

# Guide to Computer Forensics and Investigations

## Sixth Edition

### Chapter 1

#### *Understanding The Digital Forensics Profession and Investigations*

CENGAGE



1



### 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.

2

2



## 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.

3

3



## 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.

4

4



## 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.

5



## 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.

6

6



## Digital Forensics and Other Related Disciplines (2 of 3)

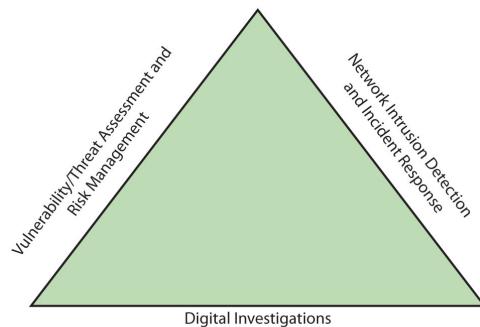


Figure 1-1 The investigations triad



## Digital Forensics and Other Related Disciplines (3 of 3)

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



## 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.

9

9



## 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.

10

10



## 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 public 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.

11



## Preparing for Digital Investigations (1 of 3)

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

12



## 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



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

13

13



## 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



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

14

14



## 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

The Computer Fraud and Abuse Act of 1986 makes it a crime for anyone to access without authorization a computer or computer system used by a financial institution, US government agency, or any organization or individual involved in interstate or foreign commerce or communication.



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

15

15



## 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



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

16

16



## 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.

17



## 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



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

18

18



## 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



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

19

19



## 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



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

20

20

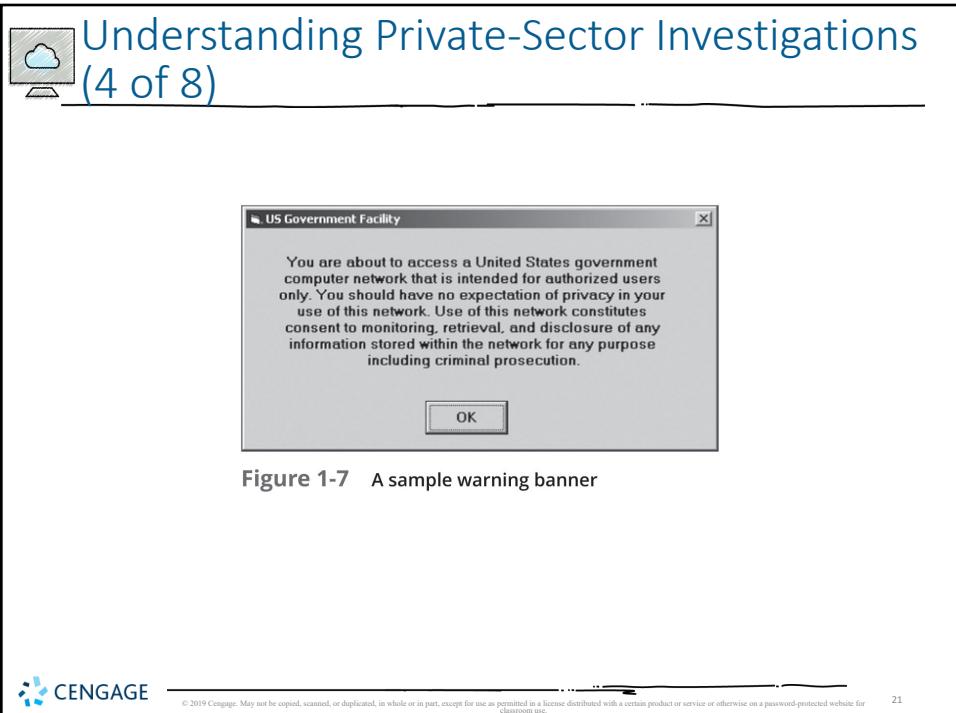


Figure 1-7 A sample warning banner

21

A screenshot of a Windows-style dialog box titled "Understanding Private-Sector Investigations (5 of 8)". The text inside the box is identical to the one in Figure 1-7: "You are about to access a United States government computer network that is intended for authorized users only. You should have no expectation of privacy in your use of this network. Use of this network constitutes consent to monitoring, retrieval, and disclosure of any information stored within the network for any purpose including criminal prosecution." At the bottom of the box is an "OK" button.

• 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

22



## 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.

23



## 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.

24

24



## 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



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

25

25



## 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



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

26

26



## 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



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

27

27



## 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



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

28

28



## 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.

29



## 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.

30



## 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.

31

31



## 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.

32

32



## 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.

33

33



## 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.

34

34



## 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.

35

35



## Planning Your Investigation (4 of 5)

**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 as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

36

36



## 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 of Test	
Page ___ of ___			

**Figure 1-10 A single-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.

37

37



## 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.

38

38



## 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



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

39

39



## 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



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

40

40



## 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.

41

41



## 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.

42

42



## 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.

43



## 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.

44



## 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.

45

45



## 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.

46

46



## 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



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

47



## 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



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

48

48



## 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



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

49

49



## 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 sniffer
  - Threat assessment specialist (typically an attorney)



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

50

50



## 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.

51

51



## 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.

52

52



## 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



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

53

53



## 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



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

54

54



## 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



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

55

55



## 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



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

56

56



## 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.

57



## 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.

58



## 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



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

59

59



## 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



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

60

60



## 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



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

61

61



## 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



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

62

62



## Understanding Bit-stream Copies (2 of 2)

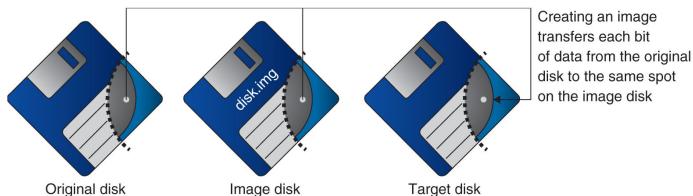


Figure 1-11 Transfer of data from original to image to target



© 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.

63

63

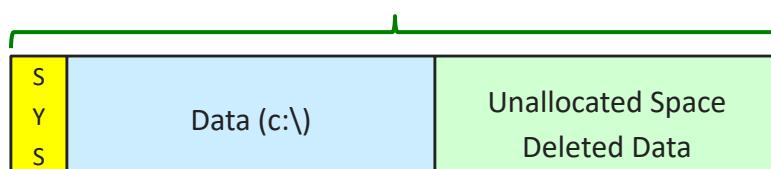


## Understanding Bit-stream Copies

- A normal “copy” of a hard drive



- A forensic image/bitstream copy



64

64



## 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.

65

65



## 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.

66

66



## 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



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

67

67



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

68

68

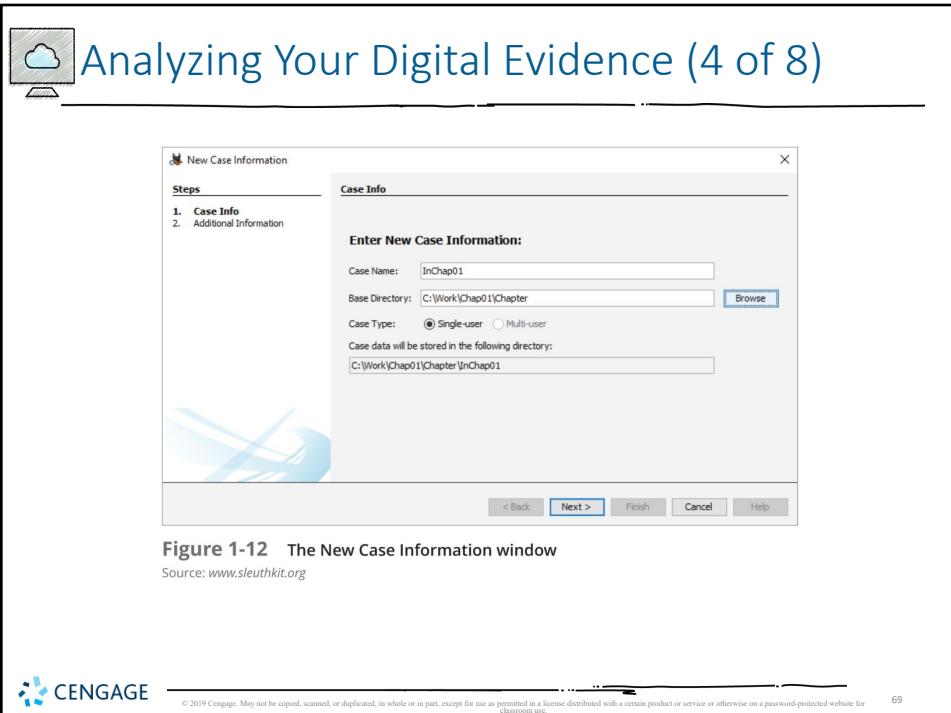


Figure 1-12 The New Case Information window

Source: [www.sleuthkit.org](http://www.sleuthkit.org)

**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

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except 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 screenshot shows the 'Keyword search' interface of the SleuthKit tool. At the top, there's a header with a cloud icon and the title 'Analyzing Your Digital Evidence (6 of 8)'. Below the header is a toolbar with icons for file operations and a 'Keyword Lists' dropdown. The main area contains a search bar with the term 'George' entered, a 'Search' button, and three radio buttons for search modes: 'Exact Match' (selected), 'Substring Match', and 'Regular Expression'. The status bar at the bottom indicates '10 Results'.

**Figure 1-18** Entering a keyword search term  
Source: [www.sleuthkit.org](http://www.sleuthkit.org)

71

The screenshot shows the search results for the keyword 'George'. The interface has a header with a cloud icon and the title 'Analyzing Your Digital Evidence (7 of 8)'. Below the header is a toolbar with icons for file operations and a 'Keyword search' dropdown. The main area displays a table of search results. The columns are 'Name', 'Location', 'Modified Time', 'Change Time', and 'Access Time'. There are 10 results listed, all of which contain the keyword 'George'. The results include various file types such as .dd, .doc, .txt, and .pdf. The 'Location' column shows paths like '/Unalloc\_16\_12134\_1474560/jmg\_1rcp01.dd' and '/Unalloc\_16\_12134\_1474560/jmg\_1rcp01.dd/CarveFiles/00000000.doc'. The 'Modified Time' column shows dates like '2009-09-00 00:00:00' and '2009-12-09 06:51:50 PST'. The 'Change Time' and 'Access Time' columns show '0000-00-00 00:00:00' for most entries. The status bar at the bottom indicates '10 Results'.

**Figure 1-19** Viewing the results of searching for the keyword "George"  
Source: [www.sleuthkit.org](http://www.sleuthkit.org)

72

The screenshot shows a digital forensics interface with a title bar "Analyzing Your Digital Evidence (8 of 8)". Below the title is a "Directory Listing" table with 10 results. The table columns include Name, Location, Modified Time, Change Time, Access Time, and Created Time. The results list various files such as "Unloc\_01\_221294\_1474960", "00000041.doc", "00000041.txt", "00000048.txt", "00000048.htm", "Billing Letter.doc", "confirmation.htm", "F0000049.doc", "Income.xls", "letter 1.txt", and "Regrets.doc". Below the table is a hex editor window showing binary data in groups of FF FF FF. At the bottom of the interface are tabs for Hex, Strings, File Metadata, Results, Indexed Text, and Help, along with page navigation controls.

**Figure 1-20** Viewing search results found in unallocated drive space  
Source: www.sleuthkit.org

CENGAGE

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

73

The screenshot shows a digital forensics interface with a title bar "Completing the Case (1 of 2)". Below the title is a bulleted list of steps for completing a case:

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

**CENGAGE**

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

74

74



## 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.

75



## 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.

76

76



## 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.

77



## 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.

78



## 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

# Guide to Computer Forensics and Investigations

## Sixth Edition

### *Chapter 3*

#### *Data Acquisition*

CENGAGE



1



### 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.

2

2



## 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.

3

3



## 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.

4

4



## 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
    - Retry reads on weak media spots



CENGAGE

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

5



## 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
  - Used by EnCase, FTK, and X-Ways 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.

6

6



## 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



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

7

7



## Determining the Best Acquisition Method (1 of 4)

- Types of acquisitions
  - **Static acquisitions**
    - Preferred method on powered-off system, but limitations due to encrypted drives
  - **Live acquisitions**
    - Computer powered on, logged on by suspect (password/passphrase available)
- 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



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

8

8



## 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
    - Hardware/software errors or incompatibilities (e.g., older drives)
  - Tools can adjust disk's geometry configuration
  - Tools: EnCase and X-Ways



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

9

9



## 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



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

10

10



## Determining the Best Acquisition Method (4 of 4)

- When making a copy, consider:
  - Size of the source disk
    - Lossless compression might be useful
      - ZIP files won't compress much more
      - JPEGs use lossy compression and degrade image quality
    - Use digital signatures for verification (e.g., MD5 or SHA-1)
  - When working with large drives, an alternative is using lossless compression
    - E.g., for 3 TB SATA drive, can create disk-to-image file on 2 TB target drive
  - Whether you can retain the disk
  - Time to perform the acquisition
  - Where the evidence is located



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

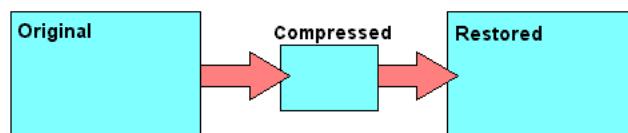
11

11



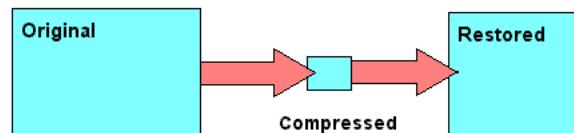
## Lossless vs. Lossy Compression

### LOSSLESS



E.g., PNG

### LOSSY



E.g., MP3, JPG



12

12



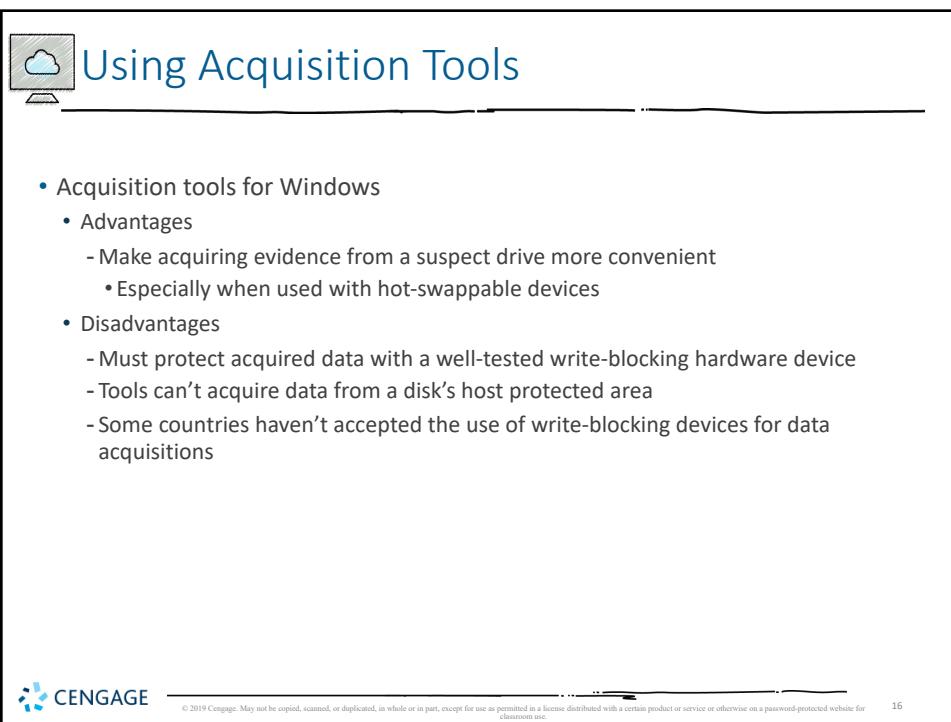
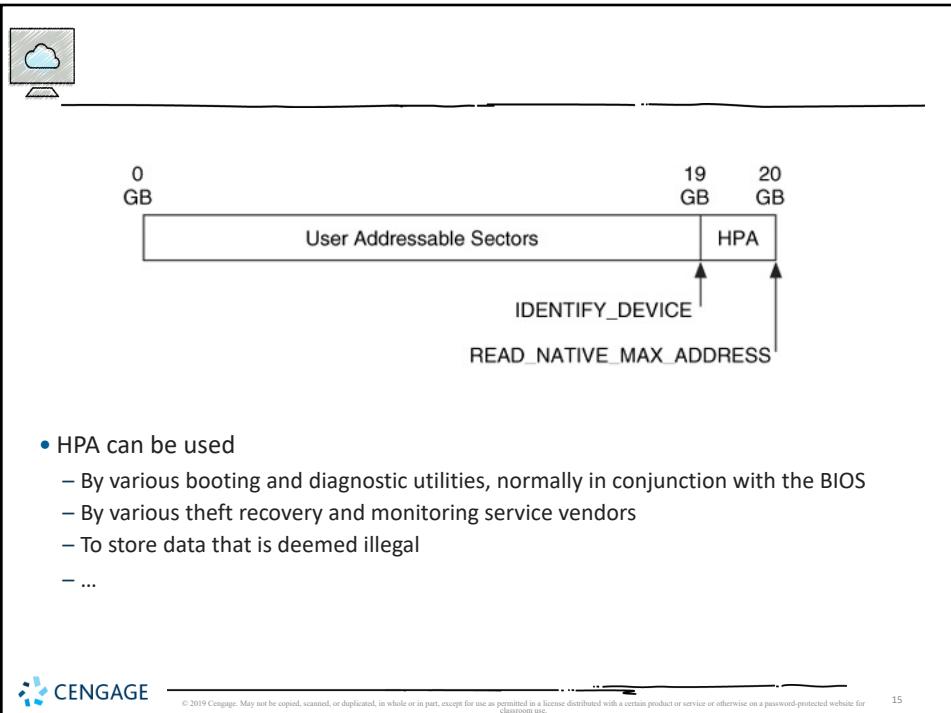
## Lossless vs. Lossy Compression

Lossless pixel compression



## 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





## 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



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

17

17



## 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
  - Windows will write to Recycle Bin, and sometimes to NTFS Journal, just from booting up with a hard drive connected
  - Linux kernel 2.6 and later write metadata to the drive, such as mount point configurations for an ext2 or ext3 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

These changes corrupt  
the evidence



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

18

18



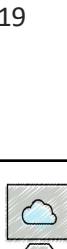
## Acquiring Data with a Linux Boot CD (2 of 6)

- 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)



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

19



## 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



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

20

20



## 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.

21

21



## 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



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

22

22



## 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



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

23

23



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

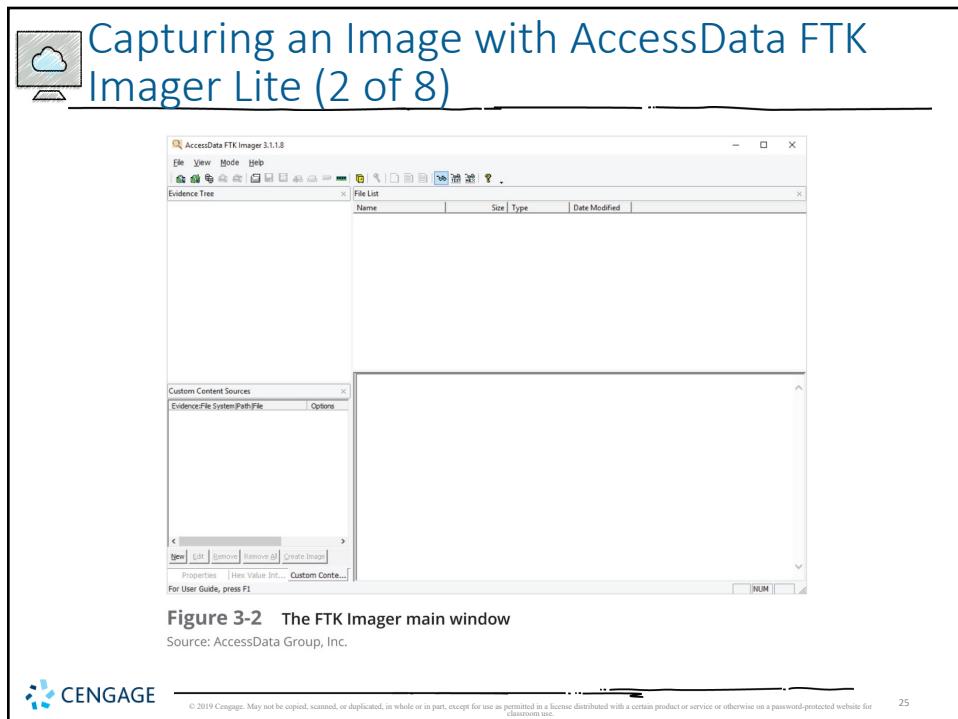
- Included with AccessData Forensic Toolkit
- Designed for viewing evidence disks and disk-to-image files
- Makes disk-to-image copies of evidence drives
  - At logical partition and physical drive level
  - Can segment the image file
- Evidence drive must have a hardware write-blocking device
  - Or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



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

24

24



**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.

25

- FTK Imager can't acquire a drive's host protected area
  - But ProDiscover can
- 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



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

26

26

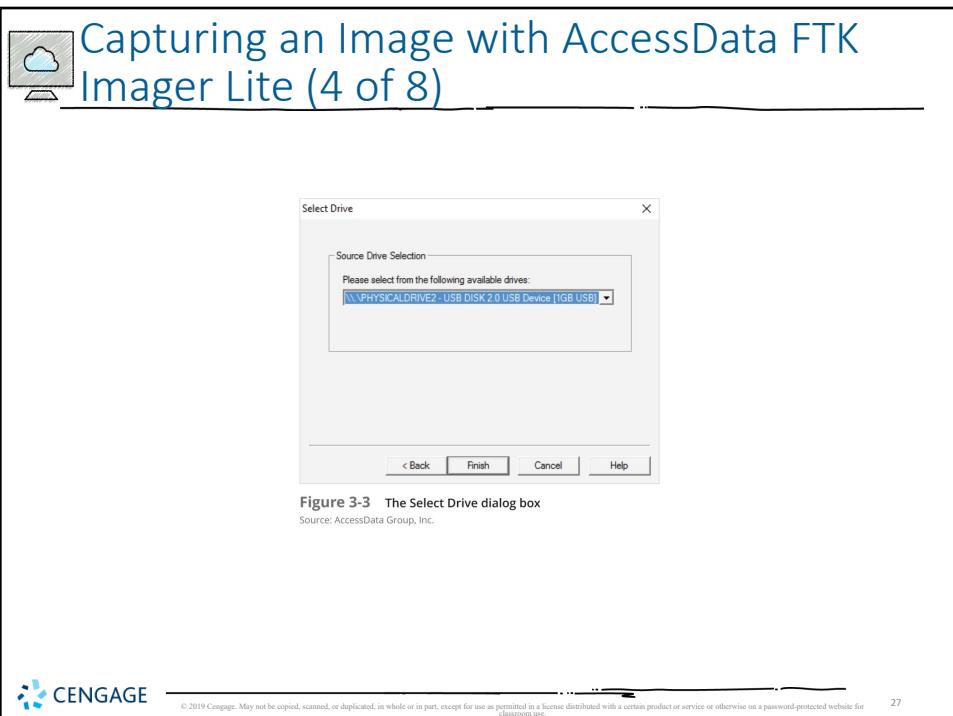


Figure 3-3 The Select Drive dialog box

Source: AccessData Group, Inc.

27

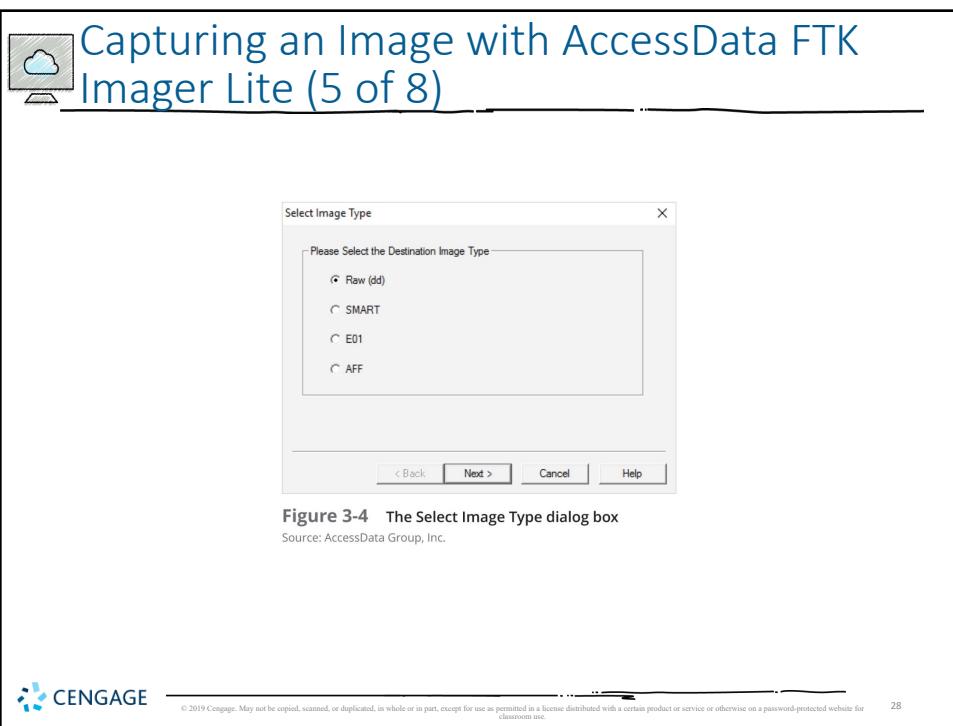
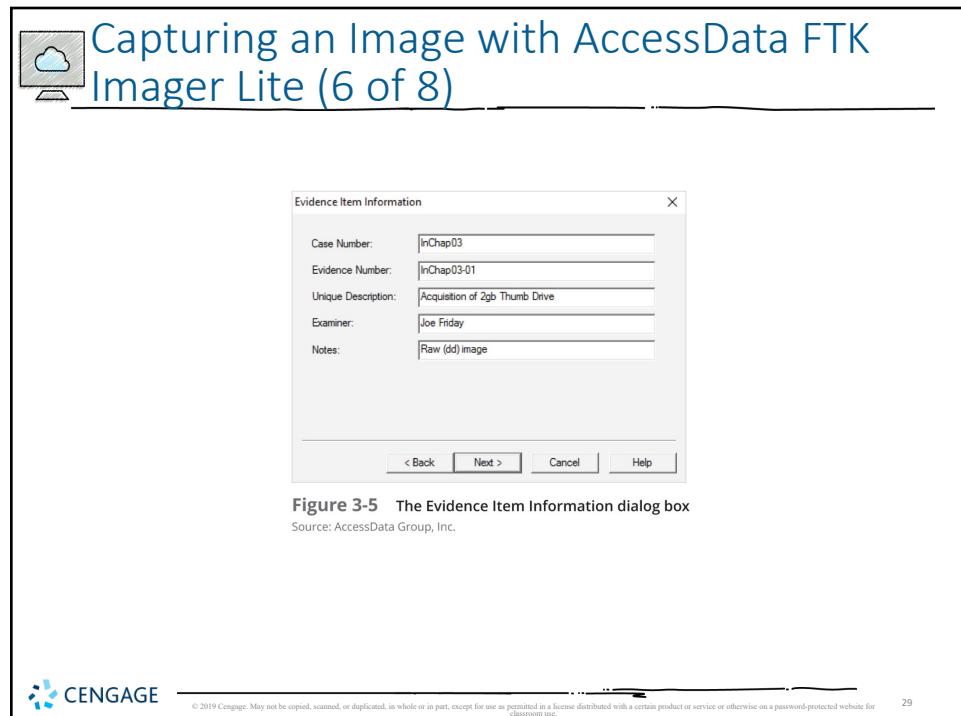


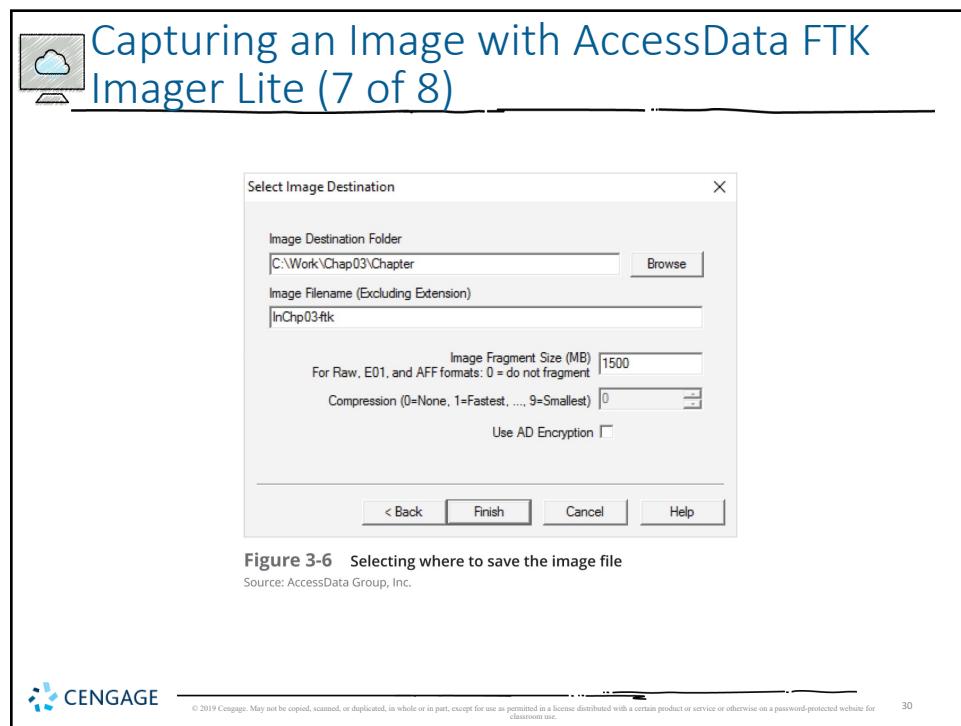
Figure 3-4 The Select Image Type dialog box

Source: AccessData Group, Inc.

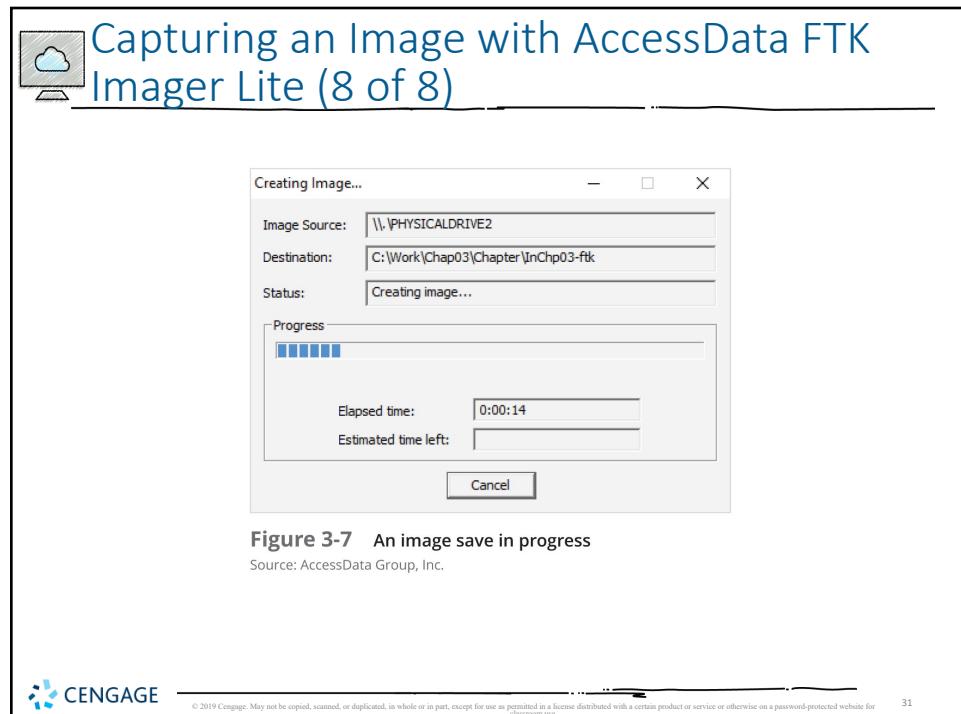
28



29



30



**Figure 3-7 An image save in progress**

Source: AccessData Group, Inc.



31

The slide has a title "Validating Data Acquisitions" with a cloud icon. The content is a bulleted list:

- 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
  - MD5 has collisions, so it is not perfect, but it's still widely used
  - SHA-1 has some collisions, but it's better than MD5

**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
  - MD5 has collisions, so it is not perfect, but it's still widely used
  - SHA-1 has some collisions, but it's better than MD5

**CENGAGE**

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

32



## 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



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

33

33



## 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



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

34

34



## 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 (1B GB) of data



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

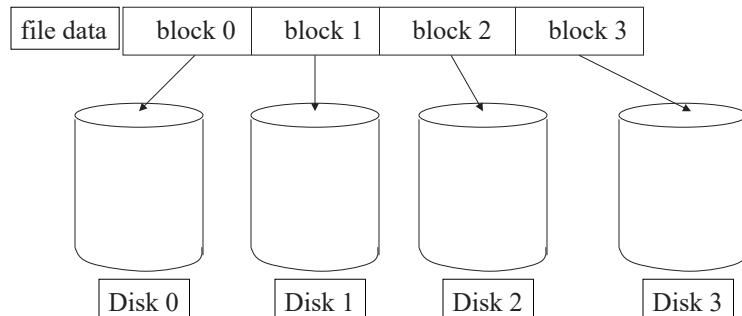
35

35



## Striping

- Take file data and map it to different disks
- Allows for reading data in parallel



36

36



## Parity

- Way to do error checking and correction
- Add up all the bits that are 1
  - If even number, set parity bit to 0
  - If odd number, set parity bit to 1
- To actually implement this, do an exclusive OR of all the bits being considered
- Consider the following 2 bytes

<u>byte</u>	<u>parity</u>
10110011	1
01101010	0

- If a single bit is bad, it is possible to correct it



CENGAGE

37

37



## Mirroring

- Keep two copies of data on two separate disks
- Gives good error recovery
  - If some data is lost, get it from the other source
- Expensive
  - Requires twice as many disks
- Write performance can be slow
  - Have to write data to two different spots
- Read performance is enhanced
  - Can read data from file in parallel



CENGAGE

38

38



## 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 (Striped)
  - Provides rapid access and increased storage
  - Biggest disadvantage is lack of redundancy ... nor error detection
- RAID 1 (Mirrored)
  - Designed for data recovery (i.e., redundancy)
  - More expensive than RAID 0 (space and performance)



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

39

39



## Understanding RAID (2 of 7)

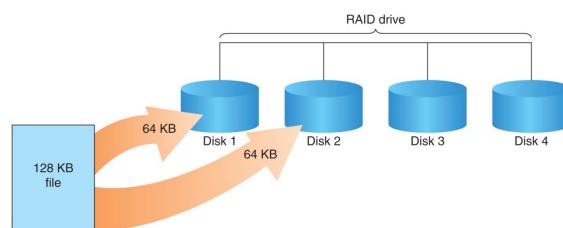


Figure 3-8 RAID 0: Striping



© 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.

40

40



## Understanding RAID (2 of 6)

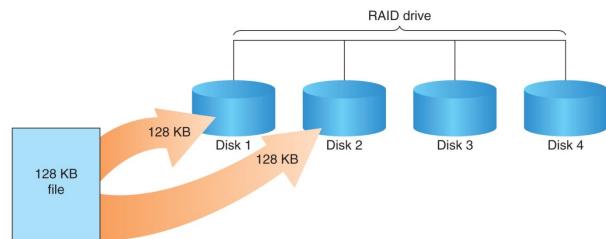


Figure 3-9 RAID 1: Mirroring



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

41

41



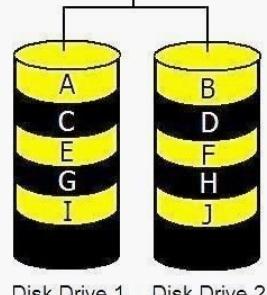
## Understanding RAID

### Block of Data

A	B
C	D
E	F
G	H
I	J

Data in one block is divided into multiple chunks of the same size

### RAID 0



The data chunks are sequentially striped across the two disk drives. Note that only one copy of the data strips exist on the drives.



42

42



## 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
    - Parity disk used to reconstruct corrupted or lost data
  - Slower than RAID 0 (read/write performance)
- RAID 3
  - Uses data striping on a **byte** level and dedicated parity disk
  - Requires at least three disks
- RAID 4
  - Similar to RAID 3
  - Data is written in **blocks** and dedicated parity 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.

43

43



## Understanding RAID (4 of 6)

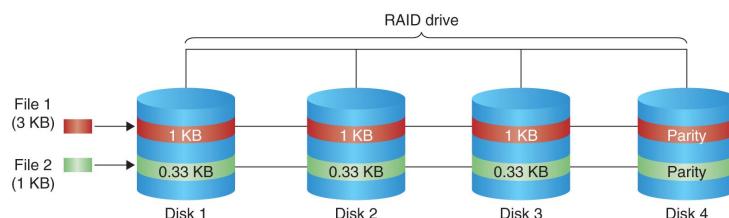


Figure 3-10 RAID 2: Striping (bit level)



© 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.

44

44



## 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 (RAID 1+0)
  - Stripe file data across multiple disks
    - Mirror each stripe onto a second disk
  - Provides fast access and redundancy
- RAID 15 (1+5)
  - Combination of RAID 1 and RAID 5
  - More costly option



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

45

45



## Understanding RAID (6 of 6)

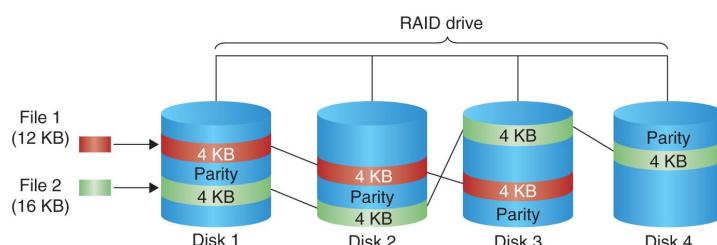


Figure 3-11 RAID 5: Block-level striping with distributed parity



© 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.

46

46



## 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.

47



## 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.

48

48



## 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



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

49

49



## 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



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

50

50



## 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



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

51

51



## 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.

52

52



## 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.

53

53



## 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.

54

54



## 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.

55

55



## 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.

56

56



## 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.

57



## 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.

58



## 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



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

59



## 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



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

60

60



## ILook Investigator |Ximager

- 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.

61

61



## 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.

62

62



## 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.

63

63



## 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.

64

64



## 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.

65

# Guide to Computer Forensics and Investigations

## Sixth Edition

### Chapter 4

#### *Processing Crime and Incident Scenes*

 CENGAGE



1



### 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.

2

2



## 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.

3

3



## 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.

4

4



## 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.

5



## 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.

6

6



## 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.

7

7



## Understanding Rules of Evidence (3 of 7)

- Business-record exception
  - A statutory exception to the rule against hearsay in Federal and most state courts
  - 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.

8

8



## 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.

9

9



## 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.

10

10



## 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.

11

11



## 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.

12

12



## 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)
  - A non-governmental organization (NGO) is a group that functions independently of any government, usually a non-profit, that is established on multiple levels to serve a social or political goal (i.e., humanitarian cause, environment protection)
- 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



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

13



## 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



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

14

14



## 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



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

15



## 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



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

16

16



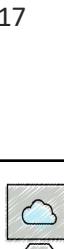
## Collecting Evidence in Private-Sector Incident Scenes (5 of 6)

- 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



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

17



## 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



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

18

18



## 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



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

19



## 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

Seize and examine, by persons qualified to do so, and in a laboratory setting, any and all electronic data processing and computer storage devices, including; central processing units, internal and peripheral storage devices such as fixed disks, external hard disks, floppy disk drives and diskettes, tape drives and tapes, optical storage devices, optical readers and scanning devices, CD Rom drives and Compact Disks and related hardware, digital cameras and digital storage media, operating logs, software and operating instructions or operating manuals, computer materials, software and programs used to communicate with other terminals via telephone or other means, and any computer modems, monitors, printers, etc., that may have been used while engaging in [specify the illegal conduct], as defined in the Annotated Code of Maryland, amended and revised.

Sample search warrant wording  
for computer evidence



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

20



## 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 when find **commingled evidence**
  - 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.

21

21



## 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.

22

22



## 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.

23

23



## 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.

24

24



## 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



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

25

25



## 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



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

26

26



## 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



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

27

27



## 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



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

28

28



## 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



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

29

29



## 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



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

30

30



## 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



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

31

31



## 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



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

32

32



## 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.

33

33



## 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



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

34

34



## 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)



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

35

35



## 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



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

36

36



## 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



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

37

37



## 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



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

38

38



## 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



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

39

39



## 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
- [www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf](http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf)
- [www.iso27001security.com/html/27037.html](http://www.iso27001security.com/html/27037.html)
- Civil investigations follow same rules
  - Consult with your attorney for extra guidelines



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

40

40



## 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.

41



## 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.

42

42



## 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.

43



## 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.

44

44



## 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



## 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



## 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.

47



## 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.

48

48



## 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.

49

49



## 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.

50

50



## 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 (storage area network)
  - 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



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

51

51



## 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
    - Costs: drive: \$400 to \$800; tape: \$40



4-mm DAT drive and tape



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

52

52



## 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
  - High-speed, high-capacity tape drive
- 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



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

53



## 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



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

54

54



## 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.

55

55



## 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



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

56

56



## 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



CENGAGE

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

57



## 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.

58



## 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)**



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

59

59



## 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
  - Although keyed hash set cannot identify files as nonkeyed hash methods can, it can produce a unique hash set for digital evidence
- You can use the MD5 function in FTK Imager to obtain the digital signature of a file or an entire drive



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

60

60



## Obtaining a Digital Hash (4 of 4)

Drive/Image Verify Results

Name	D:\
Sector count	252192
MD5 Hash	
Computed hash	ac13531a4076f2ddf692153ad7b4804b
SHA1 Hash	
Computed hash	4b67c0203045cd9503f21d4e0539e12eff
Bad Sector List	
Bad sector(s)	No bad sectors found

Close

**Figure 4-6** Using FTK Imager Lite to verify hash values  
Source: AccessData Group, Inc.

CENGAGE

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

61



## 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

CENGAGE

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

62

62



## 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



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

63

63



## 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.

64

64



## An example of a Criminal Investigation (2 of 2)

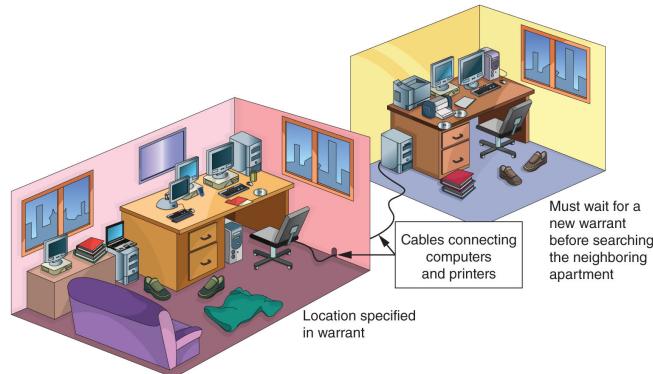


Figure 4-7 Search warrant limits



© 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.

65

65



## 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



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

66

66



## 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.

67

67



## 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



CENGAGE

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

68

68



## 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.

69

69



## 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.

70

70



## 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.

71

# 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



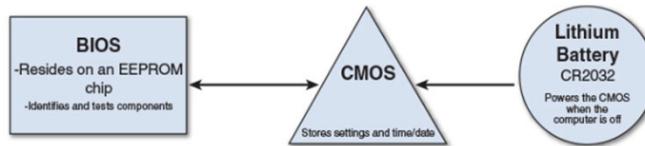
## Understanding File Systems

- **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



## 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
  - Software stored on a small, nonvolatile chip on the motherboard
    - Controls the startup process and loads the OS into memory
    - Used to identify and configure much of the hardware in a computer





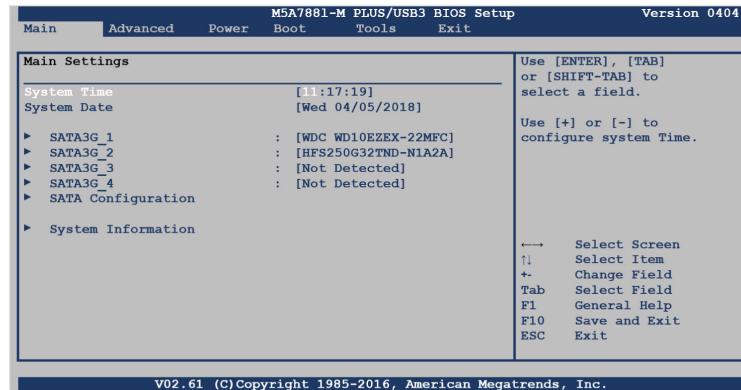
## Understanding the Boot Sequence (2 of 3)

- **Bootstrap process**

- Contained in ROM, tells the computer how to proceed
- Displays the key or keys you press to open the CMOS setup screen
  - Could be Delete, F2, F10, Ctrl+Alt+Insert, Ctrl+A, Ctrl+S, Ctrl+F1, or something else
- CMOS should be modified to boot from a forensic floppy disk or CD



## Understanding the Boot Sequence (3 of 3)



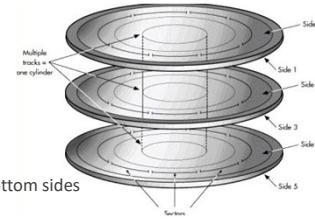
**Figure 5-1** A typical CMOS setup screen

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



## Understanding Disk Drives (1 of 4)

- Disk drives are made up of one or more platters coated with magnetic material
- Disk drive components
  - **Geometry**
    - Disk's logical structure of platters, tracks, and sectors
  - **Head**
    - The device that reads and writes data to a drive
    - There are two heads per platter that read and write the top and bottom sides
  - **Tracks**
    - Concentric circles on a disk platter where data is located
  - **Cylinders**
    - A column of tracks on two or more disk platters (each platter has two surfaces – top and bottom)
  - **Sectors**
    - A section on a track
    - Most current drives use 4096-byte sectors (up from 512-byte sectors of the past)



© 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.

7



## Understanding Disk Drives (2 of 4)

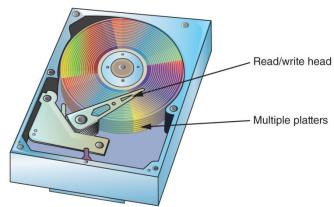
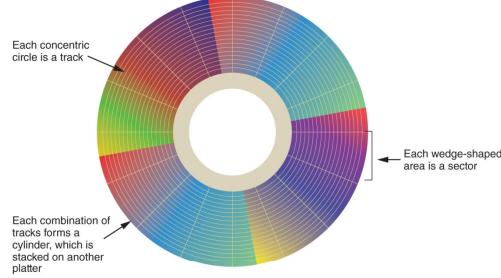


Figure 5-2 Components of a disk drive



© 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.

8



## Understanding Disk Drives (3 of 4)

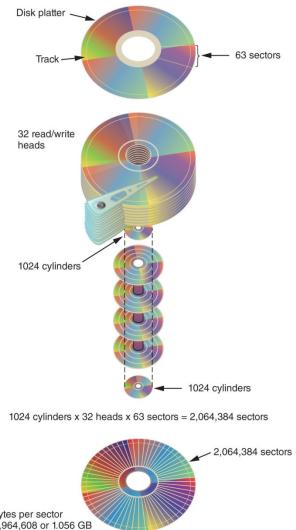


Figure 5-3 CHS calculation



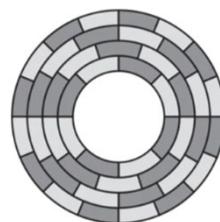
© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

9



## Understanding Disk Drives (4 of 4)

- Properties handled at the drive's hardware or firmware level
  - **Zone bit recording (ZBR)**
    - How most manufacturers deal with platter's inner tracks having a smaller circumference (and thus, less space to store data) than outer tracks
  - **Track density**
    - The space between each track
  - **Areal density**
    - The number of bits in one square inch of a disk platter (includes unused space between tracks)
  - **Head and cylinder skew**
    - Used to improve disk performance
    - **Head skew:** staggering from platter to platter within cylinder
    - **Cylinder skew:** staggering from track to track on given platter
    - As read-write head moves from one track to another, starting sectors are offset to minimize lag time



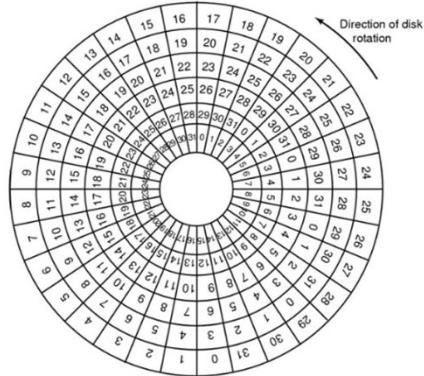
© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

10



## Cylinder Skew

- How much skew?
- Example
  - 10000 rpm
    - Drive rotates in 6 ms
  - Track has 300 sectors
    - New sector every 20  $\mu$ s
  - Track seek time 800  $\mu$ s
    - Time to position head/arm over the proper track into proper cylinder
  - Cylinder skew: 40 sectors pass on seek

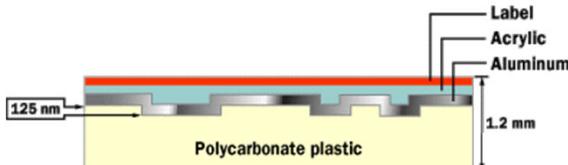
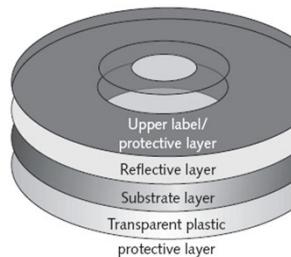


© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

11



## Examining Disk Platters

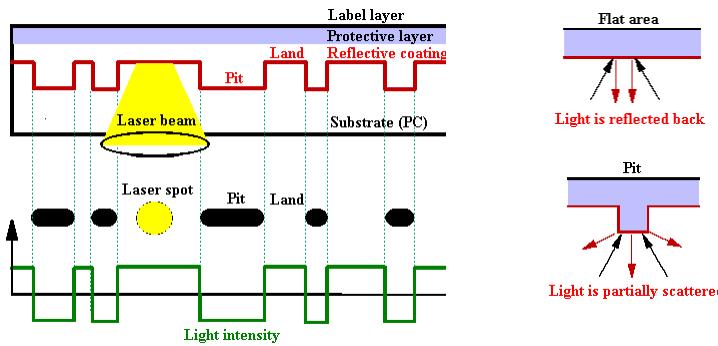


- In addition to the standard "read laser", there is a "write laser" that is more powerful than the read laser, so it interacts with the disc differently: it alters the surface instead of just bouncing light off it
  - Laser burns flat areas, called **lands**
  - Lower areas are called **pits**



12

## Focused Laser Reading the Pits

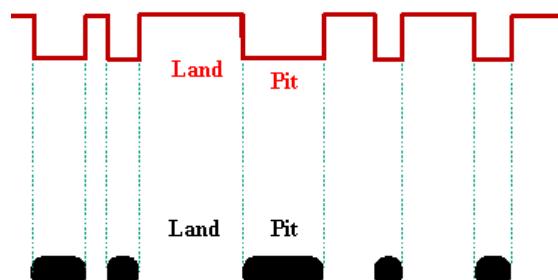


- The laser moves in the radial direction over the fast-spinning disk and scans the data track
    - The laser scatters when it scans a pit, which translates into a drop in reflected beam intensity

## Transitions and Reading Bits

- Transitions
    - From lands to pits have binary value 1 (on)
    - No transition has binary value 0 (off)

001001001010000000010000010000101000001001000





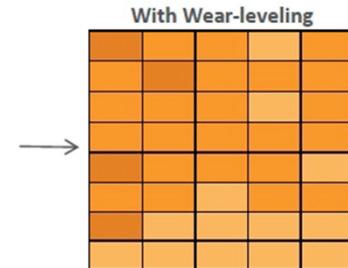
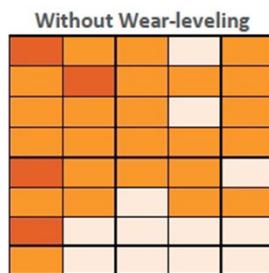
## Solid-State Storage Devices

- 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



## Solid-State Storage Devices

- High Cycles
- Medium Cycles
- Low Cycles





## 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
  - Varies according to the disk size
- 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.

17



## 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.

18



## 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

Table 5-1 Hexadecimal codes in the partition table

Hexadecimal code	File system
01	DOS 12-bit FAT (floppy disks)
04	DOS 16-bit FAT for partitions smaller than 32 MB
05	Extended partition
06	DOS 16-bit FAT for partitions larger than 32 MB
07	NTFS and exFAT
08	AIX bootable partition
09	AIX data partition
0B	DOS 32-bit FAT
0C	DOS 32-bit FAT for interrupt 13 support
0F	Extended Partition with Logical Block Address (LBA)
17	Hidden NTFS partition (D9 and earlier)
18	Hidden FAT12 partition
1E	Hidden VFAT partition
3C	Partition Magic recovery partition
66-69	Novel partitions
81	Linux
82	Linux swap partition (can also be associated with Solaris partitions)
83	Linux native file systems (Ext2, Ext3, Ext4, Reiser, Xfs)
86	FAT16 volume/stripe set (Windows NT)
87	High Performance File System (HPFS) fault-tolerant mirrored partition or NTFS volume/stripe set
A5	FreeBSD and BSD/OS
A6	OpenBSD
A9	NetBSD
C7	Typical of a corrupted NTFS volume/stripe set
EB	BeOS

© 2015 Cengage Learning®

19



## Disk Partitions (2 of 3)

- The partition table is in the **Master Boot Record (MBR)**
  - Located at sector 0 of the disk drive
- MBR stores information about partitions on a disk and their locations, size, and other important items
- 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.

20

## Master Boot Record Structure

**Structure of a Master Boot Record**

Address			Description	Size in bytes
Hex	Oct	Dec		
0000	0000	0	code area	440 (max. 446)
01B8	0670	440	disk signature (optional)	4
01BC	0674	444	Usually nulls; 0x0000	2
01BE	0676	446	<b>Table of primary partitions</b> (Four 16-byte entries, IBM partition table scheme)	64
01FE	0776	510	55h	MBR signature; 0xAA55 <sup>[1]</sup>
01FF	0777	511	AAh	
<b>MBR, total size: 446 + 64 + 2 =</b>				<b>512</b>

Source: Wikipedia

**Layout of one 16-byte partition record**

Offset	Field length (bytes)	Description
0x00	1	status <sup>[7]</sup> (0x80 = bootable (active), 0x00 = non-bootable, other = invalid <sup>[8]</sup> )
0x01	3	CHS address of first absolute sector in partition. <sup>[9]</sup> The format is described in the next 3 bytes.
0x01	1	head <sup>[10]</sup>
0x02	1	sector is in bits 5–0; <sup>[11]</sup> bits 9–8 of cylinder are in bits 7–6
0x03	1	bits 7–0 of cylinder <sup>[12]</sup>
0x04	1	partition type <sup>[13][14]</sup>
0x05	3	CHS address of last absolute sector in partition. <sup>[15]</sup> The format is described in the next 3 bytes.
0x05	1	head
0x06	1	sector is in bits 5–0; bits 9–8 of cylinder are in bits 7–6
0x07	1	bits 7–0 of cylinder
0x08	4	LBA of first absolute sector in the partition <sup>[16]</sup>
0x0C	4	number of sectors in partition, in little-endian format <sup>[16]</sup>



© 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.

21

## Disk Partitions (3 of 3)

**Figure 5-4 The partition table in a hexadecimal editor**

Source: X-Ways AG, [www.x-ways.net](http://www.x-ways.net)

The screenshot shows a hex editor window displaying the MBR and its four partition entries. The MBR starts at offset 0x00000000 and ends at 0x0000001F. The four partitions begin at offset 0x00000020. Partition 1 (NTFS) starts at 0x00000020 and ends at 0x0000003F. Partition 2 (FAT32) starts at 0x00000040 and ends at 0x0000005F. Partition 3 (FAT16) starts at 0x00000060 and ends at 0x0000007F. Partition 4 (Unallocated space) starts at 0x00000080 and ends at 0x0000009F. The table below summarizes the key fields for each partition:

Partition	Start Address	End Address	File System	Partition Type	First Sector Offset	Last Sector Offset	Number of Sectors
1	0x00000020	0x0000003F	NTFS	0x00000000	0x00000000	0x00000000	0x00000000
2	0x00000040	0x0000005F	FAT32	0x00000001	0x00000000	0x00000000	0x00000000
3	0x00000060	0x0000007F	FAT16	0x00000002	0x00000000	0x00000000	0x00000000
4	0x00000080	0x0000009F	Unallocated	0x00000003	0x00000000	0x00000000	0x00000000



© 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.

22



## Partition Table Example (1 of 4)

00 01 01 00 DE FE 3F 04 3F 00 00 00 86 39 01 00

Byte 0: 00 = inactive (not bootable)

- Only one partition on a Windows system should be bootable

Bytes 1 – 3: Split up as

| h7 – h0 | c9 c8 s5 – s0 | c7 – c0 |

In binary, we have

0000 0001 0000 0001 0000 0000  
h7h6h5h4 h3h2h1h0 c9c8s5s4 s3s2s1s0 c7c6c5c4 c3c2c1c0

So: H = 1, C = 0, S = 0x1 = 1



© 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.

23



## Partition Table Example (2 of 4)

00 01 01 00 DE FE 3F 04 3F 00 00 00 86 39 01 00

Byte 4: Partition Type 0xDE

- Look this one up in a table. It is a Dell PowerEdge Server Utility (FAT fs)

1	FAT12	24	NEC DOS	81	Minix / old Lin	c1	DRDOS/sec (FAT-
2	XENIX root	39	Plan 9	82	Linux swap / So ci	c2	DRDOS/sec (FAT-
3	XENIX usr	3c	DOS partition	93	Linux	c6	DRDOS/sec (FAT-
4	FAT16 <32M	40	Venix 80286	84	OS/2 hidden C:	c7	Syrius
5	Extended	41	PPC PreP Boot	95	Linux extended da	da	Non-ES data
6	FAT16	42	SFS	86	NTFS volume set da	da	CPR / CCR / .
7	HFS/NTFS	4d	QNQ4.x	87	NTFS volume set da	da	Dell Utility
8	AIX	4e	QNQ4.x 2nd part	88	Linux plain text f	f	BootIt
9	AIX bootable	4f	QNQ4.x 3rd part	8e	Linux LVM	e1	DOS access
a	OS/2 Boot Manag	50	Ontrack DM	93	Amoeba	e3	DOS R/O
b	W95 FAT32	51	Ontrack DM6 Aux	94	Amoeba BBT	e4	SpeedStor
c	W95 FAT32 (LBA)	52	Ontrack DM6 Aux	95	Amoeba OS	eb	DOS fs
d	W95 FAT16 (LBA)	53	Ontrack DM6 Aux	96	IBM Thinkpad hi	ee	GPT
e	W95 Etenda (LBA)	54	Ontrack DM6 Aux	97	FreeBSD	f0	EFI (FAT-12/16/
10	OPUS	55	EZ-Drive	a6	OpenBSD	f0	Linux/PA-RISC b
11	Hidden FAT12	56	Golden Bow	a7	NeXTSTEP	f1	SpeedStor
12	Compaq diagnost	5c	Priam Edisk	a8	UFS Darwin	f4	SpeedStor
14	Hidden FAT16 <3	61	SpeedStor	a9	NetBSD	f2	DOS secondary
16	Hidden FAT16	63	GNU HURD or Sys	ab	Amorce Darwin	fb	VMware VMFS
17	Hidden HPFS/NTF	64	Novell Netware	b7	BSDI fs	fc	VMware VMKCORE
18	AST SmartSleep	65	Novell Netware	b8	BSDI swap	fd	Linux raid auto
1b	Hidden W95 FAT3	70	DiskSecure Mult	bb	Boot Wizard hid	fe	LANstep
1c	Hidden W95 FAT3	75	PC/IX	be	Amorce Solaris	ff	BBT



© 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.

24



## Partition Table Example (3 of 4)

00 01 01 00 DE **FE 3F 04 3F 00 00 00** 86 39 01 00

Bytes 5 – 7: End of Partition

Split up as | h7 – h0 | c9 c8 s5 – s0 | c7 – c0 |

1111 1110 0011 1111 0000 0100

So: H = 0xFE, C = 0x04, S = 0x3F

Bytes 8 – 12: LBA 3F 00 00 00 in Little Endian

That is 00 00 00 3F is the real start LBA

- Go to Sector 63 and find the FAT boot sector



## Partition Table Example (4 of 4)

00 01 01 00 DE FE 3F 04 3F 00 00 00 **86 39 01 00**

Bytes 13 – 16: Number of Sectors in the partition (in Little Endian)

Value is 0x 86 39 01 00

Translate into true value:

0x 00 01 39 86 = 80,262 sectors

- We have a Dell partition of size 40MB
  - Invisible to Windows and could be used to hide data
  - Dell uses area to help with recovery from OS disasters



## 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



## 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



## 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



## Examining FAT Disks (4 of 7)

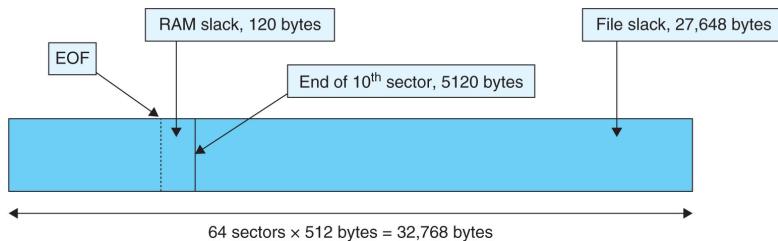


Figure 5-8 File slack space

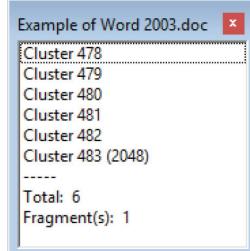


## Examining FAT Disks (5 of 7)

- 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



## Examining FAT Disks (6 of 7)



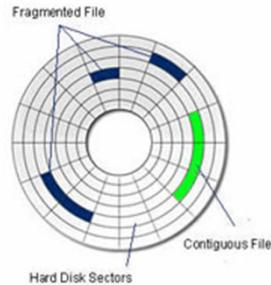
**Figure 5-9** Chained sectors associated with clusters as a result of increasing file size

Source: X-Ways AG, [www.x-ways.net](http://www.x-ways.net)



## 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



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.

33



## 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.

34



## 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



## 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



## 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



## 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**



## 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.



© 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.

39



## 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.



© 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.

40



## 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



## 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



## 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.



© 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.

43



## 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.



© 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.

44



## MFT and File Attributes (5 of 7)

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	/	ANSI ASCII
035B3400	46	49	4C	45	30	00	03	00	5F	A7	B2	00	00	00	00	00	FILE0	éï'
035B3410	03	00	01	00	38	00	00	00	80	01	00	00	04	00	00	00		
035B3420	00	00	00	00	00	00	00	00	05	00	00	00	A5	17	00	00		
035B3430	09	00	00	00	00	00	00	00	10	00	00	00	60	00	00	00		
035B3440	00	00	00	00	00	00	00	00	48	00	00	00	18	00	00	00	H	
035B3450	62	14	98	48	0A	7C	01	BC	78	9D	68	0A	7C	C9	01	b	ñh iÉ wñ h iÉ	
035B3460	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	þa)ix-E 1bdeæ@E	
035B3470	20	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
035B3480	00	00	00	00	01	00	00	00	00	00	00	00	00	00	00	00		
035B3490	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	o P	
035B34A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
035B34B0	00	00	00	00	00	00	00	04	00	00	00	00	00	00	00	00		
035B34C0	BC	78	9D	68	0A	7C	01	BC	78	9D	68	0A	7C	C9	01	b	ñh iÉ wñ h iÉ	
035B34D0	BC	78	9D	68	0A	7C	01	00	00	00	00	00	00	00	00	00	wñ h iÉ	
035B34E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
035B34F0	00	03	42	00	00	00	00	00	31	00	2E	00	74	00	78	00	B en 1. t x	
035B3500	74	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	t 8	
035B3510	00	00	00	00	00	00	00	03	00	00	00	00	00	00	00	00	(	
035B3520	00	00	00	00	00	00	00	00	10	00	00	00	1A	00	00	00	00	
035B3530	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	ñññgÝ ? n ð	
035B3540	00	00	00	00	00	00	00	00	18	00	00	00	00	00	00	00	€ P	
035B3550	79	00	00	00	00	00	00	00	41	2A	63	6F	78	8E	74	72	T A country	
035B3560	20	61	20	66	69	73	45	20	62	65	65	65	65	65	65	65	layers is like	
035B3570	74	77	69	20	63	76	73	2E	0D	0A	42	65	65	6A	61	00	two cats. Benja	
035B3580	60	69	20	64	62	64	6E	6B	6C	69	00	00	00	00	00	00	min Franklin	
035B3590	FF	ÿÿÿÿ, yg																

A: All MFT records start with FILE0  
 B: Start of attribute 0x10  
 C: Length of attribute 0x10 (value 60)  
 D: Start of attribute 0x40  
 E: Length of attribute 0x40 (value 70)  
 F: Start of attribute 0x40  
 G: Length of attribute 0x40 (value 28)  
 H: End-of-record marker (FF FF FF FF)  
 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

45



© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except 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	éï'
035B3C10	03	00	01	00	38	00	00	00	80	01	00	00	04	00	00	00		
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	08	0B	7C	01	6A	22	16	88	0B	7C	C9	01	À ~  É j" ~  É	
035B3C60	A8	D4	5D	7D	8B	7E	C9	01	6A	22	16	88	0B	7C	C9	01	~Ó)ix-E j" ~  É	
035B3C70	20	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
035B3C80	00	00	00	00	00	00	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	00	
035B3CA0	00	00	00	00	00	00	00	02	52	00	00	00	18	00	01	00	00	
035B3CB0	8A	00	00	00	00	00	00	01	10	C0	13	88	08	0B	7C	01	ñ	
035B3CC0	6A	22	16	88	0B	7C	01	01	6A	22	16	88	0B	7C	C9	01	À ~  É	
035B3CD0	6A	22	16	88	0B	7C	01	00	00	00	00	00	00	00	00	00	j" ~  É j" ~  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 en 2. r t	
035B3D00	66	00	00	00	00	00	00	00	40	00	00	00	28	00	00	00	f @ (	
035B3D10	UU	10	UU															
035B3D20	F7	7C	F1	27	DF	E7	DD	11	A8	3F	00	22	15	D5	88	06	+ñññgÝ ? n ð	
035B3D30	80	00	00	00	00	00	00	00	01	00	00	00	00	03	00	00	€ H	
035B3D40	00	00	00	00	00	00	00	00	02	00	00	00	00	00	00	00	x x	
035B3D50	40	00	00	00	00	00	00	00	00	06	00	00	00	00	00	00	x x	
035B3D60	78	05	00	00	00	00	00	00	78	05	00	00	00	00	00	00	ÿÿÿÿ, yg	
035B3D70	31	03	15	55	01	01	01	00	FF	FF	FF	FF	82	79	47	11	1 U yyy, 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

46



© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except 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.

47



## 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.

48



## MFT Structures for File Data (2 of 7)

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	/	ANSI ASCII
000002000	46	49	4C	45	3	00	03	00	11	8F	42	0C	00	00	00	00	[FILEO]	B
000002010	01	00	01	00	[38	00	01	00	D0	01	00	00	00	04	00	00		8
000002020	00	00	00	00	00	00	00	00	06	00	00	00	00	00	00	00		D
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](http://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.

49



## MFT Structures for File Data (3 of 7)

	Create date and time	Attribute 0x10	Last modified date and time	Size of attribute 0x10
035B3430	11 00 00 00 00 00 00 00	[10	00 00 00 60 00 00 00	00
035B3440	00 00 00 00 00 00 00 00	48	00 00 00 18 00 00 00	00
035B3450	62 16 9B 68 0A 7C C9 01	BC 78 9D 68 0A 7C C9 01	b >h É w x h  É	
035B3460	92 FE 26 7D 8B 7E C9 01	54 F2 62 E9 F8 D0 C9 01	'pæ}~É TòbéøðÉ	
035B3470	20 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
035B3480	00 00 00 00 09 01 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	

Last access date and time

Record update date and time

Figure 5-14 Attribute 0x10: Standard Information

Source: X-Ways AG, [www.x-ways.net](http://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.

50



## MFT Structures for File Data (4 of 7)

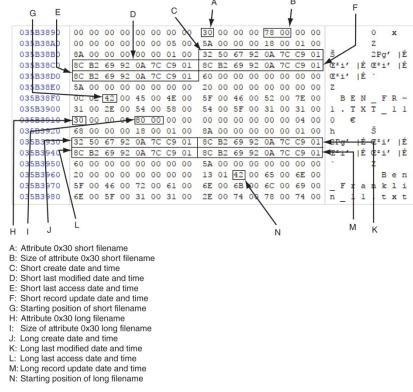


Figure 5-15 Attribute 0x30: short and long filenames

Source: X-Ways AG, [www.x-ways.net](http://www.x-ways.net)

51



© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except 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)

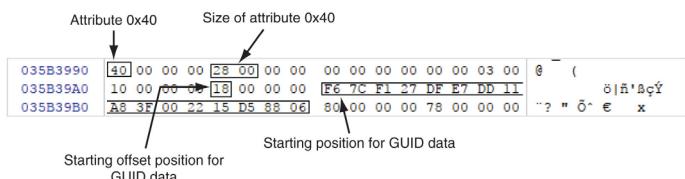


Figure 5-16 Attribute 0x40: Object\_ID

Source: X-Ways AG, [www.x-ways.net](http://www.x-ways.net)

52



© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except 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](http://www.x-ways.net)

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except 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](http://www.x-ways.net)

© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except 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



## NTFS Alternate Data Streams (2 of 2)

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
024C0E00	40	00	00	45	30	00	00	00	5C	AC	B5	00	00	00	00	
024C0E10	04	00	01	00	00	00	00	00	00	00	00	00	00	00	00	
024C0E20	00	00	00	00	00	00	00	00	07	00	00	00	01	00	00	
024C0E30	09	00	00	00	00	00	00	00	10	00	00	00	00	00	00	
024C0E40	00	00	00	00	00	00	00	00	48	00	00	00	10	00	00	
024C0E50	E1	4C	07	BB	D3	7C	C9	01	14	4A	A3	3D	C8	7D	C9	01
024C0E60	10	00	00	00	00	00	00	00	01	00	00	00	00	00	00	
024C0E70	20	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
024C0E80	00	00	00	00	00	01	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	
024C0EA0	00	00	00	00	00	00	02	00	54	00	00	00	10	00	01	
024C0EB0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
024C0EC0	B2	4C	07	BB	D3	7C	C9	01	B2	4C	07	BB	D3	7C	C9	01
024C0ED0	B2	4C	07	BB	D3	7C	C9	01	00	00	00	00	00	00	00	
024C0EE0	00	00	00	00	00	00	00	00	20	00	00	00	00	00	00	
024C0EF0	00	03	42	00	46	00	31	00	5F	00	34	00	3E	00	74	00
024C0F00	00	00	00	00	00	00	00	00	80	00	00	00	50	00	00	
024C0F10	00	00	00	00	00	00	00	00	38	00	00	00	18	00	00	
024C0F20	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
024C0F30	74	65	72	20	74	69	61	6E	20	77	65	6C	20	73	61	
024C0F40	69	64	2E	0D	0A	20	20	41	65	6E	6A	61	ED	69	6E	20
024C0F50	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
024C0F60	01	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
024C0F70	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
024C0F80	00	02	00	00	00	00	00	00	00	3B	00	00	00	00	00	
024C0F90	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
024C0FA0	3B	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
024C0FB0	3B	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
024C0FC0	3B	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
024C0FD0	3B	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
024C0FE0	3B	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
024C0FF0	3B	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
024C0F00	3B	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
024C0F10	3B	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
024C0F20	3B	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
024C0F30	3B	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
024C0F40	3B	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
024C0F50	3B	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
024C0F60	3B	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
024C0F70	3B	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
024C0F80	3B	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
024C0F90	3B	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
024C0FA0	3B	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
024C0FB0	3B	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
024C0FC0	3B	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
024C0FD0	3B	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
024C0FE0	3B	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
024C0FF0	3B	00	00	00	00	00	00	00	00	00	00	00	00	00	00	

Figure 5-24 A text alternate data stream

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



## 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.

57



## 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.

58



## 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



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.

59



## 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.

60



## 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.

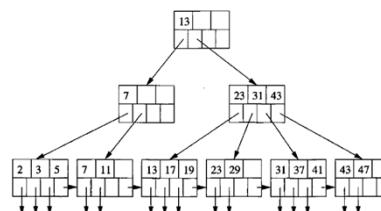
61



## Resilient File System

- ReFS uses the B+ file system structure
  - Only the leaf nodes contain records
  - Non-leaf nodes contain keys and block numbers (i.e., indices to nodes)
  - Leaf node may include pointer to next leaf node to speed sequential access
- When corruption detected, file system made consistent while remaining online
- Data storage integrity maintained through data verification and auto correction of file system
  - Instead of using [chkdsk](#)

### EXAMPLE: B+-TREE



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.

62



## 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.

63



## 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



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.

64



## 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**



## 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

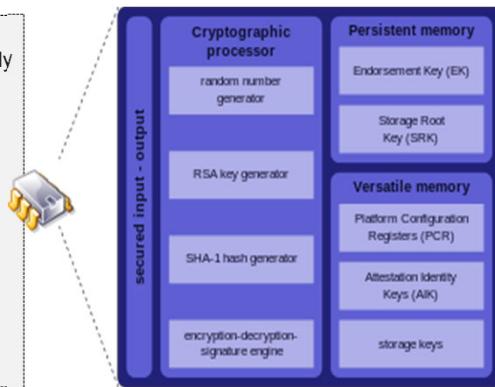




## TPM Components

- TPM (Trusted Platform Module) is an international standard for a secure crypto-processor

- 2048-bit RSA public/private **endorsement key** pair created randomly at manufacture time (non-migratable)
- **Secure I/O** path from keyboard to an application and back to terminal
- Memory curtaining to provide full isolation of sensitive areas of memory
- **Sealed storage** to protect private information so data released only to particular combination of software and hardware
- **Remote attestation** allows changes to user's computer to be detected by authorized parties



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.

67



## Examining Third-Party Disk Encryption Tools

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

68



## 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

Before modify Registry, ALWAYS backup first!



© 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.

69



## Exploring the Organization of the Windows Registry (1 of 6)

- Registry terminology:

- Registry – hierarchical dbase with system/user info
- Registry Editor – utility view/modify registry data
- HKEY – 5 or 6 categories registry divided into
- Key – folder that contains other key folders or values
- Subkey – subfolder for key displayed under another key
- Branch – key/contents, including subkeys
- Value – name/value in key
- Default value – all keys have default value (data optional)
- Hives – branches in HKEY\_USER and HKEY\_LOCAL\_MACHINE



© 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.

70



## Exploring the Organization of the Windows Registry (2 of 6)

- Registry data types:
  - REG\_DWORD (numbers)
    - Hexadecimal (decimal)
    - True = 1, False = 0
  - REG\_SZ (string)
    - Stores strings (e.g., paths to files, etc.)
    - Can be encrypted



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.

71



## Exploring the Organization of the Windows Registry (3 of 6)

**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

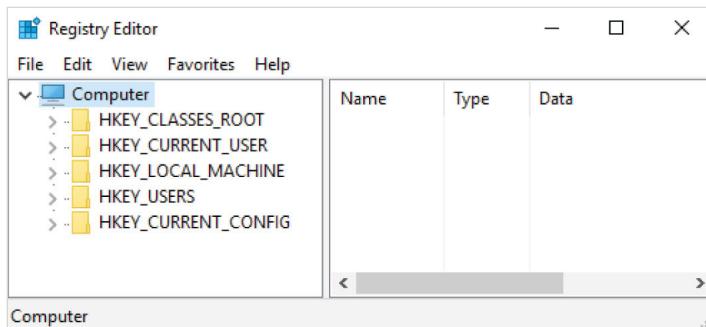


CENGAGE

© 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.

72

## Exploring the Organization of the Windows Registry (4 of 6)



**Figure 5-26** Viewing HKEYs in Registry Editor

## Exploring the Organization of the Windows Registry (5 of 6)

**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)



## Exploring the Organization of the Windows Registry (6 of 6)

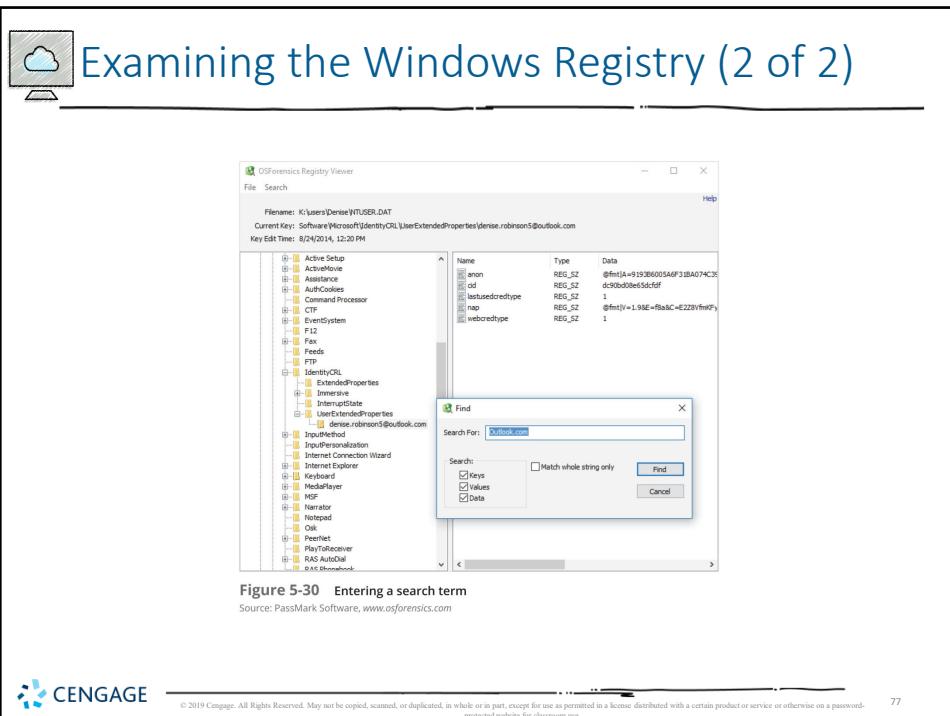
**Table 5-7** Registry HKEYs and their functions (*continued*)

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



## Examining the Windows Registry (1 of 2)

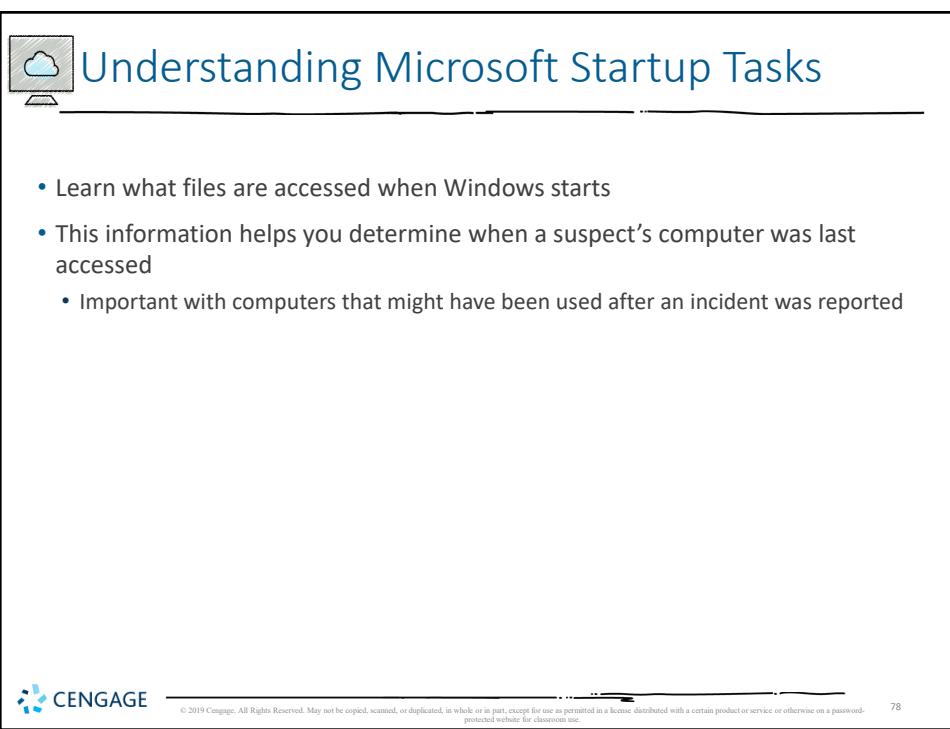
- Tools with built-in or add-on Registry viewers:
  - X-Ways Forensics
  - OSForensics
  - Forensic Explorer
  - FTK



**Figure 5-30** Entering a search term

Source: PassMark Software, [www.osforensics.com](http://www.osforensics.com)

77





## 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.

79



## 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.

80



## 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.

81



## 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.

82



## 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



© 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.

83



## 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



© 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.

84



## 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



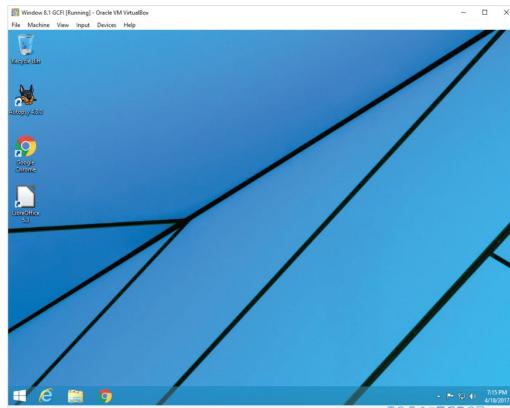
CENGAGE

© 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.

85



## 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](http://www.virtualbox.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.

86



## 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.

87



## 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.

88



## 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.

89



## 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.

90



## 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.

91

# Guide to Computer Forensics and Investigations

## Sixth Edition

### *Chapter 6*

#### *Current Digital Forensics Tools*





# 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



# 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?



# 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



# 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



# 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



# 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



# Tasks Performed by Digital Forensics Tools (4 of 20)

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

Source: X-Ways AG, [www.x-ways.net](http://www.x-ways.net)



# 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



# 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



# 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



# Tasks Performed by Digital Forensics Tools (8 of 20)

The screenshot shows the homepage of the National Software Reference Library (NSRL). At the top, there is a banner with the text "Information Technology Laboratory" and "National Software Reference Library". To the right of the banner is the NIST logo. On the left side of the main content area, there is a sidebar with the NSRL logo and two sections: "GENERAL INFORMATION" and "VOTING", each containing a list of links. The main content area has a large title "Welcome to the National Software Reference Library (NSRL) Project Web Site." Below the title, there is a paragraph about the project's purpose and support. Further down, there are two more paragraphs: one about the Reference Data Set (RDS) and another about the RDS collection.

**Welcome to the National Software Reference Library (NSRL) Project Web Site.**

This project is supported by the U.S. Department of Homeland Security, federal, state, and local law enforcement, and the National Institute of Standards and Technology (NIST) to promote efficient and effective use of computer technology in the investigation of crimes involving computers. Numerous other sponsoring organizations from law enforcement, government, and industry are providing resources to accomplish these goals, in particular the FBI who provided the major impetus for creating the NSRL out of their ACES program.

The National Software Reference Library (NSRL) is designed to collect software from various sources and incorporate file profiles computed from this software into a Reference Data Set (RDS) of information. The RDS can be used by law enforcement, government, and industry organizations to review files on a computer by matching file profiles in the RDS. This will help alleviate much of the effort involved in determining which files are important as evidence on computers or file systems that have been seized as part of criminal investigations.

The RDS is a collection of digital signatures of **known, traceable software applications**. There are application hash values in the hash set which may be considered malicious, i.e. steganography tools and hacking scripts. **There are no hash values of illicit data, i.e. child abuse images.**

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

Source: [www.nsrl.nist.gov](http://www.nsrl.nist.gov)



# Tasks Performed by Digital Forensics Tools

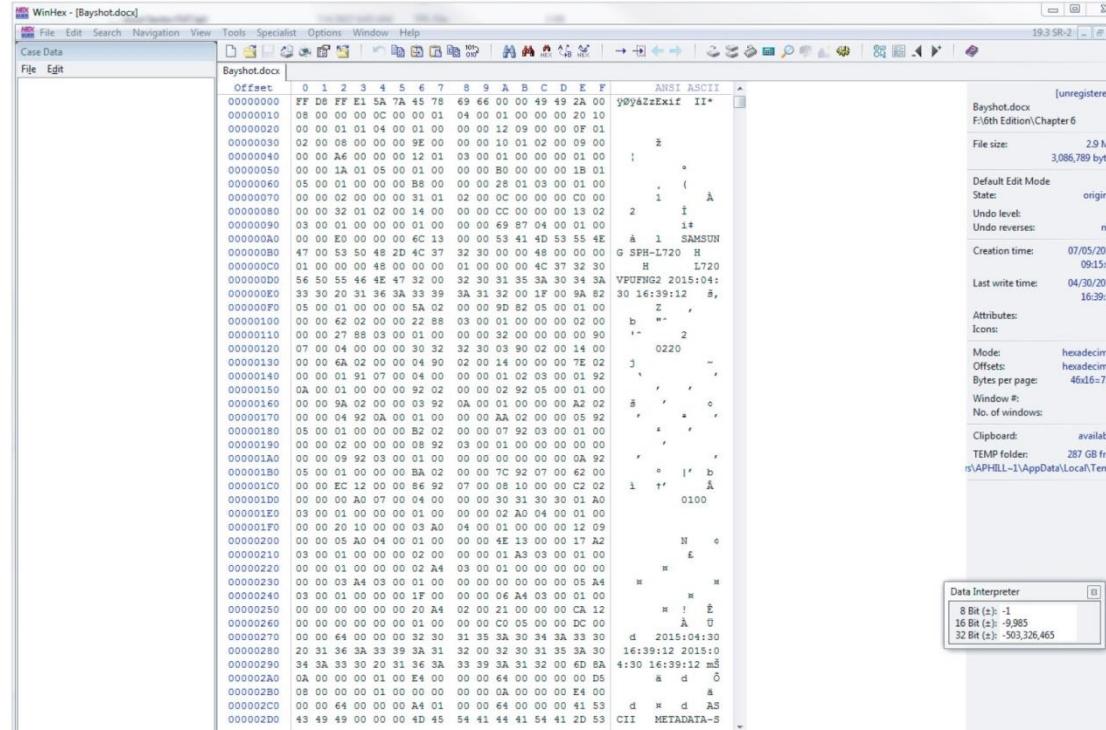
## (9 of 20)

---

- 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



# Tasks Performed by Digital Forensics Tools (10 of 20)

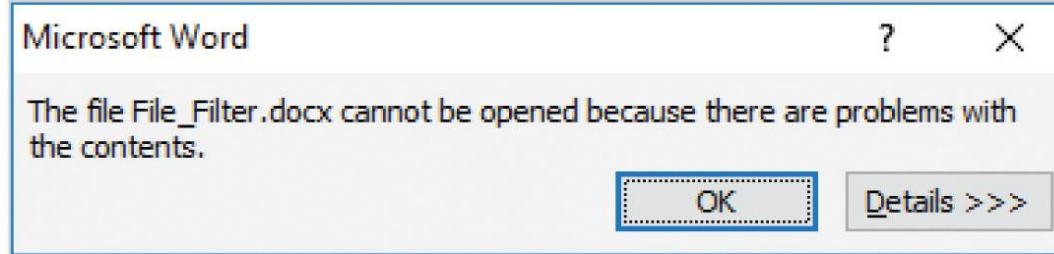


**Figure 6-3** The file header indicates a .jpeg file

Source: X-Ways AG, [www.x-ways.net](http://www.x-ways.net)



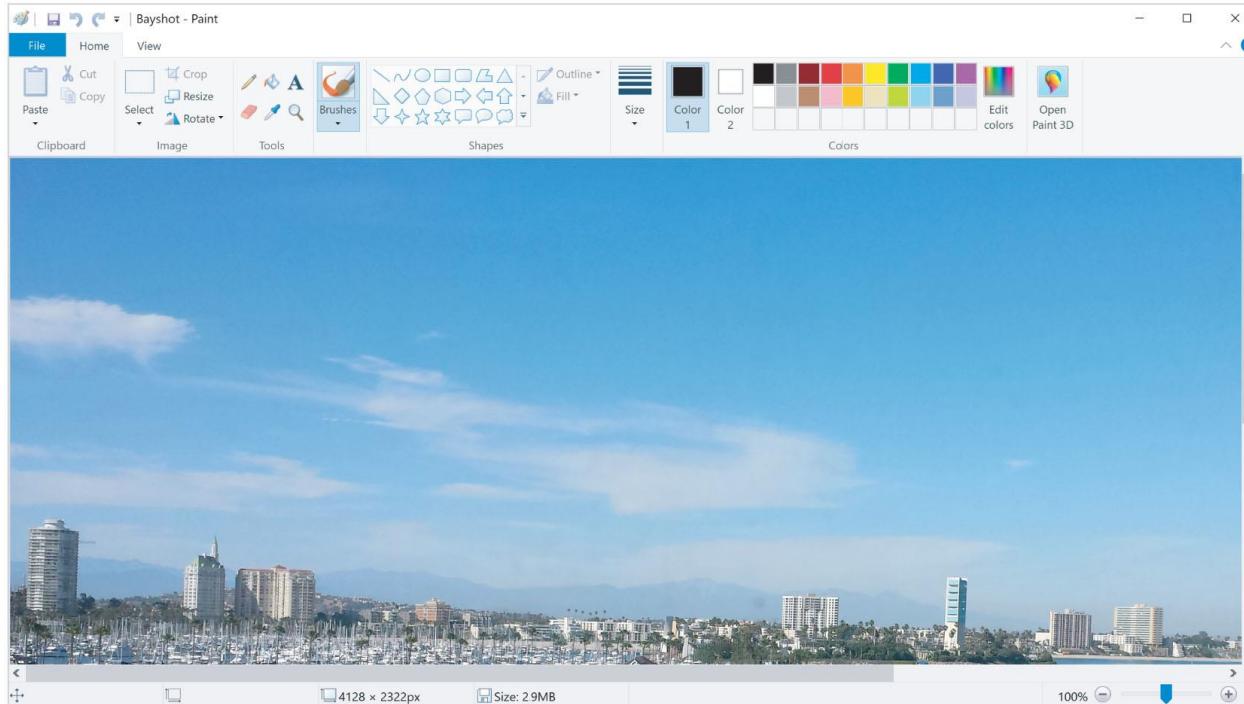
# Tasks Performed by Digital Forensics Tools (11 of 20)



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



# Tasks Performed by Digital Forensics Tools (12 of 20)



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



# 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



# 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



# Tasks Performed by Digital Forensics Tools (15 of 20)

The screenshot shows the OSForensics software interface with the title bar "OSForensics - InChap06". On the left is a vertical toolbar with icons for various tools: Start, Manage Case, File Name Search, Create Index, Search Index (which is selected), Recent Activity, Deleted Files Search, Mismatch File Search, Memory Viewer, Raw Disk Viewer, Registry Viewer, File System Browser, SQLite DB Browser, Web Browser, Passwords, System Information, Verify / Create Hash, Hash Sets, Create Signature, Compare Signature, Drive Preparation, and Drive Imaging. The main window is titled "Search Index" and contains a search bar with "nucleic acids" and a dropdown menu "Index to Search" set to "My Index - Drive-G". Below these are buttons for "Search", "Advanced...", and "Use Word List File...". A table lists search results for "nucleic acids":

Search Term	Index	Results	Total	Date	Settings
nucleic acids	My Index - Drive-G	61	61	11/15/2017, 3:13 PM	Terms: All
proteases	My Index - Drive-G	38	38	11/15/2017, 3:13 PM	Terms: All
urine	My Index - Drive-G	36	36	11/15/2017, 3:13 PM	Terms: All
haemoglobin	My Index - Drive-G	6	6	11/15/2017, 3:13 PM	Terms: All
efaproximal	My Index - Drive-G	0	0	11/15/2017, 3:13 PM	Terms: All
"red blood cell"	My Index - Drive-G	21	21	11/15/2017, 3:13 PM	Terms: All
doping	My Index - Drive-G	34	34	11/15/2017, 3:13 PM	Terms: All
triamterene	My Index - Drive-G	1	1	11/15/2017, 3:13 PM	Terms: All
hydrochlorothiazide)	My Index - Drive-G	4	4	11/15/2017, 3:13 PM	Terms: All
chlorothiazide	My Index - Drive-G	3	3	11/15/2017, 3:13 PM	Terms: All
bendroflumethiazide	My Index - Drive-G	0	0	11/15/2017, 3:13 PM	Terms: All
thiazides	My Index - Drive-G	3	3	11/15/2017, 3:13 PM	Terms: All
spironolactone	My Index - Drive-G	2	2	11/15/2017, 3:13 PM	Terms: All
metolazone	My Index - Drive-G	1	1	11/15/2017, 3:13 PM	Terms: All
indapamide	My Index - Drive-G	3	3	11/15/2017, 3:13 PM	Terms: All
furosemide	My Index - Drive-G	2	2	11/15/2017, 3:13 PM	Terms: All
etacrynic acid	My Index - Drive-G	0	0	11/15/2017, 3:13 PM	Terms: All
chlorthalidone	My Index - Drive-G	3	3	11/15/2017, 3:13 PM	Terms: All
canrenone	My Index - Drive-G	0	0	11/15/2017, 3:13 PM	Terms: All
bumetanide	My Index - Drive-G	0	0	11/15/2017, 3:13 PM	Terms: All
amiloride	My Index - Drive-G	0	0	11/15/2017, 3:13 PM	Terms: All
acetazolamide	My Index - Drive-G	0	0	11/15/2017, 3:13 PM	Terms: All
probencid	My Index - Drive-G	2	2	11/15/2017, 3:13 PM	Terms: All
mannitol	My Index - Drive-G	18	18	11/15/2017, 3:13 PM	Terms: All
hydroxyethyl starch	My Index - Drive-G	1	1	11/15/2017, 3:13 PM	Terms: All
dextran	My Index - Drive-G	20	20	11/15/2017, 3:13 PM	Terms: All
albumin	My Index - Drive-G	41	41	11/15/2017, 3:13 PM	Terms: All
glycerol	My Index - Drive-G	43	43	11/15/2017, 3:13 PM	Terms: All

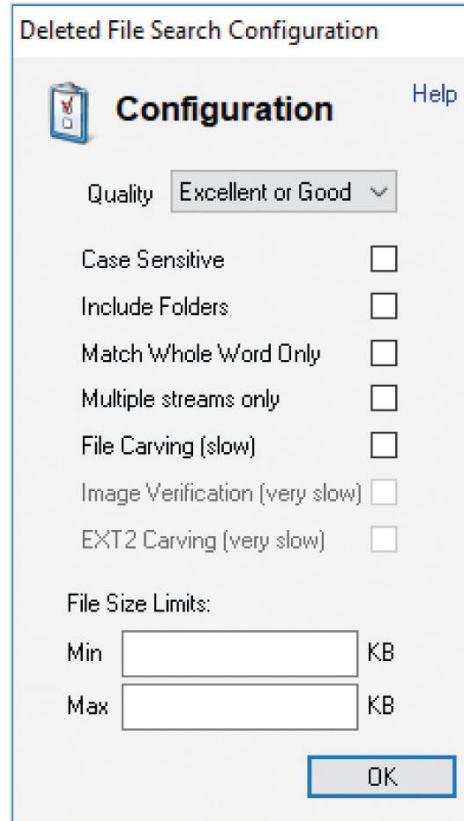
At the bottom of the search window, a status message reads: "Bulk search of My Index - Drive-G in progress, 131/131 completed from wordlist: 'Banned sports drugs.txt'".

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

Source: PassMark Software, [www.osforensics.com](http://www.osforensics.com)



# Tasks Performed by Digital Forensics Tools (16 of 20)



**Figure 6-7** Data-carving options in OS Forensics

Source: PassMark Software,  
[www.osforensics.com](http://www.osforensics.com)



# 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**



# 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



# 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



# 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



# Other Considerations for Tools

---

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



# Digital Forensics Software Tools

---

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



# 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



# 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



# 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



# 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



# 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



# 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



# 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



# 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



# 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



# 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



# 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



# 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



# 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



# 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



# 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



# 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



# 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



# 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



# 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



# 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



# 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



# 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



# 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



# 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



# 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



# 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

# Guide to Computer Forensics and Investigations

## Sixth Edition

### *Chapter 7*

#### *Linux and Macintosh File Systems*

 CENGAGE



1



### Objectives

- Describe Linux file structures
- Describe Macintosh file structures
- Use Linux 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.

2

2



## Examining Linux File Structures (1 of 4)

- 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



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

3

3



## Examining Linux File Structures (2 of 4)

Table 7-1 Linux system files

System file	Contents
/etc/exports	File systems exported to remote hosts; might include remote drive mappings
/etc/fstab	File system table of devices and mount points
/var/log/lastlog	User's last logon
/var/log/wtmp	Logon and logoff history information
/var/run/utmp	Current user's logon information
/var/log/dmesg	System messages log
System file	Contents
/var/log/syslog	System log, occasionally called system.log or kernel.log
/etc/shadow	Master password file, containing hashed passwords for the local system
/etc/group	Group memberships for the local system
/etc/passwd	Account information for the local system

© 2015 Cengage Learning®



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

4

4



## Examining Linux File Structures (3 of 4)

Table 7-2 Core top-level directories of a Linux system

Directory	Contents
/usr	Most applications and commands are in this directory or its subdirectories <code>bin</code> (stands for "binary" and contains binary files required at boot time) and <code>sbin</code> (which requires superuser permission to run the binaries in it).
/etc	Most system configuration files are stored in this directory.
/home	The home directories for all users, usually named after their usernames.
/root	The home directory for the root user (superuser), which is kept separate from other user home directories.
/dev	Device files that act as stand-ins for the devices they represent, as described in Chapter 3; for example, <code>/dev/sda</code> is the first non-IDE disk drive on the system, usually the main hard drive.
/var	Subdirectories such as <code>log</code> (often useful for investigations), <code>mail</code> (storing e-mail accounts), and <code>spool</code> (where print jobs are spooled).

© 2015 Cengage Learning®



© 2015 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

5



## 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
  - You can use the `echo` command to add notes or headings in the logs



© 2015 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

6

6



## 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
    - This was really a journaling version of Ext2
- **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



## File Structures in Ext4 (2 of 3)

- Everything is a file
  - Including disks, monitors, NIC, RAM
  - Files are objects with properties and methods
- UNIX/Linux file system consists of four components
- **Boot block**
  - Block is a disk allocation unit of at least 512 bytes
  - Contains the bootstrap code
  - UNIX/Linux computer has only one boot block, located on the main hard disk



## File Structures in Ext4 (3 of 3)

- **Superblock**

- Specifies disk geometry, available space, and keeps track of all inodes (location of the first inode and free inode list)
- 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
- Analogous to a cluster on a FAT or NTFS volume



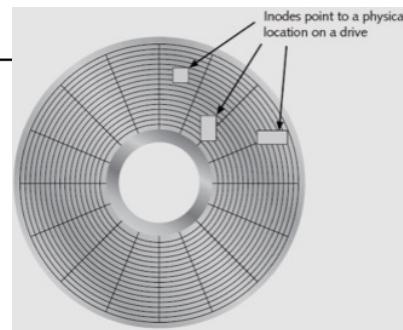
© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

9

9



## 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.

10

10



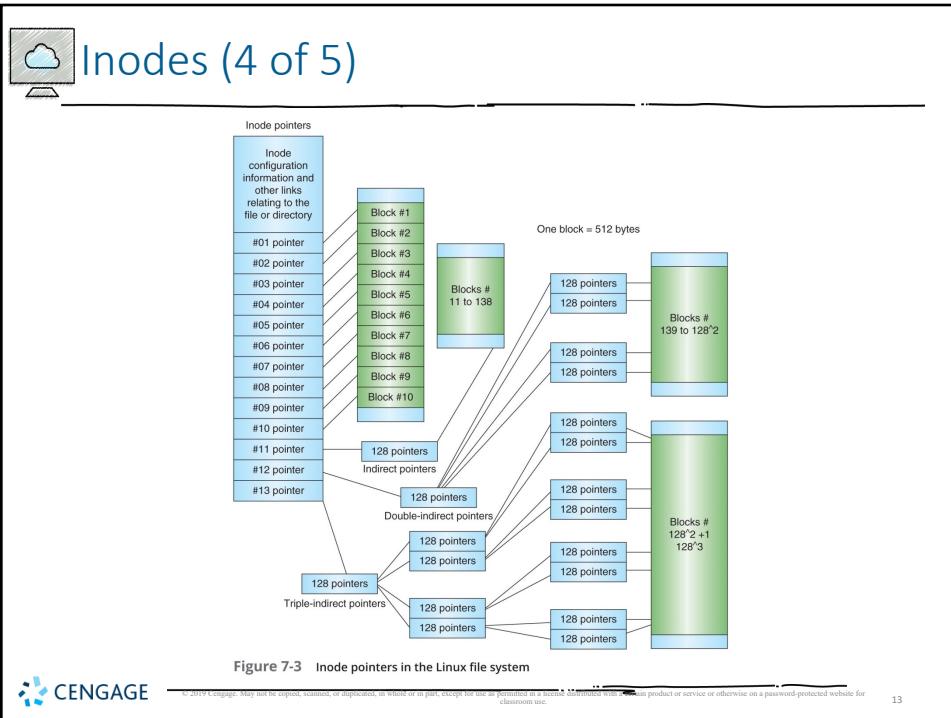
## Inodes (2 of 5)

- 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 or version number
  - Continuation inode's link

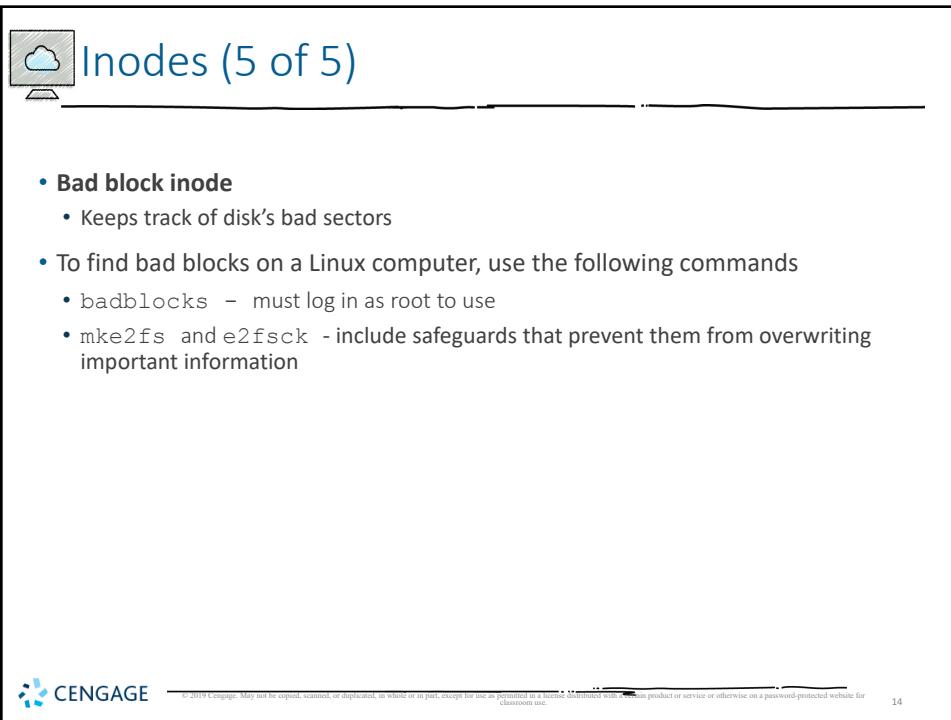


## Inodes (3 of 5)

- 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**
    - Pointers 11-13 are needed for large files



13



14



## 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



## Hard Links and Symbolic Links (2 of 6)

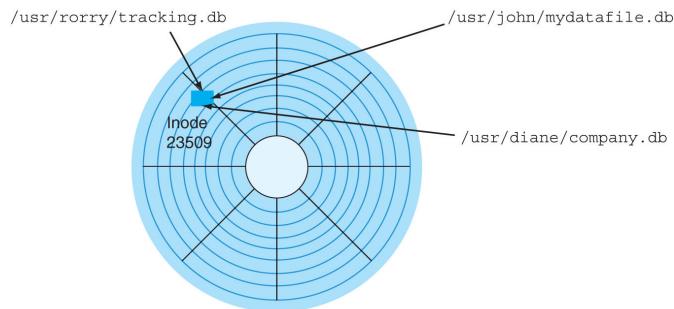


Figure 7-4 Hard-linked files with different filenames



## Hard Links and Symbolic Links (3 of 6)

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

17



## Hard Links and Symbolic Links (4 of 6)

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

Source: [www.ubuntutv.com](http://www.ubuntutv.com)



18



## 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



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

19

19



## Hard Links and Symbolic Links (6 of 6)

The screenshot shows a terminal window titled "Ubuntu 16.04 [Running] - Oracle VM VirtualBox". The terminal session is as follows:

```
student@Ubuntu16:~/tmp$ cd /tmp
student@Ubuntu16:~/tmp$ mkdir testsyn
student@Ubuntu16:~/tmp$ cd testsyn
student@Ubuntu16:~/tmp/testsyn$ touch test1 test2
student@Ubuntu16:~/tmp/testsyn$ cd ..
student@Ubuntu16:~/tmp$ ln -s /tmp/testsyn/mysyn
student@Ubuntu16:~/tmp$ ls -l mysyn
test1
test2
student@Ubuntu16:~/tmp$ ls -l mysyn
lrwxrwxrwx 1 student student 12 Jun 25 22:20 mysyn -> /tmp/testsyn
```

A callout bubble points to the line "lrwxrwxrwx 1 student student 12 Jun 25 22:20 mysyn -> /tmp/testsyn" with the text "Symbolic link".

Figure 7-8 Creating a symbolic link

Source: [www.ubuntu.com](http://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.

20

20



## 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
- MAC OS X is built on a core called Darwin
  - Consists of a Berkeley Software Distribution (BSD) UNIX application layer
- With OS X, Macintosh moved to the Intel processor and became UNIX based

### Even later versions

- Mojave, version 10.14
- Catalina, version 10.15
- Big Sur, version 11
- Monterey, version 12



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

21



## 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



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

22



## 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

For example, a word processing file might store its text in the data fork, while storing any embedded images in the same file's resource fork

Source: Wikipedia (Resource Fork)



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

23



## An Overview of Mac File Structures (2 of 7)

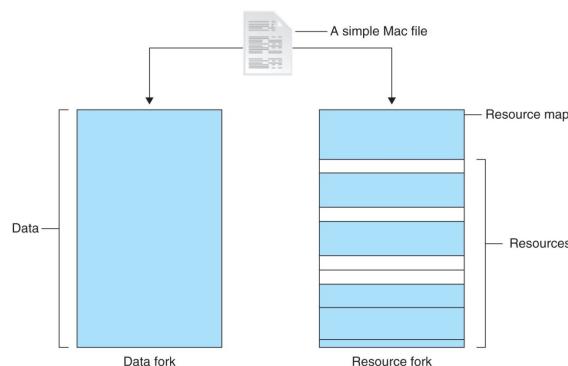


Figure 7-9 The resource fork and data fork in a macOS file



© 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.

24

24



## 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



## An Overview of Mac File Structures (4 of 7)

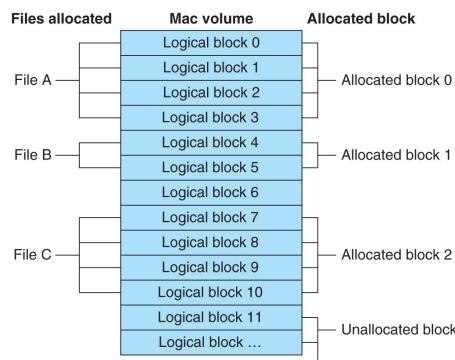


Figure 7-10 Logical and allocation block structures



## An Overview of Mac File Structures (5 of 7)

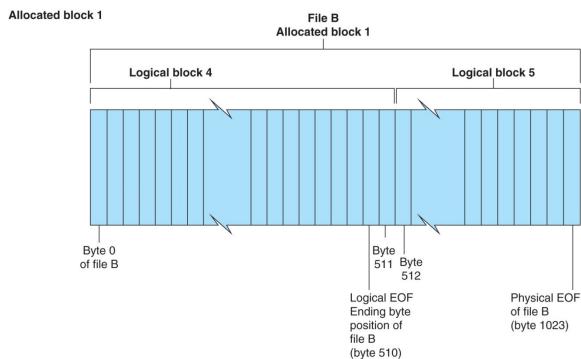


Figure 7-11 Logical EOF and physical EOF



© 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.

27

27



## 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
  - Used by Mac File Manager when list of contiguous blocks of a file becomes too long

extents



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

28

28



## 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**
  - The header node stores information about the B\*-tree file
  - The index node stores link information to previous and next nodes
  - The map node stores a node descriptor and map record

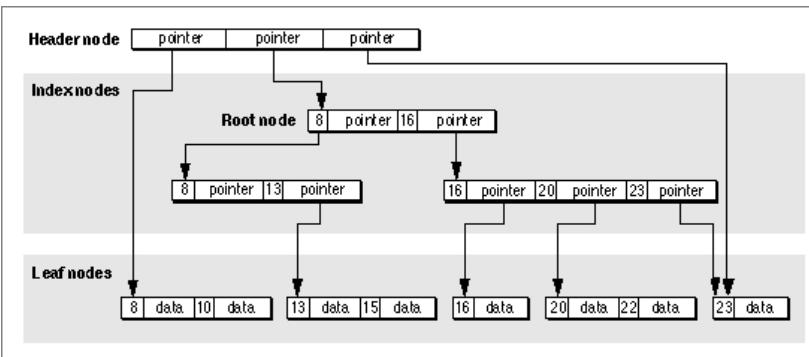


© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

29



## B\*-Trees



- Directory contents are derived from searching the catalog B\*-tree



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

30

30



## HFS System Files

HFS block position	HFS structure	Purpose of structure
0	Boot block	Startup volume containing boot instructions. Also stores system files and Finder information.
1		
2	Master Directory Block (MDB)	Contains volume creation date and time and location of other system files, such as Volume Bitmap. A duplicate of this file called the Alternate MDB is located at the second-to-last block on the volume. Its purpose is to provide information to the OS disk utilities.
3	Volume Bitmap	Tracks used and unused blocks on the volume.
	Catalog	Lists all files and directories on the volume. It's a B*-tree file that uses the extents overflow file to coordinate all file allocations to the volume.
	Extents overflow file	Lists the extra extents, which are the allocated blocks used to store data files. It's a B*-tree file.

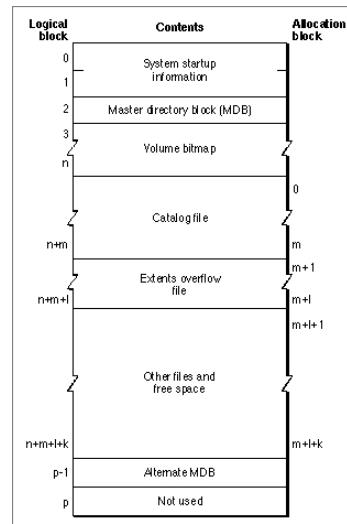


© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

31



## An Overview of Mac File 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.

32



## HFS+ System Files

HFS+ byte offset (fixed starting position)	HFS+ structure	Purpose of structure
0	Boot blocks	No change from HFS.
1024	Volume Information Block (VIB)	Replaces the MDB used in HFS.
Not fixed	Allocation file	Tracks available free blocks on the volume; replaces the HFS Volume Bitmap.
Not fixed	Extents overflow file	For files with more than eight extents, additional extents are recorded and managed through this B*-tree system file.
Not fixed	Catalog	Similar to an HFS catalog, this improved version allows up to eight extents for each file's forks. It's a B*-tree file.
Not fixed	Attributes file	Stores new file attribute information that isn't available in HFS. The new attributes are inline data attribute records, fork data attribute records, and extension attribute records.
Not fixed	Startup file	New to HFS+, this file can boot non-HFS and HFS+ volumes.
Not fixed	Alternate VIB	Same file as the HFS Alternate MDB.
	Reserved (512 bytes)	Last sector of the volume; used by Apple during manufacturing.



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

33

33



## 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



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

34

34



## 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



## 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 Trash folder
  - If a file is deleted at the command line, however, it doesn't show up in the trash





## 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



## 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



## 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** – which mounts drives
  - 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



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

39

39



## Using Linux Forensics Tools

- Most commercial computer forensics tools can analyze Linux Ext2, Ext3, Ext4, ReiserFS, and Reiser4 file systems
  - ReiserFS is a general-purpose, journaled computer file system
- 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



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

40

40



## Installing Sleuth Kit and Autopsy (1 of 3)

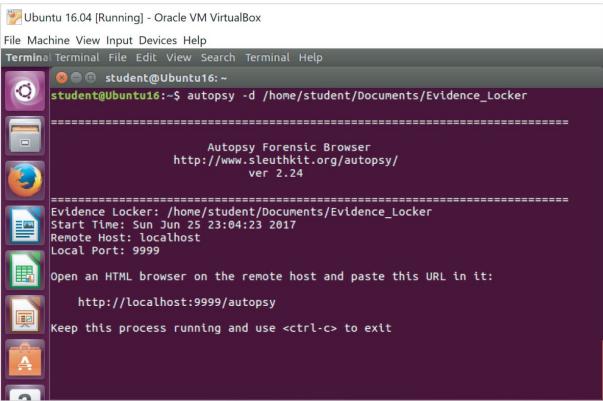
- Download the most current source code from [www.sleuthkit.org](http://www.sleuthkit.org)
- To run Sleuth Kit and Autopsy Browser, you need to have root privileges

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

41



## Installing Sleuth Kit and Autopsy (2 of 3)



The screenshot shows a terminal window titled "Ubuntu 16.04 [Running] - Oracle VM VirtualBox". The window contains the following text:

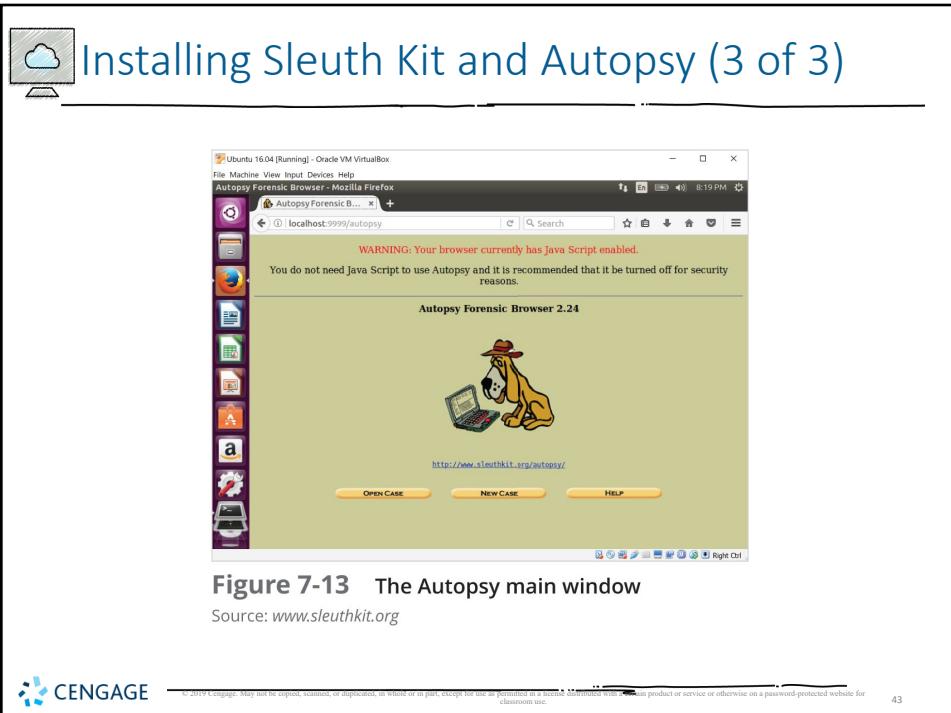
```
student@Ubuntu16:~$ autopsy -d /home/student/Documents/Evidence_Locker
=====
Autopsy Forensic Browser
http://www.sleuthkit.org/autopsy/
ver 2.24
=====
Evidence Locker: /home/student/Documents/Evidence_Locker
Start Time: Sun Jun 25 23:04:23 2017
Remote Host: localhost
Local Port: 9999
Open an HTML browser on the remote host and paste this URL in it:
    http://localhost:9999/autopsy
Keep this process running and use <ctrl-c> to exit
```

**Figure 7-12 Starting Autopsy in Linux**

Source: [www.sleuthkit.org](http://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 issued by the electronic product or service or otherwise on a password-protected website for classroom use.

42



43

## 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

44

## Examining a Case with Sleuth Kit and Autopsy (2 of 3)

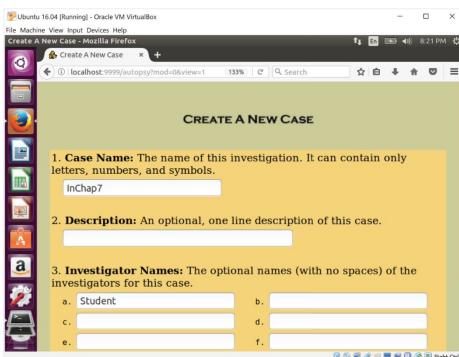


Figure 7-14 The Create a New Case dialog box

Source: [www.sleuthkit.org](http://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 issued by the electronic product or service on a password-protected website for classroom use.

45

## Examining a Case with Sleuth Kit and Autopsy (3 of 3)

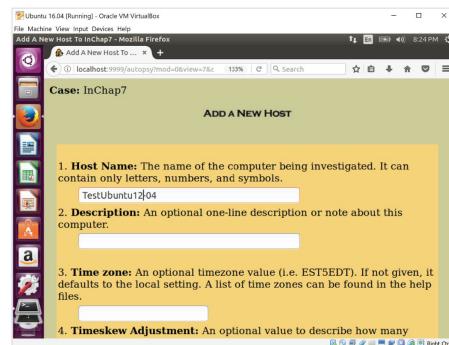


Figure 7-15 The Add a New Host dialog box

Source: [www.sleuthkit.org](http://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 issued by the electronic product or service on a password-protected website for classroom use.

46

46



## 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



## 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



## 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

# Guide to Computer Forensics and Investigations

## Sixth Edition

### *Chapter 8*

#### *Recovering Graphics Files*

CENGAGE



1



## 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.

2

2



## 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.

3

3



## Understanding Bitmap and Raster Images

- **Bitmap images**
  - Grids of individual **pixels** ("picture elements")
- **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

Bits	Colors Possible
1	2
2	4
4	16
8	256
16	65,536
24	16,777,216
32	4,294,967,296

0	0	1	2	3
0	1	2	3	2
1	2	3	2	1
2	3	2	1	0
3	2	1	0	0

0 =	
1 =	
2 =	
3 =	




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.

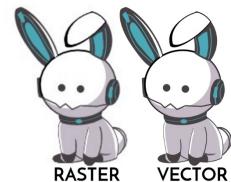
4

4



## 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



© 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.

5

5



## 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



© 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.

6

6



## 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.

7



## 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.

8

8



## Understanding Digital Photograph File Formats (1 of 8)

- Witnesses or suspects can create their own digital photos
  - What about **deepfakes**?
    - Often used to falsely portray somebody doing or saying something and being somewhere
    - The exposure of such fakes would require evidence (or an "alibi") to the contrary
      - Technological innovations are being developed to detect and classify deepfakes by identifying issues with image resolution, scaling, rotation, and splicing
    - U.S. Defense Advanced Research Projects Agency (DARPA) has a [Media Forensics program](#)
  - 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



© 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.

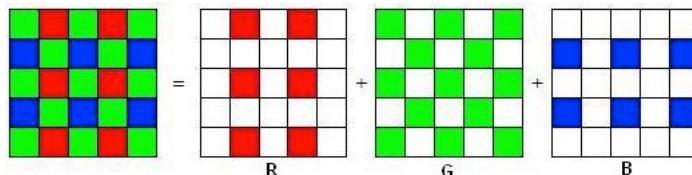
9

9



## 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**
    - Reconstruct a full color image from the incomplete color samples output from an image sensor overlaid with a color filter array (CFA)



© 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.

10

10



## Understanding Digital Photograph File Formats (3 of 8)

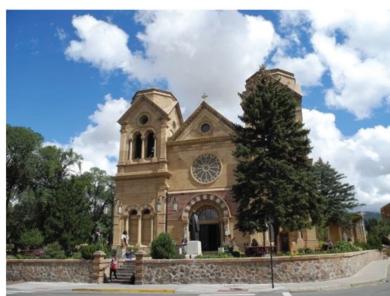
- Examining the Exchangeable Image File format
- **Exchangeable Image File (Exif) format**
  - Commonly used to store digital pictures
  - Developed by JEITA as a standard for storing metadata in JPEG and TIF files
    - Japan Electronics and Information Technology Industries Association
- Exif format 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, ProDiscover, or Magnet Forensics AXIOM
- Exif file stores metadata at the beginning of the file



## Understanding Digital Photograph File Formats (4 of 8)

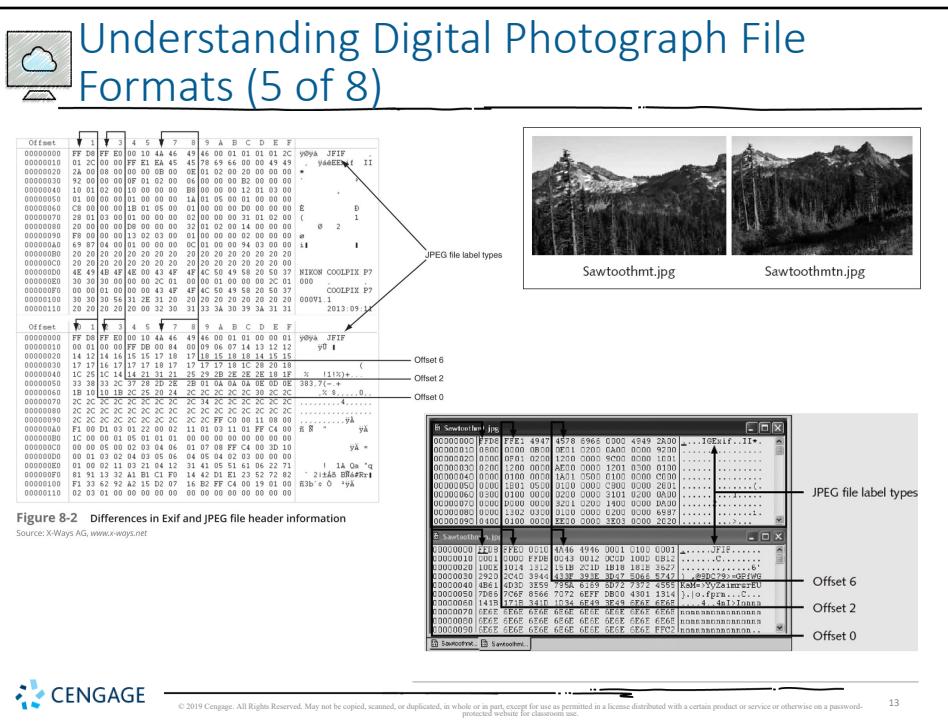


Exif picture file

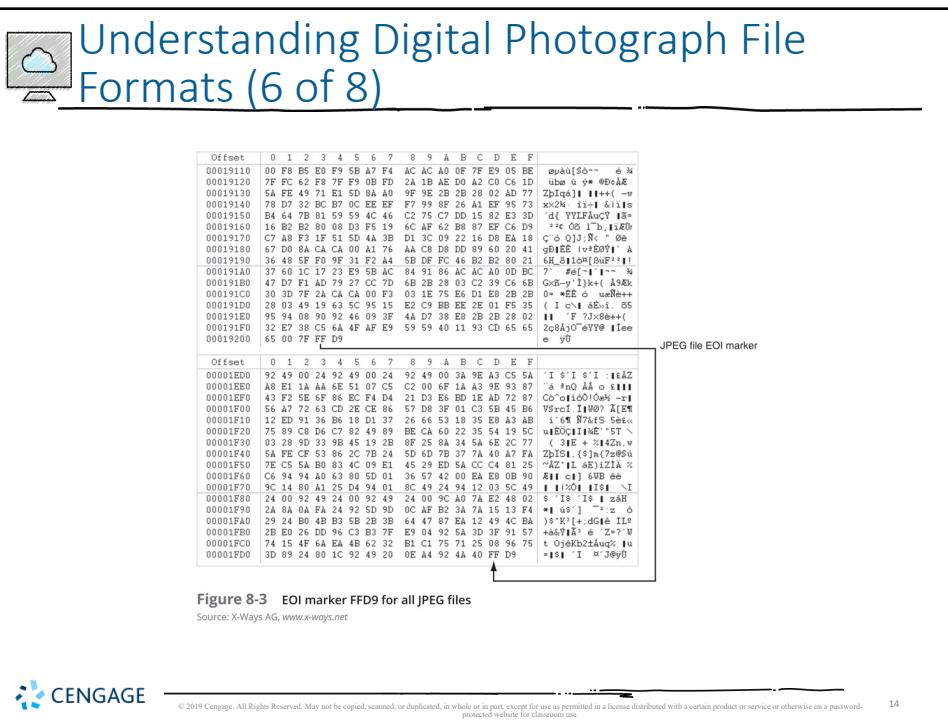


JPEG picture file

**Figure 8-1** Similar Exif and JPEG photos



13



14



## Understanding Digital Photograph File Formats (7 of 8)

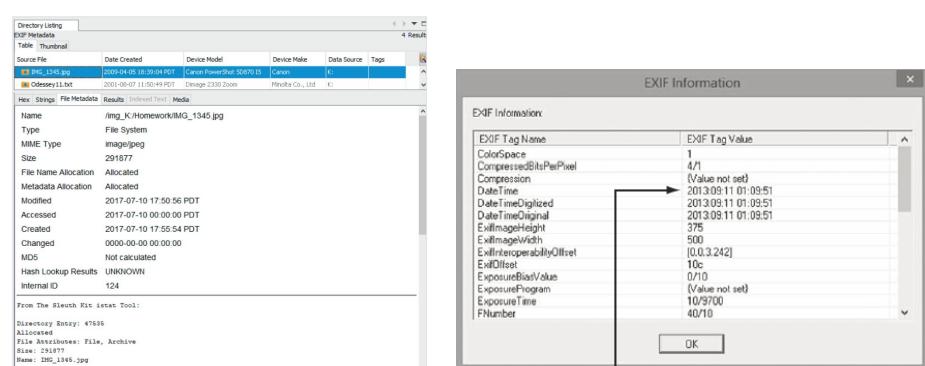
- Examining the Exchangeable Image File format (cont'd)
  - With tools such as Autopsy, ProDiscover, and Exif Reader
    - You can extract metadata as evidence for your case

**CENGAGE**

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

15

15



**EXIF Information**

EXIF Tag Name	EXIF Tag Value
ColorSpace	1
CompressedBitsPerPixel	4/1
Compression	(Value not set)
DateCreated	2013-03-11 01:09:51
DateImageDigitized	2013-03-11 01:09:51
DateImageOriginal	2013-03-11 01:09:51
ExifImageHeight	375
ExifImageWidth	500
ExifInteroperabilityOffset	[0.0.3.242]
ExifOffset	10c
ExposureBiasValue	0/10
ExposureProgram	(Value not set)
ExposureTime	10/9700
FNumber	40/10

Camera-recorded date and time of photo

**Figure 8-4** ProDiscover displaying metadata from an Exif JPEG file  
Courtesy of Technology Pathways, LLC

**CENGAGE**

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

16

16



## 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.

17

17



## 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.

18

18



## Run-Length Encoding

- Simplest method of compression
- Replace consecutive repeating occurrences of a symbol by one occurrence of the symbol followed by the number of occurrences

a. Original data

BBBBBBBBBAAAAAAAANNNNNNNNNNN

b. Compressed data

B09A16N01M10



© 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.

19

19



## Huffman Coding (1 of 4)

- Assigns shorter codes to symbols that occur more frequently and longer codes to those that occur less frequently
- Example
  - Assume text file uses only five characters (A, B, C, D, E)
  - Assign character weight based on frequency of use

Character	A	B	C	D	E
Frequency	17	12	12	27	32



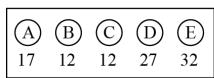
© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

20

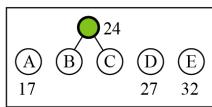
20



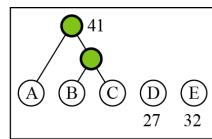
## Huffman Coding (2 of 4)



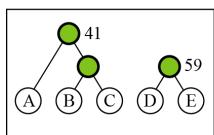
a.



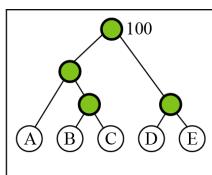
b.



c.



d.



e.

1. Begin with a forest of trees. All trees are one node, with the weight of the tree equal to the weight of the character in the node. Characters that occur most frequently have the highest weights. Characters that occur least frequently have the smallest weights.

2. Repeat this step until there is only one tree:

Choose two trees with the smallest weights, call these trees  $T_1$  and  $T_2$ . Create a new tree whose root has a weight equal to the sum of the weights  $T_1 + T_2$  and whose left subtree is  $T_1$  and whose right subtree is  $T_2$ .

3. The single tree left after the previous step is an optimal encoding tree.



© 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.

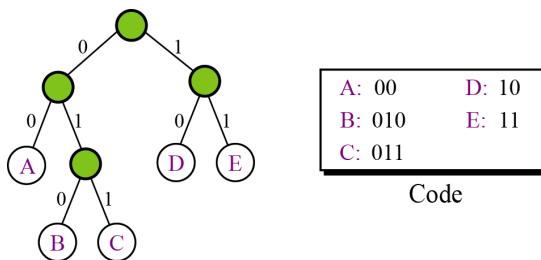
21

21



## Huffman Coding (3 of 4)

- Character's code found by starting at the root and following the branches that lead to that character
- The code itself is the bit value of each branch on the path, taken in sequence



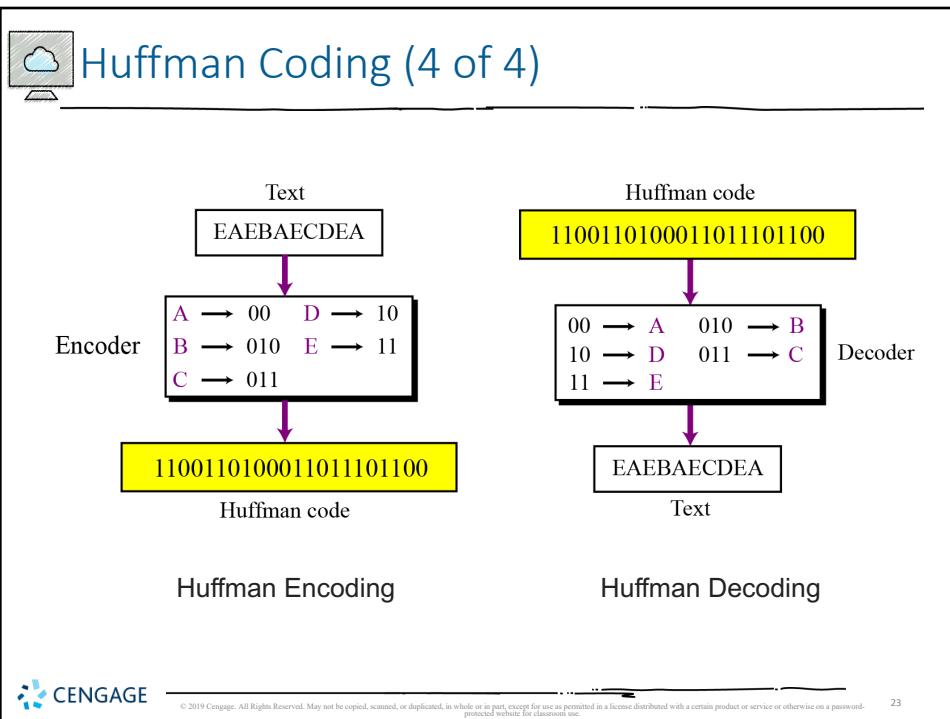
Final tree and code



© 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.

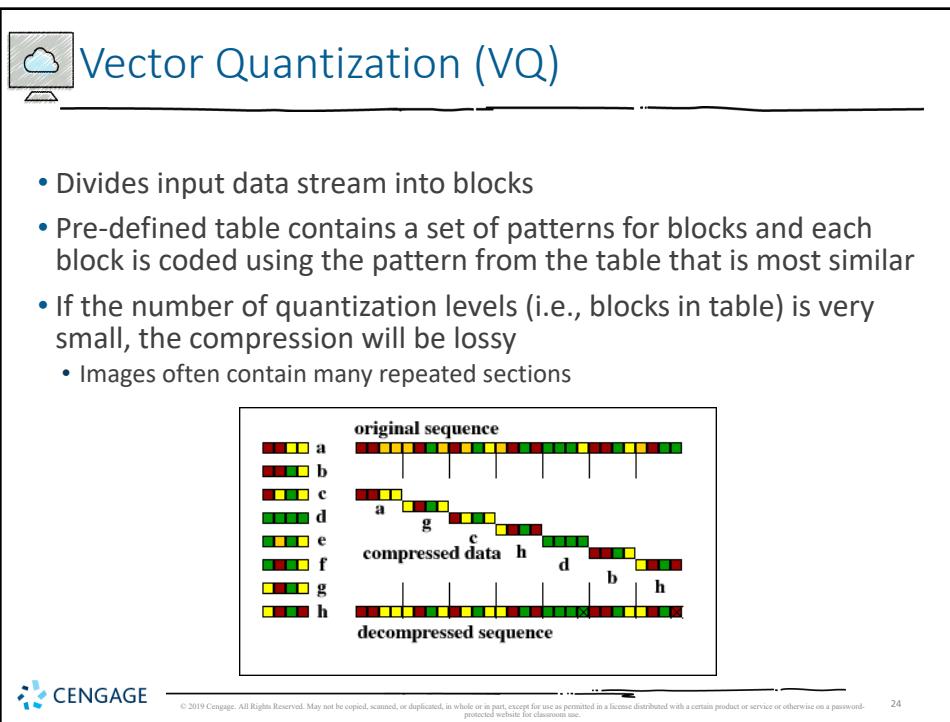
22

22



23

23



24

24



## 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.

25

25



## 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 file 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.

26

26



## 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



© 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.

27

27



## 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.



© 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.

28

28



## 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](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.

29



## 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**

 © 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.

30



## 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 or ProDiscover to search for and extract (recover) possible evidence of JPEG files
  - False hits are referred to as **false positives**



© 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.

31

31



## Searching for and Carving Data from Unallocated Space (2 of 6)

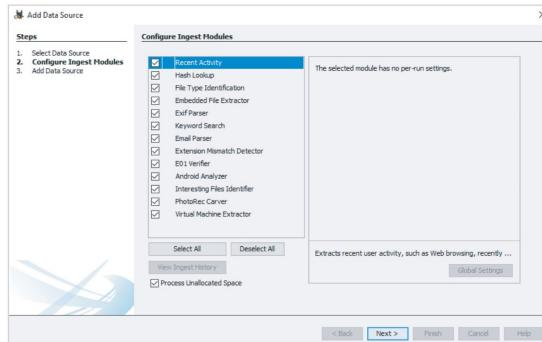


Figure 8-7 Processing options in the Configure Ingest Modules window  
Source: [www.sleuthkit.org](http://www.sleuthkit.org)



© 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.

32

32

## Searching for and Carving Data from Unallocated Space (3 of 6)

**Figure 8-8** Parsing Exif metadata in Autopsy

Source: [www.sleuthkit.org](http://www.sleuthkit.org)



## Searching for and Carving Data from Unallocated Space (4 of 6)

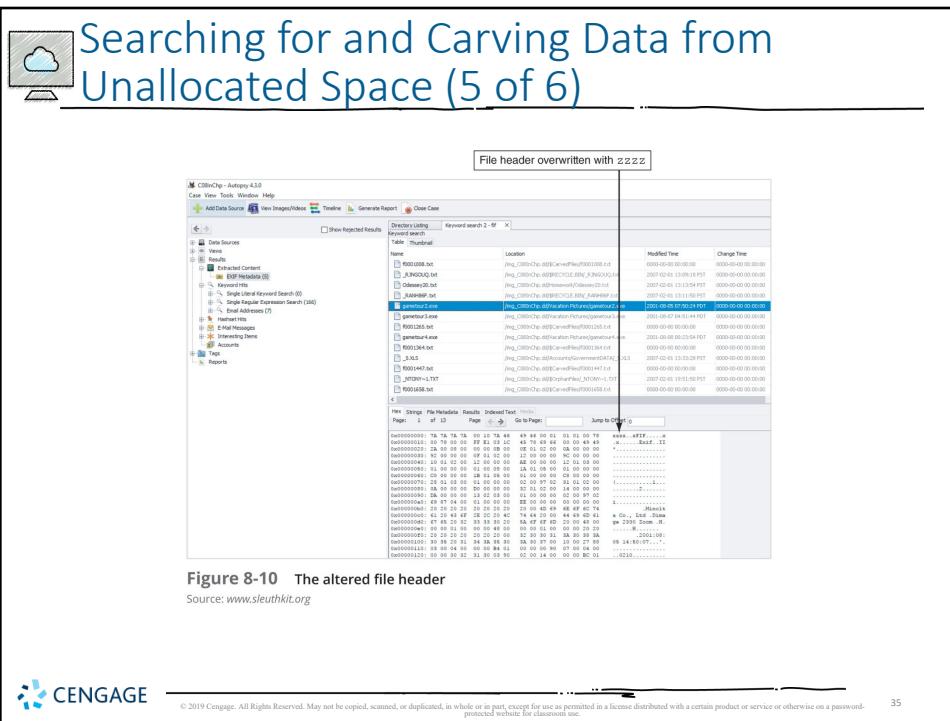
The screenshot shows the Oracle Database Diagnostic Pack interface with the following details:

- Navigation Bar:** Includes links for Home, Case, View, Monitor, Help, and several tabs: Database Health, View Diagnostic Results, Timeline, Generate Report, and Close Case.
- Search Bar:** Contains fields for Keyword, Keyword Scope, and a search button.
- Left Sidebar:** Lists categories such as Data Sources, Home, Reports, and Tags, along with specific items like Database Health, Recent Items, and Recent Reports.
- Central Grid:** A large table displaying search results with columns: ID, Location, Modified Time, Change Time, Access Time, Checked Time, Size, Flagged#, Flagged#, Node, and Status. The data includes various log entries and error messages.
- Bottom Navigation:** Includes links for Home, Page, Page Number, Previous, Next, Go to Page, and Jump to Offset.

**Figure 8-9** The results of searching for “fif”

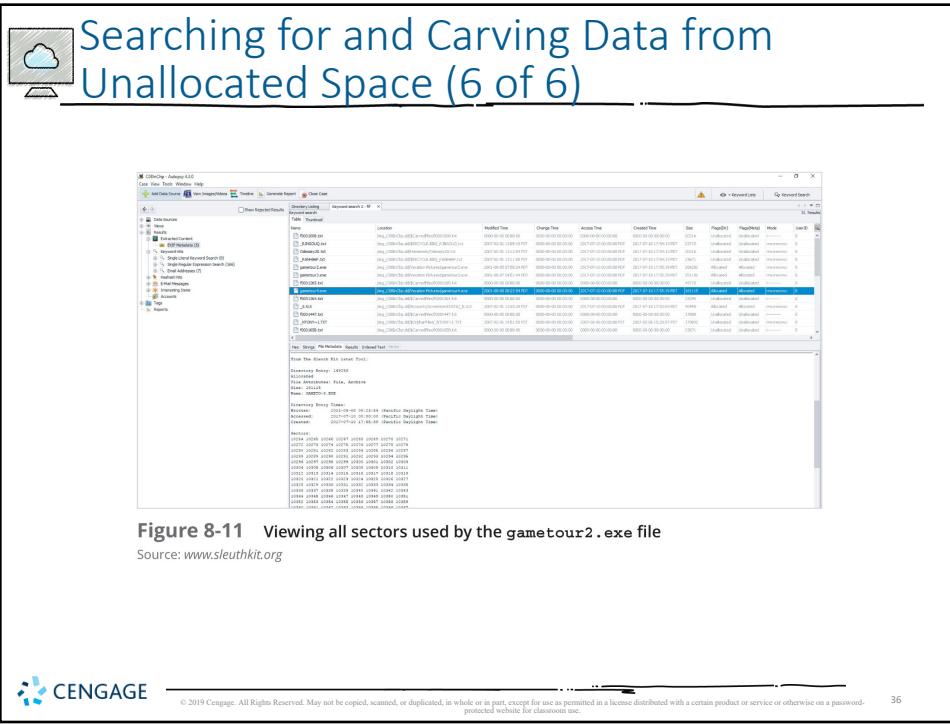
Source: [www.sleuthkit.org](http://www.sleuthkit.org)





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.

35



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.

36

## Searching for and Carving Data from Unallocated Space (1 of 5)

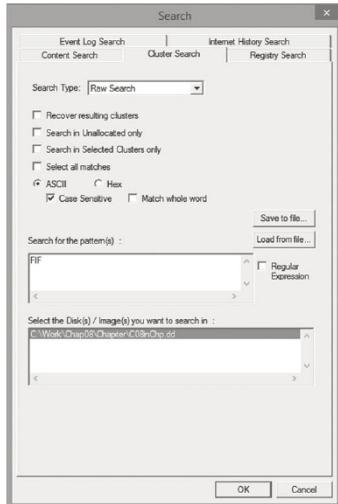


Figure 8-7 Searching clusters in ProDiscover



© 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.

37

37

## Searching for and Carving Data from Unallocated Space (2 of 5)

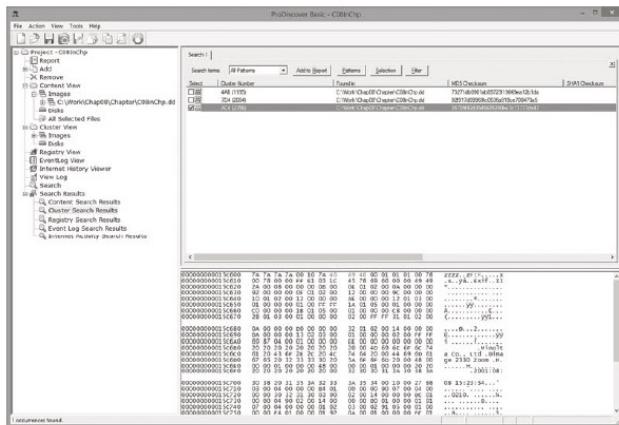


Figure 8-8 Completed cluster search for FIF  
Courtesy of Technology Pathways, LLC



© 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.

38

38



## Searching for and Carving Data from Unallocated Space (3 of 5)

File header overwritten with zzzz

```

000000000015c600 7A 7A 7A 7A 00 10 7A 46 49 46 00 01 01 01 00 78 → zzzz,zFIE,...,x
000000000015c610 00 78 00 00 FF E1 03 1C 45 78 69 66 00 00 49 49 .x.,yA..EXf..II
000000000015c620 2A 00 08 00 00 00 00 00 00 00 00 00 00 00 00 00 ..0..02..09..04..00..00
000000000015c630 97 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..0..03..00..00..00..00
000000000015c640 10 01 02 00 12 00 00 00 AE 00 00 00 12 01 03 00 ..0..04..00..00..00..00
000000000015c650 01 00 00 00 01 00 FF FF 1A 02 05 00 02 00 00 00 ..0..05..00..00..00..00
000000000015c660 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..0..06..00..00..00..00
000000000015c670 2A 01 02 00 00 00 00 00 02 00 FF FF 32 02 02 00 ..0..07..00..00..00..00
000000000015c680 0A 00 00 00 00 00 00 00 32 05 02 00 14 00 00 00 ..0..08..00..00..00..00
000000000015c690 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..0..09..00..00..00..00
000000000015c6A0 69 87 04 00 01 00 00 00 EE 00 00 00 00 00 00 00 ..0..0A..00..00..00..00
000000000015c6B0 20 20 20 20 20 20 20 20 20 00 40 69 6E 6C 74 ..1.....Minolt
000000000015c6C0 61 20 43 6E 21 2C 20 4C 74 64 20 00 44 69 6D 61 ..a co., Ltd. Dima
000000000015c6D0 07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..g.....Zoom .H.
000000000015c6E0 00 00 01 00 00 00 00 00 00 00 01 00 00 00 00 00 ..0..01..00..00..00..00
000000000015c6F0 20 20 20 20 20 20 20 20 32 30 31 3A 30 38 3A ..2001:08:
000000000015c700 30 38 20 31 35 3A 32 33 3A 35 34 00 10 00 27 88 08 15:23:54...
000000000015c710 03 00 04 00 00 00 84 01 00 00 90 07 00 04 00 ..0..0210....%.
000000000015c720 00 00 30 32 31 30 03 90 02 00 14 00 00 00 8C 01 ..0..0210....%.
000000000015c730 00 00 04 90 05 00 14 00 00 00 00 00 00 00 00 00 ..0..0210....%.
000000000015c740 00 00 01 00 00 00 02 00 00 00 00 00 00 00 00 00 ..0..0210....%.
000000000015c750 00 00 E4 01 00 00 01 92 04 00 01 00 00 00 EC 01 ..0..0210....%.
000000000015c760 00 00 02 92 05 00 01 00 00 00 00 00 F4 01 00 00 04 92 ..0..0210....%.
000000000015c770 0A 00 01 00 00 FC 01 00 00 09 92 03 00 01 00 ..0..0210....%.
000000000015c780 00 00 00 00 FF FF 0A 92 05 00 01 00 00 00 04 02 ..0..0210....%.
000000000015c790 00 00 7C 92 07 00 08 01 00 00 02 00 00 00 A0 00 ..0..0210....%.
000000000015c7A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..0..0210....%.
000000000015c7B0 00 00 01 00 A1 96 02 A0 04 00 01 00 00 00 80 03 ..0..0210....%.
000000000015c7C0 00 00 03 A0 04 00 01 00 00 00 00 00 58 02 00 00 00 ..0..0210....%.
000000000015c7D0 00 00 64 00 04 00 00 64 00 64 00 32 30 30 31 3A 30 ..0..0210....%.
000000000015c7E0 38 3A 30 38 20 31 35 3A 32 33 3A 35 34 00 32 30 ..0..0210....%.

```

**Figure 8-9 Content of cluster AC4(2756)**  
Courtesy of Technology Pathways, LLC

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

39



## Searching for and Carving Data from Unallocated Space (4 of 5)

List of Clusters

List of Clusters for the file:  
C:\Wook\Chap08\ChapterC08inClip.dd\New Folder\gametour4.exe

ac4 (2756)
ac5 (2757)
ac6 (2758)
ac7 (2759)
ac8 (2760)
ac9 (2761)

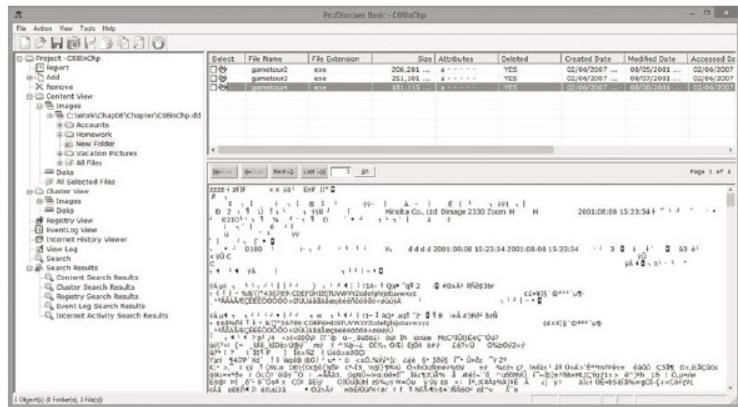
**Figure 8-10 Viewing all clusters used by the gametour4.exe file**  
Courtesy of Technology Pathways, LLC

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

40

40

## Searching for and Carving Data from Unallocated Space (5 of 5)



**Figure 8-11** Mislabeled file that appears to be altered intentionally  
Courtesy of Technology Pathways, LLC



© 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.

41

## 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



© 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.

42

42

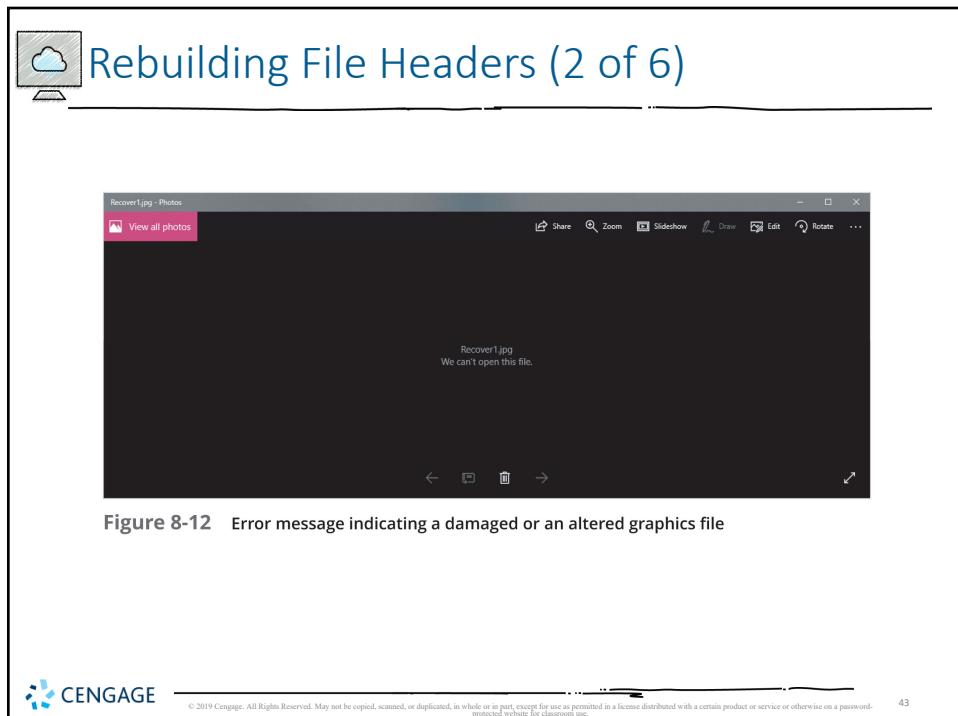


Figure 8-12 Error message indicating a damaged or an altered graphics file

43

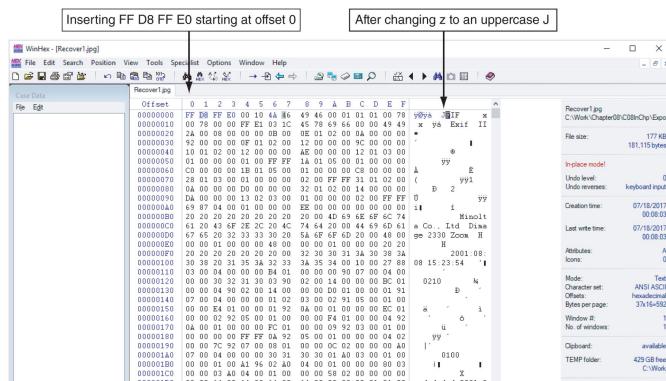
Offset	0	1	2	3	4	5	6	7	8	A	B	C	D	E	F
00000010	40	72	74	72	00	10	74	46	49	46	00	01	01	00	78
00000011	00	78	00	00	FF	E1	03	4C	45	78	69	66	00	00	49
00000012	00	00	00	00	00	00	00	00	00	00	00	00	00	00	49
00000013	92	00	00	00	00	00	01	02	00	12	00	00	00	9C	00
00000014	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000015	10	01	02	00	12	00	00	00	AE	00	00	00	12	01	00
00000016	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000017	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000018	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000019	28	01	03	00	00	00	00	00	02	00	FF	FF	31	01	02
0000001A	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000001B	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000001C	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000001D	69	87	04	00	01	00	00	00	00	00	00	00	00	00	00
0000001E	20	20	29	29	29	29	29	29	20	00	4D	49	4E	4F	74
0000001F	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000020	67	65	20	32	33	33	33	30	29	5A	4F	4F	4D	20	00
00000021	00	00	01	00	00	00	00	49	00	00	00	00	00	00	00
00000022	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000023	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000024	30	36	20	31	35	34	32	33	3A	35	34	00	10	00	27
00000025	03	00	04	00	00	00	00	00	00	00	00	00	00	00	00
00000026	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000027	00	00	04	90	00	00	14	00	00	00	00	00	00	00	00
00000028	07	00	04	00	00	00	00	01	02	03	00	02	01	05	00
00000029	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000002A	00	00	02	92	05	00	01	00	00	00	F4	01	00	00	04
0000002B	04	00	01	00	00	00	00	00	00	00	00	00	00	00	00
0000002C	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000002D	00	00	00	02	A9	00	00	00	00	00	00	58	02	00	00
0000002E	00	00	00	64	00	64	00	64	00	00	00	32	30	30	3A
0000002F	38	5A	30	38	20	31	35	3A	32	33	3A	35	34	00	32

Figure 8-13 Recover1.jpg open in WinHex  
Source: X-Ways AG, [www.xwsys.net](http://www.xwsys.net)



44

## Rebuilding File Headers (4 of 6)



**Figure 8-14** Inserting correct hexadecimal values for a JPEG file

Source: X-Ways AG, [www.xways.net](http://www.xways.net)

45

45

## 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		R	S	T	U	V	W	X	Y	Z	[	]	]	
6		a	b	c	d	e	f	g	h	i	j	k	l	m	
7		q	r	s	t	u	v	w	x	y	z	{	}		

Second hexadecimal number

— First hexadecimal number

**Figure 8-15** ASCII equivalents of hexadecimal values

 CENGAGE

46

46

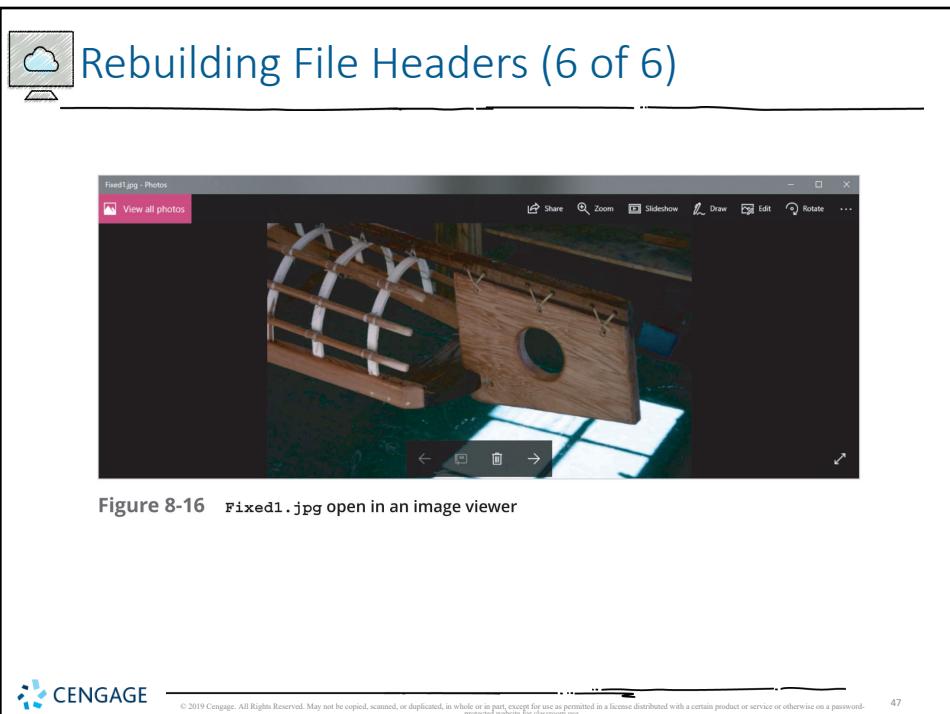


Figure 8-16 Fixed1.jpg open in an image viewer



## 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

© 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 \(\[www.fileformat.info/format/all.htm\]\(http://www.fileformat.info/format/all.htm\)\)](http://www.fileformat.info/format/all.htm)
  - [Extension Informer \(<http://extension.informer.com>\)](http://extension.informer.com)
  - [The Graphics File Formats Page \(\[www.martinreddy.net/gfx\]\(http://www.martinreddy.net/gfx\)\)](http://www.martinreddy.net/gfx)



© 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.

49

49



## 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



© 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.

50

50



## 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
00000010	00	84	42	20	C0	10	03	FA	18	00	85	C2	62	50	88	2C
00000020	2A	0F	12	88	C6	20	EE	F8	98	08	01	05	01	C2	63	D1
00000030	A8	7C	4E	4D	24	88	45	E4	F2	89	5C	1A	39	2B	96	4C
00000040	26	53	39	A4	A6	4B	35	9A	C6	67	13	59	1C	EE	7D	16
00000050	9B	CC	27	51	27	E4	7C	06	FE	8F	BF	DF	70	87	EC	51
00000060	FF	1C	01	80	C0	00	15	56	3F	0E	86	BF	A9	00	60	00
00000070	48	28	00	FD	B0	00	1F	6F	CA	2D	6A	91	58	9B	42	00
00000080	51	C0	10	06	38	04	7D	D3	40	36	B8	80	00	09	5F	B9
00000090	D2	61	8F	E0	14	86	DA	05	B5	43	29	F1	C8	BB	F9	F5
000000A0	4B	84	51	41	00	4C	03	F9	FE	FA	C4	D2	00	A0	7C	03
000000B0	E6	C3	05	8F	48	24	51	F0	04	86	29	26	00	D1	61	00

Figure 8-17 A TIF file open in WinHex

Source: X-Ways AG, [www.x-ways.net](http://www.x-ways.net)



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

51

51



## 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
00000010	64	20	03	00	05	00	01	00	34	00	00	00	02	00	40	00
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	03	00	B4	00	00	00	00	00
00000040	6F	00	41	75	74	68	6F	72	00	58	65	72	6F	78	00	43
00000050	6F	72	70	00	00	44	61	74	65	00	4A	72	6C	00	32	31
00000060	20	31	39	39	39	00	43	6F	70	79	72	69	67	68	74	00
00000070	43	6F	70	79	72	69	67	68	74	00	28	43	29	00	31	39
00000080	39	35	2D	31	39	39	36	00	58	65	72	6F	78	00	43	6F
00000090	72	70	6F	72	61	74	69	6F	6E	2C	20	41	6C	20	52	rporation. All R
000000A0	69	67	68	74	73	20	52	65	73	65	72	76	65	64	00	00
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](http://www.x-ways.net)



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

52

52



## 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



© 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.

53

53



## Understanding Steganography in Graphics Files (1 of 7)

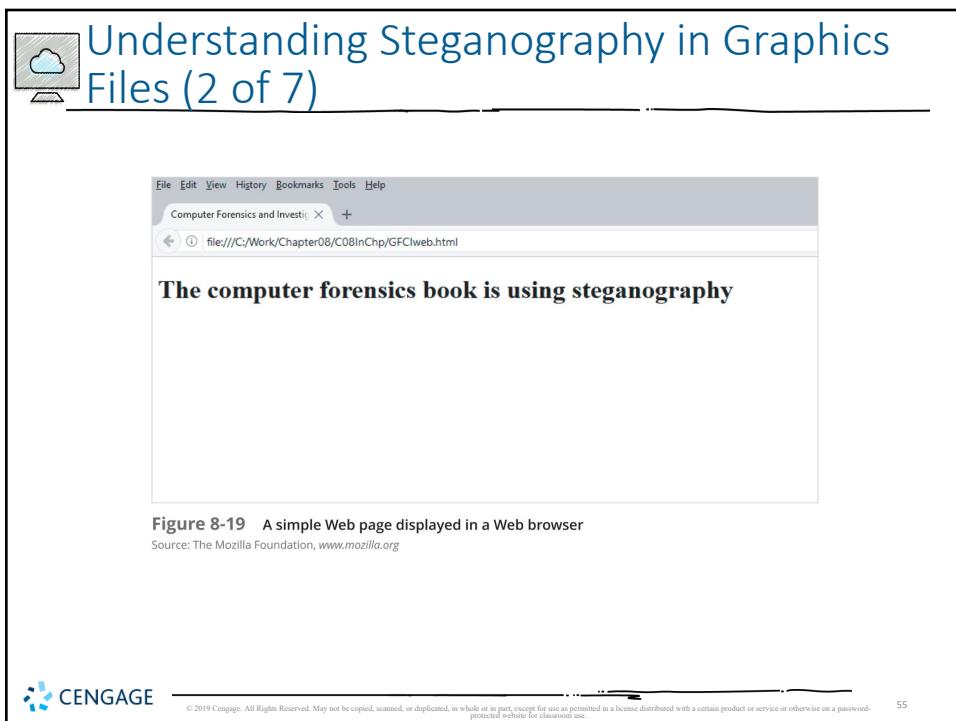
- Steganography hides information inside image files
  - An ancient technique
- Two major forms: **insertion** and **substitution**
- Insertion
  - Hidden data is not displayed when viewing host file in its associated program
    - You need to analyze the data structure carefully
  - Example: Web page



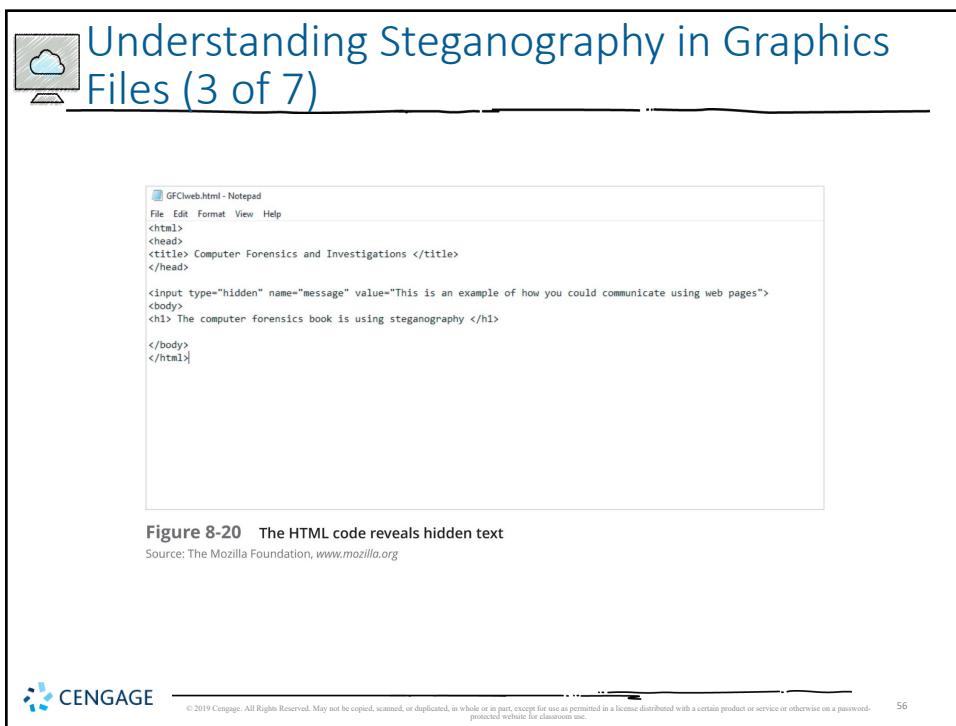
© 2019 Cengage. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

54

54



55



56



## 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



© 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.

57



## 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



© 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.

58

## Understanding Steganography in Graphics Files (6 of 7)



Figure 8-21 Original and altered images

## 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	Vallletta 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



## 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



© 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.

61

61



## Understanding Copyright Issues with Graphics

- Steganography has been used to protect copyrighted material
  - By inserting digital watermarks into a file
- Digital investigators need to be aware of copyright laws
- Copyright laws for Internet are not clear
  - There is no international copyright law
- Check the [U.S. Copyright Office \(www.copyright.gov\)](http://www.copyright.gov)
  - U.S. Copyright Office identifies what can and can't be covered under copyright law in U.S.
- **Fair use**
  - Another guideline to consider



© 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.

62

62



## 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.

63



## 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.

64



## 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.

65

# Guide to Computer Forensics and Investigations

## Sixth Edition

### *Chapter 9*

#### *Digital Forensics Analysis and Investigation*

 CENGAGE



1



### Objectives

- Determine what data to analyze in a digital forensics investigation
- Explain tools used to validate data
- Explain common data-hiding 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.

2

2



## 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



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

3

3



## 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



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

4

4



## 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.

5



## 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.

6

6



## 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



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

7



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

8



## NIST NSRL

- National Software Reference Library (NSRL)
  - A physical collection of over 5,000 software packages on secured shelves
  - A database of file “fingerprints” (or “hashes”) and additional information to uniquely identify each file on the shelves
  - A Reference Data Set (RDS) extracted from the database onto CD used by law enforcement, investigators, researchers, others



CENGAGE

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

9

9



## NIST NSRL

- Use of the NSRL
  - Eliminate as many known files as possible from the examination process using automated means
  - Discover expected file name with unknown contents
  - Identify origins of files
  - Look for malicious files, e.g., hacker tools
  - Identify duplicate files
  - Provide rigorously verified data for forensic investigations

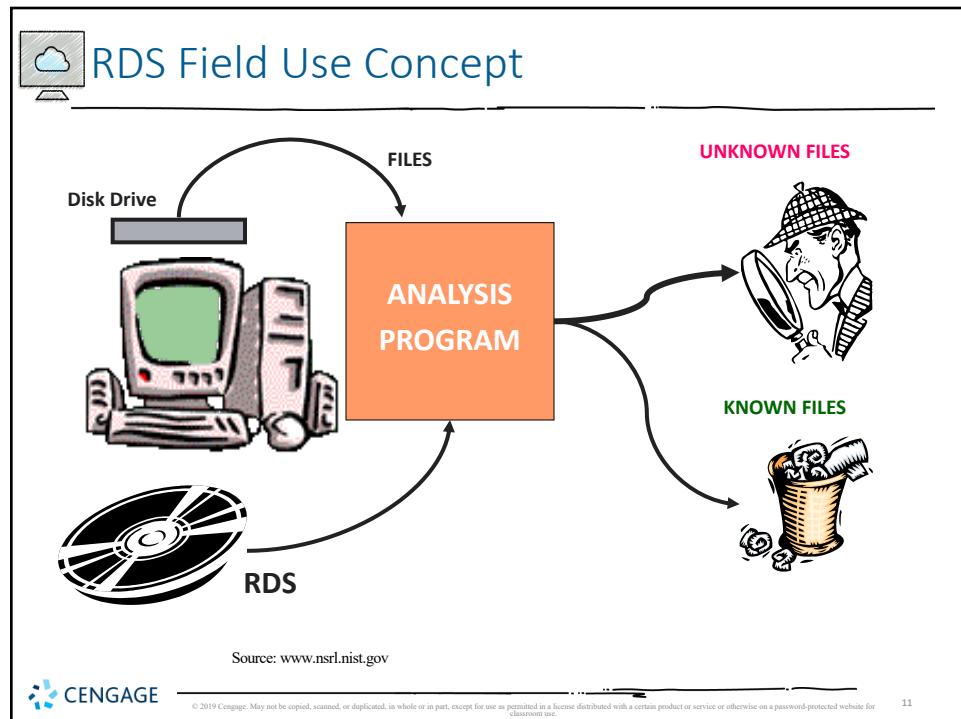


CENGAGE

© 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.

10

10



11

The diagram illustrates a Windows 2000 desktop environment. It features a blue taskbar at the bottom with icons for 'My Computer', 'Recycle Bin', and 'Taskbar'. On the desktop, there are several icons: 'Windows 2000 Professional', 'My Computer', 'Recycle Bin', 'Windows 2000 Professional', and 'Taskbar'.

- You are looking for sensitive facility maps on a computer which is running Windows 2000
- Windows 2000 operating system software contains 5933 images which are known gifs, icons, jpeg files
- Example

Source: [www.nsrl.nist.gov](http://www.nsrl.nist.gov)

**CENGAGE** © 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use. 12

12



## 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.

13

13



## Using Autopsy to Analyze Data (2 of 6)

- Autopsy can handle many formats, including:
  - Raw, Expert Witness, and virtual machine image files (.vdi and .vhdx)
- 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



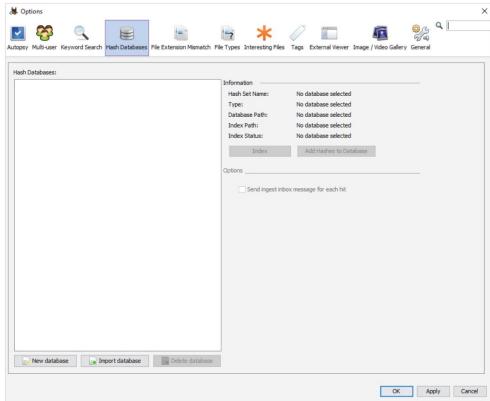
CENGAGE

© 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.

14

14

## Using Autopsy to Analyze Data (3 of 6)



The screenshot shows the 'Hash Databases' options dialog in the Autopsy forensic tool. The dialog has a tab bar at the top with 'Hash Databases' selected. Below the tabs are two main sections: 'Information' and 'Options'. Under 'Information', fields include 'Hash Set Name' (No database selected), 'Type' (No database selected), 'Database Path' (No database selected), 'Index Path' (No database selected), and 'Index Status' (No database selected). There is also a 'Indexes' button and an 'Add hashes to Database' button. Under 'Options', there is a checkbox for 'Send ingest inbox message for each hit'. At the bottom are buttons for 'New database', 'Import database', and 'Delete database', followed by 'OK', 'Apply', and 'Cancel'.

**Figure 9-1** The Hash Databases options  
Source: [www.sleuthkit.org](http://www.sleuthkit.org)

CENGAGE

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

15

## Using Autopsy to Analyze Data (4 of 6)

- Collecting Hash Values in Autopsy
  - Create a hash database of known files 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.

16

16

**Using Autopsy to Analyze Data (5 of 6)**

Source: [www.sleuthkit.org](http://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.

17

**Using Autopsy to Analyze Data (6 of 6)**

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

18



## Using OSForensics to Analyze Data (1 of 5)

- OSForensics can perform forensics analysis on the following file systems:
  - Microsoft FAT12, FAT16, and FAT32
  - Microsoft NTFS
  - Mac HFS+ and HFSX
  - Linux Ext2fs, and Ext4fs
- OSForensics 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.

19



## Using OSForensics to Analyze Data (2 of 5)

- Includes OSFMount utility which can access many formats, including:
  - Raw, Expert Witness, and Advanced Forensics Format (AFF)
  - Can also mount and examine VMware images (.vmdk), SMART images (.s01), and VHD images (.vhdx)
- Can use the NIST National Software Reference Library (NSRL)
  - Enables you to mount the NSRL ISO image
- Using the Index Feature in OS Forensics
  - OSForensics indexes text data so that you can perform searches immediately

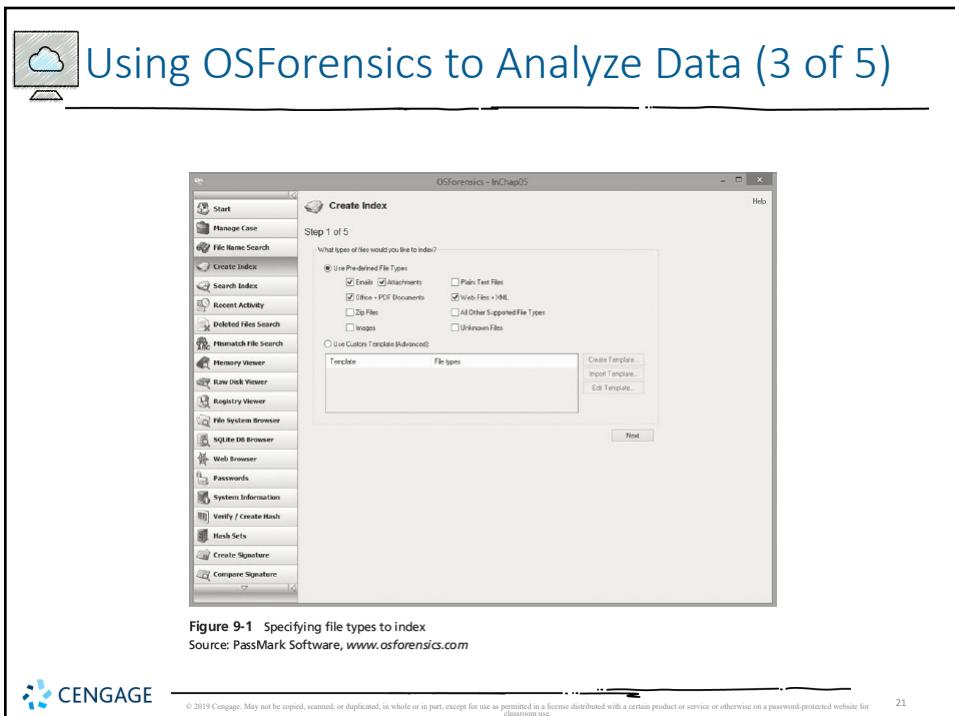


CENGAGE

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

20

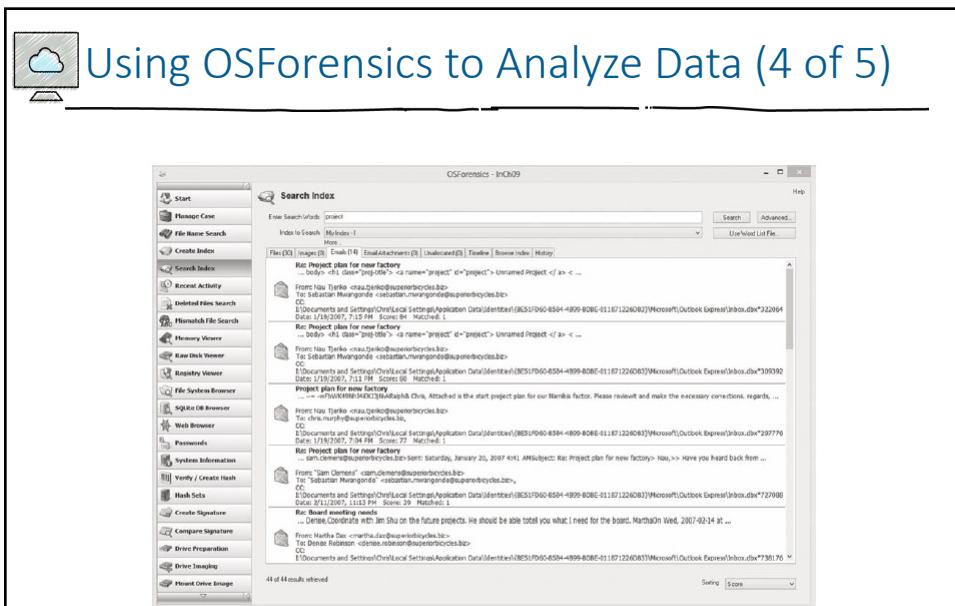
20



**Figure 9-1** Specifying file types to index  
Source: PassMark Software, [www.osforensics.com](http://www.osforensics.com)

2

21



**Figure 9-3** Entering a search term  
Source: PassMark Software, [www.osforensics.com](http://www.osforensics.com)

Source: PassMark Software [www.osforensics.com](http://www.osforensics.com)

22

22

The Add E-mail to Case icon

**E-mail Viewer**

Inbox (21 messages)

From	Subject	Date
Sue Gormley <sue@sue.com>	Office Inventory	1/1/2007, 12:08 PM
Elaine Benson <elaineb@elaineb.com>	Re: Office Inventory	1/3/2007, 2:13 PM
Bob Sauer <bob.sauer@supercycles.biz>	Re: Office Inventory	1/3/2007, 2:53 PM
Jim Smith <jim.smith@supercycles.biz>	Re: Office Inventory	1/3/2007, 7:52 PM
Bob Sauer <bob.sauer@supercycles.biz>	Re: New Product Development	1/3/2007, 3:02 PM
Martha Dax <martha.dax@supercycles.biz>	Re: New Product Development	1/3/2007, 3:02 PM
Jim Smith <jim.smith@supercycles.biz>	Re: New Product Development	1/4/2007, 3:15 AM
Bob Sauer <bob.sauer@supercycles.biz>	Re: Office Inventory	1/4/2007, 6:49 AM
Jim Smith <jim.smith@supercycles.biz>	Re: Office Inventory	1/4/2007, 11:32 AM

Re: New Product Development

From: Jim Smith <jim.smith@supercycles.biz>  
To: Martha Dax <martha.dax@supercycles.biz>  
Cc: Bob Sauer <bob.sauer@supercycles.biz>, Bart Jones <bart.jones@supercycles.biz>, Nau Tjarko <nau.tjarko@supercycles.biz>

Martha, will this be available for public release soon? Jim

On Feb 4, 2007, at 10:08 PM, Martha Dax wrote:

> Hello everybody!

> We have a new announcement to make that is very sensitive regarding a new business venture for us. It is the manufacturing of Kavaks in addition to our bicycle line of products. Our advertising people are excited about this new addition to our line of fine products.

> For security purposes this is competitive sensitive information. Do not tell anyone outside our executive staff about this info

**Figure 9-4** The E-mail Viewer window  
Source: PassMark Software, [www.osforensics.com](http://www.osforensics.com)

23

- Ensuring the integrity of data collected is essential for presenting evidence in court
- Most forensic tools offer hashing of image files
- Example - when ProDiscover loads an image file:
  - It runs a hash and compares the value with the original hash calculated when the image was first acquired
- 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.

24



## 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**

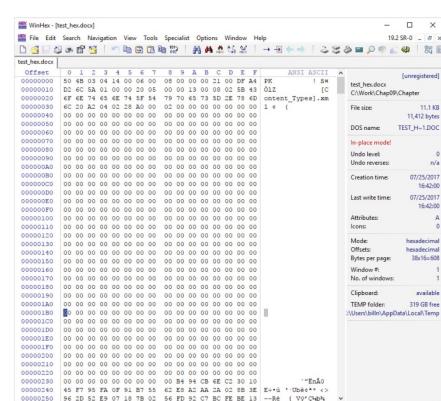
© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

25

25



## Validating with Hexadecimal Editors (2 of 6)

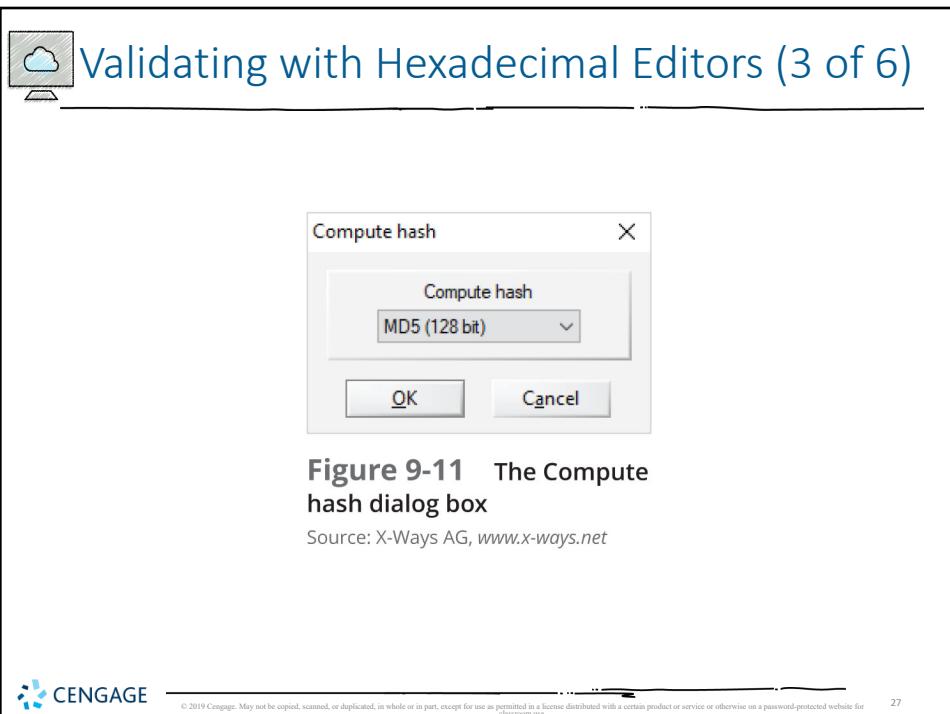


**CENGAGE**

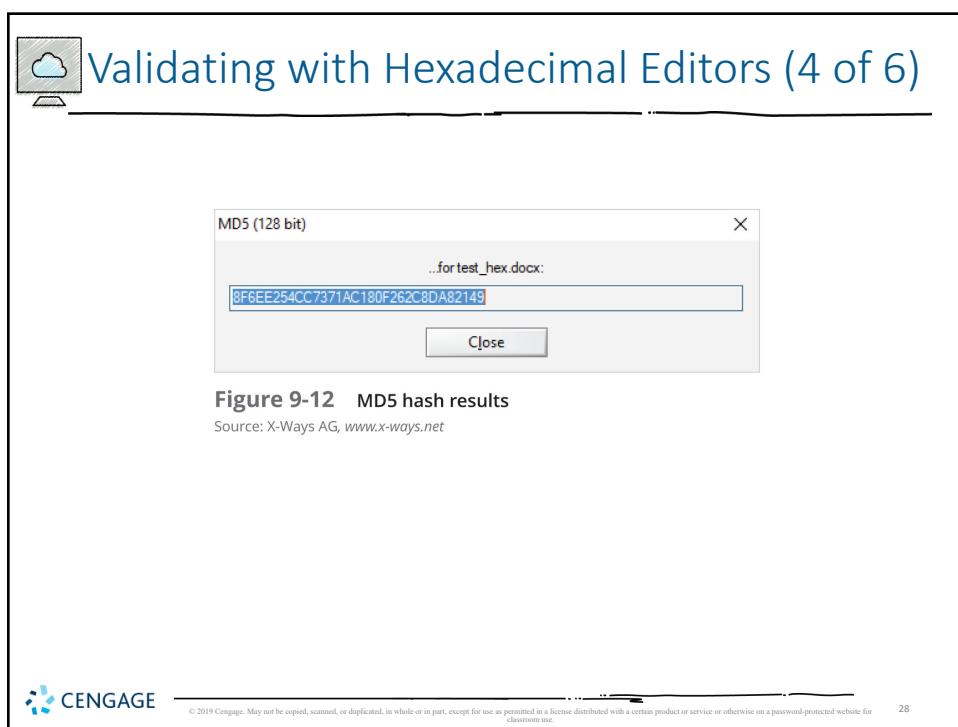
© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

26

26



27



28



## 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.

29



## 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.

30

30



## Validating with Digital Forensics Tools (1 of 6)

- ProDiscover
  - .eve files contain metadata that includes hash value
  - Has a preference you can enable for using the Auto Verify Image Checksum feature when image files are loaded
  - If the Auto Verify Image Checksum and the hashes in the .eve file's metadata don't match
    - ProDiscover will notify that the acquisition is corrupt and can't be considered reliable evidence
- Raw format image files don't contain metadata
  - You must validate them manually to ensure integrity



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

31

31



## Validating with Digital Forensics Tools (2 of 6)

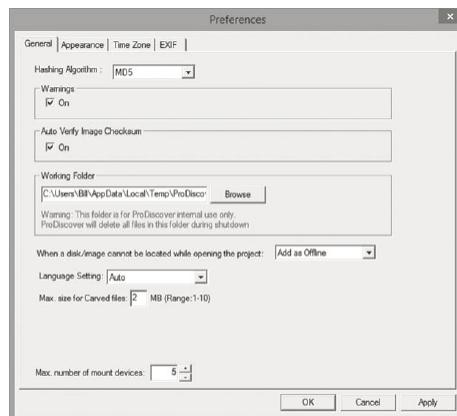


Figure 9-8 Enabling the Auto Verify Image Checksum feature  
Courtesy of Technology Pathways, LLC



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

32

32



## Validating with Digital Forensics Tools (3 of 6)

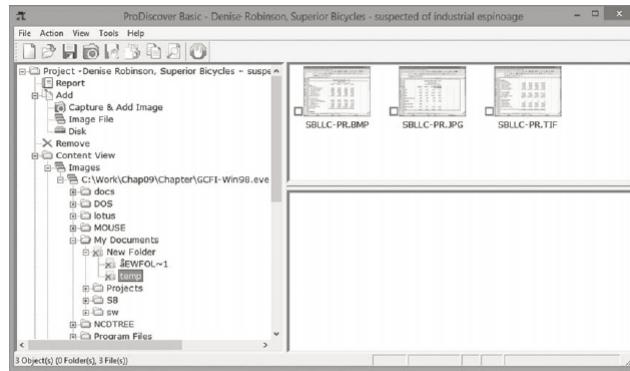


Figure 9-9 The Gallery view  
Courtesy of Technology Pathways, LLC



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

33



## Validating with Digital Forensics Tools (4 of 6)

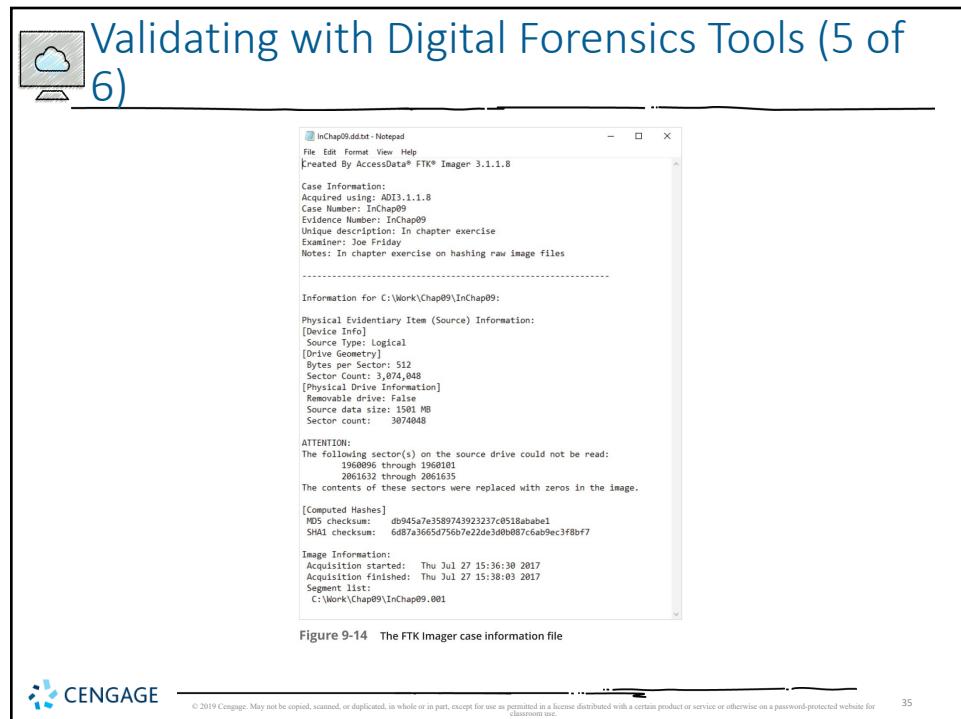
- In AccessData FTK Imager, when selecting the Expert Witness (.e01) or SMART (.s01) format:
  - Additional options for hashing all the data are available
  - Validation report lists MD5 and SHA-1 hash values
- Follow steps starting on page 393 to see how to use WinHex to hash an image file and then compare it with the original hash value FTK Imager calculated



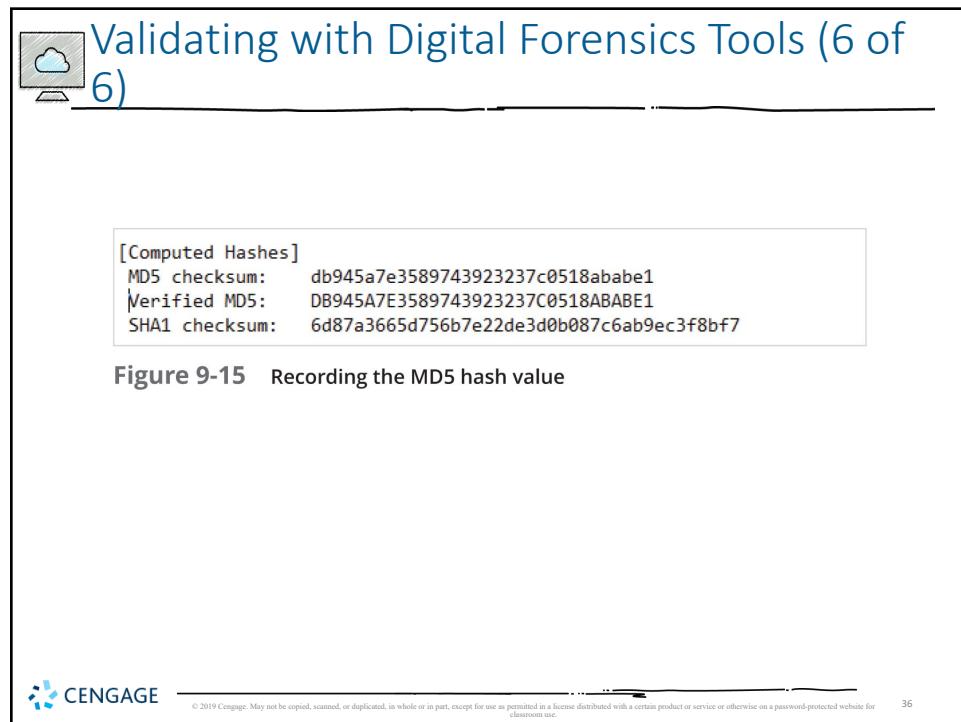
© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

34

34



35



36



## Addressing Data-Hiding Techniques

- Data hiding - changing or manipulating a file to conceal information
- Techniques:
  - Hiding entire partitions
  - Changing file names and 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.

37



## 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.

38



## Hiding Partitions (1 of 5)

- 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.

39



## Hiding Partitions (2 of 5)

- 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
- In ProDiscover, a hidden partition appears as the highest available drive letter set in the BIOS
  - Other forensics tools have their own methods of assigning drive letters to hidden partitions



CENGAGE

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

40

40

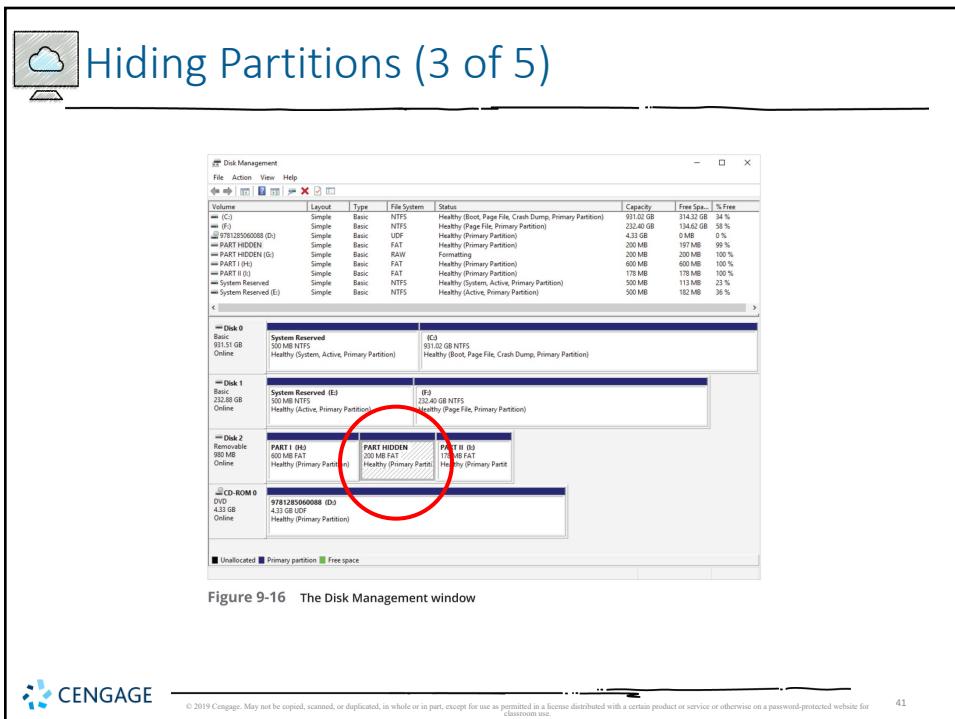


Figure 9-16 The Disk Management window



41

&lt;img alt="Screenshot of the Autopsy Forensic Browser showing a search result for 'jep\_3\Chapo\Hidden-Partition.001\ntd\_wd'. The results table shows 11 items, including several hidden files like .001, .002, .003, .004, .005, .006, .007, .008, .009, .010, .011, .012, .013, .014, .015, .016, .017, .018, .019, .020, .021, .022, .023, .024, .025, .026, .027, .028, .029, .030, .031, .032, .033, .034, .035, .036, .037, .038, .039, .040, .041, .042, .043, .044, .045, .046, .047, .048, .049, .050, .051, .052, .053, .054, .055, .056, .057, .058, .059, .060, .061, .062, .063, .064, .065, .066, .067, .068, .069, .070, .071, .072, .073, .074, .075, .076, .077, .078, .079, .080, .081, .082, .083, .084, .085, .086, .087, .088, .089, .090, .091, .092, .093, .094, .095, .096, .097, .098, .099, .0100, .0101, .0102, .0103, .0104, .0105, .0106, .0107, .0108, .0109, .0110, .0111, .0112, .0113, .0114, .0115, .0116, .0117, .0118, .0119, .0120, .0121, .0122, .0123, .0124, .0125, .0126, .0127, .0128, .0129, .0130, .0131, .0132, .0133, .0134, .0135, .0136, .0137, .0138, .0139, .0140, .0141, .0142, .0143, .0144, .0145, .0146, .0147, .0148, .0149, .0150, .0151, .0152, .0153, .0154, .0155, .0156, .0157, .0158, .0159, .0160, .0161, .0162, .0163, .0164, .0165, .0166, .0167, .0168, .0169, .0170, .0171, .0172, .0173, .0174, .0175, .0176, .0177, .0178, .0179, .0180, .0181, .0182, .0183, .0184, .0185, .0186, .0187, .0188, .0189, .0190, .0191, .0192, .0193, .0194, .0195, .0196, .0197, .0198, .0199, .01200, .01201, .01202, .01203, .01204, .01205, .01206, .01207, .01208, .01209, .01210, .01211, .01212, .01213, .01214, .01215, .01216, .01217, .01218, .01219, .01220, .01221, .01222, .01223, .01224, .01225, .01226, .01227, .01228, .01229, .01230, .01231, .01232, .01233, .01234, .01235, .01236, .01237, .01238, .01239, .01240, .01241, .01242, .01243, .01244, .01245, .01246, .01247, .01248, .01249, .01250, .01251, .01252, .01253, .01254, .01255, .01256, .01257, .01258, .01259, .01260, .01261, .01262, .01263, .01264, .01265, .01266, .01267, .01268, .01269, .01270, .01271, .01272, .01273, .01274, .01275, .01276, .01277, .01278, .01279, .01280, .01281, .01282, .01283, .01284, .01285, .01286, .01287, .01288, .01289, .01290, .01291, .01292, .01293, .01294, .01295, .01296, .01297, .01298, .01299, .012000, .012001, .012002, .012003, .012004, .012005, .012006, .012007, .012008, .012009, .012010, .012011, .012012, .012013, .012014, .012015, .012016, .012017, .012018, .012019, .012020, .012021, .012022, .012023, .012024, .012025, .012026, .012027, .012028, .012029, .012030, .012031, .012032, .012033, .012034, .012035, .012036, .012037, .012038, .012039, .012040, .012041, .012042, .012043, .012044, .012045, .012046, .012047, .012048, .012049, .012050, .012051, .012052, .012053, .012054, .012055, .012056, .012057, .012058, .012059, .012060, .012061, .012062, .012063, .012064, .012065, .012066, .012067, .012068, .012069, .012070, .012071, .012072, .012073, .012074, .012075, .012076, .012077, .012078, .012079, .012080, .012081, .012082, .012083, .012084, .012085, .012086, .012087, .012088, .012089, .012090, .012091, .012092, .012093, .012094, .012095, .012096, .012097, .012098, .012099, .012100, .012101, .012102, .012103, .012104, .012105, .012106, .012107, .012108, .012109, .012110, .012111, .012112, .012113, .012114, .012115, .012116, .012117, .012118, .012119, .012120, .012121, .012122, .012123, .012124, .012125, .012126, .012127, .012128, .012129, .012130, .012131, .012132, .012133, .012134, .012135, .012136, .012137, .012138, .012139, .012140, .012141, .012142, .012143, .012144, .012145, .012146, .012147, .012148, .012149, .012150, .012151, .012152, .012153, .012154, .012155, .012156, .012157, .012158, .012159, .012160, .012161, .012162, .012163, .012164, .012165, .012166, .012167, .012168, .012169, .012170, .012171, .012172, .012173, .012174, .012175, .012176, .012177, .012178, .012179, .012180, .012181, .012182, .012183, .012184, .012185, .012186, .012187, .012188, .012189, .012190, .012191, .012192, .012193, .012194, .012195, .012196, .012197, .012198, .012199, .012200, .012201, .012202, .012203, .012204, .012205, .012206, .012207, .012208, .012209, .012210, .012211, .012212, .012213, .012214, .012215, .012216, .012217, .012218, .012219, .012220, .012221, .012222, .012223, .012224, .012225, .012226, .012227, .012228, .012229, .012230, .012231, .012232, .012233, .012234, .012235, .012236, .012237, .012238, .012239, .012240, .012241, .012242, .012243, .012244, .012245, .012246, .012247, .012248, .012249, .012250, .012251, .012252, .012253, .012254, .012255, .012256, .012257, .012258, .012259, .012260, .012261, .012262, .012263, .012264, .012265, .012266, .012267, .012268, .012269, .012270, .012271, .012272, .012273, .012274, .012275, .012276, .012277, .012278, .012279, .012280, .012281, .012282, .012283, .012284, .012285, .012286, .012287, .012288, .012289, .012290, .012291, .012292, .012293, .012294, .012295, .012296, .012297, .012298, .012299, .012300, .012301, .012302, .012303, .012304, .012305, .012306, .012307, .012308, .012309, .012310, .012311, .012312, .012313, .012314, .012315, .012316, .012317, .012318, .012319, .012320, .012321, .012322, .012323, .012324, .012325, .012326, .012327, .012328, .012329, .012330, .012331, .012332, .012333, .012334, .012335, .012336, .012337, .012338, .012339, .012340, .012341, .012342, .012343, .012344, .012345, .012346, .012347, .012348, .012349, .012350, .012351, .012352, .012353, .012354, .012355, .012356, .012357, .012358, .012359, .012360, .012361, .012362, .012363, .012364, .012365, .012366, .012367, .012368, .012369, .012370, .012371, .012372, .012373, .012374, .012375, .012376, .012377, .012378, .012379, .012380, .012381, .012382, .012383, .012384, .012385, .012386, .012387, .012388, .012389, .012390, .012391, .012392, .012393, .012394, .012395, .012396, .012397, .012398, .012399, .012400, .012401, .012402, .012403, .012404, .012405, .012406, .012407, .012408, .012409, .012410, .012411, .012412, .012413, .012414, .012415, .012416, .012417, .012418, .012419, .012420, .012421, .012422, .012423, .012424, .012425, .012426, .012427, .012428, .012429, .012430, .012431, .012432, .012433, .012434, .012435, .012436, .012437, .012438, .012439, .012440, .012441, .012442, .012443, .012444, .012445, .012446, .012447, .012448, .012449, .012450, .012451, .012452, .012453, .012454, .012455, .012456, .012457, .012458, .012459, .012460, .012461, .012462, .012463, .012464, .012465, .012466, .012467, .012468, .012469, .012470, .012471, .012472, .012473, .012474, .012475, .012476, .012477, .012478, .012479, .012480, .012481, .012482, .012483, .012484, .012485, .012486, .012487, .012488, .012489, .012490, .012491, .012492, .012493, .012494, .012495, .012496, .012497, .012498, .012499, .012500, .012501, .012502, .012503, .012504, .012505, .012506, .012507, .012508, .012509, .012510, .012511, .012512, .012513, .012514, .012515, .012516, .012517, .012518, .012519, .012520, .012521, .012522, .012523, .012524, .012525, .012526, .012527, .012528, .012529, .012530, .012531, .012532, .012533, .012534, .012535, .012536, .012537, .012538, .012539, .012540, .012541, .012542, .012543, .012544, .012545, .012546, .012547, .012548, .012549, .012550, .012551, .012552, .012553, .012554, .012555, .012556, .012557, .012558, .012559, .012560, .012561, .012562, .012563, .012564, .012565, .012566, .012567, .012568, .012569, .012570, .012571, .012572, .012573, .012574, .012575, .012576, .012577, .012578, .012579, .012580, .012581, .012582, .012583, .012584, .012585, .012586, .012587, .012588, .012589, .012590, .012591, .012592, .012593, .012594, .012595, .012596, .012597, .012598, .012599, .0125100, .0125101, .0125102, .0125103, .0125104, .0125105, .0125106, .0125107, .0125108, .0125109, .0125110, .0125111, .0125112, .0125113, .0125114, .0125115, .0125116, .0125117, .0125118, .0125119, .0125120, .0125121, .0125122, .0125123, .0125124, .0125125, .0125126, .0125127, .0125128, .0125129, .0125130, .0125131, .0125132, .0125133, .0125134, .0125135, .0125136, .0125137, .0125138, .0125139, .0125140, .0125141, .0125142, .0125143, .0125144, .0125145, .0125146, .0125147, .0125148, .0125149, .0125150, .0125151, .0125152, .0125153, .0125154, .0125155, .0125156, .0125157, .0125158, .0125159, .0125160, .0125161, .0125162, .0125163, .0125164, .0125165, .0125166, .0125167, .0125168, .0125169, .0125170, .0125171, .0125172, .0125173, .0125174, .0125175, .0125176, .0125177, .0125178, .0125179, .0125180, .0125181, .0125182, .0125183, .0125184, .0125185, .0125186, .0125187, .0125188, .0125189, .0125190, .0125191, .0125192, .0125193, .0125194, .0125195, .0125196, .0125197, .0125198, .0125199, .0125200, .0125201, .0125202, .0125203, .0125204, .0125205, .0125206, .0125207, .0125208, .0125209, .0125210, .0125211, .0125212, .0125213, .0125214, .0125215, .0125216, .0125217, .0125218, .0125219, .0125220, .0125221, .0125222, .0125223, .0125224, .0125225, .0125226, .0125227, .0125228, .0125229, .0125230, .0125231, .0125232, .0125233, .0125234, .0125235, .0125236, .0125237, .0125238, .0125239, .0125240, .0125241, .0125242, .0125243, .0125244, .0125245, .0125246, .0125247, .0125248, .0125249, .0125250, .0125251, .0125252, .0125253, .0125254, .0125255, .0125256, .0125257, .0125258, .0125259, .0125260, .0125261, .0125262, .0125263, .0125264, .0125265, .0125266, .0125267, .0125268, .0125269, .0125270, .0125271, .0125272, .0125273, .0125274, .0125275, .0125276, .0125277, .0125278, .0125279, .0125280, .0125281, .0125282, .0125283, .0125284, .0125285, .0125286, .0125287, .0125288, .0125289, .0125290, .0125291, .0125292, .0125293, .0125294, .0125295, .0125296, .0125297, .0125298, .0125299, .0125300, .0125301, .0125302, .0125303, .0125304, .0125305, .0125306, .0125307, .0125308, .0125309, .0125310, .0125311, .0125312, .0125313, .0125314, .0125315, .0125316, .0125317, .0125318, .0125319, .0125320, .0125321, .0125322, .0125323, .0125324, .0125325, .0125326, .0125327, .0125328, .0125329, .0125330, .0125331, .0125332, .0125333, .0125334, .0125335, .0125336, .0125337, .0125338, .0125339, .0125340, .0125341, .0125342, .0125343, .0125344, .0125345, .0125346, .0125347, .0125348, .0125349, .0125350, .0125351, .0125352, .0125353, .0125354, .0125355, .0125356, .0125357, .0125358, .0125359, .0125360, .0125361, .0125362, .0125363, .0125364, .0125365, .0125366, .0125367, .0125368, .0125369, .0125370, .0125371, .0125372, .0125373, .0125374, .0125375, .0125376, .0125377, .0125378, .0125379, .0125380, .0125381, .0125382, .0125383, .0125384, .0125385, .0125386, .0125387, .0125388, .0125389, .0125390, .0125391, .0125392, .0125393, .0125394, .0125395, .0125396, .0125397, .0125398, .0125399, .0125400, .0125401, .0125402, .0125403, .0125404, .0125405, .0125406, .0125407, .0125408, .0125409, .0125410, .0125411, .0125412, .0125413, .0125414, .0125415, .0125416, .0125417, .0125418, .0125419, .0125420, .0125421, .0125422, .0125423, .0125424, .0125425, .0125426, .0125427, .0125428, .0125429, .0125430, .0125431, .0125432, .0125433, .0125434, .0125435, .0125436, .0125437, .0125438, .0125439, .0125440, .0125441, .0125442, .0125443, .0125444, .0125445, .0125446, .0125447, .0125448, .0125449, .0125450, .0125451, .0125452, .0125453, .0125454, .0125455, .0125456, .0125457, .0125458, .0125459, .0125460, .0125461, .0125462, .0125463, .0125464, .0125465, .0125466, .0125467, .0125468, .0125469, .0125470, .0125471, .0125472, .0125473, .0125474, .0125475, .0125476, .0125477, .0125478, .0125479, .0125480, .0125481, .0125482, .0125483, .0125484, .0125485, .0125486, .0125487, .0125488, .0125489, .0125490, .0125491, .0125492, .0125493, .0125494, .0125495, .0125496, .0125497, .0125498, .0125499, .0125500, .0125501, .0125502, .0125503, .0125504, .0125505, .0125506, .0125507, .0125508, .0125509, .0125510, .0125511, .0125512, .0125513, .0125514, .0125515, .0125516, .0125517, .0125518, .0125519, .0125520, .0125521, .0125522, .0125523, .0125524, .0125525, .0125526, .0125527, .0125528, .0125529, .0125530, .0125531, .0125532, .0125533, .0125534, .0125535, .0125536, .0125537, .0125538, .0125539, .0125540, .0125541, .0125542, .0125543, .0125544, .0125545, .0125546, .0125547, .0125548, .0125549, .0125550, .0125551, .0125552, .0125553, .0125554, .0125555, .0125556, .0125557, .0125558, .0125559, .0125550, .0125551, .0125552, .0125553, .0125554, .0125555, .0125556, .0125557, .0125558, .0125559, .0125560, .0125561, .0125562, .0125563, .01255

## Hiding Partitions (5 of 5)

Select	File Name	File Extension	Size	Attributes	Deleted	Created Date	Mod
	g4mMetadata		0 by...	- - - - d - ...	NO	06/05/2014 ...	06/0
	gObjId		0 by...	- - - - 3 - ...	NO	06/05/2014 ...	06/0
	gObj		0 by...	- - - - 3 - ...	NO	06/05/2014 ...	06/0
	gParse		0 by...	- - - - 8 - ...	NO	06/05/2014 ...	06/0
	StusInfo		0 by...	- - - - 8 - ...	NO	06/05/2014 ...	06/0
	StusInfo-\$1		16,504 ...	- - A0S - -	NO	06/05/2014 ...	06/0
	StusInfo-\$Max		32 b...	- - A0S - -	NO	06/05/2014 ...	06/0

**Figure 9-11** Viewing a hidden partition in ProDiscover  
Courtesy of Technology Pathways, LLC

43

## 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
  - Type B in the FAT entry corresponding to that cluster
  - 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

44



## 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



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

45

45



## Bit-Shifting (2 of 4)

Offset	0 1 2 3 4 5 6 7 8 9 A B C D E F	ANSI ASCII
00000000	E4 45 53 54 20 46 69 6C 65 0D 0A 54 65 73 74 20	TEST File Test
00000010	E4 69 6C 65 20 69 73 20 74 4F 20 73 65 65 20 68	file is to see h
00000020	6F 77 20 73 68 69 64 74 69 6E 47 20 42 69 74 73	file shifting bits
00000030	20 69 6E 47 20 42 69 74 73 69 6E 47 20 42 69 74 73	with alittle help
00000040	E4 63 74 63 20 69 6E 20 61 20 66 69 6C 65 3E	data in a file.

Page 1 of 1 | Offset: 0 | = 84 | Block: n/a | Size: n/a

Figure 9-19 Bit\_shift.txt open in WinHex

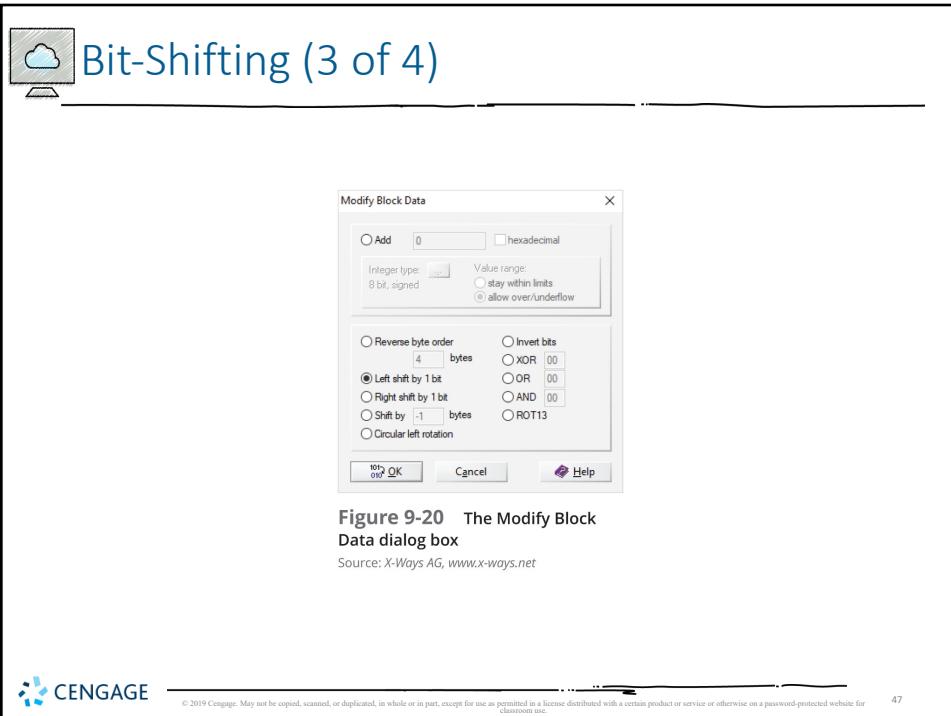
Source: X-Ways AG, [www.x-ways.net](http://www.x-ways.net)



© 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.

46

46

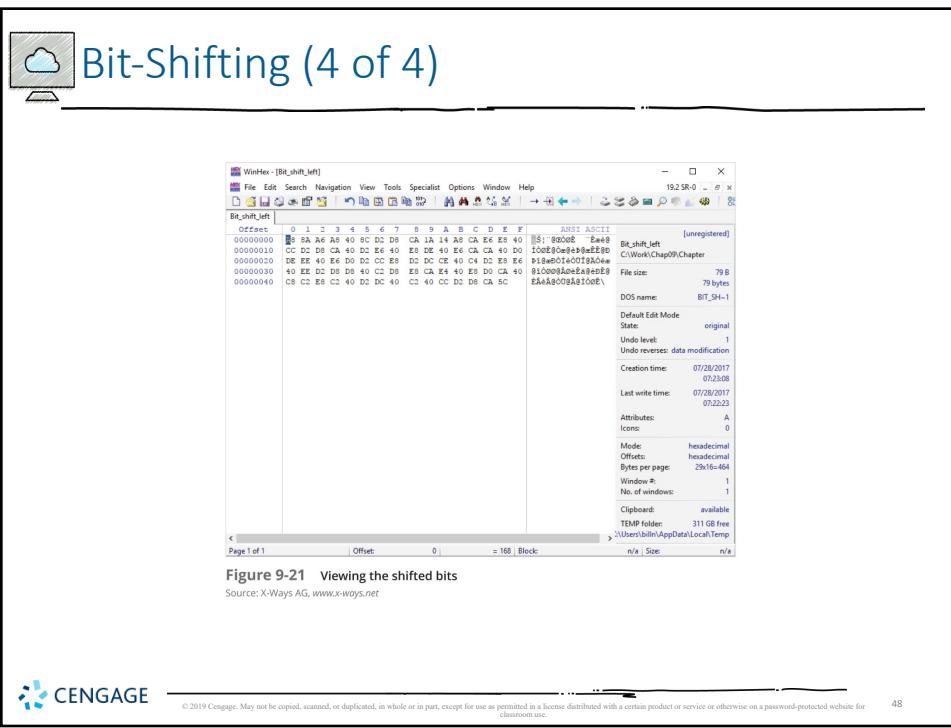


**Figure 9-20** The Modify Block Data dialog box

Source: X-Ways AG, [www.x-ways.net](http://www.x-ways.net)

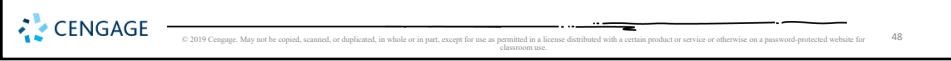


47



**Figure 9-21** Viewing the shifted bits

Source: X-Ways AG, [www.x-ways.net](http://www.x-ways.net)



48



## 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



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

49

49



## 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



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

50

50



## Understanding Steganalysis Methods (3 of 3)

- Steganalysis methods
  - Stego-only attack
    - Only have suspected steganography file to analyze
  - Known cover attack
    - Cover-media: original file, no hidden message
    - Stego-media: converted file that stores hidden message
  - Known message attack
    - Hidden message known
  - Chosen stego attack
    - Used when known steganography tool used to hide data
  - Chosen message attack
    - Create stego-media to identify patterns



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

51

51



## 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



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

52

52



## Recovering Passwords (1 of 6)

- 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



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

53



## Recovering Passwords (2 of 6)

- 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

### DICTIONARY ATTACK!



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

54

54



## Recovering Passwords (3 of 6)

- 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



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

55

55



## Recovering Passwords (4 of 6)

- **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
    - User-specific component joined to an encrypted password to distinguish identical passwords
    - Joined to password before combination concealed



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

56

56



## Recovering Passwords (4 of 6)

- Rainbow table

**TABLE 2-2** Sample Password Table

Identity	Password
Jane	qwerty
Pat	aaaaaa
Phillip	oct31witch
Roz	aaaaaa
Herman	guessme
Claire	aq3wm\$oto!4

**TABLE 2-3** Sample Password Table with Concealed Password Values

Identity	Password
Jane	0x471aa2d2
Pat	0x13b9c32f
Phillip	0x01c142be
Roz	0x13b9c32f
Herman	0x5202aac2
Claire	0x488b8c27

**TABLE 2-4** Sample Rainbow Table for Common Passwords

Original Password	Encrypted Password
asdfg	0x023c94fc
p@55w0rd	0x04ff38d9
aaaaaa	0x13b9c32f
password	0x2129f30d
qwerty	0x471aa2d2
12345678	0x4f2c4dd8
123456	0x5903c34d
aaaaa	0x8384a8c8
etc.	



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

57



## Recovering Passwords (4 of 6)

- Salted Passwords

Sample Password Table with Personalized Concealed Password Values

Identity	ID+password (not stored in table)	Stored Authentication Value
Jane	Jan+qwerty	0x1d46c346
Pat	Pat+aaaaaa	0x2d5d3e44
Phillip	Phi+oct31witch	0xc23c04d8
Roz	Roz+aaaaaa	0xe30f4d27
Herman	Herm+guessme	0x8127f48d
Claire	Cla+aq3wm\$oto!4	0x5209d942



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

58

58



## 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.

59



## 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.

60

# Guide to Computer Forensics and Investigations

## Sixth Edition

### Chapter 10

#### *Virtual Machine Forensics, Live Acquisitions, and Network Forensics*

CENGAGE



1



### 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.

2

2



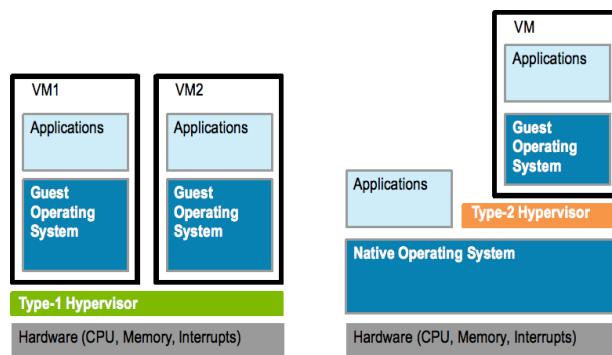
## An Overview of Virtual Machine Forensics (1 of 2)

- 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



## An Overview of Virtual Machine Forensics (2 of 2)

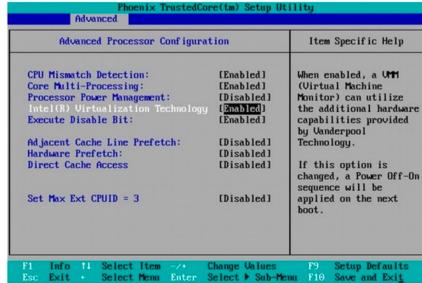
- Type 2 hypervisors are usually the ones you find loaded on a suspect machine
- Type 1 hypervisors are typically loaded on servers or workstations with a lot of RAM and storage





## Type 2 Hypervisors (1 of 5)

- 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



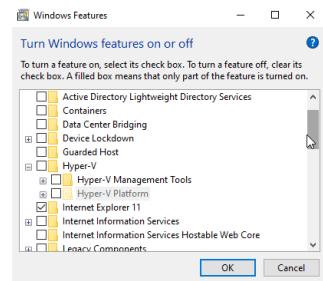
© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

5



## Type 2 Hypervisors (2 of 5)

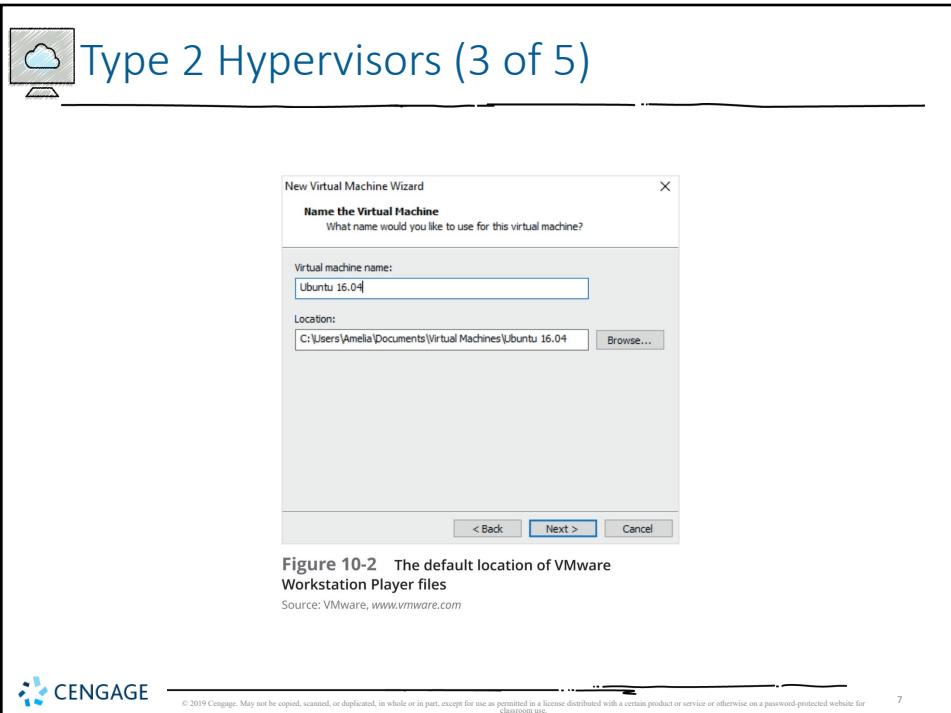
- Most widely used type 2 hypervisors:
  - Parallels Desktop - created for Macintosh users who also use Windows applications
  - KVM (Kernel-based Virtual Machine) - for Linux OS
  - Microsoft Hyper-V - new hypervisor built into Windows 10
  - VMware Workstation and Player - can be installed on almost 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 VMs



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

6

6



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

7

The screenshot shows the 'New Virtual Machine Wizard' window. The title bar says 'Name the Virtual Machine'. The main area has a sub-section titled 'Name the Virtual Machine' with the sub-instruction 'What name would you like to use for this virtual machine?'. Below this, there is a 'Virtual machine name:' field containing 'Ubuntu 16.04' and a 'Location:' field showing the path 'C:\Users\Amelia\Documents\Virtual Machines\Ubuntu 16.04'. At the bottom of the window are buttons for '< Back', 'Next >', and 'Cancel'.

**Figure 10-2** The default location of VMware Workstation Player files  
Source: VMware, [www.vmware.com](http://www.vmware.com)

**Table 10-1** Files associated with VMware

File extension	Description
.vmx	Stores configuration files
.log	Contains logs of information such as when a VM was powered off, virtual appliances added, and so on
.nvram	Keeps track of the state of a VM's BIOS
.vmdk	Stores the virtual hard drive's contents
.vmem	Stores VM paging files, which serve as RAM
.vmsd	Contains information about snapshots

Source: VMware, [www.vmware.com](http://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.

8



## Type 2 Hypervisors (5 of 5)

- 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.

9

9



## Conducting an Investigation with Type 2 Hypervisors (1 of 10)

- 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
    - Registry HKEY\_CLASSES\_ROOT shows file extensions .VMX or .VMC registered
  - 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.

10

10



## Conducting an Investigation with Type 2 Hypervisors (2 of 10)

**Ethernet**

Find a setting

Network & Internet

Status

Ethernet

Dial-up

VPN

Airplane mode

Mobile hotspot

Data usage

Proxy

VMware Network Adapter VMnet8  
No Internet

VMware Network Adapter VMnet1  
No Internet

Related settings

Change adapter options

Change advanced sharing options

Network and Sharing Center

HomeGroup

Windows Firewall

Have a question?

Get help

**Figure 10-7** Ethernet Connections on a Windows 10 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.

11



## Conducting an Investigation with Type 2 Hypervisors (3 of 10)

Registry Editor

Name	Type	Data
(Default)	REG_SZ	(value not set)
AdminUI	REG_SZ	1
CompanyName	REG_SZ	CCSF-home
Cpt	REG_SZ	COPWRIGHT (c) VMware, Inc. 1999-2009
Data	REG_SZ	MaxCpusPerVm=4&mdate=2009-04-14
DataHash	REG_SZ	ebd636f4-63c678f0-76b1c4af-cc68d116-44102a7c
Epoch	REG_SZ	2009-04-01
Field2	REG_SZ	AdminUI.Option.Epoch
Hash	REG_SZ	efcf905a-9c0e791d-76667874-cebbc433-baa59f0c
LastModified	REG_SZ	2010-10-29 @ 21:40:42 UTC
LicenseEdition	REG_SZ	ws
LicenseType	REG_SZ	User
LicenseVersion	REG_SZ	7.0
Name	REG_SZ	Sam
Option	REG_SZ	3
ProductID	REG_SZ	VMware Workstation
Serial	REG_SZ	HM484-VH02-18F3E-0U1OK-ADT3Q
StartFields	REG_SZ	Cpt, ProductID, LicenseVersion, LicenseType, Licen...

Computer\HKEY\_LOCAL\_MACHINE\SOFTWARE\VMware, Inc.\VMware Workstation\License.ws.7.0.e1.200904

- Retained even if VMware is uninstalled

**CENGAGE**

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

12

## Conducting an Investigation with Type 2 Hypervisors (4 of 10)

- 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



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

13

13

## Conducting an Investigation with Type 2 Hypervisors (5 of 10)

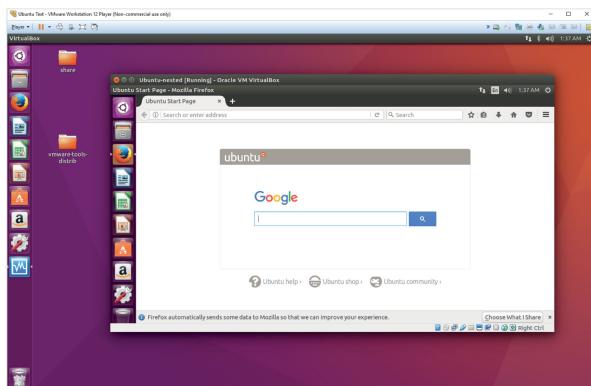


Figure 10-9 A VM nested inside another VM

Source: VMware, [www.vmware.com](http://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.

14

14



## Conducting an Investigation with Type 2 Hypervisors (6 of 10)

- 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



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

15



## Conducting an Investigation with Type 2 Hypervisors (7 of 10)

- 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



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

16

16



## Conducting an Investigation with Type 2 Hypervisors (8 of 10)

- 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



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

17



## Conducting an Investigation with Type 2 Hypervisors (9 of 10)

- 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



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

18

18



## Conducting an Investigation with Type 2 Hypervisors (10 of 10)

- 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



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

19

19



## 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



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

20

20



## 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.

21



## 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



CENGAGE

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

22



## 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
  - Search for rootkits, check firmware, image the drive over network, or shut down for later static acquisition
- Be sure to get a forensic digital hash value of all files you recover during the live acquisition



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

23

23



## 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



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

24

24



## 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



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

25

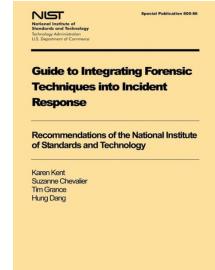
25



## 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

<https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf>



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

26

26



## Securing a Network (1 of 2)

- Applying the latest patches
- **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 (hiring, treatment, and training)
    - Technology (strong network architecture, right tools)
    - Operations (patches, updates)



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

27

27



## 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

*"The largest theft of data in CIA history happened because a specialized unit within the agency was so focused on building cyber weapons that an employee took advantage of "woefully lax" security and gave secret hacking tools to WikiLeaks, according to an internal report released on Tuesday."*

June 16, 2020



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

28

28



## 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



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

29

29



## 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
    - E.g., intruders might have transmitted a Trojan program that gives them access to the system and then installed a rootkit
- Work on an isolated system
  - Prevents **malware** from affecting other systems



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

30

30



## 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.

31

31



## Using Network Tools

- Variety of tools
  - Splunk
  - Spiceworks
  - Nagios
  - Cacti



CENGAGE

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

32

32



## 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 (command-line packet capture)
  - Tethereal (command-line version of Ethereal)



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

33

33



## Using Packet Analyzers (2 of 5)

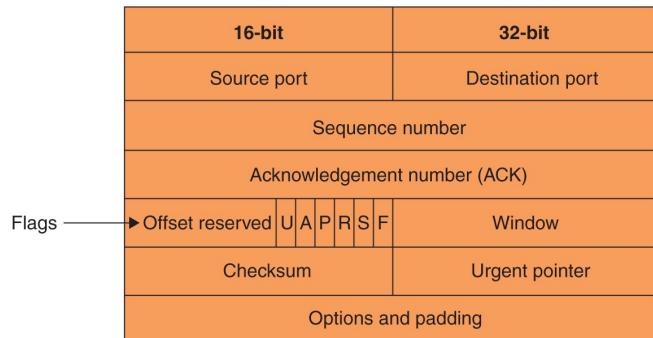


Figure 10-15 A TCP header



© 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.

34

34

 Using Packet Analyzers (3 of 5)

- Tools (cont'd)
  - Tcpsplice
    - Extracts data from 1 or more tcpdump files by time frame
  - Tcpreplay (replays packets)
  - Etherape (views network traffic graphically)
  - Netdude (GUI tool to analyze pcap files)
  - Argus (analyzes packet flows)
  - Wireshark (open source packet analyzer)
    - Follow the steps starting on page 442 to see how the Wireshark tool works

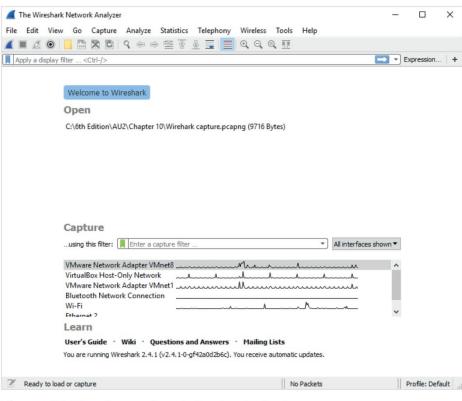


 © 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

35

35

 Using Packet Analyzers (4 of 5)



The screenshot shows the Wireshark Network Analyzer window. At the top, there's a menu bar with File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with icons for opening files, saving, zooming, and filtering. A search bar says "Enter a display filter: <ctrl-f>". The main area is titled "Welcome to Wireshark" and shows a file named "C:\6th Edition\AU2\Chapter 10\Wireshark capture.pcapng (9716 Bytes)". Below this, there's a "Capture" section with a dropdown menu set to "All interfaces shown". It lists several network interfaces: "VMware Network Adapter VMnet8", "VirtualBox Host-Only Network", "VMware Network Adapter VMnet1", "Bluetooth Network Connection", "Wi-Fi", and "Infrared". At the bottom of the window, there are links for "User's Guide", "Wiki", "Questions and Answers", and "Mailing Lists". It also indicates that "You are running Wireshark 2.4.1 (v2.4.1-0-gf420c296). You receive automatic updates." The status bar at the bottom shows "Ready to load or capture.", "No Packets", and "Profile: Default".

**Figure 10-16** The opening window in Wireshark  
Source: Wireshark Foundation, [www.wireshark.org](http://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.

36

36

The screenshot shows a Windows desktop with a Wireshark window titled "Wireshark - Follow UDP Stream (udp.stream eq 0) - wireshark\_F271C7...". The main pane displays several captured network packets, all of which are NOTIFY messages. These messages have the following headers:

- NOTIFY \* HTTP/1.1
- Host: 239.255.255.250:1900
- Cache-Control: max-age=4
- Location: 192.168.175.1:57797
- NT: uid:4E59846A-B607-4ECB-9676-8DC10ABEBASF
- NTS: ssdp:alive
- SERVER: windows/6.2 IntelUSBoverIP:1/1
- USN: uuid:4E59846A-B607-4ECB-9676-8DC10ABEBASF::IntelUSBoverIP:1

The bottom of the Wireshark window shows a toolbar with buttons for "Find Next", "Print", "Save as...", "Back", and "Close".

**Figure 10-17 Following a UDP stream**  
Source: Wireshark Foundation, [www.wireshark.org](http://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.

37

## Investigating Virtual Networks

- Virtual switch is a little different from a physical switch
  - A software application that allows communication between virtual machines
  - 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

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

38

38



## 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



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

39

39



## 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



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

40

40



## 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.

41

41



## 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.

42

42



## 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.

43

# Guide to Computer Forensics and Investigations

## Sixth Edition

### Chapter 11

#### *E-mail and Social Media Investigations*



CENGAGE

1



### 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.

2

2



## 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



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

3

3



## 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
  - In response to rampant spam on SMTP, an extension for SMTP was released in 1995, which was extended SMTP (ESMTP for short).
  - ESMTP follows the same protocols as SMTP, but adds more functionality, security, and authentication



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

4

4



## 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



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

5



## Exploring the Roles of the Client and Server in E-mail (2 of 3)

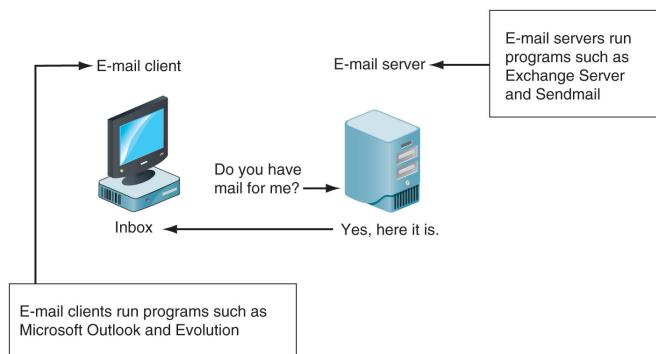


Figure 11-1 E-mail in a client/server architecture



© 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.

6

6



## 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



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

7

7



## 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.
    - When applied to information stored online, Fourth Amendment's protections are potentially far weaker because it defines "right to be secure" in spatial terms that do not directly apply to "reasonable expectation of privacy" in an online context
    - Users generally entrust the security of online information to a third party, such as an ISP. Fourth Amendment doctrine has held that in doing so, users relinquish any expectation of privacy.



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

8

8



## 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.

9



## 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.

10

10



## 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



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

11

11



## 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



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

12

12



## 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



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

13



## Viewing E-mail Headers (2 of 5)

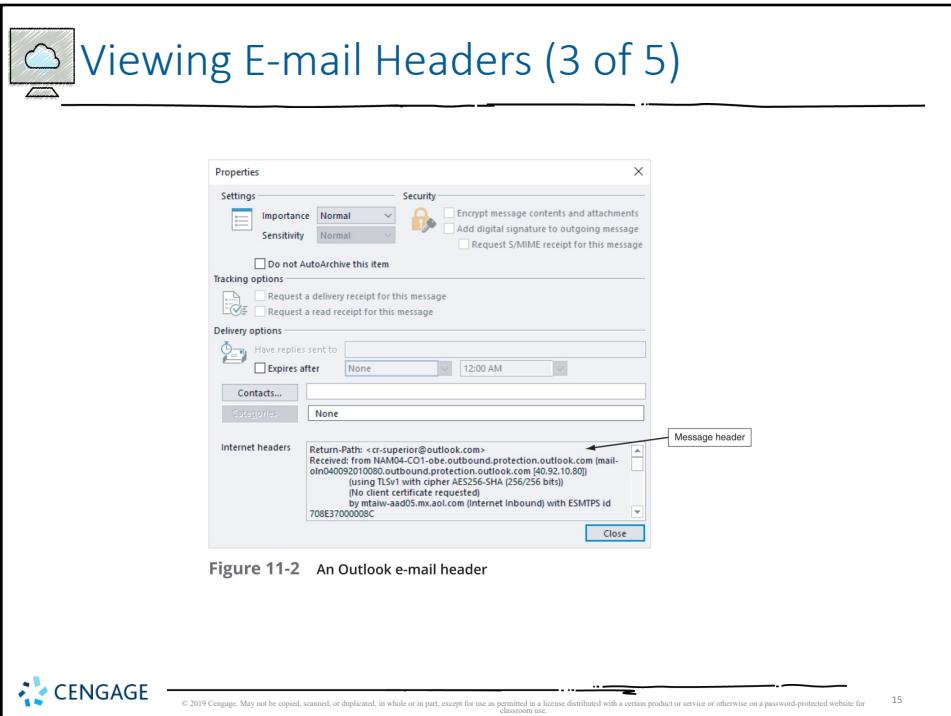
- Outlook
  - Double-click the message and then click **File, Properties**
  - Copy headers
  - Paste them to any text editor
  - Save the document as `Outlook header.txt` in your work folder



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

14

14



15

## 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.

16

16

**Figure 11-3** Viewing headers in Yahoo!

Source: Yahoo! Inc., [www.yahoo.com](http://www.yahoo.com)



# 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)

© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except 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: ccr-superior@outlook.com
2. Received: from NAM04-C01-obe.outbound.protection.outlook.com (mail-oln040092010080.outbound.protection.out
   (using TLSv1 with cipher AES256-SHA (256/256 bits))
   (No client certificate requested)
   by mtalv-aad95.mx.ao1.com (Internet Inbound) with ESMTPS id 708E37000000C
   for cb_aspen@ao1.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=rZl0oDU-St47+5BKeKvYzkl8429x4SpnNS+elR6fc;
b=galyKgShnAUxF2Rxw1P99nJSSA+Uovdar6361aQ0ng2y66ARNh3tKglXdgpuofk8mH5UTZjYdRJx4q25n2WYf8o1bQ7h38Gb

4. Received: from SNINAM04HT054.eop-NAM04.prod.protection.outlook.com (10.152.88.54) by
SNINAM04HT054.mail.protection.outlook.com (10.152.89.2) 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 DMRP14MB1033.namprd14.prod.outlook.com ([10.152.88.60]) by
SNINAM04HT054.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 DMRP14MB1033.namprd14.prod.outlook.com ([10.166.159.17]) by
DMRP14MB1033.namprd14.prod.outlook.com ([10.166.159.17]) with mapi id
15.01.1240.828; 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.

19

- 
- ## 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
- 
- © 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.
- 20



## 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](http://www.arin.net)
    - American Registry for Internet Numbers to map IP address to a domain name
  - [www.internic.com](http://www.internic.com)
    - Find a domain's IP address and point of contact
  - [www.google.com](http://www.google.com)
    - Use search engine to look for more information and additional postings on discussion boards
- Verify your findings by checking network e-mail logs against e-mail addresses



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

21

21



## 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

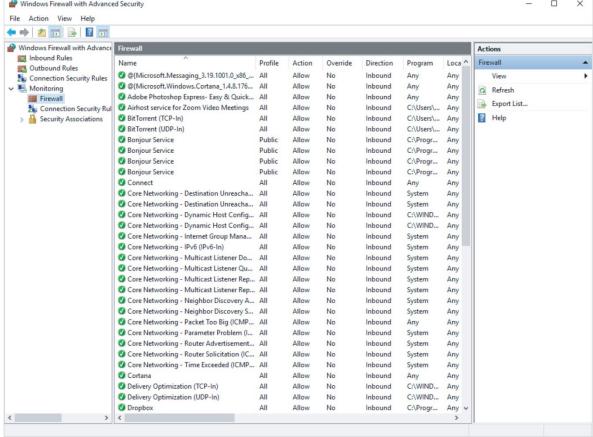


© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

22

22

## Using Network E-mail Logs (2 of 2)



The screenshot shows the Windows Firewall with Advanced Security window. The left navigation pane includes options like Firewall, Outbound Rules, Connection Security Rule, Monitoring, Firewall, and Connection Security Rule. The main area is titled 'Firewall' and lists numerous rules. Each rule entry includes columns for Name, Profile, Action, Override, Direction, Program, and Location. Most rules are categorized under 'Core Networking' or 'Windows Firewall'. A context menu is open over one of the entries, showing options like View, Refresh, Export List..., and Help.

Figure 11-5 A Windows firewall 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.

23

## 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.

24

24



## 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.

25



## 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.

26

26



## 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.

27

27



## 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.

28

28



## 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.

29



CENGAGE

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

30



## Examining Microsoft E-mail Server Logs (4 of 4)

The screenshot shows the Windows Event Viewer interface. The left pane displays a tree view of log types: Event Viewer (Local), Custom Views, Windows Logs, Application, Security, Setup, System, Forwarded Events, Applications and Services Log, Hardware Events, Internet Explorer, Kaspersky Event Log, Key Management Service, Microsoft, Microsoft Office Alerts, and Windows PowerShell. The right pane shows a list of events under the Application category. A specific event is selected, and its details are shown in the bottom pane. The event details include:

Date and Time	Source	Event ID	Task Category
9/11/2017 4:11:37 PM	Security-SPP	1003	None
9/11/2017 4:11:07 PM	Security-SPP	1003	None
9/11/2017 4:11:06 PM	Security-SPP	1003	None
9/11/2017 4:11:06 PM	Security-SPP	1003	None
9/11/2017 4:05:26 PM	Security-SPP	16384	None
9/11/2017 4:04:59 PM	Outlook	38	None
9/11/2017 4:04:56 PM	Security-SPP	1003	None
9/11/2017 4:04:55 PM	Security-SPP	1003	None
9/11/2017 4:04:55 PM	Outlook	30	None
9/11/2017 4:04:55 PM	Outlook	32	None
9/11/2017 4:04:55 PM	Outlook	45	None
9/11/2017 4:04:54 PM	Outlook	32	None
9/11/2017 4:02:53 PM	Security-SPP	16384	None

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.

31



## 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 formats 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



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

32

32



## 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



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

33

33



## 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 emails the suspect has deleted and restore them to their original state



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

34

34



## 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.

35

35



## Using OSForensics to Recover E-mail (2 of 2)

The screenshot shows the Magnet AXIOM Process software interface. The main window title is "Magnet AXIOM Process 1.2.0.6464". The left sidebar has sections for "CASE DETAILS", "EVIDENCE SOURCES", "PROCESSING DETAILS", "ARTIFACT DETAILS", and "ANALYZE EVIDENCE". The right panel is titled "CASE DETAILS" and contains several input fields:

- CASE INFORMATION:** Case number: IntChapter11; Location for case files: Folder name: IntChapter11; File path: C:\Work\Chapter11\IntChapter11; Available space: 262.11 GB.
- LOCATION FOR ACQUIRED EVIDENCE:** Folder name: IntChapter11; File path: C:\Work\Chapter11\IntChapter11; Available space: 262.11 GB.
- SCAN INFORMATION:** SCAN 1; Created on: 10/5/2017 2:11:53 AM; Scanned by: [empty]; Description: [empty].

A "GO TO EVIDENCE SOURCES" button is at the bottom right of the panel.

Figure 11-7 Entering information in the CASE DETAILS window

Source: Magnet Forensics, [www.magnetforensics.com](http://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.

36

36

## 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



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

37

37

## 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.

**Figure 11-10** WinHex



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

38

38

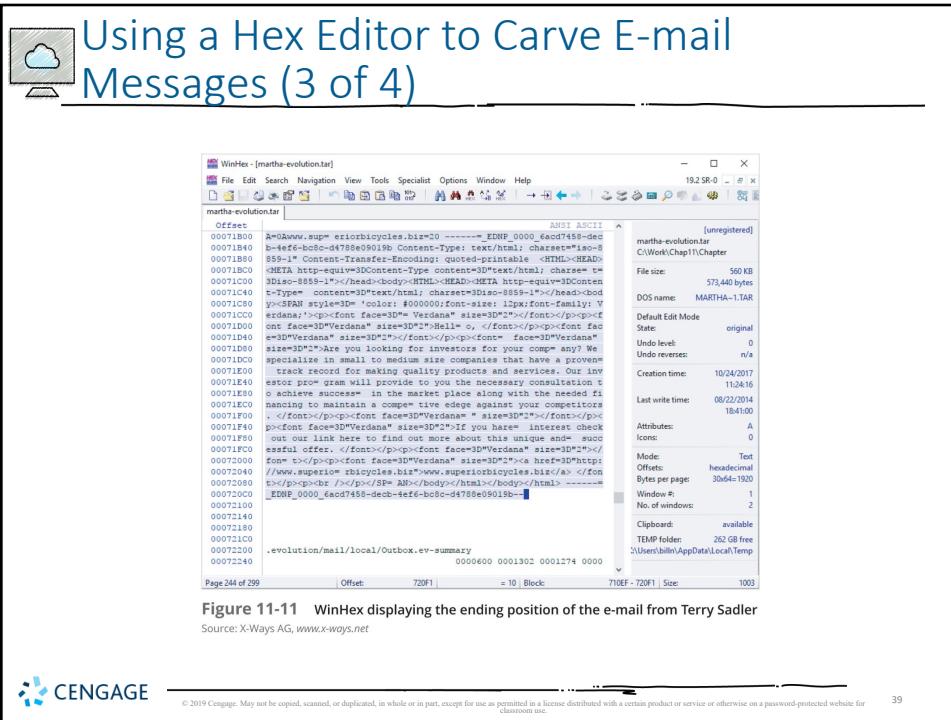


Figure 11-11 WinHex displaying the ending position of the e-mail from Terry Sadler

Source: X-Ways AG, [www.x-ways.net](http://www.x-ways.net)

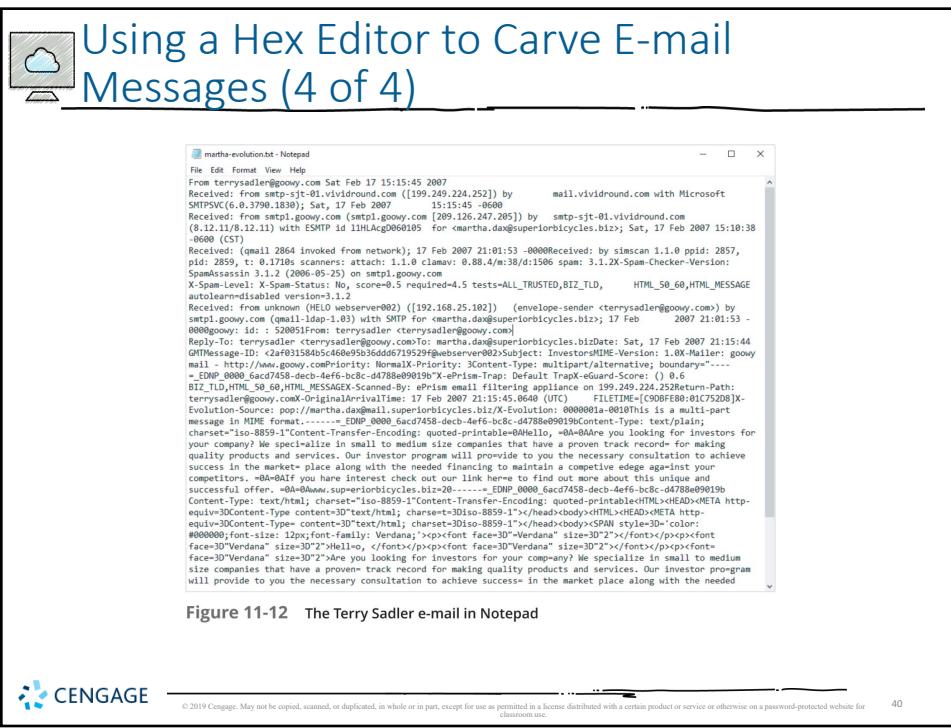
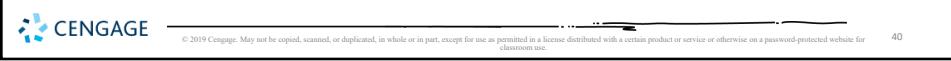


Figure 11-12 The Terry Sadler e-mail in Notepad





## 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.

41

41



## 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 recover 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.

42

42



## 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.

43



## 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.

44

44



## 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



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

45

45



## 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



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

46

46



## 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



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

47



## 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



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

48

48



## 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



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

49

49



## 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



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

50

50

# Guide to Computer Forensics and Investigations

## Sixth Edition

### Chapter 12

#### *Mobile Device Forensics and the Internet of Anything*



CENGAGE

1



### 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.

2

2



## 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.

3

3



## 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

What about Apps  
and App 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.

4

4



## 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.

5



## Mobile Phone Basics (1 of 9)

- 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.

6

6



## Mobile Phone Basics (2 of 9)

Table 12-1 Digital networks

Digital network	Description
Code Division Multiple Access (CDMA)	Developed during World War II, this technology was patented by Qualcomm after the war. One of the most common digital networks, it uses the full radio frequency spectrum to define channels. In the United States, Sprint, U.S. Cellular, and Verizon, for example, use CDMA networks.
Global System for Mobile Communications (GSM)	Another common digital network, it's used by AT&T and T-Mobile in the United States and is the standard in Europe and Asia.
Time Division Multiple Access (TDMA)	This digital network uses the technique of dividing a radio frequency into time slots; GSM networks use this technique. It also refers to a specific cellular network standard covered by Interim Standard (IS) 136.
Integrated Digital Enhanced Network (IDEN)	This Motorola protocol combines several services, including data transmission, into one network.
Digital Advanced Mobile Phone Service (D-AMPS)	This network is a digital version of the original analog standard for cell phones.
Digital network	Description
Enhanced Data GSM Environment (EDGE)	This digital network, a faster version of GSM, is designed to deliver data.
Orthogonal Frequency Division Multiplexing (OFDM)	This technology for 4G networks uses energy more efficiently than 3G networks and is more immune to interference.

© 2016 Cengage Learning®

7



CENGAGE

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

7



## Mobile Phone Basics (3 of 9)

- 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

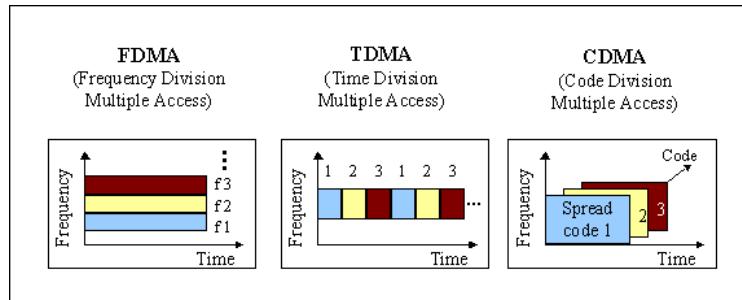
© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

8

8



## Mobile Phone Basics (4 of 9)



- **FDMA** private frequency
- **TDMA** specific frequency, but only belongs to the user during certain time slots in repeating sequence
- **CDMA** continuous unique code pattern buried within a shared signal, mingled with other users' code patterns



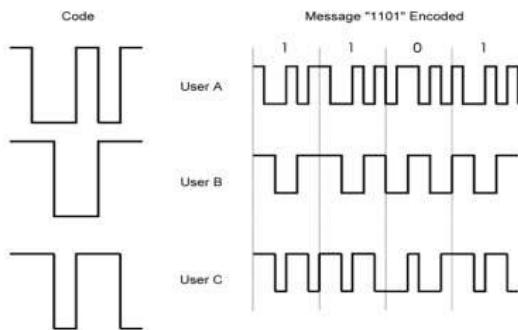
© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

9

9



## Mobile Phone Basics (5 of 9)



- CDMA explained
  - Multiple users connected to the tower with the same radio channel
  - Different users are allocated different code for transmission over the radio channel



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

10

10



## Mobile Phone Basics (6 of 9)

- 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



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

11

11



## Mobile Phone Basics (7 of 9)

- 4G networks can use the following technologies:
  - **Orthogonal Frequency Division Multiplexing (OFDM)**
    - Uses numerous parallel carriers, less susceptible to interference
  - **Mobile WiMAX**
    - Uses IEEE 802.16e standard and OFDMA
  - **Ultra Mobile Broadband (UMB)**
    - Also known as CDMA2000 EV-DO, replaced by LTE
  - **Multiple Input Multiple Output (MIMO)**
    - Used by 4G, WiMAX, and other technologies
  - **Long Term Evolution (LTE)**
    - Commonly called 4G LTE



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

12

12

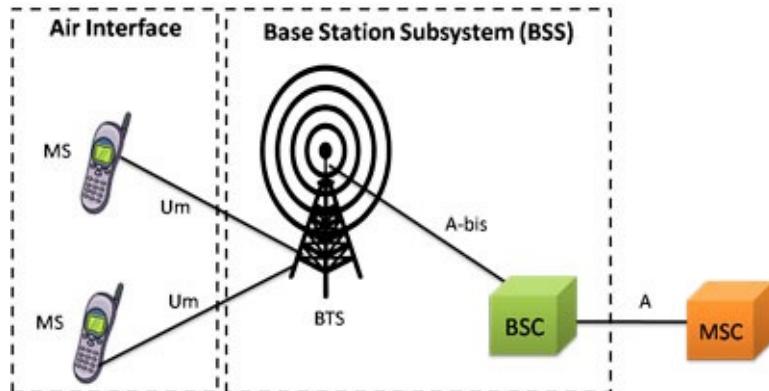


## Mobile Phone Basics (8 of 9)

- Main components used for communication:
  - *Base transceiver station (BTS)*
    - Cell phone tower and associated equipment
  - *Base station controller (BSC)*
    - Hardware & software that controls the BTS
  - *Mobile switching center (MSC)*
    - Routes calls
    - Has a database of subscribers with account and location data



## Mobile Phone Basics (9 of 9)





## 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
    - Maybe a “light” OS 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.

15



## 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.

16

16



## 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)*
    - *Work in much the same way as PCMCIA cards*
  - *MultiMediaCard (MMC)*
  - *Secure Digital (SD)*



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

17

17



## 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



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

18

18



## 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



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

19

19



## 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



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

20

20



## 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



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

21

21



## 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



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

22

22



## 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



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

23

23



## 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



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

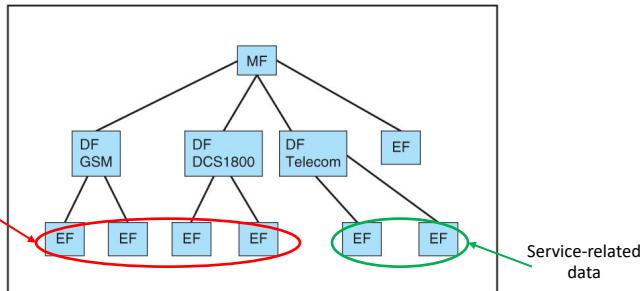
24

24



## Understanding Acquisition Procedures for Mobile Devices (6 of 7)

Network data for different frequency bands of operation



**Figure 12-1** SIM file structure



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

25

25



## 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



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

26

26



## Mobile Forensics Equipment (1 of 7)

- 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



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

27

27



## Mobile Forensics Equipment (2 of 7)

- 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
    - Also be aware the biological agents such as fingerprints may be present on the inside of case
  - 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



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

28

28



## Mobile Forensics Equipment (3 of 7)

- 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



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

29

29



## Mobile Forensics Equipment (4 of 7)

Count	No.	Status	Telephone n...	Message content
	001	message read	123	Welcome to the MTC voicemail service. Please call 123 to retrieve your messages.
	002	message read	123	Your account balance is 60.00. You have lifetime access subject to one chargeable call or
	003	message read	264013358947	Are you still at the hospital?
	004	message read	264013358947	See you there
	005	message read	264013358947	Hey baby, got anything for sale?
	006	message read	264013358947	Working late?
	007	message read	264013358947	Breakfast at 8?
	008	message read	264013358947	Too much to do?
	009	message read	264013358947	Its Friday night. My guys need stuff. Got any?
	010	message read	264013358947	I'm busy
	011	message read	264013358947	I'm back
	012	message read	264013358947	Been in South Africa. Had to see some contacts
	013	message read	264013358947	Ok after I get some sleep
	014	message read	264013358947	Your account has expired. Please recharge within 30 days.
	015	message read	264011906200	

Figure 13-4 Information available in Sim Card Reader



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

30

30



## Mobile Forensics Equipment (5 of 7)

- NIST guidelines list six types of mobile forensics methods:
  - Manual extraction
    - If can't do logical/physical extraction, look at device's content page-by-page and taking pictures
  - Logical extraction
    - File system information extracted with device connected to forensic workstation
  - Physical extraction
    - Forensic copy made so deleted files can be retrieved and other items decoded
  - Hex dumping and Joint Test Action Group (JTAG) extraction
    - Modified boot loader to access RAM for analysis
    - Invasive method to get data from processor, flash memory or other physical components
  - Chip-off
    - Remove flash memory chip and get binary level data
  - Micro read
    - Electron microscope look at logic gates



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

31

31



## Mobile Forensics Equipment (6 of 7)

- 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



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

32

32



## Mobile Forensics Equipment (7 of 7)

- 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.

33

33



## 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

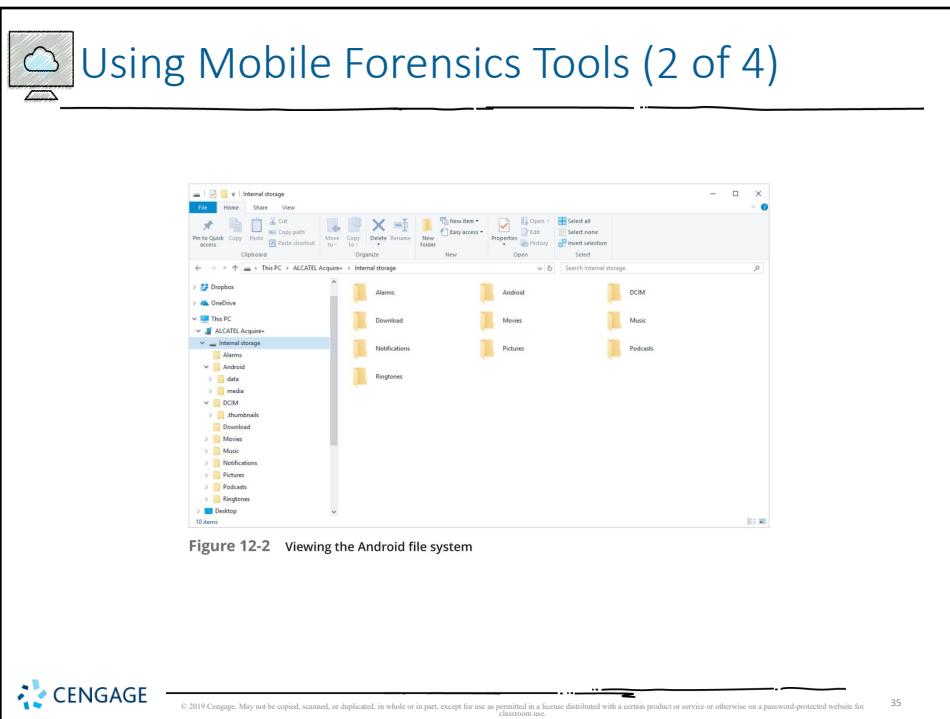


CENGAGE

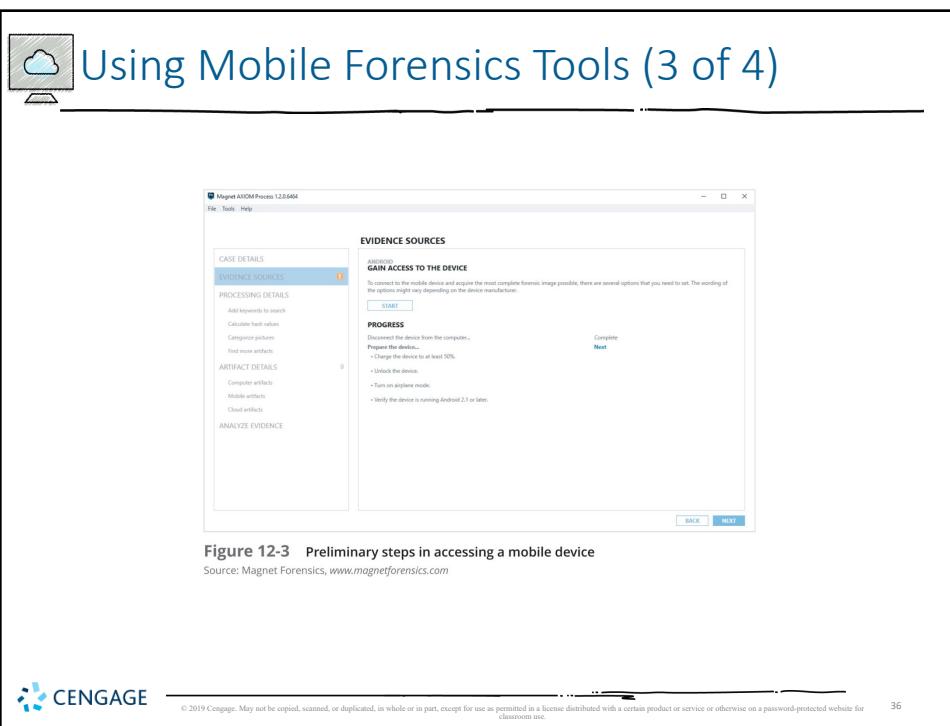
© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

34

34



35



36



## 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



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

37



## 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



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

38

38



## 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)
    - Extension and improvement to existing performance
  - Ultra-reliable and Low-latency Communications (uRLLC)
    - Ideal for mission-critical applications (self-driving cars)
  - massive Machine Type Communications (mMTC)
    - Used to connect large numbers of devices, including IoT



CENGAGE

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

39



## 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.

40

40



## 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



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

41

41



## 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



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

42

42



## 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.

43

# Guide to Computer Forensics and Investigations

## Sixth Edition

### *Chapter 13*

#### *Cloud Forensics*

 CENGAGE



1



## 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.

2

2



## 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.

3

3



## 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.

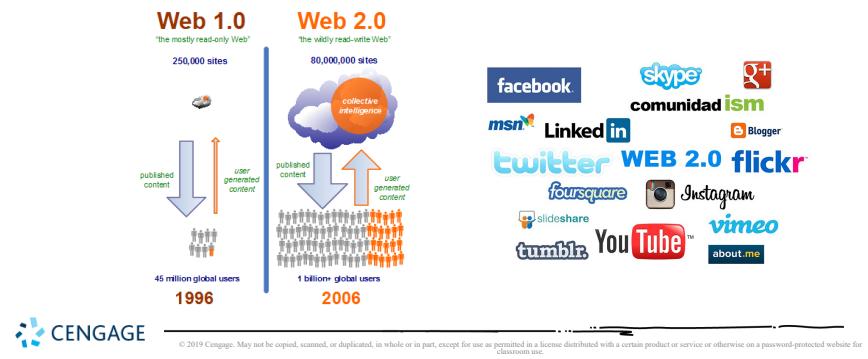
4

4



## 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

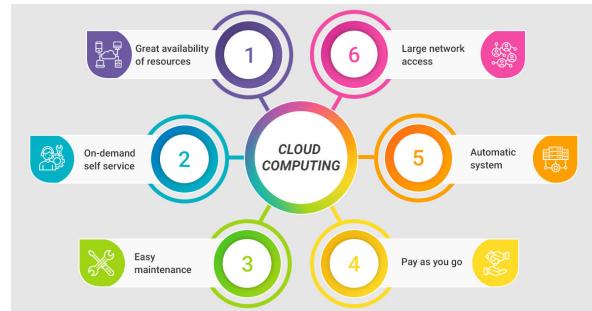


5



## Cloud Service Levels and Deployment Methods (1 of 5)

- 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



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

6

6



## Cloud Service Levels and Deployment Methods (2 of 5)

- 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



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

7



## Cloud Service Levels and Deployment Methods (3 of 5)

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.



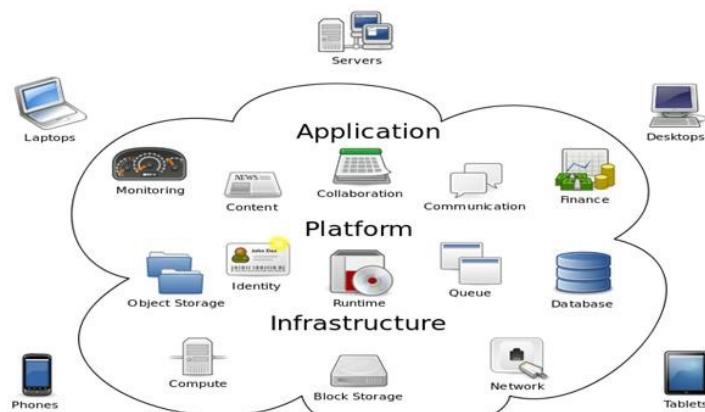
© 2019 Cengage. May not be copied, scanned, or duplicated, in whole or in part, except for use as permitted in a license distributed with a certain product or service or otherwise on a password-protected website for classroom use.

8

8



## Cloud Service Levels and Deployment Methods (4 of 5)



Source: Wikipedia



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

9



## Cloud Service Levels and Deployment Methods (5 of 5)

- 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



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

10

10



## 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



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

11

11



## 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
    - Location, administration
  - 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



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

12

12



## 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
    - Multitenancy
  - *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.

13

13



## 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.

14

14



## 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



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

15

15



## 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



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

16

16



## 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
  - Also multijurisdiction concerns, legal conflicts



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

17

17



## 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



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

18

18



## 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



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

19

19



## 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



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

20

20



## 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.

21

21



## 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.

22

22



## 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.

23

23



## 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.

24

24



## 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



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

25

25



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

26

26



## 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



## 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.

27

27



## 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.

28

28



## 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.

29



## 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.

30



## 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.

31



## 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.

32



## 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.

33

33



## 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 developed resource documentation for CSPs and their staff
  - <https://cloudsecurityalliance.org>



CENGAGE

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

34

34



## 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)<sup>2</sup>'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.

35

35



## 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.

36

36



## 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.

37

37



## 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 systems 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.

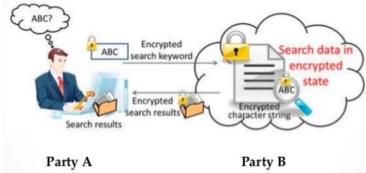
38

38

## 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

**"Homomorphic encryption** is a form of **encryption** that allows computation on ciphertexts, generating an **encrypted** result which, when decrypted, matches the result of the operations as if they had been performed on the plaintext." -- Wikipedia



- **Block chain technology**
    - Used by companies such as Bitcoin, is a way to trace your information while keeping it secure

# 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



## 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.

41

41



## 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.

42

42



## 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.

43



## 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

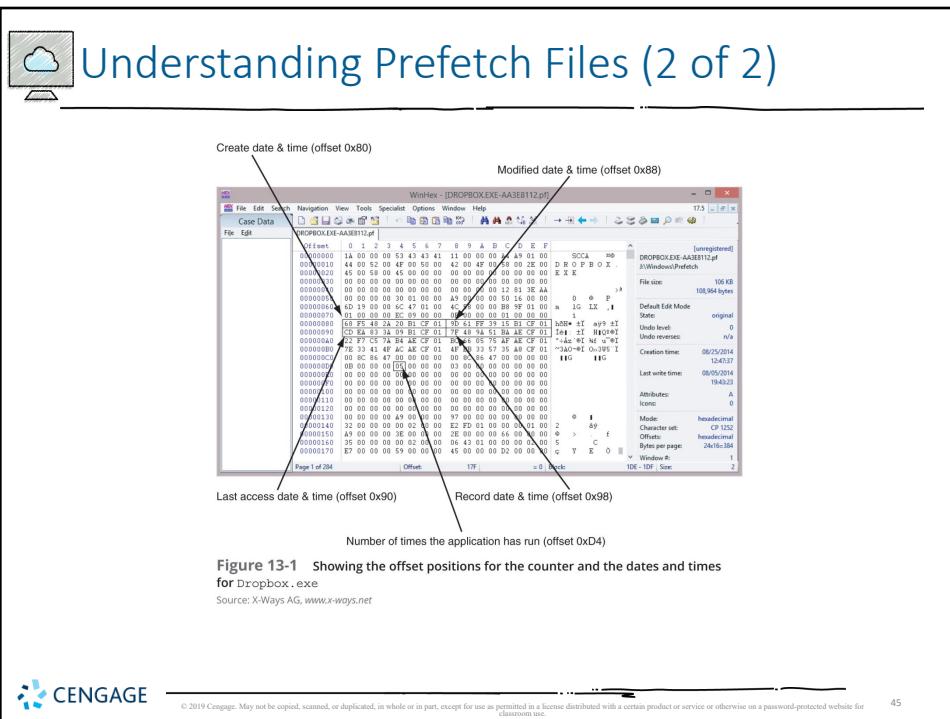


CENGAGE

© 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.

44

44



45

## 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

46



## 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.

47



## 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.

48



## 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



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

49

49



## 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)



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

50

50



## 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



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

51

51



## 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



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

52

52



## 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



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

53



## 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



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

54



## 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



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

55

55



## 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



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

56

56



## 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.

57

57



## 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



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

58

58



## 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.

59



## 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.

60



## 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