BITS Pilani

Prof. Pradnya Kashikar

WILP-CSIS

BITS Pilani
Pilani Campus

innovate achieve lead

BITS Pilani

Pilani Campus

SS ZG588 - Cyber Crimes, Forensics and Incident Handling

Contact Session - 1

Course Objectives

No	Description
CO1	Enhancing awareness of recent Cyber Crime trends and learn Investigating Cyber Crimes
CO2	Introduce Cyberspace Infrastructure attacks and handling Organization Cybersecurity Issues
CO3	Understand Digital Forensics Process, Models, Analysis and Validation, Incident Detection and Response

Text Book(s)

innovate achieve lead

T1	Computer Forensics and Cyber Crime - An Introduction 3rd Edition by Marjie T. Britz, Ph.D., Professor of Criminal Justice, Clemson University
T2	Bill Nelson, A. Philips, F. Enfinger, C. K. Steuart, Computer Forensics and Investigations, Course Technology (Cengage Learning), Indian edition, 2009
T3	Incident Response & Computer Forensics, 3rd Edition by Jason T. Luttgens and Matthew Pepe and Kevin Mandia
R1	Guide to Computer Forensics and Investigations: Processing Digital Evidence 5th Edition by Bill Nelson, Amelia Phillips and Christopher Steuart
R2	The Basics of Digital Forensics, by John Sammons
R3	Computer Network Security and Cyber Ethics 4th Edition, by Joseph Migga Kizza
R4	Computer Forensics_ Investigating Network Intrusions and Cyber Crime: EC-Council Press

Learning Outcomes -

No	Learning Outcomes
LO1	Fundamental understanding and Information on Cyber Crimes, Digital Forensics Objectives and Incident Detection and Response Reports.
LO2	Learn on how to prepare investigation on computer-related incidents or crimes and summarize.
LO3	Understand on digital forensics process, models and analysis by taking a systematic approach
LO4	Explore on evaluating needs, validating and testing digital forensics tools, Generating Incident Report Findings, and Emerging Cybercrime Trends and Issues

Evaluation Scheme:

Note: Assignment can be replaced by QUIZ also.

Syllabus for Mid-Semester Test (Open Book): Topics in Session Nos. 1 to 8
Syllabus for Comprehensive Exam (Open Book): All topics (Session Nos. 1 to 16)

Evaluation Scheme:
Legend: EC = Evaluation Component; AN = After Noon Session; FN = Fore Noon Session

No	Name	Type	Duration	Weight	Day, Date, Session, Time
EC-1	Assignment-I	Online	-	10%	August 16-30, 2022
EC-1	Assignment-II	Online	-	10%	September 16-30, 2022
EC-2	Mid-Semester Test	Open Book	2 hours	30%	Sunday, 25/09/2022 (FN)
EC-3	Comprehensive Exam	Open Book	2 hours	50%	Sunday, 27/11/2022 (FN)

Module 1 - Introduction to Cyber Crime, Digital Forensics and Incident Handling

innovate achieve lead

1.1 Information On Cyber Crime

1.2 Types Of Cyber Hackers

1.3 Cyberspace and Criminal Behavior

1.4 Traditional Problems Associated with Computer Crime

1.5 The Changing Landscape of Cybercrime

1.6 Preamble and Scheme Of Information Technology Act

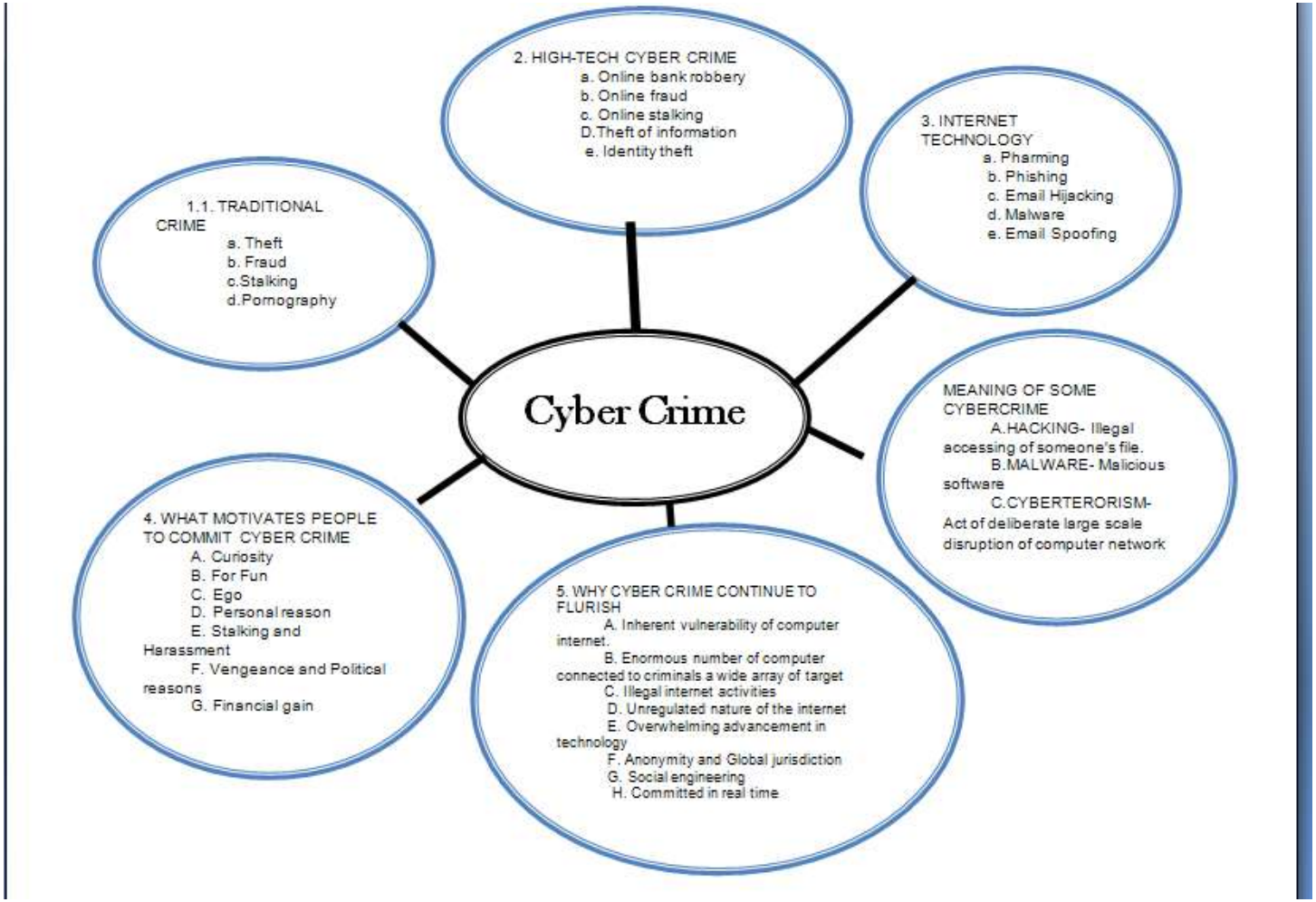
1.7 Overview of Digital Forensics and Incident Handling

1	Introduction to Cyber Crime, Forensics and Incident Handling	**Information On Cyber Crime**	T1, R3
		Types Of Cyber Hackers	
		Cyberspace and Criminal Behavior	
		Traditional Problems Associated with Computer Crime	
		The Changing Landscape of Cybercrime	
		Preamble and Scheme Of Information Technology Act	
		Overview of Digital Forensics and Incident Handling	

1.1 Information On Cyber Crime

- *Any crime that involves computers or aided by the use of computers carried out by individuals or organizations.*
- Cybercrime is criminal activity that either targets or uses a computer, a computer network or a networked device.
- Most, but not all, cybercrime is committed by cybercriminals or hackers who want to make money.
- With traditional crime reducing, global communities continue to witness a sporadic growth in cybercrime.
- Computer crime encompasses a broad range of activities. Computer fraud is any dishonest misrepresentation of fact intended to let another to do or refrain from doing something which causes loss.

1.1 Information On Cyber Crime



1.1 Information On Cyber Crime

✓ Computer Criminals:

1. **Amateurs**: regular users, who exploit the vulnerabilities of the computer system

   Motivation: easy access to vulnerable resources

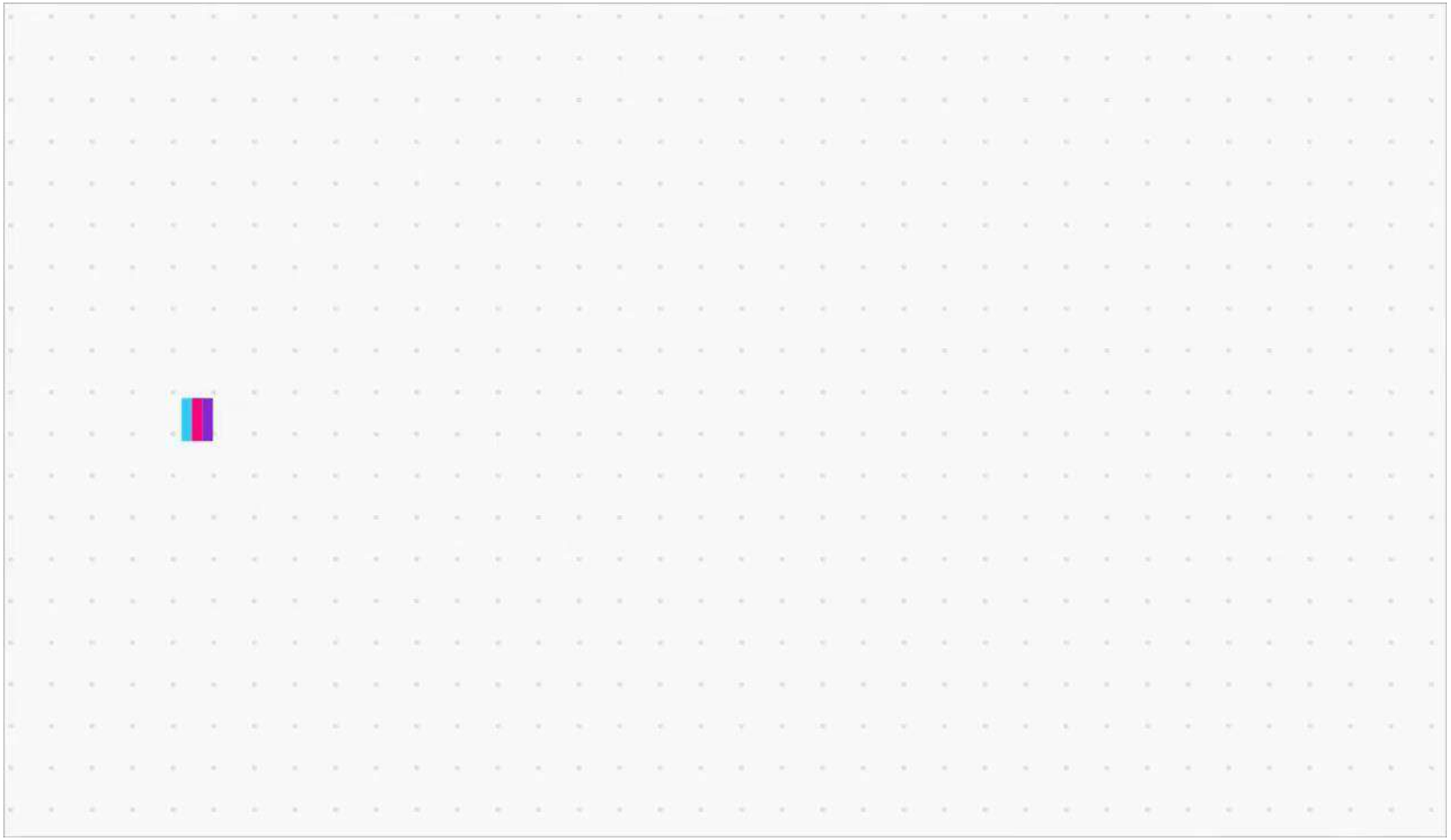
2. **Crackers**: attempt to access computing facilities for which they do not have the authorization

   Motivation: enjoy challenge, curiosity

3. **Career criminals**: professionals who understand the computer system and its vulnerabilities

   Motivation: personal gain (e.g., financial)

1.2 Types Of Cyber Hackers



1.2 Types Of Cyber Hackers

- **White Hat Hackers:** White hat hackers are the one who is authorized or the certified hackers who work for the government and organizations by performing penetration testing and identifying loopholes in their cybersecurity. They also ensure the protection from the malicious cyber crimes. They work under the rules and regulations provided by the government, that's why they are called *Ethical hackers* or *Cybersecurity experts*.
- **Black Hat Hackers:** They are often called *Crackers*. Black Hat Hackers can gain the unauthorized access of your system and destroy your vital data. The method of attacking they use common hacking practices they have learned earlier. They are considered to be as criminals and can be easily identified because of their malicious actions.
- **Gray Hat Hackers:** Gray hat hackers fall somewhere in the category between white hat and black hat hackers. They are not legally authorized hackers. They work with both good and bad intentions; they can use their skills for personal gain. It all depends upon the hacker. If a grey hat hacker uses his skill for his personal gains, he/she is considered as black hat hackers.

1.2 Types Of Cyber Hackers

- **Script Kiddies:** They are the most dangerous people in terms of hackers. A Script kiddie is an unskilled person who uses scripts or downloads tools available for hacking provided by other hackers. They attempt to attack computer systems and networks and deface websites. Their main purpose is to impress their friends and society. Generally, Script Kiddies are juveniles who are unskilled about hacking.
- **Green Hat Hackers:** They are also amateurs in the world of hacking but they are bit different from script kiddies. They care about hacking and strive to become full-blown hackers. They are inspired by the hackers and ask them few questions about. While hackers are answering their question they will listen to its novelty.
- **Blue Hat Hackers:** They are much like the script kiddies; are beginners in the field of hacking. If anyone makes angry a script kiddie and he/she may take revenge, then they are considered as the blue hat hackers. Blue Hat hackers payback to those who have challenged them or angry them. Like the Script Kiddies, Blue hat hackers also have no desire to learn.

1.2 Types Of Cyber Hackers

- **Red Hat Hackers:** They are also known as the eagle-eyed hackers. Like white hat hackers, red hat hackers also aims to halt the black hat hackers. There is a major difference in the way they operate. They become ruthless while dealing with malware actions of the black hat hackers. Red hat hacker will keep on attacking the hacker aggressively that the hacker may know it as well have to replace the whole system.
- **State/Nation Sponsored Hackers:** State or Nation sponsored hackers are those who are appointed by the government to provide them cybersecurity and to gain confidential information from other countries to stay at the top or to avoid any kind of danger to the country. They are highly paid government workers.
- **Hacktivist:** These are also called the online versions of the activists. Hacktivist is a hacker or a group of anonymous hackers who gain unauthorized access to government's computer files and networks for further social or political ends.
- **Malicious Insider or Whistle-blower:** A malicious insider or a whistle-blower could be an employee of a company or a government agency with a grudge or a strategic employee who becomes aware of any illegal activities happening within the organization and can blackmail the organization for his/her personal gain.

1.2 Types Of Cyber Hackers

1.3 Cyberspace and Criminal Behavior

Consider three hypothetical scenarios:

- **Scenario 1:** Lee steals a computer device (e.g., a printer) from a computer lab;
- **Scenario 2:** Lee breaks into a computer lab and then snoops around;
- **Scenario 3:** Lee enters a computer lab that he is authorized to use and then places an explosive device, which is set to detonate a short time later, on a computer system in the lab.

Each of the acts described in these three scenarios is criminal in nature. But should they necessarily be viewed as a computer crime or cybercrime?

Arguably, it would not have been possible to commit any of these specific crimes if computer technology had never existed. But the three criminal acts can easily be prosecuted as ordinary crimes involving theft, breaking and entering, and vandalism.

1.3 Cyberspace and Criminal Behavior

Consider the following scenario:

- **Scenario 4***:* Lee uses a computer to file a fraudulent income-tax return. Arguably, a computer is the principal tool used by Lee to carry out the criminal act.

  Has Lee has committed a *computer crime*?

  But Lee could have committed the same crime by manually filling out a standard (hardcopy) version of the income-tax forms by using a pencil or pen.

1.4 Traditional Problems Associated with Computer Crime

1. Physicality and Jurisdictional Concerns
2. Perceived Insignificance, Stereotypes, and Incompetence
3. Prosecutorial Reluctance
4. Lack of Reporting
5. Lack of Resources
6. Jurisprudential Inconsistency

1.5 The Changing Landscape of Cybercrime

- Emerging cyber threats are impacting organizations and their end-users in the current threat landscape.
- The COVID-19 pandemic has changed the way the world uses technology and increased the number of digital tools in use for many employees.
- This has shifted the threat landscape.

- Firms should secure their networked information.
- Government should assure that their laws apply to cyber crimes.
- Firms, governments, and civil society should work cooperatively to strengthen legal frameworks for cyber security.

1.6 Preamble and Scheme Of Information Technology Act

1. Information Technology Act, 2000-came into force on 17 October 2000
2. Extends to whole of India and also applies to any offence or contravention there under committed outside India by any person.
3. Section 75- Act applies to offence or contravention committed outside India by any person irrespective of his nationality, if such act involves a computer, computer system or network located in India
4. Section 2 (1) (a) –"Access" means gaining entry into ,instructing or communicating with the logical, arithmetic or memory function resources of a computer, computer resource or network
5. IT Act confers legal recognition to electronic records and digital signatures (section 4,5 of the IT Act,2000)

1.6 Preamble and Scheme Of Information Technology Act

innovate achieve lead

Computer Related Crimes under IPC and Special Laws

Sending threatening messages by email	Sec 503 IPC
Sending defamatory messages by email	Sec 499, 500 IPC
Forgery of electronic records	Sec 463, 470, 471 IPC
Bogus websites, cyber frauds	Sec 420 IPC
Email spoofing	Sec 416, 417, 463 IPC
Online sale of Drugs	NDPS Act
Web-Jacking	Sec. 383 IPC
Online sale of Arms	Arms Act

1.7 Overview of Digital Forensics and Incident Handling

What is Digital Forensics??

- Digital forensics involves the preservation, identification, extraction, documentation, and interpretation of computer media for evidentiary and/or root cause analysis.
- Evidence might be required for a wide range of computer crimes and misuses
- Multiple methods of
  - Discovering data on computer system
  - Recovering deleted, encrypted, or damaged file information
  - Monitoring live activity
  - Detecting violations of corporate policy
- Information collected assists in arrests, prosecution, termination of employment, and preventing future illegal activity

1.7 Overview of Digital Forensics and Incident Handling

What Constitutes Digital Evidence?

- Any information being subject to human intervention or not, that can be extracted from a computer.
- Must be in human-readable format or capable of being interpreted by a person with expertise in the subject.

Computer Forensics Examples

- Recovering thousands of deleted emails
- Performing investigation post employment termination
- Recovering evidence post formatting hard drive
- Performing investigation after multiple users had taken over the system

1.7 Overview of Digital Forensics and Incident Handling

Who Uses Computer Forensics?

- Criminal Prosecutors
  - Rely on evidence obtained from a computer to prosecute suspects and use as evidence
- Civil Litigations
  - Personal and business data discovered on a computer can be used in fraud, divorce, harassment, or discrimination cases
- Insurance Companies
  - Evidence discovered on computer can be used to mollify costs (fraud, worker's compensation, arson, etc)

1.7 Overview of Digital Forensics and Incident Handling

Who Uses Computer Forensics?

- Private Corporations
  - Obtained evidence from employee computers can be used as evidence in harassment, fraud, and embezzlement cases
- Law Enforcement Officials
  - Rely on computer forensics to backup search warrants and post-seizure handling
- Individual/Private Citizens
  - Obtain the services of professional computer forensic specialists to support claims of harassment, abuse, or wrongful termination from employment

1.7 Overview of Digital Forensics and Incident Handling

Steps Of Computer Forensics

According to many professionals, Computer Forensics is a four (4) step process

- Acquisition
  - Physically or remotely obtaining possession of the computer, all network mappings from the system, and external physical storage devices
- Identification
  - This step involves identifying what data could be recovered and electronically retrieving it by running various Computer Forensic tools and software suites

1.7 Overview of Digital Forensics and Incident Handling

innovate achieve lead

Steps Of Computer Forensics –

- Evaluation
  - Evaluating the information/data recovered to determine if and how it could be used against the suspect for employment termination or prosecution in court
- Presentation
  - This step involves the presentation of evidence discovered in a manner which is understood by lawyers, non-technically staff/management, and suitable as evidence as determined by the nations and internal laws

1.7 Overview of Digital Forensics and Incident Handling

Incident Handling –

- Cyber Forensics and Incident Handling Forensics is an essential part of cybersecurity.
- Any cyber incident must be solved through the cyber forensics team who can find out the exact issue and how the mishap takes place.
- Cybersecurity and forensics have another essential terminology that is often used in this field - incident handling.
- Computer security incidents are some real or suspected offensive events related to cybercrime and cybersecurity and computer networks.
- Forensics investigators or internal cybersecurity professionals are hired in organizations to handle such events and incidents, known as incident handlers.

1.7 Overview of Digital Forensics and Incident Handling

innovate achieve lead

Incident Handling –

Incidents are categorized into three types:

- **Low-level incidents**: where the impact of cybercrime is low.
- **Mid-level incidents**: The impact of cybercrime is comparatively high and needs security professionals to handle the situations.
- **High-level events**: where the impact of cybercrime is the most serious and needs security professionals, and forensic investigators to handle the situations and analyze the scenario, respectively.

Thank you

BITS Pilani

Prof. Pradnya Kashikar

WILP-CSIS

BITS Pilani
Pilani Campus

innovate achieve lead

BITS Pilani

Pilani Campus

SS ZG588 - Cyber Crimes, Forensics and Incident Handling

Contact Session - 2

Course Objectives

No	Description
CO1	Enhancing awareness of recent Cyber Crime trends and learn Investigating Cyber Crimes
CO2	Introduce Cyberspace Infrastructure attacks and handling Organization Cybersecurity Issues
CO3	Understand Digital Forensics Process, Models, Analysis and Validation, Incident Detection and Response

Text Book(s)

innovate achieve lead

T1	Computer Forensics and Cyber Crime - An Introduction 3rd Edition by Marjie T. Britz, Ph.D., Professor of Criminal Justice, Clemson University
T2	Bill Nelson, A. Philips, F. Enfinger, C. K. Steuart, Computer Forensics and Investigations, Course Technology (Cengage Learning), Indian edition, 2009
T3	Incident Response & Computer Forensics, 3rd Edition by Jason T. Luttgens and Matthew Pepe and Kevin Mandia
R1	Guide to Computer Forensics and Investigations: Processing Digital Evidence 5th Edition by Bill Nelson, Amelia Phillips and Christopher Steuart
R2	The Basics of Digital Forensics, by John Sammons
R3	Computer Network Security and Cyber Ethics 4th Edition, by Joseph Migga Kizza
R4	Computer Forensics_ Investigating Network Intrusions and Cyber Crime: EC-Council Press

Learning Outcomes -

LO1	Fundamental understanding and Information on Cyber Crimes, Digital Forensics Objectives and Incident Detection and Response Reports.
LO2	Learn on how to prepare investigation on computer-related incidents or crimes and summarize.
LO3	Understand on digital forensics process, models and analysis by taking a systematic approach
LO4	Explore on evaluating needs, validating and testing digital forensics tools, Generating Incident Report Findings, and Emerging Cybercrime Trends and Issues

2	Foundation for Forensics	**Networking Concepts required for Forensics**	T1, T2
		Working with Windows and DOS Systems; Linux Boot Processes and CLI Systems	
		Introduction to Forensics Science and need for Digital Forensics; Digital Forensic Techniques	
		Understanding the Digital Forensics Profession	

Module 2 - Foundation for Forensics

innovate achieve lead

2.1 Networking Concepts required for Forensics

2.2 Working with Windows and DOS Systems; Linux Boot Processes and CLI Systems

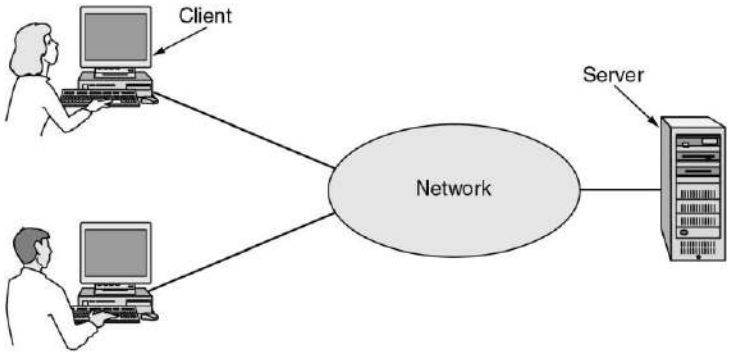
2.3 Introduction to Forensics Science and Need for Digital Forensics; Digital Forensic Techniques

2.4 Understanding the Digital Forensics Profession

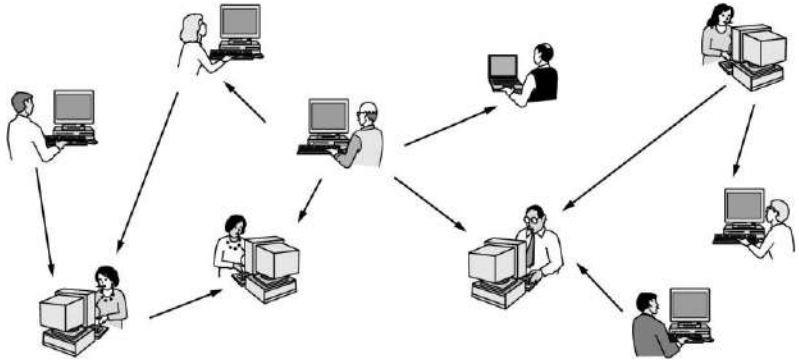
2.1 Networking Concepts required for Forensics

- Definition: computer network :: [Tanenbaum] - A collection of “autonomous” computers interconnected by a single technology

- Client-Server Applications



- Peer-to-peer applications



2.1 Networking Concepts required for Forensics

innovate achieve lead

Uses of Computer Networks:

Business Applications

- The client-server model involves requests and replies

Home Applications

– Access to remote information
– Person-to-person communication
– Interactive entertainment
– Electronic commerce

2.1 Networking Concepts required for Forensics

innovate achieve lead

Uses of Computer Networks:

Mobile Users – Some forms of e-commerce –

Tag	Full name	Example
B2C	Business-to-consumer	Ordering books on-line
B2B	Business-to-business	Car manufacturer ordering tires from supplier
G2C	Government-to-consumer	Government distributing tax forms electronically
C2C	Consumer-to-consumer	Auctioning second-hand products on-line
P2P	Peer-to-peer	File sharing

Social Issues

Wireless	Mobile	Applications
No	No	Desktop computers in offices
No	Yes	A notebook computer used in a hotel room
Yes	No	Networks in older, unwired buildings
Yes	Yes	Portable office; PDA for store inventory

2.1 Networking Concepts required for Forensics

Let us understand what are –

- Local Area Networks
- Metropolitan Area Networks
- Wide Area Networks
- Wireless Networks
- Internetworks

2.1 Networking Concepts required for Forensics

2.1 Networking Concepts required for Forensics

Network Taxonomy –

There are two major ways to classify a network:

- The size of the network
- The transmission technology used by the network

There is no defined taxonomy into which all computer networks can be classified, but these two network features are acceptable for general classifications.

2.1 Networking Concepts required for Forensics

innovate achieve lead

Transmission Technologies –

There are two types of transmission technologies:

1. **Broadcast –**

- uses a single communications channel
- the channel is shared
- information sent from any one machine on the network is received by all other machines on the network
- each piece of data received by a computer is checked to see if it is addressed to that computer

2. **Point-to-point -**

- Point-to-point networks consist of a large number of individual connections between pairs of computers.
- The data travels through the network and is directed by machines along the way.
- Although these intermediate machines look at the data to see where it is going, they do not (should not) look at the data itself.

2.1 Networking Concepts required for Forensics

innovate achieve lead

Network Size –

- We can also classify networks based on their physical size.
- Different technologies may be used based on the size of the network.
- We can determine the type of network based on the physical distance that the network covers.

Interprocessor Distance	Processors located in same	
1 m	Square Meter	Personal Area Network
10 m	Room	Local Area Network
100 m	Building	
1 km	Campus	
10 km	City	Metropolitan Area Network
100 km	Province	Wide Area Network
1000 km	Continent	
10,000 km	Planet	The Internet

2.1 Networking Concepts required for Forensics

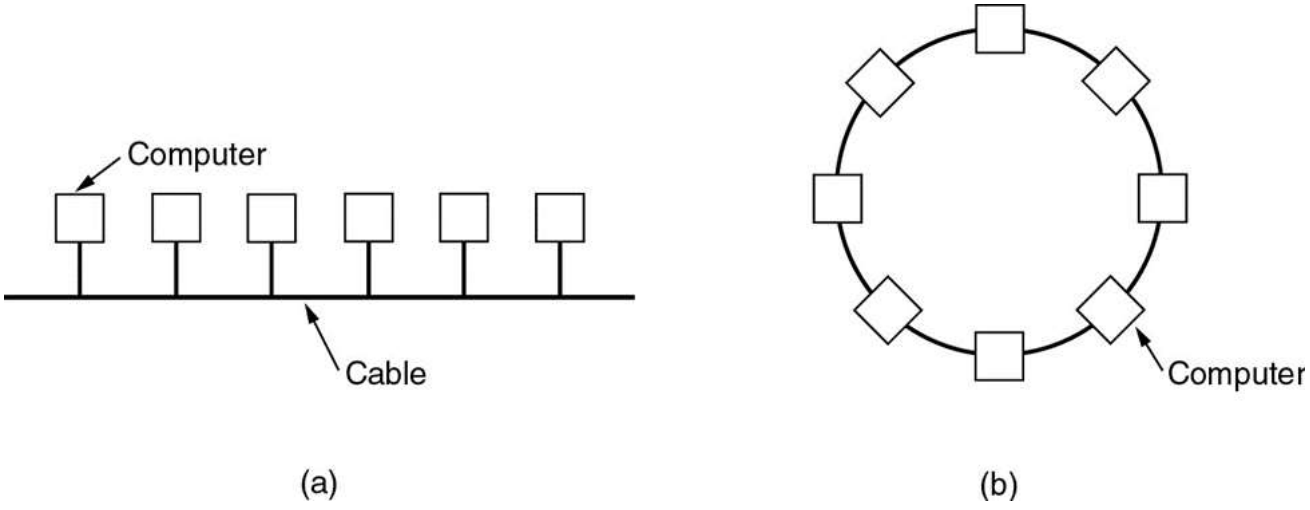
Personal Area Network –

- A network meant for one person.
- A personal computer network:
  - a wireless keyboard and mouse
  - a networked printer
  - a PDA connection
- Devices to control pacemakers
- Remote controls for car stereos

2.1 Networking Concepts required for Forensics

Local Area Network (LAN) –

- Usually privately-owned networks
- Confined to a building or several buildings on a campus or company location.
- Usually used to connect personal computers for data interchange and to share resources such as printers and server machines.



(a) Bus (b) Ring

2.1 Networking Concepts required for Forensics

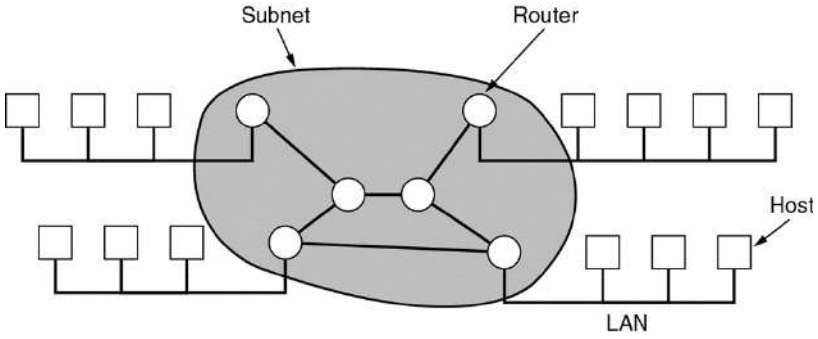
Metropolitan Area Network (MAN) –

- MANs are usually large enough to cover a city.
- Best known example – a cable TV network.
- Originally intended for TV only, it quickly became used for computer networks once the cable companies determined that there was money to be made.
- The topology of a MAN usually results in a series of computers with a single entry point at the **head end** of the network.
- It is at the head end that the MAN would be connected to another network.

2.1 Networking Concepts required for Forensics

Wide Area Network (WAN) –

- WANs are much larger than MANs, covering a whole country or other large geographical area.
- The user computers in a WAN are called **hosts**.
- Host computers on various LANs are connected via a **communication subnet**. The subnet consists of **routers** and transmission lines.
- A **router** is a specialized piece of switching hardware that is responsible for determining the direction that data packets should be sent.
- Routers are responsible for directing data down transmission lines from one LAN to another.



2.1 Networking Concepts required for Forensics

innovate achieve lead

Wireless Networks –

Wireless networks can be divided into three main categories:

1. **System Interconnection**
   - We can use wireless technology to interconnect our system.
     - wireless mouse
     - wireless keyboard
     - wireless PDA [Personal Digital Assistants]
   - Bluetooth is a wireless technology that would allow all sorts of digital devices to “talk” to each other just by being close.
2. **Wireless LANs**
   - Computers and printers can connect to the network with a radio communication link.
   - There is usually a (or some) central access point or base station where the radio connections are converted to wire connections.
   - Computers may also be able to talk directly to one another if close enough together.
3. **Wireless WANs**
   - Cell phone networks are a good example of wireless WANs.
   - We are on our third generation of wireless WANs – there was analog voice, digital voice, and now digital voice and data.
   - Distances are much greater than LANs, but bandwidth is much lower.

2.1 Networking Concepts required for Forensics

Internetworks –

- A collection of interconnected networks is called an **internetwork** or **internet**.
- Connections are usually made through **gateways** that can provide the translation between the two different technologies.
- An internetwork is formed when distinct networks are connected.

2.1 Networking Concepts required for Forensics

2.2 Working with Windows and DOS Systems, Linux Boot Processes and CLI Systems

The operating systems, DOS and Windows are mainly differentiated by the fact that DOS is a single tasking, single user, CLI based operating system developed in the year of 1979.

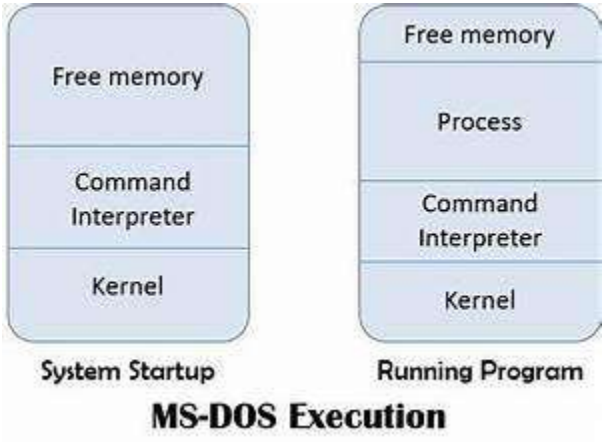
On the other hand, all the windows version are multitasking, multiuser and GUI based operating system.

DOS provides **single programming, single tasking and single user environment while windows offer multiprogramming, multitasking and multiuser system**.

DOS permitted the use of keyboard only while with windows, mouse and keyboard both can be used.

Windows supports multimedia application whereas DOS cannot support it. There are no drivers are used in DOS, therefore it involves the dealing with the hardware to get the job done.

However, windows involve the use of drivers which made the work easier.



MS-DOS Execution

2.2 Working with Windows and DOS Systems, Linux Boot Processes and CLI Systems

Windows is a Microsoft product there are various versions of Windows such as Windows 2000, Windows NT, Windows XP, Windows Vista, Windows 7, Windows 8 and Windows 10. Windows OS is created for serving features such as reliability, compatibility, performance, extensibility and internal support. It is GUI (Graphical User Interface) based where the instead of typing commands manually, we use icons and images to give instructions with the help of a mouse.

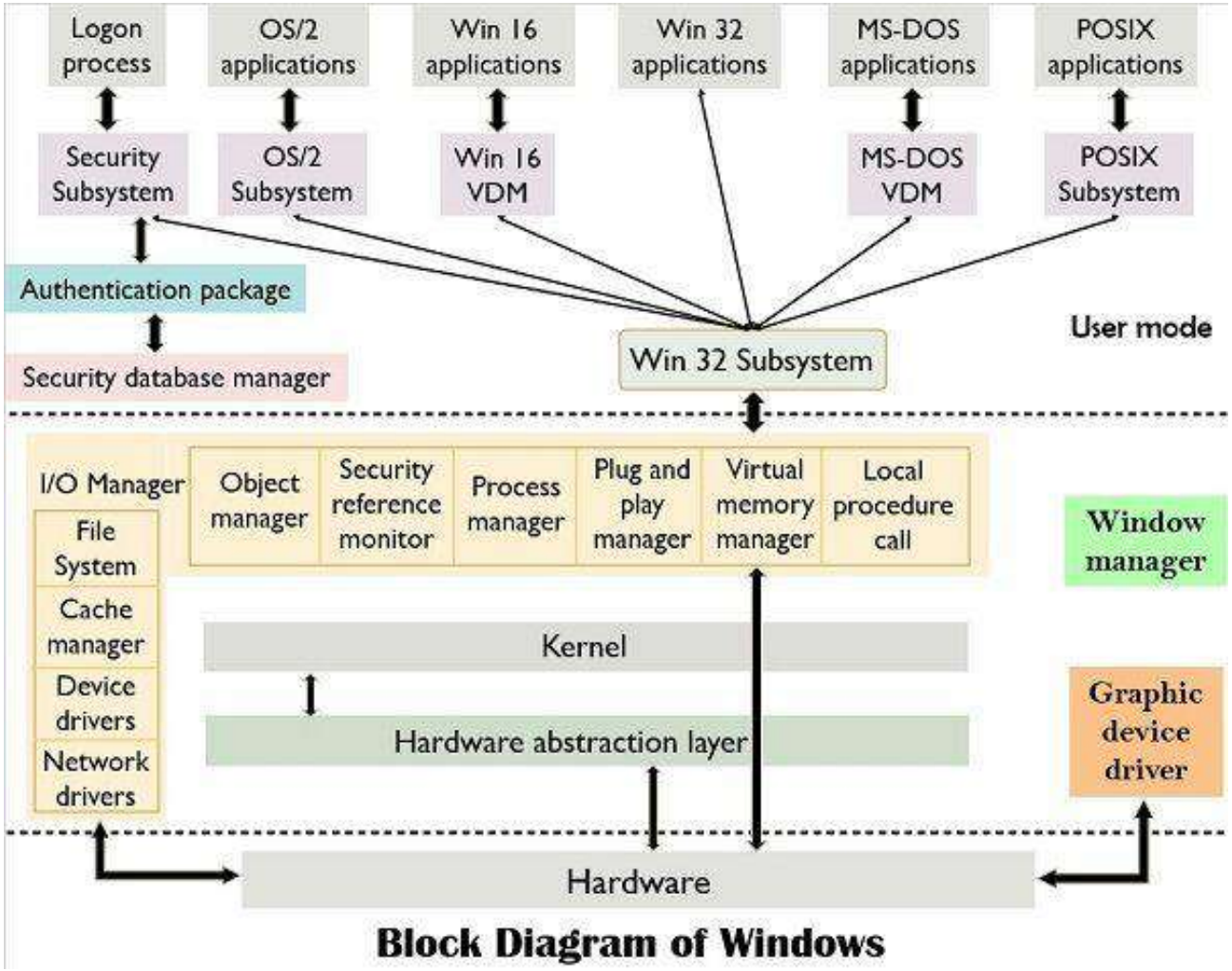
Windows is portable, initially written in C and C++ languages where processor reliable code is separated in a dynamic link library (DLL) known as the hardware abstraction layer (HAL). Upper layers of windows depend on HAL, inspite of the hardware. It is very reliable and handles error conditions with ease.

2.2 Working with Windows and DOS Systems, Linux Boot Processes and CLI Systems

Windows operating system can defend the system from defects and attacks with the help of hardware protection for the virtual memory and software protection mechanism for operating system resources.

It employs an NTFS file system which can easily recover from different kind of file system errors after the system crash.

2.2 Working with Windows and DOS Systems, Linux Boot Processes and CLI Systems



Block Diagram of Windows

2.2 Working with Windows and DOS Systems, Linux Boot Processes and CLI Systems

Linux Boot Processes -

An operating system (OS) is the low-level software that manages resources, controls peripherals, and provides basic services to other software. In Linux, there are 6 distinct stages in the typical booting process.

1. BIOS

- BIOS stands for Basic Input/Output System. In simple terms, the BIOS loads and executes the Master Boot Record (MBR) boot loader.
- When you first turn on your computer, the BIOS first performs some integrity checks of the HDD or SSD.
- Then, the BIOS searches for, loads, and executes the boot loader program, which can be found in the Master Boot Record (MBR). The MBR is sometimes on a USB stick or CD-ROM such as with a live installation of Linux.
- Once the boot loader program is detected, it's then loaded into memory and the BIOS gives control of the system to it.

2. MBR

- MBR stands for Master Boot Record, and is responsible for loading and executing the GRUB boot loader.
- The MBR is located in the 1st sector of the bootable disk, which is typically /dev/hda, or /dev/sda, depending on your hardware. The MBR also contains information about GRUB, or LILO in very old systems.

2.2 Working with Windows and DOS Systems, Linux Boot Processes and CLI Systems

Linux Boot Processes –

3. GRUB

- Sometimes called GNU GRUB, which is short for GNU GRand Unified Bootloader, is the typical boot loader for most modern Linux systems.

4. Kernel

- The kernel is often referred to as the core of any operating system, Linux included. It has complete control over everything in your system.
- In this stage of the boot process, the kernel that was selected by GRUB first mounts the root file system that's specified in the grub.conf file. Then it executes the /sbin/init program, which is always the first program to be executed. You can confirm this with its process id (PID), which should always be 1.
- The kernel then establishes a temporary root file system using Initial RAM Disk (initrd) until the real file system is mounted.

2.2 Working with Windows and DOS Systems, Linux Boot Processes and CLI Systems

Linux Boot Processes –

5. Init

- At this point, your system executes runlevel programs. At one point it would look for an init file, usually found at /etc/inittab to decide the Linux run level.
- Modern Linux systems use systemmd to choose a run level instead.

6. Runlevel programs

- Depending on which Linux distribution you have installed, you may be able to see different services getting started. For example, you might catch starting sendmail …. OK.
- These are known as runlevel programs, and are executed from different directories depending on your run level.

2.2 Working with Windows and DOS Systems, Linux Boot Processes and CLI Systems

CLI [Command Line Interface] Systems –

- CLI is a command line program that accepts text input to execute operating system functions.
- In the 1960s, using only computer terminals, this was the only way to interact with computers.
- In the 1970s an 1980s, command line input was commonly used by Unix systems and PC systems like MS-DOS and Apple DOS.
- Today, with graphical user interfaces (GUI), most users never use command-line interfaces (CLI).
- However, CLI is still used by software developers and system administrators to configure computers, install software, and access features that are not available in the graphical interface.

2.2 Working with Windows and DOS Systems, Linux Boot Processes and CLI Systems

Basic Linux CLI Commands

Command	Description
ls	List the directory (folder) system.
cd *pathname*	Change directory (folder) in the file system.
cd ..	Move one level up (one folder) in the file system.
cp	Copy a file to another folder.
mv	Move a file to another folder.
mkdir	Creates a new directory (folder).
rmdir	Remove a directory (folder).
clear	Clears the CLI window.
exit	Closes the CLI window.
man *command*	Shows the manual for a given command.

2.2 Working with Windows and DOS Systems, Linux Boot Processes and CLI Systems

Basic Windows CLI Commands

Command	Description
dir	List the directory (folder) system.
cd *pathname*	Change directory (folder) in the file system.
cd \	Move to the root folder of the file system.
cd ..	Move one level up (one folder) in the file system.
copy	Copy a file to another folder.
move	Move a file to another folder.
type *filename*	Type a file.
mkdir or md	Creates a new directory (folder).
rmdir or rd	Removes a directory (folder).
cls	Clears the CLI window.
exit	Closes the CLI window.
help *command*	Shows the manual for a given command.

2.3 Introduction to Forensics Science and Need for Digital Forensics, Digital Forensic Techniques

Introduction to Forensics Science –

- **Digital Forensics** is defined as the process of preservation, identification, extraction, and documentation of computer evidence which can be used by the court of law.
- It is a **science** of finding evidence from digital media like a computer, mobile phone, server, or network.
- Digital Forensics helps the forensic team to analyses, inspect, identifies, and preserve the digital evidence residing on various types of electronic devices.

2.3 Introduction to Forensics Science and Need for Digital Forensics, Digital Forensic Techniques

Need for Digital Forensics –

1. It helps to recover, analyse, and preserve computer and related materials in such a manner that it helps the investigation agency to present them as evidence in a court of law.
2. It helps to postulate the motive behind the crime and identity of the main culprit.
3. Designing procedures at a suspected crime scene which helps you to ensure that the digital evidence obtained is not corrupted.
4. Data acquisition and duplication: Recovering deleted files and deleted partitions from digital media to extract the evidence and validate them.
5. Helps you to identify the evidence quickly, and also allows you to estimate the potential impact of the malicious activity on the victim
6. Producing a computer forensic report which offers a complete report on the investigation process.
7. Preserving the evidence by following the chain of custody.

2.3 Introduction to Forensics Science and Need for Digital Forensics, Digital Forensic Techniques

Example Uses of Digital Forensics

In recent time, commercial organizations have used digital forensics in following a type of cases:

- Intellectual Property theft
- Industrial espionage
- Employment disputes
- Fraud investigations
- Inappropriate use of the Internet and email in the workplace
- Forgeries related matters
- Bankruptcy investigations
- Issues concern with the regulatory compliance

2.3 Introduction to Forensics Science and Need for Digital Forensics, Digital Forensic Techniques

Advantages of Digital forensics

Here, are pros/benefits of Digital forensics

- To ensure the integrity of the computer system.
- To produce evidence in the court, which can lead to the punishment of the culprit.
- It helps the companies to capture important information if their computer systems or networks are compromised.
- Efficiently tracks down cybercriminals from anywhere in the world.
- Helps to protect the organization's money and valuable time.
- Allows to extract, process, and interpret the factual evidence, so it proves the cybercriminal action's in the court.

2.3 Introduction to Forensics Science and Need for Digital Forensics, Digital Forensic Techniques

Disadvantages of Digital Forensics -

Here, are major cos/ drawbacks of using Digital Forensic

- Digital evidence accepted into court. However, it is must be proved that there is no tampering
- Producing electronic records and storing them is an extremely costly affair
- Legal practitioners must have extensive computer knowledge
- Need to produce authentic and convincing evidence
- If the tool used for digital forensic is not according to specified standards, then in the court of law, the evidence can be disapproved by justice.
- Lack of technical knowledge by the investigating officer might not offer the desired result

2.3 Introduction to Forensics Science and Need for Digital Forensics, Digital Forensic Techniques

Challenges faced by Digital Forensics

Here, are major challenges faced by the Digital Forensic:

- The increase of PC's and extensive use of internet access
- Easy availability of hacking tools
- Lack of physical evidence makes prosecution difficult.
- The large amount of storage space into Terabytes that makes this investigation job difficult.
- Any technological changes require an upgrade or changes to solutions.

2.3 Introduction to Forensics Science and Need for Digital Forensics, Digital Forensic Techniques

Digital Forensic Techniques –

Disk Forensics:

- It deals with extracting data from storage media by searching active, modified, or deleted files.

Network Forensics:

- It is a sub-branch of digital forensics. It is related to monitoring and analysis of computer network traffic to collect important information and legal evidence.

Wireless Forensics:

- It is a division of network forensics. The main aim of wireless forensics is to offers the tools need to collect and analyse the data from wireless network traffic.

Database Forensics:

- It is a branch of digital forensics relating to the study and examination of databases and their related metadata.

2.3 Introduction to Forensics Science and Need for Digital Forensics, Digital Forensic Techniques

Digital Forensic Techniques –

Malware Forensics:

- This branch deals with the identification of malicious code, to study their payload, viruses, worms, etc.

Email Forensics

- Deals with recovery and analysis of emails, including deleted emails, calendars, and contacts.

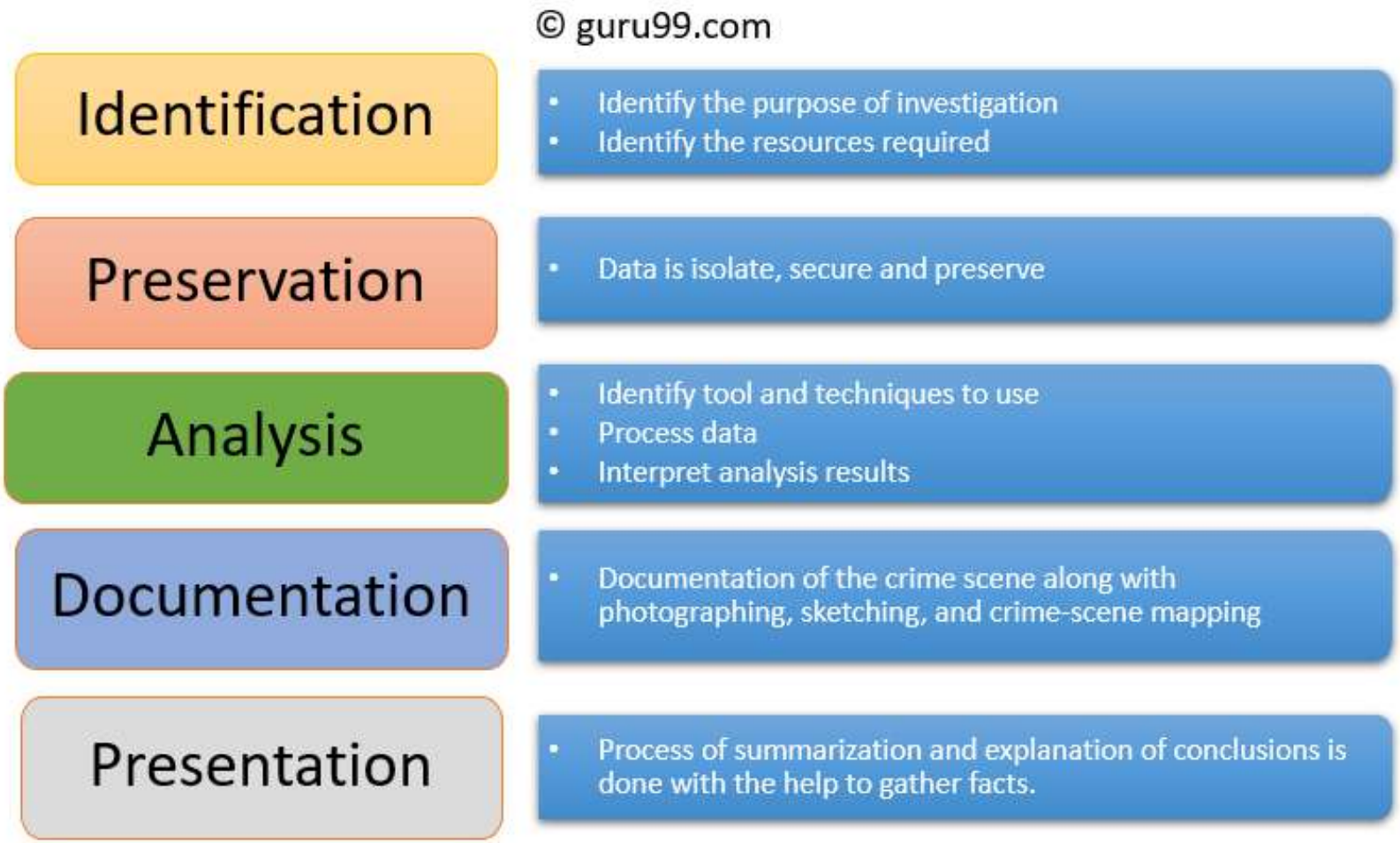
Memory Forensics:

- It deals with collecting data from system memory (system registers, cache, RAM) in raw form and then carving the data from Raw dump.

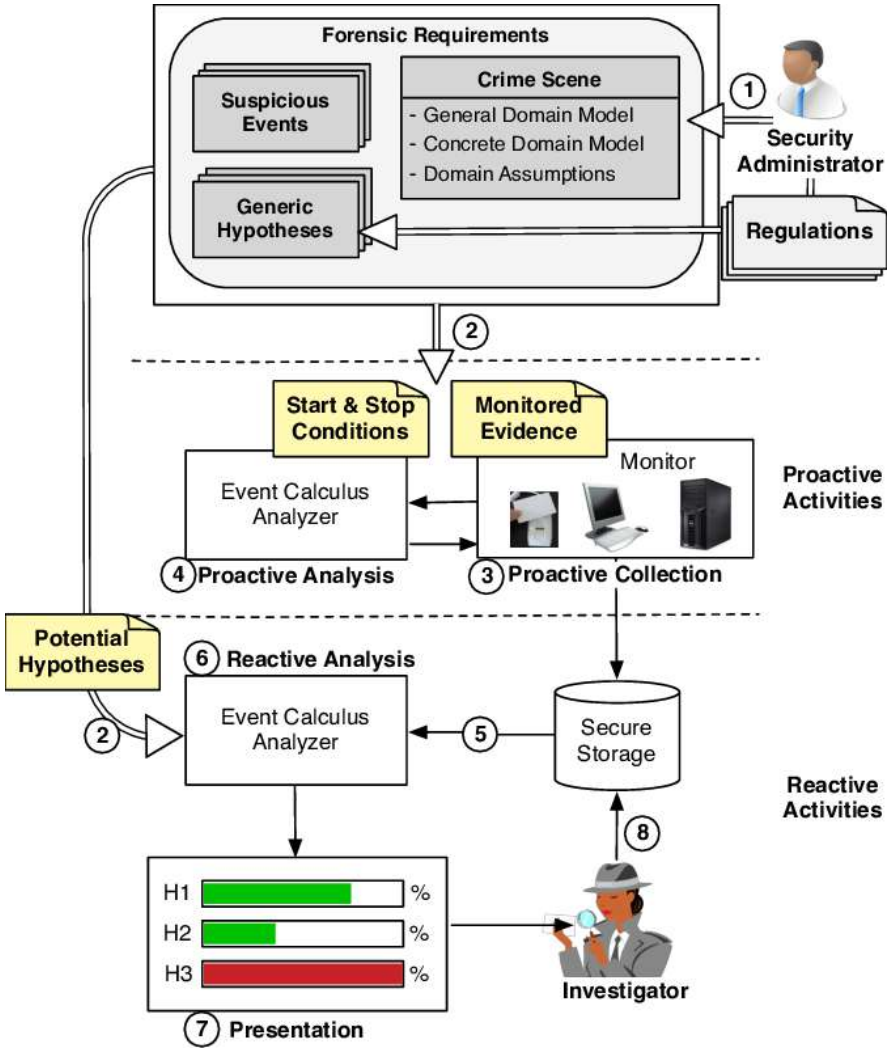
Mobile Phone Forensics:

- It mainly deals with the examination and analysis of mobile devices. It helps to retrieve phone and SIM contacts, call logs, incoming, and outgoing SMS/MMS, Audio, videos, etc.

2.3 Introduction to Forensics Science and Need for Digital Forensics, Digital Forensic Techniques



2.3 Introduction to Forensics Science and Need for Digital Forensics, Digital Forensic Techniques



2.4 Understanding the Digital Forensics Profession

- By the 1970s, electronic crimes were increasing, especially in the financial sector.
- To be a successful computer forensics investigator, you must be familiar with more than one computing platform.
- The law of search and seizure protects the rights of all people, excluding people suspected of crimes.
- The definition of digital forensics has evolved over the years from simply involving and securing and analyzing digital information stored on a computer for use as evidence in civil, criminal, or administrative cases.

2.4 Understanding the Digital Forensics Profession

Thank you

BITS Pilani

Prof. Pradnya Kashikar

WILP-CSIS

BITS Pilani
Pilani Campus

innovate achieve lead

BITS Pilani

Pilani Campus

SS ZG588 - Cyber Crimes, Forensics and Incident Handling

Contact Session - 3

Course Objectives

No	Description
CO1	Enhancing awareness of recent Cyber Crime trends and learn Investigating Cyber Crimes
CO2	Introduce Cyberspace Infrastructure attacks and handling Organization Cybersecurity Issues
CO3	Understand Digital Forensics Process, Models, Analysis and Validation, Incident Detection and Response

Text Book(s)

innovate achieve lead

T1	Computer Forensics and Cyber Crime - An Introduction 3rd Edition by Marjie T. Britz, Ph.D., Professor of Criminal Justice, Clemson University
T2	Bill Nelson, A. Philips, F. Enfinger, C. K. Steuart, Computer Forensics and Investigations, Course Technology (Cengage Learning), Indian edition, 2009
T3	Incident Response & Computer Forensics, 3rd Edition by Jason T. Luttgens and Matthew Pepe and Kevin Mandia
R1	Guide to Computer Forensics and Investigations: Processing Digital Evidence 5th Edition by Bill Nelson, Amelia Phillips and Christopher Steuart
R2	The Basics of Digital Forensics, by John Sammons
R3	Computer Network Security and Cyber Ethics 4th Edition, by Joseph Migga Kizza
R4	Computer Forensics_ Investigating Network Intrusions and Cyber Crime: EC-Council Press

Learning Outcomes -

No	Learning Outcomes
LO1	Fundamental understanding and Information on Cyber Crimes, Digital Forensics Objectives and Incident Detection and Response Reports.
LO2	Learn on how to prepare investigation on computer-related incidents or crimes and summarize.
LO3	Understand on digital forensics process, models and analysis by taking a systematic approach
LO4	Explore on evaluating needs, validating and testing digital forensics tools, Generating Incident Report Findings, and Emerging Cybercrime Trends and Issues

Module 3 - Computer Crime and Identity Theft / Fraud

3.1 Traditional Computer Crime; Contemporary Computer Crime

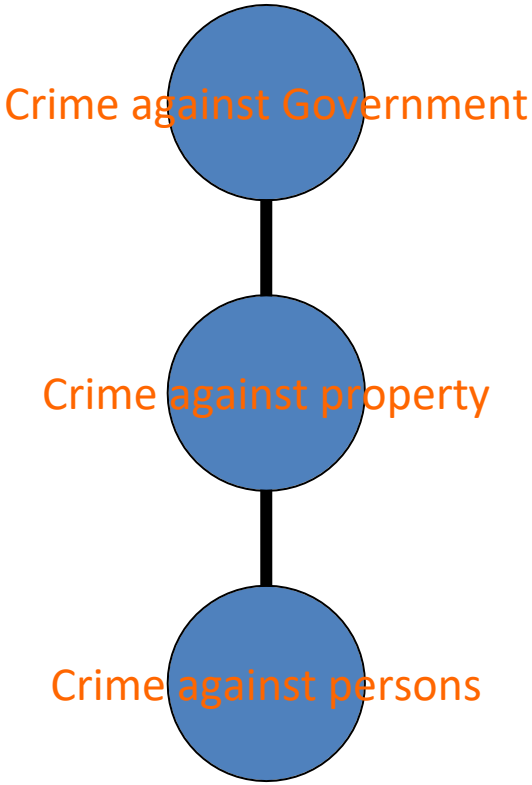
3.2 Identity Theft and Identity Fraud; Identifying Digital Evidence; Preparing for a search; Securing a computer crime scene;

3.3 Seizing Digital Evidence at the scene; Storing Digital Evidence; Obtaining a Digital Hash; Reviewing a Case

3	Computer Crime and Identity Theft/Fraud	**Traditional Computer Crime; Contemporary Computer Crime**	T1,T2, R1
		Identity Theft and Identity Fraud; Identifying Digital Evidence; Preparing for a search; Securing a computer crime scene;	
		Seizing Digital Evidence at the scene; Storing Digital Evidence; Obtaining a Digital Hash; Reviewing a Case	

3.1. Traditional Computer Crime and Contemporary Computer Crime

Computer Crime, **E-Crime**, **Hi-Tech Crime** or **Electronic Crime** is where a computer is the target of a crime or is the means adopted to commit a crime.



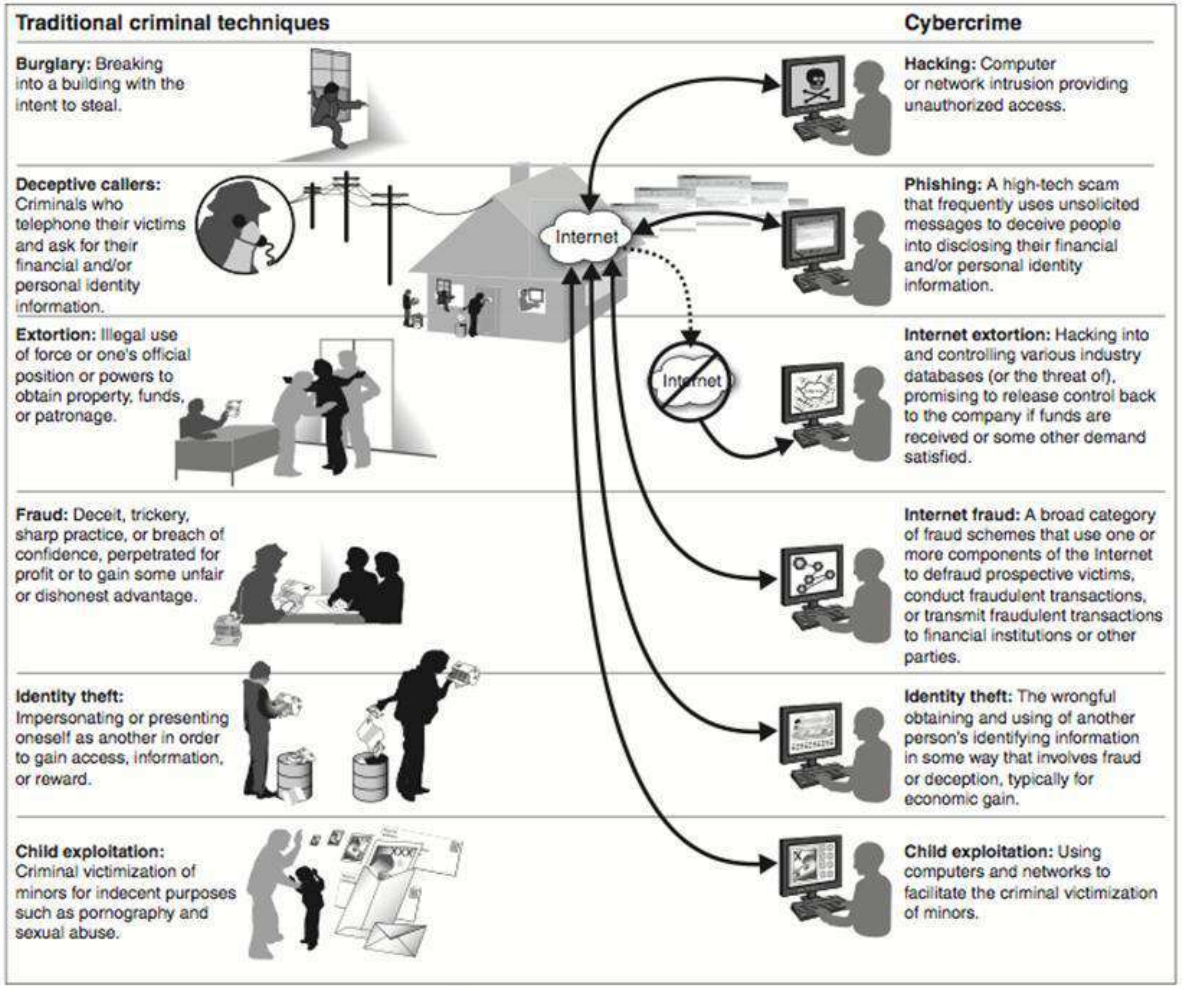
3.1. Traditional Computer Crime and Contemporary Computer Crime

All activities performed with criminal intentions in Cyber space or webs are considered to be **Cyber Crime**. These could be either the criminal activities in the conventional sense by use electronic media or activities, newly evolved with the progress of Information Technology. The classification of Cyber Crime can be broadly done as follows.

- Credit card frauds
- Cyber pornography
- Sale of illegal articles-narcotics, weapons, wildlife
- Intellectual Property crimes-software piracy, copyright infringement, trademarks violations, theft of computer source code
- Email spoofing
- Forgery
- Defamation
- Cyber stalking (section 509 IPC)
- Phishing
- Cyber terrorism
- Online gambling
- Hacking

3.1. Traditional Computer Crime and Contemporary Computer Crime

Figure 1: Comparison between Traditional Criminal Techniques and Cybercrime



Source: GAO.

3.1. Traditional Computer Crime and Contemporary Computer Crime

3.1. Traditional Computer Crime and Contemporary Computer Crime

3.2. Identity Theft and Identity Fraud, Identifying Digital Evidence, Preparing for a search, Securing a computer crime scene

Identity theft and identity fraud are terms used to refer to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain.

Food for thought:

1. People who seek out your personal information and then use it to commit crimes are called:_____.

2. Which of the following are ways to help prevent identity theft. (Check all that apply.)

__A. Never send personal information via email or instant messages.

__B. Always send personal information via email or instant messages.

__C. Lock my office door.

__D. Don't tell anybody my name.

3.2. Identity Theft and Identity Fraud

Answers:

1. Identity thieves
2. A and C are correct. D would probably help too, but seems a bit extreme!

Identity theft and identity fraud

These are the terms used to refer to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain.

https://www.rd.com/list/shred-documents/

https://www.cnet.com/culture/thunderstruck-a-tale-of-malware-acdc-and-irans-nukes/

3.2. Identity Theft and Identity Fraud

3.2. Identifying Digital Evidence, Preparing for a search, Securing a computer crime scene

Types of Evidence -

- **Real Evidence**: Real evidence is any evidence that speaks for itself without relying on anything else. In electronic terms, this can be a log produced by an audit function— provided that the log can be shown to be free from contamination.

- **Testimonial Evidence:** Testimonial evidence is any evidence supplied by a witness. As long as the witness can be considered reliable, testimonial evidence can be almost as powerful as real evidence.

- **Hearsay:** Hearsay is any evidence presented by a person who was not a direct witness. Hearsay is generally inadmissible in court and should be avoided.

3.2. Identifying Digital Evidence, Preparing for a search, Securing a computer crime scene

Minimize handling and corruption of original data:

Once you've created a master copy of the original data, don't touch it or the original. Any changes made to the originals will affect the outcomes of any analysis later done to copies.

Account for any changes and keep detailed logs of your actions:

Sometimes evidence alteration is unavoidable. In these cases, it is absolutely essential that the nature, extent, and reasons for the changes be documented.

Comply with the five rules of evidence:

Following these rules is essential to guaranteeing successful evidence collection.

Do not exceed your knowledge:

If you ever find yourself —out of your depth,‖ either go and learn more before continuing (if time is available) or find someone who knows the territory.

3.2. Identifying Digital Evidence, Preparing for a search, Securing a computer crime scene

Follow your local security policy:

If you fail to comply with your company's security policy, you may find yourself with some difficulties.

Capture as accurate an image of the system as possible:

Capturing an accurate image of the system is related to minimizing the handling or corruption of original data.

Be prepared to testify:

If you're not willing to testify to the evidence you have collected, you might as well stop before you start. No one is going to believe you if they can't replicate your actions and reach the same results.

Work fast:

The faster you work, the less likely the data is going to change. Volatile evidence may vanish entirely if you don't collect it in time. If multiple systems are involved, work parallel.

3.2. Identifying Digital Evidence, Preparing for a search, Securing a computer crime scene

Proceed from volatile to persistent evidence:

Always try to collect the most volatile evidence first.

Don’t shutdown before collecting evidence:

You should never, ever shutdown a system before you collect the evidence. Not only do you lose any volatile evidence, but also the attacker may have trojaned the startup and shutdown scripts, plug-and-play devices may alter the system configuration, and temporary file systems may be wiped out.

Don’t run any programs on the affected system:

The attacker may have left trojaned programs and libraries on the system; you may inadvertently trigger something that could change or destroy the evidence you’re looking for.

https://resources.infosecinstitute.com/topic/7-best-computer-forensics-tools/

3.2. Identifying Digital Evidence, Preparing for a search, Securing a computer crime scene

Collection Steps –

1. Find the Evidence: Use a checklist. Not only does it help you to collect evidence, but it also can be used to double-check that everything you are looking for is there.
2. Find the Relevant Data: Once you've found the evidence, you must figure out what part of it is relevant to the case.
3. Create an Order of Volatility: The order of volatility for your system is a good guide and ensures that you minimize loss of uncorrupted evidence.
4. Remove external avenues of change: It is essential that you avoid alterations to the original data.
5. Collect the Evidence: Collect the evidence using the appropriate tools for the job.
6. Document everything: Collection procedures may be questioned later, so it is important that you document everything you do. Timestamps, digital signatures, and signed statements are all important.
7. https://www.forensicsciencesimplified.org/digital/how.html

3.3. Seizing Digital Evidence at the scene, Storing Digital Evidence, Obtaining a Digital Hash, Reviewing a Case

There are two basic forms of collection:

Freezing the Scene –

- It involves taking a snapshot of the system in its compromised state. You should then start to collect whatever data is important onto removable non-volatile media in a standard format.
- All data collected should have a cryptographic message digest created, and those digests should be compared to the originals for verification.

Honeypotting –

- It is the process of creating a replica system and luring the attacker into it for further monitoring.
- The placement of misleading information and the attacker's response to it is a good method for determining the attacker's motives.

3.3. Seizing Digital Evidence at the scene, Storing Digital Evidence, Obtaining a Digital Hash, Reviewing a Case

Searching and Seizing

1. There is no one methodology for performing a computer forensic investigation and analysis.
2. There are too many variables for to be just one way. Some of the typical variable that comes to the mind includes operating systems; software applications; cryptographic algorithms and applications; and hardware platforms.
3. But moving beyond these obvious variables spring other equally challenging variables: law, international boundaries, publicity, and methodology.

3.3.1. Seizing Digital Evidence at the scene,

1. With proper search warrants, law enforcement can seize all computing systems and peripherals.
2. In corporate investigations, you might have similar authority; however, you might have the authority only to make an image of the suspect's drive.
3. Depending on company policies, corporate investigators rarely have the authority to seize all computers and peripherals.
4. You might be looking for specific evidence, such a particular e-mail message or spreadsheet.
5. In a criminal matter, investigators seize entire drives to preserve as much information as possible and ensure that no evidence is overlooked.
6. If you have any questions, doubts, or concerns, consult with your attorney for additional guidance

3.3.2. Storing Digital Evidence

1. With digital evidence, you need to consider how and on what type of media to save it and what type of storage device is recommended to secure it.
2. The media you use to store digital Evidence usually depends on how long you need to keep it.
3. If you investigate criminal matters, store the evidence as long as you can.
4. The ideal media on which to store digital data are CD- Rs or DVDs.
5. These media have long lives, but copying data to them takes a long time.
6. Older CDs had lives up to five years. Research is currently being done on CD-Rs and CD-RWs with life spans of only one or two years.
7. Today's larger drives demand more storage capacity; 200 GB drives are common, and DVDs can store up to only 17 GB of data.

3.3.3. Obtaining a Digital Hash

1. To verify data integrity, different methods of obtaining a unique identity for file data have been developed.
2. One of the first methods, the Cyclic Redundancy Check (CRC) is a mathematical algorithm that determines whether a file's contents have changed.
3. The most recent version is CRC-32. CRC, however, is not considered a forensic hashing algorithm.
4. The first algorithm for computer forensics use was Message Digest 5 (MD5). Like CRC, MD5 is a mathematical formula that translates a file into a hexadecimal code value, or a hash value.
5. If a bit or byte in the file changes, it alters the hash value, a unique hexadecimal value that identifies a file or drive. (Before you process or analyse a file, you can use a software tool to calculate its hash value.)
6. After you process the file, you produce another digital hash. If it's the same as the original one, you can verify the integrity of your digital evidence with mathematical proof that the file didn't change

3.3.4. Reviewing a Case

1. Some of which are repeated in the following list.
2. Later in this section, you apply each task to a hypothetical investigation to create a preparation plan for searching an incident or crime scene.
3. The following are the general tasks you perform in any computer forensics case:

- Identify the case requirements.
- Plan your investigation.
- Conduct the investigation.
- Complete the case report.
- Critique the case.

Case study

https://www.iasj.net/iasj/download/6e2dd4cac5720eb3

Thank you

BITS Pilani

Prof. Pradnya Kashikar

WILP-CSIS

BITS Pilani
Pilani Campus

innovate achieve lead

BITS Pilani

Pilani Campus

SS ZG588 - Cyber Crimes, Forensics and Incident Handling

Contact Session - 4

Course Objectives

No	Description
CO1	Enhancing awareness of recent Cyber Crime trends and learn Investigating Cyber Crimes
CO2	Introduce Cyberspace Infrastructure attacks and handling Organization Cybersecurity Issues
CO3	Understand Digital Forensics Process, Models, Analysis and Validation, Incident Detection and Response

Text Book(s)

innovate achieve lead

T1	Computer Forensics and Cyber Crime - An Introduction 3rd Edition by Marjie T. Britz, Ph.D., Professor of Criminal Justice, Clemson University
T2	Bill Nelson, A. Philips, F. Enfinger, C. K. Steuart, Computer Forensics and Investigations, Course Technology (Cengage Learning), Indian edition, 2009
T3	Incident Response & Computer Forensics, 3rd Edition by Jason T. Luttgens and Matthew Pepe and Kevin Mandia
R1	Guide to Computer Forensics and Investigations: Processing Digital Evidence 5th Edition by Bill Nelson, Amelia Phillips and Christopher Steuart
R2	The Basics of Digital Forensics, by John Sammons
R3	Computer Network Security and Cyber Ethics 4th Edition, by Joseph Migga Kizza
R4	Computer Forensics_ Investigating Network Intrusions and Cyber Crime: EC-Council Press

Learning Outcomes -

No	Learning Outcomes
LO1	Fundamental understanding and Information on Cyber Crimes, Digital Forensics Objectives and Incident Detection and Response Reports.
LO2	Learn on how to prepare investigation on computer-related incidents or crimes and summarize.
LO3	Understand on digital forensics process, models and analysis by taking a systematic approach
LO4	Explore on evaluating needs, validating and testing digital forensics tools, Generating Incident Report Findings, and Emerging Cybercrime Trends and Issues

4	Digital Forensic Process, Analysis and Validation	**Phases of Digital Forensic Process**	T1, R1, R2
		Digital Forensic Process Models	
		Digital Forensics Analysis and Validation	

Module 4 - Digital Forensic Process, Analysis and Validation

innovate achieve lead

4.1 Phases of Digital Forensic Process

4.2 Digital Forensic Process Models

4.3 Digital Forensics Analysis and Validation

4.1. Phases of Digital Forensic Process

- Digital Forensics helps the forensic team to analyse, inspect, identify, and preserve the digital evidence residing on various types of electronic devices.
- Computer forensics also referred to as computer forensic analysis, electronic discovery, electronic evidence discovery, digital discovery, data recovery, data discovery, computer analysis, and computer examination.
- Computer evidence can be useful in criminal cases, civil disputes, and human resources/ employment proceedings.

4.1. Phases of Digital Forensic Process

Important landmarks from the history of Digital Forensics:

- Hans Gross (1847 -1915): First use of scientific study to head criminal investigations
- FBI (1932): Set up a lab to offer forensics services to all field agents and other law authorities across the USA.
- In 1978 the first computer crime was recognized in the Florida Computer Crime Act.
- Francis Galton (1982 - 1991): Conducted first recorded study of fingerprints
- In 1992, the term Computer Forensics was used in academic literature.

4.1. Phases of Digital Forensic Process

- 1995 International Organization on Computer Evidence (IOCE) was formed.
- In 2000, the First FBI Regional Computer Forensic Laboratory established.
- In 2002, Scientific Working Group on Digital Evidence (SWGDE) published the first book about digital forensic called "Best practices for Computer Forensics".
- In 2010, Simson Garfinkel identified issues facing digital investigations.

4.1. Phases of Digital Forensic Process

Intent:

- Data acquisition and duplication: Recovering deleted files and deleted partitions from digital media to extract the evidence and validate them.
- Helps you to identify the evidence quickly, and also allows you to estimate the potential impact of the malicious activity on the victim
- Producing a computer forensic report which offers a complete report on the investigation process.
- Preserving the evidence by following the chain of custody.

4.1. Phases of Digital Forensic Process

Intent:

- It helps to recover, analyze, and preserve computer and related materials in such a manner that it helps the investigation agency to present them as evidence in a court of law.
- It helps to postulate the motive behind the crime and identity of the main culprit.
- Designing procedures at a suspected crime scene which helps you to ensure that the digital evidence obtained is not corrupted.

- https://www.computer.org/publications/tech-news/research/digital-forensics-security-challenges-cybercrime

FTK Imager - Forensic Acquisition Tool - FTK Imager Tutorial - FTK Image Loading Analysis - YouTube

4.1. Phases of Digital Forensic Process

Uses of Computer Forensics:

- Processing hidden files — files that are not visible or accessible to the user — that contain past usage information. Often, this process requires reconstructing and analyzing the date codes for each file and determining when each file was created, last modified, last accessed and when deleted.
- Running a string-search for e-mail, when no e-mail client is obvious

4.1. Phases of Digital Forensic Process

Uses of Computer Forensics:

- Recovering deleted files such as documents, graphics, and photos.
- Searching unallocated space on the hard drive, places where an abundance of data often resides.
- Tracing artifacts, those tidbits of data left behind by the operating system. Our experts know how to find these artifacts and, more importantly, they know how to evaluate the value of the information they find

4.1. Phases of Digital Forensic Process

"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

4.1. Phases of Digital Forensic Process

Process of Digital forensics includes following phases:

1. Identification
2. Preservation
3. Analysis
4. Documentation
5. Presentation

4.1. Phases of Digital Forensic Process

1. Identification:

- First, find the evidence, noting where it is stored.
- Identify the purpose of the investigation
- The identification process mainly includes things like what evidence is present, where it is stored, and lastly, how it is stored (in which format)
- Also identify the resources required.
- Electronic storage media can be personal computers, Mobile phones, PDAs, etc.

4.1. Phases of Digital Forensic Process

2. Preservation –

- Isolate the data before you preserve.
- This includes preventing people from possibly tampering with the evidence.
- Care should be taken that digital evidence is not tampered with.
- Data is secured by using various security mechanisms.

4.1. Phases of Digital Forensic Process

3. Analysis –

- Identify tools and techniques to use
- Investigation agents reconstruct fragments of data
- Process the data
- Draw conclusions based on evidence found.
- It might take numerous iterations of examination to support a specific crime theory.
- Interpret analysis results using various tools and softwares

4.1. Phases of Digital Forensic Process

4. Documentation –

- Following that, create a record of all the data to recreate the crime scene.
- Documentation should be maintained related to crime scene including photographs, cctv footage, sketching, logs, videos, crime-scene mapping, phone calls and chatting records, communication and activity maps.
- It helps in recreating the crime scene and reviewing it.

4.1. Phases of Digital Forensic Process

5. Presentation –

- Lastly, summarize and draw a conclusion.
- Process of summarization and explanations of conclusions is done to gather the facts
- In this last step, the process of summarization and explanation of conclusions is done.
- However, it should be written in a layperson's terms using abstracted terminologies.
- All abstracted terminologies should reference the specific details.

4.2. Digital Forensic Process Models

A. Computer Forensic Investigative Process (1984)

- Methodology for dealing with digital evidence investigation was proposed by pollitt. It has 4 distinct phases.

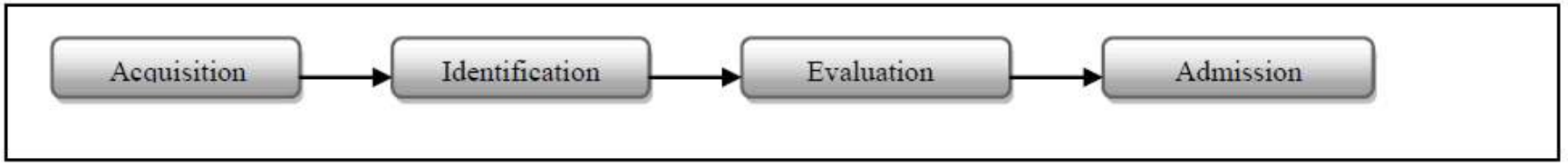


Figure 1: Computer Forensic Investigative Process

- In Acquisition phase, evidence was acquired in acceptable manner with proper approval from authority.
- It is followed by Identification phase whereby the tasks to identify the digital components from the acquired evidence and converting it to the format understood by human.
- The Evaluation phase comprise of the task to determine whether the components identified in the previous phase, is indeed relevant to the case being investigated and can be considered as a legitimate evidence.
- In the final phase, Admission, the acquired & extracted evidence is presented in the court of law

4.2. Digital Forensic Process Models

B. DFRWS Investigative Model (2001)

- G. Palmer held the 1st Digital Forensics Research Workshop (DFRWS) and proposed a general purpose digital forensics investigation process. It has 6 phases.

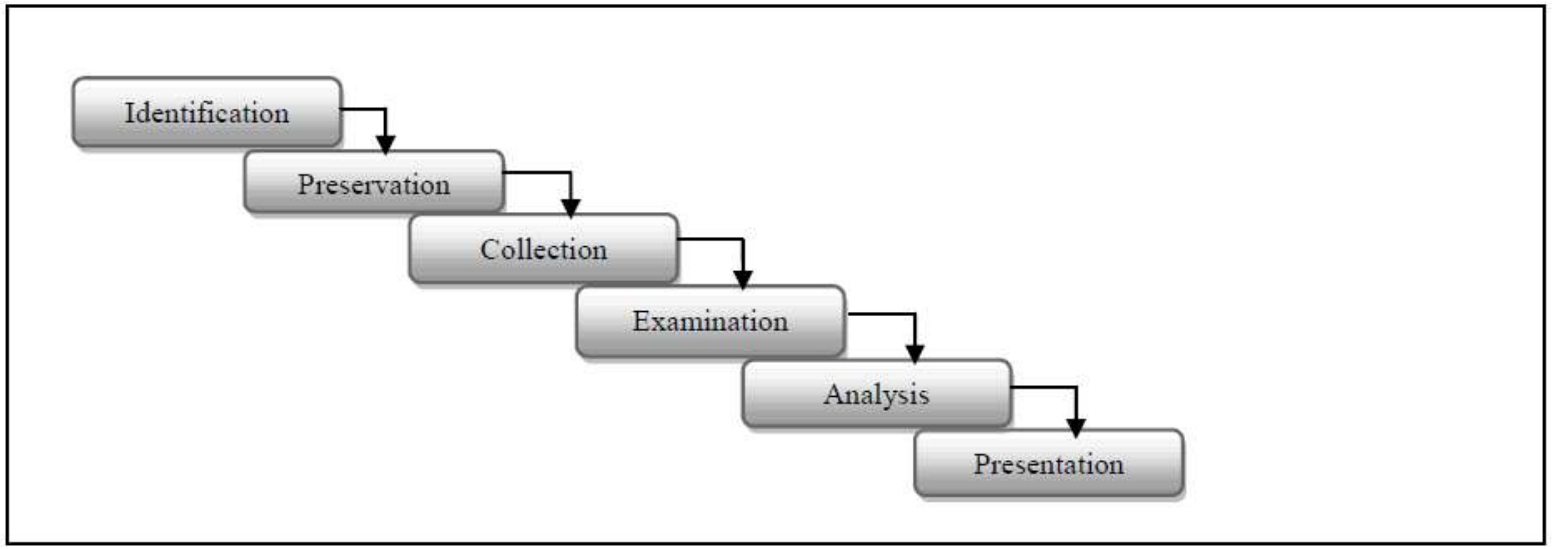


Figure2: DFRWS Investigative Model

4.2. Digital Forensic Process Models

- DFRWS Investigative model started with an Identification phase, in which profile detection, system monitoring, audit analysis, etc, were performed.
- It is immediately followed by Preservation phase, involving tasks such as setting up a proper case management and ensuring an acceptable chain of custody.
- This phase is crucial so as to ensure that the data collected is free from contamination.
- The next phase is known as Collection, in which relevant data are being collected based on the approved methods utilizing various recovery techniques.
- Following this phase are two crucial phases, namely, Examination phase and Analysis phase.
- In these two phases, tasks such as evidence tracing, evidence validation, recovery of hidden/encrypted data, data mining, timeline, etc, were performed.
- The last phase is Presentation. Tasks related to this phase are documentation, expert testimony, etc

4.2. Digital Forensic Process Models

C. Abstract Digital Forensics Model (ADFM) (2002)

- Reith, Carr & Gunsch, proposed an enhanced model known as Abstract Digital Forensic Model. In this model, there is three additional phases than DFRWS, thus expanding the number of phases to nine.

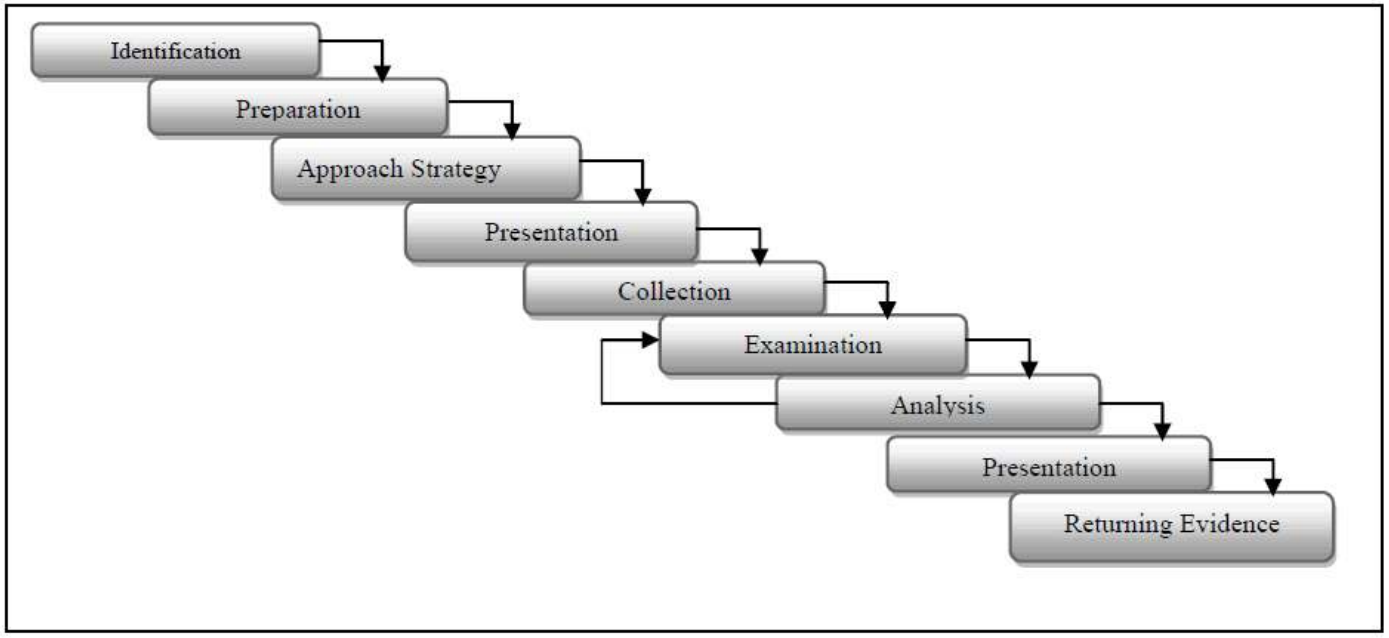


Figure 3: Abstract Digital Forensics Model

4.2. Digital Forensic Process Models

The 3 significant phases introduced in this model were Preparation, Approach Strategy and Returning Evidence.

In Preparation phase, activity such as preparing tools, identify techniques and getting management support, were done.

Approach Strategy was introduced with the objective to maximize the acquisition of untainted evidence and at the same time to minimize any negative impact to the victim and surrounding people.

In order to ensure that evidences are safely return to the rightful owner or properly disposed, the Returning Evidence phase was also introduced.

https://www.geeksforgeeks.org/chain-of-custody-digital-forensics/#:~:text=Chain%20of%20Custody%20refers%20to,evidence%20may%20be

4.2. Digital Forensic Process Models

- The 1st phase in ADFM is Identification phase. In this phase, the task to recognize and determine type of incident is performed. Once the incident type was ascertained, the next phase, Preparation, is conducted, followed by Approach Strategy phase.
- Physical and digital data acquired must be properly isolated, secured and preserved. There is also a need to pay attention to a proper chain of custody.
- All of these tasks are performed under Preservation phase. Next is the Collection phase, whereby, data extraction and duplication were done. Identification and locating the potential evidence from the collected data, using a systematic approach are conducted in the next following phase, known as Examination phase.
- The task of determining the significant of evidence and drawing conclusion based on the evidence found is done in Analysis phase.
- In the following phase, Presentation phase, the findings are summarized and presented. The investigation processes is completed with the carrying out of Returning Evidence phase.

4.2. Digital Forensic Process Models

D. Integrated Digital Investigation Process (IDIP) (2003)

- Integrated Digital investigation process was proposed by Carrier & Spafford in 2003, to combine the various available investigative processes into one integrated model. The author introduces the concept of digital crime scene which refers to the virtual environment created by software and hardware where digital evidence of an incident or crime exists.

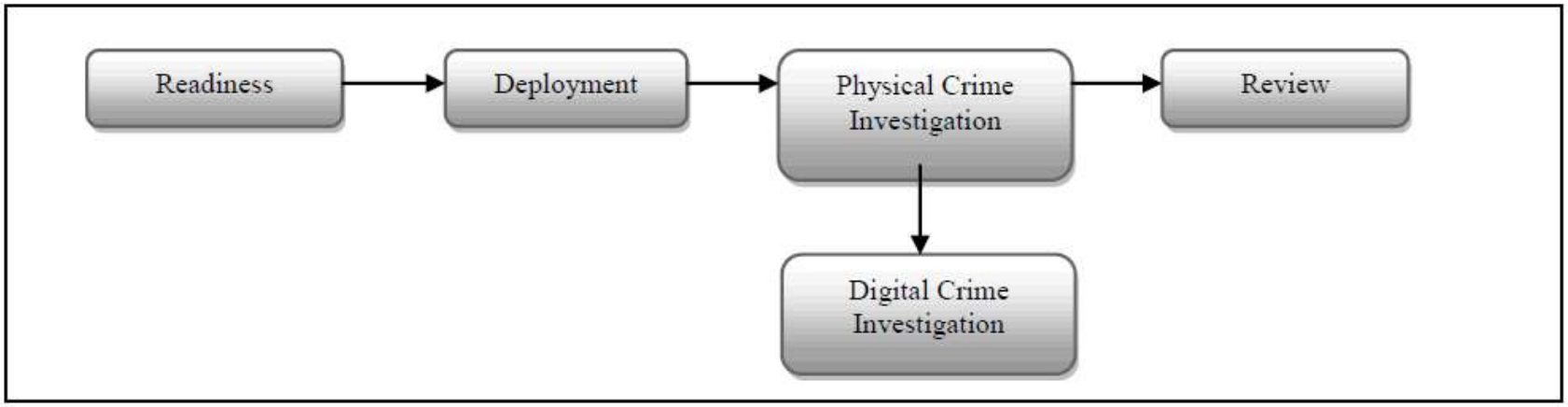
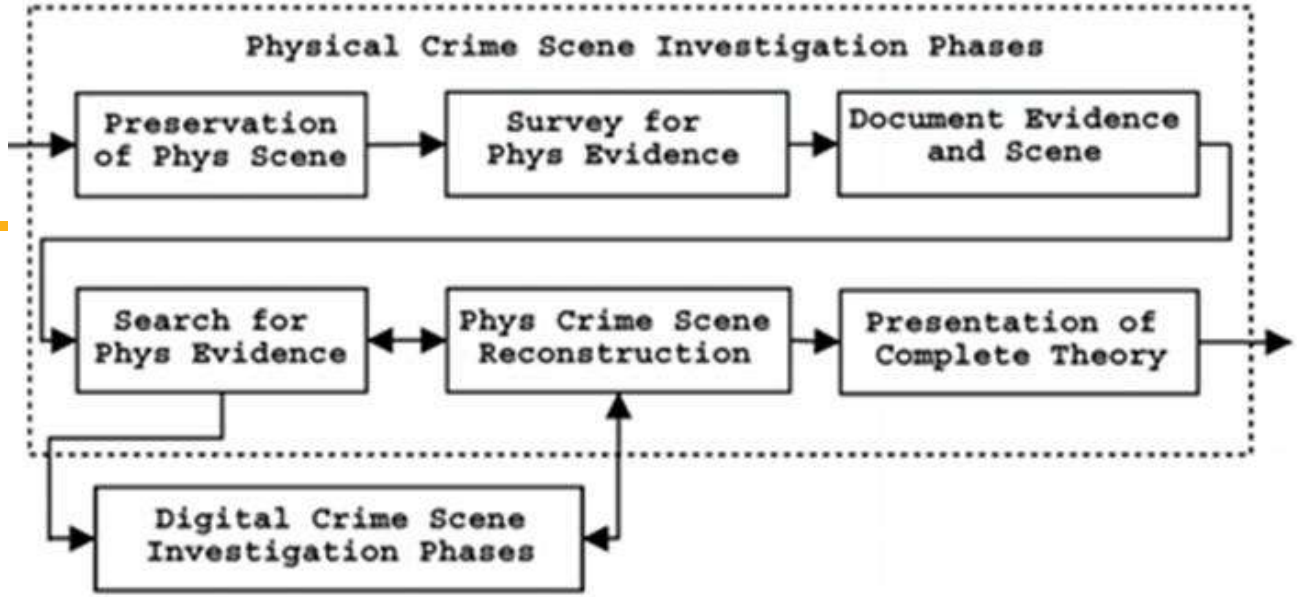
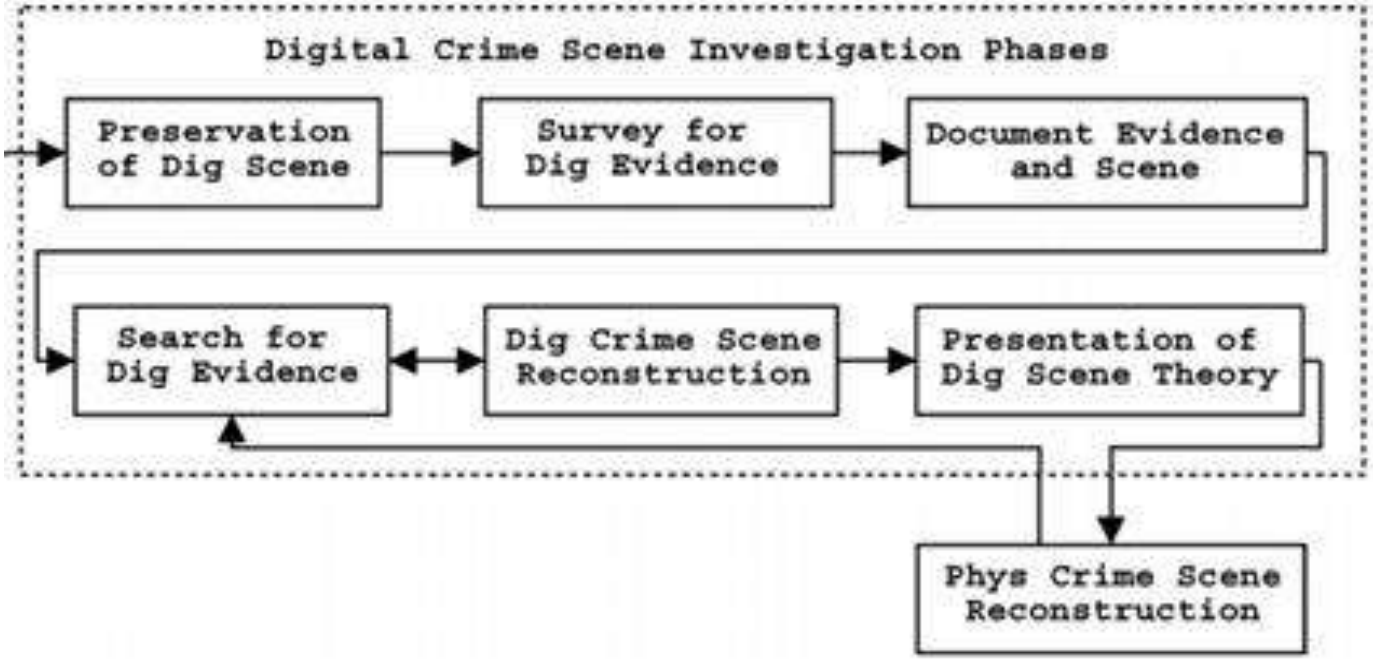


Figure 4: Integrated Digital Investigation Process


Physical Crime Scene Investigation Phases
Preservation of Phys Scene
Survey for Phys Evidence
Document Evidence and Scene
Search for Phys Evidence
Phys Crime Scene Reconstruction
Presentation of Complete Theory
Digital Crime Scene Investigation Phases


Digital Crime Scene Investigation Phases
Preservation of Dig Scene
Survey for Dig Evidence
Document Evidence and Scene
Search for Dig Evidence
Dig Crime Scene Reconstruction
Presentation of Dig Scene Theory
Phys Crime Scene Reconstruction

4.2. Digital Forensic Process Models

- The process started with a phase that require for the physical and operational infrastructure to be ready to support any future investigation.
- In this Readiness phase, the equipment must be ever ready and the personnel must be capable to use it effectively.
- This phase is indeed an ongoing phase throughout the lifecycle of an organization.
- It also consists of 2 sub-phases namely, Operation Readiness and Infrastructure Readiness.
- Immediately following the Readiness phase, is Deployment phase, which provide a mechanism for an incident to be detected and confirmed.
- Two sub-phases are further introduced, namely, Detection & Notification and Confirmation & Authorization.
- Collecting and analysing physical evidence are done in Physical scene Investigation phase. The sub-phases introduced are Preservation, Survey, Documentation, Search & Collection, Reconstruction and Presentation.
- Digital crime scene Investigation is similar to Physical crime scene Investigation with exception that it is now focusing on the digital evidence in digital environment.
- The last phase is Review phase. The whole investigation processes are reviewed to identify areas of improvement that may results in new procedures or new training requirements

4.3. Digital Forensics Analysis and Validation

1. Determining What Data to Collect and Analyse

    Using Access Data Forensic Toolkit to Analyse Data

2. Validating Forensic Data

    Validating with Hexadecimal Editors

3. Addressing Data-Hiding Techniques

    Hiding Partitions

    Marking Bad Clusters

    Bit-Shifting

4. Performing Remote Acquisitions

    Remote Acquisitions with Runtime Software

4.3. Digital Forensics Analysis and Validation

1. Data Analysis and Recovery Using ProDiscover Basic and AccessData FTK Imager (Computer Forensics) – YouTube
2. Forensic Investigation With FTK Imager & Autopsy GUI – YouTube

Thank you

BITS Pilani

Prof. Pradnya Kashikar

WILP-CSIS

BITS Pilani
Pilani Campus

innovate achieve lead

BITS Pilani

Pilani Campus

SS ZG588 - Cyber Crimes, Forensics and Incident Handling

Contact Session - 5

Course Objectives

No	Description
CO1	Enhancing awareness of recent Cyber Crime trends and learn Investigating Cyber Crimes
CO2	Introduce Cyberspace Infrastructure attacks and handling Organization Cybersecurity Issues
CO3	Understand Digital Forensics Process, Models, Analysis and Validation, Incident Detection and Response

Text Book(s)

innovate achieve lead

T1	Computer Forensics and Cyber Crime - An Introduction 3rd Edition by Marjie T. Britz, Ph.D., Professor of Criminal Justice, Clemson University
T2	Bill Nelson, A. Philips, F. Enfinger, C. K. Steuart, Computer Forensics and Investigations, Course Technology (Cengage Learning), Indian edition, 2009
T3	Incident Response & Computer Forensics, 3rd Edition by Jason T. Luttgens and Matthew Pepe and Kevin Mandia
R1	Guide to Computer Forensics and Investigations: Processing Digital Evidence 5th Edition by Bill Nelson, Amelia Phillips and Christopher Steuart
R2	The Basics of Digital Forensics, by John Sammons
R3	Computer Network Security and Cyber Ethics 4th Edition, by Joseph Migga Kizza
R4	Computer Forensics_ Investigating Network Intrusions and Cyber Crime: EC-Council Press

Learning Outcomes -

No	Learning Outcomes
LO1	Fundamental understanding and Information on Cyber Crimes, Digital Forensics Objectives and Incident Detection and Response Reports.
LO2	Learn on how to prepare investigation on computer-related incidents or crimes and summarize.
LO3	Understand on digital forensics process, models and analysis by taking a systematic approach
LO4	Explore on evaluating needs, validating and testing digital forensics tools, Generating Incident Report Findings, and Emerging Cybercrime Trends and Issues

Module 5 - Disk Structures (File Systems) and Data-hiding techniques

innovate achieve lead

5.1 Learn about different Disk Structures (File Systems);

RAID Data Acquisitions, acquiring data from different media/tools

5.2 Learn data-hiding techniques, Hiding Partitions; Steganography;

Encrypted Files; Recovering Passwords

5.3 Learn the different types of graphics files; Locate and recover

graphics files

5	Disk Structures (File Systems) and Data-hiding techniques	**Learn about different Disk Structures (File Systems); RAID Data Acquisitions, acquiring data from different media/tools**	T2, R1
		Learn data-hiding techniques, Hiding Partitions; Steganography; Encrypted Files; Recovering Passwords	
		Learn the different types of graphics files; Locate and recover graphics files	

5.1.1 Understanding File Systems

- To investigate digital evidence effectively, you must understand how the most commonly used OSs work and how they store files.
- A file system gives an OS a road map to data on a disk.
- The type of file system an OS uses determines how data is stored on the disk.
- When you need to access a suspect's computer to acquire or inspect data related to your investigation, you should be familiar with both the computer's OS and file system so that you can access and modify system settings when necessary.

5.1.1 Understanding File Systems

- To ensure that you don't contaminate or alter data on a suspect's system, you must know how to access and modify Complementary Metal Oxide Semiconductor (CMOS), BIOS, Extensible Firmware Interface (EFI), and Unified Extensible Firmware Interface (UEFI) settings.
- A computer stores system configuration and date and time information in the CMOS when power to the system is off.
- The system BIOS or EFI contains programs that perform input and output at the hardware level.
- BIOS is designed for x86 computers and typically used on disk drives with Master Boot Records (MBRs). EFI is designed for x64 computers and uses GUID Partition Table (GPT)–formatted disks.
- BIOS and EFI are designed for specific firmware. In an effort to reduce the relationship with firmware, Intel developed UEFI, which defines the interface between a computer's firmware and the OS.

5.1.1 Understanding File Systems

- When a subject's computer starts, you must make sure it boots to a forensically configured CD, DVD, or USB drive, because booting to the hard disk overwrites and changes evidentiary data.
- To do this, you access the CMOS setup by monitoring the computer during the bootstrap process to identify the correct key or keys to use.
- The bootstrap process, which is contained in ROM, tells the computer how to proceed.
- As the computer starts, the screen usually displays the key or keys, such as the Delete key, you press to open the CMOS setup screen.
- You can also try unhooking the keyboard to force the system to tell you what keys to use. The key you press to access CMOS depends on the computer's BIOS.
- Many BIOS manufacturers use the Delete key to access CMOS; other manufacturers use Ctrl+Alt+Insert, Ctrl+A, Ctrl+S, or Ctrl+F1, F2, or F10.

5.1.1 Understanding File Systems

- A safe method for verifying the BIOS is removing all hard drives from the computer, which enables you to start the computer to verify its BIOS date and time without accessing the disk drive.

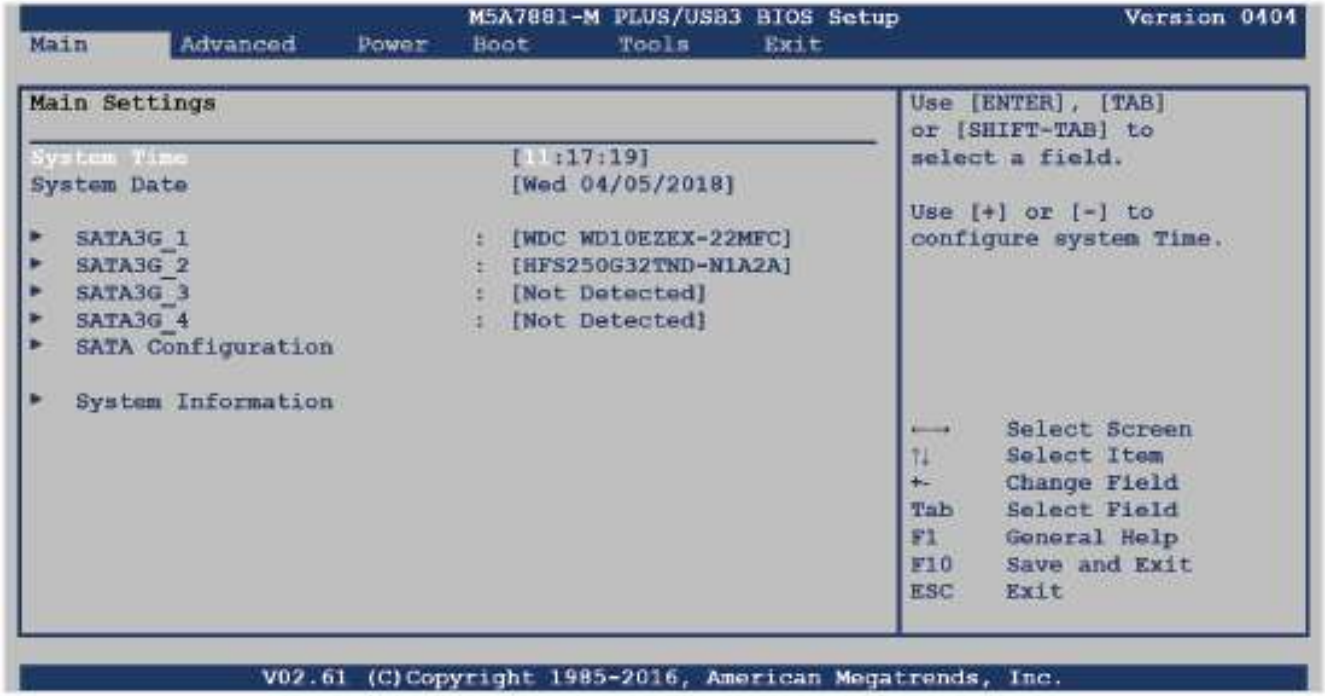


Figure 5-1 A typical CMOS setup screen

Source: American Megatrends, Inc., *https://ami.com/en/*

5.1.1 Understanding File Systems

innovate achieve lead

Exploring Microsoft File Structures

- Because most PCs use Microsoft software products, you should understand Microsoft file systems so that you know how Windows and DOS computers store files.
- In particular, you need to understand clusters, File Allocation Table (FAT), and NT File System (NTFS).
- The method an OS uses to store files determines where data can be hidden.
- When you examine a computer for forensic evidence, you need to explore these hiding places to determine whether they contain files or parts of files that might be evidence of a crime or policy violation.
- In Microsoft file structures, sectors are grouped to form **clusters**, which are storage allocation units of one or more sectors.
- Clusters range from 512 bytes up to 32,000 bytes each.

5.1.1 Understanding File Systems

- Combining sectors minimizes the overhead of writing or reading files to a disk.
- The OS groups one or more sectors into a cluster.
- The number of sectors in a cluster varies according to the disk size. For example, a double-sided floppy disk has one sector per cluster; a hard disk has four or more sectors per cluster.
- Clusters are numbered sequentially, starting at 0 in NTFS and 2 in FAT.
- The first sector of all disks contains a system area, the boot record, and a file structure database.
- The OS assigns these cluster numbers, referred to as **logical addresses**.

5.1.1 Understanding File Systems

- They point to relative cluster positions; for example, cluster address 100 is 98 clusters from cluster address 2.

- Sector numbers, however, are referred to as **physical addresses** because they reside at the hardware or firmware level and go from address 0 (the first sector on the disk) to the last sector on the disk.

- Clusters and their addresses are specific to a logical disk drive, which is a disk partition.

5.1.1 Understanding File Systems

innovate achieve lead

The following steps show you how to determine a disk's OS by using WinHex:

Before beginning the following activity, create a *Work*\Chap05\Chapter work folder on your system.

1. Start a Web browser, and go to **http://x-ways.net**. Under the Software Products heading, click **WinHex**. Download and install this program, after checking with your instructor about where to install it on your computer.

2. Insert a USB drive into a USB port.

3. Right-click the **WinHex** desktop icon and click **Run as administrator**.

If necessary, click **Continue** or **Yes** in the UAC message box. In Windows 10 or later, it's recommended that you create a desktop shortcut in File Explorer for the WinHex.exe file, which is usually in the C:\Program Files\WinHex folder. In older Windows versions, the path might be C:\Program Files (x86)\Winhex. To start the program, you right-click the WinHex desktop icon and click "Run as administrator."

5.1.1 Understanding File Systems

4. Click **Tools**, **Open Disk** from the menu to see a list of logical drives. Click the **C** drive (or your working drive), and click **OK**. If an error message is displayed, you can ignore it because it won't affect your analysis for this activity.

5. Click **Tools**, **Open Disk** again, but this time, click your USB drive in the Edit Disk list, and then click **OK**. Compare the file system label for this drive with the one you saw in Step 4. Leave WinHex open for the next activity.

For other file system structures ad investigations, read chapter 5 from T2

5.1.2 RAID data acquisitions

- Acquisitions of RAID drives can be challenging and frustrating for digital forensics examiners because of how RAID systems are designed, configured, and sized.
- Size is the biggest concern because many RAID systems are now pushing into exabytes or more of data.
- **Redundant array of independent disks (RAID)** is a computer configuration involving two or more physical disks.
- Originally, RAID was developed as a data-redundancy measure to minimize data loss caused by a disk failure.
- As technology improved, RAID also provided increased storage capabilities.

5.1.2 RAID data acquisitions

- Several levels of RAID can be implemented through software (known as “software RAID”) or special hardware controllers (known as “hardware RAID”).
- Software RAID is typically implemented from the host computer’s OS.
- Hardware RAID uses its own controller as well as a processor and memory connected to the host computer.
- For Windows XP, 2000, and NT servers and workstations, RAID 0 or 1 is available.
- For a high-end data-processing environment, RAID 5 is common and is often based in special RAID towers.
- These high-end RAID systems usually have integrated controllers that connect to high-end servers or mainframes.
- These systems provide redundancy and high-speed data access and can make many small disks appear as one very large drive.

5.1.2 RAID data acquisitions

There's no simple method for getting an image of a RAID server's disks. You need to address the following concerns:

- How much data storage is needed to acquire all data for a forensics image?
- What type of RAID is used? Is it Windows RAID 0 or 1 or an integrated hardware firmware vendor's RAID 5, 10, or 15?
- Is it another unknown configuration or OS?
- If it's a RAID 1, 10, or 15 server, do you need to have all drives connected so that the OS sees their contents?
- Some older RAID 1 systems required connecting both drives to make the data readable, which might also apply to RAID 10 and 15.
- Do you have an acquisition tool capable of copying the data correctly?
- Can the tool read a forensic copy of a RAID image?
- Can the tool read split data saves of each RAID disk, and then combine all images of each disk into one RAID virtual drive for analysis?

5.1.2 RAID data acquisitions

- With the larger disks now available, copying small RAID systems to one large disk is [Small Computer Systems Interface] drives in a RAID 0 tower requires about a 300 GB SATA [Serial Advanced Technology Attachment] or IDE (PATA - Parallel Advanced Technology Attachment) drive.
- Less data storage is needed if a proprietary format acquisition is used with compression applied.
- All forensics analysis tools can analyse an image because they see the acquired data as one large drive, not eight separate drives.
- Several forensics vendors have added RAID recovery features.
- These vendors typically specialize in one or two types of RAID formats.

5.1.2 RAID data acquisitions

- The following are some vendors offering RAID acquisition functions:
    - Guidance Software EnCase
    - X-Ways Forensics
    - AccessData FTK [Forensic Toolkit]
    - Runtime Software
    - R-Tools Technologies

- You should know which vendor supports which RAID format and keep up to date on the latest improvements in these products.

- Being able to separate each physical disk into smaller save sets eliminates the need to have one large drive for storing acquired data.

5.1.2 RAID data acquisitions

Web links to follow for practical work -

1.

11. Cyber Forensics - Investigating a Case Using AccessData FTK - Anand K – YouTube

2.

FTK Imager - Loading a multi-part disk image - YouTube

5.1.3 Acquiring data from different media / tools

- Recent improvements in forensics tools include the capability to acquire disk data or data fragments (sparse or logical) remotely.
- With this feature, you can connect to a suspect computer remotely via a network connection and copy data from it.
- Remote acquisition tools vary in configurations and capabilities.
- Some require manual intervention on remote suspect computers to initiate the data copy.
- Others can acquire data surreptitiously through an encrypted link by pushing a remote access program to the suspect's computer.
- From an investigation perspective, being able to connect to a suspect's computer remotely to perform an acquisition has tremendous appeal.

5.1.3 Acquiring data from different media / tools

- It saves time because you don't have to go to a suspect's computer, and it minimizes the chances of a suspect discovering that an investigation is taking place.
- Most remote acquisitions have to be done as live acquisitions, not static acquisitions.
- When performing remote acquisitions, advanced privileges are required to push agent applications to the remote system.
- There are some drawbacks to consider, such as antivirus, antispyware, and firewall tools.
- Most of these security programs can be configured to ignore remote access programs.
- However, if suspects have administrator rights on their computers, they could easily install their own security tools that trigger an alarm to notify them of remote access intrusions.

5.1.3 Acquiring data from different media / tools

Remote Acquisition with ProDiscover

ProDiscover Incident Response is designed to be integrated as a network intrusion analysis tool and is useful for performing remote acquisitions. When connected to a remote computer, it uses the same ProDiscover acquisition method described previously. After the connection is established, the remote computer is displayed in the Capture Image dialog box. This tool offers all the functions and features of other tools in the ProDiscover suite plus the following:

- Capture volatile system state information.
- Analyze current running processes on a remote system.
- Locate unseen files and processes on a remote system that might be running malware or spyware.
- Remotely view and listen to IP ports on a compromised system.
- Run hash comparisons on a remote system to search for known Trojans and rootkits.
- Create a hash inventory of all files on a system remotely (a negative hash search capability) to establish a baseline if it gets attacked.

5.1.3 Acquiring data from different media / tools

Remote Acquisition with EnCase Enterprise

Guidance Software was the first forensics vendor to develop a remote acquisition and analysis tool based on its desktop tool EnCase. This remote tool, EnCase Endpoint Investigator, can perform the following functions:

- Search and collect internal and external network systems over a wide geographical area
- Support multiple OSs and file systems
- Triage to help determine systems' relevance to an investigation
- Perform simultaneous searches of up to five systems at a time
- For more information, see *www.guidancesoftware.com/docs/default-source/document-library/product-brief/encase-endpoint-investigator-product-overview.pdf*.

5.1.3 Acquiring data from different media / tools

Remote Acquisition with R-Tools R-Studio

The R-Tools suite of software is designed for data recovery. As part of this recovery capability, the R-Studio network edition can remotely access networked computer systems. Data acquired with R-Studio network edition creates raw format acquisitions, and it's capable of recovering many different file systems, including ReFS. For more information on R-Studio, see *www.r-studio.com*.

5.1.3 Acquiring data from different media / tools

innovate achieve lead

Remote Acquisition with WetStone US-LATT PRO

US-LATT PRO, part of a suite of tools developed by WetStone, can connect to a networked computer remotely and perform a live acquisition of all drives connected to it. For more information on this tool, see *www.wetstonetech.com/product/us-latt/*.

Remote Acquisition with F-Response

F-Response is a vendor-neutral specialty remote access utility designed to work with any digital forensics program. When installed on a remote computer, it sets up a security read-only connection that allows forensics examiners to access it. With F-Response, examiners can access remote drives at the physical level and view raw data. After the F-Response connection has been set up, any forensics acquisition tool can be used to collect digital evidence.

F-Response is sold in four different versions: Enterprise Edition, Consultant + Convert Edition, Consultant Edition, and TACTICAL Edition.

For the latest information on F-Response, see *www.f-response.com*.

5.1.3 Acquiring data from different media / tools

PassMark Software ImageUSB

PassMark Software has an acquisition tool called ImageUSB for its OSForensics analysis product. To create a bootable flash drive, you need Windows XP or later and ImageUSB downloaded from the OSForensics Web site. For more information on ImageUSB, see *www.osforensics.com/tools/write-usb-images.html*.

5.1.3 Acquiring data from different media / tools

ASR Data SMART

ASR Data SMART is a Linux forensics analysis tool that can make image files of a suspect drive. SMART can produce proprietary or raw format images and includes the following capabilities:

- Robust data reading of bad sectors on drives
- Mounting suspect drives in write-protected mode
- Mounting target drives, including NTFS drives, in read/write mode
- Optional compression schemes to speed up acquisition or reduce the amount of storage needed for acquired digital evidence

For more information on SMART, see *www.asrdata.com*.

5.1.3 Acquiring data from different media / tools

Summarizing -

- To acquire RAID disks, you need to determine the type of RAID and which acquisition tool to use. With a firmware hardware RAID, acquiring data directly from the RAID server might be necessary.

- Remote network acquisition tools require installing a remote agent on the suspect computer. The remote agent can be detected if suspects install their own security programs, such as a firewall.

https://accessdata.com/product-download/forensic-toolkit-ftk-version-7.1.0

https://ad-pdf.s3.amazonaws.com/ftk/7.x/FTK_Install_Guide.pdf

5.2.1 Data hiding Techniques

- Data hiding involves changing or manipulating a file to conceal information.

- Data hiding techniques include hiding entire partitions, changing file extensions, setting file attributes to hidden, bit-shifting, using encryption, and setting up password protection.

5.2.1 Data hiding Techniques

Hiding Files by Using the OS

- One of the first techniques used to hide data is changing file extensions,.
- For example, a suspect wanting to hide an Excel spreadsheet containing incriminating evidence could change its extension from `.xlsx` to `.jpg`.
- An investigator who tries to open the file in Excel will get an error message stating that the file can't be opened.
- Advanced digital forensics tools, however, check file headers and compare the file extension to verify that it's correct.
- If there's a discrepancy, the tool flags the file as a possible altered file that requires more analysis.
- Another hiding technique is selecting the Hidden attribute in a file's Properties dialog box, so an investigator who's trying to view files in File Explorer should select the option to view hidden files, folders, and drives. Digital forensics tools can identify hidden files for investigators, however.

5.2.2 Hiding Partitions

- One way to hide partitions is with the Windows disk partition utility, `diskpart`. By using the `diskpart remove` *`letter`* command at the PowerShell prompt, you can unassign the partition's letter, which hides it from view in File Explorer.

- To unhide the partition, use the `diskpart assign` *`letter`* command.

- Other disk management tools, such as IM-Magic, EaseUS Partition Master, and Linux Grand Unified Bootloader (GRUB), are available, too.

- For more information on the `diskpart` command, see w*ww.diskpartition.com/diskpart/assign-drive-letter-4125.html*

5.2.2 Hiding Partitions

- To detect whether this technique has been used, be sure to account for all disk space when you're examining an evidence drive.
- Analyze any disk areas containing space you can't account for so that you can determine whether they contain additional evidence.
- If a FAT partition containing clusters marked as bad is converted to an NTFS partition, the bad clusters remain marked as bad, so the conversion to NTFS doesn't affect the content of these clusters.
- Most GUI tools skip clusters marked as bad in FAT and NTFS, and these clusters might contain valuable evidence for your investigation.

5.2.3 Steganography

- **steganography** comes from the Greek word for “hidden writing.” It’s defined as hiding messages in such a way that only the intended recipient knows the message is there.
- The term for detecting and analyzing steganography files is “steganalysis.”
- In addition to steganography, digital watermarking was developed as a way to protect file ownership.
- Some digital watermarks are designed to be visible—for example, to notify users that an image is copyrighted.
- The digital watermarks used for steganography aren’t usually visible. For example, when viewing two files that look the same, but one has an invisible digital watermark, they appear to be the same file.
- Their file sizes might even be identical.

5.2.3 Steganography

innovate achieve lead

Web links to follow:

1.

What is Steganography? – YouTube

2.

Cyber Security : Steganography | Introduction - YouTube

3.

Learning Computer Forensics Tutorial | Steganography Techniques: Images And Video - YouTube

5.2.3 Steganography

- However, if you run an MD5 or SHA-1 hash comparison on both files, you'll find that the hash values aren't equal.
- few steganography tools available for lossy graphics files.
- These tools insert data into the graphics file but often alter the original file in size and clarity.
- One way to hide data is to use steganography tools, many of which are freeware or shareware, to insert information into a variety of files.
- If you encrypt a plaintext file with PGP and insert the encrypted text into a steganography file, for example, cracking the encrypted message is extremely difficult.

5.2.3 Steganography

Steganalysis methods –

• *Stego-only attack*—Used when only the file containing the possible steganography content is available for analysis; it's similar to a cyphertext attack. This attack is one of the most difficult to perform because all you have to analyze is the suspected steganography file.

• *Known cover attack*—Used when the **cover-media**, the original file with no hidden message, and the **stego-media**, the converted cover-media file that stores the hidden message, are available for analysis. By analyzing the original and steganography files, further comparisons can be made to identify common patterns that might help decipher the message.

5.2.3 Steganography

- *Known message attack*—Used when the hidden message is revealed later, allowing further analysis of new messages. Similar to the known cover attack, this method uses comparative analysis to decipher the message. Because the message is known, deciphering it takes less effort.

- *Chosen stego attack*—Used when a steganography tool and stego-media were used to hide the message content. Because this method uses a known steganography tool, the analyst applies password or passphrase recovery techniques to decipher the message.

- *Chosen message attack*—Used to identify corresponding patterns used in stego-media. This technique creates stego-media and then analyzes them to determine how data is configured in the file. The analyst then uses these known configuration patterns to compare with suspected stego-media to determine what the message might be.

5.2.4 Encrypted Files

- People who want to make data unreadable can use advanced encryption programs, such as PGP or BestCrypt. Encrypted files are encoded to prevent unauthorized access.
- To decode an encrypted file, users supply a password or pass-phrase.
- Without the pass-phrase, recovering the contents of encrypted files is difficult.
- Many commercial encryption programs use a technology called **key escrow**, which is designed to recover encrypted data if users forget their passphrases or if the user key is corrupted after a system failure.
- Forensics examiners can also use key escrow to attempt to recover encrypted data.

5.2.4 Encrypted Files

- Although some vendors have developed key recovery tools, the resources needed to crack encryption schemes are usually beyond what's available to small or medium organizations.
- If you do encounter encrypted data in an investigation, make an effort to persuade the suspect to reveal the encryption passphrase.
- Some encryption schemes are so complex that the time to crack them can be measured in days, weeks, years, and even decades. Key sizes of 128 bits to 4096 bits make the job of breaking them with a brute-force attack nearly impossible with current technology.
- Quantum computing is progressing to make many current encryption schemes obsolete.
- Currently, there are some encryption schemes that will remain unbroken with commercially available tools.

5.2.5 Recovering Passwords

Password recovery is becoming more common in digital forensics analysis. Several password-cracking tools are available for handling password-protected data or systems. Some of these products are integrated into a digital forensics tool, such as OSForensics. Others, including the following, are stand-alone tools that typically require extracting password files or accessing a suspect's disk or image file directly:

- Last Bit (*http://lastbit.com/password-recovery-methods.asp*)
- AccessData PRTK (*http://accessdata.com/product-download* at the Decryption Products link)
- ophcrack (*http://ophcrack.sourceforge.net*)
- John the Ripper (*www.openwall.com/john*)
- Passware (*www.lostpassword.com/kit-forensic.htm*)

5.2.5 Recovering Passwords

- These tools use a dictionary attack or brute-force attack to crack passwords.
- Brute force attacks use every possible letter, number, and character found on a keyboard.
- Eventually, a brute-force attack can crack any password; however, this method can require a lot of time and processing power, especially if the password is very long.
- In a dictionary attack, the program uses common words found in the dictionary and tries them as passwords.
- Most password crackers have dictionaries in a variety of languages, including English, French, Russian, and even Swahili.
- With some password-cracking tools, you can import additional unique words extracted from evidence.
- In FTK, for example, you can export a word list to PRTK that can be added to the dictionary.

5.2.5 Recovering Passwords

- With many of these programs, you can build profiles of a suspect to help determine his or her password.
- These programs consider information such as names of relatives or pets, favourite colours, and schools attended.
- The principle behind these programs is that people have a habit of using things they're comfortable with, especially if it requires memorizing something secret, such as a password.
- This method of password cracking is known as a "hybrid attack."
- Many password-protected OSs and applications store passwords in the form of MD5 or SHA hash values.
- Because of this storage method, a brute-force attack requires converting a dictionary password from plaintext to a hash value.
- This process requires additional CPU cycle time to process each attempt to match the dictionary password to the OS or application password.

5.2.5 Recovering Passwords

- Another method has been developed that hashes passwords in a dictionary.
- A **rainbow table** is a file containing the hash values for every possible password that can be generated from a computer's keyboard.
- Because rainbow tables already contain these hash values and no conversion is necessary, this method is much faster than a dictionary or brute-force attack.
- For more information on rainbow tables and where to download them, visit *http://project-rainbowcrack.com* and *http://project-rainbowcrack.com/table.htm*.
- As good as rainbow tables are for cracking passwords, however, a new
- scheme of protecting passwords has been developed that adds extra bits to a password and then hashes it.
- This technique, called **salting passwords**, alters hash values, which makes cracking passwords more difficult.

5.2.5 Recovering Passwords

It should be noted that algorithms for password encryption vary from simple to complex. When attempting to crack a password, research the encryption method used by the application or OS. You might be able to identify known weaknesses that could help you determine the password.

Summarizing –

- Data hiding involves changing or manipulating a file to conceal information. Data-hiding techniques include changing file extensions, setting file attributes to hidden, hiding partitions, bit-shifting, using steganography, and using encryption and password protection.
- There are three ways to recover passwords: dictionary attacks, brute-force attacks, and rainbow tables. Rainbow tables are the quickest method because they contain predefined hash values of all known passwords. If passwords have been salted, however, recovering them can take much longer, and some might not be recoverable at all.

5.3.1 Different types of graphics files

Graphic files contain digital photographs, line art, three-dimensional images, text data converted to images, and scanned replicas of printed pictures,

1. Bitmap images: collection of dots

2. Vector graphics: based on mathematical instructions

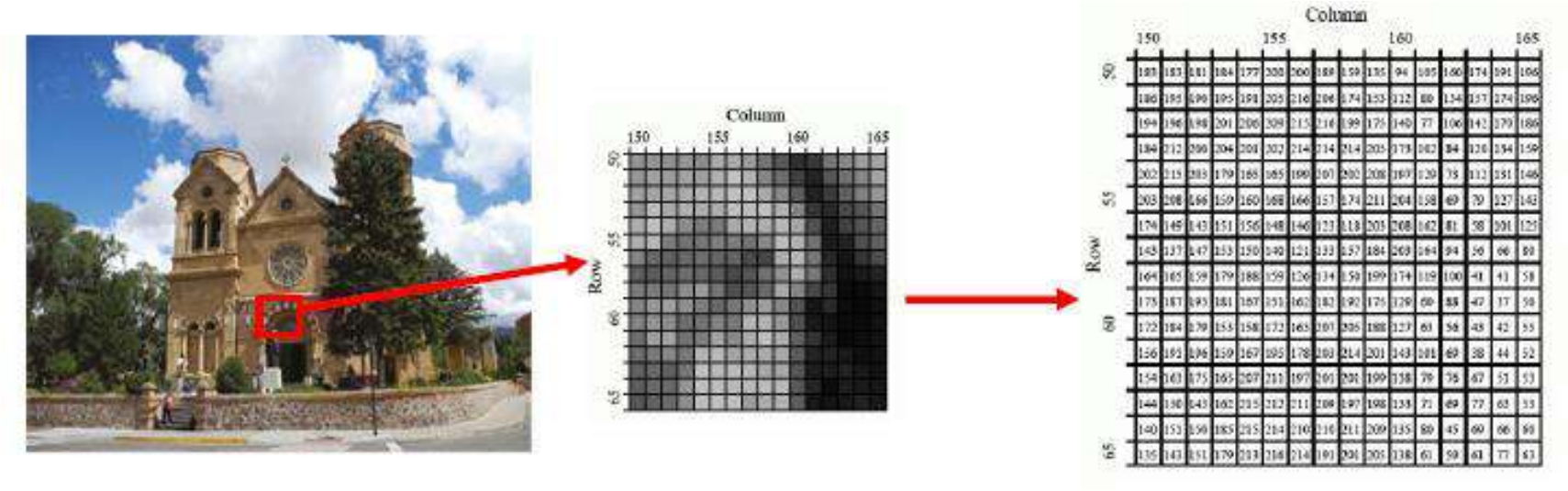
3. Metafile graphics: combination of bitmap and vector

5.3.1 Different types of graphics files

Types of programs

1. Graphics editors
2. Image viewers

A digital image is a “grid" of pixels with different range of values



5.3.1 Different types of graphics files

innovate achieve lead

Standard graphics File formats -

Standard bitmap File formats

- Portable Network Graphic (.png)
- Graphic Interchange Format (.gif)
- Joint Photographic Experts Group (.jpeg, .jpg)
- Tagged Image File Format (.tiff, .tif)
- Window Bitmap (.bmp)

Standard vector File formats

- Hewlett Packard Graphics Language (.hpgl)
- Autocad (.dxf)

5.3.1 Different types of graphics files

Nonstandard graphics File formats

Standard bitmap File formats

- Targa (.tga)
- Raster Transfer Language (.rtl)
- Adobe Photoshop (.psd) and Illustrator (.ai)
- Freehand (.fh11)
- Scalable Vector Graphics (.svg)
- Paintbrush (.pcx)

5.3.2 Locate and recover graphics files

Operating system built-in tools for recovering graphics are:

- Time consuming
- Results are difficult to verify
- Digital forensics tools

Image headers - contain information about graphics files

- Instead of memorizing header information, them with good header samples
- Use header information to create a baseline analysis

Prior to analysing image's headers, first reconstruct fragmented image files

- Identify data patterns the graphic file uses
- Identified patterns of modified images' headers

5.3.2 Locate and recover graphics files

Repairing Damaged Headers

- When examining recovered fragments from files in slack or free space, You might find data that appears to be a header.
- If header data is partially overwritten, you must reconstruct the header to make it readable.
- By comparing the hexadecimal values of known graphics file formats with the pattern of the file header.
- When examining recovered fragments from les in slack or free space, You might find data that appears to be a header for a common graphics file type.
- If header data is partially overwritten, you must reconstruct the header to make it readable.
- By comparing the hexadecimal values of known graphics file formats with the pattern of the file header you found Each graphics file has a unique header value.
- Example: A JPEG file has the hexadecimal header value FFD8, followed by the label JFIF for a standard JPEG or Exif file at offset 6

Thank you

BITS Pilani

Prof. Pradnya Kashikar

WILP-CSIS

BITS Pilani
Pilani Campus

innovate achieve lead

BITS Pilani

Pilani Campus

SS ZG588 - Cyber Crimes, Forensics and Incident Handling

Contact Session - 6

Course Objectives

No	Description
CO1	Enhancing awareness of recent Cyber Crime trends and learn Investigating Cyber Crimes
CO2	Introduce Cyberspace Infrastructure attacks and handling Organization Cybersecurity Issues
CO3	Understand Digital Forensics Process, Models, Analysis and Validation, Incident Detection and Response

Text Book(s)

innovate achieve lead

T1	Computer Forensics and Cyber Crime - An Introduction 3rd Edition by Marjie T. Britz, Ph.D., Professor of Criminal Justice, Clemson University
T2	Bill Nelson, A. Philips, F. Enfinger, C. K. Steuart, Computer Forensics and Investigations, Course Technology (Cengage Learning), Indian edition, 2009
T3	Incident Response & Computer Forensics, 3rd Edition by Jason T. Luttgens and Matthew Pepe and Kevin Mandia
R1	Guide to Computer Forensics and Investigations: Processing Digital Evidence 5th Edition by Bill Nelson, Amelia Phillips and Christopher Steuart
R2	The Basics of Digital Forensics, by John Sammons
R3	Computer Network Security and Cyber Ethics 4th Edition, by Joseph Migga Kizza
R4	Computer Forensics_ Investigating Network Intrusions and Cyber Crime: EC-Council Press

Learning Outcomes -

No	Learning Outcomes
LO1	Fundamental understanding and Information on Cyber Crimes, Digital Forensics Objectives and Incident Detection and Response Reports.
LO2	Learn on how to prepare investigation on computer-related incidents or crimes and summarize.
LO3	Understand on digital forensics process, models and analysis by taking a systematic approach
LO4	Explore on evaluating needs, validating and testing digital forensics tools, Generating Incident Report Findings, and Emerging Cybercrime Trends and Issues

Module 6 - Network and Cloud Forensics; Mobile Device and Security

innovate achieve lead

6.1 Network Forensics, Cloud Forensics and Virtual Machine Forensics

6.2 Honeypots; Security in Mobile Systems and Cloud

6.3 Mobile Device Forensics: Inside Mobile Devices; SIM Card File Structure

6.4 Investigating Network Traffic; Investigating Web Attacks and Wireless Attacks

6	Network and Cloud Forensics; Mobile Device and Security	Network Forensics, Cloud Forensics and Virtual Machine Forensics	T1, R1, R3, R4
		Honeypots; Security in Mobile Systems and Cloud	

6.1 Network Forensics, Cloud Forensics and Virtual Machine Forensics

Network Forensics

- Network forensics is used to determine how a security breach occurred; however, steps must be taken to harden networks before a security breach happens, particularly with recent increases in network attacks, viruses, and other security incidents.
- Hardening includes a range of tasks, from applying the latest patches to using a layered network defense strategy, which sets up layers of protection to hide the most valuable data at the innermost part of the network.
- It also ensures that the deeper into the network an attacker gets, the more difficult access becomes and the more safeguards are in place.
- The National Security Agency (NSA) developed a similar approach, called the defense in depth (DiD) strategy. DiD have three modes of protection:
  - • People
  - • Technology
  - • Operations

6.1 Network Forensics

- If one mode of protection fails, the others can be used to thwart the attack. Listing people as a mode of protection means organizations must hire well-qualified people and treat them well so that they have no reason to seek revenge.
- In addition, organizations should make sure employees are trained adequately in security procedures and are familiar with the organization's security policy.
- Physical and personnel security measures are included in this mode of protection.
- The technology mode includes choosing strong network architecture and using tested tools, such as intrusion detection systems (IDSs) and firewalls.
- Regular penetration testing coupled with risk assessment can help improve network security, too.
- Having systems in place that allow quick and thorough analysis when a security breach occurs is also part of the technology mode of protection.

6.1 Network Forensics

- **Network forensics** is the process of collecting and analysing raw network data and tracking network traffic systematically to ascertain how an attack was carried out or how an event occurred on a network.
- Because network attacks are on the rise, there's more focus on this field and an increasing demand for skilled technicians.
- Labour forecasts predict a shortfall of network forensics specialists in law enforcement, legal firms, companies, and universities.
- When intruders break into a network, they leave a trail.
- Being able to spot variations in network traffic can help you track intrusions, so knowing your network's typical traffic patterns is important.

6.1 Network Forensics, Cloud Forensics and Virtual Machine Forensics

- For example, if a company's peak use is typically between 6 a.m. and 6 p.m., that's when you should expect spikes.
- If a usage spike occurs during the night, the network administrator should recognize it as unusual activity and take steps to investigate it.
- Network forensics can also help you determine whether a network is truly under attack or a user has inadvertently installed an untested patch or custom program.
- A lot of time and resources can be wasted determining that a bug in a custom program or an untested open-source program caused an "attack."

6.1 Network Forensics, Cloud Forensics and Virtual Machine Forensics

The Need for Established Procedures –

- Network forensics examiners must establish standard procedures for how to acquire data after an attack or intrusion incident.
- Typically, network administrators want to find compromised machines, get them offline, and restore them as quickly as possible to minimize downtime.
- However, taking the time to follow standard procedures is essential to ensure that all compromised systems have been found and to ascertain attack methods in an effort to prevent them from happening again.
- Procedures must be based on an organization's needs and should complement the network infrastructure.
- The increase in cybercrimes has prompted many groups to begin compiling procedures and protocols to follow when a network intrusion occurs.
- Network administrators need to learn how to stop intruders and determine how they got in; what they copied, altered, or deleted; and whether they're still on the network.

6.1 Network Forensics, Cloud Forensics and Virtual Machine Forensics

Developing Procedures for Network Forensics

- Network forensics can be a long, tedious process, and unfortunately, the trail can go cold quickly.
- A standard procedure often used in network forensics is as follows:

1. Always use a standard installation image for systems on a network. This image isn't a bit-stream image but an image containing all the standard applications used. You should also have MD5 and SHA-1 hash values of all application and OS files.
2. When an intrusion incident happens, make sure the vulnerability has been fixed to prevent other attacks from taking advantage of the opening.
3. Attempt to retrieve all volatile data, such as RAM and running processes, by doing a live acquisition before turning the system off.
4. Acquire the compromised drive and make a forensic image of it.
5. Compare files on the forensic image with the original installation image. Compare hash values of common files, such as Win.exe and standard dynamic link libraries (DLLs), and ascertain whether they have changed.

6.1 Network Forensics

innovate achieve lead

Using Network Tools

- A variety of tools are available for network administrators to perform remote shutdowns, monitor device use, and more.
- The tools covered in this chapter are a combination of freeware and enterprise software; some tools have free demo versions.
- Tools such as Splunk (*www.splunk.com*), Spiceworks (*www.spiceworks.com*), Nagios (*www.nagios.org*), and Cacti (*www.cacti.net*) help you monitor your network efficiently and thoroughly.
- For example, you can consult records that the tool generates to prove an employee ran a program without permission.
- You can also monitor your network and shut down machines or processes that could be harmful.
- Although these tools are helpful for network administrators, imagine what would happen if an attacker (or even an internal user) could get administrative rights to the network and start using these tools.

6.1 Network Forensics

innovate achieve lead

Using Packet Analyzers

- **Packet analysers** are devices or software placed on a network to monitor traffic.
- Most network administrators use them for increasing security and tracking bottlenecks.
- However, attackers can use them to get information covertly. Most packet analysers work at Layer 2 or 3 of the OSI model.
- To understand what's happening on a network, often you have to look at the higher layers by using custom software that comes with switches and routers, however.
- Some analysers perform packet captures, some are used for analysis, and some handle both tasks.
- Your organization needs to have policies about using these tools to comply with new federal laws on digital evidence.

6.1 Network Forensics

innovate achieve lead

Using Packet Analyzers

- Windows has many tools capable of capturing and analysing packets, but you can't feed the data they collect directly into other tools. Most tools can read anything captured in Pcap (packet capture) format.

- (Libpcap is the version for Linux, and Winpcap is the version for Windows.) Programs such as tcpdump and Wireshark (*www.wireshark.org*) use the Pcap format, for example.

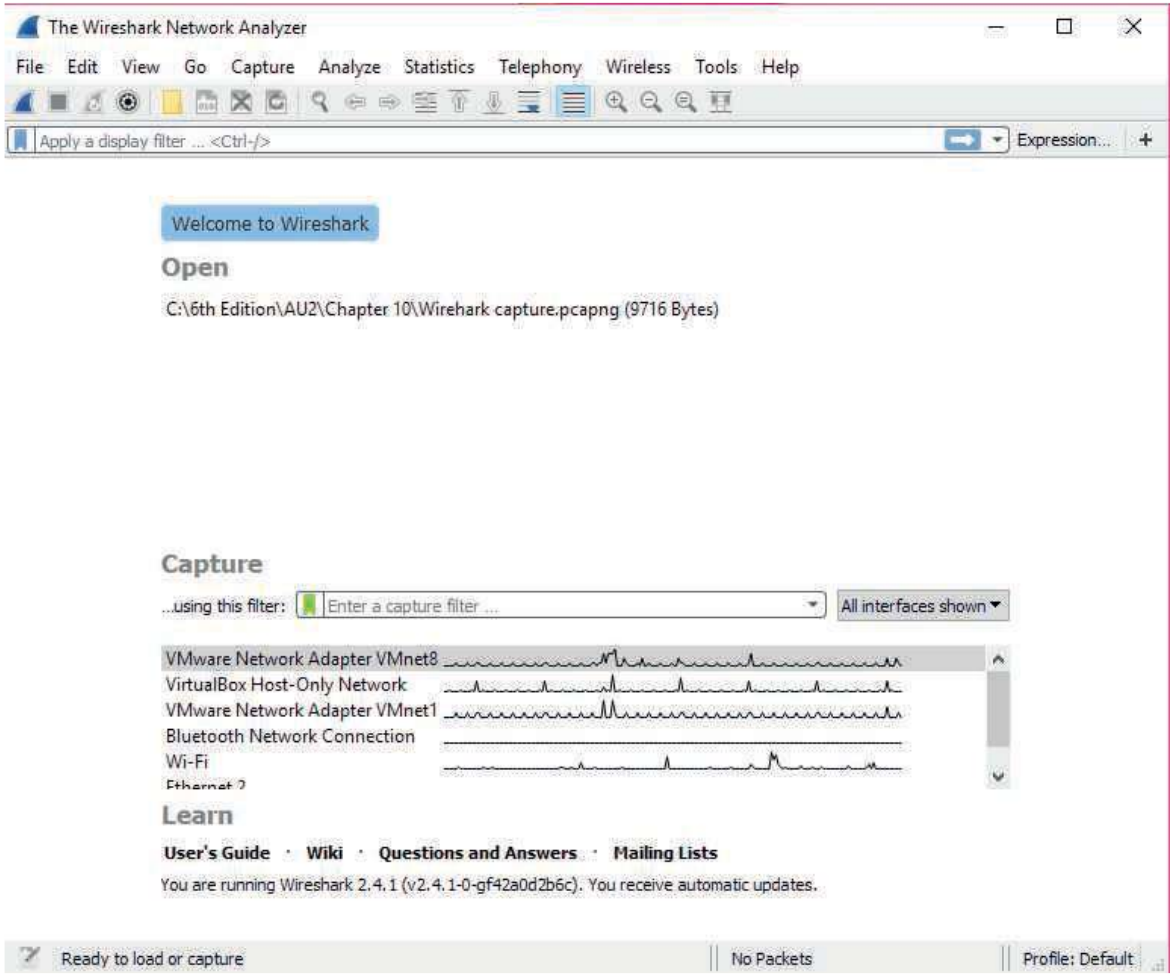
- To take advantage of the strengths in different tools, many investigators do a capture with tcpdump and then analyze the capture in Wireshark.

6.1 Network Forensics, Cloud Forensics and Virtual Machine Forensics

- Wireshark can be used in a real-time environment to open saved trace files from packet captures.
- An important feature is its capability to rebuild sessions.
- To use this feature, right-click a frame in the upper pane and click Follow TCP Stream.
- Wireshark then traces the packets associated with an exploit.
- To see how this tool works, download the most recent version of Wireshark for Windows (*www.wireshark.org/download.html*) and install it on your workstation. Then follow these steps:

6.1 Network Forensics

1. Start Wireshark, Notice the list of networks with traffic.



The opening window in Wireshark

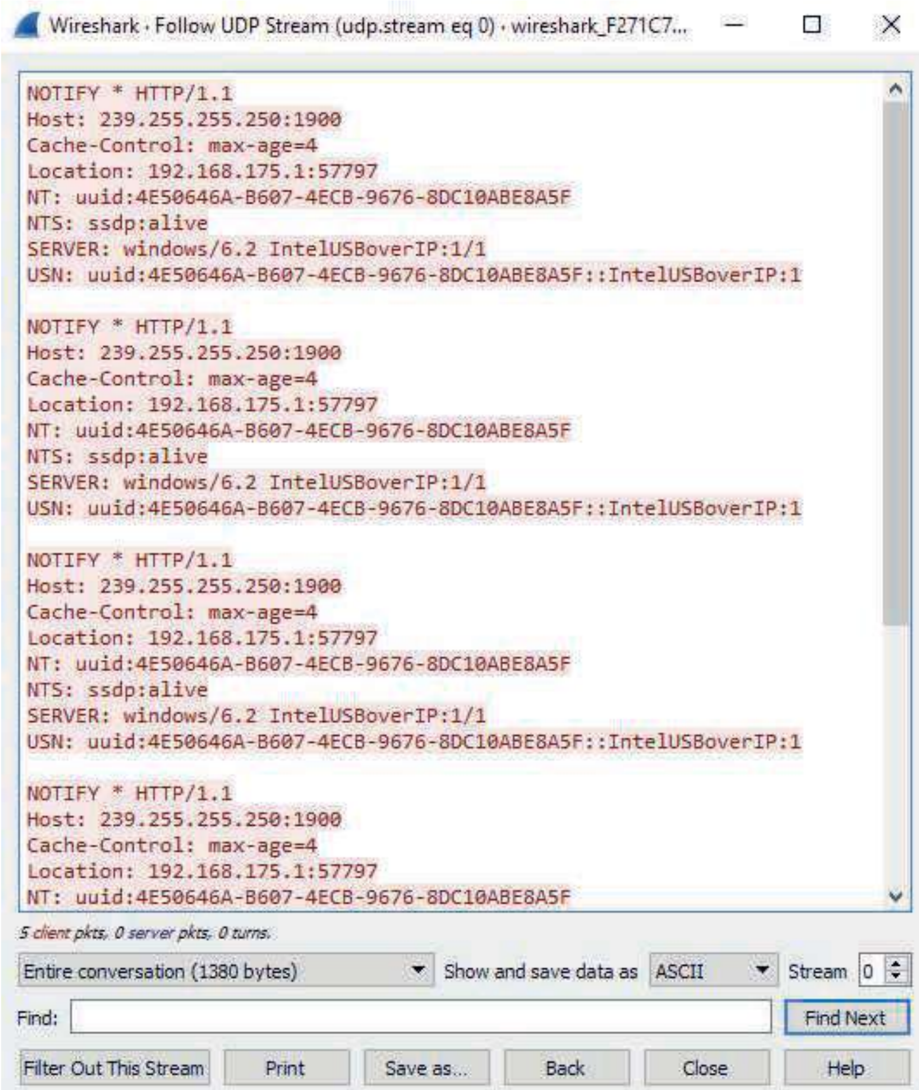
6.1 Network Forensics

2. Double-click a network that's showing activity. (If you're not on a live network, ping another student or yourself and visit some Web sites and download a file to generate traffic. Then start this activity again.)

3. After several frames have been captured, click **Stop**.

4. After the trace has been loaded, scroll through the upper pane until you see a UDP frame or an SSOP [Shrink Small Outline Package] frame. Right-click the frame, point to **Follow**, and click **UDP Stream**. You should see a window similar to Figure shown on the next slide:

6.1 Network Forensics



Following a UDP stream

6.1 Network Forensics

5. Review the information in this window, and then exit Wireshark.

You can find information on network forensics tools at many of the Web sites mentioned in this chapter. If you're interested in learning even more about network forensics, the next section covers the Honeynet Project.

6.1 Cloud Forensics

- Web service that applied digital marketing research to business subscribers so that they could do their own market analysis; this service eventually led the way to the cloud.
- Amazon created Amazon Mechanical Turk in 2002, which provided storage, computations, and human intelligence, and then started its Elastic Compute Cloud (EC2) in 2006, a Web service aimed at supporting small businesses.
- It enabled people and small businesses to rent processing time to run their own applications from a centralized source.
- After Web 2.0 in 2009, other providers started their own cloud services, such as Google Apps, Apple iCloud, Microsoft OneDrive, and more.

6.1 Cloud Forensics

innovate achieve lead

Cloud Service Levels and Deployment Methods

- The National Institute of Standards and Technology defines cloud computing in its NIST Special Publication 800-145 document “The NIST Definition of Cloud Computing” (*http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf*, 2011) as a computing storage system that provides on-demand network access for multiple users and can allocate storage to users to keep up with changes in their needs.

6.1 Cloud Forensics

The cloud has three basic service levels:

• *SaaS*—**Software as a service (SaaS)** means applications are delivered via the Internet. A familiar one is Google Docs, which is similar to office suites such as Microsoft Office or LibreOffice. Data is stored in the cloud, and files can be accessed and shared with others.

• *PaaS*—**Platform as a service (PaaS)** means an OS has been installed on a cloud server. Users can then install their own applications, settings, and tools in the cloud environment. The cloud provider maintains just the hardware for customers, who are responsible for their own system administration and application support.

• *IaaS*—**Infrastructure as a service (IaaS)** means customers can rent hardware, such as servers and workstations, and install whatever OSs and applications they need. IaaS can come in handy when customers can't afford to purchase hardware or pay someone to maintain it but can afford to rent. In addition, this service level makes it easy to add hardware during peak business periods, such as tax season or end-of-year accounting, and then cut back on hardware when it's not needed during slow periods.

6.1 Cloud Forensics

Table below describes where investigators find evidence of cloud access, depending on the type of cloud service level:

Service level	Locations of evidence
SaaS	Most likely stored on a desktop, laptop, tablet, or smartphone.
PaaS	Most likely found on a desktop or server, although it could also be stored on a company network or the remote service provider's infrastructure.
IaaS	Usually found on a desktop or server; infrastructure equipment can be owned by the company or the remote service provider.

6.1 Cloud Forensics

- The deployment methods for a cloud are public, private, community, and hybrid.
- A **public cloud** is accessible to anyone, and typically, the only identification required is an e-mail address.
- This deployment method offers no security, but it's popular because of its ease of use.
- Next is a **private cloud**, which can be accessed only by people who have the necessary credentials, such as logon names and passwords; sometimes location is used as a way to restrict access, too.
- Most companies have private clouds.
- A **community cloud** is a way to bring people together for a specific purpose.
- For example, say a city wants all small businesses to have access to the same documents and templates.
- By creating a community cloud, the city can make these files accessible to those who have a current business license.
- A **hybrid cloud** enables a company to keep some information private and designate other files as public or community information.

6.1 Cloud Forensics

- Cloud forensics procedures are needed in many situations, such as cyber criminals attacking a cloud, policy violations in accessing a cloud, data recovery, reports of suspicious activity, fraud, and data breaches.
- The organizational dimension addresses the structure of the cloud, such as location of data storage and administration of services.
- The legal dimension covers service agreements and other jurisdictional matters because a cloud's data storage can be located anywhere in the world and even cross nations' boundaries.
- The technical dimension deals with procedures and specialized applications designed to perform forensics recovery and analysis in the cloud.

6.1 Cloud Forensics

innovate achieve lead

The following are capabilities forensics tools should have to handle acquiring data from a cloud:

- ***Forensic data collection***—Tools must be able to identify, label, record, and acquire data from the cloud.

- ***Elastic, static, and live forensics***—To meet the elastic nature of clouds, tools must be able to expand and contract their data storage capabilities as the demand for services changes.

- ***Evidence segregation***—Clouds are set up for **multitenancy**, meaning many different unrelated businesses and users share the same applications and storage space, so forensics tools must be able to separate each customer's data.

- ***Investigations in virtualized environments***—Because cloud operations typically run in a virtual environment, forensics tools should have the capability to examine virtual systems. Although most cloud architecture is composed of virtual machines, the actual cloud is much more complex. The failover capability is necessary in case a VM fails, and there are virtualized switches and routers along with multi-tenant and multi-cloud environments. Becoming proficient as a cloud manager on platforms such as vSphere takes a few years of experience maintaining these systems.

6.1 Cloud Forensics

innovate achieve lead

Accessing Evidence in the Cloud

- Cloud forensics typically involves litigation of criminal or civil matters.
- When information or evidence is needed, warrants and subpoenas are used to get it from parties involved in the investigation or litigation.
- When evidence needs to be seized, warrants are used in criminal cases and issued by law enforcement.
- When only information is needed, subpoenas are typically issued for civil and criminal cases.
- In the United States, the Electronic Communications Privacy Act (ECPA) describes five mechanisms the government can use to get electronic information from a provider: search warrants, subpoenas, subpoenas with prior notice to the subscriber or customer, court orders, and court orders with prior notice to the subscriber or customer.

6.1 Cloud Forensics

Search Warrants

- A search warrant can be used only in criminal cases, and it must be requested by a law enforcement officer who has evidence of probable cause that a crime was committed and evidence of it can be found at the location specified in the warrant.
- There has been a lot of litigation over the concept of “probable cause,” but not much case law applies to searches conducted in the cloud.

6.1 Cloud Forensics

Tools for Cloud Forensics

- In the early days of the cloud, very few tools designed for cloud forensics were available, but many digital, network, and e-discovery tools were used to handle collecting and analyzing data from the cloud. Some vendors with integrated tools that can be applied to cloud forensics include the following:

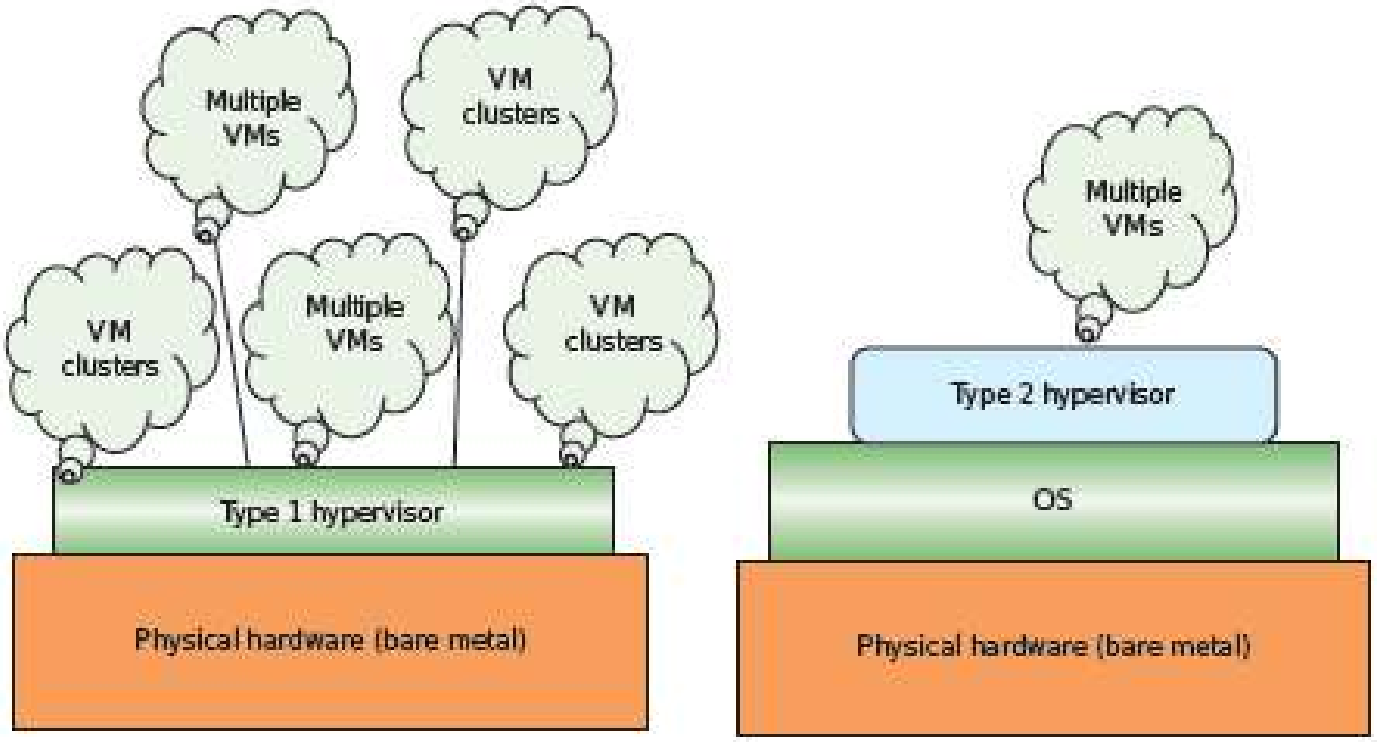
1. Guidance Software EnCase eDiscovery and its incident response and EnCase Cybersecurity tools
2. AccessData Digital Forensics Incident Response services and AD eDiscovery can collect cloud data from Office 365, SharePoint, and OneDrive for Business (*http://accessdata.com/blog/3-challenges-to-data-collection-in-the-cloud*, 2017)
3. F-Response and its cloud server forensics utility

6.1 Virtual Machine Forensics

- Virtual machines are now common for both personal and business use, so forensics investigators need to know how to analyse them and use them to analyse suspect drives and systems containing malware.
- virtual machines (VMs) help offset hardware costs for companies; in many companies, even full networks are virtual, which reduces costs substantially.
- VMs are also handy when you want to run legacy or uncommon Oss and software along with the other software on your computer.
- The software that runs virtual machines is called a “hypervisor.” There are two types of hypervisors: type 1 and type 2.
- A **type 1 hypervisor** runs on “bare metal,” meaning it loads on physical hardware and doesn’t require a separate OS, although many type 1 hypervisors incorporate Linux-based operating systems.
- Literally thousands of VMs can be hosted on a single type 1 hypervisor and many more on a cluster of these hosts.
- A **type 2 hypervisor** rests on top of an existing OS, such as Windows, Linux, or macOS.

6.1 Virtual Machine Forensics

Figure below illustrates the difference between the two:



Type 1 and type 2 hypervisors

6.1 Virtual Machine Forensics

- With rising hardware and software costs, companies have to pay careful attention to making the best investments for IT infrastructures.
- New versions of software require more RAM, hard drive space, and resources, and redeploying new versions of Oss and applications two or three times a year isn’t cost effective.
- Enter virtual machines, which make it possible for one server to support an entire department or company.
- With virtual machines in use, a well-equipped workstation or reasonably priced server can take care of all a small company’s needs.

6.1 Virtual Machine Forensics

Type 2 Hypervisors

- Type 2 hypervisors can be used on a laptop, a desktop, or even a tablet to simulate an OS environment, such as running a Windows Server 2016 VM on a Linux host.
- Companies often use these hypervisors to run legacy hardware that works only with a specific OS, such as Windows XP. Although VMs should be kept on a separate network, this setup can be a useful solution if hardware replacement costs are beyond a company's budget.
- Type 2 hypervisors are usually the ones you find loaded on a suspect machine.
- Type 1 hypervisors are typically, but not exclusively, loaded on servers or workstations with a lot of RAM and storage.
- Because users tend to be more familiar with type 2 hypervisors, you examine them first before moving on to type 1 hypervisors.

6.1 Virtual Machine Forensics

Most widely used type 2 hypervisors:

Parallels Desktop

Parallels Desktop (*www.parallels.com/products/desktop/*) was created for Macintosh users who also use Windows applications. It runs both legacy and current Windows OSs as well as Linux. Unlike most type 2 hypervisors, it isn't free but is generally under US$100.

KVM

The KVM (Kernel-based Virtual Machine; *www.linux-kvm.org/page/Main_Page*) hypervisor is for the Linux OS. This open-source hypervisor enables you to choose between an Intel and an AMD CPU and to run Linux or Windows VMs. It's now included as part of most Linux kernels. Like many type 2 hypervisors, it supplies virtualized hardware, such as graphics cards and network adapters. The version from Red Hat deploys it as a type I hypervisor.

6.1 Virtual Machine Forensics

Microsoft Hyper-V

- Microsoft began its venture into virtualization with Virtual PC, which allowed you to create VMs that could run non-Windows OSs. Its new hypervisor is built into Windows 10, and unlike most programs, it isn't downloaded.

- To install it, go to Windows PowerShell and enter Enable-WindowsOptionalFeature -Online -FeatureName:Microsoft-Hyper-V -All.
  (This command doesn't work in the Home Edition of Windows, however.)

- After it's installed, you can create virtual machines in Hyper-V Manager and create a network for VMs to access the Internet.

6.1 Virtual Machine Forensics

VMware Workstation and Workstation Player

VMware Workstation (*www.vmware.com/products/workstation*) is a solid workhorse, and although the standard version isn't free, a trial version is available.

Take a look at some of its features:

- Can be installed on almost any device, including tablets
- Can install Microsoft Hyper-V Server on it
- Can create encrypted VMs
- Capable of supporting up to 16 CPUs, 8 TB of storage, and 20 virtual networks

6.1 Network Forensics, Cloud Forensics and Virtual Machine Forensics

Weblinks for reference:

1. http://youtube.com/watch?v=fy-24WTNiyY
2. http://youtube.com/watch?v=yIVXjl4SwVo
3. Cloud Computing & Computer Forensics.mp4 – YouTube
4. Cloud forensics #DigitalForensics #ComputerSecurity#CloudDeploymentModel#Computer DataStorage#SasS - YouTube

6.2 Honeypots, Security in Mobile Systems and Cloud

- In computer terminology, a **honeypot** is a trap set to detect, deflect or in some manner counteract attempts at unauthorized use of information systems.
- Generally it consists of a computer, data or a network site that appears to be part of a network but which is actually isolated and protected, and which seems to contain information or a resource that would be of value to attackers.
- A honeypot that masquerades as an open proxy is known as a *sugarcane.*

6.2 Honeypots, Security in Mobile Systems and Cloud

- A honeypot is valuable as a surveillance and early-warning tool.
- While often a computer, a honeypot can take on other forms, such as files or data records, or even unused IP address space.
- Honeypots should have no production value and hence should not see any legitimate traffic or activity.
- Whatever they capture can then be surmised as malicious or unauthorized.

6.2 Honeypots, Security in Mobile Systems and Cloud

- One very practical implication of this is that honeypots designed to thwart spam by masquerading as systems of the types abused by spammers to send spam can categorize the material they trap 100% accurately: it is all illicit.
- A honeypot needs no spam-recognition capability, no filter to separate ordinary e-mail from spam. Ordinary e-mail never comes to a honeypot.
- Honeypots can carry risks to a network, and must be handled with care.
- If they are not properly walled off, an attacker can use them to actually break into a system.

6.2 Honeypots, Security in Mobile Systems and Cloud

- The Honeynet Project (*www.honeynet.org*) was developed to make information widely available in an attempt to thwart Internet and network attackers.
- Many people participate in this worldwide project, which is now a non-profit organization.
- The objectives are awareness, information, and tools.
- The first step is to make people and organizations aware that threats exist and they might be targets.
- The second is to provide information on how to protect against these threats, including how attackers operate, how they communicate, and what tactics they use.
- Finally, for people who want to do their own research, the Honeynet Project offers tools and methods.
- A major threat is **distributed denial-of-service (DDoS)** attacks.
- A trace of a DDoS attack might go through other organizations' networks, not just yours or your ISP's.

6.2 Honeypots, Security in Mobile Systems and Cloud

- The machines are known as **zombies** because they have unwittingly become part of the attack.
- When the first DDoS attacks began, the main concerns were the high monetary impact and the amount of time it took to track down these attacks.
- Another major threat is **zero day attacks**.
- Attackers look for holes in networks and OSs and exploit these weaknesses before patches are available.
- Vendors usually aren't aware that these vulnerabilities exist, so they haven't developed and released patches for them.
- Penetration testers attempt to break into networks to find undiscovered vulnerabilities and then predict where the next onslaught of network attacks will come from.
- In any organization, you have to determine the value of the data you're protecting and weigh it against the price of the defense system you plan to install.
- When an attack strikes, your first response is to stop it and prevent it from going further. Then you need to see what defense procedures worked and what additional procedures might be needed.
- Training and informing IT staff are critical.

6.2 Honeypots, Security in Mobile Systems and Cloud

- The Honeynet Project was set up as a resource to help network administrators deal with DDoS and other attacks.
- It involves installing honeypots and honeywalls at different locations in the world.
- A **honeypot** is a computer set up to look like any other machine on your network; its purpose is to lure attackers to your network, but it contains no information of real value.
- You can take the honeypot offline to analyze it and not affect the running of your network.
- **Honeywalls** are computers set up to monitor what's happening to honeypots on your network and record what attackers are doing (see *www.honeynet.org/papers/cdrom/*).
- Honeypots and honeywalls are commonly used to attract intruders and see what they're attempting to do on a network.

6.2 Honeypots, Security in Mobile Systems and Cloud

- Mobile security, or more specifically mobile device security, is the **protection of smartphones, tablets, and laptops from threats associated with wireless computing**.
- It has become increasingly important in mobile computing.
- One particular concern is the security of personal and business information now stored on smartphones.

6.2 Honeypots, Security in Mobile Systems and Cloud

There are three prime targets for attackers:

- Data: smartphones are devices for data management, and may contain sensitive data like credit card numbers, authentication information, private information, activity logs (calendar, call logs);
- Identity: smartphones are highly customizable, so the device or its contents can easily be associated with a specific person.
- Availability: attacking a smartphone can limit access to it and deprive the owner of its use.

6.2 Honeypots, Security in Mobile Systems and Cloud

There are a number of threats to mobile devices, including annoyance, stealing money, invading privacy, propagation, and malicious tools. Vulnerability in mobile devices is a weak spot that will allow an attacker to decrease a systems security. There are three elements that intercepts when vulnerability occurs and they are a **system weakness, attacker access to the flaw, and attacker competence to exploit the flaw.**

- Botnets: attackers infect multiple machines with malware that victims generally acquire via e-mail attachments or from compromised applications or websites. The malware then gives hackers remote control of "zombie" devices, which can then be instructed to perform harmful acts.
- Malicious applications: hackers upload malicious programs or games to third-party smartphone application marketplaces. The programs steal personal information and open backdoor communication channels to install additional applications and cause other problems.
- Malicious links on social networks: an effective way to spread malware where hackers can place Trojans, spyware, and backdoors.
- Spyware: hackers use this to hijack phones, allowing them to hear calls, see text messages and e-mails as well as track someone's location through GPS updates.

6.2 Honeypots, Security in Mobile Systems and Cloud

The source of these attacks are the same actors found in the non-mobile computing space:

- Professionals, whether commercial or military, who focus on the three targets mentioned above. They steal sensitive data from the general public, as well as undertake industrial espionage. They will also use the identity of those attacked to achieve other attacks;
- Thieves who want to gain income through data or identities they have stolen. The thieves will attack many people to increase their potential income;
- Black hat hackers who specifically attack availability. Their goal is to develop viruses, and cause damage to the device. In some cases, hackers have an interest in stealing data on devices.
- Grey hat hackers who reveal vulnerabilities. Their goal is to expose vulnerabilities of the device. Grey hat hackers do not intend on damaging the device or stealing data.

6.2 Honeypots, Security in Mobile Systems and Cloud

When a smartphone is infected by an attacker, the attacker can attempt several things:

1. The attacker can manipulate the smartphone as a zombie machine, that is to say, a machine with which the attacker can communicate and send commands which will be used to send unsolicited messages (spam) via sms or email;
2. The attacker can easily force the smartphone to make phone calls. For example, one can use the API (library that contains the basic functions not present in the smartphone) PhoneMakeCall by Microsoft, which collects telephone numbers from any source such as yellow pages, and then call them. But the attacker can also use this method to call paid services, resulting in a charge to the owner of the smartphone. It is also very dangerous because the smartphone could call emergency services and thus disrupt those services.
3. A compromised smartphone can record conversations between the user and others and send them to a third party. This can cause user privacy and industrial security problems;
4. An attacker can also steal a user's identity, usurp their identity (with a copy of the user's sim card or even the telephone itself), and thus impersonate the owner. This raises security concerns in countries where smartphones can be used to place orders, view bank accounts or are used as an identity card.

6.2 Honeypots, Security in Mobile Systems and Cloud

5. The attacker can reduce the utility of the smartphone, by discharging the battery. For example, they can launch an application that will run continuously on the smartphone processor, requiring a lot of energy and draining the battery. One factor that distinguishes mobile computing from traditional desktop PCs is their limited performance. Frank Stajano and Ross Anderson first described this form of attack, calling it an attack of "battery exhaustion" or "sleep deprivation torture“.

6. The attacker can prevent the operation and/or be starting of the smartphone by making it unusable. This attack can either delete the boot scripts, resulting in a phone without a functioning OS, or modify certain files to make it unusable (e.g. a script that launches at startup that forces the smartphone to restart) or even embed a startup application that would empty the battery.

7. The attacker can remove the personal (photos, music, videos, etc.) or professional data (contacts, calendars, notes) of the user.

Thank you

BITS Pilani

Prof. Pradnya Kashikar

WILP-CSIS

BITS Pilani
Pilani Campus

innovate achieve lead

BITS Pilani

Pilani Campus

SS ZG588 - Cyber Crimes, Forensics and Incident Handling

Contact Session - 7

Course Objectives

No	Description
CO1	Enhancing awareness of recent Cyber Crime trends and learn Investigating Cyber Crimes
CO2	Introduce Cyberspace Infrastructure attacks and handling Organization Cybersecurity Issues
CO3	Understand Digital Forensics Process, Models, Analysis and Validation, Incident Detection and Response

Text Book(s)

innovate achieve lead

T1	Computer Forensics and Cyber Crime - An Introduction 3rd Edition by Marjie T. Britz, Ph.D., Professor of Criminal Justice, Clemson University
T2	Bill Nelson, A. Philips, F. Enfinger, C. K. Steuart, Computer Forensics and Investigations, Course Technology (Cengage Learning), Indian edition, 2009
T3	Incident Response & Computer Forensics, 3rd Edition by Jason T. Luttgens and Matthew Pepe and Kevin Mandia
R1	Guide to Computer Forensics and Investigations: Processing Digital Evidence 5th Edition by Bill Nelson, Amelia Phillips and Christopher Steuart
R2	The Basics of Digital Forensics, by John Sammons
R3	Computer Network Security and Cyber Ethics 4th Edition, by Joseph Migga Kizza
R4	Computer Forensics_ Investigating Network Intrusions and Cyber Crime: EC-Council Press

Learning Outcomes -

No	Learning Outcomes
LO1	Fundamental understanding and Information on Cyber Crimes, Digital Forensics Objectives and Incident Detection and Response Reports.
LO2	Learn on how to prepare investigation on computer-related incidents or crimes and summarize.
LO3	Understand on digital forensics process, models and analysis by taking a systematic approach
LO4	Explore on evaluating needs, validating and testing digital forensics tools, Generating Incident Report Findings, and Emerging Cybercrime Trends and Issues

Module 6 - Network and Cloud Forensics; Mobile Device and Security

innovate achieve lead

6.1 Network Forensics, Cloud Forensics and Virtual Machine Forensics

6.2 Honeypots; Security in Mobile Systems and Cloud

6.3 Mobile Device Forensics: Inside Mobile Devices; SIM Card File Structure

6.4 Investigating Network Traffic; Investigating Web Attacks and Wireless Attacks

7	Network and Cloud Forensics; Mobile Device and Security	**Mobile Device Forensics: Inside Mobile Devices; SIM Card File Structure**	T2, R4
		Investigating Network Traffic; Investigating Web Attacks and Wireless Attacks	

7.1.1. Mobile device Forensics

- **Mobile device forensics helps to retrieve information from a cell phone, smartphone** tablet, or other mobile device and explores social media content on mobile devices in more depth.
- So many devices access the Internet; practically anything can be online and connected, which poses new challenges in investigations.
- People store a wealth of information on cell phones and smartphones, and the thought of losing your phone and, therefore, the information stored on it can be a frightening prospect.
- Despite this concern, not many people think about securing their phones, although they routinely lock and secure laptops or desktops.
- The use of smartphones for illicit activities—such as identity theft, child pornography, and bank fraud—has become more prevalent.

7.1.1. Mobile device Forensics

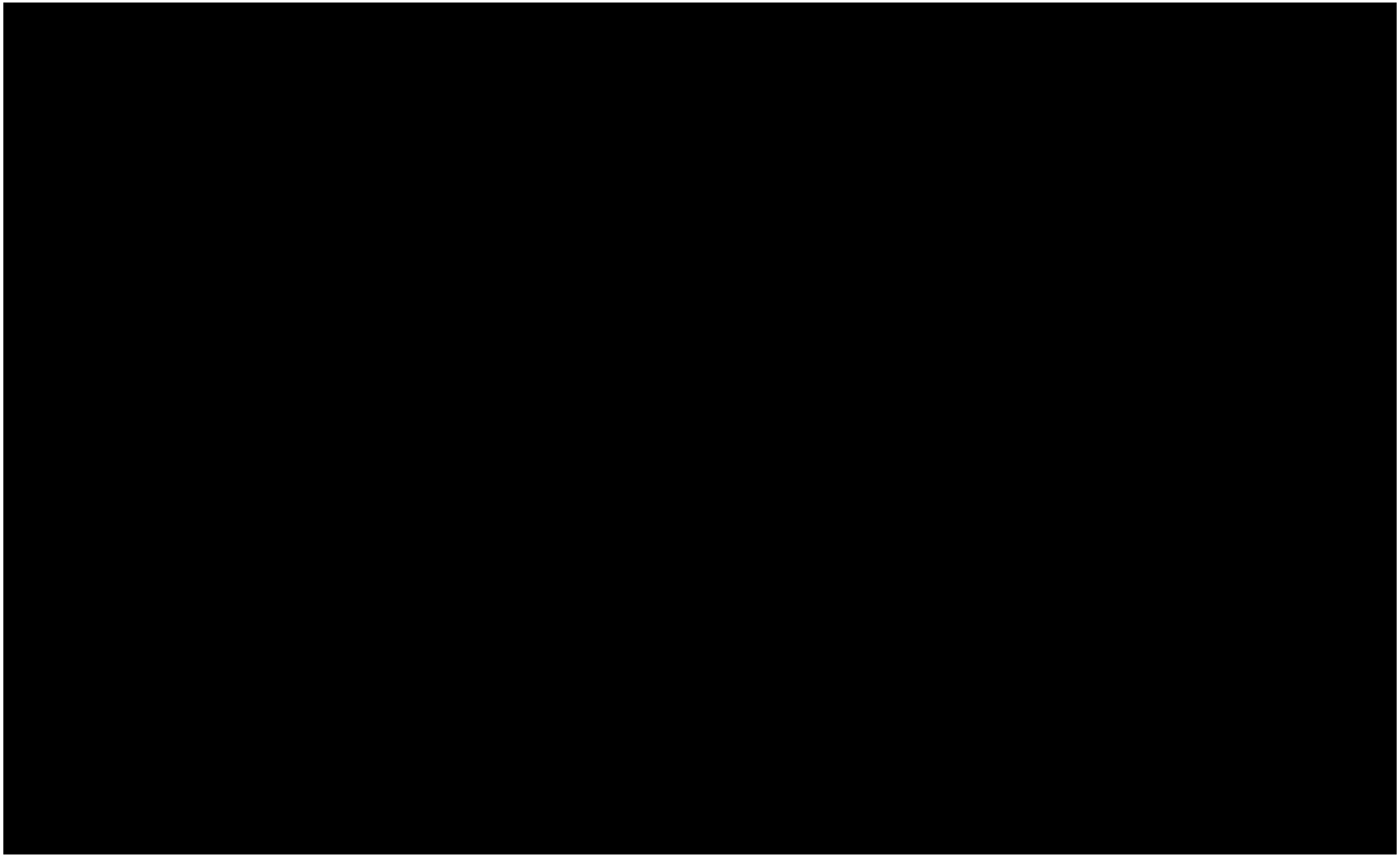
Depending on your phone's model, the following information might be stored on it:

- Incoming, outgoing, and missed calls
- Multimedia Message Service (MMS; text messages) and Short Message Service (SMS) messages
- E-mail accounts
- Instant messaging (IM) logs
- Web pages
- Photos, videos, and music files
- Calendars and address books
- Social media account information
- GPS data
- Voice recordings and voicemail
- Bank account logins
- Access to your home

7.1.1. Mobile device Forensics

- Because mobile devices are seized at the time of arrest, police used to look through them as a routine matter.
- Because phones often contain private or sensitive information, any information that doesn't pertain to the case must be redacted from the public record.
- Despite the usefulness of these devices in providing clues for investigations, investigating smartphones and other mobile devices is a challenging task in digital forensics.
- No single standard exists for how and where phones store messages, although many phones use similar storage schemes.
- In addition, new phones come out about every six months, and they're rarely compatible with previous models.
- Therefore, the cables, software, and accessories used for forensics acquisitions can become obsolete in a short time.

7.1.1. Mobile device Forensics



7.1.2 Inside mobile devices

- By the end of 2008, mobile phones had gone through three generations: analog, digital personal communications service (PCS), and **third-generation (3G)**.
- 3G introduced unheard-of capabilities, such as being able to download while you were walking or in a moving vehicle.
- Sprint Nextel introduced the **fourth-generation (4G)** network in 2009.
- **Fifth-generation (5G)** cellular networks, expected to be finalized in 2020, will incorporate emerging technologies, including the ever-expanding cloud and device-to-device networks.

7.1.2 Inside mobile devices

Although digital networks use different technologies, they operate on the same basic principles. Geographic areas are divided into cells resembling honeycombs.

As described in NIST, three main components are used for communication with these cells:

- ***Base transceiver station (BTS)***—This component is made up of radio transceiver equipment that defines cells and communicates with mobile phones; it's sometimes referred to as a "cell phone tower," although the tower is only one part of the BTS equipment.

- ***Base station controller (BSC)***—This combination of hardware and software manages BTSs and assigns channels by connecting to the mobile switching center.

- ***Mobile switching center (MSC)***—This component connects calls by routing digital packets for the network and relies on a database to support subscribers. This central database contains account data, location data, and other key information needed during an investigation. If you have to retrieve information from a carrier's central database, you usually need a warrant or subpoena.

7.1.2 Inside mobile devices

- Mobile devices can range from simple phones to **smartphones**, tablets, and smartwatches.
- The hardware consists of a microprocessor, ROM, RAM, a digital signal processor, a radio module, a microphone and speaker, hardware interfaces (such as keypads, cameras, and GPS devices), and an LCD display.
- Many have removable memory cards and up to 64 GB of internal memory, and Bluetooth and Wi-Fi are included in most mobile devices.

7.1.2 Inside mobile devices

- Most basic phones have a proprietary OS, although smartphones use the same OSs as PCs (or stripped-down versions of them).
- These OSs include Windows Mobile, RIM OS, Android (based on Linux), Google OS, and iOS (for Apple devices).
- Typically, phones store system data in **electronically erasable programmable read-only memory (EEPROM)**, which enables service providers to reprogram phones without having to access memory chips physically.
- Many users take advantage of this capability by reprogramming their phones to add features or switch to different service providers.
- Although this reprogramming isn't supported officially by service providers, instructions on how to do so are readily available on the Internet.
- The OS is stored in ROM, which is non-volatile memory, so along with other data, it's available even if the phone loses power

7.1.2 Inside mobile devices

SIM Cards

- **Subscriber identity module (SIM) cards** are usually found in GSM devices and consist of a microprocessor and internal memory.
- SIM cards are similar to standard memory cards, except the connectors are aligned differently.
- iPhones and many Android phones have micro SIM and nano SIM slots.
- However, some can be accessed only if the phone has been unlocked.
- GSM refers to mobile phones as “mobile stations” and divides a station into two parts: the SIM card and the mobile equipment (ME), which is the remainder of the phone.
- The SIM card is necessary for the ME to work and serves these additional purposes:
  - Identifies the subscriber to the network
  - Stores service-related information
  - Can be used to back up the device

7.1.2 Inside mobile devices

- SIM cards come in three sizes: standard, micro, and nano. Portability of information is what makes SIM cards so versatile.
- By switching a SIM card between compatible phones, users can move their provider usage and other information to another phone automatically without having to notify the service provider.
- For example, if you travel between neighbouring countries often, you could have a GSM phone and two SIM cards.
- When you travel to another country, you simply switch to the other SIM card.
- With phones on which this switching is allowed, information such as your contact list is stored on the phone, so when you switch to another carrier, all you have to do is change the SIM card.
- Another common practice is switching to another SIM card when you have used most of your monthly minutes on your main SIM card.

7.1.2 Inside mobile devices

- The main concerns are loss of power, synchronization with cloud services, and remote wiping.
- All mobile devices have volatile memory, so making sure they don't lose power before you can retrieve RAM data is critical.
- At the investigation scene, determine whether the device is on or off. If it's off, leave it off, but find the charger and attach it as soon as possible.
- Note this step in your log if you can't determine whether the device was charged at the time of seizure.
- If the device is on, check the display for the battery's current charge level.
- Because mobile devices are often designed to synchronize with applications on a user's laptop or tablet, any mobile device attached to a PC or tablet via a USB cable or micro USB cable should be disconnected immediately.
- Many people use their smartphones to get Internet access for tablets or laptops, so you might find these devices already connected to the Internet.
- Disconnecting them immediately helps prevent synchronization that might occur automatically on a pre-set schedule and overwrite data on the device.

7.1.2 Inside mobile devices

- In addition, collect the laptop and any peripheral devices to determine whether the hard drive contains any information that's been transferred and then deleted from the mobile device, including pictures, videos, and other files that have been transferred and then deleted.
- Depending on the warrant or subpoena, the time of seizure might be relevant.
- In addition, messages might be received on the mobile device after seizure that may or may not be admissible in court.
- If you determine that the device should be turned off to preserve battery power or prevent a possible attack, note the time and date when you take this step.

7.1.2 Inside mobile devices

The alternative is to isolate the device from incoming signals with one of the following options:

- Place the device in airplane mode, if this feature is available.
- Place the device in a paint can, preferably one that previously contained radio wave-blocking paint.
- Use a Faraday bag that conforms to Faraday wire cage standards. Many allow plugging a unit into a power source
- Turn the device off.

The drawback of using these isolating options is that the mobile device is put into roaming mode, which accelerates battery drainage. Most mobile devices shut themselves off or enter a “sleep state” after reaching a certain low battery level.

In either case, a phone that’s been seized for investigation must be isolated from incoming signals and from broadcasting.

7.1.2 Inside mobile devices

- There are three conditions: The device is on and unlocked, the device is on and locked, and the device is off.
- If it's on and unlocked, you must isolate it from the network, disable the screen lock, and remove the passcode, among other tasks.
- If the device is on and locked, what you can and can't do varies depending on the type of device, such as whether it's a BlackBerry, an iPhone, or an Android.
- If the device is off, you should attempt a physical static acquisition and then turn the device on, determine whether it's locked, and then follow the procedure for either a locked or unlocked condition.
- As devices become more sophisticated, turning them off means removing the battery.

7.1.2 Inside mobile devices

To determine whether you should do a logical acquisition or physical acquisition, you need to know where information is stored. As with laptops and desktops, a logical acquisition involves accessing files and folders as you would see them when looking at them in File Explorer. A physical acquisition is a bit-by-bit acquisition done to find deleted files or folders. You should check the following locations for information, keeping in mind that with mobile devices, often you need manufacturers' tools:

- Internal memory
- SIM card
- Removable or external memory cards
- Network provider

7.1.2 Inside mobile devices

- Because of wiretap laws, checking providers' servers requires a search warrant.
- In addition, because most newer phones and phone plans store voicemail on the phone, you need a search warrant for the device, too.
- You might also need information from the service provider to determine where the suspect or victim was at the time of a call, to access backups of contacts, and more.
- In the past, you had to serve the provider with a warrant to have a triangulation of a cell tower done to determine location.
- This is still true if you're doing an ongoing investigation and don't have the device.
- If, however, you have the device, you can usually retrieve GPS data from it.
- For iPods and iPads, syncing and backups tend to occur in the iCloud; other providers offer a similar cloud backup.

7.1.2 Inside mobile devices

- Given how crucial smartphones are now, people who lose them are concerned about the amount of sensitive information that can be gathered from them.
- Because of the growing problem of mobile devices being stolen, service providers have started using remote wiping to remove a user's personal information stored on a stolen device, and this procedure often results in the loss of valuable information for investigations.
- Remote wiping is usually done to remove an account so that a thief can't use the phone and rack up charges.
- It also erases all contacts, the calendar, and other personal information, such as photos and bank logins, stored on the device.
- In some instances, it restores the device to the original factory settings.

7.1.2 Inside mobile devices

- Depending on the device and service provider, the device owner or the service provider can do the remote wipe.
- Remote wiping can be used by device owners trying to protect their information.
- Memory storage on a mobile device is usually a combination of volatile and non-volatile memory.
- Volatile memory requires power to maintain its contents, but non-volatile memory doesn't.
- Although the locations of data vary from one phone model to the next, volatile memory usually contains data that changes frequently, such as missed calls, text messages, and sometimes even user files.
- Non-volatile memory, on the other hand, contains OS files and stored user data, such as a personal information manager (PIM) and backed-up files.

7.1.2 Inside mobile devices

7.1.3 SIM card file structure

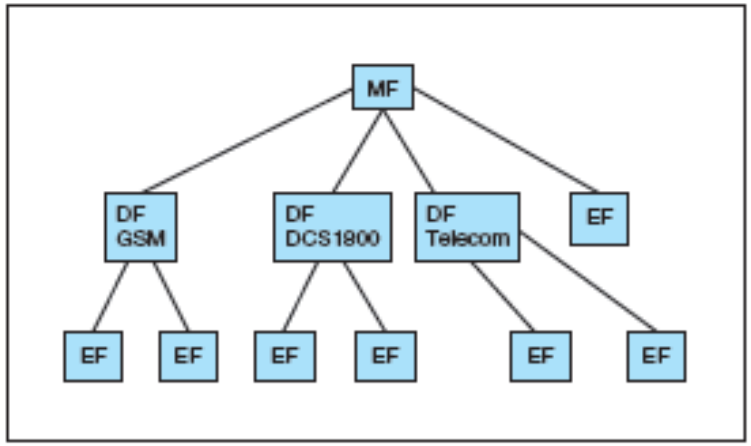


Figure 12-1 SIM file structure

- As mentioned, memory resides in the phone and in the SIM card, if the device is equipped with one. The file system for a SIM card is a hierarchical structure. (Figure 12-1).
- This file structure begins with the root of the system (MF).
- The next level consists of directory files (DF), and under them are files containing elementary data (EF).
- In this figure, the EFs under the GSM and DCS1800 DFs contain network data on different frequency bands of operation.
- The EFs under the Telecom DF contain service-related data.

7.1.3 SIM card file structure

- You can retrieve quite a bit of data from a SIM card, depending on whether the phone is GSM or CDMA. The information that can be retrieved falls into four categories:
    1. Service-related data, such as identifiers for the SIM card and subscriber
    2. Call data, such as numbers dialled
    3. Message information
    4. Location information

- If power has been lost, you might need PINs or other access codes to view files.
- Typically, users keep the original PIN assigned to the SIM card, so when you're collecting evidence at the scene, look for users' manuals and other documentation that can help you access the SIM card.

- With most SIM cards, you have three attempts at entering an access code before the device is locked, which then requires calling the service provider to get the PIN unlock key (PUK) and waiting a certain amount of time before trying again. Common codes to try are 1-1-1-1 or 1-2-3-4.

7.1.3 SIM card file structure

SIM Card Readers

- With GSM phones and many newer models of mobile devices, the next step is accessing the SIM card, which you can do by using a combination hardware/software device called a "SIM card reader."
- To use this device, you should be in a forensics lab equipped with antistatic devices.
- In addition, biological agents, such as fingerprints, might be present on the inside of the case, so you should consult the lead investigator when you're ready to proceed to this step.
- The general procedure is as follows:
    1. Remove the device's back panel.
    2. Remove the battery.
    3. Remove the SIM card from its holder.
    4. Insert the SIM card into the card reader, which you insert into your forensic workstation's USB port.
- A variety of SIM card readers are available. Some are forensically sound and some are not; make sure you note this feature in your investigation log.
- Using a tool that takes pictures of each screen can be valuable because these screen captures can provide additional documentation.

Mobile Phone Forensics Tools and Methods

- The best method of retrieving information, of course, is acquiring a forensic image, which enables you to recover deleted text messages and similar data.
- With Android devices, the process can be as simple as using AccessData FTK Imager to perform a logical acquisition and a low-level analysis.
- iPhone acquisition procedures are similar, and several good tools are available, such as MacLockPick 3.0 (*http://macforensicslab.com/product/maclockpick/*), which is designed to deal with iPhones, iPads, iOS, and Mac OS X Lion (now macOS).
- It can also extract iPhoto information, handle plug-in apps, and pull the user's online history.

- **The NIST guidelines list six types of mobile forensics methods:**

1. *Manual extraction*—This method involves looking at the device's content page by page and taking pictures. It's used if investigators can't do a logical or physical extraction.

- ***Logical extraction***—The mobile device is connected to a forensic workstation via a wired (USB cable, for example) or wireless (such as Bluetooth) connection, and then the file system information is extracted.
- ***Physical extraction***—As with a logical extraction, the mobile device is attached to a forensic workstation. However, a forensic copy is made so that deleted files can be retrieved and other items decoded.
- ***Hex dumping and Joint Test Action Group (JTAG) extraction***—Hex dumping involves using a modified boot loader to access the RAM for analysis. The JTAG extraction method gets information from the processor, flash memory, or other physical components. It's a highly invasive method.
- ***Chip-off***—This method requires physically removing flash memory chip and gathering information at the binary level.
- ***Micro read***—This method looks at logic gates with an electron microscope and can be used even when data has been overwritten on magnetic media. It's very expensive, however, so it's typically used only in cases involving national security.

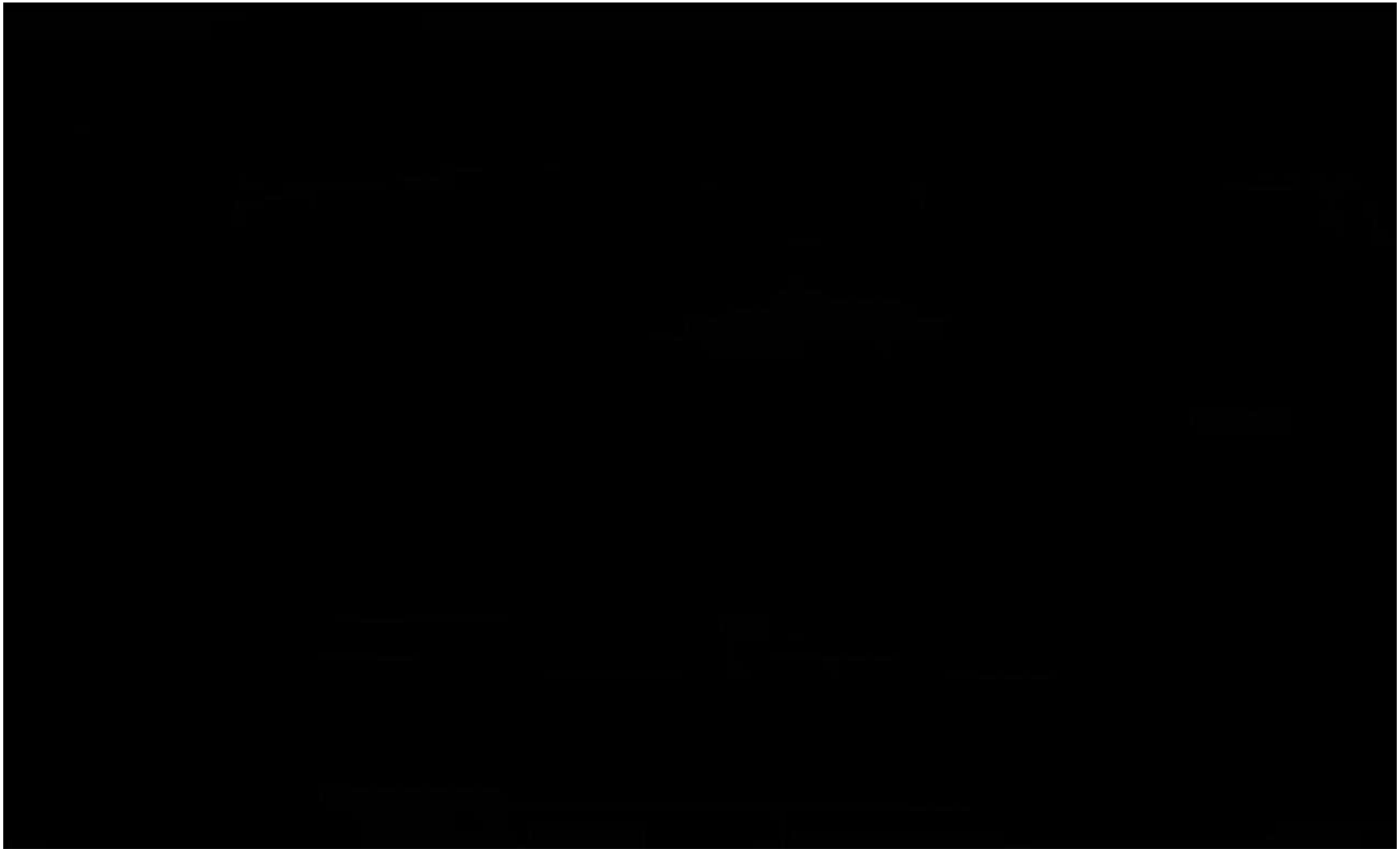
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf

7.2.1 Investigating Network Traffic

Links for reference:

1. http://youtube.com/watch?v=Hl0IpoS503A
2. Best Android Forensic Tool - For Everyone – YouTube
3. http://youtube.com/watch?v=8HTPTtEfChA
4. investigate web attack - YouTube

7.2.1 Investigating Network Traffic



7.2.2 Investigating Web attacks and Wireless attacks

Investigate Web Attack

Thank you.

https://timesofindia.indiatimes.com/india/70-indian-government-private-websites-face-international-cyber-attacks-over-prophet-row/articleshow/92167143.cms

https://economictimes.indiatimes.com/news/politics-and-nation/bjps-official-website-hacked-taken-offline/videoshow/68274001.cms

BITS Pilani

Prof. Pradnya Kashikar

WILP-CSIS

BITS Pilani
Pilani Campus

innovate achieve lead

BITS Pilani

Pilani Campus

SS ZG588 - Cyber Crimes, Forensics and Incident Handling

Contact Session - 8

Course Objectives

No	Description
CO1	Enhancing awareness of recent Cyber Crime trends and learn Investigating Cyber Crimes
CO2	Introduce Cyberspace Infrastructure attacks and handling Organization Cybersecurity Issues
CO3	Understand Digital Forensics Process, Models, Analysis and Validation, Incident Detection and Response

Text Book(s)

innovate achieve lead

T1	Computer Forensics and Cyber Crime - An Introduction 3rd Edition by Marjie T. Britz, Ph.D., Professor of Criminal Justice, Clemson University
T2	Bill Nelson, A. Philips, F. Enfinger, C. K. Steuart, Computer Forensics and Investigations, Course Technology (Cengage Learning), Indian edition, 2009
T3	Incident Response & Computer Forensics, 3rd Edition by Jason T. Luttgens and Matthew Pepe and Kevin Mandia
R1	Guide to Computer Forensics and Investigations: Processing Digital Evidence 5th Edition by Bill Nelson, Amelia Phillips and Christopher Steuart
R2	The Basics of Digital Forensics, by John Sammons
R3	Computer Network Security and Cyber Ethics 4th Edition, by Joseph Migga Kizza
R4	Computer Forensics_ Investigating Network Intrusions and Cyber Crime: EC-Council Press

Learning Outcomes -

No	Learning Outcomes
LO1	Fundamental understanding and Information on Cyber Crimes, Digital Forensics Objectives and Incident Detection and Response Reports.
LO2	Learn on how to prepare investigation on computer-related incidents or crimes and summarize.
LO3	Understand on digital forensics process, models and analysis by taking a systematic approach
LO4	Explore on evaluating needs, validating and testing digital forensics tools, Generating Incident Report Findings, and Emerging Cybercrime Trends and Issues

Module 7 - Digital Forensic Tools and Labs

7.1 Digital Forensics Hardware and Software Tools

7.2 Evaluating Digital Forensics Tools Needs; Understand Tasks done by Digital Forensics Tools and Labs

7.3 Understanding Forensics Lab Accreditation Requirements

7.4 Determining the Physical Requirements for a Digital Forensics Lab

8	Digital Forensic Tools and Labs	**Digital Forensics Hardware and Software Tools**	T1, R1, R2
		Evaluating Digital Forensics Tools Needs, Understand Tasks done by Digital Forensics Tools and Labs	
		Understanding Forensics Lab Accreditation Requirements	
		Determining the Physical Requirements for a Digital Forensics Lab	

Digital Forensics Hardware and Software Tools

- If there's one important source of forensic evidence, it's computers.
- However, newer criminals aren't the only ones taking advantage of the technology—their traditional counterparts, too, have turned to computers.
- But there's one silver lining here: these criminals can be caught and prosecuted by a digital forensic engineer who can reliably extract the forensic information from these machines.
- Computer forensics tools extract reliable and accurate information.

Digital Forensics Hardware and Software Tools

Forensic Toolkit (FTK)

- FTK is an inexpensive forensic software tool created by AccessData.
- Its one-touch-button interface makes it very easy to use.
- AccessData has also come up with ACE—a forensic certification that's based on its software.
- FTK has turned the behind-the-scenes, hard work of setting up searches by automating certain procedures. For example, just by pressing a button pops up an email.
- The FTK report generator is what does all the hard yards.
- Basically, it puts a useful report into the automated hands of forensic software while still enabling the examiner to control the report if they want.

Digital Forensics Hardware and Software Tools

Forensic Recovery of Evidence Device (FRED)

- Digital Intelligence came up with FRED—a forensic workstation that has an interface for every occasion.
- Besides the laboratory version, FRED is also compatible with mobile phones, facilitating the extraction of evidence in the field for rapid analysis.
- But what does FRED do? It combines almost every interface into a single, convenient workstation, freeing you of connecting/disconnecting a toolbox littered with interfaces.
- There's another helpful FRED feature: upon request, it allows you to collect software packages loaded on it.
- This may include FTK, EnCase, and the like.

Digital Forensics Hardware and Software Tools

- Many organizations consider EnCase as the gold standard for almost every computer forensic examination.
- It's unlike any of its competitors as it allows you to tailor it for unique searches.
- If you have a computer forensic toolbox, don't forget to make EnCase a part of it.
- EnCase has a ton of built-in forensic features, for instance, web page carving, e-mail searches, keyword searches, etc.
- You can use EnCase as a full-blown network forensic-analysis tool or a more subtle, mobile device acquisition tool—the options are endless.
- Two of its best features are:
  1. Fully automated report function: It quickly builds reports for you.
  2. Scripting language: You can tailor searches.

Evaluating Digital Forensics Tools Needs

- Digital Forensics is a branch of forensic science that focuses on identifying, acquiring, processing, analysing and reporting on data stored on a computer, digital devices or other digital storage media.
- The computer, digital device or other digital storage system which holds valuable data for investigation is known as electronic evidence.
- Such examples are laptops, smartphones, servers, Digital Video recorders, CCTV systems, drones, GPS systems, and game consoles.
- The main goal of digital forensics is to extract data from the electronic evidence, process the data into useful information and present the findings for prosecution.
- All processes involved, therefore, should utilize sound forensic techniques to ensure that the findings are admissible in court.

Tasks done by Digital Forensics Tools and Labs

innovate achieve lead

The main tasks done by digital forensic tools and labs are:

- Management system
- Document control
- Subcontracting of tests and calibrations
- Purchasing services and supplies
- Service to the customer
- Complaints
- Corrective action
- Preventive action
- Test and calibration methods and method validation
- Assuring the quality of test and calibration results
- Reporting the results

Understanding Forensics Lab Accreditation Requirements

- This ISO outlines 5 major requirements for DFL as follows: i) General Requirement ii) Structural Requirement iii) Resource Requirement iv) Process Requirement v) Management System Requirement
- Digital Forensics Laboratory (DFL) accreditation based on ISO/IEC 17025:2017 standard and accrediting body's supplemental requirement The General Requirement addresses confidentiality and impartiality statements.
- The Structural Requirement, on the other hand, addresses the legality of the laboratory and overall responsibility of the lab and its organization.
- The Resource Requirement specifies the requirement for personnel, laboratory environment, equipment, and contractors.
- Meanwhile, the Process Requirement touches on request from stakeholder, methods, exhibits, reporting of results, complaints, nonconforming works, and control of data.
- The last requirement, the Management System, addresses risk management, corrective actions, internal audits, and management review.

Understanding Forensics Lab Accreditation Requirements

- Laboratory accreditation The accreditation of laboratories and processes seems to offer fewer practical problems of implementation.
- The chosen international standard is ISO 17025.
- This standard specifies the general requirements for the competence for laboratories to carry out tests and/or calibrations, including sampling. It covers testing and calibration performed using standard methods, non-standard methods, and laboratory-developed methods.
- It is not specific to forensic science. It seems to work well for traditional “wet” forensic science laboratories which carry out series of individual tests on DNA, blood, fibre, fingerprints and paint fragments.
- Senior forensic scientists will have researched the underlying science and arranged for it to be written up in a peer-reviewed journal; they will have designed tests which incorporate the science but also cover the management aspects of practical forensics – to include recording and reporting.
- Once established, commoditised routine work can be passed on to forensic technicians.

Understanding Forensics Lab Accreditation Requirements

- The overall process needs “validation”.
- For each process what is required is a statement of end-user requirements, a formal specification, a risk assessment indicating the potential limits of the value of the process, a formal statement of the acceptance criteria, a formal validation plan followed by an exercise and assessment followed by a report supported if necessary by a library of results.
- All this must be properly documented.
- At the end of the process there is a statement of validation completion.
- Assessment is carried out by a third party.

Determining the Physical Requirements for a Digital Forensics Lab

- Physical Security Recommendations in the level of **physical security** required for a forensics lab depends on the nature of investigations performed in the lab.
- The **assessment of risk** for a forensics lab varies from organization to organization.
- If the organization is a regional forensics lab, then the assessed risk is high as the tabs deal with multiple cases and different types of evidence.
- This may not be true for the forensics lab of a private firm.
- Maintain a log register at the entrance of the lab to record the following data name of visitor with date, time, purpose of the visit, name of contact person, and address of the visitor.
- Provide visitors with passes to distinguish them from the lab staff, Place an alarm in the lab to provide an additional layer of protection and deploy guards around the premises of the lab

Determining the Physical Requirements for a Digital Forensics Lab

- Place closed-circuit cameras in the lab and around its premises to **monitor** human movement within the lab.
- Ensure security of the lab by keeping all the windows closed.
- This helps prevent unauthorized physical access to the lab from a covert channel.
- Place fire extinguishers within and outside the lab, and provide training to the lab personnel and guards on how to use the fire extinguisher, so that personnel know how to use the equipment effectively in case of fire.
- Shield workstations from transmitting electromagnetic signals, as electronic equipment emit electromagnetic radiation, which can be helpful to discover the data the equipment is transmitting or displaying.

Digital Forensic Lab Guidelines - YouTube

Thank you.

BITS Pilani

Prof. Pradnya Kashikar

WILP-CSIS

BITS Pilani
Pilani Campus

innovate achieve lead

BITS Pilani

Pilani Campus

SS ZG588 - Cyber Crimes, Forensics and Incident Handling

Contact Session - 9

Course Objectives

No	Description
CO1	Enhancing awareness of recent Cyber Crime trends and learn Investigating Cyber Crimes
CO2	Introduce Cyberspace Infrastructure attacks and handling Organization Cybersecurity Issues
CO3	Understand Digital Forensics Process, Models, Analysis and Validation, Incident Detection and Response

Text Book(s)

innovate achieve lead

T1	Computer Forensics and Cyber Crime - An Introduction 3rd Edition by Marjie T. Britz, Ph.D., Professor of Criminal Justice, Clemson University
T2	Bill Nelson, A. Philips, F. Enfinger, C. K. Steuart, Computer Forensics and Investigations, Course Technology (Cengage Learning), Indian edition, 2009
T3	Incident Response & Computer Forensics, 3rd Edition by Jason T. Luttgens and Matthew Pepe and Kevin Mandia
R1	Guide to Computer Forensics and Investigations: Processing Digital Evidence 5th Edition by Bill Nelson, Amelia Phillips and Christopher Steuart
R2	The Basics of Digital Forensics, by John Sammons
R3	Computer Network Security and Cyber Ethics 4th Edition, by Joseph Migga Kizza
R4	Computer Forensics_ Investigating Network Intrusions and Cyber Crime: EC-Council Press

Learning Outcomes -

No	Learning Outcomes
LO1	Fundamental understanding and Information on Cyber Crimes, Digital Forensics Objectives and Incident Detection and Response Reports.
LO2	Learn on how to prepare investigation on computer-related incidents or crimes and summarize.
LO3	Understand on digital forensics process, models and analysis by taking a systematic approach
LO4	Explore on evaluating needs, validating and testing digital forensics tools, Generating Incident Report Findings, and Emerging Cybercrime Trends and Issues

Module 8 - Organizations and Cyber Crime, Criminology and Organized Crime

innovate achieve lead

8.1 Organizations and Cyber Crime

8.2 Criminology and Theories

8.3 Organized Crime and Technology

9	Organizations and Cyber Crime, Criminology and Organized Crime	Organizations and Cyber Crime Criminology and Theories Organized Crime and Technology	T1, R1

https://www.esecurityplanet.com/networks/code-spaces-destroyed-by-cyber-attack/

https://www.youtube.com/watch?v=D7oODKb-WXM

https://www.theguardian.com/business/2022/apr/05/the-works-close-stores-cyber-attack-uk-security-breach

Organizations and cyber crimes

- Data breaches, denial-of-service attacks, malware, and corporate espionage are just some of the threats organizations have had to deal with these past several years.
- With the threat of a cyberattack looming on the horizon, businesses need to re-assess how they collect, store, and protect sensitive information. Many organizations have stopped the practice of storing their customers' personal and financial information on their servers.
- There's no data breach if there's nothing to steal.
- Some companies have even shut down their online storefronts due to growing concerns that they can't protect against an attack. Sixty percent of organizations that suffer a breach go out of business after six months.
- Because the recent attacks have been mainstream, customers are now demanding to know how firms handle their data.

Organizations and cyber crimes

- Even if cybercriminals can't break into a company's network, they can still cause problems by way of identity theft and fraud. Stolen personal information from one source can be the point of entry for another.
- Businesses need to have a good identity monitoring service in place to watch out for leaks and breaches that can affect their staff and clients.
- Companies that suffer a breach not only lose a treasure trove of sensitive data, they also lose business and face stiff fines or even lawsuits. As mentioned earlier, more than half of small businesses that get attacked aren't able to recover.
- If they pull through, there will always be a stigma that they're not taking their customer's information seriously.

Organizations and cyber crimes

- Another favorite of cybercriminals is disrupting operations by using a denial-of-service (DoS) attack.
- A DoS attack will make websites or online stores unavailable to its users.
- Customers that can't log in or use a company's services are a significant revenue loss that can go viral.
- People who report on the issue and rant on social media can permanently damage the reputation of the affected company.

- The attack that forced Code Spaces out of business – what went wrong? - IT Governance UK Blog

Criminology and Theories

- Criminology is the study of why individuals commit crimes and why they behave in certain situations.
- Understanding why a person commits a crime, one can develop ways to control crime or rehabilitate the criminal. There are many theories in criminology.
- Some attribute crime to the individual; they believe that an individual weights the pros and cons and makes a conscious choice whether or not to commit a crime.
- Others believe it is the community's responsibility to ensure that their citizens do not commit crime by offering them a safe and secure place in which to live.
- Some ascertain that some individuals have latent traits that will determine how they will react when put in certain negative conditions.
- By studying these theories and applying them to individuals, perhaps psychologists can deter criminals from repeating crimes and help in their rehabilitation.

Criminology and Theories

- **Choice Theory:** The belief that individuals choose to commit a crime, looking at the opportunities before them, weighing the benefit versus the punishment, and deciding whether to proceed or not.
- **Classical Theory:** Similar to the choice theory, this theory ascertains that people think before they proceed with criminal actions; that when one commits a crime, it is because the individual decided that it was advantageous to commit the crime.
- **Conflict Theory:** The conflict theory holds that crime results from the conflicts in society among the different social classes, and that laws actually arise from necessity as a result of conflict, rather than a general consensus.

Criminology and Theories

- **Critical Theory:** Critical theory upholds the belief that a small few, the elite of the society, decide laws and the definition of crime; those who commit crimes disagree with the laws that were created to keep control of them.
- **Labelling Theory:** Those who follow the labelling theory of criminology ascribe to the fact that an individual will become what he is labelled or what others expect him to become; the danger comes from calling a crime a crime and a criminal a criminal.
- **Life Course Theory:** The theory that a person's "course" in life is determined by short (transitory) and long (trajectory) events in his life, and crime can result when a transitory event causes stress in a person's life causing him to commit a crime against society.

Criminology and Theories

innovate achieve lead

- **Positivist Theory:** The positivist rejects the idea that each individual makes a conscious, rational choice to commit a crime; rather, some individuals are abnormal in intelligence, social acceptance, or some other way, and that causes them to commit crime.
- **Rational Choice Theory:** Reasons that an individual thinks through each action, deciding on whether it would be worth the risk of committing a crime to reap the benefits of that crime, whether the goal be financial, pleasure, or some other beneficial result.
- **Routine activity theory:** Followers of the routine activity theory believe that crime is inevitable, and that if the target is attractive enough, crime will happen; effective measures must be in place to deter crime from happening.

Criminology and Theories

- **Social Control Theory:** Theorists believe it is society's responsibility to maintain a certain degree of stability and certainly in an individual's life, to make the rules and responsibilities clear, and to create other activities to thwart criminal activity.
- **Social disorganization theory:** Suggests that crime occurs in communities that experience breakdown in social mores and opportunities, such as in highly populated, lower income, urban communities.
- **Social Learning Theory:** Social learning indicates that individuals learn from those around them; they base their morals and activities on what they see others in their social environment doing.

Criminology and Theories

- **Strain Theory:** The theory holds that individuals will turn to a life of crime when they are strained, or when they are unable to achieve the goals of the society, whether power, finance, or some other desirable goal.
- **Trait Theory:** Those who follow the trait theory believe that individuals have certain traits that will contribute to whether or not they are capable of committing a crime when pushed in a certain direction, or when they are in duress.

Organized Crime & Technology

- Cyber organized crime can include organized criminal groups engaging in cybercrime and cybercriminals or other groups that do not meet the criteria established by the Organized Crime Convention, that engage in activities typically associated with organized crime.
- Organized cyber crime groups may be small or large, loosely affiliated or well-defined; some groups are almost corporate in nature, with established leadership and various members filling specific functional roles.

Organized Crime & Technology

- **Hacktivists:** Some groups of cyber criminals are driven by a particular political or social agenda. “Hacktivists” tend to be more interested in embarrassing companies or publicizing damning evidence of some sort and are usually not interested in robbing their targets of money or assets.
- What is hacktivism? (techtarget.com)
- **Terrorists:** The threat of terrorism increased significantly in the aftermath of the September 11 attacks. Thankfully, most terror organizations lack the technical savvy and resources to pull off major cyber attacks. In fact, according to The International Cyber Terrorism Regulation Project, terrorist cyber crime tends to involve mostly the publication of propaganda, psychological campaigns (such as beheading videos), intelligence, information sharing and other communication.

Organized Crime & Technology

- **State-backed hackers:** Espionage continues to be prevalent in the modern world. Recent history is replete with examples of alleged state-backed hacking campaigns. The Stuxnet worm hack of the 2000s was allegedly developed by the U.S. and its allies to disrupt Iran's nuclear program. China has been accused of digital espionage involving U.S. industrial secrets. In 2020, hackers allegedly backed by the Russian government accessed U.S. government and corporate networks by exploiting software made by SolarWinds.

- **Insider threats:** Criminal organizations can also target insiders with blackmail. The goal is to obtain corporate secrets, sensitive data, passwords and other types of access to secure networks that could result in the theft of money or information.

- **Blurred lines:** As with most things, the real world is rarely neatly divided into precise categories. Many organized cyber crime groups participate in hacking "all of the above." A terrorist organization, for example, could employ tech-savvy individuals to recruit new members, run hacktivism campaigns and deploy a phishing campaign or ransomware attack to obtain sensitive cyber security information and finance terror operations.

Organized Crime & Technology

Examples of Organized crimes –

- **Botnets**—a botnet is a network of computers that attackers infected with malware, compromised and connected them to a central command & control center. The attackers enlist more and more devices into their botnet, and use them to send spam emails, conduct DDoS attacks, click fraud, and cryptomining. Users are often unaware their computer is being used as a platform for cyber crime.
- **Ransomware and other malware**—Ransomware is malware that encrypts data on a local machine and demands a ransom to unlock it. There are hundreds of millions of other types of malware that can cause damage to end-user devices and result in data exfiltration.

Organized Crime & Technology

Examples of Organized crimes –

- **Phishing and other social engineering attacks**—phishing involves sending misleading messages via email or other channels, that cause internet users to provide personal information, access malicious websites or download malicious payloads.
- **Fraud and identity theft**—fraud is the theft of funds by an attacker pretending to be the owner of an account, or using stolen cards or credentials. Identity theft is a related concept, and involves compromising a user's online accounts to enable an attacker to perform actions in their name.

Organized Crime & Technology

Examples of Organized crimes –

- **Flood attacks**—most modern flood attacks are DDoS attacks, which leverage a botnet to hit a website or organization with massive amounts of fake traffic. Flood attacks can be targeted at the network layer, choking an organization's bandwidth and server resources, or at the application layer, bringing down a database or email server for example.
- **Browser hijacking**—attacks like cross site scripting (XSS) can cause malicious code to run in a user's browser. This can result in session hijacking, drive-by downloads and other illicit activity carried out in the user's browser without their consent.

Case study examples

innovate achieve lead

- **In 2013-2016**, Yahoo experienced a data breach which resulted in the theft of 3 billion user accounts. For some of these accounts, the attackers got hold of private information and passwords, which could be used to access user accounts in other online services. Much of this data is available today, either free or for a price, on the dark web.
- **In 2014**, US retailer Home Depot's point of sale systems were breached. Attackers stole 50 million personal credit cards, and for some time any credit card swiped at Home Depot stores was captured and its details compromised by the attackers.

Case study examples

- **In 2016**, the largest ever distributed denial of service (DDoS) attack took place, which used over 1 million connected devices in the Internet of Things, which were compromised by the attackers due to software vulnerabilities. The attack caused outages in the global domain name system (DNS) and popular services including Twitter, Netflix and PayPal.
- **In 2017**, the WannaCry attack, allegedly launched by North Korea, unleashed a type of ransomware which not only locks down content on user devices, but also rapidly spreads itself. WannaCry infected 300,000 computers around the world, and users were asked to pay hundreds of dollars to decrypt and restore their data.

Air Force Network - Wikipedia

Thank you.

BITS Pilani

Prof. Pradnya Kashikar

WILP-CSIS

BITS Pilani
Pilani Campus

innovate achieve lead

BITS Pilani

Pilani Campus

SS ZG588 - Cyber Crimes, Forensics and Incident Handling

Contact Session - 10

Course Objectives

No	Description
CO1	Enhancing awareness of recent Cyber Crime trends and learn Investigating Cyber Crimes
CO2	Introduce Cyberspace Infrastructure attacks and handling Organization Cybersecurity Issues
CO3	Understand Digital Forensics Process, Models, Analysis and Validation, Incident Detection and Response

Text Book(s)

innovate achieve lead

T1	Computer Forensics and Cyber Crime - An Introduction 3rd Edition by Marjie T. Britz, Ph.D., Professor of Criminal Justice, Clemson University
T2	Bill Nelson, A. Philips, F. Enfinger, C. K. Steuart, Computer Forensics and Investigations, Course Technology (Cengage Learning), Indian edition, 2009
T3	Incident Response & Computer Forensics, 3rd Edition by Jason T. Luttgens and Matthew Pepe and Kevin Mandia
R1	Guide to Computer Forensics and Investigations: Processing Digital Evidence 5th Edition by Bill Nelson, Amelia Phillips and Christopher Steuart
R2	The Basics of Digital Forensics, by John Sammons
R3	Computer Network Security and Cyber Ethics 4th Edition, by Joseph Migga Kizza
R4	Computer Forensics_ Investigating Network Intrusions and Cyber Crime: EC-Council Press

Learning Outcomes -

No	Learning Outcomes
LO1	Fundamental understanding and Information on Cyber Crimes, Digital Forensics Objectives and Incident Detection and Response Reports.
LO2	Learn on how to prepare investigation on computer-related incidents or crimes and summarize.
LO3	Understand on digital forensics process, models and analysis by taking a systematic approach
LO4	Explore on evaluating needs, validating and testing digital forensics tools, Generating Incident Report Findings, and Emerging Cybercrime Trends and Issues

Module 9 - Investigating Internet Crime and E-Mail Crime

9.1 Introduction to Investigating Internet Crime; Conducting an Investigation and Completing the case

9.2 Processing Crime and Incident Scenes, Steps for Investigating Internet Crime

9.3 Examining E-mail Headers, Tracking E-Mails

9.4 Investigating E-Mail Crime and Violations

9.5 Remediation Case Study

10	Investigating Internet Crime and E-Mail Crime	**Introduction to Investigating Internet Crime; Conducting an Investigation and Completing the case**	T2, R1,R4
		Processing Crime and Incident Scenes, Steps for Investigating Internet Crime	
		Examining E-mail Headers, Tracking E-Mails	
		Investigating E-Mail Crime and Violations	

[Email Header Analysis and Forensic Investigation - YouTube]

Introduction to Investigating Internet Crime

1. The use of the Internet and other computer networks has seen explosive growth. As a result, any crime could involve devices that communicate through the Internet or through a network.

2. The investigator should be aware that criminals may use the Internet for numerous reasons, including—

■ Trading/sharing information (e.g., documents, photographs, movies, sound files, text and graphic files, and software programs).

■ Concealing their identity.

■ Assuming another identity.

■ Identifying and gathering information on victims.

■ Communicating with co-conspirators.

■ Distributing information or misinformation.

■ Coordinating meetings, meeting sites, or parcel drops.

Introduction to Investigating Internet Crime

1. Investigations vary in scope and complexity. Evidence of the crime may reside on electronic devices in numerous jurisdictions and may encompass multiple suspects and victims.
2. Complex evidentiary issues are frequently encountered in Internet and network investigations.
3. Sources of information needed to investigate the case may be located anywhere in the world and may not be readily available to the investigator, such as—

■ Victims and suspects and their computers.

■ Data on workstations/servers/routers of third parties such as businesses, government

entities, and educational institutions.

■ Internet Service Provider records.

Introduction to Investigating Internet Crime

1. Digital evidence is fragile and can easily be lost. For example:

- It can change with usage.
- It can be maliciously and deliberately destroyed or altered.
- It can be altered due to improper handling and storage.

2. For these reasons, evidence should be expeditiously retrieved and preserved.

3. Also consider that when investigating offenses involving the Internet, time, date, and time zone information may prove to be very important.

4. Server and computer clocks may not be accurate or set to the local time zone.

5. The investigator should seek other information to confirm the accuracy of time and date stamps.

Introduction to Investigating Internet Crime

innovate achieve lead

1. Just as every house has an address, every computer connected to the Internet has an address.
2. This is referred to as an Internet Protocol (IP) address. This chapter explains how IP addresses are assigned and how to trace the addresses to their source.
3. The investigator may also be presented with other types of addresses.
4. Some examples of these addresses are e-mail addresses and World Wide Web addresses.

   Type Example

   E-mail address: someone@nist.gov

   Web site address: www.nist.gov

   Internet Protocol address: 129.6.13.23

5. All of these may be traced to provide investigative leads.

Conducting an Investigation and Completing the case

innovate achieve lead

Where's the evidence?

Information can be found in numerous locations, including—

- User's computer.
- ISP for the user.
- ISP for a victim and/or suspect.
- Log files contained on the victim's and/or suspect's—

— Routers.

— Firewalls.

— Web servers.

— E-mail servers.

— Other connected devices.

Conducting an Investigation and Completing the case

1. An investigator should not attempt to examine a computer system if the investigator has not received special training in forensic examination of computers.
2. The investigator should follow agency policy or contact an agency with a forensic examination capability.
3. A forensic investigation of a computer system might reveal additional information, such as—
    - Other e-mail messages related to the investigation.
    - Other e-mail addresses.
    - Sender information.
    - Content of the communications.
    - IP addresses.
    - Date and time information.
    - User information.
    - Attachments.
    - Passwords.
    - Application logs that show evidence of spoofing.

Processing Crime and Incident Scenes

1. At the scene, the best judgment of the investigator (based on training, experience, and available resources) will dictate the investigative approach.
2. In some cases a forensic examination of the computer will be needed.
3. The investigator should be aware that any action taken on the computer system might affect the integrity of the evidence.
4. Only in exigent circumstances (e.g., imminent threat of loss of life or serious physical injury) should an investigator attempt to gain information directly from a computer on the scene.
5. Any action taken should be well documented.
6. In some cases it may be sufficient to collect information from the complainant (and computer), document the incident, and forego a forensic examination of the complainant's computer.
7. However, if a suspect's computer is identified and recovered, in most situations it should be submitted for forensic examination to preserve the integrity of the evidence.

Steps for Investigating Internet Crime

1. Although this special report focuses on the technical portion of these investigations, it is important to remember that a traditional investigative process must be followed:
2. Witnesses must be identified and interviewed, evidence must be collected, investigative processes should be documented, and chain-of-custody and the legal process must be followed.
3. In addition, the investigator should consider the following:
    - Was a crime committed?
    - Who has jurisdiction?
    - What resources are needed to conduct the investigation?
    - Are sufficient resources available to support the investigation?
    - What other resources are available?
    - Are there legal issues for discussion with the prosecutor?

Examining E-mail Headers

Examining E-mail Messages

1. After you have determined that a crime has been committed involving e-mail, first access the victim's computer to recover the evidence.
2. Using the victim's e-mail client, find and copy any potential evidence.
3. It might be necessary to log on to the e-mail service and access any protected or encrypted files or folders.
4. If you can't actually sit down at the victim's computer, you have to guide the victim on the phone to open and print a copy of an offending message, including the header.
5. The header contains unique identifying numbers, such as the IP address of the server that sent the message.
6. This information helps you trace the e-mail to the suspect.

Examining E-mail Headers

innovate achieve lead

Copying an E-mail Message

- Before you start an e-mail investigation, you need to copy and print the e-mail involved in the crime or policy violation.
- You might also want to forward the message as an attachment to another email address, depending on your organization's guidelines.
- The following activity shows you how to use Outlook 2007, included with Microsoft Office, to copy an e-mail message to a USB drive. (Note: Depending on the Outlook version you use, the steps might vary slightly.)
- You use a similar procedure to copy messages in other e-mail programs, such as Outlook Express and Evolution.

Examining E-mail Headers

If Outlook or Outlook Express is installed on your computer, follow these steps:

- Insert a USB drive into a USB port.
- Open Windows Explorer or the Computer window, navigate to the USB drive, and leave this window open.
- Start Outlook by clicking Start, pointing to All Programs, pointing to Microsoft Office, and clicking Microsoft Office Outlook 2007.

Examining E-mail Headers

- In the Mail Folders pane, click the folder containing the message you want to copy. For example, click the Inbox folder. A list of messages in that folder is displayed in the pane in the middle. Click the message you want to copy.
- Resize the Outlook window so that you can see the message you want to copy and the USB drive icon in Windows Explorer or the Computer window.
- Drag the message from the Outlook window to the USB drive icon in Windows Explorer or the Computer window.
- Click File, Print from the Outlook menu to open the Print dialog box. After printing the e-mail so that you have a copy to include in your final report, exit Outlook.

Examining E-mail Headers

Viewing E-mail Headers

- After you copy and print a message, use the e-mail program that created it to find the e-mail header.
- This section includes instructions for viewing e-mail headers in a variety of e-mail programs, including Windows GUI clients, a UNIX command-line e-mail program, and some common Web based e-mail providers.
- After you open e-mail headers, copy and paste them into a text document so that you can read them with a text editor, such as Windows.

Tracking E-Mails

To retrieve an Outlook e-mail header, follow these steps:

- Start Outlook, and then select the original of the message you copied in the previous section.
- Right-click the message and click Message Options to open the Message Options dialog box. The Internet headers text box at the bottom contains the message header.
- Select all the message header text, and then press Ctrl+C to copy it to the Clipboard.

Tracking E-Mails

innovate achieve lead

- Start Notepad, and then press Ctrl+V in a new document window to paste the message header text.
- Save the document as Outlook Header.txt in your work folder. Then close the document and exit Outlook. To retrieve an Outlook Express e-mail header, follow these steps:

1. Start Outlook Express, and then display the message you want to examine.
2. Right-click the message and click Properties to open a dialog box showing general information about the message.
3. Click the Message Source button to view the e-mail's HTML source code, which can be helpful in examining possible phishing messages.

Tracking E-Mails

4. Select all the message header text, and then press Ctrl+C to copy it to the Clipboard.
5. Start Notepad, and then press Ctrl+V in a new document window to paste the message header text.
6. Save the document as Outlook Express Header.txt in your work folder, and then exit Notepad.
7. Close all open windows and dialog boxes, and then exit Outlook Express.

Investigating E-Mail Crime and Violations

1. Investigating crimes or policy violations involving e-mail is similar to investigating other types of computer abuse and crimes.
2. Your goal is to find out who's behind the crime or policy violation, collect the evidence, and present your findings to build a case for prosecution or arbitration.
3. E-mail crimes and violations depend on the city, state, and sometimes country in which the e-mail originated.
4. For example, in Washington State, sending unsolicited e-mail is illegal. However, in other states, it isn't considered a crime. Consult with an attorney for your organization to determine what constitutes an e-mail crime

Investigating E-Mail Crime and Violations

- Committing crimes with e-mail is becoming commonplace, and more investigators are finding communications that link suspects to a crime or policy violation through e-mail.
- For example, some people use e-mail when committing crimes such as narcotics trafficking, extortion, sexual harassment, stalking, fraud, child abductions, terrorism, child pornography, and so on.
- Because email has become a major communication medium, any crime or policy violation can involve e-mail

Investigating E-Mail Crime and Violations

Using Specialized E-mail Forensics Tools

- For many e-mail investigations, you can rely on e-mail message files, e-mail headers, and e-mail server log files.
- However, if you can't find an e-mail administrator willing to help with the investigation, or you encounter a highly customized e-mail environment, you can use data recovery tools and forensics tools designed to recover e-mail files.
- As technology has progressed in e-mail and other services, so have the tools for recovering information lost or deleted from a hard drive.
- In previous chapters, we have reviewed many tools for data recovery, such as ProDiscover Basic and Access Data FTK.

Investigating E-Mail Crime and Violations

You can also use these tools to investigate and recover e-mail files. Other tools, such as the ones in the following list, are specifically created for e-mail recovery, including recovering deleted attachments from a hard drive:

- Data Numen for Outlook and Outlook Express
- FINAL e MAIL for Outlook Express and Eudora
- Sawmill-GroupWise for log analysis office_agent.html)
- DBX tract for Outlook Express
- Fookes Aid4Mail and Mail Bag Assistant for Outlook, Thunderbird, and Eudora
- Paraben E-Mail Examiner, configured to recover several e-mail formats
- Access Data FTK for Outlook and Outlook Express
- On track Easy Recovery Email Repair for Outlook and Outlook Express
- R-Tools R-Mail for Outlook and Outlook Express.
- Office Recovery's Mail Recovery for Outlook, Outlook Express, Exchange, Exchange Server, and IBM Lotus Notes

Internet Investigations Report Format

Case Number:_____ **Date:**_____

Investigator:_____ **ID #:**_____

Case Type: _____

Victim:_____ **Target:**_____

Evidence:_____

_____ _____

Evidence collection method:

The investigator used the following tools to document the collection of the evidence collected in the Internet during this investigation:

- SnagIt
- WebCase
- Internet Explorer

Internet Investigations Report Format

innovate achieve lead

Targeted Internet Protocols and Identifying Information:

1. **Websites:**

a. www…….com

2. IRC:

a. Username bob1234 on
b. IRC Server xxxxx
c. IRC channel “cardz”

Identified Target(s):

1. Bob Smith

Internet Investigations Report Format

innovate achieve lead

Details:

This investigation is about Internet content found at the following URL
http://www.....com hosted by a hosting service provider XXXXXX which appears to be hosted in the United States.

The domain is registered to:

The content on the URL appears to be….

Conclusion: Brief description of the violations and evidence supporting they occurred.

Thank you

BITS Pilani

Prof. Pradnya Kashikar

WILP-CSIS

BITS Pilani
Pilani Campus

innovate achieve lead

BITS Pilani

Pilani Campus

SS ZG588 - Cyber Crimes, Forensics and Incident Handling

Contact Session - 11

Course Objectives

No	Description
CO1	Enhancing awareness of recent Cyber Crime trends and learn Investigating Cyber Crimes
CO2	Introduce Cyberspace Infrastructure attacks and handling Organization Cybersecurity Issues
CO3	Understand Digital Forensics Process, Models, Analysis and Validation, Incident Detection and Response

Text Book(s)

innovate achieve lead

T1	Computer Forensics and Cyber Crime - An Introduction 3rd Edition by Marjie T. Britz, Ph.D., Professor of Criminal Justice, Clemson University
T2	Bill Nelson, A. Philips, F. Enfinger, C. K. Steuart, Computer Forensics and Investigations, Course Technology (Cengage Learning), Indian edition, 2009
T3	Incident Response & Computer Forensics, 3rd Edition by Jason T. Luttgens and Matthew Pepe and Kevin Mandia
R1	Guide to Computer Forensics and Investigations: Processing Digital Evidence 5th Edition by Bill Nelson, Amelia Phillips and Christopher Steuart
R2	The Basics of Digital Forensics, by John Sammons
R3	Computer Network Security and Cyber Ethics 4th Edition, by Joseph Migga Kizza
R4	Computer Forensics_ Investigating Network Intrusions and Cyber Crime: EC-Council Press

Learning Outcomes -

No	Learning Outcomes
LO1	Fundamental understanding and Information on Cyber Crimes, Digital Forensics Objectives and Incident Detection and Response Reports.
LO2	Learn on how to prepare investigation on computer-related incidents or crimes and summarize.
LO3	Understand on digital forensics process, models and analysis by taking a systematic approach
LO4	Explore on evaluating needs, validating and testing digital forensics tools, Generating Incident Report Findings, and Emerging Cybercrime Trends and Issues

Module 10 - Cyberspace Infrastructure and Enterprise Security

innovate achieve lead

10.1 Computer Communication Networks; Computer Network Infrastructure Weaknesses, Vulnerabilities and Attacks

10.2 Enterprise Security Attacks and Challenges

10.3 Information Security Protocols and Best Practices

11	Cyberspace Infrastructure and Enterprise Security	**Computer Communication Networks; Computer Network Infrastructure Weaknesses, Vulnerabilities and Attacks**	T3, R3
		Enterprise Security Attacks and Challenges	
		Information Security Protocols and Best Practices	

Computer Communication Networks

- A computer communication network system consists of hardware, software, and human ware.
- The hardware and software allow the human ware—the users—to create, exchange, and use information.
- The hardware consists of a collection of nodes that include the end systems, commonly called *hosts*, and intermediate switching elements that include hubs, bridges, routers and gateways.
- We will collectively call all of these *network* or *computing elements*, or sometimes without loss of generality, just *network elements*.
- The software, all application programs and network protocols, synchronize and coordinate the sharing and exchange of data among the network elements and the sharing of expensive resources in the network.
- Network elements, network software, and users, all work together so that individual users get to exchange messages and share resources on other systems that are not readily available locally.
- The network elements may be of diverse hardware technologies and the software may be different, but the whole combo must work together in unison.

Computer Communication Networks

- This concept that allows multiple, diverse underlying hardware technologies and different software regimes to interconnect heterogeneous networks and bring them to communicate is called *internetworking* technology.
- Internetworking technology makes possible the movement and exchange of data and the sharing of resources among the network elements.
- This is achieved through the low- level mechanisms provided by the network elements and the high- level communication facilities provided by the software running on the communicating elements.
- Let us see how this infrastructure works by looking at the hardware and software components and how they produce a working computer communication network.

Computer Communication Networks

Network Types

- The connected computer network elements may be each independently connected on the network or connected in small clusters, which are in turn connected together to form bigger networks via connecting devices.
- The size of the clusters determines the network type.
- There are, in general, two network types: a local area network (LAN) and a wide area network (WAN).
- A LAN consists of network elements in a small geographical area such as a building
- floor, a building, or a few adjacent buildings.
- The advantage of a LAN is that all network elements are close together so the communication links maintain a higher speed data movement.
- Also, because of the proximity of the communicating elements, high- cost and quality communicating elements can be used to deliver better service and higher reliability.

Computer Communication Networks

- WANs cover large geographical areas.
- Some advantages of a WAN include the ability to distribute services to a wider community and the availability of a wide array of both hardware and software resources that may not be available in a LAN.
- However, because of the large geographical areas covered by WANs, communication media are slow and often unreliable.

Network Topology

- WAN networks are typically found in two topologies: mesh and tree.
- WANs using a mesh topology provide multiple access links between network elements.
- The multiplicity of access links offers an advantage in network reliability because whenever a network element failure occurs, the network can always find a bypass to the failed element and the network continues to function.

Computer Communication Networks

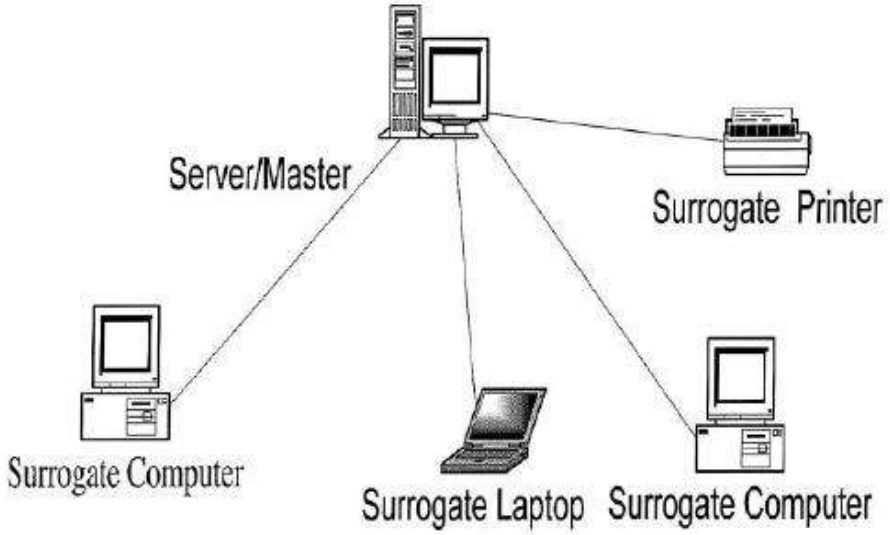


Figure 5.1 A LAN Network

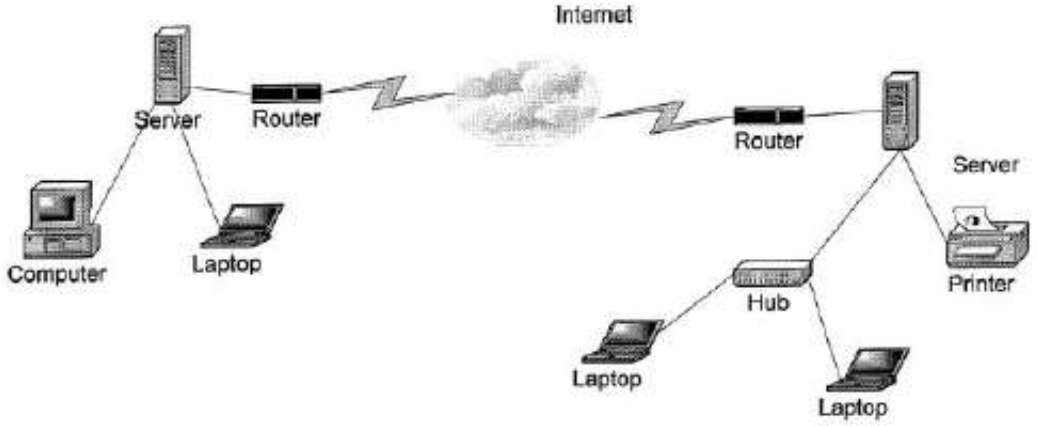


Figure 5.2 A WAN Network

Computer Communication Networks

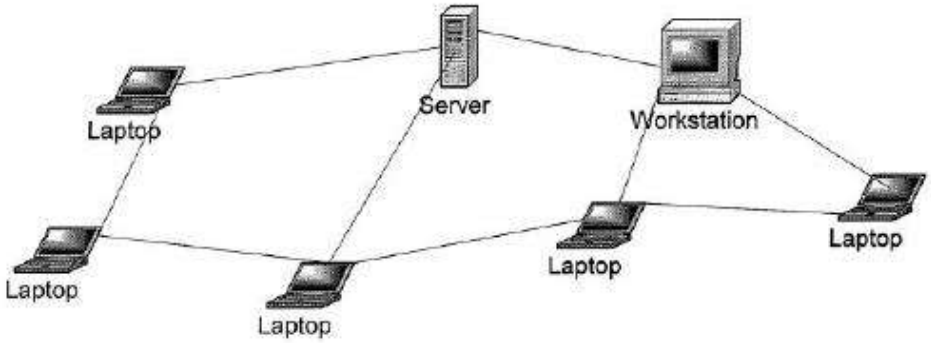


Figure 5.3 A Mesh Network

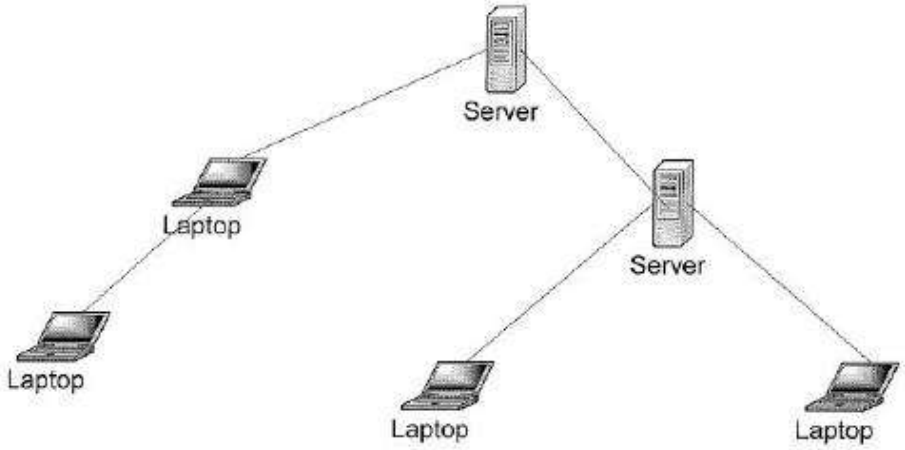


Figure 5.4 A Tree Topology

Computer Communication Networks

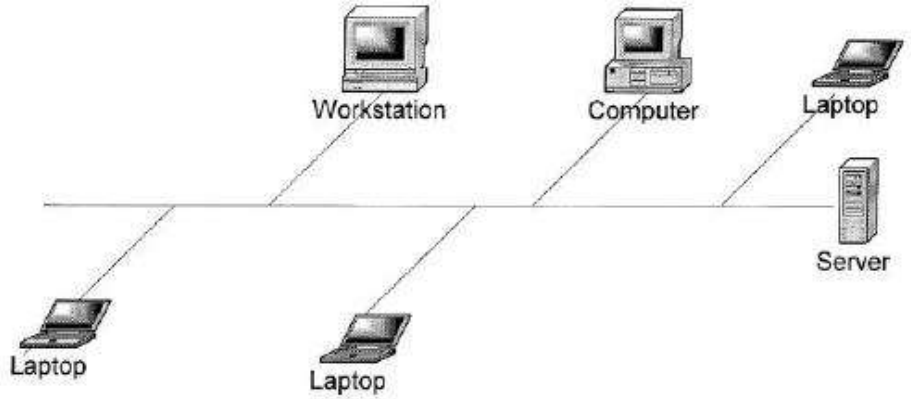


Figure 5.5 A Bus Topology

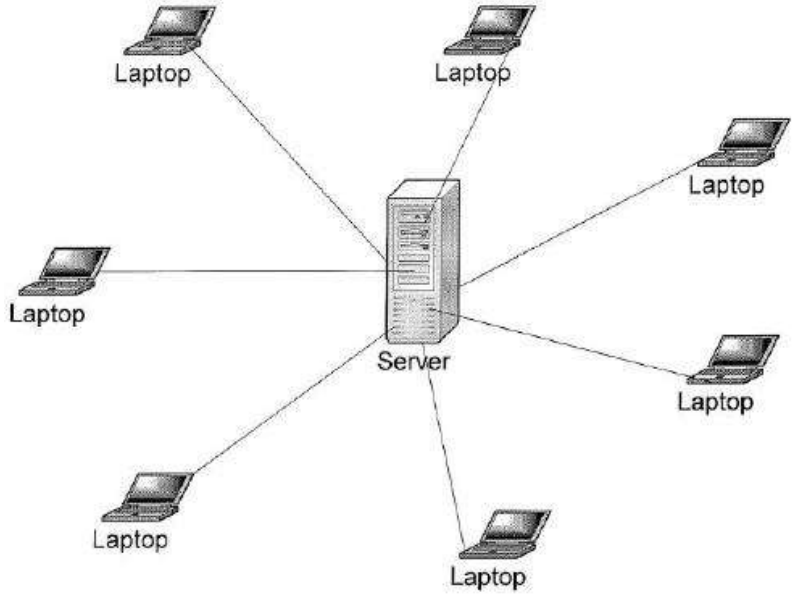


Figure 5.6 A Star Topology

Computer Communication Networks

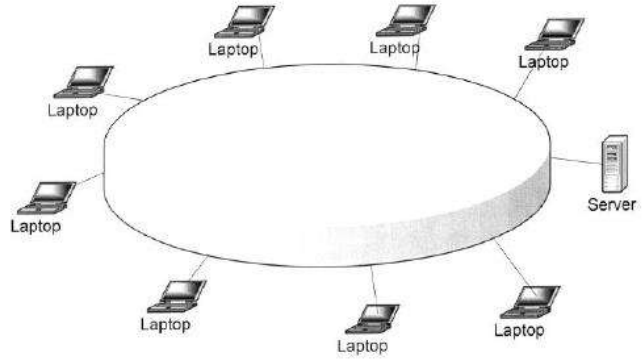


Figure 5.7 A Ring Topology

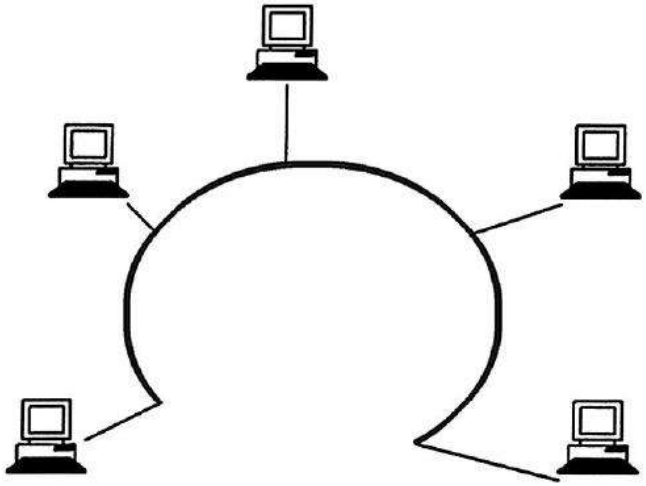


Figure 5.8 A Bus and Star Topology Hub

Computer Communication Networks

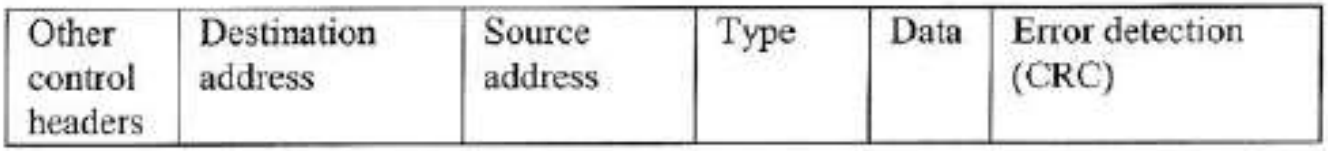


Figure 5.10 Ethernet Frame Data Structure

as CSMA/CD. CSMA/CD makes sure that an element never transmits a data frame when it senses that some other element on the network is transmitting.

Table 5.1 Popular Ethernet Technologies

Technology	Transmission medium	Topology	Speed
10Base2	Coaxial	Bus	10Mbps
10Base-T	Twisted	Star	10Mbps
100Base-T	Copper wire	Star	100Mbps
Gigabit	Optical fiber	Star	Gigabps

Computer Communication Networks

Transmission Media

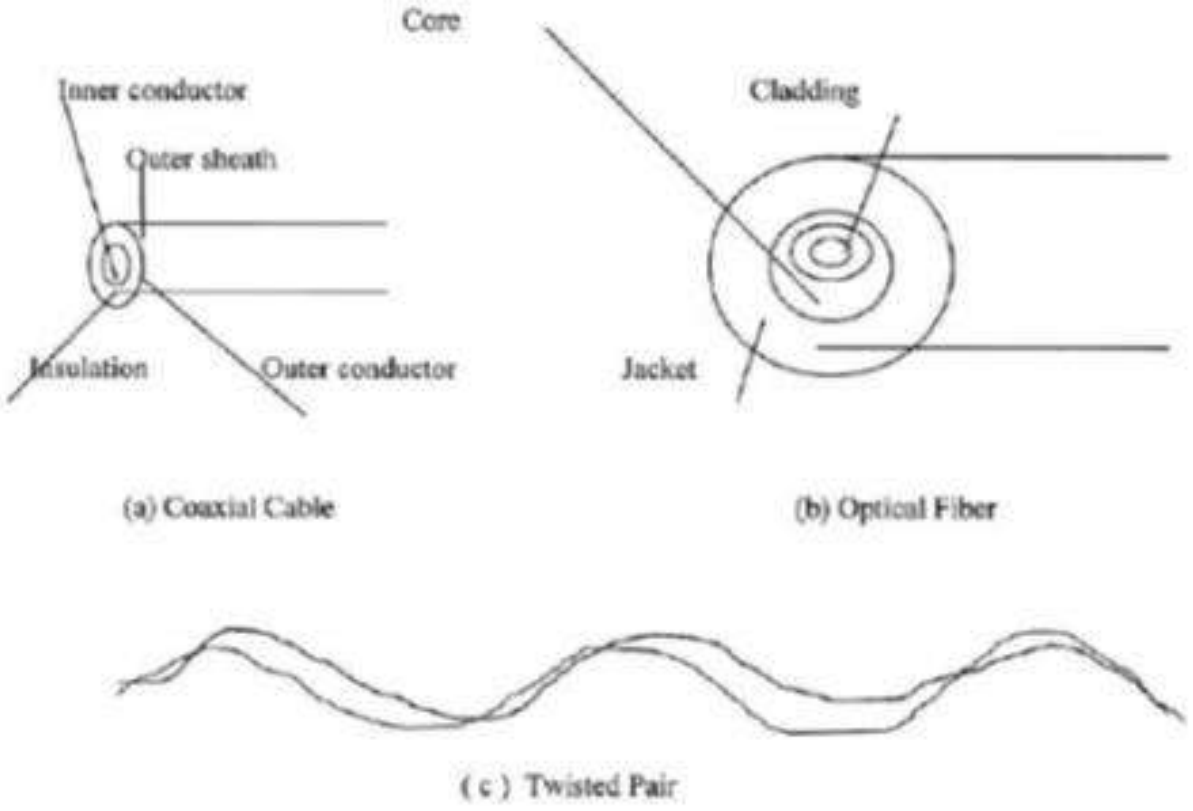
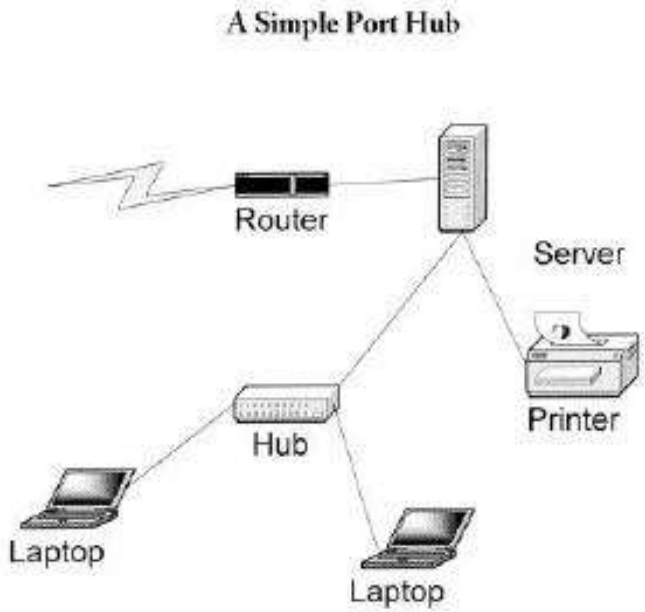


Figure 5.14 Types of Physical Media

Computer Communication Networks

Connecting Devices



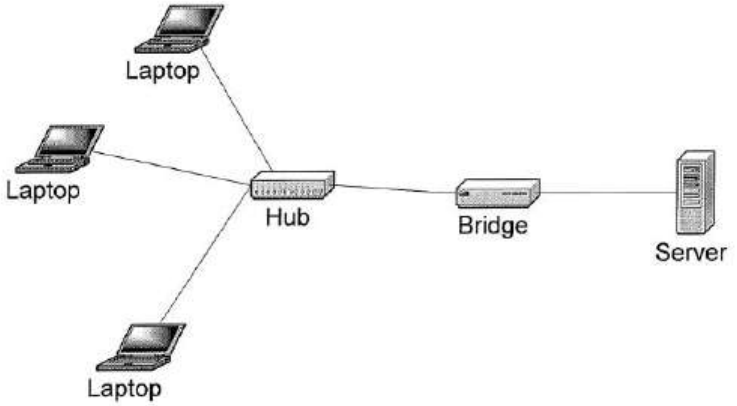


Figure 5.16 A Simple Bridge

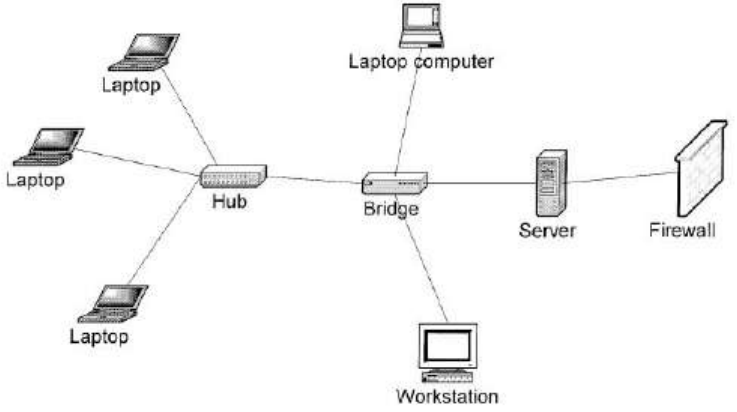


Figure 5.17 A Multiple Port Bridge

Computer Communication Networks

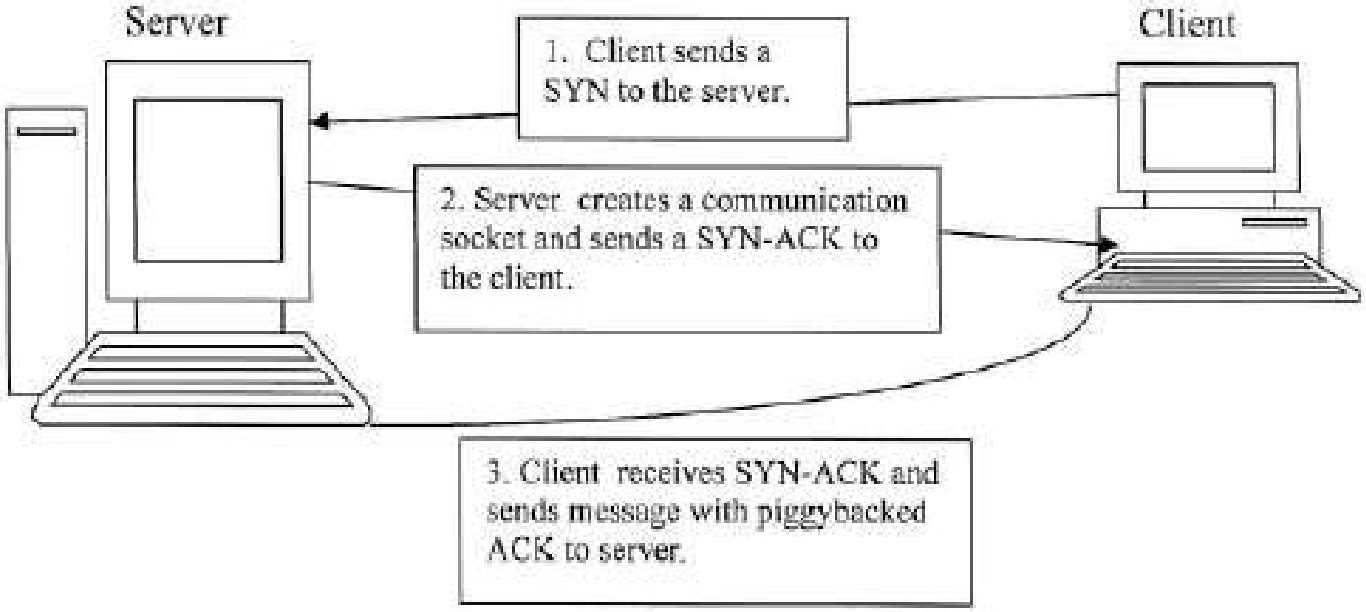


Figure 5.21 A Connection-Oriented Three-Way Handshake

Computer Communication Networks

Layer	Description
Application	The interface between the user and all network application software.
Presentation	Responsible for message syntax, conversions, compression, and encryption.
Session	Responsible for the organization and synchronization of source and destination during a communication session
Transport	Determines the class of service necessary for communication over the network. Among the classes are the connection-oriented and the connectionless.
Network	This is responsible for mainly routing messages in the network from source to destination.
Data link	Responsible for acknowledging and retransmitting frames as an error control. It also controls the amount and speed of transmission on the network.
Physical	Responsible for placing bits on the transmission medium and has protocols that make all connectors and adaptors work.

Figure 5.23 OSI Protocol Layers and Corresponding Services

Computer Communication Networks

Layer	Delivery Unit	Protocols
Application	Message	File Transfer Protocol (FTP), Name Server Protocol (NSP), Simple Mail Transfer Protocol (SMTP), Simple Network Management Protocol (SNMP), HTTP, Remote file access (telnet), Remote file server (NFS), Name Resolution (DNS)
Transport	Segment	Transmission Control Protocol (TCP), User Datagram Protocol (UDP)
Network	Datagram	Internet Protocol (IP), Internet Control Message Protocol (ICMP), Internet Group Management Protocol (IGMP)
Data Link	Frame	CSMA/CD for Ethernet and Token Ring
Physical	Bit Stream	All network card drivers

Figure 5.24 TCP/IP Protocol Stack

Computer Network Infrastructure Weaknesses, Vulnerabilities and Attacks

- The hardware infrastructure and corresponding underlying protocols suffer from weak points and sometimes gaping loopholes partly as a result of the infrastructure's open architecture protocol policy.
- When computers are communicating, they follow these etiquette patterns and protocols and we call this procedure a handshake. In fact, for computers it is called a three- way handshake.
- The three- way handshake establishes a trust relationship between the sending and receiving elements.
- However, network security exploits that go after infrastructure and protocol loopholes do so by attempting to undermine this trust relationship created by the three- way handshake.

Computer Network Infrastructure Weaknesses, Vulnerabilities and Attacks

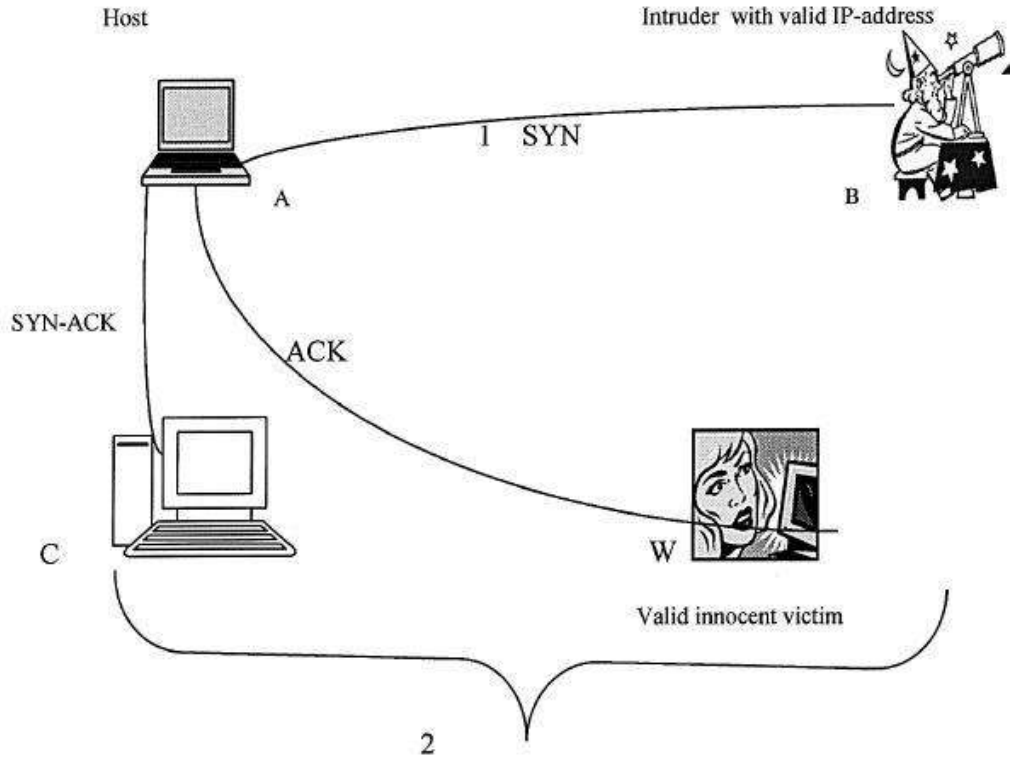
IP-Spoofing

- Internet Protocol spoofing (IP-spoofing) is a technique used to set up an attack on computer network communicating elements by altering the IP addresses of the source element in the data packets by replacing them with bogus addresses.
- IP- spoofing creates a situation that breaks down the normal trust relationship that should exist between two communicating elements.

SYN Flooding

- SYN flooding is an attack that utilizes the breakdown in the trust relationship between two or more communicating elements to overwhelm the resources of the targeted element by sending huge volumes of spoofed packets.
- SYN flooding works as follows. SYN flooding does not only affect one victim's server.
- It may also ripple through the network creating secondary and subsequent victims.

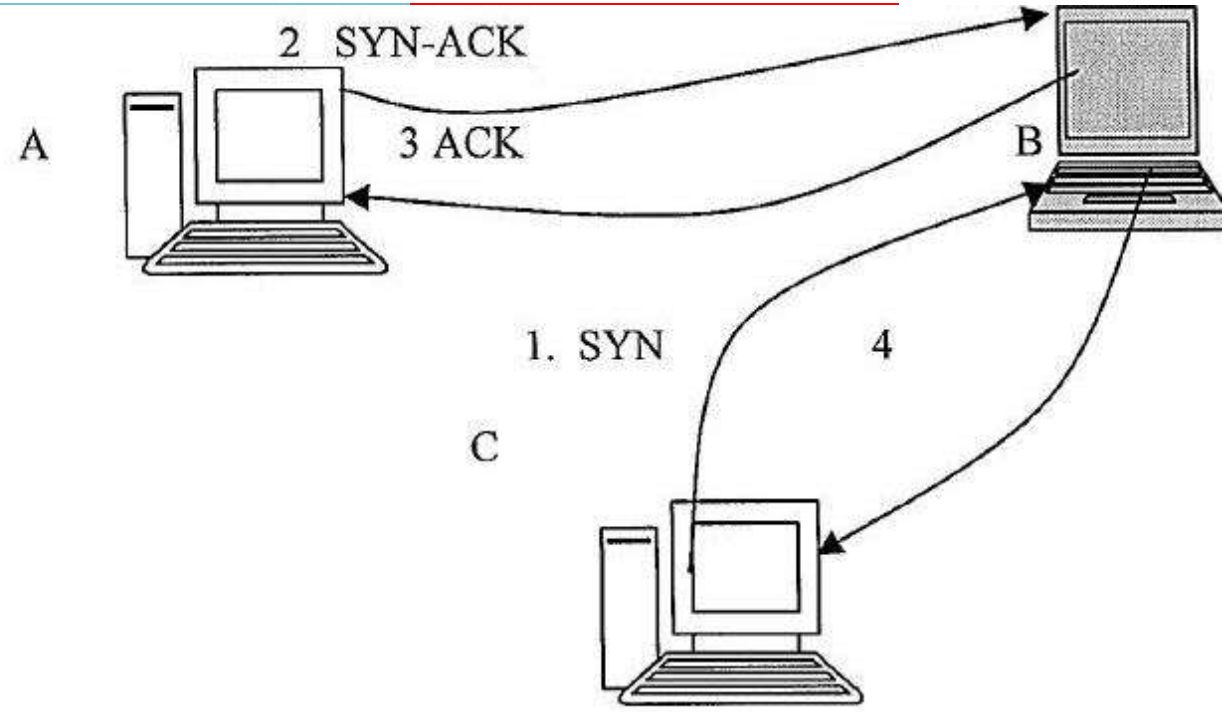
Computer Network Infrastructure Weaknesses, Vulnerabilities and Attacks



1. B sends A streams SYN with randomly changing source addresses from valid IP addresses.
2. A sends a stream of SYN-ACK to each valid addressed SYN - these are sent to hosts with no knowledge of what is going on and have no involvement in the attack. These victims have no addresses in the global Internet routing tables, therefore, they are not reachable.

Computer Network Infrastructure Weaknesses, Vulnerabilities and Attacks

Sequence Numbers Attack



1. C, the attacker, opens a connection with B by sending (SYN, ISNa) masquerading as A, where ISNa is the initial sequence number for A.
2. B responds by sending an SYN-ACK to A (ACK, ISNb, ISNa).
3. A acknowledges B by sending ACK(ISNa, ISNb). Although A does NOT know anything about the SYN to B, it responds anyway by using the guessed ISNb.
4. B now believes it has a legitimate session with A. However C, the intruder, is actually communicating with B.

Computer Network Infrastructure Weaknesses, Vulnerabilities and Attacks

Scanning and Probing Attacks

- In a scanning and probing attack, the intruder or intruders send large quantities of packets from a single location.
- The activity involves mostly a Trojan horse remote controlled program with a distributed scanning engine that is configured to scan carefully selected ports.
- Currently, the most popular ports are port 80, used by World Wide Web applications, port 8080, used by World Wide Web proxy services, and port 3128, used by most common squid proxy Services.

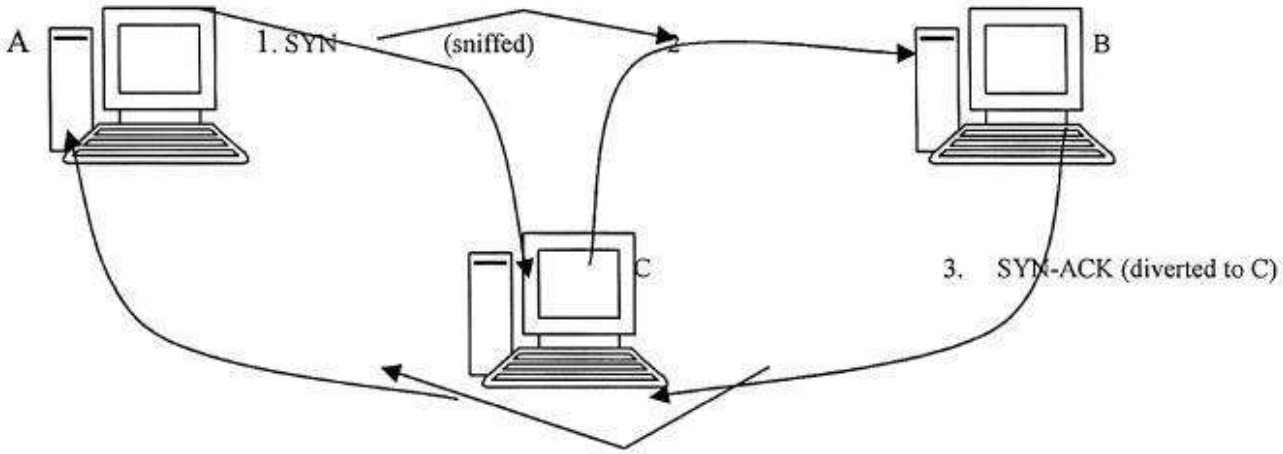
Low Bandwidth Attacks

- A low bandwidth attack starts when a hacker sends a low volume, intermittent series of scanning or probing packets from various locations.
- The attack may involve several hackers from different locations, all concurrently scanning and probing the network for vulnerabilities.
- Low bandwidth attacks can involve as few as five to ten packets per hour, from as many different sources.

Computer Network Infrastructure Weaknesses, Vulnerabilities and Attacks

Session Attacks

- Many other types of attacks target sessions already in progress and break into such sessions.
- Let us look at several of these, namely packet sniffing, buffer overflow, and session hijacking.



1. A sends a SYN packet to B for login containing source and destination address and password.
2. C, the intruder, sniffs the packet A is sending to B and gets A's and B's address and A's password to B.
3. B, with no knowledge of C in the midiaum, sends a SYN-ACK and permission to enter to A.
4. C is now in full access to both A and B after sniffing the SYN-ACK.

Computer Network Infrastructure Weaknesses, Vulnerabilities and Attacks

Distributed Denial of Service Attacks

- Distributed denial of service (DDoS) attacks are generally classified as nuisance attacks in the sense that they simply interrupt the services of the system.
- System interruption can be as serious as destroying a computer's hard disk or as simple as using up all the system's available memory.
- DDoS attacks come in many forms but the most common are the Ping of Death, smurfing, the teardrop, and the land.c.

Network Operating Systems and Software Vulnerabilities

- Network infrastructure exploits are not limited to protocols.
- There are weaknesses and loopholes in network software that include network operating systems, Web browsers, and network applications.
- Such loopholes are quite often targets of aggressive hacker attacks like planting Trojan viruses, deliberately inserting backdoors, stealing sensitive information, and wiping out files from systems.
- Such exploits have become common.

Enterprise Security Attacks and Challenges

The six components comprise the major divisions of cyberspace resources and together they form the cyberspace infrastructure and environment are as follows:

1. hardware, like computers, printers, scanners, servers and communication media
2. software, including application and special programs, system backups and diagnostic programs, and system programs like operating systems and protocols
3. data in storage, transition, or undergoing modification;
4. people, including users, system administrators, and hardware and software manufacturers
5. documentation, including user information for hardware and software, administrative procedures, and policy documents
6. supplies, including paper and printer cartridges.

Enterprise Security Attacks and Challenges

- Although all of these resources make up cyberspace, and any one of them is a potential target for a cyberspace attack, they do not have the same degree of vulnerability.
- Some are more vulnerable than others and, therefore, are targeted more frequently by attackers.
- Cyberspace has brought about an increasing reliance on these resources through computers running national infrastructures like telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services that include medical, police, fire, and rescue, and, of course, government services.
- These are central to national security, economic survival, and the social well- being of people.
- Such infrastructures are deemed critical because their incapacitation could lead to chaos in any country.

Enterprise Security Attacks and Challenges

- A cyberspace attack or *e-attack* is a cyberspace threat that physically affects the integrity of any one of these cyberspace resources.
- Most cyberspace attacks can be put in one of three categories: natural or inadvertent attacks, human errors, or intentional threats.
- Natural or inadvertent attacks include accidents originating from natural disasters like fire, floods, windstorms, lightning, and earthquakes.
- They usually occur very quickly and without warning, and they are beyond human capacity, often causing serious damage to affected cyberspace resources.
- Not much can be done to prevent natural disaster attacks on computer systems.
- However, precautions can be taken to lessen the impact of such disasters and to quicken the recovery from the damage they cause.

Enterprise Security Attacks and Challenges

- Human errors are caused by unintentional human actions.
- Unintended human actions are usually due to design problems. Such attacks are called *malfunctions*.
- Malfunctions, though occurring more frequently than natural disasters, are as unpredictable as natural disasters. They can affect any cyber resource, but they attack computer hardware and software resources more.
- In hardware, malfunctions can be a result of power failure or simply a power surge, electromagnetic influence, mechanical wear and tear, or human error.
- Software malfunctions result mainly from logical errors and occasionally from human errors during data entry.
- Malfunctions resulting from logical errors often cause a system to halt. However, there are times when such errors may not cause a halt to the running program, but may be passed on to later stages of the computation.
- If that happens and the errors are not caught in time, they can result in bad decision making. A bad decision may cost an organization millions of dollars.
- Most cyberspace attacks are intentional, originating from humans, caused by illegal or criminal acts from either insiders or outsiders.

Enterprise Security Attacks and Challenges

Types of Attacks

- Because of the many cyberspace resources, the varying degrees of vulnerabilities of these resources, the motives of the attackers, and the many topographies involved, e- attacks fall into a number of types.

- Let us put these types into two categories:

1. penetration attacks

2. denial of service attacks.

Enterprise Security Attacks and Challenges -

1. penetration attacks

- Penetration attacks involve breaking into systems using known security vulnerabilities to gain access to any cyberspace resource.
- With full penetration, an intruder has full access to all of a system's cyberspace resources or *e-resources*.
- Full penetration, therefore, allows an intruder to alter data files, change data, plant viruses, or install damaging Trojan horse programs into the system.
- It is also possible for intruders, especially if the victim computer is on a network, to use a penetration attack as a launching pad to attack other network resources.
- According to William Stallings, there are three **classes of intruders:**

  (i) **Masquerader**: This is a person who gains access to a computer system using other peoples' accounts without authorization.

  (ii) **Misfeasor**: This is a legitimate user who gains access to system resources for which there is no authorization.

  (iii) **Clandestine user**: This is a person with supervisory control who uses these privileges to evade or suppress auditing or access controls.
- Penetration attacks can be local, where the intruder gains access to a computer on a LAN on which the program is run, or global on a WAN like the Internet, where an e- attack can originate thousands of miles from the victim Computer.

Enterprise Security Attacks and Challenges -

1. penetration attacks

There are three types of penetration attacks: viruses, non- virus malicious attacks from insiders, and non- virus malicious attacks from outsiders.

a) Viruses

- Because viruses comprise a very big percentage of all cyberspace attacks, we will devote some time to them here.
- The term *virus* is derived from the Latin word *virus*, which means poison.
- A computer virus, defined as a self- propagating computer program designed to alter or destroy a computer system resource, follows almost the same pattern but instead of using a living body, it uses software to attach itself, grow, reproduce, and spread.
- As it spreads in the new environment, it attacks major system resources that include the surrogate software itself, data, and sometimes hardware, weakening the capacity of these resources to perform the needed functions and eventually bringing the system down.

Enterprise Security Attacks and Challenges -

1. penetration attacks

- Once a computer attack, most often a virus attack, is launched the attacking agent scans the victim system looking for a healthy body for a surrogate.
- If one is found, the attacking agent tests to see if it has already been infected.
- Viruses do not like to infect themselves, hence, wasting their energy.
- If an uninfected body is found, then the virus attaches itself to it to grow, multiply, and wait for a trigger event to start its mission.
- The mission itself has three components:

(i) to look further for more healthy environments for faster growth, thus spreading more;

(ii) to attach itself to any newly found body; and

(iii) once embedded, either to stay in the active mode ready to go at any trigger event or to lie dormant until a specific event occurs.

Enterprise Security Attacks and Challenges -

1. penetration attacks

We can follow Stephenson's10 virus classification and put all these viruses into the following categories:

- **Parasites**: These are viruses that attach themselves to executable files and replicate in order to attack other files whenever the victim's programs are executed.
- **Boot sector**: These were seen earlier. They are viruses that affect the boot sector of a disk.
- **Stealth**: These are viruses that are designed to hide themselves from any antivirus software.
- **Memory-resident**: As seen earlier, these are viruses that use system memory as a beachhead to attack other programs.
- **Polymorphic**: These are viruses that mutate at every infection, making their detection difficult.

Enterprise Security Attacks and Challenges -

1. penetration attacks

b) Theft of Proprietary Information

- Theft of proprietary information involves acquiring, copying or distributing information belonging to a third party.
- This may also involve certain types of knowledge obtained through legitimate employment.
- It also includes all information as defined in the intellectual property statutes such as copyrights, patents, trade secrets, and trademarks.
- These types of attacks originate mainly from insiders within the employee ranks, who may steal the information for a number of motives.

Enterprise Security Attacks and Challenges -

1. penetration attacks

c) Fraud

- The growth of online services and access to the Internet have provided fertile ground for cyberspace fraud or *cyberfraud*.
- New novel online consumer services that include cybershopping, online banking, and other online conveniences have enabled consumers to do business online.
- However, crooks and intruders have also recognized the potential of cyberspace with its associated new technologies.
- These technologies are creating new and better ways to commit crimes against unsuspecting consumers.
- Most online computer attacks motivated by fraud are in a form that gives the intruder consumer information like social security numbers, credit information, medical records, and a whole host of vital personal information usually stored on computer system databases.

Enterprise Security Attacks and Challenges -

1. penetration attacks

d) Sabotage

- Sabotage is a process of withdrawing efficiency. It interferes with the quantity or quality of one's skills, which may eventually lead to low quality and quantity of service.
- Sabotage as a system attack is an internal process that can be initiated by either an insider or an outsider. Sabotage motives vary depending on the attacker, but most are meant to strike a target, usually an employer, that benefits the attacker.
- The widespread use of the Internet has greatly increased the potential for and the number of incidents of these types of attacks.

e) Espionage

- By the end of the cold war, the United States, as a leading military, economic, and information superpower, found itself a constant target of military espionage. As the cold war faded, military espionage shifted and gave way to economic espionage.
- In its pure form, economic espionage targets economic trade secrets which, according to the 1996 U.S. Economic Espionage Act, are defined as all forms and types of financial, business, scientific, technical, economic, and engineering information and all types of intellectual property including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, and codes, whether they are tangible or not, stored or not, or compiled or not.

Enterprise Security Attacks and Challenges -

1. penetration attacks

f) Network and Vulnerability Scanning

- Scanners are programs that keep a constant electronic surveillance of a computer or a network, looking for computers and network devices with vulnerabilities.
- Computer vulnerabilities may be in the system hardware or software.
- Scanning the network computers for vulnerabilities allows the attacker to determine all possible weaknesses and loopholes in the system.
- This opens up possible attack avenues.

Enterprise Security Attacks and Challenges -

1. penetration attacks

g) Password Crackers

- Password crackers are actually worm algorithms. These algorithms have four parts: the first part, which is the most important, gathers password data used by the remaining three parts from hosts and user accounts.
- Using this information, it then tries to either generate individual passwords or crack passwords it comes across. During the cracking phase, the worm saves the name, the encrypted password, the directory, and the user information field for each account.
- The second and third parts trivially break passwords that can be easily broken using information already contained in the passwords.
- Around 30 percent of all passwords can be guessed using only literal variations or comparison with favourite passwords.
- This list of favourite passwords consists of roughly 432 words, most of them proper nouns and common English words.
- And the last part takes words in the user dictionaries and tries to decrypt them one by one.
- This may prove to be very time consuming and also a little harder. But with time, it may yield good guesses.

Enterprise Security Attacks and Challenges -

1. penetration attacks

h) Employee Network Abuse

- Although concerns of computer attacks on companies and corporations have traditionally been focused on outside penetration of systems, inside attacks have chronically been presenting serious problems in the workplace.
- An insider is someone who has been explicitly or implicitly granted access privileges that allow him or her the use of a particular system's facilities.
- Incidents of insider abuse are abound in the press highlighting the fundamental problems associated with insider system misuse.
- Insider net abuse attacks are fundamentally driven by financial fraud, vendettas, and other forms of intentional misuse.

i) Embezzlement

- Embezzlement is an inside job by employees. It happens when a trusted employee fraudulently appropriates company property for personal gain.
- Embezzlement is widespread and happens every day in both large and small businesses, although small businesses are less likely to take the precautions necessary to prevent it.
- Online embezzlement is challenging because it may never be found. And, if found, sometimes it takes a long time to correct it, causing more damage.

Enterprise Security Attacks and Challenges -

1. penetration attacks

j) Computer Hardware Parts Theft

- Although theft of computing devices seem to be going down, the vice is still high after all these years.
- There are several reasons for this, including the miniaturization of computing devices, which makes them easier to conceal and be taken away.
- Also, because storage technology has approved in tandem with miniaturization, the devices are storing more valuable data, hence attracting more attention of device thieves.
- Thirdly, while the storage capacity and the computation power have been increasing as the sizes become smaller, the prices of these devices have been dramatically dropping, making them more available in many places and increasing their probability of being stolen.
- There are additional reasons that the theft of computing devices has remained in the top tier of the computing security problem

Enterprise Security Attacks and Challenges -

2. Denial of Service Attacks

- Denial of service attacks, commonly known as distributed denial of service (DDoS) attacks, are not penetration attacks.
- They do not change, alter, destroy, or modify system resources.
- They do, however, affect a system by diminishing the system's ability to function; hence, they are capable of bringing a system down without destroying its resources.
- These types of attacks made headlines when a Canadian teen attacked Internet heavyweights Amazon, eBay, E*Trade, and CNN.
- Like penetration e- attacks, DDoS attacks can also be either local, shutting down LAN computers, or global, originating thousands of miles away on the Internet, as was the case in the Canadian generated DDoS attacks.
- The attacks in this category include among others IP- spoofing, SYN flooding, smurfing, buffer overflow, and sequence number sniffing.

Information Security Protocols and Best Practices

security policies are very important in the overall security plan of a system for several reasons including:

- **Firewall installations**: If a functioning firewall is to be configured, its rule base must be based on a sound security policy.

- **User discipline**: All users in the organization who connect to a network like the Internet through a firewall, must conform to the security policy.

Information Security Protocols and Best Practices

A good security policy must have the following components:

- A security policy access rights matrix.
- Logical access restriction to the system resources.
- Physical security of resources and site environment.
- Cryptographic restrictions.
- Policies and procedures.
- Common attacks and possible deterrents.
- A well- trained workforce.
- Equipment certification.
- Audit trails and legal evidence.
- Privacy concerns.
- Security awareness training.
- Incident handling.

Information Security Protocols and Best Practices

Most vulnerability assessment services will provide system administrators with:

- Network mapping and system fingerprinting of all known vulnerabilities.
- A complete vulnerability analysis and ranking of all exploitable weaknesses based on potential impact and likelihood of occurrence for all services on each host.
- A prioritized list of mis- configurations.

To the network security team, vulnerability scanning has a number of benefits including the following:

- It identifies weaknesses in the network, the types of weaknesses, and where they are. It is up to the security team to fix the identified loopholes.
- Once network security administrators have the electronic network security inventory, they can quickly and thoroughly test the operating system privileges and permissions, the chief source of network loopholes, test the compliance to company policies, the most likely of network security intrusions, and finally set up a continuous monitoring system.
- Once these measures are taken, it may lead to fewer security breaches, thus increasing customer confidence.
- When there are fewer and less serious security breaches, maintenance costs are lower and the worry of data loss is diminished.

Information Security Protocols and Best Practices

Firewalls commonly use the following forms of control techniques to police network traffic inflow and outflow:

- **Direction control**: This is to determine the source and direction of service requests as they pass through the firewall.
- **User control**: This controls local user access to a service within the firewall perimeter walls. By using authentication services like IPSec, this control can be extended to external traffic entering the firewall perimeter.
- **Service control**: This control helps the firewall decide whether the type of Internet service is inbound or outbound. Based on this, the firewall decides if the service is necessary. Such services may range from filtering traffic using IP addresses or TCP/UDP port numbers to provide an appropriate proxy software for the service.
- **Behaviour control**: This control determines how particular services at the firewall are used. The firewall chooses from an array of services available to it.

Information Security Protocols and Best Practices

There are two commonly used organization firewall policies:

(i) Deny everything: A deny- everything-not-specifically-allowed policy sets the firewall to deny all services and then add back those services allowed.

(ii) Allow everything: An allow- everything-not-specifically-denied policy sets the firewall to allow everything and then deny the services considered unacceptable.

In particular firewalls are needed to prevent intruders from:

- Entering and interfacing with the operations of an organization's network system,
- Deleting or modifying information that is either stored or in motion within the organization's network system, and
- Acquiring proprietary information.

Thank you !

BITS Pilani

Prof. Pradnya Kashikar

WILP-CSIS

BITS Pilani
Pilani Campus

innovate achieve lead

BITS Pilani

Pilani Campus

SS ZG588 - Cyber Crimes, Forensics and Incident Handling

Contact Session - 12

Course Objectives

No	Description
CO1	Enhancing awareness of recent Cyber Crime trends and learn Investigating Cyber Crimes
CO2	Introduce Cyberspace Infrastructure attacks and handling Organization Cybersecurity Issues
CO3	Understand Digital Forensics Process, Models, Analysis and Validation, Incident Detection and Response

Text Book(s)

innovate achieve lead

T1	Computer Forensics and Cyber Crime - An Introduction 3rd Edition by Marjie T. Britz, Ph.D., Professor of Criminal Justice, Clemson University
T2	Bill Nelson, A. Philips, F. Enfinger, C. K. Steuart, Computer Forensics and Investigations, Course Technology (Cengage Learning), Indian edition, 2009
T3	Incident Response & Computer Forensics, 3rd Edition by Jason T. Luttgens and Matthew Pepe and Kevin Mandia
R1	Guide to Computer Forensics and Investigations: Processing Digital Evidence 5th Edition by Bill Nelson, Amelia Phillips and Christopher Steuart
R2	The Basics of Digital Forensics, by John Sammons
R3	Computer Network Security and Cyber Ethics 4th Edition, by Joseph Migga Kizza
R4	Computer Forensics_ Investigating Network Intrusions and Cyber Crime: EC-Council Press

Learning Outcomes -

No	Learning Outcomes
LO1	Fundamental understanding and Information on Cyber Crimes, Digital Forensics Objectives and Incident Detection and Response Reports.
LO2	Learn on how to prepare investigation on computer-related incidents or crimes and summarize.
LO3	Understand on digital forensics process, models and analysis by taking a systematic approach
LO4	Explore on evaluating needs, validating and testing digital forensics tools, Generating Incident Report Findings, and Emerging Cybercrime Trends and Issues

Module 11 - Incident Detection and Characterization

innovate achieve lead

Pre-Incident Preparation

Getting the Investigation Started

Initial Development of Leads

Discovering the Scope of the Incident

12	Incident Detection and Characterization	**Pre-Incident Preparation**	T3
		Getting the Investigation Started	
		Initial Development of Leads	
		Discovering the Scope of the Incident	

CNIT 121: Computer Forensics -- Sam Bowne (samsclass.info)

Incident Detection and Characterization

- When an event is detected, we've seen that many organizations tend to transition directly to an investigation.
- In some cases, the details of the event may justify a quick jump to investigate.
- In most cases, however, we believe that an extra step is needed to get the investigation started on the right foot.
- Many investigations that start prior to confirmation of basic facts.
- They often suffer from a lack of focus and end up wasting time and resources.
- Sometimes people are excited about new information and are caught up in the heat of the moment.
- As with any real-life scenario, as you receive new information, you should always evaluate it with logic, common sense, and your own experience.
- Take, for example, what happened during Hurricane Sandy in October 2012? A number of individuals posted false reports on the Internet regarding "breaking news," such as flooding on the New York Stock Exchange trading floor. Although the flooding was certainly possible, there was little pause to consider whether the source was reliable— or anything else about the report. The media and public were caught up in the moment, and, for a short period, believed that information was true and accurate.

Incident Detection and Characterization

- We see parallels to this in the incident response world—investigators sometimes react to new information without a proper evaluation first.
- For example, when your detection system reports an event, do you immediately take action, or do you try to verify the information? Detection systems can misrepresent or omit events or event details.
- No system is completely accurate.
- You must act as the gatekeeper, standing between events and investigations.
- To do that, you should build an overall picture of the incident and then collect and verify the initial facts.
- This will allow you to develop context.
- Next, you should determine what is appropriate—and possible—for the investigation to accomplish.
- Finally, this process needs to move quickly, because your organization's security, electronic data, and reputation are at stake.

Pre-Incident Preparation

- Pre-incident preparation is designed to help create an infrastructure that allows an organization to methodically investigate and remediate.
- This will help ensure your team is properly prepared to investigate, collect, analyse, and report information that will allow you to address the common questions posed during an incident:
  - What exactly happened? What is the damage and how did the attackers get in?
  - Is the incident ongoing?
  - What information was stolen or accessed?
  - What resources were affected by the incident?
  - What are the notification and disclosure responsibilities?
  - What steps should be performed to remediate the situation?
  - What actions can be taken to secure the enterprise from similar incidents?

Pre-Incident Preparation

The investigation itself is challenging. Extracting the necessary data from your information systems and managing communications will be equally challenging unless you prepare. This chapter will help you make preparations that significantly contribute to a successful investigation. We cover three high-level areas:

A) Preparing the organization This area includes topics such as identifying risk, policies for a successful IR, working with outsourced IT, global infrastructure concerns, and user education.

B) **Preparing the IR team** This area includes communication procedures and resources such as hardware, software, training, and documentation.

C) **Preparing the infrastructure** This area includes asset management, instrumentation, documentation, investigative tools, segmentation, and network services.

Pre-Incident Preparation

innovate achieve lead

A) PREPARING THE ORGANIZATION FOR INCIDENT RESPONSE

Computer security is a technical subject, and because there is a perceived ease to it, many organizations tend to focus on the technical issues: buy an appliance, install agents, and analyse “big data” in the cloud. Money is easier to come by than skilled personnel or committing to self-improvement. However, during most investigations, we are regularly faced with significant organizational challenges of a nontechnical nature.

In this section we cover some of the most common challenge areas:

- Identifying risk
- Policies that promote a successful IR
- Working with outsourced IT
- Thoughts on global infrastructure issues
- Educating users on host-based security

Pre-Incident Preparation

innovate achieve lead

Identifying Risk

The initial steps of pre-incident preparation involve getting the big picture of your corporate risk. What are your critical assets? What is their exposure? What is the threat? What regulatory requirements must your organization comply with? (These generally have some associated risk.) By identifying risk, you can ensure that you spend resources preparing for the incidents most likely to affect your business. Critical assets are the areas within your organization that are critical to the continued success of the organization. The following are some examples of critical assets:

- **Corporate reputation** Do consumers choose your products and services in part due to their confidence in your organization's ability to keep their data safe?
- **Confidential business information** Do you have critical marketing plans or a secret product formula? Where do you store patents, source code, or other intellectual property?
- **Personally identifiable information** Does your organization store or process PII data?
- **Payment account data** Does your organization store or process PCI data?

Pre-Incident Preparation

- Critical assets are the ones that produce the greatest liability, or potential loss, to your organization.
- Liability occurs through exposures.
- Consider what exposures in your people, processes, or technology result in or contribute to loss.
- Examples of exposures include unpatched web servers, Internet-facing systems, disgruntled employees, and untrained employees.
- Another contributing factor is who can actually exploit these exposures: Anyone connected to the Internet? Anyone with physical access to a corporate building? Only individuals physically within a secure area? Combine these factors to prioritize your risk.
- For example, the most critical assets that have exposures accessible only to trusted individuals within a controlled physical environment may present less risk than assets with exposures accessible to the Internet.
- Risk identification is critical because it allows you to spend resources in the most efficient manner.
- Not every resource within your environment should be secured at the same level. Assets that introduce the most risk receive the most resources.

Pre-Incident Preparation

Policies That Promote a Successful IR

Every investigative step your team makes during an IR is impacted by policies that should be in place long before that first notification occurs. In most situations, information security policies are written and executed by the organization's legal counsel in cooperation with the CISO's office and compliance officers.

Typical policies include:

- **Acceptable Use Policy** Governs what the expected behaviour is for every user.
- **Security Policy** Establishes expectations for the protection of sensitive data and resources within the organization. Subsections of this policy may address physical, electronic, and data security matters.
- **Remote Access Policy** Establishes who can connect to the organization's resources and what controls are placed on the connections.
- **Internet Usage Policy** Establishes appropriate use of general Internet resources, including expectation of privacy and notification of monitoring by or on behalf of the organization.

Pre-Incident Preparation

- The policies that IR teams should be most concerned about would address expectations on the search and seizure of company-owned resources and interception of network traffic.
- If these two (admittedly general) issues are covered, the team should be able to perform most investigative actions.
- Be aware of local privacy laws that will affect your actions.
- An action performed in one office may run afoul of federal laws in another.
- Ecommerce Fraud + 11 Fraud Prevention Strategies (bigcommerce.com)

Pre-Incident Preparation

innovate achieve lead

Working with Outsourced IT

- In many larger organizations, and even some mid or small size, we have found there is a good chance that at least some IT functions are outsourced.
- If the investigation requires a task to be performed by the outsourced provider, there may be challenges in getting the work done.
- Usually processes are in place for requesting the work, which may require project plans, approvals, or other red tape. There may also be an additional cost, sometimes charged per system, for minor configuration changes such as host-based firewall rules.
- In some cases, there may be no vehicle to accomplish a requested task because it falls outside the scope of the contract.
- We have experienced this situation when an organization requested log files from an outsourced service for analysis.
- These challenges may prevent the investigation from moving forward effectively.
- What every organization should do is work with their providers to ensure arrangements are in place that include service level agreements (SLAs) for responsiveness to critical requests and options to perform work that is out of scope of the contract.
- Without the proper agreements in place, you may find yourself helpless in an emergency.

Pre-Incident Preparation

innovate achieve lead

Thoughts on Global Infrastructure Issues

In recent years, we've performed a number of intrusion investigations with large multinational organizations. During those investigations, we were met with new and interesting challenges that gave us some insight into how hard it is to properly investigate an incident that crosses international borders. Although we don't have all the answers, we can make you aware of some of the challenges you may face so you have time to prepare.

1. Privacy and Labour Regulations

As investigators, we should normally view an organization's network as a large source of evidence just waiting for us to reach out and find it. One may not immediately consider that the network spans five countries on three continents, each with its own local privacy laws and regulations. It's easy to get yourself into trouble if you decide to search for indicators of compromise and the method you use violates local privacy laws or federal labour regulations. If you plan to investigate an incident that involves a network spanning more than one country, you will need to do some homework before you begin. You should contact the organization's legal counsel within each country to discuss the situation and determine what actions you can, and cannot, take.

Pre-Incident Preparation

innovate achieve lead

2. Team Coordination

Another significant challenge with incidents that span the globe is coordination. Because both personnel and technology resources will be spread out over many time zones, staying organized will require careful planning and constant effort to ensure everyone is in sync. Because some staff may be sleeping while you are awake, getting things done may take more time. Tracking tasks and performing handoffs will be critical to ensure that acceptable progress is made. Scheduling a meeting could take days because participants are in different time zones.

3. Data Accessibility

During an investigation, massive amounts of data are collected for analysis. Oftentimes, it is in the form of singularly large data sets, such as hard disk images. When the core team is responsible for performing the majority of the analysis tasks, you must find a way to efficiently transfer this data to the team members with forensic analysis experience. Although you should keep in mind any customs documentation or restrictions in the source and destination countries, the greatest challenge will be the delay in getting relevant data into the right hands. If there is any question whether data needs to be transferred, begin the process immediately. Multiple days have been lost from miscommunication or indecision.

Pre-Incident Preparation

Educating Users on Host-Based Security

- Users play a critical role in your overall security.
- The actions users take often circumvent your best-laid security plans. Therefore, user education should be a part of pre-incident preparation.
- Users should know what types of actions they should and should not take on their systems, from both a computer-security and an incident-response perspective.
- Users should be aware of the common ways attackers target and take advantage of them to compromise the network.
- Users should be educated about the proper response to suspected incidents. Typically, you will want users to immediately notify a designated contact. In general, users should be instructed to take no investigative actions, because these actions can often destroy evidence and impede later response.
- A specific issue you should address is the danger inherent in server software installed by users. Users might install their own web or FTP servers without authorization, thereby jeopardizing the overall security of your organization.
- Removing administrative privileges, which is a configuration change that helps to mitigate this risk. However, users can sometimes find ways around security measures and should be made aware of the danger associated with installing unauthorized software.

Pre-Incident Preparation

innovate achieve lead

B) PREPARING THE IR TEAM

- As we introduced in the previous chapter, the core IR team is composed of several disciplines: IT, investigators, forensic examiners, and even external consultants.
- Each is likely to come to the team with different skills and expectations.
- You will want to ensure that your team is composed of hard workers who show attention to detail, remain in control, do not rush the important things, and document what they are doing.

Pre-Incident Preparation

innovate achieve lead

Defining the Mission

Defining the mission of your IR team will help keep the team focused and set expectations with the rest of your organization. All elements of the team's mission must be fully endorsed and supported by top management; otherwise, the IR team will not be able to make an impact within the organization.

The team's mission may include all or some of the following:

- • Respond to all security incidents or suspected incidents using an organized, formal investigative process.
- • Conduct a complete impartial investigation.
- • Quickly confirm or dispel whether an intrusion or security incident actually occurred.
- • Assess the damage and scope of an incident.
- • Control and contain the incident.
- • Collect and document all evidence related to an incident.
- • Select additional support when needed.
- • Protect privacy rights established by law and/or corporate policy.
- • Provide a liaison to proper law enforcement and legal authorities.
- • Maintain appropriate confidentiality of the incident to protect the organization from unnecessary exposure.
- • Provide expert testimony.
- • Provide management with recommendations that are fully supported by facts.

Pre-Incident Preparation

innovate achieve lead

Communication Procedures

- During an incident, you will have several teams working concurrently: your core investigative team, ancillary teams, legal teams, and system administrators who not only respond to the core team's tasks, but who often perform pertinent actions on their own.

- Good communication is paramount, and defining how that works before an incident begins is essential. This section discusses tactical and ad-hoc communications.

Pre-Incident Preparation

innovate achieve lead

Internal Communications

- In a large number of recent investigations, the attackers made a beeline to the e-mail servers. On a number of servers, it is discovered evidence that the attackers retrieved the e-mail boxes of C-level employees and senior IT administrators.
- Shortly thereafter, the attackers returned and searched the entire mail server for strings related to the investigation.
- Sadly, the threat of the attackers watching you watching them is not theoretical. Keep the following Communications Security (ComSec) issues in mind when preparing for an IR:
  - • *Encrypt e-mail*. Before an incident occurs, procure S/MIME certificates for members of the core and ancillary IR teams. Check with your organization's IT department, as they may issue certificates to employees at no direct cost to you. Alternatives such as PGP may be used; however, integration with common mail clients is traditionally poor.
  - • *Properly label all documents and communications*. Phrases such as "Privileged & Confidential," "Attorney Work Product," and "Prepared at Direction of Counsel" may be prudent, or even required. You should seek legal counsel to establish what labels, if any, are appropriate.
  - • *Monitor conference call participation*. Ensure that your conference call system allows you to monitor who has called in or who is watching a screencast. Keep an eye on the participant list and disconnect unverified parties.
  - • *Use case numbers or project names to refer to an investigation*. Using project names helps to keep details out of hallway conversations, meeting invitations, and invoices for external parties. This is less applicable to possible interception by the attackers as it is to minimizing the number of personnel who have details on the IR. Outwardly, treat it as you would any other project. The fewer people who know about a possible lapse in security, the better.

Pre-Incident Preparation

innovate achieve lead

Communicating with External Parties

- If an organization is lucky, the impact of an intrusion will not require notification or consultation with external entities.
- With the growing amount of governance and legislation, not to mention incident disclosure language in contracts, it is highly likely that your organization will need to determine how it communicates with third parties.
- Planning for potential disclosure is a process that should involve legal counsel, compliance officers, as well as C-level personnel.
- A few questions to consider when determining the content and timing of any notification are
  - • When does an incident meet a reporting threshold? Immediately at detection? Perhaps after the incident has been confirmed?
  - • How is a notification passed to the third party? What contract language is in place to protect confidentiality?
  - • If the incident warrants a public disclosure, who is responsible for the contents and timing of the communication? How is the disclosure to occur?
  - • What penalties or fines are levied against your organization post-disclosure? Consider whether the timing of the notification impacts this factor
  - • What investigative constraints are expected after the disclosure? Is a third party required to participate in the investigation?
  - • How does disclosure affect remediation?

Pre-Incident Preparation

Deliverables: A sample list of deliverables for an IR team follows:

Name	Purpose	Delivery Target
Case Status Report	Update stakeholders on progress of an individual case.	Recurring: Daily or as required
Live Response Report	Document findings from initial live response triage of a single system.	Draft: Within one business day Final: Within two business days
Forensic Examination Report	Document the detailed findings from forensic analysis performed on an item of evidence.	Draft: Within four business days Final: Within six business days
Malware Analysis Report	Document the findings from analysis of suspected malicious software.	Draft: Within three business days Final: Within five business days
Intrusion Investigation Report	Consolidate all reports and findings related to a single incident and create a high-level executive summary.	Draft: Within five business days of completion of the investigation Final: Within eight business days of completion of the investigation

Pre-Incident Preparation

innovate achieve lead

Evidence Handling

- Evidence is the source of findings for any investigation, and must be handled appropriately.
- Attention to detail and strict compliance are mandatory with respect to evidence handling.
- If the integrity of the evidence is called into question, the findings of an investigation may no longer provide value to your organization.
- To prevent that from happening, we recommend that you implement appropriate evidence handling policy and procedures.
- Typically, they will include guidance on evidence collection, documentation, storage, and shipment.

Pre-Incident Preparation

innovate achieve lead

Internal Knowledge Repository

- As your IR team performs investigations and interacts with other departments in your organization, they will accumulate knowledge that should to be documented in a central location.
- Some information may only be related to a single incident, and can be stored in the ticketing or case management system that the IR team uses.
- Other information may be related to the organization as a whole, and should be documented in a knowledge repository that the IR team maintains.
- The knowledge repository should be logically organized and searchable so that the team can effectively locate relevant information.

Pre-Incident Preparation

innovate achieve lead

C) PREPARING THE INFRASTRUCTURE FOR INCIDENT RESPONSE

- Over the years, we have responded to hundreds of incidents, from computer intrusions to fraud investigations.
- Although the elements of proof for the investigations differ, the source of actionable leads and relevant data remain fairly consistent, as well as the methods used to extract and analyse that data.
- Regardless of the investigation, the IR team should have the ability to acquire data and search for relevant material across the enterprise as easily as it does on a single machine.
- It is not surprising then that, good information security practices and change management procedures promote rapid response and ease the remediation process organizations frequently have challenges with. [continued….]

Pre-Incident Preparation

- They broadly fall into two categories: computing devices (such as servers, desktops, and laptops) and networking.
- Within each of these two categories, we will cover the top four areas that we have seen many organizations struggle with.
- Here is an outline of these areas:

  - Computing device configuration
  - Asset management
  - Performing a survey
  - Instrumentation
  - Additional steps to improve security
  - Network configuration
  - Network segmentation and access control
  - Documentation
  - Instrumentation
  - Network services

Getting the Investigation Started

- The initial facts about an event are all an investigation has to get started—so it's a good idea to get them right.
- It's also important to gather additional information about those facts so you can establish context.
- For example, an IP address is more useful if you know what system it belongs to and what role that system performs.
- Also, a time that an event occurred is less useful if you don't know the corresponding time zone.
- Without that context, it's easy to jump to the wrong conclusions about what an event means.
- Over time, validating facts and establishing context becomes second nature.

Getting the Investigation Started

Incident Summary Checklist

The first checklist you should complete is used to gather the basic vitals of an incident; it is called the Incident Summary Checklist. The purpose of this checklist is to record high-level information about the incident. The information collected should provide you with a general sense of what has happened, and should help identify areas where your response protocol might need attention.

- Date and time the incident was reported. Record the date and time that an individual or automated system initially brought the issue to the IR team's attention.

- The date and time the incident was detected. Normally, the time an incident is reported is more recent than the actual detection time. Be sure to track down and record when the issue was actually detected.

Getting the Investigation Started

- Contact information of the person documenting this information.
- Contact information of the person who reported the incident.
- Contact information of the person who detected the incident. If the organization was notified by an external party, ensure that all details are recorded and the original, written communication is preserved.
- The nature of the incident. Provide a categorization of what was detected—mass malware, spear phishing attempt, failed logins, unauthorized access, and so on.
- The type of affected resources. At times, the detection or notification gives details on the data or resources that may have been affected. Retain all data provided, whether it is PCI related or CAD drawings of your latest missile-rate gyroscope. Beyond lending credence to the notification, it helps define scope.
- How the incident was detected. Provide a brief summary of what the detection method was, such as an antivirus alert, an IDS alert, or that a user reported suspicious behaviour.
- The unique identifier and location of the computers affected by the incident. Be sure to obtain a truly unique identifier—the IP address may not be unique, due to DHCP leases. It's typically more useful to get the host name or an asset tag number.

Getting the Investigation Started

- Who accessed the systems since detection? It's important to record who accessed the system since detection, in case the investigators need details about what they did. Sometimes IT staff or others may take actions that they perceive as "helpful" but are difficult to differentiate from malicious activity.
- Who is aware of the incident?
- Whether the incident is currently ongoing.
- Whether there is a requirement to keep knowledge of the incident on a "need-to-know" basis.

- Once you've completed the Incident Summary Checklist, you can move on to getting more details about specific areas. The order of completion for the following checklists should be based on the needs of the situation. You can also enlist help and complete more than one at a time. We'll present them in the order we generally use.

Getting the Investigation Started

Incident Detection Checklist

The next checklist is used to gather additional details about how the incident was detected and the detection systems themselves. We've solved many "incidents" just by thoroughly collecting and examining details about the detection. Looking at the details allowed us to see that something was misinterpreted, and that there really was no incident. Taking extra time to validate the detection, in our experience, is time well spent.

- Was the detection through an automated or manual process? Did a person or an automated system detect the incident? Note that this detection could have been from an external source, so getting an idea of whether an automated system tipped them off or if it was a result of manual analysis is important to factor into its validity.
- What information was part of the initial detection? Record the details regarding the information present in the initial detection. If the initial detection was an alert, do you have a copy of it? If the detection was from a person, have you spoken with them to document what they saw? Use healthy scepticism and be sure to get your eyes on raw data to confirm what you are being told or shown. Ensure all data you collect is preserved properly.

Getting the Investigation Started

- What sources provided the data that contributed to the detection? If the source was a person or persons, record their contact information. If the source was one or more automated systems, provide the detail about each one that contributed to the detection. Note the time zone stored by the automated system.

- Has someone acquired and validated that the source data is accurate? If so, who? If a person was involved in the detection, has someone validated the methods and the data they examined? If it was an automated system, has someone verified both the raw data and the criteria that the detection was based on?

- Is the source data involved being preserved? Depending on the system or method used, the data related to the detection may not be automatically preserved. Or, it may be purged from the systems within a certain number of hours or days. Take care to ensure the information relevant to the detection is not lost.

Getting the Investigation Started

- How long have the detection sources been in operation and who runs them? Sometimes we find that a detection system was recently brought online, and is generating false positives, or perhaps the output is being misinterpreted due to lack of experience. Record how long each system has been in place and who is responsible for maintaining and reviewing it.

- What are the detection and error rates? Talk to the folks who run the system and review the alerts. Find out how often this type of detection occurs. Gain an understanding of the error rate.

- Has anything related to the data sources changed? In some cases, we find that an administrator recently performed tweaks or upgrades to a system. You should talk to the persons responsible for the data source systems and find out if any maintenance has been performed recently. There may have been some undesired side effects.

Getting the Investigation Started

Collect Additional Details

- If your detection details seem accurate and consistent, the next step is to move on to collect additional information about specific elements related to the detection.
- You should go one level down and collect details about the individual systems, the networks, and potentially malicious files.
- Also, feel free to dig into any other data points collected in the Incident Summary Checklist. [give o the next slide..]

Getting the Investigation Started

Individual System Details For each system involved, consider collecting the following information. You should avoid grouping systems together into a single document, because it's easy to overlook details if you don't take the time to ask these questions about each individual system.

- Physical location
- The asset tag number
- The system's make and model
- The operating system installed
- Primary function of the system
- The responsible system administrator or user
- The assigned IP addresses
- The system's host name and domain
- The critical information stored on the system
- Whether backups exist for the system
- Whether the system is still connected to the network
- A list of malware detected, from the time of your investigation back to the beginning of log data
- A list of any remediation steps that have been taken
- If any data is being preserved, what process is being used and where it is being stored

Getting the Investigation Started

Network Details Documenting details about the network is just as important, even in cases where network details do not initially seem to be important. At a minimum, consider the following points:

- **A list of all external malicious IP addresses or domain names involved**

Record any IP addresses, domain names, or host names involved with the incident. Perform some quick research—check a whois service.

- **Whether network monitoring is being conducted**

If network administrators have set up network capture devices, determine who is performing it, where the capture is being performed (physically and logically), where the data is being stored, and who has access to it. Clarify the filtering rules applied to the capture as well as whether the capture contains sessions' full content or only header (connection) information.

- **A list of any remediation steps that have been taken**

Determine whether steps such as blocking IP addresses or certain domain names have been redirected to a "blackhole." Find out when those controls were put in place.

- **If any data is being preserved, what process is being used and where it is being stored**

Similar to individual system details, be sure that any data related to network detection is being properly handled and tracked.

- **Updates to network diagrams and configurations** Obtain any updates to network diagrams and configurations since they were initially collected as part of a pre-incident exercise.

Getting the Investigation Started

Malware Details

For each malicious file related to the incident you will want to document the following items:

- The date and time of detection.
- How the malware was detected.
- The list of systems where the malware was found.
- The name of the malicious file, and what directory was it present in.
- What the detection mechanism determined, such as the name and family of the malicious file.
- If the malware is active during the IR and if active network connections are present.
- Whether a copy of the malware is preserved, either manually or through a quarantine process.
- The status of any analysis. Has the malware been analyzed for network and host indicators of compromise?
- Whether the malware was submitted to third parties, either through automated processes or via direct action by an employee.

Getting the Investigation Started

Building an Attack Timeline

- In every investigation we perform, we maintain a timeline of events.
- Timelines keep us organized, provide context, help identify inconsistencies, and provide an overall picture of what happened.
- It's important to realize that events will not necessarily be entered in chronological order.
- It is recommended that you will be entering events as you learn about them, not as they occur (or occurred).

Getting the Investigation Started

•The following table is an abbreviated example of a timeline, sorted by the event time:

Date Added	Event Time (UTC)	Host	Event Description	Data Source
2013-05-08	2012-11-14 18:16:24	host6492581	Infected e-mail attachment opened by the user profile "bob. smith."	File system, recent documents list
2013-05-08	2012-11-14 18:20:44	host6492581	C:\WINDOWS\ Prefetch\IPCONFIG. EXE-5874FA11.pf created.	File system metadata
2013-05-08	2012-11-14 18:21:16	host6492581	C:\WINDOWS\ Prefetch\GSECDUMP. EXE-54F3F8EA.pf created.	File system metadata
2013-05-07	2012-11-15 07:13:00	n/a	User Bob Smith called the IT security department to report a suspicious e-mail he opened the prior day.	Security ticketing System
2013-05-08	2013-05-08 05:15:00	n/a	Live response data collected from user Bob Smith's computer, host6492581	Security ticketing system

Getting the Investigation Started

- Comparing new information against a timeline can help to validate new leads.
- For example, if you uncover information that suggests the initial attack occurred six months before the oldest date you currently recorded, you either have a major breakthrough in the case or you are looking at unrelated information.
- Another example might be with sequences of events.
- Imagine a scenario where you find that an attacker created a file, and then transferred it out of the network.
- After putting the information into a timeline, you notice that the timestamp your proxy server recorded for the transfer is before the creation date of the file.
- Because the file must exist prior to transfer, something is wrong with the data you are looking at or how you are interpreting it.

Getting the Investigation Started

- The attack timeline focuses on significant attacker activities.
- Record details such as when an attacker accessed a system, when files were created, when data was transferred, and when tools were executed.
- It is also important to record the source of the data on the timeline. For example, if you make an entry that an attacker accessed a system, include where you found that information.
- Finally, don’t forget to record the unique identifier of the system the event occurred on.

Getting the Investigation Started

UNDERSTANDING INVESTIGATIVE PRIORITIES

To run a successful investigation, the goals and desired outcome must be considered. Every case type has its own considerations—whether the goal is litigation or simply a stronger security posture. A team needs to understand what should be proven or discovered and how to present the results.

What Are Elements of Proof?

- In a legal sense, the elements of proof define the supporting elements of a claim.
- If you were to investigate a claim of larceny, for example, your principal element of proof may be to establish that material was taken with the intent to deprive another person of that property.
- The investigations that an enterprise incident response team performs may not be as easily defined as larceny or copyright infringement, however.
- During intrusion investigations, we develop a broader definition of "elements of proof," where the driving claims are few and broad in the beginning and narrow in scope and develop greater detail as time goes on.

Initial Development of Leads

- Leads are actionable items about stolen data, network indicators, identities of potential subjects, or issues that led to the compromise or security incident.
- In this we will study various methods of turning leads into actionable items and discuss methods for generating indicators and sweeping an environment to detect where malicious activity has occurred.
- Actionable items, or tasks, are the sole means for getting anything done in the course of an investigation.
- They can be indicators that you can use to sweep your entire enterprise, network traffic signatures, or merely serve as a resource if an employee needs to be interviewed.

Initial Development of Leads

- The process of lead generation should be continuous.
- During most computer intrusion investigations, if you find that leads are becoming scarce, it is often due to the investigative methods rather than an actual lack of data.
- Depending on the state of the investigation, you may want to create an informal process to categorize and prioritize leads.
- This process is especially useful with new IR teams.

We perform the following three operations on leads before allocating time or resources:

- Clarify the data.
- Verify the veracity of the lead.
- Determine the context of the lead.

Initial Development of Leads

innovate achieve lead

ACTING ON LEADS

- Your team has a pile of good leads: a spreadsheet of potentially suspect IP addresses, a list of malicious files' MD5 hashes, and a bit of intelligence that a system in your organization has been communicating to a command-and-control server over TCP/443. Now what?
- We need to turn these leads into viable indicators, the kind that can detect the ongoing events as well as future attacks.
- You also want to be able to detect suspicious conditions that aren't directly related to the information you currently have.
- After all, you know that something else must be occurring in order to allow those suspicious connections to be initiated.
- In this section we walk through an iterative process that occurs over the lifetime of the investigation.
- We also cover more traditional leads—those that require humans to converse, a topic you probably weren't expecting in a book on investigating computer crime.

Initial Development of Leads

Turning Leads into Indicators

- Most of the leads that IR teams generate consist of detectable characteristics of malicious actions.
- They can be represented in two types of indicators.
- The first type, *property-based* indicators, describes a set of known observable characteristics of malicious software or actions—a registry key, an MD5 hash, or a mutex with a unique name, for example. Some leads are less specific, where a combination of characteristics
- can define a malicious or suspicious act—unexpected executable files in the /Windows/Help directory, for example. We call these *methodology-based* or *anomalybased* indicators.
- These all can be turned into indicators that one can use with single-run or enterprise-wide live response to help determine the scope of an incident.
- Recall that we use indicators primarily for the scoping of an incident; discover once, search everywhere.
- Leads can result in host-based indicators, network-based indicators, or a combination
- of both. Imagine the ability to take all of the intelligence you learn from reverse engineering a remote access trojan and rapidly tasking your network and server teams with performing searches for existing data and monitoring for future events.

Initial Development of Leads

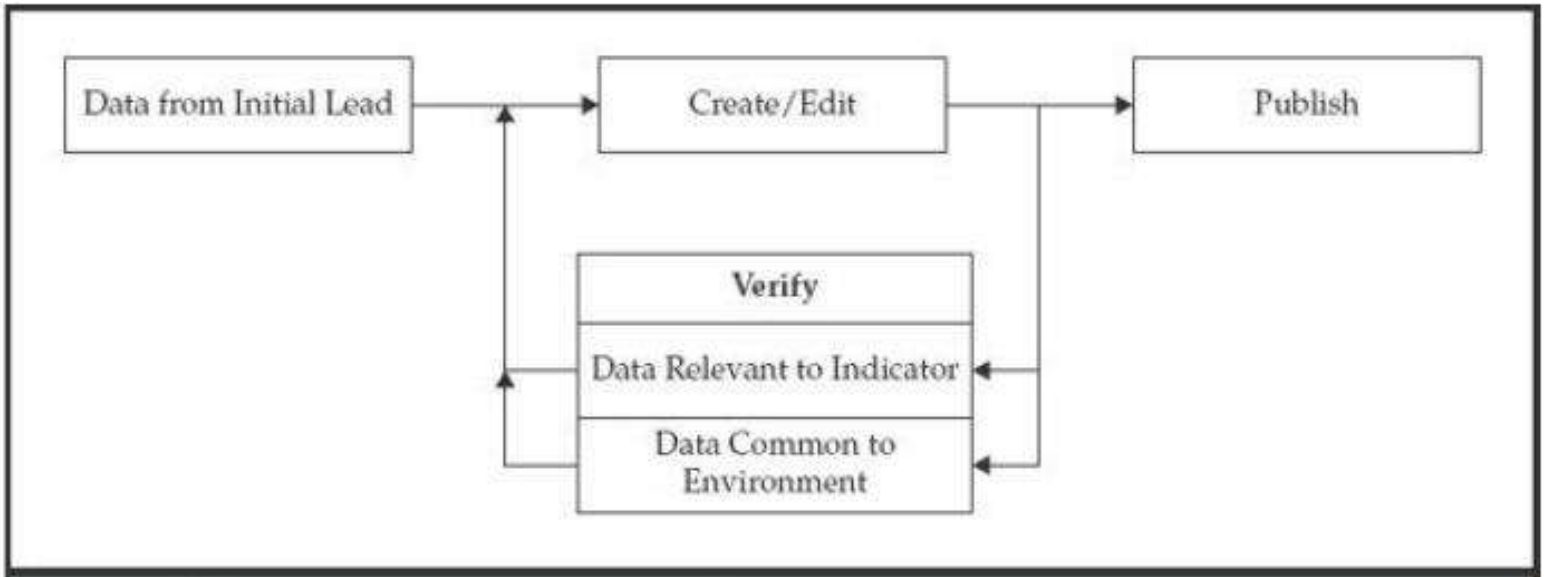


Figure 5-1. Indicator development lifecycle

Initial Development of Leads

The Lifecycle of Indicator Generation

- The lifecycle of indicator development starts with some amount of initial information, as one would expect.
- Any potential data source can feed this process.
- The most useful results come from high-fidelity sources such as a forensic examination or a quality malware analysis report.
- At times, the initial information consists solely of simple characteristics of a suspected attack.
- In any case, the team members responsible for the generation of indicators should follow a process before unleashing an indicator across the enterprise or importing it into the network security monitors, especially if the indicator is from an external source.
- Indicator development is an iterative process where the target is to generate robust, sustainable signatures that can generate reliable information.

Initial Development of Leads

innovate achieve lead

Reporting an Incident to Law Enforcement

- When you begin to pursue external leads, you may opt to report the incident to law enforcement instead of taking action through civil litigation.
- Many factors can play a role in this decision, and we have found that most organizations prefer to avoid notifying law enforcement.
- Although the investigative tools and legal options are far greater and more effective with their involvement, the primary justification for avoiding notification is simply to avoid a public relations issue.
- In the United States, there are very few situations where notification of criminal acts is required.
- Your counsel will know where these bright lines exist and will manage notification.
- When your leads take you to foreign entities, such as ISPs or hosting sites, the process to obtain information can get quite complicated.
- In most situations, foreign governments require civil requests be filed through official channels.
- The State Department and federal law enforcement agencies maintain relationships with foreign governments and provide the means to request information from commercial entities in each country.
- The process can take a fair amount of time to complete, and we have found that some companies will respond to less-formal preservation requests when they know that official paperwork is being completed.

Discovering the Scope of the Incident

We will cover three areas that should help you discover the scope:

- Examining initial data
- Gathering and reviewing preliminary evidence
- Determining a course of action

Discovering the Scope of the Incident

Examining Initial Data

- As part of the detection event, you should have some initial information about the detection.
- For example, if the event was structured query language (SQL) injection, you should have a date, time, and the source and destination IP addresses.
- You will also want to talk to the staff that manages the detection system to see if any other details are available.
- Use a “trust but verify” approach—ask if you can see the alert details.
- You may notice that there is additional information that is useful to the investigation.
- Ask about other detection systems and what they detect and record—there may be systems in place that could provide additional information.
- Keep in mind that network administrators may not think like investigators.
- You should not assume they would tell you about “important information,” because they may not know what is important to the investigation.

Discovering the Scope of the Incident

Gathering and Reviewing Preliminary Evidence

- In this step, you have to determine what sources of preliminary evidence may be able to help and then decide which sources you will actually use.
- Finally, you will collect and review the evidence. You will need to find evidence sources that quickly provide initial answers.
- Ideally, you should identify sources of evidence that come from several categories and require low effort to analyse.
- For example, if an investigative question is to determine if malware executed on a system, you might consider the following evidence sources:
  - Artifacts the malware directly creates on the system, such as files or registry keys
  - Operating system artifacts, such as Windows prefetch, that are indirect artifacts
  - Application artifacts, such as Internet browser history or software metering tools
  - Network artifacts, such as firewall logs that might record network connections

Discovering the Scope of the Incident

Determining a Course of Action

- Once you have gathered and reviewed preliminary evidence, you will need to make decisions about what major activities to perform.
- Those activities normally include preserving evidence, but could also be posturing or containment actions.
- As with any decision, there are a number of factors you can weigh to help you make a choice. We find it helpful to ask ourselves the following questions throughout the scoping process:
    - Will the action help answer an investigative question?
    - Will the action answer my questions quickly?
    - Am I following the evidence?
    - Am I putting too much effort into a single theory?
    - Am I using multiple independent sources of evidence?
    - Do I understand the level of effort?
    - Am I staying objective?
    - Am I tracking the earliest and most recent evidence of compromise?
    - Have I uncovered something that requires immediate remediation?

Discovering the Scope of the Incident

CUSTOMER DATA LOSS SCENARIO

- In this scenario, you work in the IT security department for a large online retailer.
- Your company has been receiving increased complaints from customers regarding e-mail spam.
- The customers indicate that shortly after becoming a new customer, they begin to receive a large amount of e-mail spam.
- This scenario is initially a bit less “concrete” than others are, because there is no real alert data or other indication of a security issue.
- Nevertheless, concern is mounting, and IT security has been asked to investigate.

Discovering the Scope of the Incident

AUTOMATED CLEARING HOUSE (ACH) FRAUD SCENARIO

- In this scenario, you work for a local hardware store chain.
- You are the IT director and the IT security manager.
- You were just informed by your CEO that the company's bank called to let him know they stopped an ACH transfer of $183,642.73.
- The transfer was to an account that has never been used before and was flagged by their fraud prevention system.
- The bank indicates that the CFO's online banking account was used.
- The CFO says he did not make that transfer request. Your CEO confirms that the transfer request was not legitimate. Your CEO wants you to figure out how this happened.
- You can start by reviewing the information the bank provided:

  - The transfer request was initiated online using your CFO's online banking account.
  - The requested transfer amount was US$183,642.73.
  - The transfer request was initiated one day ago, at 4:37 P.M. GMT-5 (EST).
  - The source IP address was your company's public Internet IP address (your firewall).

Discovering the Scope of the Incident

QUESTIONS

1. If your evidence sources do not include multiple independent categories, what steps could you take to increase confidence in your conclusions?

2. In the ACH fraud scenario, think of another reasonable theory for how an attacker might have gained access to the CFO's computer. Explain how you would proceed with investigating that theory.

3. In the customer data loss scenario, a number of steps were taken to verify the customers' complaints. List at least two other useful steps you could have taken to help verify the customers' complaints or isolate the source of the data loss.

Thank you !

SOC 101: Real-time Incident Response Walkthrough - YouTube

What is incident response in cyber security [A step-by-step guide to perform the cybersecurity IRP] - YouTube

BITS Pilani

Prof. Pradnya Kashikar

WILP-CSIS

BITS Pilani
Pilani Campus

innovate achieve lead

BITS Pilani

Pilani Campus

SS ZG588 - Cyber Crimes, Forensics and Incident Handling

Contact Session - 13

Course Objectives

No	Description
CO1	Enhancing awareness of recent Cyber Crime trends and learn Investigating Cyber Crimes
CO2	Introduce Cyberspace Infrastructure attacks and handling Organization Cybersecurity Issues
CO3	Understand Digital Forensics Process, Models, Analysis and Validation, Incident Detection and Response

Text Book(s)

innovate achieve lead

T1	Computer Forensics and Cyber Crime - An Introduction 3rd Edition by Marjie T. Britz, Ph.D., Professor of Criminal Justice, Clemson University
T2	Bill Nelson, A. Philips, F. Enfinger, C. K. Steuart, Computer Forensics and Investigations, Course Technology (Cengage Learning), Indian edition, 2009
T3	Incident Response & Computer Forensics, 3rd Edition by Jason T. Luttgens and Matthew Pepe and Kevin Mandia
R1	Guide to Computer Forensics and Investigations: Processing Digital Evidence 5th Edition by Bill Nelson, Amelia Phillips and Christopher Steuart
R2	The Basics of Digital Forensics, by John Sammons
R3	Computer Network Security and Cyber Ethics 4th Edition, by Joseph Migga Kizza
R4	Computer Forensics_ Investigating Network Intrusions and Cyber Crime: EC-Council Press

Learning Outcomes -

No	Learning Outcomes
LO1	Fundamental understanding and Information on Cyber Crimes, Digital Forensics Objectives and Incident Detection and Response Reports.
LO2	Learn on how to prepare investigation on computer-related incidents or crimes and summarize.
LO3	Understand on digital forensics process, models and analysis by taking a systematic approach
LO4	Explore on evaluating needs, validating and testing digital forensics tools, Generating Incident Report Findings, and Emerging Cybercrime Trends and Issues

Module 12 - Incident Response and software Tools

innovate achieve lead

12.1	Incident Response process and handling an Incident
12.2	Investigating Applications
12.3	Incident Capture Tools; Analysis Tools; Response Tools
12.4	Remediation Introduction and Case Study

13	Incident Response and software Tools	**Incident Response process and handling an Incident**	T3, R1
		Investigating Applications	
		Incident Capture Tools; Analysis Tools; Response Tools	
		Remediation Introduction and Case Study	

Incident Response process

- The incident response process consists of all the activities necessary to accomplish the goals of incident response.
- The overall process and the activities should be well documented and understood by your response team, as well as by stakeholders throughout your organization.
- The process consists of three main activities, and we have found that it is ideal to have dedicated staff for each:
    - Initial response
    - Investigation
    - Remediation

Incident Response process

- Initial response is an activity that typically begins the entire IR process.
- Once the team confirms that an incident is under way and performs the initial collection and response steps, the investigation and remediation efforts are usually executed concurrently.
- The investigative team's purpose is solely to perform investigatory tasks.
- During the investigation, this team continually generates lists of what we call "leads."
- Leads are actionable items about stolen data, network indicators, identities of potential subjects, or issues that led to the compromise or security incident.
- These items are immediately useful to the remediation team, whose own processes take a significant amount of time to coordinate and plan.
- In many cases, the activity that your team witnesses may compel you to take immediate action to halt further progress of an intrusion.

Incident Response process

Initial Response

- The main objectives in this step include assembling the response team, reviewing network-based and other readily available data, determining the type of incident, and assessing the potential impact.
- The goal is to gather enough initial information to allow the team to determine the appropriate response.
- Typically, this step will not involve collecting data directly from the affected system.
- The data examined during this phase usually involves network, log, and other historical and contextual evidence.
- This information will provide you the context necessary to help decide the appropriate response.
- For example, if a banking trojan is found on the CFO's laptop, your response will probably be quite different than if it is found on a receptionist's system. Also, if a full investigation is required, this information will be part of the initial leads.

Incident Response process

Some common tasks you may perform during this step are:

- Interview the person(s) who reported the incident. Gather all the relevant details they can provide.
- Interview IT staff who might have insight into the technical details of an incident.
- Interview business unit personnel who might have insight into business events that may provide a context for the incident.
- Review network and security logs to identify data that would support that an incident has occurred.
- Document all information collected from your sources.

Incident Response process

Investigation

- The goal of an investigation is to determine facts that describe what happened, how it happened, and in some cases, who was responsible.
- As a commercial IR team, the “who” element may not be attainable, but knowing when to engage external help or law enforcement is important.
- Without knowing facts such as how the attacker gained access to your network in the first place, or what the attacker did, you are not in a good position to remediate.
- It may feel comforting to simply pull the plug and rebuild a system that contains malware, but can you sleep at night without knowing how the attacker gained access and what they did?
- A five-step process, shown in the figure on the next slide, that promotes an effective investigation.

Incident Response process

innovate achieve lead

IOC – Indicators of Compromise

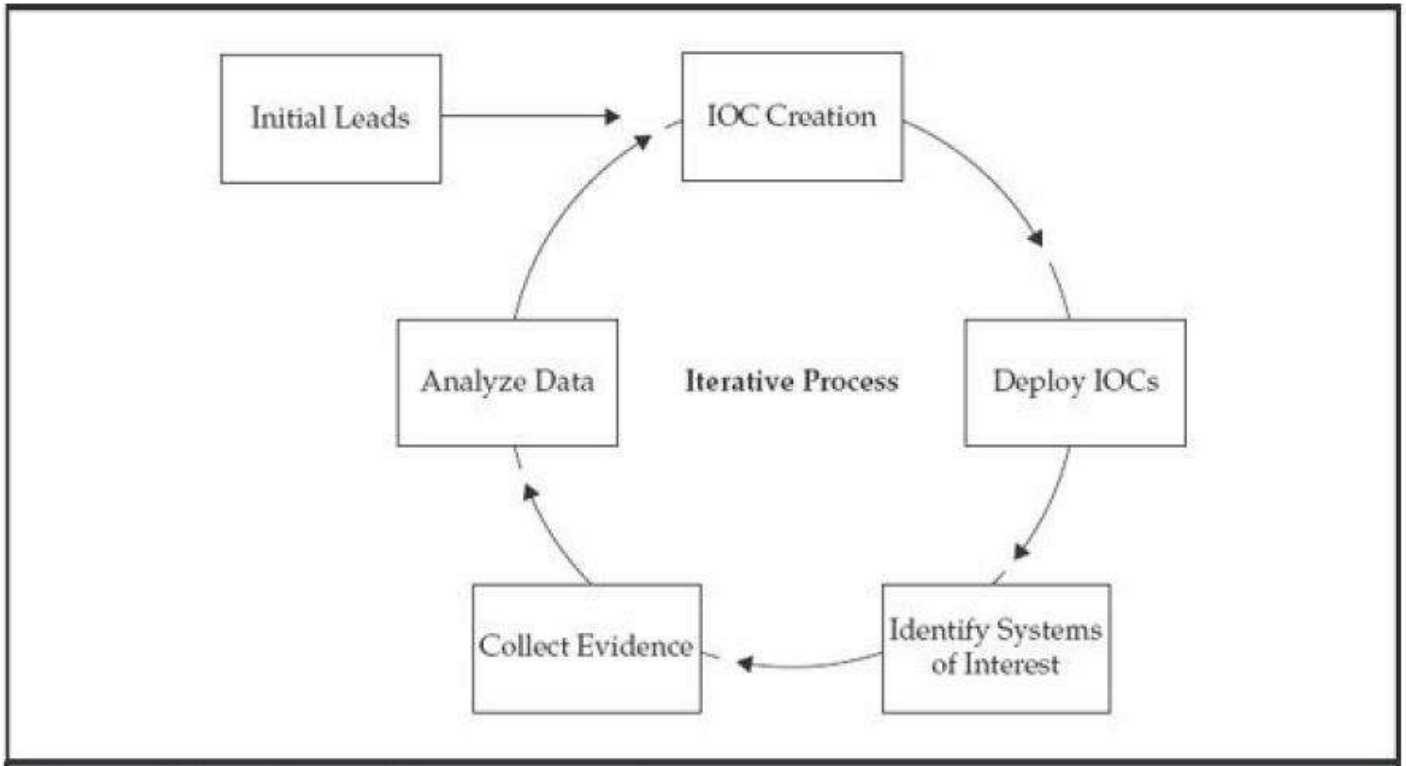


Figure 2-2. The incident response lifecycle

Handling an Incident

innovate achieve lead

Reporting

- Even within a single investigation, there can be so many findings that communicating the totality of the investigation would have been difficult without formal, periodic reports.
- In many investigations, the high-level findings are based on numerous technical facts that, without proper documentation, may be difficult to communicate.
- Reports are also a primary deliverable for incident response teams, for a few reasons.
- Reports not only provide documented results of your efforts, but they also help you to stay focused and perform quality investigations.
- We use a standard template and follow reporting and language guidelines, which tends to make the reporting process consistent. Reporting forces you to slow down, document findings in a structured format, verify evidence, and think about what happened.

Handling an Incident

innovate achieve lead

Incident Response process:

- Define what a “computer security incident” means in your organization.
- Identify critical data, including where it is stored and who is responsible for it.
- Create an incident tracking process and system for identifying distinct incidents.
- Understand the legal and compliance requirements for your organization and the data you handle.
- Define the capabilities you will perform in house, and what will be outsourced.
- Find and train IR talent.
- Create formal documentation templates for the incident response process.
- Create procedures for evidence preservation on the common operating systems in your environment.
- Implement network-based and host-based solutions for IOC creation and searching.
- Establish reporting templates and guidelines.
- Create a mechanism or process to track significant investigative information.

Investigating Applications

innovate achieve lead

Investigating Applications

- While examining forensic evidence, it's common to find artifacts that are not part of the operating system.
- User applications, such as Internet browsers, e-mail clients, office suites, and chat programs, store data on nearly every computer.
- There are also service applications, such as web servers, database servers, and e-mail servers, that support both user applications and the IT infrastructure.
- These data sources are often a critical source of evidence for an investigation.
- Therefore, it's important to understand how to identify and analyse application data.
- Because there are many ways an application creator can choose to store data, you will encounter many different data formats.
- Sometimes an application uses only a single format whereas other applications use multiple formats.
- The creator will normally choose formats that are well suited for the requirements of the application.
- Those formats can range from standard open source data structures to closed proprietary formats.

Investigating Applications

- Some application artifacts are independent of the operating system.
- For example, certain web browser history files are the same for any operating system that you use the browser on.
- You can take advantage of this during an investigation by using similar tools or techniques to review application data from many different operating systems.
- Application data is important because it is a layer of potential evidence in addition to operating system artifacts.
- Some of the most common application categories that are relevant to an intrusion investigation are e-mail clients, web browsers, and instant messaging clients.

Investigating Applications

WHAT IS APPLICATION DATA?

- Data that is created, stored, or maintained by an application is considered application data.
- There are many different ways application data is stored and represented.
- Those storage methods, and the available data, regularly change over time.
- Some applications remain fairly stable, whereas others can change dramatically from month to month.
- Because of this, the tools and methods for investigating applications can also change dramatically over time.

Investigating Applications

innovate achieve lead

WHERE IS APPLICATION DATA STORED?

As you begin to examine a system to look for application data, you may find yourself wondering where to start. More to the point, how do you know what applications are installed on the system and where related application data is located? Although applications can store data in custom locations, most operating systems have a convention. Knowing these conventions can help you quickly discover useful application data.

Windows –

- Default application installation directory
- Default application data directories
- Registry uninstall information
- Default registry configuration data locations

Investigating Applications

innovate achieve lead

OS X

Apple OS X has two main locations you should inspect if you are searching for applications or related data:

- Default application installation directory
- Application user data directory

Linux

- In Linux, the locations of application-related data will vary based on the distribution you are investigating and any customizations that may be in place.
- We use two categories of methods to locate application data. The first is to manually inspect the file system, and the second is to query the package manager.
- Manually inspecting the file system can take a lot of time and become very tedious if you don’t have something to point you in the right direction.
- To help, there is a convention that most Linux distributions follow called the Filesystem Hierarchy Standard (FHS).
- The FHS defines the directory structure that Linux distributions should follow.

Investigating Applications

Most distributions conform to some portion of the standard, so inspecting the following locations should provide you with good leads:

- **Systemwide configuration data** In most Linux distributions, the /etc and /usr/local/etc/directories are the primary locations where systemwide application configuration data is stored.

- **User application data** User-specific application data is typically found in subdirectories under the user's home directory, by default /home/{username}.

- **Executable locations** The standard directories where you will find executables are /bin, /sbin, /usr/bin, /usr/sbin, /usr/local/bin, and /usr/local/sbin.

- **Add-on software** A location where some third-party applications and application data are installed to is /opt.

Investigating Applications

innovate achieve lead

High-level steps in investigating applications:

1. **Configure an environment**

You will need to configure an environment that is conducive to performing your research. Much like when you're examining malware, it is likely that you will need to frequently re-run tests. A virtual machine with snapshot capability makes this very easy to perform.

2. **Obtain the application**

If you do not already have a copy of the application, you will need to obtain one. If the software is freely available, you can simply download a copy. If the software is commercial, you may need to purchase it. However, in some cases, the manufacturers provide trial or demo versions of their software.

3. Configure instrumentation

Instrumentation is software or tools that allow you to monitor the execution of the application and identify potential artifacts of interest. The instrumentation you can use varies by operating system. The most common operating system we encounter is Microsoft Windows, and one of the best tools is Microsoft's Process Monitor. The Apple OS X command "dtruss" and the Linux (and other Unix variant) command "strace" display all syscalls that a process makes.

Investigating Applications

4. Perform installation Perform the application installation while your instrumentation is active. You may find useful artifacts during the installation process. Those artifacts may help answer if an application is currently, or was ever, installed on a system under investigation. After the installation is complete, you may want to stop your instrumentation and save the output.

5. **Execute the application** You should try to execute the application consistent with how it is used in the environment that is part of the investigation. You should perform appropriate configuration and execute functionality that is of interest. This will help to produce relevant artifacts.

6. **Review instrumentation data** Once execution is complete, stop the instrumentation and review the output. Output from monitoring program execution often contains thousands of events. You will need to search through the output for events of interest, such as file creation or modification.

7. **Adjust instrumentation and re-perform testing as needed** If needed, you may need to refine your instrumentation to only monitor the paths that the application executables reside in. For example, if you are using Microsoft's Process Monitor, you may want to add filters to restrict file monitoring. You may need to execute the application multiple times and refine filters until the data collected is easy to analyse.

Investigating Applications

innovate achieve lead

WEB BROWSERS

Web browsers are among the most popular computer applications today. Web browsers are applications that retrieve, process, and present data. Today, that data is most commonly Hypertext Markup Language (HTML) and numerous multimedia formats. When rendered by the browser, the HTML and multimedia are combined to present useful information that is commonly called a “web page.” Your web browser can retrieve data from your local computer or from another computer, commonly called a server or a site, that can be on your local network, in a nearby city, or halfway around the world. Web browsers can also send data back to those servers as part of an interactive process, such as e-commerce, collaboration environments, or a computer game. As the capabilities of web browsers increase, more and more traditional applications, such as word processors and e-mail clients, are becoming “web apps”— interactive sessions within a web browser that closely resemble a traditional application. This trend makes it very important for incident responders to Understand how web browsers work.

Investigating Applications

Throughout the process of sending, receiving, processing, and presenting data, the browser creates many artifacts on a system. Nearly all web browsers maintain the following:

- **History** As you visit websites, a browser will normally record the Uniform Resource Locator (URL) you accessed, as well as the date and time. This makes it convenient for you to revisit a site you recently browsed to.

- **Cache** As you access sites, the browser will store local copies of data that is retrieved. This is used to speed up the browsing process, because some items are used repeatedly on a single site or across multiple sites. The default amount of cache saved varies by browser, and can be modified by the user.

- **Cookies** Cookies are small bits of information that a site may instruct your browser to store. They are commonly used to save site preferences and maintain session information. Most browsers can be configured to restrict (deny) cookies for specific sites or for all sites.

Incident Capture Tools, Analysis Tools, Response Tools

- During an investigation, these artifacts can provide critical evidence that allows you to explain what happened.
- Whether you are investigating the victim of social engineering, or an attacker who logged in to a system and performed malicious actions, web browser artifacts can provide you with useful leads.
- Several tools are able to process artifacts from all major web browsers.
- Commercial forensic suites, including EnCase and FTK, have the ability to parse most browser artifacts, although support for the most recent versions of browsers tends to lag.
- The best commercial options for analysing browser artifacts are tools that focus specifically on browser artifacts.
- Two tools which are found particularly good are Digital Detective NetAnalysis and Magnet Forensics Internet Evidence Finder.

- Conducting Investigations on the Dark Web on JSTOR

Incident Capture Tools, Analysis Tools, Response Tools

Digital Detective NetAnalysis www.digital-detective.co.uk/netanalysis.asp
Internet Evidence Finder www.magnetforensics.com/software/internet-evidence-finder

These commercial tools provide comprehensive browser artifacts analysis. They do not cost as much as a full forensic suite, so they may be a good option for some organizations. There are also many free tools you can use. Free tools tend to focus on a single browser, so we will mention those in each browser section in this chapter. There are at least two exceptions to that—NirSoft's BrowsingHistoryViewer and Mandiant's RedLine—both of which can display the browsing history for Internet Explorer, Mozilla Firefox, Google Chrome, and Safari, all in a single view.

articles.forensicfocus.com/2013/12/10/forensic-analysis-of-the-ese-database-in-internet-explorer-10

E-MAIL CLIENTS

- There are many types of investigations where e-mail is a key source of evidence.
- In intrusion investigations, a common initial attack vector is *spear phishing*—this is when an attacker targets victims with social engineering e-mails.
- In scareware scams, attackers sometimes send e-mail from faked or stolen e-mail accounts.
- In other criminal activity, miscreants may use e-mail to coordinate activity or transfer data. And finally, don't forget that e-mail accounts are also a direct target—some attackers are interested in stealing e-mail.
- In all these cases, it is important to know what common e-mail applications are in use and understand where data is stored, what is stored, and how to analyse it.

E-MAIL CLIENTS

- The most basic piece of data is the e-mail it itself. E-mail content contains two main sections—one called the “body” and one called “headers.”
- The body is the actual content of the e-mail, such as text or attachments.
- It is common for the body to be encoded in the Multipurpose Internet Mail Extensions (MIME) format.
- This encoding standard was created so newer multimedia contents are handled correctly as the e-mail passes through different types e-mail systems.
- The headers consist of handling information, such as the sender’s e-mail address, the recipient’s e-mail address, a sent date, a subject, a list of servers the e-mail was passed through, and many other possible fields.
- E-mail headers can be extremely complex to decode.
- If you are looking for some extra help, the following Internet resources should be of assistance.
- Be careful with the Google Apps link, though, because you probably don’t want to paste sensitive data into the site.

Data Format

- Outlook uses a file format called the Personal Folder File (PFF).
- In a Microsoft Exchange–based environment, Outlook will store a copy of e-mail offline in a file called the Offline Storage Table (OST), which is a form of PFF.
- In non-Exchange environments, such as Post Office Protocol (POP), or in Outlook archives, the file format used is the Personal Storage Table (PST), also a form of PFF.
- These files will also contain additional data such as calendar appointments and contacts.
- Because both of these forms are based on the PFF format, most tools that parse OST will also parse PST, and vice versa.
- Even though the PFF format is proprietary, there is good documentation from third parties.
- The Downloads section of the Libpff project website contains several very good documents on the PFF format.

Tools

There are two categories of tools you can use to analyze OST and PST files:

- **Commercial forensics tools** Guidance Software's EnCase and AccessData's FTK can parse and analyze OST and PST files natively. For example, within EnCase, you can simply right-click the file and select View File Structure. EnCase displays the e-mail data file contents as a tree that you can browse and search just like a file system.
- **Open source tools** The best maintained and documented open source project we know of for OST and PST parsing is "libpff." This project provides the code to compile an executable called "pffexport," which can export items from an OST or PST file. In Windows, you can compile the libpff tools using an environment such as Cygwin.
- Because Apple Mail e-mail messages are stored in plain text, you can use many tools to examine them. Basic command-line tools, such as grep or strings, may be all you need to locate messages of interest. More robust GUI-based search tools, such as PowerGREP, are also very effective. You can also convert the emlx format into standard mbox, and use a free e-mail client such as Mozilla Thunderbird to view the e-mail.

Facebook Chat

- The popular social media site Facebook provides a built-in web-based text and video chat client.
- Facebook users can use the client to communicate with anyone in their “friends” list that has chat enabled.
- The client logs data by default to the user’s Facebook profile as “messages” on the server.
- If the recipient is not available at the time a chat is sent, Facebook servers will place the message in their inbox—similar to sending an offline message to the user.
- All chats therefore take place through the web-based client—there is not a local install of software.
- This presents a challenge if you don’t have access to the user’s account on Facebook through a search warrant or other legal process.

Log Storage

- Facebook logs are not stored on a user's system.
- Because the system is web based, Facebook chat messages are stored on Facebook servers.
- While the web client is active, the messages may be manually copied out of the message window using normal copy/paste commands.
- Otherwise, it is possible that artifacts of the chat sessions are present in memory, page files, hibernation files, unallocated space, or in Internet browser cache files.
- Those artifacts are present through indirect processes and are not stored by design.
- Therefore, the presence of artifacts is unpredictable, and, even when present, may be incomplete or inaccurate.

Log Format

Facebook chat messages in memory are formatted in JavaScript Object Notation (JSON). When sent as a chat message, the message is stored with the tag “msg” with the following fields:

- “text” (includes the body of the message)
- “messageID”
- “time” (message time in UTC as a Unix millisecond timestamp)
- “from” (the Facebook ID of the sender)
- “to” (the Facebook ID of the recipient)
- “from_name” (in plain text)
- “to_name” (in plain text)
- “sender_offline” (false if the chat partner was online at the time the message was sent)

Incident Capture Tools, Analysis Tools, Response Tools

Here is an example of a message (the full Facebook IDs were sanitized with *xxxx*):


```
{"msg":{"text":"This is some chat",
   "messageId":"mid.13674559xxxxx:df1f767dba525b7d49","time":1367418992627,
   "clientTime":1367418992627,"msgID":"13674559xxxxx:2710102545",
   "offline_threading_id":null},"from":1000057544xxxxx,"id":15519xxxxx,
   "to":15519xxxxx,"from_name":"Author_Writer","from_first_name":"Author",
   "to_name":"Recipient_Receiver","to_first_name":"Recipient",
   "tab_type":"friend","sender_offline":false,"show_orca_callout":false
   ,"window_id":"35525xxxxx","type":"msg"
}
```

Incident Capture Tools, Analysis Tools, Response Tools

It’s unlikely you will find Facebook chat messages in Internet browser cache files. Main memory is the most common place to find messages. At least one tool Internet Evidence Finder (IEF), can carve memory images for chat fragments. Additionally, you can try keyword searches for portions of the JSON message format, such as the following:

- {“msg”:
- {“text”:
- “from”:
- “id”:

The last two can be particularly useful if you know the Facebook ID of the sender and recipient. Each individual message sent or received will have a tagged wrapper, making the process tedious if the image contains a large number of messages.

Artifacts

Facebook artifacts can remain in Internet browser cache files, the page file, memory, or unallocated locations. Facebook running natively in a browser does not store logs or preferences offline intentionally.

Tools

Partly because Facebook does not store logs on a user's local system, very few commercial tools have been created to parse Facebook chats. A tool that can parse Facebook chat messages, along with many other evidence items, is Internet Evidence Finder (IEF). IEF can analyse a memory image for Facebook chat items, including all the JSON fields we outlined in the Facebook "Log Format" section.

Incident Capture Tools, Analysis Tools, Response Tools

- During an investigation, operating system artifacts are only part of the picture.
- Application-related artifacts will add to your understanding of an incident, and sometimes may be your only source of evidence.
- Keep in mind, however, that the operating system may leave application artifacts in unexpected places—like free space or the Windows page file—that are beyond the control of the application.

Remediation Introduction and Case Study

Remediation

- Remediation plans will vary greatly, depending on the circumstances of the incident and the potential impact.
- The plan should consider factors from all aspects of the situation, including legal, business, political, and technical. The plan should also include a communication protocol that defines who in the organization will say what, and when.
- Finally, the timing of remediation is critical. Remediate too soon, and you may fail to account for new or yet-to-be-discovered information.
- Remediate too late, and considerable damage could occur, or the attacker could change tactics.
- The best time to begin remediation is when the detection methods that are in place enter a steady state.
- That is, the instrumentation you have configured with the IOCs [Indicators of Compromise] stop alerting you to new unique events.

Remediation Introduction and Case Study

- We recommend starting remediation planning as early in the incident response process as possible so that you can avoid overtasking your team and making mistakes.
- Some incidents require significantly more effort on remediation activities than the actual investigation.
- There are many moving parts to any organization and undertaking the coordination of removing a threat is no easy task.
- The approach we take is to define the appropriate activities to perform for each of the following three areas:

  - Posturing
  - Tactical (short term)
  - Strategic (long term)

Remediation Introduction and Case Study

- ***Posturing*** is the process of taking steps that will help ensure the success of remediation.
- Activities such as establishing protocol, exchanging contact information, designating responsibilities, increasing visibility, scheduling resources, and coordinating timelines are all a part of the posturing step.
- ***Tactical*** consists of taking the actions deemed appropriate to address the current incident.
- Activities may include rebuilding compromised systems, changing passwords, blocking IP addresses, informing customers of a breach, making an internal or public announcement, and changing a business process.
- Finally, throughout an investigation, organizations will typically notice areas they can improve upon.
- However, you should not attempt to fix every security problem that you uncover during an incident; make a to-do list and address them after the incident is over.
- The ***Strategic*** portion of remediation addresses these areas, which are commonly long-term improvements that may require significant changes within an organization.
- Although strategic remediation is not part of a standard IR lifecycle, we mention it here so that you are aware of this category and use it to help stay focused on what is important.

Remediation Introduction and Case Study

innovate achieve lead

Tracking of Significant Investigative Information

- Your investigations must have a mechanism to easily track critical information and share it with the ancillary teams and the organization's leadership.
- You should also have a way to refer to specific incidents.
- Establish an incident numbering or naming system and use that to refer to and document any information and evidence related to a specific incident.

significant investigative information is as follows:

• **List of evidence collected** This should include the date and time of the collection and the source of the data, whether it be an actual person or a server. Ensure that a chain of custody is maintained for each item. Keep the chain of custody with the item, and its presence in this list is an indicator to you that an item has been handled properly.

• **List of affected systems** Track how and when the system was identified. Note that "affected" includes systems that are suspected of a security compromise as well as those simply accessed by a suspicious account.

Remediation Introduction and Case Study

List of any files of interest

This list usually contains only malicious software but may also contain data files or captured command output. Track the system the file was found on as well as the file system metadata.

- **List of accessed and stolen data** Include file names, content, and the date of suspected exposure.
- **List of significant attacker activity** During examinations of live response or forensic data, you may discover significant activities, such as logins and malware execution. Include the system affected and the date and time of the event.
- **List of network-based IOCs** Track relevant IP addresses and domain names.
- **List of host-based IOCs** Track any characteristic necessary to form a well-defined indicator.
- **List of compromised accounts** Ensure you track the scope of the account's access, local or domain-wide.
- **List of ongoing and requested tasks for your teams** During our investigations, we usually have scores of tasks pending at any point. From requests for additional information from the ancillary teams, to forensic examinations, it can be easy to let something fall through the cracks if you are not organized.

Useful links

http://youtube.com/watch?v=X4lPEpATNxg

http://youtube.com/watch?v=PhROeWMPBqU

http://youtube.com/watch?v=NL1ShMo4Gm4

Thank you !

BITS Pilani

Prof. Pradnya Kashikar

WILP-CSIS

BITS Pilani
Pilani Campus

innovate achieve lead

BITS Pilani

Pilani Campus

SS ZG588 - Cyber Crimes, Forensics and Incident Handling

Contact Session - 14

Course Objectives

No	Description
CO1	Enhancing awareness of recent Cyber Crime trends and learn Investigating Cyber Crimes
CO2	Introduce Cyberspace Infrastructure attacks and handling Organization Cybersecurity Issues
CO3	Understand Digital Forensics Process, Models, Analysis and Validation, Incident Detection and Response

Text Book(s)

innovate achieve lead

T1	Computer Forensics and Cyber Crime - An Introduction 3rd Edition by Marjie T. Britz, Ph.D., Professor of Criminal Justice, Clemson University
T2	Bill Nelson, A. Philips, F. Enfinger, C. K. Steuart, Computer Forensics and Investigations, Course Technology (Cengage Learning), Indian edition, 2009
T3	Incident Response & Computer Forensics, 3rd Edition by Jason T. Luttgens and Matthew Pepe and Kevin Mandia
R1	Guide to Computer Forensics and Investigations: Processing Digital Evidence 5th Edition by Bill Nelson, Amelia Phillips and Christopher Steuart
R2	The Basics of Digital Forensics, by John Sammons
R3	Computer Network Security and Cyber Ethics 4th Edition, by Joseph Migga Kizza
R4	Computer Forensics_ Investigating Network Intrusions and Cyber Crime: EC-Council Press

Learning Outcomes -

No	Learning Outcomes
LO1	Fundamental understanding and Information on Cyber Crimes, Digital Forensics Objectives and Incident Detection and Response Reports.
LO2	Learn on how to prepare investigation on computer-related incidents or crimes and summarize.
LO3	Understand on digital forensics process, models and analysis by taking a systematic approach
LO4	Explore on evaluating needs, validating and testing digital forensics tools, Generating Incident Report Findings, and Emerging Cybercrime Trends and Issues

Module 13 - Incident Report Writing

13.1 Processing of Evidence and Report Preparation

13.2 Reporting Standards and Guidelines for Writing Reports

13.3 Report Writing for High-Tech Investigations

13.4 Generating Report Findings with Forensics Software Tools

14	Incident Report Writing	**Processing of Evidence and Report Preparation**	T1, T3, R1
		Reporting Standards and Guidelines for Writing Reports	
		Report Writing for High-Tech Investigations	
		Generating Report Findings with Forensics Software Tools	

Processing of Evidence and Report Preparation

- While many investigations focus primarily on evidence stored on a suspect computer system, others concentrate exclusively on a variety of storage media, and still others include a combination of both.
- In all cases, automated or manual recovery efforts are appropriate.
- Whatever the case may be, investigation of portable storage devices should be separate from computer system.
- Due to the voluminous nature of some cases, it is imperative that investigative procedures remain the same (as much as possible) across investigations.
- This will ensure a continuity across investigations and enhance testimonial validity.
- In addition, it will reduce confusion, and increase the efficiency and subsequent effectiveness of the search.

Processing of Evidence and Report Preparation

- Regardless of the software employed, investigators must thoroughly capture a complete schematic of the suspect system, keeping detailed notes to assist them with often delayed courtroom presentation.
- Such documentation must include any and all changes made to the data collected including justifications for modifications.
- In addition, this documentation should include a schematic of evidence volatility, providing justification for deviations from SOP.
- Keep in mind that all analysis activities should be conducted with a forensic machine, due to the possibility of intentional sabotage or accidental contamination or destruction.
- Finally, all forensic tools should be properly validated prior to use.

Processing of Evidence and Report Preparation

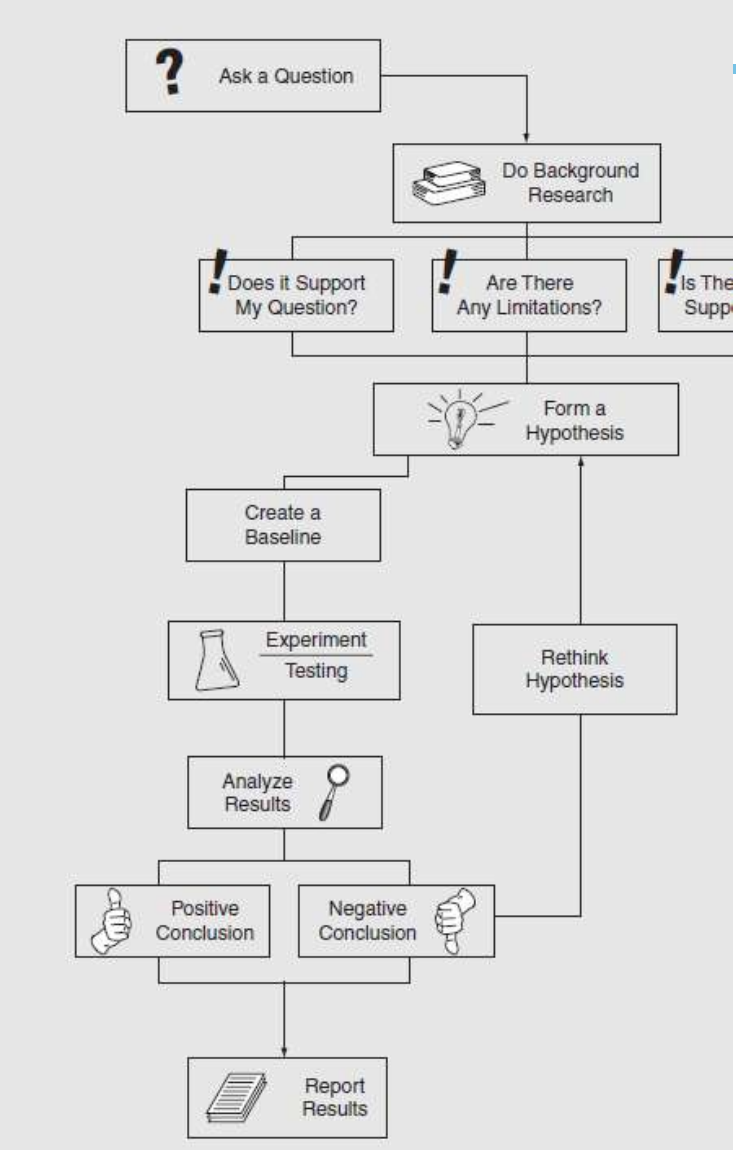
Selecting a Forensic Tool

The selection of technology is often the hardest for any forensic examiner as there are many excellent choices out there. There are some basic rules that can be applied to be able to weed through the variety of materials on each of the tools available to help select the best options.

Ask the following questions when selecting digital forensic technology:

- **Is it read only?** • Yes • No
- **Can I repeat my results?** • What are your validation steps?
- **Is the data verified and if so, how?**
  - What hash values are used?
  - Can those values be repeated?
  - Are there other validations?
- **Was it designed for forensics, and are the images gathered valid?**
  - Is it a commercial tool that is being used in forensics?
  - How is the image file created?

Processing of Evidence and Report Preparation



- The importance of documentation cannot be overstated.
- Judicial oversight and defense challenges require that scrupulous attention be directed toward the documentation of any and all activities conducted on a particular piece of evidence.
- As such, analysts should continue the documentation process which was initiated by the evidence technicians or on-scene investigators by retrieving and updating the evidence logs.
- At a minimum, lab analysis should include the name, rank, and identifying information for any individual tasked with the analysis of such evidence; the condition of the evidence upon delivery to the analyst; the date and time of evidence arrival and return; and the name, rank, and identifying information of the person delivering such evidence.

Processing of Evidence and Report Preparation

User/System Data	Artifacts
User profiles—data that pertains to or was created by an individual user	**Metadata**—In its strictest sense, metadata is data about data. Such informational data includes data on file modification, access, creation, revision, and deletion dates. It has two types: system metadata—operating system dependant and which contains information about the file. Application metadata—information embedded within the file itself. This final type is transient, moving with the file.
Program files—software applications that were installed in the computer	**Windows system registry**—database employed with Windows operating system which store configuration information
Temporary files (temp file)—temporary data files that were created by applications	**Event logs or log files**—files which record and document any significant occurrence in a system or program
Special application-level files—includes Internet history and e-mail	**Swap files**—computer memory files written to the hard drive **Printer spool**—information stored in buffers awaiting printing **Recycle bin**—temporary location of deleted files

Processing of Evidence and Report Preparation

Evidence from Internet Activity

Once computers have been properly imaged and verified, investigative steps will vary based on individual case characteristics. However, almost any case may involve the Internet in some way. As noted by the National Institute of Justice, criminals may use the Internet for a variety of reasons, including, but not limited to, the following:

- trading or sharing of information (i.e., documents, photographs, movies, graphics, software, etc.)
- concealing their identity
- assuming another identity
- identifying and gathering information on victims
- communication with co-conspirators
- distributing information or misinformation
- coordinating meetings, meeting sites, or parcel drops

Processing of Evidence and Report Preparation

As such, criminal evidence may reside in a variety of places, and even those things which appear to be innocuous at first might later prove important. As mentioned, previously, investigators must be able to document a relationship between the suspect and the evidence. In other words, investigators must demonstrate a relationship between the transactional evidence and the suspect machine. Such links might be in the following areas:

IP addresses, domain names, e-mails and IMs, Internet history, and MAC Addresses.

While most forensic packages previously discussed contain the ability to search for these things, stand-alone programs, Web sites, or court processes such as those listed in the below may also be used:

- **Internet Protocol (IP) Addresses**
- **Domain Name System** (DNS)
- **MAC Address**
- **Traceroute -** a tool designed to trace the path a packet takes upon traveling from one device to another. It is often used to narrow down the geographic location of a particular device.

Processing of Evidence and Report Preparation

A SAMPLE OF POPULAR PRODUCTS

• **Mobile Phone Examiner Plus (MPE+)**—Released by AccessData in the summer of 2011, MPE+ is designed as a stand-alone cell phone forensics software platform which provides seamless integration with the company's popular Forensic Toolkit (FTK).
Offering support for approximately 3,500 mobile devices, the product is capable of forensic analysing devices such as iPhones, iPads, Blackberries, and Androids. Some key enhancements of the latest release include, but are not limited to, the following:

• Extraction and decryption of the logical OS partition and logical user partition from iOS and iOS4 devices, including iPhone 4, iPad 1, and iPod Touch 3 & 4
• Enables full user data extraction from rooted Android devices including SQLite databases, location information and deleted data, Internet histories, username and passwords, and deleted application cache.
• Exportation and report preparation of data such as phonebook, sms/mms messages, call history, calendar, and e-mails to .cvs files

Processing of Evidence and Report Preparation

Device Seizure—Created by Paraben Software, **Device Seizure** is a combination of two earlier products. This new tool includes Palm DD Command Line Acquisition and supports PDAs using the following operating systems: Palm through 6, Windows CE/Pocket PC/Mobile 4.x and earlier, BlackBerry 4.x and earlier, and Symbian 6.0. It also supports Garmin GPS devices. It also comes with full flashers, new model support, improved manufacturer support, and new cables added to the accompanying toolbox. The platform also provides for both logical and physical acquisitions and ensures data integrity through write blocking. More Information is available at *www.paraben.com*.

UFED (**Universal Forensics Extraction Device**)—Created by CelleBrite, **UFED** is a stand-alone self-contained system which provides data extraction of content stored in cell phones. The device also has a built-in SIM card reader and cloner which allows investigators to create and insert a clone of the original. This is Especially useful as it allows the phone to function normally without registering On the mobile carrier's network, thus negating the need for Faraday bags.

Processing of Evidence and Report Preparation

XRY Complete—Created by MicroSystemation, XRY is a software application designed for Windows-based systems which provides extraction and analysis tools for a multitude of devices, including smartphones, GPS navigation units, modems, MP3 players, and tablets. It supports nearly 6,000 different mobile device profiles, and provides tools for both logical and physical extraction of data.

Processing of Evidence and Report Preparation

Report Preparation and Final Documentation

- The development of a forensic laboratory and the collection and analysis of digital Evidence are critical in criminal investigations.
- However, successful prosecution of computer-related offenses often hinges upon formal reporting and the competency and credibility of courtroom witnesses.
- Incomplete reports or inconsistent testimony can negate even the best-run investigations.
- Witnesses who are uncertain as to all aspects of their analysis or hesitant in their findings may be discredited or impeached during cross-examination.
- In addition, evidence may be ruled inadmissible if a proper chain of custody cannot be established.
- Thus, it is essential that investigators are properly trained in all methods employed and maintain comprehensive logs of their activities.
- Such logs include both traditional and computer-generated reports.

Processing of Evidence and Report Preparation

Traditional documents

- It typically include documents relating to the chain of custody of physical evidence, logs of crime-scene activity and evidence collection procedures, and the like.
- Computer-generated reports, on the other hand, typically involve those activities associated with data analysis.
- Traditionally, written logs of forensic practices were necessary as investigators moved between various tools to conduct their analysis.
- Currently, most forensic Packages are capable of creating logs and subsequent reports automatically.
- While many contemporary investigators eschew the traditional approach, it is recommended that both strategies are employed to enhance the credibility and veracity of the investigation.

Processing of Evidence and Report Preparation

At a minimum, all reports involving data analysis should include the date, time, and identification of investigative personnel for the following events:

- Evidence seizure—should also include description of the physical condition of the seized evidence including, but not limited to, extraneous defects, hardware configuration, and Internet connections
- Digital imaging and verification—should also include the software employed
- Application of forensic software—including, but not limited to, text searching, restoration of files, indexing, file viewers, data carving, e-mail viewers, etc.
- Special techniques or unique problems encountered
- Consultation with outside sources

The two most popular forensic suites for Windows platforms, Access Data's *Forensic Tool Kit (FTK)* and Guidance Software's *EnCase*, are capable of logging all activities and creating comprehensive reports automatically.

Reporting Standards and Guidelines for Writing Reports

- A forensic report presents evidence that might support further investigation and, in some situations, be admissible in court, at an administrative hearing, or as an affidavit to support issuing an arrest or a search warrant.
- A report can also provide justification for collecting more evidence and be used at a probable cause hearing, as evidence in a grand jury hearing, or at a motion hearing in civil or criminal cases.

Reporting Standards and Guidelines for Writing Reports

Types of Reports

- Digital forensics examiners are required to create different types of reports, such as a formal report consisting of facts from your findings, a preliminary written or verbal report to your attorney, and an examination plan for the attorney who has retained you.
- An **examination plan** is a document that serves as a guideline for knowing what questions to expect when you're testifying.
- Your attorney uses the examination plan as an outline and a guide for your testimony.
- You can propose changes to clarify or define information or to include substantive information the attorney might have omitted. You can also use the examination plan to help your attorney learn the terms and functions used in digital forensics.
- A **verbal report** is less structured than a written report.
- Typically, it takes place in an attorney's office, where the attorney requests the consultant's report.
- An expert hired as a trial consultant uses verbal reports often.
- Keep in mind that others can't force your attorney to repeat what you've told him or her in a verbal report.

Reporting Standards and Guidelines for Writing Reports

A verbal report is usually a preliminary report and addresses areas of investigation yet to be completed, such as the following:

- Tests that haven't been concluded
- Interrogatories that the lawyer might want to address to opposing parties
- Document production, either requests for production (to parties)
- Determining who should be deposed and the plan for deposing them

With **preliminary reports**, mention to your client that your factual statement and opinion are still tentative and subject to change as more information comes in.

A written report is frequently an affidavit or a declaration. Because this type of report is sworn to under oath (and penalty of perjury or comparable false-swearing statute), it demands attention to detail, carefully limiting what you write, and thorough documentation and support of what you write. See the following section for more guidelines on written reports.

Reporting Standards and Guidelines for Writing Reports

- The method for expressing an opinion is to have an attorney frame a hypothetical question based on available factual evidence.
- The law requires that an expert who doesn't have personal knowledge about the system or occurrence must state opinions by response to hypothetical questions, which ask the expert witness to express an opinion based on hypothetical facts without referring to a particular system or situation.
- In this regard, you as a forensics investigator (an expert witness) differ from an ordinary witness.
- You didn't see or hear the incident in dispute; you're giving evidence as an opinion based on professional knowledge and experience, even if you might never have seen the system, data, or scene.

Reporting Standards and Guidelines for Writing Reports

- Although the rules of evidence have relaxed requirements on the way an expert renders an opinion, structuring hypothetical questions for your own use helps ensure that you're basing your opinion on facts expected to be supported by evidence.
- State the facts needed to answer the question, and don't include any unnecessary facts.
- You might want to address alternative facts, however, if they allow your opinion to remain the same.
- The expression "alternative facts" might seem contradictory, but it simply means competing facts.
- In a civil case, if there weren't alternative possible facts, the case wouldn't be at trial; it would have been decided at summary judgment.

Reporting Standards and Guidelines for Writing Reports

As an expert witness, you can testify to an opinion or a conclusion if these basic conditions are met:

- The opinion, inferences, or conclusions depend on special knowledge, skill, or training not within the ordinary experience of lay witnesses or jurors.
- The witness must be shown to be qualified as a true expert in the field (which is why a curriculum vitae is important).
- The witness must testify to a reasonable degree of certainty (probability) about his or her opinion, inference, or conclusion.
- At minimum, expert witnesses must know the relevant data (facts) on which their opinion, inference, or conclusion is based, and they must be prepared to testify in response to a hypothetical question that sets forth the underlying evidence.

Reporting Standards and Guidelines for Writing Reports

The following list shows additional items to include in your report:

- Summarize your billing to date and estimate costs to complete the effort.
- Identify the tentative conclusion (rather than the preliminary conclusion).
- Identify areas for further investigation and get confirmation from the attorney on the scope of your examination.

Report Writing for High-Tech Investigations

Report Structure

A report usually includes the sections shown in the following list, although the order varies depending on organizational guidelines or case requirements:

- Abstract (or summary)
- Table of contents
- Body of report
- Conclusion
- References
- Glossary
- Acknowledgments
- Appendixes

Report Writing for High-Tech Investigations

- Each section should have a title indicating what you're discussing, so make sure it conveys the essential point of the section. If the report is long and complex, you should include an abstract.
- Typically, more people read the abstract than the entire report, so writing one for your report is important. The abstract and table of contents give readers an overview of the report and its points so that they can decide what parts they need to review.
- An abstract simply condenses the report's key points to focus on the essential information.
- The body consists of the introduction and discussion sections. The introduction should state the report's purpose and show that you're aware of its terms of reference. You should also state any methods used and any limitations and indicate how the report is structured. Introduce the problem, moving from broader issues to the specific problem, finishing the introduction with the precise aims of the report (key questions). Craft this introduction carefully, setting up the processes you used to develop the information in logical order.
- Refer to *relevant* facts, ideas, and theories as well as related research by other authors. Organize discussion sections logically under headings to reflect how you classify information and to ensure that your information remains relevant to the investigation.

Report Writing for High-Tech Investigations

- Two other main sections are the conclusion and supporting materials (references and appendixes).
- The conclusion starts by referring to the report's purpose, states the main points, draws conclusions, and possibly renders an opinion.
- References and appendixes list the supporting material to which your work refers.

- Follow a style manual's guidelines on format for presenting references, such as
  1. *Gregg Reference Manual: A Manual of Style, Grammar, Usage, and Formatting*;
  2. *The Chicago Manual of Style: The Essential Guide for Writers, Editors, and Publishers*;
  3. *MLA Style Manual and*
  4. *Guide to Scholarly Publishing* from the Modern Language Association.

- Appendixes provide additional resource material not included in the body of the report.

Report Writing for High-Tech Investigations

Writing Reports Clearly

To produce clear, concise reports, you should assess the quality of your writing, using the following criteria:

- *Communicative quality*—Is it easy to read? Think of your readers and how to make the report appealing to them.
- *Ideas and organization*—Is the information relevant and clearly organized?
- *Grammar and vocabulary*—Is the language simple and direct so that the meaning is clear and the text isn't repetitive? However, technical terms should be used consistently; you shouldn't try to use variety for these terms. Using different words for the same thing might raise questions.
- *Punctuation and spelling*—Are they accurate and consistent?

Report Writing for High-Tech Investigations

Designing the Layout and Presentation of Reports

- Layout and presentation involve many factors, including using clear titles and section headings.
- A numbering system is also part of the layout.
- Typically, report writers use one of two numbering systems: decimal numbering or legal-sequential numbering.
- After you choose a system, be sure to follow it consistently throughout the report.
- A report using the decimal numbering system divides material into sections and restarts numbering with each main section, as shown in the following example.
- With this system, readers can scan the headings and understand how one part of the report relates to the other.
- Also include following:
  - Explaining Examination and Data Collection Methods
  - Including Calculations
  - Providing for Uncertainty and Error Analysis
  - Explaining Results and Conclusions
  - Providing References
  - Including Appendixes

Generating Report Findings with Forensics Software Tools

- With many forensics software tools, log files of analysis activities and reports can be created that provide information about the findings for a case.
- Although forensics software reports what was found and where, remember that it's your responsibility to explain the significance of the evidence you recover and, if necessary, define any limitations or uncertainty that applies to your findings.
- These reports and logs are typically in text, word processing, spreadsheet, or HTML format.

Generating Report Findings with Forensics Software Tools

Reports should answer the questions you were retained to answer and keep information that doesn't support specific questions to a minimum.

- A well-defined report structure contributes to readers' ability to understand the information you're communicating. Make sure your report includes clearly labelled sections and follows a numbering scheme consistently. Ensure that supporting materials, such as figures and tables, are numbered and labelled clearly.

- Clarity of writing is critical to a report's success. Make sure to include signposts to give readers clues about the sequence of information, and avoid vague wording, jargon, and slang.

- Convey a tone of objectivity, and be detached in your observations. Synthesize what has (and has not) been learned about the problem and what the information means.

Thank you !

BITS Pilani

Prof. Pradnya Kashikar

WILP-CSIS

BITS Pilani
Pilani Campus

innovate achieve lead

BITS Pilani

Pilani Campus

SS ZG588 - Cyber Crimes, Forensics and Incident Handling

Contact Session - 15

Course Objectives

No	Description
CO1	Enhancing awareness of recent Cyber Crime trends and learn Investigating Cyber Crimes
CO2	Introduce Cyberspace Infrastructure attacks and handling Organization Cybersecurity Issues
CO3	Understand Digital Forensics Process, Models, Analysis and Validation, Incident Detection and Response

Text Book(s)

innovate achieve lead

T1	Computer Forensics and Cyber Crime - An Introduction 3rd Edition by Marjie T. Britz, Ph.D., Professor of Criminal Justice, Clemson University
T2	Bill Nelson, A. Philips, F. Enfinger, C. K. Steuart, Computer Forensics and Investigations, Course Technology (Cengage Learning), Indian edition, 2009
T3	Incident Response & Computer Forensics, 3rd Edition by Jason T. Luttgens and Matthew Pepe and Kevin Mandia
R1	Guide to Computer Forensics and Investigations: Processing Digital Evidence 5th Edition by Bill Nelson, Amelia Phillips and Christopher Steuart
R2	The Basics of Digital Forensics, by John Sammons
R3	Computer Network Security and Cyber Ethics 4th Edition, by Joseph Migga Kizza
R4	Computer Forensics_ Investigating Network Intrusions and Cyber Crime: EC-Council Press

Learning Outcomes -

No	Learning Outcomes
LO1	Fundamental understanding and Information on Cyber Crimes, Digital Forensics Objectives and Incident Detection and Response Reports.
LO2	Learn on how to prepare investigation on computer-related incidents or crimes and summarize.
LO3	Understand on digital forensics process, models and analysis by taking a systematic approach
LO4	Explore on evaluating needs, validating and testing digital forensics tools, Generating Incident Report Findings, and Emerging Cybercrime Trends and Issues

Module 14 - Emerging Cybercrime Trends, Recommendations and Practical Issues

14.1 Cybercrime Challenges, Issues, Recommendation and Suggestion in Indian context

14.2 Traditional Problems and Recommendations

14.3 Additional Approaches to Internet Crime

14.4 Future Trends and Emerging Concerns

15	Emerging Cybercrime Trends, Recommendations and Practical Issues	Cybercrime Challenges, Issues, Recommendation and Suggestion in Indian context	T1, R2
		Traditional Problems and Recommendations	
		Additional Approaches to Internet Crime	
		Future Trends and Emerging Concerns	

Cybercrime challenges & issues; Recommendation and Suggestion in Indian context

1. Refer a research paper sent to you.

2. The Challenges of Cybercrime – YouTube

Traditional Problems and Recommendations

- For the most part, the investigation and prosecution of computer-related crime has been hindered by a lack of nomenclature, due primarily to the reluctance of the Supreme Court to interpret emerging legislative actions.
- As such, investigators, prosecutors, and even trial courts have no basis for determining the legality of either questioned behaviour or law enforcement actions.
- Thus, universal definitions of computer-related crime and computer privacy must be established.

Traditional Problems and Recommendations

Establishing Technology-Neutral Legislation

- The development of computer-specific legislation must be undertaken in a manner that ensures uniformity in application and interpretation irrespective of jurisdictional climate.
- At the same time, emerging legislation must be generic enough to encompass advances in technology, assuring that application to tomorrow's technology is possible.
- Just as the applicability of the Wire Act has been questioned regarding its implementation for Internet crimes committed via cable modems (as opposed to telephone communications), the advent of wireless communications poses new questions altogether.
- Thus, legislators should develop technology-neutral legislation, which narrowly defines (and emphasizes) elemental issues like intent, while providing a broad platform for methodology employed.
- In addition, such legislation should identify traditional challenges in the analysis of digital evidence and provide justifications for the potential of protracted examination of computer materials (e.g., voluminous nature of computer containers, password-protected information, damaged media, and lack of resources).

Traditional Problems and Recommendations

Establishing Accountability for Internet Users

- Legislation must also be enacted that ensures confidentiality for those who seek it for legitimate purposes, but that denies blanket anonymity.
- This would allow legitimate surfers the luxury to browse the Web anonymously for all practical purposes, safely concealing their identities from criminals and government officials alike, while providing a mechanism for law enforcement to pursue those predators, criminals, or terrorists who attempt to mask their illegitimate activities.
- This is especially important in the wake of the events of 9/11. It is imperative that our interest in the globalization of information and communication not supersede the interests of national security.
- Unfortunately, such a balance is difficult to achieve.

Traditional Problems and Recommendations

Increasing Public Awareness and Research Capabilities

- Traditionally, computer-related crime has not garnered significant attention from most sectors of society which fail to recognize the insidious nature of the phenomenon.
- Thus, a comprehensive effort must be undertaken to educate all levels of the community, including politicians, teachers, law enforcement officials, individual consumers, and children.
- Such awareness must include the potential of computer crime, creating an appreciation of the dangers inherent in such activities (i.e., everyone must see both the threat and the exponential growth associated with computer crime).
- Once established, this collective understanding should result in additional funding for computer-related initiatives and increase public reporting and cooperation.
- In addition, baseline measurements of prevalence and typologies of offenders should be established.

Traditional Problems and Recommendations

Increasing Interagency and Intradepartmental Cooperation

- Although the law enforcement culture has long been characterized by a lack of communication and cooperation among agencies, the lack of resources available to combat computer- related crime mandates increasing the number of multijurisdictional task forces and central reporting stations.
- While law enforcement agencies have recently formed such collaborative efforts, much is left to be done.
- Local agencies, in particular, should develop formal alliances with better funded and better trained state and federal agencies.

Traditional Problems and Recommendations

Developing Relationships between Investigative Agencies and the Private Sector

- All levels of the law enforcement community must also seek out and establish partnerships with the high-tech industry for a variety of reasons.
- First and foremost, law enforcement agencies will remain overworked, understaffed, poorly funded, and technologically deficient due to the continuing struggle for external funding. High-tech corporations, with their unlimited resources and highly trained personnel, may alleviate some of this problem by donating equipment and expertise to their local agencies.
- In addition, these entities may be called upon to develop software requisite to the law enforcement mission like IP tracking systems, editing and searching tools, and general investigative utilities.
- Partnerships which emphasize ethical accountability may also result in the development of materials which preclude the proliferation of inappropriate material through filtering and professional accountability.
- For example, the Electronic Commerce and Consumer Protection Group (which includes AOL, American Express, AT&T, Dell, Visa, Microsoft, IBM, etc.) is currently developing jurisdictional regulations to address consumer protection in a global marketplace.
- Their goals include the development of a code of conduct among e-tailers to facilitate e-commerce within a secure environment, and the retention of data to identify online predators

Traditional Problems and Recommendations

Developing International Cooperation

- Traditionally, several problems and troublesome questions have erupted concerning international procedures for the preservation of digital evidence.
- One of the most ambiguous areas involves the search and seizure of computer networks, as it is questionable whether, and to what extent, the right to search and seize a specific computer installation includes the right to search databases that are accessible by this installation but that are situated in other premises.
- The importance of such questions has reached astronomical proportions, as more and more individuals and corporations are implementing off-site storage databases to protect proprietary information.
- Thus, pivotal questions including the international sovereignty over the stored data and the accessibility of the information by investigating agencies remain unresolved.

Traditional Problems and Recommendations

Standardization of Accreditation or Expertise

- Due to the inexperience of legislative authorities and the inconsistency of judicial estimation, law enforcement authorities must establish a standard of accreditation and/or expertise of forensic methodologies and examiners.
- As in any emerging discipline, such standardization would decrease Daubert/Frye challenges to the recovery of digital evidence.
- Such challenges issued to emerging or untested scientific methods require a variety of thresholds, many of which have not yet been achieved in the emerging field of computer forensics.
- Thus, the discipline should attempt to identify and address each of the following questions:
    1. Can the techniques involved in data recovery be empirically tested?
    2. Have they been subjected to peer review and publication?
    3. Does the theory or technique have the potential for a high rate of error?
    4. Does the technique enjoy a general acceptance within the scientific community?

Traditional Problems and Recommendations

Miscellaneous

- As more and more individuals are using the Internet in their daily lives, it is critical for law enforcement to establish a visible presence on the Web.
- All departments, for example, should create and maintain a departmental Web page, illustrating their commitment to contemporary problems and providing a mechanism for community input.
- In this way, technology can be used to foster positive relations with the community and establish a system conducive to anonymous reporting (i.e., the same perception of anonymity that encourages criminals creates a comfort zone for those wishing to come forward with information but are reluctant to be identified).
- In addition, it allows departments to publicize their mission statements, promote departmental initiatives, enhance their ability to update community residents (including the photographic display of missing persons and wanted individuals), and provide a mechanism for communication in emergency situations (i.e., severe weather, etc.).

Additional Approaches To Internet Crime

- Computer crime is increasing at an exponential rate as criminals move more of their operations to the cyberworld.
- Of significant concern to authorities is the increase in money laundering, organized crime, and denial of service attacks as they threaten consumer confidence, and through extension, the global economy. Unfortunately, the borderless nature of the Internet has made it extraordinarily difficult to police.
- Thus, law enforcement authorities must partner with cybercitizens to properly address the phenomenon.
- In a perfect world, such collaboration would be heartily embraced by both citizens and corporate entities.

Additional Approaches To Internet Crime

However, private and capitalist interests often discourage such participation, and legislation is needed to overcome such reluctance. Such legislation should address the following areas:

• **Utilization of existing forfeiture statutes**—

- Federal legislation provides for the seizure of all assets of a legitimate business which facilitates the laundering of money obtained in an illegal enterprise.
- Even legitimate revenue can be seized if it is intermingled with laundered funds as it serves to conceal or otherwise disguise illegal money.

Additional Approaches To Internet Crime

- **Accountability of ISP ’s hosts and e-businesses—**

- Legislation must include new accountability statutes which enable authorities to civilly punish ISPs, hosts, or other e-businesses which facilitate illegal activity.
- As the standard of proof in such cases is relatively low (i.e., preponderance of the evidence), online businesses should comply.
- In particular, legislation which mandates accountability of SMTP servers should be developed to reduce the number of DOS attacks.
- To wit, the imposition of monetary fines should be levied against operators running SMTP servers with open relays or unrestricted, anonymous-access FTP servers.

Additional Approaches To Internet Crime

- **Know your customer—**

- Legislation must encourage a grassroots approach in the business community. Those engaged in e-commerce need to be educated and recognize the dangers associated with organized crime's infiltration of e-commerce.

- "Know your customer" statutes should require businesses to
  (1) know their customers;
  (2) assure their identity; and
  (3) require transparency.

Future Trends and Emerging Concerns

- The identification, investigation, and prosecution of computer-related crime are accompanied by a myriad of unique problems.
- Unfortunately, it is anticipated that these problems will be further exacerbated by emerging technologies.
- Legal questions regarding decency and privacy are but two of the issues sure to plague future administrators.
- Advances in wireless communications and encryption technology will further complicate the legal landscape, and the increasing convergence of audio, video, and digital data will present new challenges for criminal investigators.

Future Trends and Emerging Concerns

Wireless Communications

- Although cellular telephones have been around for quite some time, the reduction of costs and the increase in communication quality have vastly expanded their audience and created a society increasingly reliant on technology.
- Fortunately for law enforcement, tapping into wireless communications has proven far easier than traditional telephonic exchanges for two primary reasons:

  (1) It is easier to identify a suspect's cellular provider than to predict which pay phone a suspect will use; and,

  (2) the Supreme Court has refused to recognize an expectation of privacy in wireless communications.

Future Trends and Emerging Concerns

- The increase in wireless communications has also complicated investigations and developed new avenues for criminal behaviour.
- It is anticipated that the increased proliferation of wireless devices will be accompanied by an increase in viruses and contaminants for all handheld devices.
- Spam, often used as a delivery vehicle for malware, will also increase.
- While the first cell phone virus was created to prove that this could be done, others are far more insidious.
- Like computer viruses, cell phone viruses are represented as unwanted executable files that are contagious after infection.
- They are spread via smart phones with connection and data capabilities in one of three ways: Internet downloads, Bluetooth wireless connection, and multimedia messaging service.
- Fortunately, wide-scale infection has not been realized due to the large number of proprietary operating systems.
- However, it is anticipated that large-scale infections will rise as universal operating systems emerge.

Future Trends and Emerging Concerns

Data Hiding: Remote Storage, Encryption, and the Like

- The increase of remote storage facilities (i.e., virtual islands of information unattached and, thus, unregulated by a sovereign state), for example, may be especially troublesome to law enforcement authorities for a variety of reasons.
- In addition to the passage of legislation targeting corporate facilitators of online crime, the government must continue to educate the public.
- To reiterate, the war against computer-related crime must be fought on all fronts.

Future Trends and Emerging Concerns

Tips for Individuals

- Use a blended data security platform which incorporates antivirus, firewall, intrusion detection, and vulnerability management. This will significantly enhance your level of security and identify if the computer has been compromised.
- Update security patches and virus definitions as they emerge to keep the protection current.
- Create passwords which include letters and numbers, avoiding words which appear in the dictionary.
- Change passwords often.
- Never view, open, or execute any e-mail attachment unless you are sure of its contents and are expecting it.
- Don’t fall prey to phishing scams and hoaxes.

Future Trends and Emerging Concerns

Governing Decency and Virtual Pornography

- Courts have been increasingly cautious and consistently ambiguous regarding the level of protection afforded online communications and in defining indecency and vulgarity on the Web.

Data Mining and Increased Interoperability

- The evolution of computer crime investigations has revealed that the prevention and detection of computer-related criminal activity is extremely difficult.
- Criminals, not bound by considerations of law and cultural norms, have employed various methods to perpetrate their nefarious schemes.
- In response, law enforcement agencies have had to employ similar tactics to identify and thwart their endeavours.
- Investigators should employ the following practices to reduce false positives:
  - Removal of duplicate records
  - Normalization or standardization of data appearance
  - Accounting for missing data points
  - Removal of unnecessary data fields
  - Identification of anomalous data points

Thank you !

BITS Pilani

Prof. Pradnya Kashikar

WILP-CSIS

BITS Pilani
Pilani Campus

innovate achieve lead

BITS Pilani

Pilani Campus

SS ZG588 - Cyber Crimes, Forensics and Incident Handling

Contact Session - 16

Course Objectives

No	Description
CO1	Enhancing awareness of recent Cyber Crime trends and learn Investigating Cyber Crimes
CO2	Introduce Cyberspace Infrastructure attacks and handling Organization Cybersecurity Issues
CO3	Understand Digital Forensics Process, Models, Analysis and Validation, Incident Detection and Response

Text Book(s)

innovate achieve lead

T1	Computer Forensics and Cyber Crime - An Introduction 3rd Edition by Marjie T. Britz, Ph.D., Professor of Criminal Justice, Clemson University
T2	Bill Nelson, A. Philips, F. Enfinger, C. K. Steuart, Computer Forensics and Investigations, Course Technology (Cengage Learning), Indian edition, 2009
T3	Incident Response & Computer Forensics, 3rd Edition by Jason T. Luttgens and Matthew Pepe and Kevin Mandia
R1	Guide to Computer Forensics and Investigations: Processing Digital Evidence 5th Edition by Bill Nelson, Amelia Phillips and Christopher Steuart
R2	The Basics of Digital Forensics, by John Sammons
R3	Computer Network Security and Cyber Ethics 4th Edition, by Joseph Migga Kizza
R4	Computer Forensics_ Investigating Network Intrusions and Cyber Crime: EC-Council Press

Learning Outcomes -

No	Learning Outcomes
LO1	Fundamental understanding and Information on Cyber Crimes, Digital Forensics Objectives and Incident Detection and Response Reports.
LO2	Learn on how to prepare investigation on computer-related incidents or crimes and summarize.
LO3	Understand on digital forensics process, models and analysis by taking a systematic approach
LO4	Explore on evaluating needs, validating and testing digital forensics tools, Generating Incident Report Findings, and Emerging Cybercrime Trends and Issues

Module 15 - Miscellaneous Topics

15.1 Data Protection Law In The Age Of Big Data And AI

15.2 Malicious Cyber Activity Distribution, Attribution and Jurisdiction

15.3 Information Privacy, Law Enforcement and Privacy Law Fundamentals

15.4 Models of Internet Governance

16	Miscellaneous Topics	**Data Protection Law In The Age Of Big Data And AI**	https://papers.ssrn.com/
		Malicious Cyber Activity Distribution, Attribution and Jurisdiction	https://www.ardcindia.org/ccpwc/
		Information Privacy, Law Enforcement and Privacy Law Fundamentals	https://www.eccouncil.org/what-is-digital-forensics/
		Models of Internet Governance	

References

Law Assignment 4 Cyber Crime Case – YouTube

https://www.youtube.com/watch?v=Pm1Wgd9bbOk

Big Data Analysis and Artificial Intelligence – YouTube

Big data for better cyber security – YouTube

Big Data Security Analytics - Key Findings of the Study - YouTube

Thank you !