is taking the exact opposite position. The controversy began with an article on Forensicmag.com in 2007 by John Barbara. In the article, Barbara raised the issue of standards and controls in digital forensics. He is a Crime Laboratory Analyst Supervisor with the Florida Department of Law Enforcement (FDLE). He is also an ASCLD/LAB inspector and has been since 1993. In the article he laid out his case citing the mandatory use of standards and controls in every other forensic discipline. He argued that the use of standards and controls is necessary to prove that the tests were performed in a scientific manner and that quality assurance measures were followed.

In the end, closely following these established scientific practices ensures that any results gained are accurate, reliable, and repeatable. He further argued that without the use of standards and controls, it would be “extremely difficult or impossible to scientifically assess the validity of the results obtained from the analysis of the physical evidence” (Barbara, 2007). Finally, he raised the admissibility standards required by the *Daubert* case.

In *Daubert*, the court said that when considering the admissibility of any scientific evidence, the focus should be on the principles and methodology and not on the conclusions that they generate.

The **Scientific Working Group on Digital Evidence (SWGDE)** doesn’t agree. Their position is that standards are being used in digital forensics, but controls are “not applicable in the computer forensics sub-discipline” (Scientific Working Group on Digital Evidence, 2008).

SWGDE’s position centers on false positives. They say that false positives do not exist in computer forensics. Tools and processes may miss evidence, but they will never find evidence that doesn’t exist. The main objective of any digital forensic examination, says SWGDE, is to find data relating to criminal activity that already exists. Therefore, there is no real value to the analysis or the results.

They conclude by saying that “validation, data integrity (through hashing), and performance verification” are a more appropriate solution than the traditional

use of standards and controls (Scientific Working Group on Digital Evidence, 2008).

SWGDE agrees, saying “New technology, typically proprietary in nature, emerges daily. As these new technologies emerge, new solutions and techniques are needed to understand and examine evidence. Comprehensive understanding and validated techniques need to move swiftly from the research community to the examiner community” (Scientific Working Group on Digital Evidence, 2008).

## CLOUD FORENSICS (FINDING/IDENTIFYING POTENTIAL EVIDENCE STORED IN THE CLOUD)

Cloud computing is a hot topic in information technology. The many benefits it brings are undeniable and not lost on organizations across the globe. As such, it's being widely adopted. The cloud, however, is a double-edged sword, and a sharp one at that. With its many benefits come major challenges from both forensic and legal perspectives.

### What Is Cloud Computing?

There are many definitions of **cloud computing** from which to choose. TechTarget describes cloud computing as “a general term for anything that involves delivering hosted services over the Internet” (TechTarget, 2007). These hosted services generally fall into a few different categories including:

- Infrastructure as a Service (IaaS).
- Software as a Service (SaaS).
- Platform as a Service (PaaS).

The term “cloud computing” is derived from the “cloud” symbol that is normally used in network diagrams to represent the Internet.

The National Institute of Standards and Technology (NIST) provides a more complex definition. They define the cloud this way: “Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction” (Mell & Grance, 2011).

Not all clouds are the same. There are **private clouds** and public clouds. **Public clouds** sell services on the open market. Technology behemoths such as Microsoft (Azure), Amazon (Amazon Web Services), Rackspace, and Google are just some of the major players in the cloud market. These **Cloud Service Providers**, or **CSPs**, can have data centers scattered around the world.

The cloud model relies heavily on virtualization and redundancy. TechTarget defines virtualization this way: “**Virtualization** is the creation of a virtual (rather than actual) version of something, such as an operating system, a server, a storage device or network resources” (TechTarget, 2000).

## ADDITIONAL RESOURCES

### Public Clouds

To get a closer look at how public cloud services are sold and managed, visit some of these providers.

<http://www.microsoft.com/en-us/cloud/default.aspx?fbid=XBzeu9E4wgy>  
<http://aws.amazon.com/>  
<http://www.rackspace.com/cloud/>

## The Benefits of the Cloud

Recognizing the many benefits of the cloud, companies and other organizations are flocking there in droves. They are seeking both the convenience and cost savings this computing model offers. The ability to essentially “dial-up” computing resources as needed is hard not to like. With the cloud, an organization’s infrastructure can expand and contract as needed. From a cost perspective, this approach can save a significant amount of money. Companies can save on much of the initial investment for network hardware and software.

Having the data or services replicated in more than one data center provides redundancy. The redundant nature of the cloud ensures that the user’s files and/or applications are safe and available whenever they need them. Should one center or its connectivity go down, the second should be able to respond.

## Cloud Forensics and Legal Concerns

The cloud may be a dream come true for those in business and information technology, but it represents a nightmare for those who deal with digital evidence. The primary challenges are twofold, one technical and the other legal. Technically, the cloud is without question not a forensically friendly environment, especially when compared to the relatively cozy confines of magnetic drives. Pulling deleted data from traditional drives has long been a staple of digital forensics. The cloud will likely be putting that to an end. Deleted files on a magnetic drive remain on the disk until they are overwritten. In the cloud, when a file is deleted the mapping is removed immediately, usually within a matter of seconds. This means that there is no remote access to the deleted data. As is the case with magnetic drives, that space is now available and will likely be overwritten in the cloud (Ruan, Carthy, Kechadi, & Crosbie, 2011).

There is an alarming lack of established forensic tools and procedures for acquiring and analyzing digital evidence in the cloud. Current tools and methodologies are largely ineffective in this environment. Much more research needs to be done.

**ALERT!****Cloud Persistence—Dropbox**

As many challenges as cloud functionality presents, in certain instances it can work in our favor. For example, Dropbox saves all deleted files (by default) for thirty days.

Dropbox's "Pack-Rat" service can keep data indefinitely (with the Pack-Rat add on). Granted, you will need a subpoena or search warrant to get to it, but the fact that it could be available is nice to know (Dropbox, 2011).

Legally, dealing with multiple jurisdictions can significantly frustrate efforts to get to the relevant data in the first place. As we've seen, CSPs can have their data centers located almost anywhere in the world. Legal requirements and procedures can vary, and vary considerably from country to country, and from jurisdiction to jurisdiction. This problem compounds exponentially if the data have crossed international boundaries.

Regulation could assist in mitigating this issue. It could help by mandating that CSPs operate in such a way that facilitates the preservation and recovery of potentially relevant data. Service Level Agreements, or SLAs, can also make a difference. An SLA is a written agreement between a customer and a provider. The SLA spells out in great detail what support and services the customer will get from the provider. As part of that agreement, the customer can require certain assurances regarding information security and how digital evidence will be preserved and collected should that ever become necessary. From a customer's perspective, this is an important detail that shouldn't be overlooked. This is particularly true in organizations where litigation is likely. Having this arrangement in place can be very beneficial to the forensic examiner, especially as opposed to starting from scratch with no protocols, procedures, or relationships in place.

## SOLID STATE DRIVES (SSD)

Magnetic drives have been a mainstay in personal computers for years. Forensically, they afford examiners the ability to recover significant amounts of user-deleted data. Those days, it appears, may very well be coming to an end. These traditional magnetic drives are being replaced more and more. Welcome to the era of solid state hard drives (SSD).

### How Solid State Drives Store Data

Traditional magnetic drives have multiple moving parts including the platters and the actuator arm (that moves the read/write head). As the name implies, solid state drives do not. SSDs are somewhat similar to RAM and USB thumb drives, storing data in tiny transistors. Unlike RAM, SSDs are nonvolatile and can store data even without power. In order to keep the charge over long periods of time, without power, SSD transistors employ an additional gate (called a floating gate), which is used to contain the charge (Bell & Boddington, 2010).

If you recall from Chapter 2, magnetic drives break the storage space up into smaller units. These units include sectors, clusters, and tracks. SSDs also separate the storage space into smaller units. The base units are called blocks and are normally 512 KB in size. Blocks are then subdivided into even smaller units called pages. Each page is typically 4 KB in size.

Wear is a concern with SSDs. Each block can only withstand a certain number of writes. Some estimates put that number somewhere between one thousand and ten thousand times. Given this limitation, you would want the drive to avoid writing to the same block over and over. Writing to the same space repeatedly will cause it to wear out faster than others. Manufacturers solved the issue by instituting a **wear leveling** process performed by the SSD.

### MORE ADVANCED

#### File Translation Layer

On a solid state drive, the computer thinks the data are stored in one location, while in reality they are physically located in another. An SSD drive uses a File Translation Layer to ensure that the computer isn't writing to the same block over and over. If the SSD detects this is occurring, it will "translate" the new writes to a less used location (Bell & Boddington, 2010).

Magnetic drives have the ability to instantly overwrite data to any sector that's labeled as unallocated. SSDs do not. Each transistor must be "reset" (erased) before it can be reused. This reset process slows down the drive. To speed things up, SSD manufacturers have configured the drive's controller to automatically reset unused portions of the drive. This process is known as **Garbage Collection**.

### The Problem: Taking out the Trash

Solid state drives have a mind of their own. Many drives initiate the Garbage Collection routine completely on their own, without any prompting by the computer at all.

This is both problematic and troubling from the perspective of the forensic analyst. First, verifying the integrity of the evidence becomes extremely difficult and jeopardizes its admissibility in court. Second, there is the automated destruction of potentially relevant data on the drive. If the Garbage Collection routine is run during or after its acquisition, validation becomes exponentially more difficult because the hash values won't match.

Today, we routinely use cryptographic hashing algorithms, such as MD5 or SHA1, to take the "digital finger print" or "digital DNA" of a hard drive. We can then retake the "fingerprint" of our clone at any time and compare it with the "fingerprint" of the original. They should match exactly, verifying the integrity of the evidence (Bell & Boddington, 2010).

## SPEED OF CHANGE

You may have noticed that the speed of technological change is a recurring theme throughout this book. Its impact is truly significant and felt across both the digital forensics and legal communities. It also impacts the organizations that rely on the results such as law enforcement and private companies. Take case backlogs, for example. In most if not all laboratories there is a significant backlog of cases including those involving digital evidence. Change contributes to this backlog by slowing down the examination process. Take an updated application such as a chat client. There can be major differences in where and how the software stores the artifacts examiners need to locate and analyze. Artifacts that may have been written to the registry in a previous version are now held exclusively in RAM and disappear when the machine is powered down.

Examiners presented with this situation will have to attempt to find a proven solution from others in the digital forensics community. Failing that, the examiner may have to conduct the research on their own and validate the results. This takes time. Message boards (such as the one for HTCIA members) and e-mail lists are worth their weight in gold in these circumstances. They provide a ready channel for communication and problem solving.

## ADDITIONAL RESOURCES

### Twitter

Twitter can be a great resource for digital forensic professionals. It can alert you to new techniques, research articles, court decisions, news, and more. There are many individuals and companies that share a great deal of news and information pertaining directly to digital forensics. Today we are bombarded with information, some good and some bad. Following well known, established entities on Twitter can help reduce the “noise” and help keep you current. This is one tool that can help you deal with the speed of change. These are just a sampling of the people and companies worth following.

### Digital Forensics

Vendors/Organizations	Individuals
@AccessDataGroup	@robtleee
@EnCase	@jtrajewski
@sansforensics	@girlunallocated
@DFMag	@keydet89
@HTCIA	@codeslack
@MFITraining	@4n6woman
@cellebrate USA	@AppleExaminer
@syngress	@chadtilbury @hal_pomeranz @4cast @CyberCrime101

(Continued)

(Continued)

**Electronic Discovery**

Vendors/Organizations	Individuals
@DiscoverTERIS	@sharonnelsonesq
@EDDUpdate	@RalphLosey
@e_discoverynews@KrollOntrack	@EUdiscovery@InfoGovernance
@Clearwell	@ComplexD
@PosseList	

## SUMMARY

Digital forensics faces many tests on the road ahead. The blinding speed of technology, new game-changing technologies such as cloud computing and solid state hard drives, and disagreements with established forensic disciplines, just to name a few. The constant, relenting pace of technology hits the DF community hard as it fights to keep pace. The speed of change affects the legal system as well. The system itself is not “built for speed” in general and certainly not for the speed of technology. The end result is that in certain situations, previously tried-and-tested tools and protocols will be ineffective. The research, development, and testing needed to solve the problem takes time.

Delivering services over the Web, cloud computing’s bread and butter, represents a major shift away from the computing model that the world has grown accustomed to. Remote applications, hardware, platforms, and infrastructure have a great many benefits; reduced costs and elasticity are just two. Behind the scenes, the cloud relies heavily on virtualization and redundancy. The massive data centers used to deliver public cloud services are likely to be widely dispersed, residing in multiple states or even different countries. Meeting the legal requirements to gain access to this data can take an astronomical amount of time. It’s entirely possible that by the time the legal burden is met, the evidence in question may no longer exist.

Solid state hard drives are another game-changing technology that must be addressed. These devices may serve the same function as our familiar magnetic drives, but they certainly don’t act like them. The storage method they use, tiny charged transistors, must be “reset” before being written to. This process slows down the drive, impacting performance. To mitigate the slowdown, drive makers have built in a process known as Garbage Collection. This process begins this reset process in only minutes. This procedure destroys data on the drive in such a way that current tools and techniques cannot recover it.

Digital evidence and its associated forensic processes are sometimes radically different from other, established disciplines. Bedrock forensic practices such

as the use of standards and controls are found to be meaningless to some in the digital forensics community. Those opposed say that unlike serology and toxicology, it simply isn't possible to get a false positive result from a digital forensic examination. The tool, they say, may miss some evidence, but it will never find evidence that wasn't already there.

These are just a few of the significant challenges faced by front-line practitioners. There is much work to be done if these challenges will be met.

## References

- Bell, Graeme B., Boddington, Richard (December 2010). *Solid State Drives: The Beginning of the End for Current Practice in Digital Forensic Recovery?* Journal of Digital Forensics, Security and Law.
- Mell, P., & Grance, T. (2011, January). *The NIST Definition of Cloud Computing*. Retrieved October 9, 2011, from: [http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145\\_cloud-definition.pdf](http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf)
- Microsoft Corporation. (n.d.). *IPv6*. Retrieved September 17, 2011, from: <http://technet.microsoft.com/en-us/network/bb530961.aspx>
- Ruan, K., Baggili, I., Carthy, J., & Kechadi, T. (n.d.). *Survey on Cloud Forensics and Critical Criteria for Cloud Forensic Capability: A Preliminary Analysis*. Dublin, Ireland: University College Dublin.
- Ruan, K., Carthy, J., Kechadi, T., & Crosbie, M. (2011). *Cloud Forensics: An Overview*. Dublin, Ireland: IBM Ireland Ltd.
- TechTarget. (2007, December). *Cloud Computing*. Retrieved October 11, 2011, from: <http://searchcloudcomputing.techtarget.com/definition/cloud-computing>

This page intentionally left blank

# Index

173

Page numbers in *italics* indicate figures and tables

## A

AAFS, *see* American Academy of Forensic Sciences  
AccessData's, 37, 38  
    FTK, 37  
    MPE+, 156  
Accreditation, 40–43  
Active data, 20  
Administrative review process, 32  
Allocated space, 22–23  
American Academy of Forensic Sciences (AAFS), 8–9  
American Society for Testing and Materials (ASTM), 9–10, 42  
American Society of Crime Laboratory Directors/  
Laboratory Accreditation Board (ASCLD/LAB), 9, 40–42  
Analysis, 138  
Android, 150  
Anonymous remailing, 127  
Antiforensics techniques, 82  
Anti-Forensics.com, 81  
Antistatic material bags, 52  
Apple FileVault, 88  
Apple OSX, 97  
Application logs, 139  
Archival data, 21  
ASCII, 14–15  
ASCLD/LAB, *see* American Society of Crime Laboratory Directors/Laboratory Accreditation Board  
ASTM, *see* American Society for Testing and Materials  
Asymmetrical encryption, 85  
Attribution, 69  
AuC, *see* Authentication Center  
Authentication Center (AuC), 147  
Authentication log, 139

## B

Base station, 147  
Base station controller (BSC), 147

Binary, 13  
Bind, Torture, Kill (BTK), 3–4  
Bit, 13–15  
BitLocker, 86–88  
BitPim, 156  
Blackberrys, 150  
Blind test, 33  
Blocks, 168  
Botnet, 135  
Browsers, 117–118  
Brute force attacks, 88–90  
BSC, *see* Base station controller  
BTK, *see* Bind, Torture, Kill  
Byte, 13–15

## C

Caesar Cipher, 84  
Call detail records (CDR), 151–152  
Campus Area Networks (CANs), 133  
CANs, *see* Campus Area Networks  
Carrier files, 92  
Casey Anthony trial, 129  
CDMA, *see* Code Division Multiple Access  
CDR, *see* Call detail records  
Cell phone, 47–49  
    acquisition, 155  
    CDR, 151–152  
    evidence, 150  
        collecting and handling, 152–154, 153  
    faraday bag and, 48, 48  
    forensic tools, 155–157  
    network signals, 48  
    SIMs, 154–155  
Cell site, 147  
Cellebrite UFED device, 156–157, 156  
Cellular networks  
    cell site, 147  
    components, 147–148  
    layout of, 146, 146  
    types of, 148–149  
Central processing unit (CPU), 19, 27  
Certification, 42–43  
CFIT, *see* Computer Forensic Tool Testing  
Chain of custody, 52, 53  
Chat clients, 124–125  
Chronological order method, 51  
Cipher text, 83  
Client/server network, 132  
Cloning, 52–56  
    eDiscovery, 56  
    forensic image formats, 55  
    forensically clean media, 55  
    process of, 54–55  
    purpose of, 54  
    risks and challenges, 55  
Cloud  
    benefits of, 166  
    computing, 19–20, 165–166  
    forensics, 165–167  
    private and public, 165  
Cloud Service Provider (CSP), 165  
Code Division Multiple Access (CDMA), 148–149  
Complex encryption schemes, 86  
Computer Forensic Tool Testing (CFIT), 9, 36  
*Computer Security Incident Handling Guide*, 137  
Computer storage devices, 109–110  
Computing environments, 19–20  
Consent, 105–106  
    forms, 106  
Containment, 138  
Cookies, 120–121  
CPU, *see* Central processing unit  
CRC, *see* Cyclical redundancy check  
Crime scenes, 46–49  
Criminal law  
    duty to preserve, 111–113  
    ECPA, 105  
    eDiscovery, 111–113  
    e-mail, 105

Criminal law (*Cont.*)  
 off-site analysis, 109–110  
 private searches, 105  
   in workplace, 112–113  
 reasonable expectation of privacy,  
   104–105  
 SCA, 110–111  
 search warrant requirement,  
   exceptions, 105–108  
   warrant, 108–111  
 Cryptographic algorithm, 83  
 CSI effect, 10  
 CSP, *see* Cloud Service Provider  
 Cybernap process, 66  
 Cyclical redundancy check (CRC), 134

**D**

Data  
   destruction, 94  
   hiding, 94  
   persistence, 22–23  
   safe, 31  
   sampling, 112  
*Daubert*, 164  
   *v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579 (1993), 114  
 DCC, *see* Direct Client Connection  
 DCO, *see* Device Configuration Overlays  
 DDoS, *see* Distributed Denial of Service  
 Dead system, 56–59  
 Decimal, 13  
 Deep sleep modes, 66  
 Deleted data, 66  
 Detection, 138  
 Device Configuration Overlays (DCO), 22  
 Device logs, 139  
 Dictionary attack, 88, 90–92  
 Digital evidence, 111  
 Digital forensics, 2–3, 69  
   tools  
     hardware, 36–39  
     selection, 36  
   uses of  
     AAFS, 8–9  
     administrative matters, 6–7  
     ASTM, 9–10  
     civil litigation, 4–5  
     criminal investigations, 3–4  
     intelligence, 5–6  
     Locard's exchange principle, 7  
     NIST, 9

scientific method, 7  
 SWGDE, 8  
 Digital solutions, 30  
 Direct Client Connection (DCC), 125  
 Directional antenna, 152  
 Distributed Denial of Service (DDoS), 135  
 DNS, *see* Domain Name Server  
 Document and Media Exploitation (DOMEX), 5  
 Documentation process, 49  
 Domain Name Server (DNS), 118  
 DOMEX, *see* Document and Media Exploitation  
 Drive wiping, 94–99  
 Dutch National High Tech Crime Unit (NHTCU), 136  
 Dutch NHTCU, *see* Dutch National High Tech Crime Unit  
 Duty to preserve, 111–112  
 Dynamic page, 118

**E**

ECPA, *see* Electronic Communications Privacy Act  
 ECS, *see* Electronic communication service  
 eDiscovery, *see* Electronic Discovery  
 EFS, *see* Encrypting File System  
 Electronic communication service (ECS), 110  
 Electronic Communications Privacy Act (ECPA), 105  
 Electronic Discovery (eDiscovery), 4, 56, 111–113  
 Electronic Serial Number (ESN), 149  
 Electronically stored information (ESI), 111  
 E-mail, 105  
   accessing, 126  
   as evidence, 126–127  
   headers, 128–129  
   protocols, 126  
   tracing, 127–128  
   URL, 117  
 EMF, *see* Enhanced Meta File  
 Encoding schemes, 14  
 Encrypting File System (EFS), 87  
 Encryption, 94  
   algorithms, 85–86  
   breaking passwords, 88–89  
   definition, 83–84  
   key space, 86  
   types of, 86–88

Enhanced Meta File (EMF), 70  
 Eradication, 138  
 ESI, *see* Electronically stored information  
 ESN, *see* Electronic Serial Number  
 Evidence Eliminator, 78  
 Examiner's final report, 35  
 Exigent circumstances, 107  
 External drives, 70  
 External test, 33

**F**

Faraday bag, 48, 48  
 FAT, *see* File Allocation Table  
 FDE, *see* Full disk encryption  
 FDLE, *see* Florida Department of Law Enforcement  
 Federal Rules of Civil Procedure, 4  
 FEPAC, *see* Forensic Science Education Programs Accreditation Commission  
 Fidelity National Information Services Inc. (FIS), 131  
 File Allocation Table (FAT), 21  
 File carving, 15, 66  
 File extensions, 15–16, 16  
 File header, 26  
 File signature analysis, 15–16, 16  
 File system, 21–22  
 File Translation Layer, 168  
 FileVault, 86  
 Firewall, 135  
 FIS, *see* Fidelity National Information Services Inc.  
 Flash based hard drives, 18  
 Flash memory, 18  
 Florida Department of Law Enforcement (FDLE), 164  
 Footer, 26  
 Footprinting/fingerprinting, 136  
 Forensic cloning, 56  
 Forensic examiner in judicial system, role of, 10  
 Forensic image formats, 55  
 Forensic laboratories  
   evidence storage, 31–32  
   lab security, 30–31  
   virtual labs, 30  
 Forensic science, 2  
   committee, 9  
   gold standard of, 7  
 Forensic Science Education Programs Accreditation Commission (FEPAC), 8  
 Forensic Toolkit (FTK), 37, 39

Forensic tools, 40, 41, 70  
 Forensically clean media, 55  
 Fourth Amendment, 104  
 Frye Test, 113  
 FTK, *see* Forensic Toolkit  
 Full disk encryption (FDE), 86

## G

GANs, *see* Global area networks  
 Garbage Collection, 168  
 Gateway, 135  
 GB, *see* Gigabytes  
 Gigabytes (GB), 46  
 Global area networks (GANs), 133  
 Global Positioning System (GPS), 157–160  
 Global System for Mobile Communication (GSM), 148–149  
 Gnutella, 119  
 GPS, *see* Global Positioning System  
 GSM, *see* Global System for Mobile Communication

## H

Hackers, 132  
 Handoff, 148  
 Hard drives, 54  
 Hardware write blocking (HWB) device, 36  
 Hash functions, 59  
 Hashing  
     algorithms, types of, 59  
     example of, 59–60  
     uses of, 60  
 Header, 26, 127  
 Hexadecimal, 14  
     numbers, 96  
 HFS+, *see* Hierarchical File System Plus  
 Hiberfile.sys, 66–67  
 Hibernation, 67  
 Hierarchical File System Plus (HFS+), 22  
 HLR, *see* Home Location Register  
 Home Location Register (HLR), 147  
 Host Protected Area (HPA), 22  
 HPA, *see* Host Protected Area  
 HTML, *see* Hypertext Markup Language  
 HTTP, *see* Hypertext Transfer Protocol  
 HWB device, *see* Hardware write blocking device  
 Hybrid sleep, 67

Hypertext Markup Language (HTML), 118  
 Hypertext Transfer Protocol (HTTP), 117

## I

IaaS, *see* Infrastructure as a Service  
 ICC-ID, *see* Integrated Circuit Card Identifier  
 ICQ, 125–126  
 iDEN, *see* Integrated Digitally Enhanced Network  
 Identity Spoofing (IP Spoofing), 136  
 IDS, *see* Intrusion Detection System  
 IMAP, *see* Internet Message Access Protocol  
 IMEI, *see* International Mobile Equipment Identifier  
 IMSI, *see* International Mobile Subscriber Identity  
 Index.dat file, 120  
 Infrastructure as a Service (IaaS), 19–20  
 Insider threat, 130–131  
 Integrated Circuit Card Identifier (ICC-ID), 154  
 Integrated Digitally Enhanced Network (iDEN), 149  
 Internal test, 33  
 International electronic discovery, 113  
 International Mobile Equipment Identifier (IMEI), 149  
 International Mobile Subscriber Identity (IMSI), 154  
 Internet  
     history, 122–123  
     HTML, 118  
     HTTP, 117  
     index.dat file, 120  
     IP, 118  
     P2P, 119–120  
     TLD, 117  
     whois, 119  
 Internet Message Access Protocol (IMAP), 126  
 Internet Protocol (IP), 118  
     address, 133  
 Internet Relay Chat (IRC), 125  
 Internet Service Providers (ISPs), 110, 134, 140  
 Interworking functions, 147  
 Intranets, 133  
 Intrusion Detection System (IDS), 135

iOS, 150  
 IP, *see* Internet Protocol  
 IRC, *see* Internet Relay Chat  
 ISPs, *see* Internet Service Providers

## J

JavaScript, 118

## K

Key space, 86

## L

LAN, *see* Local Area Network  
 Lands, 18  
 Latent data, 21  
 Legacy data, 21  
 Link files, 78–79  
 Live system  
     live acquisition concerns, 56–57  
     live collection  
         advantage of, 57–58  
         conducting and documenting, 58–59  
         principles of, 58  
 Local Area Network (LAN), 133  
 Locard's exchange principle, 7  
 Log files, 139–140

## M

Magnetic disks, 17, 17–18  
 Mainframe system, 19  
 Malware, 31  
 Man-In-The Middle-Attack, 136  
 MANs, *see* Metropolitan Area Networks  
 Marshall University Digital Forensics, 14  
 MEID, 153  
 Memory, 16–19  
     cards, 46–47  
 Message ID, 127  
 Metadata, 72–75  
     removing, 74–75  
 Metropolitan Area Networks (MANs), 133  
 Microsoft's TechNet, 67  
 Mini-computers, 145  
 MMS, *see* Multimedia Messaging Services  
 Mobile Switching Center (MSC), 147–148  
 Most Recently Used (MRU), 76, 76  
 Moussaoui, Zacarias, 5–6  
 MRU, *see* Most Recently Used  
 MSC, *see* Mobile Switching Center

Multimedia Messaging Services (MMS), 148  
Multiple tools, 35

**N**

NAS, *see* National Academy of Sciences  
National Academy of Sciences (NAS), 8  
National Initiative Cyber Security Education (NICE), 9  
National Institute of Standards and Technology (NIST), 8, 36, 137, 165  
National Software References Library, 9  
Network intrusion detection system (NIDS), 135  
Network security tools  
evidence and investigations  
log files, 139–140  
tools, 140–141  
firewall, 135  
hacks and attacks, 135–137  
incident response, 137–139  
Network signals, protecting cell phones from, 48  
Networked computer, 19  
New Technology File System (NTFS), 21, 87  
NICE, *see* National Initiative Cyber Security Education  
NIDS, *see* Network intrusion detection system  
NIST, *see* National Institute of Standards and Technology  
Nonvolatile memory, 18–19  
NTFS, *see* New Technology File System  
NTUSER.DAT file, 123  
NukeOnDelete, 71  
Numbering schemes, 13–15

**O**

Obfuscation, 84  
Office of the Inspector General (OIG), 6  
Off-site analysis, 109–110  
OIG, *see* Office of the Inspector General  
Open Handset Alliance, 150  
Open test, 32  
Operating system (OS), 149–150  
logs, 139  
Optical media, 18

Optical storage, 18  
Order of volatility, 49  
OS, *see* Operating system  
Oxygen Forensic Suite, 156

**P**

PaaS, *see* Platform as a Service  
Packet switching, 134  
Pages, 168  
file, 25–26  
PANS, *see* Personal Area Networks  
Paraben Corporation, 156  
Password Recovery Toolkit (PRTK), 89  
Password reset, 90  
Patch, 132  
Patriot Act, 105  
Payload files, 92  
Peer-to-peer (P2P), 119–120, 133  
Personal Area Networks (PANs), 133  
Personal Identification Number (PIN), 151, 155  
Personal Unlock Key (PUK), 151  
Photography, 50–51  
PIN, *see* Personal Identification Number  
Plain text, 83  
Plain view doctrine, 107  
Platform as a Service (PaaS), 19–20  
POI, *see* Points of Interest  
Points of Interest (POI), 158  
POP, *see* Post Office Protocol  
Post Office Protocol (POP), 126  
Postincident activity, 138  
P2P, *see* Peer-to-Peer  
Predictive text, 151  
Prefetch, 78  
Prepaid cell phones, 149  
Preparation phase, 138  
Preprinted forms, 34  
Print spooling, 70  
Private clouds, 165  
Private searches, 105  
in workplace, 112–113  
Probable cause, 104  
Proficiency testing, 32  
PRTK, *see* Password Recovery Toolkit  
PSTN, *see* Public Switched Telephone Network  
Public clouds, 165  
Public Switched Telephone Network (PSTN), 148  
PUK, *see* Personal Unlock Key

Push to Talk, 149  
Push-button tools, 40

**Q**

QA, *see* Quality assurance  
Quality assurance (QA)  
documentation, 34–35  
tool validation, 33–34

**R**

RAM, *see* Random Access Memory  
Random Access Memory (RAM), 19, 26  
preserving evidence in, 57  
RCFL program, *see* Regional Computer Forensic Laboratory program  
RCS, *see* Remote computing service  
Reasonable expectation of privacy, 104–105  
Recovery, 138  
Recycle bin, 70–72, 72  
Regional Computer Forensic Laboratory (RCFL) program, 30  
Registry, 67–70  
internet explorer artifacts, 123–124  
Remote computing service (RCS), 110  
Removable storage media, 47  
Resetting passwords, 88  
Restore points (RP), 76–77  
Routers, 139  
direct data, 135  
logs, 140  
RP, *see* Restore points  
Rules of Civil Procedure, 111

**S**

SaaS, *see* Software as a Service  
SARC, *see* Steganography Analysis and Research Center  
SCA, *see* Stored Communications Act  
Scientific method, 7  
Scientific Working Group for DNA Analysis Methods (SWGDM), 8  
Scientific Working Group on Digital Evidence (SWGDE), 8, 43, 164–165  
Scientific Working Groups (SWGs), 8  
SEC, *see* Securities and Exchange Commission  
Sectors, 23, 23–24

Secure Erase options, 97  
 Securities and Exchange Commission (SEC), 6–7  
 Security identifier (SID), 69  
 Sedona Conference, 111  
 Service Level Agreements (SLAs), 167  
 Shadow copies, 77–78  
 Short Message Service (SMS), 148  
 Short Message Service Center (SMSC), 147  
 SID, *see* Security identifier  
 SIFT, 39  
 SIM, *see* Subscriber Identity Module  
 Simple Mail Transfer Protocol (SMTP), 126  
 Slack space, 23, 25, 25  
 SLAs, *see* Service Level Agreements  
 Sleep mode, 67  
 Small-scale devices, 38  
 Smartphone, 159  
 SMS, *see* Short Message Service  
 SMSC, *see* Short Message Service Center  
 SMTP, *see* Simple Mail Transfer Protocol  
 Sniffer, 135, 140  
 Social engineering, 132, 136  
 Social media evidence, 129  
 Social networking sites, 129  
 Software, 39–40  
 Software as a Service (SaaS), 19–20  
 Solid state drive (SSD), 18, 167–168  
 SOPs, *see* Standard Operating Procedures  
 Spindle, 17  
 Spoliation, 111  
 Spoofing, 127  
 Spooling, 70  
 SSD, *see* Solid state drive  
 Stand-alone computer, 19  
 Standard Operating Procedures (SOPs), 32  
 Standards & controls, 164–165  
 Static Web page, 118  
 Steganography, 92–94  
 Steganography Analysis and Research Center (SARC), 93

Stored Communications Act (SCA), 110–111  
 Subscriber Identity Module (SIM), 154–155  
 Swap space, 25–26  
 SWGDAM, *see* Scientific Working Group for DNA Analysis Methods  
 SWGDE, *see* Scientific Working Group on Digital Evidence  
 SWGs, *see* Scientific Working Groups  
 Symmetrical encryption, 85  
 System encryption, 57

**T**

Tapes, 21  
 TCP/IP, *see* Transmission Control Protocol/Internet Protocol  
 TDMA, *see* Time Division Multiple Access  
 Technical review process, 32  
 Technical Working Groups (TWGs), 8  
 Temporary Internet Files (TIF), 121–122  
 Third parties, 107  
 Thumb drives, 70  
 Thumbnail cache, 75–76  
 TIF, *see* Temporary Internet Files  
 Time Division Multiple Access (TDMA), 149  
 TLD, *see* Top Level Domain  
 Top Level Domain (TLD), 117  
 TPM, *see* Trusted Platform Module  
 Track log, 157–158  
 Trackpoints, 157–158  
 Transistors, 18  
 Transmission Control Protocol/Internet Protocol (TCP/IP), 132  
 Triangulation, 152  
 Trilateration, 157  
 TrueCrypt, 88  
 Trusted Platform Module (TPM), 87  
 TWGs, *see* Technical Working Groups  
 Twitter, 169–170

**U**

Unallocated space, 22–23  
 Unicode, 14–15  
 Uniform Resource Locator (URL), 117, 123  
 United States Secret Service (USSS), 136  
*United States v. Frye*, 113  
 URL, *see* Uniform Resource Locator  
 USSS, *see* United States Secret Service

**V**

Vance, Christopher, 159–160  
 Virtual memory, 26  
 Virtualization, 165  
 Visitor Location Register (VLR), 147  
 VLR, *see* Visitor Location Register  
 Voice-mail, 154  
 Volatile memory, 18–19

**W**

WAN, *see* Wide Area Network  
 Warp speed, 135  
 Warrant, 108–111  
 Waypoints, 158  
 Wear leveling process, 168  
 Web browsers  
     chat clients, 124–125  
     cookies, 120–121  
     ICQ, 125–126  
     internet history, 122–123  
     IRC, 125  
     registry, internet explorer artifacts, 123–124  
     TIF, 121–122  
 Whois, 119  
 Wide Area Network (WAN), 133  
 Windows Registry, 67  
 Wiretap Act, 105  
 Write block, 36

**Z**

Zombies, 135  
*Zubalake v. USB Warburg*, 111

This page intentionally left blank



# A Career in Cybersecurity

## Cybersecurity Webinar Series

Speaker: Lonnie Harris

Hostess: Kara Sullivan

Cisco Networking Academy

18 October 2018

# Welcome to the 3rd session of the Cybersecurity webinar series

- Use the Q and A panel to ask questions.
- Use the Chat panel to communicate with attendees and panelists.
- A link to a recording of the session will be sent to all registered attendees.
- Please take the feedback survey at the end of the webinar.

# • Cybersecurity Webinar Series

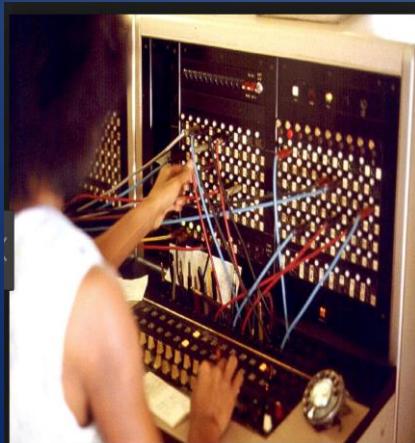
- Session 1: Cybersecurity Basics, Recording available
- Session 2: Security Threats & Breaches, Recording available
- Session 3: A Career in Cybersecurity, Today!

Access Series @  
<http://bit.ly/cybersecseries>

# A Career in Cybersecurity

Lonnie Harris – Cybersecurity Architect  
2018

# THE EVOLUTION OF COMMUNICATION - VOICE



# THE EVOLUTION OF COMMUNICATION - INTERNET

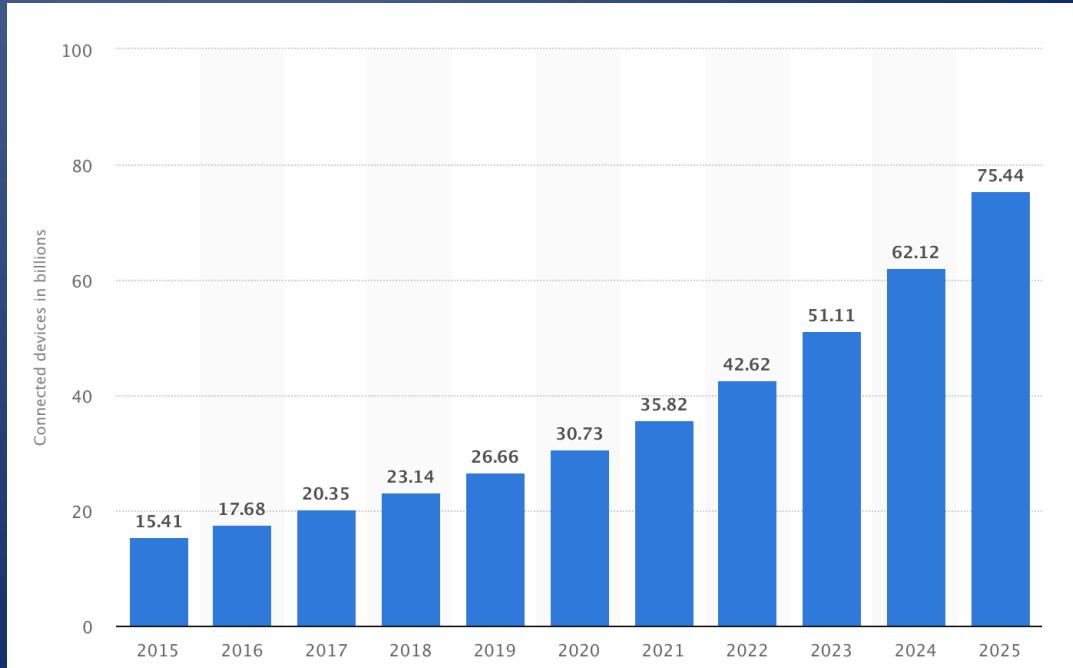


- Age of digital communication via computers
- Mosaic was the first browser for sound, video, forms, and history files
- Birth of world wide web (WWW)
- Email services – GMAIL, Hotmail, Yahoo
- The Internet of Things



# THE EVOLUTION OF COMMUNICATION - (INTERNET OF THINGS IOT)

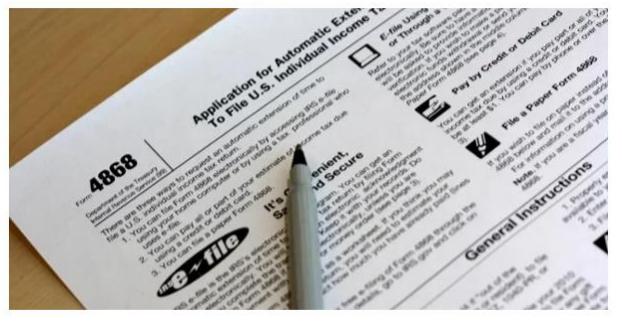
- Statistics shows the number of connected devices (IoT) worldwide from 2015 to 2025
- For 2020, the installed base of Internet of Things devices is forecasted to grow to almost 31 BILLION worldwide



# CYBERSECURITY JOB REPORTS

- Every IT position is also a cybersecurity position now; having to be involved with protecting and defending apps, data, devices, infrastructure, and people. The cybersecurity workforce shortage is even worse than what the jobs numbers suggest.





## Russians Attack 2018 U.S. Elections Via Facebook, Social Media

DAVID PIERSON, LOS ANGELES TIMES - MCCLATCHY ON AUG 1, 2018



# Major life-threatening cyber attack on UK 'in little doubt' in near future, warns security chief

The National Cyber Security Centre warns that a life-threatening incident will almost inevitably strike the UK.

00:14, UK,  
Tuesday 16 October 2018



We'd be crippled by a cyberattack on our utilities

Washington Post

1 day ago



ONWASA victim of cyber attack; utility refuses to pay ransom

WITN

11 hours ago



# EXERCISE

- Open a web browser and navigate to the Shodan [website](https://www.shodan.io/) at <https://www.shodan.io/>.
- After successfully logging in, you will see your account page, as shown below. Click the **Shodan** link to return to the homepage.
- top web cameras used for home security
- Nest Cam Indoor Network Camera - 3 MP - 1080p - Day/Night - 3 Pack rated 4.5 out of 5 stars  
[,922 reviews](#)
- Type **NEST** as the keyword and press **Enter**. How many results did you get for your search
- Attackers looks for unsupported operating system, known vulnerabilities or published attacks
- Use an Internet search to discover the well-known 2017 cyberattack that targeted older Windows operating systems

# CHOOSING THE RIGHT SIDE

cy·ber·at·tack

/sībərətak/

*noun*

noun: **cyber-attack**

an attempt by hackers to damage or destroy a computer network or system.

eth·i·cal hack·er

*noun*

noun: **ethical hacker**; plural noun: **ethical hackers**

a person who hacks into a computer network in order to test or evaluate its security, rather than with malicious or criminal intent.

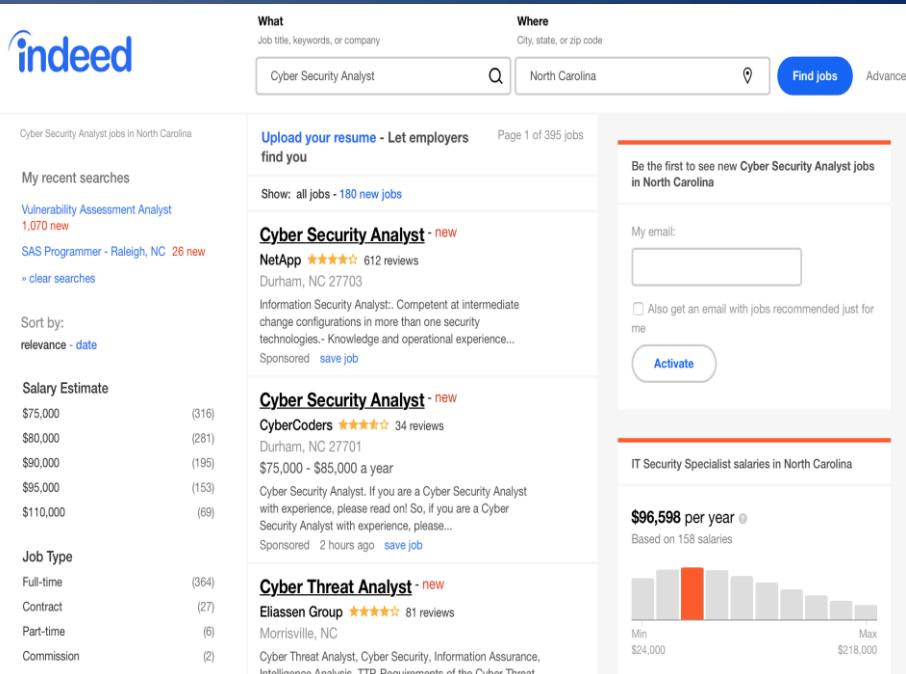
"ethical hackers are becoming a mainstay of the effort to make corporate networks more secure"

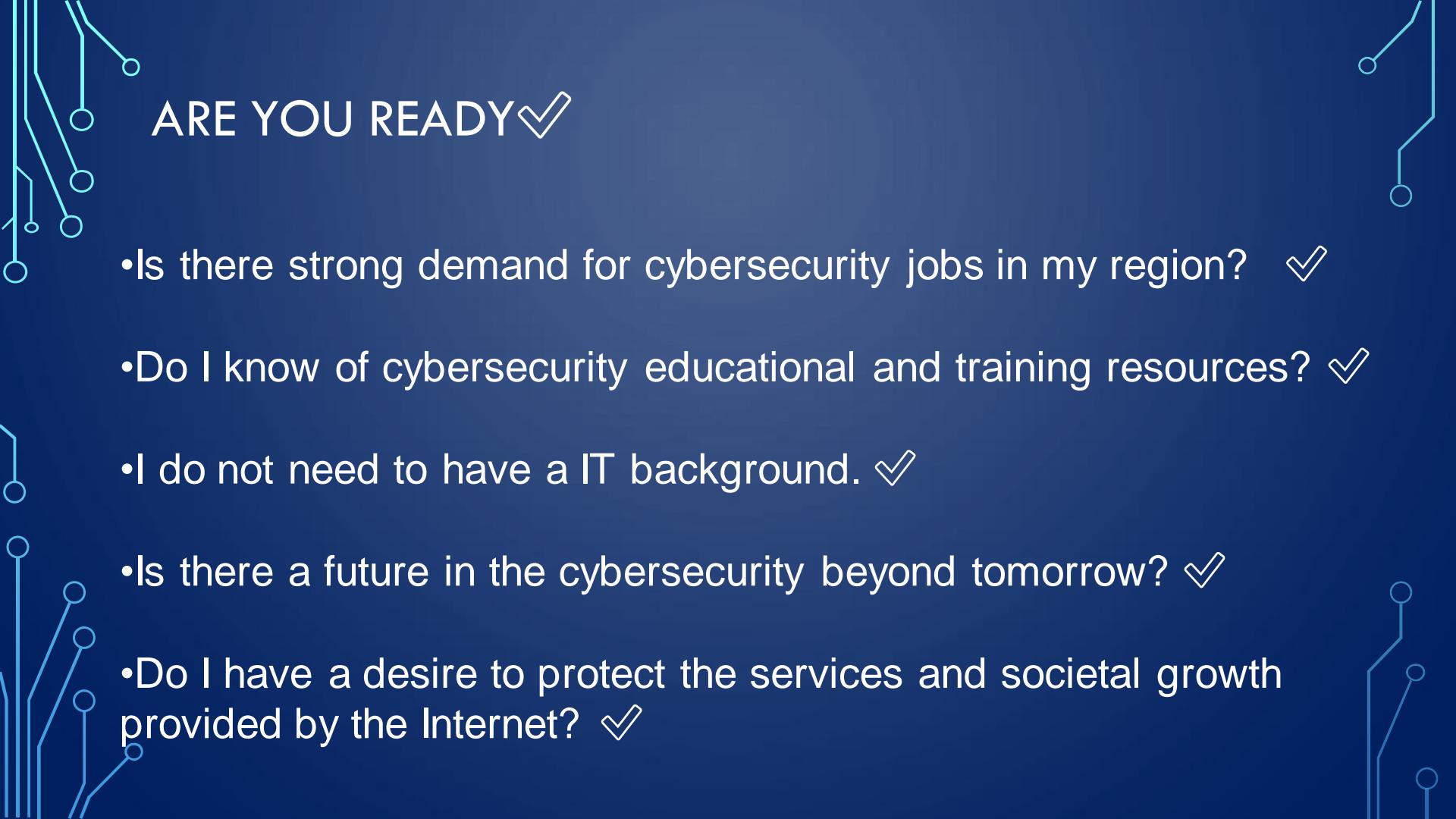
# CYBERSECURITY ROLES AND SKILLS

Job Title	Skills
• Network Engineer	• Network Admin., Troubleshooting, TCP/IP, Software Installation, Active Directory
• Systems Engineer	• Servers, Storage, Data Center, Cloud Computing, Networking
• Software Developer	• Programming ,JavaScript, Python,Databases, Data Analytics
• Business Analyst	• Business Analysis, Microsoft office, Project Management, Process Management, Requirements Analysis
• Data Analysts	• Data Analysis, Customer Support, Organization skills, Microsoft Office, Problem Solving
• Software/System QA	• Software Development, Test Suites, Troubleshooting, Requirements Analysts, Web Design
• Systems/Network Administrator	• Network Operations, DevOps, Troubleshooting, Integration, Customer Services
• Technical Support	• Troubleshooting, Customer Service, Microsoft Office, Windows, hardware/Software
• Security Engineer	• Network Security, Linux, Vulnerability Assessment, Firewalls, Intrusion Detection

# RESOURCES TO GET STARTED

- Cyber Seek is helping to close the cybersecurity skills gap by creating interactive career pathway  
<https://www.cyberseek.org>
- Cisco Networking Academy  
<https://www.netacad.com>
- 1000+ cybersecurity analysts jobs in North Carolina 10/16/2018





# ARE YOU READY?

- Is there strong demand for cybersecurity jobs in my region? ✓
- Do I know of cybersecurity educational and training resources? ✓
- I do not need to have a IT background. ✓
- Is there a future in the cybersecurity beyond tomorrow? ✓
- Do I have a desire to protect the services and societal growth provided by the Internet? ✓



**WANTED AND URGENTLY NEEDED:  
CYBERSECURITY PROS TO  
SERVE THEIR COUNTRY**

**RESUME PLACE**

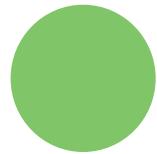
# Q&A



# Qualifications for Certificate of Participation



Must Participate in all 3 sessions of the Cybersecurity webinar series – whether through recordings or live sessions



Opportunity to earn a certificate will stay open for one month – until 18 November



Request certificate @  
<http://netacad.cvent.com/CertificateRequestForm>

# Intro to Cybersecurity Self-Enroll Course

## Introduction to Cybersecurity

Learn how to protect yourself online and in social media while discovering careers in cybersecurity.

Enroll Now



You can enroll today to learn more @ <http://bit.ly/introsecurity>



**INFOSEC**

I N S T I T U T E

# Introduction to Computer Forensics & Digital Investigation

By: Irfan Shakeel



Irfan Shakeel

## Table of Contents

Table of Contents .....	2
Case Scenario .....	4
The Need for Forensics .....	4
What is Computer Forensics? .....	4
Computer Forensics Process .....	5
Identification .....	5
Collection .....	5
Examination .....	5
Analysis .....	5
Reporting .....	6
Computer Forensics Team .....	6
First Responder .....	7
Rules of Computer Forensics .....	7
3 A's of Computer Forensics .....	8
Evidence & Its Types .....	9
Digital Evidence .....	9
Rules of Evidence .....	10
<i>Chain of Custody</i> .....	10
Chain of Custody Form .....	12
Sources of Evidence .....	13
Gathering Digital Evidence – The Procedure .....	14
Volatile Evidence .....	15
Why the Volatile Data/Evidence is so Important .....	16
Volatile Data Collection Strategy .....	16
System Profiling .....	16
..... .....	17
..... .....	18
..... .....	20
Evidence Management .....	27
Modes of Attack .....	27
Computer Forensics - Systematic Approach .....	29
Module 2: Legal Aspects of Computer Forensics .....	30
Legal Process: .....	30
U.S Statutory Law .....	32
Wiretap Act Electronic Communication Privacy Act .....	33
Pen/Trap & Trace Act 18 U.S.C. §§ 3121-27 .....	33
Stored Wire and Electronic Communication Act - 18 U.S.C. §§ 2701-12 .....	33
Intellectual Property laws: .....	34
Module 3: File System structure & Architecture .....	36
Storage Media: .....	36
Hard Drive .....	36
File System & Structure .....	41
Microsoft Windows File Systems .....	43
Windows Registry .....	47
Linux File Systems .....	49
Inodes .....	49
Journaling File System .....	50
Module4: Evidence Acquisition & Investigation .....	54
Storage Media Image: .....	54
Hashing to Verify the Integrity of the Image .....	60
Image Acquisition on Linux .....	62

Data Analysis .....	65
Disk Analysis on Linux – Autopsy .....	73
End Note: .....	79

## ***Module1: Foundation of Computer Forensics***

### ***Case Scenario***

Alex is the computer forensics investigator and has been hired to investigate data theft case in an organization. The general manager of the organization believes that some of their employees are involved in illegal activities including the network breach and the transfer of their confidential data, which is against the organizational policy. Alex has performed his investigation, collected the evidences and then he submitted his final report. According to the report, two employees were found responsible for the data theft. Based on this report, a case has been lodged against them.

In the scenario mentioned above, the organization was the client, Alex was the service provider and the service that was being provided is called computer forensics & digital investigation services.

The objective of this course is to discuss Alex' work:

- Work process of computer forensics
- The process of initiating and performing the investigation
- Legal laws & boundaries
- Techniques to gather evidence
- The scope of the forensic work

### ***The Need for Forensics***

The world has become a global village since the advent of computer, digital devices & the internet. Life seems impossible without these technologies, as they are necessary for our workplace, home, street, and everywhere. Information can be stored or transferred by desktop computers, laptop, routers, printers, CD/DVD, flash drive, or thumb drive. The variations and development of data storage and transfer capabilities have encouraged the development of forensic tools, techniques, procedures and investigators.

In the last few years, we have witnessed the increase in crimes that involved computers. As a result, computer forensics and digital investigation have emerged as a proper channel to identify, collect, examine, analysis and report the computer crimes.

### ***What is Computer Forensics?***

As a rule of thumb, “Forensic is the scientific tests or techniques used in connection with the detection of crime.” - Wikipedia. Furthermore, forensic is the process of using scientific techniques during the identification, collection, examination and reporting the evidence to the court.

So what computer forensics is all about?

According to Dr. H.B.Wolfe computer forensics is, “A methodical series of techniques and procedures for gathering evidence, from computing equipment and various storage devices and digital media that can be presented in a court of law in a coherent and meaningful format.”

If we further define computer forensics then, it is the procedure to collect, analyze and presentation of digital evidence to the court.

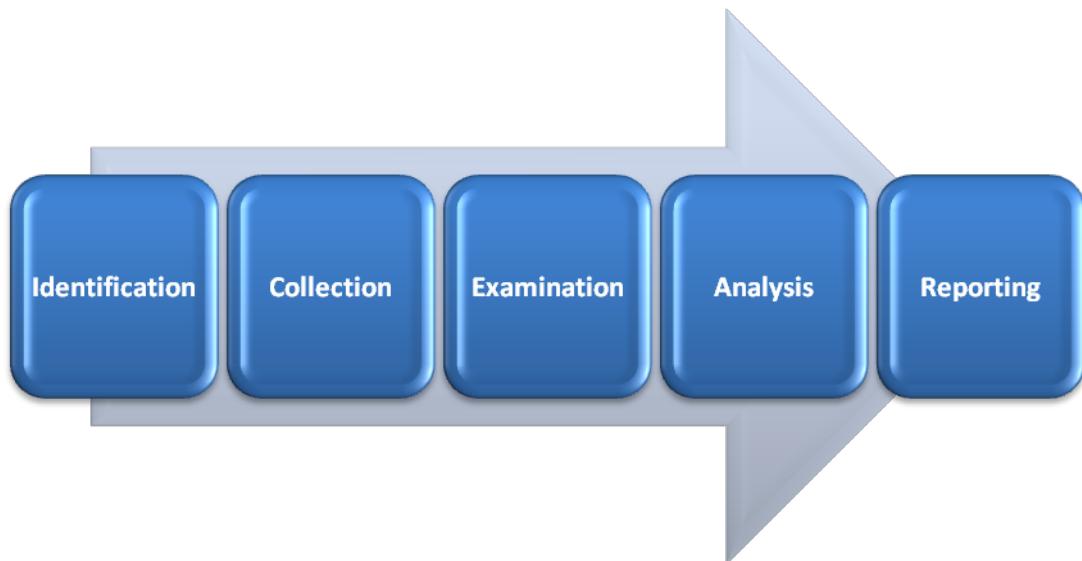
The scope of computer forensics is not limited to investigating a crime only. Apart from this,

computer forensics can be used for:

- Data recovery
- Log monitoring
- Data acquisition (from the retired or damaged devices)
- Fulfill the compliance needs

## ***Computer Forensics Process***

Computer forensics work procedure or work process can be divided into 5 major parts:



### **Identification**

The first process of computer forensics is to identify the scenario or to understand the case. At this stage, the investigator has to identify the purpose of investigation, type of incident, parties that involved in the incidence, and the resources that are required to fulfill the needs of the case.

### **Collection**

The collection (chain of custody) is one of the important steps because your entire case is based on the evidence collected from the crime scene. Collection is the data acquisition process from the relevant data sources while maintaining the integrity of data. Timely execution of the collection process is crucial in order to maintain the confidentiality and integrity of the data. Important evidence may lost if not acted as required.

### **Examination**

The aim of third process is to examine the collected data by following standard procedures, techniques, tools and methodology to extract the meaningful information related to the case.

### **Analysis**

Since all five processes are linked together, the analysis is the procedure to analyze the data acquired after examination process. At this stage, the investigator search for the possible evidence

against the suspect, if any. Use the tools and techniques to analyze the data. Techniques and tools should be justified legally, because it helps you to create and present your report in front of the court.

## **Reporting**

This is the final, but the most important step. At this step, an investigator needs to document the process used to collect, examine and analyze the data. The investigation report also consists the documentation of how the tools and procedures were being selected. The objective of this step is to report and present the findings justified by evidences.

Every step mentioned above can be further divided into many parts and every part has its own standard operating procedures, we look into them in detail in the coming chapters.

## ***Computer Forensics Team***

Law enforcement and security agencies are responsible for investigating a computer crime, however every organization should have the capability to solve their basic issues and investigation by themselves.

Even an organization can hire experts from small or mid-size computer investigation firms. Also you can create your own firm that provides computer forensic services. To do so, you need a forensics lab, permission from the government to establish a forensics business, the right tools with the right people and rules/policies to run the business effectively and efficiently.

As discussed, an organization should have enough capability to handle and solve the basic issues by their own people. Without this ability, it is very hard for an organization to determine the fraud, illegal activities, policy, or network breach or even they will find it hard to implement the cyber security rules in the organization. The need of such abilities may vary and it depends on the nature of business, security threats and the possible loss.

Here are the key people that a computer investigation firm should have:

- **Investigators:** This is a group of people (number depends on the size of the firm) who handle and solve the case. It is their job to use the forensic tools and techniques in order to find the evidence against the suspect. They may call the law enforcement agencies, if required. Investigators are supposed to act immediately after the occurrence of the event that is suspected of criminal activity.
- **Photographer:** To record the crime scene is as important as investigating it. The photographer's job is to take photographs of the crime scene (IT devices and other equipment).
- **Incident Handlers (first responder):** Every organization, regardless of type, should have incident handlers in their IT department. The responsibility of these people is to monitor and act if any computer security incidence happen, such as breaching of network policy, code injection, server hijacking, RAT or any other malicious code installation. They generally use the variety of computer forensics tools to accomplish their job.
- **IT Engineers & technicians** (other support staff): This is the group of people who run the daily operation of the firm. They are IT engineers and technicians to maintain the forensics lab. This team should consist of network administrator, IT support, IT security engineers and desktop support. The key role of this team is to make sure the smooth organizational functions, monitoring, troubleshooting, data recovery and to maintain the required backup.
- **Attorney:** Since computer forensics directly deal with investigation and to submit the case in the court, so an attorney should be a part of this team.

## **First Responder**

The first responder and the function of the first responder is crucial for computer forensics and investigation. The first responder is the first person notified, and take action to the security incident. The first responder toolkit will be discussed in the upcoming chapters, but at this stage, I will discuss the roles and responsibilities of the first responder.

The first responder is a role that could be assigned to anyone, including IT security engineers, network administrator and others. The person who is responsible to act as a first responder should have knowledge, skills and the toolkit of first responders.

The first responder should be ready to handle any situation and his/her action should be planned and well documented. Some core responsibilities are as follows:

- Figure out or understand the situation, event and problem.
- Gather and collect the information from the crime scene
- Discuss the collected information with the other team members
- Document each and everything

First responder or incident handlers should have first-hand experience of Information security, different operating systems and their architectures.

## ***Rules of Computer Forensics***

There are certain rules and boundaries that should be keep in mind while conducting an investigation.

Matthew Braid, in his AusCERT paper, ‘Collecting Electronic Evidence after a System Compromise’ has provided the rules of computer forensics:

1. Minimize or eliminate the chances to examining the original evidence:

Make the accurate and exact copy of the collected information to minimize the option of examining the original. This is the first and the most important rule that should be considered before doing any investigation, create duplicates and investigate the duplicates. You should make the exact copy in order to maintain the integrity of the data.

2. Don't Proceed if it is beyond your knowledge

If you see a roadblock while investigating, then stop at that moment and do not proceed if it is beyond your knowledge and skills, consult or ask an experienced to guide you in a particular matter. This is to secure the data, otherwise the data might be damaged which is unbearable. Do not take this situation as a challenge, go and get additional training because we are in the learning process and we love to learn.

3. Follow the rules of evidence

You might be worried because we have not discussed any rule of evidence yet, but the next topic will be about evidence. The rule of evidence must be followed during the investigation process to make sure that the evidence will be accepted in court.

#### **4. Create Document**

Document the behavior, if any changes occur in evidence. An investigator should document the reason, result and the nature of change occurred with the evidence. Let say, restarting a machine may change its temporary files, note it down.

#### **5. Get the written permission and follow the local security policy**

Before starting an investigation process, you should make sure to have a written permission with instruction related to the scope of your investigation. It is very important because during the investigation you need to get access or need to make copies of the sensitive data, if the written permission is not with you then you may find yourself in trouble for breaching the IT security policy.

#### **6. Be ready to testify**

Since you are collecting the evidence than you should make yourself ready to testify it in the court, otherwise the collected evidence may become inadmissible.

#### **7. Your action should be repeatable**

Do not work on trial-and -error, else no one is going to believe you and your investigation. Make sure to document every step taken. You should be confident enough to perform the same action again to prove the authenticity of the evidence.

#### **8. Work fast to reduce data loss**

Work fast to eliminate the chances of data loss, volatile data may lost if not collected in time. While automation can also be introduced to speed up the process, do not create a rush situation. Increase the human workforce where needed.

Always start collecting data from volatile evidence.

#### **9. Don't shut down before collecting evidence**

This is a rule of thumb, since the collection of data or evidence itself is important for an investigation. You should make sure not to shut down the system before you collect all the evidence. If the system is shut down, then you will lose the volatile data. Shutdown and rebooting should be avoided at all cost.

#### **10. Don't run any program on the affected system**

Collect all the evidence, copy them, create many duplicates and work on them. Do not run any program, otherwise you may trigger something that you don't want to trigger. Think of a Trojan horse.

### ***3 A's of Computer Forensics***

Computer forensics methodology has been presented by Kruse & Heiser in their book titled “Computer Forensics: Incident Response Essentials”. They have provided the 3A's of computer forensics that are applicable for Windows and other OS as well.

- 1. Acquire** the evidence without altering or damaging the original.
- 2. Authenticate** that the recovered evidence is same as the original seized data.
- 3. Analyze** data without any alterations

## **Evidence & Its Types**

Evidence is the key to prove the case in the court, evidence from a legal point of view can be divided into many types and each type do have its own characteristics in it. To keep the characteristics in mind during evidence collection helps an investigator to make the case stronger.

Admissible is the important characteristics of any evidence, it is generally the first rule of every evidence. Let's discuss the multiple types of evidence:

1. Real / tangible evidence: As the name suggests, real evidence consists of a tangible/physical material e.g hard-drive, flash drive, etc. Apart from the material, human can also be treated as real evidence e.g. an eye witness.
2. Original evidence: As law-pedia defines, “Evidence of a statement made by a person other than the testifying witness, which is offered to prove that the statement was actually made rather than to prove its truth.” This is generally an out of court statement.
3. Hearsay evidence: It is also referred as “out of court statement”, it is made in court, to prove the truth of the matter declared.
4. Testimony: When a witness takes oath in a court and give his/her statement in front of the court.

Evidence should be admissible, accurate and authentic; otherwise, it can be challenged while presenting the case in the court.

## **Digital Evidence**

Digital devices are not limited to computer, mobile phones and internet only; every electronic device having processing and storage capability can be used in crime. For example, mp3 player can be used to transfer the encoded message; electronic appliances might be used as storage to store the illegal documents.

The duty of investigator or first responder is to identify and seize the digital device for further investigation.

Digital information expressed or represent by the binary units of 1's (ones) and 0's (zeros). Digital information is stored in electronic devices by sending the instructions via software, program or code. The same way this information can be retrieved from the electronic device by using the program, here computer forensics software comes.

So what is digital evidence and where are the key sources to get the evidence?

**Digital evidence:** According to Wikipedia, “Digital evidence or electronic evidence is any probative information stored or transmitted in digital form that a party to a court case may use at trial.”

Digital evidence is any information that can be transmitted or stored by an electronic device.

## **Characteristics of Digital Evidence:**

- Timing is one of the important characteristics of digital evidence, first responder has responded immediately; otherwise, the data may be lost. For example, devices run on batteries may shutdown and current network connection may be lost.

- Just like fingerprints or any other biometric evidence, digital evidence is also hidden or latent, which requires a process to unearth.
- Digital evidence might be destroyed or damaged. Quick response and chain of custody is the key in computer forensics, you need to act according to the situation otherwise the important data might be damaged (intentionally or unintentionally).

## ***Rules of Evidence***

Matthew Braid, in his AusCERT paper, ‘Collecting Electronic Evidence after a System Compromise’ has defined the five rules of evidence:

### **1. Admissible**

The first and the most important rule is that your evidence should be able to use in court as an evidence.

### **2. Authentic**

Evidence should be authentic and it should be related and relevant to the case, you need to prove in front of the court that the collected evidence is authentic. Fail to do so, means the failure of the investigation.

### **3. Complete or Whole**

The court will not accept half evidence, you should be unbiased during your investigation and your evidence should not show the one prospective of the incident. As Matthew says, “*it is vital to collect evidence that eliminates alternative suspects. For instance, if you can show the attacker was logged in at the time of the incident, you also need to show who else was logged in and demonstrate why you think they didn’t do it. This is called Exculpatory Evidence and is an important part of proving a case.*”

### **4. Reliable**

Reliability of the evidence is important, but the process is also important and it should not create any doubt on the evidence.

### **5. Believable or Acceptable**

The evidence presented in the court should be in layman’s language, clear and easy to understand. You should present a well-crafted version of the document with the reference to the technical document.

## ***Chain of Custody***

This particular term is not only related to the computer forensics, any case or even any investigation has this important aspect. “Chain of Custody” is the process to acquire, secure, move and store the evidence until the time it is presented in court. While seizing the electronic device, you should tag it with the date/time of acquiring, case number and evidence numbers. This information is crucial while creating a case in the court. Evidence custodian is responsible to collect, transfer and store the evidence in the forensics lab. Anyone doing this job should understand its importance and he/she should not waste the valuable time.

Chain (strong metal use to connect or link between stuff) of custody, as the name says, “chain of custody shows how the evidence is acquired, managed, transferred or transported during the investigation process. And who involve in the process, what their responsibilities are and for how

much time they store the evidence and how they transfer it to someone else.” This important process tells the story of the evidence, if not carefully done then the opposite attorney can challenge and even dismiss the presented evidence.

In order to justify the chain of custody, you need to provide the evidence. You must provide the evidence that you maintained, documenting the chain-of-custody during the investigation process and you or anyone has not damaged or altered the evidence whether intentionally or unintentionally. “Chain of custody form” is the tool used to keep record of every important aspect, here is the sample chain-of-custody form:

# Chain of Custody Form

Case number: \_\_\_\_\_

Case officer Name: \_\_\_\_\_

Officer ID #: \_\_\_\_\_

Date/time of seized: \_\_\_\_\_

Location of seizure: \_\_\_\_\_

Information of the Evidence		
Item number	Quantity	Description (model number, vendor name, current condition)

Chain of Custody				
Item #	Date/Time	Released by	Received By	Comments & remarks

As you can see the aforementioned chain-of-custody form, this is the evidence that says about the parties who involved in maintaining the evidence. Court may call anyone to testify the process of how he/she delivered the evidence to the other party and how he/she stored the evidence in the lab.

As discussed in the previous topic that **Authentication** is the foremost rule of the evidence, you need to prove that the evidence is authentic and chain of custody plays a tremendous role along the way of authentication. It's not enough in order to just testify following the fact by what was compiled. Having a documented process in place that can track compiled information as well as ensure it is preserved but not manipulated with is also required.

Computer forensics expert organizations should have the guidelines and process that should support the admissibility of evidence into legal actions, including information on how the evidences have been acquired and handled, preserving the integrity of tools and equipment, maintaining the chain of custody, and storing evidence appropriately. The court might dismiss the case, if you fail to maintain the proper chain-of-custody, because the evidence can be challenged on the basis of every rule of evidence discussed earlier:

- **Admissibility:** How you will prove what you are presenting as evidence? There is no way; you need a document to support your argument.
- **Authentic:** If there is no chain-of-custody, then you will fail to prove that the presented evidence is authentic and gathered from the crime scene.
- **Complete or whole:** Again, you need a document to prove it.
- **Reliable:** Who is going to believe that you or anyone else have not altered or modified the evidence? You need to have a signed document and the people who can testify.
- **Believable:** The fifth rule is already void if fail to maintain the other four rules.

This is why the chain-of-custody is very important because the entire case is based on the evidence and the evidence is based on chain-of-custody process.

You should be ready to testify the steps taken while handling the evidence: who did what with the evidence and why?

You should bring the chain-of-custody of form in the court to justify your words. Technology has made our life very easy, we have cloud computing; you can store the evidence (soft-copy) in the cloud to reduce the transfer of the evidence. Now you will have a strong point to be presented in the court that the real evidence has been uploaded in the cloud in the very place to avoid the risk.

## Sources of Evidence

So what are the key sources of evidence or how computer forensics investigator gets the evidence? Since evidence could be anything and could be everywhere. In one case, you need to get evidence from mp3 player, and on some other case, evidence has to be retrieved from iPhone. The source is not limited and it depends on the nature of the case you are working on. Highly technical skills and expertise are required to examine and acquire the evidence from these sources. This is why this mini course has been designed. We look into the structure of many hardware devices as well as the file format of many operating systems. Apart from real evidence (tangible), sometimes you need to investigate for human testimony. So social engineering or the human skill set is also required to investigate the human and get the valuable information.

While investigating or acquiring evidence, you need to maintain the integrity and confidentiality of the data. This is very important as you might damage or retire the evidence, which you should not do.

As a rule, an investigator look for evidence in every electronic devices directly or indirectly related to the crime scene.

These are a few sources from where the evidence might be collected:

1. Hard-drive
2. Firewall logs
3. System logs
4. Social networking websites

5. Website that was visited
6. Email
7. GPS devices
8. Security camera's
9. Networking equipment
10. PDA (personal digital assistant)
11. Chat room or chat server

There are many sources, think about Internet of things.

### ***Gathering Digital Evidence – The Procedure***

The process to gather the digital evidence is simple and it should be followed to avoid any damage. The successful outcome of the process means you have secured the evidence effectively and efficiently.

So let's discuss the general procedure:



So it the four step process.

- Identification

There is a difference between data, information and an evidence, you should have a clear idea and you should distinguish between data and evidence. You need to extract evidence from the data, so identify the possible source from you can extract the evidence.

- Collection & Preservation

Once identified, collect it. Make sure to preserve the evidence to as close as original state. Document any change, if made.

- Analysis

Mark the qualified people to analyze the collected evidence to find the cause and effect relationship.

- Verification & Presentation

Verify the steps taken and the tools that were used. Presentation is vital, craft the document to be

presented in front of non-technical personnel and linked every step with the technical document for reference purpose, the presentation is very important to share your work otherwise it has no value.

## **Volatile Evidence**

Under the heading of volatile evidence, we will discuss the process and methodology to collect the volatile evidence. First, we should look into the volatile data and what volatile data is. What are the characteristics of a volatile data?

Usually, computer forensics deals with the procedures and techniques to identify, collect, examine, analyze and report the data available in the storage of an electronic device. However, a smart investigator always tries to collect information about the current status of the device. The job of the first responder is crucial to do this. Usually they take the device in custody and shut it down to move it into the forensics lab. In the forensics lab, the persistence or the stored data, is collected from the suspicious storage device. However, rebooting or shutdown is the major cause of data loss, especially the volatile data. In order to collect the volatile data, the first responder needs a running system.

The first responder has to create their own toolkit to gather the volatile data. In the recent years, we have seen rapid development of the forensic tools. For example, we have EnCase, NTI's law enforcement suite, and FTK. However, almost all the tools focus on collecting the persistent data. There are many open source tools available that can be the part of the first responder toolkit, and some of the open source tools are exclusively being created to gather the data, but most of them do not get the complete set of volatile data. It is highly recommended for a first responder to get their set of tools. They should also learn the commands to gather the volatile data manually.

As you now understand the concept of volatile data, here are some definitions for reference:

### **What is Volatile Data?**

Carnegie Mellon University defines it as follows: "*Volatile data is any data stored in system memory that will be lost when the machine loses power or is shut down.*"

Therefore, there are generally two sets of data:

- Persistent
- Volatile

#### **Persistent data:**

Persistent data is stored in the nonvolatile storage devices, for example; hard-drive, USB, CD/DVD and other external storage device. This type of data usually not lost after rebooting or shutting down the machine. At the start of the investigation process, you need to differentiate between persistent and volatile data. You should make a policy to get the volatile data first; else, it may be lost.

Persistent data is usually collected in the forensics lab.

#### **Volatile Data:**

Volatile data is stored in the system memory. This data will be lost if the system is rebooted or shut down. Matthew Braid, in his AusCERT paper, 'Collecting Electronic Evidence after a System Compromise' has created a list of evidence sources ordered by relative volatility. An example Order of Volatility would be:

- Registers and Cache
- Routing Tables

- Arp Cache
- Process Table
- Kernel Statistics and Modules
- Main Memory
- Temporary File Systems
- Secondary Memory
- Router Configuration
- Network Topology

## Why the Volatile Data/Evidence is so Important

Volatile data give an insight of the current state of the suspicious machine. It tells you about the logged-in users, processes that are running, and open ports with their remote connection. In the broader perspective, you can get the timeline of the suspicious machine, who, what and why they were using the machine when the incident happened. You can also get the date/time and the user who is likely responsible for the security incident.

Volatile data gives an investigator a broader perspective, an idea about the whole scenario, and how to proceed with the case.

### ***Volatile Data Collection Strategy***

Following are the key points that should be considered before starting the collection process:

1. **Do not use the suspicious machine programs:** create or establish your own command shell to gather the volatile information. The first responder toolkit should carry a command shell to use when required, and at this stage, you should use it.
2. **Method to store the collected information:** The process to transfer the collected evidence of the suspicious machine to the remote or collection system is very important and you should have a plan in mind to do so. Netcat is handy to establish connections so you may use it.

There are mainly two types of information that an investigator has to collect during the process:

1. **Volatile system information:** As the name suggests, collect the current running process, and configuration of the system.
2. **Volatile network information:** Collect the information about the network, open ports and the connectivity of the suspicious machine.

## System Profiling

An investigator has to get the profile of the system. It is the job of the network administrator to maintain the profile of every system. However, the system profile can be created in the run time.

Typically, the following information should be collected to compile the system profile:

OS type and version	total amount of physical memory
system installation date	pagefile location

registered owner	installed physical hardware and configurations
system directory	installed software applications

### Systeminfo.exe

The aforementioned command is for Windows OS, and it allows you to collect some important information about the system.

```
C:\>Documents and Settings\ehacking>systeminfo
Host Name: EHACKING-8A446B
OS Name: Microsoft Windows XP Professional
OS Version: 5.1.2600 Service Pack 2 Build 2600
OS Manufacturer: Microsoft Corporation
OS Configuration: Standalone Workstation
OS Build Type: Uniprocessor Free
Registered Owner: ehacking
Registered Organization: ehacking
Product ID: 55274-648-5295662-23651
Original Install Date: 1/30/2014, 3:42:12 PM
System Up Time: 0 Days, 1 Hours, 13 Minutes, 16 Seconds
System Manufacturer: innotek GmbH
System Model: VirtualBox
System Type: X86-based PC
Processor(s):
  1 Processor(s) Installed.
    [01]: x86 Family 6 Model 37 Stepping 5 GenuineIntel ~ 2649 Mhz
BIOS Version: UBOX - 1
Windows Directory: C:\WINDOWS
System Directory: C:\WINDOWS\system32
Boot Device: \Device\HarddiskVolume1
System Locale: en-us;English <United States>
Input Locale: en-us;English <United States>
Time Zone: <GMT-08:00> Pacific Time <US & Canada>; Tijuana
Total Physical Memory: 191 MB
Available Physical Memory: 74 MB
Virtual Memory: Max Size: 2,048 MB
Virtual Memory: Available: 2,009 MB
Virtual Memory: In Use: 39 MB
Page File Location(s): C:\pagefile.sys
Domain: WORKGROUP
Logon Server: \\EHACKING-8A446B
Hotfix(s):
  1 Hotfix(s) Installed.
    [01]: Q147222
Network Card(s):
  1 NIC(s) Installed.
    [01]: AMD PCNET Family PCI Ethernet Adapter
      Connection Name: Local Area Connection 3
      DHCP Enabled: No
      IP address(es)
        [01]: 192.168.1.9

C:\>Documents and Settings\ehacking>
```

The following information has been retrieved:

registered owner	BIOS version
system uptime	system directory
original install date	number of network cards installed

In case of a Linux machine, you can use the following commands:

`cat /proc/meminfo`  
`cat /proc/cpuinfo`

```
root@kali:~# cat /proc/cpuinfo
processor       : 0
vendor_id      : GenuineIntel
cpu family     : 6
model          : 37
model name     : Intel(R) Core(TM) i7 CPU      M 620 @ 2.67GHz
stepping        : 5
microcode      : 0x4
cpu MHz        : 2667.000
cache size     : 4096 KB
physical id    : 0
siblings        : 4
core id         : 0
cpu cores      : 2
apicid          : 0
initial apicid : 0
fdiv_bug        : no
f00f_bug        : no
coma_bug        : no
fpu             : yes
fpu_exception   : yes
cpuid level    : 11
wp              : yes
flags           : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat
      sse sse2 ss ht tm pbe nx rdtscp lm constant_tsc arch_perfmon pebs bts xtopology no
      dq dtes64 monitor ds_cpl vmx smx est tm2 ssse3 cx16 xptr pdcm pcid sse4_1 sse4_2 po
      tpr_shadow vnmi flexpriority ept vpid
bogomips        : 5319.87
clflush size    : 64
```

## PSTools

It comes with multiple command line tools and it was exclusively created for system administrators to perform their administrative operations. You need to get it from the official Microsoft website. Get the file and then extract all the utilities to acquire the volatile data from the suspicious machine. It is the combination of multiple tools and we will discuss them one-by-one (when needed). At this stage, let's try PSInfo utility.

An investigator wants to get the information of the running software on the suspicious machine, so this command-line utility is very handy.



```
C:\Documents and Settings\ehacking\Desktop\PSTools>PsInfo.exe -s "software"
PsInfo v1.27 - Local and remote system information viewer
Copyright <C> 2001-2009 Mark Russinovich
Sysinternals - www.sysinternals.com

System information for \\EHACKING-8A446B:

Applications:
Linphone version 3.6.1
WebFldrs XP 9.50.7523
Zoiper 2.35

C:\Documents and Settings\ehacking\Desktop\PSTools>_
```

### ***Uname – Linux***

If you are a Linux user then you might have heard about this command before. Uname is used to create system profile. If an investigator wants to know the machine name, OS and kernel version then use this command on the suspicious machine.



```
root@kali:~# uname -v
#1 SMP Debian 3.12.6-2kali1 (2014-01-06)
root@kali:~# uname -a
Linux kali 3.12-kali1-686-pae #1 SMP Debian 3.12.6-2kali1 (2014-01-06) i686 GNU/
Linux
root@kali:~# █
```

What activities have been performed after starting the suspicious computer? Yes, it is the most important question that an investigator has to think about, and they should have to find the history of executed commands along with the system date and time. Finding command history along with the date/time is very crucial because you need to make your evidence and the process admissible.

It is not necessary that the current system, date/time is similar to the actual date/time. Find the current system date/time and then document it. Document the date/time after executing every forensic tool.

```

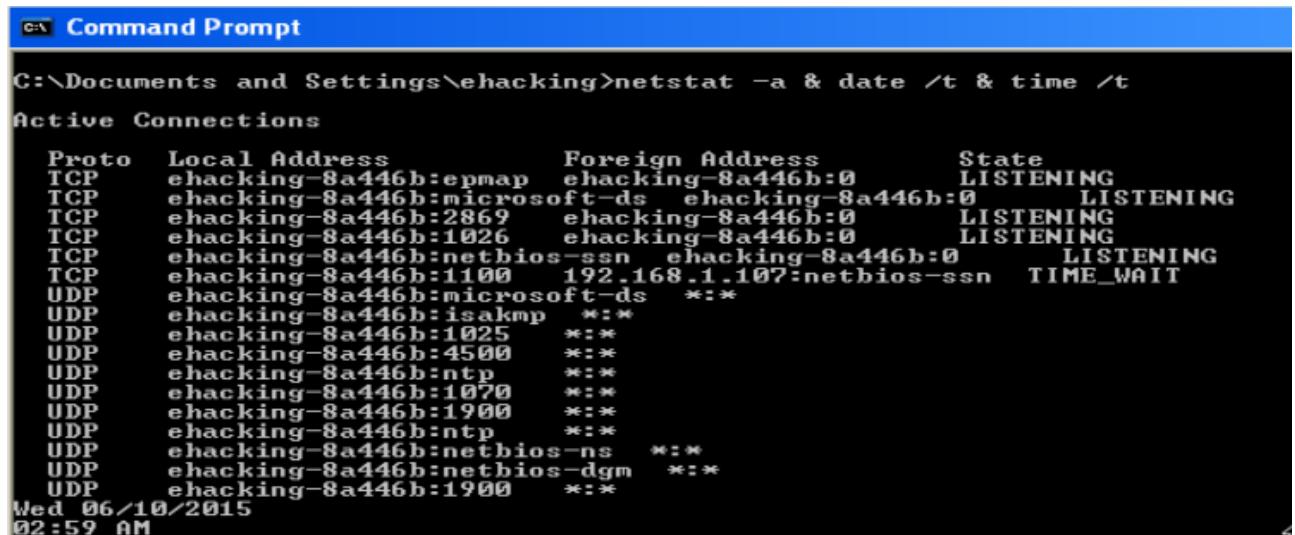
root@kali:~# netstat -a ; date
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address          Foreign Address        State
tcp      0      38 192.168.1.108:37563    199.16.156.70:https   FIN_WAIT1
tcp      0      0 192.168.1.108:34287    173.194.124.0:https  ESTABLISHED
tcp      0      0 192.168.1.108:42072    sb-in-f113.1e100.:https ESTABLISHED
tcp      0      0 192.168.1.108:37572    199.16.156.70:https  ESTABLISHED
tcp      0      0 192.168.1.108:37559    199.16.156.70:https  ESTABLISHED
tcp      0      0 192.168.1.108:45771    173.194.124.41:https ESTABLISHED
tcp      0      0 192.168.1.108:37571    199.16.156.70:https  ESTABLISHED
tcp      0      0 192.168.1.108:34105    173.194.124.22:https ESTABLISHED
tcp      0      0 192.168.1.108:55993    wn-in-f189.1e100.:https ESTABLISHED
tcp      0      0 192.168.1.108:41091    184.173.90.195:sta:http ESTABLISHED
udp      0      0 *:53116                *:*
udp      0      0 *:bootpc               *:*
udp6     0      0 [::]:19628             [::]:*                 

Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type      State       I-Node Path
unix    2      [ ACC ]     STREAM    LISTENING  9084   /root/.cache/keyring-
XSFH1h/control
unix    2      [ ACC ]     STREAM    LISTENING  13334  /root/.cache/keyring-

```

After executing the aforementioned command, an investigator can get lots of valuable information. For example, the incoming and outgoing connection. The important things are to find is whether the attacker has added any user accounts or not, and has the attacker(s) installed any software in the machine?

And here on Windows:



```

C:\Documents and Settings\ehacking>netstat -a & date /t & time /t
Active Connections

 Proto  Local Address          Foreign Address        State
 TCP    ehacking-8a446b:epmap  ehacking-8a446b:0      LISTENING
 TCP    ehacking-8a446b:microsoft-ds  ehacking-8a446b:0      LISTENING
 TCP    ehacking-8a446b:2869  ehacking-8a446b:0      LISTENING
 TCP    ehacking-8a446b:1026  ehacking-8a446b:0      LISTENING
 TCP    ehacking-8a446b:netbios-ssn  ehacking-8a446b:0      LISTENING
 TCP    ehacking-8a446b:1100  192.168.1.107:netbios-ssn  TIME_WAIT
 UDP    ehacking-8a446b:microsoft-ds  *:*
 UDP    ehacking-8a446b:isakmp   *:*
 UDP    ehacking-8a446b:1025  *:*
 UDP    ehacking-8a446b:4500  *:*
 UDP    ehacking-8a446b:ntp    *:*
 UDP    ehacking-8a446b:1070  *:*
 UDP    ehacking-8a446b:1900  *:*
 UDP    ehacking-8a446b:ntp    *:*
 UDP    ehacking-8a446b:netbios-ns  *:*
 UDP    ehacking-8a446b:netbios-dgm  *:*
 UDP    ehacking-8a446b:1900  *:*

Wed 06/10/2015
02:59 AM

```

Make sure to record every activity, documentation is the key, since you need to submit your report to court.

### **Current System Uptime**

You are acquiring volatile data, is it worthwhile? Check the system uptime to know the time when the suspicious machine was started. It also helps you to understand whether the incident occurred during the uptime period or someone else has rebooted after the incident.

For Linux and Windows respectively:

```

root@kali:~# uptime
03:16:02 up 2:09, 3 users, load average: 0.34, 0.35, 0.33
root@kali:~# w -s
03:16:14 up 2:09, 3 users, load average: 0.42, 0.36, 0.34
USER      TTY      FROM          IDLE WHAT
root      tty7      :0           2:09m gdm-session-worker [pam/gdm3]
root      pts/0      :0.0        53:17 /usr/lib/virtualbox/VirtualBox
root      pts/1      :0.0        6.00s w -s

```

```

C:\Documents and Settings\ehacking>net statistics workstation
Workstation Statistics for \\EHACKING-8A446B

Statistics since 6/10/2015 2:24 AM

Bytes received                                8086
Server Message Blocks <SMBs> received          68
Bytes transmitted                             8818
Server Message Blocks <SMBs> transmitted       66
Read operations                               0
Write operations                            0
Raw reads denied                           0
Raw writes denied                          0

Network errors                               0
Connections made                           6
Reconnections made                         0
Server disconnects                         0

Sessions started                           0
Hung sessions                            0
Failed sessions                           0
Failed operations                          0
Use count                                 10
Failed use count                          0

The command completed successfully.

```

## *Legitimate VS Illegitimate Processes*

The first responder investigates the cyber-crime, and a cyber-criminal might inject the malicious software in the suspicious machine before the incident to get the remote access or after the incident to monitor the further activities. Anything is possible; so from the investigation point of view, you should check the current processes of the suspicious machine. The objective is to identify the malicious service, and software running on the machine.

*The key to examine is to have a list of legitimate system and application processes and then compare it with the running processes (PID or process identifier).*

Harlan Carvey in his paper “Windows Forensics and Incident Recovery” has suggested documenting the following information about running processes.

- the process’ executable image
- the command line used to initiate the process
- how long the process has been running
- the security context that it runs in
- modules or libraries (DLLs) it accesses
- memory that the process consumes

Let's try to find the running processes:

1. After executing the following command, several executable files have been identified. Let's take svchost.exe (PID=912) for further analysis:

```
C:\Documents and Settings\ehacking>netstat -ab
Active Connections

  Proto  Local Address          Foreign Address          State      PID
  TCP    ehacking-8a446b:epmap  ehacking-8a446b:0      LISTENING  912
  c:\windows\system32\WS2_32.dll
  C:\WINDOWS\system32\RPCRT4.dll
  c:\windows\system32\rpcss.dll
  C:\WINDOWS\system32\svchost.exe
  -- unknown component(s) --
  [svchost.exe]
```

2. How long has this service (912) been running? PsList has the answer:

```
C:\Documents and Settings\ehacking\Desktop\PSTools>pslist svchost
pslist v1.3 - Sysinternals PsList
Copyright <C> 2000-2012 Mark Russinovich
Sysinternals - www.sysinternals.com

Process information for EHACKING-8A446B:

Name           Pid  Pri Thd  Hnd   Priv     CPU Time   Elapsed Time
svchost        832   8   16   192   2924    0:00:00.030   1:29:19.756
svchost        912   8   10   258   1636    0:00:00.050   1:29:19.586
```

3. And how much virtual memory is this process (912) consuming at the moment? Again Pslist with a specific command.

```
C:\Documents and Settings\ehacking\Desktop\PSTools>pslist -me svchost
pslist v1.3 - Sysinternals PsList
Copyright <C> 2000-2012 Mark Russinovich
Sysinternals - www.sysinternals.com

Process memory detail for EHACKING-8A446B:

Name           Pid      UM      WS      Priv  Priv Pk  Faults  NonP  Page
svchost        832  60424  4372   2924  23176  1258      5    70
svchost        912 34680  3844   1636  1640  1109     13    66
```

4. Apart from the processes, what services are running? Use *PsService* command.

Again, are you documenting everything? If not, then at the end of the investigation you will have nothing in hand. Make sure you are documenting because you are left with no other choice.

5. Use Pslist to find valuable information of the suspicious machine:

Pri: Priority	WS: Working set	Thd: Number of threads
WSPk: Working set peak	Hnd: Number of handles	Priv: Private memory
VM: Virtual memory	NonP: Non-paged memory	Mem: Memory usage

Process information for EHACKING-8A446B:										
Name	Pid	Pri	Thd	Hnd	Priv	CPU Time		Elapsed Time		
Idle	0	0	1	0	0	0:05:10.746		0:00:00.000		
System	4	8	50	247	0	0:00:01.952		0:00:00.000		
smss	352	11	3	21	168	0:00:00.020		0:05:13.640		
csrss	524	13	11	392	1744	0:00:00.250		0:05:13.450		
winlogon	548	13	21	509	6632	0:00:00.270		0:05:13.390		
services	668	9	16	256	1888	0:00:00.270		0:05:13.340		
lsass	680	9	20	327	3564	0:00:00.090		0:05:13.320		
svchost	832	8	18	195	2944	0:00:00.020		0:05:13.280		

What about Linux? Let's look into the Forensic tools to be used for Linux machine:

### For Linux

“*Top*” is the command that needs to be executed in the terminal to find the running processes. It prints result after sorting, the most CPU-intensive tasks are at top. Here you can see the process ID, time and most importantly the executed command to run the process.

```
top - 19:57:52 up 3:32, 3 users, load average: 0.38, 0.61, 0.59
Tasks: 157 total, 2 running, 155 sleeping, 0 stopped, 0 zombie
%Cpu(s): 3.0 us, 3.5 sy, 0.5 ni, 91.4 id, 0.3 wa, 0.0 hi, 1.3 si, 0.0 st
KiB Mem: 4008652 total, 3428512 used, 580140 free, 86400 buffers
KiB Swap: 8103932 total, 0 used, 8103932 free, 2492932 cached

PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND
6536 root 20 0 535m 261m 246m S 11.6 6.7 2:11.48 VirtualBox
```

### PS

Apart from *top*, we have another command that provides the information of the current running processes, ID, CPU usage, memory usage and other useful information.

\$ ps ax	To get the full list of running processes
\$ ps -ef	
\$ ps -U user	Find the other system users running processes
\$ ps -C program_name	Find the history of a particular program
\$ ps -A	View all the processes
\$ ps r	View the running process only

```
root@kali:~# ps -A
  PID TTY      TIME CMD
    1 ?        00:00:01 init
    2 ?        00:00:00 kthreadd
    3 ?        00:00:53 ksoftirqd/0
    5 ?        00:00:00 kworker/0:0H
    7 ?        00:00:02 migration/0
    8 ?        00:00:00 rcu_bh
    9 ?        00:00:07 rcu_sched
   10 ?        00:00:00 watchdog/0
   11 ?        00:00:00 watchdog/1
   12 ?        00:00:02 migration/1
   13 ?        00:00:00 ksoftirqd/1
   15 ?        00:00:00 kworker/1:0H
   16 ?        00:00:00 watchdog/2
```

### **Volatile evidence from Network:**

#### **Fport:**

We have another forensics tool to discuss; the objective is to find the open TCP/IP and UDP ports and what applications are listening on those ports. An investigator should map the ports to the running processes and you should document the process identification number and the path.

You can download the fport from [Mcafee website](#).

```
C:\Documents and Settings\ehacking\Desktop\fport>Fport
FPort v2.0 - TCP/IP Process to Port Mapper
Copyright 2000 by Foundstone, Inc.
http://www.foundstone.com

  Pid  Process          Port  Proto Path
  912  System           ->  135   TCP
  4   System           ->  139   TCP
  4   System           ->  445   TCP
  468  System           ->  1027  TCP
  1156 System           ->  2869  TCP
  0   System           ->  2869  TCP
  0   System           ->  123   UDP
  0   System           ->  137   UDP
  0   System           ->  138   UDP
  912  System           ->  445   UDP
  4   System           ->  500   UDP
  1156 System           ->  1025  UDP
  0   System           ->  1026  UDP
  0   System           ->  1101  UDP
  0   System           ->  1900  UDP
  468  System           ->  4500  UDP
```

The key to this test is to find and examine associated (with suspicious machine) IP addresses with their open ports. By examining network information, the first responder may easily get an idea whether the incident happened remotely or locally. During the evidence gathering process, look for unfamiliar or abnormal open ports with the services running, you may get the trace of RAT (remote administrative tools) or any other type of backdoor.

Apart from fport, you can also use the netstat -an command to get the communication history:

```
C:\Documents and Settings\ehacking\Desktop\fport>netstat -an
```

#### Active Connections

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	127.0.0.1:1027	0.0.0.0:0	LISTENING
TCP	192.168.1.9:139	0.0.0.0:0	LISTENING
UDP	0.0.0.0:445	*.*	
UDP	0.0.0.0:500	*.*	
UDP	0.0.0.0:1025	*.*	
UDP	0.0.0.0:4500	*.*	
UDP	127.0.0.1:123	*.*	
UDP	127.0.0.1:1026	*.*	
UDP	127.0.0.1:1900	*.*	
UDP	192.168.1.9:123	*.*	
UDP	192.168.1.9:137	*.*	
UDP	192.168.1.9:138	*.*	
UDP	192.168.1.9:1900	*.*	

*Netstat -anb* is also a very useful command that displays the list of TCP/IP connection, protocol, local or MAC addresses and IP addresses.

In the following screen, you can see the local and remote IP, protocol, status and PID of a service.

```
C:\Documents and Settings\ehacking\Desktop\fport>netstat -anb
```

#### Active Connections

Proto	Local Address	Foreign Address	State	PID
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	912
c:\windows\system32\WS2_32.dll				
C:\WINDOWS\system32\RPCRT4.dll				
c:\windows\system32\rpcss.dll				
C:\WINDOWS\system32\svchost.exe				
-- unknown component(s) --				
[svchost.exe]				
TCP	0.0.0.0:445 [System]	0.0.0.0:0	LISTENING	4
TCP	127.0.0.1:1027 [alg.exe]	0.0.0.0:0	LISTENING	468
TCP	192.168.1.9:139 [System]	0.0.0.0:0	LISTENING	4
UDP	0.0.0.0:500 [lsass.exe]	*.*		680
UDP	0.0.0.0:445 [System]	*.*		4

Other native windows commands are also useful in getting volatile network evidences, *NBTstat -s* shows the connection of the local suspicious machine with the remote IP so that an investigator can map the shared resources on the network.

#### Net

The Net command has various functions, user accounts policy, shared resources on the network, network statistics and many other information can be acquired. Let say *net share* to find the information of the share folder and other shared resources, for example a printer.

```
C:\Documents and Settings\ehacking\Desktop\fport>net share
```

Share name	Resource	Remark
ADMIN\$	C:\WINDOWS	Remote Admin
C\$\	C:\	Default share
IPC\$		Remote IPC

The command completed successfully.

You don't need to get any forensics tool at the moment to investigate the suspicious Linux machine. Linux native commands are handy and they provide a great deal of information to the investigator.

Active Internet connections (w/o servers)					
Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State
Active UNIX domain sockets (w/o servers)					
Proto	RefCnt	Flags	Type	State	I-Node Path
unix	12	[ ]	DGRAM	8053	/dev/log
unix	3	[ ]	STREAM	CONNECTED	50441
unix	3	[ ]	STREAM	CONNECTED	13740
unix	3	[ ]	STREAM	CONNECTED	13527 @/tmp/dbus-oR7S9ZGcP
unix	2	[ ]	DGRAM		10566
unix	3	[ ]	STREAM	CONNECTED	69690 @/tmp/dbus-oR7S9ZGcP
unix	3	[ ]	STREAM	CONNECTED	11252 /var/run/dbus/system
bus_socket					
unix	3	[ ]	STREAM	CONNECTED	13484
unix	3	[ ]	STREAM	CONNECTED	11897

On the above screen you can see the protocol, status of the process, the path of the program that is running and other useful information.

### ***Logged on Users***

In this section, we will try to extract the information of the legitimate users on the suspicious machine. What is the total number of authorized users? Moreover, what are their names and profiles? Access time, remote access or local access?

PSLoggedon: is the part of Pstools and it allows you to see the locally and remotely logged on users:

```
C:\Documents and Settings\ehacking\Desktop\PSTools>PSloggedon
PsLoggedon v1.34 - See who's logged on
Copyright <C> 2000-2010 Mark Russinovich
Sysinternals - www.sysinternals.com

Users logged on locally:
 6/10/2015 9:23:23 PM      EHACKING-8A446B\ehacking

No one is logged on via resource shares.

C:\Documents and Settings\ehacking\Desktop\PSTools>_
```

*Net user*: It is the native windows command to find the local and remote users of the suspicious machine.

```
C:\Documents and Settings\ehacking\Desktop\PSTools>net user
User accounts for \\EHACKING-8A446B

Administrator          ehacking
HelpAssistant          SUPPORT_388945a0
The command completed successfully.
```

On Linux machine, *last* is one of the important command. It allows an investigator to see history of logged on users local or remote.

```
root@kali:~# last
root      pts/2      :0.0          Thu Jun 11 01:54  still logged in
root      pts/1      :0.0          Thu Jun 11 00:44  still logged in
root      pts/1      :0.0          Wed Jun 10 23:26 - 00:44  (01:17)
root      pts/0      :0.0          Wed Jun 10 21:22  still logged in
root      tty7       :0           Wed Jun 10 20:49  still logged in
(unknown tty7   :0           Wed Jun 10 20:46 - 20:49  (00:03)
reboot    system boot 3.12-kali1-686-p Wed Jun 10 20:46 - 01:55  (05:09)
root      pts/1      :0.0          Wed Jun 10 19:57 - 20:18  (00:20)
root      pts/0      :0.0          Wed Jun 10 19:34 - crash  (01:11)
```

Locate the, etc. directory on the terminal and then open the *passwd* file, this file contains user account information with the encrypted passwords.

```
root@kali:~# cd /etc
root@kali:/etc# cat passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
```

## **Evidence Management**

In the previous topics, you have learned to find and gather the volatile data/evidence. Getting evidence is not enough; management of evidence is the art. Strict policies and procedures should be created to manage the evidence. Make sure to maintain the integrity of the data, chain of custody should not be broken. Evidence management guide should be created and your organizational policy should emphasize to implement it. Key points to ponder:

- Create a list of possible data that can be retrieved from the list of devices
- From where the electronic device retrieved
- What are the methodology to store the evidence? Make the place secure, limit the access rights
- Make sure that you can do all the process again and it will provide the same result
- Document everything, every tool that you are using, every process and everything

You need to carefully manage the evidence and if you failed, then you will most likely to fail in the proceedings.

## **Modes of Attack**

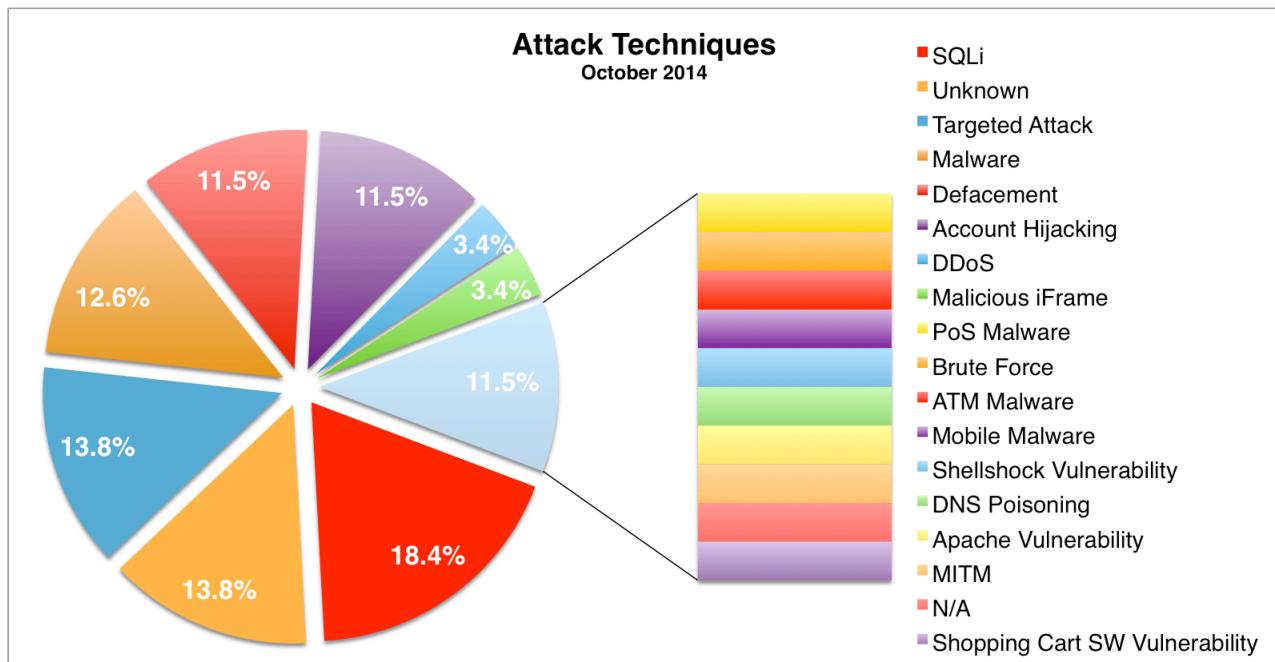
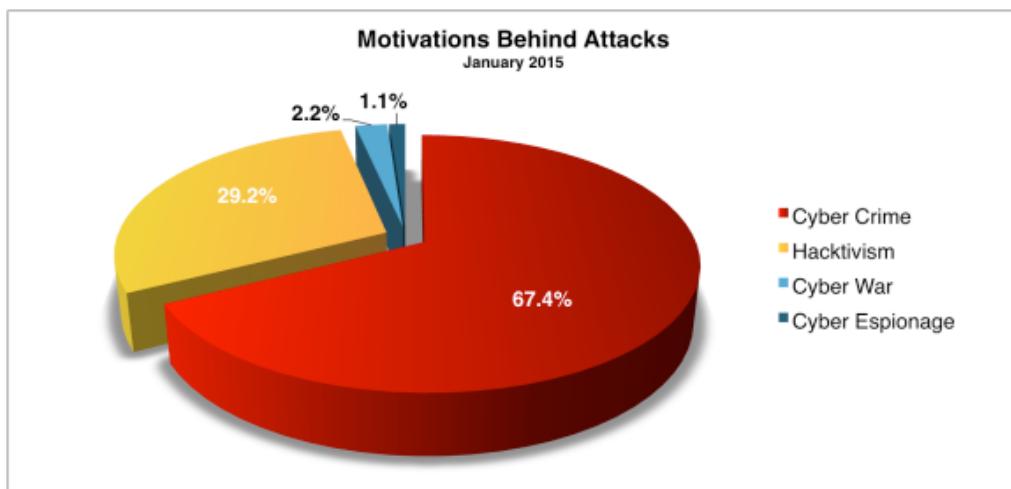
Computer forensics and digital investigation depend on the nature of cyber-crime occurred. First, the identification of the crime informs the investigator to take the possible steps. What are the mode

of cyber-attack, and what is cyber-crime? What kind of crime should an investigator investigate? In this section, the answers of the aforementioned questions will be addressed. We can generally divide the mode of attack into two types:

- Internal or insider attacks
- External or outsider attacks

Some statistics:

- Survey results given on cybersenate.com shows the motivation of the attack is cyber-crime
- Result mentioned on hackmageddon.com shows that SQL-injection is the most common type of cyber-attack in 2014.



A few examples of cyber-crime:

- Financial frauds
- Laptop or other device theft

- Insider Internet abuse
- Data theft
- Unauthorized access whether locally or remotely
- Viruses, worms and backdoor
- Denial of service attack
- and many more...

## ***Computer Forensics - Systematic Approach***

An investigator should have a standard guideline and steps to use during the investigation, which we call a systematic approach. Every step is based on specific reasons and they are linked together. Systematic approaches may differ, and it depends on the local laws and your own organization policy.

1. **Initial assessment of the case:** Before starting the actual investigation, you should look at the broader prospective of the case and the possible outcomes. Keep in mind that you have to be suspicious of everyone and everything. Do not try to imagine the result at first, because if you do so then you unintentionally work in that particular direction. Communicate with the relevant people about the incident; try to gather as much information as you can.  
What is the nature of the case? What is the situation after the incident?
2. **Create a design to approach the case:** You should have everything, every possible step in your mind and you should write them down. Create the process to handle this particular case. How you are going to approach the authority, the victim and the suspect? How you are going to seize the machines? What legal documents you might need to do this and how you are going to get the legal documents?
3. **Required resources:** What resources this case might require? Human resources, technical, and the software that required. Do you have the necessary software or do you need to get it? If you need assistance from any other company or team, this also comes under the required resources, create the list and get them at first place.
4. **Identify the risks:** Risk assessment should be done to evaluate the possible risks that are involved in the particular case. Based on the experience, your organization should have the list of possible problems occurred during an investigation, even you can judge the risk based on your own experience. After identification, take the necessary steps to minimize or mitigate the risks.
5. **Analyze the data:** This is the time to collect/gather evidence from the captured devices, use the software and processes that you have defined earlier to extract the information.
6. **Investigation:** All right, you have collected the data. Now investigate the extracted evidence and point out the culprit.
7. **Complete report:** Creation a report is very important; write a complete report; mentions the taken steps, tools/processes and the outcomes.
8. **Critique the case:** Self-evaluation is the key, since you need to forward your report to court. After completing the report, you should thoroughly review the entire case. Find your weaknesses and improve them for future cases.

## Module 2: Legal Aspects of Computer Forensics

Anyone doing computer forensics must aware of the legal aspect and implication of the case. You can't simply investigate or seize any machine without following the proper laws and regulations. The legal aspects are important, since the case will go to the court and apart from the hearing, you need to follow laws while investigating otherwise you will find yourself in trouble.

### Legal Process:

The legal process depends on your local laws and rules. Somehow, we can make a standard process because every case should have the following in it:

- Complaint
- Investigation
- Prosecution

The aforementioned steps are actually the stages of a case. In the first stage, a complaint received, the investigator will investigate the complaint, and with the help of prosecutor, collect, analyze and report to build a case.

You can't start a criminal investigation by yourself. A criminal investigation requires evidence of an illegal act. If evidence is not found, then the criminal investigation cannot be started. Someone should inform the local police about the crime that has been committed and based on receiving the complaint the further investigation would be started. At the very first step, the local police investigate the crime. They report the type of the case to the top management and then a specialist will be assigned to look after the case.

Not every policeman is not a computer expert. Sometimes they only know the basics about digital devices. During the seizure process, they might damage the critical evidence. To avoid any mishaps, CTIN has defined levels of law enforcement expertise. Bill Nelson, Amelia & Christopher Steuart have also mentioned in their book:

1. The Police officer is responsible for acquiring and seizing the digital evidence on the crime scene.
2. Managing high-tech investigations, teaching investigators what to ask for, and understanding computer terminology and what can and can't be retrieved from digital evidence. The assigned detectives usually handle the case.
3. Specialist training in retrieving digital evidence, normally conducted by a data recovery or computer forensics expert, network forensics expert, or Internet fraud investigator. This person might also be qualified to manage a case, depending on his or her background.

You, as an investigator should have knowledge and expertise of computer forensics, and how to handle cyber-crime cases. You have to judge the level of expertise of the other team members and assign their roles, responsibilities and the expected performance. Follow the systematic approach discussed in the previous chapter, look for the evidence and then create a strong case supported by the evidences.

Your job as a computer investigator is to investigate the digital devices, extract the evidence and create the report. From this point onward, the job of a prosecutor is started. As an investigator, you need to submit the final report with the evidences to the government attorney, the level of authority depends on the nature of the case, and your local laws.

Computer forensics is comparatively a new field of study to the court and many of the existing laws used to prosecute computer-related crimes, legal precedents, and practices related to computer forensics are in a state of flux. The United States Department of Justice's Cyber-crime Web Site is the rich source to get the latest updates even case study of the cyber-crime cases. You can find the available guides on evidence management and other topics related to computer forensics. As it was discussed that you should collect evidence in a way that is legally admissible in a court.

There are two core areas of law related to cyber-crime.

1. U.S. Constitution

- 4th Amendment “Protection against unreasonable search and seizure”
- 5th Amendment “Protection against self-incrimination”

2. U.S. Statutory Law

- 18 U.S.C. 2510-22 (The Wiretap Act )
- 18 U.S.C. 3121-27 (The Pen Registers and Trap and Trace Devices Statute)
- 18 U.S.C. 2701-12 (The Stored Wired and Electronic Communication Act)

Although the amendments were written before there were problems occurred by misusing the electronic devices, the principles in them apply to how computer forensics is practiced.

## **U.S. Constitution:**

### **4<sup>th</sup> Amendments:**

*“The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized. ”*

See the following excerpt from a U.S. Department of Justice Manual, you can see that the 4<sup>th</sup> amendments can be applied in computer cases:

*“When confronted with this issue, courts have analogized electronic storage devices to closed containers, and have reasoned that accessing the information stored within an electronic storage device is akin to opening a closed container. Because individuals generally retain a reasonable expectation of privacy in the contents of closed containers, see United States v. Ross, 456 U.S. 798, 822-23 (1982), they also generally retain a reasonable expectation of privacy in data held within electronic storage devices. Accordingly, accessing information stored in a computer ordinarily will implicate the owner’s reasonable expectation of privacy in the information. See United States v. Barth, 26 F. Supp. 2D 929, 936- 37 (W.D. Tex. 1998) (finding reasonable expectation of privacy in files stored on hard drive of personal computer); United States v. Reyes, 922 F. Supp. 818, 832- 33 (S.D.N.Y. 1996) (finding reasonable expectation of privacy in data stored in a pager); United States v. Lynch, 908 F. Supp. 284, 287 (D.V.I. 1995) (same);*

*United States v. Chan, 830 F. Supp. 531, 535 (N.D. Cal. 1993) (same); United States v. Blas, 1990 WL 265179, at \*21 (E.D. Wis. Dec. 4, 1990) (“[A]n individual has the same expectation of privacy in a pager, computer, or other electronic data storage and retrieval device as in a closed container.”).*

The 4<sup>th</sup> amendment gives power to the general public and protects them from unreasonable searches and seizures. In general, the principles set forth by the 4th amendment provide for individuals to enjoy a “reasonable expectation of privacy.” Network administrator and even investigator have to understand that the individual is allowed to enjoy the privacy. Some key points that you should understand are:

- The 4<sup>th</sup> amendment only restricts the right of Government agent, not the private individuals (you should consult with the legal adviser to find out whether your organization can be considered “Government” or not).
- The level of expected privacy is substantially less outside of the home, although not eliminated.
- In case, if the item protected by the 4<sup>th</sup> amendment lost; the privacy enjoyed from this amendment is also dissolved. If it finds that the process, methodology and tools have violated 4<sup>th</sup> amendment while recovering the evidence, then the information or evidence will become inadmissible by the courts.

## 5<sup>th</sup> Amendments:

You need to carefully understand the 5<sup>th</sup> amendment because it directly affects the cryptography, as stated that:

*“No person shall be compelled in any criminal case to be a witness against himself.”*

As mentioned in the paper “Center for Democracy and Technology. Impact of the McCain-Kerrey Bill on Constitutional Privacy Rights”:

*Under the Fifth Amendment, an individual cannot be compelled to testify to his or her memorized key.*

The word memorized is very important in this context; keep in mind that the key (passkey) is never written on anywhere. The 5<sup>th</sup> amendment protects an individual from being compelled to provide the incriminating testimony. Remember, it does not provide protection if the evidence is written somewhere.

## U.S Statutory Law

Anyone without the restriction of their profession, concerned with computer forensics must know the following statutory law:

- 18 U.S.C. 2510-22 (The Wiretap Act )
- 18 U.S.C. 3121-27 (The Pen Registers and Trap and Trace Devices Statute)
- 18 U.S.C. 2701-12 (The Stored Wired and Electronic Communication Act)

These laws highly affects the work process and methodology of the first responder, computer administrator and anyone collecting computer records and working on digital investigation.

The first two laws (18 U.S.C. 2510-22 & 18 U.S.C. 3121-27) are dealing with real time electronic communication, while the third law (18 U.S.C. 2701-12) deals with stored data of the electronic communication.

Let discuss the real-time electronic communication first. Before discussing the exceptions and prohibited acts, we should discuss the electronic communication based on OSI model.

The wiretap act and pen trap/trace act both deal with real time communication; however, they focus on different aspects of this communication. The real time communication can further be divided into two parts:

- Content

- Non-content

In every communication, both the aforementioned information are there, so what data should be treated as non-content and what should be treated as the actual content? I will explain the both from the OSI point of view. OSI is a seven layer theoretical model that explain the flow of electronic communication; these two laws are act on the following layer of OSI model:

Pen trap/trace act	<ul style="list-style-type: none"> <li>• Data link layer (2)</li> <li>• Network layer (3)</li> <li>• Transport layer (4)</li> </ul>	Non-content
Wiretap act	<ul style="list-style-type: none"> <li>• Session layer (5)</li> <li>• Presentation layer (6)</li> <li>• Application layer (7)</li> </ul>	Content

## Wiretap Act Electronic Communication Privacy Act

The law prohibited:

*“intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication.”*

Wiretap act prohibits the interception of real time electronic communication so you should think twice before using the sniffing tools like wireshark, ethereal, TCPdump, etc.<sup>1</sup> There are some exceptions and you should find a way out through them.

Keep in mind that this law does not restrict to gather or intercept signaling information, however pen trap/trace act restrict the intercept of signaling information.

## Pen/Trap & Trace Act 18 U.S.C. §§ 3121-27

This act prohibits from getting this signaling information for, example, routing info, dialing codes and other outgoing signaling information. The law says:

*“no person may install or use a pen register or a trap and trace device without first obtaining a court order under section 3123 of this title or under the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.).”*

So what does pen register, trap and trace means? Well, the legal document provides the admissible definition and they are:

18 U.S. Code § 3127(4):

*the term “trap and trace device” means a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication;*<sup>2</sup>

## Stored Wire and Electronic Communication Act - 18 U.S.C. §§ 2701-12

Unlike the two acts discussed in the previous topics, stored wire & electronic communication act deals with the stored information of any communication. Apart from this statute, there are HIPAA & FERPA too. They also deal with the level of protection, access & disclosure of stored

---

1 <https://www.law.cornell.edu/uscode/text/18/2511>

2 <https://www.law.cornell.edu/uscode/text/18/part-II/chapter-206>

communication. Some prohibitions are:

1. “*a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service;*”
2. “*a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service*”

### ***Intellectual Property laws:***

Intellectual properties are the rights own by individual or a group of people (organization) over their own creation, creation including the content, logo and other properties. Intellectual property laws can be further divided into copyright laws, trademark and trade secret laws, etc.

#### **17 U.S. Code § 506 - Criminal offenses**

This particular law is about copyright and it address the following areas:

- Criminal Infringement  
*(Any person who willfully infringes a copyright shall be punished)*
- Forfeiture, Destruction, and Restitution
- Fraudulent Copyright Notice
- Fraudulent Removal of Copyright Notice
- False Representation
- Rights of Attribution and Integrity

*“Any person who, with fraudulent intent, removes or alters any notice of copyright appearing on a copy of a copyrighted work shall be fined not more than \$2,500”*

*“Any person who knowingly makes a false representation of a material fact in the application for copyright registration provided shall be fined”*

#### **18 U.S. Code § 2320 - Trafficking in counterfeit goods or services (Trademark)**

Legal definition of the term traffic is:

*“to transport, transfer, or otherwise dispose of, to another, for purposes of commercial advantage or private financial gain, or to make, import, export, obtain control of, or possess, with intent to so transport, transfer, or otherwise dispose of”*

This particular law is related to the copyrighted content (document, text, video, audio) and the registered trademark. This law is aim to restrict the transfer of content by using any means (for example email, USB drive, CD/DVD and other media) and it restricts the usage of the stuff for any commercial or even a financial gain.

According to 18 U.S. Code § 2320(b)(a)) the penalty would be:

*“...shall be fined not more than \$2,000,000 or imprisoned not more than 10 years, or both...”*

As a computer forensics investigator, you should always seek legal advice, because it is the part of your job. Follow the rules and regulations and create a strong case supported by evidence and by

following laws. This is the end of second module; we will discuss the file system from the next module.

## Module 3: File System structure & Architecture

It is crucial for a computer forensics investigator to understand the file system of multiple operating systems, how they create/modify files and how they interact with storage devices (hard-drive, USB, etc.). What kind of the storage devices do we have and what are their structures. This module discusses the technicalities of modern computer devices with the aim to provide the inside and understanding of storage medium and architecture of the current famous operating systems.

### Storage Media:

Generally, there are two types of disk drives or storage media for that matter:

- Fixed storage
- External or removal storage

As a computer user, you must have used both types of drives, and you must know the basic difference between both drives. This chapter does not aim to differentiate drive with another type of drive, but this chapter aims to discuss the structure of different drives. Yes, fixed storage are the built-in storage space available in any electronic device and the external or removal is the one that you can plug and play with. The rapid growth in computer industry has introduced many storage mediums, apart from the traditional media types, for example hard-drive and CD (compact disk), files can be stored in USB drive, mp3 player, mobile phones, digital camera, etc.

### Hard Drive

To understand the *file*, file system, how OS interact with storage media (hard-drive), how the flow of information works, etc., you need to understand the physical or hardware of hard-drive. It is also important to understand the place where data actually store, so that you will be able to retrieve it during your investigation. A hard drive is made up of one or more platters coated with magnetic material, data stored or recorded magnetically onto the disk. Following are the important components of the hard-drive:

- Platter
- Head
- Tracks
- Cylinder
- Sector

The platter is the place where data stored magnetically, so platter is one of the important component of the hard-drive. The hard-drive platter is made up of aluminum alloy, glass and ceramic is also used in the creation of platter. It is important to understand that the area where data stores composed of magnetic media coating done by iron oxide substance. Data is stored on the both front and back sides of the platter which is also known as **side0** and **side1**. The data of each platter are physically stored into tracks and sectors.



Image source: [https://media.licdn.com/mpr/mpr/shrinknp\\_800\\_800/p/8/005/0a2/349/2636bc8.jpg](https://media.licdn.com/mpr/mpr/shrinknp_800_800/p/8/005/0a2/349/2636bc8.jpg)

- The head is the actual device that reads and writes data on platter, hard-drive consists of multiple platters with heads inserted between them, head can read both sides of the platter.

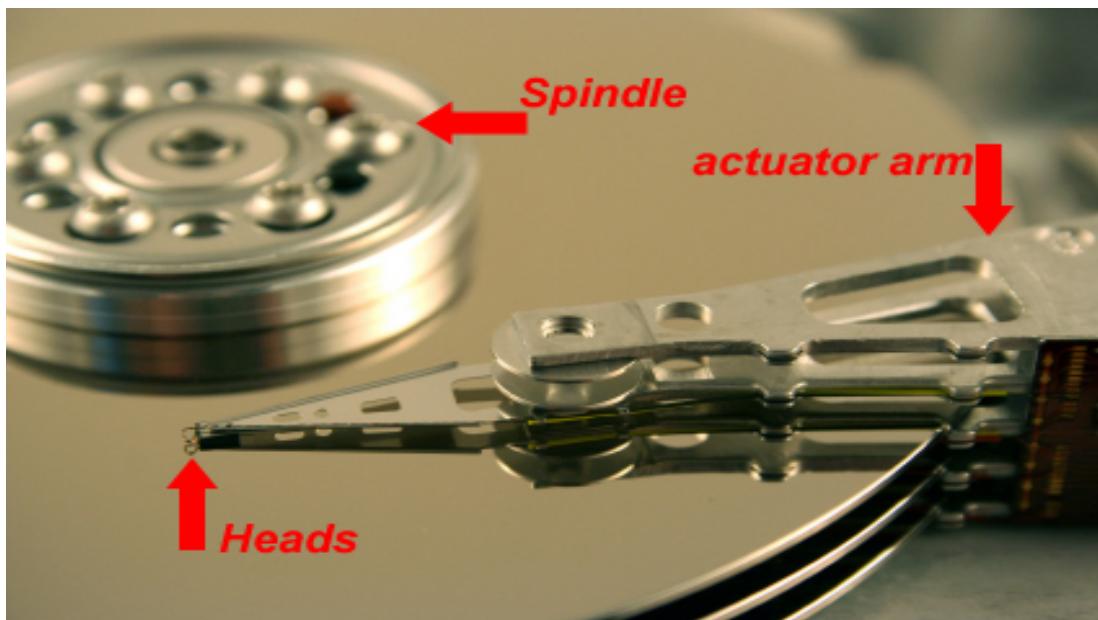


Image source: <http://www.dtidatarecovery.com/resourcecenter/harddrive.jpg>

- Tracks are the part of platter; a track is an individual concentric circle on the platter where data recorded. Every track has its own unique identification number for tracking, and the number starts from 0 at outer edge and moves an inner portion till the center of the circle reaching the value around 1023. Head access the track in one position at a time, and a single

hard-drive consists of more than a thousand of the tracks.

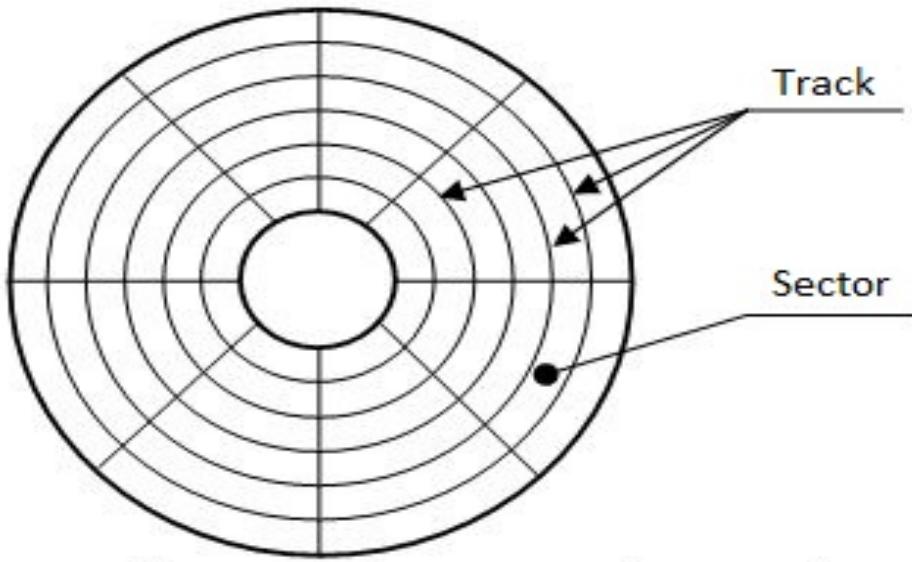


Image source: <http://recover-tools.com/wp-content/uploads/2014/09/2.jpg>

- Cylinder is a combination of tracks, or cylinder is a column of tracks and formed when tracks are lined up.
- Sector is the small storage section on the track which divides it. The size of a sector is 512 bytes.

The maximum storage of the hard-drive can determine by a mathematical formula that needs input information of the hardware of that drive:

**Bytes on a disk** = Number of cylinders \* Number of heads \* Number of sectors (group of 512 or more bytes)

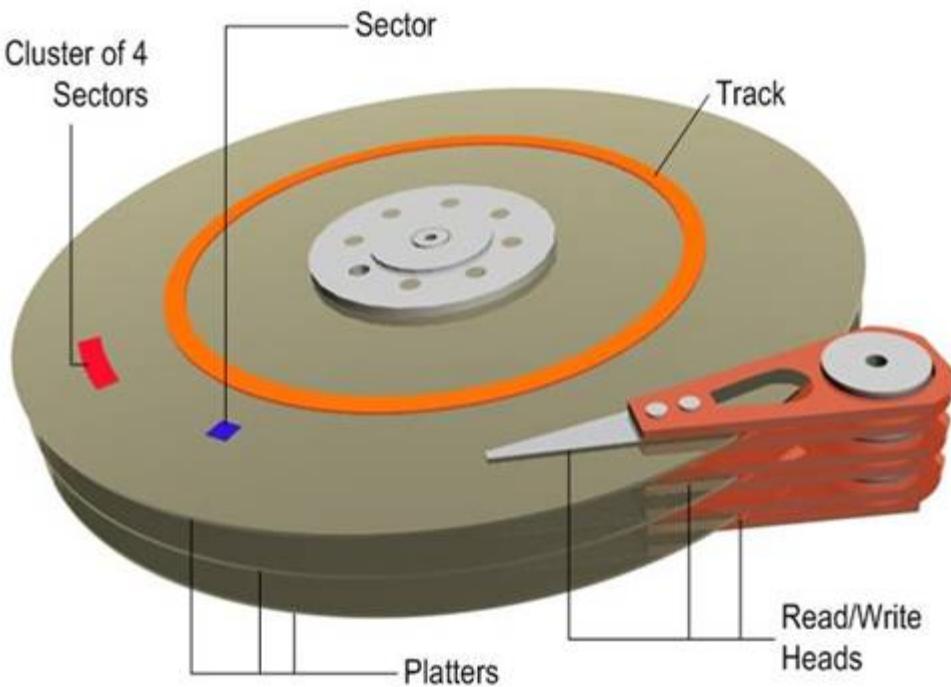
Let say:

Cylinder	= 1024
Heads	= 32
Sectors	= 63

$$\text{Bytes on a disk} = 1024 * 32 * 63 = 2064384 \text{ sectors}$$

where 1 sector is equals to 512 bytes, hence:

$$\text{Bytes on a disk} = 2064384 * 512 = 1056964608 \text{ or } \mathbf{1.056 \text{ GB}}$$



*image source: <https://i-technet.sec.s-msft.com/dynimg/IC306536.jpg>*

In the above picture, you can see the important components of the hard-drive, there functions have already been discussed, so lets move on further.

### Cluster:

Cluster is an important component that we should discuss, it is somehow linked to the sector discussed above or it may be referred as the group of sectors. The cluster is an allocation unit and a space allocated for files and directories to be stored. The minimum size can be one sector/cluster. If small files store on a file system with large cluster will waste the disk space, and this wasted space is called **slack space**. Cluster size or number of cluster is always calculated of an exponent of 2.

$$1 \text{ sector} = 2^0$$

$$8 \text{ sectors} = 2^3$$

## How to determine the Cluster size:

Open the command prompt and type chkdsk to check the hard disk:

```
C:\Documents and Settings\ehacking>chkdsk
The type of the file system is NTFS.

WARNING! F parameter not specified.
Running CHKD SK in read-only mode.

CHKD SK is verifying files (stage 1 of 3)...
File verification completed.
CHKD SK is verifying indexes (stage 2 of 3)...
Index verification completed.
CHKD SK is verifying security descriptors (stage 3 of 3)...
Security descriptor verification completed.

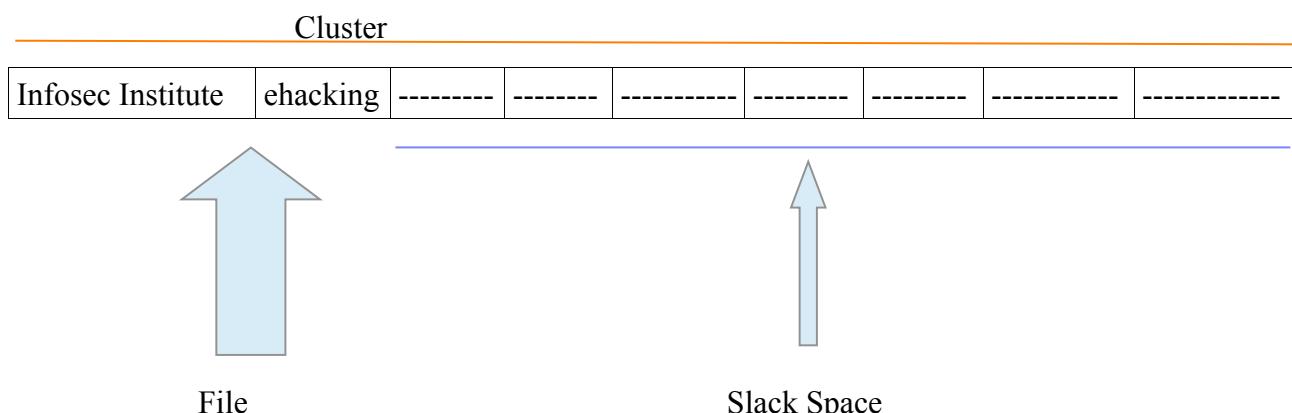
10474348 KB total disk space.
 1571664 KB in 10455 files.
   2688 KB in 730 indexes.
      0 KB in bad sectors.
   66600 KB in use by the system.
  54432 KB occupied by the log file.
 8833396 KB available on disk.

 4096 bytes in each allocation unit.
 2618587 total allocation units on disk.
 2208349 allocation units available on disk.

C:\Documents and Settings\ehacking>_
```

Here you can see “**4096**” bytes in each allocation, allocation unit is the cluster actually. Hence the size is 4096 bytes.

## Slack Space:



Refer to the concept created above, slack space is the free or unused space in a cluster, this space is available between the end of the actual file and the allocated data unit (end of cluster).

Slack space and investigating slack space are way too important for forensics expert because this space can contain salient information about the suspect and evidence can be retrieved from this space. For example, if suspect deleted all of the files and directories that filled the entire cluster and then saved or created some new files that filled half of the cluster only to mislead the investigator, the other half of the cluster may have the information of the deleted file which can be retrieved and can be used as evidence against the suspect.

## File System & Structure

A file or a data file is a collection of data and information grouped under one particular name called file name. The file can be made up of many data types for example, audio, video, text, etc.

The file system is the workflow, process and method that defines how the data is stored and where they are placed on logical volumes. The logical volume is the result of the partition process, and it is a partition acting as a single entity that has been formatted with a file system. Understanding the file system is crucial for forensics investigator, as you must know the location and distribution of various types of files and how they structured on mapped in the memory.

Before the hard drive or any other storage media are used to store the file, the disk must be partitioned and formatted into multiple logical volumes. In the Microsoft Windows file system, the logical units are labeled as C, D, E, F and so on. Hidden partitions can also be created to hide the intended data; this space can be created between the primary partition and the first logical partition. This unused space is referred as **partition gap**, hidden data can alter by using the disk editor utility.

Different operating systems may have different file systems and structure. However, there are some common traits that you can find in every file system, for example, the concept of directories and files.

## Types of File System

File system can further divided into four types:

- *Disk file system*: Manage data or files in the storage devices
- *Network file system (NFS)*: Run network services and structure
- *Database file system*: Instead of hierarchical structured management, files identified by their characteristics
- *Special purpose file system*

List of file systems are available on many websites even on Wikipedia, here are most common types of file system:

### ***Disk file system***

- ADFS – Acorn filing system, successor to DFS.
- BFS – the Be File System used on BeOS
- EFS – Encrypted file system, An extension of NTFS
- EFS (IRIX) – an older block filing system under IRIX.
- Ext – Extended file system, designed for Linux systems
- Ext2 – Extended file system 2, designed for Linux systems
- Ext3 – Extended file system 3, designed for Linux systems, (ext2+journalling)
- FAT – Used on DOS and Microsoft Windows, 12 and 16 bit table depths
- FAT32 – FAT with 32 bit table depth
- FFS (Amiga) – Fast File System, used on Amiga systems. Nice for floppies, but useless on hard drives.
- FFS – Fast File System, used on \*BSD systems
- Files-11 – OpenVMS file system
- HFS – Hierarchical File System, used on older Mac OS systems

- FS – and PFS2, PFS3, etc. Technically interesting file system available for the Amiga, performs very well under a lot of circumstances. Very simple and elegant.
- ReiserFS – File system which uses journaling
- Reiser4 – File system which uses journaling, newest version of ReiserFS
- SFS – Smart File System, available for the Amiga.
- Sprite – The original log-structured file system.
- UDF – Packet based file system for WORM/RW media such as CD-RW and DVD.
- UFS – UNIX File system, used on older BSD systems
- UFS2 – UNIX File system, used on newer BSD systems
- UMSDOS – FAT file system extended to store permissions and metadata, used for Linux.
- VxFS – Veritas file system, first commercial journaling file system;
- HP-UX, Solaris, Linux, AIX
- XFS – Used on SGI IRIX and Linux systems
- ZFS – Used on Solaris 10

### ***Network File system***

- Andrew File System
- AppleShare
- BeeGFS
- DCE Distributed File System
- NFS
- Red Hat Storage Server
- Arla (file system)
- OpenAFS
- OpenSFS
- XtreemFS
- Server Message Block

### ***Special purpose file system***

- Tmpfs (temporary file storage facility on many UNIX-like operating systems)
- ftpfs (ftp access)
- kernfs (BSD)
- Procfs
- Encrypting File System

- Wii Backup File System
- WebDAV

## **Microsoft Windows File Systems**

Since Windows is the most common operating system, let's start discussing the file system of windows first. The primary file system in windows can be divided into two types:

- FAT
- NTFS

FAT and NTFS both use different cluster size depending on the size of the volume, and each file system has a maximum number of clusters that it can support.

### ***File Allocation Table (FAT):***

As Microsoft says:

*“The first FAT file system was developed by Microsoft in 1976. That system was based on the BASIC programming language and allowed programs and data to be stored on a floppy disk. Since that time, the FAT file system has been improved upon multiple times to take advantage of advances in computer technology, and to further refine and enrich the FAT file system itself.”*

*“Today, the FAT file system has become the ubiquitous format used for interchange of media between computers, and, since the advent of inexpensive, removable flash memory, also between digital devices. The FAT file system is now supported by a wide variety of OSs running on all sizes of computers, from servers to personal digital assistants. In addition, many digital devices such as still and video cameras, audio recorders, video game systems, scanners, and printers make use of FAT file system technology.”*

reference: <http://www.dpreview.com/articles/8269265213/microsoftisfat>

The FAT database contains file names, directory names, cluster number and attribute of a file; and it is typically written on the outermost track of the disk.

### ***FAT versions:***

- **FAT12:** The oldest file system and it created to use for floppy disks. It has a limited amount of storage, volume not more than 16 MB. It uses 12-bit file allocation table entry to address an entry into file system. It was designed for MS-DOS 1.0
- **FAT16:** It uses 16-bit file allocation table entry to address an entry into file system; this is why it is called FAT16. It was created for large disk and it can handle the storage capacity up to 2 GB, and for some newer OSs the capacity is up to 4GB.
- **FAT32:** It is the advance file system as compared to the FAT12 and FAT16. It uses 32-bit file allocation table where the top 4 bits are reserved. Cluster size used: 4096-32768 bytes. It can access up to 2 TB of disk storage.

### ***New Technology File System(NTFS):***

NTFS has several improvements over the FAT, it is the primary file system used by Windows XP and later versions. NTFS supports large file names and it supports the large storage media. It is known as a recoverable file system; it can automatically recover or restore the consistency of the file system when an error occurs. It also supports encryption, compression and permission is being

defined for the user or group level.

**List of NTFS Metafiles:**

File name	Description
\$MFTMirr	Duplicate of the first vital entries of \$MFT, usually 4 entries (4 Kilobytes).
\$LogFile	Contains transaction log of file system metadata changes.
\$AttrDef	A table of MFT attributes that associates numeric identifiers with names.
\$Bitmap	An array of bit entries: each bit indicates whether its corresponding cluster is used (allocated) or free (available for allocation).
\$UpCase	A table of unicode uppercase characters for ensuring case-insensitivity in Win32 and DOS namespaces.
\$Extend	A file system directory containing various optional extensions, such as \$Quota, \$ObjId, \$Reparse or \$UsnJrnl.
\$Extend\\$Quota	Holds disk quota information. Contains two index roots, named \$O and \$Q.
\$Extend\\$ObjId	Holds link tracking information. Contains an index root and allocation named \$O.
\$Extend\\$Reparse	Holds reparse point data (such as symbolic links). Contains an index root and allocation named \$R.
.	Root directory. Directory data is stored in \$INDEX_ROOT and \$INDEX_ALLOCATION attributes both named \$I30.
\$MFT	Describes all files on the volume, including file names, timestamps, stream names, and lists of cluster numbers where data streams reside, indexes, security identifiers, and file attributes like "read only", "compressed", "encrypted", etc.
\$Boot	Volume boot record. This file is always located at the first clusters on the volume. It contains bootstrap code (see NTLDR/BOOTMGR) and a BIOS parameter block including a volume serial number and cluster numbers of \$MFT and \$MFTMirr.
\$Volume	Contains information about the volume, namely the volume object identifier, volume label, file system version, and volume flags (mounted, chkdsk requested, requested \$LogFile resize, mounted on NT 4, volume serial number updating, structure upgrade request). This data is not stored in a data stream, but in special MFT attributes: If present, a volume object ID is stored in an \$OBJECT_ID record; the volume label is stored in a \$VOLUME_NAME record, and the remaining volume data is in a \$VOLUME_INFORMATION record. Note: volume serial number is stored in file \$Boot

Source: <https://en.wikipedia.org/?title=NTFS#Metafiles>

## NTFS vs. FAT

Criteria	NTFS	FAT32	FAT16	FAT12
OS	Windows NT	DOS v7 and higher	DOS All versions	DOS All versions

	Windows 2000 Windows XP Windows 2003 Server Windows 2008 Windows Vista Windows 7	Windows 98 Windows ME Windows 2000 Windows XP Windows 2003 Server Windows Vista Windows 7	of Microsoft Windows	of Microsoft Windows
Volume size	232 clusters minus 1 cluster	32GB for all OS. 2TB for some OS	2GB for all OS. 4GB for some OS	16MB
Files on volume	4,294,967,295 (232-1)	4194304	65536	
Max file size	244 bytes (16 TeraBytes) minus 64KB	4GB minus 2 Bytes	2GB (Limit Only by Volume Size)	16MB (Limit Only by Volume Size)
Boot Sector Location	First and Last Sectors	First Sector and Copy in Sector #6	First Sector	First Sector
File attributes	Standard and Custom	Standard Set	Standard Set	Standard Set
Compression	Yes	No	No	No
Encryption	Yes	No	No	No
Permission	Yes	No	No	No
Disk quotas	No	No	No	No
Built-in security	Yes	No	No	No
Recoverability	Yes	No	No	No
Performance	Low on small volumes High on Large	High on small volumes Low on large	Highest on small volumes Low on large	High
Fault Tolerance	Max	Minimal	Average	Average

Let's compare them on the basis of volumes and the cluster size.

Volume size	FAT16 cluster size	FAT32 cluster size	NTFS cluster size
7MB – 16MB	2KB	Not supported	512 bytes
17 MB–32 MB	512 bytes	Not supported	512 bytes
33 MB–64 MB	1 KB	512 bytes	512 bytes
65 MB–128 MB	2 KB	1 KB	512 bytes
129 MB–256 MB	4 KB	2 KB	512 bytes
257 MB–512 MB	8 KB	4 KB	512 bytes
513 MB–1,024 MB	16 KB	4 KB	1 KB

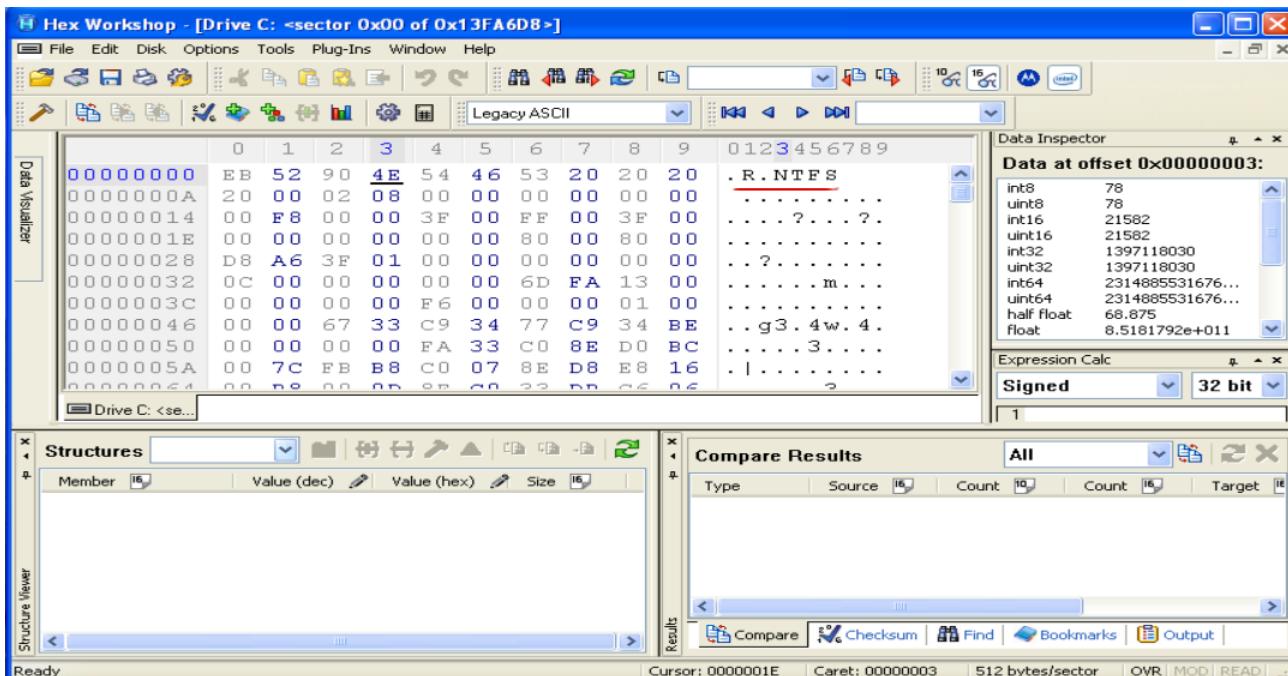
1,025 MB–2 GB	32 KB	4 KB	2 KB
2 GB–4 GB	64 KB	4 KB	4 KB
4 GB–8 GB	Not supported	4 KB	4 KB
8 GB–16 GB	Not supported	8 KB	4 KB
16 GB–32 GB	Not supported	16 KB	4 KB
32 GB–2 terabytes	Not supported	Not supported	4 KB

Apart from Windows, you should understand the file system of other operating system including Linux. Now we will use the hex workshop to analyze the partition physical level. You need to understand the hexadecimal codes to understand the file systems of various operating systems. Here is the list of the hexadecimal codes with the respectable file system.

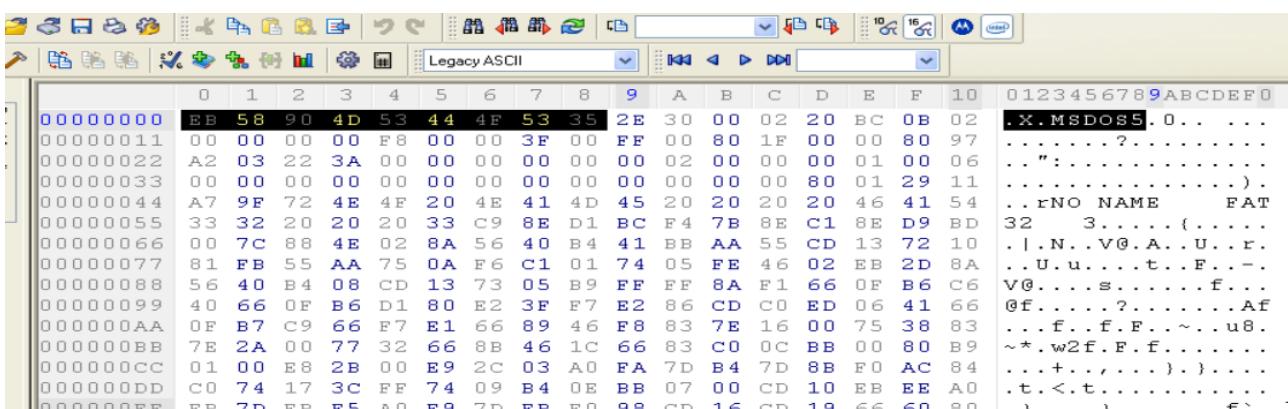
Hexadecimal code	File system
01	DOS 12-bit FAT
04	DOS 16-bit FAT for partitions smaller than 32 MB
05	Extended partition
06	DOS 16-bit FAT for partitions larger than 32 MB
07	NTFS
08	AIX bootable partition
09	AIX data partition
0B	DOS 32-bit FAT
0C	DOS 32-bit FAT for interrupt 13 support
17	Hidden NTFS partition (XP and earlier)
1B	Hidden FAT32 partition
1E	Hidden VFAT partition
3C	Partition Magic recovery partition
66-69	Novell partitions
81	Linux
82	Linux swap partition (can also be associated with Solaris partitions)
83	Linux native file systems (Ext2, Ext3, Reiser, Xafs)
86	FAT16 volume/stripe set (Windows NT)
87	High Performance File System (HPFS) fault-tolerant mirrored partition or NTFS volume/stripe set
A5	FreeBSD and BSD/386
A6	OpenBSD
A9	NetBSD
C7	Typical of a corrupted NTFS volume/stripe set

Let's do it. Download Hex workshop ([www.hexworkshop.com](http://www.hexworkshop.com)) and install it to analyze.

- After installation, click on the icon and open the program
- In Hex workshop, click on **Disk → Open Drive** and see the list of logical drives. In the example below, I have clicked on my **C:** drive to analyze it.



Here “.R.NTFS” shows that the partition has been formatted as an NTFS drive. If you see MSD0S5.0 or MSWIN4.1 in the first logical sector, then it means that the drive formatted as FAT.



## Windows Registry

Windows registry is the hierarchical database; it contains the information of the users, applications, hardware, etc. Windows registry know everything about a program, where the program is stored, its version and every setting of that program. During execution of any task, windows continuously refer to the registry. Data in registry stores at Binary file.

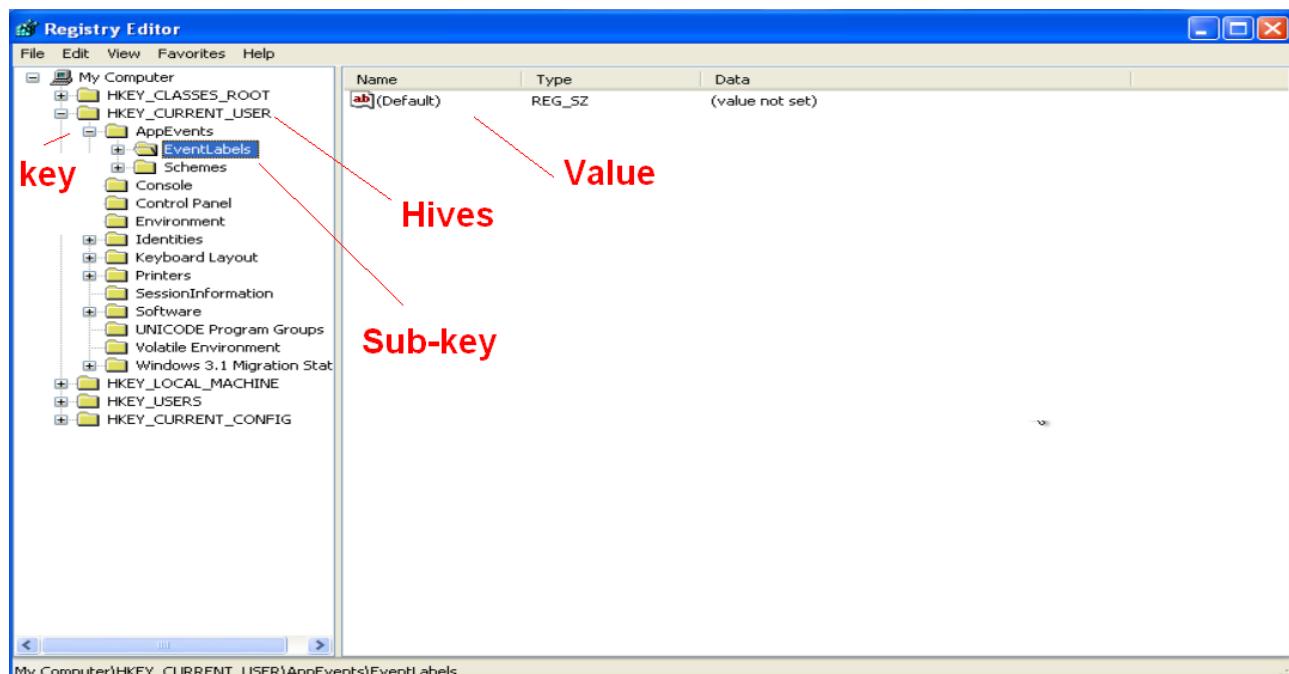
### Windows Registry Structure:

- The hives

- Handle key
- Key
- Sub-key
- Value

- The hives: It is the branches in HKEY\_USER and HKEY\_LOCAL\_MACHINE.
- Hkey or handle key: They are the categories of hives
- Key: Every Hkey divides into different folders named key.
- Sub-key: Another key displayed under key is called sub-key
- Value: It is the content of a particular key

“REGedit” run this command to open the registry editor.



### *Registry Hkey/hives & their functions:*

Hkey	Functions
HKEY_CURRENT_USER	This hive contains information of the current logged-in user. Information including the configuration and preference settings.
HKEY_LOCAL_MACHINE	The machine configuration, hardware and installed software information are available under this hive
HKEY_CLASSES_ROOT	A symbolic link to HKEY_LOCAL_MACHINE\SOFTWARE\Classes; provides file type and file extension information, URL protocol prefixes, and so forth

HKEY_USERS	It contains information of all the users ever logged-in on this machine
HKEY_DYN_DATA	It contains information about hardware Plug and Play.

The following table shows the registry and the supporting files:

Hive	Supporting files
HKEY_CURRENT_CONFIG	System, System.alt, System.log, System.sav
HKEY_CURRENT_USER	Ntuser.dat, Ntuser.dat.log
HKEY_LOCAL_MACHINE\SAM	Sam, Sam.log, Sam.sav
HKEY_LOCAL_MACHINE\Security	Security, Security.log, Security.sav
HKEY_LOCAL_MACHINE\Software	Software, Software.log, Software.sav
HKEY_LOCAL_MACHINE\System	System, System.alt, System.log, System.sav
HKEY_USERS\DEFAULT	Default, Default.log, Default.sav

## ***Linux File Systems***

In the previous topics, we have discussed Windows OS file systems and now under the heading of Linux file system, we will discuss the file system and architecture of Linux OS. Linux or it is for UNIX supports multiple file systems and it is the open-source OS. Before discussing the file systems, we should discuss some basic concept related to file system in Linux.

### **What is a File?**

In Linux, everything is file while the others are processes, file is connected with the storage media and whatever you store, it informs the file. The file is the collection of data; data may be your text, image, video, etc. To manage the files on Linux, ordered tree structure has been created where the root contains large branches, and the branches contain a regular file (leaves of a tree for that matter).

### **What is Directory?**

Directory is a special file that contains other files and sub-directories. Directory can be further divided into two types:

- Root directory
- Sub-directory

Since Linux is based on tree structure, hence we have root or root directory. You can't change the root directory, you can't rename it. It is denoted by a forward slash (/). Sub-directory is the branch of the tree, we have many sub-directories of a single root (single OS), it can be created/deleted and you can also rename them.

### **Inodes**

The inode is the basic concept in Linux file system, each file in Linux is represented by inodes which is the structure of the file system. Each inode contains the information of the file, timestamps, size, file type, owner of the file, permission, etc. It is also called Index number because

each inode is identified by a unique assigned number in the file system. If we summarize, then it is the database stores metadata about each file and directory. It is used to track the file on the hard-drive. The inode contains entries and each entry is 128 bytes in size.

The inode contains the following attributes of the file:

- Inode number (identification number)
- Access control list
- Owner of the file
- Group which file belongs to
- Permission (read, write, executable, etc.)
- Size of the file
- Type of the file
- File access, modification and deletion time

The inode has nothing to do with the content (data) and even name of the file, it only works to manage the file within the file system by assigning a unique number to every file.

```
# ls -i filename  
# stat filename
```

```
root@kali:~# ls -i k.mp3  
2883850 k.mp3  
root@kali:~# stat k.mp3  
  File: `k.mp3'  
  Size: 127268          Blocks: 256          IO Block: 4096   regular file  
Device: 801h/2049d      Inode: 2883850      Links: 1  
Access: (0644/-rw-r--r--)  Uid: (    0/    root)  Gid: (    0/    root)  
Access: 2015-06-03 18:44:53.072547953 +0500  
Modify: 2015-06-03 18:44:36.728547534 +0500  
Change: 2015-06-03 18:44:36.728547534 +0500  
 Birth: -  
root@kali:~#
```

In the above example, I have analyzed a mp3 file. The first output shows the identification number of this particular file, while the second output provides more details about the file.

## Journaling File System

Journaling file system introduced in Linux is the main reason that many corporations switched to Linux, however it is no longer a unique reason because there are other file systems available having capability. The file systems before **Ext3** are based on static structure, they don't have journaling functionality. However, **Ext3** and beyond file system has journaling capability. So what journaling file system is all about?

According to Wikipedia: “A journaling file system is a file system that keeps track of changes not yet committed to the file system's main part by recording the intentions of such changes in a data structure known as a "journal", which is usually a circular log.”

If a system is not properly shutdown (think of power failure), then journaling file system provides

the consistency of the data (whether you have saved the file or not). Journaling file system first write into another part of hard-drive called journal where it stores the logs of the file. So journaling file system is always consistent.

## File Systems in Linux

As discussed, Linux supports many file systems, but EXT (Extended file system) is the most common and the most famous file system.

EXT file has versions:

- ext2
- ext3
- ext4

Ext was designed in 1992 by the French developer Remy Card as a first file system created for Linux kernel. Partition size was limited to 64 MB and 14 bytes was the limit for file names.

### EXT2

Ext was immediately superseded by ext2. The second extended file system was created by Remy Card in 1993. Ext2 was the most famous and the default file system in Linux until the launch of ext3. However, USB and other removal storage media are still using ext2 as their first choice file system. Ext2 does not support journaling; this is the main reason why ext2 is recommended for USB drives because these drives does not need to do the journaling. It supports maximum file length of 255 bytes and the max file size is 2 TB. In ext2, the directories and files are not indexed, so searching a file within large amount of files may take time.

Block Size	Max file size	Max file system size
1 KB	16 GB	4 TB
2 KB	256 GB	8 TB
4 KB	2 TB	16 TB
8 KB	2 TB	32 TB

### EXT3

The third extended file system was launched in 2001 and developed by Stephen Tweedie. It has journaling which is the main edge of it over ext2. Ext3 is more advanced than ext2, because it has the capability to index the directories and files by using an H-tree. Maximum individual file size is 2 TB, overall the file system can be up to 32 TB. The Ext2 file system can be switched to ext3 without taking backup.

Block Size	Max file size	Max file system size
1 KB	16 GB	4 TB
2 KB	256 GB	8 TB

4 KB	2 TB	16 TB
8 KB	2 TB	32 TB

## EXT4

The fourth extended file system is the successor of ext3 with the aim to improve the performance and stability. It was released in Linux kernel version 2.6.28 in 2008. It uses 48 bit addressing system which allows the maximum file size of 16 TB and the maximum volume size of 1 EB. User has given the rights to turn on/off the journaling in ext4.

Let's compare EXT with Windows file system on the basis on Journaling and size:

File System	Max File Size	Partition Size	Journaling
FAT 16	2 GB	2 GB	No
FAT32	4 GB	8 TB	No
NTFS	2 TB	256 TB	Yes
ext2	2 TB	32 TB	No
ext3	2 TB	32 TB	Yes
ext4	16 TB	1 EB	Yes

As discussed, the file system is the tree-based structure where we have root (/). Here you can see the content of the root location.

```
root@kali:~# cd /
root@kali:/# ls -F
0      dev/  initrd.img@  media/  opt1/  run/      srv/  usr/
bin/   etc/  lib/       mnt/   proc/  sbin/     sys/  var/
boot/  home/ lost+found/  opt/    root/  selinux/ tmp/  vmlinuz@
root@kali:/#
```

Where,

usr/	Partition for user program
home/	Where user stores its data (content)
Var/	Stores temporary data
Opt/	Stores third party software
lost+found/	Files that were saved during failures are here.
Lib/	Library file for the programs
Boot/	The startup files and the kernel
Dev/	It contains the information about the hardware
Root/	Admin user home directory
Mnt/	Mount point for external file systems (USB, CD, etc.)
Sbin/	It has the programs run by the system

## Determine the file system of a machine

Use *df -T* command:

```
df -T | awk '{print $1,$2,$NF}' | grep '^/dev'
```

```
root@kali:~# df -T | awk '{print $1,$2,$NF}' | grep '^/dev'  
/dev/disk/by-uuid/6f826894-bab1-4c23-9c30-0835ee5373b3 ext4 /
```

In the following example, you can see the external drive along with the internal drives. Let's find their file system information.

```
root@kali:~/# fdisk -l  
  
Disk /dev/sda: 500.1 GB, 500107862016 bytes  
255 heads, 63 sectors/track, 60801 cylinders, total 976773168 sectors  
Units = sectors of 1 * 512 = 512 bytes  
Sector size (logical/physical): 512 bytes / 4096 bytes  
I/O size (minimum/optimal): 4096 bytes / 4096 bytes  
Disk identifier: 0x000c4335  
  
      Device Boot   Start     End   Blocks Id System  
/dev/sda1    *     2048 960561151 480279552  83 Linux  
/dev/sda2        960563198 976771071 8103937   5 Extended  
Partition 2 does not start on physical sector boundary.  
/dev/sda5        960563200 976771071 8103936   82 Linux swap / Solaris  
  
Disk /dev/sdb: 4026 MB, 4026531840 bytes
```

/dev/sdb represents the external media (USB in my case), so here we go:

```
root@kali:~# file -sL /dev/sdb  
/dev/sdb: sticky x86 boot sector, code offset 0x58, OEM-ID "MSDOS5.0", sectors/cluster 8  
reserved sectors 1056, Media descriptor 0xf8, heads 255, hidden sectors 63, sectors 786-  
257 (volumes > 32 MB), FAT (32 bit), sectors/FAT 7664, reserved3 0x1800000, reserved 0x0,  
serial number 0x72841154, unlabeled
```

For the internal partition:

```
root@kali:~# file -sL /dev/sda1  
/dev/sda1: sticky Linux rev 1.0 ext4 filesystem data, UUID=6f826894-bab1-4c23-9c30-0835ee-  
5373b3 (needs journal recovery) (extents) (large files) (huge files)
```

This is it. In this section we have discussed many important topics of Linux file system including the journaling concept and inodes, the information of the root, sub-directories discussed above are very important, and you should look inside them while investigating the case. In the next module, we will see the techniques to gather evidence and how to analyze them.

## **Module4: Evidence Acquisition & Investigation**

Many important topics have been discussed in the previous module and now the objective of this module is to introduce forensic software and to demonstrate their usage. In the first module, we have discussed the rules that you must follow during evidence acquisition process. There are many tools, both commercial and open-source are available, and somehow many of them are same as per their function; every investigator has its own toolkit and you should make your own. The selection of toolkit highly depends on your mindset, way of work and the expected cases. Anyhow, let's discuss some important concept first.

### **Storage Media Image:**

Creating storage media image is crucial for investigating a case and finding evidence out of it. Evidence acquisition & investigation process are:

- Creating image of storage media (suspect media)
- Verifying the integrity by hashing
- Analyze the storage media and its content

Creating an image is nothing but making a copy of the suspect device and analyze the copied version of the storage media. Media image is a file that contains data (actual content) and the structure of the media, here media means any storage device; for example, hard-drive, USB, CD/DVD, etc.

*Note: Never investigate the original device, take the copy of the device and investigate it.*

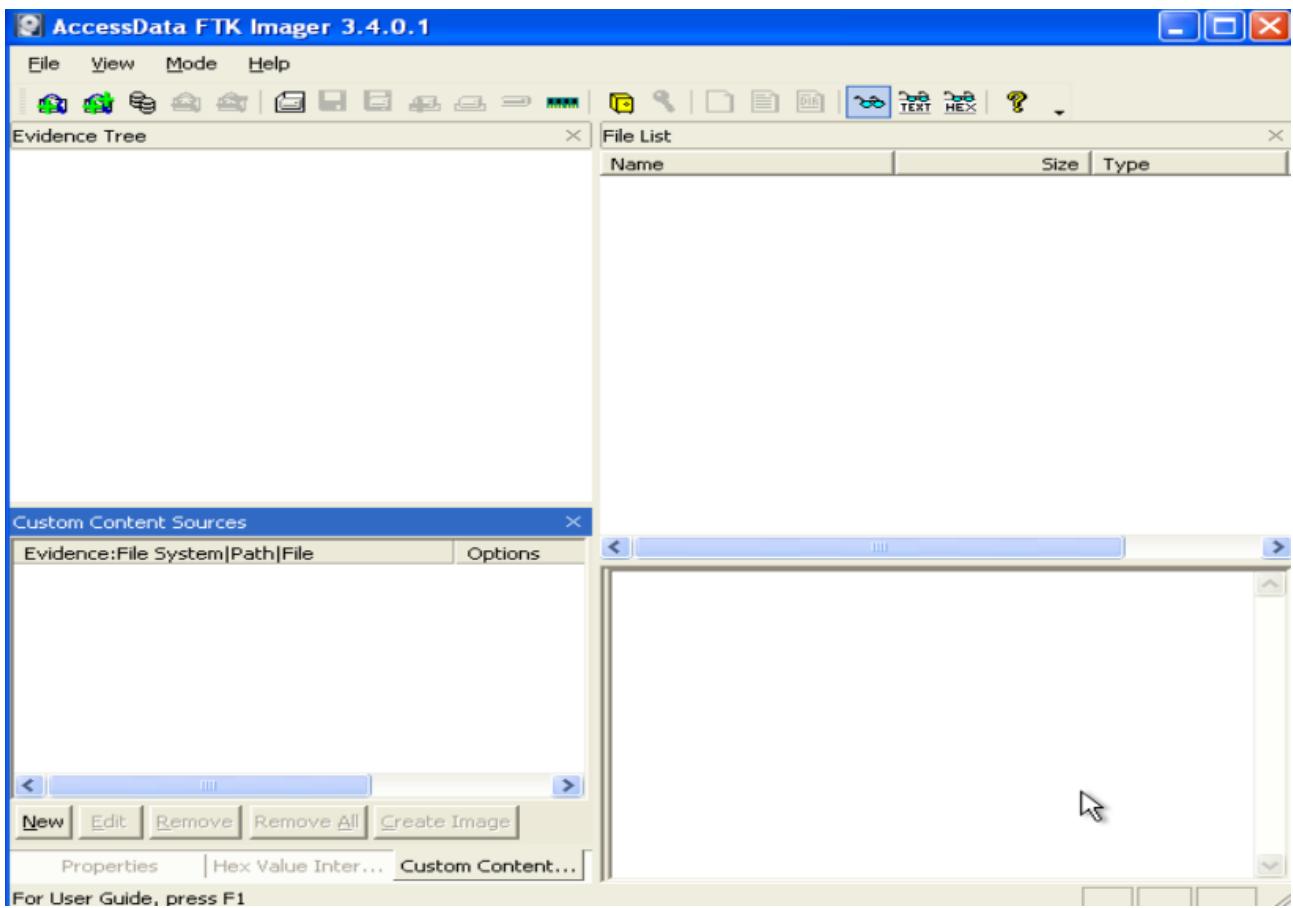
AccessData Corp. is a well-known company that provides computer forensics tools/software. In this guide, we will use their software and apart AccessData, we will use some open-source software too.

### **AccessData FTK Imager – Forensics Tool**

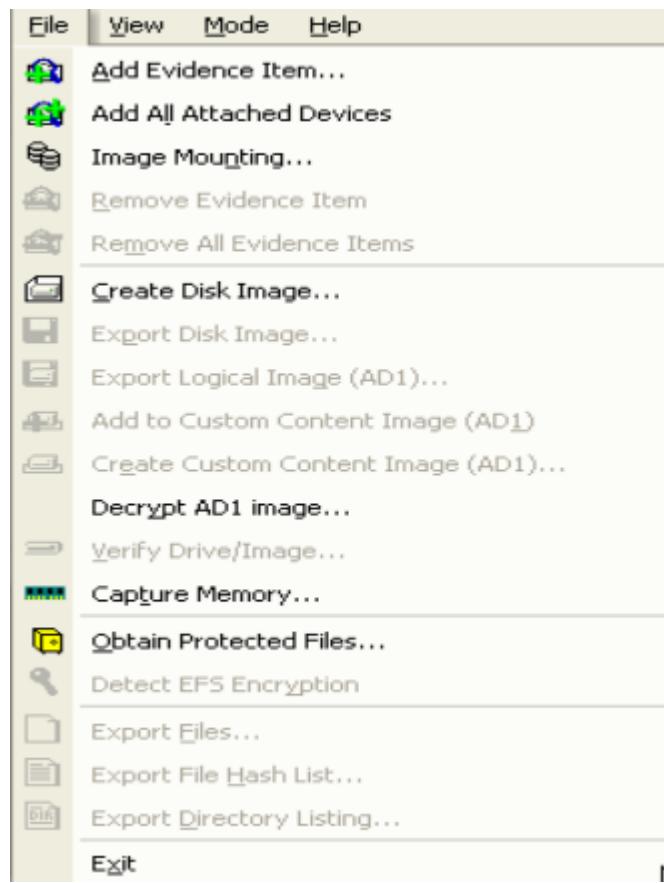
FTK image is a wonderful software that can create an image of the storage media, it can also preview the content of the created image, and you can export the image for further investigation. Keep in mind that an image can be created locally or remotely.

In this scenario, I am taking an image of a removal drive (USB) and the same image will be used throughout this guide.

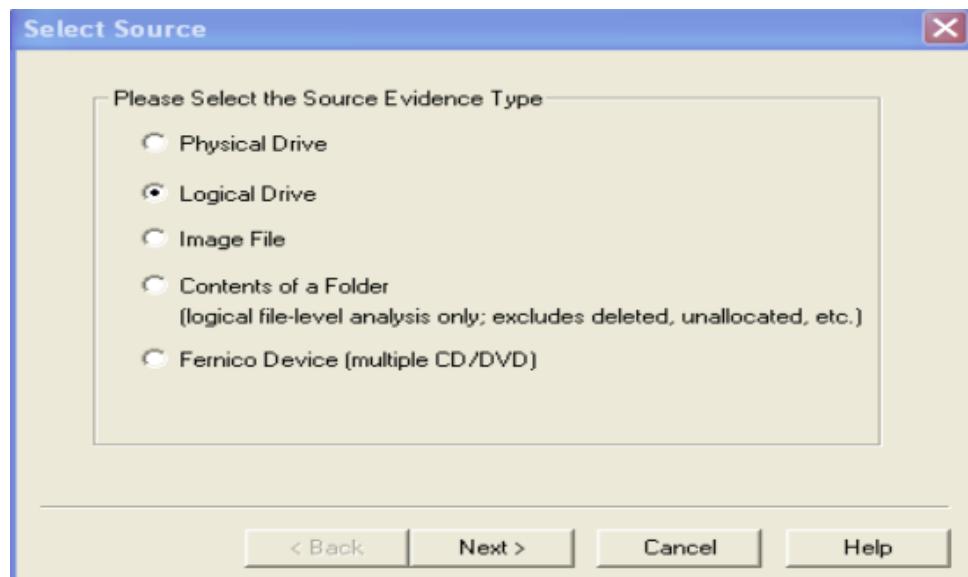
- Download the FTK imager and install it.
- Click on the icon, open the software and here is the main window:



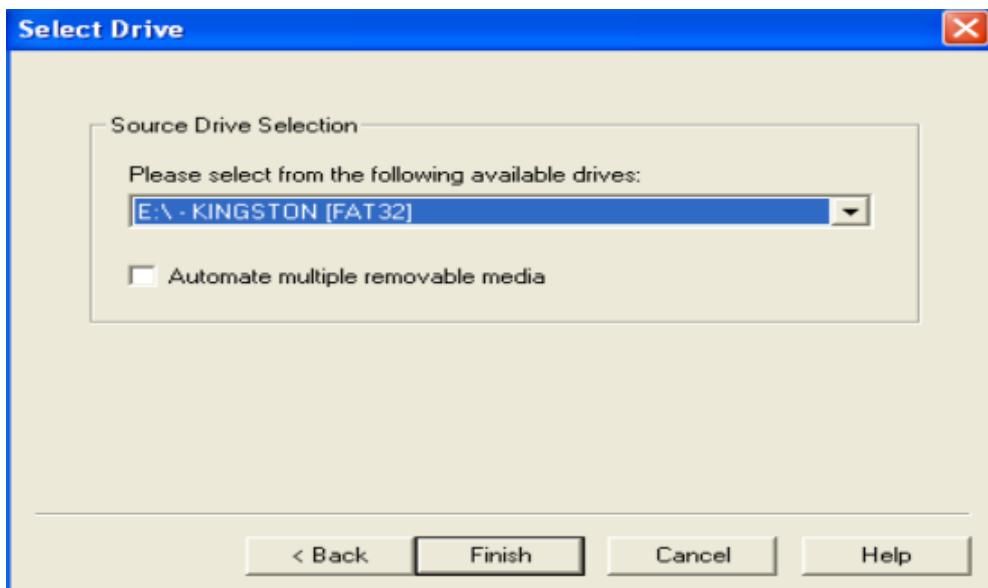
- Click on the **File**, here you can see multiple options to take images from. Information from memory can also be collected, and you can image the individual item too.



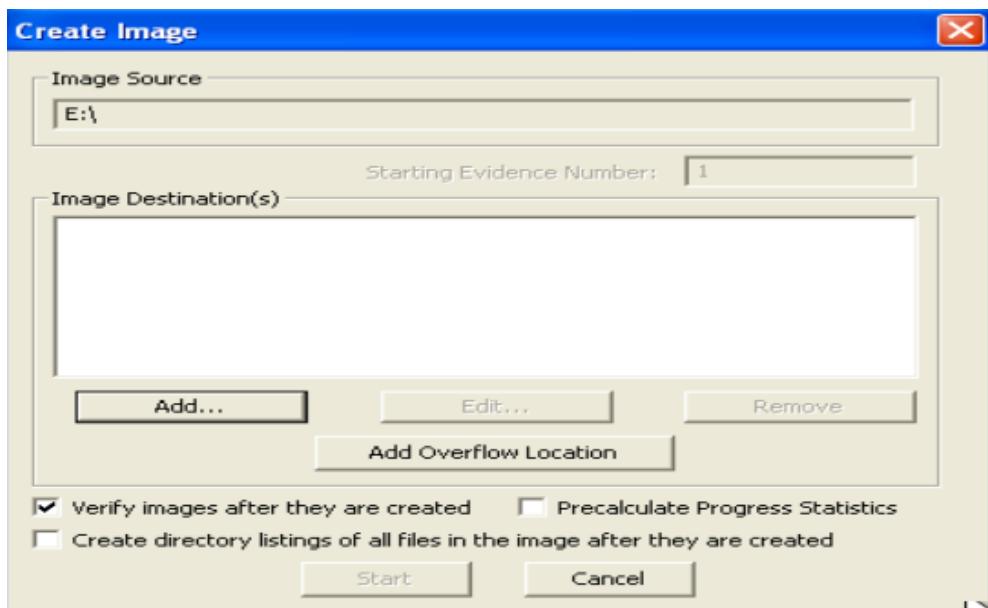
- Click on **Create disk image** option. Now select the device type. In our situation, **logical drive**.



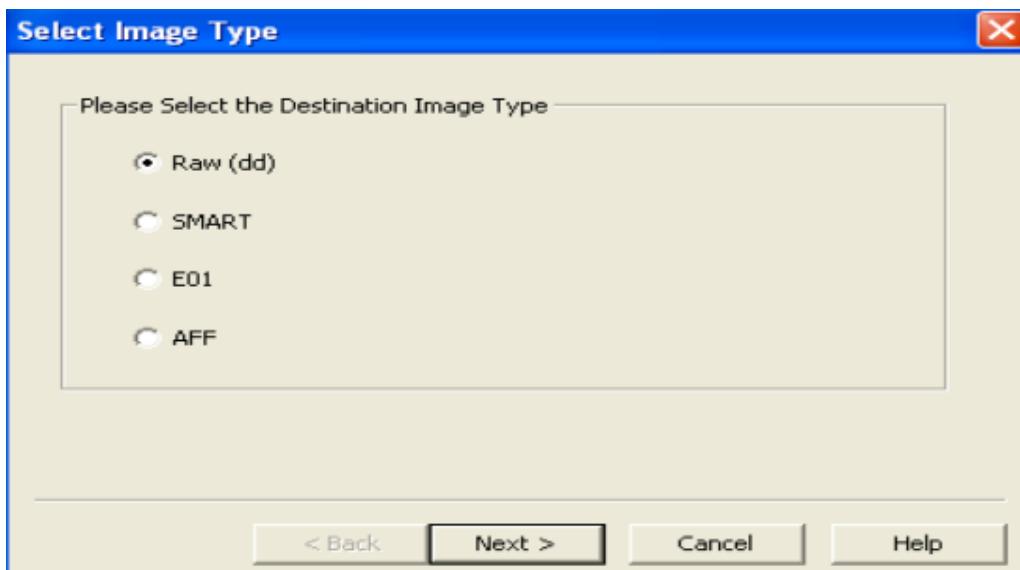
- Select the drive and **finish** the procedure



- In the next window, select the destination drive or folder, where you want this image to be saved.



- You need to select the image type. Here **E01** file format is for EnCase (famous digital forensics program). **AFF** stores all the data along with metadata in a single file, while **SMART** stores the metadata in separate file. We will select the **RAW (DD)** option, that is the RAW image file format and it can also be analyzed in Linux operating system. Select the type and click next.



- The next window is for administrating and managing purpose, you need to enter the

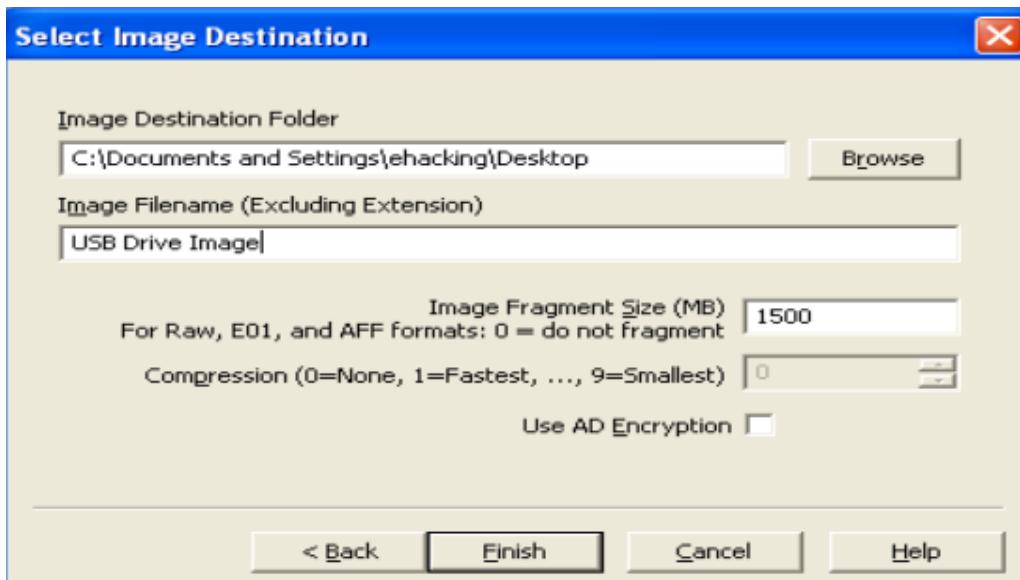
A screenshot of a Windows-style dialog box titled "Evidence Item Information". It contains five text input fields:

- Case Number: 00456-June-20-15
- Evidence Number: 03
- Unique Description: The Acquired USB drive
- Examiner: Irfan Shakeel
- Notes: (empty)

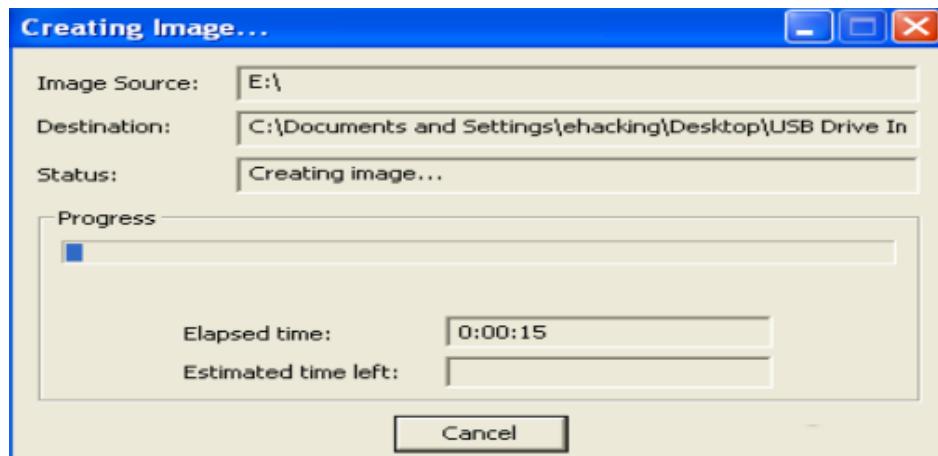
At the bottom are buttons for "< Back", "Next >" (highlighted in blue), "Cancel", and "Help".

information relevant to the case.

- In the window, enter the destination path and the name of the Image. If you are analyzing large drive, then you can split the image into multiple parts, **image fragmented size** is the failed to provide this information.



- The process may take time, and it depends on the disk size.



- You need to verify the hash to make sure the integrity of the acquired data. The following window will appear after the creation of the image. Here you can see the information of MD5 and SHA1 hash and their results. Since the values are matched, hence it indicates that nobody has altered the disk and you got the exact copy of the suspect device.

Drive/Image Verify Results	
Name	USB Disk Image.001
Sector count	7864257
MD5 Hash	
Computed hash	008afe66328b8fd4b19574db711a7d93
Report Hash	008afe66328b8fd4b19574db711a7d93
Verify result	Match

- In order to view the summary of the overall process, create on **image summary**. This same information has also been printed in the text format (available at the same location).

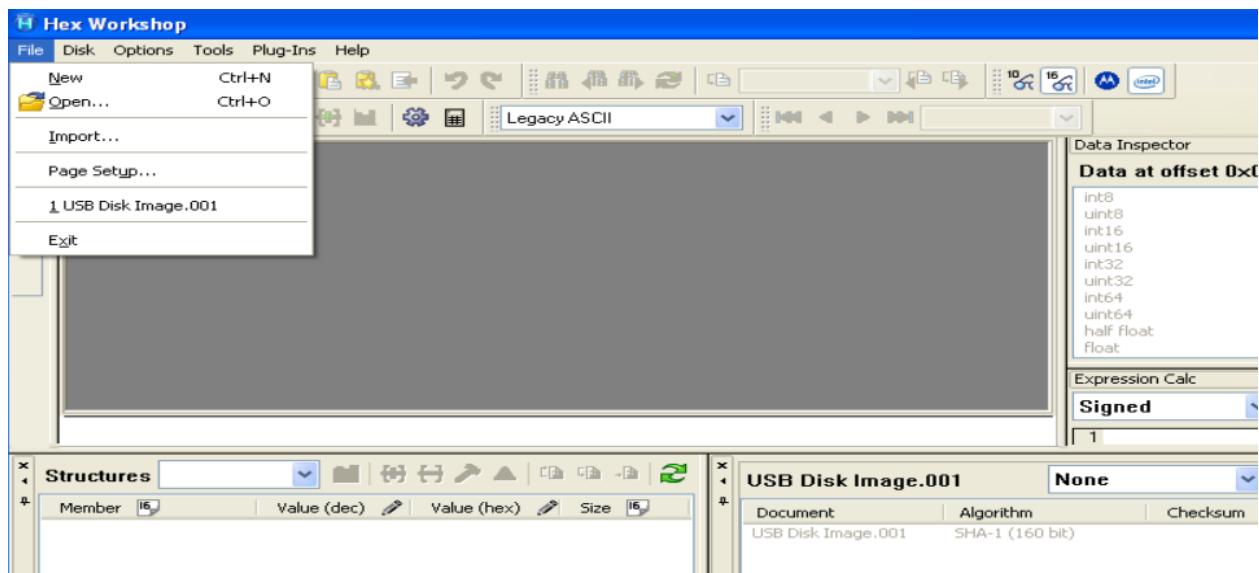
This is it. This is how you create an exact copy of the suspect device for investigation purposes; make sure to keep the hash details with you to verify the integrity in the investigation process where you will be touching the data.

## Hashing to Verify the Integrity of the Image

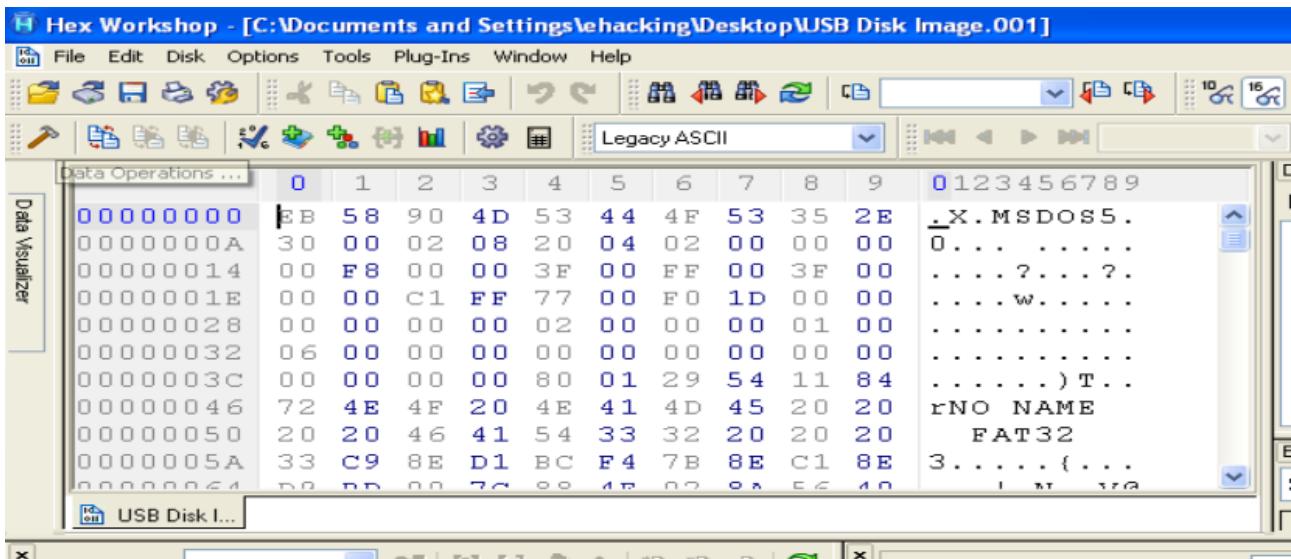
Hashing process is to match the image with the source media or drive. Hashing is as if you are doing a biometric verification of a human. There are many algorithms created for hashing, and hashing can be used for many reasons, including encryption, but in our scenario we are discussing hashing from a forensics point of view. MD5, 128bit, 32 character algorithm is one of the famous amongst the list of algorithms. If you alter the data acquired from the suspect disk, it will change its hash value. It is crucial to maintain the integrity; otherwise, you can't verify in court that you did not change the evidence in any way.

Following are the steps to verify the integrity of the data; Hex workshop is the software for this purpose:

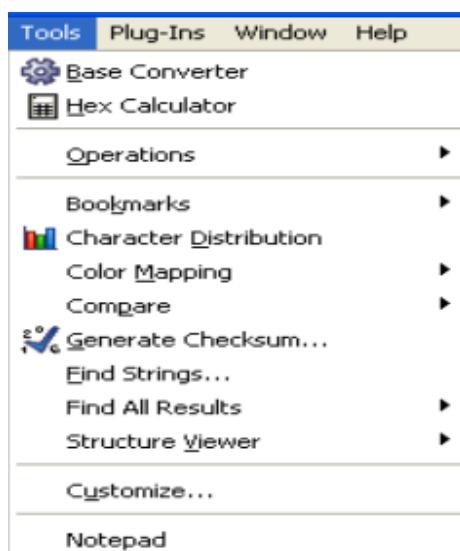
- Open Hex workshop → File → Open



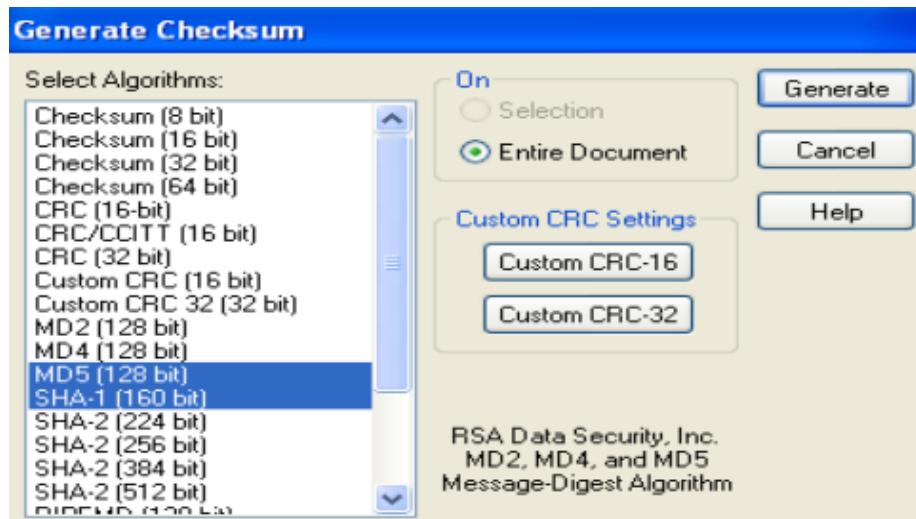
- Browse and select the image file created in the previous topic, you will witness the hexadecimal values like this:



- This hexadecimal values and the characters are the content of the storage media. If alter any of these values, the hash will also be changed. So conduct a fair investigation, never try to change the evidence else, you will make the legal process very difficult. Now click on **Tools** → **generate checksum**



- List of algorithms is there, select MD5 and SHA1 for verification and click on **Generate**



- Generating hash values may take little time and it depends on the file size. So here is the result, as you can see that the created image has not been changed yet because the hash values are similar:

```
Image Verification Results:
Verification started: Sat Jun 20 03:29:27 2015
Verification finished: Sat Jun 20 03:30:52 2015
MD5 checksum: 008afe66328b8fd4b19574db711a7d93 : verified
SHA1 checksum: 4565875743354338fc99d28b45205994e29de969 : verified

Hex workshop Result

MD5: 008AFE66328B8FD4B19574DB711A7D93
SHA1: 4565875743354338FC99D28B45205994E29DE969
```

- Changing the name or even extension for that matter, does not change the hash value. You can try this. However, if you change any value (data) then the hash will be changed respectively.

## Image Acquisition on Linux

In the previous topics, we have discussed software and processes to create an image of the suspect device on Windows OS. The same functions can be performed on Linux machine too, there are open-source tools available that can make your job effective and efficient. DD is an UNIX command that is very important for forensic experts, this is the command-line utility means you don't have the graphical user interface to execute the functions. Creating image via DD is equivalent with the other software for example, FTK imager.

**dcfldd** is the command-line utility and it is the advanced version of DD. Many forensics tasks can be done by using this command:

- Image verification: dcfldd can verify the integrity of the data and provides a solution to check the target device, whether it is matched with the input file or not.
- Split out: If you are analyzing a large disk, then you can split the image on multiple files. It helps you to transfer the data.
- Multiple output: This utility has an ability to output multiple files and disks at a time.
- Log output: It creates txt file of the logs and the hashes.

There is another utility named “**dc3dd**” that is also useful in forensic examination, however, it has some limitation as comparing to **dcfldd**. We will use dcfldd to acquire an image.

The objectives of this case are:

- Creating image of a disk in Linux
- Understand the procedure to mount a directory or even partition
- Where the disk image data is
- Verify the integrity by creating and comparing hashes

Let's do it:

- Open Kali Linux terminal and type the command “**fdisk -l**”. The output contains the list of partitions. Here you can see the partitions; SDA1, SDA2, SDA5 and SDB which is an external device (USB).

```
root@kali:~# fdisk -l

Disk /dev/sda: 500.1 GB, 500107862016 bytes
255 heads, 63 sectors/track, 60801 cylinders, total 976773168 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 4096 bytes
I/O size (minimum/optimal): 4096 bytes / 4096 bytes
Disk identifier: 0x000c4335

      Device Boot      Start        End      Blocks   Id  System
/dev/sda1  *        2048    960561151    480279552   83  Linux
/dev/sda2          960563198    976771071     8103937     5  Extended
Partition 2 does not start on physical sector boundary.
/dev/sda5          960563200    976771071     8103936   82  Linux swap / Solaris

Disk /dev/sdb: 4026 MB, 4026531840 bytes
124 heads, 62 sectors/track, 1022 cylinders, total 7864320 sectors
```

- Take SDB for further analysis. On the terminal type “**parted -l**” to see the space of each drive. Here you can see the type of the drive (SDB) which is **FAT32**. In addition, the size is “4027MB”.

```

root@kali:~# parted -l
Model: ATA MARSHAL MAL2500S (scsi)
Disk /dev/sda: 500GB
Sector size (logical/physical): 512B/4096B
Partition Table: msdos

Number  Start   End     Size    Type      File system  Flags
 1      1049kB  492GB  492GB   primary   ext4         boot
 2      492GB   500GB  8298MB  extended
 5      492GB   500GB  8298MB  logical   linux-swap(v1)

```

```

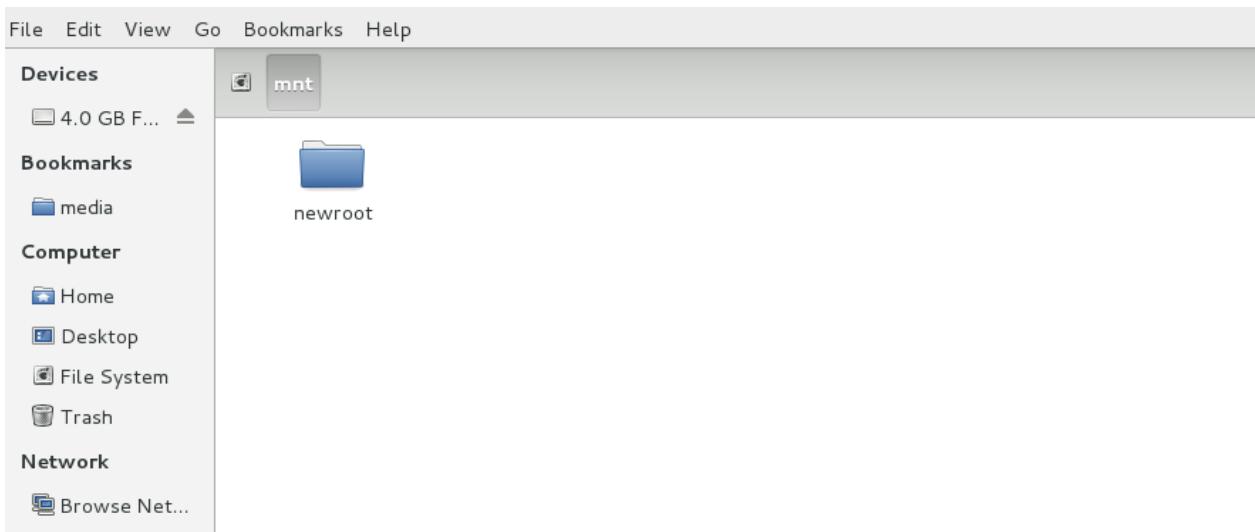
Model: hp v220w (scsi)
Disk /dev/sdb: 4027MB
Sector size (logical/physical): 512B/512B
Partition Table: loop

File system      Flags
 1      0.00B  4027MB  4027MB  fat32

```



- It's time to mount the drive. We need to mount the drive first so that we will be able to make any changes to it. Mounting in Linux is like loading a drive or simply opening a drive. First, we need to create a location, you can do this by locating the file system in Linux too, but here I am performing all tasks from the terminal. Click on the file system → **mnt**, here you should create a folder.



On your terminal type **sudo mkdir /mnt/locat**

- **Sudo**, provides the administrative rights to perform the job

```

root@kali:~# sudo mkdir /mnt/locat
root@kali:~# 

```

- **mkdir** a simple command to make a directory and the another directory

- After creating the location, mount the drive to the location. Use the command “**sudo mount /dev/sdb /mnt/locat**”

```
root@kali:~# sudo mount /dev/sda1 /mnt/locat
root@kali:~#
```

- Once mounted, create a new folder for incident. **mkdir /mnt/locat/case**
- Note everything, **fdisk -l > /mnt/locat/case/fdisk.txt**
- Create image of the disk by using:

```
dcfldd if=/dev/sdb hash=md5,sha256 hashwindow=1G md5log=/root/md5.txt
sha256log=/root/sha256.txt hashconv=after conv=noerror,sync of=/root/driveimage.dd
```

```
root@kali:~# dcfldd if=/dev/sdb hash=md5,sha256 hashwindow=1G md5log=/root/md5.txt
sha256log=/root/sha256.txt hashconv=after conv=noerror,sync of=/root/driveimage.dd
The quieter you become, the more you are able to hear.
122880 blocks (3840Mb) written.
122880+0 records in
122880+0 records out
root@kali:~#
```

- Here, **Hash=md5,sha256** represents the type of the algorithms to be used

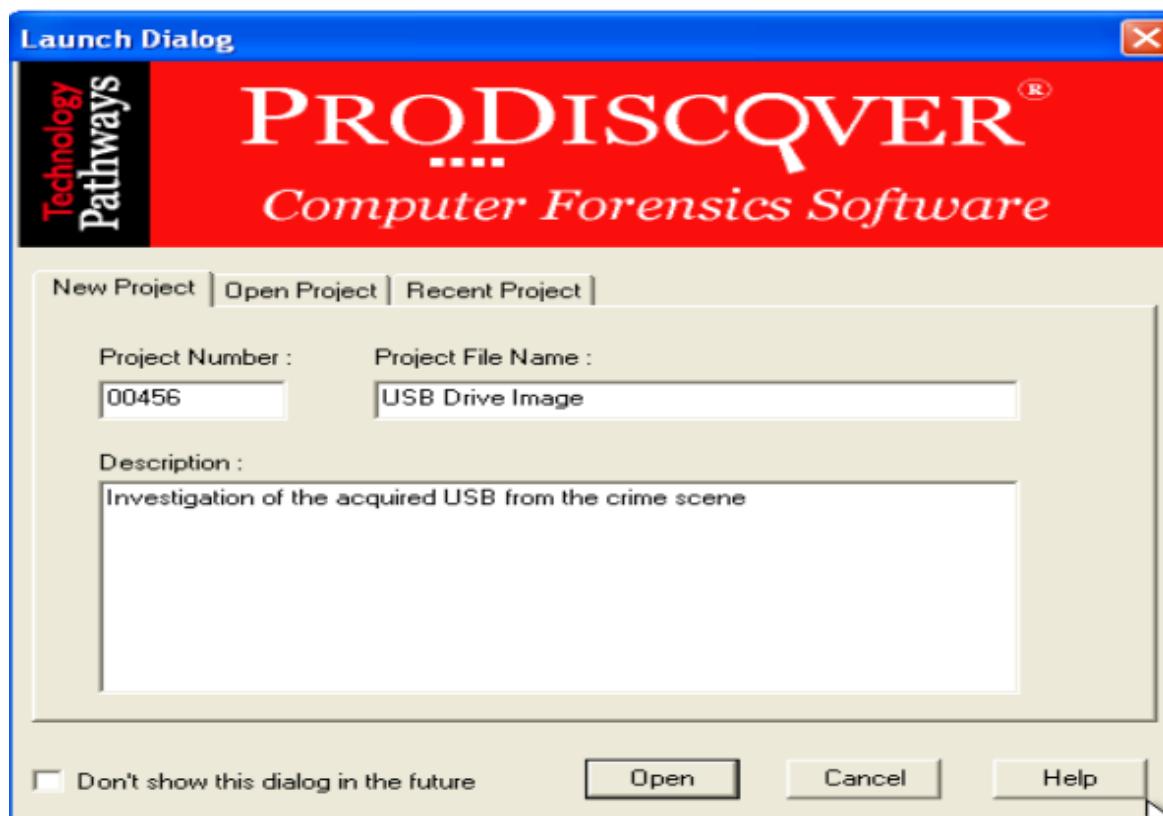
This is it, the process to create an image of a disk on a Linux machine. Now you have witnessed the procedure on both the Linux and Windows machine. In the next topic we will analyze the created images.

## **Data Analysis**

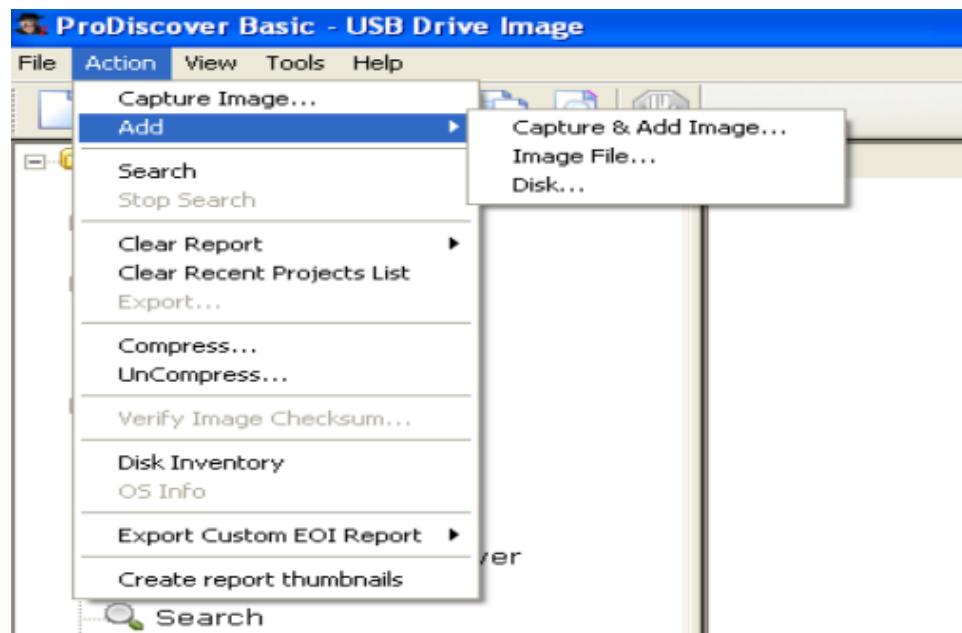
After the acquisition and verification of the storage media image, the next step is to analyze the content to find the possible evidences of the case. During the investigation process, you should consider that the suspect is smart and he/she might try to hide, delete and encrypt the important evidence. First, analyze the clearly visible files and folders and then look for the hidden and deleted items. Take a deep look into every file and directories.

In the previous step, we have successfully created the image and the image has also been verified to maintain the integrity of the data. Now let's move further. **ProDiscover Basic** is the forensics software that we are going to use to analyze the data. This particular software can be used to achieve both the purposes, creating image and analysis. Anyway, in this particular scenario, we will use prodiscover to analyze the file and then we will create the report.

- This is the first window, where it asks information related to the project that you are starting to work on.



- To add an image, click on **Action → Add → Image** Prodiscover has a wonderful feature to create an image. You can even create an image of the disk from this software. I am using the same image created in the previous topic.



- On the left navigation menu, click on **Images → the name of the drive** Here you can see

the content of the acquired (suspect) disk. Your job is now to analyze every file and folder and to look for the possible evidence. The biggest mistake that you should not make, is the damage to the data; otherwise the integrity of the data will be lost and you won't be able to prove anything in the court.

The screenshot shows the ProDiscover Basic software interface. On the left, there's a navigation pane with various options like Project - USB Drive Image, Content View, Cluster View, Registry View, EventLog View, Internet History Viewer, View Log, Search, and Search Results. A specific item under Content View, 'C:\Documents and Settings', is selected and highlighted in blue. The main right pane displays a table of files with columns for Select, File Name, File Extension, Size, Attributes, Deleted, and Created Date. The table lists numerous files including 'PSTools.zip', 'fport.zip', 'ListDlls.zip', and several media files like 'Tere ishq na...mp3' and 'VoIP Is Ever...docx'. Most files are marked as 'a -----' for attributes, while some are marked as 'd -----'.

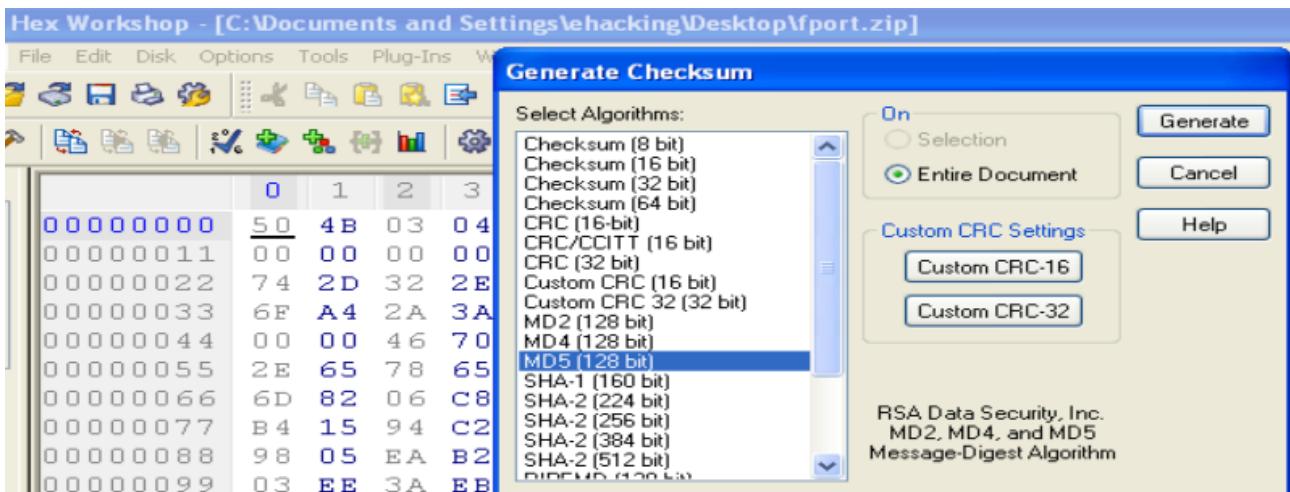
Select	File Name	File Extension	Size	Attributes	Deleted	Created Date
<input type="checkbox"/>	ÀNTITL~1			- d -----	YES	02/23/2015 ...
<input type="checkbox"/>	New Recordi...			- d -----	NO	02/23/2015 ...
<input type="checkbox"/>	Spectrum (I...			- d -----	YES	02/02/2015 ...
<input type="checkbox"/>	ÀECYCLER			- d -----	YES	02/03/2015 ...
<input type="checkbox"/>	Section 01			- d -----	NO	02/23/2015 ...
<input type="checkbox"/>	Final			- d -----	NO	02/23/2015 ...
<input type="checkbox"/>	All Files			- d -----	NO	12/31/1969 ...
<input type="checkbox"/>	PSTools	zip	1,686,759...	a -----	NO	06/10/2015 ...
<input type="checkbox"/>	fport	zip	57,843 ...	a -----	NO	06/10/2015 ...
<input type="checkbox"/>	ListDlls	zip	269,722 ...	a -----	NO	06/10/2015 ...
<input type="checkbox"/>	Tere ishq na...	mp3	4,564,113...	a -----	NO	06/12/2015 ...
<input type="checkbox"/>	Jo bheji thi d...	mp3	4,165,798...	a -----	NO	06/12/2015 ...
<input type="checkbox"/>	ÀCTIVE~1	FLV	179,399,09...	a -----	YES	02/02/2015 ...
<input type="checkbox"/>	Spectrum (I...	zip	6,969,620...	a -----	YES	02/02/2015 ...
<input type="checkbox"/>	VoIP Is Ever...	zip	10,643 ...	a -----	YES	02/02/2015 ...
<input type="checkbox"/>	VoIP Is Ever...	docx	13,186 ...	a -----	YES	02/02/2015 ...
<input type="checkbox"/>	SeventhSon....	avi	682,372,74...	a -----	YES	02/02/2015 ...
<input type="checkbox"/>	Video Render	zip	63,303,424...	a -----	YES	02/02/2015 ...
<input type="checkbox"/>	ÀOIP	JPG	123,497 ...	a -----	YES	02/02/2015 ...

There is a way to copy the data and then view it in the user-friendly mode, but how? Follow the procedure below, by doing this you can maintain the integrity.

- The technique is very simple. Let say you want to analyze a single file, and then simply copy it and it on any other place, use Hex workshop to get the hash of that file and then do whatever you want to do. After completing the job, make sure to reanalyze the file again and compare it with the previously taken hash.

This screenshot shows a context menu open over a specific file entry in the file list. The menu includes options such as View, View As INFO/\$I, Copy File, Copy All Selected Files, Compare To Hashkeeper, Show Cluster Numbers, Add to Registry Viewer, Add to Event Log Viewer, View EXIF Data, View ACL Info, and Gallery View. The main window to the right shows a list of files with their names, sizes, and attributes. The file 'fport.zip' is currently selected.

- Here you can see, I have pasted this file somewhere else and generating the MD5 hash via Hex workshop.



Get the hash information and store it. Open this file without any fear, acquire the evidence, close the file, reanalyze the hash and you are done.

Click on **Save Project** to save the project and use it whenever you want.

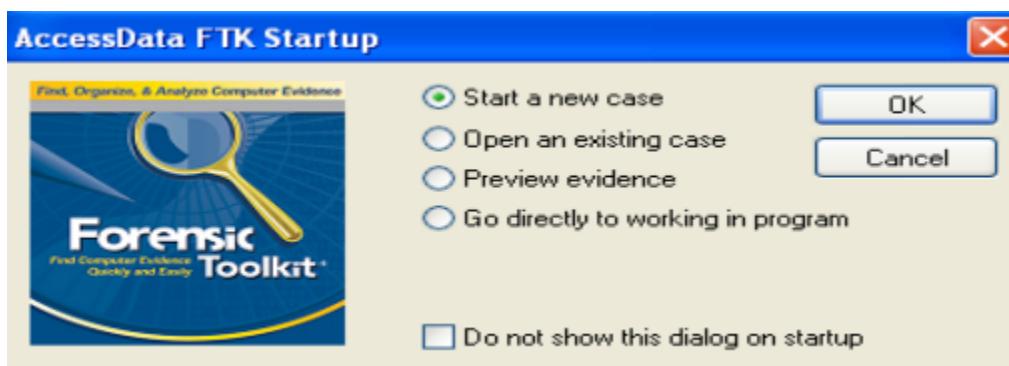
## AccessData Forensics Toolkit (FTK)

Accessdata FTK is a premium computer forensics and digital investigation software, it has:

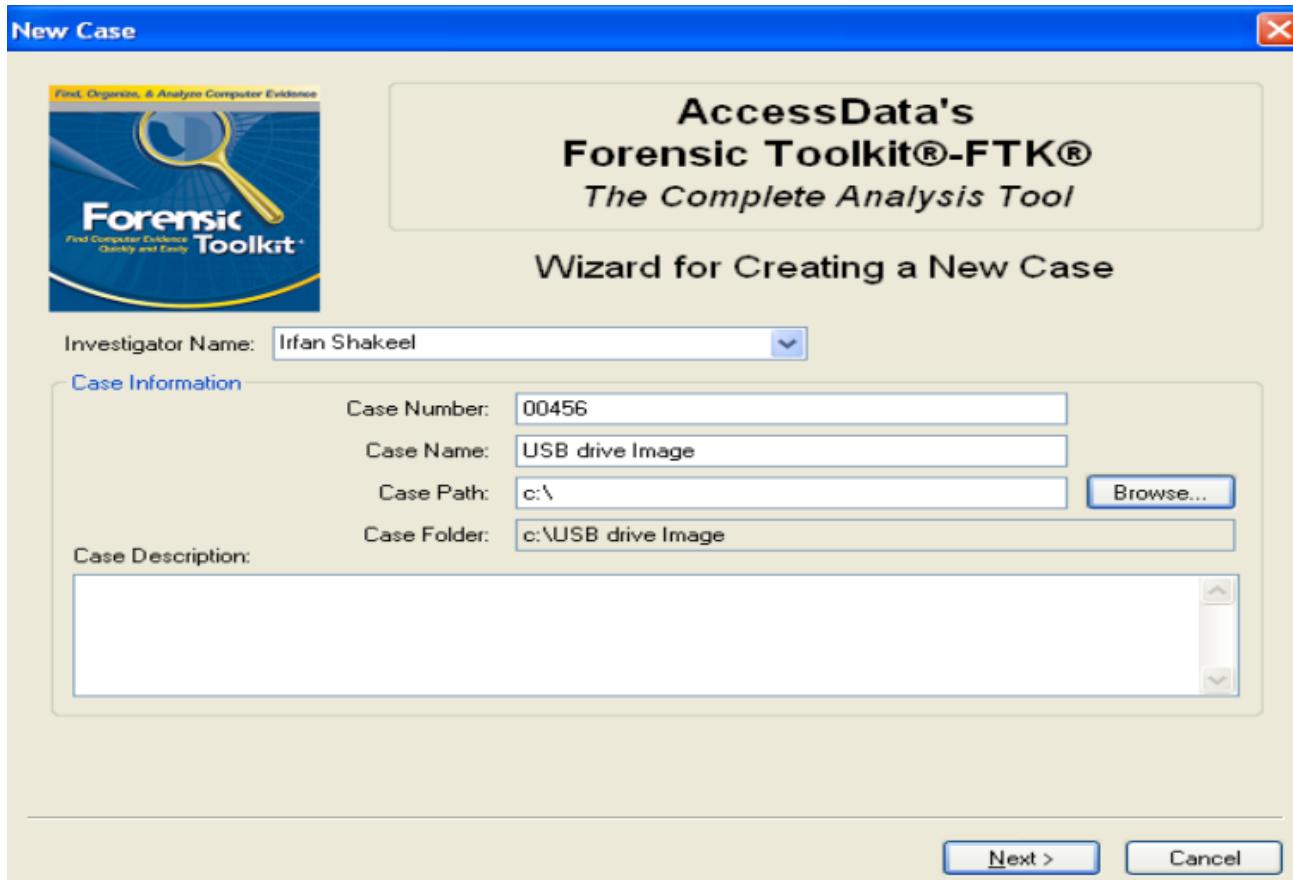
- Court cited solution
- Database driven for speed and resiliency
- Easily expandable given unified database
- An integrated feature set
- Interoperability with AccessData solutions

If the suspect has tried or successfully removed or wiped out the evidence, then don't worry, FTK is the best solution to find and recover the deleted files and folder. It has a strong case management and administration database too.

- After installation, open the program. You will be asked to create a case or work on any existing case. In our scenario, I am opening a case.



- Provide the detail of the case, as discussed; it has strong case management ability. Make sure to provide the right information that you use to maintain the database of the cases.



- It is recommended to leave the default case log options that provides approximately all the features of the software.

## Case Log Options



### Case Log Options

The case log is a text file named FTK.log in the case folder. It gets created automatically by FTK and contains a record of events that occur during the course of the case. You can choose which type of events you would like to be logged.

You can also add your own comments to the log file at any time by selecting "Add Case Log Entry..." under the "Tools" menu item, and you can view the log file by selecting "View Case Log" under the "Tools" menu item.

#### Events to go in the Case Log

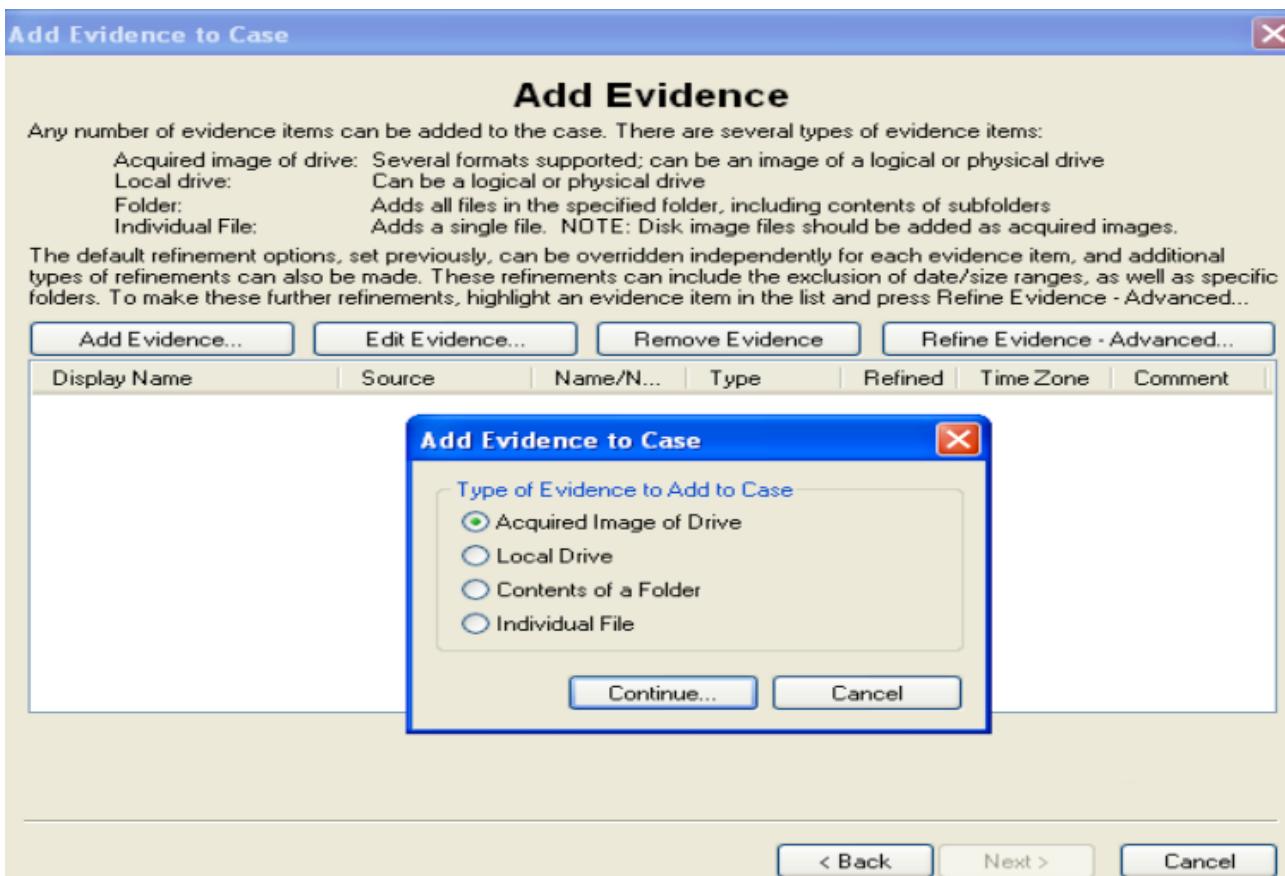
- |  |  |
|--|--|
| <input checked="" type="checkbox"/> Case and evidence events         | Events related to the addition and processing of file items when evidence is added or when using Analysis Tools later in the case. |
| <input checked="" type="checkbox"/> Error messages                   | Events related to any error conditions encountered during the case.  |
| <input checked="" type="checkbox"/> Bookmarking events               | Events related to the addition and modification of bookmarks.  |
| <input checked="" type="checkbox"/> Searching events                 | Events related to searching. All search queries and resulting hit counts will be recorded.   |
| <input checked="" type="checkbox"/> Data carving / Internet searches | Events related to special data carving or internet keyword searches that are performed during the case.                            |
| <input checked="" type="checkbox"/> Other events                     | Other events not related to the above, such as copying, viewing, and ignoring files.   |

< Back

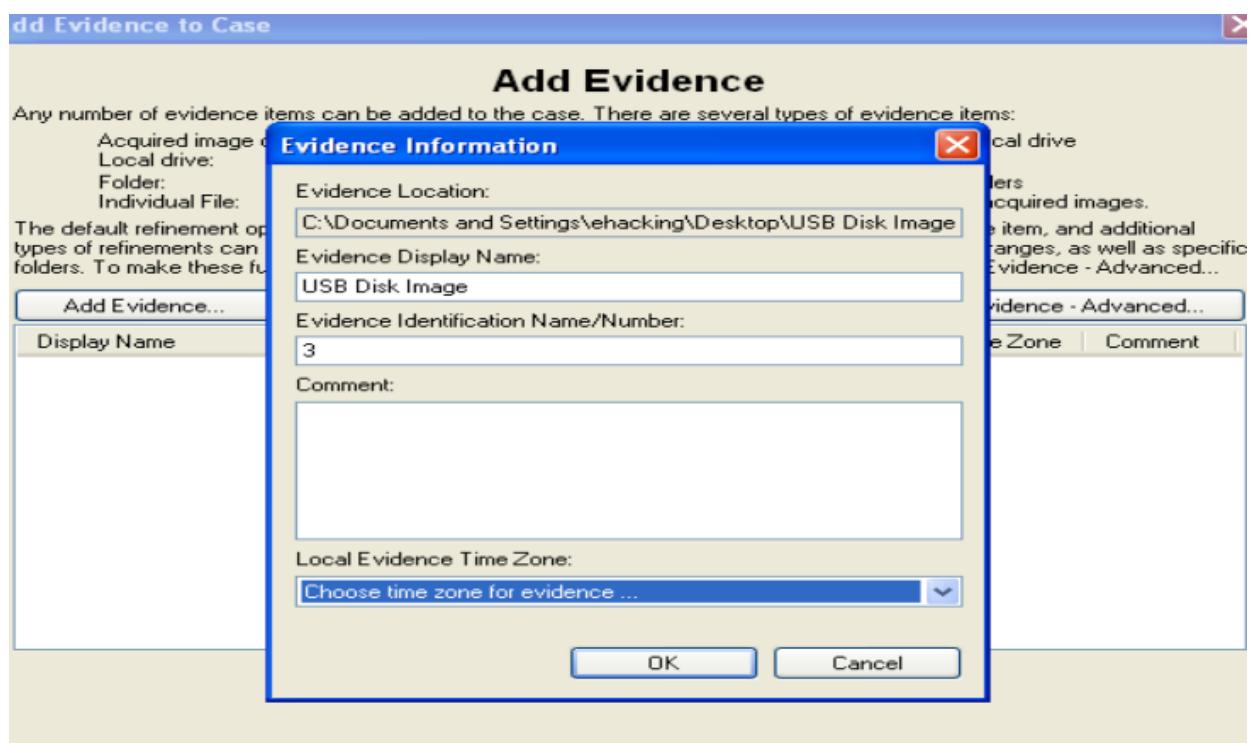
Next >

Cancel

- Click on Next and in the following window; you need to provide the image of the drive. Here I am browsing the image created before.



- Select the time zone and provide the evidence number (identification).



- The process to load the evidence image take some time depending on the size of the image.

When it is done, you will see the following summarize window, here you can see that total file items are 233 and 39 are deleted files, which were being removed by someone before taking the image of the disk (hmmmm interesting). There are six documents in the image while 37 multimedia files and the other useful information mentioned in the screen.

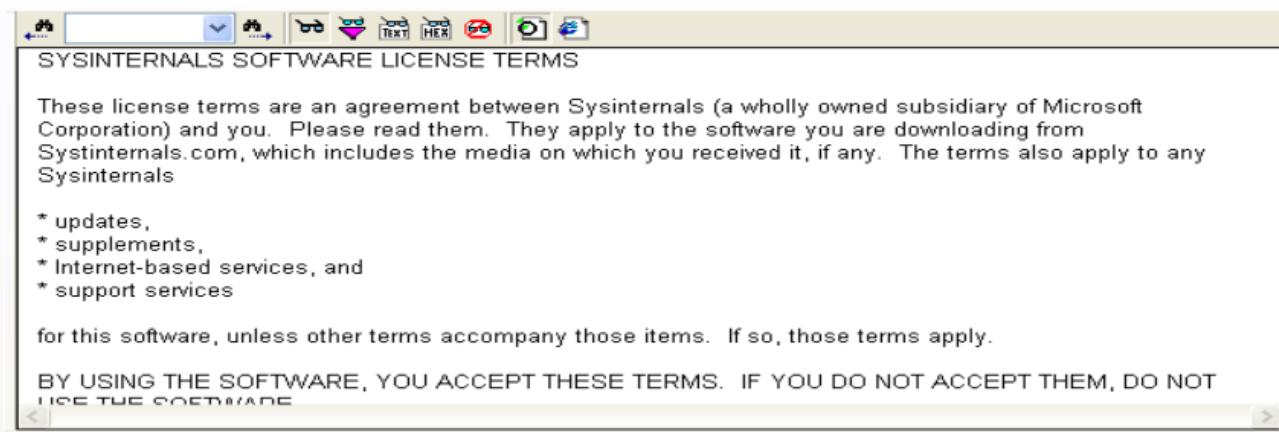
Evidence Items		File Status		File Category	
Evidence Items:	1	KFF Alert Files:	0	Documents:	6
<b>File Items</b>		Bookmarked Items:	0	Spreadsheets:	0
Total File Items:	233	Bad Extension:	0	Databases:	0
Checked Items:	0	Encrypted Files:	0	Graphics:	0
Unchecked Items:	233	From E-mail:	0	Multimedia:	37
Flagged Thumbnails:	0	<b>Deleted Files:</b>	<b>39</b>	E-mail Messages:	0
Other Thumbnails:	0	From Recycle Bin:	0	Executables:	15
Filtered In:	233	Duplicate Items:	10	Archives:	3
Filtered Out:	0	OLE Subitems:	0	Folders:	22
<b>Unfiltered</b>	<b>Filtered</b>	Flagged Ignore:	0	Slack/Free Space:	114
<b>All Items</b>	<b>Actual Files</b>	KFF Ignorable:	0	Other Known Type:	0
		Data Carved Files:	0	Unknown Type:	36

- Let's explore the image, here the folder with a cross sign mean that they have been removed. You can recover them to analyze.

The screenshot shows the FTK Explorer interface. On the left, there is a file tree view under the 'Case' section. It shows a 'USB Disk Image' with several sub-folders and files. Some files like 'IECYCLER' and 'INTITL~1' are marked with a red X, indicating they are deleted. On the right, there is a hex dump viewer showing binary data for a specific sector. Below the hex dump is a table of file metadata:

File Name	Full Path	Recycle Bi...	Ext	File Type	Category	Subject	Cr Date
Cut Videos	USB Disk Image\NO NAME-FAT32\Final\Cut Vi...			Folder	Folder		2/23/2015 6:10:
Dos	USB Disk Image\NO NAME-FAT32\Final\Dos			Folder	Folder		2/23/2015 2:00:
Fot 3 and 4	USB Disk Image\NO NAME-FAT32\Final\Fot 3 a...			Folder	Folder		2/23/2015 5:42:
Passive MITM P	USB Disk Image\NO NAME-FAT32\Final\Passiv...			Folder	Folder		2/23/2015 6:10:
Section 01	USB Disk Image\NO NAME-FAT32\Final\Sectio...			Folder	Folder		2/23/2015 1:25:
Section 02	USB Disk Image\NO NAME-FAT32\Final\Sectio...			Folder	Folder		2/23/2015 1:27:
Section 03	USB Disk Image\NO NAME-FAT32\Final\Sectio...			Folder	Folder		2/23/2015 1:25:
Section 04	USB Disk Image\NO NAME-FAT32\Final\Sectio...			Folder	Folder		2/23/2015 1:25:
Spooft 1 2	USB Disk Image\NO NAME-FAT32\Final\Spoo ...			Folder	Folder		2/23/2015 8:02:

- FTK has an ability to show the files in the user-friendly mode, here you can view the image, video file, text, unzip the folder and every other function. In the example below, I am reading a text file within FTK window.



Columns	Recycle Bi...	Ext	File Type	Category	Subject	Cr Date	Mod Date	Acc Date
rd...	txt	Plain Text D...	Document			2/23/2015 12:39:10 ...	2/23/2015 12:50:06 ...	2/22/2015 11:
p...	txt	Plain Text D...	Document		N/A		7/28/2006 9:32:44 AM	N/A
>...	txt	Plain Text D...	Document		N/A		7/28/2006 9:32:44 AM	N/A
p...	txt	Plain Text D...	Document		N/A		11/6/2007 8:17:34 AM	N/A
F...	txt	Plain Text D...	Document		N/A		6/5/2002 10:30:00 PM	N/A
\...	txt	Plain Text D...	Document			2/22/2015 11:19:36 ...	2/22/2015 11:19:36 ...	2/22/2015 11:

Therefore, this is how you create an image of a storage media and how an investigator should investigate the drive while maintaining integrity of the data. Every steps are mentioned above needs practice, create your forensics lab and perform the tasks. In the next topic, we will analyze a drive in a Linux machine.

## Disk Analysis on Linux – Autopsy

Sleuth Kit is the open-source computer forensics investigation suite, Autopsy is the front-end or user interface of Sleuth Kit. You can run Autopsy on Linux, Windows and MAC OS. Autopsy is very useful while analyzing FAT, NTFS, Ext3 and other file systems. If you want to conduct an investigation on the command-line, then use Sleuth Kit while the GUI is called Autopsy. It is available on the famous Linux distribution Kali Linux, so you need not to worry about the installation. You can open .dd extension of the disk image (we have created the file format while creating the image).

Important features are:

- Timeline Analysis: Displays system events in a graphical interface to help identify activity.
- Keyword Search: Text extraction and index-searched modules enable you to find files that mention specific terms and find regular expression patterns.
- Web Artifacts: Extracts web activity from common browsers to help identify user activity.
- Registry Analysis: Uses RegRipper to identify recently accessed documents and USB devices.
- LNK File Analysis: Identifies short cuts and accessed documents
- Email Analysis: Parses MBOX format messages, such as Thunderbird.
- EXIF: Extracts geo location and camera information from JPEG files.
- File Type Sorting: Group files by their type to find all images or documents.
- Media Playback: View videos and images in the application and not require an external viewer.

- Thumbnail viewer: Displays thumbnail of images to help quick view pictures.

Let's do it:

- On the Kali Linux **Applications** → **Kali Linux** → **Forensics** → **Digital Forensics** →

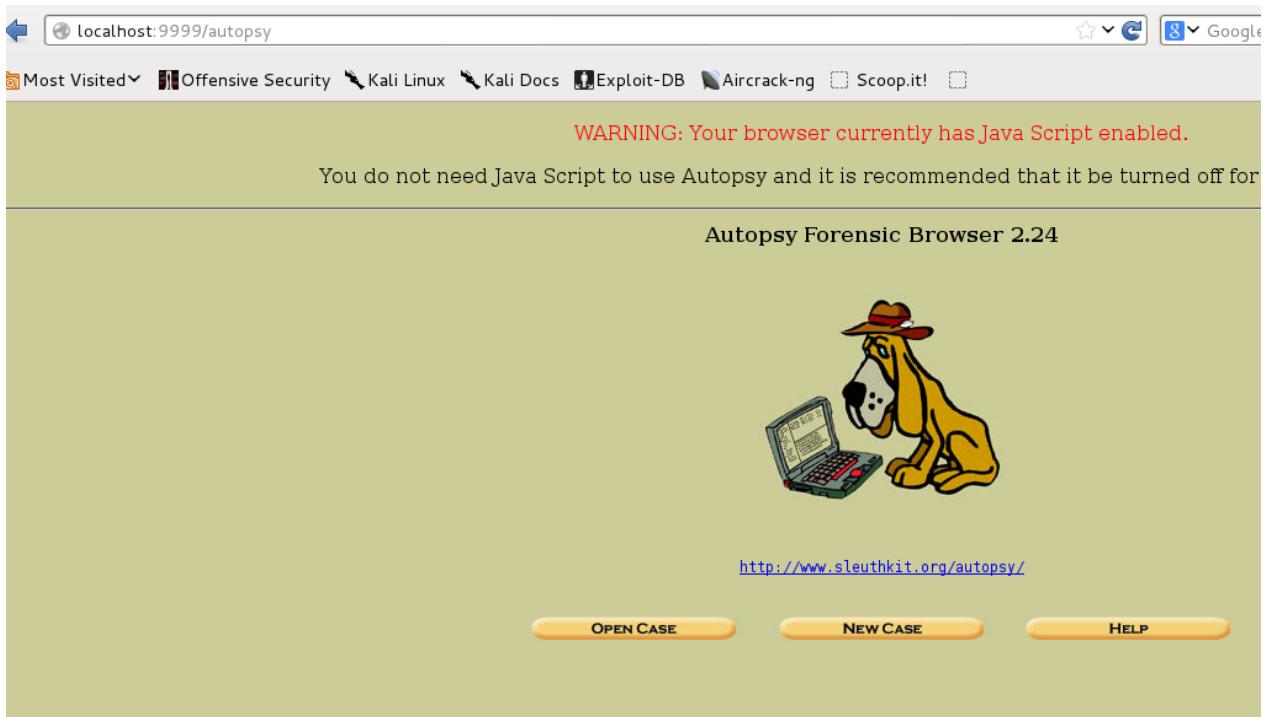
```

Terminal
File Edit View Search Terminal Help
=====
Autopsy Forensic Browser
http://www.sleuthkit.org/autopsy/
ver 2.24
=====
Evidence Locker: /var/lib/autopsy
Start Time: Sun Jun 21 05:32:06 2015
Remote Host: localhost
Local Port: 9999

Open an HTML browser on the remote host and paste this URL in it:
http://localhost:9999/autopsy
Keep this process running and use <ctrl-c> to exit
The quieter you become, the more you are able to hear
Autopsy

```

- Copy the local host URL and open your favorite browser, paste it and then you will see the first window of Autopsy.



- Click on **New Case**, it will ask the details of the case. Put the relevant information because it is for administrative and management purpose (think if you are investigating so many cases at the same time). You need to create history of every case. Put the information and click on New case:

## CREATE A NEW CASE

1. **Case Name:** The name of this investigation. It can contain only letters, numbers, and symbols.

00456-Data Theft

2. **Description:** An optional, one line description of this case.

Case given by XYZ

3. **Investigator Names:** The optional names (with no spaces) of the investigators for this case.

a. Irfan Shakeel  
c.  
e.  
g.  
i.

b. Rob  
d.  
f.  
h.  
j.

NEW CASE

CANCEL

HELP

- In the next window, click on **Add host**, provide the information and you can leave them blank. Click on **Add host** to proceed.
- Click on **Add image** and you will see the following window.

No images have been added to this host yet

Select the Add Image File button below to add one

ADD IMAGE FILE

CLOSE HOST

HELP

FILE ACTIVITY TIME LINES

IMAGE INTEGRITY

HASH DATABASES

VIEW NOTES

EVENT SEQUENCER

- Provide the path where the disk image is saved and move further.



- Select the calculate option so that Autopsy calculate the hash, that you will match with the previously created hash to make sure that the image is not changed.

**Local Name:** images/USB.dd

**Data Integrity:** An MD5 hash can be used to verify the integrity of the image. (With split images, this hash is for the full image file)

Ignore the hash value for this image.  
 Calculate the hash value for this image.  
 Add the following MD5 hash value for this image:  
  
 Verify hash after importing?

- Select the appropriate option from the tab to start your analysis, click on **File Analysis**



- You will see the content of the acquired image, now click on any file and take notes of the evidence.

Current Directory: [/2/](#)

[ADD NOTE](#) [GENERATE MD5 LIST OF FILES](#)

DEL	Type dir / in	NAME	WRITTEN	ACCESSED	CHANGED	SIZE	UID	GID	META
	d / d	<a href="#">\$OrphanFiles/</a>	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0	0	0	<a href="#">12881</a>
	d / d	<a href="#">..</a>	2003-08-10 09:15:05 (PKT)	2003-08-10 13:02:02 (PKT)	2003-08-10 09:15:05 (PKT)	1024	0	0	<a href="#">2</a>
	d / d	<a href="#">..</a>	2003-08-10 09:15:05 (PKT)	2003-08-10 13:02:02 (PKT)	2003-08-10 09:15:05 (PKT)	1024	0	0	<a href="#">2</a>
	d / d	<a href="#">.001/</a>	2003-08-10 09:15:57 (PKT)	2003-08-10 13:02:03 (PKT)	2003-08-10 09:15:57 (PKT)	1024	0	0	<a href="#">11105</a>
	r / r	<a href="#">.bash_history</a>	1997-01-14 13:28:11 (PKT)	1997-01-14 13:28:11 (PKT)	1997-01-14 13:28:11 (PKT)	23	0	0	<a href="#">1042</a>
	d / d	<a href="#">bin/</a>	2003-08-10 09:27:37 (PKT)	2003-08-10 13:02:03 (PKT)	2003-08-10 09:27:37 (PKT)	2048	0	0	<a href="#">1843</a>
	d / d	<a href="#">boot/</a>	1997-01-02 10:26:46 (PKT)	1997-01-02 10:26:46 (PKT)	1997-01-02 10:26:46 (PKT)	1024	0	0	<a href="#">3681</a>
	d / d	<a href="#">dev/</a>	2003-08-10 09:30:31 (PKT)	2003-08-10 13:02:02 (PKT)	2003-08-10 09:30:31 (PKT)	34816	0	0	<a href="#">7363</a>

- Analyze any file and then click on ASCII report to generate the basic report of the file.

r / r	<a href="#">ash.static</a>	2000-02-04 00:12:24 (PKT)	2000-02-04 00:12:24 (PKT)	1997-01-02 10:28:04 (PKT)	263064	0	0	<a href="#">1891</a>
l / l	<a href="#">awk</a>	1997-01-02 10:28:47 (PKT)	1997-02-13 12:38:02 (PKT)	1997-01-02 10:28:47 (PKT)	4	0	0	<a href="#">1911</a>
r / r	<a href="#">basename</a>	2000-03-07 16:15:36 (PKT)	2003-08-10 13:22:01 (PKT)	1997-01-02 10:30:04 (PKT)	5756	0	0	<a href="#">2003</a>
r / r	<a href="#">bash</a>	2000-02-27 22:44:41 (PKT)	2003-08-11 00:30:00 (PKT)	1997-01-02 10:27:31 (PKT)	316848	0	0	<a href="#">1856</a>

ASCII ([display - report](#)) \* Hex ([display - report](#)) \* ASCII Strings ([display - report](#)) \* Export \* Add Note  
File Type: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), dynamically linked (uses shared libs), for GNU/Linux 2.0.0, stripped

- Here is the sample report:

## Autopsy string Report

### GENERAL INFORMATION

```
File: /2//bin/basename  
MD5 of file: aled9b75c6481f7a612b54639b87cf64 -  
SHA-1 of file: 77ee338bb226062cble17e6356460d7ef3a14504 -  
MD5 of ASCII strings: 6fa6125e6ab04178241514121ceb5079 -  
SHA-1 of ASCII strings: 57a92a5efaaadde95264434ad15c48a82da045620 -
```

```
Image: '/var/lib/autopsy/00456-Data-Theft/host1/images/USB.dd'  
Offset: 10260 to 112859  
File System Type: ext
```

```
Date Generated: Sun Jun 21 06:03:50 2015  
Investigator: Rob
```

### META DATA INFORMATION

```
inode: 2003  
Allocated  
Group: 1  
Generation Id: 551086309  
uid / gid: 0 / 0  
mode: rrrwxr-xr-x  
size: 5756  
num of links: 1
```

```
Inode Times:  
Accessed: Sun Aug 10 13:22:01 2003  
File Modified: Tue Mar 7 16:15:36 2000  
Inode Modified: Thu Jan 2 10:30:04 1997
```

```
Direct Blocks:  
13348 13349 13350 13351 13352 13353
```

```
File Type: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), dynamically linked (uses shared libs), fo
```

### CONTENT

```
/lib/ld-linux.so.2  
gmon_start_  
libc.so.6
```

We have discussed the process to create a disk image, and how to view the content without compromising the integrity of the data. You have also witnessed the usage of most common computer forensic tools; you should not stop here and keep practicing every feature of the tools mentioned in the topics discussed earlier.

### ***End Note:***

This is the end of this mini course, but not certainly the end of knowledge and skills. It is highly recommended to create a forensics lab of your own to practice the skills acquired while reading this course material. Technology is changing every day, we have so many storage media and it is your job to understand the media so that you will be able to investigate whenever needed. Get the software discussed in this mini course and practice the evidence management of your own. Try your level best to maintain the integrity at every level, you might have noticed that, I have used this term so many times in the course. Yes, because it is crucial for your case.

Best of luck for your practice.



Republic of the Philippines  
National Police Commission  
**PHILIPPINE NATIONAL POLICE**  
**ANTI-CYBERCRIME GROUP**  
Camp BGen Rafael T Crame, Quezon City



### **DIGITAL FORENSIC UNIT CHECKLIST OF REQUIREMENTS**

#### **Type of Physical Evidence: CELLULAR PHONE**

Ownership: **Owned by Victim (Alive)**

1. Notarized letter of consent of the victim
2. Photocopy of the victim's valid Identification card
3. Memorandum Request for DFE
4. Spot Report/Investigation Report
5. Destination Storage Media (USB Flash Drive)

Ownership: **Owned by Victim (Deceased)**

1. Notarized letter of consent of the victim's nearest of kin
2. Photocopy of valid Identification card of the person who gave the consent
3. Memorandum Request for DFE
4. Spot Report/Investigation Report
5. Destination Storage Media (USB Flash Drive)

Ownership: **Owned by Suspect/s**

1. Court Order
2. Memorandum Request for DFE
3. Spot Report/Investigation Report
4. Destination Storage Media (USB Flash Drive)

#### **Type of Physical Evidence: COMPUTER HARD DRIVE**

1. Court Order
2. Memorandum Request for DFE
3. Spot Report/Investigation Report
4. Destination Storage Media (External Hard Drive)

#### **Type of Physical Evidence: CCTV FOOTAGE/ VIDEOS**

1. Court Order or Notarized letter of consent of the CCTV Footage/Video owner or his/her authorized representative
2. Photocopy of valid Identification card of the person who gave the consent
3. Memorandum Request for DFE
4. Spot Report/Investigation Report
5. Destination Storage Media (USB Flash Drive)



Republic of the Philippines  
National Police Commission  
**NATIONAL HEADQUARTERS, PHILIPPINE NATIONAL POLICE**  
**DIRECTORATE FOR INVESTIGATION AND DETECTIVE MANAGEMENT**  
Camp BGen Rafael T Crame, Quezon City



**DEC 04 2017.**

Investigative Directive No. 2017 - 17

### **Directive on the Referral and Conduct of Digital Forensic Examination**

#### **1. REFERENCES:**

- a. Republic Act No. 10175 otherwise known as the "Cybercrime Prevention Act of 2012";
- b. Police Operational Procedure (POP) Revised 2013;
- c. NAPOLCOM Memorandum Circular 2013-220 entitled "Approving the Activation of the Philippine National Police Anti-Cybercrime Group as a National Support Unit";
- d. The Revised Rules on Criminal Procedures;
- e. DOJ Legal Opinion No. LML-L-25H15-982 dated August 25, 2015; and
- f. DIDM IMPLAN re PNP Anti-Illegal Drugs Campaign Plan Project: "Double Barrel".

#### **2. BACKGROUND:**

The Anti-Cybercrime Group (ACG), created pursuant to Republic Act 10175, is responsible for the efficient and effective enforcement of its provisions<sup>1</sup>. Under the law and its Implementing Rules and Regulations, one of the functions of the ACG is to *conduct data recovery and forensic analysis on computer systems and other electronic evidence seized*.<sup>2</sup> These functions are also substantially laid down in NAPOLCOM Memorandum Circular 2013-220 and its PNP implementing orders, which mandates the ACG to perform the following tasks,<sup>3</sup> among others:

- *Conduct data recovery and forensic analysis on all computers, computer peripherals and storage devices, and other digital evidence seized by PNP units and any other law enforcement agencies within the country.*
- *Provide operational support to investigative units within the PNP, including the search, seizure, evidence preservation, and forensic examination of all digital evidence from crime scenes.*
- *Formulate guidelines for Cybercrime investigation, forensic evidence recovery and forensic data analysis.*

---

<sup>1</sup> Section 10, RA 10175

<sup>2</sup> Section 10, IRR of RA 10175

<sup>3</sup> NAPOLCOM Resolution No. 2013-220, February 27, 2013 and General Order No. DPL-12-09

To accomplish these tasks, the ACG maintains a Digital Forensic Laboratory (DFL) in the National Headquarters, and deploys Digital Forensic Examiners to its various field units/offices to provide technical assistance to cybercrime investigators and other operating units of the PNP, whenever it is alleged that a computer or computer system is used in the commission of the crime, or is the object of a cybercrime.

Since the ACG's creation up to the present, the DFL receives numerous requests from various PNP units for the conduct of digital forensic examinations on seized or recovered computers, computer systems, and storage devices.

Although the ACG understands that it is mandated to conduct *data recovery and forensic analysis on all computers, computer peripherals and storage devices, and other digital evidence seized by PNP units*, it is also aware that this obligation must be exercised with regard and consideration to established rules and legal procedures.

A review of the requests from other units would reveal that the devices referred for digital forensic examination were recovered from either of the following kinds of police operations:

- 1) Pursuant to a Search Warrant for cybercrime or cyber-enabled crime, where computer and other digital devices are the objects to be searched;
- 2) Pursuant to a Search Warrant for a traditional crime, where computer and other digital devices are not included as objects to be searched;
- 3) Seized through search incidental to a lawful arrest for a cybercrime or cyber-enabled crime;
- 4) Seized through search incidental to a lawful arrest for a traditional crime; or
- 5) From scenes of the crime during the conduct of police investigation.

### **3. RATIONALE:**

The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures, and their right to privacy of communications and correspondence, are rights protected by no less than the Philippine Constitution. The right to privacy to one's affairs may be inferred in the ban against unreasonable search and seizure and the prohibition against self-incrimination.

In recognition of these rights, certain laws, the Revised Rules on Criminal Procedures, the PNP Police Operational Procedure, and various jurisprudence had laid down sufficient parameters to guide state agents in ensuring that state action does not result to violation of any of the foregoing rights, and that evidence obtained are admissible in evidence in any judicial or quasi-judicial proceedings.

Established is the general rule that search and seizure requires court warrant, and that a search without a warrant may only be made in exceptional circumstances, such as when a person is lawfully arrested, and he has in his possession dangerous weapons or anything which may have been used or constitute proof in the commission of an offense<sup>4</sup>. The rules were clear until the advent of information and communications technology (ICT) produced a new type of evidence: *Digital Evidence*.

Unlike obtaining traditional evidence, the gathering of digital information is carried out by the search and examination of the contents of a digital device, the tapping or surveillance of network traffic, the interception of intangible communications, or the making of digital copies. The search and seizure of digital evidence has thus created a new forensic field in law enforcement investigation and prosecution, known as *Digital Forensics*.

The advent of digital evidence raised a number of questions, like, to what extent and circumstances may the police conduct a warrantless search of the contents of a person's mobile device upon a person's arrest? If the rules provide for the conduct of routine search after a valid warrantless arrest, does this search extend to the contents of the digital device seized from the arrested person in a forensic laboratory?

#### **4. PURPOSE**

This Investigative Directive prescribes the requirements to be observed by all PNP units in referring seized digital devices to the PNP ACG or in requesting for technical assistance for the conduct of digital forensic examination and analysis. The procedures and principles shall ensure that digital evidence is gathered in a manner that is admissible in any judicial, administrative or quasi-judicial bodies and the chain of custody is observed.

#### **5. GENERAL GUIDELINES:**

The following laws and rules established guidelines in determining proper law enforcement conduct in the search and seizure of digital evidence:

##### **1) Republic Act No. 10175 or the “Cybercrime Prevention Act”**

Under Section 15, search and seizure warrant is required before law enforcement authorities may conduct forensic analysis or examination. It states that:

**Section 15. Search, Seizure and Examination of Computer Data.** — Where a search and seizure warrant is properly issued, the law enforcement authorities shall likewise have the following powers and duties.

---

<sup>4</sup> Section 13 of Rule 126, Revised Rules on Criminal Procedure

Within the time period specified in the warrant, to conduct interception, as defined in this Act, and:

- (a) To secure a computer system or a computer data storage medium;
- (b) To make and retain a copy of those computer data secured;
- (c) To maintain the integrity of the relevant stored computer data;
- (d) To conduct forensic analysis or examination of the computer data storage medium; and
- (e) To render inaccessible or remove those computer data in the accessed computer or computer and communications network.

Section 18 discusses the consequence when evidence is obtained without observing the rule laid down above, which is also a general principle in law:

**Section 18. Exclusionary Rule.** — Any evidence procured without a valid warrant or beyond the authority of the same shall be inadmissible for any proceeding before any court or tribunal.

## 2) Police Operational Procedures Revised 2013

The PNP POP Revised 2013 has also echoed the same principle laid down under RA No. 10175. It dedicated an entire rule on Cybercrime Incident Response Procedure under Rule 36. In order to highlight the procedure, it is imperative to quote some pertinent rules on the search and seizure of data from digital devices:

### **36.2 Guidelines for Cybercrime Incident First Responder**

1) When responding to a cybercrime incident, or to a scene of the crime where computers (or electronic device, digital media, and other similar devices) are present, it is imperative for the First Responder (FR) to be able to protect, seize, and search the same and to be able to recognize potential evidence, using the following questions as guidelines to determine its role in the commission of the crime:

- (1) Is it a contraband or fruit of a crime?
- (2) Is it a tool used for the commission of the crime?
- (3) Is it only incidental to the crime, i.e. being used to store evidence of the crime?
- (4) Is it both instrumental to the crime and a storage device for evidence?

- 2) After identifying the theories as to the role of the computer in the commission of the crime, the following questions essential to any further police intervention should be considered by the first responder:
  - (1) Is there probable cause to seize the hardware?
  - (2) Is there probable cause to seize the software?
  - (3) Is there probable cause to seize the data?
  - (4) Where will the search and seizure be conducted?
- 3) Search of computers (*or electronic device, digital media, and other similar devices*) and seizure of data therefrom require a warrant issued by the court. (emphasis supplied)
- 4) Appropriate collection techniques shall be used to preserve the data sought to be seized.
- 5) The evidence seized shall be subjected to forensic examination by trained personnel. The result of the forensic examination, as well as the testimony of the forensic expert, shall be made available during the trial.

#### **36.4 Guidelines in the Treatment of Other Electronic Data Storage Devices**

The FR should understand that other electronic devices may contain viable evidence associated with the crime. The FR must ensure that, **unless an emergency exists**, the device should not be accessed. Should it be necessary to access the device, the FR should ensure that all actions associated with the manipulation of the device should be noted in order to document the chain of custody and ensure its admission as evidence in court.

To summarize, under the Cybercrime Prevention Act, one of the methods<sup>5</sup> of obtaining digital evidence is through the implementation of a search and seizure warrant. When a search and seizure is issued for a cybercrime offense, the operating team is now vested with the authority to conduct forensic examination, analysis and interception of a digital device or a communication, among others, during the life of the warrant.

This is the same principle laid down in the Police Operational Procedures as stated above. The POP states that search and seizure of computers requires a warrant, unless **an emergency exists**. Emergency or exigent circumstance has long been recognized as exception to the general rule of the necessity of a warrant before a search can be made. Emergency circumstance as exception includes those circumstances when police officers have reasonable ground to believe that a crime was being committed, however, they have no opportunity to apply for a search warrant from the courts because the latter were closed<sup>6</sup>.

---

<sup>5</sup> Another method is through the preservation, disclosure of data and interception under Section 13, 14, and 15 of RA 10175

<sup>6</sup> People v. De Gracia, G.R. Nos. 102009-10, July 6, 1994

### **3) Exigent Circumstance as culled from People vs. Enojas<sup>7</sup> (with discussion of *Riley v. California*<sup>8</sup>)**

In this case, Enojas was stopped by police officers when he suspiciously parked his taxi in front of a store. He was invited by the officers to go with them to the police station. On their way, the officers apprehended two robbers who exchanged gunshots with them, killing an officer. Enojas fled the scene.

The officers searched Enojas' abandoned car and found his mobile phone. They monitored the text messages on the phone and communicated with the other suspects, resulting to an entrapment operation. Enojas, along with the other suspects, were charged for murder.

The Court found that the text messages were properly admissible because the police officer, posing as Enojas, had personal knowledge of the messages and was competent to testify about them.

The search and seizure of information without a warrant under exigent circumstances is also recognized as an exception to the general rule in the latest American jurisprudence of *Riley v. California*<sup>9</sup>, where the US Supreme Court had the occasion to distinguish search incidental to a lawful arrest vis-à-vis extensive search of a digital device, in this manner:

“Digital data stored on a cell phone cannot itself be used as a weapon to harm an arresting officer or to effectuate the arrestee’s escape. Officers may examine the phone’s physical aspects to ensure that it will not be used as a weapon, but the data on the phone can endanger no one. To the extent that a search of cell phone data might warn officers of an impending danger, e.g., that the arrestee’s confederates are headed to the scene, such a concern is better addressed through consideration of case-specific exceptions to the warrant requirement, such as exigent circumstances.”

---

<sup>7</sup> G.R. No. 204894, March 10, 2014

<sup>8</sup> 573 US \_ 2014

<sup>9</sup> *Supra*.

## **6. SPECIFIC GUIDELINES**

R.A. No. 10175 states that the ACG<sup>10</sup> shall exclusively handle cases involving violations of the law. This means that cybercrimes, particularly defined in Section 4, shall be exclusively investigated by the ACG. However, other units may avail of the conduct of digital forensic examinations (and other authorities under Section 15 of RA No. 10175) for violations under Revised Penal Code (RPC) and other special laws, when it is alleged that the commission is by, through, and with the use of ICT.

The PNP ACG Digital Forensic Laboratory (DFL) shall conduct digital forensics examination and analysis on computers and other digital devices referred by other PNP units, either through technical assistance during the implementation of the warrant or in the laboratory, provided the following requirements are observed:

### **a. Search Warrant for an ICT-Enabled Crime**

- 1) The request for technical assistance shall be signed by the head of office and accompanied by a copy of the Warrant which indicates in the title that it was issued for an offense committed through ICT;
- 2) A Pre-Operational Coordination addressed to the Director, ACG or his authorized representatives shall be submitted at least three days prior to the implementation of the Warrant;
- 3) The conduct of forensic examination shall be valid during the life of the search warrant, which is ten (10) days from issuance;
- 4) If the on-site forensic examination is not yet complete, but the life of the warrant has already expired or the warrant was returned to court, the implementing unit shall request the court, upon the return of the warrant or the expiration of the 10-day period, for an extension of time to conduct digital forensic examination, and to issue orders directing the ACG to conduct the same;
- 5) Upon securing the said Court Order, the head of office, through the investigator-on-case and/or the evidence custodian, shall make a request to the ACG for the conduct of further examination, attaching the Court Order and enumerating therein the kind of digital evidence to be searched and examined by the forensic personnel;

---

<sup>10</sup> To include the Cybercrime Division of the NBI

- 6) The above request shall be accompanied by a destination/hard drive, which shall be at least twice the memory of the device being examined;
- 7) Before the lapse of the period of examination, the requesting unit/office shall coordinate with the DFL, through any means of communication, whether the examination may be complete before the lapse of the period given by the court. If the examination cannot be completed within the time provided in the Order, the requesting party shall make a Motion to the court for the extension of time to complete the examination;
- 8) Once the examination is complete, all data shall, within forty-eight (48) hours after the expiration of the time to conduct digital forensic examination, be deposited with the Issuing Court, if no criminal action has been instituted, otherwise, it shall be deposited with the Hearing Court;
- 9) The data shall be in a sealed package, and shall be accompanied by an affidavit of the law enforcement authority executing it stating the dates and times covered by the examination, and the law enforcement authority who may access the deposit, among other relevant data;
- 10) The law enforcement authority shall also certify that no duplicates or copies of the whole or any part thereof have been made, or if made, that all such duplicates or copies are included in the package deposited with the court; and
- 11) The package so deposited shall not be opened, or the recordings replayed, or used in evidence, or the contents revealed, except upon order of the court.

**b. Search Warrant for Traditional Crimes**

The digital forensic examination of computers or devices confiscated by PNP unit pursuant to the implementation of a search warrant for traditional crimes shall only be made when there is a court order directing the ACG to conduct the same, even if computers or devices were listed as items to be seized in the search warrant.

**c. Search and Seizure Incidental to a Lawful Arrest**

- 1) When the warrantless arrest of a suspect is pursuant to a cybercrime or ICT-enabled crime, the arresting officers may conduct a thorough search of his person, to include the confiscation of the device believed to have been used in the commission of an offense. Under exigent circumstances, the contents of the device may be searched by the personnel themselves *contemporaneous* to the arrest, or they may opt

- 2) to seek, as soon as the exigency of the circumstance becomes apparent, for technical assistance from the ACG;
- 3) The request shall be made, as much as possible, through a written request; however, if the said written request will defeat the purpose of examination, other forms of communications available to the PNP (use of official mobile numbers and emails) may be made, by the head of office to the Director of the ACG or his representatives; and
- 4) In cases where exigency is not present, the examination shall only be made when there is an Order from a competent court directing the ACG to conduct the said examination, following the other requirements discussed above.

**d. Consented Search**

- 1) When a crime is under investigation of a PNP unit, and the complainant or his witness desires that the police examine a legally owned computer or device in order to obtain evidence therefrom, the investigator-on-case shall cause the owner to sign a Consent to Search form, and attach the same to the unit's request to the ACG. In cases where the legal owner is deceased, the consent form shall be accomplished by the spouse or any direct family member.
- 2) In case of minors, consent shall be conformed by the parents or guardians, or in their absence, the DSWD or LSWDO as the case may be.
- 3) For requests coming from partners and other stakeholders, digital forensic examination may be extended to them provided it can be shown that the digital device is voluntarily submitted and there is legal purpose for the examination, recovery or preservation of data.

**e. CCTV Examination and Enhancement**

- 1) In cases where the request is for the enhancement of CCTV footage/s, a document showing consent of the CCTV owner shall be attached to the request.

**f. Other Forms**

- 1) When a digital or electronic device is recovered in a crime scene, and the owner thereof is dead, digital forensic examination may be made without a Court warrant. The requesting PNP unit shall specify in the request the type of information or data that shall be searched and seized.

- 2) When the owner of an electronic or digital device recovered from the crime scene is unknown or unidentified, the investigating unit shall obtain a search warrant from the court directing the ACG to conduct digital forensic examination on the device.
- 3) The search and seizure of government-issued computer or device to a public employee may be searched without a warrant<sup>11</sup>, provided it is shown that (a) the employee cannot have any reasonable expectation of privacy under the circumstances; and (b) the scope of the intrusion requested by the government agency is reasonable.
- 4) In requests for digital forensic examinations of computers owned by companies, pursuant to a criminal investigation conducted by a PNP unit, the company, through an authorized representative, shall issue a certification that the computer or device so requested for examination is owned by the company and company policy states that the user thereof does not expect privacy over said device.

## **7. ADDITIONAL GUIDELINES**

- a. All requests for technical assistance to the ACG shall be signed by the concerned unit commander/chief.
- b. The ACG reserves its right not to receive any electronic devices submitted for digital forensic analysis or examination, if upon initial evaluation/assessment, the said device(s) is/are beyond the capability of the digital forensic laboratory to examine.
- c. The ACG DFL shall notify the requesting party once the examination and analysis of the digital device is already complete. Upon notification, the requesting party shall have 45 days to claim the result of examination. If, after the expiration of the 45-day period from notification, the requesting party fails to claim the digital forensic result, the requesting party or responsible officer shall be administratively charged for Neglect of Duty.

## **8. RESPONSIBILITIES**

- a. DDIDM
  1. Supervise the implementation of this Investigative Directive; and
  2. Perform other tasks as directed.

---

<sup>11</sup> Pollo v. Constantino-David, et. al. G. R. No. 181881, October 18, 2011

- b. D, ACG
  - 1) Responsible for the effective implementation of this Investigative Directive; and
  - 2) Perform other tasks as directed.
- c. RDs, PROs
  - 1) Responsible for the proper dissemination and compliance of this Investigative Directive up to the Police Community Precinct (PCP) level of their respective AOR; and
  - 2) Perform other tasks as directed.
- d. D, LS
  - 1) Provide legal support and advice in implementing this Investigative Directive; and
  - 2) Perform other tasks as directed.

## **9. ADMINISTRATIVE SANCTIONS**

The filing of any administrative charge pursuant to NAPOLCOM MC 2016-002 shall proceed against a personnel who commit infractions, either through commission or omission, relative to the guidelines set forth in this Investigative Directive.

## **10. EFFECTIVITY**

This Directive shall take effect 15 days upon the date of signing. All prior issuances inconsistent with this Directive are deemed repealed.



AUGUSTO M MARQUEZ, JR  
Police Director

### **Distribution:**

RDs, PROs  
D, ACG  
D, LS

### **Copy furnished:**

PNP Command Group  
D- Staff  
Dirs, NSUs



# CRYPTOLOGY

Godwin S. Monserate

MSIT, CCNA/CCAI



# Objectives

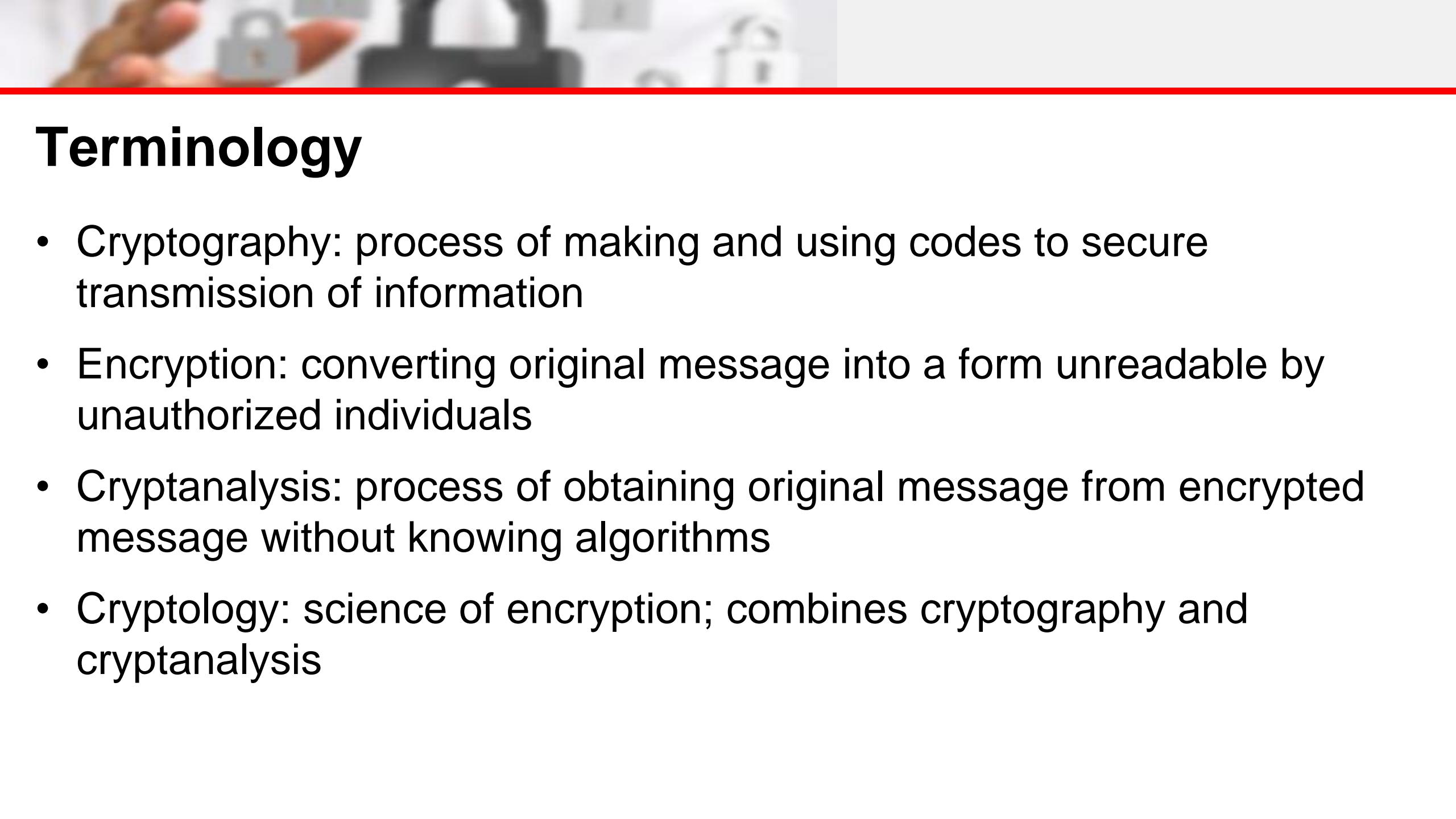
- Explain the difference between cryptology, cryptography and cryptanalysis
- Understand the basic principles of cryptography
- Understand the operating principles of the most popular tools in the area of cryptography
- List and explain the major protocols used for secure communications

# History and Timeline of Cryptography

- 1,900 BCE - Monumental Hieroglyphs of the Old Kingdom of Egypt
- 1,500 BCE - Mesopotamian Secrets of Pottery
- 800 - Al-Kindi, "The Philosopher of the Arabs"
- 1467 - Leon Battista Alberti, "The Father of Western Cryptography"
- 1586 - The Babington Plot
- 1853 - Vigenère's autokey cipher and the weaker Vigenère cipher
- 1917 - The Vernam Cipher
- 1923 - The Enigma Rotor Machine
- 1940 - Edgar Allan Poe Cracks the Code!
- 1942 - WW2 Japanese Navy Cryptography
- 1943 - The Colossus Computer
- 1953 - The VIC Cipher
- 1975 - The Data Encryption Standard
- 1976 - Diffie-Hellman key exchange
- 1991 - Phil Zimmermann, PGP (Pretty Good Privacy)
- 2001 - Advanced Encryption Standard
- November 2, 2007 -- NIST hash function competition announced.
- 2009 - Bitcoin network was launched.
- 2010 - The master key for High-bandwidth Digital Content Protection (HDCP) and the private signing key for the Sony PlayStation 3 game console are recovered and published using separate cryptoanalytic attacks. PGP Corp. is acquired by Symantec.
- 2012 - NIST selects the Keccak algorithm as the winner of its SHA-3 hash function competition.

# History and Timeline of Cryptography

- 2013 - Edward Snowden discloses a vast trove of classified documents from NSA. See Global surveillance disclosures (2013–present)
- 2013 - Dual\_EC\_DRBG is discovered to have a NSA backdoor.
- 2013 - NSA publishes Simon and Speck lightweight block ciphers.
- 2014 - The Password Hashing Competition accepts 24 entries.
- 2015 - Year by which NIST suggests that 80-bit keys be phased out.
- References
  - [http://www.cypher.com.au/crypto\\_history.htm](http://www.cypher.com.au/crypto_history.htm)
  - <https://www.timetoast.com/timelines/the-history-of-cryptography>
  - [https://en.wikipedia.org/wiki/Timeline\\_of\\_cryptography#2000\\_and\\_beyond](https://en.wikipedia.org/wiki/Timeline_of_cryptography#2000_and_beyond)



# Terminology

- Cryptography: process of making and using codes to secure transmission of information
- Encryption: converting original message into a form unreadable by unauthorized individuals
- Cryptanalysis: process of obtaining original message from encrypted message without knowing algorithms
- Cryptology: science of encryption; combines cryptography and cryptanalysis

# **Abash/Atbash Cipher**

- **Abash Cipher is one of the easiest methods for cryptography and crypto-analysis.**
- **It was first used for the Jewish language but it can be used for the other languages.**
- **The way of cryptography is to make the last letter of the language to the first letter.**
- **The method of cryptography in English:**

**Plain:** ABCDEFGHIJKLMNOPQRSTUVWXYZ

**Cipher:** ZYXWVUTSRQPONMLKJIHGFEDCBA

- **Example:**

<b>Plain Text:</b>	money
<b>Cipher Text:</b>	nlmvb

# Answer this Cipher... using Transposition Cipher Encryption

u	y	h	f		t	i	i	o	n
a	t	t		t		h	k	h	e
e	b		u	c	t	l	s	j	n
a	r	o	o	t	i	n	f	m	
r	s	c	s	a	n	e	a	u	
s	d	u	n	e	c	r	a		i
s		i	y		s	m	t	i	p
h			e	e	n	t	l	t	r
y	c	o		p	t	g	y	r	r
h			p			a	y		



# Cryptology Model



BOB

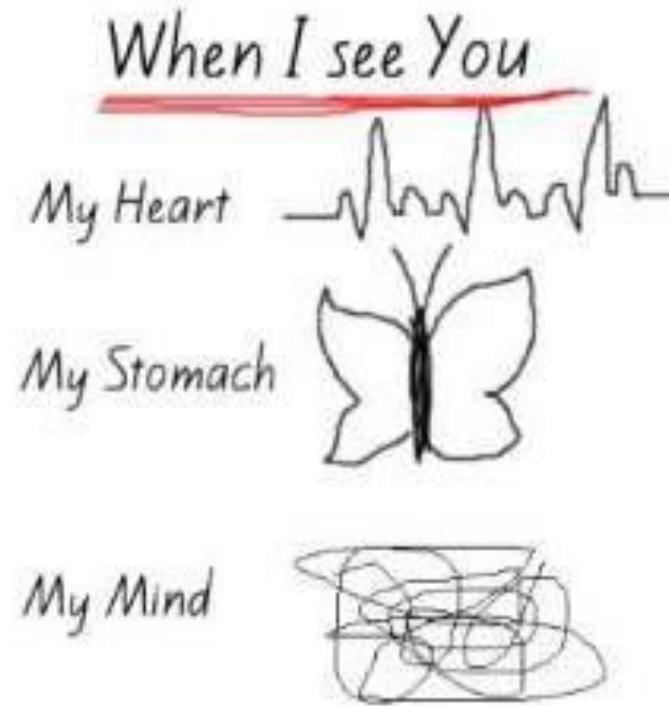


ALICE

# Cryptology Model



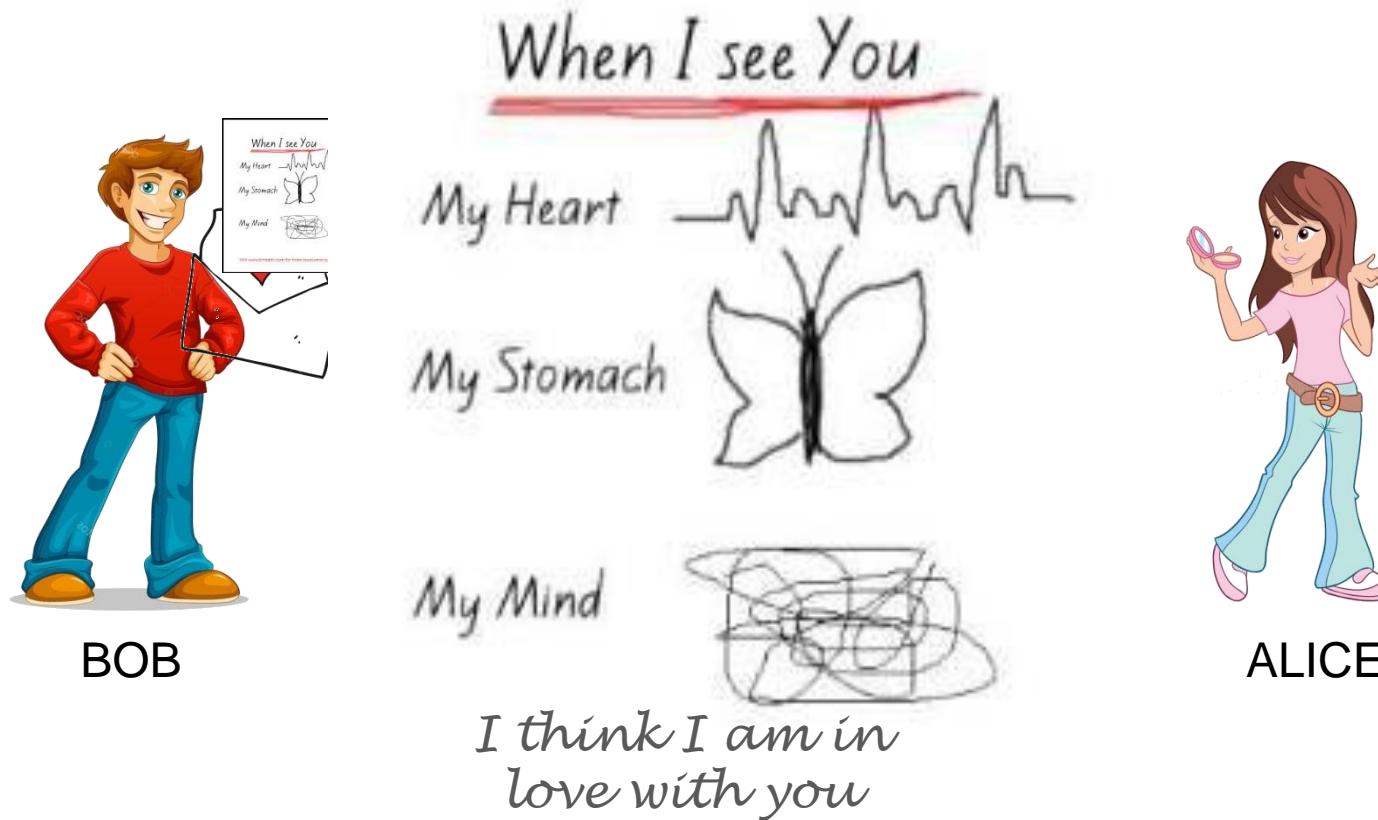
BOB



ALICE

*I think I am in  
love with you*

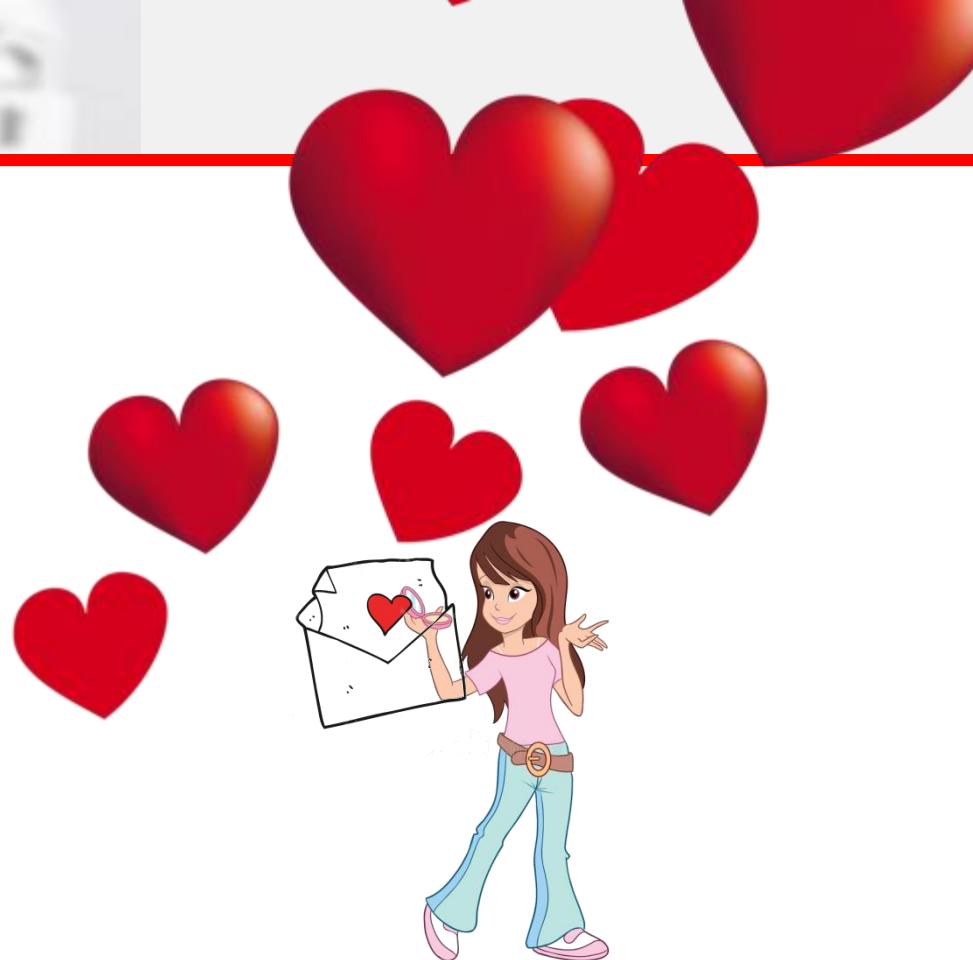
# Cryptology Model



# Cryptology Model



BOB



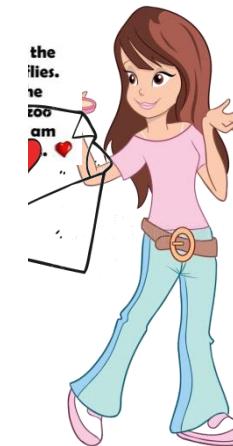
ALICE

# Cryptology Model

**Forget the  
butterflies.  
I feel the  
whole zoo  
when I am  
with you. ❤**



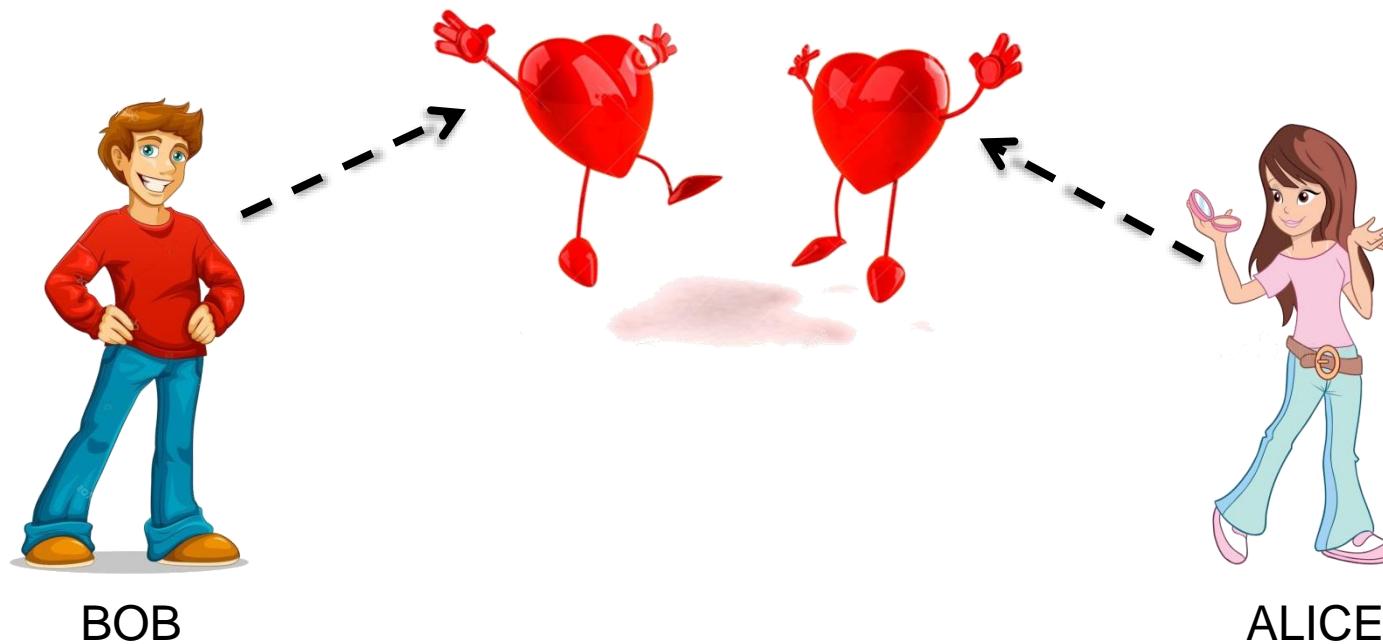
BOB



ALICE



# Cryptology Model



# Cryptology Model - Adversary



BOB



ALICE



EVE (Eavesdropper)



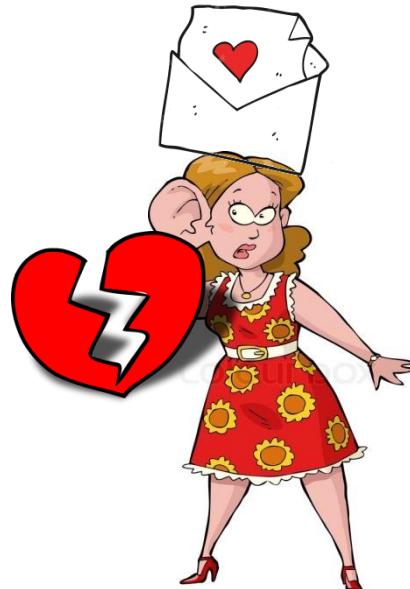
# Cryptology Model



BOB



ALICE



EVE (Eavesdropper)



# Cryptology Model



BOB



ALICE



EVE (Eavesdropper)



# Cryptology Model



BOB



ALICE



EVE (Eavesdropper)



# Cryptology Model – Applying Encryption





# Cryptology Model – Applying Encryption



BOB

ENCRYPTED  
MESSAGE



ALICE

# Cryptology Model – Applying Encryption

ENCRYPTED  
MESSAGE



BOB



ALICE



EVE (Eavesdropper)

# Cryptology Model – Applying Encryption



BOB



EVE (Eavesdropper)



ALICE

# Cryptology Model – Applying Encryption



BOB



EVE (Eavesdropper)



ALICE



# Cryptology Model – Applying Encryption

DECRYPT THE  
MESSAGE



BOB



ALICE



EVE (Eavesdropper)





# Cryptology Model – Applying Encryption



BOB

ENCRYPTED  
MESSAGE



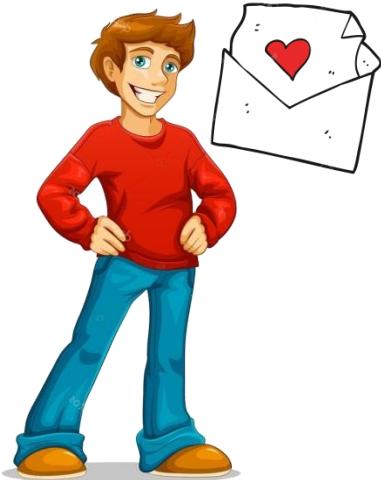
ALICE



EVE (Eavesdropper)

# Cryptology Model – Applying Encryption

DECRYPT  
MESSAGE



BOB



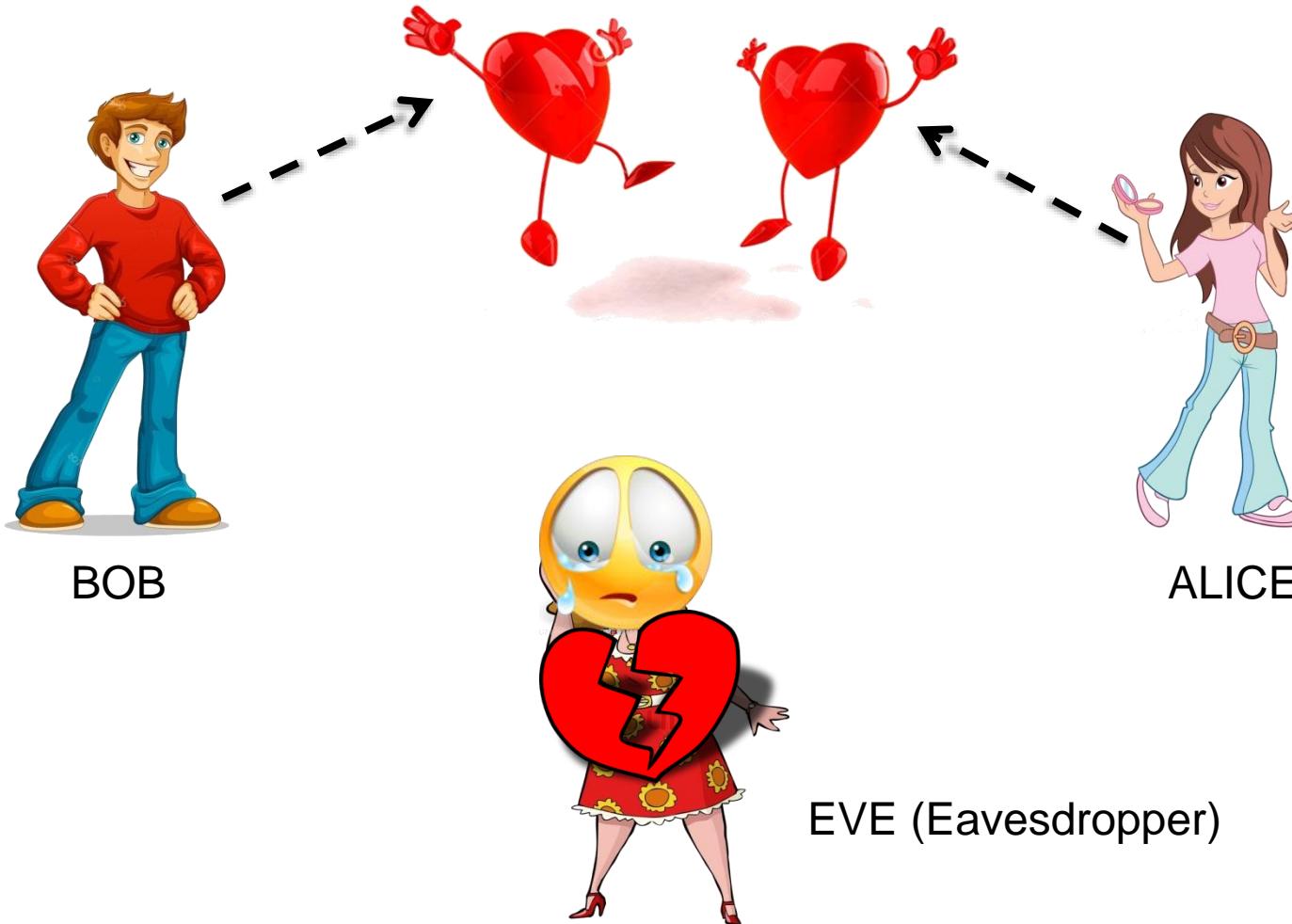
ALICE



EVE (Eavesdropper)

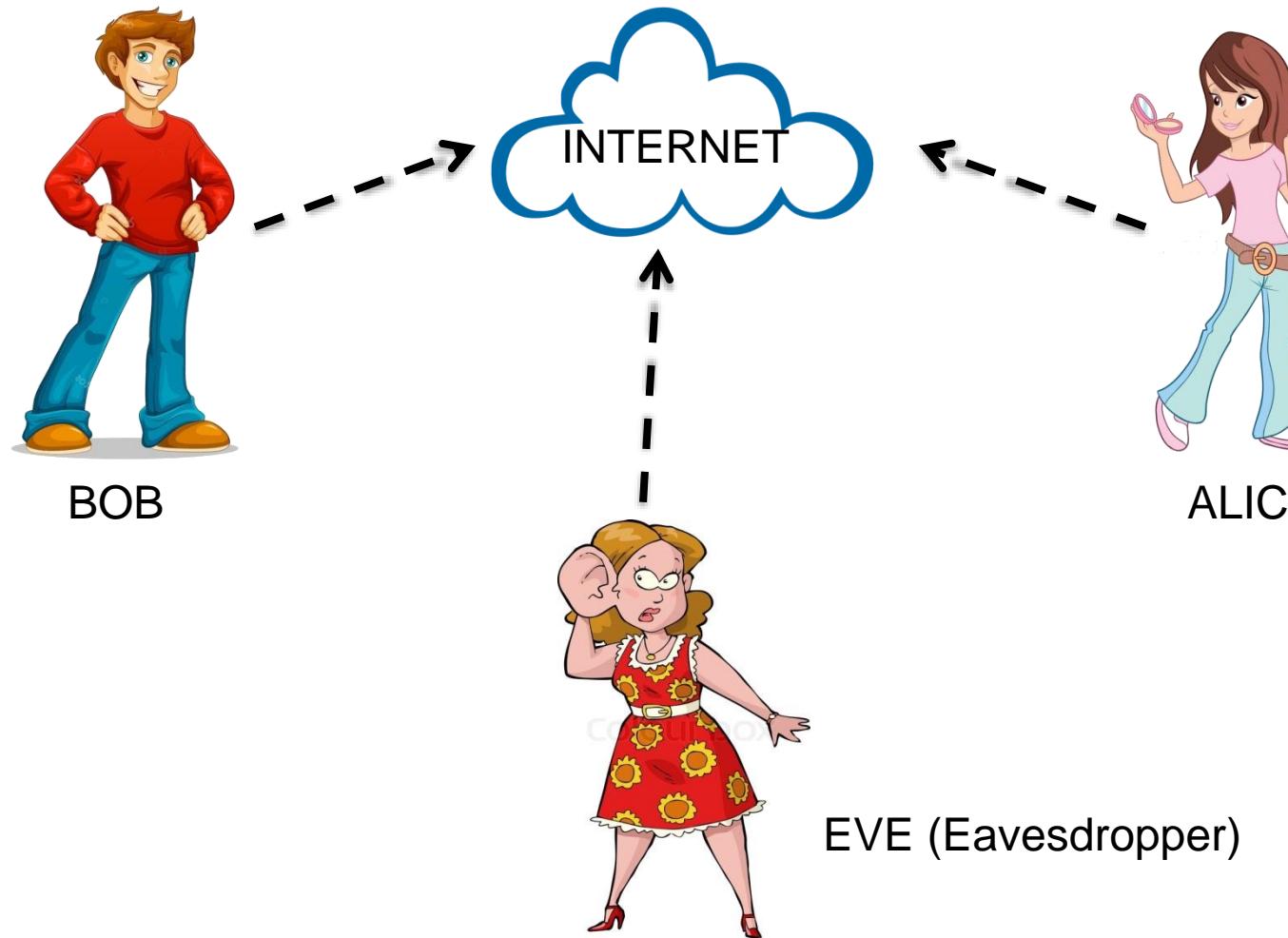


# Cryptology Model – Applying Encryption

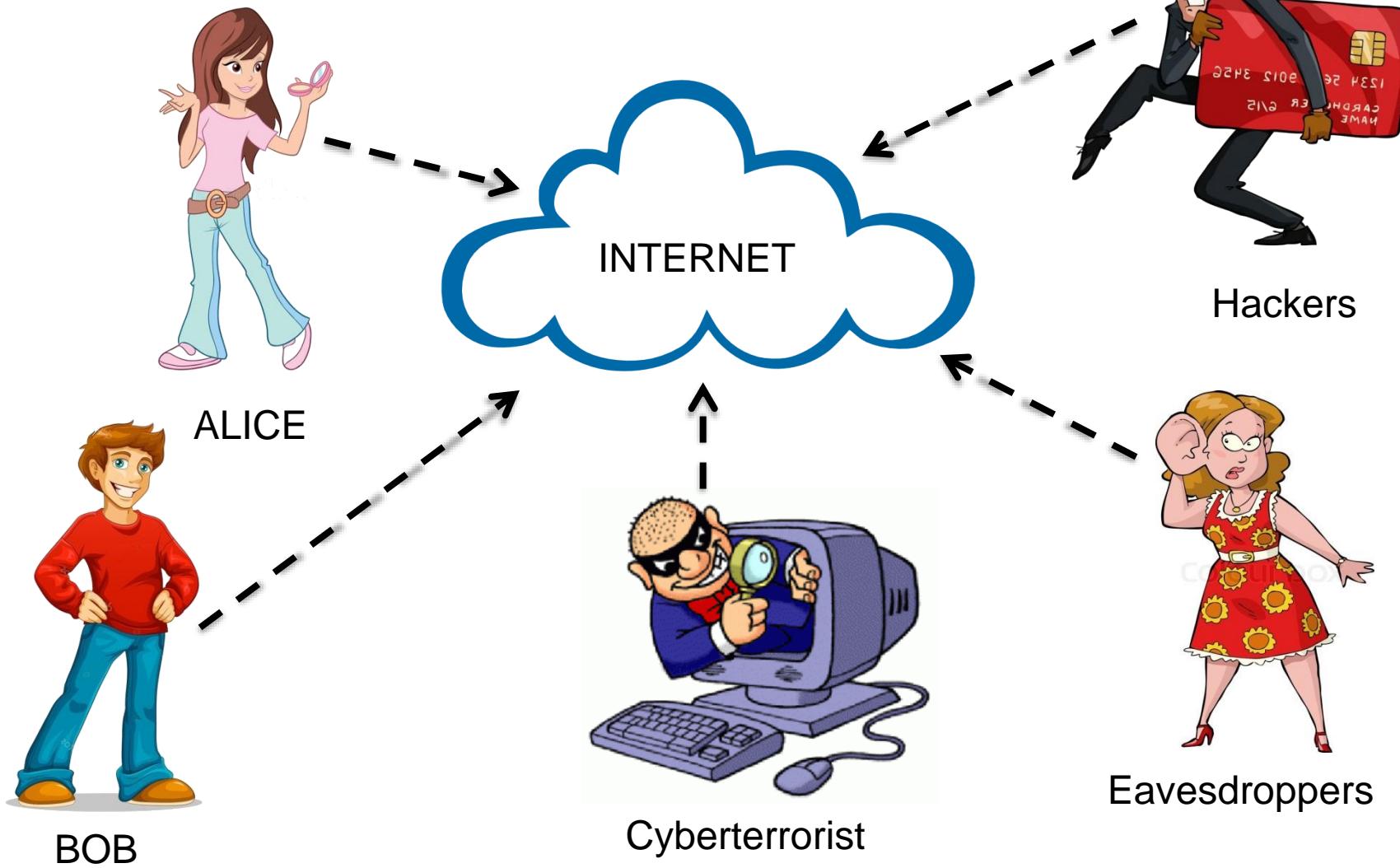




# Cryptology in the Internet



# Is there any need for Encryption?





# Principles of Cryptography

- With emergence of technology, need for encryption in information technology environment greatly increased
- All popular Web browsers use built-in encryption features for secure e-commerce applications



# Terminologies

- **Plaintext** – message or information that can be directly read by humans or a machine, ordinary readable text before being encrypted.
- **Ciphertext** is also known as encrypted or encoded information
- **Key** is a variable value that is applied using an algorithm to a string or block of unencrypted text to produce encrypted text, or to decrypt encrypted text.
- **Encryption** is the conversion of electronic data into another form, called **ciphertext**, which cannot be easily understood by anyone except authorized parties.
- **Decryption** is the process of taking encoded or encrypted text or other data and converting it back into text that you or the computer can read and understand.

# Elements of Cryptosystems

- Cryptosystems typically made up of algorithms, data handling techniques, and procedures
- Substitution cipher: substitute one value for another

m: Plaintext

c: Ciphertext

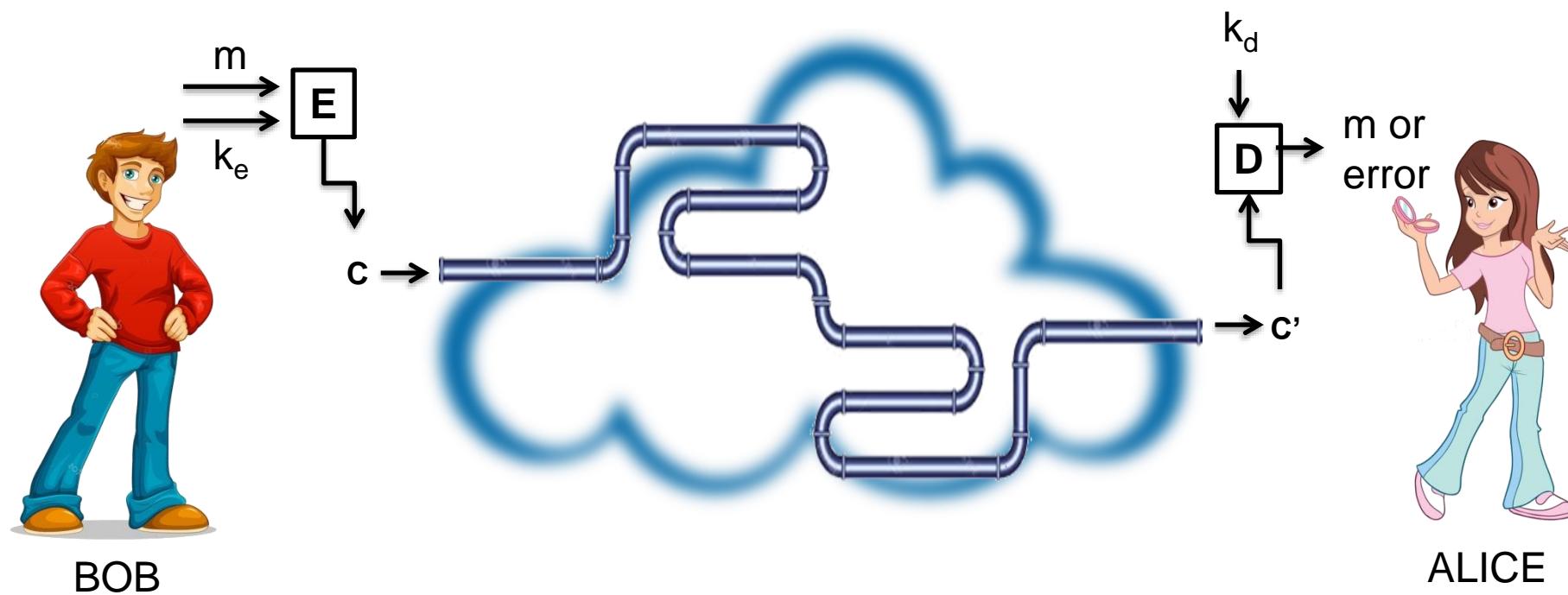
$k_e$ : Encryption Key

E: Encryption Program

$k_d$ : Decryption Key

D: Decryption Program

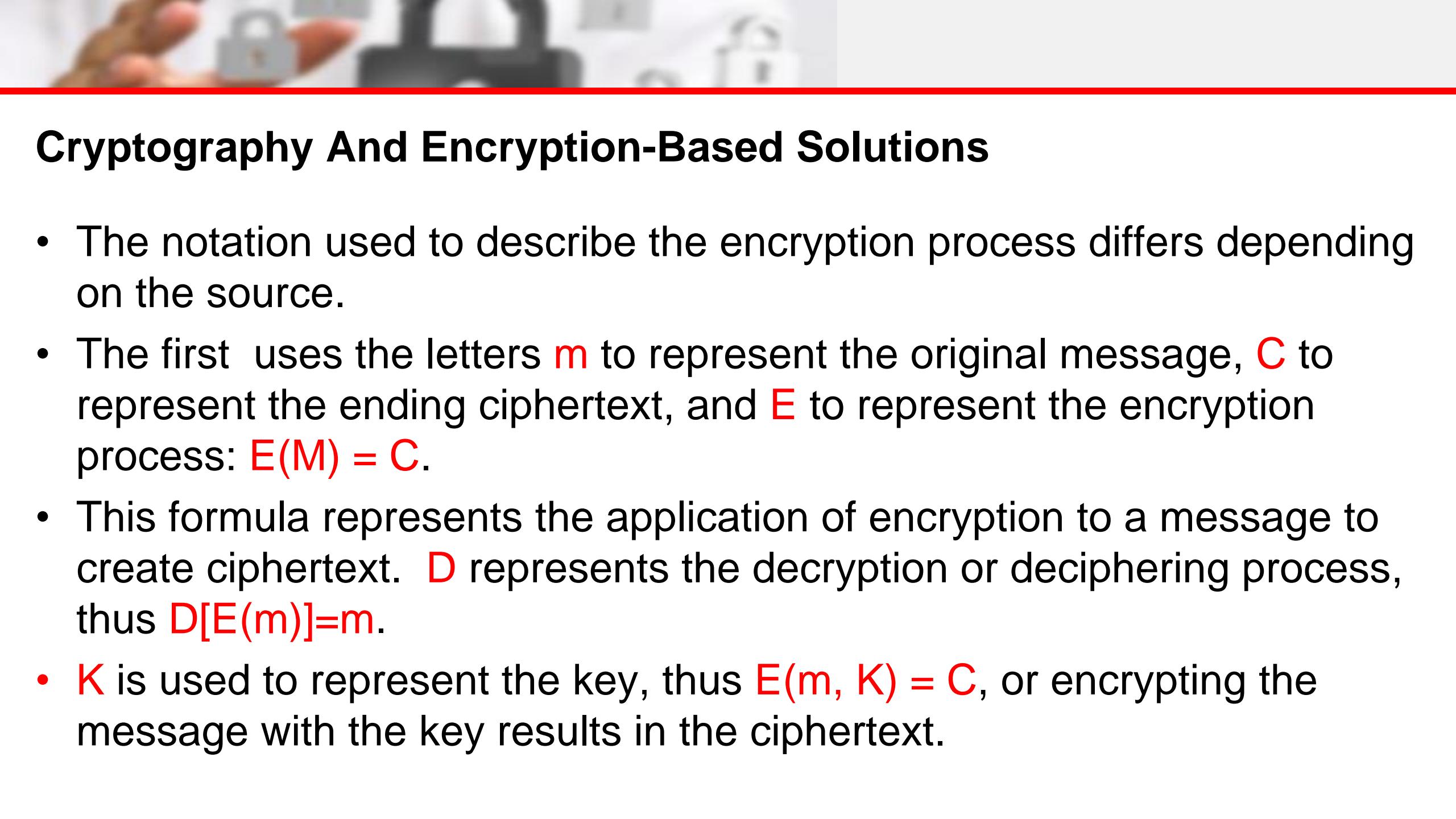
# Cryptosystem



m: Plaintext  
c: Ciphertext

$k_e$ : Encryption Key  
E: Encryption Program

$k_d$ : Decryption Key  
D: Decryption Program



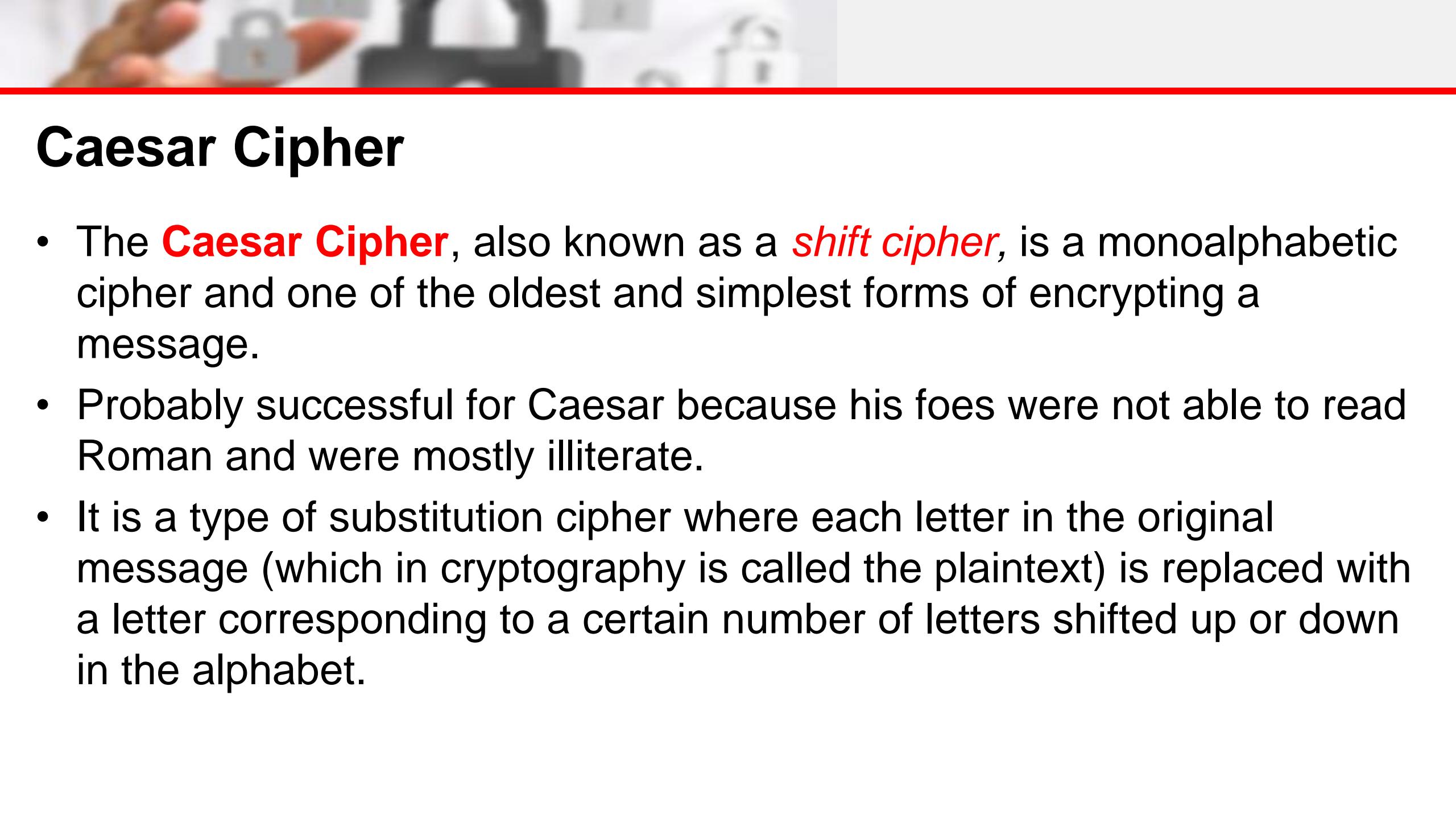
# Cryptography And Encryption-Based Solutions

- The notation used to describe the encryption process differs depending on the source.
- The first uses the letters **m** to represent the original message, **C** to represent the ending ciphertext, and **E** to represent the encryption process:  $E(M) = C$ .
- This formula represents the application of encryption to a message to create ciphertext. **D** represents the decryption or deciphering process, thus  $D[E(m)] = m$ .
- **K** is used to represent the key, thus  $E(m, K) = C$ , or encrypting the message with the key results in the ciphertext.



# Different Types of Ciphers

- **Monoalphabetic Ciphers**
- A monoalphabetic cipher mixes up the characters of the alphabet and uses that same arrangement for the entire message.
- The simple case would be to advance each letter some number of spaces, for example moving 10 letters down the alphabet, **A → L**
- There are only 25 possibilities to check, so this type of cipher is trivial to solve



# Caesar Cipher

- The **Caesar Cipher**, also known as a *shift cipher*, is a monoalphabetic cipher and one of the oldest and simplest forms of encrypting a message.
- Probably successful for Caesar because his foes were not able to read Roman and were mostly illiterate.
- It is a type of substitution cipher where each letter in the original message (which in cryptography is called the plaintext) is replaced with a letter corresponding to a certain number of letters shifted up or down in the alphabet.

# Monoalphabetic Ciphers Tool



# How to use Caesar Cipher Encryption

- For example, here's the Caesar Cipher encryption of a full message, using a right shift of 3.



A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W

Plaintext:

THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG

Ciphertext:

QEB NRFZH YOLT KCLU GRJMP LSBO QEB IXWV ALD

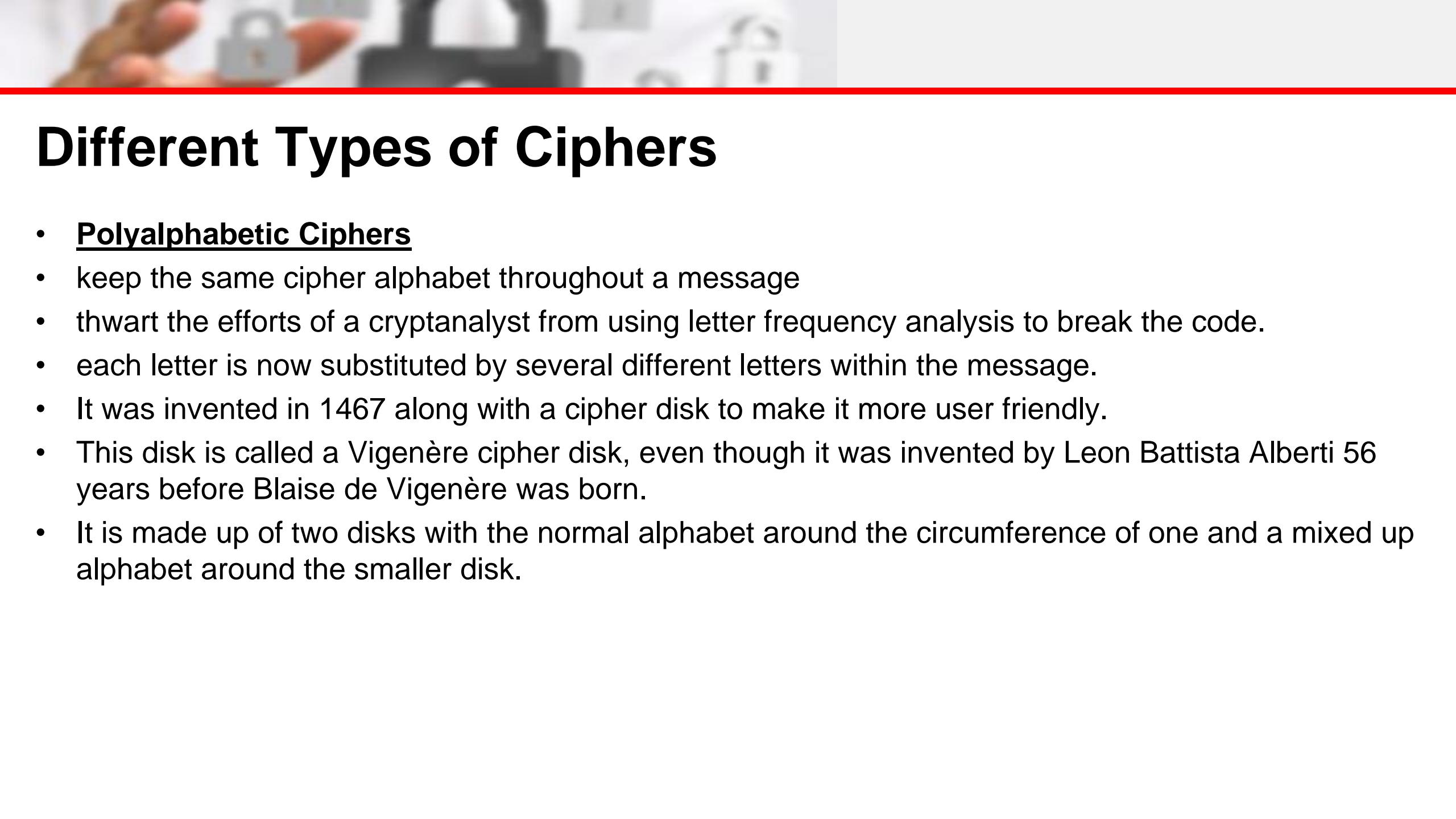
# Caesar Cipher Mathematical form

- The Caesar Cipher can be expressed in a more mathematical form as follows:

$$E_n(x) = (x + n) \bmod 26$$

- Decryption of the encrypted text (called the **ciphertext**) would be carried out similarly, subtracting the shift amount.

$$D_n(x) = (x - n) \bmod 26$$



# Different Types of Ciphers

- **Polyalphabetic Ciphers**
- keep the same cipher alphabet throughout a message
- thwart the efforts of a cryptanalyst from using letter frequency analysis to break the code.
- each letter is now substituted by several different letters within the message.
- It was invented in 1467 along with a cipher disk to make it more user friendly.
- This disk is called a Vigenère cipher disk, even though it was invented by Leon Battista Alberti 56 years before Blaise de Vigenère was born.
- It is made up of two disks with the normal alphabet around the circumference of one and a mixed up alphabet around the smaller disk.

# Polyalphabetic Ciphers Tool



Vigenère cipher disk



Jefferson Wheel Cypher

# Vigenere Encryption and Decryption

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y



# Encrypting message

1. Plaintext: **I LOVE YOU ALICE**
2. Create a keyword is **CEBUCITY**. Then, the keyword must be repeated
3. Remove all spaces and punctuation, and dividing the result into 5-letter blocks. As a result, the above plaintext and keyword become the following:

ILOVE YOUAL ICE  
CEBUC ITYCE BUC

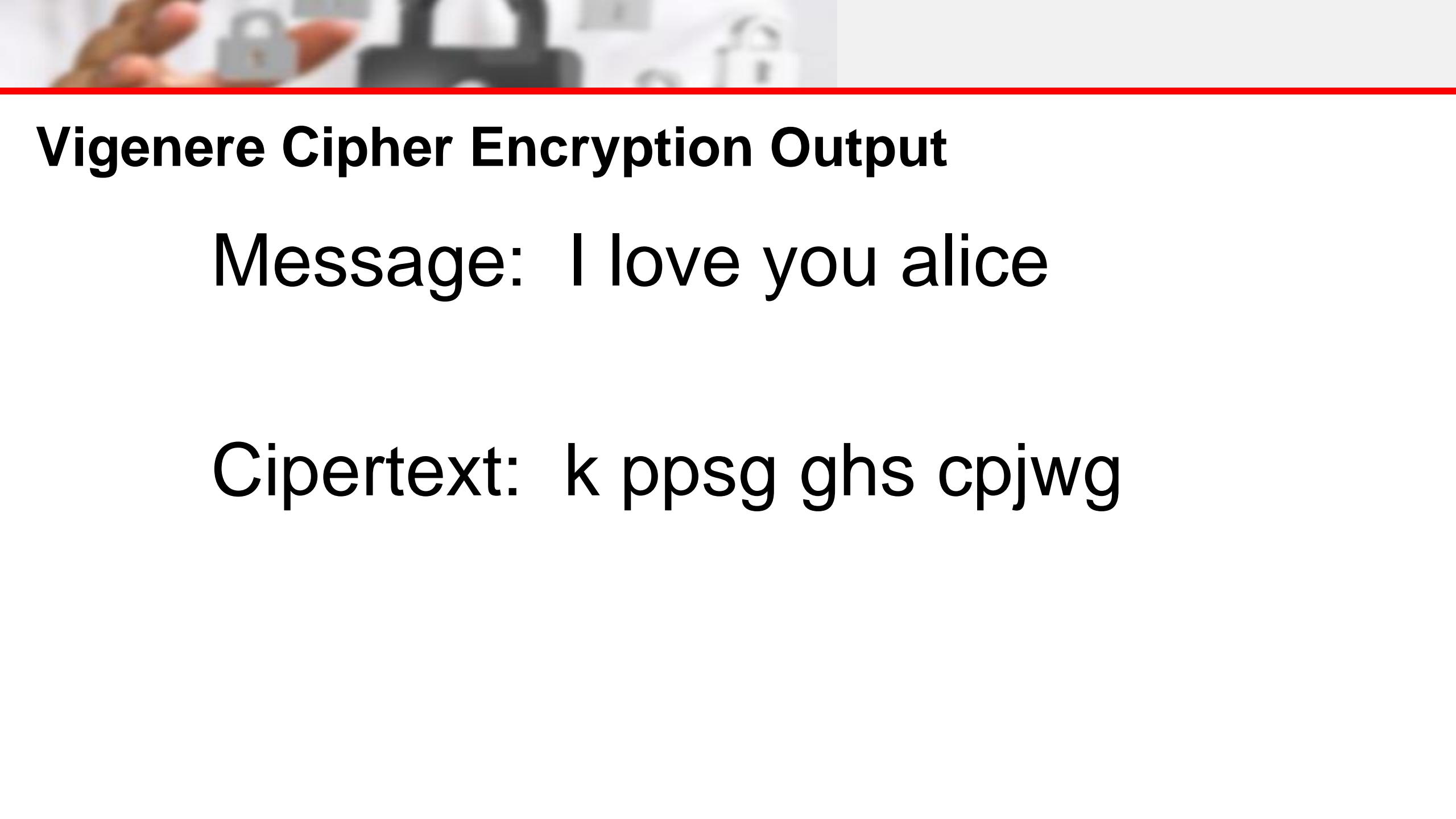
# How to use Vigenere Cipher Encryption

1. To encrypt, pick a letter in the plaintext and its corresponding letter in the keyword
2. use the keyword letter and the plaintext letter as the row index and column index, respectively, and the entry at the row-column intersection is the letter in the ciphertext.
3. For example, plaintext is **I**, keyword letter is **C**. Row of I and column of C, intersect at **K** which is the encrypted result.

Col	i	I	o	v	e	y	o	u	a	I	i	c	e
Row	c	e	b	u	c	i	t	y	c	e	b	u	c
encryption	K	P	P	Q	G	H	G	T	C	P	J	E	M

# Vigenere Encryption and Decryption

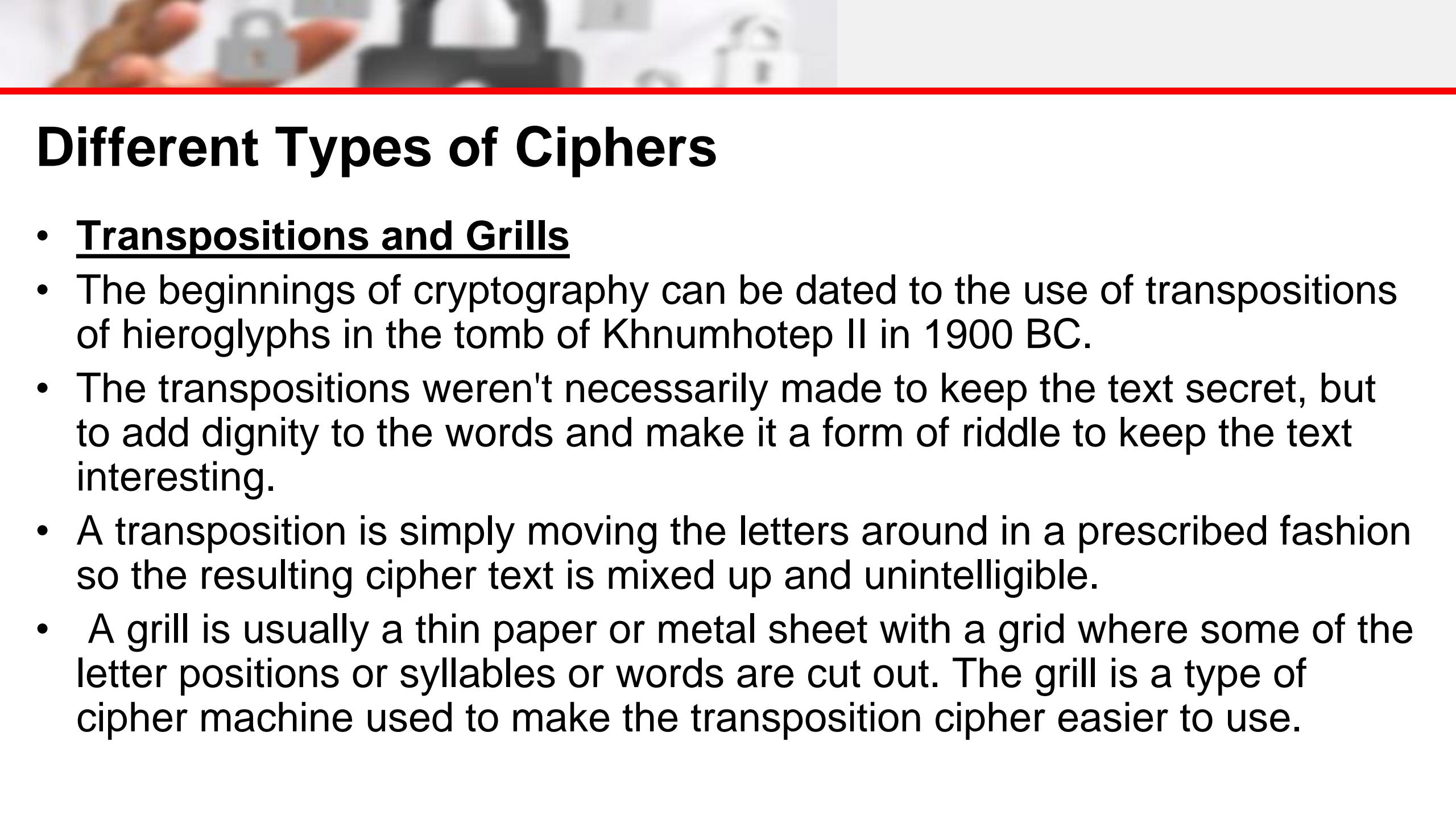
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y



# Vigenere Cipher Encryption Output

Message: I love you alice

Ciphertext: k ppsg ghs cpjwg



# Different Types of Ciphers

- **Transpositions and Grills**
- The beginnings of cryptography can be dated to the use of transpositions of hieroglyphs in the tomb of Khnumhotep II in 1900 BC.
- The transpositions weren't necessarily made to keep the text secret, but to add dignity to the words and make it a form of riddle to keep the text interesting.
- A transposition is simply moving the letters around in a prescribed fashion so the resulting cipher text is mixed up and unintelligible.
- A grill is usually a thin paper or metal sheet with a grid where some of the letter positions or syllables or words are cut out. The grill is a type of cipher machine used to make the transposition cipher easier to use.

# Transposition Ciphers Tool



# How to use Transposition Cipher Encryption

1. Create a plaintext example:

Meet at three pm today at the usual location

2. Arrange the plaintext according to 6 columns character and create a keyword eg. ZEBRAS

Z	E	B	R	A	S
m	e	e	t	a	t
t	h	r	e	e	p
m	t	o	d	a	y
a	t	t	h	e	u
s	u	a	l	l	o
c	a	t	i	o	n

# How to use Transposition Cipher Encryption

1. Arrange the plaintext according to 6 columns character using the keyword ZEBRAS
2. Look for Alphabetic sequence of the word ZEBRA e.i. A, B, E, R, S, Z

aeaelo

Z	E	B	R	A	S
m	e	e	t	a	t
t	h	r	e	e	p
m	t	o	d	a	y
a	t	t	h	e	u
s	u	a	l	I	o
c	a	t	i	o	n

# How to use Transposition Cipher Encryption

1. Arrange the plaintext according to 6 columns character and create a keyword eg. ZEBRAS
2. Look for Alphabetic sequence of the word ZEBRA e.i. A, B, E, R, S Z

aeaelo erotat

Z	E	B	R	A	S
m	e	e	t	a	t
t	h	r	e	e	p
m	t	o	d	a	y
a	t	t	h	e	u
s	u	a	l	l	o
c	a	t	i	o	n

# How to use Transposition Cipher Encryption

1. Arrange the plaintext according to 6 columns character and create a keyword eg. ZEBRAS
2. Look for Alphabetic sequence of the word ZEBRA e.i. A, B, E, R, S Z

aeaelo erotat  
ehttua

Z	E	B	R	A	S
m	e	e	t	a	t
t	h	r	e	e	p
m	t	o	d	a	y
a	t	t	h	e	u
s	u	a	l	l	o
c	a	t	i	o	n

# How to use Transposition Cipher Encryption

1. Arrange the plaintext according to 6 columns character and create a keyword eg. ZEBRAS
2. Look for Alphabetic sequence of the word ZEBRA e.i. A, B, E, R, S Z

aeaelo erotat  
ehttua tedhli

Z	E	B	R	A	S
m	e	e	t	a	t
t	h	r	e	e	p
m	t	o	d	a	y
a	t	t	h	e	u
s	u	a	l	l	o
c	a	t	i	o	n

# How to use Transposition Cipher Encryption

1. Arrange the plaintext according to 6 columns character and create a keyword eg. ZEBRAS
2. Look for Alphabetic sequence of the word ZEBRA e.i. A, B, E, R, S Z

aeaelo erotat  
ehttua tedhli  
tpyuon

Z	E	B	R	A	S
m	e	e	t	a	t
t	h	r	e	e	p
m	t	o	d	a	y
a	t	t	h	e	u
s	u	a	l	l	o
c	a	t	i	o	n

# How to use Transposition Cipher Encryption

1. Arrange the plaintext according to 6 columns character and create a keyword eg. ZEBRAS
2. Look for Alphabetic sequence of the word ZEBRA e.i. A, B, E, R, S Z

aeaelo erotat  
ehttua tedhli  
tpyuon mtmasc

Z	E	B	R	A	S
m	e	e	t	a	t
t	h	r	e	e	p
m	t	o	d	a	y
a	t	t	h	e	u
s	u	a	l	l	o
c	a	t	i	o	n

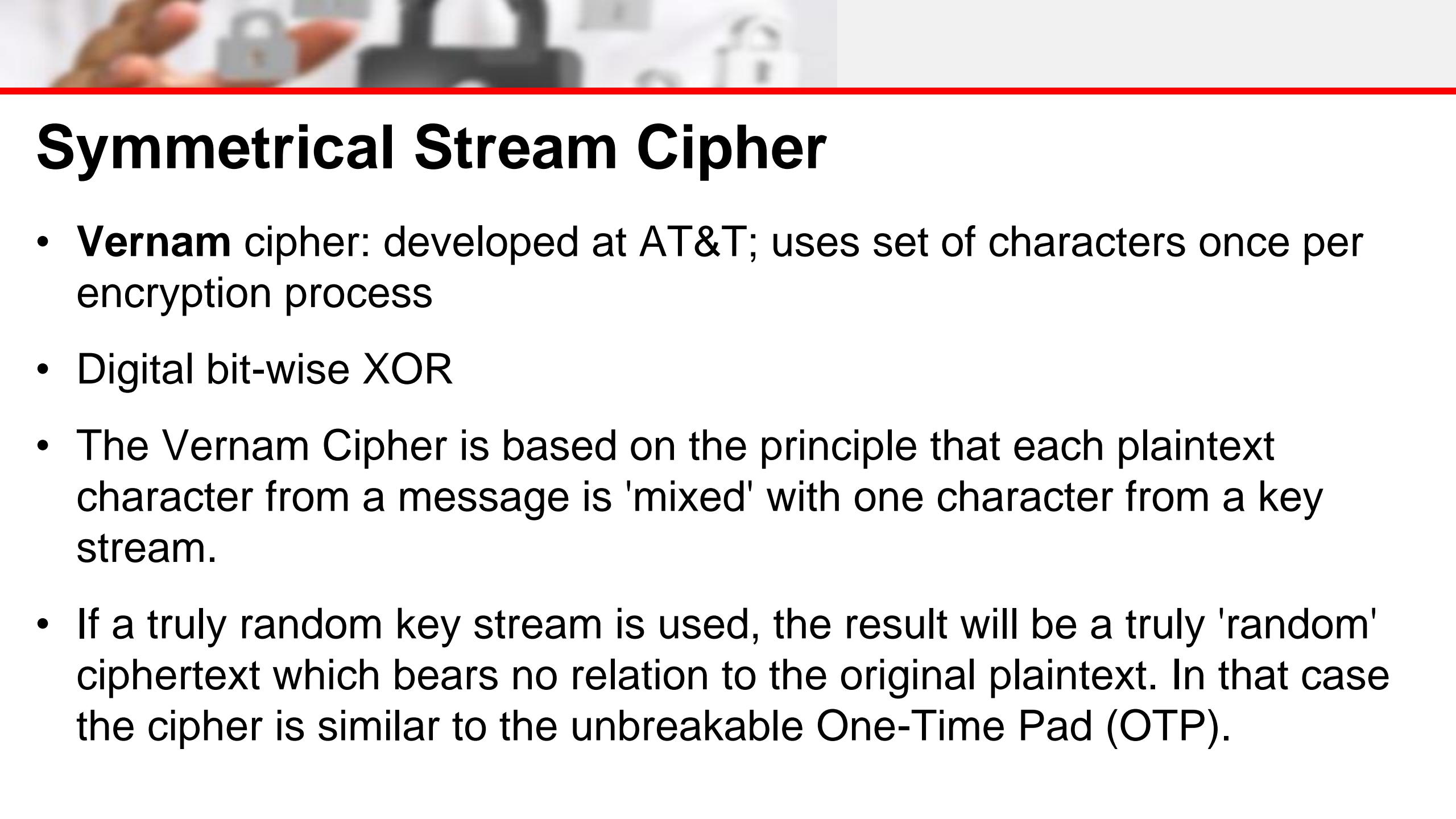
# How to use Transposition Cipher Encryption

1. Look for Alphabetic sequence of the word ZEBRA e.i. A, B, E, R, S Z
2. The result will be...

Z	E	B	R	A	S
m	e	e	t	a	t
t	h	r	e	e	p
m	t	o	d	a	y
a	t	t	h	e	u
s	u	a	l	l	o
c	a	t	i	o	n

Meet at three pm today at the usual location

aeaelo erotat ehttua tedhli tpyuon mtmasc



# Symmetrical Stream Cipher

- **Vernam** cipher: developed at AT&T; uses set of characters once per encryption process
- Digital bit-wise XOR
- The Vernam Cipher is based on the principle that each plaintext character from a message is 'mixed' with one character from a key stream.
- If a truly random key stream is used, the result will be a truly 'random' ciphertext which bears no relation to the original plaintext. In that case the cipher is similar to the unbreakable One-Time Pad (OTP).



# Vernam Cipher Security

- The above procedure is 100% safe if, and only if, the following conditions are all met:
  1. There are only two copies of the key (OTP),
  2. Both sides of the communications link have the same key (OTP),
  3. The key (OTP) is used only once,
  4. The key (OTP) is destroyed immediately after use,
  5. The key (OTP) contains truly random characters,
  6. The equipment is hack proof or uncompromised,
  7. The key (OTP) was not compromised during transport.

# How to use Vernam Cipher Encryption

1. Create a plaintext and group the characters 6 columns, find the value of the text in the alphabet and convert it to binary:

**Meet at three pm today at the usual location**

Plaintext						Plaintext Value in the Alphabet					
meetat	M	e	e	t	a	t		13	5	5	20
threep	t	h	r	e	e	p		20	8	18	5
mtoday	m	t	o	d	a	y		13	20	15	4
attheus	a	t	t	h	e	u		1	20	20	8
suallo	s	u	a	l	l	o		19	21	1	12
cation	c	a	t	i	o	n		3	1	20	9

# How to use Vernam Cipher Encryption

## Binary Value of the plaintext

Plaintext Value in Binary Digits					
00001101	00000101	00000101	00010100	00000001	00010100
00010100	00001000	00010010	00000101	00000101	00010000
00001101	00010100	00001111	00000100	00000001	00011001
00000001	00010100	00010100	00001000	00000101	00010101
00010011	00010101	00000001	00001100	00001100	00001111
00000011	00000001	00010100	00001001	00001111	00001110



# How to use Vernam Cipher Encryption

## Decimal Value of the OTP

Decimal Value of the One Time Pad					
14	25	24	20	7	19
8	6	22	19	14	14
14	14	12	2	2	13
18	3	26	5	24	15
25	9	11	3	18	26
7	6	19	19	25	21



# How to use Vernam Cipher Encryption

- Create a key (One Time Pad)

One Time Pad - Key					
00001110	00011001	00011000	00010100	00000111	00010011
00001000	00000110	00010110	00010011	00001110	00001110
00001110	00001110	00001100	00000010	00000010	00001101
00010010	00000011	00011010	00000101	00011000	00001111
00011001	00001001	00001011	00000011	00010010	00011010
00000111	00000110	00010011	00010011	00011001	00010101

# Binary XOR Operation

The inputs to a binary **XOR** operation can only be **0** or **1** and the result can only be **0** or **1**

The binary **XOR** operation (also known as the binary **XOR** function) will always produce a **1** output if either of its inputs is **1** and will produce a **0** output if both of its inputs are **0** or **1**.

If we call the inputs **A** and **B** and the output **C** we can show the **XOR** function as:

A		B		C
0	<b>XOR</b>	0	->	0
0	<b>XOR</b>	1	->	1
1	<b>XOR</b>	0	->	1
1	<b>XOR</b>	1	->	0

# How to use Vernam Cipher Encryption

- Compute for the Cyphertext using XOR

Result of XOR (Plaintext, OTP) value in Binary digits					
00000011	00011100	00011101	00000000	00000110	00000111
00011100	00001110	00000100	00010110	00001011	00011110
00000011	00011010	00000011	00000110	00000011	00010100
00010011	00010111	00000100	00001101	00011101	00011010
00001010	00011100	00001010	00001111	00011110	00010101
00000100	00000111	00000111	00011010	00010110	00011011

- 00001101
- 00001110
- 00000011 = 3
- 00000101
- 00011001
- 00011100

# How to use Vernam Cipher Encryption

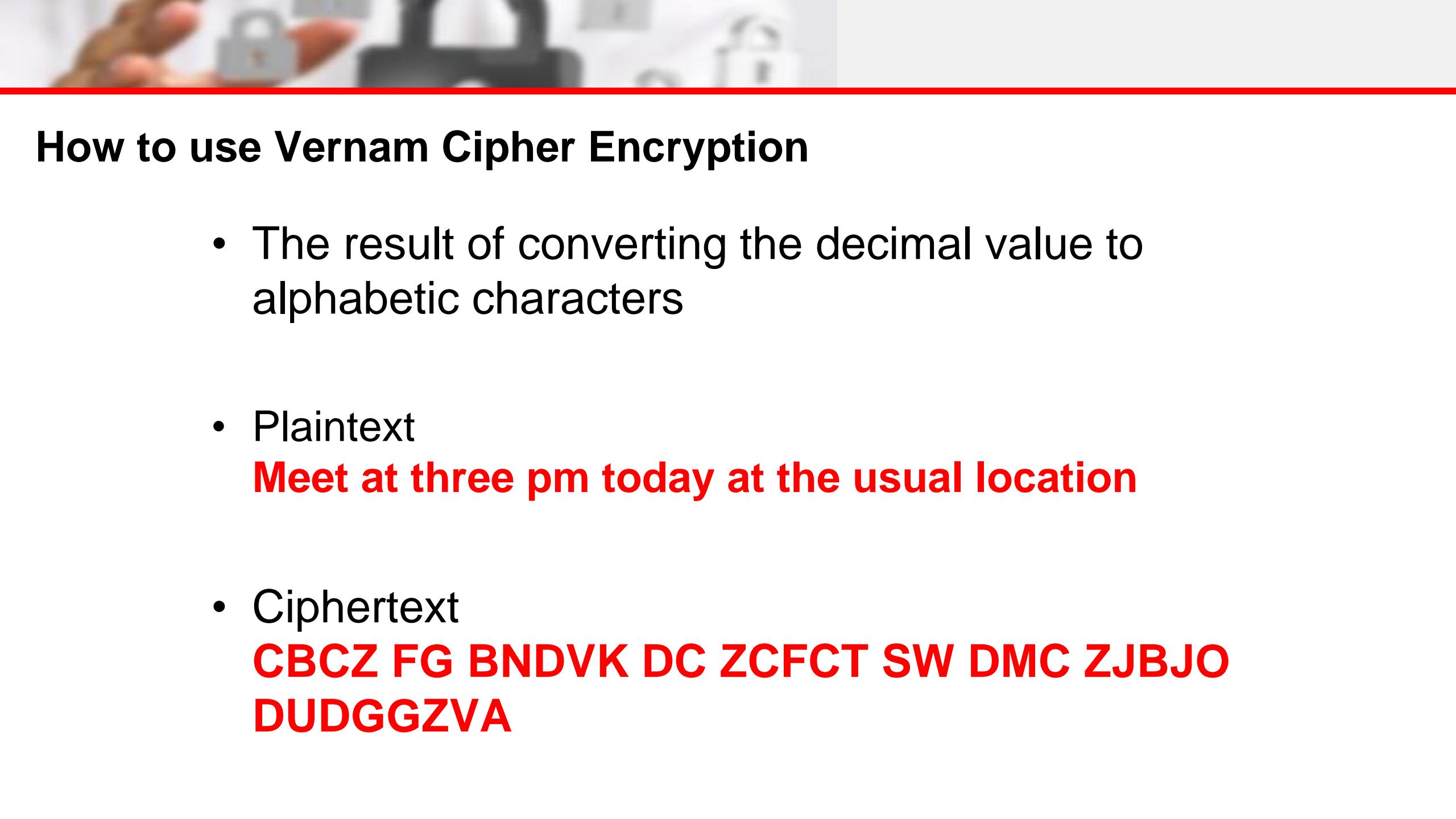
- Convert the binary value into decimal, use the result and look for the value in the alphabet table

Decimal Value of the XOR(Plaintext, OTP)					
3	28	29	0	6	7
28	14	4	22	11	30
3	26	3	6	3	20
19	23	4	13	29	26
10	28	10	15	30	21
4	7	7	26	22	27

# How to use Vernam Cipher Encryption

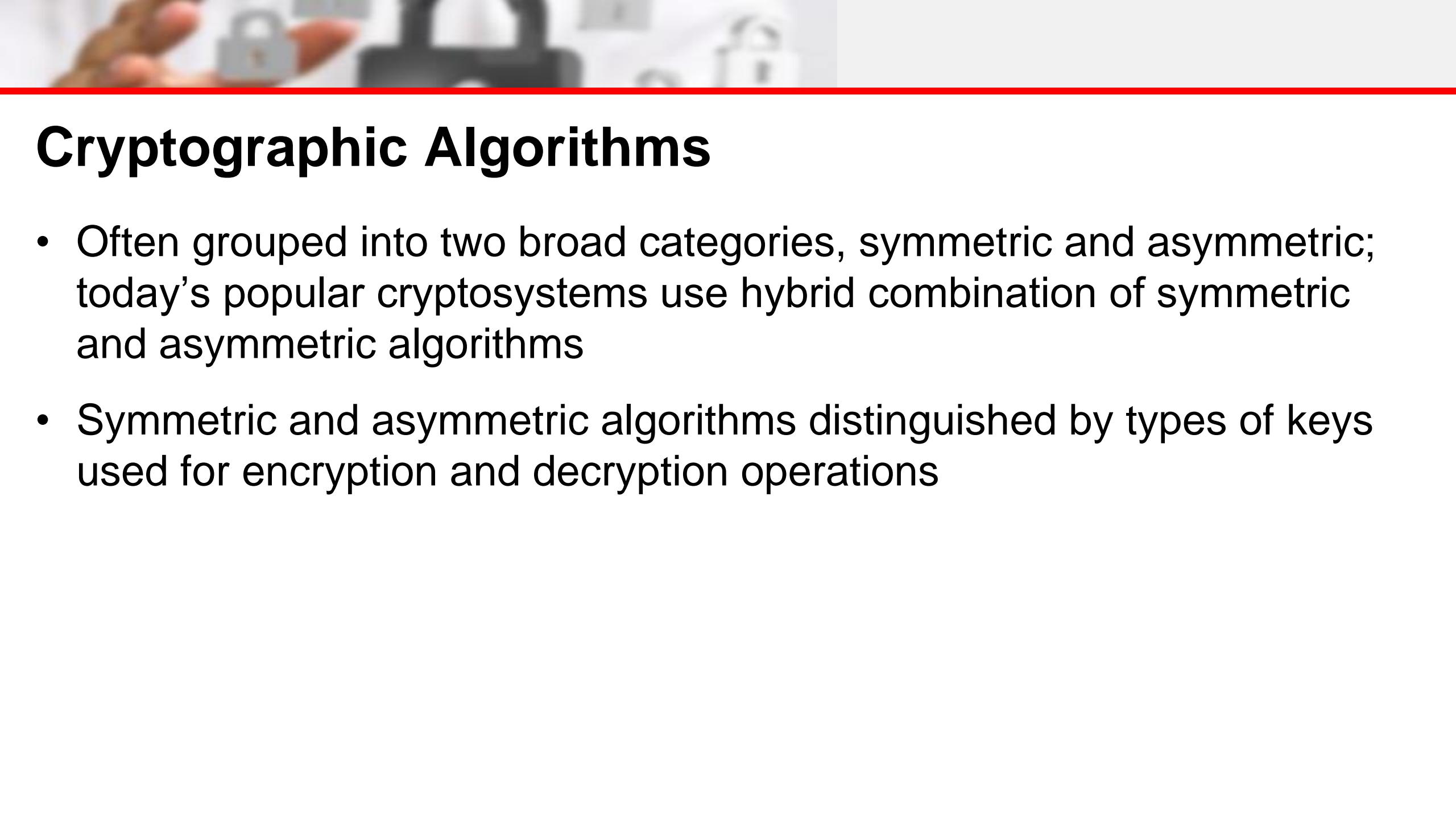
- Convert the binary value into decimal, use the result and look for the value in the alphabet table

Alphabet Value of the XOR Result					
C	B	C	Z	F	G
B	N	D	V	K	D
C	Z	C	F	C	T
S	W	D	M	C	Z
J	B	J	O	D	U
D	G	G	Z	V	A



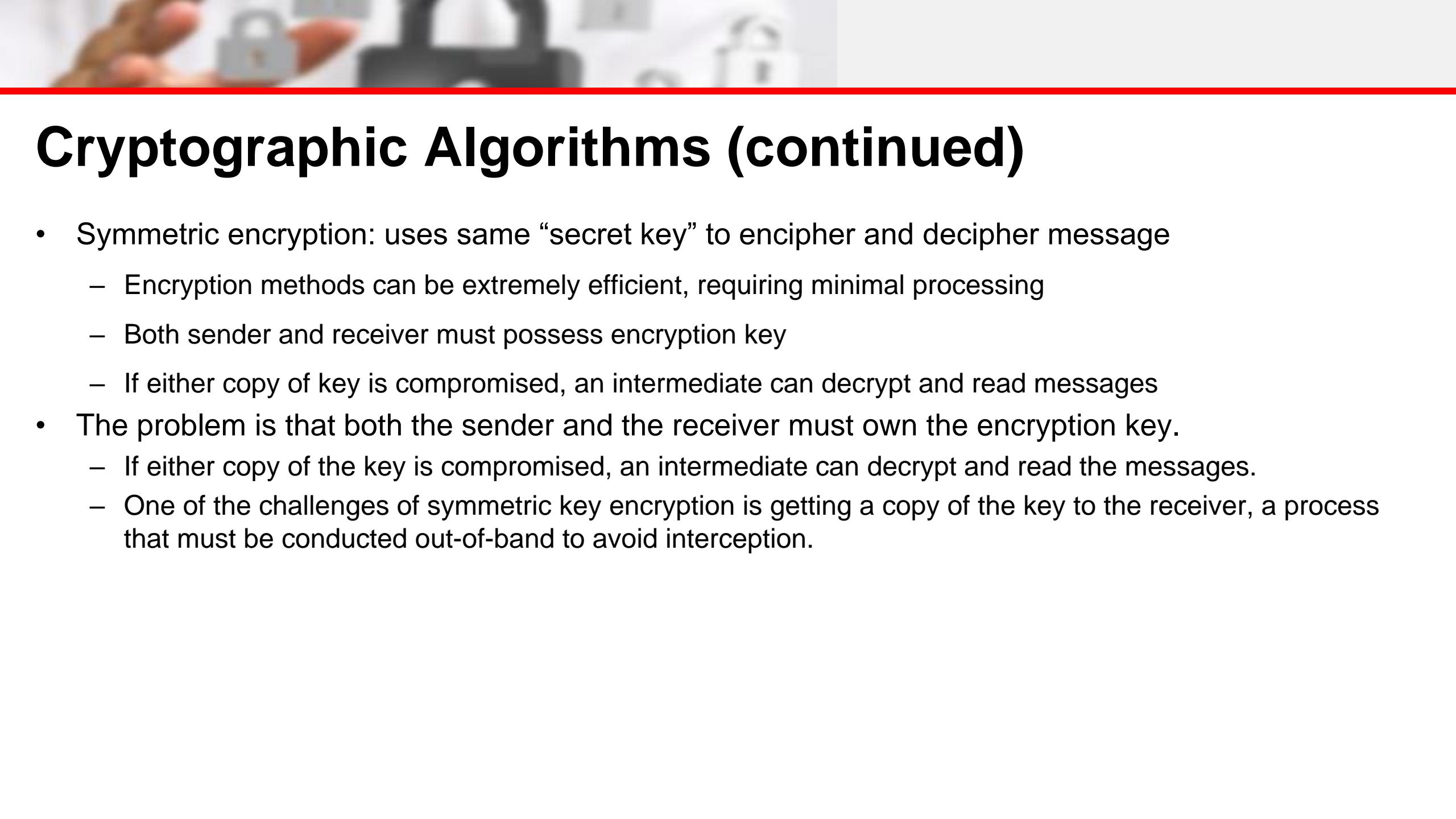
# How to use Vernam Cipher Encryption

- The result of converting the decimal value to alphabetic characters
- Plaintext  
**Meet at three pm today at the usual location**
- Ciphertext  
**CBCZ FG BNDVK DC ZCFCT SW DMC ZJBJO  
DUDGGZVA**



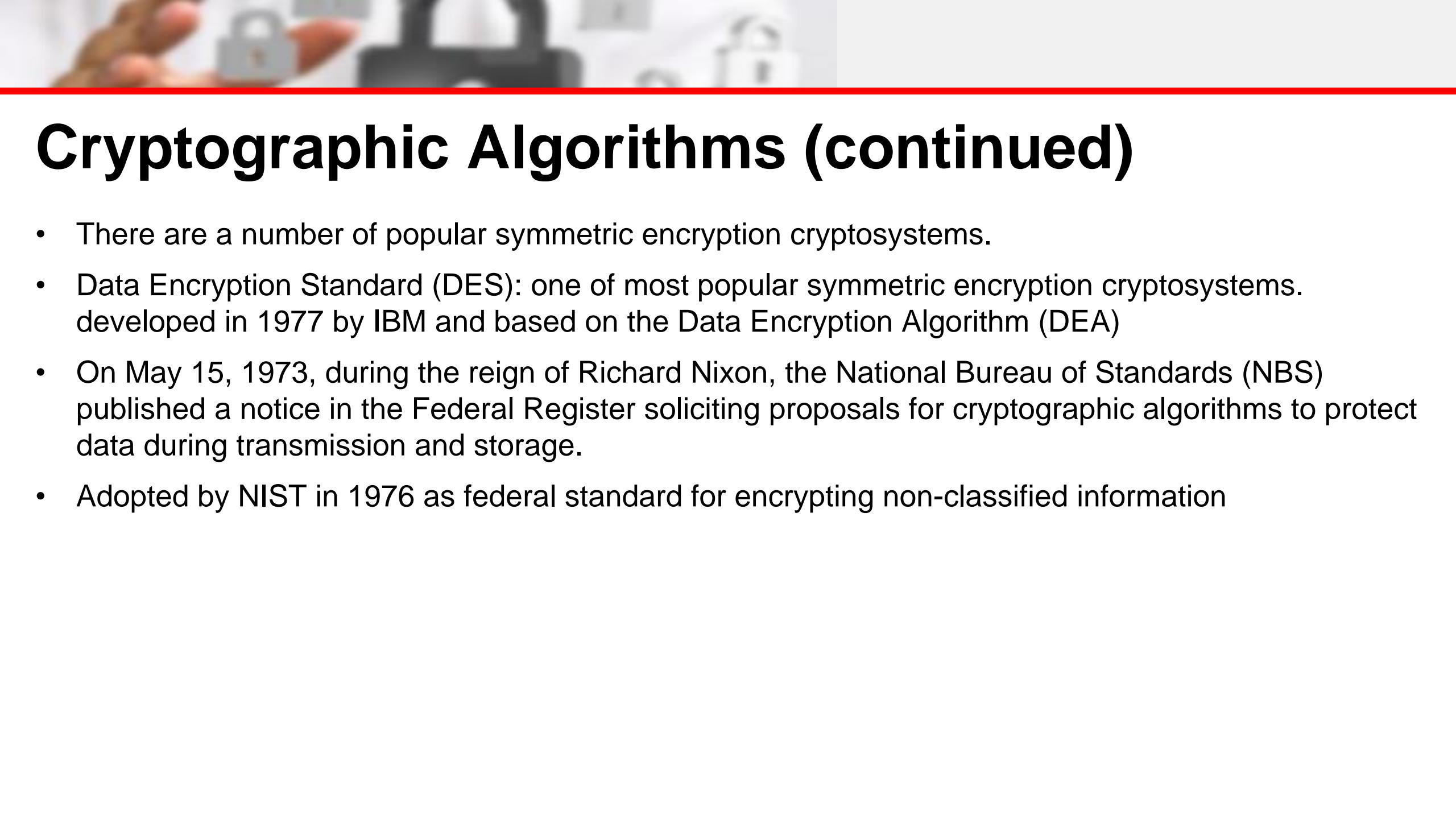
# Cryptographic Algorithms

- Often grouped into two broad categories, symmetric and asymmetric; today's popular cryptosystems use hybrid combination of symmetric and asymmetric algorithms
- Symmetric and asymmetric algorithms distinguished by types of keys used for encryption and decryption operations



# Cryptographic Algorithms (continued)

- Symmetric encryption: uses same “secret key” to encipher and decipher message
  - Encryption methods can be extremely efficient, requiring minimal processing
  - Both sender and receiver must possess encryption key
  - If either copy of key is compromised, an intermediate can decrypt and read messages
- The problem is that both the sender and the receiver must own the encryption key.
  - If either copy of the key is compromised, an intermediate can decrypt and read the messages.
  - One of the challenges of symmetric key encryption is getting a copy of the key to the receiver, a process that must be conducted out-of-band to avoid interception.



# Cryptographic Algorithms (continued)

- There are a number of popular symmetric encryption cryptosystems.
- Data Encryption Standard (DES): one of most popular symmetric encryption cryptosystems. developed in 1977 by IBM and based on the Data Encryption Algorithm (DEA)
- On May 15, 1973, during the reign of Richard Nixon, the National Bureau of Standards (NBS) published a notice in the Federal Register soliciting proposals for cryptographic algorithms to protect data during transmission and storage.
- Adopted by NIST in 1976 as federal standard for encrypting non-classified information



# Cryptographic Algorithms (continued)

- DEA uses a 64-bit block size and a 56-bit key. The algorithm begins by adding parity bits to the key (resulting in 64 bits) and then applies the key in 16 rounds of XOR, substitution, and transposition operations.
- With a 56 bit key, the algorithm has 256 possible keys to choose from (over 72 quadrillion).
- DES was cracked in 1997 when Rivest-Shamir-Aldeman (RSA) put a bounty on the algorithm.



# DES Encryption

- This is the encrypted form of
- $M = 0123456789ABCDEF$
- $C = 85E813540F0AB405$

# How DES Work?

1. Step 1: Create 16 subkeys, each of which is 48-bits long. Create a key.

**K = 133457799BCDFF1**

2. Convert the key into Binary (ASCII → Hex → Binary)

00010011 00110100 01010111 01111001 10011011 10111100 11011111 11110001

3. Create blocks of 64 bits

8 Bits								8 Bits								8 Bits								8 Bits							
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	0	1	0	0	1	1	0	0	1	1	0	1	0	0	0	1	0	1	0	1	1	1	0	1	1	1	1	0	0	1
8 Bits								8 Bits								8 Bits								8 Bits							
32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
1	0	0	1	1	0	1	1	1	0	1	1	1	1	0	0	1	1	0	1	1	1	1	1	1	1	1	1	0	0	0	1

# How DES Work?

- a. Change the order using the permutation table –  
these is a randomly generated numbers from 0 - 55

PC – 1 (56 bits)						
57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

# How DES Work?

b. Result after changing the order of the original text using the random permutation table

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
57	49	41	33	25	17	9	1	58	50	42	34	26	18	10	2	59	51	43	35	27	19	11	3	60	52	44	36	63
1	1	0	0	1	1	0	0	1	0	1	0	1	0	1	0	1	1	1	1	1	1	1	1	0	1	1	1	1

29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55
55	47	39	31	23	15	7	62	54	46	38	30	22	14	6	61	53	45	37	29	21	13	5	28	20	12	4
1	0	1	1	1	0	1	0	1	0	1	0	1	0	1	0	1	1	0	0	1	1	0	1	0	0	0

# How DES Work?

- c. Next, split this key into left and right halves, L0 and R0, where each half has 28 bits.

L0	1	1	1	1	0	0	0	0	1	1	0	0	1	1	0	0	1	0	1	0	1	0	1	0	1	1	1	1
R0	0	1	0	1	0	1	0	1	0	1	1	0	0	1	1	0	0	1	1	1	1	1	0	0	0	1	1	1

# How DES Work?

- d. With L<sub>0</sub> and R<sub>0</sub> Refined, we now to create sixteen blocks L<sub>n</sub> and R<sub>n</sub>,  $1 \leq n \leq 16$ . Each pair of blocks L<sub>n</sub> and R<sub>n</sub> is formed from the previous pair L<sub>n-1</sub> and R<sub>n-1</sub>, respectively, for  $n = 1, 2, \dots, 16$

Iteration Number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Number of Left Shifts	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

# How DES Work?

**Example:** From original pair,  $L_0$  and  $R_0$  we obtain:

$$L_0 = 1111000011001100101010101111$$
$$R_0 = 0101010101100110011110001111$$
$$L_0 = \textcolor{red}{1}111000011001100101010101111$$
$$R_0 = \textcolor{green}{0}101010101100110011110001111$$

# How DES Work?

**Example:** From original pair,  $L_0$  and  $R_0$  we obtain:

$L_0 = \textcolor{red}{1}11100001100110010101010111$

$R_0 = \textcolor{green}{0}10101010110011001111000111$

# How DES Work?

**Example:** From original pair,  $L_0$  and  $R_0$  we obtain:

$L_1 = 111000011001100101010101111\textcolor{red}{1}$

$R_1 = 101010101100110011110001111\textcolor{green}{0}$

# How DES Work?

**Example:** Output from the shifted pair  $L_o$  and  $R_o$  we obtain:

$L_1 = 1110000110011001010101011111$

$R_1 = 1010101011001100111100011110$

# How DES Work?

**Example:** From shifted pair,  $L_1$  and  $R_1$ , we obtain  
 $L_2$  and  $R_2$

$L_1 = 1110000110011001010101011111$

$R_1 = 1010101011001100111100011110$

# How DES Work?

**Example:** From original pair,  $L_0$  and  $R_0$  we obtain:

$L_2 = 11000011001100101010101111\textcolor{red}{11}$

$R_2 = 01010101100110011110001111\textcolor{green}{01}$

# How DES Work?

**Example:** From original pair,  $L_0$  and  $R_0$  we obtain:

$$L_2 = 110000110011001010101011111$$

$$R_2 = 0101010110011001111000111101$$

# How DES Work?

**Example:** From original pair,  $L_0$  and  $R_0$  we obtain  $L_1$  and  $R_1$  and  $L_2$  and  $R_2$ , using 1 shift

$L_0 = 1111000011001100101010101111$

$R_0 = 0101010101100110011110001111$

$L_1 = 1110000110011001010101011111$

$R_1 = 1010101011001100111100011110$

$L_2 = 1100001100110010101010111111$

$R_2 = 0101010110011001111000111101$

# How DES Work?

Basing on the shifting table, L3 and R3 are obtained from L2 and R2, respectively, by **two left shifts**, and L16 and R16 are obtained from L15 and R15, respectively, by one left shift.

In all cases, by a single left shift is meant a rotation of the bits one place to the left, so that after one left shift the bits in the 28 positions are the bits that were previously in positions 2, 3,..., 28, 1.

# How DES Work?

**Example:** From shifted pair,  $L_2$  and  $R_2$  we obtain:

$$L_2 = 110000110011001010101011111$$

$$R_2 = 0101010110011001111000111101$$

# How DES Work?

**Example:** From shifted pair,  $L_2$  and  $R_2$  we obtain:

$L_2 = 1110000110011001010101011111$

$R_2 = 0101010110011001111000111101$

# How DES Work?

**Example:** From shifted pair,  $L_2$  and  $R_2$  we obtain:

$$L_3 = 00001100110010101010111111$$
$$R_3 = 0101011001100111100011110101$$

# How DES Work?

**Example:** From shifted pair,  $L_2$  and  $R_2$  we obtain:

$$L_3 = 000011001100101010101111111$$

$$R_3 = 0101011001100111100011110101$$

# How DES Work?

**Example:** From shifted pair,  $L_3$  and  $R_3$  we obtain:

$L_3 = 00001100110010101010111111$

$R_3 = 01010110011001110001110101$

# How DES Work?

**Example:** From shifted pair,  $L_3$  and  $R_3$  we obtain:

$$L_4 = 001100110010101010111111100$$

$$R_4 = 0101100110011110001111010101$$

# How DES Work?

***This will go on until it satisfies the switch table***

Iteration Number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Number of Left Shifts	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

# How DES Work?

$$L_5 = 11001100101010101111110000$$
$$R_5 = 0110011001111000111101010101$$
$$L_6 = 001100101010111111000011$$
$$R_6 = 1001100111100011110101010101$$
$$L_7 = 110010101011111100001100$$
$$R_7 = 01100111100011110101010110$$
$$L_8 = 00101010101111110000110011$$
$$R_8 = 1001111000111101010101011001$$



# How DES Work?

***L<sub>9</sub> and L<sub>9</sub> Goes back to 1 - shift***

$L_9 = 010101010111111100001100110$

$R_9 = 0011110001111010101010110011$

***L<sub>10</sub> and L<sub>10</sub> goes back again to 2 - shifts***

$L_{10} = 0101011111110000110011001$

$R_{10} = 1111000111101010101011001100$

# How DES Work?

$$L_{12} = 01011111100001100110010101$$
$$R_{12} = 00011110101010110011001111$$
$$L_{13} = 011111110000110011001010101$$
$$R_{13} = 01111010101011001100111100$$
$$L_{14} = 1111111000011001100101010101$$
$$R_{14} = 11101010101100110011110001$$
$$L_{15} = 1111100001100110010101010111$$
$$R_{15} = 1010101010110011001111000111$$



# How DES Work?

**$L_{16}$  and  $L_{16}$  goes back again to 1 - shift**

$L_{16} = 1111000011001100101010101111$

$R_{16} = 0101010101100110011110001111$

# How DES Work?

1. Create a Key of 48 bits by performing DES Algorithm
  - a. Change the order using the permutation table – PC 2, a randomly generated numbers from 0 - 47
  - We now form the keys  $K_n$ , for  $1 \leq n \leq 16$ , by applying the following permutation table to each of the concatenated pairs  $L_n R_n$ . Each pair has 56 bits, but PC-2 only uses 48 of these.

# How DES Work?

Create a Key of 48 bits

PC – 2 (48 bit)					
14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

The first bit of  $K_n$  is the 14th bit of  $L_nR_n$ , the second bit the 17th, and so on, ending with the 48th bit of  $K_n$  being the 32th bit of  $L_nR_n$ .

# How DES Work?

- Use 48 bit permutation for  $L_1$  and  $R_1$ ,

$L_1 = 1110000110011001010101011111$

$R_1 = 1010101011001100111100011110$

**L1R1 is equals to...**

1110000 1100110 0101010 1011111 1010101 0110011 0011110 0011110

***Result for 48-bit permutation K1***

$K_1 = 000110 110000 001011 101111 111111 000111 000001 110010$

How? refer to the table for conversion

# Permutation Table using 48-bit

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
14	17	11	24	1	5	3	28	15	6	21	10	23	19	12	4	26	8	16	7	27	20	13	2	41
0	0	0	1	1	0	1	1	0	0	0	0	0	0	1	0	1	1	1	0	1	1	1	1	1
25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47		
52	31	37	47	55	30	40	51	45	33	48	44	49	39	56	34	53	46	42	50	36	29	32		
1	1	1	1	0	0	0	0	1	1	1	0	0	0	0	0	1	1	1	0	0	1	0		

***Thus the result...***

$$K_1 = 000110\ 110000\ 001011\ 101111\ 111111\ 000111\ 000001\ 110010$$

# How DES Work?

- Use 48 bit permutation for  $L_1$  and  $R_1$

**L2R2 is equals to...**

110000110011001010101011111010101011001100111000111101

**L3R3 is equals to...**

0000110011001010101011111101010110011001110001110101

***Result for 48-bit permutation K2 and K3***

$K_2 = 011110\ 011010\ 111011\ 011001\ 110110\ 111100\ 100111\ 100101$

$K_3 = 010101\ 011111\ 110010\ 001010\ 010000\ 101100\ 111110\ 011001$

# Permutation Table using 48-bit

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
14	17	11	24	1	5	3	28	15	6	21	10	23	19	12	4	26	8	16	7	27	20	13	2	41
0	1	1	1	1	0	0	1	1	0	1	0	1	1	1	0	1	1	0	1	1	0	0	1	1
0	1	0	1	0	1	0	1	1	1	1	1	1	1	0	0	1	0	0	0	1	0	1	0	0

25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	
52	31	37	47	55	30	40	51	45	33	48	44	49	39	56	34	53	46	42	50	36	29	32	
1	0	1	1	1	1	1	1	1	1	0	0	1	0	0	1	1	1	1	0	0	1	0	1
1	0	0	0	1	1	0	1	1	0	0	1	1	1	1	1	0	0	1	1	0	0	1	

***Thus the result...***

$$K_2 = 011110\ 011010\ 111011\ 011001\ 110110\ 111100\ 100111\ 100101$$

$$K_3 = 010101\ 011111\ 110010\ 001010\ 010000\ 101100\ 111110\ 011001$$

# Permutation Table using 48-bit

$K_4 = 011100\ 101010\ 110111\ 010110\ 110110\ 110011\ 010100\ 011101$

$K_5 = 011111\ 001110\ 110000\ 000111\ 111010\ 110101\ 001110\ 101000$

$K_6 = 011000\ 111010\ 010100\ 111110\ 010100\ 000111\ 101100\ 101111$

$K_7 = 111011\ 001000\ 010010\ 110111\ 111101\ 100001\ 100010\ 111100$

$K_8 = 111101\ 111000\ 101000\ 111010\ 110000\ 010011\ 101111\ 111011$

$K_9 = 111000\ 001101\ 101111\ 101011\ 111011\ 011110\ 011110\ 000001$

$K_{10} = 101100\ 011111\ 001101\ 000111\ 101110\ 100100\ 011001\ 001111$

$K_{11} = 001000\ 010101\ 111111\ 010011\ 110111\ 101101\ 001110\ 000110$

$K_{12} = 011101\ 010111\ 000111\ 110101\ 100101\ 000110\ 011111\ 101001$

$K_{13} = 100101\ 111100\ 010111\ 010001\ 111110\ 101011\ 101001\ 000001$

$K_{14} = 010111\ 110100\ 001110\ 110111\ 111100\ 101110\ 011100\ 111010$

$K_{15} = 101111\ 111001\ 000110\ 001101\ 001111\ 010011\ 111100\ 001010$

$K_{16} = 110010\ 110011\ 110110\ 001011\ 000011\ 100001\ 011111\ 110101$

# Summary of Step 1

1. Created 16 subkeys, each of which is 48-bits long.
  - a. We created a KEY
  - b. Convert the key into binary of 64 bit long
  - c. We permuted or changed the order of the 64 bit binary digit using the **PC-1 table**
  - d. We shifted the binary according to the shift table
  - e. We permuted the shifted key on a 48 bit long key **PC-2 table.**

## Step 2: Encode each 64-bit block of data.

1. Create a 64 bits of the message data **M**
  - **M** = 0123456789ABCDEF
  - **M** = 0000 0001 0010 0011 0100 0101 0110 0111 1000 1001 1010  
1011 1100 1101 1110 1111
2. Use an *initial permutation (IP)* of the 64 bits of the message data. (use IP table)
3. Perform permutation similar to 56 bit and 48 bit permutation.

# 64-bit long message in binary

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
0	0	0	0	0	0	0	1	0	0	1	0	0	0	1	1	0

18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33
1	0	0	0	1	0	1	0	1	1	0	0	1	1	1	1

34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49
0	0	0	1	0	0	1	1	0	1	0	1	0	1	1	1

50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	
1	0	0	1	1	0	1	1	1	1	0	1	1	1	1	1

## Step 2: Encode each 64-bit block of data.

Initial Permutation (IP)							
58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

# Permutated Message in IP 64-bit table

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
58	50	42	34	26	18	10	2	60	52	44	36	28	20	12	4	62
1	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	1

17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
54	46	38	30	22	14	6	64	56	48	40	32	24	16	8	57
1	0	0	1	1	0	0	1	1	1	1	1	1	1	1	1

33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
49	41	33	25	17	9	1	59	51	43	35	27	19	11	3	61
1	1	1	0	0	0	0	1	0	1	0	1	0	1	0	1

49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
53	45	37	29	21	13	5	63	55	47	39	31	23	15	7
1	1	1	0	0	0	0	1	0	1	0	1	0	1	0

# Permutated Message in IP 64-bit table

- $M = 0000 \text{ } 0001 \text{ } 0010 \text{ } 0011 \text{ } 0100 \text{ } 0101 \text{ } 0110 \text{ } 0111 \text{ } 1000 \text{ } 1001$   
 $1010 \text{ } 1011 \text{ } 1100 \text{ } 1101 \text{ } 1110 \text{ } 1111$
- $IP = 1100 \text{ } 1100 \text{ } 0000 \text{ } 0000 \text{ } 1100 \text{ } 1100 \text{ } 1111 \text{ } 1111 \text{ } 1111 \text{ } 0000$   
 $1010 \text{ } 1010 \text{ } 1111 \text{ } 0000 \text{ } 1010 \text{ } 1010$

## Step 2: Continuation

- Next divide the permuted block **IP** into a left half  $L_0$  of 32 bits, and a right half  $R_0$  of 32 bits.
- $L_0 = 1100\ 1100\ 0000\ 0000\ 1100\ 1100\ 1111\ 1111$
- $R_0 = 1111\ 0000\ 1010\ 1010\ 1111\ 0000\ 1010\ 1010$

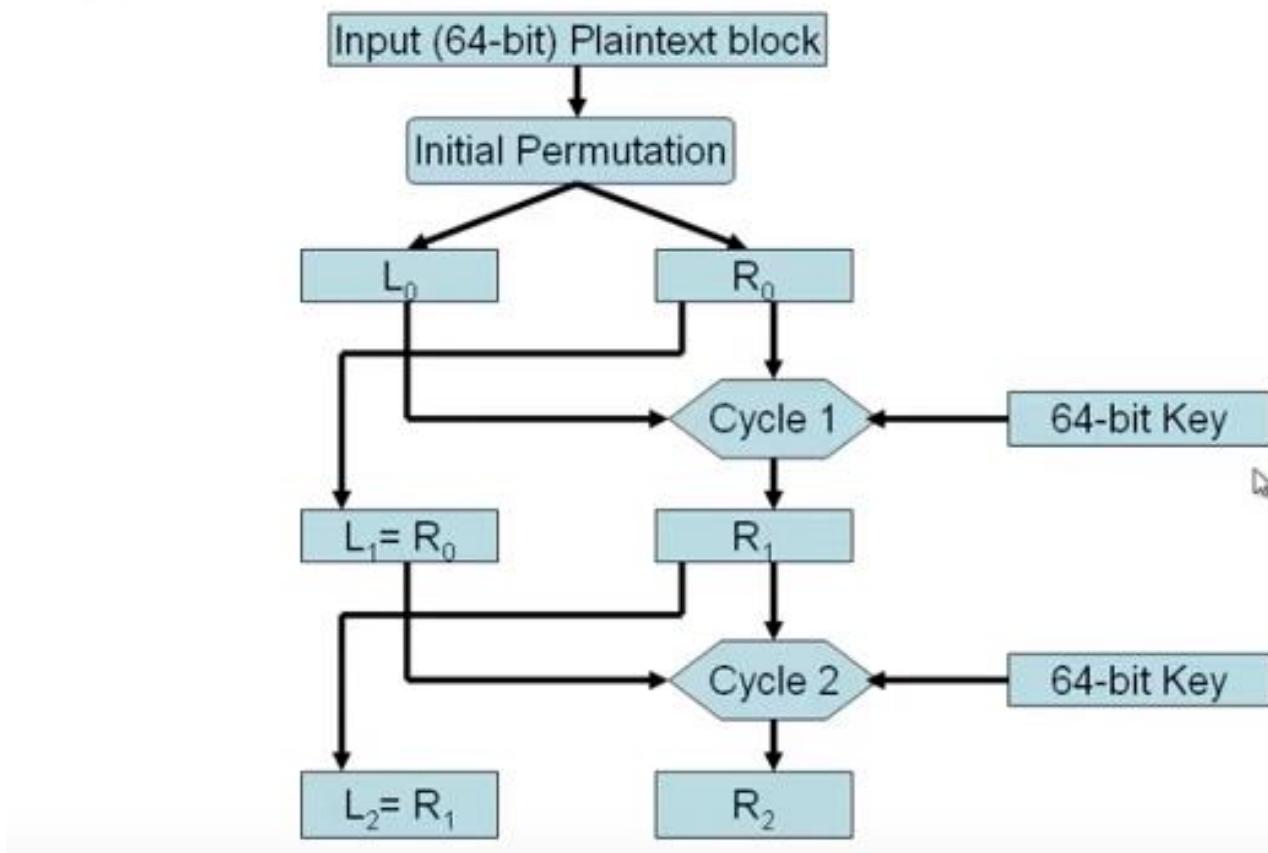
## Step 2: Continuation

- We now proceed through 16 iterations, for  $1 \leq n \leq 16$ , using a function  $f$  which operates on two blocks--a data block of 32 bits and a key  $K_n$  of 48 bits--to produce a block of 32 bits.
- **Let + denote XOR addition, (bit-by-bit addition modulo 2).** Then for  $n$  going from 1 to 16 we calculate

$$\begin{aligned}L_n &= R_{n-1} \\R_n &= L_{n-1} + f(R_{n-1}, K_n)\end{aligned}$$

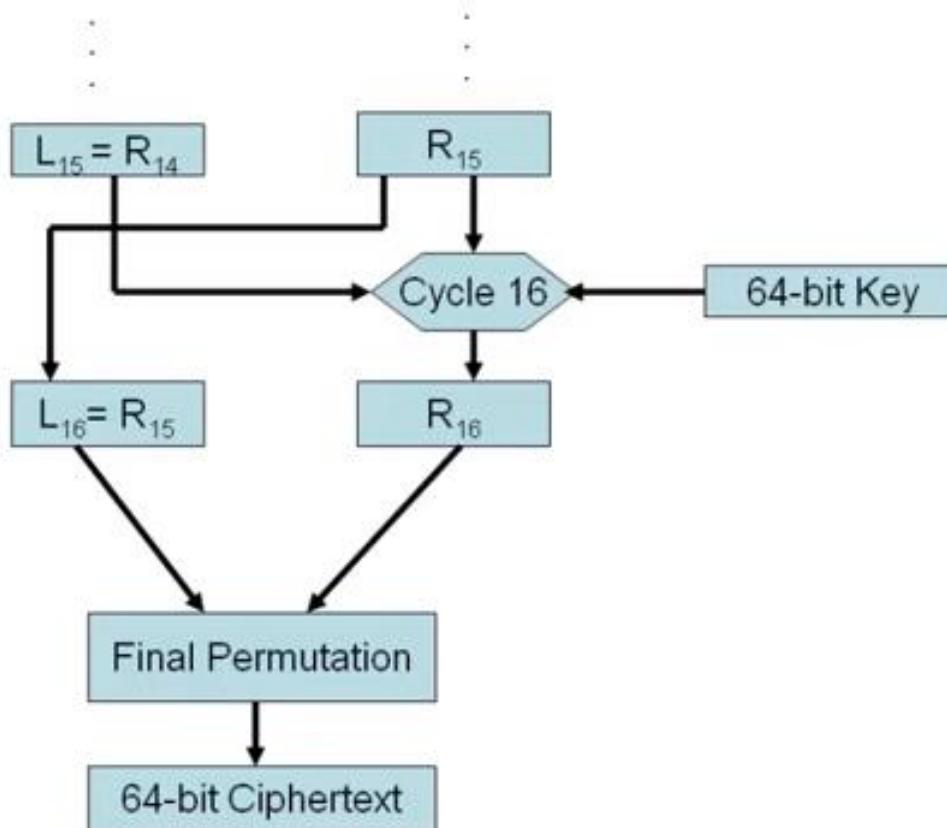
# Step 2: Continuation

## Cycles of Substitution and Permutation



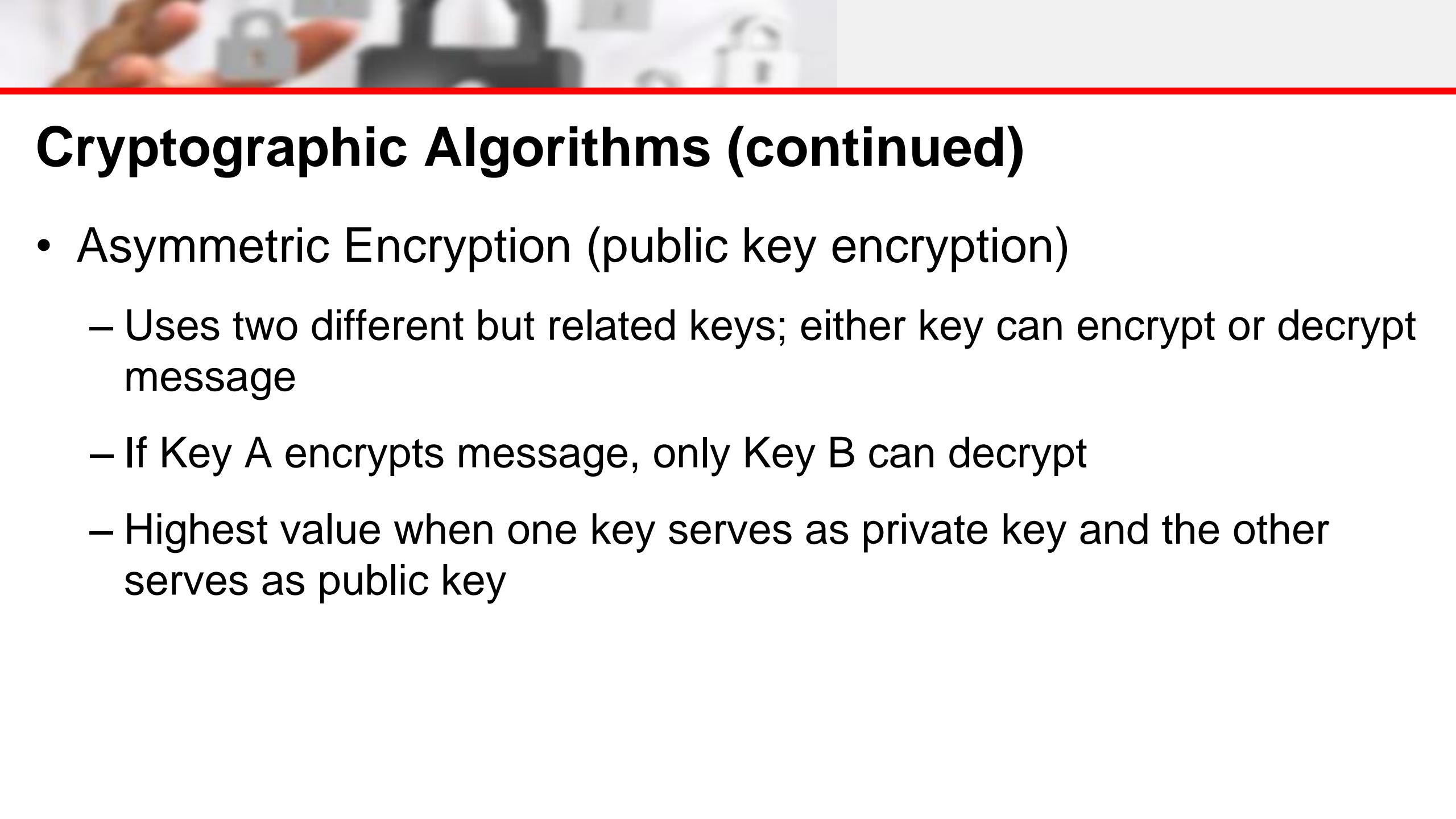
# Step 2: Continuation

## Cycles of Substitution and Permutation



# Final Output

- This is the encrypted form of
- **M** = 0123456789ABCDEF
- **C** = 85E813540F0AB405
- Rivest-Shamir-Aldeman (Cracked DES)



# Cryptographic Algorithms (continued)

- Asymmetric Encryption (public key encryption)
  - Uses two different but related keys; either key can encrypt or decrypt message
  - If Key A encrypts message, only Key B can decrypt
  - Highest value when one key serves as private key and the other serves as public key



# Examples of Asymmetric Encryption

- Examples of **asymmetric encryption or public key encryption** are **DSA, RSA and PGP**.
- **RSA** is an algorithm used by modern computers to encrypt and decrypt messages. It is an asymmetric cryptographic algorithm. Asymmetric means that there are two different keys. This is also called *public key cryptography*, because one of them can be given to everyone.
- The other key must be kept private. It is based on the fact that finding the factors of an integer is hard (the factoring problem).



# Examples of Asymmetric Encryption

- RSA stands for Ron **Rivest**, Adi **Shamir** and Leonard **Adleman**, who first publicly described it in 1978.
- A user of RSA creates and then publishes the product of two large prime numbers, along with an auxiliary value, as their public key.
- The prime factors must be kept secret. Anyone can use the public key to encrypt a message, but with currently published methods, if the public key is large enough, only someone with knowledge of the prime factors can feasibly decode the message.
- Using the acoustic cryptanalysis, carried out by Daniel Genkin, Adi Shamir (who co-invented RSA), and Eran Tromer, uses what's known as a *side channel attack*.

# How does RSA Work?

- **Step 1** – Choose two prime numbers, Prime1 and Prime2
- Prime1 and Prime2 should be very large prime numbers, at minimum 100 digits long but as larger is more secure and less efficient.
- Prime 1 and Prime2 should not be the same prime number

```
2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47,  
53, 59, 61, 67, 71, 73, 79, 83, 89, 97;
```

- $p = \text{prime 1}$ ;  $q = \text{prime 2}$ ;  $n = p \times q$

# How does RSA Work?

- **Step 1 – Choose two prime numbers, Prime1 and Prime2**

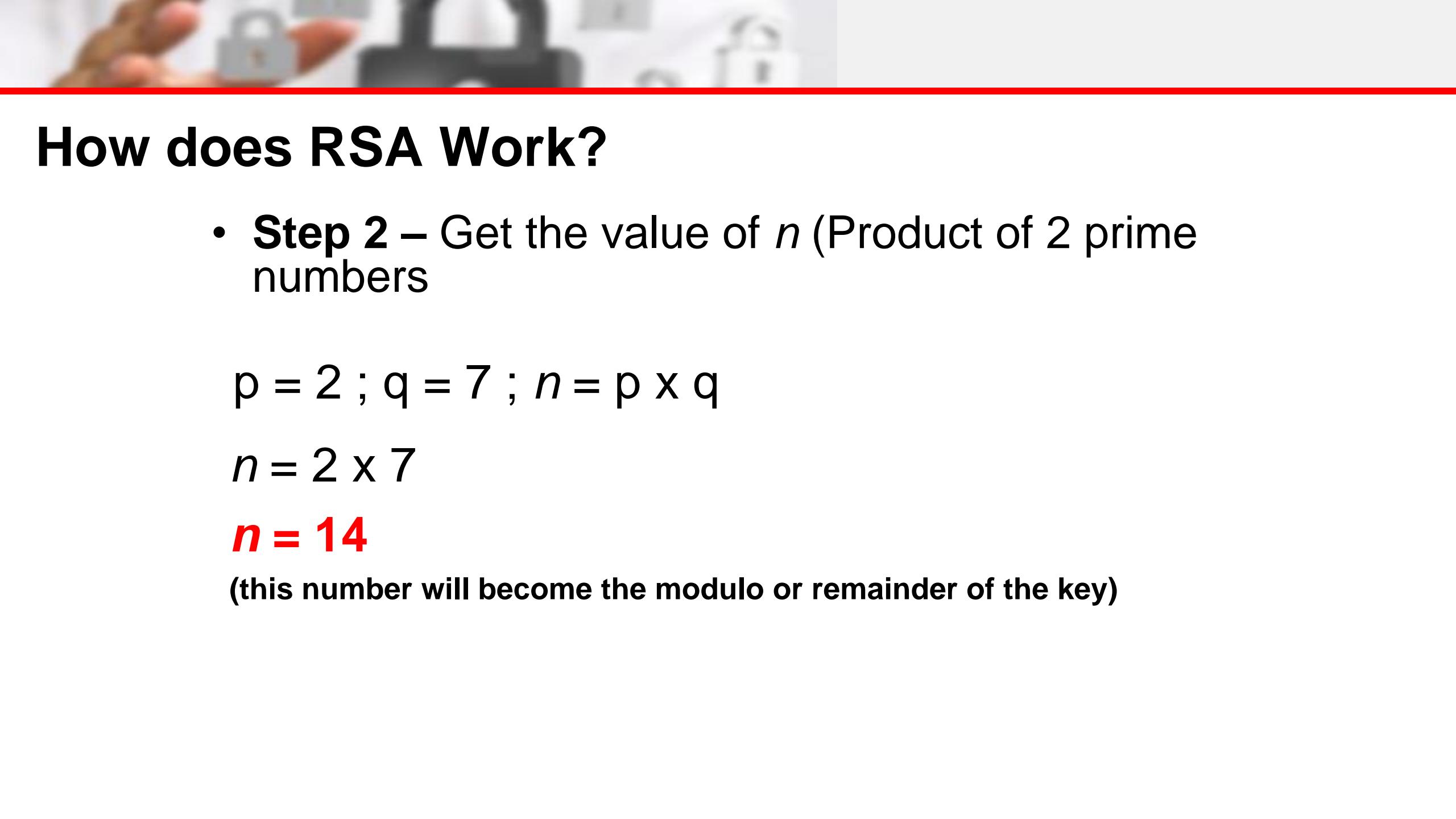
```
2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47,  
53, 59, 61, 67, 71, 73, 79, 83, 89, 97;
```

$$p = 2 ; q = 7 ; n = p \times q$$

$$n = 2 \times 7$$

$$\text{n = 14}$$

(this number will become the modulo or remainder of the key)



# How does RSA Work?

- **Step 2 –** Get the value of  $n$  (Product of 2 prime numbers)

$$p = 2 ; q = 7 ; n = p \times q$$

$$n = 2 \times 7$$

**$n = 14$**

(this number will become the modulo or remainder of the key)

# How does RSA Work?

## Step 3 – Find the Totient of ProductOfPrimes

- Totient - The **totient** function , also called Euler's **totient** function, is defined as the number of positive integers that are relatively prime to (i.e., do not contain any factor in common with) , where 1 is counted as being relatively prime to all numbers.
- Represented with the symbol  $\Phi$  (Phi)
- $\text{Totient} = \Phi N$

# How does RSA Work?

## Step 3 – Find the Totient of ProductOfPrimes

- Get the Totient =  $\phi(14)$
- $\Phi$  – Phi
- Look for the numbers that has a common factor of 1 – 14, and 2 and 7
- Cross out the numbers

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14

# How does RSA Work?

## Step 3 – Find the Totient of ProductOfPrimes

- Cross out the numbers that has a common factor of 1 – 14, and 2 and 7, except 1. 1  
3  
5  
7  
9  
11  
13
- Remove all even numbers because it has factors of 14, and similar factors of 2 and 7 1  
3  
5  
7  
9  
11  
13

# How does RSA Work?

## Step 3 – Find the Totient of ProductOfPrimes

- Cross out the numbers that has a common factor of 1 – 14, and 2 and 7      1
- Remove 7      3
- That leaves 1, 3, 5, 9, 11, 13 (6 remaining numbers)      5
- They are called **co-prime** with 14, since they share no common factors with 14.      9  
11
- **Totient =  $\Phi N = 6$**       13



# How does RSA Work?

## Step 3 – Find the Totient of ProductOfPrimes

- Totient =  $\varphi(\text{ProductOfPrimes})$
- $\Phi$  – Phi
- Totient =  $\Phi(14)$
- Totient =  $(\text{Prime1} - 1) * (\text{Prime2} - 1)$
- Totient =  $(2-1) * (7-1)$
- Totient =  $(1) * (6)$
- **Totient =  $\Phi N = 6$**



# How does RSA Work?

## Step 4 – Choose a number for e (*Encryption key*)

e – stands for Encryption key and should obey the following rules:

- Should be  $1 < e < \Phi N$
- Should be co-prime with N and  $\Phi N$
- $1 < e < \Phi N = \{ 2, 3, 4, 5 \}$
- co-prime with N and  $\Phi N = 5$
- {2,3 4} are factors of 14 and 6 while 5 is not

**e = 5** ; encryption key or the lock key<sub>e</sub>(5,14)

# How does RSA Work?

## Step 5 – Choose a number for $d$ (*decryption*)

$d$  – stands for Decryption and should obey the following rule

$$d = de \pmod{\Phi N} = 1$$

$$d = 5d \pmod{6} = 1$$

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
5	4	3	2	1	0	5	4	3	2	1	0	5	4	3	2	1	0	5



$$\mathbf{d = 11 ; key_d(11,14)}$$

# Encrypting and Decrypting RSA

1. Create a message:

Meet at three pm

2. Convert the message into its numeric value – using the alphabet table, the following numeric value is identified

m	e	e	t	a	t	t	h	r	e	e	p	m
13	5	5	20	1	20	20	8	18	5	5	16	13

3. Compute for the ciphertext using the formula;

$$e = 5, \text{ mod } = 14; c = m^e \pmod{14}$$

$$c = 13^5 \pmod{14};$$

$$c = 371293 \pmod{14}$$

$$c = 13$$

# Encrypting and Decrypting RSA

4. Look for the value of the **c** in the alphabetic table:

$c = 13, c = 3 \dots c = 13$

Iterate until the entire message is converted into a cipher

ciper	13	3	3	6	1	6	6	8	2	3	3	4	13
ciphertext	m	c	c	f	a	f	f	h	b	c	c	d	m

Message

Meet at three pm

Cyphertext

Mccfaffhbccdm

# Encrypting and Decrypting RSA

1. To decrypt, reverse the process of encryption :

mccfaffhbccdm

2. Convert the message into its numeric value – using the alphabet table, the following numeric value is identified

Ciphertext	m	c	c	f	a	f	f	h	b	c	c	d	m
value	13	3	3	6	1	6	6	8	2	3	3	4	13

3. Compute for the message using the formula;

$$d = 11, \text{ mod} = 14; m = c^d \pmod{14}$$

$$c = 13^{11} \pmod{14};$$

$$m = 1792160394037 \pmod{14}$$

$$m = 13$$

# Encrypting and Decrypting RSA

4. Look for the value of the *m* in the alphabetic table:

$$m = 13, m = 5 \dots m = 13$$

Iterate until the entire message is converted into a cipher

m	13	5	5	20	1	20	20	8	18	5	5	16	13
Ciphertext	m	e	e	t	a	t	t	h	r	e	e	p	m

Ciphertext

Mccfaffhbccdm

Message

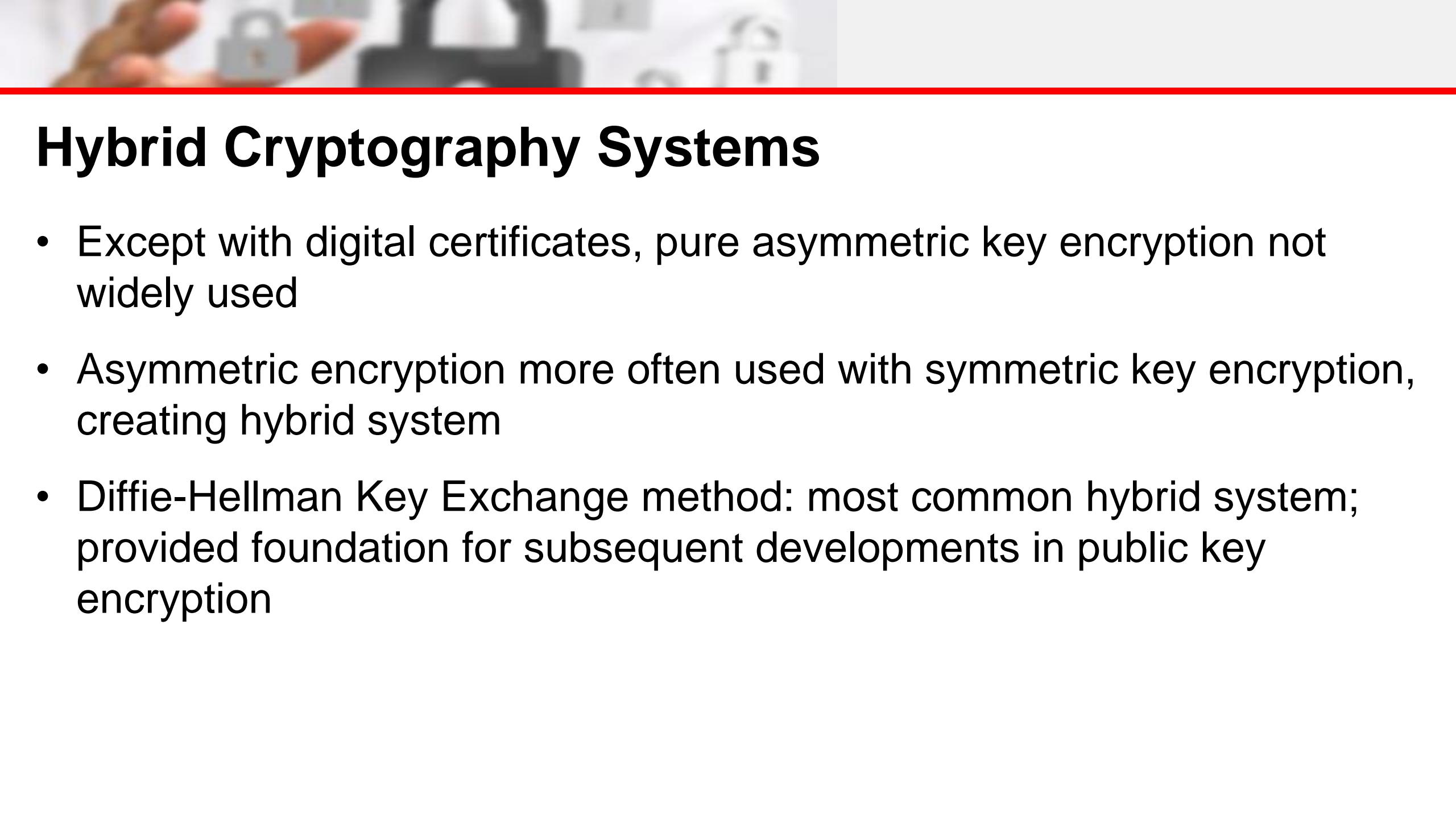
Meet at three pm



# Encryption Key Power

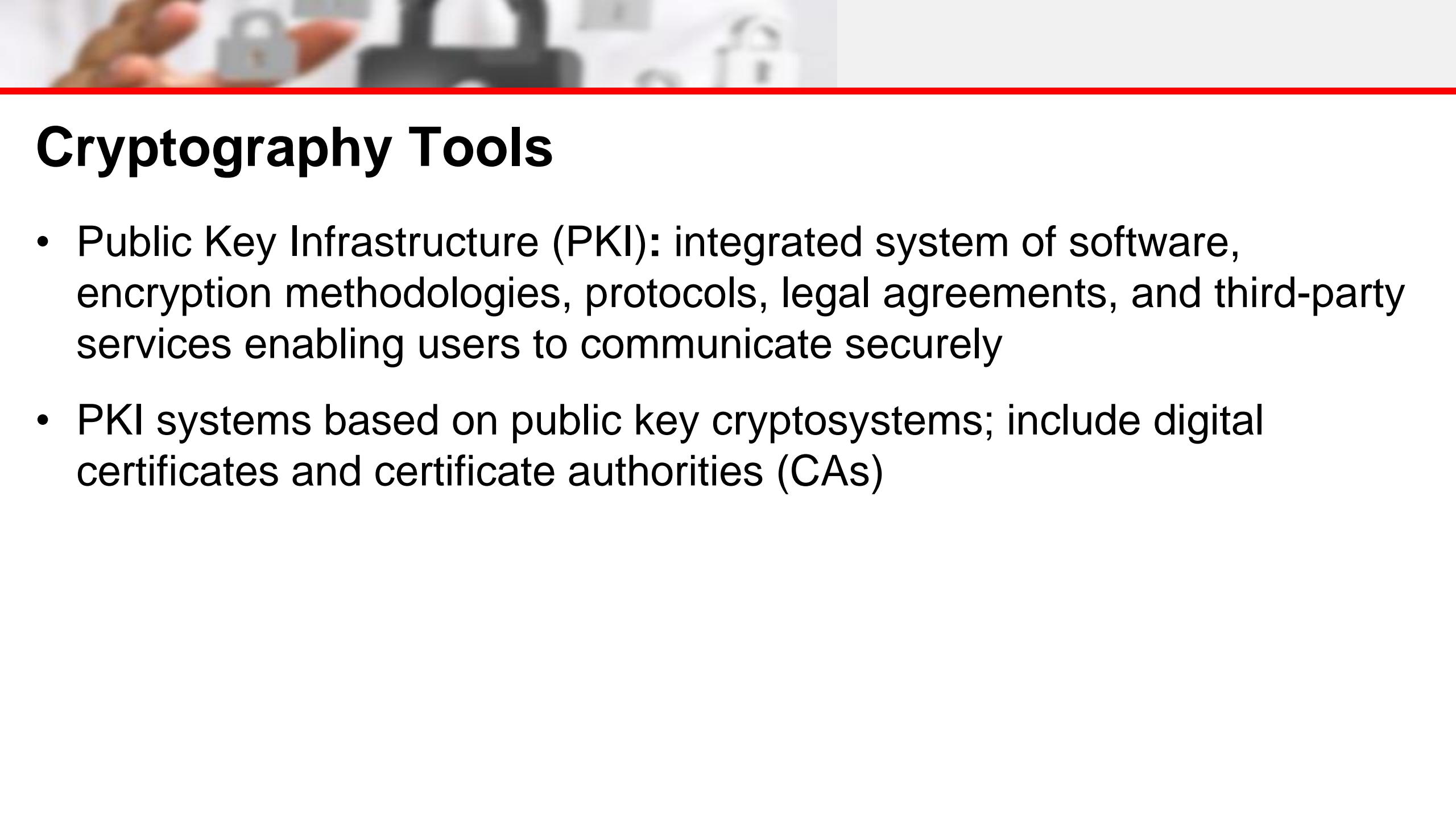
Number of Bits in Key	Odds of Cracking: 1 in	Estimated Time to Crack*
8	256	.000032 seconds
16	65,536	.008192 seconds
24	16,777,216	2.097 seconds
32	4,294,967,296	8 minutes 56.87 seconds
56	72,057,594,037,927,900	285 years 32 weeks 1 day
64	18,446,744,073,709,600,000	8,090,677,225 years
128	3.40282E+38	5,257,322,061,209,440,000,000 years
256	1.15792E+77	2,753,114,795,116,330,000,000,000,000, 000,000,000,000,000,000,000 years
512	1.3408E+154	608,756,305,260,875,000,000,000,000, 000,000,000,000,000,000,000,000,000, 000,000,000,000,000,000,000,000,000, 000,000,000 years

[NOTE]\*Estimated Time to Crack is based on a general-purpose personal computer performing eight million guesses per second.



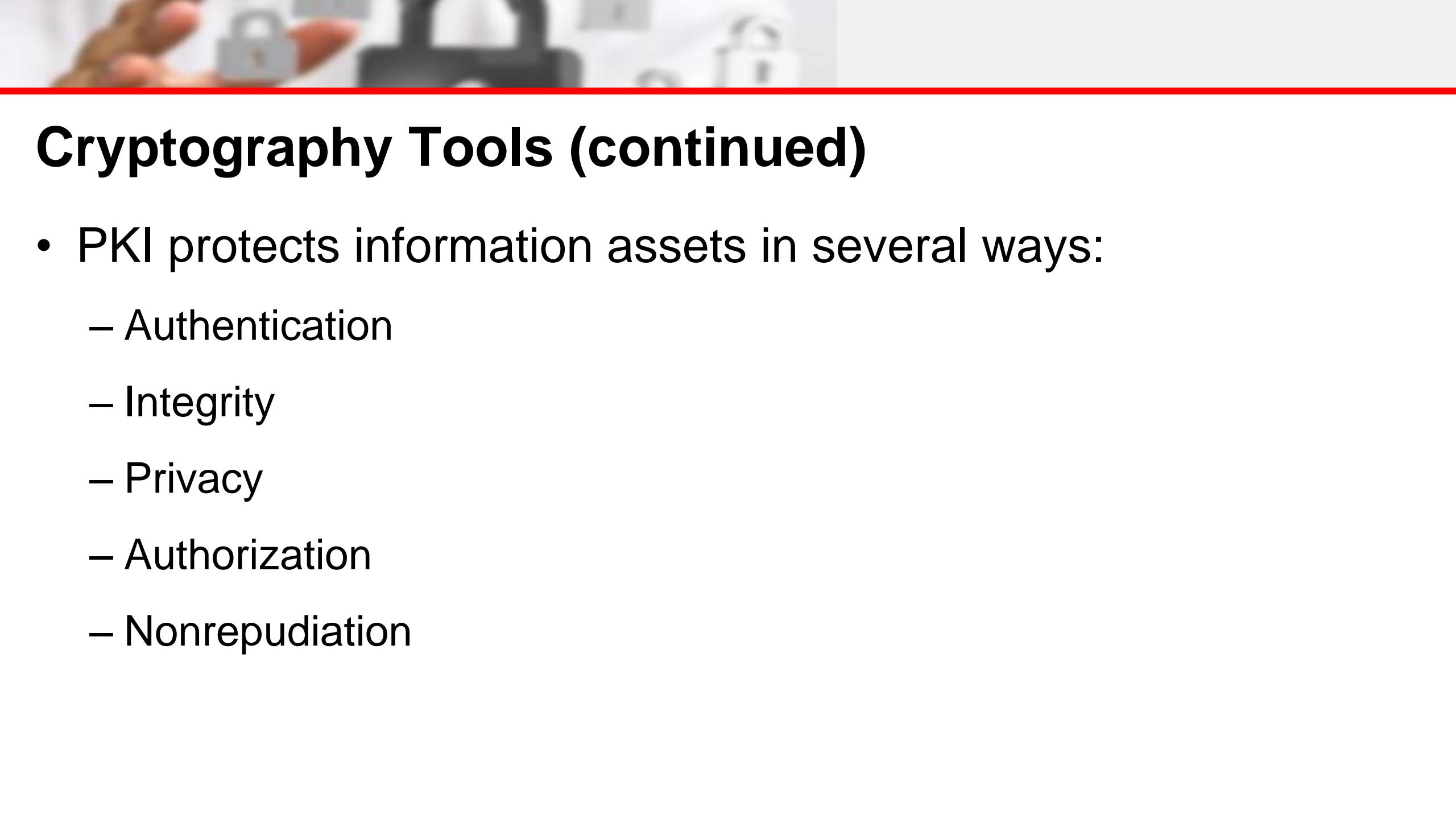
# Hybrid Cryptography Systems

- Except with digital certificates, pure asymmetric key encryption not widely used
- Asymmetric encryption more often used with symmetric key encryption, creating hybrid system
- Diffie-Hellman Key Exchange method: most common hybrid system; provided foundation for subsequent developments in public key encryption



# Cryptography Tools

- Public Key Infrastructure (PKI): integrated system of software, encryption methodologies, protocols, legal agreements, and third-party services enabling users to communicate securely
- PKI systems based on public key cryptosystems; include digital certificates and certificate authorities (CAs)



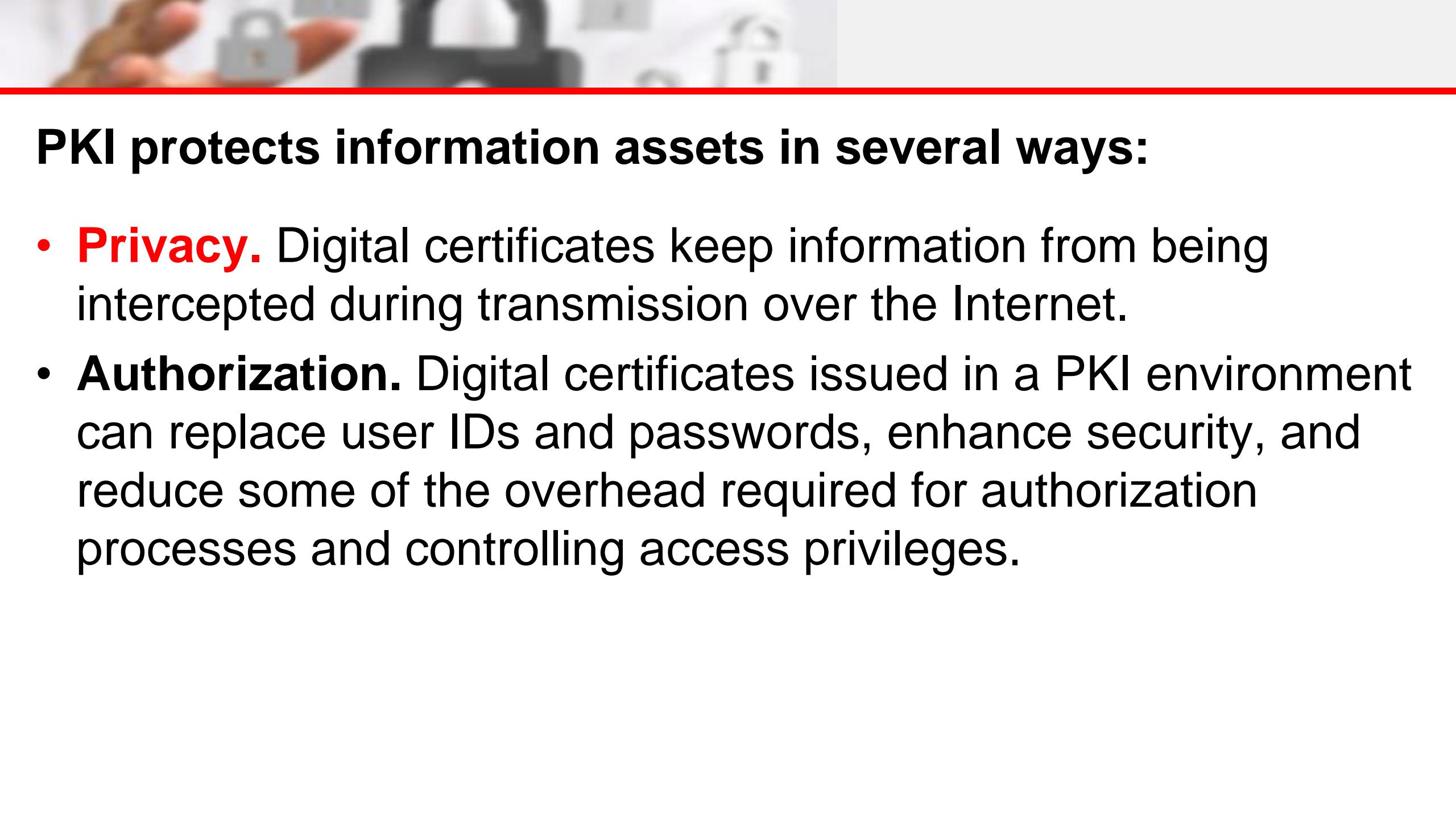
# Cryptography Tools (continued)

- PKI protects information assets in several ways:
  - Authentication
  - Integrity
  - Privacy
  - Authorization
  - Nonrepudiation



## PKI protects information assets in several ways:

- **Authentication.** Digital certificates in a PKI system permit parties to validate the identity of other of the parties in an Internet transaction.
- **Integrity.** A digital certificate demonstrates that the content signed by the certificate has not been altered while being moved from server to client.



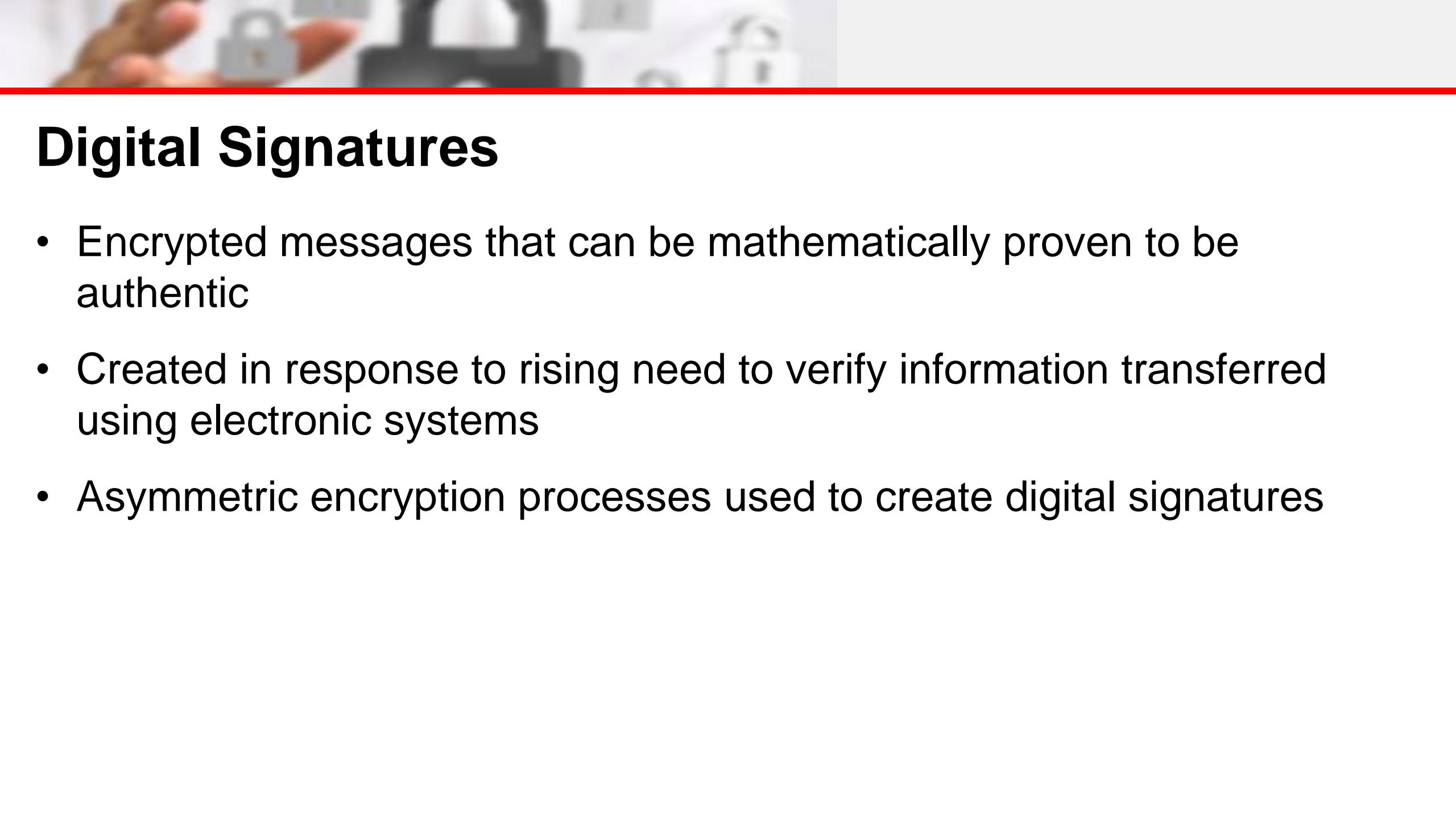
## PKI protects information assets in several ways:

- **Privacy.** Digital certificates keep information from being intercepted during transmission over the Internet.
- **Authorization.** Digital certificates issued in a PKI environment can replace user IDs and passwords, enhance security, and reduce some of the overhead required for authorization processes and controlling access privileges.



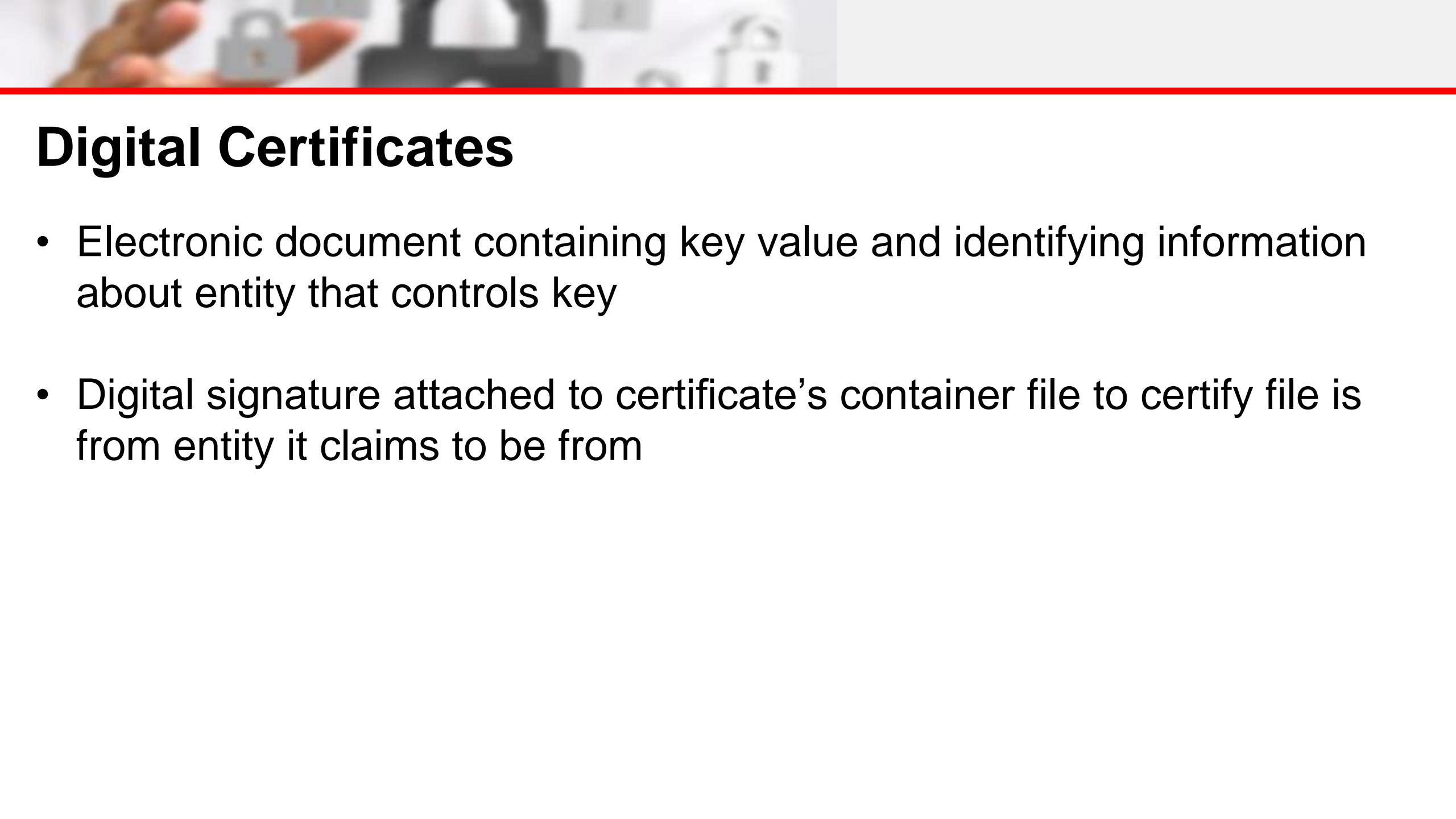
## PKI protects information assets in several ways:

- **Nonrepudiation.** Digital certificates can validate actions, making it less likely that customers or partners can later repudiate a digitally signed transaction.



# Digital Signatures

- Encrypted messages that can be mathematically proven to be authentic
- Created in response to rising need to verify information transferred using electronic systems
- Asymmetric encryption processes used to create digital signatures



# Digital Certificates

- Electronic document containing key value and identifying information about entity that controls key
- Digital signature attached to certificate's container file to certify file is from entity it claims to be from

# Digital Certificates and Signatures

The image displays two side-by-side windows titled "Certificate" with tabs for "General", "Details", and "Certification Path". Both windows show "Certificate Information" with a purpose section and issuance details.

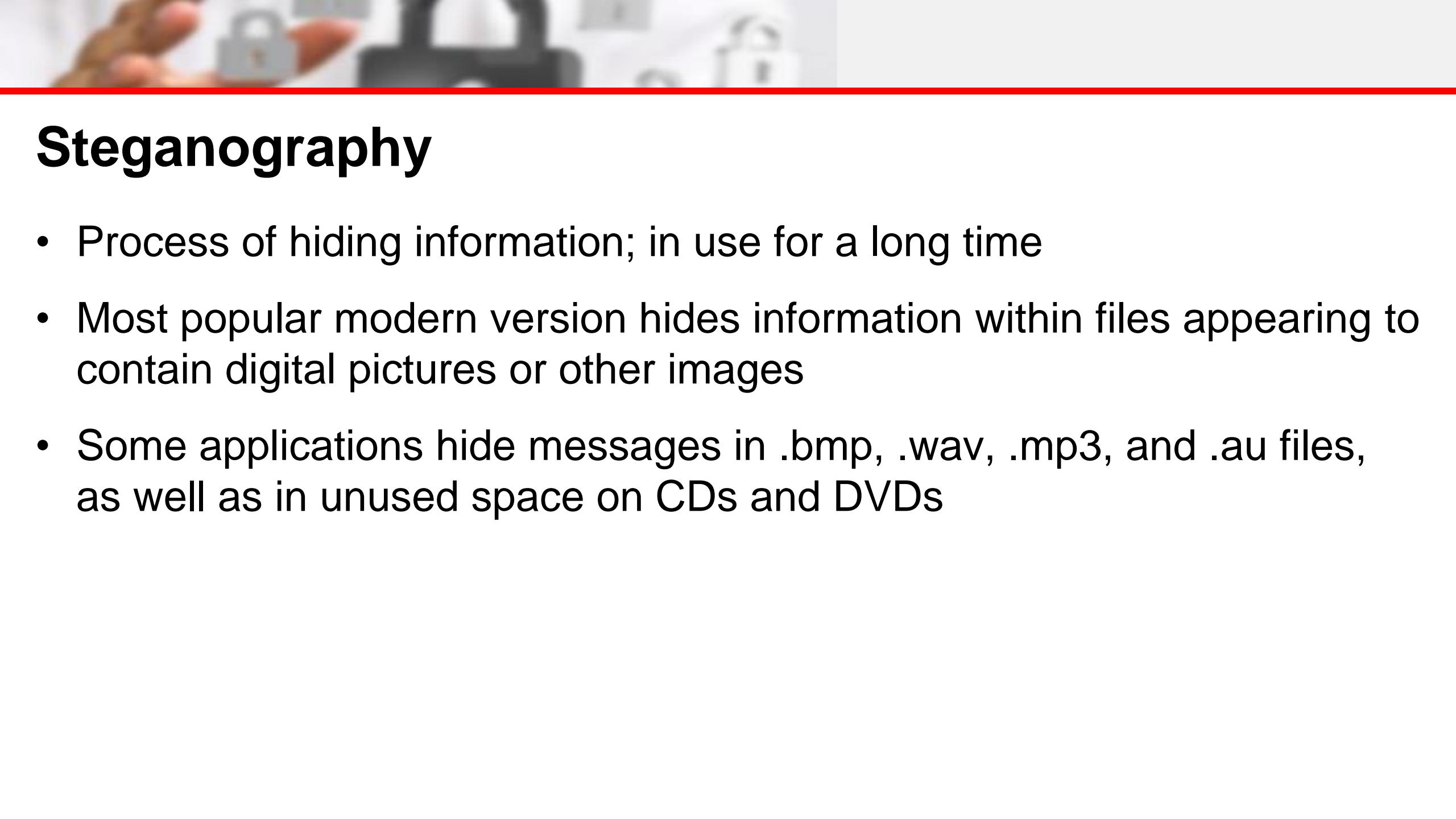
**Left Window (Comodo RSA Code Signing CA):**

- Purpose:** Ensures software came from software publisher, Protects software from alteration after publication, All issuance policies.
- Issued to:** COMODO RSA Code Signing CA
- Issued by:** COMODO RSA Certification Authority
- Valid from:** 5/ 9/ 2013 to 5/ 9/ 2028

**Right Window (DigiCert SHA2 High Assurance Server CA):**

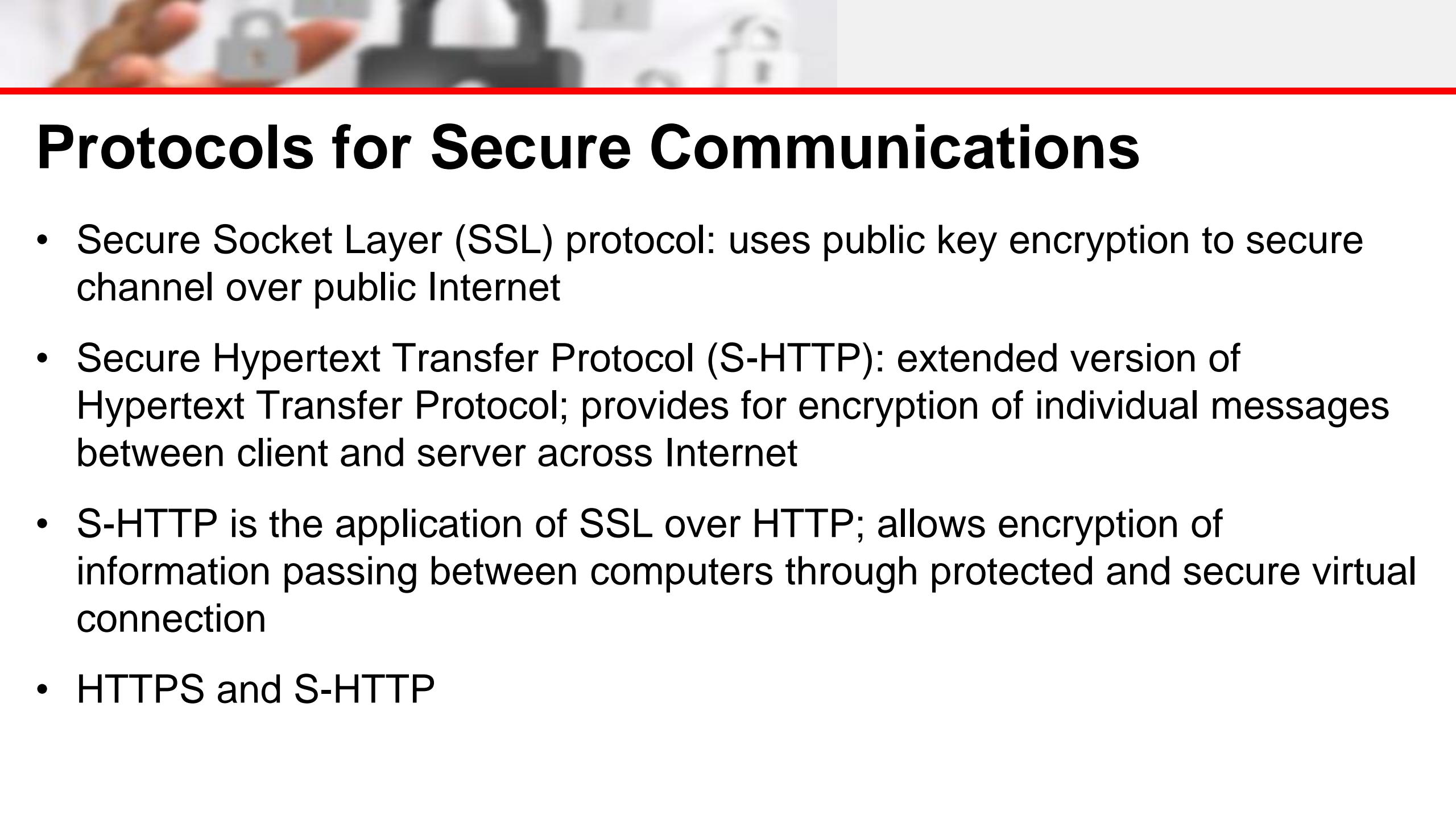
- Purpose:** Ensures the identity of a remote computer, Proves your identity to a remote computer, All issuance policies.
- Issued to:** DigiCert SHA2 High Assurance Server CA
- Issued by:** DigiCert High Assurance EV Root CA
- Valid from:** 10/ 22/ 2013 to 10/ 22/ 2028

Both windows include links to "Issuer Statement" and "Learn more about certificates" and have an "OK" button at the bottom right.



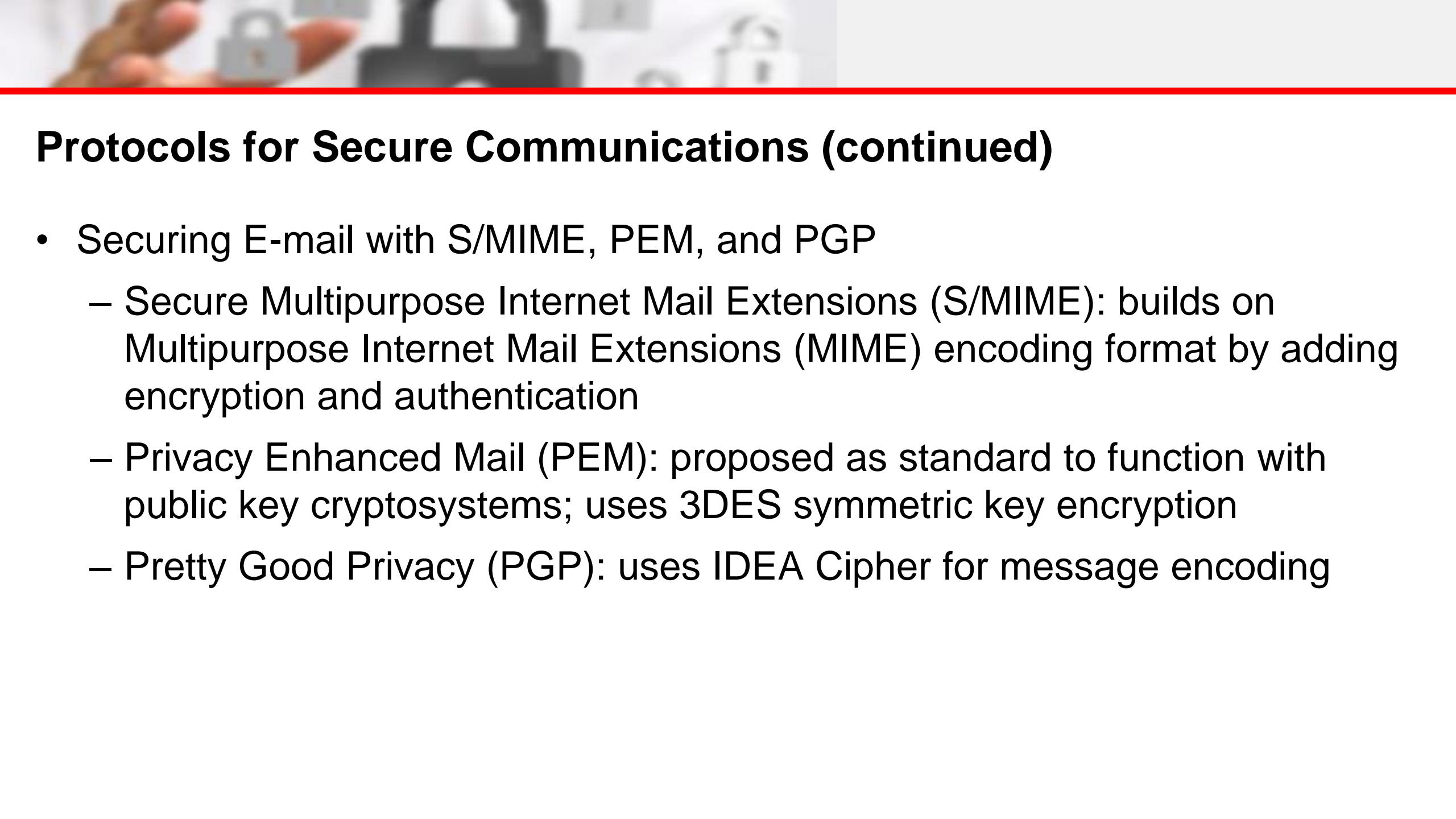
# Steganography

- Process of hiding information; in use for a long time
- Most popular modern version hides information within files appearing to contain digital pictures or other images
- Some applications hide messages in .bmp, .wav, .mp3, and .au files, as well as in unused space on CDs and DVDs



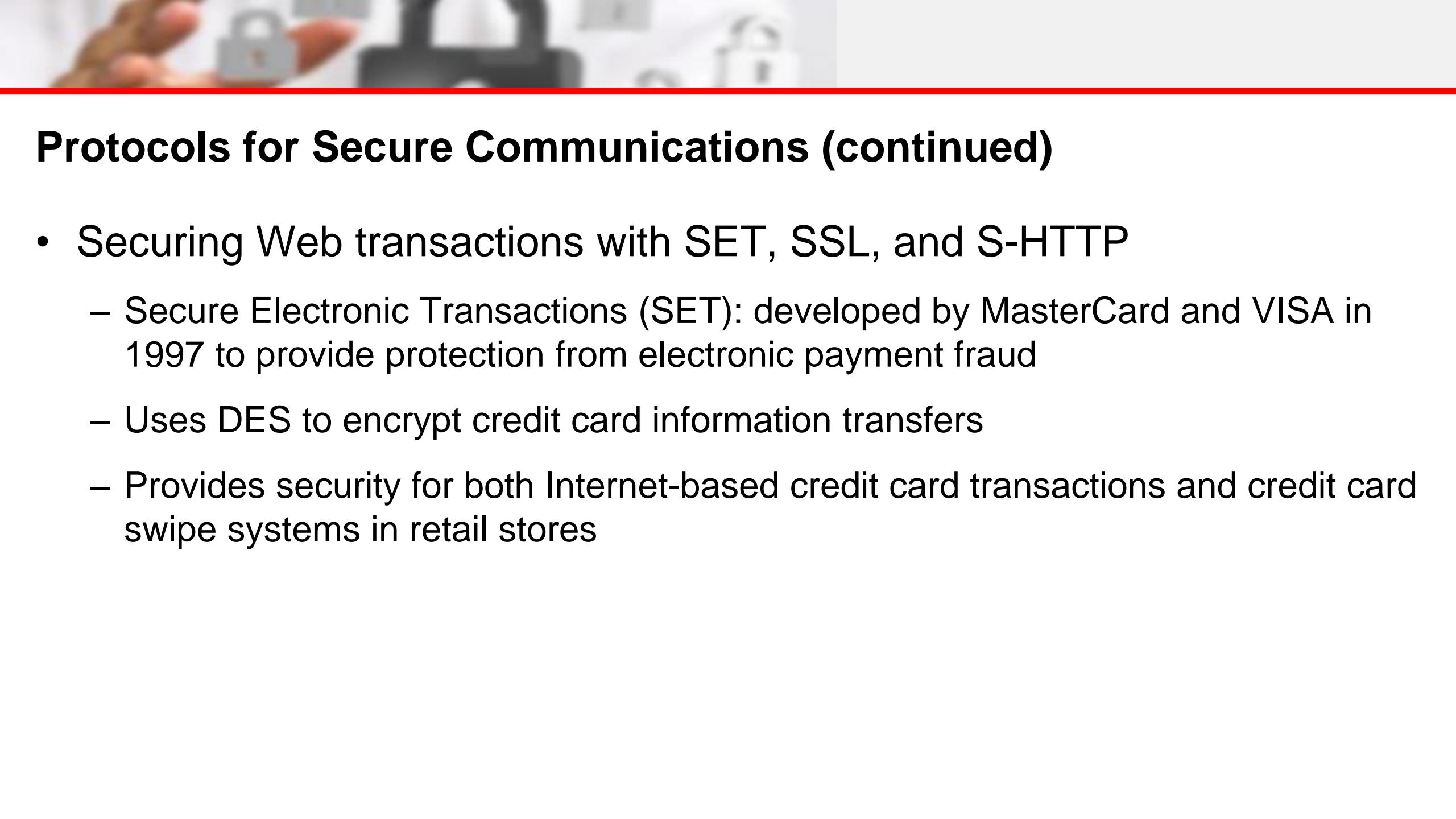
# Protocols for Secure Communications

- Secure Socket Layer (SSL) protocol: uses public key encryption to secure channel over public Internet
- Secure Hypertext Transfer Protocol (S-HTTP): extended version of Hypertext Transfer Protocol; provides for encryption of individual messages between client and server across Internet
- S-HTTP is the application of SSL over HTTP; allows encryption of information passing between computers through protected and secure virtual connection
- HTTPS and S-HTTP



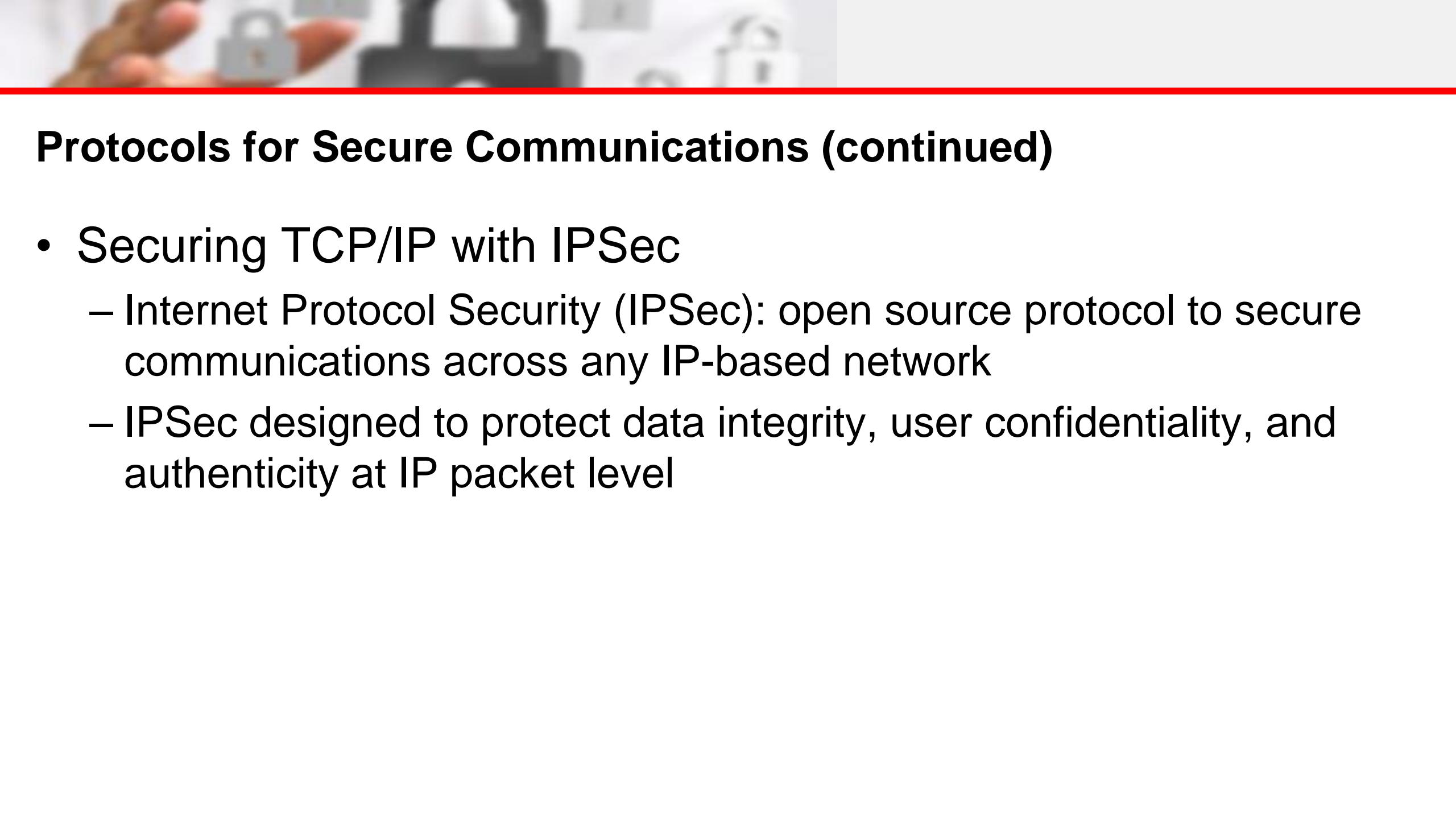
## Protocols for Secure Communications (continued)

- Securing E-mail with S/MIME, PEM, and PGP
  - Secure Multipurpose Internet Mail Extensions (S/MIME): builds on Multipurpose Internet Mail Extensions (MIME) encoding format by adding encryption and authentication
  - Privacy Enhanced Mail (PEM): proposed as standard to function with public key cryptosystems; uses 3DES symmetric key encryption
  - Pretty Good Privacy (PGP): uses IDEA Cipher for message encoding



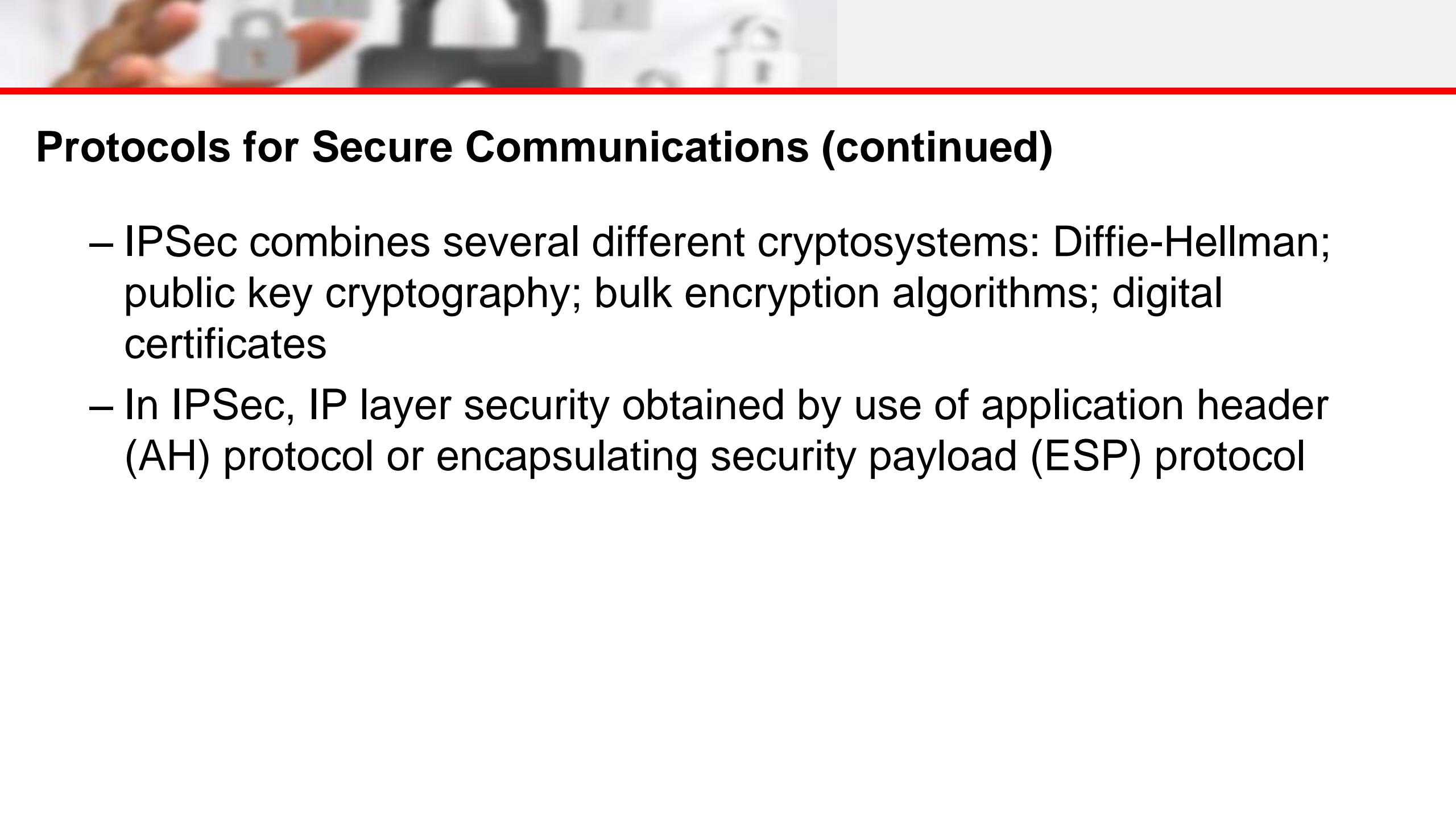
## Protocols for Secure Communications (continued)

- Securing Web transactions with SET, SSL, and S-HTTP
  - Secure Electronic Transactions (SET): developed by MasterCard and VISA in 1997 to provide protection from electronic payment fraud
  - Uses DES to encrypt credit card information transfers
  - Provides security for both Internet-based credit card transactions and credit card swipe systems in retail stores



## Protocols for Secure Communications (continued)

- Securing TCP/IP with IPSec
  - Internet Protocol Security (IPSec): open source protocol to secure communications across any IP-based network
  - IPSec designed to protect data integrity, user confidentiality, and authenticity at IP packet level



## Protocols for Secure Communications (continued)

- IPSec combines several different cryptosystems: Diffie-Hellman; public key cryptography; bulk encryption algorithms; digital certificates
- In IPSec, IP layer security obtained by use of application header (AH) protocol or encapsulating security payload (ESP) protocol



## Protocols for Secure Communications (continued)

- Freeware and low-cost commercial PGP versions are available for many platforms
- PGP security solution provides six services: authentication by digital signatures; message encryption; compression; e-mail compatibility; segmentation; key management



# Hashing

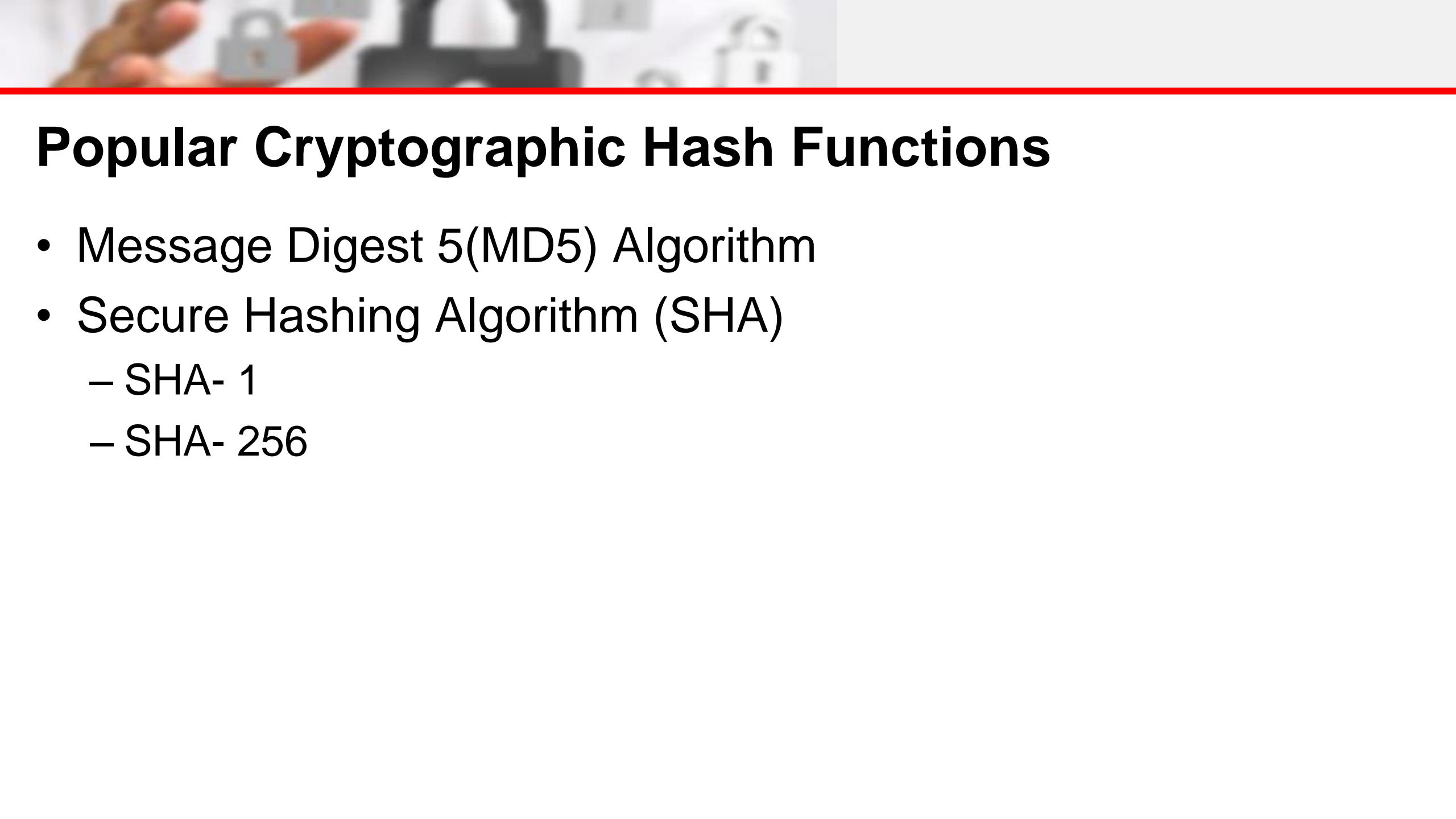
Engr. Juliet S. Mendez

MBA, CCNA



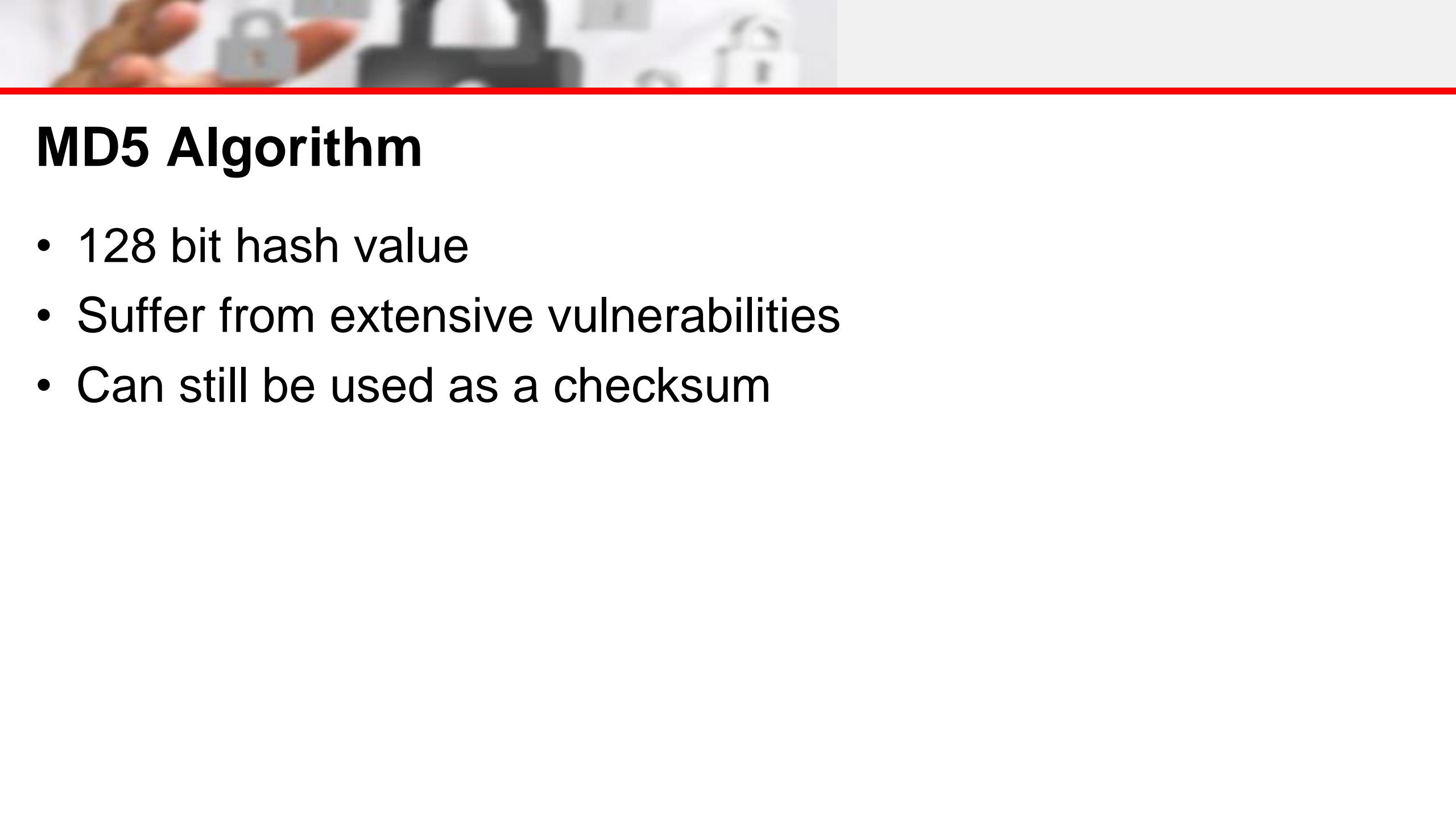
# Hashing

- Any function that can be used to map data of arbitrary size of data of fixed size.
- Used in checksums, check digits, fingerprints, lossy compression, randomization functions, error-correcting codes and ciphers
- File Verification
- Password Storage
- Database Searching



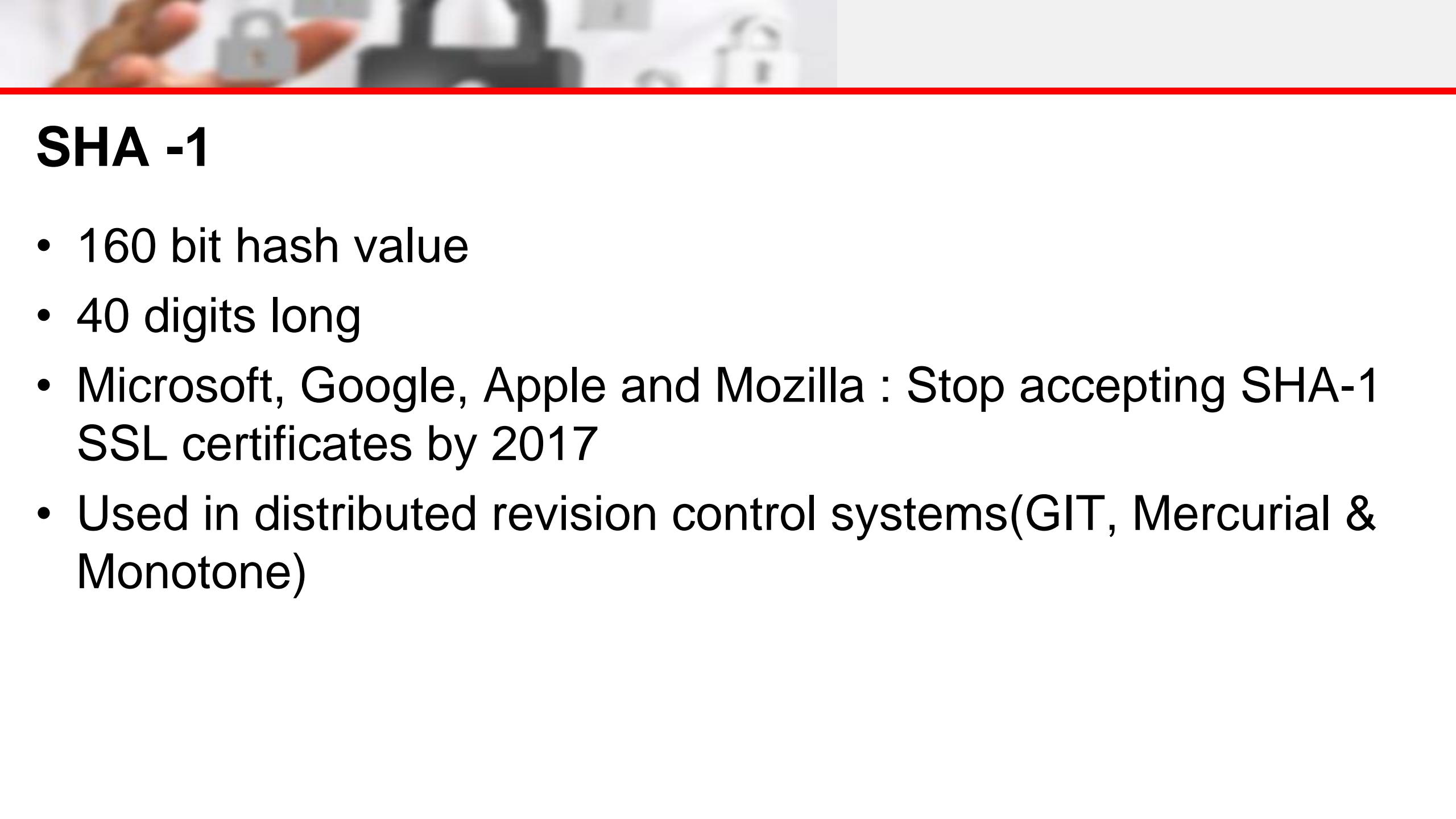
# Popular Cryptographic Hash Functions

- Message Digest 5(MD5) Algorithm
- Secure Hashing Algorithm (SHA)
  - SHA- 1
  - SHA- 256



# MD5 Algorithm

- 128 bit hash value
- Suffer from extensive vulnerabilities
- Can still be used as a checksum



## SHA -1

- 160 bit hash value
- 40 digits long
- Microsoft, Google, Apple and Mozilla : Stop accepting SHA-1 SSL certificates by 2017
- Used in distributed revision control systems(GIT, Mercurial & Monotone)

# SHA-2

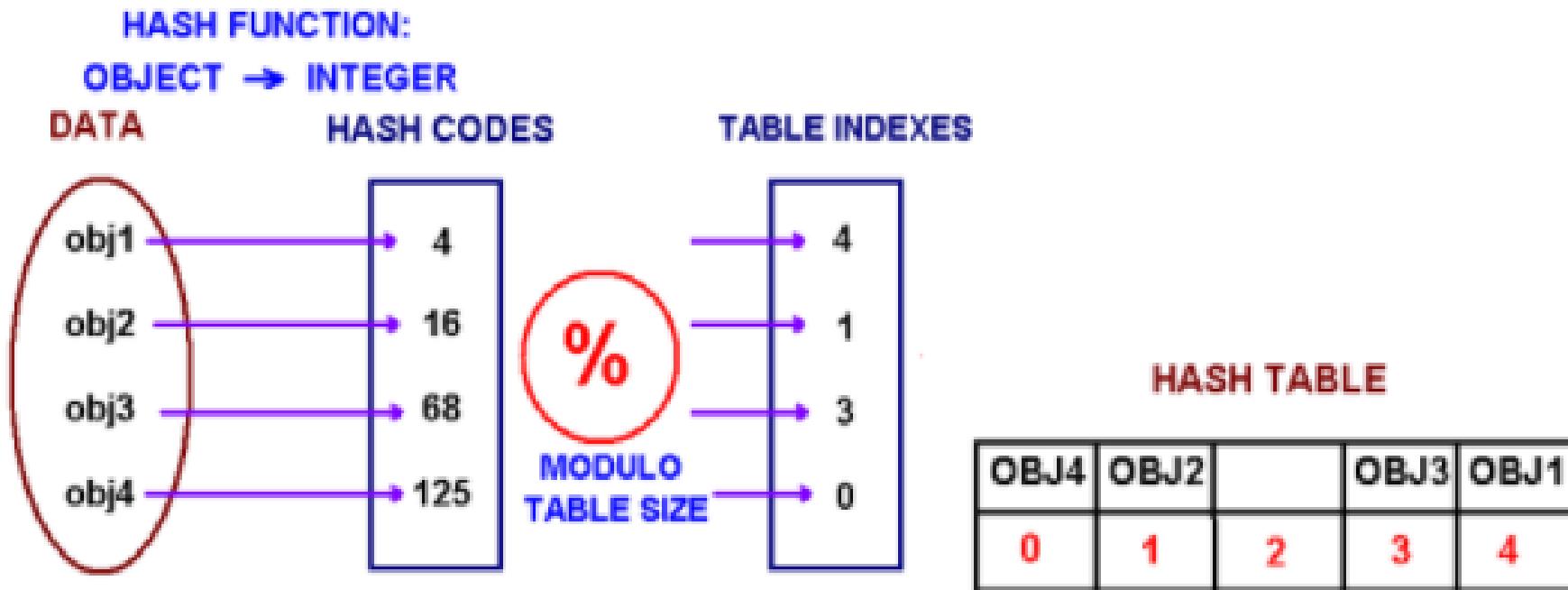
- Consist of six hash functions with hash values
  - SHA-224
  - SHA-256
  - SHA-384
  - SHA-512

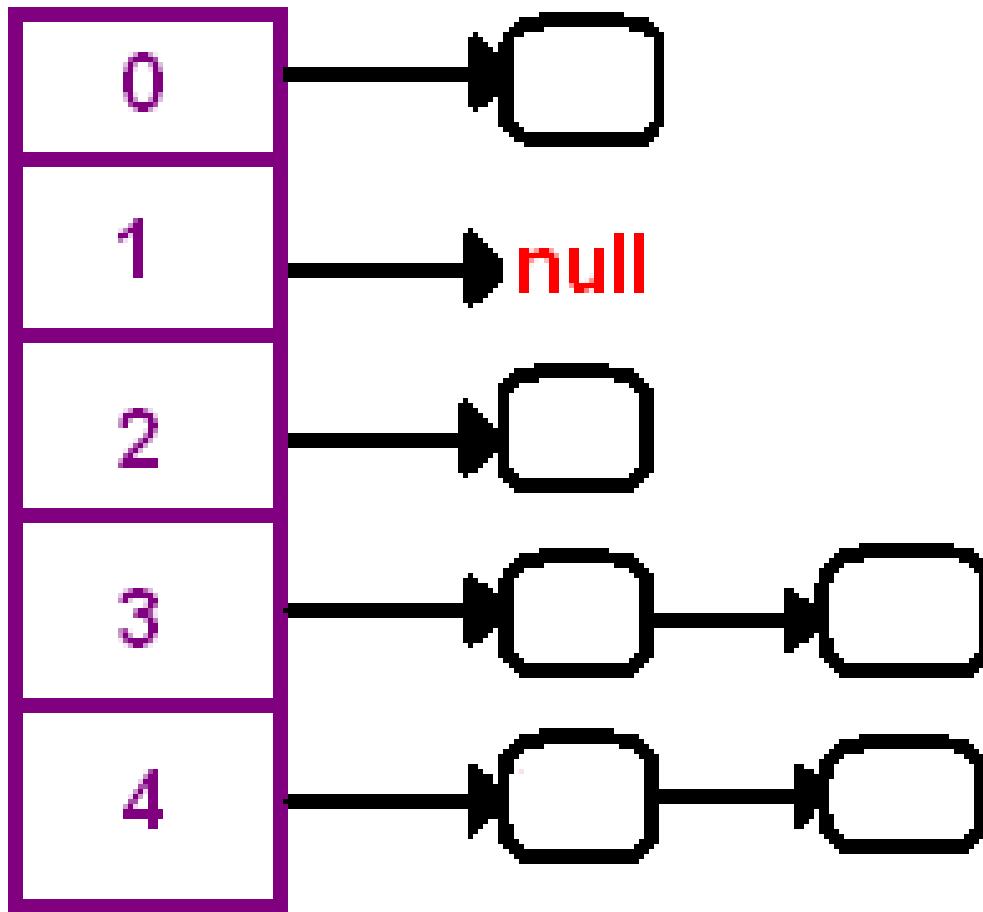
Published in	Year	Attack method	Attack	Variant	Rounds	Complexity
<i>New Collision Attacks Against Up To 24-step SHA-2<sup>[32]</sup></i>	2008	Deterministic	Collision	SHA-256	24/64	$2^{28.5}$
				SHA-512	24/80	$2^{32.5}$
<i>Preimages for step-reduced SHA-2<sup>[33]</sup></i>	2009	Meet-in-the-middle	Preimage	SHA-256	42/64	$2^{251.7}$
					43/64	$2^{254.9}$
				SHA-512	42/80	$2^{502.3}$
					46/80	$2^{511.5}$
<i>Advanced meet-in-the-middle preimage attacks<sup>[34]</sup></i>	2010	Meet-in-the-middle	Preimage	SHA-256	42/64	$2^{248.4}$
				SHA-512	42/80	$2^{494.6}$
<i>Higher-Order Differential Attack on Reduced SHA-256<sup>[2]</sup></i>	2011	Differential	Pseudo-collision	SHA-256	46/64	$2^{178}$
					33/64	$2^{46}$
<i>Bicliques for Preimages: Attacks on Skein-512 and the SHA-2 family<sup>[1]</sup></i>	2011	Biclique	Preimage	SHA-256	45/64	$2^{255.5}$
				SHA-512	50/80	$2^{511.5}$
			Pseudo-preimage	SHA-256	52/64	$2^{255}$
				SHA-512	57/80	$2^{511}$
<i>Improving Local Collisions: New Attacks on Reduced SHA-256<sup>[35]</sup></i>	2013	Differential	Collision	SHA-256	31/64	$2^{65.5}$
			Pseudo-collision	SHA-256	38/64	$2^{37}$
<i>Branching Heuristics in Differential Collision Search with Applications to SHA-512<sup>[36]</sup></i>	2014	Heuristic differential	Pseudo-collision	SHA-512	38/80	$2^{40.5}$
<i>Analysis of SHA-512/224 and SHA-512/256<sup>[37]</sup></i>	2016	Differential	Collision	SHA-256	28/64	practical
				SHA-512	27/80	practical
			Pseudo-collision	SHA-512	39/80	practical

## SHA- 3

- released on August 5, 2015 by NIST
- Is a subset of Keccak
- Data is absorbed into sponge, result is squeezed out.

# Storing Hash Function





# JAVA Sample Code

```
17 |     public static void main(String[] args) {  
18 |         // TODO code application logic here  
19 |         Integer obj1 = new Integer(2009);  
20 |         String obj2 = new String("ABC");  
21 |         System.out.println("hashCode for an integer is " + obj1.hashCode());  
22 |         System.out.println("hashCode for a string is " + obj2.hashCode());  
23 |     }  
24 | }
```

# Formula

$$s.charAt(0) * 31^{n-1} + s.charAt(1) * 31^{n-2} + s.charAt(2) * 31^{n-3} + \dots + s.charAt(n-1)$$

where  $s$  = string value in ASCII and  $n$  = length

Sample Computation:

**ABC**

$$ABC = 'A' * 31^2 + 'B' * 31 + 'C'$$

$$ABC = 65 * 31^2 + 66 * 31 + 67$$

$$ABC = 64578$$

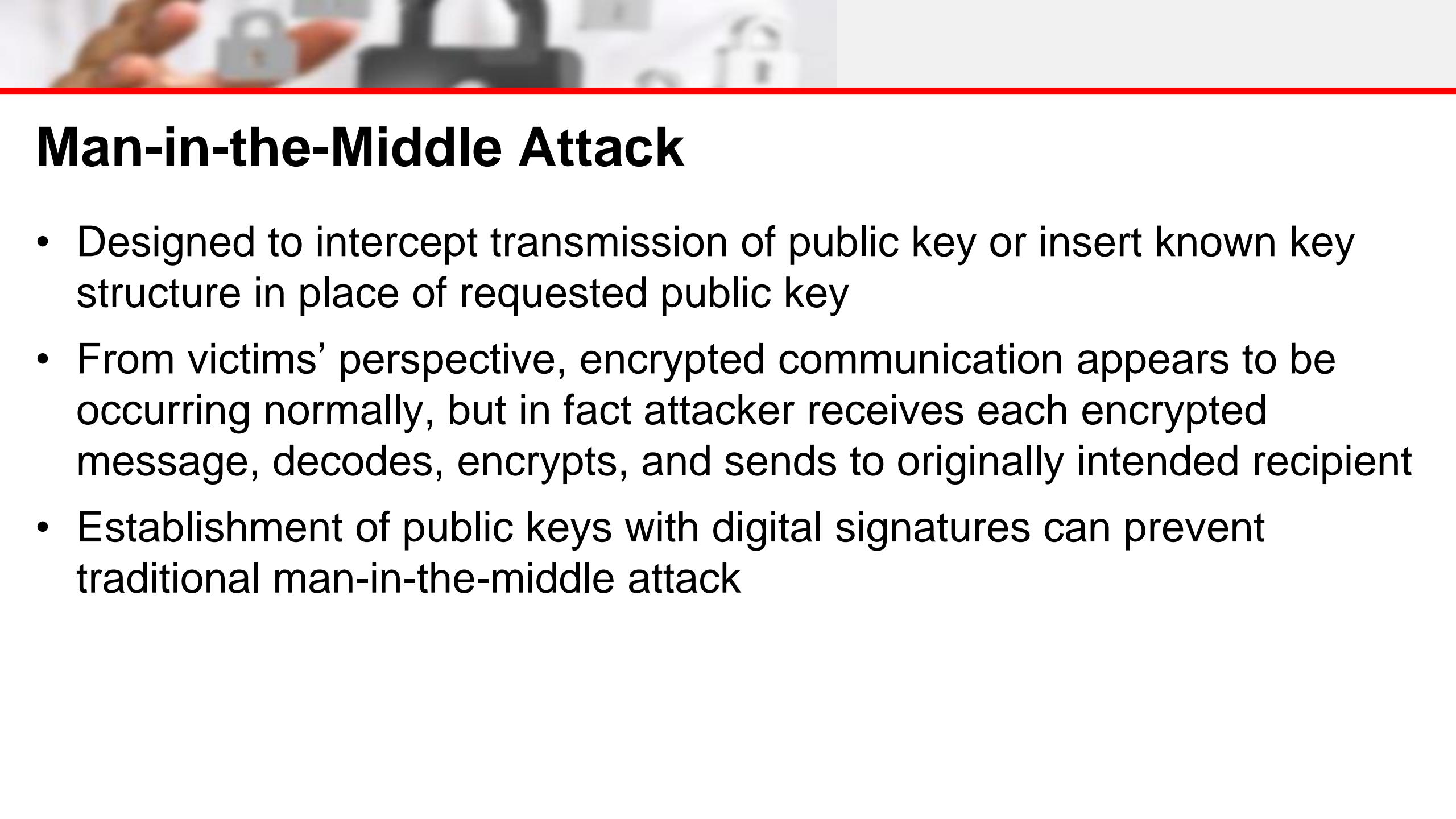


# Attack on Crytosystems



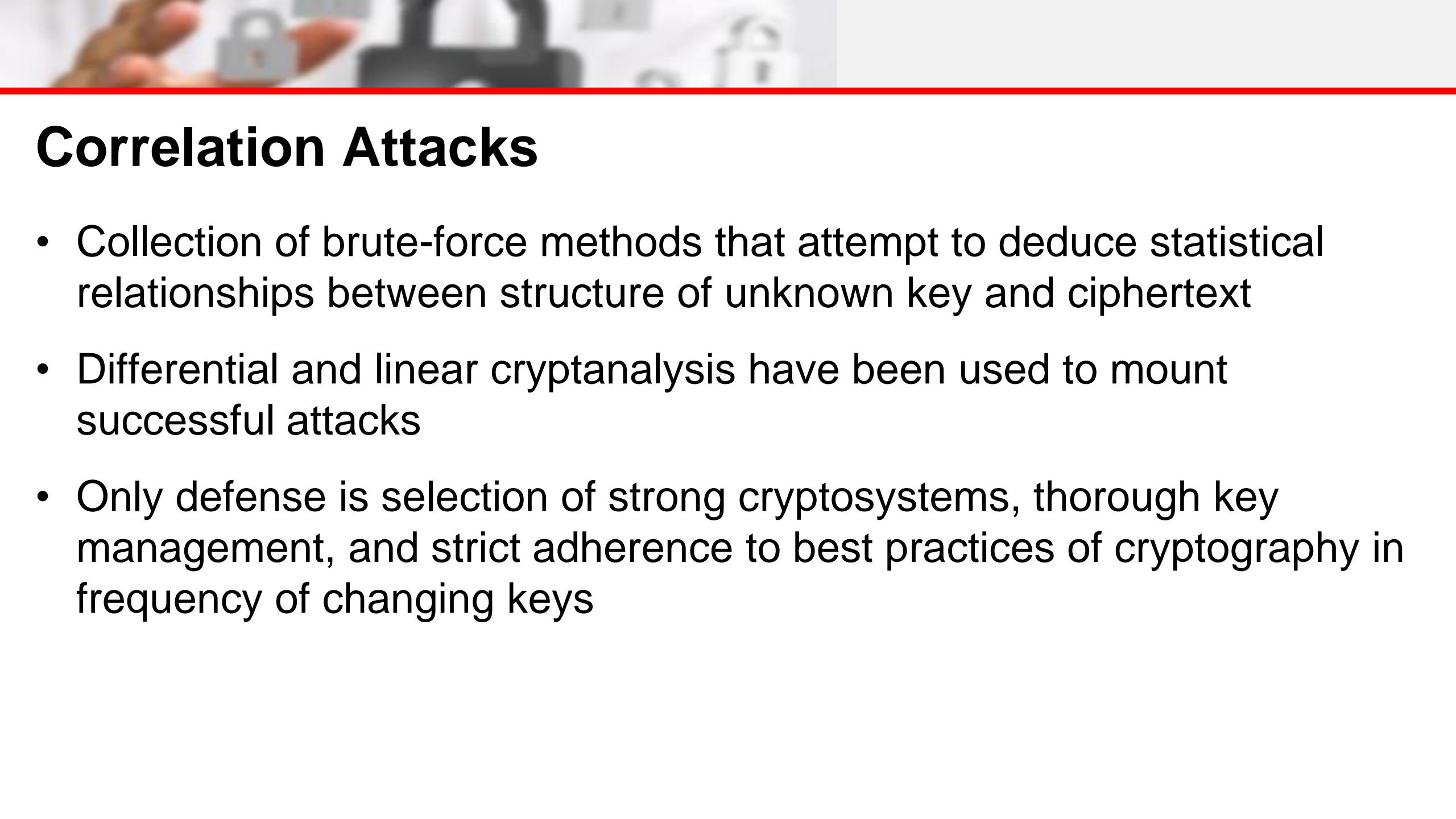
# Attacks on Cryptosystems

- Attempts to gain unauthorized access to secure communications have typically used brute force attacks (ciphertext attacks)
- Attacker may alternatively conduct known-plaintext attack or selected-plaintext attach schemes



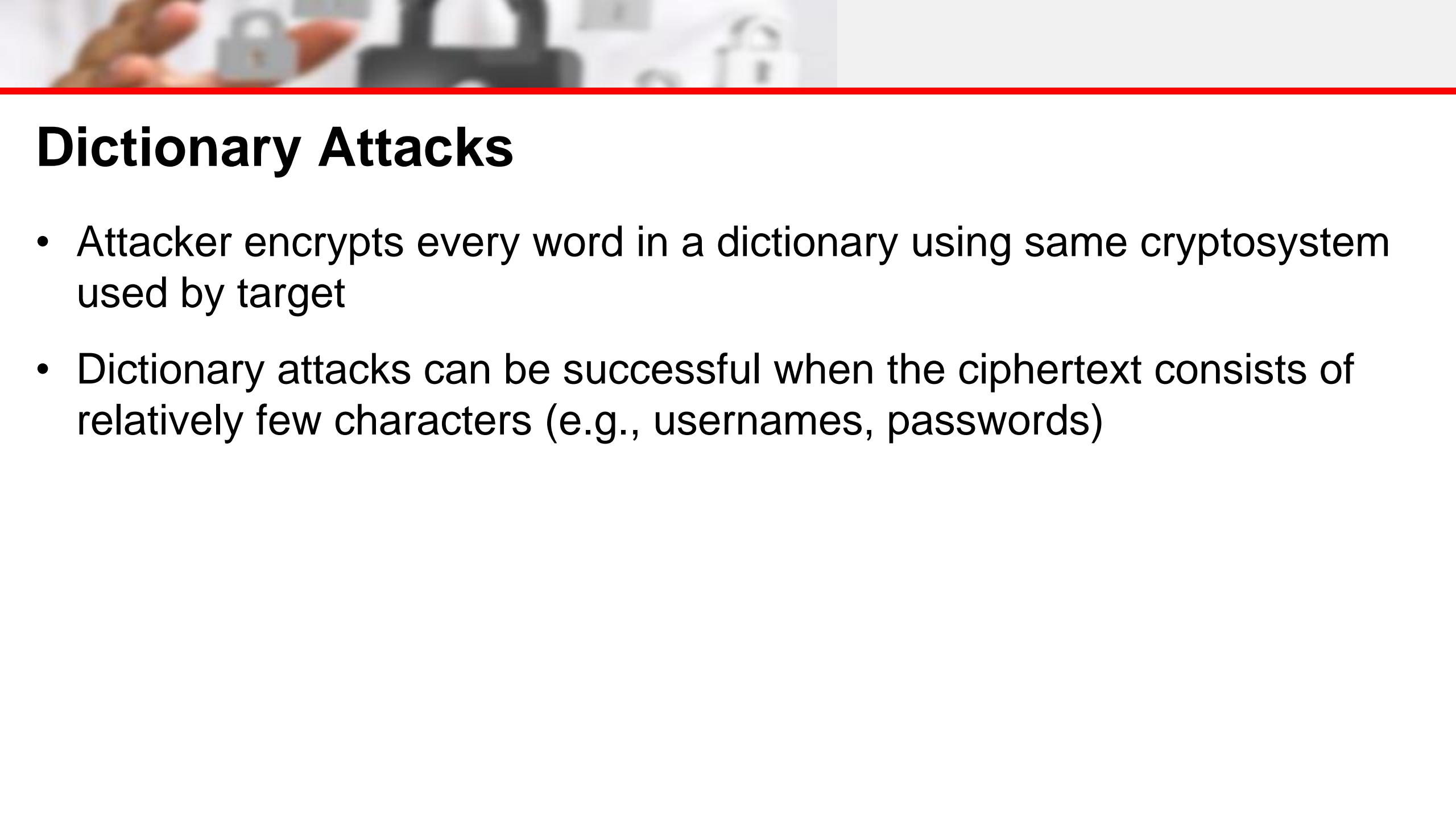
# Man-in-the-Middle Attack

- Designed to intercept transmission of public key or insert known key structure in place of requested public key
- From victims' perspective, encrypted communication appears to be occurring normally, but in fact attacker receives each encrypted message, decodes, encrypts, and sends to originally intended recipient
- Establishment of public keys with digital signatures can prevent traditional man-in-the-middle attack



# Correlation Attacks

- Collection of brute-force methods that attempt to deduce statistical relationships between structure of unknown key and ciphertext
- Differential and linear cryptanalysis have been used to mount successful attacks
- Only defense is selection of strong cryptosystems, thorough key management, and strict adherence to best practices of cryptography in frequency of changing keys



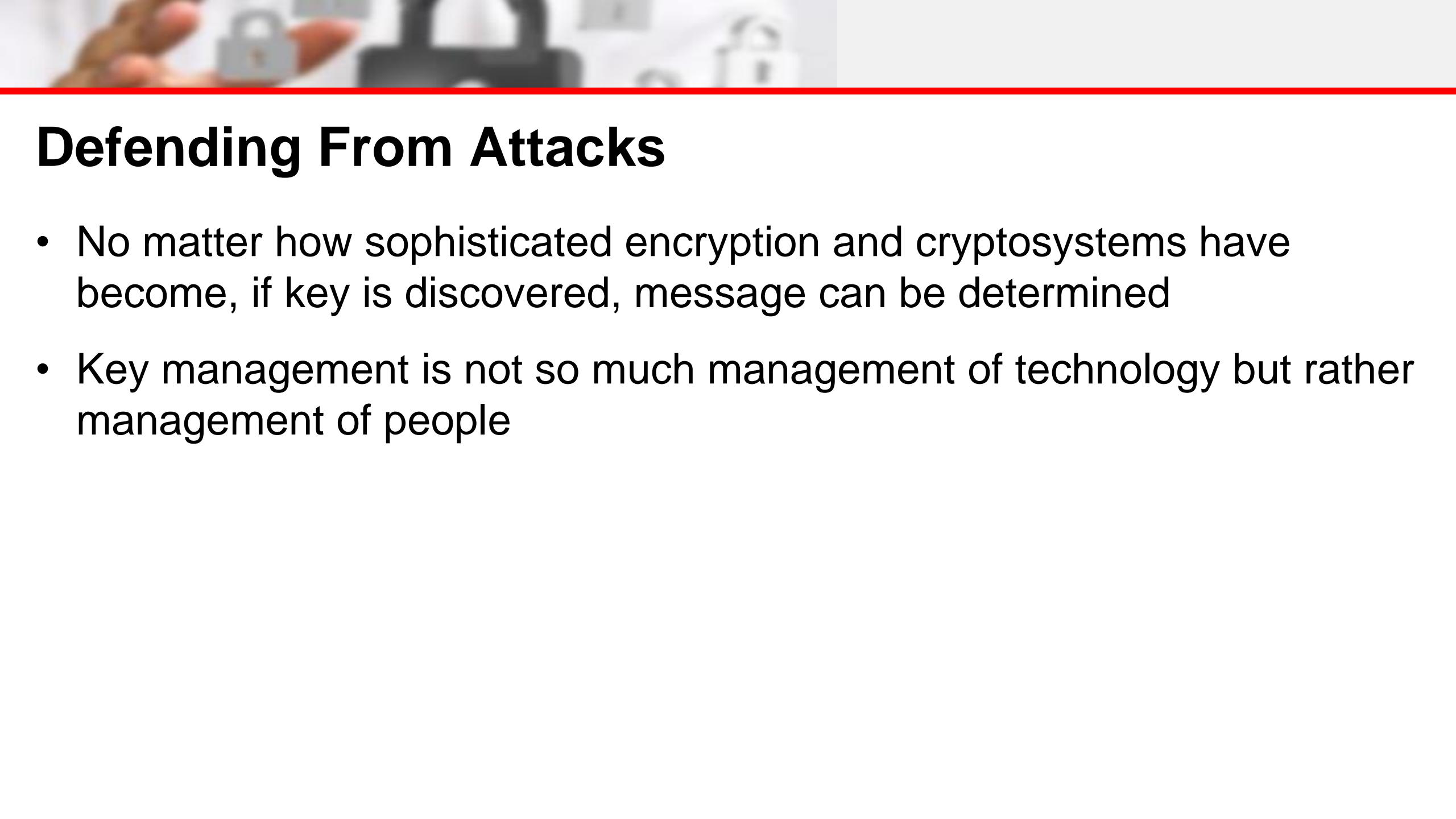
# Dictionary Attacks

- Attacker encrypts every word in a dictionary using same cryptosystem used by target
- Dictionary attacks can be successful when the ciphertext consists of relatively few characters (e.g., usernames, passwords)



# Timing Attacks

- Attacker eavesdrops during victim's session; uses statistical analysis of user's typing patterns and inter-keystroke timings to discern sensitive session information
- Can be used to gain information about encryption key and possibly cryptosystem in use
- Once encryption successfully broken, attacker may launch a replay attack (an attempt to resubmit recording of deciphered authentication to gain entry into secure source)



# Defending From Attacks

- No matter how sophisticated encryption and cryptosystems have become, if key is discovered, message can be determined
- Key management is not so much management of technology but rather management of people



# Video Clip – Cyber Security

- Video Clip showing simple definition about cybersecurity, how does it work and why do we need it.
- Cyber codes



Thank you

Have a nice day!!!



**Answer to the Ciphertext**

---

**WELCOME TO CEBU  
CARAGA STATE UNIVERSITY  
CABADBARAN CAMPUS**



# Summary

- Cryptography and encryption provide sophisticated approach to security
  - Many security-related tools use embedded encryption technologies
  - Encryption converts a message into a form that is unreadable by the unauthorized
- Many tools are available and can be classified as symmetric or asymmetric, each having advantages and special capabilities
- Strength of encryption tool dependent on key size but even more dependent on following good management practices
- Cryptography is used to secure most aspects of Internet and Web uses that require it, drawing on extensive set of protocols and tools designed for that purpose
- Cryptosystems are subject to attack in many ways

# Cryptography

NOVEMBER 6, 2015 by [ed harmoush](#) [leave a comment](#)



Do you do online banking? Do you work from home? Do you use VPNs to access company resources? All these would not be possible without Cryptography.

Cryptography is the art of keeping secrets, specifically through any form of communication.

Cryptography has existed for thousands of years, but has become increasingly more important in recent history due to the explosion of the Internet and the need for data privacy and secure online communications.

But what does “secure communication” even mean? Typically, it refers to (at least) these four concepts:

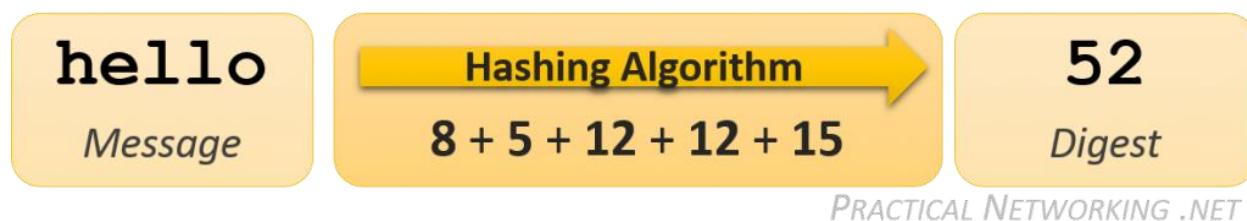
- **Confidentiality** – Assuring only the intended recipients in communication have access to the message.
- **Integrity** – Assuring that the message cannot be modified in transit without the other party being made aware.
- **Authentication** – Assuring the other party is indeed who they claim to be.
- **Anti-Replay** – Assuring the message cannot be maliciously re-transmitted.

# Hashing Algorithm

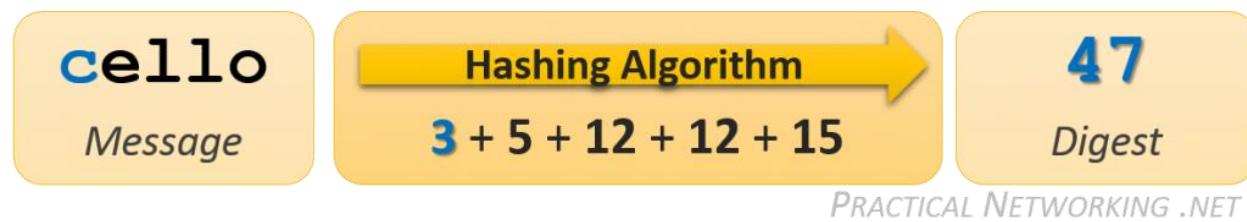
The first concept we need to discuss in our exploration of Cryptography is that of a **Hashing Algorithm**.

A Hashing Algorithm is a mathematical **formula that takes a Message of arbitrary length as input and produces as output a representational sample** of the original data.

For instance, a rudimentary example of a hashing algorithm is simply adding up all the letter values of a particular message. (A=1, B=2, C=3, etc...):



The result of a hashing algorithm is called a message **Digest** (or sometimes Checksum, or Fingerprint). The result of our example hashing on the original message of `hello` was 52. If someone were to change our original message and process it through the same hashing algorithm, the result would be different:



By comparing the message digests of each calculation, it is easy to determine that our message has changed.

Obviously, the Hashing algorithm used in the example is full of flaws. There are many words that when processed through the example algorithm that might result in the same Digest. Had the original Message been changed to `cellt`, the resulting digest would still be 52, and we would be unaware that the original Message had been altered.

In reality, a legitimate hashing algorithm must maintain four qualities before it is approved for industry usage:

- 1. It is mathematically impossible to extract the original message from the digest.**

It should be impossible to reverse the hashing algorithm and recover the original Message knowing just the resulting Digest. In fact, Hashing is sometimes referred to as *one-way encryption*: the message can be encrypted but is impossible to decrypt. This is accomplished using one-way functions within the hashing algorithm.

In a way, our example Hashing algorithm satisfied this condition. It is impossible to derive *hello* knowing only a resulting digest of *52*. Mostly because there could be thousands of messages that result in the identical digest.

- 2. A slight change to the original message causes a drastic change in the resulting digest.**

Any minor modification – even as small as changing a single character – to the original Message should greatly alter the computed digest. This is sometimes referred to as the Avalanche effect.

It is possible because a Hashing algorithm is not simply one calculation. It is a series of calculations, done iteratively over and over. As a result, a small change in the beginning, creates an exponentially bigger and bigger change in the resulting digest. Just like a snowball tumbling down a mountain forming an avalanche.

- 3. The result of the hashing algorithm is always the same length.**

It is vital for the resulting Digest to not provide any hints or clues about the original Message – including its length. A digest should not grow in size as the length of the Message increases.

In our example Hashing algorithm, the longer the word, the bigger the resulting digest would be as we are adding more and more letters together. However in an industry approved hashing algorithm, hashing the word *hello* would produce a digest the same size as hashing the entire library of congress.

- 4. It is infeasible to construct a message which generates a given digest.**

With our example hashing algorithm, if given the digest of *52*, it would not be overly difficult to generate a list of words that might have been the original message. This is what this attribute is trying to prevent.

In a proper hashing algorithm, this should be infeasible — short of attempting every possible combination of messages until you found a match (aka, brute-forcing the algorithm). But even this becomes infeasible given a large enough digest size.

In the [next article](#) in this series, we will look at exactly *how* Hashing Algorithms are used to detect modified messages. But for now, we will continue to look at additional aspects of Hashing Algorithms.

## Digest Lengths

Below is a table with commonly seen, industry recognized hashing algorithms:

Algorithm	Digest Length
<a href="#">MD5</a>	128 Bits
<a href="#">SHA or SHA1</a>	160 Bits
<a href="#">SHA256</a>	256 Bits
<a href="#">SHA384</a>	384 Bits

Each of these Hashing algorithms satisfy the four cryptography hashing algorithm properties, as described above. The primary difference between each of them is the size of the resulting digest.

As with passwords, it is typically considered that a hashing algorithm which results in a longer digest tends to be regarded as more secure.

## Hashing Demonstration with Linux

To take it a step further, I would like to demonstrate how you can use a hashing algorithm from a standard Linux terminal. Note that if you are unfamiliar with Linux, feel free to skip this section — it is not crucial to learning the aforementioned concepts. If you have at least some Linux familiarity, however, it might help to see these algorithms in action.

The standard Linux terminal typically comes with at least two of the Hashing Algorithms mentioned above: MD5 and SHA1. You can use the `echo` command along with `md5sum` or `sha1sum` to run either algorithm on a string of text:

```
$ echo "Practical Networking .net" | md5sum  
018aa3ff55842e546c661b7027aed5d7 -
```

If you typed the exact same command into any Linux terminal, the resulting digest would be the exact same. In fact, if you fed the string `Practical Networking .net` into any MD5 algorithm, you would see the exact same digest (*remember, the `echo` command also appends a new line character to the string*). If we were to change something small, the resulting digest should be completely different. For example, we can capitalize the `n` in `.net` and take a look at how the digest changes:

```
$ echo "Practical Networking .Net" | md5sum  
6b9298494fb90a1a57efddae60fbfc1 -
```

We could also run a much larger sample of text through the MD5 algorithm. We can echo the same string 10,000 times and calculate the `md5sum`, and notice the resulting digest is still the same length (but the digest is different, of course):

```
$ for i in {1..10000}; do echo "Practical Networking.net"; done | md5sum  
938a98abd28c5da2dee6aa07bbc25134 -
```

Try these same examples using `sha1sum`. If you don't have easy access to a Linux shell, you can use a [free online Linux terminal](#).

# Message Integrity

In the world of secured communications, Message **Integrity** describes the concept of ensuring that **data has not been modified in transit**. This is typically accomplished with the use of a Hashing algorithm. We learned earlier [what a Hashing Algorithm does](#). Now we can take a look at how they are actually used to provide Message Integrity.

The basic premise is a sender wishes to send a message to a receiver, and wishes for the integrity of their message to be guaranteed. The sender will calculate a hash on the message, and include the digest with the message.

On the other side, the receiver will independently calculate the hash on *just* the message, and compare the resulting digest with the digest which was sent with the message. If they are the same, then the message must have been the same as when it was originally sent.

PRACTICAL NETWORKING .NET



Pretty straight forward. Except for one major problem. Can you guess what it is?

If someone intercepted the message, changed it, and recalculated the digest before sending it along its way, the receiver's hash calculation would also match the modified message. Preventing the receiver from knowing the message was modified in transit!

So how is this issue averted? By adding a Secret Key known only by the Sender and Receiver to the message before calculating the digest. In this context, the Secret Key can be any series of characters or numbers which are only known by the two parties in the conversation.

Before sending the message, the Sender combines the Message with a Secret key, and calculates the hash. The resulting digest and the message are then sent across the wire (*without the Secret!*).

The Receiver, also having the same Secret Key, receives the message, adds the Secret Key, and then re-calculates the hash. If the resulting digest matches the one sent with the message, then the Receiver knows two things:

1. The message was definitely not altered in transit.
2. The message was definitely sent by someone who had the Secret Key — ideally only the intended sender.

This animation reflects this process:

PRACTICAL NETWORKING .NET



When using a Secret Key in conjunction with a message to attain Message Integrity, the resulting digest is known as the **Message Authentication Code**, or **MAC**. There are many different methods for creating a MAC, each combining the secret key with the message in different ways. The most prevalent MAC in use today, and the one worth calling out specifically, is known as an **HMAC**, or [Hash-based Message Authentication Code](#).

Of course, this doesn't answer the question of "How did the Sender and Receiver establish mutual secret keys?" This is known as the Key Exchange problem, which comes up a few times in cryptography. However, the answer lies outside the scope of the concept of Integrity, and will be discussed in another article in this [series](#).

# Confidentiality

Confidentiality is the concept of hiding or scrambling your data so that only the intended recipient has access. This is typically accomplished by some means of **Encryption**.

Data before it has been encrypted is referred to as **Plain text**, or **Clear text**. After the data has been encrypted, it is referred to as **Cipher text**. The Cipher text should be completely unrecognizable, revealing no patterns or hints as to what the original Plain text was. Only the intended receiver(s) should have the ability to **Decrypt** the Cipher text and extract the original Plain text.

The process by which the Plain text is converted to Cipher text is known as the **Encryption Algorithm**.



In this basic encryption example, all that is needed to reverse the encryption and decrypt the Cipher text is insight into what happened in the Encryption Algorithm. You've probably picked up by now, that to take `hello` and scramble it to `lohel`, all I did was shift the letters forward twice. To undo this, you just need to shift the letters back twice.

There are, however, a few issues with this type of basic encryption:

- **It does not scale.** For each new person you wish to securely exchange data with, you would need to devise a new encryption algorithm. You wouldn't want the communication you had between you and your bank to be secured the same way as it was between you and your employer. How many different algorithms could you come up with before you were forced to reuse them?
- **Once the algorithm is discovered, the security is comprised for all time.** Everything that was secured with the compromised algorithm in the past is now fully decryptable. And everything that you might ever continue to secure with that algorithm in the future is now fully decryptable.

- **In the end, all you've done is obfuscate the data.** It may be enough to prevent a passerby from accidentally reading your Clear text, but it won't be enough to thwart a truly determined hacker.

As a result of these weaknesses, modern confidentiality makes use of what is sometimes referred to as **Cryptographic Encryption**. Which is **combining a publicly known encryption algorithm along with a secret key**.

The math behind the algorithm is publicly disclosed, which gives it the benefit of having been vetted by many mathematicians and cryptographers before any particular algorithm is accepted for common use.

The secret key can be a randomly generated set of characters — which makes it easy to produce. It is not difficult to use a different key for each entity you wish to speak securely with, even if the algorithm for each of these parties is the exact same. It is also not difficult to periodically regenerate the secret key, so even if a particular key becomes compromised, only a subset of your communication can be decoded.

There are two types of Cryptographic Encryption: **Symmetric Encryption** and **Asymmetric Encryption**. The main difference between the two types of encryption can be summarized as follows:

- Symmetric encryption – Encrypt and Decrypt using the *same* key.
- Asymmetric encryption – Encrypt and Decrypt using *two different* keys.

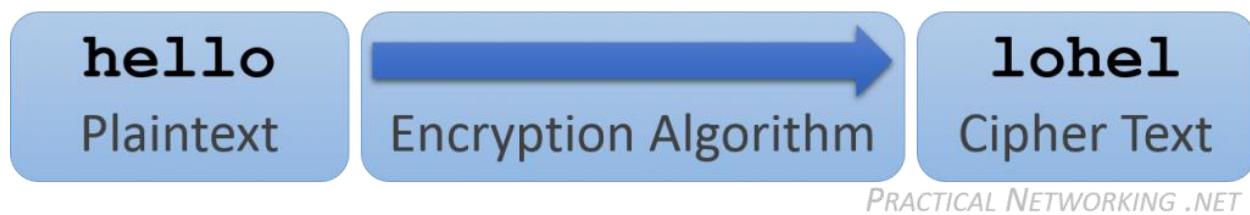
We will look at both of these and how they are used to provide Confidentiality in more detail in next articles in this series.

# Confidentiality

Confidentiality is the concept of hiding or scrambling your data so that only the intended recipient has access. This is typically accomplished by some means of **Encryption**.

Data before it has been encrypted is referred to as **Plain text**, or **Clear text**. After the data has been encrypted, it is referred to as **Cipher text**. The Cipher text should be completely unrecognizable, revealing no patterns or hints as to what the original Plain text was. Only the intended receiver(s) should have the ability to **Decrypt** the Cipher text and extract the original Plain text.

The process by which the Plain text is converted to Cipher text is known as the **Encryption Algorithm**.



In this basic encryption example, all that is needed to reverse the encryption and decrypt the Cipher text is insight into what happened in the Encryption Algorithm. You've probably picked up by now, that to take `hello` and scramble it to `lohel`, all I did was shift the letters forward twice. To undo this, you just need to shift the letters back twice.

There are, however, a few issues with this type of basic encryption:

- **It does not scale.** For each new person you wish to securely exchange data with, you would need to devise a new encryption algorithm. You wouldn't want the communication you had between you and your bank to be secured the same way as it was between you and your employer. How many different algorithms could you come up with before you were forced to reuse them?
- **Once the algorithm is discovered, the security is comprised for all time.** Everything that was secured with the compromised algorithm in the past is now fully decryptable. And everything that you might ever continue to secure with that algorithm in the future is now fully decryptable.

- **In the end, all you've done is obfuscate the data.** It may be enough to prevent a passerby from accidentally reading your Clear text, but it won't be enough to thwart a truly determined hacker.

As a result of these weaknesses, modern confidentiality makes use of what is sometimes referred to as **Cryptographic Encryption**. Which is **combining a publicly known encryption algorithm along with a secret key**.

The math behind the algorithm is publicly disclosed, which gives it the benefit of having been vetted by many mathematicians and cryptographers before any particular algorithm is accepted for common use.

The secret key can be a randomly generated set of characters — which makes it easy to produce. It is not difficult to use a different key for each entity you wish to speak securely with, even if the algorithm for each of these parties is the exact same. It is also not difficult to periodically regenerate the secret key, so even if a particular key becomes compromised, only a subset of your communication can be decoded.

There are two types of Cryptographic Encryption: **Symmetric Encryption** and **Asymmetric Encryption**. The main difference between the two types of encryption can be summarized as follows:

- Symmetric encryption – Encrypt and Decrypt using the *same* key.
- Asymmetric encryption – Encrypt and Decrypt using *two different* keys.

We will look at both of these and how they are used to provide Confidentiality in more detail in next articles in this series.

# Asymmetric Encryption

Earlier, we learned that Symmetric encryption is an encryption scheme that uses the same key to encrypt and decrypt. Conversely, **Asymmetric encryption**, uses different keys to encrypt and decrypt. Lets take a look at a simple example.

For the sake of simplicity, let us pretend for this example that there are only the lower case letters `a - z` available. No capitals, no numbers, no symbols. This would give us a total of 26 possible characters.



In the example above, we are taking the plain text of `hello`, and encrypting it with an Asymmetric encryption key of `5`. This results in our cipher text, `mjqqt`.

Instead of simply reversing the encryption, as you would for a Symmetric encryption, let us instead continue rotating the letters forward `21` more times:



Notice if we continue to move forward, with a Decryption key of `21`, we end up back where we started at the original plain text of `hello`.

Now obviously, in this simplistic example, we could have simply rotated backwards with the Encryption key of `5`. But in a real Asymmetric encryption algorithm, attempting to re-use the Encryption key (either forwards or backwards) would simply scramble the text further.

That said, there is something significant worth pointing out that we can learn from the Asymmetric encryption example above.

We used an Encryption key of 5, and were able to decrypt successfully with a Decryption key of 21. *BUT*, we could also have used an Encryption key of 21, and a successfully decrypted with a Decryption key of 5. The **Asymmetric keys are mathematically linked**. What one key encrypts, only the other can decrypt — and *vice versa*.

Can you determine another set of keys that would work as an Asymmetric key pair for the simple example above?

## A Tale of Two Keys

So what can we do with an Asymmetric Key Pair?

We discussed earlier the existence of the two keys — that they are mathematically linked, and that whatever data is encrypted by one of the keys can only be decrypted by the other key.



One of these keys is stored securely, and *never* shared with anyone else. This key is from then on referred to as the **Private Key**. In the rest of this series, this key will always be checkered, and point to the left.



The other key is made available to the world. This key then becomes your **Public Key**. In the rest of the series, this key will always be solid colored, and pointing to the right. The “key pair” will be identified by the matching color.

**Every participant in Asymmetric encryption has their own, unique key pair.** Each of these keys can be used in different ways in order to attain different security features. These will be outlined in a [dedicated article](#) in this series.

## Comparison with Symmetric Encryption

Understandably, the math involved in Asymmetric encryption is slightly more complex than what might be required with Symmetric encryption. As a result, the CPU cost of Asymmetric encryption tends to be higher than its symmetric counterpart.

Moreover, a side effect of the math is also that the resulting cipher text often ends up being larger than the original plain text. If you only intend to Asymmetrically encrypt a small amount of text, then this is negligible. But if you are looking to encrypt bulk data transfer, this makes Asymmetric encryption not ideal.

That said, the primary (and most significant) benefit to using Asymmetric encryption is **the Private Key never needs to be shared**. As opposed to Symmetric encryption, where the *same* Secret Key must exist on both sides of the conversation.

As a result, Asymmetric encryption is regarded as more secure than its symmetric counterpart. There is no risk of compromise while the key is being transferred (since it never needs to be transferred at all). There is no risk of compromise from the other party's potential lack of security (since the other party never has your Private key).

# Using Asymmetric Keys

We've established how Asymmetric encryption makes use of two mathematically linked keys: One referred to as the Public Key, and the other referred to as the Private Key. We've also established that what one key encrypts, only the other can decrypt.

These two attributes allow us to perform two separate operations with a Key Pair.

## Asymmetric Encryption

Below is an illustration of **Bob** (on the right in red) looking to send an encrypted message to **Alice** (on the left in purple).

Since **Bob** and **Alice** are two different entities, they each have their own set of Public and Private Keys. Their public keys are on the inside, available to each other. While their private keys are on the outside, hidden and out of reach.



PRACTICAL NETWORKING .NET

When Bob has a message he wishes to securely send to **Alice**, he will use **Alice's Public Key to Encrypt** the message. Bob will then send the encrypted message to Alice. **Alice will then use her Private Key to Decrypt** the message and extract the original message.

Since Bob encrypted the message with **Alice's Public key**, he knows that the only possible key that could extract the message is **Alice's Private key**. And since Alice never shared her key with anyone, Bob knows that only Alice was able to read the message.

Thus, the concept of confidentiality can be provided with an Asymmetric key pair.

## Asymmetric Message Signing

But confidentiality isn't the only thing you can do with a Public and Private Key. Remember, *either* key can be used for encryption. This fact can be used to give us one additional feature from an asymmetric key pair.

Let us imagine that now Alice wants to send a message to Bob. This time, however, Alice does not care about the [confidentiality](#) of her message. Which is to say, she doesn't care if anyone can read it. But she is very concerned that Bob knows beyond a shadow of a doubt that it was definitely Alice that sent the message.



PRACTICAL NETWORKING .NET

Alice can use **her own Private Key to encrypt the message**. Which makes it so the only key in the world that can decrypt her message is **her Public key** — which she knows Bob (and anyone else) has access to.

The message is sent to Bob, who then uses **Alice's Public Key to decrypt the message**. If Bob was able to successfully extract a message, and not a scrambled series of bits, then he can be assured that the message must have been originally encrypted by **Alice's Private Key**. And since Alice never shared her Private Key with anyone, Bob can be assured that Alice indeed sent the message.

This process is known as **Message Signing**. It is a creative use of the fact that the keys are mathematically linked, and that what one key encrypts, only the other can decrypt.

## Real World Usage

Now that we have illustrated the basic premise. We can take it a step further and really look at how these concepts are actually used in modern cryptography.

## Real World Encryption

Earlier, we discussed that Asymmetric encryption is slower and has properties which make it not ideal for bulk encryption. We should instead find a way to use Symmetric encryption, since it is better suited for bulk data encryption. But with Symmetric encryption, we have to deal with the Key Exchange issue.

The solution is to use what is sometimes referred to as **Hybrid encryption**, which **combines the strengths of both Symmetric and Asymmetric encryption**, while avoiding all their weaknesses.

Let's describe how that works by continuing to use Alice and Bob from above as an example.

Bob starts by randomly generating a **Symmetric Secret Key**. Then, instead of Bob using Alice's public key to encrypt the *message* directly, Bob uses **Alice's Public Key** to encrypt the **Symmetric Secret Key**. This encrypted symmetric key is sent across the wire to Alice.

Alice can then use **her Private Key** to extract the **Secret Key** that Bob sent. At this point, both parties now have an identical **Secret Key** that they can use to Symmetrically encrypt as much data as they please, in both directions.



PRACTICAL NETWORKING .NET

In this way, Bob and Alice use Asymmetric Keys to securely exchange a Symmetric Key, which is then used for Symmetric encryption. They are getting the security of Asymmetric encryption, with the speed and efficiency of Symmetric encryption — the best of both worlds.

## Real World Signatures

Similarly, the Message Signing process is more than simply using the Private Key to encrypt the message. Again, the limitations of Asymmetric encryption would end up imposing a limitation on what sort of data can be signed.

Can you guess what method is employed to reduce the message of variable length to a constant, more manageable representational value?

You guessed it... a [Hashing algorithm](#). Lets talk through it using Bob and Alice.

Alice wants to sign a message to Bob. She runs her message through a Hashing Algorithm, and then encrypts the resulting digest with her own Private Key. The encrypted digest then gets sent to Bob, along with the original message.

Bob then uses Alice's public key to decrypt the digest he received, then he independently calculates the hash of the original message. Bob then compares the (now decrypted) digest which was sent, and the digest which he calculated.

If they are the same, then Bob knows that Alice indeed must have sent the original message.

Moreover, Bob also knows that the message has not changed since Alice calculated the original digest — the signature had the bonus effect of also ensuring the [Integrity](#) of the original message!

## Math is Hard

Most people can wrap their mind around [Symmetric encryption](#) fairly easily. Take a starting value, perform some mathematical operation, and you end up with cipher text. To convert it back, you simply perform the operation in reverse.

But [Asymmetric encryption](#) is slightly more complicated. Without prior exposure to Asymmetric encryption, its difficult to imagine a mathematical operation that you can perform on a starting value that is *impossible* to reverse. Even if you know the Public Key and the Algorithm used.

To that end, we've added an article as an appendix to the [Cryptography series](#) which explores the math behind a widely used Asymmetric algorithm in use today.

If math causes your eyes to glaze over, feel free to skip it, so long as you understand the basic concepts described throughout this series. But if you are slightly curious about how an Asymmetric algorithm works, head on over to the post on the [RSA algorithm](#).

# Authentication

In Cryptography, the concept of **Authentication** serves to **provide proof that the other side of a communication is indeed who they claim to be**, and who you intend for them to be.

There are multiple ways to verify the opposing party's Authentication. We will look at three of the most common:

- Username and Password
- Pre-Shared-Key
- Digital Certificates

## Username and Password

Using a username and a password to identify who you are to a server is extremely common. Each user on a website can create a unique username, as well as a password tied specifically to that user. If the user is able to reproduce the password, then we can be assured that they are indeed the user they claim to be.

This is how most bank websites and email clients identify who you are.

The password itself should not be sent across the wire. That would easily lead to potential compromise. Instead, the password is run through some sort of hashing algorithm, and the resulting digest is then sent across the wire.

On the receiving end, it would be poor security practice to store the user's passwords directly. Instead, all that is stored is a hash of the password. Then, the digest sent with the user can be compared to the digest in the server's password database to see if they match. If they match, then the user must have had the expected password.

This is why most online websites that use a username and password are unable to recover lost passwords — all they can do is reset them. The password itself is never stored, only the digest of the password — which, as you recall, is impossible to reverse engineer and 'decrypt'.

Within this Authentication scheme, there are three different types of passwords that can exist:

- Something you *know*
- Something you *have*
- Something you *are*

### Something you *know*

This is the common password. You memorize a series of letters, special characters, words, and/or numbers, and you prove you *know* them when asked for the password.

This scheme is susceptible to users using weak passwords, storing them insecurely, or reusing them for different websites.

### Something you *have*

This requires you to reproduce a physical object that only you can have in order to validate you are who you say you are. An ATM card or an employee badge are examples.

Today, many websites will send a random code to your phone via SMS when you are trying to log in, forcing you to have possession of your phone to log in. In such a case, even though you are inputting the random code to prove you are who you say you are, the code's purpose is simply to validate that you *have* your phone.

This is also the same concept behind the [various authentication tokens](#) in use today. You carry it around, and when you need to identify yourself, you input the code on the token (which changes every 30-60 seconds). If you can put in the code the server is expecting, then you must have *had* the token.

Often, the code you input is further prefixed or suffixed with a password known only to you. This would then create a system that validates who you are with both something you *know* (the password), and something you *have* (the token).

### Something you *are*

Lastly, the various types of bio-metric identification fall under the category of something you *are*. Systems like fingerprint scanners or retina scanners or hand-print scanners all identify you based upon an attribute that is physically tied to who you *are*. Only you can have your hand. Only you can have your eyes. And so on.

Facial recognition, or even voice recognition, also falls under this category.

A password can be eavesdropped or shoulder-surfed. A token or mobile phone can be stolen. But bio-metrics can not be compromised without seriously maiming or killing the user being impersonated.

### Two-factor Authentication

Many websites or security services offer or require what is known as **Two-factor Authentication**. This means the user is being identified from a password scheme from *two different* categories above.

For instance, the example above of a random code sent to your phone via SMS and your regular username and password is a perfect example of Two-factor authentication. To successfully authenticate against such a system you would need to both *know* your password, as well as *have* your mobile phone.

If a website simply required you to enter two passwords, or a password and a pin, this would *not* qualify as two-factor authentication because both methods of authentication fall under *something you know*.

## Pre-Shared-Keys

The concept of Pre-Shared-Key authentication is to share a secret key or passphrase between two communicating nodes, then see if the two nodes can show proof of having said key.

This Pre-Shared-Key (PSK) should be shared out-of-band. For example, if you mean to use PSKs to prove someone's identity on the other side of the Internet, you should not use the Internet to share the key. You might use the phone, or a fax machine, or carrier pigeons.

Later on, if either node can show they have the correct PSK, it proves that the party on the other side of the wire is indeed the same entity which you initially exchanged the PSK with.

Obviously, simply sending the PSK across the wire to prove you have it would be a huge security flaw. We also can't simply run the PSK through a [hashing function](#) and send the resulting digest, because an eavesdropper could then capture the digest and spoof our identity in the future by reusing the same digest.

Instead, you would want to combine the PSK with values that are tied to that particular authentication session, so that the hash of the PSK is only good for *that one* session.

For example, in the case of IPsec, both parties generate and publicly exchange a random number. The PSK is then hashed together with both random numbers, and the resulting digest is shared. If both parties can generate the same digest, then they must have had the correct PSK. Furthermore, if an eavesdropper captures the verification digest and tries to reuse it to spoof the identify of one of the parties in a future session, they will be unable to because the future session will have different random numbers.

There are two primary differences between Pre-Shared-Key authentication and Username and Password authentication. The first: the PSK must be initially shared out-of-band. It can not be initially established using the medium upon which you want a secure connection. The second: the PSK is shared among two individuals, whereas a username and password is always unique to each user (or ought to be, at least).

## Digital Certificates

The final authentication scheme we are going to discuss is that of Digital Certificates. This is the primary method of identification in use on the Internet. The protocols securing your browsing session when visiting a webpage of HTTPS make heavy use of Digital Certificates (SSL/TLS).

A digital certificate works similar to a driver's license. It contains the identity of a particular individual or website, and it is issued by a governing entity (the state you live in).

Inside a digital certificate is a very important piece of information: a [Public Key of an Asymmetric Key Pair](#). This key is used to verify that the entity who presents the certificate is the true owner of the certificate. Much like your picture or signature on your driver's license.

Recall that with an Asymmetric Key pair, one key is kept private and never shared with anyone, and the other key is made public. Anyone can get a hold of anyone else's digital certificate (and therefore, public key), but theoretically,

only one person can exist with the correlating private key. Before accepting a digital certificate as proof of someone's identity, that someone must provide evidence that they are in possession of the matching private key.

There are two ways this can be verified. We'll take a look at an example of Alice presenting a Digital Certificate to Bob, and how she can provide evidence that she is in possession of the private key.

1. If Alice presents Bob with her Certificate, Bob can generate a random value and encrypt it with Alice's Public Key. Alice should be the only person with the correlating Private Key, and therefore, Alice should be the only person that can extract the random value. If she can then prove to Bob that she extracted the correct value, then Bob can be assured that Alice is indeed the true owner of the certificate.
2. Alice can encrypt a value known to both parties with her Private Key, and send the resulting Cipher Text to Bob. If Bob can decrypt it with Alice's Public Key, it proves Alice must have had the correlating Private Key.

These two methods are the basis for how authentication works with digital signatures.

# Anti-Replay

## The Problem

Before we can describe the solution, we must first adequately describe the problem Anti-Replay is trying to solve.

Imagine your local bank branch office. Imagine someone going to that branch location, and depositing \$100 in cash into their account. At some point following the transaction, that branch location will send some packets to the bank headquarters which essentially state to increase their account balance by \$100.

Those packets will cross the branch office's Internet Service Provider (ISP) network on their route to the Bank Headquarters. If a malicious user (or even the depositor themselves) happens to work at the ISP, it would not be overly difficult to capture the packets going from the Branch to the Headquarters that day, and by time reference, narrow down the particular packet(s) that make up the deposit's transaction.

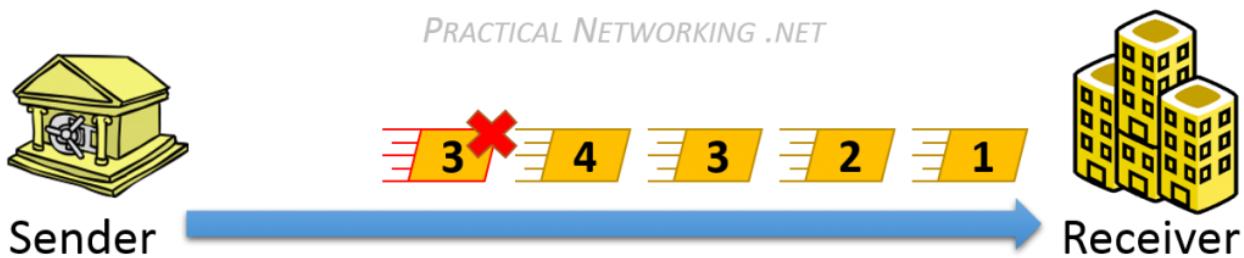
If the packets were protected by [Confidentiality](#), the malicious user would be prevented from reading into the data packet itself. If the packets were protected by an [Integrity](#) scheme, the malicious user would be unable to increase the deposit amount to \$1000 or \$10,000. But, despite those two protections, there would be nothing that would prevent the malicious user from simply duplicating those packets and putting them back on the wire in order to continually re-deposit \$100 over and over again.

...nothing if not for Anti-Replay protection, that is.

## The Solution

Anti-Replay protection exists specifically to thwart the scenario described above. Anti-Replay injects what is known as a **Sequence Number** into the data packet. This number typically starts at 1, and increases with every packet sent, uniquely identifying one packet from the one prior.

On the receiving end, the last Sequence Number received is tracked. If a packet with a repeated sequence number is ever received, it can be discarded and presumed to be a Replayed packet. Take this example:



Notice, the packet with Sequence Number #3 is a replayed packet. The receiver can easily detect this because they have already received a packet with Sequence Number #3, and was expecting #5 next.

The sequence number, along with the data, will be protected by some sort of [Message Integrity](#) scheme to prevent a malicious user from tampering with the numbers in order to send a replayed packet. The sequence number should be included in the [Hashing algorithm](#), along with the Message and the Secret Key. In this way, any illicit modification of any of these fields will be detected.

#### Sequence Number and Finite Fields

It is important to keep in mind that **the Sequence Number is a finite field**. Which is to say, it does not go on forever.

It has a pre-defined ranged based upon the number of bits allocated in the Data Packet. For example, if the data packet only allows a 16 bit field for the Sequence Number, you would have a total range of 1 – [65536](#).

It is important to consider this maximum so that it does not impose a limit on the number of packets that can be sent. Or worse, create a looped sequence number vulnerability when the sequence number rolls back to zero.

For example, using the banking transaction above, let us assume the packets only used a 16 bit Sequence Number field, and the captured packets included Sequence Numbers 10,000-10,099. The malicious user could simply wait for the Sequence number to loop past 65,536 and restart at 0, then count out 9,999 packets, and inject the replayed 10,000-10,099. Since the replayed packets would have arrived at the right time, they would have been accepted by the receiver.

This is addressed by forcing a [rotation of the Secret Keys](#) used in the Encryption and Integrity algorithms when the Sequence Number resets back to zero. This aids to ensure the continued, indefinite avoidance of replayed packets.

If an attacker attempts to replay a packet before the Sequence Number resets, then the repeated Sequence Number itself would identify the replayed packet. If an attacker attempts to replay a packet after the Sequence Number resets, then the *old packet* secured with the *old keys* will identify the packet was replayed.

# Rivest Shaman Adleman

The RSA algorithm is the most widely used [Asymmetric Encryption](#) algorithm deployed to date.

The acronym is derived from the last names of the three mathematicians who created it in 1977: Ron **Rivest**, Adi **Shamir**, Leonard **Adleman**.

In order to understand the algorithm, there are a few terms we have to define:

- **Prime** – A number is said to be Prime if it is only divisible by 1 and itself. Such as: 2, 3, 5, 7, 11, 13, etc.
- **Factor** – A factor is a number you can multiple to get another number. For example, the factors of 12 are 1, 2, 3, 4, 6, and 12.
- **Semi-Prime** – A number is Semi Prime if its only factors are prime (excluding 1 and itself). For example:  
**12** is *not* semi-prime — one of its factors is 6, which is not prime.  
**21** is semi-prime — the factors of 21 are 1, **3**, **7**, 21. If we exclude 1 and 21, we are left with 3 and 7, both of which are Prime.  
(Hint: Anytime you multiply two Prime numbers, the result is always Semi Prime)
- **Modulos** – This is a fancy way of simply asking for a [remainder](#). If presented with the problem  $12 \text{ MOD } 5$ , we simply are asking for the remainder when dividing 12 by 5, which results in 2.

With that out of the way, we can get into the algorithm itself.

## RSA Key Generation

The heart of Asymmetric Encryption lies in finding two mathematically linked values which can serve as our Public and Private keys. As such, the bulk of the work lies in the generation of such keys.

To acquire such keys, there are five steps:

### 1. Select two Prime Numbers: P and Q

This really is as easy as it sounds. Select two prime numbers to begin the key generation. For the purpose of our example, we will use the numbers 7 and 19, and we will refer to them as **P** and **Q**.

## 2. Calculate the Product: ( $P \times Q$ )

We then simply multiply our two prime numbers together to calculate the product:

$$7 \times 19 = 133$$

We will refer to this number as  $N$ . Bonus question: given the terminology we reviewed above, what kind of number is  $N$ ?

## 3. Calculate the Totient of $N$ : $(P-1) \times (Q-1)$

There is a lot of clever math that goes into both defining and acquiring a Totient. Most of which will be beyond the intended scope of this article. So for now, we will simply accept that the formula to attain the Totient on a Semi Prime number is to calculate the product of one subtracted from each of its two prime factors. Or more simply stated, to calculate the Totient of a Semi-Prime number, calculate  $P-1$  times  $Q-1$ .

Applied to our example, we would calculate:

$$(7-1) \times (19-1) = 6 \times 18 = 108$$

We will refer to this as **T** moving forward.

## 4. Select a Public Key

The Public Key is a value which must match three requirements:

- It must be Prime
- It must be less than the Totient
- It must NOT be a factor of the Totient

Let us see if we can get by with the number 3: 3 is indeed Prime, 3 is indeed less than 108, but regrettably 3 is a factor of 108, so we can not use it. Can you find another number that would work? Here is a hint, there are multiple values that would satisfy all three requirements.

For the sake of our example, we will select 29 as our **Public Key**, and we will refer to it as **E** going forward.

## 5. Select a Private Key

Finally, with what we have calculated so far, we can select our Private Key (which we will call **D**). The Private Key only has to match one requirement: The Product of the Public Key and the Private Key when divided by the Totient, must result in a remainder of 1. Or, to put it simply, the following formula must be true:

$$(D^E) \bmod N = 1$$

There are a few values that would work for the Private Key as well. But again, for the sake of our example, we will select 41. To test it against our formula, we could calculate:

$$(41^29) \bmod 133 = 1$$

We can use a calculator to validate the [result is indeed 1](#). Which means 41 will work as our Private Key.

And there you have it, we walked through each of these five steps and ended up with the following values:



Now we simply pick a value to be used as our Plaintext message, and we can see if Asymmetric encryption really works the way they say it does.

For our example, we will go ahead and use **99** as our Plaintext message.

*(the math gets pretty large at this point, if you are attempting to follow along, I suggest to use the [Linux Bash Calculator](#) utility)*

## Message Encryption

Using the keys we generated in the example above, we run through the Encryption process. Recall, that with Asymmetric Encryption, we are [encrypting with the Public Key, and decrypting with the Private Key](#).

The formula to Encrypt with RSA keys is:  $\text{cipher Text} = M^E \bmod N$

If we plug that into a calculator, we get:

$$99^{29} \bmod 133 = 92$$

The result of 92 is our Cipher Text. This is the value that would get sent across the wire, which only the owner of the correlating Private Key would be able to decrypt and extract the original message. Our key pair was 29 (public) and 41 (private). So lets see if we really can extract the original message, using our Private Key:

The formula to Decrypt with RSA keys is: Original Message =  $M^D \text{ MOD } N$

If we plug that into a calculator, we get:

$$92^{41} \text{ MOD } 133 = 99$$

As an experiment, go ahead and try plugging in the Public Key (29) into the Decryption formula and see if that gets you anything useful. You'll notice that, as was stated before, it is impossible to use the same key to both encrypt and decrypt.

## Message Signing

But remember, [that isn't all we can do with a key pair](#). We can also use same key pair in the opposite order in order to verify a message's signature.

To do this, we will use the same formulas as above, except this time we will reverse the use of the Public and Private Key. We're going to encrypt with the Private Key and see if we can decrypt with the Public Key.

We'll use the same formula to encrypt, except this time we will use the Private Key:

$$\text{Signature} = M^D \text{ MOD } N$$

If we plug that into a calculator, we get:

$$99^{41} \text{ MOD } 133 = 36$$

The result of 36 is the Signature of the message. If we can use the correlating public key to decrypt this and extract the original message, then we know that only whoever had the original Private Key could have generated a signature of 36.

Again, the same Decryption formula, except this time we will use the Public Key:

Original Message =  $M^E \text{ MOD } N$

If we plug that into a calculator, we get:

$$36^{29} \text{ MOD } 133 = 99$$

# Diffie-Hellman

NOVEMBER 4, 2015 by [ed harmoush](#) [6 comments](#)

This article is a part of a [series](#) on [Cryptography](#). Use the navigation boxes to view the rest of the articles.

## Cryptography

- [Hashing Algorithm](#)
- [Message Integrity](#)
- [Confidentiality](#)
- [Symmetric Encryption](#)
- [Asymmetric Encryption](#)
- [Using Asymmetric Keys](#)
- [Authentication](#)
- [Anti-Replay](#)
- [RSA Example](#)
- [Diffie-Hellman](#)

How can two people in a crowded room derive a secret that only the pair know, without revealing the secret to anyone else that might be listening?

That is exactly the scenario the Diffie-Hellman Key Exchange exists to solve.

The **Diffie-Hellman Key Exchange is a means for two parties to jointly establish a shared secret over an unsecure channel**, without having any prior knowledge of each other.

They never actually exchange the secret, just some values that both combine which let them attain the same resulting value.

Conceptually, the best way to visualize the Diffie-Hellman Key Exchange is with the ubiquitous [paint color mixing](#) demonstration. It is worth quickly reviewing it if you are unfamiliar with it.

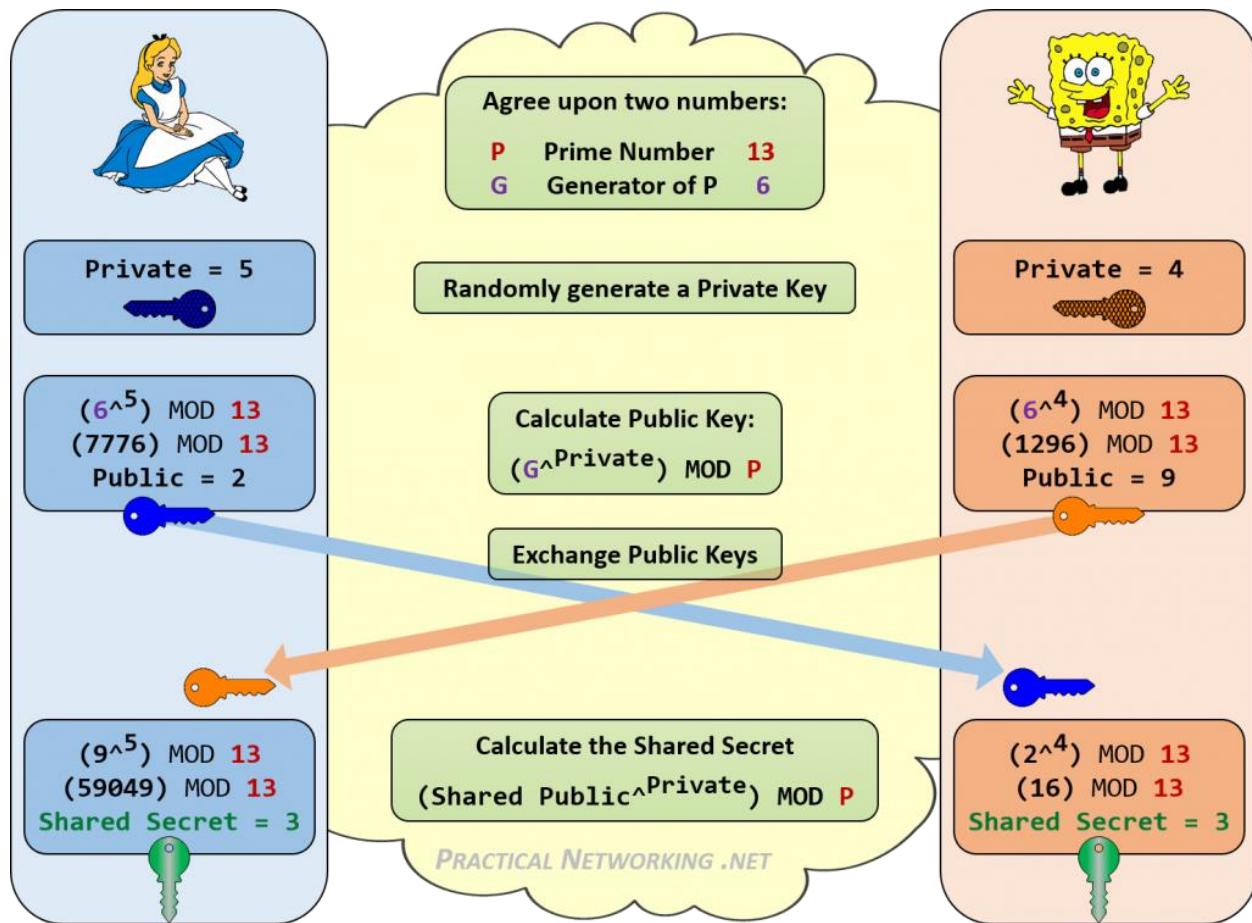
However, in this article we want to go a step further and actually show you the math in the Diffie-Hellman Key Exchange.

## DH Math

Before you get into the math of Diffie-Hellman, you will want to have a basic understanding of what a **Prime** number is, and what the **Modulus** operation is

(aka, remainder division). Both of these terms have been defined in [another article](#).

Below is an infographic outlining all the steps of the Diffie-Hellman exchange between Alice and Bob.



Notice how both Alice and Bob were able to attain the same Shared Secret of 3. Anyone listening in on their DH Key exchange would only know the Public Values, and the starting P and G values. There is no consistent way to combine those numbers (13, 6, 2, 9) to attain 3.

## DH Numbers

In our example, we used a Prime number of 13. Since this Prime number is also used as the Modulus for each calculation, the entire key space for the

resulting Shared Secret can only ever be 0-12. The bigger this number, the more difficult a time an attacker will have in brute forcing your shared secret.

Obviously, we were using very small numbers above to help keep the math relatively simple. True DH exchanges are doing math on numbers which are vastly larger. There are three typical sizes to the numbers in Diffie-Hellman:

---

DH Group 1      768 bits

---

DH Group 2      1024 bits

---

DH Group 5      1536 bits

The bit-size is a reference to the Prime number. This directly equates to the entire key space of the resulting Shared Secret. To give you an idea of just how large this key space is:

In order to fully write out a 768 bit number, you would need [232 decimal digits](#).  
In order to fully write out a 1024 bit number, you would need [309 decimal digits](#).

In order to fully write out a 1536 bit number, you would need [463 decimal digits](#).

## Using the Shared Secret

Once the Shared Secret has been attained, it typically becomes used in the calculation to establish a joint [Symmetric Encryption key](#) and/or a joint [HMAC Key](#) – also known as Session Keys.

But it is important to point out that the Shared Secret itself should not directly be used as the Secret Key. If it were, all you can be assured of is that throughout the secure conversation you are still speaking to the same party that was on the other side of the Diffie-Hellman exchange.

However, you still have no confirmation or assurance as to who the other party is. Just that no one else can all of a sudden pretend to be them in the middle of your secure conversation.

The generation of the actual Session Keys should include the DH Shared Secret, along with some other value that would only be known to the intended other party, like something from the Authentication scheme you chose.

Sources:

<https://www.practicalnetworking.net/series/cryptography/cryptography/>  
<https://www.practicalnetworking.net/series/cryptography/hashing-algorithm/>  
<https://www.practicalnetworking.net/series/cryptography/message-integrity/>  
<https://www.practicalnetworking.net/series/cryptography/confidentiality/>  
<https://www.practicalnetworking.net/series/cryptography/symmetric-encryption/>  
<https://www.practicalnetworking.net/series/cryptography/asymmetric-encryption/>  
<https://www.practicalnetworking.net/series/cryptography/using-asymmetric-keys/>  
<https://www.practicalnetworking.net/series/cryptography/authentication/>  
<https://www.practicalnetworking.net/series/cryptography/anti-replay/>  
<https://www.practicalnetworking.net/series/cryptography/rsa-example/>  
<https://www.practicalnetworking.net/series/cryptography/diffie-hellman/>

# Digital Certificate - Implementing SSL for your website

INFORMATION ASSURANCE AND SECURITY 1  
GODWIN S. MONSERATE

# What is a Digital Certificate?

---

- A **Digital Certificate** is an electronic "password" that allows a person, organization to exchange data securely over the Internet using the public key infrastructure (PKI).
- **Digital Certificate** is also known as a public key **certificate** or **identity certificate**.

# What is a Digital Certificate?

---

- A digital certificate (DC) is a digital file that certifies the identity of an individual or that certifies the identity of an individual or institution, or even a router seeking institution, or even a router seeking access to computer- based information.
- It access to computer- based information. It is issued by a Certification Authority, and serves the same purpose as a driver's and serves the same purpose as a driver's license or a passport

# What is a Digital Certificate?

---

- The Certification Authority (CA) signs the certificate with their own private key. An SSL/Digital Certificate typically contains the following information:
  - Owner's public key
  - Owner's name
  - Expiration date of the public key
  - Name of the issuer (the Certifying Authority that issued the Digital Certificate)
  - Serial number of the Digital Certificate
  - Digital signature of the issuer

# Certification Authorities

---

- CA's are the digital world's equivalent to passport offices.
- They issue digital equivalent to passport offices.
- They issue digital certificates and validate holders' and validate holders' identity and authority.
- They embed an individual or institution's public key along with other identifying information into each digital certificate and then cryptographically sign it as a tamper-proof seal verifying the integrity of the data within it and validating its use.

# What does it do?

---

- Digital Certificates can be used for a variety of electronic transactions including e-mail, electronic commerce, groupware and electronic funds transfers.
- If you are running an online e-commerce website, an electronic banking website or any other electronic services website then customers may abandon your website due to concerns about privacy and security.
- You will hence need to provide secure access to your website visitors via **https** protocol.
- To do this you will need to setup your website on a dedicated IP address and install a valid digital certificate on your hosting server.

# What does it do?

---

- Digital Certificates, bind an identity to a pair of electronic keys that can be used to encrypt and sign digital information.
- A Digital Certificate makes it possible to verify someone's claim that they have the right to use a given key, helping to prevent people from using phony keys to impersonate other users.
- Used in conjunction with encryption, Digital Certificates provide a more complete security solution, assuring the identity of all parties involved in a transaction.
- A digital certificate also is known as public key certificate allows exchanging data securely over the internet using public key infrastructure

# Sample Digital Certificate

Digital signature example email

casey.crane@sectigostore.com  
To casey.crane@sectigostore.com  
Signed By casey.crane@sectigostore.com

1:40 PM

**Digital Signature: Valid**

Subject: Digital signature example email  
From: casey.crane@sectigostore.com  
Signed By: casey.crane@sectigostore.com

The digital signature on this message is Valid and Trusted.

For more information about the certificate used to digitally sign the message, click Details.

Warn me about errors in digitally signed email before message opens.

**Message Security Properties**

Subject: Digital signature example email

Messages may contain encryption and digital signature layers. Each digital signature layer may contain multiple signatures.

**Security Layers**

Select a layer below to view its description.

- ✓ Subject: Digital signature example email
  - ✓ Digital Signature Layer
    - ✓ Signer: casey.crane@sectigostore.com

Description:

OK: Signed by casey.crane@sectigostore.com using RSA/SHA256 at 1:39:54 PM 6/19/2020.

Click any of the following buttons to view more information about or make changes to the selected layer:

Edit Trust... View Details... Trust Certificate Authority...

Warn me about errors in digitally signed email.

# Types of Digital Certificates

---

- There are 4 main types of Digital Certificates
  1. Server Certificates or /TLS/SSL Certificate
  2. Personal Certificates
  3. Organizational Certificates or Client Certificate
  4. Developer's Certificates or Code Signing Certificate

# Types of Digital Certificates

---

- Server Certificates
  - Allows visitors to exchange personal information such as credit card numbers, free from the threat of interception or tampering.
  - Server Certificates are a must for building and designing e-commerce sites as confidential information is shared between clients, customers and vendors.
  - TLS/SSL (Transport Layer Security/Secure Socket Layer) Certificates are installed on the server. The purpose of these certificates is to ensure that all communication between the client and the server is private and encrypted.
  - The server could be a web server, app server, mail server, LDAP server, or any other type of server that requires authentication to send or receive encrypted information. The address of a website with a TLS/SSL certificate will start with “<https://>” instead of “<http://>”, where the “s” stands for “secure.”

# Types of Digital Certificates

---

- Personal Certificates
  - Personal Certificates allow one to authenticate a visitor's identity and restrict access to specified content to particular visitors.
  - Personal Certificates are perfect for business to business communications such as offering suppliers and partners controlled access to special web sites for updating product availability, shipping dates and inventory management.

# Types of Digital Certificates

---

- Organization Certificates
  - are used by corporate entities to identify employees for secure e-mail and web-based transaction.
  - Client Certificates or Digital IDs are used to identify one user to another, a user to a machine, or a machine to another machine.
  - One common example is emails, where the sender digitally signs the communication, and the recipient verifies the signature.
  - Client certificates authenticate the sender and the recipient.
  - Client certificates also take the form of two-factor authentication when the user needs to access a protected database or arrives at the gateway to a payment portal, where they'll be expected to enter their passwords and be subjected to further verification.

# Types of Digital Certificates

---

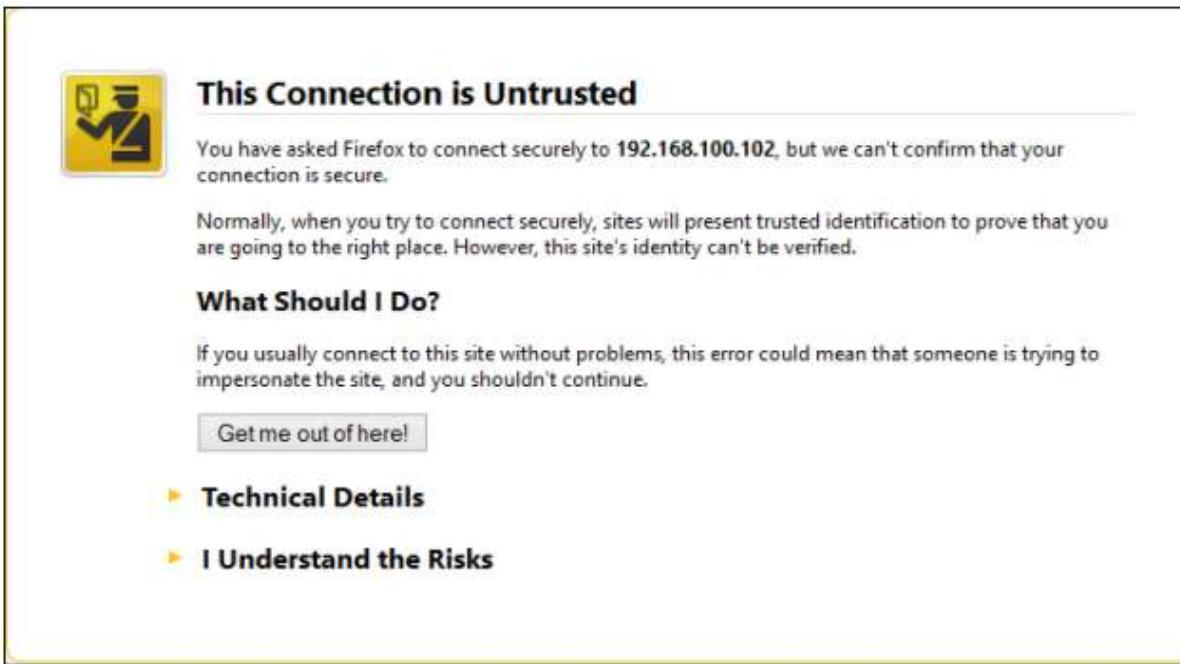
- Developer Certificates
  - Prove authorship and retain integrity of distributed software programs e.g. installing a software on a computer system in most instances requires what is called a “serial key”
  - Used to sign software or files that are downloaded over the internet. They’re signed by the developer/publisher of the software.
  - Their purpose is to guarantee that the software or file is genuine and comes from the publisher it claims to belong. They’re especially useful for publishers who distribute their software for download through third-party sites. Code signing certificates also act as a proof that the file hasn’t been tampered with since download.

# Signed vs Self-signed certificates

---

- In theory, certificate authorities are supposed to exercise due diligence before signing digital certificates submitted to them through Certificate Signing Request or CSRs.
- They need to verify first whether the information placed on the digital certificates are in fact true. This is important because their attestation would later on serve as the sole basis that certain websites who are able to present certs signed by them can really be trusted.
- It would be safe to assume that signed certificates are more reliable and trustworthy than self-signed certificates. In fact, when a user attempts to connect to your site and your site only has a self-signed certificate, the user's browser will display something like this:

# Signed vs Self-signed certificates



The screenshot shows a Firefox browser window displaying a security warning. The title bar says "This Connection is Untrusted". The main content area has a yellow warning icon on the left. The text reads: "You have asked Firefox to connect securely to 192.168.100.102, but we can't confirm that your connection is secure. Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified." Below this, under "What Should I Do?", it says: "If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue." There are two buttons: "Get me out of here!" and "I Understand the Risks". Additionally, there are two links: "Technical Details" and "I Understand the Risks".

- Self-signed certificates are relatively safe to use internally, i.e., within your organization, where you have more control over the servers that operate in the network.
- So, for instance, you can use it to add security to a **web file transfer** that takes place behind your corporate firewall.

# Implementing SSL in Website

---

# What is an SSL?

---

- SSL stands for **Secure Sockets Layer**, a now-deprecated cryptographic protocol that has kept only its name in common use. All SSL certificates are technically TLS certificates, TLS being the successor of the SSL technology.
- TLS or **Transport Layer Security** is a more advanced and secure protocol, that's been now the standard encryption technology for more than a decade.

# What is an SSL Certificate

---

- **SSL Certificate** is a digitally signed Certificate which is built of complex hashing functions and algorithm that keeps user's information encrypted during the data transmission form Client to Server and server to client.
- So, here both term SSL Certificate and Digital Certificate comes up different meaning and definition.

# What is an SSL Certificate

---

- Also known as **SSL Certificate** is a digitally signed certification by an established authority to confirm the identity of your website/business and uses encryption to send/receive data between your website and its visitors.
- SSL certificate authenticates the connection between web server and browsers by encrypting communication between the website and its users.
- It is issued for a domain by a trusted authority referred as Certificate Authority (CA). Example CAs are Comodo and Thawte.

# What does it do?

---

- An SSL certificate allows you to establish your credentials when doing business or other transactions on the Web.
- It is generally used when a website wants to accept sensitive information like passwords, credit card details and other sensitive information.
- The SSL Certificate protects your customer's personal data including passwords, credit cards and identity information. Thus, getting an SSL certificate for your website is the easiest way to increase your customer's confidence in your online business.

# When do you require an SSL/Digital Certificate?

---

- An SSL Certificate does 2 things:
  - a. Encrypt the information sent from your website visitor's browser to your website
  - b. Authenticate your website's identity.
- By doing these 2 things, an SSL Certificate protects your customers and in turn increases their trust in your online business.
- This is especially important if your website requires users to login using passwords or enter sensitive information such as credit card details.
- Many customers actively look for the SSL lock icon before handing over sensitive data.

# How do you know you have a digital certificate?

- If you come across a website whose URL begins with **https://**, you can view the website's SSL Certificate by clicking on the lock icon in the address bar of your browser.



# Types of SSL Certificates

---

- Certifying authorities provide SSL certificates in a few variety of branded names, each serving a specific purpose.
- For example, Comodo sells a basic SSL certificate in the name of *Positive SSL* while Thawte sells an equivalent certificate named as *SSL 123 Certificate*.
- Likewise, a wildcard SSL certificate is named as *Positive SSL Wildcard* by Comodo and *Wildcard Server Certificate* by Thawte.

# Types of SSL Certificates

---

- Broadly there are two types of SSL certificates:
  1. **Basic SSL certificate:** allows you to secure one sub-domain. For example, if your e-commerce website is store.yourwebsitename.com, a basic SSL will secure only this sub domain and hence people will be able to access your website as https://store.yourwebsitename.com. If you want to also secure www.yourwebsitename.com, you may need to purchase a second separate certificate for this second sub-domain. A basic SSL certificate is quite well suited for small websites and blogs.
  2. **Wildcard SSL certificate:** allows you to secure your primary domain name as well as all its sub-domains. Thus one certificate will secure both www.yourwebsitename.com and store.yourwebsitename.com, and any other sub domains such as support.yourwebsitename.com, webmail.yourwebsitename.com, etc. A Wildcard SSL is best suited for large e-commerce websites.

# How to get an SSL Certificate for your website?

---

- To be issued an SSL Certificate, you need to purchase one from a web service provider and then go through a process that entails the following:
- **Step 1: Purchasing SSL**
  - As a first step you place an order for an ssl certificate with the web service provider. While placing order, you will need to specify the exact domain name for which you require the ssl certificate.
  - For example, if you need to secure store.yourwebsitename.com, you should specify store.yourwebsitename.com while placing order and not www.yourwebsitename.com.
  - Once your order has been executed by the service provider, you will be provided with a control panel from where you can apply for your certificate.

# How to get an SSL Certificate for your website?

---

- **Step 2: Private Key and CSR Generation**
  - Prior to applying/enrolling for a Certificate with the CA, you must generate a minimum of 2048-bit Private Key and CSR pair from your hosting server.
  - Digital IDs make use of a technology called *Public Key Cryptography*, which uses Public and Private Key files.
  - The *Public Key*, also known as a *Certificate Signature Request (CSR)*, is the key that will be sent to the CA.
  - The Public Key is generated on your server and validates the computer-specific information about your web server and Organization when you request a Certificate from a CA.

# How to get an SSL Certificate for your website?

---

- **Step 2: Private Key and CSR Generation**
  - The *Private Key* will remain on your hosting server and should never be released into the public. Even the Certifying Authority will *not* have access to your Private Key.
  - It is generated locally on your server and is *never* transmitted to the CA or any browser visiting your website. The integrity of your Digital ID depends on your Private Key being controlled exclusively by you.
  - A CSR *cannot* be generated without generating a Private Key file. Similarly the Private Key file *cannot* be generated without generating a CSR file.
  - In certain web server software platforms like Microsoft IIS, both are generated simultaneously through the Wizard on the web server.

# How to get an SSL Certificate for your website?

---

- **Step 2: Private Key and CSR Generation**
  - Most hosting service providers provide you with a hosting management control panel which has an *SSL/TLS Manager* interface using which you can generate your CSR - private key pair.
  - You will be required to enter certain relevant details about your organization while generating the CSR.
  - On completion of this process, your hosting server will generate an encoded file, viz. your CSR. This CSR can now be used to submit your SSL Certificate application to the Certificate Authority.

# How to get an SSL Certificate for your website?

---

- **Step 3: Enrollment**
  - After you have generated a minimum of 2048-bit Private Key and CSR pair from your web hosting server, the next step is to submit your Enrollment information to the CA for the CA to verify your information and issue the Digital certificate to you.
  - The enrollment is done from the interface that the web service provider will provide to you after you have purchased the SSL certificate.

# How to get an SSL Certificate for your website?

---

- **Step 3: Enrollment**
  - Enrollment essentially requires you to submit a form wherein you provide relevant details about your organization such as Organization name, Contact details, Admin email address, Approver Email Address, etc.
  - The contact details that you provide here must match with the ones available in your domain's whois lookup.
  - Also, you must ensure that prior to enrollment, your domain is not privacy protected and that it's whois information is publicly visible.
  - Subsequently, after the certificate is issued to you, you may re-enable your domain's privacy protection.

# How to get an SSL Certificate for your website?

---

- **Step 4: Verification Process & Certificate Issue**
  - After you have submitted the enrollment form, the Certifying Authority will now carry out a verification of your organization and the information you have submitted. If required, they may call you at your specified phone number for additional verification of your business.
  - This process is much faster and usually automatic when you apply for a basic ssl certificate. Subsequently, after the CA is satisfied with the verification, you will receive an email from the CA to approve the issue of ssl certificate.
  - After you have done the approval, you will receive an email from the CA informing you that your certificate has been issued. The email will also contain information on how you can retrieve the issued certificate.

# How to get an SSL Certificate for your website?

- Image shows how your issued ssl certificate will look:

-----BEGIN CERTIFICATE-----

```
MIIFSjCCBDKgAwIBAgIQFlfpO4e21iGqtPdVpJhgyTANBgkqhkiG9w0BAQsFADCBK  
DELMAkGA1UEBhMCR0IxGzAZBgNVBAgTEkdyZWF0ZXIgTWFlY2hlc3RlcjEQMA4  
GA1UEBxMHU2FsZm9yZDEaMBgGA1UEChMRQ09NT0RPIENBIExpbWI0ZWQxNj  
A0BgNVBAMTLUNPTU9ETyBSU0EgRG9tYWIuFZhbGIKYXRpb24gU2VjdXJlFNlcn  
ZlciBDQTAefw0xNDEyMjYwMDAwMDBaFw0xNTEyMjYyMzU5NTlaMFAxITAfBgnVB  
AsTGERvbWFnbiBDB250cm9sIzZhbGIKYXRIZDETMBEGA1UECxMKQ09NT0RPIF  
NTTDEWMBQGA1UEAxMNY2hIY2tydWtpLmNvbTCCASlwDQYJKoZIhvcNAQEBBQ  
ADggEPADCCAQoCggEBAMLSmJbGejxsYtsbB38B6IdhLg7oig1UYB6e4JasxAQ+  
2RJrrLDZC96VH/ZAVQtIvgn688P2/3YV39v74fE07nT1bqvSxy9YoExJ+XcgIhM60w  
GjFy6qCFbHUHxXlxD08aAM9HR+jw+qM9N94ggFlzP2IKhFYfVOPy94du74+K9Jh  
HuuyiJrCo6gwyuOO7wQgwDFF68XZCMFF1KTuRXZI/22KuyysjvAIRUnMfae8TkKx1  
UlVDBga84ImDMAzjDzZy9c6rLaJf1sJG5xYztdAcfxGXduah8IDf1w8IudEXIGS2mq/  
HWWQ1jbBZY+NkUuyql0I9Rr9+nAYxb7AsCAwEAAoOCAd0wgghZMB8GA1Udlw  
QYMBaAFJCvajqUWgyYkOoSvnpfQ7Q6KNrnMB0GA1UdDgQWBFRhyEKEP+A1  
7ts7xofRSogFFwTNDAOBgNVHQ8BAf8EBAMCBaAwDAYDVR0TAQH/BAIwADAdB  
gNVHSUEFjAUBgrgBgfBQcDAQYIKwYBBQUHawIwTwYDVR0gBEgwRJA6BgsRB  
gEEAbIxAQICBzArMCKGCCsGAQUFBwIBFh1odHRwczovL3NIY3VzS5jb21vZG8u  
Y29tL0NQUzAlBgZngQwBAgEwWAYDVR0fBE0wSzBjoEegRYZDaHR0cDovL2NyB  
C5jb21vZG9jY85jb20vQ09NT0RPUINBRG9tYWIuVmFsawRhdGlvbINIY3VzVNlc  
nZlickNBmNybDCBhQYIKwYBBQUHAQEeTB3ME8GCCsGAQUFBzACHkNodHRwO  
i8vY3J0LmNvbW9kb2NhLmNvbS9DT01PRE9SU0FEb21haW5WYwpZGF0  
aW9uU2VjdXJIU2VydmlvQ0EuY3J0MCQGCCsGAQUFBzABhhodHRwO18vb2Nz  
cC5jb21vZG9jY85jb20wKwYDVR0RBCQwloINY2hIY2tydWtpLmNvbYIRd3d3LmN  
oZWNrcnVraS5jb20wDQYJKoZIhvcNAQELBQADggEBAENwx+m50sywf1OBGliA+  
hTxFAYftejh0+IPyUqhcvfVpDx10WIHTzBweyqmjqYIIEGxnhq5ctrX4r2LPs3OMMu  
zy74iyRHgFfc4ipC23YrLdLy0Mq9tPiTyizhyDvF0mbGJ/dR9sQIQDGEEPvuJ7u9iRN  
44E2DDNI2dC1dndpU6zHSpf0aEnqgynAbpehOD2nCE4VuZbyL9i/m+v+Wduu+E  
voGCpBy9qISBI5vGon/0k6Ko2tlI7nnSSYpyf9rJKQ2U/EICeZyTM4VHHBpOskGf2  
5C9heY7LiowTdr5RnyWQJ0LOMew/w28KS3ebDpMU+HECAENqCnAD8Xi/s=
```

-----END CERTIFICATE-----

# How to get an SSL Certificate for your website?

---

- **Step 5: Certificate Installation**
- This is the final step wherein you need to install the issued certificate on your hosting server.
- Additionally, you will also need to install the SSL Certificate of the Certificate Authority (known as the CA bundle).
- The CA bundle contains root and intermediate certificates of the CA and is available for download from the website of the CA.
- Depending upon the web server where you intend to install your SSL Certificate, you need to refer to the appropriate instructions provided by your hosting service provider.
- Once successfully installed, your website will become accessible via **https://....**

# Difference between Digital Certificate and SSL Certificate

---

- **Digital Certificate:**
  - A Digital Certificate is a digital "password" which permits an individual, organization to exchange information securely across the Web utilizing the public key infrastructure (PKI).
  - Digital Certificate can be referred to as a public key certification or identity certification.
- **SSL Certificate:**
  - SSL Certificates are small data files which bind a cryptographic key to a company's particulars. Once installed on an internet server, then it activates the padlock along with the https protocol also enables safe connections from a web server to a browser.
  - Normally, SSL is used to secure credit card transactions, information transport and logins, and much more lately has become the standard when procuring browsing of social networking websites.

# Digital Signatures and Certificates

**Encryption** – Process of converting electronic data into another form, called cipher text, which cannot be easily understood by anyone except the authorized parties. This assures data security.

**Decryption**– Process of translating code to data.

- Message is encrypted at the sender's side using various encryption algorithms and decrypted at the receiver's end with the help of the decryption algorithms.
- When some message is to be kept secure like username, password, etc., encryption and decryption techniques are used to assure data security.

## Types of Encryption

1. **Symmetric Encryption**– Data is encrypted using a key and the decryption is also done using the same key.
2. **Asymmetric Encryption**-Asymmetric Cryptography is also known as public key cryptography. It uses public and private keys to encrypt and decrypt data. One key in the pair which can be shared with everyone is called the public key. The other key in the pair which is kept secret and is only known by the owner is called the private key. Either of the keys can be used to encrypt a message; the opposite key from the one used to encrypt the message is used for decryption.

**Public key**– Key which is known to everyone. Ex-public key of A is 7, this information is known to everyone.

**Private key**– Key which is only known to the person who's private key it is.  
**Authentication**-Authentication is any process by which a system verifies the identity of a user who wishes to access it.

**Non-repudiation**– Non-repudiation means to ensure that a transferred message has been sent and received by the parties claiming to have sent and received the message. Non-repudiation is a way to guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message.

**Integrity**– to ensure that the message was not altered during the transmission.  
**Message digest** -The representation of text in the form of a single string of digits, created using a formula called a one way hash function. Encrypting a message digest with a private key creates a digital signature which is an electronic means of authentication..

## Digital Signature

A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software or digital document.

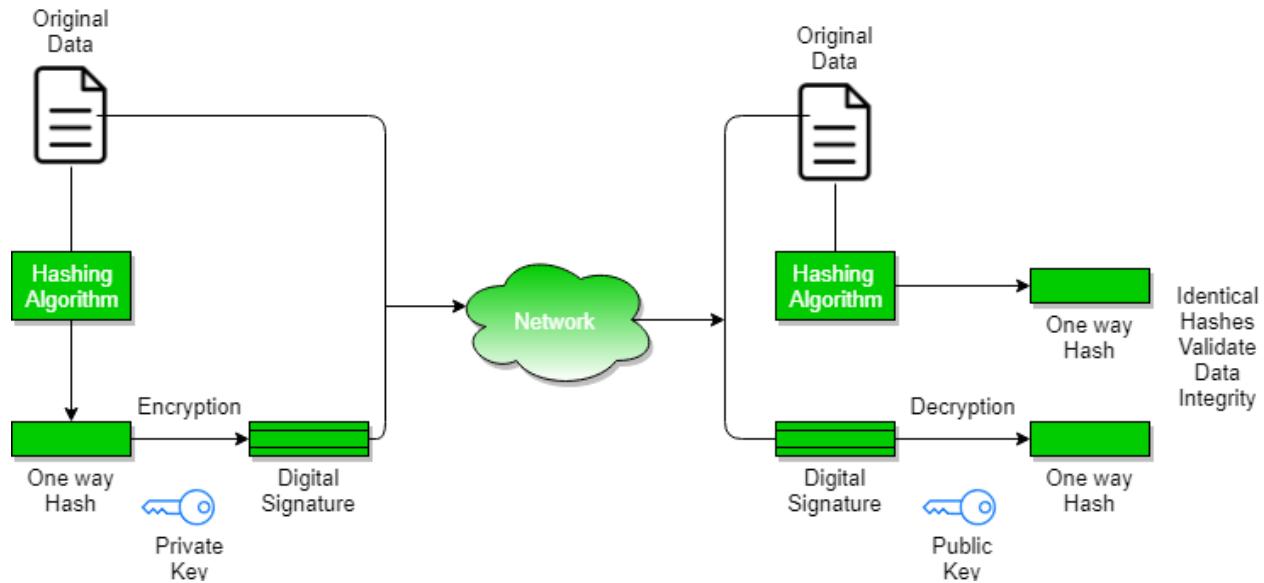
1. **Key Generation Algorithms :** Digital signature are electronic signatures, which assures that the message was sent by a particular sender. While performing digital transactions authenticity and integrity should be assured, otherwise the data can be altered or someone can also act as if he was the sender and expect a reply.
2. **Signing Algorithms:** To create a digital signature, signing algorithms like email programs create a one-way hash of the electronic data which is to be signed. The signing algorithm then encrypts the hash value using the private key (signature key). This encrypted hash along with other information like the hashing algorithm is the digital signature. This digital signature is appended with the data and sent to the verifier. The reason for encrypting the hash instead of the entire message or document is that a hash function converts any arbitrary input into a much shorter fixed length value. This saves time as now instead of signing a long message a shorter hash value has to be signed and moreover hashing is much faster than signing.
3. **Signature Verification Algorithms :** Verifier receives Digital Signature along with the data. It then uses Verification algorithm to process on the digital signature and the public key (verification key) and generates some value. It also applies the same hash function on the received data and generates a hash value. Then the hash value and the output of the verification algorithm are compared. If they both are equal, then the digital signature is valid else it is invalid.

**The steps followed in creating digital signature are :**

1. Message digest is computed by applying hash function on the message and then message digest is encrypted using private key of sender to form the digital signature. (digital signature = encryption (private key of sender, message digest) and message digest = message digest algorithm(message)).
2. Digital signature is then transmitted with the message.(message + digital signature is transmitted)
3. Receiver decrypts the digital signature using the public key of sender.(This assures authenticity, as only sender has his private key so only sender can encrypt using his private key which can thus be decrypted by sender's public key).
4. The receiver now has the message digest.
5. The receiver can compute the message digest from the message (actual message is sent with the digital signature).

The message digest computed by receiver and the message digest (got by decryption on digital signature) need to be same for ensuring integrity.

Message digest is computed using one-way hash function, i.e. a hash function in which computation of hash value of a message is easy but computation of the message from hash value of the message is very difficult.



## Digital Certificate

Digital certificate is issued by a trusted third party which proves sender's identity to the receiver and receiver's identity to the sender.

A digital certificate is a certificate issued by a Certificate Authority (CA) to verify the identity of the certificate holder. The CA issues an encrypted digital certificate containing the applicant's public key and a variety of other identification information. Digital certificate is used to attach public key with a particular individual or an entity.

### Digital certificate contains:

1. Name of certificate holder.
2. Serial number which is used to uniquely identify a certificate, the individual or the entity identified by the certificate
3. Expiration dates.
4. Copy of certificate holder's public key. (used for decrypting messages and digital signatures)
5. Digital Signature of the certificate issuing authority.

Digital certificate is also sent with the digital signature and the message.

### **Digital certificate vs digital signature :**

Digital signature is used to verify authenticity, integrity, non-repudiation ,i.e. it is assuring that the message is sent by the known user and not modified, while digital certificate is used to verify the identity of the user, maybe sender or receiver. Thus, digital signature and certificate are different kind of things but both are used for security. Most websites use digital certificate to enhance trust of their users.

<b>Feature</b>	<b>Digital Signature</b>	<b>Digital Certificate</b>
Basics / Definition	Digital signature is like a fingerprint or an attachment to a digital document that ensures its authenticity and integrity.	Digital certificate is a file that ensures holder's identity and provides security.
Process / Steps	Hashed value of original message is encrypted with sender's secret key to generate the digital signature.	It is generated by CA (Certifying Authority) that involves four steps: Key Generation, Registration, Verification, Creation.
Security Services	<b>Authenticity of Sender, integrity of the document and non-repudiation.</b>	It provides security and <b>authenticity</b> of certificate holder.
Standard	It follows Digital Signature Standard (DSS).	It follows X.509 Standard Format

Source:

<https://www.geeksforgeeks.org/digital-signatures-certificates/>

# Introduction to Digital Certificates

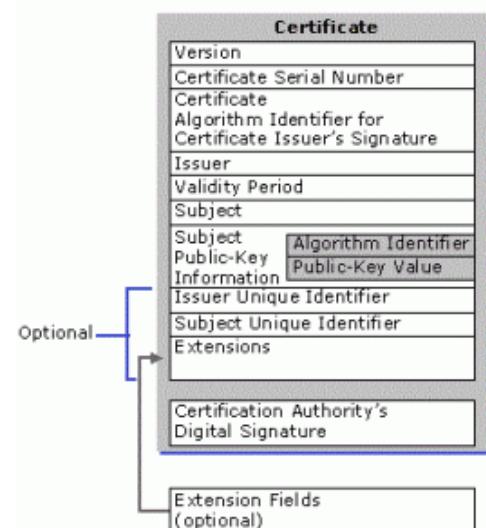
## What is a digital certificate?

A digital signature or ID is more commonly known as a digital certificate. To digitally sign an Office document, you must have a current (not expired) digital certificate. Digital certificates are typically issued by a certificate authority (CA), which is a trusted third-party entity that issues digital certificates for use by other parties. There are many commercial third-party certificate authorities from which you can either purchase a digital certificate or obtain a free digital certificate. Many institutions, governments, and corporations can also issue their own certificates.

A digital certificate is necessary for a digital signature because it provides the public key that can be used to validate the private key that is associated with a digital signature. Digital certificates make it possible for digital signatures to be used as a way to authenticate digital information.

Digital certificates function similarly to identification cards such as passports and drivers' licenses. Digital certificates are issued by recognized (government) authorities. When someone requests a certificate, the authority verifies the identity of the requester, certifies that the requester meets all requirements to receive the certificate, and then issues it. When a digital certificate is presented to others, they can verify the identity of its owner because the certificate provides the following security benefits:

- It contains personal information to help identify and trace the owner.
- It contains the information that is required to identify and contact the issuing authority.
- It is designed to be tamper-resistant and difficult to counterfeit.
- It is issued by an authority that can revoke the identification card at any time (for example, if the card is misused or stolen).
- It can be checked for revocation by contacting the issuing authority.



A digital certificate is necessary for a digital signature because it provides the public key that can be used to validate the private key that is associated with a digital signature. Digital certificates make it possible for digital signatures to be used as a way to authenticate digital information.

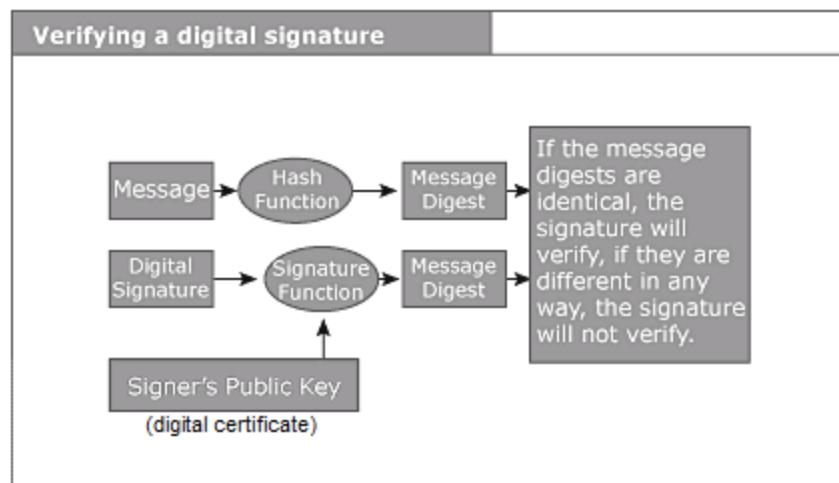
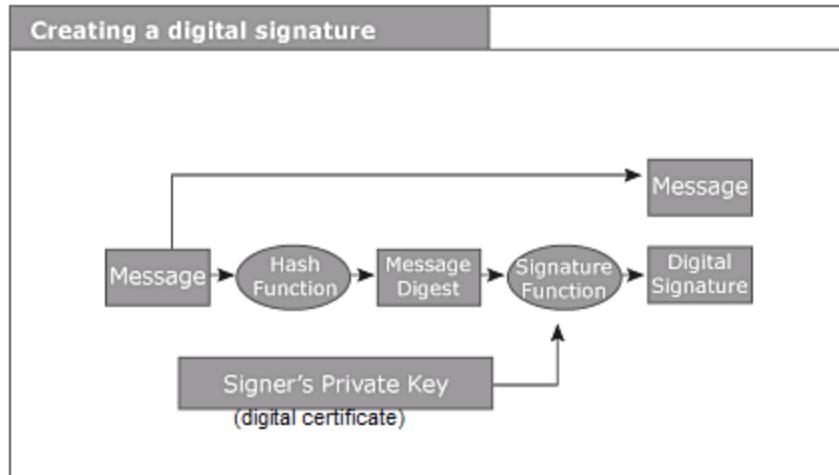
## Example of a Digital Certificate



## The use of a digital certificate to sign documents

When the signer uses a certificate to digitally sign a document, other people (known as relying parties) can trust the digital signature because they trust the CA has done their part to ensure the signer matches their digital identity.

So, technically speaking the difference between a digital signature and digital certificate is that a certificate binds a digital signature to an entity, whereas a digital signature is to ensure that a data/information remain secure from the point it was issued. In other words: digital certificates are used to verify the trustworthiness of a person (sender), while digital signatures are used to verify the trustworthiness of the data being sent.



Creating a digital signature using digital certificates (private key)

### The difference between a digital signature and digital certificate

Digital business with digital *trust*A digital signature and a digital certificate, while both security measures, are different in the ways they are implemented and the background why they are implemented for. The technology industry loves to use acronyms and words that seem to either overlap with other similar words, or that are a slight variation on a word, but with widely different meanings. To understand more, these are the comparison Between Digital Signature vs Digital Certificate (Infographics)

## Digital Signature



It verifies the identity of the document.

## Digital Certificate



It verifies the identity of the ownership of an online medium.

## Digital Signature



It is issued to a specific individual by an authorized agency.

## Digital Certificate



It is issued after the background check of the applicant by the Certificate Authority(CA).

## Digital Signature



It ensures that the signer cannot non-repudiate the signed document.

## Digital Certificate



It ensures that two parties who are exchanging the information are secured.

## Digital Signature



It works on DSS (Digital Signature Standard).

## Digital Certificate



It works on the principles of public-key cryptography standards.

## Digital Signature



The digital signature uses a mathematical function (Hashing function).

## Digital Certificate



It contains personal information to help in identifying the trace of the owner.

## Digital Signature



It is widely used for avoiding forging the document.

## Digital Certificate



It is used in an online transaction for the trustworthiness of the data and the sender.

## Digital Signature



It is an attachment to a document that can be viewed as a signature.

## Digital Certificate



It is a medium to prove the holder's identity for a particular transaction.

## Digital Signature



It ensures the sender and the receiver have the same document containing the same data.

## Digital Certificate



It builds the trust between the user and the business (Certificate holder).

## Digital Signature



It is created using SHA-1 or SHA-2 algorithms.

## Digital Certificate



It is created in the X.509 format.

## Digital Signature



It uses the RSA algorithm if there is a need for message encryption.

## Digital Certificate



It encrypts that data and only the receiver can decrypt it.

## Key Difference Between Digital Signature vs Digital Certificate

Let us discuss some of the major key differences between Digital Signature and Digital Certificate:

- The digital signature is used to identify the owner of the document whereas the digital certificate is a document that identifies the identity of the organization.
- The digital signature is signed created by the signer's private key and verified by the public key of a signer whereas digital certificate is issued by a third party and an end-user can check its validity and authenticity.
- The digital signature uses a mathematical function (Hashing function) wherein a Digital certificate contains personal information to help in identifying the trace of the owner.
- A digital signature is created using DSS (Digital Signature Standard) whereas digital certificate works on the principles of public-key cryptography standards.
- A digital signature uses the RSA algorithm when there is a need for message encryption whereas digital certificate is proof that the data transmission will be on the secured layer and in an encrypted way.
- Digital signatures are used to validate the sent data whereas digital certificates are used to validate the identity of the sender.
- With a digital certificate, an end user may have a relationship with the sender whereas in the digital certificate the end user trusts the third party and does not have a relationship with the business owner or the entity.

## Digital Signature vs Digital Certificate Comparison Table

Let's discuss the top comparison between Digital Signature vs Digital Certificate:

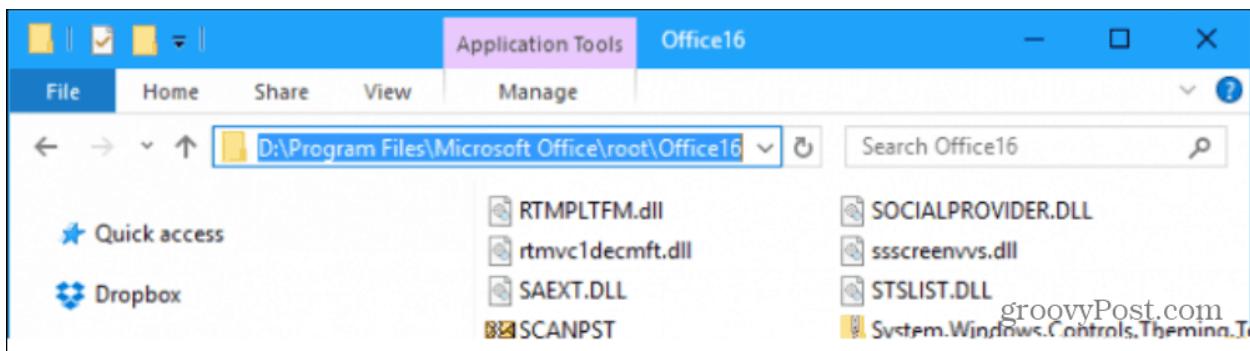
Digital Signature	Digital Certificate
It verifies the identity of the document.	It verifies the identity of the ownership of an online medium.
It is issued to a specific individual by an authorized agency.	It is issued after the background check of the applicant by the Certificate Authority(CA).
It ensures that the signer cannot non-repudiate the signed document.	It ensures that two parties who are exchanging the information are secured.
It works on DSS (Digital Signature Standard)	It works on the principles of public-key cryptography standards.
The digital signature uses a mathematical function (Hashing function).	It contains personal information to help in identifying the trace of the owner.
It is widely used for avoiding forging the document.	It is used in an online transaction for the trustworthiness of the data and the sender.
It is an attachment to a document that can be viewed as a signature.	It is a medium to prove the holder's identity for a particular transaction.
It ensures the sender and the receiver have the same document containing the same data.	It builds the trust between the user and the business (Certificate holder).
It is created using SHA-1 or SHA-2 algorithms.	It is created in the X.509 format.
It uses the RSA algorithm if there is a need for message encryption.	It encrypts that data and only the receiver can decrypt it.

## How to Create a Self-Signed Digital Certificate in Microsoft Office 2016

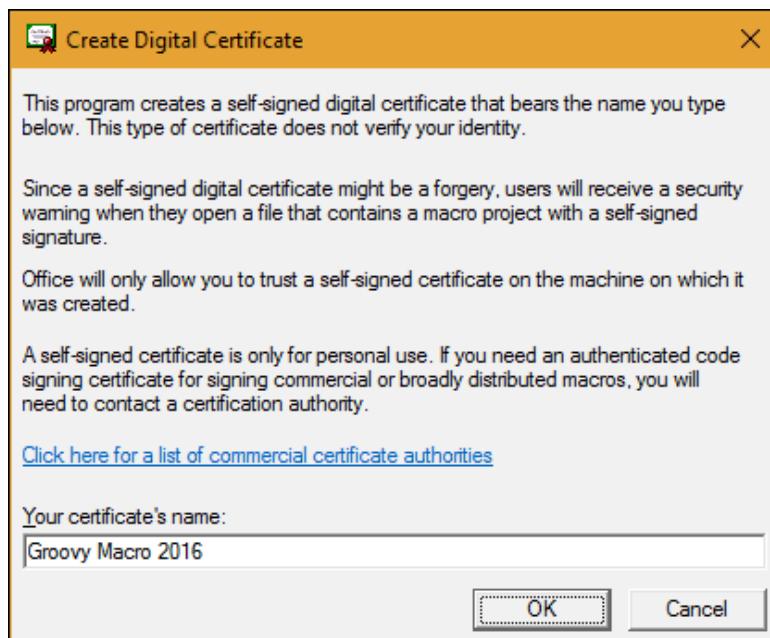
One of the most compelling parts of the Microsoft Office productivity suite for power users is automating functionality using Visual Basic for Application code. Applications such as Word, Excel, and Outlook can be used to create Macros. Macros are small bits of programming code used for performing repetitive tasks. In versions of Office before 2007, VBA support was notorious for being exploited. Since then, Microsoft has enhanced the security within the suite, limiting the impact of rogue code causing potential damage.

### Setup Self-Signed Digital Certificate in Office 2016 Applications

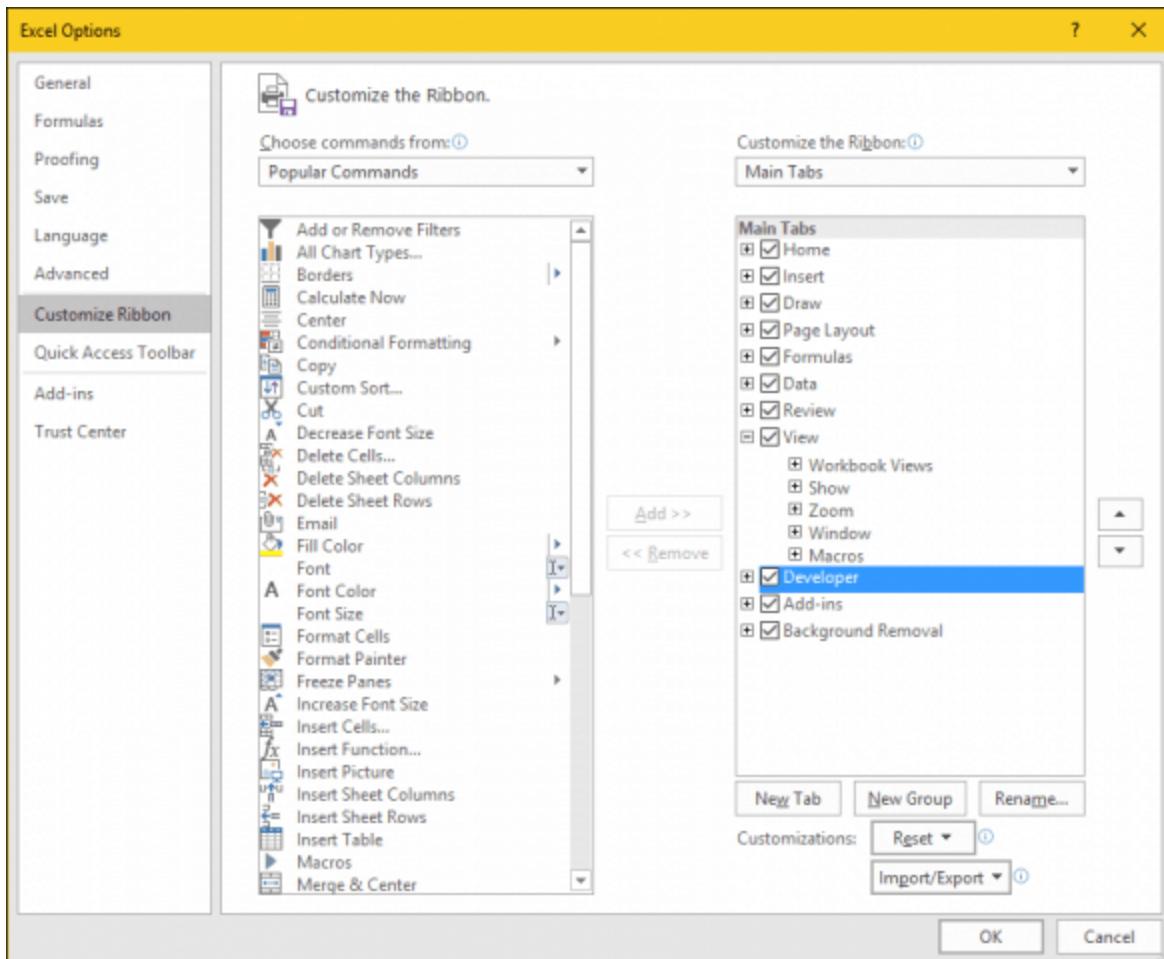
The Digital Certificate for VBA Projects can now be found within **Program Files > Microsoft Office > root > Office16**.



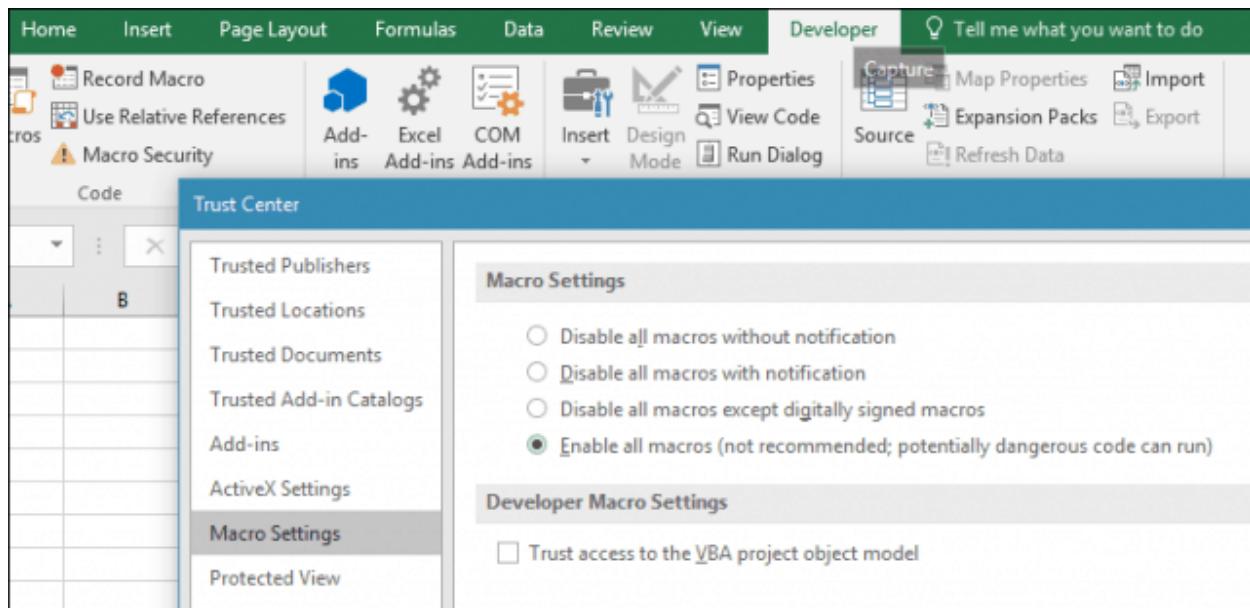
Double click the SELFCERT file, enter a name for your Digital Certificate, then click OK.



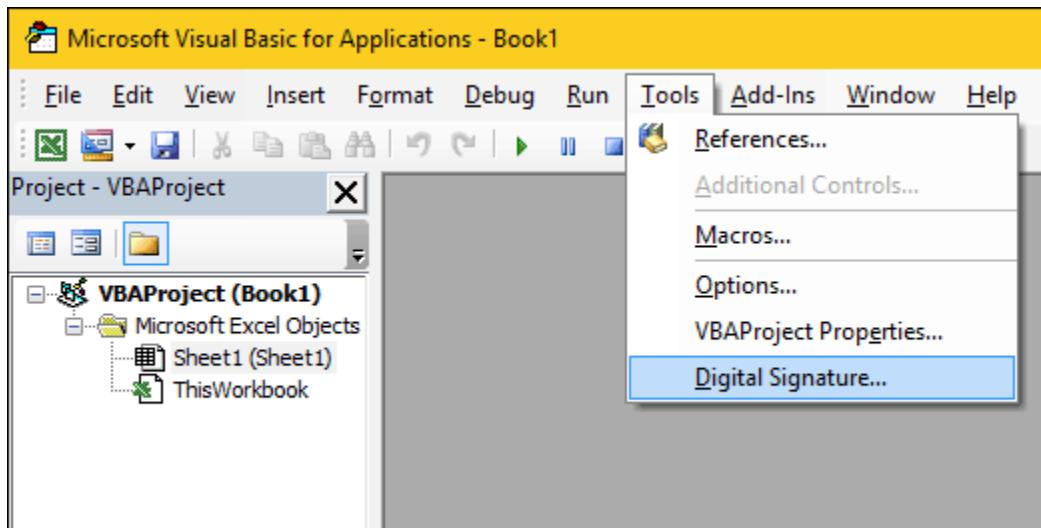
Launch any of the Office applications you would like to use the digital certificate in. For this article, I am going to use Excel. The first thing you will need to do is enable the *Developer* tab. Click File > Options > Customize Ribbon > check the box *Developer* then click OK.



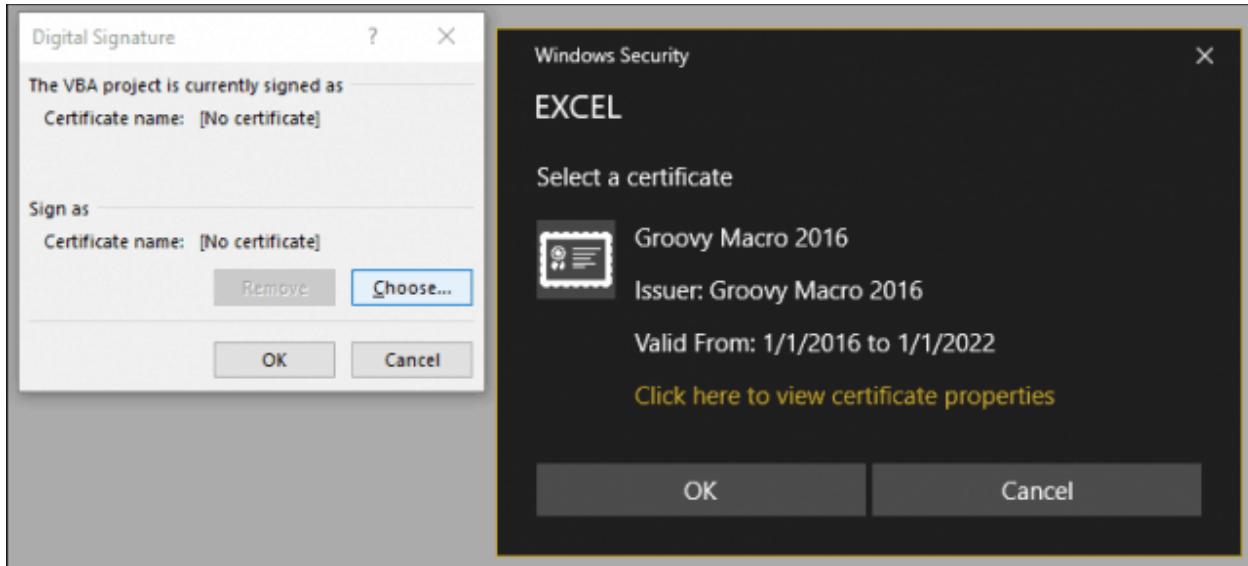
Select the Developer tab, then click the *Macro Security* button within the *Code* group, select the *Enable all Macros* radio box, then click *OK*.



Within the *Code* group, click *Visual Basic*. The Visual Basic for Applications component will be launched. Next, click Tools, then click Digital Signature.

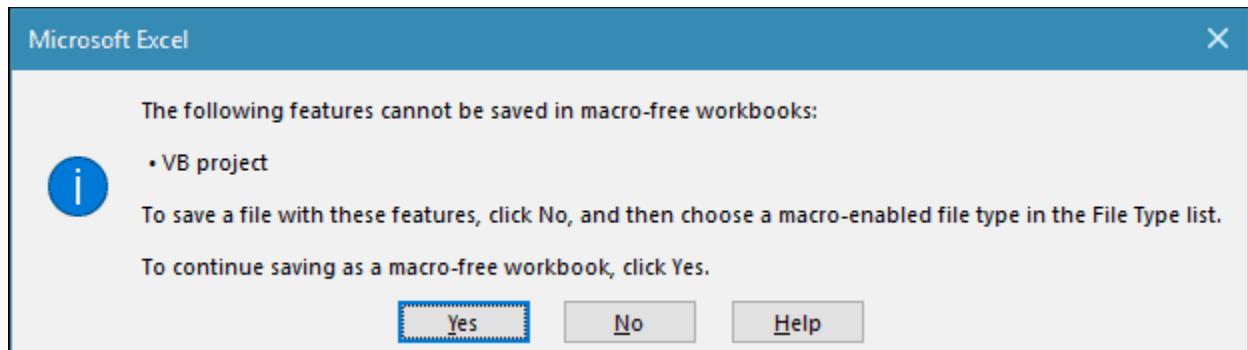


Click Choose, the recently created digital certificate will be presented. Click OK, then proceed to save your project.

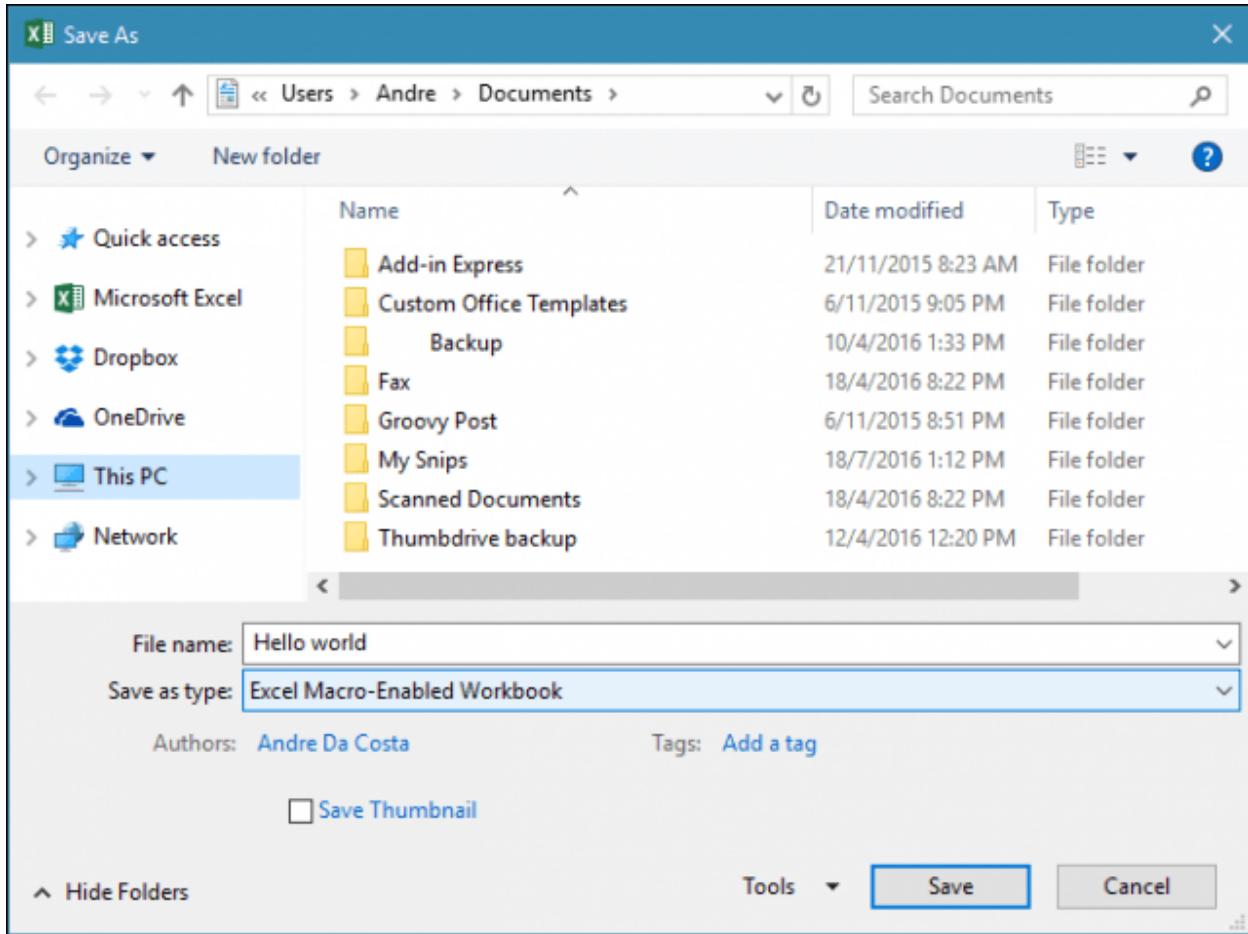


## Ensuring your Macros Work

I noted earlier; Microsoft has made security changes to how Macros work in Office applications over the years. Saving your Macro's is not allowed in a standard workbook or document.



Instead, users must correctly choose Macro-Enabled as the file type when saving.



Users can manage their signed certificate by using launching Internet Options. First, click Start, then **type:** *internet options*, hit Enter on your keyboard, select the *Content* tab, then click *Manage Certificates*. Here you have the choice of deleting or exporting your certificate for use on another computer.

Certificates

Intended purpose: <All>

Personal Other People Intermediate Certification Authorities Trusted Root Certification

Issued To	Issued By	Expiratio...	Friendly Name
adacosta@mrdee.o...	Communications Server	3/9/2015	<None>
e8e5cc039d51e3db	Token Signing Public Key	22/7/2016	<None>
Groovy Macro 2016	Groovy Macro 2016	1/1/2022	<None>

Import... Export... Remove Advanced

Certificate intended purposes

Code Signing

View

Close

Sources:

[How to Create a Self-Signed Digital Certificate in Microsoft Office 2016 \(groovypost.com\)](#)

[What is Digital Certificate? | A Technology Overview from Comodo](#)

[PowerPoint Presentation \(globalsign.com\)](#)

[What is a Digital Signature? \(techtarget.com\)](#)

[What Is a Digital Signature \(and How Does it Work\) | SignATURELY](#)

[The difference between a digital signature and digital certificate » AET Europe](#)

## **Introduction to Digital Signature**

### **What is a digital signature?**

You can use a digital signature for many of the same reasons that you might sign a paper document. A digital signature is used to authenticate digital information — such as form templates, e-mail messages, and documents — by using computer cryptography. Digital signatures help to establish the following assurances:

- **Authenticity** The digital signature helps to assure that the signer is who he or she claims to be.
- **Integrity** The digital signature helps to assure that the content has not been changed or tampered with since it was digitally signed.
- **Non-repudiation** The digital signature helps prove the origin of the signed content to all parties. "Repudiation" refers to the act of a signer denying any association with the signed content.

To make these assurances about a form template, you must digitally sign your form template. You can also enable digital signatures for your form template so that your users can make the same assurances about the forms that they fill out. In either case, the following requirements must be met in order to digitally sign a form or form template:

- The digital signature is valid.
- The certificate associated with the digital signature is current (has not expired).
- The signing person or organization, known as the publisher, is trusted.
- The certificate associated with the digital signature is issued to the publisher by a trusted certificate authority (CA).

Digital signatures are the digital equivalent of regular ink signatures. Just like ink signatures signal your approval or involvement in a paper document and its contents, a digital signature does the same on digital documents. And they do it far better than ink signatures can.

Digital signatures use a Public Key Infrastructure (PKI), a standard format that provides high security and acceptance to your document. This combination of a public key and a private key is what makes a digital signature so safe.

Through the PKI and the processes involved in creating electronic signatures and storing digitally signed documents, you can be sure that your signature cannot be forged, and once signed. The document cannot be altered.

This makes a digital document with an e-signature secure enough to be valid worldwide, including anywhere within the United States and the European Union.

Furthermore, A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software or digital document. It's the digital equivalent of a handwritten signature or stamped seal, but it offers far more inherent security. A digital signature is intended to solve the problem of tampering and impersonation in digital communications.

Digital signatures can provide evidence of origin, identity and status of electronic documents, transactions or digital messages. Signers can also use them to acknowledge informed consent.

Digital signatures are based on public key cryptography, also known as asymmetric cryptography. Using a public key algorithm, such as RSA (Rivest-Shamir-Adleman), two keys are generated, creating a mathematically linked pair of keys, one private and one public.

Digital signatures work through public key cryptography's two mutually authenticating cryptographic keys. The individual who creates the digital signature uses a private key to encrypt signature-related data, while the only way to decrypt that data is with the signer's public key.

If the recipient can't open the document with the signer's public key, that's a sign there's a problem with the document or the signature. This is how digital signatures are authenticated.

Digital signature technology requires all parties trust that the individual creating the signature has kept the private key secret. If someone else has access to the private signing key, that party could create fraudulent digital signatures in the name of the private key holder.

## What are the benefits of digital signatures?

Security is the main benefit of digital signatures. Security capabilities embedded in digital signatures ensure a document is not altered and signatures are legitimate. Security features and methods used in digital signatures include the following:

Personal identification numbers (PINs), passwords and codes. Used to authenticate and verify a signer's identity and approve their signature. Email, username and password are the most common methods used.

**Asymmetric cryptography.** Employs a public key algorithm that includes private and public key encryption and authentication.

**Checksum.** A long string of letters and numbers that represents the sum of the correct digits in a piece of digital data, against which comparisons can be made to detect errors or changes. A checksum acts as a data fingerprint.

**Cyclic redundancy check (CRC).** An error-detecting code and verification feature used in digital networks and storage devices to detect changes to raw data.

**Certificate authority (CA) validation.** CAs issue digital signatures and act as trusted third parties by accepting, authenticating, issuing and maintaining digital certificates. The use of CAs helps avoid the creation of fake digital certificates.

**Trust service provider (TSP) validation.** A TSP is a person or legal entity that performs validation of a digital signature on a company's behalf and offers signature validation reports.

### **Other benefits to using digital signatures include the following:**

**Timestamping.** By providing the data and time of a digital signature, timestamping is useful when timing is critical, such as for stock trades, lottery ticket issuance and legal proceedings.

**Globally accepted and legally compliant.** The public key infrastructure (PKI) standard ensures vendor-generated keys are made and stored securely. Because of the international standard, a growing number of countries are accepting digital signatures as legally binding.

**Time savings.** Digital signatures simplify the time-consuming processes of physical document signing, storage and exchange, enabling businesses to quickly access and sign documents.

**Cost savings.** Organizations can go paperless and save money previously spent on the physical resources and on the time, personnel and office space used to manage and transport them.

**Positive environmental impact.** Reducing paper use also cuts down on the physical waste generated by paper and the negative environmental impact of transporting paper documents.

**Traceability.** Digital signatures create an audit trail that makes internal record-keeping easier for business. With everything recorded and stored digitally, there are fewer opportunities for a manual signee or record-keeper to make a mistake or misplace something.

## **How Do Digital Signatures Work?**

### **1. The digital signing software**

To properly use a digital signature, you can't just get a JPEG of your signature and paste it on a Word document. You need an electronic signature app to do the job.

Electronic signature solutions, like:

1. Adobe Sign - Tracking and document management
2. Secured Signing - With video confirmation
3. DocuSign - Handles multiple recipients
4. OneSpan Sign - For large and small organizations
5. SignEasy - Reusable templates
6. Signaturely

Make your digital signatures effective by becoming a TSP and certifying the document for you, keeping it safe.

Signaturely, for example, uses ISO 27001 and FIRMA certified data centers managed by Amazon. This allows Signaturely to access AWS data centers to securely store all your data on the cloud, ensuring only your signer's eyes can access it. The data you send to or from Signaturely is also encrypted in transit through 256-bit encryption. Signaturely also gives you the power further to protect your data through 2-Factor Authentication (2FA) to ensure you are the only person accessing your Signaturely account. Electronic signature platforms like Signaturely also handle all parts of the digital signing process for you, ensuring everything about the digital signing process is valid and legally binding.

## **2. Signing up for a platform for electronic signatures**

Since e-signatures are only valid when using the right software, you'll need to choose one that works for you. There are a few options available for digitally signing documents, but you can get started for free by creating a an account.

Any E-Signature application offers a forever-free account allowing you up to three sent documents for free per month.

Start by creating a new account with your name, email address, and password, or sign up with your Google login for an even faster process. Within seconds you'll be able to access platform to create your new document.

## **3. Create or upload your documents**

E-signature applications like Adobe, SecureSign, or Signaturely varies on the processes in signing your document, these processes differs but you will still get the same result. You can get started immediately with the contracts you have. There are no unnecessary processes so that you can set up your contract immediately.

Simply upload your document, and use the editor to add the signature fields. That's it.

You can either upload them directly from your computer or import them directly by connecting your DropBox, Google Drive, OneDrive, or Box accounts.

When the document has been uploaded, simply open it with the editor to add the signature fields, positioning them exactly where someone would sign if they were using an ink signature.

#### **4. Send signature requests**

When your document is fully digitized and ready to be signed, it's time to send a signature request to your signees. This process can be completed entirely in-app, letting do the heavy lifting for you.

All you need to do is to add the signees' names and email addresses. If your contract needs to be signed by people in a specific order, you can have the app send the document to them one after the other as each individual signs the agreement.

The e-signature app will then guide your signees through each step of the signing process, starting with creating their e-signature and continuing through the whole signing process step by step until each signature has been added to the document.

#### **5. Wait for your digital documents to return**

It is understandable that it can be nerve-wracking to wait for a document to be returned. The longer you wait, the more questions you ask yourself, like: "Have they seen it yet?" When did they see it? Should I call them and ask why they haven't signed the document?

Other application uses dashboard, so you can easily track your documents as they progress. It lets you know who has signed, when, and who has yet to sign. Other apps will remind the signee that their signature is still required, so you don't have to get directly involved. This gentle reminder is usually enough to nudge someone into signing without pressuring them into it.

#### **Using powerful encryption and security keys to protect your document**

When your signees open a document, their only option will be to sign it. They can't alter, edit, or change anything on the document. When a user signs the document, the signature records a timestamp. Once all users have signed, the document automatically locks itself, preventing further edits. You and your signees can know that the document you're signing cannot be altered in any way.

The digital signature signing software, such as an email program, is used to provide a one-way hash of the electronic data to be signed.

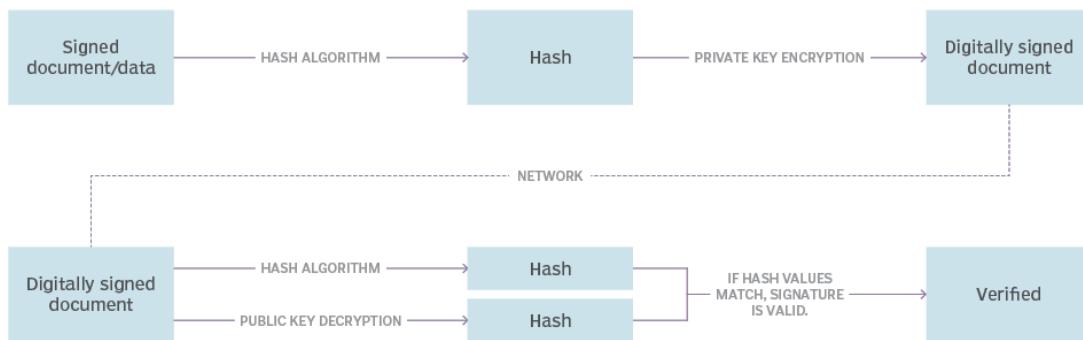
A hash is a fixed-length string of letters and numbers generated by an algorithm. The digital signature creator's private key is then used to encrypt the hash. The encrypted hash -- along with other information, such as the hashing algorithm -- is the digital signature.

The reason for encrypting the hash instead of the entire message or document is a hash function can convert an arbitrary input into a fixed-length value, which is usually much shorter. This saves time as hashing is much faster than signing.

The value of a hash is unique to the hashed data. Any change in the data, even a change in a single character, will result in a different value. This attribute enables others to use the signer's public key to decrypt the hash to validate the integrity of the data.

If the decrypted hash matches a second computed hash of the same data, it proves that the data hasn't changed since it was signed. If the two hashes don't match, the data has either been tampered with in some way and is compromised or the signature was created with a private key that doesn't correspond to the public key presented by the signer -- an issue with authentication.

## The digital signature process



## Sample signing scenario

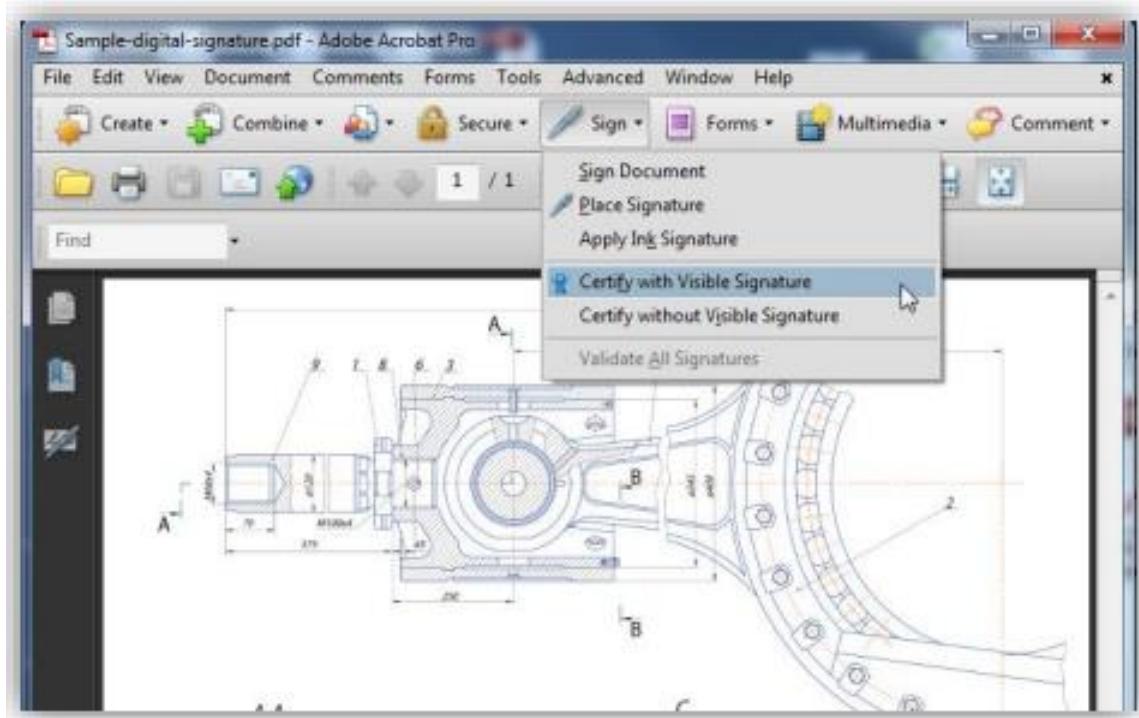
### Scenario:

Leslie has a drawing she needs to submit to Joe. There are a number of programs that can be used to apply the signature (e.g., Adobe LiveCycle, BlueBeam, etc.), but in this example, we're going to use Adobe Acrobat. Per this project's specifications, Leslie needs to certify the document and insert her Professional Engineer seal. There are two components to the signature process – creating the signature and validating it. We'll start with the first part – Leslie applying the digital signature.

## Applying the signature

These are the steps Leslie will go through to apply the digital signature.

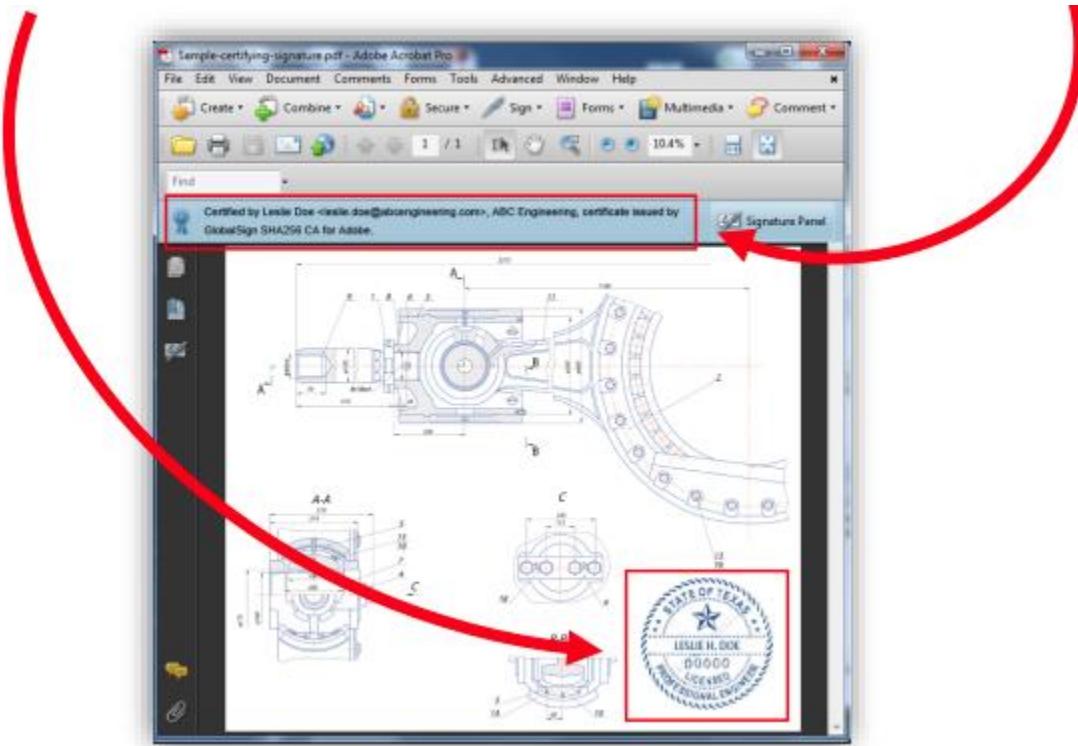
1. Leslie opens her drawing in Acrobat. She clicks “Certify with Visible Signature”.



2. After she chooses where she would like the visible signature to appear, she selects the certificate she wants to use to sign the document, chooses how she wants the signature to appear (her PE seal), and disallows any changes to be made to the document after the signature is applied.



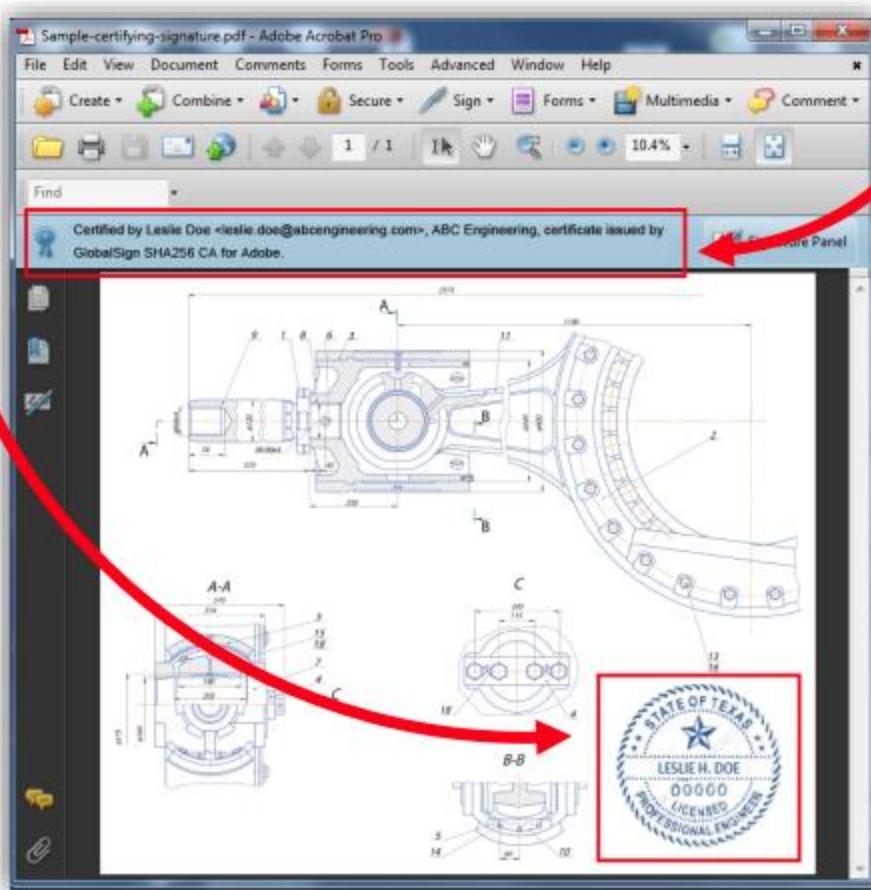
- Finally, she enters her password and the signature is applied. The document now includes two key trust indicators - a notice at the top of the document stating that it has been certified by Leslie, whose identity was verified by a third party CA (in this case GlobalSign) and her PE seal. The document is ready to send to Joe.



## Verifying the signature

These are the steps Joe will go through to verify Leslie's signature. Note: Adobe Reader automatically verifies the signature, so Joe doesn't actually need to do anything beyond open the document in Reader. Here we'll walk you through what to look for in a digitally signed document and show you how you can find details about the digital signature.

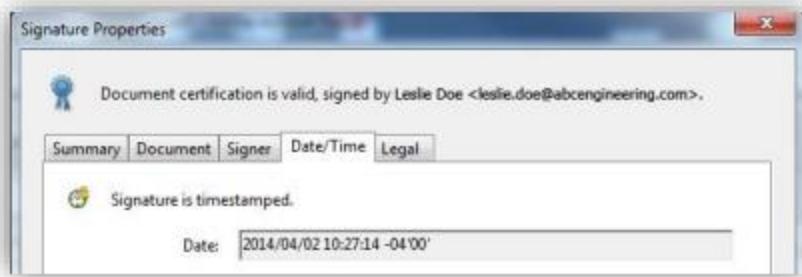
- Joe opens the PDF in Adobe Reader and sees the same two trust indicators explained above - the notice at the top of the document and Leslie's engineering seal



2. Clicking the seal verifies Leslie's signature and reaffirms that no changes have been made to the document since she signed it.



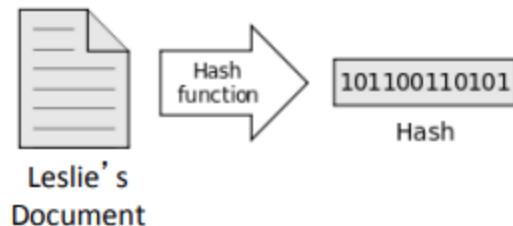
3. Joe can view "Signature Properties" for more information, including a timestamp of when the document was signed.



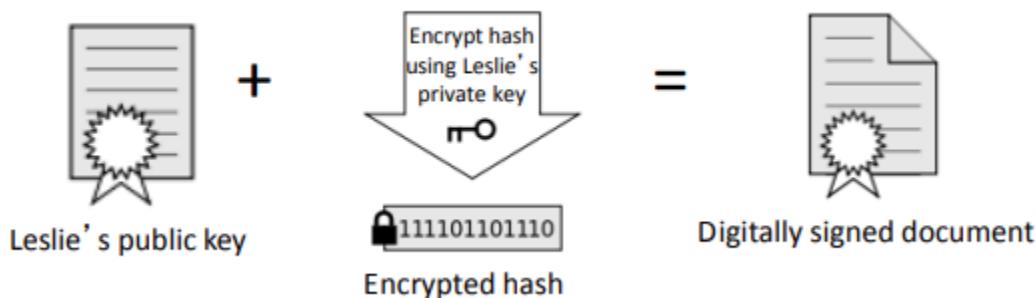
## Behind the scenes of the signing process

### A. Applying the Signature

- When Leslie clicks "sign" in Adobe Acrobat, a unique digital fingerprint (called a hash) of the document is created using a mathematical algorithm. This hash is specific to this particular document; even the slightest change would result in a different hash.



- This hash is encrypted using Leslie's private key from her digital certificate. The encrypted hash and Leslie's public key are combined into a digital signature, which is appended to the document.

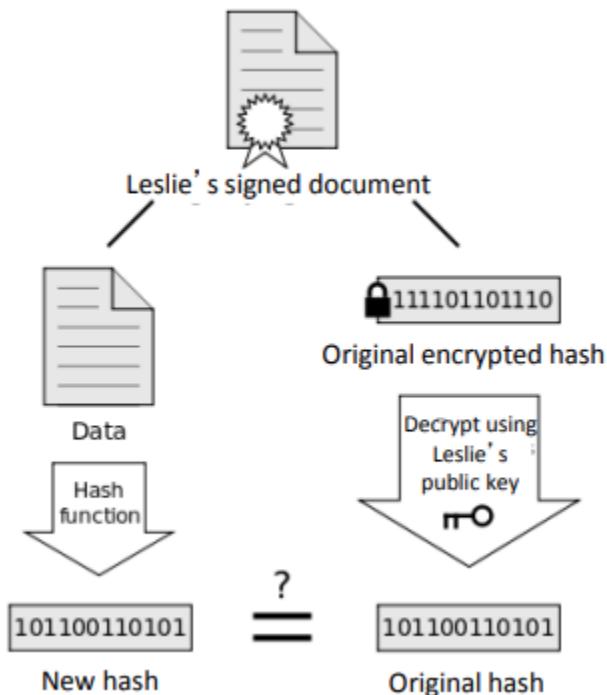


- Leslie can now share the digitally signed document with Joe

## B. Verifying the Signature

- When Joe opens the signed PDF, Adobe Reader automatically uses Leslie's public key (which was included in the digital signature with the document) to decrypt the document hash.

Reader calculates a new hash for Leslie's document. If this new hash matches the decrypted hash from Step 1, Reader knows that the document has not been altered and displays the message, "The Document has not been modified since this signature was applied."



Reader also checks the validity of the certificate Leslie used to apply the signature (i.e., that it has not been revoked) and verifies that the public key used in the signature belongs to Leslie.

## Other signing scenarios

We ran through a basic scenario, in which Leslie simply needed to send a certified PDF stamped with her PE seal to Joe. There are a number of options when applying digital signatures to fit your specific workflow, document type, or any applicable government regulations.

- Digital version of handwritten signature
- Instead of a PE seal, Leslie could have included an image of her handwritten signature.

- Multiple signatures within one document
- Leslie chose to not allow any changes to be made to the document after she applied her signature, but she could have allowed other digital signatures to be applied.
- Sign multiple pages of the same document
- Leslie could have added her PE seal to multiple pages to the document.

Sources:

[How to Create a Self-Signed Digital Certificate in Microsoft Office 2016 \(groovypost.com\)](#)

[What is Digital Certificate? | A Technology Overview from Comodo](#)

[PowerPoint Presentation \(globalsign.com\)](#)

[What is a Digital Signature? \(techtarget.com\)](#)

[What Is a Digital Signature \(and How Does it Work\) | SignATURELY](#)

[The difference between a digital signature and digital certificate » AET Europe](#)