

MODULE 1

CYBER 20MCA267 FORENSICS



What is Forensic (Forensic Science)

- Related to scientific methods of solving crimes, involving examining the objects or substances that are involved in the crime:
- Scientific tests or techniques used in connection with the detection of crime
- Forensic(science) - use of scientific methods(proven) or expertise to investigate crimes or examine evidence that might be presented in a court of law
 - diverse array of disciplines, from fingerprint to DNA analysis

Challenges

- How do you ensure that forensic methods produce reliable results?
- How do you communicate findings to a jury or other nonexperts in a way that is accurate and understandable?
- How do you keep up with new technology without falling behind on casework?

What is Cyber (Cyberspace)

- The term **cyber** or **cyberspace** has today come to signify everything related to computers:

The Internet, websites, data, emails, networks, software, data storage devices (such as hard disks, USB disks etc) and

even Airplanes, ATM machines, Baby monitors, Biometric devices, Bitcoin wallets, Cars, CCTV cameras, Drones, Gaming consoles, Health trackers, Medical devices, Power plants, Self-aiming rifles, Ships, Smart-watches, Smartphones, Cloud & more.

"The modern thief can steal more with a computer than with a gun. Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb".



Cyber forensics

Cyber forensics, also called **digital or computer forensics**, is a field of technology that uses investigation techniques to help identify, collect, and store evidence from an electronic device.

Cyber forensics

- Computer forensics / Digital forensics
- application of investigation and analysis techniques to gather and preserve evidence from a particular computing device in a way that is suitable for presentation in a court of law
- process of extracting data as proof for a crime (that involves electronic devices) while following proper investigation rules to nab the culprit by presenting the evidence to the court
- The main aim of cyber forensics is to maintain the thread of evidence and documentation to find out who did the crime digitally

- It is a science of finding evidence from digital media
 - It can recover deleted files, chat logs, emails, etc
 - It can also get deleted SMS, Phone calls.
 - It can get recorded audio of phone conversations
 - It can determine which user used which system and for how much time.
 - It can identify which user ran which program.
 - It can detect whether image/video is real or fake

Objectives of cyber forensics

- 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.

- 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.

Process of Digital forensics

Identification

- Identify the purpose of investigation
- Identify the resources required

Preservation

- Data is isolate, secure and preserve

Analysis

- Identify tool and techniques to use
- Process data
- Interpret analysis results

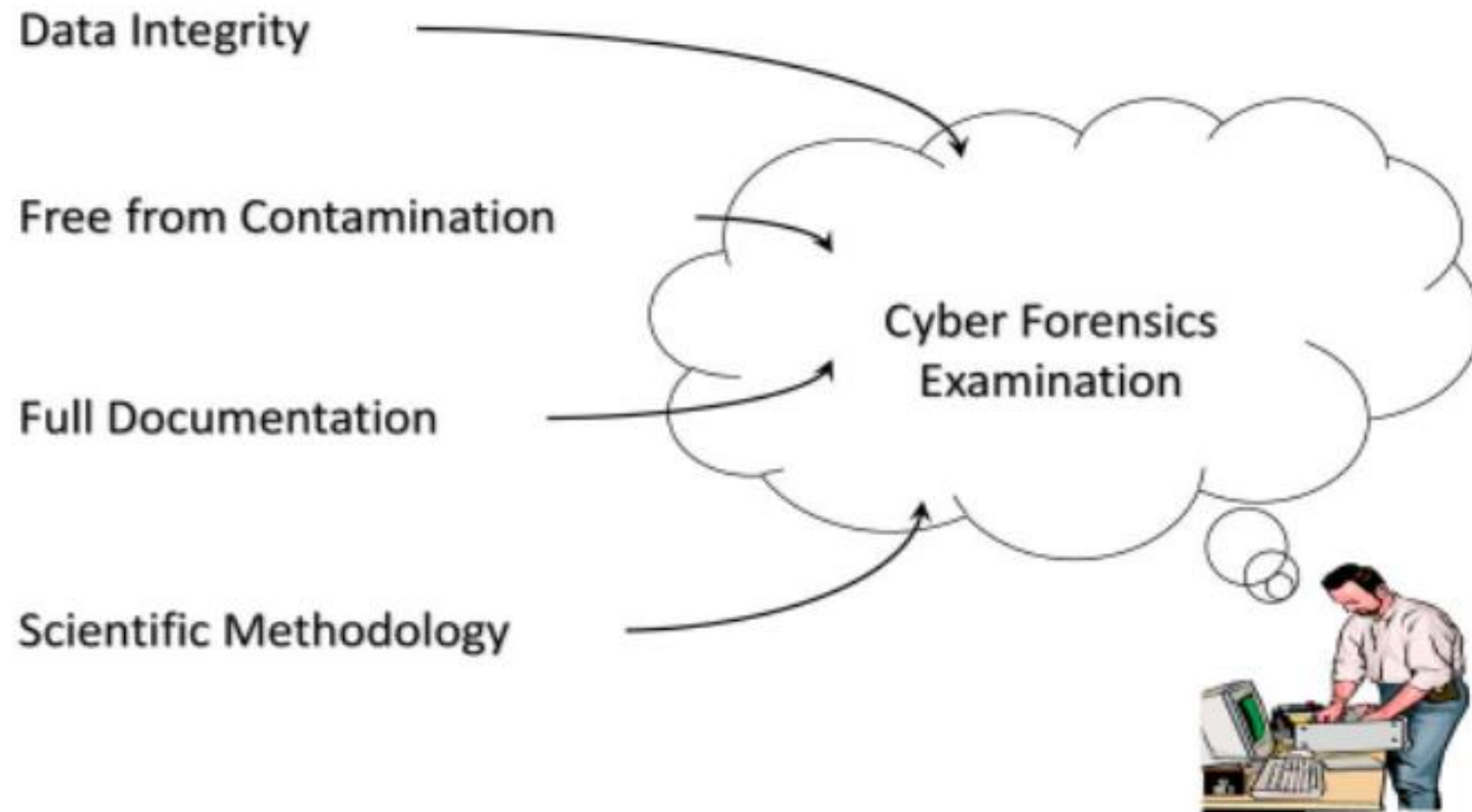
Documentation

- Documentation of the crime scene along with photographing, sketching, and crime-scene mapping

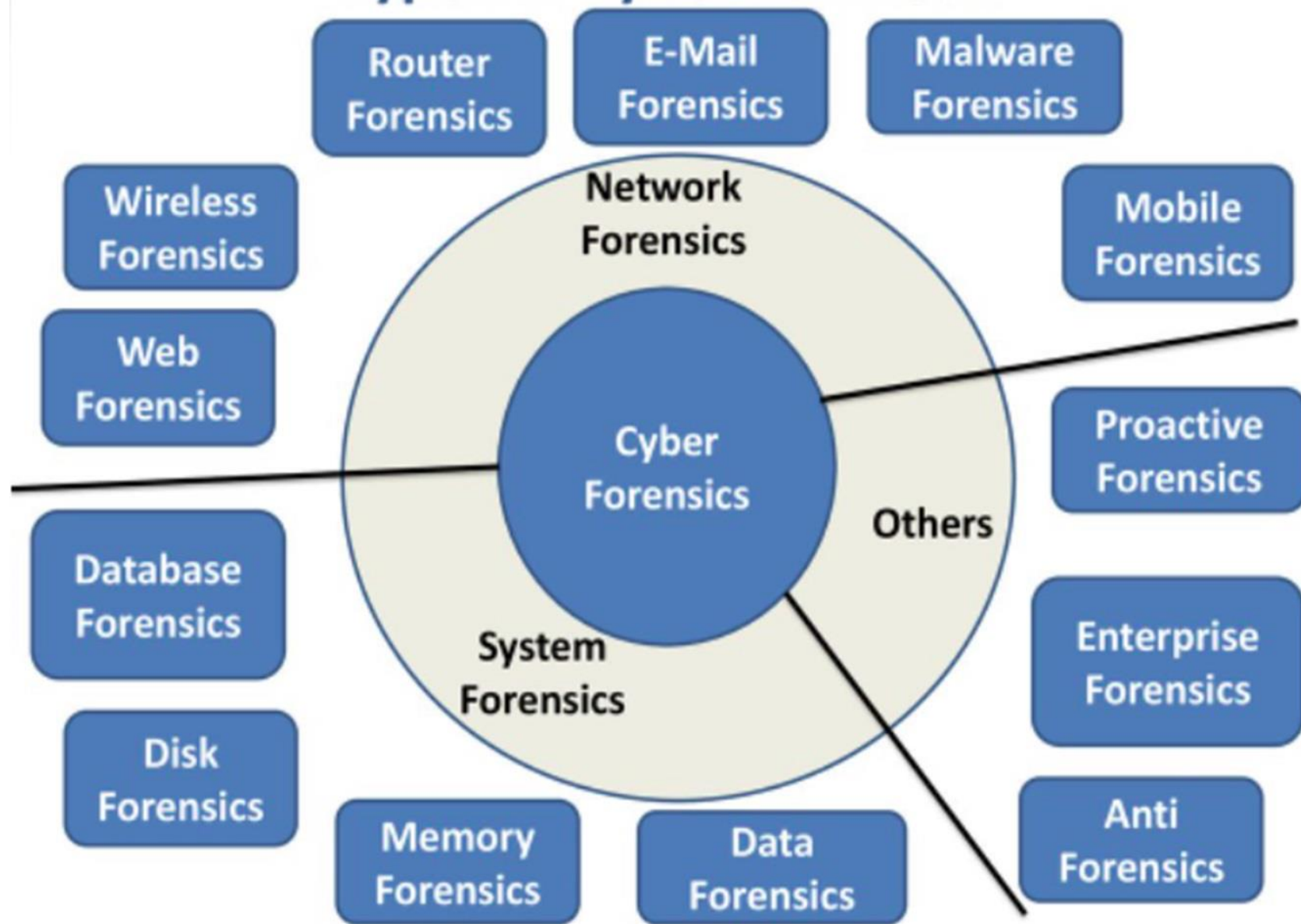
Presentation

- Process of summarization and explanation of conclusions is done with the help to gather facts.

Cyber Forensics Principles



Types of Cyber Forensics



Cyber Forensics – Evidence examp^l



Cyber/Digital Forensics

- The application of computer science and investigative procedures for a legal purpose involving the analysis of digital evidence after proper search authority, chain of custody, validation with mathematics, use of validated tools, repeatability, reporting, and possible expert presentation.

- In October 2012, an ISO standard for digital forensics was ratified - **ISO 27037** Information technology - Security techniques
 - Guidelines for identification, collection, acquisition and preservation of digital evidence

Digital Forensics Government bodies

- FBI Computer Analysis and Response Team (CART) was formed in 1984 to handle cases involving digital evidence.
- Indian Computer Emergency Response Team (CERT-IN or ICERT) -2004

An Overview of a Computer

Crime

- Computers can contain information that helps law enforcement determine:
 - Chain of events leading to a crime
 - Evidence that can lead to a conviction
- Law enforcement officers should follow proper procedure when acquiring the evidence
 - Digital evidence can be easily altered by an overeager investigator
- A potential challenge: information on hard disks might be password protected so forensics tools may be need to be used in your investigation



Cybercrimes

A cyber crime is any criminal activity which takes place on or over the medium of computers or internet or other technology recognised by the Information Technology Act

- <https://cybercrime.gov.in/>

A simple yet sturdy definition of cybercrime would be "**unlawful acts wherein the computer is either a tool or a target or both**".

Cyber crimes are any crimes that involve a computer and a network.

In some cases, the computer may have been used in order to commit the crime, and in other cases, the computer may have been the target of the crime.

General Categories of cybercrime

Crimes against
people



Crimes against
property



Crimes against the
government



General Categories of cybercrime

- **Individual** Cybercrimes against individuals involve crimes like online harassment, distribution and trafficking of child pornography, manipulation of personal information, use of obscene data, and identity theft for personal benefit.
- **Property**- Usage, and transmission of harmful programs, theft of information and data from financial institutions, trespassing cyberspace, computer vandalism, and unauthorized possession of information digitally, are some of the crimes under the property.

➤ **Government**- The crimes that come under this are cyber terrorism, manipulation, threats, and misuse of power against the Government and citizens. Groups or Individuals terrorizing Government websites is when this form of cyber terrorism occurs.

1. Cyber Crimes against Persons:

- Harassment via E-Mails: It is very common type of harassment through sending letters, attachments of files & folders i.e. via e-mails. At present harassment is common as usage of social sites i.e. Facebook, Twitter etc. increasing day by day.
- **Cyber-Stalking:** It means expressed or implied a physical threat that creates fear through the use to computer technology such as internet, e-mail, phones, text messages, webcam, websites or videos.
- **Dissemination of Obscene Material:** It includes Indecent exposure/ Pornography (basically child pornography), hosting of web site containing these prohibited materials. These obscene matters may cause harm to the mind of the adolescent and tend to deprave or corrupt their mind.

- **Defamation:** It is an act of imputing any person with intent to lower down the dignity of the person by hacking his mail account and sending some mails with using vulgar language to unknown persons mail account.
- **Hacking:** It means unauthorized control/access over computer system and act of hacking completely destroys the whole data as well as computer programmes. Hackers usually hacks telecommunication and mobile network.
- **Cracking:** It is amongst the gravest cyber crimes known till date. It is a dreadful feeling to know that a stranger has broken into your computer systems without your knowledge and consent and has tampered with precious confidential data and information.

- **E-Mail Spoofing:** A spoofed e-mail may be said to be one, which misrepresents its origin. It shows it's origin to be different from which actually it originates.
- **SMS Spoofing:** Spoofing is a blocking through spam which means the unwanted uninvited messages. Here an offender steals identity of another in the form of mobile phone number and sending SMS via internet and receiver gets the SMS from the mobile phone number of the victim. It is very serious cyber crime against any individual.
- **Carding:** It means false ATM cards i.e. Debit and Credit cards used by criminals for their monetary benefits through withdrawing money from the victim's bank account mala-fidely. There is always unauthorized use of ATM cards in this type of cyber crimes.

- **Cheating & Fraud:** It means the person who is doing the act of cyber crime i.e. stealing password and data storage has done it with having guilty mind which leads to fraud and cheating.
- **Child Pornography:** It involves the use of computer networks to create, distribute, or access materials that sexually exploit underage children.
- **Assault by Threat:** refers to threatening a person with fear for their lives or lives of their families through the use of a computer network i.e. E-mail, videos or phones.

. Crimes Against Persons Property:

- **Intellectual Property Crimes:** Intellectual property consists of a bundle of rights. Any unlawful act by which the owner is deprived completely or partially of his rights is an offence.
- The common form of IPR violation may be said to be software piracy, infringement of copyright, trademark, patents, designs and service mark violation, theft of computer source code, etc.
- **Cyber Squatting:** It means where two persons claim for the same Domain Name either by claiming that they had registered the name first on by right of using it before the other or using something similar to that previously. For example two similar names i.e. www.yahoo.com and www.yaahoo.com.

- **Cyber Vandalism:** Vandalism means deliberately destroying or damaging property of another.
- Thus cyber vandalism means destroying or damaging the data when a network service is stopped or disrupted. It may include within its purview any kind of physical harm done to the computer of any person.
- These acts may take the form of the theft of a computer, some part of a computer or a peripheral attached to the computer.
- **Hacking Computer System:** Hacktivism attacks those included Famous Twitter, blogging platform by unauthorized access/control over the computer.
- Due to the hacking activity there will be loss of data as well as computer. Also research especially indicates that those attacks were not mainly intended for financial gain too and to diminish the reputation of particular person or company.

- **Transmitting Virus:** Viruses are programs that attach themselves to a computer or a file and then circulate themselves to other files and to other computers on a network.
- They usually affect the data on a computer, either by altering or deleting it. Worm attacks plays major role in affecting the computerize system of the individuals.
- **Cyber Trespass:** It means to access someone's computer without the right authorization of the owner and does not disturb, alter, misuse, or damage data or system by using wireless internet connection.

- **Internet Time Thefts:** Basically, Internet time theft comes under hacking. It is the use by an unauthorized person, of the Internet hours paid for by another person.
- The person who gets access to someone else's ISP user ID and password, either by hacking or by gaining access to it by illegal means, uses it to access the Internet without the other person's knowledge.
- You can identify time theft if your Internet time has to be recharged often, despite infrequent usage.

. Cybercrimes Against Government:

- **Cyber Terrorism:** Cyber terrorism is a major burning issue in the domestic as well as global concern. The common form of these terrorist attacks on the Internet is by distributed denial of service attacks, hate websites and hate e-mails, attacks on sensitive computer networks etc.
- Cyber terrorism activities endanger the sovereignty and integrity of the nation.
- **Cyber Warfare:** It refers to politically motivated hacking to conduct sabotage and espionage(spying). It is a form of information warfare sometimes seen as analogous to conventional warfare although this analogy is controversial for both its accuracy and its political motivation.

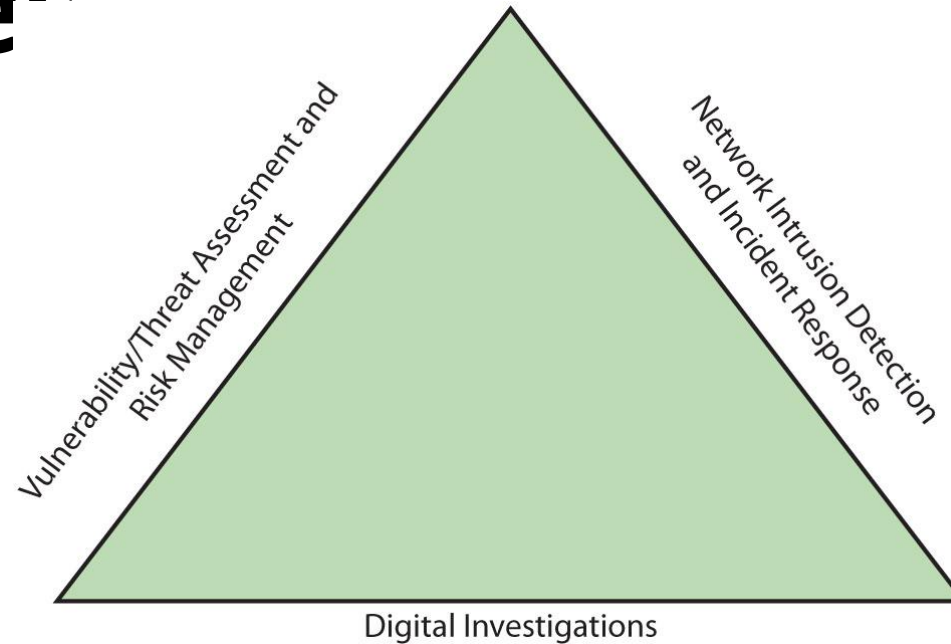
- **Cyberterrorism** is the use of the [Internet](#) to conduct violent acts that result in, or threaten, loss of life or significant bodily harm, in order to achieve political gains through [intimidation](#).
- It is also sometimes considered an act of Internet terrorism where [terrorist](#) activities, including acts of deliberate, large-scale disruption of computer networks, especially of personal computers attached to the Internet by means of tools such as [computer viruses](#), [computer worms](#), [phishing](#), and other malicious software and hardware methods and programming scripts.

- **Distribution of pirated software:** It means distributing pirated software from one computer to another intending to destroy the data and official records of the government.
- **Possession of Unauthorized Information:** It is very easy to access any information by the terrorists with the aid of internet and to possess that information for political, religious, social, ideological objectives.

Digital Forensics and Other Related

- **Disciplines** Investigating digital devices includes:
 - Collecting data securely
 - Examining suspect data to determine details such as origin and content
 - Presenting digital information to courts
 - Applying laws to digital device practices
- Digital forensics is different from **data recovery**
 - Which involves retrieving information that was deleted by mistake or lost during a power surge or server crash
- Forensics investigators often work as part of a team, known as the investigations triad

Digital Forensics and Other Related Discipline~



- Vulnerability/threat assessment and risk management
 - Tests and verifies the integrity of stand-alone workstations and network servers
- Network intrusion detection and incident response
 - Detects intruder attacks by using automated tools and monitoring network firewall logs
- Digital investigations
 - Manages investigations and conducts forensics analysis of systems suspected of containing evidence

Understanding Case Law

- Existing laws can't keep up with the rate of technological change
- When statutes don't exist, case law is used
 - Allows legal counsel to apply previous similar cases to current one in an effort to address ambiguity in laws
- Examiners must be familiar with recent court rulings on search and seizure in the electronic environment

Preparing for Digital Investigations

- Digital investigations fall into two categories:
 - Public-sector investigations
 - Private-sector investigations

Government agencies

Article 8 in the Charter of Rights of Canada

U.S. Fourth Amendment search
and seizure rules



Private organizations

Company policy violations

Litigation disputes



Public-sector and private-sector investigations

- Public-sector investigations involve government agencies responsible for criminal investigations and prosecution
- Fourth Amendment to the U.S. Constitution
 - Restrict government **search and seizure**
- The **Department** of Justice (DOJ) updates information on computer search and seizure regularly
- Private-sector investigations focus more on policy violations

Understanding Law Enforcement Agency Investigations

- When conducting public-sector investigations, you must understand laws on computer-related crimes including:
 - Standard legal processes
 - Guidelines on search and seizure
 - How to build a criminal case
- The Computer Fraud and Abuse Act was passed in 1986
 - Specific state laws were generally developed later

Following Legal Processes

- A criminal investigation usually begins when someone finds evidence of or witnesses a crime
 - Witness or victim makes an **allegation** to the police
- Police interview the complainant and writes a report about the crime
- Report is processed and management decides to start an investigation or log the information in a **police blotter**
 - **Blotter is a historical database of previous crimes**

- **Digital Evidence First Responder (DEFR)**
 - Arrives on an incident scene, assesses the situation, and takes precautions to acquire and preserve evidence
- **Digital Evidence Specialist (DES)**
 - Has the skill to analyze the data and determine when another specialist should be called in to assist
- **Affidavit** - a sworn statement of support of facts about or evidence of a crime
 - Must include **exhibits** that support the allegation

Understanding Private-Sector Investigations

- Private-sector investigations involve private companies and lawyers who address company policy violations and litigation disputes
 - Example: wrongful termination
- Businesses strive to minimize or eliminate litigation
- Private-sector crimes can involve:
 - E-mail harassment, falsification of data, gender and age discrimination, embezzlement, sabotage, and industrial espionage

- Businesses can reduce the risk of litigation by publishing and maintaining policies that employees find easy to read and follow
- Most important policies define rules for using the company's computers and networks
 - Known as an "Acceptable use policy"
- **Line of authority** - states who has the legal right to initiate an investigation, who can take possession of evidence, and who can have access to evidence

- Business can avoid litigation by displaying a **warning banner** on computer screens
 - Informs end users that the organization reserves the right to inspect computer systems and network traffic at will

 US Government Facility



You are about to access a United States government computer network that is intended for authorized users only. You should have no expectation of privacy in your use of this network. Use of this network constitutes consent to monitoring, retrieval, and disclosure of any information stored within the network for any purpose including criminal prosecution.

OK

- Sample text that can be used in internal warning banners:
 - Use of this system and network is for official business only
 - Systems and networks are subject to monitoring at any time by the owner
 - Using this system implies consent to monitoring by the owner
 - Unauthorized or illegal users of this system or network will be subject to discipline or prosecution

- Businesses are advised to specify an **authorized requester** who has the power to initiate investigations
- Examples of groups with authority
 - Corporate security investigations
 - Corporate ethics office
 - Corporate equal employment opportunity office
 - Internal auditing
 - The general counsel or legal department

- During private investigations, you search for evidence to support allegations of violations of a company's rules or an attack on its assets
- Three types of situations are common:
 - Abuse or misuse of computing assets
 - E-mail abuse
 - Internet abuse
- A private-sector investigator's job is to minimize risk to the company

- The distinction between personal and company computer property can be difficult with cell phones, smartphones, personal notebooks, and tablet computers
- Bring your own device (BYOD) environment
 - Some companies state that if you connect a personal device to the business network, it falls under the same rules as company property

Maintaining Professional

Conduct

- Professional conduct - includes ethics, morals, and standards of behavior
- An investigator must exhibit the highest level of professional behavior at all times
 - Maintain objectivity
 - Maintain credibility by maintaining confidentiality
- Investigators should also attend training to stay current with the latest technical changes in computer hardware and software, networking, and forensic tools

Preparing a Digital Forensics Investigation

- The role of digital forensics professional is to gather evidence to prove that a suspect committed a crime or violated a company policy
- Collect evidence that can be offered in court or at a corporate inquiry
 - Investigate the suspect's computer
 - Preserve the evidence on a different computer
- **Chain of custody**
 - Route the evidence takes from the time you find it until the case is closed or goes to court

An Overview of a Computer

Crime

- Computers can contain information that helps law enforcement determine:
 - Chain of events leading to a crime
 - Evidence that can lead to a conviction
- Law enforcement officers should follow proper procedure when acquiring the evidence
 - Digital evidence can be easily altered by an overeager investigator
- A potential challenge: information on hard disks might be password protected so forensics tools may be need to be used in your investigation



The police raided a suspected drug dealer's home and found a desktop computer, several USB drives (also called "flash drives" or "thumb drives"), a tablet computer, and a cell phone in a bedroom. The computer was "bagged and tagged," meaning it was placed in **evidence bags along with the storage media** and then labelled with tags as part of the search and seizure.

The lead detective on the case wants you to examine the computer and cell phone to find and organize data that could be evidence of a crime, such as files containing names of the drug dealer's contacts, text messages, and photos. The acquisitions officer gives you documentation of items the investigating officers collected with the computer, including a list of other storage media, such as removable disks and flash drives. The acquisitions officer also notes that the computer is a Windows 8 system, and the machine was running when it was discovered. Before shutting down the computer, the acquisitions officer photographs all open windows on the Windows desktop, including one showing File Explorer, and gives you the photos. (Before shutting down the computer, a live acquisition should be done to capture RAM, too.)

An Overview of a Company Policy Violation

- Employees misusing resources can cost companies millions of dollars
- Misuse includes:
 - Surfing the Internet
 - Sending personal e-mails
 - Using company computers for personal tasks

PREPARING A CASE

Example describes a company policy violation. Manager Steve Billings has been receiving complaints from customers about the job performance of one of his sales representatives, George Montgomery. George has worked as a representative for several years. He's been absent from work for two days but hasn't called in sick or told anyone why he wouldn't be at work. Another employee, Martha, is also missing and hasn't informed anyone of the reason for her absence. Steve asks the IT Department to confiscate George's hard drive and all storage media in his work area. He wants to know whether any information on George's computer and storage media might offer a clue to his whereabouts and job performance concerns. To help determine George's and Martha's whereabouts, you must take a systematic approach, described in the following section, to examining and analyzing the data found on George's desk.

Taking a Systematic Approach

Steps for problem solving

1. **Make an initial assessment about the type of case you're investigating**—To assess the type of case you're handling, talk to others involved in the case and ask questions about the incident. Have law enforcement or company security officers already seized the computer, disks, peripherals, and other components? Do you need to visit an office or another location? Was the computer used to commit a crime, or does it contain evidence about another crime?

2. Determine a preliminary design or approach to the case—Outline the general steps you need to follow to investigate the case. If the suspect is an employee and you need to acquire his or her system, determine whether you can seize the computer during work hours or have to wait until evening or weekend hours. If you're preparing a criminal case, determine what information law enforcement officers have already gathered.

3. Create a detailed checklist—Refine the general outline by creating a detailed checklist of steps and an estimated amount of time for each step. This outline helps you stay on track during the investigation.

4. Determine the resources you need—Based on the OS of the computer you're investigating, list the software you plan to use for the investigation, noting any other software, tools, or expert assistance you might need.

5. Obtain and copy an evidence drive—In some cases, you might be seizing multiple computers along with CDs, DVDs, USB drives, mobile devices, and other removable media.

6. Identify the risks—List the problems you normally expect in the type of case you're handling. This list is known as a standard risk assessment. For example, if the suspect seems knowledgeable about computers, he or she might have set up a logon scheme that shuts down the computer or overwrites data on the hard disk when someone tries to change the logon password.

7. Mitigate or minimize the risks—Identify how you can minimize the risks. For example, if you're working with a computer on which the suspect has likely password-protected the hard drive, you can make multiple copies of the original media before starting. Then if you destroy a copy during the process of retrieving information from the disk, you have additional copies.

8. Test the design—Review the decisions you've made and the steps you've completed. If you have already copied the original media, a standard part of testing the design involves comparing hash values to ensure that you copied the original media correctly.

9. Analyze and recover the digital evidence—Using the software tools and other resources you've gathered, and making sure you've addressed any risks and obstacles, examine the disk to find digital evidence.

10. Investigate the data you recover—View the information recovered from the disk, including existing files, deleted files, e-mail, and Web history, and organize the files to help find information relevant to the case.

11. Complete the case report—Write a complete report detailing what you did and what you found.

12. Critique the case—Self-evaluation and peer review are essential parts of professional growth. After you complete a case, review it to identify successful decisions and actions and determine how you could have improved your performance.

PLANNING AN INVESTIGATION

For all digital investigations, you must be prepared for the unexpected, so you should always have a contingency plan for the investigation. A contingency plan can consist of anything to help you complete the investigation, from alternative software and hardware tools to other methods of approaching the investigation.

Assessing the Case

- Systematically outline the case details
 - Situation
 - Nature of the case
 - Specifics of the case
 - Type of evidence
 - Known disk format
 - Location of evidence
- Based on these details, you can determine the case requirements

Planning Your Investigation

- A basic investigation plan should include the following activities:
 - Acquire the evidence
 - Complete an evidence form and establish a chain of custody
 - Transport the evidence to a computer forensics lab
 - Secure evidence in an **approved secure container**
 - Prepare your **forensics workstation**
 - Retrieve the evidence from the secure container
 - Make a forensic copy of the evidence
 - Return the evidence to the secure container
 - Process the copied evidence with computer forensics tools

- An **evidence custody form** helps you document what has been done with the original evidence and its forensics copies
 - Also called a chain-of-evidence form
- Two types
 - **Single-evidence form**
 - Lists each piece of evidence on a separate page
 - **Multi-evidence form**

Organization X
Security Investigations

This form is to be used for one to ten pieces of evidence

Case No.:		Investigating Organization:	
Investigator:			
Nature of Case:			
Location where evidence was obtained:			
Description of evidence:		Vendor Name	Model No./Serial No.
Item #1			
Item #2			
Item #3			
Item #4			
Item #5			
Item #6			
Item #7			
Item #8			
Item #9			
Item #10			

Evidence Recovered by:			Date & Time:	
Evidence Placed in Locker:			Date & Time:	
Item #	Evidence Processed by	Disposition of Evidence		Date/Time
				Page __ of __

Metropolis Police Bureau High-tech Investigations Unit

This form is to be used for only one piece of evidence.
Fill out a separate form for each piece of evidence.

Case No.:		Unit Number:	
Investigator:			
Nature of Case:			
Location where evidence was obtained:			
Item # ID	Description of evidence:	Vendor Name	Model No./Serial No.
Evidence Recovered by:			Date & Time:
Evidence Placed in Locker:			Date & Time:
Evidence Processed by	Disposition of Evidence		Date/Time

Evidence Processed by	Disposition of Evidence	Date/Time
		Page ____ of ____

Figure 1-10 A single-evidence form

Securing Your Evidence

- Use evidence bags to secure and catalog the evidence
- Use computer safe products when collecting computer evidence
 - Antistatic bags
 - Antistatic pads
- Use well padded containers
- Use evidence tape to seal all openings
 - CD drive bays
 - Insertion slots for power supply electrical cords and USB cables

- Write your initials on tape to prove that evidence has not been tampered with
- Consider computer specific temperature and humidity ranges
- Make sure you have a safe environment for transporting and storing it until a secure evidence container is available

Procedures for Private-Sector High-Tech Investigations

- As an investigator, you need to develop formal procedures and informal checklists
 - To cover all issues important to high-tech investigations
 - Ensures that correct techniques are used in an investigation

Employee Termination Cases

- The majority of investigative work for termination cases involves employee abuse of corporate assets
- Incidents that create a hostile work environment are the predominant types of cases investigated
 - Viewing pornography in the workplace
 - Sending inappropriate e-mails
- Organizations must have appropriate policies in place

Internet Abuse Investigations

- To conduct an investigation you need:
 - Organization's Internet proxy server logs
 - Suspect computer's IP address
 - Suspect computer's disk drive
 - Your preferred computer forensics analysis tool

Internet Abuse Investigations

- Recommended steps
 - Use standard forensic analysis techniques and procedures
 - Use appropriate tools to extract all Web page URL information
 - Contact the network firewall administrator and request a proxy server log
 - Compare the data recovered from forensic analysis to the proxy server log
 - Continue analyzing the computer's disk drive data

E-mail Abuse Investigations

- To conduct an investigation you need:
 - An electronic copy of the offending e-mail that contains message header data
 - If available, e-mail server log records
 - For e-mail systems that store users' messages on a central server, access to the server
 - Access to the computer so that you can perform a forensic analysis on it
 - Your preferred computer forensics analysis tool

E-mail Abuse Investigations

- Recommended steps
 - Use the standard forensic analysis techniques
 - Obtain an electronic copy of the suspect's and victim's e-mail folder or data
 - For Web-based e-mail investigations, use tools such as FTK's Internet Keyword Search option to extract all related e-mail address information
 - Examine header data of all messages of interest to the investigation

Industrial Espionage Investigations

- All suspected industrial espionage cases should be treated as criminal investigations
- Staff needed
 - Digital investigator who is responsible for disk forensic examinations
 - Technology specialist who is knowledgeable of the suspected compromised technical data
 - Network specialist who can perform log analysis and set up network sniffers
 - Threat assessment specialist (typically an attorney)

Industrial Espionage Investigations

- Guidelines when initiating an investigation
 - Determine whether this investigation involves a possible industrial espionage incident
 - Consult with corporate attorneys and upper management
 - Determine what information is needed to substantiate the allegation
 - Generate a list of keywords for disk forensics and sniffer monitoring
 - List and collect resources for the investigation
 - Determine goal and scope of the investigation
 - Initiate investigation after approval from management

Industrial Espionage Investigations

- Planning considerations
 - Examine all e-mail of suspected employees
 - Search Internet newsgroups or message boards
 - Initiate physical surveillance
 - Examine facility physical access logs for sensitive areas
 - Determine suspect location in relation to the vulnerable asset
 - Study the suspect's work habits
 - Collect all incoming and outgoing phone logs

Industrial Espionage Investigations

- Steps to conducting an industrial espionage case
 - Gather all personnel assigned to the investigation and brief them on the plan
 - Gather resources to conduct the investigation
 - Place surveillance systems at key locations
 - Discreetly gather any additional evidence
 - Collect all log data from networks and e-mail servers
 - Report regularly to management and corporate attorneys
 - Review the investigation's scope with management and corporate attorneys

Interviews and Interrogations in High-Tech Investigations

- Becoming a skilled interviewer and interrogator can take many years of experience
- **Interview**
 - Usually conducted to collect information from a witness or suspect
 - About specific facts related to an investigation
- **Interrogation**
 - Process of trying to get a suspect to confess

Interviews and Interrogations in High-Tech Investigations

- Role as a digital investigator
 - To instruct the investigator conducting the interview on what questions to ask
 - And what the answers should be
- Ingredients for a successful interview or interrogation
 - Being patient throughout the session
 - Repeating or rephrasing questions to zero in on specific facts from a reluctant witness or suspect
 - Being tenacious

Conducting an Investigation

- Gather resources identified in investigation plan
- Items needed
 - Original storage media
 - Evidence custody form
 - Evidence container for the storage media
 - Bit-stream imaging tool
 - Forensic workstation to copy and examine your evidence
 - Securable evidence locker, cabinet, or safe

Gathering the Evidence

- Avoid damaging the evidence
- Steps
 - Meet the IT manager to interview him
 - Fill out the evidence form, have the IT manager sign
 - Place the evidence in a secure container
 - Carry the evidence to the computer forensics lab
 - Complete the evidence custody form
 - Secure evidence by locking the container

Understanding Bit-Stream Copies

- Bit-stream copy
 - Bit-by-bit copy of the original storage medium
 - Exact copy of the original disk
 - Different from a simple backup copy
 - Backup software only copy known files
 - Backup software cannot copy deleted files, e-mail messages or recover file fragments
- Bit-stream image
 - File containing the bit-stream copy of all data on a disk or partition
 - Also known as “image” or “image file”
- Copy image file to a target disk that matches the original disk’s manufacturer, size and model

Understanding Bit-stream Copies

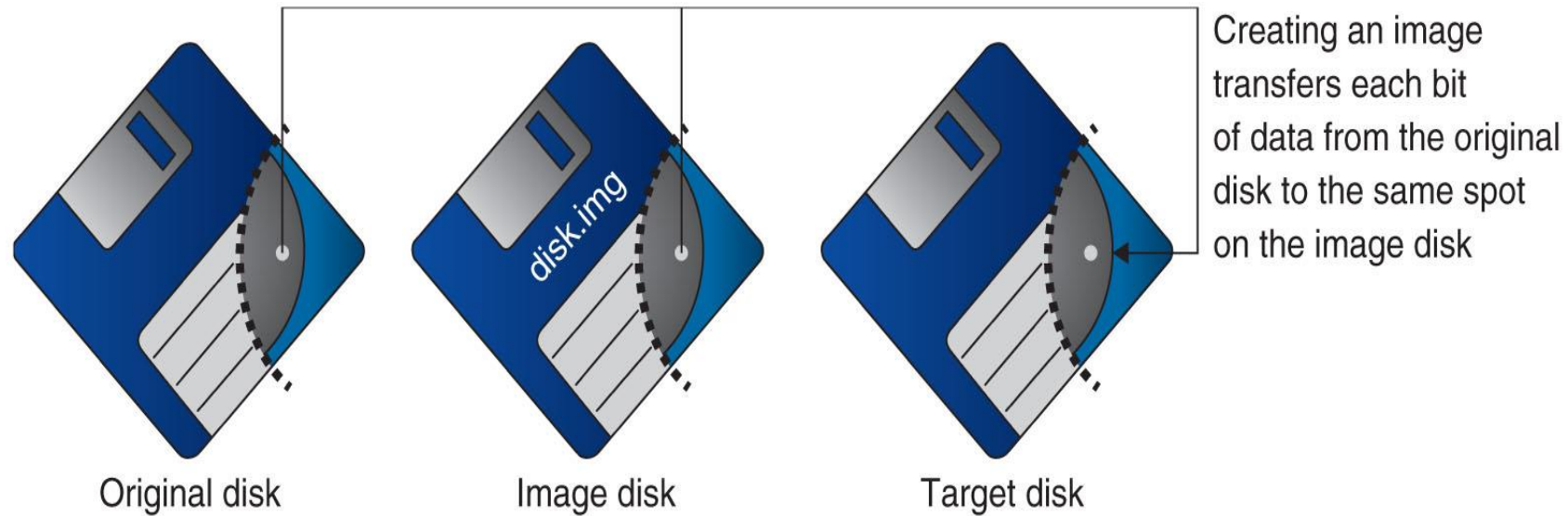


Figure 1-11 Transfer of data from original to image to target

Acquiring an Image of Evidence Media

- First rule of computer forensics
 - Preserve the original evidence
- Conduct your analysis only on a copy of the data
- Several vendors provide MS-DOS, Linux, and Windows acquisition tools
 - Windows tools require a write-blocking device when acquiring data from FAT or NTFS file systems

Analyzing Your Digital Evidence

- Your job is to recover data from:
 - Deleted files
 - File fragments
 - Complete files
- Deleted files linger on the disk until new data is saved on the same physical location
- Tools can be used to retrieve deleted files
 - Autopsy

- Steps to analyze a USB drive
 - Start Autopsy
 - Create a new case
 - Type the case name
 - Select the working folder
- Steps to add source data
 - Select data source type
 - Select image file
 - Keep the default settings in the Configure Ingest Modules window

- Steps to display the contents of the acquired data
 - Click to expand **Views, File Types, By Extension, and Documents**
 - Select file to display
 - Click **Tag and Comment**
 - Click the **New Tag Name** button
- Analyze the data
 - Search for information related to the complaint
- Data analysis can be most time-consuming task

New Case Information

Steps

1. **Case Info**
2. Additional Information

Case Info

Enter New Case Information:

Case Name:

Base Directory:

Case Type: ☒ Single-user ☐ Multi-user


Case data will be stored in the following directory:

< Back Next > Finish Cancel Help


Figure 1-12 The New Case Information window


Source: www.sleuthkit.org


- With Autopsy you can:
 - Search for keywords of interest in the case
 - Display the results in a search results window
 - Click each file in the search results window and examine its content in the data area
 - Export the data to a folder of your choice
 - Search for specific filenames
 - Generate a report of your activities
- Additional features of Autopsy
 - Display binary (nonprintable) data in the Content Viewer



10

 Keyword Lists

 Keyword Search

 Search

☒ Exact Match ☐ Substring Match ☐ Regular Expression

Figure 1-18 Entering a keyword search term

Source: www.sleuthkit.org

Directory Listing
Keyword search 1 - George X

Keyword search
10 Results

Table Thumbnail

Name	Location	Modified Time	Change Time	Access Time
Unalloc_16_121344_1474560	/img_Inchp01.dd//\$Unalloc/Unalloc_16_121344_1474560	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
f0000000.doc	/img_Inchp01.dd/\$CarvedFiles/f0000000.doc	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
f0000047.txt	/img_Inchp01.dd/\$CarvedFiles/f0000047.txt	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
f0000048.txt	/img_Inchp01.dd/\$CarvedFiles/f0000048.txt	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
Billing Letter.doc	/img_Inchp01.dd/Billing Letter.doc	2005-12-09 06:50:28 PST	0000-00-00 00:00:00	2005-12-09 00:00:00 PST
f0000049.doc	/img_Inchp01.dd/\$CarvedFiles/f0000049.doc	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
confirmation.txt	/img_Inchp01.dd/confirmation.txt	2005-12-09 06:52:58 PST	0000-00-00 00:00:00	2005-12-09 00:00:00 PST
Income.xls	/img_Inchp01.dd/Income.xls	2005-12-09 06:52:18 PST	0000-00-00 00:00:00	2005-12-09 00:00:00 PST
letter1.txt	/img_Inchp01.dd/letter1.txt	2005-12-09 06:51:50 PST	0000-00-00 00:00:00	2005-12-09 00:00:00 PST
Regrets.doc	/img_Inchp01.dd/Regrets.doc	2005-12-09 06:50:52 PST	0000-00-00 00:00:00	2005-12-09 00:00:00 PST

Hex Strings File Metadata Results Indexed Text Media

Matches on page: 1 of 1 Match Page: 1 of 1 Page Search Results

```

f0000048.txt Earl,
We need to meet on the 18th of August to confirm the work I am
doing for you. Please contact me ASAP.

George

-----METADATA-----

Content-Encoding: windows-1252
Content-Type: text/plain; charset=windows-1252

```

Figure 1-19 Viewing the results of searching for the keyword “George”

Source: www.sleuthkit.org

Directory Listing
Keyword search 1 - George
X

Keyword search
10 Results

Table
Thumbnail

Name	Location	Modified Time	Change Time	Access Time	Created Time
Unalloc_16_121344_1474560	/img_Inchp01.dd//\$Unalloc/Unalloc_16_121344_1474560	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
f0000000.doc	/img_Inchp01.dd/\$CarvedFiles/f0000000.doc	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
f0000047.txt	/img_Inchp01.dd/\$CarvedFiles/f0000047.txt	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
f0000048.txt	/img_Inchp01.dd/\$CarvedFiles/f0000048.txt	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
Billing Letter.doc	/img_Inchp01.dd/Billing Letter.doc	2005-12-09 06:50:28 PST	0000-00-00 00:00:00	2005-12-09 00:00:00 PST	2005-12-09 06:50:28 PST
f0000049.doc	/img_Inchp01.dd/\$CarvedFiles/f0000049.doc	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
confirmation.txt	/img_Inchp01.dd/confirmation.txt	2005-12-09 06:52:58 PST	0000-00-00 00:00:00	2005-12-09 00:00:00 PST	2005-12-09 06:52:58 PST
Income.xls	/img_Inchp01.dd/Income.xls	2005-12-09 06:52:18 PST	0000-00-00 00:00:00	2005-12-09 00:00:00 PST	2005-12-09 06:52:18 PST
letter1.txt	/img_Inchp01.dd/letter1.txt	2005-12-09 06:51:50 PST	0000-00-00 00:00:00	2005-12-09 00:00:00 PST	2005-12-09 06:51:50 PST
Regrets.doc	/img_Inchp01.dd/Regrets.doc	2005-12-09 06:50:52 PST	0000-00-00 00:00:00	2005-12-09 00:00:00 PST	2005-12-09 06:50:52 PST

Hex
Strings
File Metadata
Results
Indexed Text
Media

Page: 1 of 82
Page
Go to Page:
Jump to Offset 0

0x00000000:	D0 CF 11 E0 A1 B1 1A E1	00 00 00 00 00 00 00 00
0x00000010:	00 00 00 00 00 00 00 00	3E 00 03 00 FE FF 09 00>.....
0x00000020:	06 00 00 00 00 00 00 00	00 00 00 00 01 00 00 00
0x00000030:	2A 00 00 00 00 00 00 00	00 10 00 00 2C 00 00 00	*.....
0x00000040:	01 00 00 00 FE FF FF FF	00 00 00 00 29 00 00 00)
0x00000050:	FF FF FF FF FF FF FF FF	FF FF FF FF FF FF FF FF
0x00000060:	FF FF FF FF FF FF FF FF	FF FF FF FF FF FF FF FF
0x00000070:	FF FF FF FF FF FF FF FF	FF FF FF FF FF FF FF FF
0x00000080:	FF FF FF FF FF FF FF FF	FF FF FF FF FF FF FF FF
0x00000090:	FF FF FF FF FF FF FF FF	FF FF FF FF FF FF FF FF
0x000000a0:	FF FF FF FF FF FF FF FF	FF FF FF FF FF FF FF FF
0x000000b0:	FF FF FF FF FF FF FF FF	FF FF FF FF FF FF FF FF
0x000000c0:	FF FF FF FF FF FF FF FF	FF FF FF FF FF FF FF FF
0x000000d0:	FF FF FF FF FF FF FF FF	FF FF FF FF FF FF FF FF
0x000000e0:	FF FF FF FF FF FF FF FF	FF FF FF FF FF FF FF FF
0x000000f0:	FF FF FF FF FF FF FF FF	FF FF FF FF FF FF FF FF
0x00000100:	FF FF FF FF FF FF FF FF	FF FF FF FF FF FF FF FF
0x00000110:	FF FF FF FF FF FF FF FF	FF FF FF FF FF FF FF FF
0x00000120:	FF FF FF FF FF FF FF FF	FF FF FF FF FF FF FF FF
0x00000130:	FF FF FF FF FF FF FF FF	FF FF FF FF FF FF FF FF
0x00000140:	FF FF FF FF FF FF FF FF	FF FF FF FF FF FF FF FF
0x00000150:	FF FF FF FF FF FF FF FF	FF FF FF FF FF FF FF FF
0x00000160:	FF FF FF FF FF FF FF FF	FF FF FF FF FF FF FF FF
0x00000170:	FF FF FF FF FF FF FF FF	FF FF FF FF FF FF FF FF
0x00000180:	FF FF FF FF FF FF FF FF	FF FF FF FF FF FF FF FF
0x00000190:	FF FF FF FF FF FF FF FF	FF FF FF FF FF FF FF FF

Figure 1-20 Viewing search results found in unallocated drive space

Source: www.sleuthkit.org

Completing the Case

- You need to produce a final report
 - State what you did and what you found
- Include Autopsy report to document your work
- **Repeatable findings**
 - Repeat the steps and produce the same result
- If required, use a report template
- Report should show conclusive evidence
 - Suspect did or did not commit a crime or violate a company policy

Completing the Case

- Keep a written journal of everything you do
 - Your notes can be used in court
- Answer the six Ws:
 - Who, what, when, where, why, and how
- You must also explain computer and network processes
- Autopsy Report Generator
 - Can generate reports in different styles: plain text, HTML and Excel

Critiquing the Case

- Ask yourself the following questions:
 - How could you improve your performance in the case?
 - Did you expect the results you found? Did the case develop in ways you did not expect?
 - Was the documentation as thorough as it could have been?
 - What feedback has been received from the requesting source?
 - Did you discover any new problems? If so, what are they?
 - Did you use new techniques during the case or during research?

Summary

- Digital forensics involves systematically accumulating and analyzing digital information for use as evidence in civil, criminal, and administrative cases
- Investigators need specialized workstations to examine digital evidence
- Public-sector and private-sector investigations differ; public-sector typically require search warrants before seizing digital evidence

- Always use a systematic approach to your investigations
- Always plan a case taking into account the nature of the case, case requirements, and gathering evidence techniques
- Both criminal cases and corporate-policy violations can go to court
- Plan for contingencies for any problems you might encounter
- Keep track of the chain of custody of your evidence

- Internet abuse investigations require examining server log data
- For attorney-client privilege cases, all written communication should remain confidential
- A bit-stream copy is a bit-by-bit duplicate of the original disk
- Always maintain a journal to keep notes on exactly what you did
- You should always critique your own work