Guide to Computer Forensics and Investigations Sixth Edition

Chapter 1

Understanding The Digital Forensics Profession and Investigations

CENGAGE

Objectives

- Describe the field of digital forensics
- Explain how to prepare computer investigations and summarize the difference between public-sector and private-sector investigations
- Explain the importance of maintaining professional conduct
- Describe how to prepare a digital forensics investigation by taking a systematic approach
- Describe procedures for private-sector digital investigations
- Explain requirements for data recovery workstations and software
- Summarize how to conduct an investigation, including critiquing a case

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

An Overview of Digital Forensics (1 of 3)

- **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

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

An Overview of Digital Forensics (2 of 3)

- The Federal Rules of Evidence (FRE) was created to ensure consistency in federal proceedings
  - Signed into law in 1973
  - Many states' rules map to the FRE
- FBI Computer Analysis and Response Team (CART) was formed in 1984 to handle cases involving digital evidence
- By late 1990s, CART teamed up with Department of Defense Computer Forensics Laboratory (DCFL)

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

An Overview of Digital Forensics (3 of 3)

- The **Fourth Amendment** to the U.S. Constitution protects everyone's right to be secure from search and seizure
  - Separate **search warrants** might not be necessary for digital evidence
- Every U.S. jurisdiction has case law related to the admissibility of evidence recovered from computers and other digital devices

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Digital Forensics and Other Related Disciplines (1 of 3)

- 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

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Digital Forensics and Other Related Disciplines (2 of 3)

Figure 1-1 The investigations triad

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Digital Forensics and Other Related Disciplines (3 of 3)

- Vulnerability/threat assessment and risk management
  - Tests and verifies the integrity of stand-along 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

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

A Brief History of Digital Forensics

- By the early 1990s, the International Association of Computer Investigative Specialists (IACIS) introduced training on software for digital forensics
- IRS created search-warrant programs
- ASR Data created Expert Witness for Macintosh
- ILook is currently maintained by the IRS Criminal Investigation Division
- AccessData Forensic Toolkit (FTK) is a popular commercial product

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

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

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Developing Digital Forensics Resources

- To supplement your knowledge:
  - Develop and maintain contact with computing, network, and investigative professionals
  - Join computer user groups in both the pubic and private sectors
    - Example: **Computer Technology Investigators Network (CTIN)** meets to discuss problems with digital forensics examiners encounter
  - Consult outside experts

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Preparing for Digital Investigations (1 of 3)

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

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Preparing for Digital Investigations (2 of 3)

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

Figure 1-4 **Public-sector and private-sector investigations**

iStock.com/RobinsonBecquart, iStock.com/buzbuzzer

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Preparing for Digital Investigations (3 of 3)

- 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

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

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

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Following Legal Processes (1 of 2)

- 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

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Following Legal Processes (2 of 2)

- **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

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding Private-Sector Investigations (1 of 8)

- 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

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding Private-Sector Investigations (2 of 8)

- 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

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding Private-Sector Investigations (3 of 8)

- 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

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding Private-Sector Investigations (4 of 8)

Figure 1-7 A sample warning banner

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding Private-Sector Investigations (5 of 8)

- 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

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding Private-Sector Investigations (6 of 8)

- 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

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding Private-Sector Investigations (7 of 8)

- 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

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding Private-Sector Investigations (8 of 8)

- 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

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

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

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

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

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

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

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

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

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Taking a Systematic Approach (1 of 2)

- Steps for problem solving
  - Make an initial assessment about the type of case you are investigating
  - Determine a preliminary design or approach to the case
  - Create a detailed checklist
  - Determine the resources you need
  - Obtain and copy an evidence drive

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Taking a Systematic Approach (2 of 2)

- Steps for problem solving (cont'd)
  - Identify the risks
  - Mitigate or minimize the risks
  - Test the design
  - Analyze and recover the digital evidence
  - Investigate the data you recover
  - Complete the case report
  - Critique the case

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

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

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Planning Your Investigation (1 of 5)

- 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**

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Planning Your Investigation (2 of 5)

- A basic investigation plan (cont'd):
  - 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

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Planning Your Investigation (3 of 5)

- 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**

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Planning Your Investigation (4 of 5)

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 ___

Figure 1-9 A sample multi-evidence form used in a private-sector environment

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Planning Your Investigation (5 of 5)

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
		Page __ of ___

Figure 1-10 A single-evidence form

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Securing Your Evidence (1 of 2)

- 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

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Securing Your Evidence (2 of 2)

- 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

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

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

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

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

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Internet Abuse Investigations (1 of 2)

- 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

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Internet Abuse Investigations (2 of 2)

- 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

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

E-mail Abuse Investigations (1 of 2)

- 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

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

E-mail Abuse Investigations (2 of 2)

- 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

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Attorney-Client Privilege Investigations (1 of 4)

- Under **attorney-client privilege (ACP)** rules for an attorney
  - You must keep all findings confidential
- Many attorneys like to have printouts of the data you have recovered
  - You need to persuade and educate many attorneys on how digital evidence can be viewed electronically
- You can also encounter problems if you find data in the form of binary files

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Attorney-Client Privilege Investigations (2 of 4)

- Steps for conducting an ACP case
  - Request a memorandum from the attorney directing you to start the investigation
  - Request a list of keywords of interest to the investigation
  - Initiate the investigation and analysis
  - For disk drive examinations, make two bit-stream images using different tools for each image
  - Compare hash signatures on all files on the original and re-created disks

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Attorney-Client Privilege Investigations (3 of 4)

- Steps for conducting an ACP case (cont'd)
  - Methodically examine every portion of the disk drive and extract all data
  - Run keyword searches on allocated and unallocated disk space
  - For Windows OSs, use specialty tools to analyze and extract data from the Registry
  - For binary data files such as CAD drawings, locate the correct software product
  - For unallocated data recovery, use a tool that removes or replaces nonprintable data

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Attorney-Client Privilege Investigations (4 of 4)

- Steps for conducting an ACP case (cont'd)
  - Consolidate all recovered data from the evidence bit-stream image into folders and subfolders
- Other guidelines
  - Minimize written communications with the attorney
  - Any documentation written to the attorney must contain a header stating that it's "Privileged Legal Communication—Confidential Work Product"
  - Assist the attorney and paralegal in analyzing data

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Industrial Espionage Investigations (1 of 5)

- 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)

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Industrial Espionage Investigations (2 of 5)

- 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

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Industrial Espionage Investigations (3 of 5)

- Guidelines (cont'd)
  - Determine goal and scope of the investigation
  - Initiate investigation after approval from management
- 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

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Industrial Espionage Investigations (4 of 5)

- Planning considerations (cont'd)
  - Determine suspect location in relation to the vulnerable asset
  - Study the suspect's work habits
  - Collect all incoming and outgoing phone logs
- 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

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Industrial Espionage Investigations (5 of 5)

- Steps (cont'd)
  - 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

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Interviews and Interrogations in High-Tech Investigations (1 of 2)

- 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

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Interviews and Interrogations in High-Tech Investigations (2 of 2)

- 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

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding Data Recovery Workstations and Software

- Investigations are conducted on a computer forensics lab (or data-recovery lab)
  - In data recovery, the customer or your company just wants the data back
- Computer forensics workstation
  - A specially configured PC
  - Loaded with additional bays and forensics software
- To avoid altering the evidence use:
  - Write-blockers devices
    - Enable you to boot to Windows without writing data to the evidence drive

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Setting Up Your Workstation for Digital Forensics (1 of 2)

- Basic requirements
  - A workstation running Windows 7 or later
  - A write-blocker device
  - Digital forensics acquisition tool
  - Digital forensics analysis tool
  - Target drive to receive the source or suspect disk data
  - Spare PATA or SATA ports
  - USB ports

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Setting Up your Workstation for Digital Forensics (2 of 2)

- Additional useful items
  - Network interface card (NIC)
  - Extra USB ports
  - FireWire 400/800 ports
  - SCSI card
  - Disk editor tool
  - Text editor tool
  - Graphics viewer program
  - Other specialized viewing tools

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

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

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

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

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding Bit-Stream Copies (1 of 2)

- 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

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding Bit-stream Copies (2 of 2)

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

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

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

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Analyzing Your Digital Evidence (1 of 8)

- 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

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Analyzing Your Digital Evidence (2 of 8)

- 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

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Analyzing Your Digital Evidence (3 of 8)

- 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

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Analyzing Your Digital Evidence (4 of 8)

Figure 1-12 The New Case Information window

Source: *www.sleuthkit.org*

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Analyzing Your Digital Evidence (5 of 8)

- 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

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Analyzing Your Digital Evidence (6 of 8)

Figure 1-18 Entering a keyword search term

Source: *www.sleuthkit.org*

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Analyzing Your Digital Evidence (7 of 8)

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

Source: *www.sleuthkit.org*

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Analyzing Your Digital Evidence (8 of 8)

Directory Listing | Keyword search 1 - George

Keyword search — 10 Results

Table | Thumbnail

Name	Location	Modified Time	Change Time	Access Time	Created Time
Unalloc_16_121344_1474560	/img_Inchp01.dd//$Unalloc/Unalloc_16_121344_1474560	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00
f0000000.doc	/img_Inchp01.dd/$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
f0000047.txt	/img_Inchp01.dd/$CarvedFiles/f0000047.txt	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00
f0000048.txt	/img_Inchp01.dd/$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
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
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
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
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
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
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

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*

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Completing the Case (1 of 2)

- 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

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Completing the Case (2 of 2)

- 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

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

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?

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Summary (1 of 3)

- 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

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Summary (2 of 3)

- 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

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Summary (3 of 3)

- 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

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Guide to Computer Forensics and Investigations Sixth Edition

Chapter 2

The Investigator's Office and Laboratory

CENGAGE

Objectives

- Describe certification requirements for digital forensics labs
- List physical requirements for a digital forensics lab
- Explain the criteria for selecting a basic forensic workstation
- Describe components used to build a business case for developing a forensics lab

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding Forensics Lab Certification Requirements

- **Digital forensics lab**
  - Where you conduct your investigation
  - Store evidence
  - House your equipment, hardware, and software
- **ANSI-ASQ National Accreditation Board (ANAB)**
  - Provides accreditation of crime and forensics labs worldwide
  - Accreditation includes forensics labs that analyze digital evidence
  - Audits lab functions and procedures

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Identifying Duties of the Lab Manager and Staff (1 of 2)

- Lab manager duties:
  - Set up processes for managing cases
  - Promote group consensus in decision making
  - Maintain fiscal responsibility for lab needs
  - Enforce ethical standards among lab staff members
  - Plan updates for the lab
  - Establish and promote quality-assurance processes
  - Set reasonable production schedules
  - Estimate how many cases an investigator can handle

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Identifying Duties of the Lab Manager and Staff (2 of 2)

- Lab manager duties (cont'd):
  - Estimate when to expect preliminary and final results
  - Create and monitor lab policies for staff
  - Provide a safe and secure workplace for staff and evidence
- Staff member duties:
  - Knowledge and training:
    - Hardware and software
    - OS and file types
    - Deductive reasoning
  - Work is reviewed regularly by the lab manager
- Check the ANAB Web site for online manual and information

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Lab Budget Planning (1 of 3)

- Break costs down into monthly, quarterly, and annual expenses
- Use past investigation expenses to extrapolate expected future costs
- Expenses for a lab include:
  - Hardware
  - Software
  - Facility space
  - Training personnel

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Lab Budget Planning (2 of 3)

- Estimate the number of cases your lab expects to examine
  - Identify types of computers you're likely to examine
- Take into account changes in technology
- Use statistics to determine what kind of computer crimes are more likely to occur
- Use this information to plan ahead your lab requirements and costs

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Lab Budget Planning (3 of 3)

- Check statistics from the **Uniform Crime Report**
  - For federal reports
- Identify crimes committed with specialized software
- When setting up a lab for a private company, check:
  - Hardware and software inventory
  - Problems reported last year
  - Future developments in computing technology
- Time management is a major issue when choosing software and hardware to purchase

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Acquiring Certification and Training (1 of 5)

- Update your skills through appropriate training
  - Thoroughly research the requirements, cost, and acceptability in your area of employment
- International Association of Computer Investigative Specialists (IACIS)
  - Created by police officers who wanted to formalize credentials in digital investigations
  - Candidates who complete the IACIS test are designated as a **Certified Forensic Computer Examiner (CFCE)**

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Acquiring Certification and Training (2 of 5)

- **ISC² Certified Cyber Forensics Professional (CCFP)**
  - Requires knowledge of
    - Digital forensics
    - Malware analysis
    - Incident response
    - E-discovery
    - Other disciplines related to cyber investigations

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Acquiring Certification and Training (3 of 5)

- **High-Tech Crime Network (HTCN)**
  - Certified Computer Crime Investigator, Basic and Advanced Level
  - Certified Computer Forensic Technician, Basic and Advanced Level
- **EnCase Certified Examiner (EnCE) Certification**
  - Open to the public and private sectors
  - Specific to use and mastery of EnCase forensics analysis
  - Candidates are required to have a licensed copy of EnCase

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Acquiring Certification and Training (4 of 5)

- AccessData Certified Examiner (ACE) Certification
  - Open to the public and private sectors
  - Specific to use and mastery of AccessData Ultimate Toolkit
  - The exam has a knowledge base component and a practical skills component
- Other Training and Certifications
  - EC-Council
  - SysAdmin, Audit, Network, Security (SANS) Institute
  - Defense Cyber Investigations Training Academy (DCITA)

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Acquiring Certification and Training (5 of 5)

- Other training and certifications (cont'd)
  - International Society of Forensic Computer Examiners (ISFCE)
  - Computer Technology Investigators Network (CTIN)
  - Digital Forensics Certification Board (DFCB)
  - Cloud Security Alliance (CSA)
  - Federal Law Enforcement Training Center (FLETC)
  - National White Collar Crime Center (NW3C)

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Determining the Physical Requirements for a Computer Forensics Lab

- Most of your investigation is conducted in a lab
- Lab should be secure so evidence is not lost, corrupted, or destroyed
- Provide a safe and secure physical environment
- Keep inventory control of your assets
  - Know when to order more supplies

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Identifying Lab Security Needs

- **Secure facility**
  - Should preserve integrity of evidence data
- Minimum requirements
  - Small room with true floor-to-ceiling walls
  - Door access with a locking mechanism
  - Secure container
  - Visitor's log
- People working together should have same access level
- Brief your staff about security policy

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Conducting High-Risk Investigations

- High-risk investigations demand more security than the minimum lab requirements
  - **TEMPEST** facilities
    - Electromagnetic Radiation (EMR) proofed
  - TEMPEST facilities are very expensive
    - You can use low-emanation workstations instead

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Using Evidence Containers (1 of 4)

- Known as evidence lockers
  - Must be secure so that no unauthorized person can easily access your evidence
- Recommendations for securing storage containers:
  - Locate them in a restricted area
  - Limited number of authorized people to access the container
  - Maintain records on who is authorized to access each container
  - Containers should remain locked when not in use

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Using Evidence Containers (2 of 4)

- If a combination locking system is used:
  - Provide the same level of security for the combination as for the container's contents
  - Destroy any previous combinations after setting up a new combination
  - Allow only authorized personnel to change lock combinations
  - Change the combination every six months or when required

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Using Evidence Containers (3 of 4)

- If you're using a keyed padlock:
  - Appoint a key custodian
  - Stamp sequential numbers on each duplicate key
  - Maintain a registry listing which key is assigned to which authorized person
  - Conduct a monthly audit
  - Take an inventory of all keys
  - Place keys in a lockable container
  - Maintain the same level of security for keys as for evidence containers
  - Change locks and keys annually
  - Do not use a master key for several locks

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Using Evidence Containers (4 of 4)

- Container should be made of steel with an internal cabinet or external padlock
- If possible, acquire a media safe
- When possible, build an evidence storage room in your lab
- Keep an evidence log
  - Update it every time an evidence container is opened and closed

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Overseeing Facility Maintenance

- Immediately repair physical damages
- Escort cleaning crews as they work
- Minimize the risk of static electricity
  - Antistatic pads
  - Clean floor and carpets
- Maintain two separate trash containers
  - Materials unrelated to an investigation
  - Sensitive materials
- When possible, hire specialized companies for disposing sensitive materials

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Considering Physical Security Needs

- Enhance security by setting security policies
- Enforce your policy
  - Maintain a sign-in log for visitors
    - Anyone that is not assigned to the lab is a visitor
    - Escort all visitors all the time
  - Use visible or audible indicators that a visitor is inside your premises
    - Visitor badge
  - Install an intrusion alarm system
  - Hire a guard force for your lab

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Auditing a Digital Forensics Lab

- Auditing ensures proper enforcing of policies
- Audits should include inspecting the following facility components and practices:
  - Ceiling, floor, roof, and exterior walls of the lab
  - Doors and doors locks
  - Visitor logs
  - Evidence container logs
  - At the end of every workday, secure any evidence that’s not being processed in a forensic workstation

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Determining Floor Plans for Digital Forensics Labs (1 of 7)

- How you configure the work area will depend on:
  - Your budget
  - Amount of available floor space
  - Number of computers you assign to each computing investigator
- Ideal configuration is to have:
  - Two forensic workstations
  - One non-forensic workstation with Internet access

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Determining Floor Plans for Digital Forensics Labs (2 of 7)

- Small labs usually consist of:
  - One or two forensic workstations
  - A research computer with Internet access
  - A workbench (if space allows)
  - Storage cabinets

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Determining Floor Plans for Digital Forensics Labs (3 of 7)

Figure 2-2 Small or home-based lab

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Determining Floor Plans for Digital Forensics Labs (4 of 7)

- Mid-size labs are typically those in a private business
  - Have more workstations
  - Should have at least two exits, for safety reasons
  - Cubicles or separate offices should be part of the layout to reinforce need-to-know policy
  - More library space for software and hardware storage

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Determining Floor Plans for Digital Forensics Labs (5 of 7)

Figure 2-3 Mid-size digital forensics lab

CENGAGE
© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Determining Floor Plans for Digital Forensics Labs (6 of 7)

- State law enforcement or the FBI usually runs most large or regional digital forensics labs
  - Have a separate evidence room
  - One or more custodians might be assigned to manage and control traffic in and out of the evidence room
  - Should have at least two controlled exits and no windows

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Determining Floor Plans for Digital Forensics Labs (7 of 7)

Figure 2-4 Regional digital forensics lab

CENGAGE
© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Selecting a Basic Forensic Workstation

- Depends on budget and needs
- Use less powerful workstations for mundane tasks
- Use multipurpose workstations for resource-heavy analysis tasks

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Selecting Workstations for a Lab

- Police labs have the most diverse needs for computing investigation tools
  - A lab might need legacy systems and software to match what's used in the community
- A small, local police department might have one multipurpose forensic workstation with one or two basic workstations or high-end laptops
- You can now use a laptop PC with USB 3.0 or SATA hard disks to create a lightweight, mobile forensic workstation

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Selecting Workstations for Private-Sector Labs

- Requirements are easy to determine
  - Businesses can conduct internal investigations
- Identify the environment you deal with
  - Hardware platform
  - Operating system
- With some digital forensics programs
  - You can work from a Windows PC and examine both Windows and Macintosh disk drives

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Stocking Hardware Peripherals

- Any lab should have in stock:
  - Digital camera
  - Assorted antistatic bags
  - External CD/DVD drive
  - IDE cables
  - Ribbon cables for floppy disks
  - Extra USB 3.0 or newer cables and SATA cards
  - SCSI cards, preferably ultrawide
  - Graphics cards, both PCI and AGP types
  - Assorted FireWire and USB adapters
  - Hard disk drives and USB drives
  - At least two 2.5-inch Notebook IDE hard drives to standard IDE/ATA or SATA adapter
  - Computer hand tools

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Maintaining Operating Systems and Software Inventories

- Maintain licensed copies of software such as:
  - Microsoft Office (current and older version)
  - Hexadecimal editor
  - Programming languages (Visual Studio, Perl, or Python)
  - Specialized viewers (Quick View)
  - Third-party or open-source office suite
  - Quicken and QuickBooks accounting applications

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Using a Disaster Recovery Plan

- A disaster recovery plan ensures that you can restore your workstation and investigation files to their original condition
  - Recover from catastrophic situations, virus contamination, and reconfigurations
- Includes backup tools such as Norton Ghost
- **Configuration management**
  - Keep track of software updates to your workstation
- For labs using high-end RAID servers:
  - You must consider methods for restoring large data sets
  - Large-end servers must have adequate data backup systems in case of a major failure or more than one drive

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Planning for Equipment Upgrades

- **Risk management**
  - Involves determining how much risk is acceptable for any process or operation
  - Identify equipment your lab depends on so it can be periodically replaced
  - Identify equipment you can replace when it fails
- Computing components last 18 to 36 months under normal conditions
  - Schedule upgrades at least every 18 months
    - Preferably every 12 months

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Building a Business Case for Developing a Forensics Lab

- Enlist the support of managers and other team members
- **Business case**
  - Plan you can use to sell your services to management or clients
- Demonstrate how the lab will help your organization to save money and increase profits
  - Compare cost of an investigation with cost of a lawsuit
  - Protect intellectual property, trade secrets, and future business plans

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Preparing a Business Case for a Digital Forensics Lab (1 of 3)

- Investigators must plan ahead to ensure that money is available for facilities, tools, supplies, and training for your forensics lab
- **Justification**
  - You need to justify to the person controlling the budget the reason a lab is needed
  - Requires constant efforts to market the lab's services to previous, current, and future customers and clients
- **Budget development** - needs to include:
  - Facility cost
  - Hardware requirements
  - Software requirements
  - Miscellaneous budget needs

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Preparing a Business Case for a Digital Forensics Lab (2 of 3)

- **Approval and acquisition**
  - You must present a business case with a budget to upper management for approval
- **Implementation**
  - As part of your business case, describe how implementation of all approved items will be processed
  - A timeline showing expected delivery or installation dates and expected completion dates must be included
  - Schedule inspection dates

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Preparing a Business Case for a Digital Forensics Lab (3 of 3)

- **Acceptance testing** - consider the following items:
  - Inspect the facility to make sure it meets security criteria for containing and controlling digital evidence
  - Test all communications
  - Test all hardware to verify it is operational
  - Install and start all software tools
- **Correction for Acceptance**
  - Your business case must anticipate problems that can cause delays in lab production
- **Production**
  - After all essential corrections have been made the lab can go into production
  - Implement lab operations procedures

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Summary (1 of 2)

- A digital forensics lab is where you conduct investigations, store evidence, and do most of your work
- Seek to upgrade your skills through training
- A lab facility must be physically secure so that evidence is not lost, corrupted, or destroyed
- It is harder to plan a computer forensics lab for a police department than for a private organization or corporation

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Summary (2 of 2)

- A forensic workstation needs to have adequate memory, storage, and ports to deal with common types of cases that come through the lab
- Prepare a business case to enlist the support of your managers and other team members when building a forensics lab

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Guide to Computer Forensics and Investigations Sixth Edition

Chapter 3

Data Acquisition

CENGAGE

Objectives (1 of 2)

- List digital evidence storage formats
- Explain ways to determine the best acquisition method
- Describe contingency planning for data acquisitions
- Explain how to use acquisition tools

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Objectives (2 of 2)

- Explain how to validate data acquisitions
- Describe RAID acquisition methods
- Explain how to use remote network acquisition tools
- List other forensic tools available for data acquisitions

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding Storage Formats for Digital Evidence

- Data in a forensics acquisition tool is stored as an image file
- Three formats
  - Raw format
  - Proprietary formats
  - Advanced Forensics Format (AFF)

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Raw Format

- Makes it possible to write bit-stream data to files
- Advantages
  - Fast data transfers
  - Ignores minor data read errors on source drive
  - Most computer forensics tools can read raw format
- Disadvantages
  - Requires as much storage as original disk or data
  - Tools might not collect marginal (bad) sectors

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Proprietary Formats

- Most forensics tools have their own formats
- Features offered
  - Option to compress or not compress image files
  - Can split an image into smaller segmented files
  - Can integrate metadata into the image file
- Disadvantages
  - Inability to share an image between different tools
  - File size limitation for each segmented volume
- The Expert Witness Compression format is unofficial standard

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Advanced Forensics Format

- Developed by Dr. Simson L. Garfinkel as an open-source acquisition format
- Design goals
  - Provide compressed or uncompressed image files
  - No size restriction for disk-to-image files
  - Provide space in the image file or segmented files for metadata
  - Simple design with extensibility
  - Open source for multiple platforms and Oss
  - Internal consistency checks for self-authentication
- File extensions include .afd for segmented image files and .afm for AFF metadata
- AFF is open source

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Determining the Best Acquisition Method (1 of 4)

- Types of acquisitions
  - **Static acquisitions** and **live acquisitions**
- Four methods of data collection
  - Creating a disk-to-image file
  - Creating a disk-to-disk
  - Creating a logical disk-to-disk or disk-to-data file
  - Creating a sparse data copy of a file or folder
- Determining the best method depends on the circumstances of the investigation

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Determining the Best Acquisition Method (2 of 4)

- Creating a disk-to-image file
  - Most common method and offers most flexibility
  - Can make more than one copy
  - Copies are bit-for-bit replications of the original drive
  - Compatible with many commercial forensics tools
- Creating a disk-to-disk
  - When disk-to-image copy is not possible
  - Tools can adjust disk's geometry configuration
  - Tools: EnCase and X-Ways

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Determining the Best Acquisition Method (3 of 4)

- **Logical acquisition** or **sparse acquisition**
  - Can take several hours; use when your time is limited
  - Logical acquisition captures only specific files of interest to the case
  - Sparse acquisition collects fragments of unallocated (deleted) data
  - For large disks
  - PST or OST mail files, RAID servers

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Determining the Best Acquisition Method (4 of 4)

- When making a copy, consider:
  - Size of the source disk
    - Lossless compression might be useful
    - Use digital signatures for verification
  - When working with large drives, an alternative is using lossless compression
  - Whether you can retain the disk
  - Time to perform the acquisition
  - Where the evidence is located

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Contingency Planning for Image Acquisitions

- Create a duplicate copy of your evidence image file
- Make at least two images of digital evidence
  - Use different tools or techniques
- Copy **host protected area** of a disk drive as well
  - Consider using a hardware acquisition tool that can access the drive at the BIOS level
- Be prepared to deal with encrypted drives
  - **Whole disk encryption** feature in Windows called BitLocker makes static acquisitions more difficult
  - May require user to provide decryption key

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Using Acquisition Tools

- Acquisition tools for Windows
  - Advantages
    - Make acquiring evidence from a suspect drive more convenient
      - Especially when used with hot-swappable devices
  - Disadvantages
    - Must protect acquired data with a well-tested write-blocking hardware device
    - Tools can’t acquire data from a disk’s host protected area
    - Some countries haven’t accepted the use of write-blocking devices for data acquisitions

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Mini-WinFE Boot CDs and USB Drives

- Mini-WinFE
  - Enables you to build a Windows forensic boot CD/DVD or USB drive so that connected drives are mounted as read-only
- Before booting a suspect's computer:
  - Connect your target drive, such as a USB drive
- After Mini-WinFE is booted:
  - You can list all connected drives and alter your target USB drive to read-write mode so you can run an acquisition program

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Acquiring Data with a Linux Boot CD (1 of 6)

- Linux can access a drive that isn't mounted
- Windows OSs and newer Linux automatically mount and access a drive
- Forensic Linux Live CDs don't access media automatically
  - Which eliminates the need for a write-blocker
- Using Linux Live CD Distributions
  - Forensic Linux Live CDs
    - Contain additionally utilities

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Acquiring Data with a Linux Boot CD (2 of 6)

- Using Linux Live CD Distributions (cont'd)
  - Forensic Linux Live CDs (cont'd)
    - Configured not to mount, or to mount as read-only, any connected storage media
    - Well-designed Linux Live CDs for computer forensics
      - Penguin Sleuth Kit
      - CAINE
      - Deft
      - Kali Linux
      - Knoppix
      - SANS Investigative Forensic Toolkit (SIFT)

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Acquiring Data with a Linux Boot CD (3 of 6)

- Preparing a target drive for acquisition in Linux
  - Current Linux distributions can create Microsoft FAT and NTFS partition tables
  - **fdisk** command lists, creates, deletes, and verifies partitions in Linux
  - **mkfs.msdos** command formats a FAT file system from Linux
  - If you have a functioning Linux computer, follow steps starting on page 105 to learn how to prepare a target drive for acquisition

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Acquiring Data with a Linux Boot CD (4 of 6)

- Acquiring data with `dd` in Linux
  - `dd` ("data dump") command
    - Can read and write from media device and data file
    - Creates raw format file that most computer forensics analysis tools can read
  - Shortcomings of `dd` command
    - Requires more advanced skills than average user
    - Does not compress data
  - `dd` command combined with the split command
    - Segments output into separate volumes

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Acquiring Data with a Linux Boot CD (5 of 6)

- Acquiring data with `dd` in Linux (cont'd)
  - Follow the step starting on page 112 in the text to make an image of an NTFS disk on a FAT32 disk
- Acquiring data with `dcfldd` in Linux
  - The `dd` command is intended as a data management tool
    - Not designed for forensics acquisitions

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Acquiring Data with a Linux Boot CD (6 of 6)

- Acquiring data with `dcfldd` in Linux (cont'd)
  - `dcfldd` additional functions
    - Specify hex patterns or text for clearing disk space
    - Log errors to an output file for analysis and review
    - Use several hashing options
    - Refer to a status display indicating the progress of the acquisition in bytes
    - Split data acquisitions into segmented volumes with numeric extensions
    - Verify acquired data with original disk or media data

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Capturing an Image with AccessData FTK Imager Lite (1 of 8)

- Included with AccessData Forensic Toolkit
- Designed for viewing evidence disks and disk-to-image files
- Makes disk-to-image copies of evidence drives
  - At logical partition and physical drive level
  - Can segment the image file
- Evidence drive must have a hardware write-blocking device
  - Or run from a Live CD, such as Mini-WinFE

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Capturing an Image with AccessData FTK Imager Lite (2 of 8)

Figure 3-2 The FTK Imager main window

Source: AccessData Group, Inc.

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Capturing an Image with AccessData FTK Imager Lite (3 of 8)

- FTK Imager can't acquire a drive's host protected area
- Use a write-blocking device and follow these steps
  - Boot to Windows
  - Connect evidence disk to a write-blocker
  - Connect target disk to write-blocker
  - Start FTK Imager Lite
  - Create Disk Image - use Physical Drive option
  - See Figures on the following slides for more steps

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Capturing an Image with AccessData FTK Imager Lite (4 of 8)

Figure 3-3 The Select Drive dialog box

Source: AccessData Group, Inc.

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Capturing an Image with AccessData FTK Imager Lite (5 of 8)

Figure 3-4 The Select Image Type dialog box

Source: AccessData Group, Inc.

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Capturing an Image with AccessData FTK Imager Lite (6 of 8)

Figure 3-5 The Evidence Item Information dialog box

Source: AccessData Group, Inc.

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Capturing an Image with AccessData FTK Imager Lite (7 of 8)

Figure 3-6 Selecting where to save the image file

Source: AccessData Group, Inc.

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Capturing an Image with AccessData FTK Imager Lite (8 of 8)

Figure 3-7 An image save in progress

Source: AccessData Group, Inc.

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Validating Data Acquisitions

- Validating evidence may be the most critical aspect of computer forensics
- Requires using a hashing algorithm utility
- Validation techniques
  - CRC-32, MD5, and SHA-1 to SHA-512

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Linux Validation Methods

- Validating `dd`-acquired data
  - You can use `md5sum` or `sha1sum` utilities
  - `md5sum` or `sha1sum` utilities should be run on all suspect disks and volumes or segmented volumes
- Validating `dcfldd` acquired data
  - Use the `hash` option to designate a hashing algorithm of `md5`, `sha1`, `sha256`, `sha384`, or `sha512`
  - `hashlog` option outputs hash results to a text file that can be stored with the image files
  - `vf` (verify file) option compares the image file to the original medium

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Windows Validation Methods

- Windows has no built-in hashing algorithm tools for computer forensics
  - Third-party utilities can be used
- Commercial computer forensics programs also have built-in validation features
  - Each program has its own validation technique
- Raw format image files don’t contain metadata
  - Separate manual validation is recommended for all raw acquisitions

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Performing RAID Data Acquisitions

- Acquisition of RAID drives can be challenging and frustrating because of how RAID systems are
  - Designed
  - Configured
  - Sized
- Size is the biggest concern
  - Many RAID systems now have exabytes of data

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding RAID (1 of 7)

- **Redundant array of independent disks (RAID)**
  - Computer configuration involving two or more disks
  - Originally developed as a data-redundancy measure
- RAID 0
  - Provides rapid access and increased storage
  - Biggest disadvantage is lack of redundancy
- RAID 1
  - Designed for data recovery
  - More expensive than RAID 0

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding RAID (2 of 7)

Figure 3-8 RAID 0: Striping

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding RAID (2 of 6)

Figure 3-9 RAID 1: Mirroring

CENGAGE
© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding RAID (3 of 6)

- RAID 2
  - Similar to RAID 1
  - Data is written to a disk on a bit level
  - Has better data integrity checking than RAID 0
  - Slower than RAID 0
- RAID 3
  - Uses data stripping and dedicated parity
  - Requires at least three disks
- RAID 4
  - Similar to RAID 3
  - Data is written in blocks

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding RAID (4 of 6)

Figure 3-10 RAID 2: Striping (bit level)

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding RAID (5 of 6)

- RAID 5
  - Similar to RAIDs 0 and 3
  - Places parity recovery data on each disk
- RAID 6
  - Redundant parity on each disk
- RAID 10 (1+0), or mirrored striping
  - Combination of RAID 1 and RAID 0
  - Provides fast access and redundancy
- RAID 15 (1+5)
  - Combination of RAID 1 and RAID 5
  - More costly option

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding RAID (6 of 6)

Figure 3-11 RAID 5: Block-level striping with distributed parity

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Acquiring RAID Disks (1 of 2)

- Address the following concerns:
  - How much data storage is needed?
  - What type of RAID is used?
  - Do you need to have all drives connected?
  - Do you have the right acquisition tool?
  - Can the tool read a forensically copied RAID image?
  - Can the tool read split data saves of each RAID disk?
- Copying small RAID systems to one large disk is possible

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Acquiring RAID Disks (2 of 2)

- Vendors offering RAID acquisition functions
  - Guidance Software EnCase
  - X-Ways Forensics
  - AccessData FTK
  - Runtime Software
  - R-Tools Technologies
- Occasionally, a RAID system is too large for a static acquisition
  - Retrieve only the data relevant to the investigation with the sparse or logical acquisition method

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Using Remote Network Acquisition Tools

- You can remotely connect to a suspect computer via a network connection and copy data from it
- Remote acquisition tools vary in configurations and capabilities
- Drawbacks
  - Antivirus, antispyware, and firewall tools can be configured to ignore remote access programs
  - Suspects could easily install their own security tools that trigger an alarm to notify them of remote access intrusions

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Remote Acquisition with ProDiscover (1 of 3)

- ProDiscover Incident Response functions:
  - Capture volatile system state information
  - Analyze current running processes
  - Locate unseen files and processes
  - Remotely view and listen to IP ports
  - Run hash comparisons
  - Create a hash inventory of all files remotely

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Remote Acquisition with ProDiscover (2 of 3)

- PDServer remote agent
  - ProDiscover utility for remote access
  - Needs to be loaded on the suspect
- PDServer installation modes
  - Trusted CD
  - Preinstallation
  - Pushing out and running remotely
- PDServer can run in a stealth mode
  - Can change process name to appear as OS function

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Remote Acquisition with ProDiscover (3 of 3)

- Remote connection security features
  - Password protection
  - Encryption
  - Secure communication protocol
  - Write-protected trusted binaries
  - Digital signatures

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Remote Acquisition with EnCase Enterprise

- Remote acquisition features
  - Search and collect internal and external network systems over a wide geographical area
  - Support multiple Oss and file systems
  - Triage to help determine system's relevance to an investigation
  - Perform simultaneous searches of up to five systems at a time

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Remote Acquisition with R-Tools R-Studio

- R-Tools suite of software is designed for data recovery
- Can remotely access networked computer systems
- Creates raw format acquisitions
- Supports various file systems

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

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

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Remote Acquisition with F-Response

- F-Response
  - A vendor-neutral remote access utility
  - Designed to work with any digital forensics program
  - Sets up a security read-only connection
    - Allows forensics examiners to access it
- Four different version of F-Response
  - Enterprise Edition, Consultant + Convert Edition, Consultant Edition, and TACTICAL Edition

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Using Other Forensics-Acquisition Tools

- Other commercial acquisition tools
  - PassMark Software ImageUSB
  - ASRData SMART
  - Runtime Software
  - ILookIX Investigator IXimager
  - SourceForge

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

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
  - ImageUSB downloaded from the OSForensics Web site

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

ASR Data SMART

- ASR Data SMART
  - A Linux forensics analysis tool that can make image files of a suspect drive
  - Can produce proprietary or raw format images
- Capabilities:
  - Data reading of bad sectors
  - Can mount drives in write-protected mode
  - Can mount target drives in read/write mode
  - Compression schemes to speed up acquisition or reduce amount of storage needed

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Runtime Software

- Runtime Software offers shareware programs for data acquisition and recovery:
  - DiskExplorer for FAT and NTFS
- Features:
  - Create a raw format image file
  - Segment the raw format or compressed image for archiving purposes
  - Access network computers' drives

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

ILook Investigator IXimager

- IXimager
  - Runs from a bootable floppy or CD
  - Designed to work only with ILookIX
  - Can acquire single drives and RAID drives
  - Supports:
    - IDE (PATA)
    - SCSI
    - USB
    - FireWire

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

SourceForge

- SourceForge provides several applications for security, analysis, and investigations
- For a list of current tools, see:
  - SourceForge-Tools
- Windows version of `dcfldd`
  - SourceForge-dcfldd

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Summary (1 of 3)

- Forensics data acquisitions are stored in three different formats:
  - Raw, proprietary, and AFF
- Data acquisition methods
  - Disk-to-image file
  - Disk-to-disk copy
  - Logical disk-to-disk or disk-to-data file
  - Sparse data copy

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Summary (2 of 3)

- Several tools available
  - Lossless compression is acceptable
- Plan your digital evidence contingencies
  - Make a copy of each acquisition
- Write-blocking devices or utilities must be used with GUI acquisition tools
- Always validate acquisition
- A Linux Live CD, such as SIFT, Kali Linux, or Deft, provides many useful tools for digital forensics acquisitions

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Summary (3 of 3)

- Preferred Linux acquisition tool is `dcfldd` (not `dd`)
- Use a physical write-blocker device for acquisitions
- To acquire RAID disks, determine the type of RAID
  - And then which acquisition tool to use
- Remote network acquisition tools require installing a remote agent on the suspect computer

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Guide to Computer Forensics and Investigations Sixth Edition

Chapter 4

Processing Crime and Incident Scenes

CENGAGE

Objectives (1 of 2)

- Explain the rules for controlling digital evidence
- Describe how to collect evidence at private-sector incident scenes
- Explain guidelines for processing law enforcement crime scenes
- List the steps in preparing for an evidence search
- Describe how to secure a computer incident or crime scene

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Objectives (2 of 2)

- Explain guidelines for seizing digital evidence at the scene
- List procedures for storing digital evidence
- Explain how to obtain a digital hash
- Review a case to identify requirements and plan your investigation

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Identifying Digital Evidence (1 of 2)

- **Digital evidence**
  - Can be any information stored or transmitted in digital form
- U.S. courts accept digital evidence as physical evidence
  - Digital data is treated as a tangible object
- Groups such as the **Scientific Working Group on Digital Evidence (SWGDE)** set standards for recovering, preserving, and examining digital evidence

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Identifying Digital Evidence (2 of 2)

- General tasks investigators perform when working with digital evidence:
  - Identify digital information or artifacts that can be used as evidence
  - Collect, preserve, and document evidence
  - Analyze, identify, and organize evidence
  - Rebuild evidence or repeat a situation to verify that the results can be reproduced reliably
- Collecting digital devices while processing a criminal or incident scene must be done systematically

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding Rules of Evidence (1 of 7)

- Consistent practices help verify your work and enhance your credibility
- Comply with your state's rules of evidence or with the Federal Rules of Evidence
- Evidence admitted in a criminal case can be used in a civil suit, and vice versa
- Keep current on the latest rulings and directives on collecting, processing, storing, and admitting digital evidence

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding Rules of Evidence (2 of 7)

- Data you discover from a forensic examination falls under your state's rules of evidence
  - Or the Federal Rules of Evidence (FRE)
- Digital evidence is unlike other physical evidence because it can be changed more easily
  - The only way to detect these changes is to compare the original data with a duplicate
- Another concern when dealing with digital records is the concept of hearsay
  - Hearsay is secondhand or indirect evidence

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding Rules of Evidence (3 of 7)

- Business-record exception
  - Allows “records of regularly conducted activity,” such as business memos, reports, records, or data compilations
- Business records are authenticated by verifying that they were created
  - “at or near the time by, or from information transmitted by, a person with knowledge”
- Business records are admissible
  - “if the record was kept in the course of a regularly conducted business activity, and it was the regular practice of that business activity to make the record”
- Computer records are usually divided into:
  - **Computer-generated records**
  - **Computer-stored records**

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding Rules of Evidence (4 of 7)

- Computer-generated and computer-stored records must be shown to be authentic and trustworthy
  - To be admitted into evidence
- Computer-generated records are considered authentic if the program that created the output is functioning correctly
  - Usually considered an exception to hearsay rule
- Collecting evidence according to approved steps of evidence control helps ensure that the computer evidence is authentic

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding Rules of Evidence (5 of 7)

- When attorneys challenge digital evidence
  - Often they raise the issue of whether computer-generated records were altered or damaged
- One test to prove that computer-stored records are authentic is to demonstrate that a specific person created the records
  - The author of a Microsoft Word document can be identified by using file metadata
- Follow the steps starting on page 150 of the text to see how to identify file metadata

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding Rules of Evidence (6 of 7)

- The process of establishing digital evidence's trustworthiness originated with written documents and the "best evidence rule"
- Best evidence rule states:
  - To prove the content of a written document, recording, or photograph, ordinarily the original file is required
- Federal Rules of Evidence
  - Allow a duplicate instead of originals when it is produced by the same impression as the original

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding Rules of Evidence (7 of 7)

- As long as bit-stream copies of data are created and maintained properly
  - The copies can be admitted in court, although they aren't considered best evidence
- Example of not being able to use original evidence
  - Investigations involving network servers
  - Removing a server from the network to acquire evidence data could cause harm to a business or its owner, who might be an innocent bystander to a crime or civil wrong

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Collecting Evidence in Private-Sector Incident Scenes (1 of 6)

- Private-sector organizations include:
  - Small to medium businesses, large corporations, and non-government organizations (NGOs)
- Non-government organizations (NGO) must comply with state public disclosure and federal Freedom of Information Act (FOIA) laws
  - And make certain documents available as public records
- FOIA allows citizens to request copies of public documents created by federal agencies

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Collecting Evidence in Private-Sector Incident Scenes (2 of 6)

- A special category of private-sector businesses includes ISPs and other communication companies
- ISPs can investigate computer abuse committed by their employees, but not by customers
  - Except for activities that are deemed to create an emergency situation
- Investigating and controlling computer incident scenes in the corporate environment
  - Much easier than in crime scenes
  - Incident scene is often a workplace

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Collecting Evidence in Private-Sector Incident Scenes (3 of 6)

- Typically, businesses have inventory databases of computer hardware and software
  - Help identify the computer forensics tools needed to analyze a policy violation
    - And the best way to conduct the analysis
- Corporate policy statement about misuse of digital assets
  - Allows corporate investigators to conduct covert surveillance with little or no cause
  - And access company systems without a warrant

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Collecting Evidence in Private-Sector Incident Scenes (4 of 6)

- Companies should display a warning banner and publish a policy
  - Stating that they reserve the right to inspect computing assets at will
- Private-sector investigators should know under what circumstances they can examine an employee's computer
  - Every organization must have a well-defined process describing when an investigation can be initiated

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Collecting Evidence in Private-Sector Incident Scenes (5 of 6)

- If a private-sector investigator finds that an employee is committing or has committed a crime
  - Employer can file a criminal complaint with the police
- Employers are usually interested in enforcing company policy
  - Not seeking out and prosecuting employees
- Private-sector investigators are mainly concerned with protecting company assets

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Collecting Evidence in Private-Sector Incident Scenes (6 of 6)

- If you discover evidence of a crime during a company policy investigation
  - Determine whether the incident meets the elements of criminal law
  - Inform management of the incident
  - Stop your investigation to make sure you don't violate Fourth Amendment restrictions on obtaining evidence
  - Work with the corporate attorney on how to respond to a police request for more information

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Processing Law Enforcement Crime Scenes (1 of 2)

- You must be familiar with criminal rules of search and seizure
- You should also understand how a search warrant works and what to do when you process one
- Law enforcement officer may search for and seize criminal evidence only with **probable cause**
  - Refers to the standard specifying whether a police officer has the right to make an arrest, conduct a personal or property search, or obtain a warrant for arrest

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Processing Law Enforcement Crime Scenes (2 of 2)

- With probable cause, a police officer can obtain a search warrant from a judge
  - That authorizes a search and seizure of specific evidence related to the criminal complaint
- The Fourth Amendment states that only warrants “particularly describing the place to be searched, and the persons or things to be seized” can be issued

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding Concepts and Terms Used in Warrants (1 of 3)

- **Innocent information**
  - Unrelated information
  - Often included with the evidence you're trying to recover
- Judges often issue a **limiting phrase** to the warrant
  - Allows the police to separate innocent information from evidence

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding Concepts and Terms Used in Warrants (2 of 3)

- **Plain view doctrine**
  - Objects falling in plain view of an officer who has the right to be in position to have that view are subject to seizure without a warrant and may be introduced into evidence
  - Three criteria must be met:
    - Officer is where he or she has a legal right to be
    - Ordinary senses must not be enhanced by advanced technology in any way
    - Any discovery must be by chance

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding Concepts and Terms Used in Warrants (3 of 3)

- The plain view doctrine's applicability in the digital forensics world is being rejected
- Example - In a case where police were searching a computer for evidence related to illegal drug trafficking:
  - If an examiner observes an .avi file and find child pornography, he must get an additional warrant or an expansion of the existing warrant to continue the search for child pornography

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Preparing for a Search

- Preparing for a computer search and seizure
  - Probably the most important step in digital investigations
- To perform these tasks
  - You might need to get answers from the victim and an informant
    - Who could be a police detective assigned to the case, a law enforcement witness, or a manager or coworker of the **person of interest** to the investigation

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Identifying the Nature of the Case

- When you're assigned a digital investigation case
  - Start by identifying the nature of the case
    - Including whether it involves the private or public sector
- The nature of the case dictates how you proceed
  - And what types of assets or resources you need to use in the investigation

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Identifying the Type of OS or Digital Device

- For law enforcement
  - This step might be difficult because the crime scene isn't controlled
- If you can identify the OS or device
  - Estimate the size of the drive on the suspect's computer
    - And how many devices to process at the scene
- Determine which OSs and hardware are involved

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Determining Whether You Can Seize Computers and Digital Devices (1 of 2)

- The type of case and location of the evidence
  - Determine whether you can remove digital evidence
- Law enforcement investigators need a warrant to remove computers from a crime scene
  - And transport them to a lab
- If removing the computers will irreparably harm a business
  - The computers should not be taken offsite

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Determining Whether You Can Seize Computers and Digital Devices (2 of 2)

- Additional complications:
  - Files stored offsite that are accessed remotely
  - Availability of cloud storage, which can't be located physically
    - Stored on drives where data from many other subscribers might be stored
- If you aren't allowed to take the computers to your lab
  - Determine the resources you need to acquire digital evidence and which tools can speed data acquisition

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Getting a Detailed Description of the Location

- Get as much information as you can about the location of a digital crime
- Identify potential hazards
  - Interact with your **HAZMAT** (hazardous materials) team
- HAZMAT guidelines
  - Put the target drive in a special HAZMAT bag
  - HAZMAT technician can decontaminate the bag
  - Check for high temperatures

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Determining Who Is in Charge

- Private-sector computing investigations
  - Usually require only one person to respond to an incident
- Law enforcement agencies
  - Typically handle large-scale investigations
- Designate lead investigators in large-scale investigations
  - Anyone assigned to the scene should cooperate with the designated leader to ensure the team addresses all details when collecting evidence

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Using Additional Technical Expertise

- Determine whether you need specialized help to process the incident or crime scene
- You may need to look for specialists in:
  - OSs
  - RAID servers
  - Databases
- Finding the right person can be a challenge
- Educate specialists in investigative techniques
  - Prevent evidence damage

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Determining the Tools You Need (1 of 5)

- Prepare tools using incident and crime scene information
- Create an **initial-response field kit**
  - Should be lightweight and easy to transport
- Create an **extensive-response field kit**
  - Includes all tools you can afford to take to the field
  - When at the scene, extract only those items you need to acquire evidence

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Determining the Tools You Need (2 of 5)

Figure 4-4 Items in an initial-response field kit

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Determining the Tools You Need (3 of 5)

Table 4-1 Tools in an initial-response field kit

Number needed	Tools
1	Small computer toolkit
1	Large-capacity drive
1	Set of Japanese Industrial Standard (JIS) screwdrivers
1	Set of ANSI screwdrivers
2	Antistatic wrist bands
1	IDE ribbon cable (ATA-33 or ATA-100)
1	SATA cables
1	Forensic boot media containing an acquisition utility
1	Laptop IDE 40- to 44-pin adapter, other adapter cables
1	Laptop or tablet computer
1	FireWire or USB dual write-protect external bay
1	Flashlight

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Determining the Tools You Need (4 of 5)

Table 4-1 Tools in an initial-response field kit (*continued*)

Number needed	Tools
1	Digital camera with extra batteries or 35mm camera with film and flash
10	Evidence log forms
1	Notebook or digital dictation recorder
10	Computer evidence bags (antistatic bags)
20	Evidence labels, tape, and tags
1	Permanent ink marker
10	USB drives (or a portable hard drive)

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Determining the Tools You Need (5 of 5)

Table 4-2 Tools in an extensive-response field kit

Number needed	Tools
Varies	Assorted technical manuals, ranging from OS references to forensic analysis guides
1	Initial-response field kit
1	Laptop or tablet with cables and connectors
2	Electrical power strips
1	Additional hand tools, including bolt cutters, pry bar, and hacksaw
1	Leather gloves and disposable latex gloves (assorted sizes)
1	Set of JIS screwdrivers
1	Set of ANSI screwdrivers
2	Antistatic wristbands
1	Hand truck and luggage cart
10	Large garbage bags and large cardboard boxes with packaging tape
1	Rubber bands of assorted sizes
1	Magnifying glass
1	Ream of printer paper
1	Small brush for cleaning dust from digital devices
10	USB drives of varying sizes
2	External hard drives (1 TB or larger) with power cables
Assorted	Converter cables
5	Additional assorted hard drives or USB drives for data acquisition

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Preparing the Investigation Team

- Before initiating the search:
  - Review facts, plans, and objectives with the investigation team you have assembled
- Goal of scene processing
  - To collect and secure digital evidence
- Digital evidence is volatile
  - Develop skills to assess facts quickly
- Slow response can cause digital evidence to be lost

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Securing a Computer Incident or Crime Scene (1 of 2)

- Goals
  - Preserve the evidence
  - Keep information confidential
- Define a secure perimeter
  - Use yellow barrier tape
  - Legal authority for a corporate incident includes trespassing violations
  - For a crime scene, it includes obstructing justice or failing to comply with a police officer

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Securing a Computer Incident or Crime Scene (2 of 2)

- **Professional curiosity** can destroy evidence
  - Involves police officers and other professionals who aren't part of the crime scene processing team
- **Automated Fingerprint Identification System (AFIS)**
  - A computerized system for identifying fingerprints that's connected to a central database
  - Used to identify criminal suspects and review thousands of fingerprint samples at high speed
- Police can take elimination prints of everyone who had access to the crime scene

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Seizing Digital Evidence at the Scene

- Law enforcement can seize evidence
  - With a proper warrant
- Corporate investigators might have the authority only to make an image of the suspect's drive
- When seizing digital evidence in criminal investigations
  - Follow U.S. DOJ standards for seizing digital data
- Civil investigations follow same rules
- Consult with your attorney for extra guidelines

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Preparing to Acquire Digital Evidence (1 of 2)

- The evidence you acquire at the scene depends on the nature of the case
  - And the alleged crime or violation
- Ask your supervisor or senior forensics examiner in your organization the following questions:
  - Do you need to take the entire computer and all peripherals and media in the immediate area?
  - How are you going to protect the computer and media while transporting them to your lab?
  - Is the computer powered on when you arrive?

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Preparing to Acquire Digital Evidence (2 of 2)

- Ask your supervisor or senior forensics examiner in your organization the following questions (cont'd):
  - Is the suspect you're investigating in the immediate area of the computer?
  - Is it possible the suspect damaged or destroyed the computer, peripherals, or media?
  - Will you have to separate the suspect from the computer?

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Processing an Incident or Crime Scene (1 of 4)

- Guidelines
  - Keep a journal to document your activities
  - Secure the scene
    - Be professional and courteous with onlookers
    - Remove people who are not part of the investigation
  - Take video and still recordings of the area around the computer
    - Pay attention to details
  - Sketch the incident or crime scene
  - Check state of computers as soon as possible

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Processing an Incident or Crime Scene (2 of 4)

- Guidelines (cont'd)
  - Don't cut electrical power to a running system unless it's an older Windows 9x or MS-DOS system
  - Save data from current applications as safely as possible
  - Record all active windows or shell sessions
  - Make notes of everything you do when copying data from a live suspect computer
  - Close applications and shut down the computer

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Processing an Incident or Crime Scene (3 of 4)

- Guidelines (cont'd)
  - Bag and tag the evidence, following these steps:
    - Assign one person to collect and log all evidence
    - Tag all evidence you collect with the current date and time, serial numbers or unique features, make and model, and the name of the person who collected it
    - Maintain two separate logs of collected evidence
    - Maintain constant control of the collected evidence and the crime or incident scene

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Processing an Incident or Crime Scene (4 of 4)

- Guidelines (cont'd)
  - Look for information related to the investigation
    - Passwords, passphrases, PINs, bank accounts
  - Collect as much personal information as possible about the suspect or victim
  - Collect documentation and media related to the investigation
    - Hardware, software, backup media, documentation, manuals

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Processing Data Centers with RAID Systems

- Sparse acquisition
  - Technique for extracting evidence from large systems
  - Extracts only data related to evidence for your case from allocated files
    - And minimizes how much data you need to analyze
- Drawback of this technique
  - It doesn’t recover data in free or slack space

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Using a Technical Advisor (1 of 2)

- A technical advisor can help:
  - List the tools you need to process the incident or crime scene
  - Guide you about where to locate data and helping you extract log records
    - Or other evidence from large RAID servers
  - Create the search warrant by itemizing what you need for the warrant

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Using a Technical Advisor (2 of 2)

- Responsibilities
  - Know all aspects of the seized system
  - Direct investigator handling sensitive material
  - Help secure the scene
  - Help document the planning strategy
  - Conduct ad hoc trainings
  - Document activities
  - Help conduct the search and seizure

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Documenting Evidence in the Lab

- Record your activities and findings as you work
  - Maintain a journal to record the steps you take as you process evidence
- Your goal is to be able to reproduce the same results
  - When you or another investigator repeat the steps you took to collect evidence
- A journal serves as a reference that documents the methods you used to process digital evidence

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Processing and Handling Digital Evidence

- Maintain the integrity of digital evidence in the lab
  - As you do when collecting it in the field
- Steps to create image files:
  - Copy all image files to a large drive or a SAN
  - Start your forensics tool to analyze the evidence
  - Run an MD5 or SHA-1 hashing algorithm on the image files to get a digital hash
  - Secure the original media in an evidence locker

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Storing Digital Evidence (1 of 2)

- The media you use to store digital evidence usually depends on how long you need to keep it
- CDs, DVDs
  - Lifespan: 2 to 5 years
- Solid-state USB drives
  - Optimum choice
  - More durable
- Magnetic tapes - 4-mm DAT
  - Capacity: 40 to 72 GB
  - Slow read and write speeds
  - Lifespan: 30 years

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Storing Digital Evidence (2 of 2)

- Super Digital Linear Tape (Super-DLT or SDLT)
  - Specifically designed for large RAID data backups
  - Can store more than 1 TB of data
- Smaller external SDLT drives can connect to a workstation through a SCSI card
- Don’t rely on one media storage method to preserve your evidence
  - Make two copies of every image to prevent data loss
  - Use different tools to create the two images

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Evidence Retention and Media Storage Needs (1 of 2)

- To help maintain the chain of custody for digital evidence
  - Restrict access to lab and evidence storage area
- Lab should have a sign-in roster for all visitors
  - Maintain logs for a period based on legal requirements
- You might need to retain evidence indefinitely
  - Check with your local prosecuting attorney's office or state laws to make sure you're in compliance

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Evidence Retention and Media Storage Needs (2 of 2)

Evidence Activity Log

This form is for tracking access by examiners of evidence items. Use one form for each piece of evidence.

Case Number:	
Evidence Number:	
Evidence Description:	

Examiner's Name	Date Logged Out	Time	Date Logged In	Time

Figure 4-5 A sample log file

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Documenting Evidence (1 of 2)

- Create or use an evidence custody form
- An evidence custody form serves the following functions:
  - Identifies the evidence
  - Identifies who has handled the evidence
  - Lists dates and times the evidence was handled
- You can add more information to your form
  - Such as a section listing MD5 and SHA-1 hash values

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Documenting Evidence (2 of 2)

- Include any detailed information you might need to reference
- Evidence bags also include labels or evidence forms you can use to document your evidence
  - Use antistatic bags for electronic components

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Obtaining a Digital Hash (1 of 4)

- **Cyclic Redundancy Check (CRC)**
  - Mathematical algorithm that determines whether a file's contents have changed
  - Not considered a forensic hashing algorithm
- **Message Digest 5 (MD5)**
  - Mathematical formula that translates a file into a hexadecimal code value, or a **hash value**
  - If a bit or byte in the file changes, it alters the hash value**,** which can be used to verify a file or drive has not been tampered with

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Obtaining a Digital Hash (2 of 4)

- Three rules for forensic hashes:
  - You can't predict the hash value of a file or device
  - No two hash values can be the same
  - If anything changes in the file or device, the hash value must change
- **Secure Hash Algorithm version 1 (SHA-1)**
  - Another hashing algorithm
  - Developed by the **National Institute of Standards and Technology (NIST)**

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Obtaining a Digital Hash (3 of 4)

- In both MD5 and SHA-1, collisions have occurred
- Most digital forensics hashing needs can be satisfied with a **nonkeyed hash set**
  - A unique hash number generated by a software tool, such as the Linux `md5sum` command
- **Keyed hash set**
  - Created by an encryption utility's secret key
- You can use the MD5 function in FTK Imager to obtain the digital signature of a file or an entire drive

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Obtaining a Digital Hash (4 of 4)

Figure 4-6 Using FTK Imager Lite to verify hash values

Source: AccessData Group, Inc.

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Reviewing a Case

- 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

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Sample Civil Investigation

- Most cases in the corporate environment are considered **low-level investigations**
  - Or noncriminal cases
- Common activities and practices
  - Recover specific evidence
    - Suspect's Outlook e-mail folder (PST file)
  - **Covert surveillance**
    - Its use must be well defined in the company policy
    - Risk of civil or criminal liability
  - **Sniffing** tools for data transmissions

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

An example of a Criminal Investigation (1 of 2)

- Computer crimes examples
  - Fraud
  - Check fraud
  - Homicides
- Need a warrant to start seizing evidence
  - Limit searching area

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

An example of a Criminal Investigation (2 of 2)

Figure 4-7 Search warrant limits

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Reviewing Background Information for a Case

- Throughout the book, you use data files from the hypothetical M57 Patents case
  - A startup company doing art patent searches
  - A computer sold on Craigslist was discovered to contain “kitty” porn
  - It was traced back to M57 Patents
  - An employee is suspected of downloading the porn

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Planning the Investigation

- Background information on the case
  - Main players:
    - Pat McGoo, CEO
    - Terry, the IT person
    - Jo and Charlie, the patent researchers
- Police made forensic copies of:
  - The image of the computer sold on Craigslist
  - Images of five other machines found at M57
  - Images of four USB drives found at M57
  - RAM from the imaged machines
  - Network data from the M57 Patents servers

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Conducting the Investigation: Acquiring Evidence with OSForensics

- Follow the steps outlined on pages 182-186 of the text
  - To use OSForensics to analyze an image file

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Summary (1 of 3)

- Digital evidence is anything stored or transmitted on electronic or optical media
- In the private sector, incident scene is often in a contained and controlled area
- Companies should publish the right to inspect computer assets policy
- Private and public sectors follow same computing investigation rules
- Criminal cases
  - Require warrants

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Summary (2 of 3)

- Protect your safety and health as well as the integrity of the evidence
- Follow guidelines when processing an incident or crime scene
  - Security perimeter
  - Video recording
- As you collect digital evidence, guard against physically destroying or contaminating it
- Forensic hash values verify that data or storage media have not been altered

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Summary (3 of 3)

- To analyze computer forensics data, learn to use more than one vendor tool
- You must handle all evidence the same way every time you handle it
- After you determine that an incident scene has digital evidence, identify the digital information or artifacts that can be used as evidence

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Guide to Computer Forensics and Investigations Sixth Edition

Chapter 5

Working with Windows and CLI Systems

CENGAGE

Objectives

- Explain the purpose and structure of file systems
- Describe Microsoft file structures
- Explain the structure of NTFS disks
- List some options for decrypting drives encrypted with whole disk encryption
- Explain how the Windows Registry works
- Describe Microsoft startup tasks
- Explain the purpose of a virtual machine

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding File Systems

- **File system**
  - Gives OS a road map to data on a disk
- 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
  - You should be familiar with both the computer's OS and file systems

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding the Boot Sequence (1 of 3)

- Complementary Metal Oxide Semiconductor (CMOS)
  - Computer stores system configuration and date and time information in the CMOS
    - When power to the system is off
- Basic Input/Output System (BIOS) or Extensible Firmware Interface (EFI)
  - Contains programs that perform input and output at the hardware level

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding the Boot Sequence (2 of 3)

- **Bootstrap process**
  - Contained in ROM, tells the computer how to proceed
  - Displays the key or keys you press to open the CMOS setup screen
- CMOS should be modified to boot from a forensic floppy disk or CD

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding the Boot Sequence (3 of 3)

Figure 5-1 A typical CMOS setup screen

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

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding Disk Drives (1 of 4)

- Disk drives are made up of one or more platters coated with magnetic material
- Disk drive components
  - Geometry
  - Head
  - Tracks
  - Cylinders
  - Sectors

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding Disk Drives (2 of 4)

Figure 5-2 Components of a disk drive

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding Disk Drives (3 of 4)

Figure 5-3 CHS calculation

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding Disk Drives (4 of 4)

- Properties handled at the drive's hardware or firmware level
  - **Zone bit recording (ZBR)**
  - **Track density**
  - **Areal density**
  - **Head and cylinder skew**

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Solid-State Storage Devices

- All flash memory devices have a feature called **wear-leveling**
  - An internal firmware feature used in solid-state drives that ensures even wear of read/writes for all memory cells
- When dealing with solid-state devices, making a full forensic copy as soon as possible is crucial
  - In case you need to recover data from unallocated disk space

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Exploring Microsoft File Structures (1 of 2)

- In Microsoft file structures, sectors are grouped to form **clusters**
  - Storage allocation units of one or more sectors
- Clusters range from 512 bytes up to 32,000 bytes each
- Combining sectors minimizes the overhead of writing or reading files to a disk

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Exploring Microsoft File Structures (2 of 2)

- Clusters are numbered sequentially starting at 0 in NTFS and 2 in FAT
  - First sector of all disks contains a system area, the boot record, and a file structure database
- OS assigns these cluster numbers, called **logical addresses**
- Sector numbers are called **physical addresses**
- Clusters and their addresses are specific to a logical disk drive, which is a disk partition

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Disk Partitions (1 of 3)

- A **partition** is a logical drive
- Windows OSs can have three primary partitions followed by an extended partition that can contain one or more logical drives
- Hidden partitions or voids
  - Large unused gaps between partitions on a disk
- **Partition gap**
  - Unused space between partitions

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Disk Partitions (2 of 3)

- The partition table is in the **Master Boot Record (MBR)**
  - Located at sector 0 of the disk drive
- In a hexadecimal editor, such as WinHex, you can find the first partition at offset 0x1BE
  - The file system's hexadecimal code is offset 3 bytes from 0x1BE for the first partition

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Disk Partitions (3 of 3)

Figure 5-4 The partition table in a hexadecimal editor

Source: X-Ways AG, *www.x-ways.net*

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Examining FAT Disks (1 of 7)

- **File Allocation Table (FAT)**
  - File structure database that Microsoft originally designed for floppy disks
- FAT database is typically written to a disk's outermost track and contains:
  - Filenames, directory names, date and time stamps, the starting cluster number, and file attributes
- Three current FAT versions
  - FAT16, FAT32, and exFAT (used for mobile personal storage devices)
- Cluster sizes vary according to the hard disk size and file system

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Examining FAT Disks (2 of 7)

Table 5-2 Sectors and bytes per cluster

Drive size	Sectors per cluster	FAT16
8–32 MB	1	512 bytes
32–64 MB	2	1 KB
64–128 MB	4	2 KB
128–256 MB	8	4 KB
256–512 MB	16	8 KB
512–1024 MB	32	16 KB
1024–2048 MB	64	32 KB
2048–4096 MB	128	64 KB

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Examining FAT Disks (3 of 7)

- Microsoft OSs allocate disk space for files by clusters
  - Results in **drive slack**
    - Unused space in a cluster between the end of an active file's content and the end of the cluster
- Drive slack includes:
  - **RAM slack** and **file slack**
- An unintentional side effect of FAT16 allowing large clusters was that it reduced fragmentation
  - As cluster size increased

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Examining FAT Disks (4 of 7)

Figure 5-8 File slack space

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Examining FAT Disks (5 of 7)

- When you run out of room for an allocated cluster
  - OS allocates another cluster for your file
- As files grow and require more disk space, assigned clusters are chained together
  - The chain can be broken or fragmented
- When the OS stores data in a FAT file system, it assigns a starting cluster position to a file
  - Data for the file is written to the first sector of the first assigned cluster

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Examining FAT Disks (6 of 7)

Figure 5-9 Chained sectors associated with clusters as a result of increasing file size

Source: X-Ways AG, *www.x-ways.net*

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Examining FAT Disks (7 of 7)

- When this first assigned cluster is filled and runs out of room
  - FAT assigns the next available cluster to the file
- If the next available cluster isn't contiguous to the current cluster
  - File becomes fragmented

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Deleting FAT Files

- In Microsoft OSs, when a file is deleted
  - Directory entry is marked as a deleted file
    - With the HEX E5 character replacing the first letter of the filename
    - FAT chain for that file is set to 0
- Data in the file remains on the disk drive
- Area of the disk where the deleted file resides becomes **unallocated disk space**
  - Available to receive new data from newly created files or other files needing more space

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Examining NTFS Disks (1 of 3)

- **NT File System (NTFS)**
  - Introduced with Windows NT
  - Primary file system for Windows 10
- Improvements over FAT file systems
  - NTFS provides more information about a file
  - NTFS gives more control over files and folders
- NTFS was Microsoft's move toward a journaling file system
  - It records a transaction before the system carries it out

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Examining NTFS Disks (2 of 3)

- In NTFS, everything written to the disk is considered a file
- On an NTFS disk
  - First data set is the **Partition Boot Sector**
  - Next is **Master File Table (MFT)**
- NTFS results in much less file slack space
- Clusters are smaller for smaller disk drives
- NTFS also uses **Unicode**
  - An international data format

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Examining NTFS Disks (3 of 3)

Table 5-3 Cluster sizes in an NTFS disk

Drive size	Sectors per cluster	Cluster size
7–512 MB	8	4 KB
512 MB–1 GB	8	4 KB
1–2 GB	8	4 KB
2 GB–2 TB	8	4 KB
2–16 TB	8	4 KB
16–32 TB	16	8 KB
32–64 TB	32	16 KB
64–128 TB	64	32 KB
128–256 TB	128	64 KB

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

NTFS System Files (1 of 3)

- MFT contains information about all files on the disk
  - Including the system files the OS uses
- In the MFT, the first 15 records are reserved for system files
- Records in the MFT are called **metadata**

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

NTFS File System (2 of 3)

Table 5-4 Metadata records in the MFT

Filename	System file	Record position	Description
`$Mft`	MFT	0	Base file record for each folder on the NTFS volume; other record positions in the MFT are allocated if more space is needed.
`$MftMirr`	MFT 2	1	The first four records of the MFT are saved in this position. If a single sector fails in the first MFT, the records can be restored, allowing recovery of the MFT.
`$LogFile`	Log file	2	Previous transactions are stored here to allow recovery after a system failure in the NTFS volume.
`$Volume`	Volume	3	Information specific to the volume, such as label and version, is stored here.

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

NTFS File System (3 of 3)

Table 5-4 Metadata records in the MFT (*continued*)

Filename	System file	Record position	Description
`$AttrDef`	Attribute definitions	4	A table listing attribute names, numbers, and definitions.
`$`	Root filename index	5	This is the root folder on the NTFS volume.
`$Bitmap`	Boot sector	6	A map of the NTFS partition shows which clusters are in use and which are available.
`$Boot`	Boot sector	7	Used to mount the NTFS volume during the bootstrap process; additional code is listed here if it's the boot drive for the system.
`$BadClus`	Bad cluster file	8	For clusters that have unrecoverable errors, an entry of the cluster location is made in this file.
`$Secure`	Security file	9	Unique security descriptors for the volume are listed in this file. It's where the access control list (ACL) is maintained for all files and folders on the NTFS volume.
`$Upcase`	Upcase table	10	Converts all lowercase characters to uppercase Unicode characters for the NTFS volume.
`$Extend`	NTFS extension file	11	Optional extensions are listed here, such as quotas, object identifiers, and reparse point data.
		12–15	Reserved for future use.

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

MFT and File Attributes (1 of 7)

- In the NTFS MFT
  - All files and folders are stored in separate records of 1024 bytes each
- Each record contains file or folder information
  - This information is divided into record fields containing metadata
- A record field is referred to as an **attribute ID**
- File or folder information is typically stored in one of two ways in an MFT record:
  - Resident and nonresident

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

MFT and File Attributes (2 of 7)

- Files larger than 512 bytes are stored outside the MFT
  - MFT record provides cluster addresses where the file is stored on the drive's partition
    - Referred to as **data runs**
- Each MFT record starts with a header identifying it as a resident or nonresident attribute

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

MFT and File Attributes (3 of 7)

Table 5-5 Attributes in the MFT

Attribute ID	Purpose
0x10	$Standard Information This field contains data on file creation, alterations, MFT changes, read dates and times, and DOS file permissions.
0x20	$Attribute_List Attributes that don't fit in the MFT (nonresident attributes) are listed here along with their locations.
0x30	$File_Name The long and short names for a file are contained here. Up to 255 Unicode bytes are available for long filenames. For POSIX requirements, additional names or hard links can also be listed. Files with short filenames have only one attribute ID 0x30. In older Windows OSs, long filenames have two ID 0x30s in the MFT record: one for the short name and one for the long name. In Windows 10, there's only one 0x30 that combines the short and long filenames.
0x40	$Object_ID ($Volume_Version in Windows NT) Ownership and who has access rights to the file or folder are listed here. Every MFT record is assigned a unique GUID. Depending on your NTFS setup, some file records might not contain this attribute ID.
0x50	$Security_Descriptor Contains the access control list (ACL) for the file.
0x60	$Volume_Name The volume-unique file identifier is listed here. Not all files need this unique identifier.
0x70	$Volume_Information This field indicates the version and state of the volume.
0x80	$Data File data for resident files or data runs for nonresident files.
0x90	$Index_Root Implemented for use of folders and indexes.
0xA0	$Index_Allocation Implemented for use of folders and indexes.

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

MFT and File Attributes (4 of 7)

Table 5-5 Attributes in the MFT (*continued*)

Attribute ID	Purpose
0xB0	$Bitmap A bitmap indicating cluster status, such as which clusters are in use and which are available.
0xC0	$Reparse_Point This field is used for volume mount points and Installable File System (IFS) filter drivers. For the IFS, it marks specific files used by drivers.
0xD0	$EA_Information For use with OS/2 HPFS.
0xE0	For use with OS/2 HPFS.
0x100	$Logged_Utility_Stream This field is used by Encrypting File System (EFS) in Windows 2000 and later.

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

MFT and File Attributes (5 of 7)

A: All MFT records start with FILE0
B: Start of attribute 0x10
C: Length of attribute 0x10 (value 60)
D: Start of attribute 0x30
E: Length of attribute 0x30 (value 70)
F: Start of attribute 0x40
G: Length of attribute 0x40 (value 28)
H: Start of attribute 0x80
I: Length of attribute 0x80 (value 70)
J: Attribute 0x80 resident flag
K: Starting position of resident data

Figure 5-10 Resident file in an MFT record

Source: X-Ways AG, *www.x-ways.net*

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

MFT and File Attributes (6 of 7)

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
035B3C00	46	49	4C	45	30	00	03	00	5F	A7	B2	00	00	00	00	00	FILE0 _§²
035B3C10	03	00	01	00	38	00	00	00	80	01	00	00	00	04	00	00	8 €
035B3C20	00	00	00	00	00	00	00	00	05	00	00	00	A5	17	00	00	¥
035B3C30	09	00	00	00	00	00	00	00	10	00	00	00	60	00	00	00	`
035B3C40	00	00	00	00	00	00	00	00	48	00	00	00	18	00	00	00	H
035B3C50	10	C0	13	88	0B	7C	C9	01	6A	22	16	88	0B	7C	C9	01	À ˆ |É j" ˆ |É
035B3C60	A8	D4	5D	7D	8B	7E	C9	01	6A	22	16	88	0B	7C	C9	01	¨Ô]}‹~É j" ˆ |É
035B3C70	20	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
035B3C80	00	00	00	00	09	01	00	00	00	00	00	00	00	00	00	00	
035B3C90	00	00	00	00	00	00	00	00	30	00	00	00	70	00	00	00	0 p
035B3CA0	00	00	00	00	00	00	02	00	52	00	00	00	18	00	01	00	R
035B3CB0	8A	00	00	00	00	00	01	00	10	C0	13	88	0B	7C	C9	01	Š À ˆ |É
035B3CC0	6A	22	16	88	0B	7C	C9	01	6A	22	16	88	0B	7C	C9	01	j" ˆ |É j" ˆ |É
035B3CD0	6A	22	16	88	0B	7C	C9	01	00	00	00	00	00	00	00	00	j" ˆ |É
035B3CE0	00	00	00	00	00	00	00	00	20	00	00	00	00	00	00	00	
035B3CF0	08	03	42	00	65	00	6E	00	32	00	2E	00	72	00	74	00	B e n 2 . r t
035B3D00	66	00	00	00	00	00	00	00	40	00	00	00	28	00	00	00	f @ (
035B3D10	00	00	00	00	00	00	04	00	10	00	00	00	18	00	00	00	
035B3D20	F7	7C	F1	27	DF	E7	DD	11	A8	3F	00	22	15	D5	88	06	÷|ñ'ßçÝ ¨? " Õˆ
035B3D30	80	00	00	00	48	00	00	00	01	00	00	00	00	00	03	00	€ H
035B3D40	00	00	00	00	00	00	00	00	02	00	00	00	00	00	00	00	
035B3D50	40	00	00	00	00	00	00	00	00	06	00	00	00	00	00	00	@
035B3D60	78	05	00	00	00	00	00	00	78	05	00	00	00	00	00	00	x x
035B3D70	31	03	15	55	01	00	01	00	FF	FF	FF	FF	82	79	47	11	1 U ÿÿÿÿ,yG

A: Start of nonresident attribute 0x80
B: Length of nonresident attribute 0x80
C: Attribute 0x80 nonresident flag
D: Starting point of data run
E: End-of-record marker (FF FF FF FF) for the MFT record

Figure 5-12 **Nonresident file in an MFT record**

Source: X-Ways AG, *www.x-ways.net*

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

MFT and File Attributes (7 of 7)

- When a disk is created as an NTFS file structure
  - OS assigns logical clusters to the entire disk partition
- These assigned clusters are called **logical cluster numbers (LCNs)**
  - Become the addresses that allow the MFT to link to nonresident files on the disk's partition
- When data is first written to nonresident files, an LCN address is assigned to the file
  - This LCN becomes the file's **virtual cluster number (VCN)**

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

MFT Structures for File Data (1 of 7)

- For the header of all MFT records, the record fields of interest are as follows:
  - *At offset 0x00* - the MFT record identifier FILE
  - *At offset 0x1C to 0x1F* - size of the MFT record
  - *At offset 0x14* - length of the header (indicates where the next attribute starts)
  - *At offset 0x32 and 0x33* - the update sequence array, which stores the last 2 bytes of the first sector of the MFT record

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

MFT Structures for File Data (2 of 7)

MFT record identifier

Length of the MFT record header

Size of the entire MFT record

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
000002000	46	49	4C	45	30	00	03	00	11	8F	42	0C	00	00	00	00	FILE0 B
000002010	01	00	01	00	38	00	01	00	D0	01	00	00	00	04	00	00	8 Ð
000002020	00	00	00	00	00	00	00	00	06	00	00	00	00	00	00	00	
000002030	05	02	77	69	00	00	00	00	10	00	00	00	60	00	00	00	wi `

Update sequence array: This data goes into position/offset IE and IF

Note: This data is swapped with data in position IE and IF of the MFT record

Figure 5-13 An MFT header

Source: X-Ways AG, *www.x-ways.net*

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

MFT Structures for File Data (3 of 7)

Figure 5-14 **Attribute 0x10: Standard Information**

Source: X-Ways AG, *www.x-ways.net*

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

MFT Structures for File Data (4 of 7)

A: Attribute 0x30 short filename
B: Size of attribute 0x30 short filename
C: Short create date and time
D: Short last modified date and time
E: Short last access date and time
F: Short record update date and time
G: Starting position of short filename
H: Attribute 0x30 long filename
I: Size of attribute 0x30 long filename
J: Long create date and time
K: Long last modified date and time
L: Long last access date and time
M: Long record update date and time
N: Starting position of long filename

Figure 5-15 Attribute 0x30: short and long filenames

Source: X-Ways AG, *www.x-ways.net*

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

MFT Structures for File Data (5 of 7)

Figure 5-16 **Attribute 0x40: Object_ID**

Source: X-Ways AG, *www.x-ways.net*

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

MFT Structures for File Data (6 of 7)

Figure 5-17 **Attribute 0x80: Data for a resident file**

Source: X-Ways AG, *www.x-ways.net*

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

MFT Structures for File Data (7 of 7)

Figure 5-18 Attribute 0x80: Data for a nonresident file

Source: X-Ways AG, *www.x-ways.net*

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

NTFS Alternate Data Streams (1 of 2)

- **Alternate data streams**
  - Ways data can be appended to existing files
  - Can obscure valuable evidentiary data, intentionally or by coincidence
- In NTFS, an alternate data stream becomes an additional file attribute
  - Allows the file to be associated with different applications
- You can only tell whether a file has a data stream attached by examining that file's MFT entry

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

NTFS Alternate Data Streams (2 of 2)

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
024C0E00	46	49	4C	45	30	00	03	00	5C	AC	B2	00	00	00	00	00	FILE0 \¬²
024C0E10	04	00	01	00	38	00	00	00	B8	01	00	00	00	04	00	00	8 ¸
024C0E20	00	00	00	00	00	00	00	00	07	00	00	00	A1	00	00	00	¡
024C0E30	09	00	00	00	00	00	00	00	10	00	00	00	60	00	00	00	`
024C0E40	00	00	00	00	00	00	00	00	48	00	00	00	18	00	00	00	H
024C0E50	B2	4C	07	BB	D3	7C	C9	01	14	4A	A3	3D	C8	7D	C9	01	²L »Ó|É J£=È}É
024C0E60	14	4A	A3	3D	C8	7D	C9	01	60	69	A5	EC	F8	D0	C9	01	J£=È}É `i¥ìøÐÉ
024C0E70	20	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
024C0E80	00	00	00	00	09	01	00	00	00	00	00	00	00	00	00	00	
024C0E90	00	00	00	00	00	00	00	00	30	00	00	00	70	00	00	00	0 p
024C0EA0	00	00	00	00	00	00	02	00	54	00	00	00	18	00	01	00	T
024C0EB0	8A	00	00	00	00	00	01	00	B2	4C	07	BB	D3	7C	C9	01	Š ²L »Ó|É
024C0EC0	B2	4C	07	BB	D3	7C	C9	01	B2	4C	07	BB	D3	7C	C9	01	²L »Ó|É ²L »Ó|É
024C0ED0	B2	4C	07	BB	D3	7C	C9	01	00	00	00	00	00	00	00	00	²L »Ó|É
024C0EE0	00	00	00	00	00	00	00	00	20	00	00	00	00	00	00	00	
024C0EF0	09	03	42	00	46	00	31	00	5F	00	34	00	2E	00	74	00	B F 1 _ 4 . t
024C0F00	78	00	74	00	00	00	00	00	80	00	00	00	50	00	00	00	x t € P
024C0F10	00	00	18	00	00	00	05	00	38	00	00	00	18	00	00	00	8
024C0F20	57	65	6C	6C	20	64	6F	6E	65	20	69	73	20	62	65	74	Well done is bet
024C0F30	74	65	72	20	74	68	61	6E	20	77	65	6C	6C	20	73	61	ter than well sa
024C0F40	69	64	2E	0D	0A	20	20	42	65	6E	6A	61	6D	69	6E	20	id. Benjamin
024C0F50	46	72	61	6E	6B	6C	69	6E	80	00	00	00	58	00	00	00	Franklin€ X
024C0F60	01	06	40	00	00	00	06	00	00	00	00	00	00	00	00	00	@
024C0F70	00	00	00	00	00	00	00	00	50	00	00	00	00	00	00	00	P
024C0F80	00	02	00	00	00	00	00	00	3B	00	00	00	00	00	00	00	;
024C0F90	3B	00	00	00	00	00	00	00	68	00	69	00	64	00	64	00	; h i d d
024C0FA0	65	00	6E	00	00	00	00	00	31	01	31	A2	00	00	21	E4	e n 1 1¢ !ä
024C0FB0	FF	FF	FF	FF	82	79	47	11	00	00	00	00	00	00	00	00	ÿÿÿÿ‚yG

Second attribute 0x80

Start of data run for second attribute 0x80 (location of hidden alternate data stream)

Size of second attribute 0x80

Figure 5-24 A text alternate data stream

Source: X-Ways AG, *www.x-ways.net*

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

NTFS Compressed Files

- NTFS provides compression similar to FAT DriveSpace 3 (a Windows 98 compression utility)
- With NTFS, files, folders, or entire volumes can be compressed
- Most computer forensics tools can uncompress and analyze compressed Windows data

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

NTFS Encrypting File System (EFS)

- **Encrypting File System (EFS)**
  - Introduced with Windows 2000
  - Implements a **public key** and **private key** method of encrypting files, folders, or disk volumes
- When EFS is used in Windows 2000 and later
  - A **recovery certificate** is generated and sent to the local Windows administrator account
- Users can apply EFS to files stored on their local workstations or a remote server

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

EFS Recovery Key Agent

- Recovery Key Agent implements the recovery certificate
  - Which is in the Windows administrator account
- Windows administrators can recover a key in two ways: through Windows or from a command prompt
- Commands:
  - cipher
  - copy

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Deleting NTFS Files

- When a file is deleted in Windows NT and later
  - The OS renames it and moves it to the Recycle Bin
- Can use the `del` (delete) MS-DOS command
  - Eliminates the file from the MFT listing in the same way FAT does

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Resilient File System

- **Resilient File System** (**ReFS**) - designed to address very large data storage needs
  - Such as the cloud
- Features incorporated into ReFS's design:
  - Maximized data availability
  - Improved data integrity
  - Designed for scalability
- ReFS uses disk structures similar to the MFT in NTFS

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding Whole Disk Encryption (1 of 3)

- In recent years, there has been more concern about loss of
  - **Personal identity information (PII)** and trade secrets caused by computer theft
- Of particular concern is the theft of laptop computers and handheld devices
- To help prevent loss of information, software vendors now provide whole disk encryption

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding Whole Disk Encryption (2 of 3)

- Current whole disk encryption tools offer the following features:
  - Preboot authentication
  - Full or partial disk encryption with secure hibernation
  - Advanced encryption algorithms
  - Key management function

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding Whole Disk Encryption (3 of 3)

- Whole disk encryption tools encrypt each sector of a drive separately
- Many of these tools encrypt the drive's boot sector
  - To prevent any efforts to bypass the secured drive's partition
- To examine an encrypted drive, decrypt it first
  - Run a vendor-specific program to decrypt the drive
  - Many vendors use a bootable CD or USB drive that prompts for a **one-time passphrase**

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Examining Microsoft BitLocker

- Available Vista Enterprise/Ultimate, Windows 7, 8, and 10 Professional/Enterprise, and Server 2008 and later
- Hardware and software requirements
  - A computer capable of running Windows Vista or later
  - The TPM microchip, version 1.2 or newer
  - A computer BIOS compliant with Trusted Computing Group (TCG)
  - Two NTFS partitions
  - The BIOS configured so that the hard drive boots first before checking other bootable peripherals

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Examining Third-Party Disk Encryption Tools

- Some available third-party WDE utilities:
  - Endpoint Encryption
  - Voltage SecureFile
  - Jetico BestCrypt Volume Encryption

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding the Windows Registry

- **Registry**
  - A database that stores hardware and software configuration information, network connections, user preferences, and setup information
- To view the Registry, you can use:
  - Regedit (Registry Editor) program for Windows 9x systems
  - Regedt32 for Windows 2000, XP, and Vista
  - Both utilities can be used for Windows 7 and 8

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Exploring the Organization of the Windows Registry (1 of 5)

- Registry terminology:
  - Registry
  - Registry Editor
  - HKEY
  - Key
  - Subkey
  - Branch
  - Value
  - Default value
  - Hives

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Exploring the Organization of the Windows Registry (2 of 5)

Table 5-6 Registry file locations and purposes

Filename and location	Purpose of file
Users*user-account*\`Ntuser.dat`	User-protected storage area; contains the list of most recently used files and desktop configuration settings
Windows\system32\config\`Default.dat`	Contains the computer's system settings
Windows\system32\config\`SAM.dat`	Contains user account management and security settings
Windows\system32\config\`Security.dat`	Contains the computer's security settings
Windows\system32\config\`Software.dat`	Contains installed programs' settings and associated usernames and passwords
Windows\system32\config\`System.dat`	Contains additional computer system settings
Windows\system32\config\systemprofile	Contains additional NTUSER information

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Exploring the Organization of the Windows Registry (3 of 5)

Figure 5-26 Viewing HKEYs in Registry Editor

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Exploring the Organization of the Windows Registry (4 of 5)

Table 5-7 Registry HKEYs and their functions

HKEY	Function
HKEY_CLASSES_ROOT	A symbolic link to HKEY_LOCAL_MACHINE\SOFTWARE\Classes; provides file type and file extension information, URL protocol prefixes, and so forth
HKEY_CURRENT_USER	A symbolic link to HKEY_USERS; stores settings for the currently logged-on user
HKEY_LOCAL_MACHINE	Contains information about installed hardware and software
HKEY_USERS	Stores information for the currently logged-on user; only one key in this HKEY is linked to HKEY_CURRENT_USER

(*continues*)

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Exploring the Organization of the Windows Registry (5 of 5)

Table 5-7 **Registry HKEYs and their functions** (*continued*)

HKEY	Function
HKEY_CURRENT_CONFIG	A symbolic link to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Hardware ProfileVxxxx (with xxxx representing the current hardware profile); contains hardware configuration settings
HKEY_DYN_DATA	Used only in Windows 9x/Me systems; stores hardware configuration settings

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Examining the Windows Registry (1 of 2)

- Tools with built-in or add-on Registry viewers:
  - X-Ways Forensics
  - OSForensics
  - Forensic Explorer
  - FTK

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Examining the Windows Registry (2 of 2)

Figure 5-30 Entering a search term

Source: PassMark Software, *www.osforensics.com*

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding Microsoft Startup Tasks

- Learn what files are accessed when Windows starts
- This information helps you determine when a suspect's computer was last accessed
  - Important with computers that might have been used after an incident was reported

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Startup in Windows 7, Windows 8 and Windows 10

- Windows 8 and 10 are multiplatform OSs
  - Can run on desktops, laptops, tablets, and smartphones
- The boot process uses a boot configuration data (BCD) store
- The BCD contains the boot loader that initiates the system's bootstrap process
  - Press F8 or F12 when the system starts to access the Advanced Boot Options

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Startup in Windows NT and Later (1 of 5)

- All NTFS computers perform the following steps when the computer is turned on:
  - Power-on self test (POST)
  - Initial startup
  - Boot loader
  - Hardware detection and configuration
  - Kernel loading
  - User logon

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Startup in Windows NT and Later (2 of 5)

- Startup Files for Windows Vista:
  - The Ntldr program in Windows XP used to load the OS has been replaced with these three boot utilities:
    - Bootmgr.exe
    - Winload.exe
    - Winresume.exe
  - Windows Vista includes the BCD editor for modifying boot options and updating the BCD registry file
  - The BCD store replaces the Windows XP boot.ini file

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Startup in Windows NT and Later (3 of 5)

- Startup Files for Windows XP:
  - **NT Loader (NTLDR)**
  - **Boot.ini**
  - **Ntoskrnl.exe**
  - **Bootvid.dll**
  - **Hal.dll**
  - **BootSect.dos**
  - **NTDetect.com**
  - **NTBootdd.sys**
  - **Pagefile.sys**
- **Device drivers**
  - Contain instructions for the OS for hardware devices

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Startup in Windows NT and Later (4 of 5)

Table 5-8 Windows XP system files

Filename	Description
`Ntoskrnl.exe`	The XP executable and kernel
`Ntkrnlpa.exe`	The physical address support program for accessing more than 4 GB of physical RAM
`Hal.dll`	The Hardware Abstraction Layer (described earlier)
`Win32k.sys`	The kernel-mode portion of the Win32 subsystem
`Ntdll.dll`	System service dispatch stubs to executable functions and internal support functions
`Kernel32.dll`	Core Win32 subsystem DLL file
`Advapi32.dll`	Core Win32 subsystem DLL file
`User32.dll`	Core Win32 subsystem DLL file
`Gdi32.dll`	Core Win32 subsystem DLL file

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Startup in Windows NT and Later (5 of 5)

- Contamination Concerns with Windows XP
  - When you start a Windows XP NTFS workstation, several files are accessed immediately
    - The last access date and time stamp for the files change to the current date and time
  - Destroys any potential evidence
    - That shows when a Windows XP workstation was last used

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding Virtual Machines (1 of 3)

- **Virtual machines**
  - Enable you to run another OS on an existing physical computer (known as the host computer) by emulating a computer's hardware environment
- A virtual machine is just a few files on your hard drive
  - Must allocate space to it
- A virtual machine recognizes components of the physical machine it's loaded on
  - Virtual OS is limited by the physical machine's OS

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding Virtual Machines (2 of 3)

Figure 5-31 A virtual machine running on the host computer's desktop

Source: Oracle VirtualBox, *www.virtualbox.org*

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding Virtual Machines (3 of 3)

- In digital forensics
  - Virtual machines make it possible to restore a suspect drive on your virtual machine
    - And run nonstandard software the suspect might have loaded
- From a network forensics standpoint, you need to be aware of some potential issues, such as:
  - A virtual machine used to attack another system or network

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Creating a Virtual Machine

- Common applications for creating virtual machines
  - VMware Server, VMware Player and VMware Workstation, Oracle VM VirtualBox, Microsoft Virtual PC, and Hyper-V
- Using VirtualBox
  - An open-source program (download)
- Consult with your instructor before doing the activities using VirtualBox

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Summary (1 of 3)

- When starting a suspect's computer, using boot media, such as forensic boot CDs or USB drives, you must ensure that disk evidence isn't altered
- The Master Boot Record (MBR) stores information about partitions on a disk
- Microsoft used FAT12 and FAT16 on older operating systems
- To find a hard disk's capacity, use the cylinders, heads, and sectors (CHS) calculation

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Summary (2 of 3)

- When files are deleted in a FAT file system, the hexadecimal value 0x05 is inserted in the first character of the filename in the directory
- NTFS is more versatile because it uses the Master File Table (MFT) to track file information
- Records in the MFT contain attribute IDs that store metadata about files
- In NTFS, alternate data streams can obscure information that might be of evidentiary value

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Summary (3 of 3)

- File slack, RAM slack, and drive slack are areas in which valuable information can reside on a drive
- NTFS can encrypt data with EFS and BitLocker
- NTFS can compress files, folders, or volumes
- Windows Registry keeps a record of attached hardware, user preferences, network connections, and installed software
- Virtualization software enables you to run other OSs on a host computer

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Guide to Computer Forensics and Investigations Sixth Edition

Chapter 6

Current Digital Forensics Tools

CENGAGE

Objectives

- Explain how to evaluate needs for digital forensics tools
- Describe available digital forensics software tools
- List some considerations for digital forensics hardware tools
- Describe methods for validating and testing forensics tools

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Evaluating Digital Forensics Tool Needs

- Consider open-source tools; the best value for as many features as possible
- Questions to ask when evaluating tools:
  - On which OS does the forensics tool run?
  - Is the tool versatile?
  - Can the tool analyze more than one file system?
  - Can a scripting language be used with the tool to automate repetitive functions and tasks?
  - Does it have automated features?
  - What is the vendor's reputation for providing product support?

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Types of Digital Forensics Tools

- Hardware forensic tools
  - Range from simple, single-purpose components to complete computer systems and servers
- Software forensic tools
  - Types
    - Command-line applications
    - GUI applications
  - Commonly used to copy data from a suspect's disk drive to an image file

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Tasks Performed by Digital Forensics Tools (1 of 20)

- Follow guidelines set up by NIST's **Computer Forensics Tool Testing** (**CFTT**) program
- ISO standard 27037 states: Digital Evidence First Responders (DEFRs) should use validated tools
- Five major categories:
  - Acquisition
  - Validation and verification
  - Extraction
  - Reconstruction
  - Reporting

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Tasks Performed by Digital Forensics Tools (2 of 20)

- **Acquisition**
  - Making a copy of the original drive
- Acquisition subfunctions:
  - Physical data copy
  - Logical data copy
  - Data acquisition format
  - Command-line acquisition
  - GUI acquisition
  - Remote, live, and memory acquisitions

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Tasks Performed by Digital Forensics Tools (3 of 20)

- Acquisition (cont'd)
  - Two types of data-copying methods are used in software acquisitions:
    - Physical copying of the entire drive
    - Logical copying of a disk partition
  - The formats for disk acquisitions vary
    - From raw data to vendor-specific proprietary
  - You can view a raw image file's contents with any hexadecimal editor

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Tasks Performed by Digital Forensics Tools (4 of 20)

Figure 6-1 **Viewing data in WinHex**

Source: X-Ways AG, *www.x-ways.net*

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Tasks Performed by Digital Forensics Tools (5 of 20)

- Acquisition (cont'd)
  - Creating smaller segmented files is a typical feature in vendor acquisition tools
  - Remote acquisition of files is common in larger organizations
    - Popular tools, such as AccessData and EnCase, can do remote acquisitions of forensics drive images on a network

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Tasks Performed by Digital Forensics Tools (6 of 20)

- Validation and Verification
  - **Validation**
    - A way to confirm that a tool is functioning as intended
  - **Verification**
    - Proves that two sets of data are identical by calculating hash values or using another similar method
    - A related process is filtering, which involves sorting and searching through investigation findings to separate good data and suspicious data

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Tasks Performed by Digital Forensics Tools (7 of 20)

- Validation and verification (cont'd)
  - Subfunctions
    - Hashing
      - CRC-32, MD5, SHA-1 (Secure Hash Algorithms)
    - Filtering
      - Based on hash value sets
    - Analyzing file headers
      - Discriminate files based on their types
  - **National Software Reference Library** (**NSRL**) has compiled a list of known file hashes
    - For a variety of OSs, applications, and images

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Tasks Performed by Digital Forensics Tools (8 of 20)

Figure 6-2 The home page of the National Software Reference Library

Source: *www.nsrl.nist.gov*

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Tasks Performed by Digital Forensics Tools (9 of 20)

- Validation and discrimination (cont'd)
  - Many computer forensics programs include a list of common header values
    - With this information, you can see whether a file extension is incorrect for the file type
  - Most forensics tools can identify header values

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Tasks Performed by Digital Forensics Tools (10 of 20)

Figure 6-3 The file header indicates a `.jpeg` file

Source: X-Ways AG, *www.x-ways.net*

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Tasks Performed by Digital Forensics Tools (11 of 20)

Figure 6-4 Error message displayed when trying to open a `.jpeg` file in Word

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Tasks Performed by Digital Forensics Tools (12 of 20)

Figure 6-5 `Bayshot.docx` opened in Paint

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Tasks Performed by Digital Forensics Tools (13 of 20)

- **Extraction**
  - Recovery task in a digital investigation
  - Most challenging of all tasks to master
  - Recovering data is the first step in analyzing an investigation's data

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Tasks Performed by Digital Forensics Tools (14 of 20)

- Extraction (cont'd)
  - Subfunctions of extraction
    - Data viewing
    - Keyword searching
    - Decompressing or uncompressing
    - Carving
    - Decrypting
    - Bookmarking or tagging
  - **Keyword search** speeds up analysis for investigators

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Tasks Performed by Digital Forensics Tools (15 of 20)

Figure 6-6 Using a word list to search in OSForensics

Source: PassMark Software, *www.osforensics.com*

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Tasks Performed by Digital Forensics Tools (16 of 20)

Figure 6-7 Data-carving options in OS Forensics

Source: PassMark Software, *www.osforensics.com*

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Tasks Performed by Digital Forensics Tools (17 of 20)

- Extraction (cont'd)
  - From an investigation perspective, encrypted files and systems are a problem
  - Many password recovery tools have a feature for generating potential password lists
    - For a **password dictionary attack**
  - If a password dictionary attack fails, you can run a **brute-force attack**

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Tasks Performed by Digital Forensics Tools (18 of 20)

- **Reconstruction**
  - Re-create a suspect drive to show what happened during a crime or an incident
  - Methods of reconstruction
    - Disk-to-disk copy
    - Partition-to-partition copy
    - Image-to-disk copy
    - Image-to-partition copy
    - Disk-to-image copy
    - Rebuilding files from data runs and carving

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Tasks Performed by Digital Forensics Tools (19 of 20)

- Reconstruction (cont'd)
  - To re-create an image of a suspect drive
    - Copy an image to another location, such as a partition, a physical disk, or a virtual machine
    - Simplest method is to use a tool that makes a direct disk-to-image copy
  - Examples of disk-to-image copy tools:
    - Linux dd command
    - ProDiscover
    - Voom Technologies Shadow Drive

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Tasks Performed by Digital Forensics Tools (20 of 20)

- **Reporting**
  - To perform a forensics disk analysis and examination, you need to create a report
  - Subfunctions of reporting
    - Bookmarking or tagging
    - Log reports
    - Timelines
    - Report generator
  - Use this information when producing a final report for your investigation

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Other Considerations for Tools

- Considerations
  - Flexibility
  - Reliability
  - Future expandability
- Create a software library containing older versions of forensics utilities, OSs, and other programs

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Digital Forensics Software Tools

- The following sections explore some options for command-line and GUI tools in both Windows and Linux

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Command-line Forensics Tools

- The first tools that analyzed and extracted data from floppy disks and hard disks were MS-DOS tools for IBM PC file systems
- Norton DiskEdit
  - One of the first MS-DOS tools used for computer investigations
- Command-line tools require few system resources
  - Designed to run in minimal configurations

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Linux Forensics Tools (1 of 3)

- UNIX has been mostly replaced by Linux
  - You might still encounter systems running UNIX
- Linux platforms have become more popular with home and business end users
- SMART
  - Designed to be installed on numerous Linux versions
  - Can analyze a variety of file systems with SMART
  - Many plug-in utilities are included with SMART
  - Another useful option in SMART is its hex viewer

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Linux Forensics Tools (2 of 3)

- Helix 3
  - One of the easiest suites to use
  - You can load it on a live Windows system
    - Loads as a bootable Linux OS from a cold boot
  - **Some international courts have not accepted live acquisitions as a valid forensics practice
- Kali Linux
  - Formerly known as BackTrack
  - Includes a variety of tools and has an easy-to-use KDE interface

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Linux Forensics Tools (3 of 3)

- Autopsy and SleuthKit
  - Sleuth Kit is a Linux forensics tool
  - Autopsy was the browser interface used to access Sleuth Kit's tools
  - Chapter 7 explains how to use these tools
- Forcepoint Threat Protection
  - Formerly known as Second Look
  - A Linux memory analysis tool
  - Could perform both onsite and remote memory acquisitions

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Other GUI Forensics Tools (1 of 2)

- GUI forensics tools can simplify digital forensics investigations
- Have also simplified training for beginning examiners
- Most of them are put together as suites of tools
- Advantages
  - Ease of use
  - Multitasking
  - No need for learning older OSs

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Other GUI Forensics Tools (2 of 2)

- Disadvantages
  - Excessive resource requirements
  - Produce inconsistent results
  - Create tool dependencies
    - Investigators' may want to use only one tool
    - Should be familiar with more than one type of tool

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Digital Forensics Hardware Tools

- Technology changes rapidly
- Hardware eventually fails
  - Schedule equipment replacements periodically
- When planning your budget consider:
  - Amount of time you expect the forensic workstation to be running
  - Failures
  - Consultant and vendor fees
  - Anticipate equipment replacement

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Forensic Workstations (1 of 4)

- Carefully consider what you need
- Categories
  - Stationary workstation
  - Portable workstation
  - Lightweight workstation
- Balance what you need and what your system can handle
  - Remember that RAM and storage need updating as technology advances

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Forensic Workstations (2 of 4)

- Police agency labs
  - Need many options
  - Use several PC configurations
- Keep a hardware library in addition to your software library
- Private corporation labs
  - Handle only system types used in the organization

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Forensic Workstations (3 of 4)

- Building a forensic workstation is not as difficult as it sounds
- Advantages
  - Customized to your needs
  - Save money
- Disadvantages
  - Hard to find support for problems
  - Can become expensive if careless
- Also need to identify what you intend to analyze

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Forensic Workstations (4 of 4)

- Some vendors offer workstations designed for digital forensics
- Examples
  - F.R.E.D. unit from Digital Intelligence
  - Hardware mounts from ForensicPC
- Having vendor support can save you time and frustration when you have problems
- Can mix and match components to get the capabilities you need for your forensic workstation

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Using a Write-Blocker (1 of 2)

- **Write-blocker**
  - Prevents data writes to a hard disk
- Software-enabled blockers
  - Typically run in a shell mode (Windows CLI)
  - Example: PDBlock from Digital Intelligence
- Hardware options
  - Ideal for GUI forensic tools
  - Act as a bridge between the suspect drive and the forensic workstation

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Using a Write-Blocker (2 of 2)

- You can navigate to the blocked drive with any application
- Discards the written data
  - For the OS the data copy is successful
- Connecting technologies
  - FireWire
  - USB 2.0 and 3.0
  - SATA, PATA, and SCSI controllers

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Recommendations for a Forensic Workstation (1 of 3)

- Determine where data acquisitions will take place
- With Firewire and USB write-blocking devices
  - You can acquire data easily with Digital Intelligence FireChief and a laptop computer
- If you want to reduce hardware to carry:
  - WiebeTech Forensic DriveDock with its regular DriveDock FireWire bridge or the Logicube Talon

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Recommendations for a Forensic Workstation (2 of 3)

- Recommendations when choosing stationary or lightweight workstation:
  - Full tower to allow for expansion devices
  - As much memory and processor power as budget allows
  - Different sizes of hard drives
  - 400-watt or better power supply with battery backup
  - External FireWire and USB ports
  - Assortment of drive adapter bridges

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Recommendations for a Forensic Workstation (3 of 3)

- Recommendations when choosing stationary or lightweight workstation (cont'd):
  - Ergonomic keyboard and mouse
  - A good video card with at least a 17-inch monitor
  - High-end video card and dual monitors
- If you have a limited budget, one option for outfitting your lab is to use high-end game PCs

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Validating and Testing Forensic Software

- It is important to make sure the evidence you recover and analyze can be admitted in court
- You must test and validate your software to prevent damaging the evidence

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Using National Institute of Standards and Technology Tools (1 of 3)

- NIST publishes articles, provides tools, and creates procedures for testing/validating forensics software
- Computer Forensics Tool Testing (CFTT) project
  - Manages research on forensics tools
- NIST has created criteria for testing forensics tools based on:
  - Standard testing methods
  - ISO 17025 criteria for testing items that have no current standards

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Using National Institute of Standards and Technology Tools (2 of 3)

- Your lab must meet the following criteria
  - Establish categories for digital forensics tools
  - Identify forensics category requirements
  - Develop test assertions
  - Identify test cases
  - Establish a test method
  - Report test results
- ISO 5725 - specifies results must be repeatable and reproducible

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Using National Institute of Standards and Technology Tools (3 of 3)

- NIST created the National Software Reference Library (NSRL) project
  - Collects all known hash values for commercial software applications and OS files
    - Uses SHA-1 to generate a known set of digital signatures called the Reference Data Set (RDS)
  - Helps filtering known information
  - Can use RDS to locate and identify known bad files

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Using Validation Protocols (1 of 3)

- Always verify your results by performing the same tasks with other similar forensics tools
- Use at least two tools
  - Retrieving and examination
  - Verification
- Understand how forensics tools work
- One way to compare results and verify a new tool is by using a disk editor
  - Such as Hex Workshop or WinHex

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Using Validation Protocols (2 of 3)

- Disk editors do not have a flashy interface, however they:
  - Are reliable tools
  - Can access raw data
- Digital Forensics Examination Protocol
  - Perform the investigation with a GUI tool
  - Verify your results with a disk editor
  - Compare hash values obtained with both tools

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Using Validation Protocols (3 of 3)

- Digital Forensics Tool Upgrade Protocol
  - Test
    - New releases
    - OS patches and upgrades
  - If you find a problem, report it to forensics tool vendor
    - Do not use the forensics tool until the problem has been fixed
  - Use a test hard disk for validation purposes
  - Check the Web for new editions, updates, patches, and validation tests for your tools

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Summary (1 of 3)

- Consult your business plan to get the best hardware and software
- Computer forensics tools functions
  - Acquisition
  - Validation and verification
  - Extraction
  - Reconstruction
  - Reporting
- Maintain a software library on your lab

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Summary (2 of 3)

- Computer Forensics tools types
  - Software
  - Hardware
- Forensics software
  - Command-line
  - GUI
- Forensics hardware
  - Customized equipment
  - Commercial options
  - Include workstations and write-blockers

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Summary (3 of 3)

- Tools that run in Windows and other GUI environments don’t require the same level of computing expertise as command-line tools
- Always run a validation test when upgrading your forensics tools

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Guide to Computer Forensics and Investigations Sixth Edition

Chapter 7

Linux and Macintosh File Systems

CENGAGE

Objectives

- Describe Linux file structures
- Describe Macintosh file structures
- Use Linux forensics tools

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Examining Linux File Structures (1 of 2)

- UNIX distributions
  - Silicon Graphics, Inc. (SGI) IRIX, Santa Cruz Operation (SCO) UnixWare, Sun Solaris, IBM AIX, and HP-UX
- Linux distributions
  - Ubuntu, CentOS, Mint, Fedora, and Gentoo
  - Linux is only the core of the OS
- All UNIX-like OSs have a kernel
  - So do all Windows OSs

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Examining Linux File Structures (2 of 2)

- Remember that UNIX and Linux commands are case sensitive
  - Wrong capitalization can mean your commands are rejected as incorrect or interpreted as something different
- Review some Linux commands by working through the activity on pages 310-312

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

File Structures in Ext4 (1 of 3)

- The early file system standard was **Second Extended File System** (**Ext2**)
  - **Third Extended File System** (**Ext3**) replaced Ext2 in most Linux distributions
- **Fourth Extended File System** (**Ext4**) added support for partitions larger than 16 TB
  - Improved management of large files and offered more flexibility
  - Adoption of Ext4 was slower in some Linux distributions
  - Now considered the standard file system for most distributions

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

File Structures in Ext4 (2 of 3)

- Everything is a file
  - Files are objects with properties and methods
- UNIX/Linux file system consists of four components
- **Boot block**
  - Contains the bootstrap code
  - UNIX/Linux computer has only one boot block, located on the main hard disk

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

File Structures in Ext4 (3 of 3)

- **Superblock**
  - Specifies disk geometry, available space, and keeps track of all inodes
  - Manages the file system
- **Inode blocks**
  - First data after the superblock
  - Assigned to every file allocation unit
- **Data blocks**
  - Where directories and files are stored on a disk drive
  - This location is linked directly to inodes

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Inodes (1 of 5)

- Contain file and directory metadata
  - Also link data stored in data blocks
- An assigned inode contains the following:
  - Mode and type of file or directory
  - Number of links to a file or directory
  - UID and GID of the file's or directory's owner
  - Number of bytes in the file or directory
  - File's or directory's last access time and last modified time

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Inodes (2 of 5)

- An assigned inode contains the following (cont'd):
  - Inode's last file status change time
  - Block address for the file data
  - Indirect, double-indirect, and triple-indirect block addresses for the file data
  - Current usage status of the inode
  - Number of actual blocks assigned to a file
  - File generation number of version number
  - Continuation inode's link

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Inodes (3 of 5)

- First inode has 13 pointers
  - Pointers 1 to 10 are direct pointers to data storage blocks
- Pointer 11 is an **indirect pointer**
  - Links to 128 pointer inodes and each pointer links directly to 128 blocks
  - Pointer 12 is a **double-indirect pointer**
  - Pointer 13 is a **triple-indirect pointer**

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Inodes (4 of 5)

Figure 7-3 Inode pointers in the Linux file system

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Inodes (5 of 5)

- **Bad block inode**
  - Keeps track of disk's bad sectors
- To find bad blocks on a Linux computer, use the following commands
  - `badblocks` – must log in as root to use
  - `mke2fs` and `e2fsck` - include safeguards that prevent them from overwriting important information

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Hard Links and Symbolic Links (1 of 6)

- **Hard link**
  - A pointer that allows accessing the same file by different filenames
  - Use the `ln` command to create a hard link

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Hard Links and Symbolic Links (2 of 6)

Figure 7-4 Hard-linked files with different filenames

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Hard Links and Symbolic Links (3 of 6)

- **Link count**
  - A field inside each inode that specifies the number of hard links

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Hard Links and Symbolic Links (4 of 6)

Figure 7-5 The `ls -a` command showing the dot and dot-dot notation

Source: *www.ubuntu.com*

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Hard Links and Symbolic Links (5 of 6)

- **Symbolic links**
  - Pointers to other files and aren't included in the link count
  - Also known as "soft links" or "symlinks"
  - Can point to items on other drives or other parts of the network
  - Have an inode of their own
    - Not the same as the inode of the item they are pointing to
  - Depend on the existence of the destination they are pointing to

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Hard Links and Symbolic Links (6 of 6)

Figure 7-8 Creating a symbolic link

Source: *www.ubuntu.com*

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding Macintosh File Structures (1 of 2)

- Mac OS X version 10.13
  - Code-named High Sierra
  - Current version
  - Offers better security, encryption, and performance speeds
- With OS X, Macintosh moved to the Intel processor and become UNIX based

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding Macintosh File Structures (2 of 2)

- Before OS X, **Hierarchical File System (HFS)**
  - Files stored in nested directories (folders)
- **Extended Format File System (HFS+)**
  - Introduced with Mac OS 8.1
  - Supports smaller file sizes on larger volumes, resulting in more efficient disk use
- **Apple File System (APFS)**
  - Introduced in macOS High Sierra
  - When data is written to a device, metadata is also copied to help with crash protection

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

An Overview of Mac File Structures (1 of 7)

- In Mac, a file consists of two parts:
  - **Data fork** and **resource fork**
  - Stores file metadata and application information
- The data fork typically contains data the user creates, such as text or spreadsheets
  - Applications also read and write to the data fork
- Resource block contains additional information
  - Such as menus and dialog boxes
- A volume is any storage medium used to store files
  - It can be all or part of the storage media for hard disks

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

An Overview of Mac File Structures (2 of 7)

Figure 7-9 The resource fork and data fork in a macOS file

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

An Overview of Mac File Structures (3 of 7)

- Volumes have **allocation** and **logical blocks**
  - Logical blocks cannot exceed 512 bytes
  - Allocation blocks are a set of consecutive logical blocks
- Two end of file (EOF) descriptors
  - **Logical EOF**
    - Actual ending of the file
  - **Physical EOF**
    - The number of bytes allotted on the volume for a file

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

An Overview of Mac File Structures (4 of 7)

Figure 7-10 Logical and allocation block structures

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

An Overview of Mac File Structures (5 of 7)

Figure 7-11 Logical EOF and physical EOF

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

An Overview of Mac File Structures (6 of 7)

- **Clumps**
  - Groups of contiguous allocation blocks
  - Reduce fragmentation
- Older Macintosh OSs use
  - First two logical blocks, 0 and 1, as boot blocks
  - **Master Directory Block (MDB)** or **Volume Information Block (VIB)**
    - Stores all information about a volume
  - **Volume Control Block (VCB)**
    - Stores information from the MDB when OS mounts
- **Extents overflow file**
  - Stores any file information not in the MDB or a VCB

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

An Overview of Mac File Structures (7 of 7)

- **Catalog**
  - The listing of all files and directories on the volume
  - Maintains relationships between files and directories
- **B*-tree** file system in earlier Mac version
  - Actual file data is stored on the leaf nodes
  - B*-tree also uses **header**, **index**, and **map nodes**

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Forensics Procedures in Mac (1 of 6)

- There are some differences between Linux and macOS file systems
  - Linux has the `/home/username` and `/root` directories
  - In macOS, the folders are `/users/username` and `/private/var/root`
  - The `/home` directory exists in the macOS but it is empty
  - macOS users have limited access to other user accounts' files and the guest account is disabled

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Forensics Procedures in Mac (2 of 6)

- For forensics procedures in macOS:
  - You must know where file system components are located and how both files and file components are stored
- Application settings are in three formats:
  - Plaintext, plist files, and the SQLite database
  - **Plist files** are preference files for installed applications on a system
- FileVault is used to encrypt and decrypt a user's `/users` directory

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Forensics Procedures in Mac (3 of 6)

- **Keychains**
  - Files used to manage passwords for applications, Web sites, and other system files
  - The Mac application Keychain Access enables you to restore passwords
- Deleted files are in the Trashes folder
  - If a file is deleted at the command line, however, it doesn't show up in the trash

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Forensics Procedures in Mac (4 of 6)

- Acquisition Methods in macOS
  - Make an image of the drive
  - Removing the drive from a Mac Mini case is difficult
    - Attempting to do so without Apple factory training could damage the computer
    - Also difficult for MacBook Air (need special screwdrivers)
  - Use a macOS-compatible forensic boot CD/DVD to make an image

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Forensics Procedures in Mac (5 of 6)

- Acquisition Methods in macOS (cont'd)
  - BlackBag Technologies sells acquisition products specifically designed for OS 9 and OS X
  - MacQuisition is a forensic boot CD that makes an image of a Mac drive
  - After making an acquisition, examine the image of the file system
    - The tool you use depends on the image file format

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Forensics Procedures in Mac (6 of 6)

- Acquisition Methods in macOS (cont'd)
  - Tools for working with a raw format image
    - BlackBag Technologies Macintosh Forensic Software
    - SubRosaSoft MacForensicsLab
    - Guidance Software EnCase
    - Recon Mac OS X Forensics with Palladin
    - X-Ways Forensics
    - AccessData FTK
  - First two tools can disable/enable Disk Arbitration
  - Being able to turn off the mount function in macOS
    - Allows you to connect a suspect drive to a Mac without a write-blocking device

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Using Linux Forensics Tools

- Most commercial computer forensics tools can analyze Linux Ext2, Ext3, Ext4, ReiserFS, and Reiser4 file systems
- Freeware tools include Sleuth Kit and its Web browser interface, Autopsy Forensic Browser
- Foremost
  - A freeware carving tool that can read many image file formats
  - Configuration file: foremost.conf
- **Tarball**
  - A data file containing one or more files or whole directories and their contents

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Installing Sleuth Kit and Autopsy (1 of 3)

- Download the most current source code from www.sleuthkit.org
- To run Sleuth Kit and Autopsy Browser, you need to have root privileges

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Installing Sleuth Kit and Autopsy (2 of 3)

Figure 7-12 Starting Autopsy in Linux

Source: *www.sleuthkit.org*

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Installing Sleuth Kit and Autopsy (3 of 3)

Figure 7-13 The Autopsy main window

Source: *www.sleuthkit.org*

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Examining a Case with Sleuth Kit and Autopsy (1 of 3)

- Follow instructions to use Sleuth Kit and Autopsy Browser to examine an older Linux file system
  - See Figures 7-14 and 7-15

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Examining a Case with Sleuth Kit and Autopsy (2 of 3)

Figure 7-14 The Create a New Case dialog box

Source: *www.sleuthkit.org*

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Examining a Case with Sleuth Kit and Autopsy (3 of 3)

Figure 7-15 The Add a New Host dialog box

Source: *www.sleuthkit.org*

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Summary (1 of 3)

- UNIX was created to be a multiuser, multithreaded, secure OS
- The Linux kernel is usually packaged with other software components, such as a GUI and applications
- Linux supports a wide range of file systems
- UNIX and Linux have four components defining the file system: boot block, superblock, inode block, and data block

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Summary (2 of 3)

- In the Linux file system, a hard link is a pointer that allows accessing the same file by different filenames
- Before macOS, the file systems HFS and HFS+ were used
- In older version of macOS, a file consists of two parts: a data fork and a resource fork
- A volume is any storage medium used to store files

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Summary (3 of 3)

- Plist files are preference files for installed applications on a macOS system
- In macOS, unified logging has been added for recording log files and includes new utilities to help forensics examiners
- The biggest challenge in acquiring images from macOS systems is often physical access to the drive
- Linux forensic tools are often freeware

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Guide to Computer Forensics and Investigations Sixth Edition

Chapter 8

Recovering Graphics Files

CENGAGE

Objectives

- Describe types of graphics file formats
- Explain types of data compression
- Explain how to locate and recover graphics files
- Describe how to identify unknown file formats
- Explain copyright issues with graphics

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Recognizing a Graphics File

- Graphic files contain digital photographs, line art, three-dimensional images, text data converted to images, and scanned replicas of printed pictures
  - **Bitmap images**: collection of dots
  - **Vector graphics**: based on mathematical instructions
  - **Metafile graphics**: combination of bitmap and vector
- Types of programs
  - Graphics editors
  - Image viewers

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding Bitmap and Raster Images

- Bitmap images
  - Grids of individual **pixels**
- **Raster images** - also collections of pixels
  - Pixels are stored in rows
  - Better for printing
- Image quality
  - Screen **resolution** - determines amount of detail
  - Software contributes to image quality (drivers)
  - Number of color bits used per pixel

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding Vector Graphics

- Characteristics of vector graphics
  - Uses lines instead of dots
  - Store only the calculations for drawing lines and shapes
  - Smaller than bitmap files
  - Preserve quality when image is enlarged
- CorelDRAW, Adobe Illustrator

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding Metafile Graphics

- Metafile graphics combine raster and vector graphics
- Example
  - Scanned photo (bitmap) with text or arrows (vector)
- Share advantages and disadvantages of both types
  - When enlarged, bitmap part loses quality

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding Graphics File Formats (1 of 2)

- **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)

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding Graphics File Formats (2 of 2)

- **Nonstandard graphics file formats**
  - Targa (.tga)
  - Raster Transfer Language (.rtl)
  - Adobe Photoshop (.psd) and Illustrator (.ai)
  - Freehand (.fh11)
  - Scalable Vector Graphics (.svg)
  - Paintbrush (.pcx)
- Search the Web for software to manipulate unknown image formats

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding Digital Photograph File Formats (1 of 8)

- Witnesses or suspects can create their own digital photos
- Examining the raw file format
  - **Raw file format**
    - Referred to as a digital negative
    - Typically found on many higher-end digital cameras
  - Sensors in the digital camera simply record pixels on the camera's memory card
  - Raw format maintains the best picture quality

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding Digital Photograph File Formats (2 of 8)

- Examining the raw file format (cont'd)
  - The biggest disadvantage is that it's proprietary
    - And not all image viewers can display these formats
  - The process of converting raw picture data to another format is referred to as **demosaicing**
- Examining the Exchangeable Image File format
  - **Exchangeable Image File (Exif)** format
    - Commonly used to store digital pictures
    - Developed by JEITA as a standard for storing metadata in JPEG and TIF files

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding Digital Photograph File Formats (3 of 8)

- Examining the Exchangeable Image File format (cont'd)
  - Exif format collects metadata
    - Investigators can learn more about the type of digital device and the environment in which photos were taken
  - Viewing an Exif JPEG file's metadata requires special programs
    - Exif Reader, IrfanView, or Magnet Forensics AXIOM
  - Exif file stores metadata at the beginning of the file

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding Digital Photograph File Formats (4 of 8)

Figure 8-1 Similar Exif and JPEG photos

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding Digital Photograph File Formats (5 of 8)

Figure 8-2 Differences in Exif and JPEG file header information

Source: X-Ways AG, *www.x-ways.net*

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding Digital Photograph File Formats (6 of 8)

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00019110	00	F8	B5	E0	F9	5B	A7	F4	AC	AC	A0	0F	7F	E9	05	BE	øµàù[§ô¬¬ é ¾
00019120	7F	FC	62	F8	7F	F9	0B	FD	2A	1B	AE	D0	A2	C0	C6	1D	übø ù ý* ®Ð¢ÀÆ
00019130	5A	FE	49	71	E1	5D	8A	A0	9F	9E	2B	2B	28	02	AD	77	ZþIqá]▌ ▌▌++(-w
00019140	78	D7	32	BC	B7	0C	EE	EF	F7	99	8F	26	A1	EF	95	73	x×2¼· îï÷▌ &¡ï▌s
00019150	B4	64	7B	81	59	59	4C	46	C2	75	C7	DD	15	82	E3	3D	´d{ YYLFÂuÇÝ ▌ã=
00019160	16	B2	B2	80	08	D3	F5	19	6C	AF	62	B8	87	EF	C6	D9	²²€ Óõ l¯b,▌ïÆÙ
00019170	C7	A8	F3	1F	51	5D	4A	3B	D1	3C	09	22	16	D8	EA	18	Ç¨ó Q]J;Ñ< " Øê
00019180	67	D0	8A	CA	CA	00	A1	76	AA	C8	D8	DD	89	60	20	41	gÐ▌ÊÊ ¡vªÈØÝ▌` A
00019190	36	48	5F	F0	9F	31	F2	A4	5B	DF	FC	46	B2	B2	80	21	6H_ð▌1ò¤[ßüF²²▌!
000191A0	37	60	1C	17	23	E9	5B	AC	84	91	86	AC	AC	A0	0D	BC	7` #é[¬▌´▌¬¬ ¼
000191B0	47	D7	F1	AD	79	27	CC	7D	6B	2B	28	03	C2	39	C6	6B	G×ñ-y'Ì}k+(Â9Æk
000191C0	30	3D	7F	2A	CA	CA	00	F3	03	1E	75	E6	D1	E8	2B	2B	0= *ÊÊ ó uæÑè++
000191D0	28	03	49	19	63	5C	95	15	E2	C9	BB	EE	2E	01	F5	35	(I c\▌ âÉ»î. õ5
000191E0	95	94	08	90	92	46	09	3F	4A	D7	38	E8	2B	2B	28	02	▌▌ ´F ?J×8è++(
000191F0	32	E7	38	C5	6A	4F	AF	E9	59	59	40	11	93	CD	65	65	2ç8ÅjO¯éYY@ ▌Íee
00019200	65	00	7F	FF	D9												e ÿÙ

JPEG file EOI marker

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00001ED0	92	49	00	24	92	49	00	24	92	49	00	3A	9E	A3	C5	5A	´I $´I $´I :▌£ÅZ
00001EE0	A8	E1	1A	AA	6E	51	07	C5	C2	00	6F	1A	A3	9E	93	87	¨á ªnQ ÅÂ o £▌▌▌
00001EF0	43	F2	5E	6F	86	EC	F4	D4	21	D3	E6	BD	1E	AD	72	87	Cò^o▌ìôÔ!Óæ½ -r▌
00001F00	56	A7	72	63	CD	2E	CE	86	57	D8	3F	01	C3	5B	45	B6	V§rcÍ.Î▌WØ? Ã[E¶
00001F10	12	ED	91	36	B6	18	D1	37	26	66	53	18	35	E8	A3	AB	í´6¶ Ñ7&fS 5è£«
00001F20	75	89	C8	D6	C7	82	49	89	BE	CA	60	22	35	54	19	5C	u▌ÈÖÇ▌I▌¾Ê`"5T \
00001F30	03	28	9D	33	9B	45	19	2B	8F	25	8A	34	5A	6E	2C	77	(3▌E + %▌4Zn,w
00001F40	5A	FE	CF	53	86	2C	7B	24	5D	6D	7B	37	7A	40	A7	FA	ZþÏS▌,{$]m{7z@§ú
00001F50	7E	C5	5A	B0	83	4C	09	E1	45	29	ED	5A	CC	C4	81	25	~ÅZ°▌L áE)íZÌÄ %
00001F60	C6	94	94	A0	63	80	5D	01	36	57	42	00	EA	E8	0B	90	Æ▌▌ c▌] 6WB êè
00001F70	9C	14	80	A1	25	D4	94	01	8C	49	24	94	12	03	5C	49	▌ ▌¡%Ô▌ ▌I$▌ \I
00001F80	24	00	92	49	24	00	92	49	24	00	9C	A0	7A	E2	48	02	$ ´I$ ´I$ ▌ zâH
00001F90	2A	8A	0A	FA	24	92	5D	9D	0C	AF	B2	3A	7A	15	13	F4	*▌ ú$´] ¯²:z ô
00001FA0	29	24	B0	4B	B3	5B	2B	3B	64	47	87	EA	12	49	4C	BA	)$°K³[+;dG▌ê ILº
00001FB0	2B	E0	26	DD	96	C3	B3	7F	E9	04	92	5A	3D	3F	91	57	+à&Ý▌Ã³ é ´Z=?´W
00001FC0	74	15	4F	6A	EA	4B	62	32	B1	C1	75	71	25	08	96	75	t OjêKb2±Áuq% ▌u
00001FD0	3D	89	24	80	1C	92	49	20	0E	A4	92	4A	40	FF	D9		=▌$▌ ´I ¤´J@ÿÙ

Figure 8-3 EOI marker FFD9 for all JPEG files

Source: X-Ways AG, *www.x-ways.net*

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding Digital Photograph File Formats (7 of 8)

- Examining the Exchangeable Image File format (cont'd)
  - With tools such as Autopsy and Exif Reader
    - You can extract metadata as evidence for your case

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding Digital Photograph File Formats (8 of 8)

Figure 8-4 Autopsy displaying metadata from an Exif JPEG file

Source: *www.sleuthkit.org*

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding Data Compression

- Most graphics file formats compress their data
  - GIF and JPEG
- Others, like BMP, do not compress their data
  - Use data compression tools for those formats
- **Data compression**
  - Coding data from a larger to a smaller form
  - Types
    - Lossless compression and lossy compression

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Lossless and Lossy Compression

- **Lossless compression**
  - Reduces file size without removing data
  - Based on Huffman or Lempel-Ziv-Welch coding
    - For redundant bits of data
  - Utilities: WinZip, PKZip, StuffIt, and FreeZip
- **Lossy compression**
  - Permanently discards bits of information
  - **Vector quantization (VQ)**
    - Determines what data to discard based on vectors in the graphics file
  - Utility: Lzip

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Locating and Recovering Graphics Files

- Operating system tools
  - Time consuming
  - Results are difficult to verify
- Digital forensics tools
  - Image headers
    - Compare them with good header samples
    - Use header information to create a baseline analysis
  - Reconstruct fragmented image files
    - Identify data patterns and modified headers

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Identifying Graphics File Fragments

- **Carving** or **salvaging**
  - Recovering any type of file fragments
- Digital forensics tools
  - Can carve from file slack and free space
  - Help identify image files fragments and put them together

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Repairing Damaged Headers (1 of 4)

- 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 you found

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Repairing Damaged Headers (2 of 4)

- 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
- Exercise:
  - Investigate a possible intellectual property theft by a new employee of Superior Bicycles, Inc.

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Repairing Damaged Headers (3 of 4)

Chris Robinson

From: Bob Aspen <b_aspen@aol.com>
Sent: Monday, July 10, 2017 3:32 PM
To: cr-superior@outlook.com
Subject: FW: More info

Chris,
I got cc'd this odd message from Terry Sadler.
Do you have any projects that might need some capital investment?
Bob

-----Original Message-----
From: Terry Sadler [mailto:t_sadler@zoho.com]
Sent: Monday, July 10, 2017 3:28 PM
To: Jim Shu
Subject: Re: More info

Do you have a name for the project?

On 7/10/2017 3:04 PM, Jim Shu wrote:
> Terry,
>
> Here a few more photos from Tom.
>
> How much you willing to pay for these?
>
> Jim
>

Figure 8-5 An e-mail from Terry Sadler

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Repairing Damaged Headers (4 of 4)

Chris Robinson

From: Tom Johnson <1060waddisonst@gmx.us>
Sent: Monday, July 10, 2017 2:40 PM
To: Jim Shu
Subject: You might be interested

Jim,

I had a tour of the new kayak factory. I think we can run with this to the other party interested in competing. I smuggled these files out, they are JPEG files I edited with my hex editor so that the email monitor won't pick up on them. So to view them you have to re-edit each file to the proper JPEG header of offset 0x FF D8 FF E0 and offset 6 of 4A. Then you have to rename them to a .jpg extension to view them.

Tom

Figure 8-6 The e-mail with attachments IT found

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Searching for and Carving Data from Unallocated Space (1 of 6)

- Steps
  - Planning your examination
  - Searching for and recovering digital photograph evidence
    - Use Autopsy for Windows to search for and extract (recover) possible evidence of JPEG files
    - False hits are referred to as **false positives**

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Searching for and Carving Data from Unallocated Space (2 of 6)

Figure 8-7 Processing options in the Configure Ingest Modules window

Source: *www.sleuthkit.org*

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Searching for and Carving Data from Unallocated Space (3 of 6)

Figure 8-8 Parsing Exif metadata in Autopsy

Source: *www.sleuthkit.org*

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Searching for and Carving Data from Unallocated Space (4 of 6)

Figure 8-9 The results of searching for "fif"

Source: *www.sleuthkit.org*

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Searching for and Carving Data from Unallocated Space (5 of 6)

Figure 8-10 The altered file header

Source: *www.sleuthkit.org*

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Searching for and Carving Data from Unallocated Space (6 of 6)

Figure 8-11 Viewing all sectors used by the `gametour2.exe` file

Source: *www.sleuthkit.org*

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Rebuilding File Headers (1 of 6)

- Before attempting to edit a recovered graphics file
  - Try to open the file with an image viewer first
- If the image isn't displayed, you have to inspect and correct the header values manually
- Steps
  - Recover more pieces of file if needed
  - Examine file header
    - Compare with a good header sample
    - Manually insert correct hexadecimal values
  - Test corrected file

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Rebuilding File Headers (2 of 6)

Figure 8-12 Error message indicating a damaged or an altered graphics file

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Rebuilding File Headers (3 of 6)

Figure 8-13 `Recover1.jpg` open in WinHex

Source: X-Ways AG, *www.xways.net*

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Rebuilding File Headers (4 of 6)

Figure 8-14 Inserting correct hexadecimal values for a JPEG file

Source: X-Ways AG, *www.xways.net*

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Rebuilding File Headers (5 of 6)

ASCII hexadecimal conversion table

	0	1	2	3	4	5	6	7	8	9	A	B	C	D
0	NUL	SOH	STX	ETX	EOT	ENQ	ACK	BEL	BS	HT	LF	VT	FF	CR
1	DLE	DC1	DC2	DC3	DC4	NAK	SYN	ETB	CAN	EM	SUB	ESC	FS	GS
2	SP	!	"	#	$	%	&	'	(	)	*	+	,	.
3	0	1	2	3	4	5	6	7	8	9	:	;	<	=
4	@	A	B	C	D	E	F	G	H	I	J	K	L	M
5	P	Q	R	S	T	U	V	W	X	Y	Z	[	\	]
6	`	a	b	c	d	e	f	g	h	i	j	k	l	m
7	p	q	r	s	t	u	v	w	x	y	z	{	|	}

Uppercase "A" = 41
Lowercase "a" = 61

Second hexadecimal number

First hexadecimal number

Figure 8-15 ASCII equivalents of hexadecimal values

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Rebuilding File Headers (6 of 6)

Figure 8-16 `Fixed1.jpg` open in an image viewer

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Reconstructing File Fragments

- Locate the noncontiguous clusters that make up a deleted file
- Steps
  - Locate and export all clusters of the fragmented file
  - Determine the starting and ending cluster numbers for each fragmented group of sectors
  - Copy each fragmented group of sectors in their correct sequence to a recovery file
  - Rebuild the file's header to make it readable in a graphics viewer
  - Add a `.txt` extension on all the copied sectors

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Identifying Unknown File Formats

- Knowing the purpose of each format and how it stores data is part of the investigation process
- The Internet is the best source
  - Search engines
  - Find explanations and viewers
- Popular Web sites
  - *FileFormat.info*
  - *Extension Informer*
  - *The Graphics File Formats Page*

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Analyzing Graphics File Headers (1 of 3)

- Necessary when you find files your tools do not recognize
- Use a hexadecimal editor such as WinHex
  - Record hexadecimal values in the header and use them to define a file type
- Example:
  - XIF file format is old, little information is available
  - The first 3 bytes of an XIF file are the same as a TIF file
  - Build your own header search string

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Analyzing Graphics File Headers (2 of 3)

TIF file headers start with hexadecimal 49 49 2A, equivalent to ASCII II

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	49	49	2A	00	6E	EE	05	00	80	0B	4B	2A	07	F8	06	0C	II* nî ▌ K* ø
00000010	00	84	42	20	C0	10	03	FA	18	00	85	C2	62	50	88	2C	▌B À ú ▌ÂbP▌,
00000020	2A	0F	12	88	C6	20	EF	F8	98	08	01	05	01	C2	63	D1	* ▌Æ ïø▌ ÂcÑ
00000030	A8	7C	4E	4D	24	88	45	E4	F2	89	5C	1A	39	2B	96	4C	¨|NM$▌Eäò▌\ 9+▌L
00000040	26	53	39	A4	A6	4B	35	9A	C6	67	13	59	1C	EE	7D	16	&S9¤¦K5▌Æg Y î}
00000050	9B	CC	27	51	27	E4	7C	06	FE	8F	BF	DF	70	87	EC	51	▌Ì'Q'ä| þ ¿ßp▌ìQ
00000060	FF	1C	01	80	C0	C0	00	15	56	3F	0E	86	BF	A9	00	60	ÿ €ÀÀ V? ▌¿© `
00000070	48	28	00	FD	B0	00	1F	6F	CA	2D	6A	91	58	9B	42	00	H(ý° oÊ-j´X▌B
00000080	51	C0	10	06	38	04	7D	D3	40	36	B8	80	00	09	5F	B9	QÀ 8 }Ó@6¸▌ _¹
00000090	D2	61	8F	E0	14	86	DA	05	B5	43	29	F1	C8	BB	F9	F5	Òa à ▌Ú µC)ñÈ»ùõ
000000A0	4B	84	51	41	00	4C	03	F9	FE	FA	C4	D2	00	A0	7C	03	K▌QA L ùþúÄÒ |
000000B0	E6	C3	05	8F	48	24	51	F0	04	86	29	26	00	D1	61	00	æÃ H$Qõ ▌)& Ña

Figure 8-17 A TIF file open in WinHex

Source: X-Ways AG, *www.x-ways.net*

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Analyzing Graphics File Headers (3 of 3)

XIF file header

ASCII equivalent shows the same beginning values as a TIF extension

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	49	49	2A	00	5C	01	00	00	20	65	58	74	65	6E	64	65	II* \ eXtende
00000010	64	20	03	00	05	00	01	00	34	00	00	00	02	00	40	00	d 4 @
00000020	00	00	03	00	00	00	00	00	05	00	00	00	00	00	04	00	
00000030	00	00	00	00	01	00	20	00	01	00	B4	00	00	00	00	00	
00000040	6F	00	41	75	74	68	6F	72	00	58	65	72	6F	78	00	43	o Author Xerox C
00000050	6F	72	70	00	00	44	61	74	65	00	4A	75	6C	00	32	31	orp Date Jul 21
00000060	20	31	39	39	39	00	43	6F	70	79	72	69	67	68	74	00	1999 Copyright
00000070	43	6F	70	79	72	69	67	68	74	00	28	43	29	00	31	39	Copyright (C) 19
00000080	39	35	2D	31	39	39	36	00	58	65	72	6F	78	00	43	6F	95-1996 Xerox Co
00000090	72	70	6F	72	61	74	69	6F	6E	2C	20	41	6C	6C	20	52	rporation, All R
000000A0	69	67	68	74	73	20	52	65	73	65	72	76	65	64	00	00	ights Reserved
000000B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	

Figure 8-18 An XIF file open in WinHex

Source: X-Ways AG, *www.x-ways.net*

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Tools for Viewing Images

- After recovering a graphics file
  - Use an image viewer to open and view it
- No one viewer program can read every file format
  - Having many different viewer programs is best
- Most GUI forensics tools include image viewers that display common image formats
- Be sure to analyze, identify, and inspect every unknown file on a drive

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding Steganography in Graphics Files (1 of 7)

- Steganography hides information inside image files
  - An ancient technique
- Two major forms: insertion and substitution
- Insertion
  - Hidden data is not displayed when viewing host file in its associated program
    - You need to analyze the data structure carefully
  - Example: Web page

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding Steganography in Graphics Files (2 of 7)

Figure 8-19 A simple Web page displayed in a Web browser

Source: The Mozilla Foundation, *www.mozilla.org*

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding Steganography in Graphics Files (3 of 7)

GFCIweb.html - Notepad

File Edit Format View Help

```
<html>
<head>
<title> Computer Forensics and Investigations </title>
</head>

<input type="hidden" name="message" value="This is an example of how you could communicate using web pages">
<body>
<h1> The computer forensics book is using steganography </h1>

</body>
</html>
```

Figure 8-20 The HTML code reveals hidden text

Source: The Mozilla Foundation, *www.mozilla.org*

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding Steganography in Graphics Files (4 of 7)

- Substitution
  - Replaces bits of the host file with other bits of data
  - Usually change the last two LSBs (**least significant bit**)
  - Detected with steganalysis tools (a.k.a - steg tools)
- You should inspect all files for evidence of steganography
- Clues to look for:
  - Duplicate files with different hash values
  - Steganography programs installed on suspect's drive

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding Steganography in Graphics Files (5 of 7)

Table 8-1	Bit breakdown of a secret message
Original Pixel	**Altered Pixel**
1010 1010	1010 1001
1001 1101	1001 1110
1111 0000	1111 0011
0011 1111	0011 1100

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding Steganography in Graphics Files (6 of 7)

Figure 8-21 Original and altered images

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding Steganography in Graphics Files (7 of 7)

My secret bank accounts:

Country	Bank	Account No.	Passcode	Currency Amt.
Swiss	Swiss National SA	26845622	Y1115AQ	1.2 million CHF
Caymen Is.	Caribbean Intn. Bank Ltd.	5589999	SAMMM242	5.82 million KYD
Malta	Valletta Nat. Bank Limited	57896165	558TF558	2.3 million EUR
Hong Kong	Chan Wag Bank	A5AA59	665308888	8.9 million HKD
South Africa	Rand Bank of Cape Town	6982543	AAF8	0.53 million ZAL

Figure 8-22 A hidden message in the altered image

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Using Steganalysis Tools

- Use steg tools to detect, decode, and record hidden data
- Detect variations of the graphic image
  - When done correctly you cannot detect hidden data in most cases
- Check to see whether the file size, image quality, or file extensions have changed

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding Copyright Issues with Graphics

- Steganography has been used to protect copyrighted material
  - By inserting digital watermarks into a file
- Digital investigators need to aware of copyright laws
- Copyright laws for Internet are not clear
  - There is no international copyright law
- Check the U.S. Copyright Office
  - U.S. Copyright Office identifies what can and can't be covered under copyright law in U.S.
- **Fair use**
  - Another guideline to consider

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Summary (1 of 3)

- Three types of graphics files
  - Bitmap
  - Vector
  - Metafile
- Image quality depends on various factors
- Standard file formats: .gif, .jpeg, .bmp, and .tif
- Nonstandard file formats: .tga, .rtl, .psd, and .svg
- Some image formats compress their data
  - Lossless compression
  - Lossy compression

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Summary (2 of 3)

- Digital camera photos are typically in raw and EXIF JPEG formats
- Recovering image files
  - Carving file fragments
  - Rebuilding image headers
- The Internet is best for learning more about file formats and their extensions
- Software
  - Image editors
  - Image viewers

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Summary (3 of 3)

- Steganography
  - Hides information inside image files
  - Forms
    - Insertion
    - Substitution
- Steganalysis
  - Finds whether image files hide information
- Fair use allows using copyrighted material for noncommercial or educational purposes without having to compensate the material's originator or owner

CENGAGE

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Guide to Computer Forensics and Investigations Sixth Edition

Chapter 9

Digital Forensics Analysis and Investigation

CENGAGE

Objectives

- Determine what data to analyze in a digital forensics investigation
- Explain tools used to validate data
- Explain common data-hiding techniques

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Determining What Data to Collect and Analyze (1 of 2)

- Examining and analyzing digital evidence depend on the nature of the investigation
  - And the amount of data to process
- **Scope creep** - when an investigation expands beyond the original description
  - Because of unexpected evidence found
  - Attorneys may ask investigators to examine other areas to recover more evidence
  - Increases the time and resources needed to extract, analyze, and present evidence

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Determining What Data to Collect and Analyze (2 of 2)

- Scope creep has become more common
  - Criminal investigations require more detailed examination of evidence just before trial
  - To help prosecutors fend off attacks from defense attorneys
- New evidence often isn't revealed to prosecution
  - It's become more important for prosecution teams to ensure they have analyzed the evidence exhaustively before trial

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Approaching Digital Forensics Cases (1 of 4)

- Begin a case by creating an investigation plan that defines the:
  - Goal and scope of investigation
  - Materials needed
  - Tasks to perform
- The approach you take depends largely on the type of case you're investigating
  - Corporate, civil, or criminal

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Approaching Digital Forensics Cases (2 of 4)

- Follow these basic steps for all digital forensics investigations:
  - 1. For target drives, use recently wiped media that have been reformatted and inspected for viruses
  - 2. Inventory the hardware on the suspect's computer, and note condition of seized computer
  - 3. For static acquisitions, remove original drive and check the date and time values in system's CMOS
  - 4. Record how you acquired data from the suspect drive

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Approaching Digital Forensics Cases (3 of 4)

- Follow these basic steps for all digital forensics investigations (cont'd):
  - 5. Process drive's contents methodically and logically
  - 6. List all folders and files on the image or drive
  - 7. Examine contents of all data files in all folders
  - 8. Recover file contents for all password-protected files
  - 9. Identify function of every executable file that doesn't match hash values
  - 10. Maintain control of all evidence and findings

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Approaching Digital Forensics Cases (4 of 4)

- Refining and Modifying the Investigation Plan
  - Even if initial plan is sound, at times you may need to deviate from it and follow evidence
  - Knowing the types of data to look for helps you make the best use of your time
  - The key is to start with a plan but remain flexible in the face of new evidence

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Using Autopsy to Analyze Data (1 of 6)

- Autopsy can perform forensics analysis on the following file systems:
  - Microsoft FAT, NTFS, ExFAT, UFS1, and UFS2
  - ISO 9660 and YAFFS2
  - Mac HFS+ and HFSX
  - Linux Ext2fs, Ext3fs, and Ext4fs
- Autopsy can analyze data from several sources
  - Including image files from other vendors

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Using Autopsy to Analyze Data (2 of 6)

- Autopsy can handle many formats, including:
  - Raw, Expert Witness, and virtual machine image files (.vdi and .vhd)
- Has an indexed version of the NIST National Software Reference Library (NSRL) of MD5 hashes
- Installing NSRL Hashes in Autopsy
  - Need to download the latest version

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Using Autopsy to Analyze Data (3 of 6)

Figure 9-1 The Hash Databases options

Source: *www.sleuthkit.org*

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Using Autopsy to Analyze Data (4 of 6)

- Collecting Hash Values in Autopsy
  - Create a hash database of known files of interest

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Using Autopsy to Analyze Data (5 of 6)

Figure 9-3 The Configure Ingest Modules window

Source: *www.sleuthkit.org*

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Using Autopsy to Analyze Data (6 of 6)

	A	D	E	F	G	H	I
1	Tag	Modified Time	Changed Time	Accessed Time	Created Time	Size (Bytes)	Hash
2	Special Project-A	2017-07-18 17:14:08 PDT	2017-07-18 17:14:08 PDT	2017-07-18 17:14:08 PDT	2017-07-18 17:14:08 PDT	1612854	ac2b0302898631a7b2e1feb5bd50bd1e
3	Special Project-A	2017-07-18 17:14:08 PDT	2017-07-18 17:14:08 PDT	2017-07-18 17:14:08 PDT	2017-07-18 17:14:08 PDT	55805	685f50ac4b7a03a87c8b98d1220269fa
4	Special Project-A	2017-07-18 17:14:08 PDT	2017-07-18 17:14:08 PDT	2017-07-18 17:14:08 PDT	2017-07-18 17:14:08 PDT	1612854	385f3e2f21a52c0d0d5e8cf41673b26f
5	Special Project-A	2017-07-18 17:14:08 PDT	2017-07-18 17:14:08 PDT	2017-07-18 17:14:08 PDT	2017-07-18 17:14:08 PDT	49519	ed81b47e8e6ca096194f86cf8a513feb
6							
7							
8							
9							

Figure 9-7 Hash values for Special Project files

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Validating Forensic Data

- Ensuring the integrity of data collected is essential for presenting evidence in court
- Most forensic tools offer hashing of image files
- Using advanced hexadecimal editors ensures data integrity

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Validating with Hexadecimal Editors (1 of 6)

- Advanced hexadecimal editors offer features not available in digital forensics tools, such as:
  - Hashing specific files or sectors
- With the hash value in hand
  - You can use a forensics tool to search for a suspicious file that might have had its name changed to look like an innocuous file
- WinHex provides MD5 and SHA-1 hashing algorithms

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Validating with Hexadecimal Editors (2 of 6)

Figure 9-10 Viewing a file opened in WinHex

Source: X-Ways AG, *www.x-ways.net*

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Validating with Hexadecimal Editors (3 of 6)

Figure 9-11 The Compute hash dialog box

Source: X-Ways AG, *www.x-ways.net*

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Validating with Hexadecimal Editors (4 of 6)

Figure 9-12 MD5 hash results

Source: X-Ways AG, *www.x-ways.net*

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Validating with Hexadecimal Editors (5 of 6)

- Advantage of recording hash values
  - You can determine whether data has changed
- **Block-wise hashing**
  - A process that builds a data set of hashes of sectors from the original file
  - Then examines sectors on the suspect's drive to see whether any other sectors match
  - If an identical hash value is found, you have confirmed that the file was stored on the suspect's drive

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Validating with Hexadecimal Editors (6 of 6)

- Using Hash Values to Discriminate Data
  - AccessData has its own hashing database, **Known File Filter (KFF)**
  - KFF filters known program files from view and contains has values of known illegal files
  - It compares known file hash values with files on your evidence drive to see whether they contain suspicious data
  - Other digital forensics tools can import the NSRL database and run hash comparisons

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Validating with Digital Forensics Tools (1 of 3)

- In AccessData FTK Imager, when selecting the Expert Witness (.e01) or SMART (.s01) format:
  - Additional options for hashing all the data are available
  - Validation report lists MD5 and SHA-1 hash values
- Follow steps starting on page 393 to see how to use WinHex to hash an image file and then compare it with the original hash value FTK Imager calculated

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Validating with Digital Forensics Tools (2 of 3)

InChap09.dd.txt - Notepad

File Edit Format View Help

```
Created By AccessData® FTK® Imager 3.1.1.8

Case Information:
Acquired using: ADI3.1.1.8
Case Number: InChap09
Evidence Number: InChap09
Unique description: In chapter exercise
Examiner: Joe Friday
Notes: In chapter exercise on hashing raw image files

--------------------------------------------------------------

Information for C:\Work\Chap09\InChap09:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Logical
[Drive Geometry]
 Bytes per Sector: 512
 Sector Count: 3,074,048
[Physical Drive Information]
 Removable drive: False
 Source data size: 1501 MB
 Sector count:    3074048

ATTENTION:
The following sector(s) on the source drive could not be read:
        1960096 through 1960101
        2061632 through 2061635
The contents of these sectors were replaced with zeros in the image.

[Computed Hashes]
 MD5 checksum:    db945a7e3589743923237c0518ababe1
 SHA1 checksum:   6d87a3665d756b7e22de3d0b087c6ab9ec3f8bf7

Image Information:
 Acquisition started:   Thu Jul 27 15:36:30 2017
 Acquisition finished:  Thu Jul 27 15:38:03 2017
 Segment list:
  C:\Work\Chap09\InChap09.001
```

Figure 9-14 The FTK Imager case information file

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Validating with Digital Forensics Tools (3 of 3)

```
[Computed Hashes]
 MD5 checksum:     db945a7e3589743923237c0518ababe1
 Verified MD5:     DB945A7E3589743923237C0518ABABE1
 SHA1 checksum:    6d87a3665d756b7e22de3d0b087c6ab9ec3f8bf7
```

Figure 9-15 Recording the MD5 hash value

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Addressing Data-Hiding Techniques

- Data hiding - changing or manipulating a file to conceal information
- Techniques:
  - Hiding entire partitions
  - Changing file extensions
  - Setting file attributes to hidden
  - Bit-shifting
  - Using encryption
  - Setting up password protection

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Hiding Files by Using the OS

- One of the first techniques to hide data:
  - Changing file extensions
- Advanced digital forensics tools check file headers
  - 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
- Another hiding technique
  - Selecting the Hidden attribute in a file's Properties dialog box

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Hiding Partitions (1 of 4)

- By using the Windows `diskpart remove letter` command
  - You can unassign the partition's letter, which hides it from view in File Explorer
- To unhide, use the `diskpart assign letter` command
- Other disk management tools:
  - IM-Magic, EaseUS Partition Master, and Linux Grand Unified Bootloader (GRUB)

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Hiding Partitions (2 of 4)

- To detect whether a partition has been hidden
  - Account for all disk space when examining an evidence drive
  - Analyze any disk areas containing space you can’t account for
- Many digital forensics tools can detect and view a hidden partition

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Hiding Partitions (3 of 4)

Figure 9-16 The Disk Management window

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Hiding Partitions (4 of 4)

Figure 9-18 Viewing a hidden partition in Autopsy

Source: *www.sleuthkit.org*

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Marking Bad Clusters

- A data-hiding technique used in FAT file systems is placing sensitive or incriminating data in free or slack space on disk partition clusters
  - Involves using old utilities such as Norton DiskEdit
- Can mark good clusters as bad clusters in the FAT table so the OS considers them unusable
  - Only way they can be accessed from the OS is by changing them to good clusters with a disk editor
- DiskEdit runs only in MS-DOS and can access only FAT-formatted disk media

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Bit-Shifting (1 of 4)

- Some users use a low-level encryption program that changes the order of binary data
  - Makes altered data unreadable to secure a file, users run an assembler program (also called a “macro”) to scramble bits
  - Run another program to restore the scrambled bits to their original order
- **Bit shifting** changes data from readable code to data that looks like binary executable code
- WinHex and Hex Workshop includes a feature for shifting bits

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Bit-Shifting (2 of 4)

Figure 9-19 `Bit_shift.txt` open in WinHex

Source: X-Ways AG, *www.x-ways.net*

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Bit-Shifting (3 of 4)

Figure 9-20 The Modify Block Data dialog box

Source: *X-Ways AG, www.x-ways.net*

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Bit-Shifting (4 of 4)

Figure 9-21 Viewing the shifted bits

Source: X-Ways AG, *www.x-ways.net*

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding Steganalysis Methods (1 of 3)

- **Steganography** - comes from the Greek word for “hidden writing”
  - Hiding messages in such a way that only the intended recipient knows the message is there
- Steganalysis - term for detecting and analyzing steganography files
- Digital watermarking - developed as a way to protect file ownership
  - Usually not visible when used for steganography

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding Steganalysis Methods (2 of 3)

- A way to hide data is to use steganography tools
  - Many are freeware or shareware
  - Insert information into a variety of files
- If you encrypt a plaintext file with PGP and insert the encrypted text into a steganography file
  - Cracking the encrypted message is extremely difficult

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding Steganalysis Methods (3 of 3)

- Steganalysis methods
  - Stego-only attack
  - Known cover attack
  - Known message attack
  - Chosen stego attack
  - Chosen message attack

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Examining Encrypted Files

- To decode an encrypted file
  - Users supply a password or passphrase
- Many encryption programs use a technology called "**key escrow**"
  - Designed to recover encrypted data if users forget their passphrases or if the user key is corrupted after a system failure
- Key sizes of 128 bits to 4096 bits make breaking them nearly impossible with current technology

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Recovering Passwords (1 of 4)

- Password-cracking tools are available for handling password-protected data or systems
  - Some are integrated into digital forensics tools
- Stand-alone tools:
  - Last Bit
  - AccessData PRTK
  - ophcrack
  - John the Ripper
  - Passware

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Recovering Passwords (2 of 4)

- Brute-force attacks
  - Use every possible letter, number, and character found on a keyboard
  - This method can require a lot of time and processing power
- Dictionary attack
  - Uses common words found in the dictionary and tries them as passwords
  - Most use a variety of languages

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Recovering Passwords (3 of 4)

- With many programs, you can build profiles of a suspect to help determine his or her password
- Many password-protected OSs and application store passwords in the form of MD5 or SHA hash values
- A brute-force attack requires converting a dictionary password from plaintext to a hash value
  - Requires additional CPU cycle time

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Recovering Passwords (4 of 4)

- **Rainbow table**
  - A file containing the hash values for every possible password that can be generated from a computer's keyboard
  - No conversion necessary, so it is faster than a brute-force or dictionary attack
- **Salting passwords**
  - Alters hash values and makes cracking passwords more difficult

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Summary (1 of 2)

- Examining and analyzing digital evidence depend on the nature of the investigation and the amount of data to process
- General procedures:
  - Wipe and prepare target drives, document all hardware components on the suspect's computer, check date and time values in the suspect's computer's CMOS, acquire data and document steps, list all folders and files, attempt to open password-protected files, determine function of executable files, and document steps

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Summary (2 of 2)

- Advanced digital forensics tools have features such as indexing text data, making keyword searches faster
- A critical aspect of digital forensics is validating digital evidence
  - Ensuring the integrity of data you collect is essential for presenting evidence in court
- Data hiding involves changing or manipulating a file to conceal information
- Three ways to recover passwords:
  - Dictionary attacks
  - Brute-force attacks
  - Rainbows tables

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Guide to Computer Forensics and Investigations Sixth Edition

Chapter 10

Virtual Machine Forensics, Live Acquisitions, and Network Forensics

CENGAGE

Objectives

- Explain standard procedures for conducting forensic analysis of virtual machines
- Describe the process of a live acquisition
- Explain network intrusions and unauthorized access
- Describe standard procedures in network forensics and network-monitoring tools

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

An Overview of Virtual Machine Forensics (1 of 2)

- Virtual machines are common for both personal and business use
- Investigators need to know how to analyze them and use them to analyze other suspect drives
- The software that runs virtual machines is called a “hypervisor”
- Two types of **hypervisor**:
  - **Type 1** - loads on physical hardware and doesn’t require a separate OS
  - **Type 2** - rests on top of an existing OS

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

An Overview of Virtual Machine Forensics (2 of 2)

- Type 2 hypervisors are usually the ones you find loaded on a suspect machine
- Type 1 hypervisors are typically loaded on servers or workstations with a lot of RAM and storage

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Type 2 Hypervisors (1 of 4)

- Before installing a type 2 hypervisor, enable virtualization in the BIOS before attempting to create a VM
- **Virtualization Technology (VT)** - Intel's CPU design for security and performance enhancements that enable the BIOS to support virtualization
- **Virtualization Machine Extensions (VMX)** - instruction sets created for Intel processors to handle virtualization

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Type 2 Hypervisors (2 of 4)

- Most widely used type 2 hypervisors:
  - Parallels Desktop - created for Macintosh users who also use Windows applications
  - KVM (Kernel-based Virtual Machine) - for Linux OS
  - Microsoft Hyper-V - new hypervisor built into Windows 10
  - VMware Workstation and Player - can be installed on almost any device, including tablets
    - Can install Microsoft Hyper-V Server on it
    - Can create encrypted VMs
    - Can support up to 16 CPUs, 8 TB storage, and 20 VM

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Type 2 Hypervisors (3 of 4)

Figure 10-2 The default location of VMware Workstation Player files

Source: VMware, *www.vmware.com*

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Type 2 Hypervisors (4 of 4)

- Most widely used type 2 hypervisors (cont'd):
  - VirtualBox - supports all Windows and Linux OSs as well as Macintosh and Solaris
    - Allows selecting types associated with other applications, such as VMware VMDK type or the Parallels HDD type
- Type 2 hypervisors come with templates for different OSs

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Conducting an Investigation with Type 2 Hypervisors (1 of 9)

- Begin by acquiring a forensic image of the host computer as well as network logs
  - By linking the VM's IP address to log files, you may determine what Web sites the VM accessed
- To detect whether a VM is on a host computer:
  - Look in the Users or Documents folder (in Windows) or user directories (in Linux)
  - Check the host's Registry for clues that VMs have been installed or uninstalled
  - Existence of a virtual network adapter

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Conducting an Investigation with Type 2 Hypervisors (2 of 9)

Figure 10-7 Ethernet Connections on a Windows 10 computer

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Conducting an Investigation with Type 2 Hypervisors (3 of 9)

- In addition to searching for network adapters, you need to determine whether USB drives have been attached to the host
  - They could have live VMs running on them
- A VM can also be nested inside other VMs on the host machine or a USB drive
  - Some newer Windows systems log when USB drives are attached
  - Search the Windows Registry or the system log files

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Conducting an Investigation with Type 2 Hypervisors (4 of 9)

Figure 10-9 A VM nested inside another VM

Source: VMware, *www.vmware.com*

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Conducting an Investigation with Type 2 Hypervisors (5 of 9)

- Follow a consistent procedure:
  - 1. Image the host machine
  - 2. Locate the virtualization software and VMs, using information learned about file extensions and network adapters
  - 3. Export from the host machine all files associated with VMs
  - 4. Record the hash values of associated files
  - 5. Open a VM as an image file in forensics software and create a forensic image or mount the VM as a drive

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Conducting an Investigation with Type 2 Hypervisors (6 of 9)

- Live acquisitions of VMs are often necessary
  - They include all snapshots, which records the state of a VM at a particular moment (records only changes in state, not a complete backup)
- When acquiring an image of a VM file, snapshots might not be included
  - In this case, you have only the original VM
- Doing live acquisitions of VMs is important to make sure snapshots are incorporated

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Conducting an Investigation with Type 2 Hypervisors (7 of 9)

- Follow the steps in the activity on page 426 to see how to examine your own system for evidence of a VM
- Follow the steps starting on page 427 to acquire an image of a VM

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Conducting an Investigation with Type 2 Hypervisors (8 of 9)

- Other VM Examination Methods
  - FTK Imager, Magnet AXIOM and OSForensics can mount VMs as an external drive
    - By mounting a VM as a drive, you can make it behave more like a physical computer
    - Allows you to use the same standard examination procedures for a static hard drive
  - Make a copy of a VM's forensic image and open the copy while it's running
    - Start it as a live VM so that forensics software can be used to search for clues

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Conducting an Investigation with Type 2 Hypervisors (9 of 9)

- Using VMs as Forensic Tools
  - Investigators can use VMs to run forensics tools stored on USB drives
- Follow steps starting on page 430 to see how to set up a VM on a USB drive

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Working with Type 1 Hypervisors (1 of 2)

- This section is meant to help you understand the impact Type 1 hypervisors have on forensic investigations
  - Having a good working relationship with network administrators and lead technicians can be helpful
- Type 1 hypervisors are installed directly on hardware
  - Can be installed on a VM for testing purposes
  - Capability is limited only by the amount of available RAM, storage, and throughput

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Working with Type 1 Hypervisors (2 of 2)

- Common type 1 hypervisors:
  - VMware vSphere
  - Microsoft Hyper-V 2016
  - XenProject XenServer
  - IBM PowerVM
  - Parallels Desktop for Mac
- Follow steps starting on page 433 to install XenServer as a VM in VirtualBox

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Performing Live Acquisitions (1 of 2)

- Live acquisitions are especially useful when you're dealing with active network intrusions or attacks
- Live acquisitions done before taking a system offline are also becoming a necessity
  - Attacks might leave footprints only in running processes or RAM
- Live acquisitions don't follow typical forensics procedures
- **Order of volatility (OOV)**
  - How long a piece of information lasts on a system

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Performing Live Acquisitions (2 of 2)

- Steps
  - Create or download a bootable forensic CD or USB drive
  - Make sure you keep a log of all your actions
  - A network drive is ideal as a place to send the information you collect
  - Copy the physical memory (RAM)
  - The next step varies, depending on the incident you're investigating
  - Be sure to get a forensic digital hash value of all files you recover during the live acquisition

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Performing a Live Acquisition in Windows

- Several tools are available to capture the RAM.
  - Mandiant Memoryze
  - Belkasoft RamCapturer
  - Kali Linux (updated version of BackTrack)
- GUI tools are easy to use
  - But they often require a lot of system resources
  - Might get false readings in Windows OSs
- Command-line tools give you more control

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Network Forensics Overview

- **Network forensics**
  - Process of collecting and analyzing raw network data and tracking network traffic
    - To ascertain how an attack was carried out or how an event occurred on a network
- Intruders leave a trail behind
  - Knowing your network's typical traffic patterns is important in spotting variations in network traffic
- Can also help you determine whether a network is truly under attack

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

The Need for Established Procedures

- Network forensics examiners must establish standard procedures for how to acquire data after an attack or intrusion
  - Essential to ensure that all compromised systems have been found
- Procedures must be based on an organization's needs and complement network infrastructure
- NIST created "Guide to Integrating Forensic Techniques into Incident Response" to address these needs

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Securing a Network (1 of 2)

- **Layered network defense strategy**
  - Sets up layers of protection to hide the most valuable data at the innermost part of the network
- **Defense in depth (DiD)**
  - Similar approach developed by the NSA
  - Modes of protection
    - People
    - Technology
    - Operations

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Securing a Network (2 of 2)

- Testing networks is as important as testing servers
- You need to be up to date on the latest methods intruders use to infiltrate networks
  - As well as methods internal employees use to sabotage networks
- Small companies of fewer than 10 employees often don't consider security precautions against internal threats necessary
  - Can be more susceptible to problems caused by employees revealing proprietary information

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Developing Procedures for Network Forensics (1 of 2)

- Network forensics can be a long, tedious process
- Standard procedure that is often used:
  - Always use a standard installation image for systems on a network
  - Fix any vulnerability after an attack
  - Attempt to retrieve all volatile data
  - Acquire all compromised drives
  - Compare files on the forensic image to the original installation image

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Developing Procedures for Network Forensics (2 of 2)

- In digital forensics
  - You can work from the image to find most of the deleted or hidden files and partitions
- In network forensics
  - You have to restore drives to understand attack

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Reviewing Network Logs

- Network logs record ingoing and outgoing traffic
  - Network servers
  - Routers
  - Firewalls
- Tcpdump and Wireshark - tools for examining network traffic
  - Can generate top 10 lists
  - Can identify patterns

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Using Network Tools

- Variety of tools
  - Splunk
  - Spiceworks
  - Nagios
  - Cacti

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Using Packet Analyzers (1 of 5)

- **Packet analyzers**
  - Devices or software that monitor network traffic
  - Most work at layer 2 or 3 of the OSI model
- Most tools follow the Pcap (packet capture) format
- Some packets can be identified by examining the flags in their TCP headers
- Tools
  - `Tcpdump`
  - `Tethereal`

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Using Packet Analyzers (2 of 5)

Figure 10-15 A TCP header

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Using Packet Analyzers (3 of 5)

- Tools (cont'd)
  - Tcpslice
  - Tcpreplay
  - Etherape
  - Netdude
  - Argus
  - Wireshark
    - Follow the steps starting on page 442 to see how the Wireshark tool works

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Using Packet Analyzers (4 of 5)

Figure 10-16 The opening window in Wireshark

Source: Wireshark Foundation, *www.wireshark.org*

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Using Packet Analyzers (5 of 5)

Figure 10-17 Following a UDP stream

Source: Wireshark Foundation, *www.wireshark.org*

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Investigating Virtual Networks

- Virtual switch is a little different from a physical switch
  - There's no spanning tree between virtual switches
- Additional complications
  - Hypervisors can assign MAC addresses to virtual devices
  - Devices can have the same MAC address on different virtual networks
  - Cloud service providers host networks for several to hundreds of companies
- Tools
  - Wireshark
  - Network Miner

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Examining the Honeynet Project (1 of 2)

- The Honeynet Project was developed to make information widely available in an attempt to thwart Internet and network attackers
  - Provides information about attacks methods and how to protect against them
- Objectives are awareness, information, and tools
- **Distributed denial-of-service (DDoS) attacks**
  - A major threat that may go through other organizations' networks, not just yours
  - Hundreds or even thousands of machines (**zombies**) can be used

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Examining the Honeynet Project (2 of 2)

- **Zero day attacks**
  - Another major threat
  - Attackers look for holes in networks and OSs and exploit these weaknesses before patches are available
- **Honeypot**
  - Normal looking computer that lures attackers to it
- **Honeywalls**
  - Monitor what's happening to honeypots on your network and record what attackers are doing

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Summary (1 of 3)

- Virtual machines are used extensively in organizations and are a common part of forensic investigations
- There are two types of hypervisors for running virtual machines: Type 1 and Type 2
- Virtualization Technology is Intel's CPU design for security and performance enhancements that enable the BIOS to support virtualization
- Forensic procedures for VMs start by creating an image of the host machine, and then exporting files associated with a VM

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Summary (2 of 3)

- Live acquisitions are necessary to retrieve volatile items, such as RAM and running processes
- Network forensics is the process of collecting and analyzing raw network data and systematically tracking network traffic to ascertain how an attack took place
- Steps must be taken to harden networks before a security breach happens
- Being able to spot variations in network traffic can help you track intrusions

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Summary (3 of 3)

- Several tools are available for monitoring network traffic, such as packet analyzers and honeypots
- The Honeynet Project is designed to help people learn the latest intrusion techniques that attackers are using

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Guide to Computer Forensics and Investigations Sixth Edition

Chapter 11

E-mail and Social Media Investigations

CENGAGE

Objectives

- Explain the role of e-mail in investigations
- Describe client and server roles in e-mail
- Describe tasks in investigating e-mail crimes and violations
- Explain the use of e-mail server logs
- Describe some specialized e-mail forensics tools
- Explain how to apply digital forensics methods to investigating social media communications

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Exploring the Role of E-mail in Investigations (1 of 2)

- An increase in e-mail scams and fraud attempts with phishing or spoofing
  - Investigators need to know how to examine and interpret the unique content of e-mail messages
- **Phishing** e-mails contain links to text on a Web page
  - Attempts to get personal information from reader
- **Pharming** - DNS poisoning takes user to a fake site
- A noteworthy e-mail scam was 419, or the Nigerian Scam

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Exploring the Role of E-mail in Investigations (2 of 2)

- **Spoofing** e-mail can be used to commit fraud
- Investigators can use the **Enhanced/Extended Simple Mail Transfer Protocol (ESMTP)** number in the message's header to check for legitimacy of email

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Exploring the Roles of the Client and Server in E-mail (1 of 3)

- E-mail can be sent and received in two environments
  - Internet
  - Intranet (an internal network)
- **Client/server architecture**
  - Server OS and e-mail software differs from those on the client side
- Protected accounts
  - Require usernames and passwords

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Exploring the Roles of the Client and Server in E-mail (2 of 3)

Figure 11-1 E-mail in a client/server architecture

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Exploring the Roles of the Client and Server in E-mail (3 of 3)

- Name conventions
  - Corporate: john.smith@somecompany.com
  - Public: whatever@gmail.com
  - Everything after @ belongs to the domain name
- Tracing corporate e-mails is easier
  - Because accounts use standard names the administrator establishes
- Many companies are migrating their e-mail services to the cloud

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Investigating E-mail Crimes and Violations (1 of 2)

- Similar to other types of investigations
- Goals
  - Find who is behind the crime
  - Collect the evidence
  - Present your findings
  - Build a case
- Know the applicable privacy laws for your jurisdiction
  - **Electronic Communications Privacy Act (ECPA)** and the **Stored Communications Act (SCA)** apply to e-mail.

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Investigating E-mail Crimes and Violations (2 of 2)

- E-mail crimes depend on the city, state, or country
  - Example: spam may not be a crime in some states
  - Always consult with an attorney
- Examples of crimes involving e-mails
  - Narcotics trafficking
  - Extortion
  - Sexual harassment and stalking
  - Fraud
  - Child abductions and pornography
  - Terrorism

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding Forensic Linguistics

- **Forensic Linguistics**
  - Where language and law intersect
- Four categories:
  - Language and law
  - Language in the legal process
  - Language as evidence
  - Research/teaching
- Encompasses civil cases, criminal cases, cyberterrorism cases, and other legal proceedings

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Examining E-mail Messages (1 of 2)

- Access victim's computer or mobile device to recover the evidence
- Using the victim's e-mail client
  - Find and copy any potential evidence
  - Access protected or encrypted material
  - Print e-mails
- Guide victim on the phone
  - Open and copy e-mail including headers
- You may have to recover deleted e-mails

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Examining E-mail Messages (2 of 2)

- 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 e-mail address
- With many GUI e-mail programs, you can copy an e-mail by dragging it to a storage medium
  - Or by saving it in a different location

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Viewing E-mail Headers (1 of 5)

- Investigators should learn how to find e-mail headers
  - GUI clients
  - Web-based clients
- After you open e-mail headers, copy and paste them into a text document
  - So that you can read them with a text editor
- Become familiar with as many e-mail programs as possible
  - Often more than one e-mail program is installed

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Viewing E-mail Headers (2 of 5)

- Outlook
  - Double-click the message and then click **File, Properties**
  - Copy headers
  - Paste them to any text editor
  - Save the document as `Outlook header.txt` in your work folder

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Viewing E-mail Headers (3 of 5)

Figure 11-2 An Outlook e-mail header

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Viewing E-mail Headers (4 of 5)

- Gmail
  - Click the down arrow next to the Reply circular arrow, and click **Show original**
  - Click the **Download Original** link to open the “Opening original_msg.txt” dialog box
  - Click **Open with Notepad (default)** and click **Okay**
  - Save the file in your work folder with the default name
- Yahoo
  - Click **Inbox** to view a list of messages
  - Above the message window, click **More** and click **View Raw Message**
  - Copy and paste headers to a text file

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Viewing E-mail Headers (5 of 5)


```
X-Apparently-To:                _           Mon, 11 Sep 2017 17:24:24 +0000
Return-Path: <LCwMzCwMbLSsHJzsbCwM7LRGtMzsTOxMrKws@smtp-coi-g09-025.aweber.com>
Received-SPF: pass (domain of smtp-coi-g09-025.aweber.com designates 204.194.223.25 as permitted sender)
X-YMailISG: MiNqrvsWLDsdwYue2y_8jUSdLl8maR6_T.d55zY7e6G0ngyy
 ssZsOTvSJvYtoV105Mj28Ri1jcZlAw3GVLNXUMXr9R4mw0WKWp18ulCc3mgR
 XaY8x1W9Cv9V5LTzBHu4Z8VZD12Q_tfXDLaucahaQTQMCaoSfdAgb9r9D61n
 pTnjrzwvquf7DZueBuiKzy9nJ6Val4VRv70iEdIZjiyIQlICm0hA7992w0Tw
 XQ7t3QR.x_dTIwWfCEwkIOrUhcem6QPn83fKKJ9bdOBhnDx_vlkW5c8Wry4D
 glMLouiMPg_30L9ww.lfzRXCQt1pwwzWl_XTMQh7Pl0VT6Xn2kpZ1vVjgcfi
 7HcVAAyrqxEzdhJKXmqrmACBOBUFvSh1PM9LUHi2Gb.b9zNWs4APLc7IIY_t
 .g_vQieX4_pYdvSsCAmsSJ.nmvlATRnUkpXzw.Jm4GHsnv2KWpReWKcS_YDu
 hC_HASKpnxcx81.JEDM0KkhPTA1bjv3_DlItXp8GDScFyv9Rz3ETEeLgKDH8
 6Iantym8.E_zBNCZo2UuxAUmqxpnYgZgpiMCb6.YqOJ78tf_0cGmt8BDIo20
 fWrUTx.0tAhlh8DQz1NHG3120FM9ju3c9KtuPTafQKCZXqznPDAui_uBlRwg
 fi9JboFzFFqdzunZkKrBCMevBKnp85Z1ZahJkQYragNq6es436v36ED1k3x_
 VjqwlLwYM0HuIFpg7z8R.w.Z0gi7Bi8m.WQyTP8dcAOvI6n4Fw5R4E.ILdaC
 KofwXtj7CpBqlCOw3r6PVyDYEygH6Z_83he7qG6p4H4cv7zHR6mdiygIg1Ku
 caS2UytV9MD16I_fMx6auvqi6UhgrQTvG4i7K6V.kbTQEBqDDfbmt3J0pD7W
 ElUcHFlhzf0lhRkRuXuEpIOu..NYvRRkkU2mnFPAxDh9eqUlpsXyv9plyqP9
 ZpRpE6siCkiUcesmJAUNK0RhEwzAmoNwNmkqH60.o1vwOc3pA_2YlKNbDeXS
 eUQ5JU5hRpaPMn2CqMyyHdj9WSyaxSRSCnJMPKrq4J68h3esSW9y8jH_hBFS
 aZ13BFqlfVEc9_5_P9_UqM3LMJY6YvH4126IAQgRz3KSKHkYmWmXJMnOXxOe
 Oz0oBf6D4jfvkVTDTcVeRPeEaDrEQuCTrQffMd6lZtgx25AqzzJufor61ogC
 .ee.pCy.La7YDn9UpHKnIt6iz_yD9Wtwop6gKy96bxiWdTx8v9Waa0GWLJ1y
 JwYhK6BSd95iH2cgiVUV7fQYhXvoUypBca.Ar4sq2yoEhXzy3Sqm90jXKh_P
 94nzt57KAZYvK.GHpkwHMoaHj1YCdeq1d3k61neDbhiGjJDjzwTRK4FN3krv
 VYQDwVVBx8wjG8qDA7skIT99.tCBu8DR57kC.NtOig--
X-Originating-IP: [204.194.223.25]
Authentication-Results: mta1120.mail.bf1.yahoo.com  from=send.aweber.com; domainkeys=neutral (no sig);
Received: from 127.0.0.1  (EHLO smtp-coi-g09-025.aweber.com) (204.194.223.25)
  by mta1120.mail.bf1.yahoo.com with SMTPS; Mon, 11 Sep 2017 17:24:24 +0000
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=aweber.com;
        s=dkim_s1024; t=1505149312;
        bh=6z2+thX7FQfo+chNPIhWc5SoNUcWciEf11WBF9GXfBs=;
```


Figure 11-3 Viewing headers in Yahoo!

Source: Yahoo! Inc., *www.yahoo.com*

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Examining E-mail Headers (1 of 2)

- Headers contain useful information
  - The main piece of information you're looking for is the originating e-mail's IP address
  - Date and time the message was sent
  - Filenames of any attachments
  - Unique message number (if supplied)

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Examining E-mail Headers (2 of 2)

Outlook header.txt - Notepad

File Edit Format View Help

```
1.      Return-Path: <cr-superior@outlook.com>

2.      Received: from NAM04-CO1-obe.outbound.protection.outlook.com (mail-oln040092010080.outbound.protection.out
        (using TLSv1 with cipher AES256-SHA (256/256 bits))
        (No client certificate requested)
        by mtaiw-aad05.mx.aol.com (Internet Inbound) with ESMTPS id 708E37000008C
        for <b_aspen@aol.com>; Mon, 10 Jul 2017 18:33:12 -0400 (EDT)

3.      DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=outlook.com;
 s=selector1; h=From:Date:Subject:Message-ID:Content-Type:MIME-Version;
 bh=lrZUozDUrSt47+5BKxEkYZkL84z9Xa5pdNS+eLR66fc=;
 b=galykGSNrAUEF2RXwl1P99hjSSA++U4ov0ar636laUQ0ng2y66ARNrNonxnEWhJltKgLXdgpUofKBmH5UTZjYdRJx4q26nZWYoF8o1bQ7h30Gby

4.      Received: from SN1NAM04FT054.eop-NAM04.prod.protection.outlook.com
 (10.152.88.54) by SN1NAM04HT232.eop-NAM04.prod.protection.outlook.com
 (10.152.89.67) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384) id 15.1.1240.9; Mon, 10
 Jul 2017 22:33:04 +0000

5.      Received: from DM3PR14MB1033.namprd14.prod.outlook.com (10.152.88.60) by
 SN1NAM04FT054.mail.protection.outlook.com (10.152.89.2) with Microsoft SMTP
 Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256) id
 15.1.1240.9 via Frontend Transport; Mon, 10 Jul 2017 22:33:04 +0000

6.      Received: from DM3PR14MB1033.namprd14.prod.outlook.com ([10.166.159.17]) by
 DM3PR14MB1033.namprd14.prod.outlook.com ([10.166.159.17]) with mapi id
 15.01.1240.020; Mon, 10 Jul 2017 22:33:03 +0000
```

Figure 11-4 An e-mail header with line numbers added

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Examining Additional E-mail Files

- E-mail messages are saved on the client side or left at the server
- Microsoft Outlook uses .pst and .ost files
- Most e-mail programs also include an electronic address book, calendar, task list, and memos
- In Web-based e-mail
  - Messages are displayed and saved as Web pages in the browser's cache folders
  - Many Web-based e-mail providers also offer instant messaging (IM) services

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Tracing an E-mail Message

- Determining message origin is referred to as “tracing”
- Contact the administrator responsible for the sending server
- Use a registry site to find point of contact:
  - www.arin.net
  - www.internic.com
  - www.google.com
- Verify your findings by checking network e-mail logs against e-mail addresses

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Using Network E-mail Logs (1 of 2)

- Router logs
  - Record all incoming and outgoing traffic
  - Have rules to allow or disallow traffic
  - You can resolve the path a transmitted e-mail has taken
- Firewall logs
  - Filter e-mail traffic
  - Verify whether the e-mail passed through
- You can use any text editor or specialized tools

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Using Network E-mail Logs (2 of 2)

Figure 11-5 A Windows firewall log

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding E-mail Servers (1 of 2)

- An e-mail server is loaded with software that uses e-mail protocols for its services
  - And maintains logs you can examine and use in your investigation
- E-mail storage
  - Database
  - Flat file system
- Logs
  - Some servers are set up to log e-mail transactions by default; others have to be configured to do so

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding E-mail Servers (2 of 2)

- E-mail logs generally identify the following:
  - E-mail messages an account received
  - Sending IP address
  - Receiving and reading date and time
  - E-mail content
  - System-specific information
- Contact suspect's network e-mail administrator as soon as possible
- Servers can recover deleted e-mails
  - Similar to deletion of files on a hard drive

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Examining UNIX E-mail Server Logs (1 of 2)

- Common UNIX e-mail servers: Postfix and Sendmail
- `/etc/sendmail.cf`
  - Configuration file for Sendmail
- `/etc/syslog.conf`
  - Specifies how and which events Sendmail logs
- Postfix has two configuration files
  - `master. cf and main.cf` (found in `/etc/postfix`)

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Examining UNIX E-mail Server Logs (2 of 2)

- `/var/log/maillog`
  - Records **SMTP**, **POP3, and IMAP4** communications
    - Contains an IP address and time stamp that you can compare with the e-mail the victim received
- Default location for storing log files:
  - `/var/log`
  - An administrator can change the log location
  - Use the `find` or `locate` command to find them
- Check UNIX man pages for more information

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Examining Microsoft E-mail Server Logs (1 of 4)

- Microsoft Exchange Server (Exchange)
  - Uses a database
  - Based on Microsoft Extensible Storage Engine (ESE)
- Most useful files in an investigation:
  - .edb database files, checkpoint files, and temporary files
- Information Store files
  - Database files *.edb
    - Responsible for **MAPI** information

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Examining Microsoft E-mail Server Logs (2 of 4)

- Transaction logs
  - Keep track of changes to its data
- Checkpoints
  - Marks the last point at which the database was written to disk
- Temporary files
  - Created to prevent loss when the server is busy converting binary data to readable text

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Examining Microsoft E-mail Server Logs (3 of 4)

- To retrieve log files created by Exchange
  - Use the Windows PowerShell cmdlet `GetTransactionLogStats.ps1 -Gather`
- Tracking.log
  - An Exchange server log that tracks messages
- Another log used for investigating the Exchange environment is the troubleshooting log
  - Use Windows Event Viewer to read the log

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Examining Microsoft E-mail Server Logs (4 of 4)

Figure 11-6 Viewing a log in Event Viewer

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Using Specialized E-mail Forensics Tools (1 of 3)

- Tools include:
  - DataNumen for Outlook and Outlook Express
  - FINALeMAIL for Outlook Express and Eudora
  - Sawmill-Novell GroupWise for log analysis
  - MailXaminer for multiple e-mail formatas and large data sets
  - Fookes Aid4Mail and MailBag Assistant
  - Paraben E-Mail Examiner
  - AccessData FTK for Outlook and Outlook Express
  - Ontrack Easy Recovery EmailRepair
  - R-Tools R-Mail
  - OfficeRecovery's MailRecovery

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Using Specialized E-mail Forensics Tools (2 of 3)

- Tools (continued)
  - MXToolBox for decoding e-mail headers
  - FreeViewer with free tools for various servers
- Tools allow you to find:
  - E-mail database files
  - Personal e-mail files
  - Offline storage files
  - Log files
- Advantage of using data recovery tools
  - You don’t need to know how e-mail servers and clients work to extract data from them

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Using Specialized E-mail Forensics Tools (3 of 3)

- After you compare e-mail logs with messages, you should verify the:
  - Email account, message ID, IP address, date and time stamp to determine whether there's enough evidence for a warrant
- With some tools
  - You can scan e-mail database files on a suspect's Windows computer, locate any e-mails the suspect has deleted and restore them to their original state

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Using Magnet AXIOM to Recover E-mail (1 of 2)

- Magnet AXIOM has two modules:
  - Process
  - Examine
- Follow the steps in the activity on page 472 to learn how to use Magnet AXIOM to recover e-mails

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Using OSForensics to Recover E-mail (2 of 2)

Figure 11-7 Entering information in the CASE DETAILS window

Source: Magnet Forensics, *www.magnetforensics.com*

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Using a Hex Editor to Carve E-mail Messages (1 of 4)

- Few vendors have products for analyzing e-mail in systems other than Microsoft
- **mbox** format
  - Stores e-mails in flat plaintext files
- **Multipurpose Internet Mail Extensions (MIME)** format
  - Used by vendor-unique e-mail file systems, such as Microsoft .pst or .ost
- Example: carve e-mail messages from Evolution

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Using a Hex Editor to Carve E-mail Messages (2 of 4)

Figure 11-10 WinHex displaying the beginning of the e-mail from Terry Sadler

Source: X-Ways AG, *www.x-ways.net*

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Using a Hex Editor to Carve E-mail Messages (3 of 4)

Figure 11-11 WinHex displaying the ending position of the e-mail from Terry Sadler

Source: X-Ways AG, *www.x-ways.net*

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Using a Hex Editor to Carve E-mail Messages (4 of 4)

martha-evolution.txt - Notepad

File Edit Format View Help

```
From terrysadler@goowy.com Sat Feb 17 15:15:45 2007
Received: from smtp-sjt-01.vividround.com ([199.249.224.252]) by        mail.vividround.com with Microsoft
SMTPSVC(6.0.3790.1830); Sat, 17 Feb 2007        15:15:45 -0600
Received: from smtp1.goowy.com (smtp1.goowy.com [209.126.247.205]) by   smtp-sjt-01.vividround.com
(8.12.11/8.12.11) with ESMTP id l1HLAcgD060105  for <martha.dax@superiorbicycles.biz>; Sat, 17 Feb 2007 15:10:38
-0600 (CST)
Received: (qmail 2864 invoked from network); 17 Feb 2007 21:01:53 -0000Received: by simscan 1.1.0 ppid: 2857,
pid: 2859, t: 0.1710s scanners: attach: 1.1.0 clamav: 0.88.4/m:38/d:1506 spam: 3.1.2X-Spam-Checker-Version:
SpamAssassin 3.1.2 (2006-05-25) on smtp1.goowy.com
X-Spam-Level: X-Spam-Status: No, score=0.5 required=4.5 tests=ALL_TRUSTED,BIZ_TLD,      HTML_50_60,HTML_MESSAGE
autolearn=disabled version=3.1.2
Received: from unknown (HELO webserver002) ([192.168.25.102])   (envelope-sender <terrysadler@goowy.com>) by
smtp1.goowy.com (qmail-ldap-1.03) with SMTP for <martha.dax@superiorbicycles.biz>; 17 Feb       2007 21:01:53 -
0000goowy: id: : 520051From: terrysadler <terrysadler@goowy.com>
Reply-To: terrysadler <terrysadler@goowy.com>To: martha.dax@superiorbicycles.bizDate: Sat, 17 Feb 2007 21:15:44
GMTMessage-ID: <2af031584b5c460e95b36ddd6719529f@webserver002>Subject: InvestorsMIME-Version: 1.0X-Mailer: goowy
mail - http://www.goowy.comPriority: NormalX-Priority: 3Content-Type: multipart/alternative; boundary="----
=_EDNP_0000_6acd7458-decb-4ef6-bc8c-d4788e09019b"X-ePrism-Trap: Default TrapX-eGuard-Score: () 0.6
BIZ_TLD,HTML_50_60,HTML_MESSAGEX-Scanned-By: ePrism email filtering appliance on 199.249.224.252Return-Path:
terrysadler@goowy.comX-OriginalArrivalTime: 17 Feb 2007 21:15:45.0640 (UTC)     FILETIME=[C9DBFE80:01C752D8]X-
Evolution-Source: pop://martha.dax@mail.superiorbicycles.biz/X-Evolution: 0000001a-0010This is a multi-part
message in MIME format.------=_EDNP_0000_6acd7458-decb-4ef6-bc8c-d4788e09019bContent-Type: text/plain;
charset="iso-8859-1"Content-Transfer-Encoding: quoted-printable=0AHello, =0A=0AAre you looking for investors for
your company? We speci=alize in small to medium size companies that have a proven track record= for making
quality products and services. Our investor program will pro=vide to you the necessary consultation to achieve
success in the market= place along with the needed financing to maintain a competive edege aga=inst your
competitors. =0A=0AIf you hare interest check out our link her=e to find out more about this unique and
successful offer. =0A=0Awww.sup=eriorbicycles.biz=20------=_EDNP_0000_6acd7458-decb-4ef6-bc8c-d4788e09019b
Content-Type: text/html; charset="iso-8859-1"Content-Transfer-Encoding: quoted-printable<HTML><HEAD><META http-
equiv=3DContent-Type content=3D"text/html; charse=t=3Diso-8859-1"></head><body><HTML><HEAD><META http-
equiv=3DContent-Type= content=3D"text/html; charset=3Diso-8859-1"></head><body><SPAN style=3D='color:
#000000;font-size: 12px;font-family: Verdana;'><p><font face=3D"=Verdana" size=3D"2"></font></p><p><font
face=3D"Verdana" size=3D"2">Hell=o, </font></p><p><font face=3D"Verdana" size=3D"2"></font></p><p><font=
face=3D"Verdana" size=3D"2">Are you looking for investors for your comp=any? We specialize in small to medium
size companies that have a proven= track record for making quality products and services. Our investor pro=gram
will provide to you the necessary consultation to achieve success= in the market place along with the needed
```

Figure 11-12 The Terry Sadler e-mail in Notepad

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Recovering Outlook Files (1 of 2)

- A forensics examiner recovering e-mail messages from Outlook
  - May need to reconstruct `.pst` files and messages
- With many advanced forensics tools
  - Deleted `.pst` files can be partially or completely recovered
- `Scanpst.exe` recovery tool
  - Comes with Microsoft Office
  - Can repair `.ost` files as well as `.pst` files

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Recovering Outlook Files (2 of 2)

- Guidance Software uses the SysTools plug-in
  - For Outlook e-mail through version 2013
  - Systools extracts .pst files from EnCase Forensic for analysis
- DataNumen Outlook Repair
  - One of the better e-mail recovery tools
  - Can recovery files from VMware and Virtual PC

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

E-mail Case Studies

- In the Enron Case, more than 10,00 emails contained the following personal information:
  - 60 containing credit card numbers
  - 572 containing thousands of Social Security or other identity numbers
  - 292 containing birth dates
  - 532 containing information of a highly personal nature
    - Such as medical or legal matters

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Applying Digital Forensics to Social Media Communications (1 of 2)

- **Online social networks (OSNs)** are used to conduct business, brag about criminal activities, raise money, and have class discussions
- Social media can contain:
  - Evidence of cyberbullying and witness tampering
  - A company's position on an issue
  - Whether intellectual property rights have been violated
  - Who posted information and when

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Applying Digital Forensics to Social Media Communications (2 of 2)

- Social media can often substantiate a party's claims
- OSNs involve multiple jurisdictions that might even cross national boundaries
- A warrant or subpoena is needed to access social media servers
- In cases involving imminent danger, law enforcement can file for emergency requests

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Social Media Forensics on Mobile Devices

- Mobile devices
  - Majority of social network clients
- Evidence artifacts vary depending on the social media channel and the device
- iPhone and Android devices
  - Yielded the most information, and much of the data was stored in SQLite databases

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Forensics Tools for Social Media Investigations

- Software for social media forensics is being developed
  - Not many tools are available now
- There are questions about how the information these tools gather can be used in court or in arbitration
- Using social media forensics software might also require getting the permission of the people whose information is being examined

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Summary (1 of 3)

- E-mail fraudsters use phishing, pharming, and spoofing scam techniques
- In both Internet and intranet e-mail environments, e-mail messages are distributed from one central server to connected client computers
- E-mail investigations are similar to other kinds of investigations
- Forensics linguistics is a field where language and the law intersect to determine the author of e-mails, text messages, and other online communications
- Access victim's computer to recover evidence
  - Copy and print the e-mail message involved in the crime or policy violation

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Summary (2 of 3)

- Use the e-mail program that created the message to find the e-mail header, which provides supporting evidence and can help you track the suspect to the originating location
- Investigating e-mail abuse
  - Be familiar with e-mail servers and clients' operations
- For many e-mail investigations you can rely on e-mail message files, headers, and server log files

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Summary (3 of 3)

- For e-mail applications that use the mbox format, a hexadecimal editor can be used to carve messages manually
- Social media, or OSNs can provide evidence in criminal and civil cases
  - Software for collecting OSN information is being developed
- The majority of people engaging in social media communications are mobile users
- Social media forensics tools have evolved with the technology, and many forensics suites have built-in social media tools

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Guide to Computer Forensics and Investigations Sixth Edition

Chapter 12

Mobile Device Forensics and the Internet of Anything

CENGAGE

Objectives

- Explain the basic concepts of mobile device forensics
- Describe procedures for acquiring data from mobile devices
- Summarize the challenges of forensic acquisitions of data stored on Internet of Anything devices

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding Mobile Device Forensics (1 of 3)

- People store a wealth of information on cell phones
  - People don't think about securing their phones
- Items stored on cell phones:
  - 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
  - Pictures, video, and music files

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding Mobile Device Forensics (2 of 3)

- Items stored on cell phones: (cont'd)
  - Calendars and address books
  - Social media account information
  - GPS data
  - Voice recordings and voicemail
  - Bank account logins
  - Access to your home
- A search warrant is needed to examine mobile devices because they can contain so much information

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding Mobile Device Forensics (3 of 3)

- Investigating cell phones and mobile devices is a challenging tasks in digital forensics
  - No single standard exists for how and where phones store messages
  - New phones come out about every six months and they are rarely compatible with previous models

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Mobile Phone Basics (1 of 5)

- Mobile phone technology has advanced rapidly
- By the end of 2008, mobile phones had gone through three generations:
  - Analog
  - Digital personal communications service (PCS)
  - **Third-generation (3G)**
- **Fourth-generation (4G)** was introduced in 2009
- Several digital networks are used in the mobile phone industry
- **Fifth-generation (5G)** cellular networks
  - Expected to be finalized in 2020, will incorporate emerging technologies

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Mobile Phone Basics (2 of 5)

- Most **Code Division Multiple Access (CDMA)** networks conform to IS-95
  - These systems are referred to as CDMAOne
  - When they went to 3G services, they became CDMA2000
- **Global System for Mobile Communications (GSM)** uses the **Time Division Multiple Access (TDMA)** technique
  - Multiple phones take turns sharing a channel

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Mobile Phone Basics (3 of 5)

- The 3G standard was developed by the **International Telecommunications Union (ITU)** under the United Nations
  - It is compatible with CDMA, GSM, and TDMA
  - The **Enhanced Data GSM Environment (EDGE)** standard was developed specifically for 3G

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Mobile Phone Basics (4 of 5)

- 4G networks can use the following technologies:
  - ***Orthogonal Frequency Division Multiplexing (OFDM)***
  - *Mobile WiMAX*
  - *Ultra Mobile Broadband (UMB)*
  - *Multiple Input Multiple Output (MIMO)*
  - *Long Term Evolution (LTE)*

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Mobile Phone Basics (5 of 5)

- Main components used for communication:
  - *Base transceiver station (BTS)*
  - *Base station controller (BSC)*
  - *Mobile switching center (MSC)*

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Inside Mobile Devices (1 of 5)

- Mobile devices can range from simple phones to **smartphones**, tablets, and smartwatches
- Hardware components
  - Microprocessor, ROM, RAM, a digital signal processor, a radio module, a microphone and speaker, hardware interfaces, and an LCD display
- Most basic phones have a proprietary OS
  - Although smartphones use the same OSs as PCs

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Inside Mobile Devices (2 of 5)

- Phones store system data in **electronically erasable programmable read-only memory (EEPROM)**
  - Enables service providers to reprogram phones without having to physically access memory chips
- OS is stored in ROM
  - Nonvolatile memory
  - Available even if the phone loses power

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Inside Mobile Devices (3 of 5)

- Personal digital assistants (PDAs) have been mostly replaced by iPods, iPads, and other mobile devices
- Their use has shifted to more specific markets
  - Such as medical or industrial PDAs
- Peripheral memory cards used with PDAs:
  - *Compact Flash (CF)*
  - *MultiMediaCard (MMC)*
  - *Secure Digital (SD)*

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Inside Mobile Devices (4 of 5)

- **Subscriber identity module (SIM) cards**
  - Found most commonly in GSM devices
  - Consist of a microprocessor and internal memory
  - GSM refers to mobile phones as “mobile stations” and divides a station into two parts:
    - The SIM card and the mobile equipment (ME)
  - SIM cards come in three sizes
  - Portability of information makes SIM cards versatile

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Inside Mobile Devices (5 of 5)

- **Subscriber identity module (SIM) cards** (cont'd)
  - 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
- Many phones now include SD cards for external storage

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding Acquisition Procedures for Mobile Devices (1 of 7)

- The main concerns with mobile devices are loss of power, synchronization with cloud services, and remote wiping
- All mobile devices have volatile memory
  - Making sure they don’t lose power before you can retrieve RAM data is critical
- Mobile device attached to a PC via a USB cable should be disconnected from the PC immediately
  - Helps prevent synchronization that might occur automatically and overwrite data

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding Acquisition Procedures for Mobile Devices (2 of 7)

- Depending on the warrant or subpoena, the time of seizure might be relevant
- Messages might be received on the mobile device after seizure
- Isolate the device from incoming signals with one of the following options:
  - Place the device in airplane mode
  - Place the device in a paint can
  - Use a Faraday bag
  - Turn the device off

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding Acquisition Procedures for Mobile Devices (3 of 7)

- The drawback of using these isolating options is that the mobile device is put into roaming mode
  - Accelerates battery drainage
- SANS DFIR Forensics recommends:
  - If device is on and unlocked - isolate it from the network, disable the screen lock, remove passcode
  - If device is on and locked - what you can do varies depending on the type of device
  - If device is off - attempt a physical static acquisition and turn the device on

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding Acquisition Procedures for Mobile Devices (4 of 7)

- Check these areas in the forensics lab :
  - Internal memory
  - SIM card
  - Removable or external memory cards
  - Network provider
- Checking network provider requires a search warrant or subpoena
  - A new complication has surfaced because backups might be stored in a cloud provided by the carrier or third party

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding Acquisition Procedures for Mobile Devices (5 of 7)

- Due to 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
- Memory storage on a mobile device is usually a combination of volatile and nonvolatile memory
- The file system for a SIM card is a hierarchical structure

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding Acquisition Procedures for Mobile Devices (6 of 7)

Figure 12-1 SIM file structure

CENGAGE
© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding Acquisition Procedures for Mobile Devices (7 of 7)

- Information that can be retrieved falls into four categories:
  - Service-related data, such as identifiers for the SIM card and the subscriber
  - Call data, such as numbers dialed
  - Message information
  - Location information
- If power has been lost, PINs or other access codes might be required to view files

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Mobile Forensics Equipment (1 of 6)

- Mobile forensics is an evolving science
- Biggest challenge is dealing with constantly changing phone models
- Procedures for working with mobile forensics software:
  - Identify the mobile device
  - Make sure you have installed the mobile device forensics software
  - Attach the phone to power and connect cables
  - Start the forensics software and download information

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Mobile Forensics Equipment (2 of 6)

- SIM card readers
  - A combination hardware/software device used to access the SIM card
  - You need to be in a forensics lab equipped with appropriate antistatic devices
  - General procedure is as follows:
    - Remove the device's back panel
    - Remove the battery
    - Remove the SIM card from holder
    - Insert the SIM card into the card reader

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Mobile Forensics Equipment (3 of 6)

- SIM card readers (cont'd)
  - A variety of SIM card readers are available
    - Some are forensically sound and some are not
  - Documenting messages that haven't been read yet is critical
    - Use a tool that takes pictures of each screen
- Mobile phone forensics tools and methods
  - AccessData FTK Imager
  - MacLockPick 3.0

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Mobile Forensics Equipment (4 of 6)

- NIST guidelines list six types of mobile forensics methods:
  - Manual extraction
  - Logical extraction
  - Physical extraction
  - Hex dumping and Joint Test Action Group (JTAG) extraction
  - Chip-off
  - Micro read

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Mobile Forensics Equipment (5 of 6)

- Paraben Software offers several tools:
  - E3:DS – for mobile device investigations
- DataPilot – has a collection of cables that can interface with phones from different manufacturers
- BitPam - used to view data on many CDMA phones
- Cellebrite UFED Forensic System - works with smartphones, PDAs, tablets, and GPS devices
- MOBILedit Forensic - contains a built-in write-blocker

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Mobile Forensics Equipment (6 of 6)

- Software tools differ in the information they display and the level of detail
- Some tools are designed for updating files, not retrieving data
- In general, tools designed to edit information, although they are user friendly, usually aren’t forensically sound

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Using Mobile Forensics Tools (1 of 4)

- Cellebrite is often used by law enforcement
  - You can determine the device's make and model, learn what has to be done before connecting a mobile device to the UFED device, and then retrieve the data
  - Three options for data extraction:
    - Logical
    - File system
    - Physical
- You can also simply connect a mobile device to a computer to browse the file system and examine and retrieve files
  - Needs a USB write-blocker

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Using Mobile Forensics Tools (2 of 4)

Figure 12-2 Viewing the Android file system

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Using Mobile Forensics Tools (3 of 4)

Figure 12-3 Preliminary steps in accessing a mobile device

Source: Magnet Forensics, *www.magnetforensics.com*

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Using Mobile Forensics Tools (4 of 4)

- Many mobile forensics tools are available
  - Most aren't free
- Methods and techniques for acquiring evidence will change as market continues to expand and mature
- Subscribe to user groups and professional organizations to stay abreast of what's happening in the industry

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding Forensics in the Internet of Anything (1 of 3)

- In 2010, VMware and BlackBerry were developing
  - Type 2 hypervisors for mobile devices
  - Useful for security and protecting personal information but will add another level of complexity to forensics investigations
- Separate personal information from business-related data
  - Bring your own device (BYOD) practices make it even more difficult
- Internet of Things (IoT)
  - The number of devices that connect to the Internet is higher than the amount of people
    - That number is expected to reach 50 billion in the next few decades

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding Forensics in the Internet of Anything (2 of 3)

- Evolution from Internet of Thing (IoT) to Internet of Everything (IoE) to Internet of Anything (IoA)
- IoE adds features that aren't tangible but are widespread on the Internet
  - Google search engine and YouTube
- IoA includes cars, homes, pets, livestock, and applications for making all these things work together
  - Eventually will include 5G smart devices
- 5G devices categories:
  - enhanced Mobile Broadband (eMBB)
  - Ultra-reliable and Low-latency Communications (uRLLC)
  - massive Machine Type Communications (mMTC)

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding Forensics in the Internet of Anything (3 of 3)

- 5G devices introduce new challenges for digital forensics:
  - People-to-device communications (P2D)
  - Device-to-device (D2D) communications
  - Device-to-cloud (D2C) communications
- Wearable computers will pose many new challenges for investigators
- Vehicle system forensics
  - Addresses the many parts that have sensors in cars

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Summary (1 of 3)

- People store a wealth of information on smartphones, including calls, text messages, picture and music files, address books, and more
- Mobile devices have gone through four generations: analog, digital personal communications service (PCS), third-generation (3G), and fourth-generation (4G)
- 5G standards are being negotiated and developed by the IMT 2020 working group of the International Telecommunications Union
- Mobile devices range from basic, inexpensive phones used primarily for phone calls to smartphones

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Summary (2 of 3)

- Data can be retrieved from several different places in phones
- Use of personal digital assistants (PDAs) has declined due to the popularity of smartphones
- As with computers, proper search and seizure procedures must be followed for mobile devices
- To isolate a mobile device from incoming messages, you can put it in airplane mode, turn the device off, or place it in a special treated paint can or evidence bag
- SIM cards store data in a hierarchical file structure
- Mobile device forensics is becoming more important as these devices grow in popularity

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Summary (3 of 3)

- Many software tools are available for reading data stored in mobile devices
- The Internet of Things (IoT) has resulted in yet another challenge for digital forensics investigators
- Collecting information from wearable computers will pose many new challenges for investigators

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Guide to Computer Forensics and Investigations Sixth Edition

Chapter 13

Cloud Forensics

CENGAGE

Objectives

- Describe the main concepts of cloud computing
- Summarize the legal challenges in conducting cloud forensics
- Give an overview of the technical challenges with cloud forensics
- Describe how to acquire cloud data
- Explain how to conduct a cloud investigation
- Explain what remote access tools can be used for cloud investigations

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

An Overview of Cloud Computing

- The cloud has introduced ways of managing data that didn’t exist a decade ago
- Cloud investigations have unique challenges
- New standards are being developed to improve security practices and incident responses in cloud environments

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

History of the Cloud (1 of 2)

- Idea of cloud computing came from several people:
  - Professor John McCarthy of MIT
  - Dr. J.C.R. Licklider, director at the U.S. Department of Defense Advanced Research Projects Agency (ARPA)
- In 1999, Salesforce.com developed a Web service that applied digital marketing research to business subscribers
  - This service led the way to the cloud

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

History of the Cloud (2 of 2)

- Amazon created Amazon Mechanical Turk in 2002
  - Provided storage, computations, and human intelligence
  - Started Elastic Compute Cloud (EC2) in 2006, aimed at supporting small businesses
- After Web 2.0 in 2009, other providers started their own cloud services
  - Google Apps, Apple iCloud, Microsoft OneDrive, and more

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Cloud Service Levels and Deployment Methods (1 of 4)

- The National Institute of Standards and Technology (NIST) defines cloud computing 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

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Cloud Service Levels and Deployment Methods (2 of 4)

- The cloud has three service levels:
  - **Software as a service (SaaS)** - applications are delivered via the Internet
  - **Platform as a service (PaaS)** - an OS has been installed on a cloud server
  - **Infrastructure as a service (IaaS)** - customers can rent hardware and install whatever OSs and applications they need

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Cloud Service Levels and Deployment Methods (3 of 4)

Table 13-1	Locations of evidence in different service levels
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.

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Cloud Service Levels and Deployment Methods (4 of 4)

- Deployment methods for a cloud:
  - **Public** - accessible to anyone
  - **Private** - can be accessed only by people who have the necessary credentials
  - **Community** - a way to bring people together for a specific purpose
  - **Hybrid** - enables a company to keep some information private and designate other files as public or community information

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Cloud Vendors

- Some **cloud service providers (CSPs)** and cloud applications:
  - Salesforce
  - IBM Cloud
  - Cisco Cloud Computing
  - Amazon EC2
  - AT&T Synaptic
  - Google Cloud Storage
  - HP Helion
  - Microsoft Azure
  - XenServer and XenCenter Windows Management Console
  - Rackspace
  - Oracle Cloud

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Basic Concepts of Cloud Forensics (1 of 2)

- Cloud forensics is considered a subset of network forensics
- Cloud forensics can have three dimensions:
  - Organizational - addresses the structure of the cloud
  - Legal - covers service agreements and other jurisdictional matters
  - Technical - deals with procedures and specialized applications designed to perform forensics recovery and analysis in the cloud

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Basic Concepts of Cloud Forensics (2 of 2)

- Forensic tool capabilities needed to handle acquiring data from a cloud:
  - *Forensic data collection* - must be able to identify, label, record, and acquire data from the cloud
  - *Elastic, static, and live forensics* - must be able to expand and contract their storage capabilities
  - *Evidence segregation* - different businesses and users share the same applications and storage space
  - *Investigations in virtualized environments* - should have the capability to examine virtual systems

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Legal Challenges in Cloud Forensics

- When investigating a cloud system, consider factors involving a CSP's relationship with cloud users
- This section explains:
  - A CSP's contract obligations with cloud users
  - How warrants and subpoenas are applied to CSPs and users

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Service Level Agreements (1 of 5)

- **Cloud service agreements (CSAs)** - a contract between a CSP and the customer that describes what services are being provided and at what level
  - Includes service legal agreements (SLAs)
- CSAs should also specify:
  - Support options
  - Penalties for services not provided
  - System performance
  - Fees
  - Provided software or hardware

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Service Level Agreements (2 of 5)

- CSAs define the scope of services the CSP provides:
  - Service hours
  - Restrictions applied to the customer by the CSP
  - Availability of the cloud to the customer
  - Levels of support for the customer
  - Response time for data transfers
  - Throughput, limitations
  - Contingency plan for incident response
  - Business continuity and disaster recovery plan

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Service Level Agreements (3 of 5)

- CSAs define the scope of services the CSP provides (cont'd):
  - Fees for the subscription to the cloud and fees for additional services as they occur
  - Security measures
  - Terminology of the cloud's systems and applications
- CSP components must state who is authorized to access data and what the limitations are in conducting acquisitions for an investigation

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Service Level Agreements (4 of 5)

- Policies, Standards, and Guidelines for CSPs
  - Digital forensics should review CSPs policies, standards, and guidelines for daily operations
  - Policies - detailed rules for a CSP's internal operation
  - Standards - give guidance to staff for unique operations, hardware, and software and describe the staff's obligations regarding security of the CSP environment
  - Guidelines - describe best practices for cloud processes and give staff an example of what they should strive to achieve in their work

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Service Level Agreements (5 of 5)

- CSP Processes and Procedures - are detailed documents that define workflow and step-by-step instructions for CSP staff
  - Often include hardware configuration diagrams, network maps, and application processing flowcharts
  - Digital forensics examiners can use them to understand how data is stored, manipulated, secured, backed up, restored, and accessed by CSP staff and customers
- Additional documents of interest:
  - CSP business continuity and disaster recovery plans

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Jurisdiction Issues (1 of 2)

- Although there are plans to revise current laws
  - Many cross-jurisdiction legal issues haven't been resolved
- No law ensures uniform access or required handling procedures for the cloud
- Investigators should be concerned about cases involving data commingled with other customers' data
- Often, figuring out what law controls data stored in the cloud is a challenge

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Jurisdiction Issues (2 of 2)

- How privacy rights are defined in different jurisdictions is a major factor in problems with the right to access data
- EU Directive 95/46/EC is more restrictive than rules in other countries, including the U.S.
  - Protects private information for all EU citizens
- Digital forensics examiners could be held liable when conducting an investigation involving cloud data
  - Consult with legal experts to be aware of possible restrictions

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Accessing Evidence in the Cloud (1 of 4)

- 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
  - Court orders with prior notice to the subscriber or customer

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Accessing Evidence in the Cloud (2 of 4)

- Search Warrants
  - Can be used only in criminal cases and must be requested by a law enforcement officer who has evidence of probable cause that a crime was committed
  - Law requires search warrants to contain specific descriptions of what's to be seized
  - For cloud environments, the property to be seized usually describes data rather than physical hardware, unless the CSP is the suspect

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Accessing Evidence in the Cloud (3 of 4)

- Search Warrants (cont'd)
  - Must also describe the location of items to be seized
    - Difficult when dealing with cloud data because servers are often dispersed across state or national borders
  - Must establish how it will be carried out
    - Specifying the date and time of day to minimize disruptions to people and business operations

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Accessing Evidence in the Cloud (4 of 4)

- Subpoenas and Court Orders
  - *Government agency subpoenas* - customer communications and records can't be knowingly divulged to any person or entity
    - Used to get information when it's believed there's a danger of death or serious physical injury
  - *Non-government and civil litigation subpoenas* - used to produce information from private parties for litigation
  - *Court orders* - written by judges to compel someone to do or not do something

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Technical Challenges in Cloud Forensics

- Challenges in conducting cloud forensics
  - Architecture
  - Data collection
  - Analysis of cloud forensic data
  - Anti-forensics
  - Incident first responders
  - Role management
  - Legal issues
  - Standards and training

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Architecture

- No two CSPs are configured exactly the same way
- Depending on the type of cloud architecture
  - Customer's data could be commingled
- Most CSPs keep data storage locations secret for security reasons
- Differences in recording procedures or log keeping can make it difficult to determine data's origin
  - And complicate an investigation's chain of evidence

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Analysis of Cloud Forensic Data

- Analyzing digital evidence from a cloud requires verifying the data with other data and log records
- Data may need to be reconstructed to determine what actually occurred during an incident
- Examining logs can be useful to compare the modified, last access, and create (MAC) dates and times for files

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Anti-Forensics (1 of 2)

- Anti-forensics - destroying ESI that may be potential evidence
- Hackers may use specialized malware for defeating evidence collection
- Additional methods for anti-forensics:
  - Inserting malware programs in other files
  - Using encryption to obfuscate malware programs activated through other malware programs
  - Using data-hiding utilities that append malware to existing files

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Anti-Forensics (2 of 2)

- Other techniques affect file metadata by changing the modify and last access times
- Changing timestamps can make it difficult to develop a timeline of a hacker's activities
- Calculating hash values of files and comparing the results with known good files' hash values can help identify files that might have been altered

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Incident First Responders (1 of 2)

- CSPs have personnel trained to respond to network incidents
  - They become first responders when a network intrusion occurs
- When CSPs do not have an internal first responder team, the forensics examiner should organize CSP staff to handle these tasks

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Incident First Responders (2 of 2)

- Some factors to address include:
  - Will the CSP's operations staff be cooperative and follow directions, and will management issue orders stating that you're the leader of the investigation?
  - Do you need to brief staff about operations security? For example, you might need to explain that they should talk only to others who have a need to know about the incident and the investigation's activities
  - Do you need to train staff in evidence collection procedures, including the chain of custody?

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Role Management

- Role management in the cloud covers:
  - Data owners
  - Identity protection
  - Users
  - Access controls
- As an investigator, you need to collect this information so you can identify additional victims or suspects

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Standards and Training (1 of 2)

- There is an effort to standardize cloud architectures for:
  - Operating procedures
  - Interoperability
  - Testing
  - Validation
- The Cloud Security Alliance (CSA) has develop resource documentation for CSPs and their staff

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Standards and Training (2 of 2)

- Cloud investigators should have an understanding of cloud architecture
  - In addition to basic digital and network forensic skills
- Sources for cloud forensics training:
  - (ISC)²'s Certified Cyber Forensics Professional
  - INFOSEC Institute
  - SANS Cloud Forensics with F-Response
  - National Institute of Justice Digital Forensics Training
  - University College Dublin Centre for Cybersecurity and Cybercrime Investigation

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Acquisitions in the Cloud

- Methods used to collect evidence in cloud investigations depend on the nature of the case
- Recovering deleted data from cloud storage might be limited to the type of file system the CSP uses
- With cloud systems running in a virtual environment, snapshots can give you valuable information before, during, and after an incident
  - Forensic examiners should re-create separate cloud servers from each snapshot, acquire an image of each server, and calculate a hash for all files

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Encryption in the Cloud (1 of 3)

- Many CSPs and third parties offer encryption services for cloud users as a security measure
  - Expect to find encrypted files in cloud investigations
- You need assistance from the data owner or the CSP to decrypt data with the right encryption key
  - If data owner is uncooperative, you may need to turn to the attorneys handling the case or data owner's management

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Encryption in the Cloud (2 of 3)

- Encrypted data in the cloud is in two states:
  - Data at rest - data that has been written to disk
  - Data in motion - data being transmitted over a network
- Some system also have encryption for data in use (data that's in RAM)
- If encrypted data is encountered
  - Find out from the CSP what type of encryption was used and who knows how to recover it

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Encryption in the Cloud (3 of 3)

- Vendors that offer encryption services for cloud data:
  - Atalla Cloud Encryption from Micro Focus
  - SecureCloud from Trend Micro
  - SafeGuard Encryption and Sophos Mobile Control from Sophos
- Homomorphic encryption
  - Uses an “ideal lattice” mathematical formula to encrypt data
- Block chain technology
  - Used by companies such as Bitcoin, is a way to trace your information while keeping it secure

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Conducting a Cloud Investigation

- When investigating cloud incidents:
  - Use a systematic approach just like the one covered in Chapter 1
- The type of incident determines how to proceed with planning the investigation
- If the investigation involves searching for and recovering data from cloud storage or cloud customers
  - Follow methods described in Chapters 5 and 6

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Investigating CSPs (1 of 2)

- If a CSP has no team or limited staff, investigators should ask the following questions to understand how the CSP is set up:
  - Does the investigator have the authority to use cloud staff and resources to conduct an investigation?
  - Is detailed knowledge of the cloud's topology, policies, data storage methods, and devices available?
  - Are there any restrictions on collecting digital evidence from remote cloud storage?

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Investigating CSPs (2 of 2)

- Investigators should ask the following questions to understand how the CSP is set up (cont'd):
  - For e-discovery demands on multitenant cloud systems, is the data to collect commingled with other cloud customers' unrelated data? Is there a way to separate the data to prevent violating privacy rights or confidentiality agreements?
  - Is the data of interest to the investigation local or remote? If it's in a remote location, can the CSP provide a forensically sound connection to it?

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Investigating Cloud Customers

- If a cloud customer doesn't have the CSP's application installed
  - You might find cloud-related evidence in a Web browser's cache file
- If the CSP's application is installed
  - You can find evidence of file transfers in the application's folder
  - Usually found under the user's account folder

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding Prefetch Files (1 of 2)

- Prefetch files - contain the DLL pathnames and metadata used by an application
- The OS reads the associated prefetch file and loads its information into the computer's memory
  - Speeds an application's start time
- The OS can handle other tasks instead of waiting for an application to load needed libraries
- Example:
  - Metadata in a prefetch files contains an application's MAC times in UTC format and a counter of how many times the app has run

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding Prefetch Files (2 of 2)

Figure 13-1 Showing the offset positions for the counter and the dates and times for `Dropbox.exe`

Source: X-Ways AG, *www.x-ways.net*

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Examining Stored Cloud Data on a PC (1 of 6)

- Three widely used cloud services:
  - Dropbox
  - Google Drive
  - OneDrive
- Services are free for storage up to 2 GB for Dropbox and up to 15 GB for Google Drive and OneDrive
- These applications have Registry entries
- Users must maintain control over access to their cloud accounts

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Examining Stored Cloud Data on a PC (2 of 6)

- Dropbox offers third-party applications, such as e-mail, chat, Cisco WebEx, and other collaboration tools
- Since 2012, Dropbox has used base-64 format to store content
  - Reading them requires specialized software
  - Magnet Forensics has a tool called Internet Evidence Finder (IEF) designed for this purpose

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Examining Stored Cloud Data on a PC (3 of 6)

- Gmail users have access to Google Drive for cloud data storage and applications
- Google Drive is installed in:
  - C:\Program Files (x86)\Google\Drive
- Each user has a configuration file stored in C:\Users*username*\AppData\Local\Google\Drive
  - Called a “user profile”
- If Google Drive has been installed, it creates a folder in the path C:\Users*username*\Google Drive

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Examining Stored Cloud Data on a PC (4 of 6)

- Important Google Drive files:
  - `sync_config.db` - an SQL database file with Google Drive upgrade number, highest application version number, and local synchronization root path
  - `snapshot.db` - contains information about each file accessed, the URL pathname, the modified and created dates and times in UNIX timestamp format, and the file's MD5 value and size
  - `sync_log.log` - has a detailed list of a user's cloud transactions

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Examining Stored Cloud Data on a PC (5 of 6)

- OneDrive - created by Microsoft and was originally called SkyDrive
  - Available with Windows 8 and later
  - Similar to DropBox and Google Drive and offers subscription services for Microsoft software
- OneDrive stores user profiles in the user's account path
- Log files and synchronized files are kept in various places under the user's account (depending on the Windows version)

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Examining Stored Cloud Data on a PC (6 of 6)

- You can find more information in the following Windows 8.1 log files, which are in the C:\Users\username\AppData\Local\Microsoft\Windows\SkyDrive\logs folder
  - `SyncEngine-yyyy-mm-ddnn.nnn-n.etl` manages synchronization between OneDrive and a user's computer
  - `SyncDiagnostics.log` contains client ID, clientType, clientVersion, device, deviceID, and timeUtc values

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Windows Prefetch Artifacts

- You can collect prefetch file artifacts with a disk editor or forensics tool
- Follow the steps in the activity starting on page 546 to use WinHex's Data Interpreter to find an application's MAC dates and times
  - And the number of times DropBox has run

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Tools for Cloud Forensics

- Few tools designed for cloud forensics were available
- Many digital, network, and e-discovery tools can be combined to collect and analyze cloud data
- Some vendor with integrated tools:
  - Guidance Software EnCase eDiscovery
  - AccessData Digital Forensics Incident Response
  - F-Response

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Forensic Open-Stack Tools (1 of 2)

- Forensic Open-Stack Tools (FROST) integrates with OpenStack running in IaaS cloud environments
  - Adds forensics response capabilities for a CSP
- OpenStack - an open-source computing platform intended for public and private cloud services
- FROST is the first known effort to provide a forensics response process for a cloud service

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Forensic Open-Stack Tools (2 of 2)

- A feature of FROST
  - It bypasses a VMs hypervisor
  - Collected data is placed in the cloud's **management plane**, which is a tool with application programming interfaces that allow reconfiguring the cloud on the fly
  - Special malware can take control of the virtual session and deny or alter access
  - Can also prevent or interfere with forensic analysis and data collection

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

F-Response for the Cloud

- F-Response is a remote access tool that can be applied to cloud forensics
  - Uses USB forwarding techniques to allow non-remote-capable forensics tools to access remote servers and their data storage
- Two tools are needed:
  - F-Response Enterprise or Consultant
  - KernelPro USB-Over-Ethernet

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Magnet AXIOM Cloud

- Magnet AXIOM created a Cloud module to go with its Process and Examine modules
- Magnet AXIOM Cloud
  - Retrieves information from Facebook Messenger, Skype, Instagram, Twitter, iCloud, and others
  - You still need usernames and passwords

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Summary (1 of 4)

- Three service levels are available for the cloud: software as a service, platform as a service, and infrastructure as a service
- CSPs use servers on distributive networks or mainframes that allow elasticity of resources for customers
- With multinational clouds, you should seek legal counsel before proceeding with an investigation
- Cloud investigations are necessary in cases involving cyberattacks, policy violations, data recovery, and fraud complaints

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Summary (2 of 4)

- Before initiating a cloud investigations, review the CSA to identify any restrictions that might limit collecting and analyzing data
- Technical challenges in cloud forensics involve cloud architecture, data collection, analysis of cloud forensic data, anti-forensics, incident first responders, role management, legal issues, and standards and training
- Anti-forensics is an effort to alter log records as well as date and time values of important system files and install malware to hide hacker's activities

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Summary (3 of 4)

- CSPs should have an incident response team ready to respond to network intrusions
- Role management defines the duties of CSP staff and customers
- The Cloud Security Alliance has developed resources that guide CSPs in privacy agreements and security measures
- Procedures for acquiring cloud evidence include examining network and firewall logs, performing disk acquisitions of a cloud system's OS, and examining data storage devices

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Summary (4 of 4)

- When investigating a cloud incident, apply a systematic approach to planning and processing the case
- The three cloud services Dropbox, Google Drive, and Microsoft OneDrive contain data on a user's computer or mobile device that can reveal what files were copied or accessed
- Vendors offer tools that can be combined for cloud forensics

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Guide to Computer Forensics and Investigations Sixth Edition

Chapter 14

Report Writing for High-Tech Investigations

CENGAGE

Objectives

- Explain the importance of reports
- Describe guidelines for writing reports
- Explain how to use forensics tools to generate reports

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding the Importance of Reports (1 of 3)

- Communicate the results of your investigation
  - Including expert opinion
- Forensic reports can:
  - Provide justification for collecting more evidence
  - Be used at a probable cause hearing
  - Communicate expert opinion
- U.S. district courts require expert witnesses to submit written reports
  - State courts are starting to also require them

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding the Importance of Reports (2 of 3)

- Rule 26, Federal Rules of Civil Procedure requires submission of the expert's written report that includes:
  - Testimony is based on sufficient facts or data
  - Testimony is the product of reliable principles and methods
  - Witness has applied the principles and methods reliably to the facts of the case
- Written report must specify fees paid for the expert's services
  - And list all other civil or criminal cases in which the expert has testified

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding the Importance of Reports (3 of 3)

- Keep a copy of any deposition notice or subpoena so that you can include the following:
  - Jurisdiction
  - Style of the case
  - Cause number
  - Date and location of the deposition
  - Name of the deponent
- **Deposition banks**
  - Examples of expert witness' previous testimonies

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Limiting a Report to Specifics

- All reports to clients should start with the job mission or goal
  - Find information on a specific subject
  - Recover certain important documents
  - Recover certain types of files with specific dates and times
- Before you begin writing, identify your audience and the purpose of the report

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Types of Reports (1 of 4)

- Digital forensics examiners are required to create different types of reports
- **Examination plan**
  - What questions to expect when testifying
  - Attorney uses the examination plan to guide you in your testimony
  - You can propose changes to clarify or define information
  - Helps your attorney learn the terms and functions used in computer forensics

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Types of Reports (2 of 4)

WITNESS EXAMINATION PLAN

WITNES: Joseph Friday /Factors: Expert Digital Forensic Examiner.

Direct Examination: Expert Testimony Objective/Rule/

Testimony CV

Identity and Address Iowa Bureau of Criminal Investigations

Position (Current) Digital Forensic Examiner

Undergraduate Iowa State University summa cum laude 1990 BS Computer Science

Master's Degree Purdue University, 1992 MS Electrical Engineering

Summer Internship 1989 Des Moines Police Department

Academic Appointments

Lecturer, Dept. of Computer Science, University of Iowa 1998-Current

Instructor, Iowa Police Academy

Professional Society Certifications

P.E. 1990

CISSP 2001

Memberships

American Society of Industrial Security

Publications

Journal of the Iowa State Bar Association, May 1999, "Computer Forensics on RAID Servers-Testifying to Reasonable Certainty"

Experience

How many systems have you conducted forensic examinations on?

The Client

What is your relationship to the Plaintiff? Retained by his attorney to examine the hard drive of his computer for all financial records. I have never actually met or talked to Mr. Smith.

The Specific Examination

How long does it take you to conduct this examination?

What type of files were you looking for? Why those types of files? Where did you find those files?

What condition were the files in?

What is your opinion as to the cause of that condition?

Can you say for a reasonable certainty that the financial data files were deleted intentionally? Yes.

Are you able to state to a reasonable certainty who deleted the financial data files? Yes.

What is your fee for examining the hard drive, preparing a report and testifying?

Anticipated Cross Examination – Expert Testimony

How many times have you worked for Mr. Sawyer as an expert witness? I've done 16 contracts as a consultant expert or expert witness.

Have you ever previously testified that overwriting utilities are not 100% reliable? Yes, but that was in 1994 and utilities are so far as I can tell are 100% reliable today.

Figure 14-1 A sample examination plan

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Types of Reports (3 of 4)

- Verbal report
  - Less structured
  - Attorneys cannot be forced to release verbal reports
  - Preliminary report
  - Addresses areas of investigation yet to be completed
    - Tests that have not been concluded
    - Interrogatories
    - Document production
    - Depositions

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Types of Reports (4 of 4)

- Written report
  - Affidavit or declaration
  - Limit what you write and pay attention to details
    - Include thorough documentation and support of what you write

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Guidelines for Writing Reports (1 of 2)

- Hypothetical questions based on factual evidence
  - Guide and support your opinion
  - Can be abused and overly complex
- Opinions based on knowledge and experience
- State the facts needed to answer the question
  - Don’t include any unnecessary facts

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Guidelines for Writing Reports (2 of 2)

- As an expert witness, you may testify to an opinion or conclusion, if four basic conditions are met:
  - Opinion, inferences, or conclusions depend on special knowledge, skills, or training
  - Witness should qualify as a true expert in the field
  - Witness must testify to a reasonable degree of certainty
  - Experts must know facts on which their opinions are based, or they must testify to a hypothetical question

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

What to Include in Written Preliminary Reports (1 of 2)

- Anything you write down as part of your examination for a report
  - Subject to discovery from the opposing attorney
  - **Discovery**: the process of opposing attorneys seeking information from each other
- Written preliminary reports are considered **high-risk documents**
  - It's better if there's no written report to provide
- Destroying the report could be considered destroying or concealing evidence (spoliation)

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

What to Include in Written Preliminary Reports (2 of 2)

- Include the same information as in verbal reports
- 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

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Report Structure (1 of 2)

- Structure
  - Abstract (summary)
  - Table of contents
  - Body of report
  - Conclusion
  - References
  - Glossary
  - Acknowledgements
  - Appendixes

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Report Structure (2 of 2)

- An abstract condenses the report to concentrate on the essential information
- The body consists of the introduction and discussion sections
- 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

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Writing Reports Clearly (1 of 3)

- Consider
  - Communicative quality
  - Ideas and organization
  - Grammar and vocabulary
  - Punctuation and spelling
- Lay out ideas in logical order
- Build arguments piece by piece
- Group related ideas and sentences into paragraphs
  - Group paragraphs into sections

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Writing Reports Clearly (2 of 3)

- Avoid jargon, slang, and colloquial terms
- Define technical terms
  - Consider your audience
- Considering writing style
  - Use a natural language style
  - Avoid repetition, vague language, and generalizations
  - Use active rather than passive voice
  - Avoid presenting too many details and personal observations

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Writing Reports Clearly (3 of 3)

- Considering writing style (cont'd)
  - Project objectivity
    - Communicate calm, detached observations
- Including signposts
  - Draw reader's attention to a point
  - Assist readers in scanning the text quickly by highlighting the main points and logical development of information

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Designing the Layout and Presentation of Reports (1 of 4)

- Two numbering systems are typically used
- Decimal numbering structure
  - Divides material into sections
  - Readers can scan heading
  - Readers see how parts relate to each other
- Legal-sequential numbering
  - Used in pleadings
  - Roman numerals represent major aspects
  - Arabic numbers are supporting information

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Designing the Layout and Presentation of Reports (2 of 4)

- Providing supporting material
  - Use material such as figures, tables, data, and equations to help tell the story as it unfolds
- Formatting consistently
  - How you format text is less important than being consistent in applying formatting
- Explaining examination and data collection methods
  - Explain how you studied the problem, which should follow logically from the report's purpose

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Designing the Layout and Presentation of Reports (3 of 4)

- Including calculations
  - If you use any hashing algorithms, be sure to give the common name
- Providing for uncertainty and error analysis
  - Protect your credibility
- Explaining results and conclusions
  - Explain your findings, using subheadings to divide the discussion into logical parts
  - Save broader generalizations and summaries for the report's conclusion

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Designing the Layout and Presentation of Reports (4 of 4)

- Providing references
  - Cite references by author's last name and year of publication
  - Follow a standard format
- Including appendixes
  - You can include appendixes containing material such as raw data, figures not used in the body of the report, and anticipated exhibits
  - Arrange them in the order referred to in the report

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Generating Report Findings with Forensics Software Tools

- Forensics tools generate reports when performing analysis
  - It is still your responsibility to explain the significance of the evidence
- Report formats
  - Plaintext
  - Word processor
  - Spreadsheet
  - HTML format

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Using Autopsy to Generate Reports (1 of 4)

- Follow Activity steps starting on page 575

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Using Autopsy to Generate Reports (2 of 4)

Figure 14-2 Viewing the Desktop folder

Source: *www.sleuthkit.org*

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Using Autopsy to Generate Reports (3 of 4)

Directory Listing

/img_GCFI-tj01.001/Users/Tom Johnson/Desktop — 17 Results

Table | Thumbnail

Name	Modified Time	Change Time	Access Time	Created Time	Size
[current folder]	2017-10-28 14:33:23 PDT	2017-10-28 14:33:23 PDT	2017-10-28 14:33:23 PDT	2017-10-25 15:13:01 PDT	56
[parent folder]	2017-10-25 15:13:09 PDT	2017-10-28 14:30:16 PDT	2017-10-25 15:13:09 PDT	2017-10-25 15:11:20 PDT	56
Gpg4win Documentation	2017-10-28 14:33:23 PDT	2017-10-28 14:33:23 PDT	2017-10-28 14:33:23 PDT	2017-10-28 14:33:22 PDT	56
Acrobat Reader DC.lnk	2017-10-28 14:33:22 PDT	2017-10-28 14:33:22 PDT	2017-10-28 14:33:23 PDT	2017-10-28 14:33:23 PDT	2017
desktop.ini	2017-06-16 13:54:18 PDT	2017-10-25 13:49:28 PDT	2017-10-25 15:13:01 PDT	2017-10-25 15:13:01 PDT	282
Google Chrome.lnk	2017-10-28 14:33:22 PDT	2017-10-28 14:33:22 PDT	2017-10-28 14:33:23 PDT	2017-10-28 14:33:23 PDT	2129
GPA.lnk	2017-10-28 14:33:22 PDT	2017-10-28 14:33:22 PDT	2017-10-28 14:33:23 PDT	2017-10-28 14:33:23 PDT	1091
Homegroup.lnk	2017-10-28 14:32:34 PDT	2017-10-28 14:32:34 PDT	2017-10-28 14:31:49 PDT	2017-10-28 14:31:49 PDT	1070
Kleopatra.lnk	2017-10-28 14:33:22 PDT	2017-10-28 14:33:22 PDT	2017-10-28 14:33:22 PDT	2017-10-28 14:33:22 PDT	1981
Libraries.lnk	2017-10-28 14:31:18 PDT	2017-10-28 14:32:48 PDT	2017-10-28 14:30:46 PDT	2017-10-28 14:30:46 PDT	712
Mozilla Firefox.lnk	2017-10-28 14:33:22 PDT	2017-10-28 14:33:22 PDT	2017-10-28 14:33:22 PDT	2017-10-28 14:33:22 PDT	1105
Mozilla Thunderbird.lnk	2017-10-28 14:33:22 PDT	2017-10-28 14:33:22 PDT	2017-10-28 14:33:22 PDT	2017-10-28 14:33:22 PDT	1155
Opera Mail.lnk	2017-10-28 14:33:22 PDT	2017-10-28 14:33:22 PDT	2017-10-28 14:33:22 PDT	2017-10-28 14:33:22 PDT	1856
Opera Browser.lnk	2017-10-28 14:33:22 PDT	2017-10-28 14:33:22 PDT	2017-10-28 14:33:22 PDT	2017-10-28 14:33:22 PDT	1093
Stellar MBOX to PST Converter.lnk	2017-10-28 14:33:22 PDT	2017-10-28 14:33:22 PDT	2017-10-25 15:13:01 PDT	2017-10-25 15:13:01 PDT	1006
tj-pub-key	2017-10-28 14:33:22 PDT	2017-10-28 14:33:22 PDT	2017-10-25 15:13:01 PDT	2017-10-25 15:13:01 PDT	1732
WinRAR.lnk	2017-10-28 14:33:22 PDT	2017-10-28 14:33:22 PDT	2017-10-28 14:33:22 PDT	2017-10-28 14:33:22 PDT	975

Highlighted files are tagged

Figure 14-3 Tagged files in the Desktop folder

Source: *www.sleuthkit.org*

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Using Autopsy to Generate Reports (4 of 4)

Directory Listing

/img_GCFI-tj01.001/Program Files

34 Results

Table | Thumbnail

Name	Modified Time	Change Time	Access Time	Created Time	Size
[current folder]	2017-10-28 14:49:31 PDT	2017-10-28 14:49:31 PDT	2017-10-28 14:49:31 PDT	2017-10-25 15:11:16 PDT	56
[parent folder]	2017-10-25 15:15:39 PDT	2017-10-28 14:28:23 PDT	2017-10-25 15:15:39 PDT	2017-10-23 17:10:49 PDT	56
ByteFence	2017-07-01 06:21:22 PDT	2017-10-25 15:11:16 PDT	2017-10-25 15:11:16 PDT	2017-10-25 15:11:16 PDT	48
Camouflage	2017-10-26 09:37:32 PDT	2017-10-26 09:37:32 PDT	2017-10-26 09:37:32 PDT	2017-10-26 09:37:32 PDT	480
Common Files	2017-10-25 15:11:16 PDT	2017-10-25 15:11:16 PDT	2017-10-25 15:11:16 PDT	2017-10-25 15:11:16 PDT	264
FileZilla FTP Client	2017-10-25 15:11:16 PDT	2017-10-25 15:11:16 PDT	2017-10-25 15:11:16 PDT	2017-10-25 15:11:16 PDT	248
GNU	2017-10-28 14:28:43 PDT	2017-10-28 14:28:43 PDT	2017-10-28 14:28:43 PDT	2017-10-28 14:28:19 PDT	144
Google	2017-10-28 14:35:43 PDT	2017-10-28 14:35:43 PDT	2017-10-28 14:35:43 PDT	2017-10-28 14:35:01 PDT	352
Internet Explorer	2017-07-01 06:22:40 PDT	2017-10-25 15:11:16 PDT	2017-10-25 15:11:16 PDT	2017-10-25 15:11:16 PDT	48
Java	2017-10-28 14:40:12 PDT	2017-10-28 14:40:16 PDT	2017-10-28 14:40:12 PDT	2017-10-28 14:40:12 PDT	48
Microsoft Analysis Services	2017-10-28 14:42:01 PDT	2017-10-28 14:42:16 PDT	2017-10-28 14:42:01 PDT	2017-10-28 14:42:01 PDT	48
Microsoft Office	2017-10-26 09:40:32 PDT	2017-10-26 09:40:32 PDT	2017-10-26 09:40:32 PDT	2017-10-25 15:11:16 PDT	672
Microsoft Security Client	2017-10-28 14:42:30 PDT	2017-10-28 14:42:43 PDT	2017-10-28 14:42:30 PDT	2017-10-28 14:42:30 PDT	48
Microsoft.NET	2017-10-28 14:42:56 PDT	2017-10-28 14:43:05 PDT	2017-10-28 14:42:56 PDT	2017-10-28 14:42:56 PDT	48
Mozilla Firefox	2017-10-28 14:46:33 PDT	2017-10-28 14:46:33 PDT	2017-10-28 14:46:33 PDT	2017-10-28 14:43:19 PDT	144
Mozilla Maintenance Service	2017-10-28 14:43:34 PDT	2017-10-28 14:43:53 PDT	2017-10-28 14:43:34 PDT	2017-10-28 14:43:34 PDT	48
Mozilla Thunderbird	2017-10-28 14:45:51 PDT	2017-10-28 14:45:51 PDT	2017-10-28 14:45:51 PDT	2017-10-28 14:44:03 PDT	152
MSBuild	2017-10-25 15:11:16 PDT	2017-10-25 15:11:16 PDT	2017-10-25 15:11:16 PDT	2017-10-25 15:11:16 PDT	152
Norton Security	2017-10-28 14:47:04 PDT	2017-10-28 14:47:13 PDT	2017-10-28 14:47:04 PDT	2017-10-28 14:47:04 PDT	48
NortonInstaller	2017-10-28 14:47:19 PDT	2017-10-28 14:47:26 PDT	2017-10-28 14:47:19 PDT	2017-10-28 14:47:19 PDT	48
NVIDIA Corporation	2017-10-25 15:11:16 PDT	2017-10-25 15:11:16 PDT	2017-10-25 15:11:16 PDT	2017-10-25 15:11:16 PDT	368
Quick Stego	2017-10-28 14:50:32 PDT	2017-10-28 14:50:32 PDT	2017-10-28 14:50:32 PDT	2017-10-28 14:48:44 PDT	56
Realtek	2017-07-01 06:22:40 PDT	2017-10-25 15:11:16 PDT	2017-10-25 15:11:16 PDT	2017-10-25 15:11:16 PDT	48
Reference Assemblies	2017-10-25 15:11:16 PDT	2017-10-25 15:11:16 PDT	2017-10-25 15:11:16 PDT	2017-10-25 15:11:16 PDT	152
Speccy	2017-07-01 06:22:40 PDT	2017-10-25 15:11:16 PDT	2017-10-25 15:11:16 PDT	2017-10-25 15:11:16 PDT	48
Steganofile	2017-10-28 14:51:43 PDT	2017-10-28 14:51:43 PDT	2017-10-28 14:51:43 PDT	2017-10-28 14:49:24 PDT	264
UNP	2017-10-25 15:11:16 PDT	2017-10-25 15:11:16 PDT	2017-10-25 15:11:16 PDT	2017-10-25 15:11:16 PDT	160

Highlighted folders are tagged

Figure 14-4 Tagged application folders under Program Files

Source: *www.sleuthkit.org*

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Summary (1 of 2)

- All U.S. district courts and many state courts require expert witnesses to submit written reports
- Rule 26 of the FRCP requires expert witnesses who anticipate testifying to submit written reports
- Attorneys use deposition banks to research expert witnesses' previous testimony
- Reports should answer the questions you were retained to answer

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Summary (2 of 2)

- A well-defined report structure contributes to readers' ability to understand the information you're communicating
- Clarity of writing is critical to a report's success
- Convey a tone of objectivity and be detached in your observations

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Guide to Computer Forensics and Investigations Sixth Edition

Chapter 15

Expert Testimony in Digital Investigations

CENGAGE

Objectives

- Explain guidelines for giving testimony as a fact witness or an expert witness
- Describe guidelines for testifying in court
- Explain guidelines for testifying in depositions and hearings
- Describe procedures for preparing forensics evidence for testimony

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Preparing for Testimony (1 of 4)

- **Fact witness**
  - Provides facts found in investigation
  - Explain what evidence is and how it was obtained
  - Does not offer conclusions, only facts
- **Expert witness**
  - Has opinions based on observations
  - Opinions are formed from experience and deductive reasoning
  - Opinions make the witness an expert

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Preparing for Testimony (2 of 4)

- For either types of testimony:
  - Establish communication early with attorney
  - Learn about the victim, the complainant, opposing experts or fact witnesses, and the opposing attorney
  - Learn the basic points of dispute
  - Keep notes in rough draft form and record only facts
    - Keep opinions to a minimum

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Preparing for Testimony (3 of 4)

- Confirm your findings with documentation
  - Corroborate them with other peers
- Digital forensics is only now developing a peer review process
- Check opposing experts to find strengths and weaknesses
  - Internet
  - Curriculum vitae
  - Deposition banks

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Preparing for Testimony (4 of 4)

- When preparing your testimony consider the following questions:
  - What is the client's overall theory of the case?
  - What is my story of the case?
  - What can I say with confidence?
  - How does my opinion fit into the theory of the case?
  - What is the scope of the case? Have I gone too far?
  - Have I identified the client's needs for how my testimony fits into the overall theory of the case?

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Documenting and Preparing Evidence (1 of 3)

- Document your steps
  - To prove them repeatable
- Validate your tools and verify evidence with hash algorithms to ensure integrity
- Do not use a formal checklist
  - Do not include checklist in final report
  - Opposing attorneys can challenge them
- Collect evidence and document employed tools
- Maintain chain of custody

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Documenting and Preparing Evidence (2 of 3)

- Collect the right amount of information
  - Collect only what was asked for
- Note the date and time of your forensic workstation when starting your analysis
- Keep only successful output
  - Do not keep previous runs
- Search for keywords using well-defined parameters

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Documenting and Preparing Evidence (3 of 3)

- Keep your notes simple
- List only relevant evidence on your report
- Define any procedures you use to conduct your analysis as scientific
  - And conforming to your profession's standards
  - List any textbooks, technical books, articles by recognized experts, and procedures from authoritative organizations that you relied on or referenced during examination

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Reviewing Your Role as a Consulting Expert or an Expert Witness

- Do not record conversations or telephone calls
- Federal information requirements
  - Other cases in which you have testified as an expert witness in the last four years
  - Ten years of any published writings
  - Previous compensations for testifying
- Evaluate the court's expert
- Brief your attorney on your findings and opinion of the court's expert

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Creating and Maintaining Your CV

- **Curriculum vitae (CV)**
  - Lists your education, training, and professional experience
  - Used to qualify your testimony
- Show you continuously enhance your skills
  - List any training, teaching, and experience
- Detail specific accomplishments
- List basic and advanced skills
- Include a testimony log

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Preparing Technical Definitions (1 of 2)

- Prepare definitions of technical concepts
- Use your own words and language
- Examples of definitions to prepare ahead of time:
  - Digital forensics or computer forensics
  - Hashing algorithms
  - Image files and bit-stream copies
  - File slack and unallocated space
  - File timestamps
  - Computer log files

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Preparing Technical Definitions (2 of 2)

- Examples of definitions to prepare ahead of time (cont'd)
  - Folder or directory
  - Hardware
  - Software
  - Operating system

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Preparing to Deal with the News Media

- Some legal actions generate interest from the news media
- Reasons to avoid contact with news media
  - Your comments could harm the case and create a record that can be used against you
  - You have no control over the context of the information a journalist publishes
  - You can’t rely on a journalist’s promises of confidentiality

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Testifying in Court

- Procedures during a trial
  - Your attorney presents you as a competent expert
  - Opposing attorney might attempt to discredit you
  - Your attorney guides you through your testimony
  - Opposing attorney cross-examines you
  - Your attorney might have an opportunity for redirect examination of material addressed in cross-examination
- You could be called later as a rebuttal witness

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Understanding the Trial Process

- Typical order of trial
  - Motion in limine
  - Impaneling the jury
  - Opening statements
  - Plaintiff
  - Defense
  - Rebuttal
  - Closing arguments
  - Jury instructions

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Providing Qualifications for Your Testimony

- Demonstrates you are an expert witness
  - This qualification is called **voir dire**
- Attorney asks the court to accept you as an expert on digital forensics
- Opposing attorney might try to disqualify you
  - Depends on your CV and experience

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

General Guidelines on Testifying (1 of 9)

- Be professional and polite
- Be conscious of the jury, judge, and attorneys
- If asked something you cannot answer, say:
  - That is beyond the scope of my expertise
  - I was not asked to investigate that
- Avoid overstating opinions
- Guidelines on delivery and presentation:
  - Always acknowledge the jury and direct your testimony to them

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

General Guidelines on Testifying (2 of 9)

- Guidelines on delivery and presentation: (cont'd)
  - Movement
    - Turn towards the questioner when asked
    - Turn back to the jury when answering
  - Place microphone six to eight inches from you
  - Use simple, direct language to help the jury understand you
  - Avoid humor
  - Build repetition into your explanations

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

General Guidelines on Testifying (3 of 9)

- Guidelines on delivery and presentation: (cont'd)
  - Use chronological order to describe events
  - If you're using technical terms, identify and define these terms for the jury
  - Cite the source of the evidence the opinion is based on
  - Make sure the chair's height is comfortable, and turn the chair so that it faces the jury

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

General Guidelines on Testifying (4 of 9)

- Guidelines on delivery and presentation: (cont'd)
  - Dress in a manner that conforms to the community's dress code
  - Don't memorize your testimony
  - For direct examination
    - State your opinions
    - Identify evidence to support your opinion
    - Explain the method used to arrive to that opinion
    - Restate your opinion

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

General Guidelines on Testifying (5 of 9)

- Prepare your testimony with the attorney who hired you
  - How is data (or evidence) stored on a hard drive?
  - What is an image or a bit-stream copy of a drive?
  - How is deleted data recovered from a drive?
  - What are Windows temporary files, and how do they relate to data or evidence?
  - What are system or network log files?

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

General Guidelines on Testifying (6 of 9)

- Using graphics during testimony
  - Graphical exhibits illustrate and clarify your findings
  - Your exhibits must be clear and easy to understand
  - Graphics should be big, bold, and simple
  - The goal of using graphics is to provide information the jury needs to know
  - Review all graphics with your attorney before trial
  - Make sure the jury can see your graphics, and face the jury during your presentation

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

General Guidelines on Testifying (7 of 9)

- Avoiding testimony problems
  - Recognize when conflict-of-interest issues apply to your case
    - **Conflicting out**: an attempt by opposing attorneys to prevent you from serving on an important case
  - Avoid agreeing to review a case unless you're under contract with that person
  - Avoid conversations with opposing attorneys
  - You should receive payment before testifying

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

General Guidelines on Testifying (8 of 9)

- Avoiding testimony problems (cont'd)
  - Don't talk to anyone during court recess
    - If a juror approaches you, decline to talk with him or her and promptly report the contact to the attorney who retained you
  - Make sure you conduct any conferences with your attorney in a private setting

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

General Guidelines on Testifying (9 of 9)

- Understanding prosecutorial misconduct
  - If you have found exculpatory evidence, you have an obligation to ensure that the evidence isn't concealed
  - Initially, you should report the evidence to the prosecutor handling the case
    - Be sure you document the communication
  - If this information isn't disclosed to the defense attorney in a reasonable time
    - You can report it to the prosecutor's supervisor or the judge

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Testifying During Direct Examination (1 of 2)

- Techniques
  - Work with your attorney to get the right language
  - Be wary of your inclination to be helpful
  - Review the examination plan your attorney has prepared
  - Provide a clear overview of your findings
  - Use a systematic easy-to-follow plan for describing your methods
  - Practice testifying
  - Use your own words when answering questions

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Testifying During Direct Examination (2 of 2)

- Techniques (cont'd)
  - Make sure you know the following terms before giving testimony:
    - Independent recollection
    - Customary practice
    - Documentation of the case
  - Present your background and qualifications
  - Avoid vagueness
  - When you're using graphics in a presentation, make sure the jury understands your explanations

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Testifying During Cross-Examination (1 of 4)

- Recommendations and practices
  - Use your own words
  - Keep in mind that certain words have additional meanings
  - Be aware of leading questions
  - Never guess when you do not have an answer

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Testifying During Cross-Examination (2 of 4)

- Recommendations and practices (cont'd)
  - Be prepared for challenging, pre-constructed questions
    - Did you use more than one tool?
  - Rapid-fire questions
  - Sometimes opposing attorneys declare that you aren't answering the questions
  - Keep eye contact with the jury
  - Sometimes opposing attorneys ask several questions inside one question

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Testifying During Cross-Examination (3 of 4)

- Recommendations and practices (cont'd)
  - Attorneys make speeches and phrase them as questions
  - Attorneys might put words in your mouth
  - Be patient
  - Most jurisdictions now allow the judge and jurors to ask questions
  - Avoid feeling stressed and losing control
  - Never have unrealistically high self-expectations when testifying; everyone makes mistakes

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Testifying During Cross-Examination (4 of 4)

- Avoid:
  - Being argumentative when being badgered by the opposing attorney
  - Having poor listening skills or using defensive body language
  - Being too talkative or talking too fast
  - Being too technical for the jury to understand
  - Acting surprised and unprepared to respond when presented with unknown or new information

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Preparing for a Deposition or Hearing

- **Deposition** differs from trial testimony
  - There is no jury or judge
- Opposing attorney previews your testimony at trial
- **Discovery deposition**
  - Part of the discovery process for a trial
- **Testimony preservation deposition**
  - Requested by your client
  - Preserve your testimony in case of schedule conflicts or health problems

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Guidelines for Testifying at Depositions (1 of 4)

- Some recommendations
  - Stay calm, relaxed, and confident
  - Maintain a professional demeanor
  - Use name of attorneys when answering
  - Keep eye contact with attorneys
  - Be assertive in your responses
  - Be professional and polite
  - Use facts when describing your opinion
  - Being deposed in a discovery deposition is an unnatural process

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Guidelines for Testifying at Depositions (2 of 4)

- If you prepared a written report, the opposing attorney might attempt to use it against you
- If your attorney objects to a question from the opposing attorney
  - Pause and think of what direction your attorney might want you to go in your answer
- Be prepared at the end of a deposition to spell any specialized or technical words you used

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Guidelines for Testifying at Depositions (3 of 4)

- Recognizing deposition problems
  - Discuss any problem before the deposition
    - Identify any negative aspect
  - Be prepared to defend yourself
  - Avoid
    - Omitting information
    - Having the attorney box you into a corner
    - Contradictions
  - Be professional and polite when giving opinions about opposite experts

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Guidelines for Testifying at Depositions (4 of 4)

- Recognizing deposition problems (cont'd)
  - To respond to difficult questions that could jeopardize your client's case
    - Pause before answering
  - Keep in mind that you can correct any minor errors you make during your examination
  - Discovery deposition testimony often doesn't make it to the jury
    - It might be presented to the jury, usually as part of an attempt to discredit the witness

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Guidelines for Testifying at Hearings

- Testifying at a hearing is generally comparable to testifying at a trial
- A hearing can be before an administrative agency or a legislative body or in a court
- Often administrative or legislative hearings are related to events that resulted in litigation
- A judicial hearing is held in court to determine the admissibility of certain evidence before trial
  - No jury is present

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Preparing Forensics Evidence for Testimony (1 of 3)

- Use Autopsy for Windows to extract e-mail in a forensic image
  - See Figures 15-1 and 15-2

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Preparing Forensics Evidence for Testimony (2 of 3)

Figure 15-1 E-mails sorted by sender

Source: *www.sleuthkit.org*

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Preparing Forensics Evidence for Testimony (3 of 3)

Figure 15-2 The Excel spreadsheet of Jim Shu's e-mails

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Preparing a Defense of Your Evidence-Collection Methods

- To prepare for testimony
  - You should prepare answers for questions on what steps you took to extract e-mail metadata and messages
- You might also be asked to explain specific features of the computer, OS, and applications (such as Outlook)
  - And explain how these applications and digital forensics tools work

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Summary (1 of 3)

- When cases go to trial, you as the forensics expert play one of two roles: a fact witness or an expert witness
- If you're called as a fact or expert witness in a digital forensics case, you need to prepare for your testimony thoroughly
- When you're called to testify in court, your attorney examines you on your qualifications to establish your competency as an expert or a fact witness

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Summary (2 of 3)

- Make sure you're prepared for questions opposing counsel might use to discredit you, confuse you, or throw you off the track
- Know whether you're being called as a fact witness or expert witness (or both) and whether you're being retained as a consulting expert or expert witness
- Deposition differs from a trial because there's no jury or judge

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Summary (3 of 3)

- Depositions usually fall into two categories: discovery depositions and testimony preservation depositions
- Guidelines for testifying at depositions and hearings are much the same as guidelines for courtroom testimony
- Make sure you prepare answers for questions on what steps you took to collect and analyze evidence and questions on what tools you used and how they work

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Guide to Computer Forensics and Investigations Sixth Edition

Chapter 16

Ethics for the Expert Witness

CENGAGE

Objectives

- Explain how ethics and codes apply to expert witnesses
- Explain how other organizations' codes of ethics apply to expert testimony
- Describe ethical difficulties in expert testimony
- Explain the process of carving data manually

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Applying Ethics and Codes to Expert Witnesses (1 of 3)

- **Ethics**
  - Rules you internalize and use to measure your performance
- **Codes of professional conduct or responsibility**
  - Standards that others apply to you or that you are compelled to adhere to by external forces
    - Such as licensing bodies
- People need ethics to help maintain their balance
  - And self-respect and the respect of their profession

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Applying Ethics and Codes to Expert Witnesses (2 of 3)

- Laws governing codes of professional conduct or responsibility
  - Define the lowest level of action or performance required to avoid liability
- Expert witnesses should present unbiased, specialized, and technical evidence to a jury
  - Control your biases, do not allow them to control you
- Expert witnesses testify in more than 80% of trials
  - And in many trials, multiple expert witnesses testify

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Applying Ethics and Codes to Expert Witnesses (3 of 3)

- The most important laws applying to attorneys and witnesses are the rules of evidence
- Experts are bound by their personal ethics and the ethics of their professional organizations
- In the United States, there's no state or national licensing body for digital forensics examiners
  - Your sources for ethical standards are your internal values and codes of professional associations you belong to

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Forensics Examiners' Roles in Testifying

- Digital forensics examiners have two roles:
  - Fact witness and expert witness
- As an expert witness
  - You can testify even if you weren't present when the event occurred
    - Or didn't handle the data storage device personally
- Criticism: it's possible to find and hire an expert to testify to almost any opinion on any topic
  - Beware of attorneys' opinion shopping

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Considerations in Disqualification (1 of 4)

- One of the effects of violating court rules or laws is **disqualification**
- Opposing counsel might attempt to disqualify you
  - Based on any deviations from opinions you've given in previous cases
- Some attorneys contact many experts as a ploy to disqualify them
  - Or prevent opposing counsel from hiring them
- Determine who the parties are to reduce the possibility of a conflict

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Considerations in Disqualification (2 of 4)

- Whenever you are aware of a possible disqualification issue
  - Bring it to the attention of the attorney who has retained you
- Factors to disqualify an expert include:
  - Whether the attorney informed the expert that their discussions were confidential
  - Whether the expert reviewed materials marked as confidential or attorney work product
  - Whether the expert was asked to sign a confidentiality agreement

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Considerations in Disqualification (3 of 4)

- Factors to disqualify an expert include: (cont'd)
  - Number of discussions held over a period of time
  - The type of documents that were reviewed
  - The type of information conveyed to the expert
  - The amount of time involved in discussions or meetings between the expert and attorney
  - Whether the expert provided the attorney with confidential information
  - Whether the attorney formally retained the expert

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Considerations in Disqualification (4 of 4)

- Factors to disqualify an expert include: (cont'd)
  - Whether the expert voiced concerns about being retained
  - Whether the expert was requested to perform services for the attorney
  - Whether the attorney compensated the expert

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Traps for Unwary Experts (1 of 3)

- Be cautious about the following potential traps
  - What are some differences between the attorney's motives and the investigator's duty?
  - Is the function of the expert witness in conflict with the investigator's code of professional responsibility?
  - You should anticipate that the opposing counsel will look at your organization memberships and those organizations' codes of professional responsibility
- **Contingency fees** aren't allowed except in certain limited circumstances

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Traps for Unwary Experts (2 of 3)

- Avoid obvious ethical errors
  - Don’t alter data or present false data
  - Don’t report work that was not done
  - Don’t ignore available contradictory data
  - Don’t do work beyond your expertise or competence
  - Don’t allow the attorney who retained you to influence your opinion in an unauthorized way

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Traps for Unwary Experts (3 of 3)

- Avoid obvious ethical errors (cont'd)
  - Don't accept an assignment if it cannot be done reasonably in the allowed time
  - Don't reach a conclusion before doing complete research
  - Don't fail to report possible conflicts of interest

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Determining Admissibility of Evidence

- Hypothetical questions can give you the factual structure to support and defend your opinion
- Although expert opinions can be presented without stating the underlying factual basis
  - The testimony isn't admissible if the facts on which the opinion is based are inadequate
  - Or there's not enough evidence to allow stating a legitimate opinion

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Organizations with Codes of Ethics

- No single source offers a definitive code of ethics for expert witnesses
- You must draw on standards from other organizations to form your own ethical standards
- Many organizations have rules to guide their members in areas such as:
  - Interaction with patients/clients, objectivity, role in society, fees, solicitation, independence, and contractual relationships

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

International Society of Forensic Computer Examiners (1 of 2)

- ISFCE includes guidelines such as the following:
  - Maintain the utmost objectivity in all forensic examinations and present findings accurately
  - Conduct examinations based on established, validated principles
  - Testify truthfully in all matters before any board, court, or proceeding
  - Avoid any action that would appear to be a conflict of interest

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

International Society of Forensic Computer Examiners (2 of 2)

- ISFCE includes guidelines such as the following: (cont'd)
  - Never misrepresent training, credentials, or association membership
  - Never reveal any confidential matters or knowledge learned in an examination without an order from a court of competent jurisdiction or the client's express permission

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

International High Technology Crime Investigation Association

- HTCIA core values include the following requirements related to testifying:
  - The HTCIA values the Truth uncovered within digital information and the effective techniques used to uncover that Truth, so that no one is wrongfully convicted
  - The HTCIA values the Integrity of its members and the evidence they expose through common investigative and digital forensics best practices, including specialized techniques used to gather digital evidence

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

International Association of Computer Investigative Specialists

- Standards for IACIS members include:
  - Maintain the highest level of objectivity in all forensic examinations and accurately present the facts involved
  - Thoroughly examine and analyze the evidence
  - Conduct examinations based on established, validated principles
  - Render opinions having a basis that is demonstratively reasonable
  - Not withhold any findings that would cause the facts of a case to be misrepresented or distorted

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

American Bar Association

- Be aware of the basic rules of professional conduct attorneys must follow
- ABA's Model Code of Professional Responsibility (Model Code) and its successor, the Model Rules of Professional Conduct (Model Rules)
  - Are the basis of state licensing bodies' codes
- The ABA has stated that expert witnesses do not owe a duty of loyalty to their clients

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

American Psychological Association

- For psychologists, the broadly accepted guidelines governing their conduct as experts are:
  - The American Psychological Association's (APA's) Ethical Principles of Psychologists and Code of Conduct
  - Commonly referred to as "Ethics Code"
- These guidelines offer comprehensive regulations
  - With an entire section devoted to forensics activities

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Ethical Difficulties in Expert Testimony (1 of 2)

- There are inherent conflicts between the goals of attorneys
  - And the goals of scientists or technicians (experts)
- Attorneys work in an adversarial system and look to sway the judge or jury
- Science requires experts to focus on the evidence without the influence of others' objectives
- *Daubert* and the APA's forensics guidelines
  - Can challenge experts to choose between complete impartiality and responsible advocacy

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Ethical Difficulties in Expert Testimony (2 of 2)

- Enforcing any professional organization's ethical guidelines is difficult
  - Principles can be enforced only against members of the organization
- All guidelines rely primarily on internalization of the codes and witnesses' analysis of when and how they will participate in a case
- Available guidelines set only a minimum level of acceptable performance or competence as the standard

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Ethical Responsibilities Owed to You (1 of 2)

- Your attorney owes you
  - A fair statement of the case or situation
  - Adequate time to review evidence and prepare your report
  - A reasonable opportunity to examine data, conduct testing, and investigate the matter before rendering an opinion
- Most attorneys, including opposing counsel, are competent, courteous professionals

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Ethical Responsibilities Owed to You (2 of 2)

- Some opposing counsel attempt to make discovery depositions physically uncomfortable
  - After noting a problem, you can refuse to continue with the deposition
- As a measure of protection, you might want to have your personal attorney attend the deposition
  - This attorney can't object to questions but is available to advise the attorney who retained you or to advise you during breaks

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Standard and Personally Created Forensics Tools

- The tools you use to recover, control, and track evidence are subject to review by opposing parties
  - If the court deems them unreliable, the evidence you recovered with those tools might not be admitted
    - Or might be admitted with a limiting instruction
- If you use standard tools, you simplify the process of validating them
- Personally created tools might have advantages that you can demonstrate to a judge
  - Who determines whether evidence is admissible

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

An Ethics Exercise

- By following the activities at the end of the chapter, you will be:
  - Performing a cursory exam of a Forensic Image
  - Performing a Detailed Exam of a Forensic Image
  - Performing the Exam
  - Interpreting Attribute 0x80 Data Runs
    - Finding Attribute 0x80 an MFT Record
    - Configuring Data Interpreter Options in WinHex
    - Calculating Data Runs
  - Carving Data Run Clusters Manually

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Performing a Cursory Exam of a Forensic Image

Figure 16-1 The Mount Image To Drive dialog box

Source: AccessData Group, Inc., *www.accessdata.com*

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Performing a Detailed Exam of a Forensic Image

Figure 16-5 Finding a corrupt record in the `$MFT` file

Source: X-Ways AG, *www.x-ways.net*

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Performing the Exam

- To maintain the highest possible ethical standards when conducting a forensics examination
  - You should develop a plan and review it before starting your analysis
- Preparing for an Examination
  - Planning stage should cover all possibilities, including giving an opinion of whether data was corrupted intentionally or unintentionally

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Interpreting Attribute 0x80 Data Runs

Figure 16-12 Selecting an MFT record header

Source: X-Ways AG, *www.x-ways.net*

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Carving Data Run Clusters Manually

Figure 16-22 The recovered `Kayak4(1).jpg` file

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Summary (1 of 3)

- Ethics can be defined as rules you internalize and use to measure your performance
- Digital forensics examiners don’t have the same formal codes of conduct that professions such as medicine and the law have
- You owe your client a full understanding of the facts relevant to your opinion
- Be aware of attempts to disqualify you as an expert
- Courts use many factors in determining whether to disqualify an expert

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Summary (2 of 3)

- Be aware of obvious ethical errors, such as:
  - Ignoring contradictory data
  - Performing work beyond your expertise
  - Allowing attorneys to influence your opinion
  - Reaching a conclusion before completing research
- No single source offers a definitive code of ethics for expert witnesses
- The ISFCE Code of Ethics provides guidelines for its members and the IACIS has a guide for expected behavior of forensics examiners

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

Summary (3 of 3)

- The inherent conflict between the needs of the justice system and your obligations for professional conduct can create ethical difficulties
- The attorney who has retained you, opposing counsel, and the court owe you ethical responsibilities as an expert witness
- The tools you use to recover, control, and track evidence are subject to review by opposing parties
- After carving data artifacts, analyzing as much of the information as possible is critical

CENGAGE

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.