

Cyber Forensics

The Fascinating World of Digital Evidence

Digital Forensic Science

- Digital Forensic Science (DFS):

“The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations.”

Source: (2001). Digital Forensic Research Workshop (DFRWS)

Communities

- There at least 3 distinct communities within Digital Forensics
 - Law Enforcement
 - Military
 - Business & Industry
 - Possibly a 4th – Academia

Digital Forensic Science



Community Objectives

Table 1 - Suitability Guidelines for Digital Forensic Research

Area	Primary Objective	Secondary Objective	Environment
Law Enforcement	Prosecution		After the fact
Military IW Operations	Continuity of Operations	Prosecution	Real Time
Business & Industry	Availability of Service	Prosecution	Real Time

Cyber Forensics

- Includes:
 - Networks (Network Forensics)
 - Small Scale Digital Devices
 - Storage Media (Computer forensics)
 - Code Analysis

Cyber Forensics

- The scientific examination and analysis of digital evidence in such a way that the information can be used as evidence in a court of law.

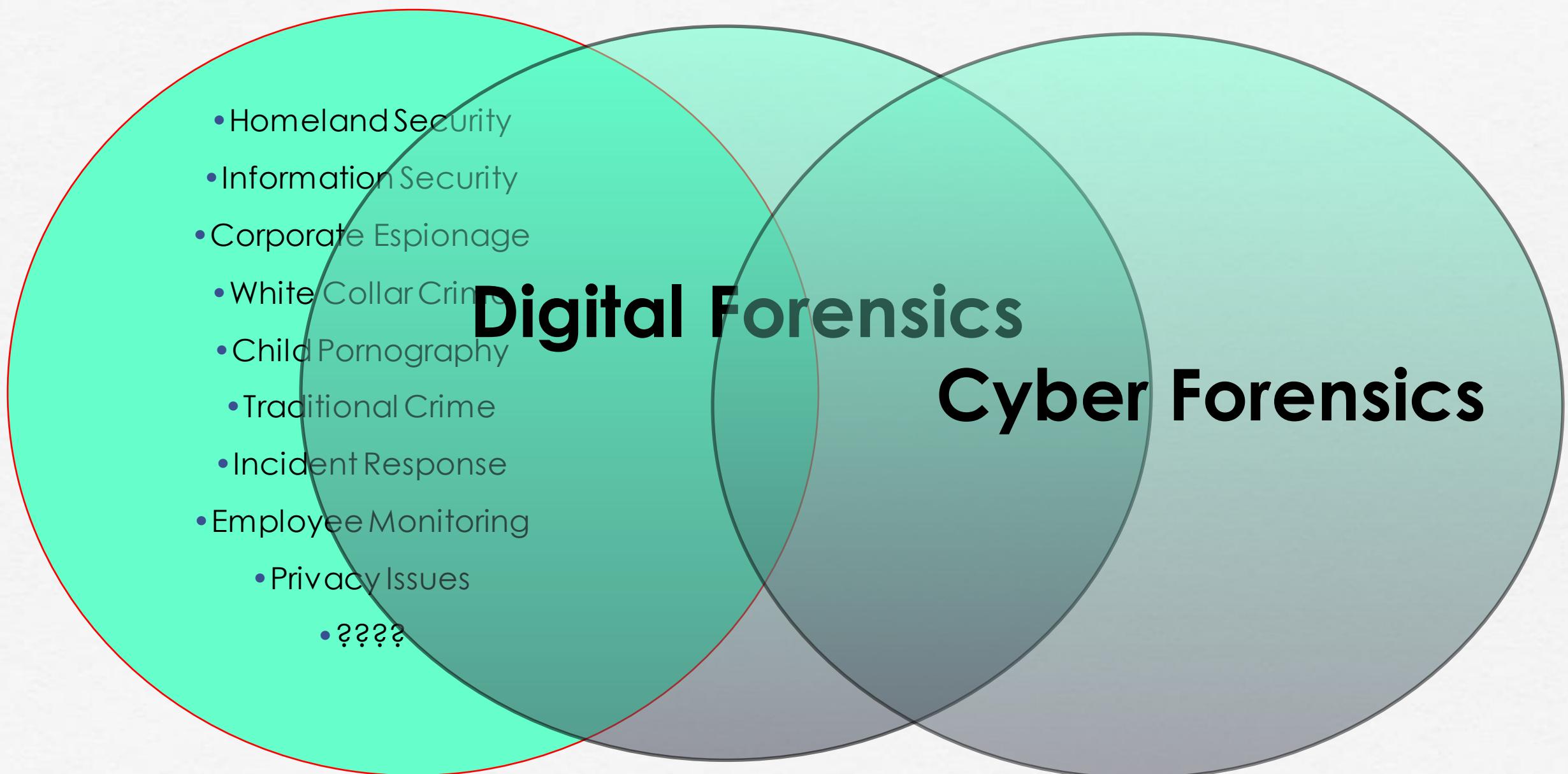
Cyber Forensic Activities

- Cyber forensics activities commonly include:
 - the **secure** collection of computer data
 - the **identification** of suspect data
 - the **examination** of suspect data to determine details such as origin and content
 - the **presentation** of computer-based information to courts of law
 - the **application** of a country's laws to computer practice.

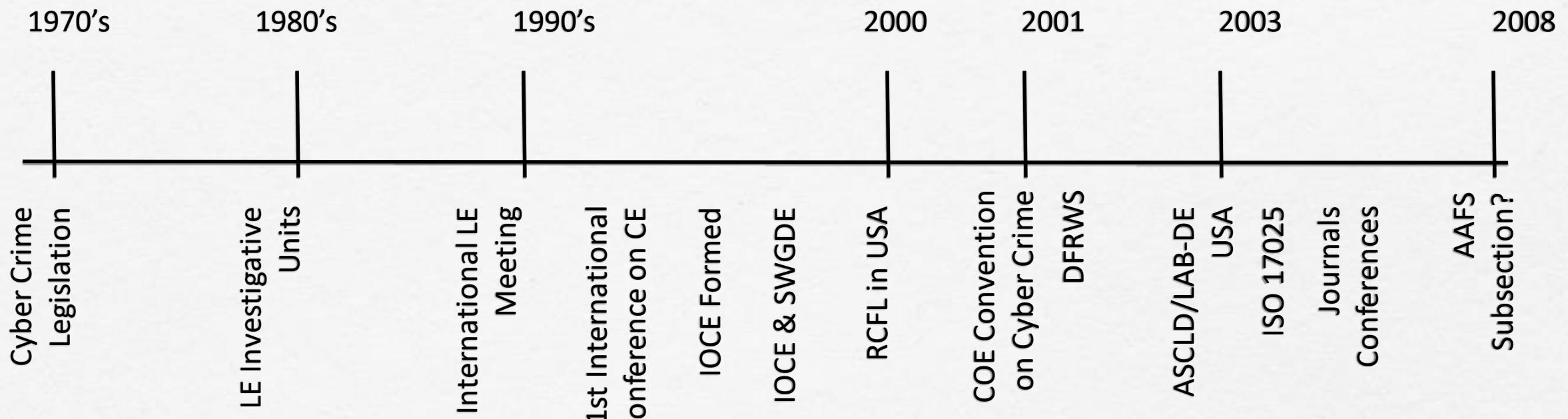
The 3 As

- The basic methodology consists of the 3 As:
 - Acquire* the evidence without altering or damaging the original
 - Authenticate* the image
 - Analyze* the data without modifying it

Context of Cyber Forensics



A Brief Timeline



Crime Scenes

- Physical Crime Scenes vs. Cyber/Digital Crime Scenes
- Overlapping principals
- The basics of criminalistics are constant across both physical and cyber/digital
- Locard's Principle applies
 - “When a person commits a crime something is always left at the scene of the crime that was not present when the person arrived”

Digital Crime Scene

□ Digital Evidence

- Digital data that establish that a crime has been committed, can provide a link between a crime and its victim, or can provide a link between a crime and the perpetrator (Carrier & Spafford, 2003)

□ Digital Crime Scene

- The electronic environment where digital evidence can potentially exist (Rogers, 2005)
- Primary & Secondary Digital Scene(s) as well

Forensic Principles

- Digital/ Electronic evidence is extremely volatile!
- Once the evidence is contaminated it cannot be de-contaminated!
- The courts acceptance is based on the best evidence principle
 - With computer data, printouts or other output readable by sight, and bit stream copies adhere to this principle.
- Chain of Custody is crucial

Cyber Forensic Principles

- **The 6 Principles are:**
 1. When dealing with digital evidence, all of the general forensic and procedural principles must be applied.
 2. Upon seizing digital evidence, actions taken should not change that evidence.
 3. When it is necessary for a person to access original digital evidence, that person should be trained for the purpose.
 4. All activity relating to the seizure, access, storage or transfer of digital evidence must be fully documented, preserved and available for review.
 5. An Individual is responsible for all actions taken with respect to digital evidence whilst the digital evidence is in their possession.
 6. Any agency, which is responsible for seizing, accessing, storing or transferring digital evidence is responsible for compliance with these principles.

Process/Phases

- Identification
- Collection
 - Bag & Tag
- Preservation
- Examination
- Analysis
- Presentation/Report

Identification

- The first step is identifying evidence and potential containers of evidence
- More difficult than it sounds
 - Small scale devices
 - Non-traditional storage media
 - Multiple possible crime scenes

Devices Identification



Identification

- Context of the investigation is very important
- Do not operate in a vacuum!
- Do not overlook non-electronic sources of evidence
- Manuals, papers, printouts, etc.

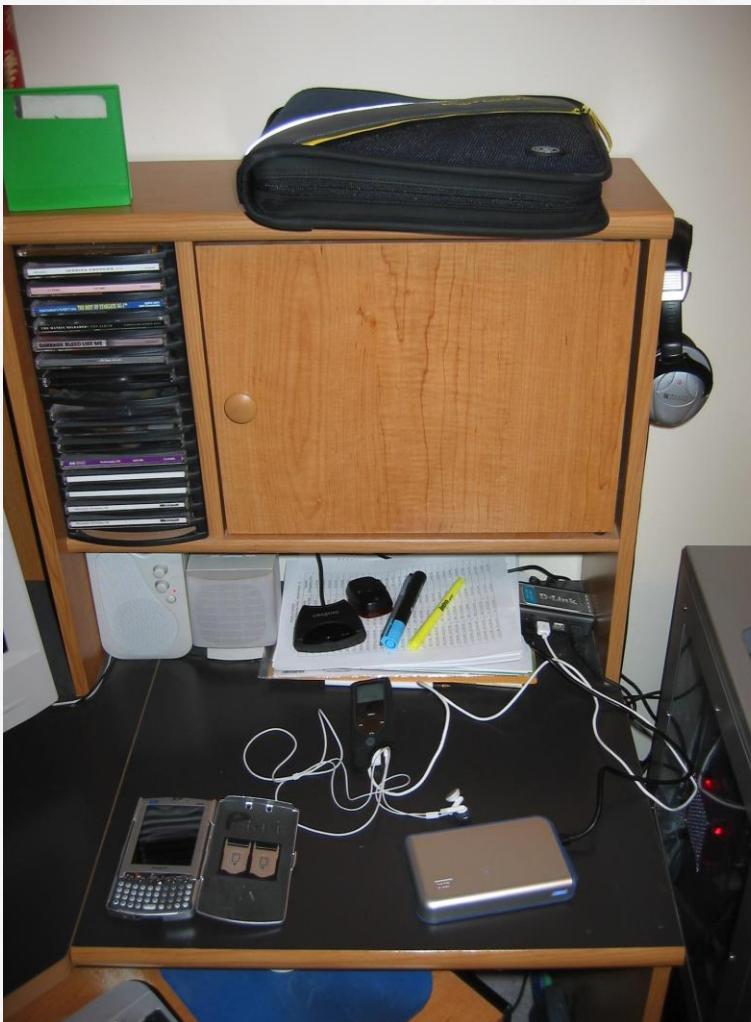
Collection

Care must be taken to minimize contamination

- Collect or seize the system(s)
- Create forensic image
 - Live or Static?
 - Do you own the system
 - What does your policy say?

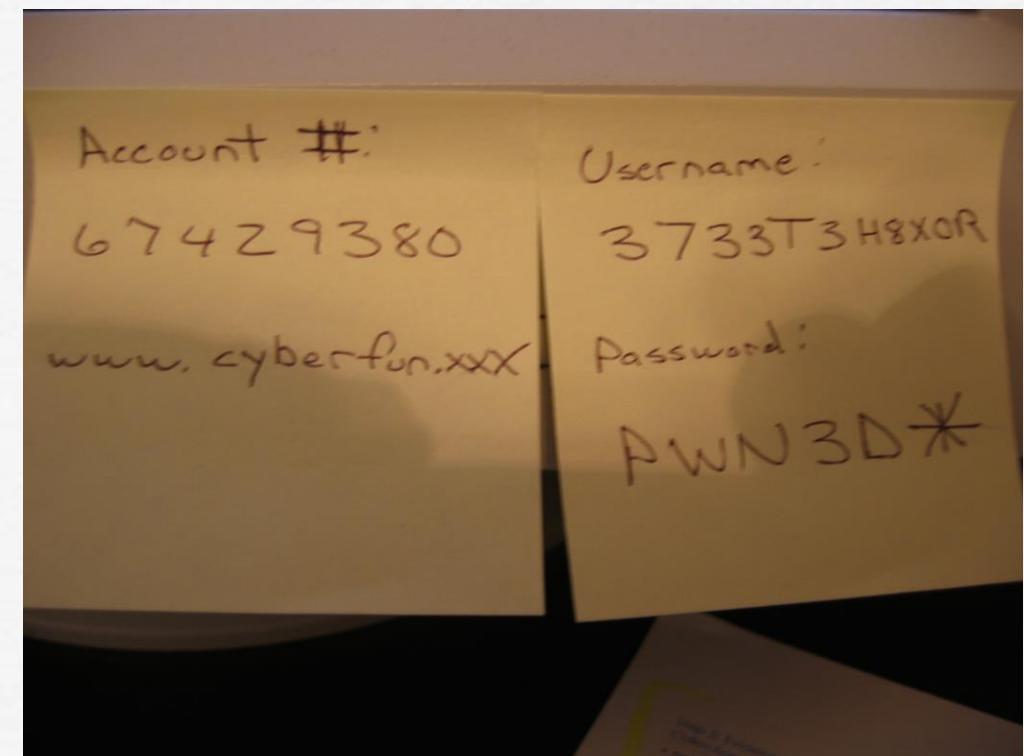


Collection: Documentation



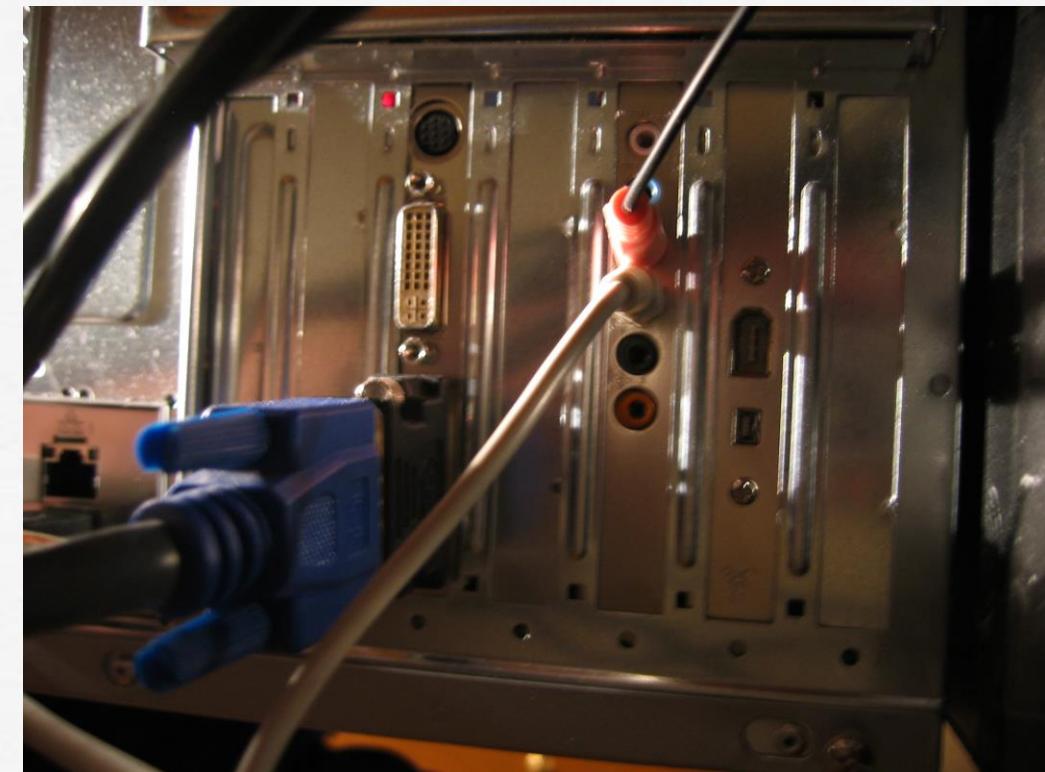
Collection: Documentation

- Take detailed photos and notes of the computer / monitor
 - If the computer is “on”, take photos of what is displayed on the monitor – DO NOT ALTER THE SCENE



Collection: Documentation

- Make sure to take photos and notes of all connections to the computer/other devices



Collection: Imaging

- Rule of Thumb: make 2 copies and don't work from the original (if possible)
- A file copy does not recover all data areas of the device for examination
- Working from a duplicate image
 - Preserves the original evidence
 - Prevents inadvertent alteration of original evidence during examination
 - Allows recreation of the duplicate image if necessary

Collection: Imaging

- Digital evidence can be duplicated with no degradation from copy to copy
 - This is not the case with most other forms of evidence



Collection: Imaging

- Write blockers
 - Software
 - Hardware
- Hardware write blockers are becoming the industry standard
 - USB, SATA, IDE, SCSI, SIM, Memory Cards
 - Not BIOS dependent
 - But still verify prior to usage!

Collection: Imaging

- Forensic Copies (Bitstream)
 - Bit for Bit copying captures all the data on the copied media including hidden and residual data (e.g., slack space, swap, residue, unused space, deleted files etc.)
- Often the “smoking gun” is found in the residual data.
- Imaging from a disk (drive) to a file is becoming the norm
 - Multiple cases stored on same media
 - No risk of data leakage from underlying media
- Remember avoid working for original
- Use a write blocker even when examining a copy!

Imaging: Authenticity & Integrity

- How do we demonstrate that the image is a true unaltered copy of the original?
 - Hashing (MD5, SHA 256)
- A mathematical algorithm that produces a unique value (128 Bit, 512 Bit)
 - Can be performed on various types of data (files, partitions, physical drive)
- The value can be used to demonstrate the integrity of your data
 - Changes made to data will result in a different value
- The same process can be used to demonstrate the image has not changed from time-1 to time-n

Examination

- Higher level look at the file system representation of the data on the media
- Verify integrity of image
 - MD5, SHA1 etc.
- Recover deleted files & folders
- Determine keyword list
 - What are you searching for
- Determine time lines
 - What is the timezone setting of the suspect system
 - What time frame is of importance
 - Graphical representation is very useful

Examination

- Examine directory tree
 - What looks out of place
 - Stego tools installed
 - Evidence Scrubbers
- Perform keyword searches
 - Indexed
 - Slack & unallocated space
- Search for relevant evidence types
 - Hash sets can be useful
 - Graphics
 - Spreadsheets
 - Hacking tools
 - Etc.
- Look for the obvious first
- When is enough enough??

Issues

- lack of certification for tools
- Lack of standards
- lack of certification for professionals
- lack of understanding by Judiciary
- lack of curriculum accreditation
- Rapid changes in technology!
- Immature Scientific Discipline

Professional Opportunities

- Law Enforcement
- Private Sector
- Intelligence Community
- Military
- Academia

The laws cover

- Theft of computer services
- Unauthorized access to protected computers
- Software piracy
- Alteration or theft of electronically stored information
- Extortion committed with the assistance of computers
- Obtaining unauthorized access to records from banks, credit card companies or customer reporting agencies.
- Traffic in stolen passwords
- Transmission of destructive virus or commands.

Digital Evidence

- Computer forensics: preservation and analysis of computers (file systems)
- Network Forensics: preservation and analysis of traffic and other logs.
- Mobile forensics: preservation and analysis of cell phones, PDAs, GPS, etc.
- Various types of digital data
 - Text
 - Digital photographs
 - Malware

Forensic Examination and Analysis

- Forensic examination: Extract and prepare data for analysis.
- Examination process involves: data translation, reduction, recovery, organization and searching.
- Forensic examination can be automated on a computer, whereas analysis requires critical thinking,

Role of Computers in Crime

- Specific role of computer will determine how it can be used as evidence.
- Is the computer the key piece, or an incidental evidence? Entire computer can be seized in case it is the key piece.

Categories of computer crime

- Computer is the object of the crime (stolen or destroyed). – target.
- Computer is the subject of the crime. (Virus, format, etc.)
- Computer is a tool in planning or executing a crime. (forge documents, break into other computers) – like a weapon.
- The symbol of a computer can be used to intimidate or deceive. A broker telling a client he has a special program.

U.S. Dep of Justice Categories

- Hardware as contraband or fruits of crime
- Hardware as an instrumentality
- Hardware as Evidence
- Information as contraband or fruits of crime
- Information as an instrumentality
- Information as evidence

Hardware as contraband or fruits of crime

- Contraband- property that a citizen not permitted to possess (eg. hardware that intercept communications)
- Fruits of crime – hardware obtained by criminal activity. Stolen or used stolen credit cards, etc.

Hardware as instrumentality

- When computer hardware has played a significant role in a crime.
- Like a gun or knife.
- Computer manufactured or configured specifically to commit crime. Think of sniffers.

Hardware as Evidence

- Any information left on the computer relating to a crime makes the hardware an evidence.

Information as contraband

- A common form of information as contraband is encryption software.
- It is illegal to export 128bit-encryption software without being approved by US govt. US non-military exports are controlled by Export Administration Regulations (EAR) and Department of State. These are placed on the United States Munitions List.
- In some countries it is illegal to use encryption software.

Information as instrumentality

- Exploits (programs that enable intruders gain access to computers)
- Programs used to break into other peoples' computers
- Program that captures login info, or guesses passwords.

Information as evidence

- Trail of digital information
- Digital cameras
- Cell phones
- Satellite tracking devices

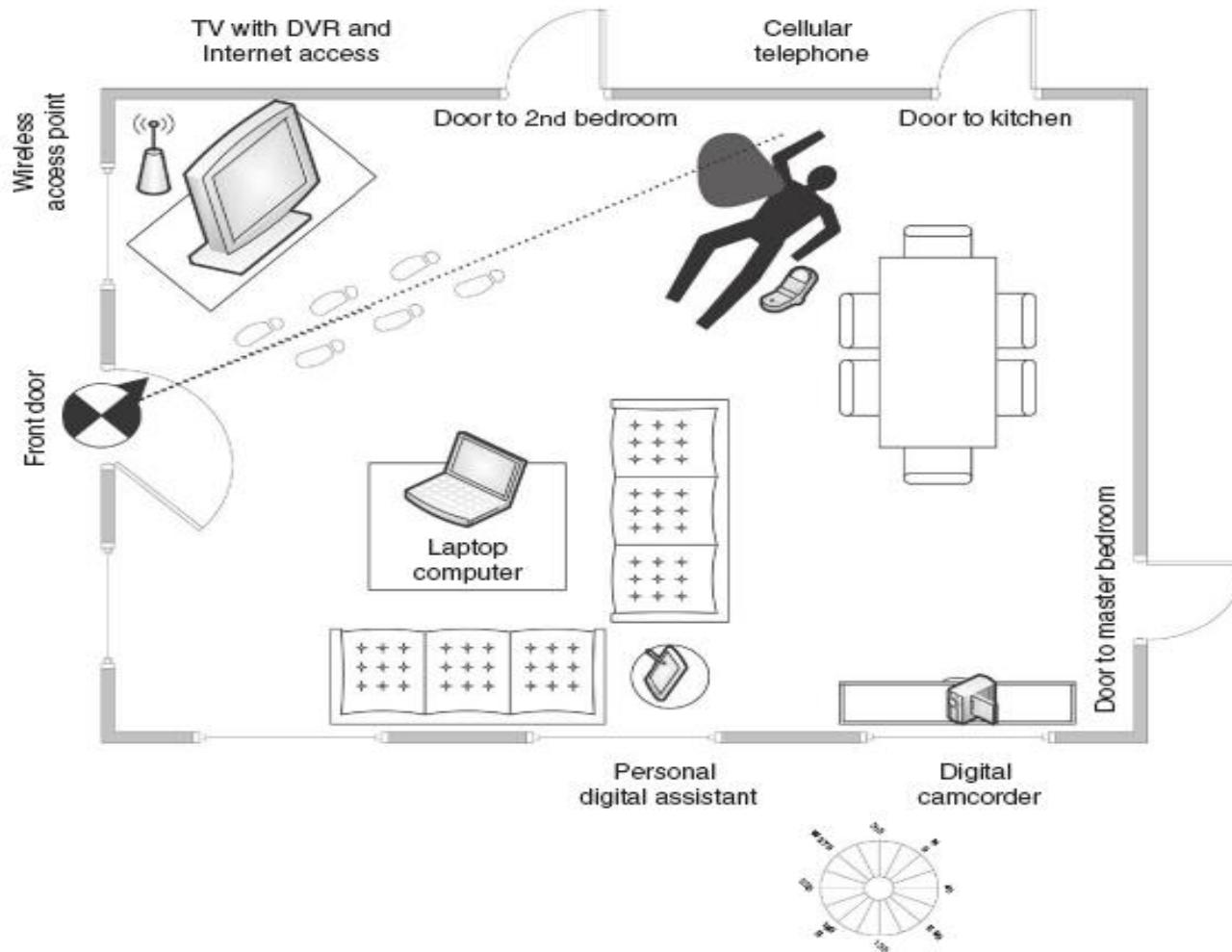
Handling a Digital Crime Scene

Source:- 1) Dr. John P. Abraham
Professor,UTPA
2) Digital evidence and computer
crime- Eoghan Casey

Introduction

- GOAL: Sequestered environment where
 - All contents are mapped and recorded
 - Accompanying photographs and basic diagrams showing areas and items
 - Evidence is frozen in place
- This chapter deals with handling individual computers as a source of evidence.
- US department of Justice and Secret Service
 - Electronic Crime Scene Investigation.
 - Best Practices for Seizing Electronic Evidence
 - Guide for first responders
- Also The good practice guide for computer based evidence by association of chief of police officers (ACPO)

Relationship Between Physical and Digital Crime Scene



Major principles

- No action taken should change data held on a computer or storage media
- Anyone accessing the computer must be competent in cyber forensics.
- An audit trail or other record of all processes applied to electronic evidence must be kept.
- Person in charge of the overall case has the responsibility of ensuring that the law and these principles are adhered to.

Authorization

- Obtain written authorizations and instructions from attorneys.
- Private and personal computer access would require warrant unless an employee agrees to the search.
- Work place computer may not require a warrant.
- Digital investigators are generally authorized to collect and examine only what is directly pertinent to the investigation.

Sample Criminal Investigation (continued)

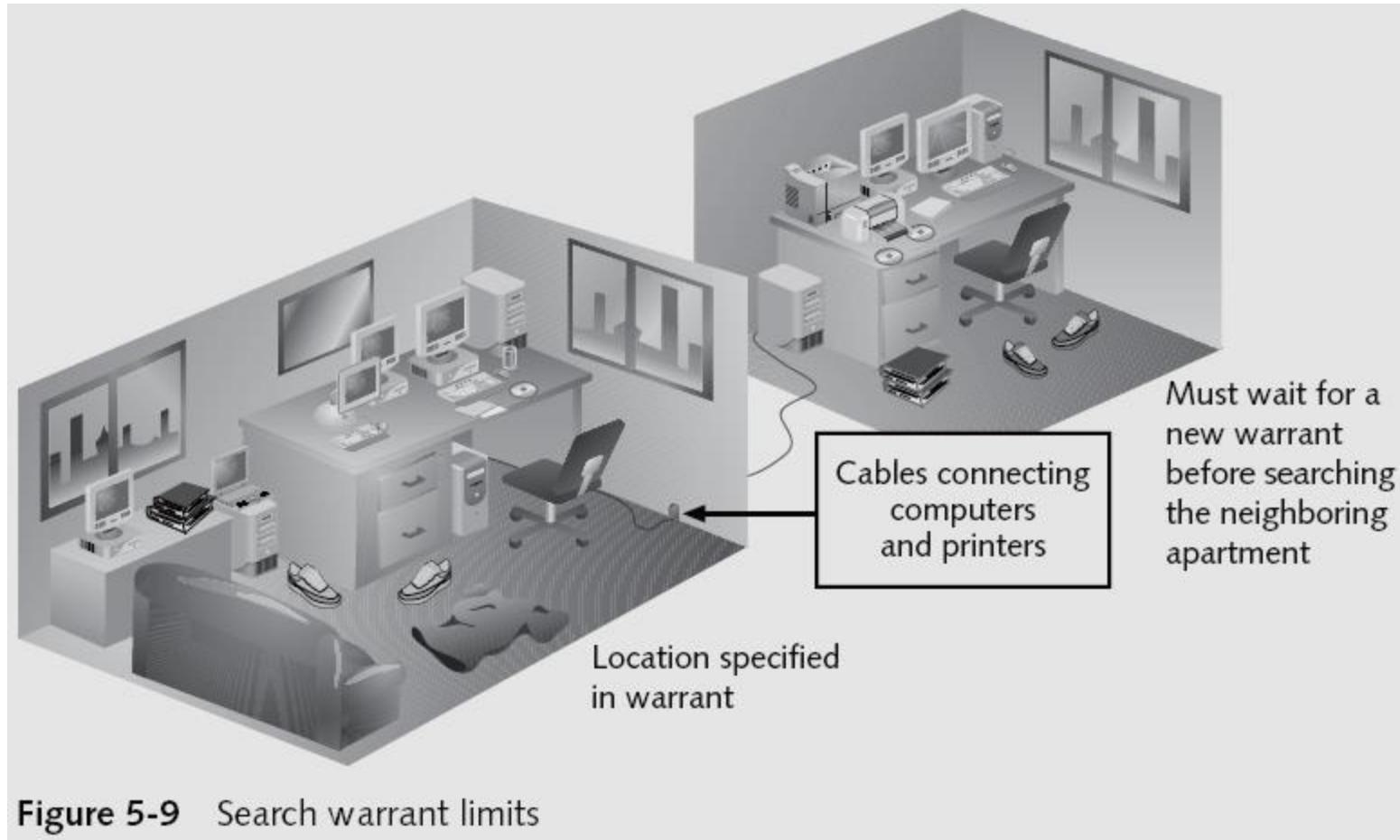


Figure 5-9 Search warrant limits

Preparing to handle digital crime scenes

- Make diagrams and have a plan as to what to examine.
- What type of tools should be brought to the scene.
- Bring questionnaire to interview individuals at the crime scene.

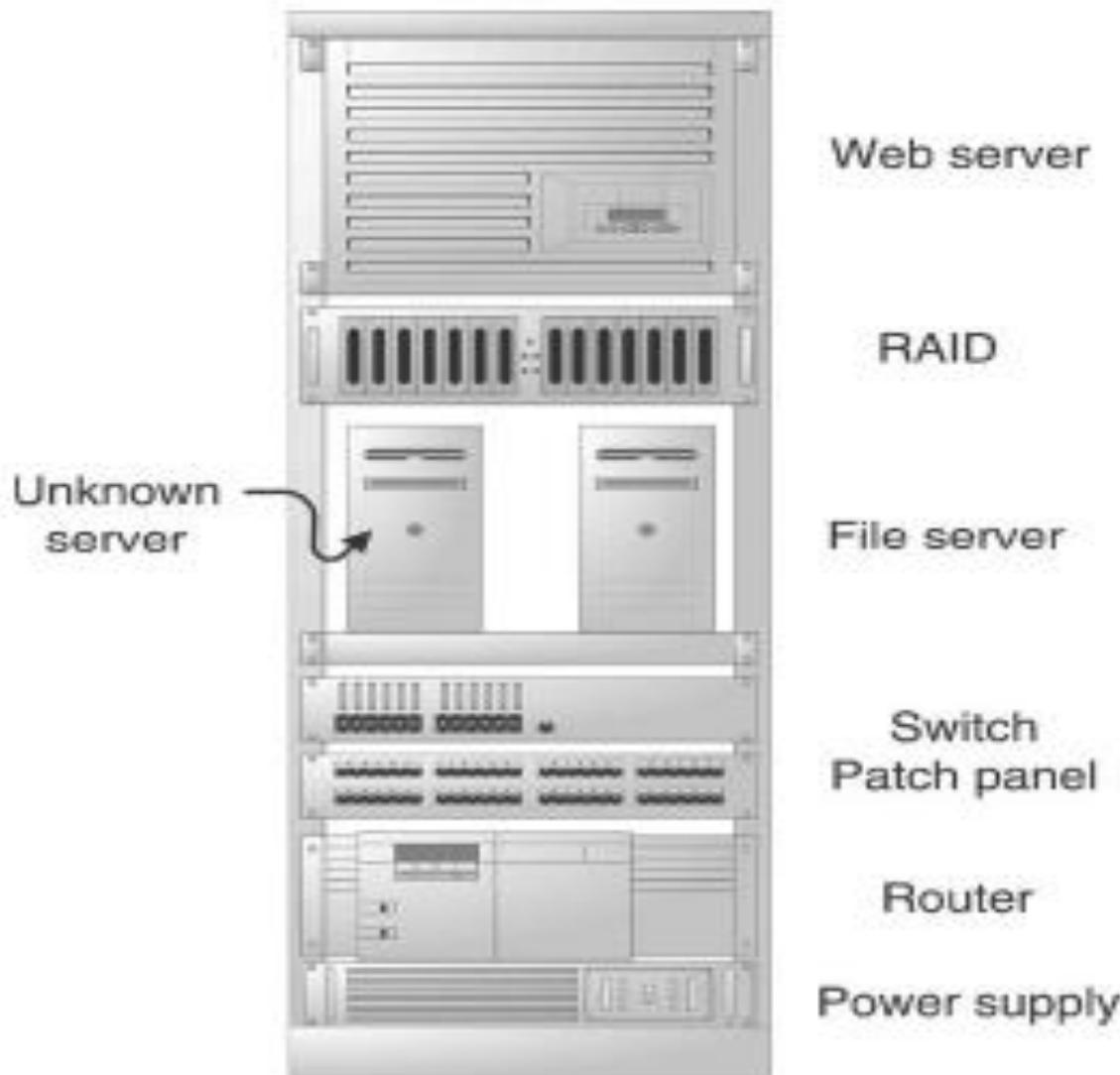
Hardware Duplicator



Surveying the Digital Crime Scene

- Look at laptops, handheld devices,
- Digital video records (DVRs)
- Gaming systems
- External hard drives
- Digital cameras
- DVDs
- Look for installation disks that give clues
- Network configurations, look for remote machine in the facility or outside.

Multiple Servers on a Rack



Preserving the Digital Crime Scene

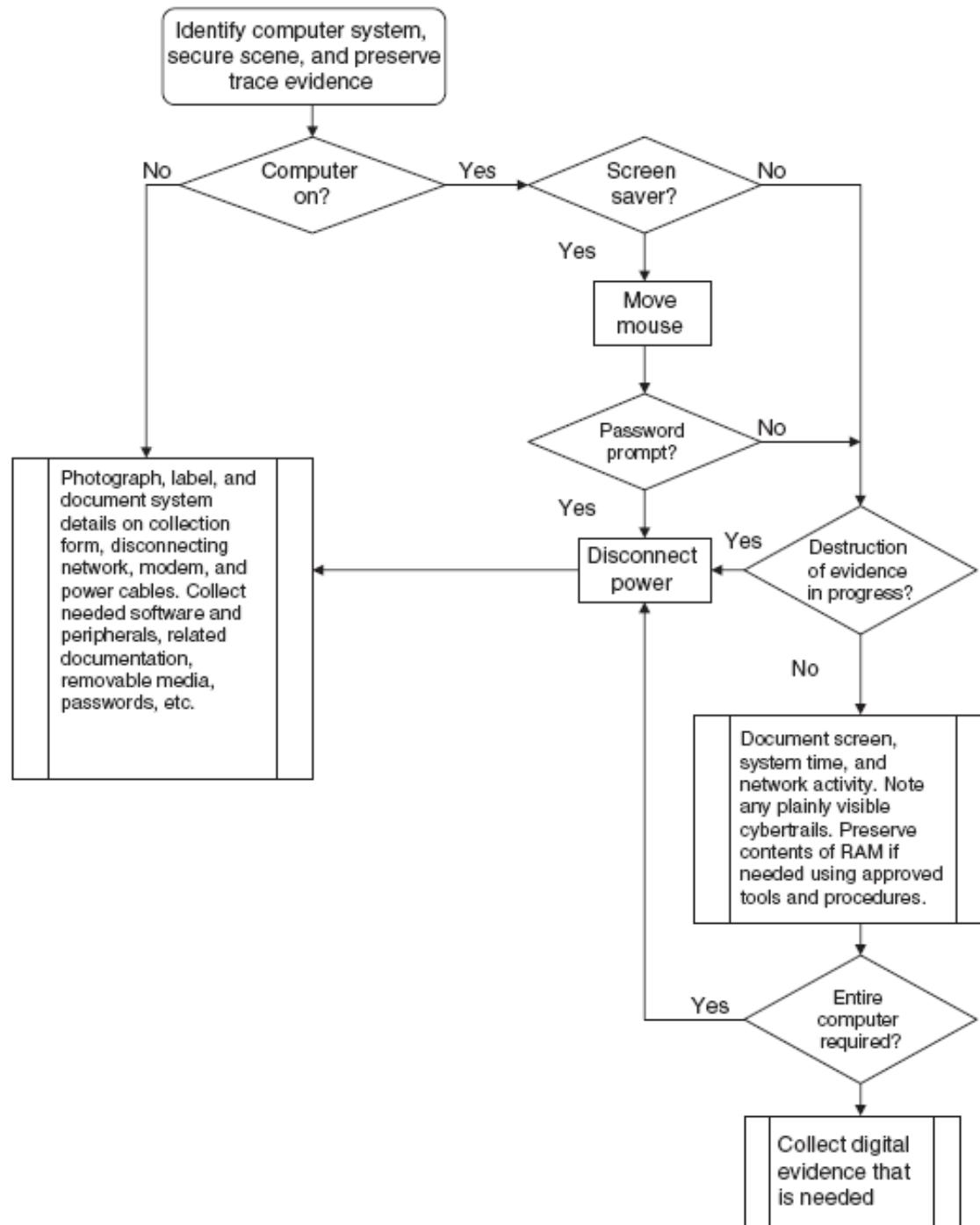
- Controlling Entry points – secure the crime scene.
- Save biometric access system data and video recordings.
- Save network level logs (copy).
- Preserve all backup media, do not overwrite backup media.
- Preserve emails on the servers.
- Keyboards may have fingerprints.

Preserving data on live systems

- The contents of volatile memory must be obtained such as a note being written.
- Which account is running under certain processes.
- Capture information related to active processes and network connections.

Shutting down

- Remove power from the back of the machine.
- Open the case and remove power to the hard drives.
- Check for missing parts
- Check for explosives.



Internet

- Wild west of technology
- As to the murderer as internet to the criminal
- New types of crimes and criminals emerging

Modus Operandi (MO)

- Method of operating
- How a crime is committed
- Repeated offenders leave similar Mos
- Mo is intended to:
 - Hide offender's identity
 - Ensure successful completion of the crime
 - Facilitate the offender's escape

Examples of MOs cyber crime

- Planning – notes, emails, etc.
- Computer system type, software, etc.
- Presurveillance of the crime scene or victim
- Offence location
- Use of weapon – computer virus etc.
- Use of aliases, ip spoofing, etc.

Technologies used for

- Selecting the victim
- Keeping the victim under surveillance
- Grooming/contacting the victim
- Stalking/harassing
- Stealing identity, money, etc.
- Destroying assets (network, intellectual property)
- Gathering and storing confidential materials
- Distributing confidential information

Case examples

- Pages 290 and 291 explains cases involving child pornography and cybersex sting operation.
- Example 1: Digital imaging technology and the Internet enhanced an existing MO.
- Example 2: Females attracted to uniforms (Blue Magnet) called groupies. A teenager contacted vulnerable, police officers and the offers eventually were caught.

Motive and Technology

- Motive – a need that impels and is satisfied by a behavior.
- Study indicates that even rapists satisfy emotional needs. FBI uses Groth rapist motivational typology.

Behavioral motivational typology

- Power reassurance – criminal behavior that restore self-confidence. Low aggression
- Power Assertive – high aggression means. Attacks to show his own virility. Not to harm necessarily but to possess.
- Anger Retaliatory – Rage toward a person, group or symbol. Retaliating for wrongs perceived or real.
- Sadistic – Anger Excitation. Sexual gratification gained from victim's pain.
- Profit oriented.

Current technologies

- Computer virus
- Trojan
- Key logger
- A public email discussion list

Digital Evidence in Violent crime

John P. Abraham

Professor

UTPA

Role of Computers in Violent Crime

- Cybertrails
 - Communications between the victim and offender
 - George Huguely, lacrosse player took the computer from the victim, his girlfriend, Yeardly Love, to hide his communications with her.
 - In 2009 Korena Roberts targeted a victim, Heather Snively using a computer and arranged a meeting with her, then she proceeded to cut the baby out her womb.
 - Serial killer Maury Travis was tracked down using the IP address he used when accessing an online map.

Mobile devices

- May contain information about communications
- Audio and video recordings related an offense.
- Provide the location of victims and suspects at key times.
 - Joe O'Reilly claimed he was at work when his wife was killed.
 - His cell phone location showed him traveling from work to the scene.

Personal computers

- Victim's computer may contain a diary
- Received and sent emails
- Evidence of fantasies, criminal activity and secret relationships
- Chandra Levi had googled for Klinge Mansion in Rock Creek Park. Even though the murder is unsolved, her body was found in the remote area of the park.

Intent and Motive

- Offender's computer or mobile device may disprove offender statements.
- Show his intent to commit a crime
- Uncover evidence of staging such as a fake suicide note.
 - William Guthrie was sent to prison partly on the basis of digital evidence showing online searches for ways to kill his wife and fabricate a suicide note.

Crime scene characteristics

- Primary and secondary crime scenes
- Primary is where the offense occurred
- Secondary may include where the victim was abducted, or clothes were discarded etc.
- Computers are treated as secondary crime scenes
- Offenders may use public computers such as library

Alibi

- Key pieces are: time and location
 - Jerry Durado was found guilty of killing his parents despite his claim that he was at work 300 miles away. A forensic analysis showed that only thing that happened in his computer at work was a virus scan.
- Telephone logs, credit card records, internet activities, etc.
- Computer times and IP address are used as Alibi. Keep in mind these can be manipulated creating a false alibi.

Investigating an alibi

- Establish reliability of digital evidence
- DHCP records will show assigned IP addresses.
- Can IP address be changed by the user?
- Can the time be changed by the user?
- A suspect claimed he was at home, doing nothing other than sending an email to his friend. The friend shared the email, and the header revealed that was not sent from the suspect's home. The date and time did not match, and the email was forged. His own computer showed evidence of attempts at forging to learn how to do it.

Computer Intrusions

How Computer Intruders Operate

- **Goals**

In practice, this means someone might break into a computer system for purposes ranging from large-scale data theft or the disruption of operations, all the way to simple harassment of a specific computer user.

Basic Methodology

- **Reconnaissance:** *This is the process of obtaining information on target organizations or individuals that may aid in the compromise of those Targets*
- **Attack:** *This is the process of applying a technique against a target System or network that will result in either unauthorized access or a denial-of-service.*
- **Entrenchment:** *This is the process of ensuring continued and hidden administrative access to target systems.*
- **Abuse:** *This is the process of conducting any further activities on targets that meet the goals of the attacker.*

Case Example: World Bank

- In July 2008, the World Bank discovered that an intruder had gained unauthorized access to their computer systems. The intrusion became apparent when a Senior System administrator's account was misused while the employee was on leave. Digital investigators determined that the intruder had most likely gained access via a Web server and then obtained administrator-level credentials that permitted access to other systems on the network.

Classic Computer Intrusion Tactics

- 1. Gather information about the target computer.
- 2. Probe the computer for vulnerabilities and attempt to exploit them.
- 3. Gain unauthorized access into the computer.
- 4. Escalate from an unprivileged account to privileged account.
- 5. Extend unauthorized access to other areas of the network.
- 6. Pursue goal of intrusion (e.g., steal information or destroy data).

Table 13.1 Examples of Tactics and Techniques Within Each Phase of a Computer Intrusion

Phase	Example Tactic	Example Technique
Reconnaissance	Identification of the target	Nslookup of a domain name to determine the IP address of the Web server
	Identification of attack surface area on the target	Scan of target Web server to determine open ports, service, and application types/versions open on those ports
Attack	Launch exploit	An exploit is launched against the target system and against a specific application on that system. The result is some method of unauthorized access, such as a reverse shell
Entrenchment	Establish continued remote access	A backdoor is uploaded to the target system through the remote shell, and a Registry setting is added to ensure that the backdoor starts at boot
	Ensure hidden access	A rootkit is uploaded to the target system through the remote shell, and executed to hide all malicious processes, network connections, and files. The rootkit is also configured to start at boot
	Remove traces of the attack	Clean or delete log entries corresponding to the intrusion
Abuse	Data theft	Sensitive documents are placed into password-protected archives and moved off the compromised system to the attacker's computer

Current Computer Intrusion Tactics

- ***Phishing:***

Sending mass e-mails that appear or claim to be from a legitimate source, in hopes that the recipient will follow instructions also contained in the e-mail. These instructions will usually lead to the recipient's entering sensitive information into a fraudulent Web site, Visiting a malicious Web server that compromises the Web browser, or executing malicious code that accompanied the e-mail.

Case Example: Phishing Scam

From: Smith Brian <[removed]@operamail.com>

Subject: Can I Trust You

Date: July 26, 2010 8:32:34 PM EDT

To: undisclosed-recipients:;

Dear friend,

I hope my email meet you well, I am SGT SMITH BRIAN a U.S. Army in Iraq. I write you this email to ask for your agreement to receive the sum of 5 Million dollars on our behalf. Once you receive the funds, you are to take a reward of 30% and keep our part. If you have a good business plan, we can invest our share in your country too. We seek your most confidentiality in this business transaction. If you are interested please reply to my private email :([removed]@gmail.com)

My partner and I need a good partner, someone we can trust to actualize this venture. The money is from oil proceeds and its legal and we are transferring it via the safe passage of a diplomatic courier. We await your response and wish to furnish you with more comprehensive details.

Regards

Sgt Smith Brian

Investigating Computer Intrusions

- **Case Example: Media Leaks**

In one incident, an organization detected employees from a competitor's network gaining unauthorized access to a server. Sufficient evidence was gathered to prove the illegal activity and to identify the competitor's employees who had committed the crime. To avoid publicity and preserve a good relationship with the competitor, the victim organization decided to resolve the problem through private communication rather than through legal action. However, an employee in the victim organization leaked the story to the press, creating a national scandal that caused more damage than the incident itself.

Goals

- Identify relevant facts .
- Determine what information, if any, was lost or stolen.
- Apprehend the intruder(s).

Investigative Methodologies

- **Intrusion Investigation versus Incident Response**
- An intrusion investigation is concerned primarily with the identification of facts that pertain to a computer network intrusion.
- An incident response, on the other hand, is concerned not only with the determination of fact, but in the containment and remediation of the incident, as well as the applications of lessons learned to further reduce future risk to the target organization.

Intrusion Investigation via the Scientific Method

Hypothesis 1: A system administrator or Web developer downloaded from the Web server as part of his/her normal job duties in maintaining that system.

Predictions for H1: When queried, either the system administrator or one of the Web developers will admit to downloading the program, and can identify the file.

Evaluation for H1: Contact and interview the system administrator, all Web developers, and any other users with access to the Web server to determine if they downloaded executable programs to the server on or about the date and time in question.

Conclusion for H1: *No staff admitted to the download of executable programs. Proceed to a new hypothesis.*

Hypothesis 2: The Web server was compromised on or before the time indicated, and the attacker was able to move malicious executables to the Web server.

- ***Predictions for H2:*** One or more malicious executables will be discovered on the server with file created times on or about 4/18/10 at 20:15.
- ***Evaluation for H2:*** Collect a duplicate image of the Web server, or conduct a live forensic preview of the device and search for executable files created on or about the time in question. Extract those files and evaluate them to determine if they are malicious in nature.
- ***Conclusion for H2:*** Multiple executables were found created at and immediately subsequent to the time in question. Initial assessment indicates that they are variants of a known backdoor and rootkit package that was not flagged by antivirus software.

Challenges of Intrusion Investigation

- *Leaving Compromised Systems Vulnerable*
- One of the more difficult decisions is whether to shut down a compromised system or collect some data from it beforehand.
- Processes in memory, network state tables, and encrypted disks may contain valuable data that are lost when a system is shut down. However, examining a live system is prone to error and may change data on the system, and can even cause the system to stop functioning.

Case Example: Dangers of Investigating Live Systems

- A routine vulnerability scan of a network detected a Trojan horse program running on a Windows XP server. Because of the critical role that this server played in the organization, a rapid response as well as recovery was required. The organization was unwilling to take the server offline because that would disrupt business operations. They wanted the server to be fixed quickly and were not concerned with apprehending the culprit. Digital investigators determined that the server had been compromised via IIS and found Web server access logs that corresponded with the initial intrusion containing the intruder's IP address.

Additionally, they found that the Trojan horse executable was named "wlogin.exe" and was installed as a service

- named "WinLogin" as shown in the following Registry key:
 - = WinLogin

- D:\>regdmp
 - \Registry
- <cut for brevity>
- (HKLM\System\CurrentControlSet\Services)
 - WinLogin
 - Type = REG_DWORD 0x00000110
 - Start = REG_DWORD 0x00000004
 - ErrorControl = REG_DWORD 0x00000000
 - ImagePath = REG_EXPAND_SZ
 - “C:\WINNT\System32\wlogin.exe”
 - DisplayName

- Furthermore, NT Application Event logs showed that Norton AntiVirus had detected the Trojan Horse but had not been able to remove it:
 - D:\>dumpel -c -l application
<cut for brevity>
 - 1/19/2010,12:32:48 AM,4,0,20,Norton AntiVirus,N/A,CONTROL, Unable to restore C:\WINNT\system32\wlogin.exe from backup file after clean failed.
 - 1/19/2010,1:09:11 AM,1,0,5,Norton AntiVirus,N/A, CONTROL, Virus Found!Virus name: BO2K.
 - Trojan Variant in File: C:\WINNT\Java\w.exe by: Scheduled scan. Action: Clean failed : Quarantine succeeded : Virus Found!Virus name: BO2K.Trojan Variant in File: C:\WINNT\system32\ wlogin.exe by: Scheduled scan. Action: Clean failed : Quarantine failed:
 - 1/19/2010,1:09:11 AM,4,0,2,Norton AntiVirus,N/A, CONTROL, ScanComplete: Viruses: 2 Infected:2 Scanned:62093 Files/Folders/DrivesOmitted:89

Observing the Intruder in Progress

- In many forms of criminal investigations, it can be beneficial for digital investigators to observe the suspect in the act of committing a crime. This will allow the digital investigator to gather additional information that can be used to identify and prosecute that suspect.

This is also true for intrusion investigations, for multiple reasons:

- Computer intrusions can be extremely complex, most especially those that extend across an enterprise network. Further observation may be necessary to determine the true scope of the incident.
- Some intruders are skilled in hiding or erasing the traces of their activities. If they are not observed in action, there may not be enough evidence left behind to pursue investigative goals.
- Many organizations are not architected and configured to retain the types of electronic records (log files, for example) that would enable an effective post-mortem investigation. Therefore, observation of current events is much more critical.

Highly Competent Adversaries

- Knowledge of computer programming, including the ability to write programs to accomplish specific tasks.
- Knowledge of system administration, including the ability to modify system configurations in order to hide traces of an attack or reduce or remove logging.
- Knowledge of network administration, including understanding of common network devices and architectures, how to set up communications throughout an enterprise, and how to locate and identify high-value target systems.
- Knowledge of computer intrusion techniques, including methods for circumventing or bypassing common security measures.
- Knowledge of digital forensics, including an understanding of the nature and location of common intrusion artifacts.

- Technical capabilities of an intruder may also reside in advanced software that the intruder was able to either write for himself or herself or obtain from a skilled programmer. These capabilities may include the following:
 - The ability to interfere with system calls to intercept and manipulate data being returned to a user.
 - The ability to manipulate operating system kernel structures in order to control data being returned to a user or to host-based defense software such as an antivirus program.
 - The ability to locate and modify key date/time stamps that would be used by a forensic examiner to generate a timeline of activity.
 - The ability to establish covert and/or encrypted channels for remote control and communication.
 - The ability to detect and forensic analysis tools and techniques.

Handling and Analysis of Malicious Code

In order to successfully complete the investigation, the digital investigator will often need to analyze the malicious programs to learn more about what they do and how they operate

- The identity of command and control servers with which malicious code is programmed to communicate
- The names and storage locations of additional files that are related to the malicious code, such as related executables, configuration files or Registry entries, a keystroke log, or an archive of stolen data.
- The purpose of the malicious code, that is, whether it is to create a backdoor, capture keystrokes, spread itself via some specific mechanism, etc.

Linking Events to an Actual Person

- It is important to remember that linking events to an actual person is a concern for all digital investigations, and especially so with computer intrusions.
- Tracing events to a specific computer system is not sufficient to claim that a specific person was using that computer system during the time of those events, and that that same person was responsible for the observed events.

Forensic Preservation of Volatile Data

- **Understanding Volatile Data**
- Volatile data are considered to be temporary or delicate in some way.
- Traditionally, *volatile data is taken to mean information stored in the RAM or memory of a computer system that will be lost when the power to that system is deactivated or otherwise removed.*

Listing showing details about processes running on a Windows system.

Process information for VWKS-02:

Name	Pid	Pri	Thd	Hnd	Priv	CPU Time	Elapsed Time
Idle	0	0	1	0	0	4:26:28.125	0:00:00.000
System	4	8	94	524	44	0:01:43.203	21:31:41.545
smss	268	11	2	29	220	0:00:00.328	21:31:41.530
csrss	432	13	9	653	2184	0:00:01.390	21:31:12.702
wininit	480	13	3	74	860	0:00:00.406	21:31:11.873
csrss	488	13	7	448	1424	0:00:02.328	21:31:11.873
winlogon	528	13	5	127	1772	0:00:00.843	21:31:11.702
services	556	9	19	236	3740	0:00:04.484	21:31:11.389
lsass	568	9	6	601	2748	0:00:02.984	21:31:11.264
lsm	576	8	10	149	1248	0:00:00.812	21:31:11.248
svchost	696	8	10	351	2600	0:00:02.296	21:31:10.077
svchost	764	8	13	304	3012	0:00:01.265	21:31:09.342
svchost	816	8	20	472	12548	0:00:03.453	21:31:09.202
svchost	916	8	19	458	28160	0:00:31.515	21:31:08.467
svchost	944	8	37	1263	18908	0:00:18.359	21:31:08.248
svchost	1128	8	10	524	4460	0:00:03.421	21:31:05.342

RFC 3227 "Order of Volatility"

Areas traditionally considered
"volatile"

Areas traditionally considered
"non-volatile"

- 1. Registers, cache
- 2. Routing table, arp cache, process table, kernel statistics, memory
- 3. Temporary file systems
- 4. Disk
- 5. Remote logging and monitoring data that is relevant to the system in question
- 6. Physical configuration, network topology
- 7. Archival media

FIGURE 13.5
Order of volatility.

- Researchers at Princeton University have successfully shown that data do not disappear from RAM instantly once power is removed. In fact, the data in RAM persist long enough .
- Princeton researchers to access RAM after a system has been powered off and to recover encryption keys from the contents. While this is more of an attacker tactic, there are forensic applications for their findings as well. At the very least, they have shown that RAM is not quite as volatile as was traditionally believed. Their interesting findings aside, it is still generally considered more practical for digital investigators to dump memory from a running system than to
- perform a cold boot acquisition. (Halderman et al., 2008).

Preserving Volatile Data

- When dealing with a computer intrusion, a typical digital investigator might use a script that will execute multiple commands in quick succession and collect the types of volatile data that are considered most important. This will commonly include commands that will collect items such as the following:
- ***Operating system date and time:*** Critical for comparison to a central time source so that any variance in the time settings of the target system can be identified.
- ***b. List of running processes:*** Collected so that an examiner can later identify unauthorized or malicious processes that may have been active on the system.
- ***c. List of loaded drivers or modules:*** Collected to identify unauthorized or malicious code that may be loaded as a driver or module as opposed to a library or standard process.
- ***d. List of loaded libraries for each process:*** Collected to identify unauthorized or malicious code that may be running as a library loaded into an otherwise legitimate process.

- **E. List of open sockets and active network connections by process:** Collected to identify any unauthorized communication sessions or open sockets that were active on the target system.
- **f. Network configuration:** Collected for various reasons, including the identification of anomalous configuration settings, as well as to simply understand the role of the system in the network in which it resides.
- **g. List of file and Registry handles by process:** Collected for various reasons, such as to make a determination as to what files and Registry entries may be connected to malicious processes.
- **h. List of currently authenticated users:** Collected to determine if there are any unauthorized authentications to the target system.

Sample Volatile Data Preservation Process

- A typical process that digital investigators follow to preserve volatile data from a single system is outlined below.
- 1. Perform an initial physical inspection of the target device, including photographing or noting the physical condition of the device, external markings such as serial numbers, etc. While doing this, the digital investigator notes the input/output options available on the device.
- 2. Authenticate to the console (monitor and keyboard as opposed to remote access) of the device using administrative credentials. Administrative credentials are typically required to execute some volatile data collection commands.
- 3. Note the contents of the screen after logon, including any windows that may be open or were opened automatically during logon. Should there be no obvious destructive processes active, the digital investigator will continue.

- 4. Insert a forensically prepared “clean” toolkit (created from trusted sources in such a way that it minimizes calls to libraries on the system). In this example, consider this toolkit to be on a CD.
5. Locate and identify the trusted shell executable on the CD, and start that shell (e.g., cmd.exe). Running a trusted shell as opposed to the local command line shell helps to circumvent interference by less sophisticated rootkits .
- **6.** Execute a command to change the path variable for the shell, so that the operating system will look on the toolkit CD for programs and libraries before turning to the local system where executables and libraries are not trusted.
- **7.** Insert a formatted USB drive that will serve as the Destination for any volatile data collection output. When dealing with systems that contain large amounts of memory, care must be taken to use a USB device large enough to store the full contents of memory.

- 8. Execute a command that will extract and present the date and time of the system. This date and time should be recorded in documentation and compared with a trusted time source, noting any discrepancy.
- **9. Execute a script that will perform the following actions:**
 - a. Execute a command that will collect a memory dump and output it to the destination USB drive
 - b. Execute a series of targeted commands that will collect data types
 - c. Create and record hash values for all outputs.
- 10. Close the trusted shell and eject all media used in the collection, and note the date and time in documentation.

Investigation of Malicious Computer Programs

Goals

- The ultimate goal of analyzing malware in an intrusion investigation will vary depending on the purpose of the attack.
- For instance, in data theft cases, the goal of malware analysis may be to determine what data were stolen
- As another example, when investigating a large-scale network intrusion, the goal of malware analysis may be to identify characteristics that can be used to search the entire network for other computers that have been compromised.
- To achieve these ultimate goals, it may be necessary to pursue more discrete goals, which commonly include answering the following questions relating to the malware:

- What is the primary purpose (or purposes) of the code?
- If the purpose is to steal or destroy information, what types of information does it target (e.g., passwords, keyboard input, files)?
- Does the program automatically create, delete, or alter any specific files?
- Does the program create additional processes or inject itself into other processes?
- Does the program automatically create, delete, or alter any specific Windows Registry keys, or other operating system configuration options on other operating systems?
- Does the program accept remote network connections?
- Does the program initiate any network connections, and if so how are the remote hosts identified?
- Does the program intercept or otherwise interfere with any legitimate operations of the operating system?
- Can the author/origination of the malware be determined?

Analysis Strategies

- ***Automated Scanning***
- Digital investigators can use automated tools to identify and deconstruct the code to determine its function. E.g. Antivirus program
- ***Static File Inspection***
- Digital investigators can inspect a static file with some simple techniques to determine some basic pieces of information. This includes using programs to extract readable strings from the file, examining executable file metadata, and checking library dependencies.
- ***Dynamic Analysis***
- Dynamic analysis of malware involves executing the code to observe its actions
- it may require that digital investigators use a debugger to run the code in a more controlled environment where execution can be controlled and routed within the program as desired

- **Virtualization**
- Loading a forensic duplicate into a virtualized environment enables digital investigators to observe malware in the context of the compromised system.
- **Disassembly and De-Compilation**
- This is the process of taking a binary executable and restoring it back to either Assembly code or to the higher-level language in which it was constructed
- **Safety**
- malicious code should never be analyzed from a system that is networked with other computers that are used for any purpose other than malicious code analysis.

Examining the Intruder's Computer

- Lists of dial-up accounts and passwords, including the one used to Commit crimes.
- Nmap scans of target networks.
- Lists of compromised hosts (trophy list and memory aid).
- List of UNIX commands executed on compromised hosts (memory aid).
- Sniffer logs from compromised hosts (digital evidence transfer).
- Directory listings from compromised UNIX hosts (digital evidence transfer).
- Stolen data from compromised hosts, including credit cards and private e-mail.
- TAR file with class characteristics linking it to compromised UNIX host.
- RAR file with stolen data from compromised computer.
- Toolkits found on compromised hosts.
- FTP and terminal emulator configuration files relating to compromised hosts.

Computer Intrusion

Introduction

- Organized criminal groups stole tens of millions of dollars from small and medium-sized organizations, using remote control programs such as ZeuS. Victims were generally tricked into accessing a malicious Web site that exploited vulnerabilities on their computer to install malicious programs designed to steal usernames and passwords for online banking.
- The attackers used the stolen credentials to transfer money out of the victim's accounts

Goals of Intruder

- someone might break into a computer system for purposes ranging from large-scale data theft or the disruption of operations, all the way to simple harassment of a specific computer user

Basic Methodology

- The four Phases are

1) Reconnaissance: *This is the process of obtaining information on target* organizations or individuals that may aid in the compromise of those targets

2) Attack: *This is the process of applying a technique against a target* system or network that will result in either unauthorized access or a denial-of-service.

3) Entrenchment: *This is the process of ensuring continued and hidden* administrative access to target systems.

4) Abuse: *This is the process of conducting any further activities on compromised* targets that meet the goals of the attacker

Classic Computer Intrusion Tactics

- 1. Gather information about the target computer.**
- 2. Probe the computer for vulnerabilities and attempt to exploit them.**
- 3. Gain unauthorized access into the computer.**
- 4. Escalate from an unprivileged account to privileged account.**
- 5. Hide tracks and instantiate a persistent reentry.**
- 6. Extend unauthorized access to other areas**

•Case Example: Phishing Scam

- From:** Smith Brian <[removed]@operamail.com>
- Subject:** Can I Trust You
- Date:** July 26, 2010 8:32:34 PM EDT
- To:** undisclosed-recipients:;
- Dear friend,
- I hope my email meet you well, I am SGT SMITH BRIAN a U.S. Army in Iraq. I write you this email to ask for your agreement to receive the sum of 5 Million dollars on our behalf. Once you receive the funds, you are to take a reward of 30% and keep our part. If you have a good business plan, we can invest our share in your country too. We seek your most confidentiality in this business transaction. If you are interested please reply to my private email :([removed]@gmail.com)
- My partner and I need a good partner, someone we can trust to actualize this venture. The money is from oil proceeds and its legal and we are transferring it via the safe passage of a diplomatic courier. We await your response and wish to furnish you with more comprehensive details.
- Regards
- Sgt Smith Brian

Table 13.1 Examples of Tactics and Techniques Within Each Phase of a Computer Intrusion

Phase	Example Tactic	Example Technique
Reconnaissance	Identification of the target	Nslookup of a domain name to determine the IP address of the Web server
	Identification of attack surface area on the target	Scan of target Web server to determine open ports, service, and application types/versions open on those ports
	Launch exploit	An exploit is launched against the target system and against a specific application on that system. The result is some method of unauthorized access, such as a reverse shell
Attack	Establish continued remote access	A backdoor is uploaded to the target system through the remote shell, and a Registry setting is added to ensure that the backdoor starts at boot
	Ensure hidden access	A rootkit is uploaded to the target system through the remote shell, and executed to hide all malicious processes, network connections, and files. The rootkit is also configured to start at boot
	Remove traces of the attack	Clean or delete log entries corresponding to the intrusion
Abuse	Data theft	Sensitive documents are placed into password-protected archives and moved off the compromised system to the attacker's computer

Social Engineering

- Social engineering refers to
- any attempt to contact legitimate users of the target system and trick them into giving out information that can be used by the intruder to break into the system.
- For example, calling someone and pretending to be a new employee who is having trouble getting started can result in useful information like computer names, operating systems, and even some information about employee accounts

Current Computer Intrusion Tactics

1) Phishing

- Sending mass e-mails that appear or claim to be from a legitimate source, in hopes that the recipient will follow instructions also contained in the e-mail.
- These instructions will usually lead to the recipient's entering sensitive information into a fraudulent Web site,
- Visiting a malicious Web server that compromises the Web browser, or executing malicious code that accompanied the e-mail

2) Drive-by download: This is a term sometimes used to refer to an attack

- where a user happens to visit a Web site hosted on an infected or malicious Web server through otherwise innocuous Web browsing.

For example,

- an individual might be Web browsing on social networking sites, and a malicious advertisement might direct that user to an infected Web server that would then infect or compromise the Web browsers through the exploitation of a

3) *Cross-site scripting: Also written as “XSS,”*

cross-site scripting is a general

- set of techniques whereby an attacker is able to execute malicious code on another system through an intermediary Web application

- 4) SQL injection: This is the placement of SQL control characters as input into
- an application with a database back end, where the application was not expecting SQL control characters. If those characters are placed properly accepted by the database server, they can be used to cause the database server to supply or modify information that should not have been

Investigating Computer Intrusion

- Common goals include the following:
 - 1) Identify relevant facts to enable containment, eradication, and remediation.
 - 2) Determine what information, if any, was lost or stolen.
 - 3) Apprehend the intruder(s).

Investigative Methodologies

Intrusion Investigation versus Incident Response

- An intrusion investigation is concerned primarily with the identification of facts that pertain to a computer network intrusion.
- An incident response, on the other hand, is concerned not only with the determination of fact, but in the containment and remediation of the incident, as well as the applications of lessons learned to further reduce future risk to the target organization.

Intrusion Investigation via the Scientific Method

- **Hypothesis 1:** A system administrator or Web developer downloaded from the Web server as part of his/her normal job duties in maintaining that system.
- **Predictions for H1:** When queried, either the system administrator or one of the Web developers will admit to downloading the program, and can identify the file.
- **Evaluation for H1:** Contact and interview the system administrator, all Web developers, and any other users with access to the Web server to determine if they downloaded executable programs to the server on or about the date and time in question.
- **Conclusion for H1:** *No staff admitted to the download of executable programs.* Proceed to a new hypothesis.

- **Hypothesis 2:** The Web server was compromised on or before the time indicated, and the attacker was able to move malicious executables to the Web server.

-

- **Predictions for H2:** One or more malicious executables will be discovered on the server with file created times on or about 4/18/10 at 20:15.

- **Evaluation for H2:** Collect a duplicate image of the Web server, or conduct a live forensic preview of the device and search for executable files created on or about the time in question. Extract those files and evaluate them to determine if they are malicious in nature.

- **Conclusion for H2:** Multiple executables were found created at and immediately subsequent to the time in question. Initial assessment indicates that they are variants of a known backdoor and rootkit package that was not flagged by antivirus software.

Challenges of Intrusion Investigation

1) ***Leaving Compromised Systems Vulnerable***

- One of the more difficult decisions is whether to shut down a compromised system or collect some data from it beforehand.
- Processes in memory, network state tables, and encrypted disks may contain valuable data that are lost when a system is shut down. However, examining a live system is prone to error and may change data on the system, and can even cause the system to stop functioning.

Case Example: Dangers of Investigating Live Systems

- A routine vulnerability scan of a network detected a Trojan horse program running on a Windows XP server. Because of the critical role that this server played in the organization, a rapid response as well as recovery was required. The organization was unwilling to take the server offline because that would disrupt business operations. They wanted the server to be fixed quickly and were not concerned with apprehending the culprit. Digital investigators determined that the server had been compromised via IIS and found Web server **access logs** that corresponded with the initial intrusion **containing the intruder's IP address**. Additionally, they found that the Trojan horse executable was named "wlogin.exe" and was installed as a service • named "WinLogin" as shown in the following Registry key:

- D:\>regdmp
- \Registry
- <cut for brevity>
- (HKLM\System\CurrentControlSet\Services)
 - WinLogin
 - Type = REG_DWORD
 - 0x00000110
 - Start = REG_DWORD
 - 0x00000004
 - ErrorControl =
 - REG_DWORD 0x00000000
 - ImagePath = REG_EXPAND_SZ
 - “C:\WINNT\System32\wlogin.exe”
 - DisplayName = WinLogin

Furthermore, NT Application Event logs showed that Norton AntiVirus had detected the Trojan Horse but had not been able to remove it:

- D:\>dumpel -c -l application
 - <cut for brevity>
- 1/19/2010,12:32:48 AM,4,0,20,Norton AntiVirus,N/A,CONTROL,
Unable to restore C:\WINNT\system32\wlogin.exe from backup file after
clean failed.
- 1/19/2010,1:09:11 AM,1,0,5,Norton AntiVirus,N/A, CONTROL, Virus
Found!Virus name: BO2K.
 - Trojan Variant in File: C:\WINNT\Java\w.exe by: Scheduled scan.
Action: Clean failed : Quarantine succeeded : Virus Found!Virus name:
BO2K.Trojan Variant in File: C:\WINNT\system32\ wlogin.exe by:
Scheduled scan. Action: Clean failed : Quarantine failed:
- 1/19/2010,1:09:11 AM,4,0,2,Norton AntiVirus,N/A, CONTROL, Scan
Complete: Viruses: 2 Infected:2 Scanned:62093
Files/Folders/DrivesOmitted:89

Observing the Intruder in Progress

- In many forms of criminal investigations, it can be beneficial for digital investigators to observe the suspect in the act of committing a crime. This will allow the digital investigator to gather additional information that can be used to identify and prosecute that suspect.

Facts about Intrusion Investigations

- Computer intrusions can be **extremely complex**, most especially those that extend across an enterprise network. Further observation may be necessary to determine the true scope of the incident.
- Some intruders are **skilled in hiding or erasing the traces** of their activities. If they are not observed in action, there may not be enough evidence left behind to pursue investigative goals.
- Many organizations are not architected and configured to retain the types of electronic records (log files, for example) that would enable an effective post-mortem investigation. Therefore, observation of current events is much more critical.

Highly Competent Adversaries

- Knowledge of computer programming, including the ability to write programs to accomplish specific tasks.
 - Knowledge of system administration, including the ability to modify system configurations in order to hide traces of an attack or reduce or remove logging.
 - Knowledge of network administration, including understanding of common network devices and architectures, how to set up communications throughout an enterprise, and how to locate and identify high-value target systems.
 - Knowledge of computer intrusion techniques, including methods for circumventing or bypassing common security measures.
 - Knowledge of digital forensics, including an understanding of the nature and location of common intrusion artifacts.

Handling and Analysis of Malicious Code

- The identity of command and control servers with which malicious code is programmed to communicate
- The names and storage locations of additional files that are related to the malicious code, such as related executables, configuration files or Registry entries, a keystroke log, or an archive of stolen data.
- The purpose of the malicious code, that is, whether it is to create a backdoor, capture keystrokes, spread itself via some specific mechanism, etc.

Linking Events to an Actual Person

- It is important to remember that linking events to an actual person is a concern for all digital investigations, and especially so with computer intrusions.
- Tracing events to a specific computer system is not sufficient to claim that a specific person was using that computer system during the time of those events, and that that same person was responsible for the observed events.

Forensic Preservation of Volatile Data

Understanding Volatile Data

Volatile data are considered to be temporary or delicate in some way. Traditionally, *volatile data is taken to mean information stored in the RAM or memory of a computer system that will be lost when the power to that system is deactivated or otherwise removed.*

- Listing showing details about processes running on a Windows system.

Process information for VWKS-02:

Name	Pid	Pri	Thd	Hnd	Priv	CPU Time	Elapsed Time
Idle	0	0	1	0	0	4:26:28.125	0:00:00.000
System	4	8	94	524	44	0:01:43.203	21:31:41.545
smss	268	11	2	29	220	0:00:00.328	21:31:41.530
csrss	432	13	9	653	2184	0:00:01.390	21:31:12.702
wininit	480	13	3	74	860	0:00:00.406	21:31:11.873
csrss	488	13	7	448	1424	0:00:02.328	21:31:11.873
winlogon	528	13	5	127	1772	0:00:00.843	21:31:11.702
services	556	9	19	236	3740	0:00:04.484	21:31:11.389
lsass	568	9	6	601	2748	0:00:02.984	21:31:11.264
lsm	576	8	10	149	1248	0:00:00.812	21:31:11.248
svchost	696	8	10	351	2600	0:00:02.296	21:31:10.077
svchost	764	8	13	304	3012	0:00:01.265	21:31:09.342
svchost	816	8	20	472	12548	0:00:03.453	21:31:09.202
svchost	916	8	19	458	28160	0:00:31.515	21:31:08.467
svchost	944	8	37	1263	18908	0:00:18.359	21:31:08.248
svchost	1128	8	10	524	4460	0:00:03.421	21:31:05.342

RFC 3227 "Order of Volatility"

Areas traditionally considered
"volatile"

Areas traditionally considered
"non-volatile"

-
- 1. Registers, cache
 - 2. Routing table, arp cache, process table, kernel statistics, memory
 - 3. Temporary file systems
 - 4. Disk
 - 5. Remote logging and monitoring data that is relevant to the system in question
 - 6. Physical configuration, network topology
 - 7. Archival media

FIGURE 13.5
Order of volatility.

- Researchers at Princeton University have successfully shown that data do not disappear from RAM instantly once power is removed. In fact, the data in RAM persist long enough for the Princeton researchers to access RAM after a system has been powered off and to recover encryption keys from the contents. While this is more of an attacker tactic, there are forensic applications for their findings as well. At the very least, they have shown that RAM is not quite as volatile as was traditionally believed. Their interesting findings aside, it is still generally considered more practical for digital investigators to dump memory from a running system than to perform a cold boot acquisition. (Halderman et al., 2008).

Preserving Volatile Data

- When dealing with a computer intrusion, a typical digital investigator might use a script that will execute multiple commands in quick succession and collect the types of volatile data that are considered most important. This will commonly include commands that will collect items such as the following:
 - ***Operating system date and time:*** Critical for comparison to a central time source so that any variance in the time settings of the target system can be identified.
 - ***List of running processes:*** Collected so that an examiner can later identify unauthorized or malicious processes that may have been active on the system.
 - ***List of loaded drivers or modules:*** Collected to identify unauthorized or malicious code that may be loaded as a driver or module as opposed to a library or standard process.
 - ***List of loaded libraries for each process:*** Collected to identify unauthorized or malicious code that may be running as a library loaded into an otherwise legitimate process.

- ***List of open sockets and active network connections by process:*** Collected to identify any unauthorized communication sessions or open sockets that were active on the target system.
- ***Network configuration:*** Collected for various reasons, including the identification of anomalous configuration settings, as well as to simply understand the role of the system in the network in which it resides.
- ***List of file and Registry handles by process:*** Collected for various reasons, such as to make a determination as to what files and Registry entries may be connected to malicious processes.
- ***List of currently authenticated users:*** Collected to determine if there are any unauthorized authentications to the target system.

Sample Volatile Data Preservation Process

- **A typical process that digital investigators follow to preserve volatile data from a single system is outlined below.**
- 1. Perform an initial physical inspection of the target device, including photographing or noting the physical condition of the device, external markings such as serial numbers, etc. While doing this, the digital investigator notes the input/output options available on the device.
- 2. Authenticate to the console (monitor and keyboard as opposed to remote access) of the device using administrative credentials. Administrative credentials are typically required to execute some volatile data collection commands.
- 3. Note the contents of the screen after logon, including any windows that may be open or were opened automatically during logon. Should there be no obvious destructive processes active, the digital investigator will continue.

4. Insert a forensically prepared “clean” toolkit (created from trusted sources in such a way that it minimizes calls to libraries on the system). In this example, consider this toolkit to be on a CD.

5. Locate and identify the trusted shell executable on the CD, and start that shell (e.g., cmd.exe). Running a trusted shell as opposed to the local command line shell helps to circumvent interference by less sophisticated rootkits .

•6. Execute a command to change the path variable for the shell, so that the operating system will look on the toolkit CD for programs and libraries before turning to the local system where executables and libraries are not trusted.

7. Insert a wiped and formatted USB drive that will serve as the destination for any volatile data collection output. When dealing with systems that contain large amounts of memory, care must be taken to use a USB device large enough to store the full contents of memory.

8. Execute a command that will extract and present the date and time of the system. This date and time should be recorded in documentation and compared with a trusted time source, noting any discrepancy.

9. Execute a script that will perform the following actions:

- a.** Execute a command that will collect a memory dump and output it to the destination USB drive.
- b.** Execute a series of targeted commands that will collect data types
- c.** Create and record hash values for all outputs.

10. Close the trusted shell and eject all media used in the collection, and note the date and time in documentation.

Investigation of Malicious Computer Programs

Goals

The ultimate goal of analyzing malware in an intrusion investigation will vary depending on the specific circumstances. For instance, in data theft cases, the goal of malware analysis may be to determine how the data was stolen and who was responsible. As another example, when investigating a large-scale network intrusion, the goal may be to identify all affected systems and mitigate the threat. To achieve these ultimate goals, it may be necessary to pursue more discrete objectives, such as identifying specific malware samples or extracting sensitive information from infected systems.

- What is the primary purpose (or purposes) of the code?
 - If the purpose is to steal or destroy information, what types of information does it target (e.g., passwords, keyboard input, files)?
 - Does the program automatically create, delete, or alter any specific files?
 - Does the program create additional processes or inject itself into other processes?
 - Does the program automatically create, delete, or alter any specific Windows Registry keys, or other operating system configuration options on other operating systems?
 - Does the program accept remote network connections?
 - Does the program initiate any network connections, and if so how are the remote hosts identified?
 - Does the program intercept or otherwise interfere with any legitimate operations of the system?
 - Can the author/origination of the malware be determined?

Analysis Strategies

Automated Scanning

Digital investigators can use automated tools to identify and deconstruct the code.

Static File Inspection

Digital investigators can inspect a static file with some simple techniques to determine its nature.

Dynamic Analysis

Dynamic analysis of malware involves executing the code to observe its actions.

Virtualization

Loading a forensic duplicate into a virtualized environment enables digital investigation.

Disassembly and De-Compilation

This is the process of taking a binary executable and restoring it back to either assembly or source code.

Safety

malicious code should never be analyzed from a system that is networked with the Internet.

Examining the Intruder's Computer

- Lists of dial-up accounts and passwords, including the one used to Commit crime.
- Nmap scans of target networks.
- Lists of compromised hosts (trophy list and memory aid).
- List of UNIX commands executed on compromised hosts (memory aid).
- Sniffer logs from compromised hosts (digital evidence transfer).
- Directory listings from compromised UNIX hosts (digital evidence transfer).
- Stolen data from compromised hosts, including credit cards and private e-mail.
- TAR file with class characteristics linking it to compromised UNIX host.
- RAR file with stolen data from compromised computer.
- Toolkits found on compromised hosts.
- FTP and terminal emulator configuration files relating to compromised hosts.

Guide to Computer Forensics and Investigations Fourth Edition

Chapter 4 Data Acquisition

Modified 9-23-10

Objectives

- 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

Objectives (continued)

- 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

Understanding Storage Formats for Digital Evidence

Understanding Storage Formats for Digital Evidence

- Two types of data acquisition
 - Static acquisition
 - Copying a hard drive from a powered-off system
 - Used to be the standard
 - Does not alter the data, so it's repeatable
 - Live acquisition
 - Copying data from a running computer
 - Now the preferred type, because of hard disk encryption
 - Cannot be repeated exactly—alters the data
 - Also, collecting RAM data is becoming more important
 - But RAM data has no timestamp, which makes it much harder to use

Understanding Storage Formats for Digital Evidence

- Terms used for a file containing evidence data
 - Bit-stream copy
 - Bit-stream image
 - Image
 - Mirror
 - Sector copy
- They all mean the same thing

Understanding Storage Formats for Digital Evidence

- Three formats
 - Raw format
 - Proprietary formats
 - Advanced Forensics Format (AFF)

Raw Format

- This is what the Linux dd command makes
- Bit-by-bit copy of the drive to a file
- Advantages
 - Fast data transfers
 - Can ignore minor data read errors on source drive
 - Most computer forensics tools can read raw format

Raw Format

- Disadvantages
 - Requires as much storage as original disk or data
 - Tools might not collect marginal (bad) sectors
 - Low threshold of retry reads on weak media spots
 - Commercial tools use more retries than free tools
 - Validation check must be stored in a separate file
 - Message Digest 5 (MD5)
 - Secure Hash Algorithm (SHA-1 or newer)
 - Cyclic Redundancy Check (CRC-32)

Proprietary Formats

- Features offered
 - Option to compress or not compress image files
 - Can split an image into smaller segmented files
 - Such as to CDs or DVDs
 - With data integrity checks in each segment
 - Can integrate metadata into the image file
 - Hash data
 - Date & time of acquisition
 - Investigator name, case name, comments, etc.

Proprietary Formats

- Disadvantages
 - Inability to share an image between different tools
 - File size limitation for each segmented volume
 - Typical segmented file size is 650 MB or 2 GB
- Expert Witness format is the unofficial standard
 - Used by EnCase, FTK, X-Ways Forensics, and SMART
 - Can produce compressed or uncompressed files
 - File extensions **.E01, .E02, .E03, ...**

Advanced Forensics Format

- Developed by Dr. Simson L. Garfinkel of Basis Technology Corporation
- 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

Advanced Forensics Format (continued)

- Design goals (continued)
 - Internal consistency checks for self-authentication
- File extensions include **.afd** for segmented image files and **.afm** for AFF metadata
- AFF is open source

Determining the Best Acquisition Method

Determining the Best Acquisition Method

- Types of acquisitions
 - **Static acquisitions** and **live acquisitions**
- Four methods
 - Bit-stream disk-to-image file
 - Bit-stream disk-to-disk
 - Logical
 - Sparse

Bit-stream disk-to-image file

- Most common method
- Can make more than one copy
- Copies are bit-for-bit replications of the original drive
- Tools: ProDiscover, EnCase, FTK, SMART, Sleuth Kit, X-Ways, iLook

Bit-stream disk-to-disk

- Used when disk-to-image copy is not possible
 - Because of hardware or software errors or incompatibilities
 - This problem is more common when acquiring older drives
- Adjusts target disk's geometry (cylinder, head, and track configuration) to match the suspect's drive
- Tools: EnCase, SafeBack (MS-DOS), Snap Copy

Logical Acquisition and Sparse Acquisition

- When your time is limited, and evidence disk is large
- Logical acquisition captures only specific files of interest to the case
 - Such as Outlook **.pst** or **.ost** files
- Sparse acquisition collects only some of the data
 - I am finding contradictory claims about this—wait until we have a real example for clarity

Compressing Disk Images

- Lossless compression might compress a disk image by 50% or more
- But files that are already compressed, like ZIP files, won't compress much more
 - Error in textbook: JPEGs use lossy compression and degrade image quality (p. 104)
- Use MD5 or SHA-1 hash to verify the image

Tape Backup

- When working with large drives, an alternative is using tape backup systems
- No limit to size of data acquisition
 - Just use many tapes
- But it's slow

Returning Evidence Drives

- In civil litigation, a discovery order may require you to return the original disk after imaging it
- If you cannot retain the disk, make sure you make the correct type of copy (logical or bitstream)
 - Ask your client attorney or your supervisor what is required—you usually only have one chance

Contingency Planning for Image Acquisitions

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 (link Ch 4c)
- Be prepared to deal with encrypted drives
 - **Whole disk encryption** feature in Windows Vista Ultimate and Enterprise editions

Encrypted Hard Drives

- Windows BitLocker
- TrueCrypt
- If the machine is on, a live acquisition will capture the decrypted hard drive
- Otherwise, you will need the key or passphrase
 - The suspect may provide it
 - There are some exotic attacks
 - Cold Boot (link Ch 4e)
 - Passware (Ch 4f)
 - Electron microscope (Ch 4g)

Using Acquisition Tools

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

Windows Write-Protection with USB Devices

- USB write-protection feature
 - Blocks any writing to USB devices
- Target drive needs to be connected to an internal PATA (IDE), SATA, or SCSI controller
- Works in Windows XP SP2, Vista, and Win 7

Acquiring Data with a Linux Boot CD

- Linux can read hard drives that are mounted as read-only
- Windows OSs and newer Linux automatically mount and access a drive
- Windows will write to the Recycle Bin, and sometimes to the 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
- All these changes corrupt the evidence

Forensic Linux Live CDs

- Configured not to mount, or to mount as read-only, any connected storage media
- Well-designed Linux Live CDs for computer forensics
 - Helix
 - Penguin Sleuth
 - FCCU (French interface)
- Preparing a target drive for acquisition in Linux
 - Modern linux distributions can use Microsoft FAT and NTFS partitions

Acquiring Data with a Linux Boot CD (continued)

- Preparing a target drive for acquisition in Linux (continued)
 - **fdisk** command lists, creates, deletes, and verifies partitions in Linux
 - **mkfs.msdos** command formats a FAT file system from Linux
- 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

Acquiring data with dd in Linux

- 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
- dd command is intended as a data management tool
 - Not designed for forensics acquisitions

Acquiring data with dcfldd in Linux

- 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

Capturing an Image with ProDiscover

Basic

- Connecting the suspect's drive to your workstation
 - Document the chain of evidence for the drive
 - Remove the drive from the suspect's computer
 - Configure the suspect drive's jumpers as needed
 - Connect the suspect drive to a **write-blocker device**
 - Create a storage folder on the target drive
- Using ProDiscover's Proprietary Acquisition Format
 - Image file will be split into segments of 650MB
 - Creates image files with an .eve extension, a log file (.log extension), and a special inventory file (.pds extension)

Capturing an Image with ProDiscover Basic (continued)

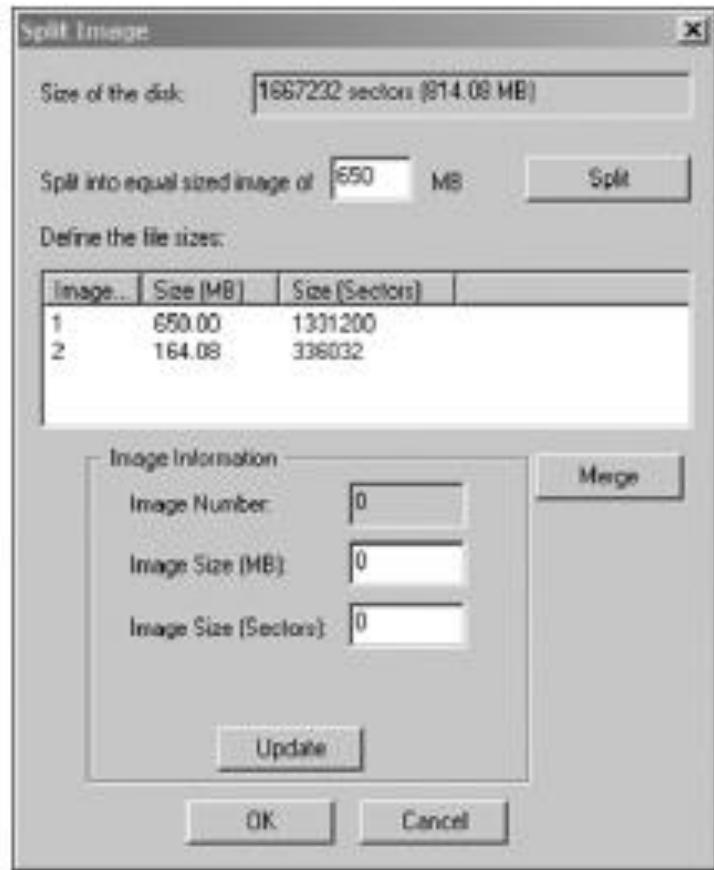


Figure 4-4 The Split Image dialog box

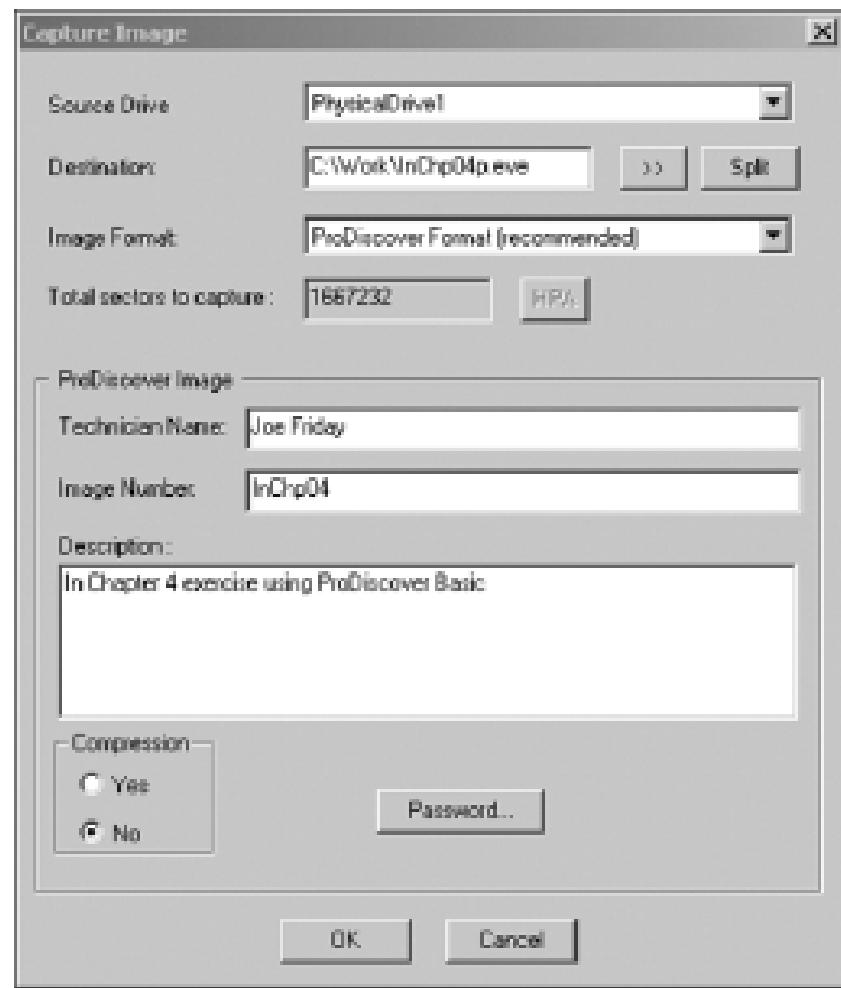


Figure 4-5 The Capture Image dialog box

Capturing an Image with ProDiscover Basic (continued)

- Using ProDiscover's Raw Acquisition Format
 - Select the UNIX style dd format in the Image Format list box
 - Raw acquisition saves only the image data and hash value

Capturing an Image with AccessData FTK Imager

- Included on AccessData Forensic Toolkit
- View 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 the USB write-protection Registry feature enabled
- FTK Imager can't acquire drive's host protected area (but ProDiscover can)

Capturing an Image with AccessData FTK Imager (continued)

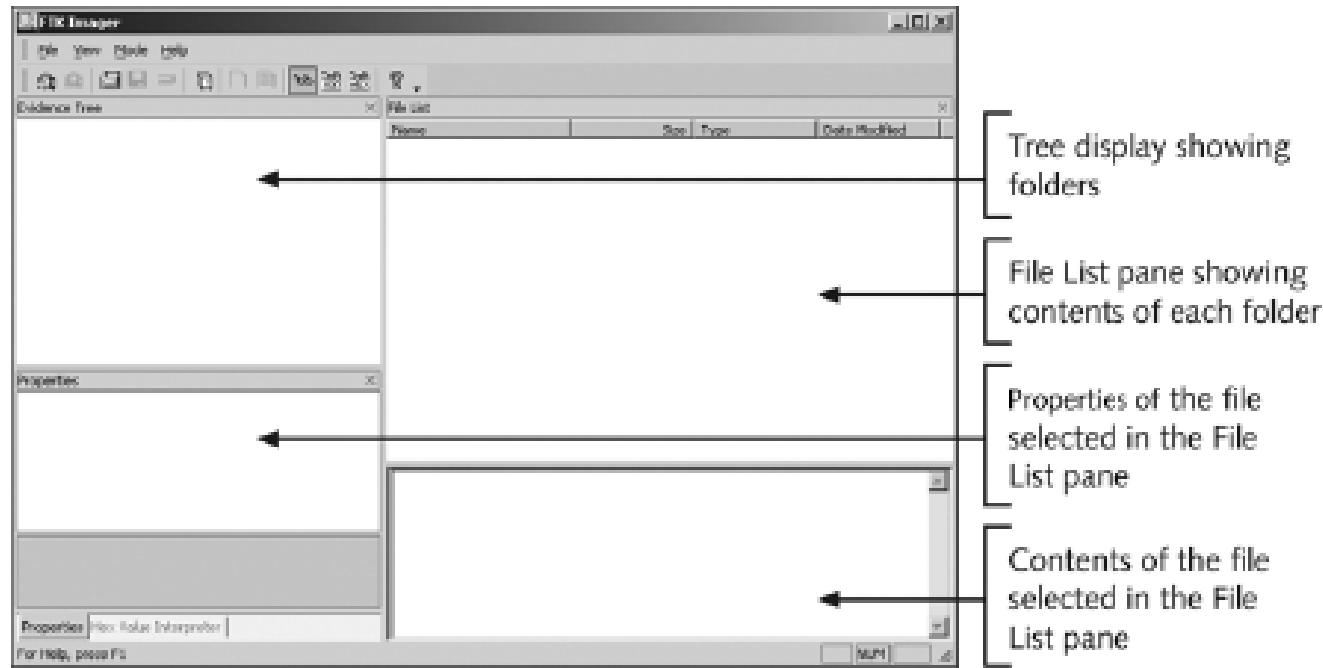


Figure 4-6 The FTK Imager main window

Capturing an Image with AccessData FTK Imager (continued)

- Steps
 - Boot to Windows
 - Connect evidence disk to a write-blocker
 - Connect target disk
 - Start FTK Imager
 - Create Disk Image
 - Use Physical Drive option

Capturing an Image with AccessData FTK Imager (continued)

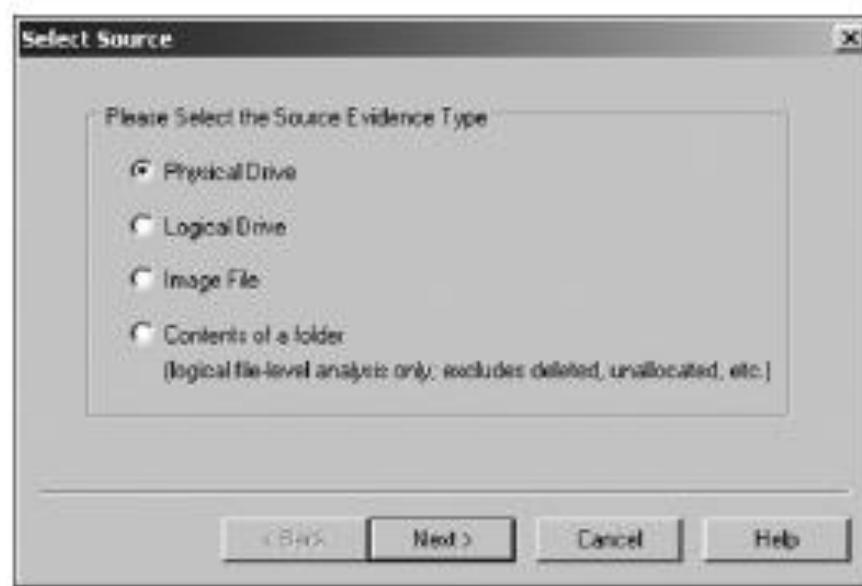


Figure 4-7 The Select Source dialog box

Capturing an Image with AccessData FTK Imager (continued)

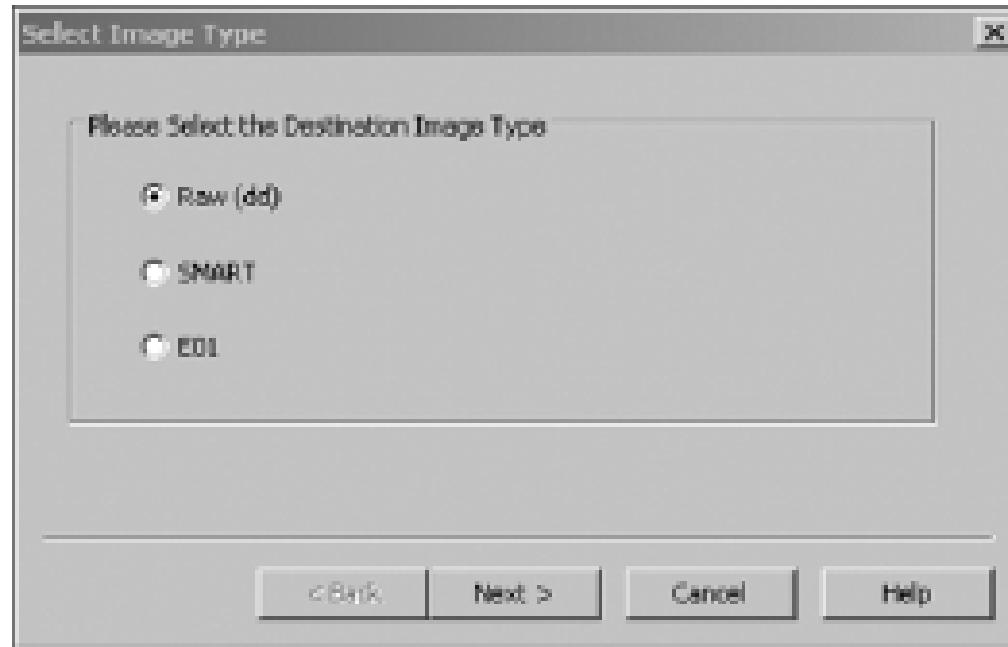


Figure 4-8 The Select Image Type dialog box

Capturing an Image with AccessData FTK Imager (continued)

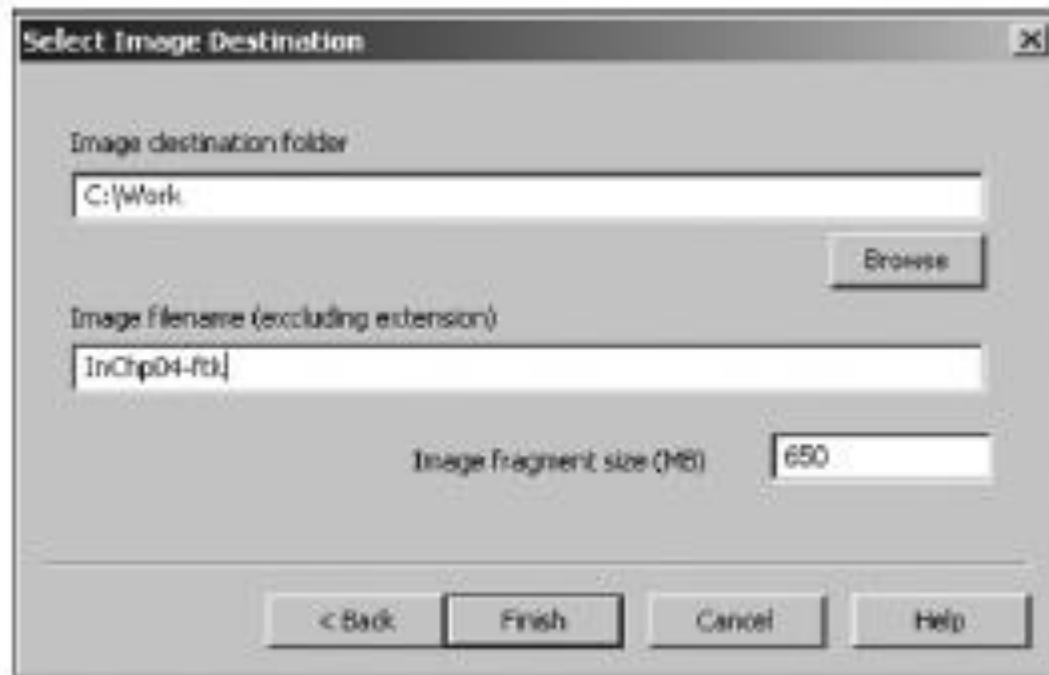


Figure 4-9 Selecting where to save the image file

Capturing an Image with AccessData FTK Imager (continued)

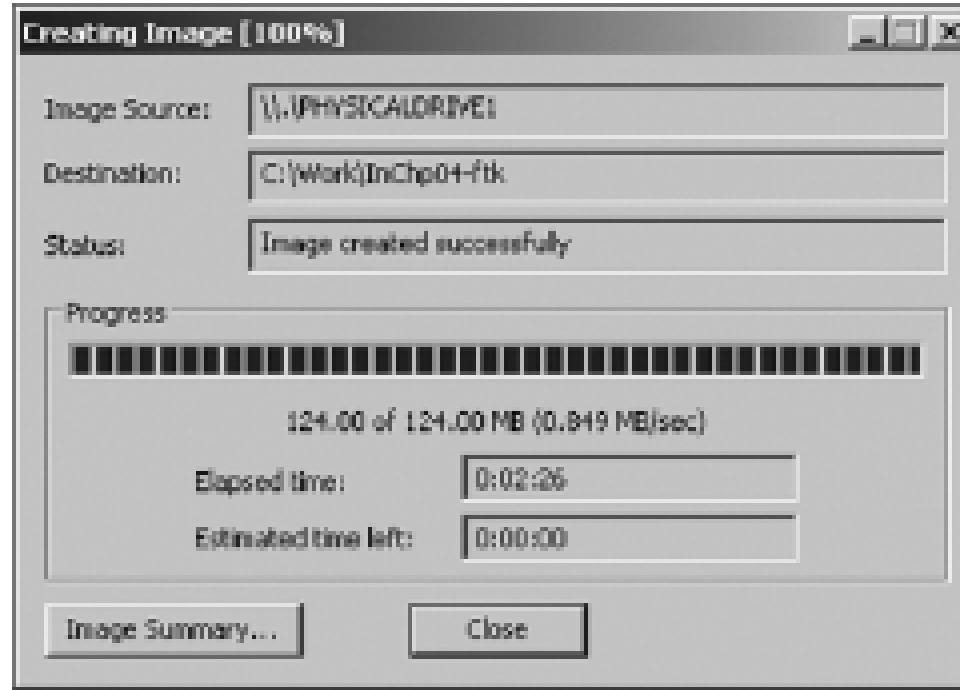


Figure 4-10 A completed image save

Validating Data Acquisitions

Validating Data Acquisitions

- 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
- A new hashing function will soon be chosen by NIST

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

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

Performing RAID Data Acquisitions

Performing RAID Data Acquisitions

- Size is the biggest concern
 - Many RAID systems now have terabytes of data

Understanding RAID

- **Redundant array of independent (formerly “inexpensive”) 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
 - Lack of redundancy
- RAID 1 (Mirrored)
 - Designed for data recovery
 - More expensive than RAID 0

Understanding RAID (continued)

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

Understanding RAID (continued)

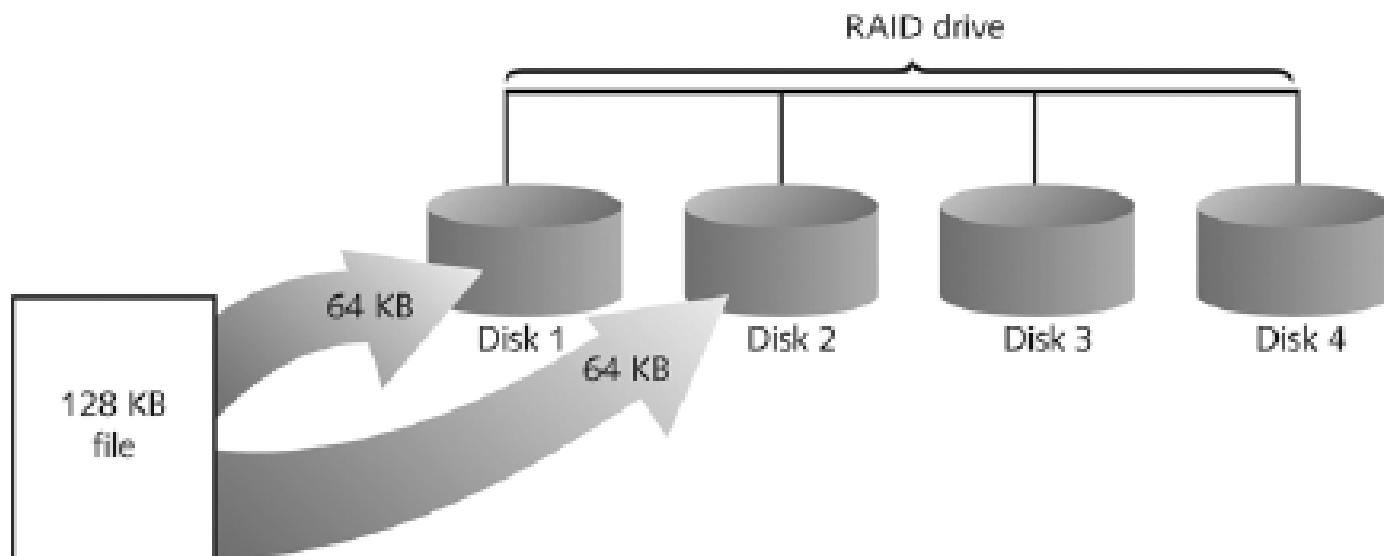


Figure 4-11 RAID 0: Striping

Understanding RAID (continued)

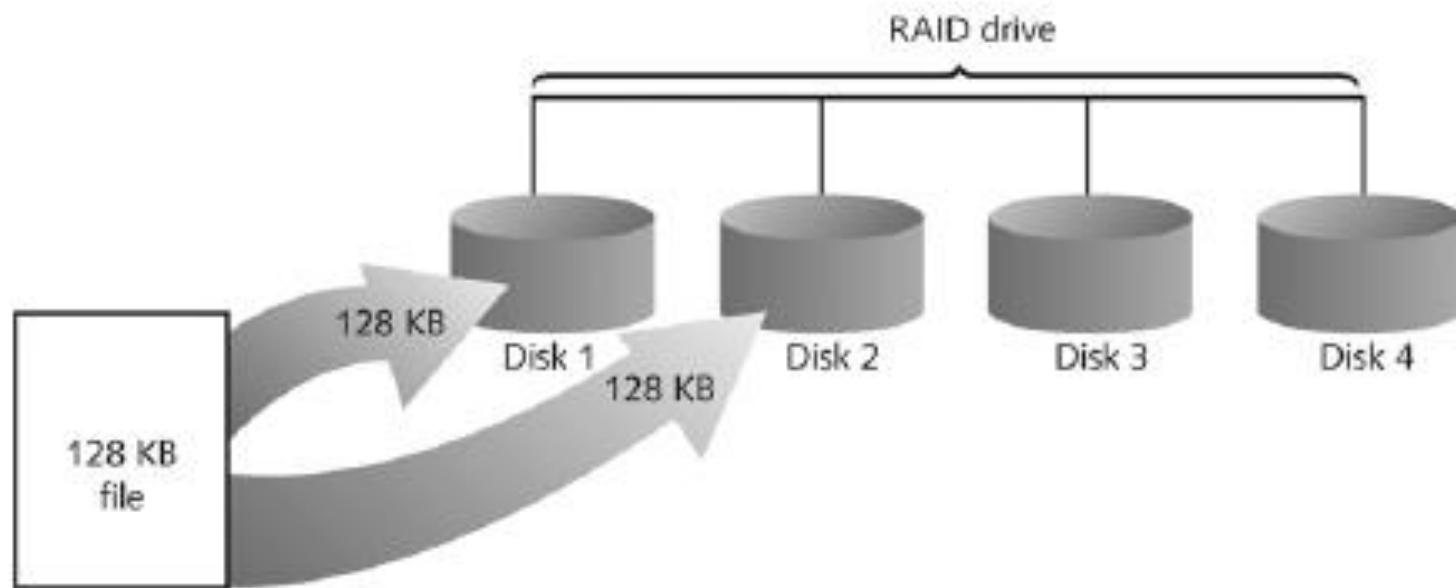


Figure 4-12 RAID 1: Mirroring

Understanding RAID (continued)

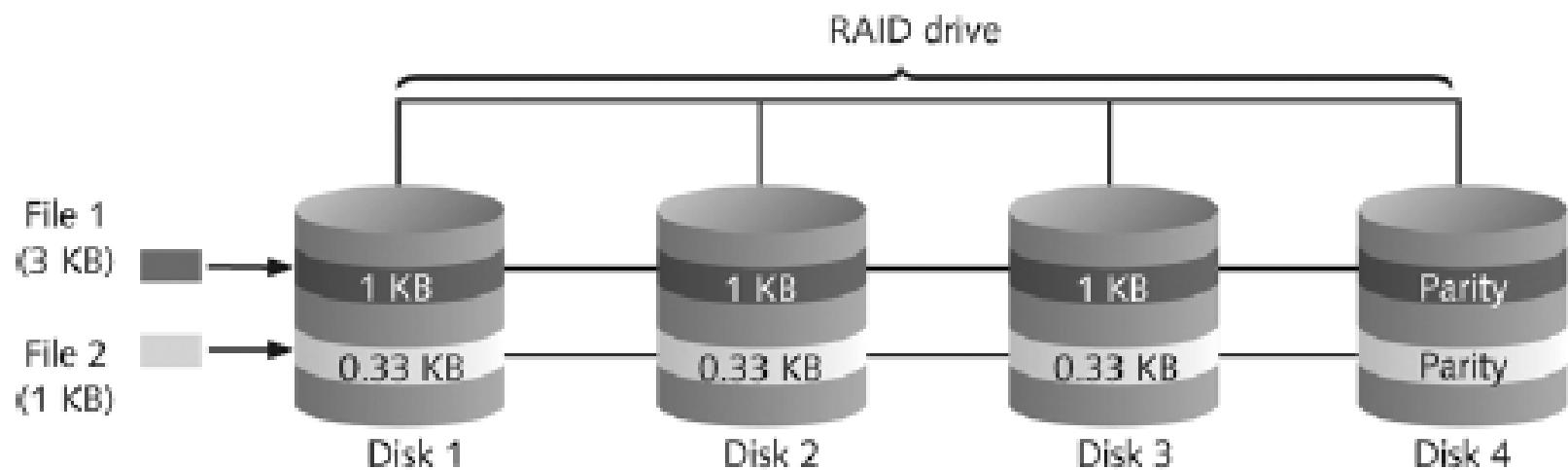


Figure 4-13 RAID 2: Striping (bit level)

Understanding RAID (continued)

- RAID 5
 - Similar to RAIDs 0 and 3
 - Places parity recovery data on each disk
- RAID 6
 - Redundant parity on each disk
- RAID 10, or mirrored striping
 - Also known as RAID 1+0
 - Combination of RAID 1 and RAID 0

Understanding RAID (continued)

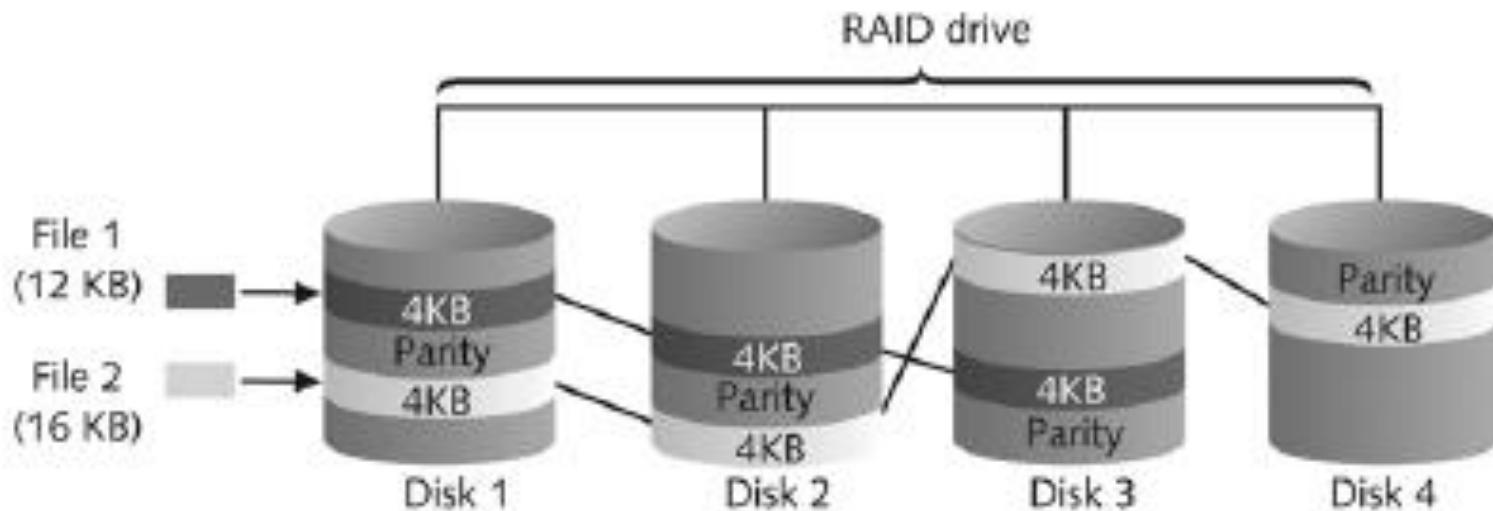


Figure 4-14 RAID 5: Block-level striping with distributed parity

Acquiring RAID Disks

- Concerns
 - How much data storage is needed?
 - What type of RAID is used?
 - 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?
- Older hardware-firmware RAID systems can be a challenge when you're making an image

Acquiring RAID Disks (continued)

- Vendors offering RAID acquisition functions
 - Technologies Pathways ProDiscover
 - Guidance Software EnCase
 - X-Ways Forensics
 - 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

Using Remote Network Acquisition Tools

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
 - LAN's data transfer speeds and routing table conflicts could cause problems
 - Gaining the permissions needed to access more secure subnets
 - Heavy traffic could cause delays and errors
 - Remote access tool could be blocked by antivirus

Remote Acquisition with ProDiscover Investigator

- Preview a suspect's drive remotely while it's in use
- Perform a live acquisition
 - Also called a “smear” because data is being altered
- Encrypt the connection
- Copy the suspect computer's RAM
- Use the optional stealth mode to hide the connection

Remote Acquisition with ProDiscover

Incident Response

- All the functions of ProDiscover Investigator plus
 - Capture volatile system state information
 - Analyze current running processes
 - Locate unseen files and processes
 - Remotely view and listen to IP ports
 - Run hash comparisons to find Trojans and rootkits
 - Create a hash inventory of all files remotely

PDServer Remote Agent

- ProDiscover utility for remote access
- Needs to be loaded on the suspect computer
- 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

Remote Connection Security Features

- Password Protection
- Encrypted communications
- Secure Communication Protocol
- Write Protected Trusted Binaries
- Digital Signatures

Remote Acquisition with EnCase Enterprise

- Remotely acquires media and RAM data
- Integration with intrusion detection system (IDS) tools
- Options to create an image of data from one or more systems
- Preview of systems
- A wide range of file system formats
- RAID support for both hardware and software

Other Remote Acquisition Tools

- R-Tools R-Studio
- WetStone LiveWire
- F-Response

Remote Acquisition with Runtime Software

- Compact Shareware Utilities
 - DiskExplorer for FAT
 - DiskExplorer for NTFS
 - HDHOST (Remote access program)
- Features for acquisition
 - Create a raw format image file
 - Segment the raw format or compressed image
 - Access network computers' drives

Using Other Forensics- Acquisition Tools

Using Other Forensics-Acquisition Tools

- Tools
 - SnapBack DatArrest
 - SafeBack
 - DIBS USA RAID
 - ILook Investigator IXimager
 - Vogon International SDi32
 - ASRData SMART
 - Australian Department of Defence PyFlag

SnapBack DatArrest

- Columbia Data Products
- Old MS-DOS tool
- Can make an image on three ways
 - Disk to SCSI drive
 - Disk to network drive
 - Disk to disk
- Fits on a forensic boot floppy
- SnapCopy adjusts disk geometry

NTI SafeBack

- Reliable MS-DOS tool
- Small enough to fit on a forensic boot floppy
- Performs an SHA-256 calculation per sector copied
- Creates a log file

NTI SafeBack (continued)

- Functions
 - Disk-to-image copy (image can be on tape)
 - Disk-to-disk copy (adjusts target geometry)
 - Parallel port laplink can be used
 - Copies a partition to an image file
 - Compresses image files

DIBS USA RAID

- Rapid Action Imaging Device (RAID)
 - Makes forensically sound disk copies
 - Portable computer system designed to make disk-to-disk images
 - Copied disk can then be attached to a write-blocker device

ILook Investigator IXimager

- IXimager
 - Runs from a bootable floppy or CD
 - Designed to work only with ILook Investigator
 - Can acquire single drives and RAID drives

ASRData SMART

- Linux forensics analysis tool that can make image files of a suspect drive
- Capabilities
 - Robust data reading of bad sectors on drives
 - Mounting suspect drives in write-protected mode
 - Mounting target drives in read/write mode
 - Optional compression schemes

Australian Department of Defence

PyFlag

- PyFlag tool
 - Intended as a network forensics analysis tool
 - Can create proprietary format Expert Witness image files
 - Uses sgzip and gzip in Linux

Guide to Computer Forensics and Investigations

Fourth Edition

Chapter 8
*Linux Boot Processes and File
Systems*

Objectives

- Explain Macintosh file structures and the boot process
- Explain UNIX and Linux disk structures and boot processes
- Describe other disk structures

Examining UNIX and Linux Disk Structures and Boot Processes

Examining UNIX and Linux Disk Structures and Boot Processes

- UNIX flavors
 - System V variants, Sun Solaris, IBM AIX, and HP-UX
 - BSD, FreeBSD, OpenBSD, and NetBSD
- Linux distributions
 - Red Hat, Fedora, Ubuntu, and Debian
 - Most consistent UNIX-like OSs
- Linux kernel is regulated under the **GNU General Public License (GPL)** agreement

Examining UNIX and Linux Disk Structures and Boot Processes

(continued)

- BSD license is similar to the GPL
 - But makes no requirements for derivative works
- Some useful Linux commands to find information about your Linux system
 - `uname -a`
 - `ls -l`
 - `ls -ul filename`
 - `netstat -s`

Table 8-4 UNIX system files

OS	System files	Purpose
AIX	/etc/exports	Configuration file
	/etc/filesystems	File system table of devices and mount points
	/etc/utmp	Current user's logon information
	/var/adm/wtmp	Logon and logoff history information
	/etc/security/lastlog	User's last logon information
	/var/adm/sulog	Substitute user attempt information
	/etc/group	Group memberships for the local system
	/var/log/syslog	System messages log
	/etc/security/passwd	Master password file for the local system
	/etc/security/failedlogin	Failed logon attempt information
HP-UX	/etc/utmp and /etc/utmpx	Current user's logon information
	/var/adm/wtmp and /var/adm/wtmpx	Logon and logoff history information
	/var/adm/btmp	Failed logon attempt information
	/etc/fstab	File system table of devices and mount points
	/etc/checklist	File system table information (version 9.x)
	/etc/exports	Configuration files
	/etc/passwd	Master password file for the local system
	/etc/group	Group memberships for the local system
	/var/adm/syslog.log	System messages log
	syslog	System log files
	/var/adm/sulog	Substitute user attempt information

Table 8-4 UNIX system files (continued)

OS	System files	Purpose
IRIX	/var/adm/syslog	System log files
	/etc(exports	Configuration files
	/etc/fstab	File system table of devices and mount points
	/var/adm/btmp	Failed logon information
	/var/adm/lastlog	User's last logon information
	/var/adm/wtmp and /var/adm/wtmpx	Logon and logoff history information
	/var/adm/sulog	Substitute user attempt information
	/etc/shadow	Master password file for the local system
	/etc/group	Group memberships for the local system
	/var/adm/utmp and /var/adm/utmpx	Current user's logon information
	/etc(exports	Configuration files
	/etc/fstab	File system table of devices and mount points
Linux	/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/messages	System messages log
	/etc/shadow	Master password file for the local system
	/etc/group	Group memberships for the local system
	/etc/passwd	Account information for local system
Solaris	/etc/group	Group information for local system
	/var/adm/sulog	Switch user log data
	/var/adm/utmp	Logon information
	/var/adm/wtmp, /var/adm/wtmpx, and /var/adm/lastlog	Logon history information
	/var/adm/loginlog	Failed logon information
	/var/adm/messages	System log files
	/etc/vfstab	Static file system information
	/etc/dfs/dfstab and /etc/vfstab	Configuration files

Examining UNIX and Linux Disk Structures and Boot Processes (continued)

- Linux file systems
 - **Second Extended File System (Ext2fs)**
 - Ext3fs, journaling version of Ext2fs
- Employs **inodes**
 - Contain information about each file or directory
 - Pointer to other inodes or blocks
 - Keep internal link count
 - Deleted inodes have count value 0

UNIX and Linux Overview

- Everything is a file
 - Including disks, monitors, NIC, RAM
 - Files are objects with properties and methods
- UNIX consists of four components
 - Boot block
 - Superblock
 - inode block
 - Data block

Boot Block and Superblock

- 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
- Superblock
 - Indicates disk geometry, available space, location of the first inode, and free inode list
 - Manages the file system
 - Multiple copies of the superblock are kept

inode Blocks and Data Blocks

- inode blocks
 - First data after the superblock
 - An inode is assigned to every file allocation unit
- Data blocks
 - Where directories and files are stored
 - This location is linked directly to inodes
 - Each sector contains 512 bytes
 - Each data block contains 1024-4096 bytes
 - Analogous to a cluster on a FAT or NTFS volume

UNIX and Linux Overview (continued)

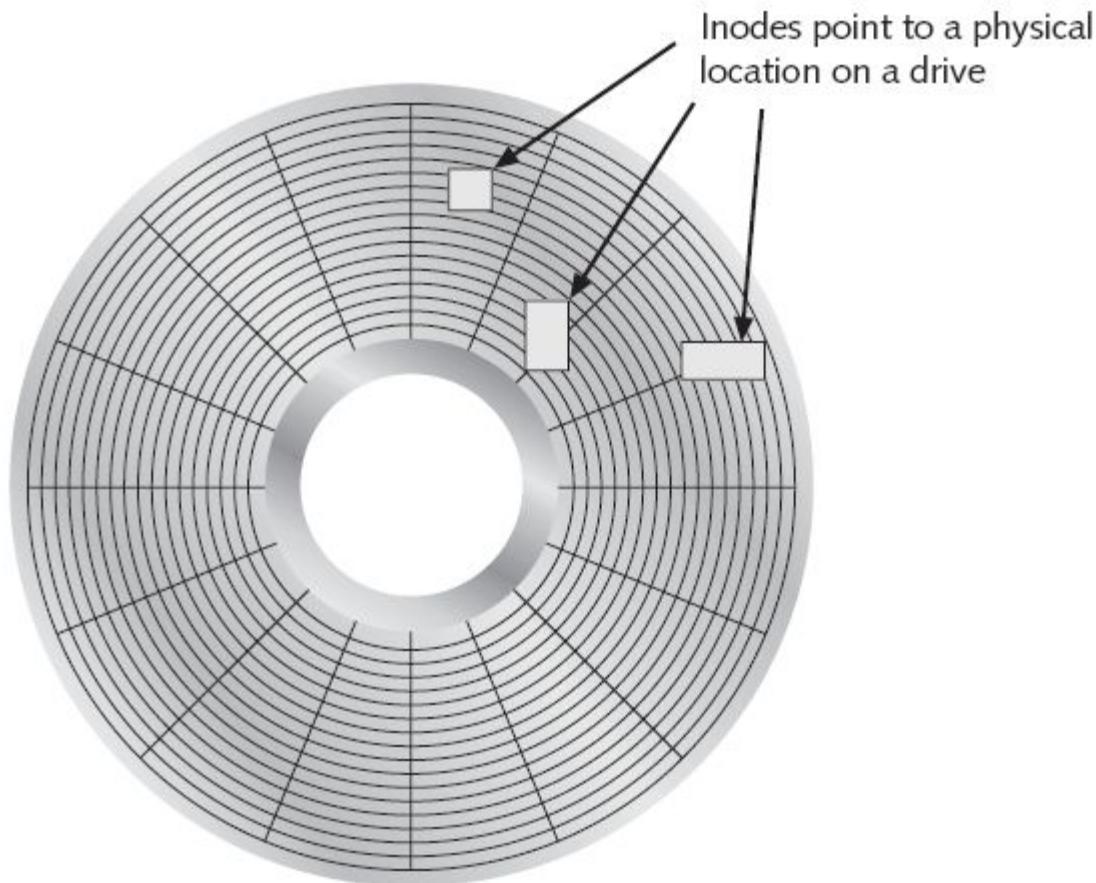


Figure 8-10 Clustering data blocks to save a file in Linux

UNIX and Linux Overview (continued)

- **Bad block inode**
 - Keeps track of disk's bad sectors
 - Commands: badblocks, mke2fs, and e2fsck
- Linux **ls** command displays information about files and directories
 - lowercase LS
- For details, use the **ls -l** command
 - lowercase LS –L

UNIX and Linux Overview (continued)

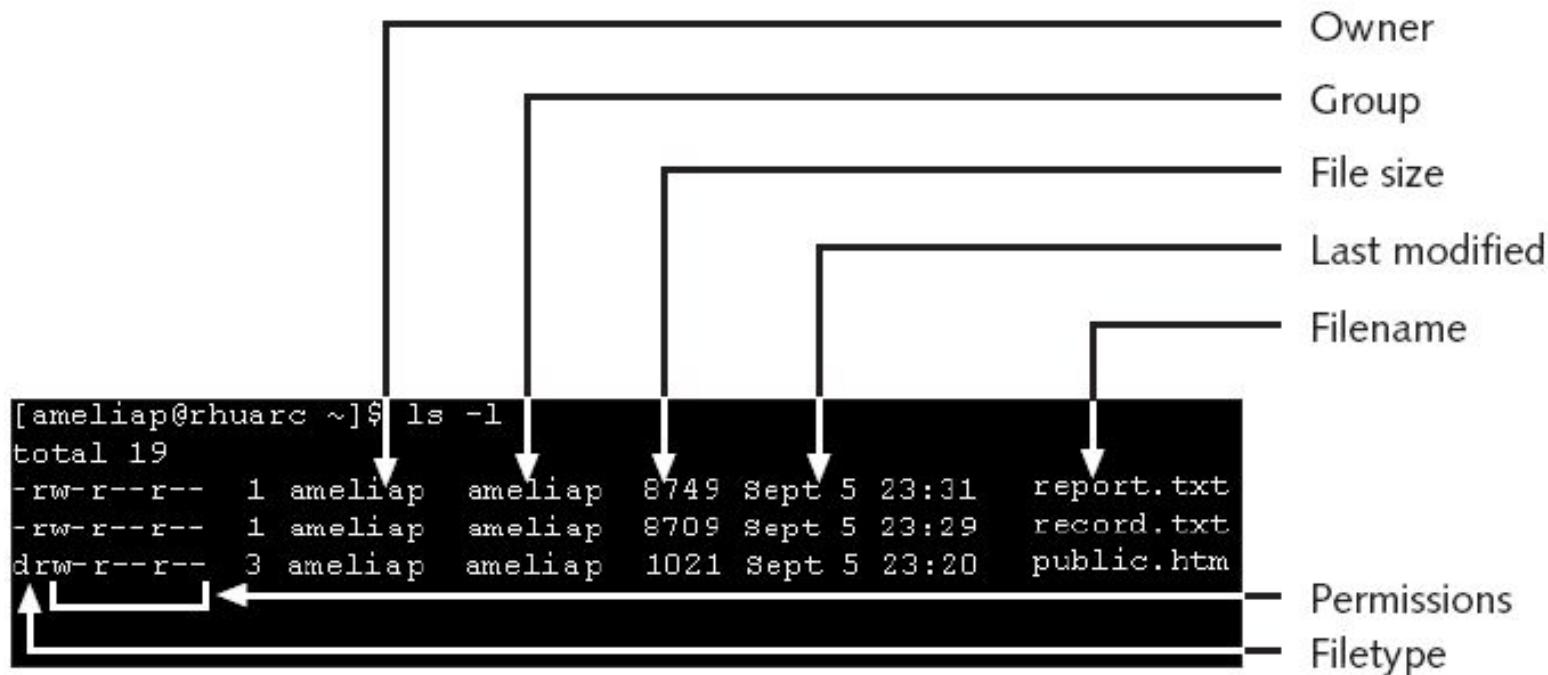


Figure 8-11 Finding information about a file

Continuation inode

- **Continuation inode**
 - Provides information about a file or directory
 - Mode and file type, the quantity of links in the file or directory, the file or directory status flag
 - Sticky bit
 - Used in some old Unix versions to make programs load faster by keeping parts of the program in RAM
 - Used in modern Unix systems to prevent users from deleting files owned by others
 - Link Ch 8h

UNIX and Linux Overview (continued)

Table 8-5 Code values for an inode

Code values	Description
4000	UID on execution—set
2000	GID on execution—set
1000	Sticky bit—set
0400	Read by owner—allowed
0200	Write by owner—allowed
0100	Execution/search by owner—allowed
0040	Read by group—allowed
0020	Write by group—allowed
0010	Execution/search by group—allowed
0004	Read by others—allowed
0002	Write by others—allowed
0001	Execution/search by others—allowed

Understanding Inodes

- Link data stored in data blocks (usually 1024 bytes)
- Ext2fs and Ext3fs are improvements over Ext
 - Data recovery easier on Ext3fs than on Ext2fs
- First inode has 13 pointers
 - Pointers 1 to 10 are direct pointers to data storage blocks
 - Pointer 11 is an **indirect pointer**
 - Pointer 12 is a **double-indirect pointer**
 - Pointer 13 is a **triple-indirect pointer**
 - Pointers 11-13 are needed for large files

Inode pointers

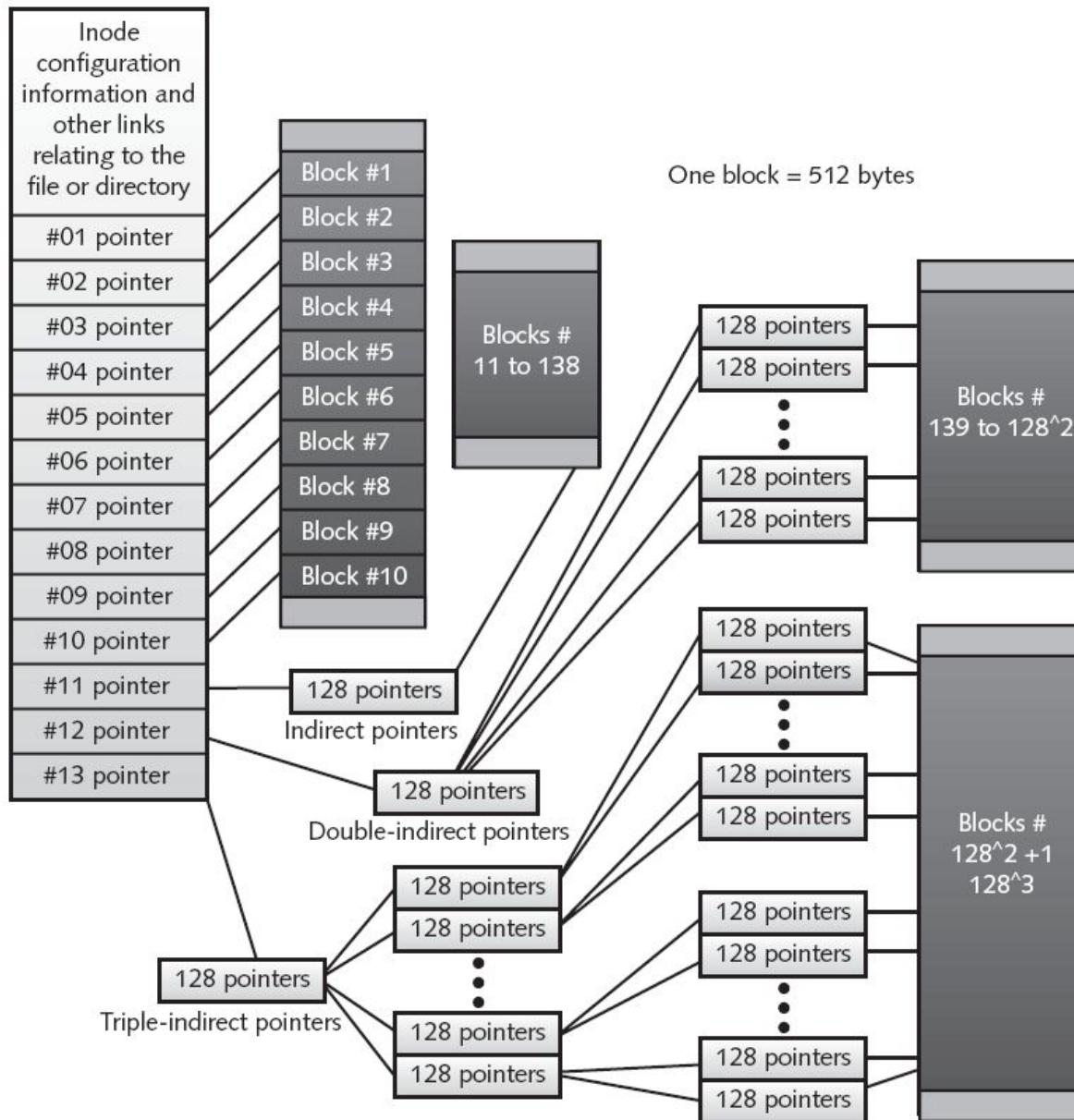


Figure 8-12 Inode pointers in the Linux file system

Understanding Inodes (continued)

Table 8-6 UNIX and Linux shell commands

Shell command	Associated options	Purpose
cat <i>file</i> more <i>file</i>		Displays the contents of a file (similar to the MS-DOS Type command)
dd	Refer to man pages for available options	Copies a disk drive by blocks, which is the same as creating an image of a disk drive
df bdf (HP-UX)	-k (Solaris)	Displays partition information for local or NFS mounted partitions
find	Refer to man pages for available options	Locates files matching a specific attribute, such as name, last modification time, or owner
netstat	-a	Identifies other systems connected via the network to a UNIX or Linux system
ps	ax (BSD) -ef (System V)	Displays the status of OS processes
uname	-a	Displays the name of the system

Understanding UNIX and Linux Boot Processes

- Instruction code in firmware is loaded into RAM
 - This is called **memory-resident** code because it is stored in ROM
- Instruction code then:
 - Checks the hardware
 - Load the boot program
- Boot program
 - Loads kernel
 - Transfers control to kernel
- Kernel's first task is to identify all devices

Understanding UNIX and Linux Boot Processes (continued)

- Kernel
 - Boots system on single-user mode
 - Runs startup scripts
 - Changes to multiuser mode, then user logs on
 - Identifies root directory, swap, and dump files
 - Sets hostname and time zone
 - Runs consistency checks on the file system and mounts partitions
 - Starts services and sets up the NIC
 - Establishes user and system accounting and quotas

Understanding Linux Loader and GRUB

- Linux Loader (LILO)
 - Old boot manager
 - Can start two or more OSs
 - Uses configuration file /etc/lilo.conf
- Grand Unified Boot Loader (GRUB)
 - More powerful than LILO
 - As LILO, it resides on MBR
 - Command line or menu driven

Understanding UNIX and Linux Drives and Partition Schemes

- Labeled as path starting at root (/) directory
 - Primary master disk (/dev/hda)
 - First partition is /dev/hda1
 - Second partition is /dev/hda2
 - Primary slave or secondary master or slave (/dev/hdb, /dev/hdc, or /dev/hdd)
 - First partition is /dev/hdb2
 - SCSI controllers
 - /dev/sda with first partition /dev/sda1
 - Linux treats SATA, USB, and FireWire devices the same way as SCSI devices

Examining UNIX and Linux Disk Structures

- Most commercial computer forensics tools can analyze UNIX UFS and UFS2
 - And Linux Ext2, Ext3, ReiserFS, and Reiser4 file systems
- Freeware tools include Sleuth Kit and its Web browser interface, Autopsy Browser
- Foremost
 - A freeware carving tool that can read many image file formats
 - Configuration file: `foremost.conf`

Examining UNIX and Linux Disk Structures (continued)

- **Tarball**
 - A data file containing one or more files or whole directories and their contents
- Installing Sleuth Kit and Autopsy
 - Requires downloading and installing the most recent updates of these tools
 - Download the most current source code from www.sleuthkit.org
 - To run Sleuth Kit and Autopsy Browser, you need to have root privileges

Examining UNIX and Linux Disk Structures (continued)

```
[joe@fridaypi ~]$ cd /usr/local/autopsy-2.08
[joe@fridaypi autopsy-2.08]$ su
Password: *****
[joe@fridaypi autopsy-2.08]$ ./autopsy
=====
Autopsy Forensic Browser
http://www.sleuthkit.org/autopsy/
ver 2.08
=====
Evidence Locker: /home/joe/work
Start Time: Mon Jan 22 07:55:33 2007
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 8-13 Starting Autopsy from a Linux terminal window



Figure 8-14 The Autopsy main window

Examining UNIX and Linux Disk Structures (continued)

- Examining a case with Sleuth Kit and Autopsy
 - Use Sleuth Kit and Autopsy Browser to analyze a Linux Ext2 and Ext3 file system
 - See Figures 8-15 through 8-18

Examining UNIX and Linux Disk Structures (continued)

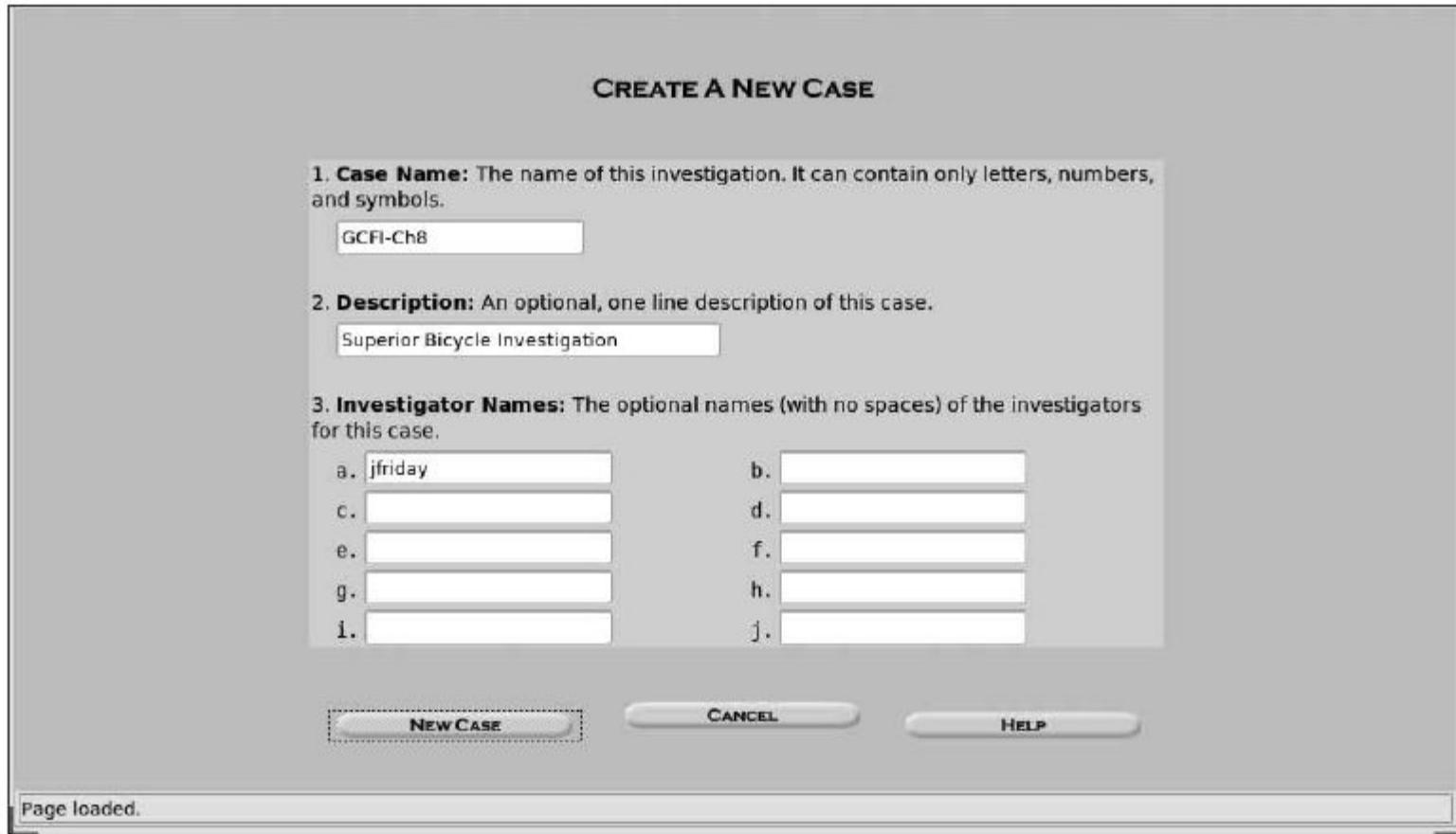


Figure 8-15 The Create A New Case dialog box

Examining UNIX and Linux Disk Structures (continued)

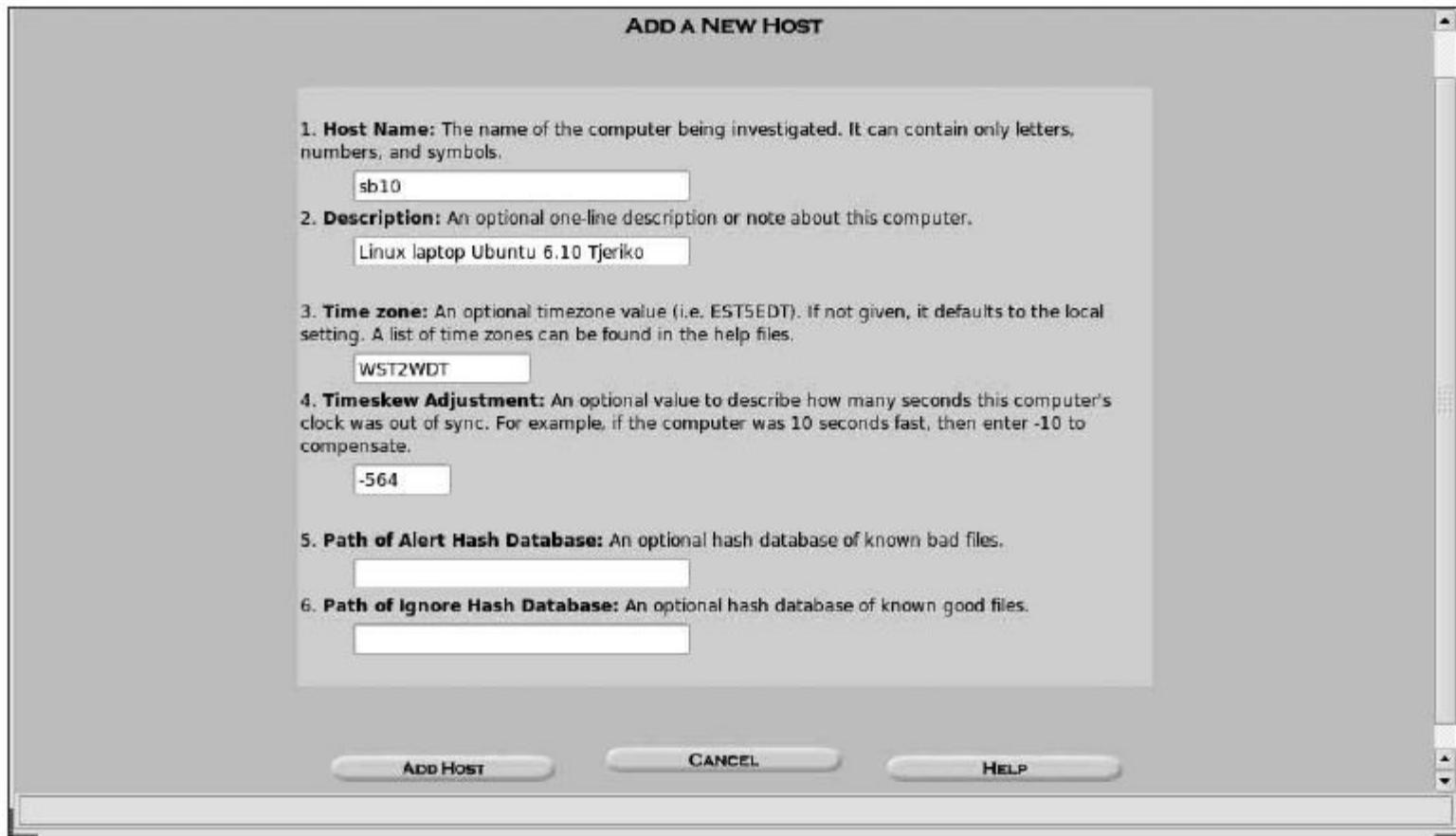


Figure 8-16 The Add A New Host dialog box

Examining UNIX and Linux Disk Structures (continued)



Figure 8-17 The Keyword Search dialog box

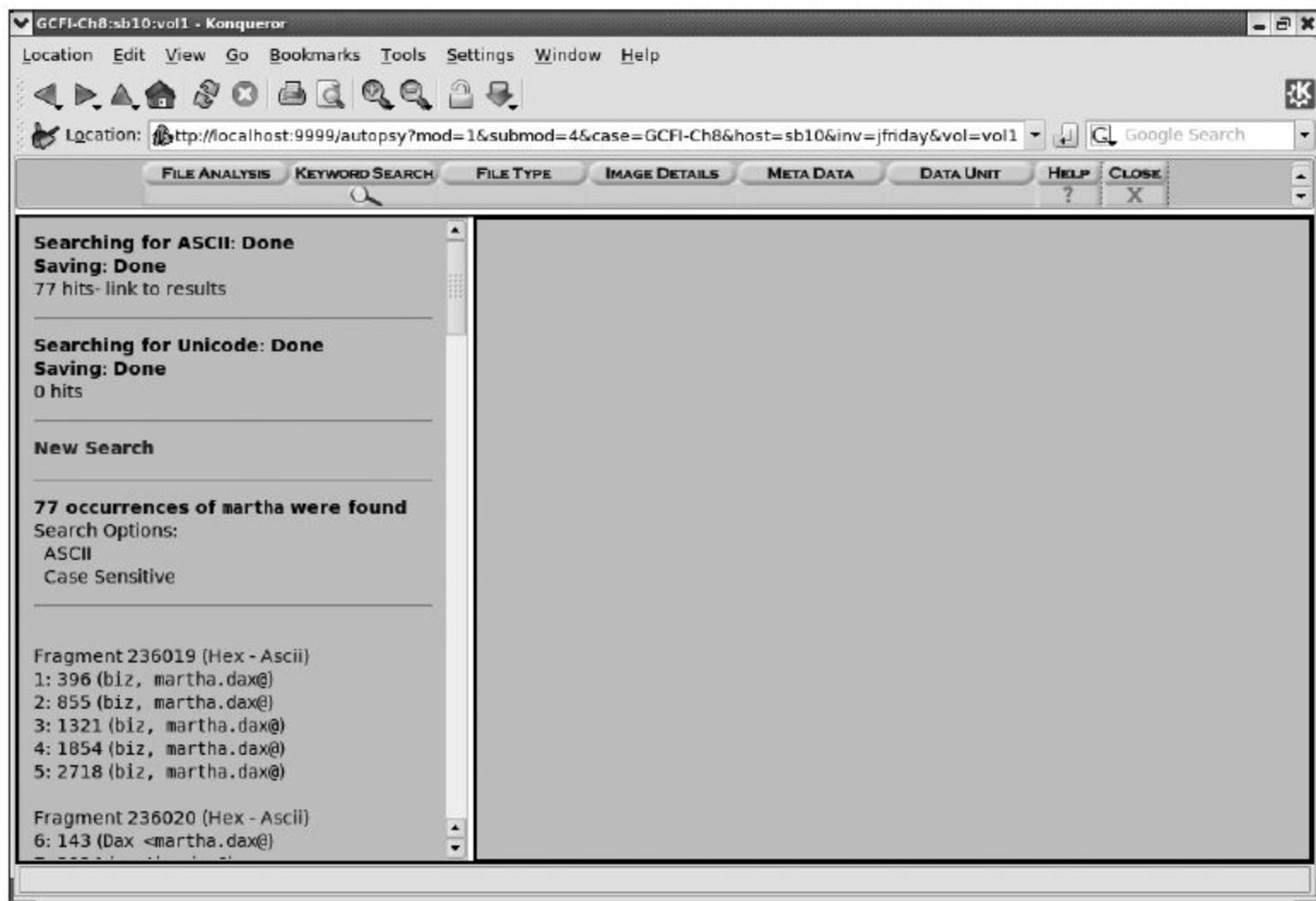


Figure 8-18 Summary of search results

Examining UNIX and Linux Disk Structures (continued)

- Examining a case with Sleuth Kit and Autopsy (continued)
 - Use the File Activity Time Lines function
 - Identifies what files were active at a specific time
 - See Figures 8-19 and 8-20

Examining UNIX and Linux Disk Structures (continued)



Figure 8-19 The Select a volume to analyze or add a new image file dialog box

Examining UNIX and Linux Disk Structures (continued)

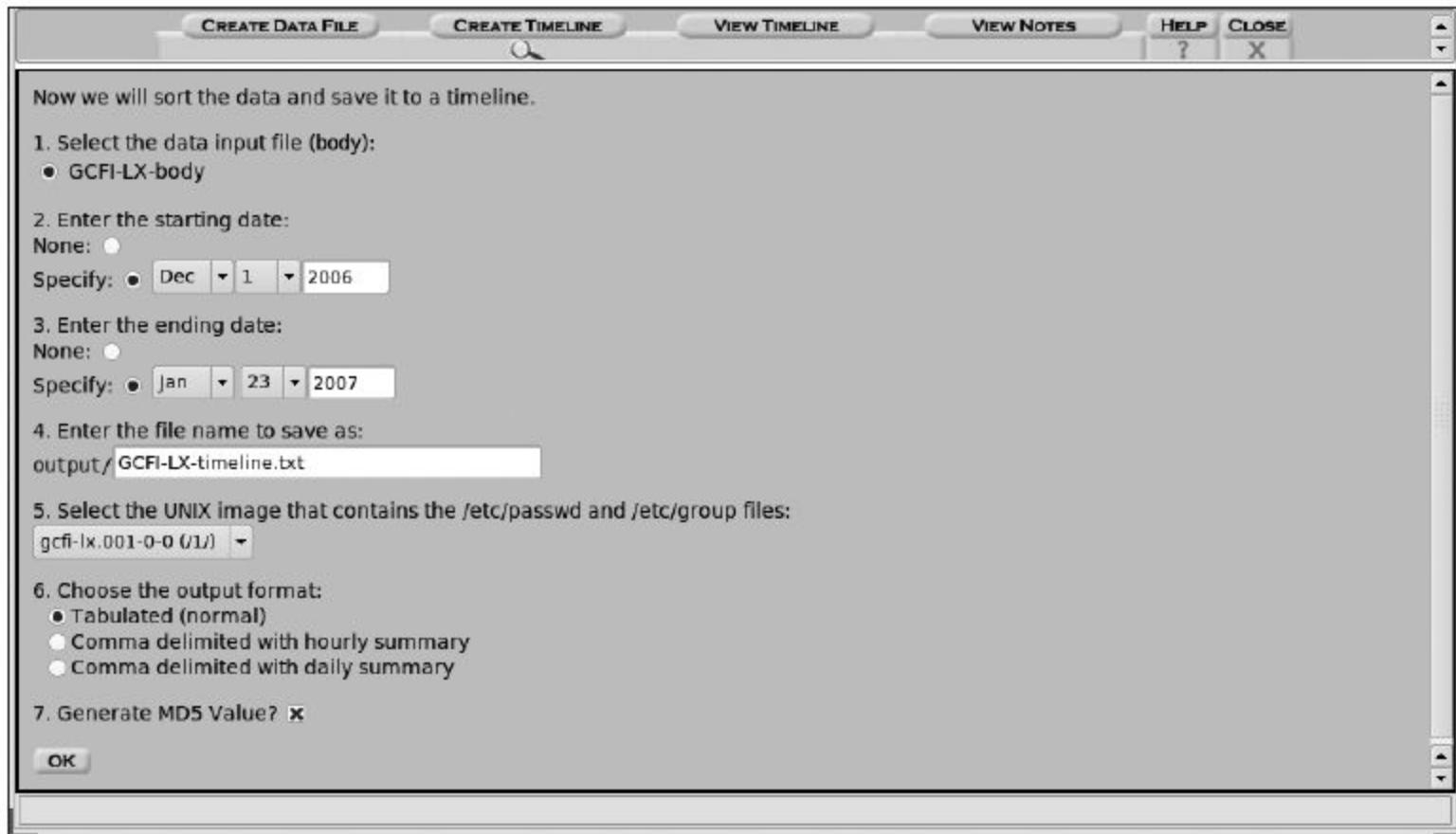


Figure 8-20 Entering timeline options

Guide to Computer Forensics and Investigations Fourth Edition

*Chapter 6
Working with Windows and DOS
Systems*

Objectives

- Explain the purpose and structure of file systems
- Describe Microsoft file structures
- Explain the structure of New Technology File System (NTFS) disks
- List some options for decrypting drives encrypted with whole disk encryption

Objectives (continued)

- Explain how the Windows Registry works
- Describe Microsoft startup tasks
- Describe MS-DOS startup tasks
- Explain the purpose of a virtual machine

Understanding File Systems

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
- A file system is usually directly related to an OS
- When you need to access a suspect's computer to acquire or inspect data
 - You should be familiar with the computer's platform

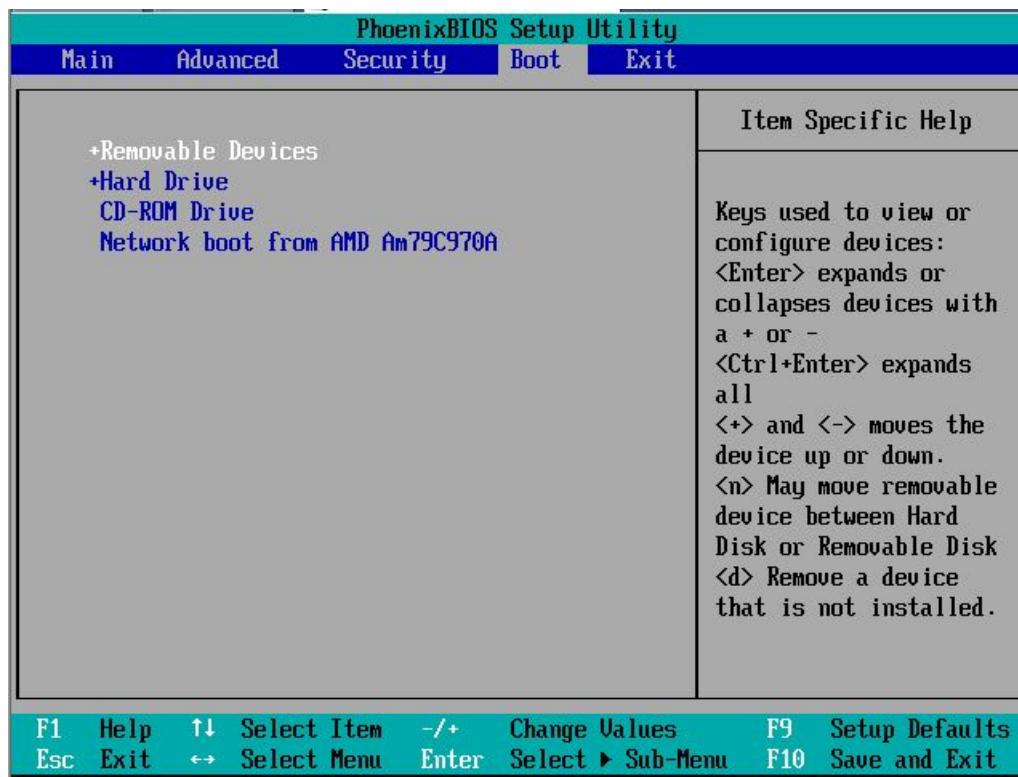
Understanding the Boot Sequence

- 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)
 - Contains programs that perform input and output at the hardware level

Understanding the Boot Sequence (continued)

- **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

BIOS Setup Utility



Understanding Disk Drives

- Disk drives are made up of one or more platters coated with magnetic material
- Disk drive components
 - Geometry
 - Head
 - Tracks
 - Cylinders
 - Sectors
 - Holds 512 bytes, you cannot read or write anything less than a sector

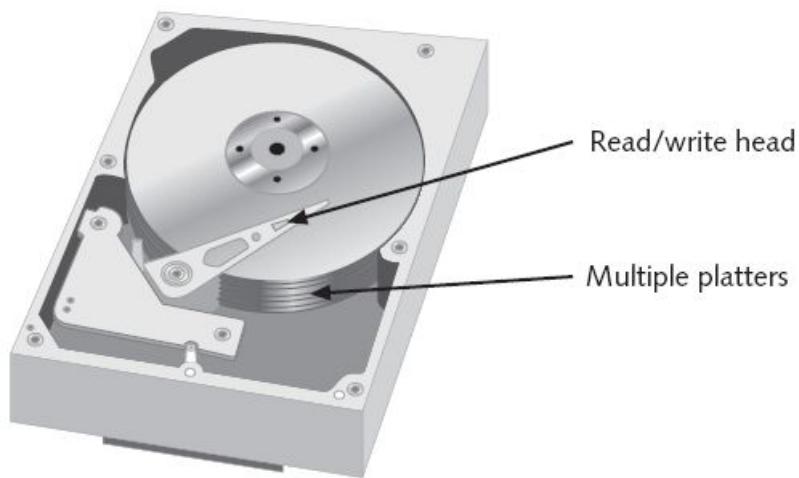
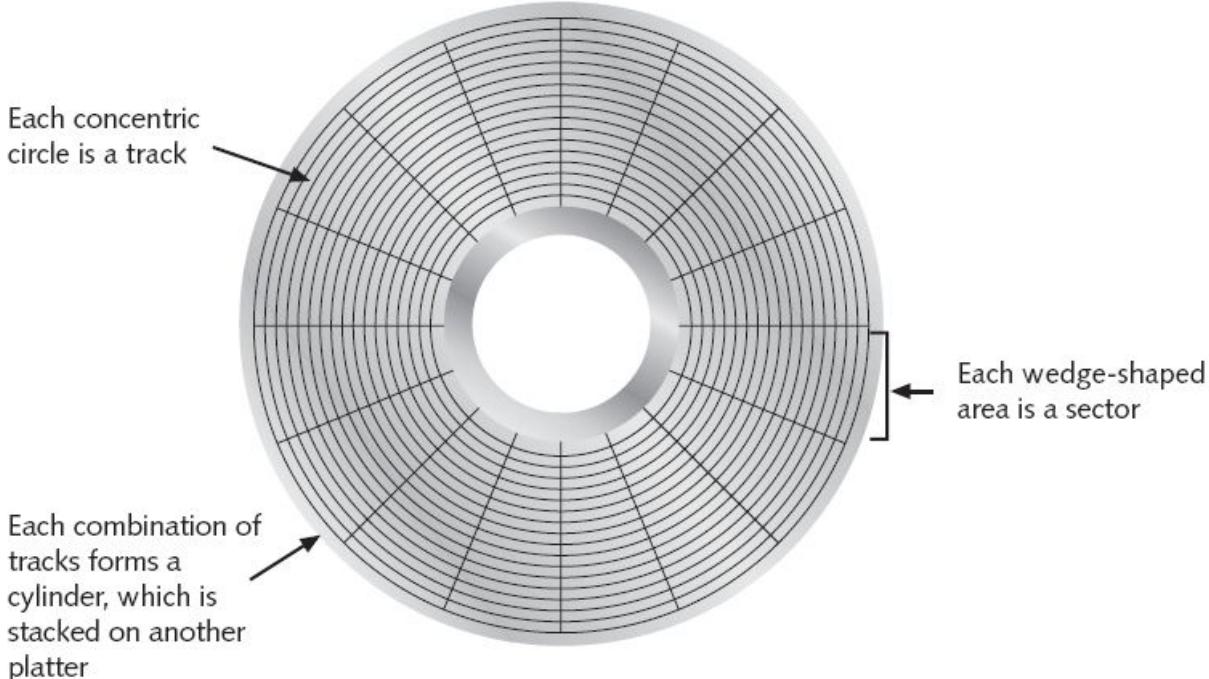
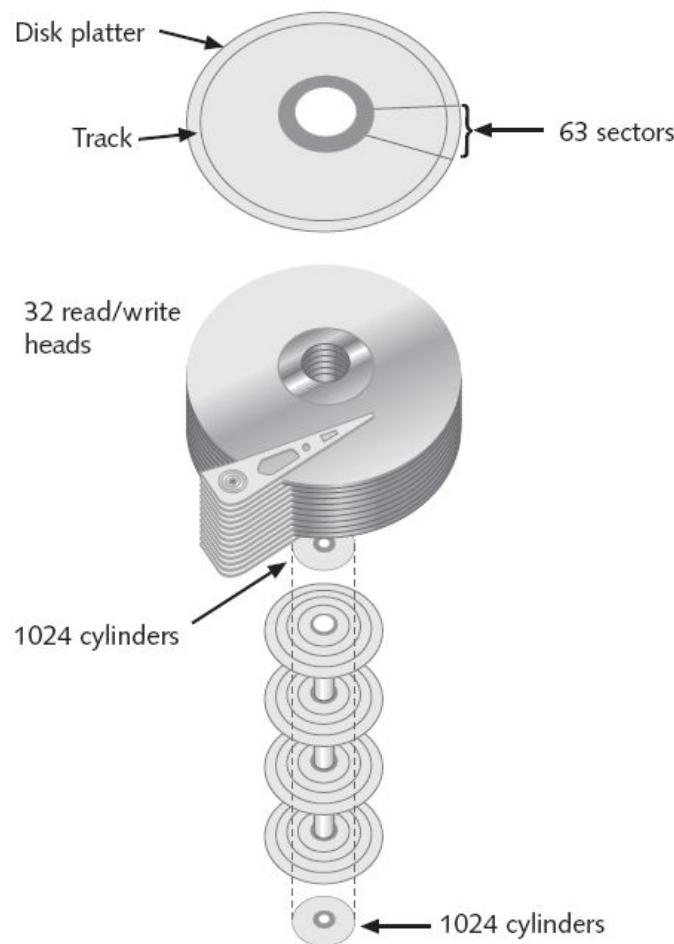


Figure 6-2 Components of the drive structure



512 bytes per sector
1,056,964,608 or 1.056 GB

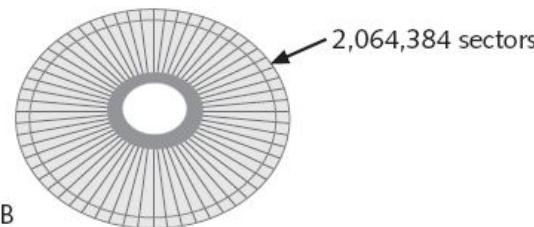


Figure 6-3 CHS calculation

Understanding Disk Drives (continued)

- Properties handled at the drive's hardware or firmware level
 - Zoned bit recording (ZBR) (resizing sectors to compensate for distance from the center)
 - Track density
 - Areal density
 - Head and cylinder skew

No Need for Multi-Path Erasure

- On older disks, the space between tracks was wider, which allowed heads to wander
- This made it possible for specialists to retrieve data from previous writes to a platter, even after erasure
 - Using an electron microscope
- On any IDE or SATA or later hard drive, this is impossible
- A single pass of zeroes erases all data on a disk so it cannot be recovered by any currently known technique

Exploring Microsoft File Structures

Exploring Microsoft File Structures

- In Microsoft file structures, sectors are grouped to form **clusters**
 - Storage allocation units of one or more sectors
- Clusters are typically 512, 1024, 2048, 4096, or more bytes each
- Combining sectors minimizes the overhead of writing or reading files to a disk

Exploring Microsoft File Structures (continued)

- Clusters are numbered sequentially starting at 2
 - 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

Disk Partitions

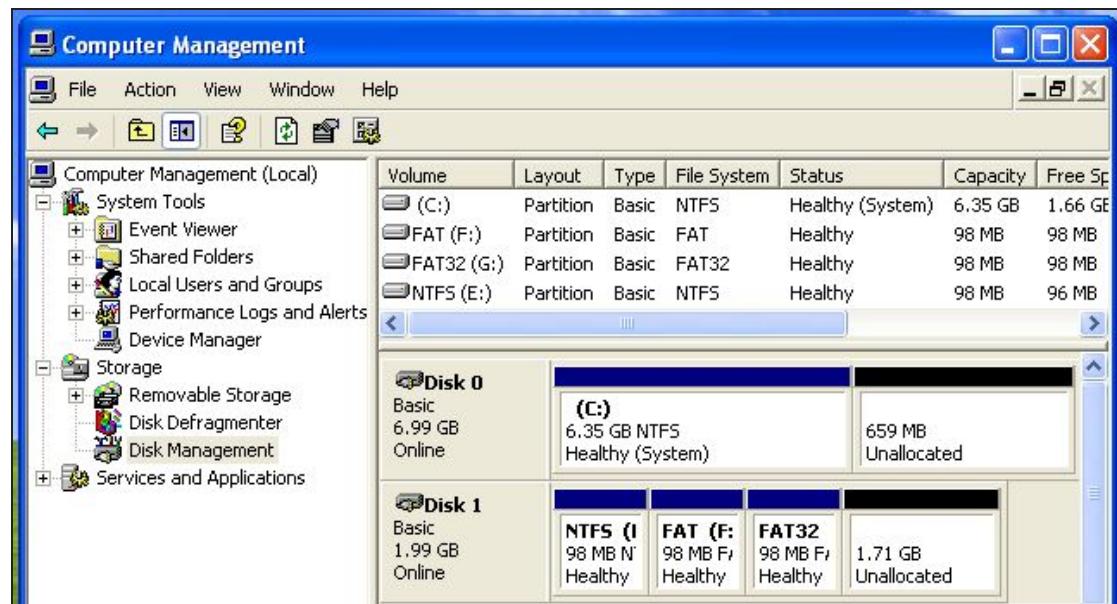
- A **partition** is a logical drive
- FAT16 does not recognize disks larger than 2 GB
 - Note error on page 202 of textbook
 - It's 2 GB, not 2 MB
 - Large disks have to be partitioned
- Hidden partitions or voids
 - Large unused gaps between partitions on a disk
- **Partition gap**
 - Unused space between partitions

Disk Partitions (continued)

- Disk editor utility can alter information in partition table
 - To hide a partition
- Can examine a partition's physical level with a disk editor:
 - HxD, Norton DiskEdit, WinHex, or Hex Workshop
- Analyze the key hexadecimal codes the OS uses to identify and maintain the file system

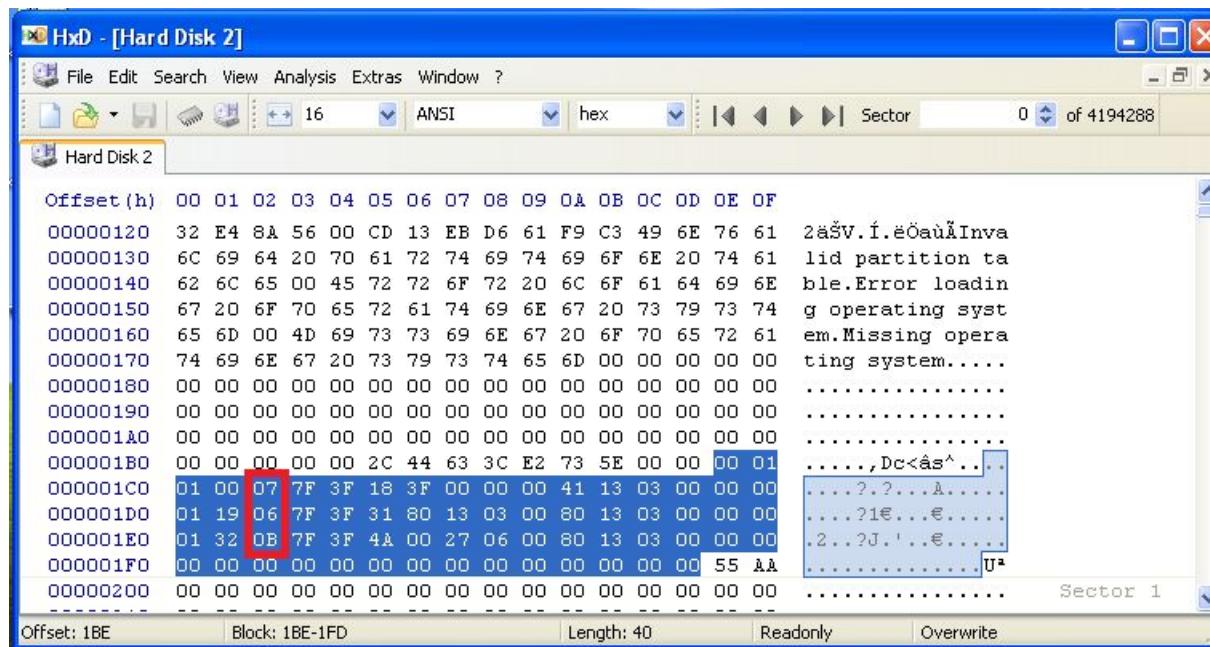
Demo: VM with Three Partitions

- Partition Types
 - NTFS: 07
 - FAT: 06
 - FAT32: 0B



Viewing the Partition Table HxD

- Start HxD, Extras, Open Disk, choose Physical Disk
- Partition Table starts at 0x1BE
- Partition Type field is at offset 0x04 in each record



Master Boot Record Structure

- From Wikipedia
- Link Ch 6a

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	Table of primary partitions (Four 16-byte entries, IBM partition table scheme)		64
01FE	0776	510	55h	MBR signature; 0xAA55 ^[1]	2
01FF	0777	511	AAh		
MBR, total size: 446 + 64 + 2 =					512

Partition Table Structure

- From Wikipedia
- Link Ch 6a

Layout of one 16-byte partition record

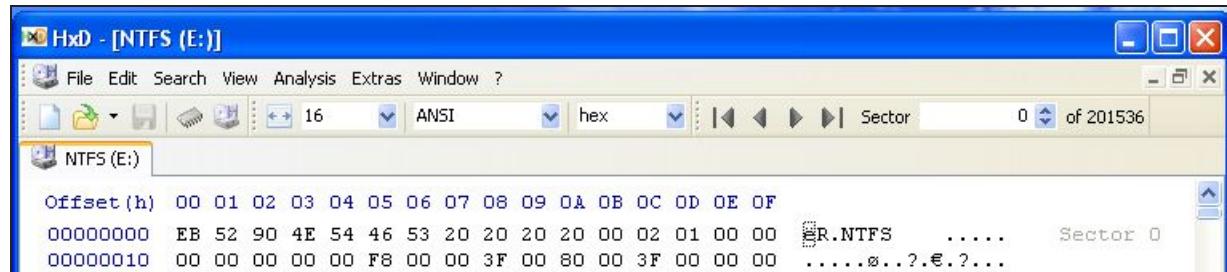
Offset	Field length (bytes)	Description
0x00	1	status ^[7] (0x80 = bootable (active), 0x00 = non-bootable, other = invalid ^[8])
0x01	3	CHS address of first absolute sector in partition. ^[9] The format is described in the next 3 bytes.
0x01	1	head ^[10]
0x02	1	sector is in bits 5–0; ^[11] bits 9–8 of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

Table 6-1 Hexadecimal codes in the partition table

Hexadecimal code	File system
01	DOS 12-bit FAT
04	DOS 16-bit FAT for partitions smaller than 32 MB
05	Extended partition
06	DOS 16-bit FAT for partitions larger than 32 MB
07	NTFS
08	AIX bootable partition
09	AIX data partition
0B	DOS 32-bit FAT
0C	DOS 32-bit FAT for interrupt 13 support
17	Hidden NTFS partition (XP and earlier)
1B	Hidden FAT32 partition
1E	Hidden VFAT partition
3C	Partition Magic recovery partition
66–69	Novell partitions
81	Linux
82	Linux swap partition (can also be associated with Solaris partitions)
83	Linux native file systems (Ext2, Ext3, Reiser, xiafs)
86	FAT16 volume/stripe set (Windows NT)
87	High Performance File System (HPFS) fault-tolerant mirrored partition or NTFS volume/stripe set
A5	FreeBSD and BSD/386
A6	OpenBSD
A9	NetBSD
C7	Typical of a corrupted NTFS volume/stripe set
EB	BeOS

Partition Mark at Start of Volume

- Start HxD, Extras, Open Disk
- NTFS

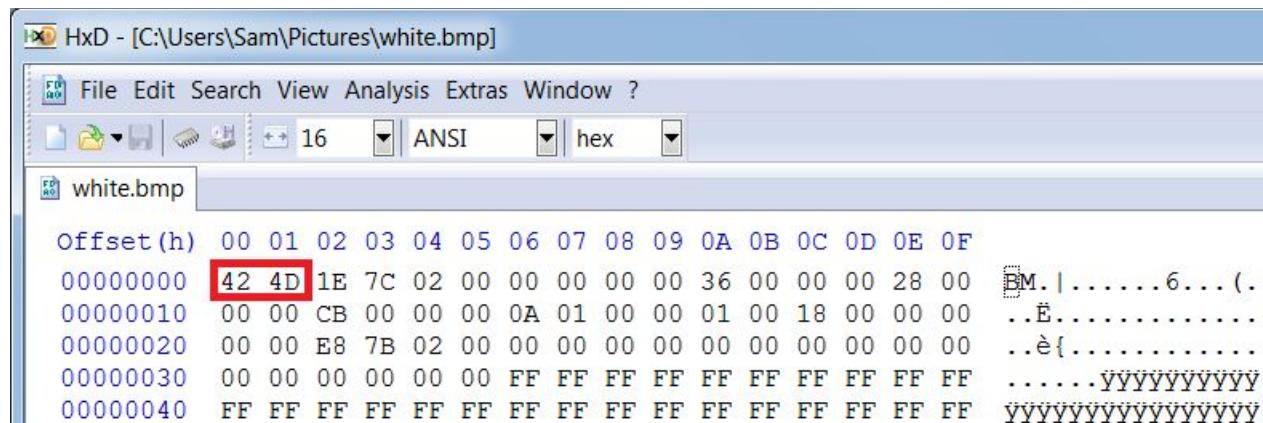


- FAT32



BMP File in HxD

- Start HxD, File, Open
- BM at start indicates a BMP file



Offset(h)	00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F	...
00000000	42 4D 1E 7C 02 00 00 00 00 00 36 00 00 00 28 00	BM. 6...(.)
00000010	00 00 CB 00 00 00 0A 01 00 00 01 00 18 00 00 00	..È.....
00000020	00 00 E8 7B 02 00 00 00 00 00 00 00 00 00 00 00	..è{.....
00000030	00 00 00 00 00 00 FFYYYYYYYYYY
00000040	FF	YYYYYYYYYYYYYYYY

Word Doc File in HxD

- Start HxD, File, Open
- Word 2003 Format uses these 7 bytes

Offset(h)	00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F	Hex	ASCII
00000000	D0 CF 11 E0 A1 B1 1A E1 00 00 00 00 00 00 00 00 00		ĐÍ.à;±.á.....
00000010	00 00 00 00 00 00 00 00 3E 00 03 00 FE FF 09 00	>...þý..
00000020	06 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00	
00000030	26 00 00 00 00 00 00 00 10 00 00 28 00 00 00 00		&.....(...
00000040	01 00 00 00 FE FF FF FF 00 00 00 00 25 00 00 00	þýÿ....%...
00000050	FF		ÿÿÿÿÿÿÿÿÿÿÿÿÿÿ

- .docx format is actually a Zip archive
 - See links Ch 6b, 6c

Master Boot Record

- On Windows and DOS computer systems
 - Boot disk contains a file called the **Master Boot Record (MBR)**
- MBR stores information about partitions on a disk and their locations, size, and other important items
- Several software products can modify the MBR, such as PartitionMagic's Boot Magic

Examining FAT Disks

- **File Allocation Table (FAT)**
 - File structure database that Microsoft originally designed for floppy disks
 - Used before Windows NT and 2000
- 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
- FAT versions
 - FAT12, FAT16, FAT32, FATX (for Xbox), and VFAT

FAT Versions

- FAT12—for floppy disks, max size 16 MB
- FAT16—allows hard disk sizes up to 2 GB
- FAT32— allows hard disk sizes up to 2 TB □
- FATX—For Xbox media
 - The date stamps start at the year 2000, unlike the other FAT formats that start at 1980
- VFAT (Virtual File Allocation Table)
 - Allows long file names on Windows (MS-DOS had 8.3 limitation)

Examining FAT Disks (continued)

- Cluster sizes vary according to the hard disk size and file system
- This table is for FAT-16

Table 6-2 Sectors and bytes per cluster

Drive size	Number of sectors per cluster	FAT16
0–32 MB	1	512 bytes
33–64 MB	2	1 KB
65–128 MB	4	2 KB
129–255 MB	8	4 KB
256–511 MB	16	8 KB
512–1023 MB	32	16 KB
1024–2047 MB	64	32 KB
2048–4095 MB	128	68 KB

Examining FAT Disks (continued)

- 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 and the end of the cluster
- Drive slack includes:
 - **RAM slack** and **file slack**
- An unintentional side effect of FAT16 having large clusters was that it reduced fragmentation
 - As cluster size increased

Examining FAT Disks (continued)

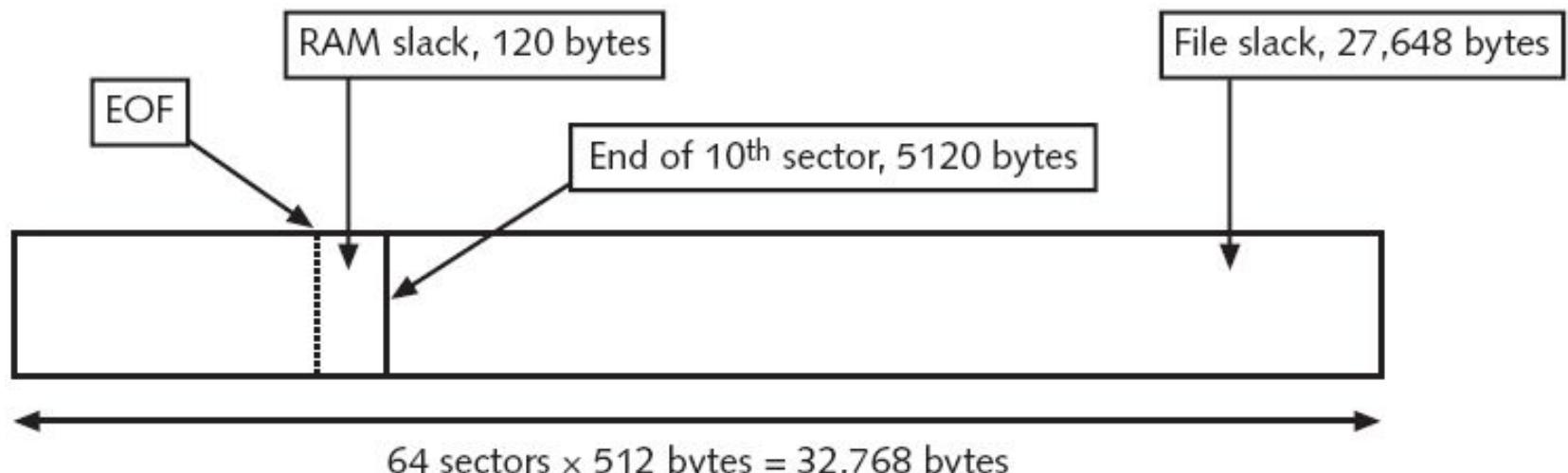


Figure 6-7 File slack space

Examining FAT Disks (continued)

- When you run out of room for an allocated cluster
 - OS allocates another cluster for your file, which creates more slack space on the disk
- As files grow and require more disk space, assigned clusters are chained together
 - The chain can be broken or fragmented

ProDiscover Showing Cluster Chain

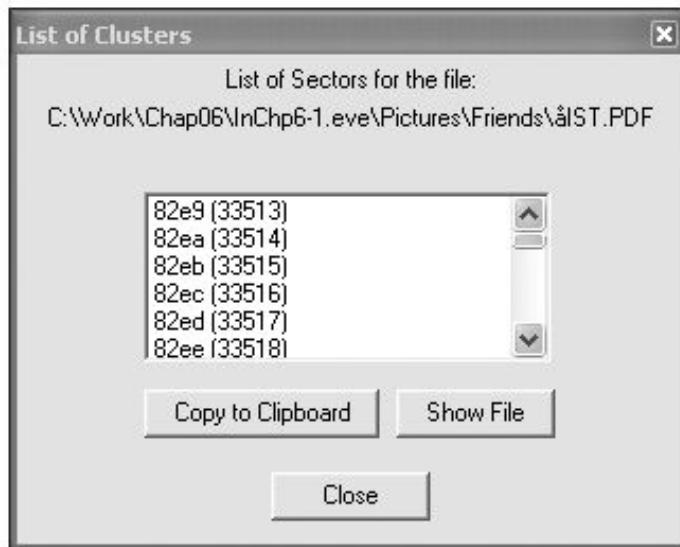


Figure 6-8 Chained sectors associated with clusters as a result of increasing file size

Examining FAT Disks (continued)

- 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
- 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

Deleting FAT Files

- In Microsoft OSs, when a file is deleted
 - Directory entry is marked as a deleted file
 - With the HEX E5 (σ) 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

iClicker Questions

Which of these always contains 512 bytes?

- A. Head**
- B. Track**
- C. Cylinder**
- D. Sector**
- E. Cluster**

Which of these has a capacity that varies with partition size?

- A. Head
- B. Track
- C. Cylinder
- D. Sector
- E. Cluster

Which file system has a maximum partition size of 2 GB?

- A. **FAT12**
- B. **FAT16**
- C. **FAT32**
- D. **FATX**
- E. **VFAT**

Which term describes padding added to data to make an integral multiple of 512 bytes?

- A. Drive slack**
- B. RAM slack**
- C. File slack**
- D. Fragmented**
- E. Unallocated space**

Examining NTFS Disks

- **New Technology File System (NTFS)**
 - Introduced with Windows NT
 - Recommended file system for Windows 2000 Pro, XP, and later versions through Windows 7 at least
- 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

Examining NTFS Disks (continued)

- 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 (continued)

- Table 3 seems to be wrong (thanks to Richard Rosson for pointing this out)
- Correct cluster sizes are at link Ch 6d

NTFS File System

- 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 (continued)

Table 6-4 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.
\$AttrDef	Attribute definitions	4	A table listing attribute names, numbers, and definitions.
\$	Root file-name index	5	This is the root folder on the NTFS volume.

NTFS File System (continued)

Table 6-4 Metadata records in the MFT (continued)

Filename	System file	Record position	Description
\$Bitmap	Boot sector	6	A map of the NTFS volume showing 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.

MFT and File Attributes

- 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 (continued)

- 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

Table 6-5 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. Long filenames have two attribute ID 0x30s in the MFT record: one for the short name and one for the long name.
0x40	\$Object_ID (for Windows NT, it's named \$Volume_Version) 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 or data runs to nonresident files.
0x90	\$Index_Root Implemented for use of folders and indexes.
0xA0	\$Index_Allocation Implemented for use of folders and indexes.
0xB0	\$Bitmap Implemented for use of folders and indexes.
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 OS2 HPFS file systems.
0xE0	\$EA For use with OS2 HPFS file systems.
0x100	\$Logged_Utility_Stream This field is used by Encrypting File System in Windows 2000 and XP.

Resident File in a MFT Record

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	G
035B3400	46	49	4C	45	30	00	03	00	9B	99	98	00	00	00	00	00	FILE0
035B3410	02	00	01	00	38	00	01	00	A8	01	00	00	00	04	00	008.....
035B3420	00	00	00	00	00	00	00	00	04	00	00	00	A8	17	00	00\$.....
035B3430	03	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	00H.....
035B3450	62	16	9B	68	0A	7C	C9	01	BC	78	9D	68	0A	7C	C9	01	b...h. E...hx.h. E.
035B3460	BC	78	9D	68	0A	7C	C9	01	BC	78	9D	68	0A	7C	C9	01	hx.h. E...hx.h. E.
035B3470	20	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	000...p.....
035B3490	00	00	00	00	00	00	00	00	30	00	00	00	70	00	00	000...p.....
035B34A0	00	00	00	00	00	00	02	00	52	00	00	00	18	00	01	00R.....
035B34B0	8A	00	00	00	00	00	01	00	62	16	9B	68	0A	7C	C9	01	I.....b...h. E.
035B34C0	BC	78	9D	68	0A	7C	C9	01	BC	78	9D	68	0A	7C	C9	01	hx.h. E...hx.h. E.
035B34D0	BC	78	9D	68	0A	7C	C9	01	00	00	00	00	00	00	00	00	hx.h. E.....
035B34E0	00	00	00	00	00	00	00	00	20	00	00	00	00	00	00	00
035B34F0	08	03	42	00	65	00	6E	00	31	00	2E	00	74	00	78	00	..B...n.1...t.x.
035B3500	74	00	00	00	00	00	00	00	40	00	00	00	28	00	00	00	t.....@...()
035B3510	00	00	00	00	00	00	03	00	18	00	00	00	18	00	00	00
035B3520	F4	7C	F1	27	DF	E7	DD	11	A8	3F	00	22	19	05	88	06	6 R'BcY...?..O .
035B3530	80	00	00	00	70	00	00	00	00	00	18	00	00	00	01	00	I....p.....
035B3540	84	00	00	00	12	00	00	00	41	20	63	6F	75	6E	74	72	T.....A countr
035B3550	79	6D	61	6E	20	62	65	74	77	69	65	6E	20	74	77	6F	yman between two
035B3560	20	6C	61	77	79	65	72	73	20	69	73	20	6C	69	6B	65	lawyers is like
035B3570	20	61	20	66	69	73	68	20	62	65	74	77	65	65	6E	20	a fish between
035B3580	74	77	6E	20	63	61	74	73	2E	0D	0A	42	65	6E	6A	61	two cats...Benja
035B3590	6D	69	6E	20	46	72	61	6E	6B	6C	69	6E	00	00	00	00	n Franklin...
035B35A0	FF	FF	FF	FF	82	79	47	11	00	00	00	00	00	00	00	00	yyyy yG.....

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

Resident File Data in the MFT

	A: Starting position of attribute 0x80 \$Data	B: Length of attribute 0x80 in little endian format	C: Interpreted little endian value
035B3530	80	00 00 00 70 00	00 00 18 00 00 00 01 00 I...P.....
035B3540	54	00 00 00 18 00 00 00	41 20 63 6F 75 6E 74 72 T.....A countr
035B3550	79	6D 61 6E 20 62 65 74	77 65 65 6E 20 74 77 6F yman between two
035B3560	20	6C 61 77 79 65 72 73	9 6B 65 lawyers is like
035B3570	20	61 20 66 69 73 68 20	5 6E 20 a fish between
035B3580	74	77 6F 20 63 61 74 73	6 6A 61 two cats...Benja
035B3590	6D	69 6E 20 46 72 61 6E	nin Franklin....
035B35A0	FF	FF FF FF 82 79 47 11	ÿÿÿÿG.....

Figure 6-10 File data for a resident file

- This figure is a repeat of a portion of the previous one

Nonresident File's MFT Record

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F		
035B3C00	46	49	4C	45	30	00	03	00	D3	BD	98	00	00	00	00	00	EFILE0...04I.....	
035B3C10	02	00	01	00	38	00	01	00	80	01	00	00	00	04	00	008...I.....	
035B3C20	00	00	00	00	00	00	00	00	05	00	00	00	A5	17	00	00M.....	
035B3C30	03	00	00	00	00	00	00	00	10	00	00	00	60	00	00	00H.....	
035B3C40	00	00	00	00	00	00	00	00	48	00	00	00	18	00	00	00A.. E..j.. I.. E..	
035B3C50	10	C0	13	88	0B	7C	C9	01	6A	22	16	88	0B	7C	C9	01	j..I.. E..j.. I.. E..	
035B3C60	6A	22	16	88	0B	7C	C9	01	6A	22	16	88	0B	7C	C9	01	
035B3C70	20	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
035B3C80	00	00	00	00	09	01	00	00	00	00	00	00	00	00	00	00	
035B3C90	00	00	00	00	00	00	00	00	30	00	00	00	70	00	00	000...p...	
035B3CA0	00	00	00	00	00	00	02	00	52	00	00	00	18	00	01	00R.....	
035B3CB0	8A	00	00	00	00	00	01	00	10	C0	13	88	0B	7C	C9	01	I.....A.. E..	
035B3CC0	6A	22	16	88	0B	7C	C9	01	6A	22	16	88	0B	7C	C9	01	j..I.. E..j.. I.. E..	
035B3CD0	6A	22	16	88	0B	7C	C9	01	00	00	00	00	00	00	00	00	j..I.. E..	
035B3CE0	00	00	00	00	00	00	00	00	20	00	00	00	00	00	00	00	
035B3CF0	08	03	42	00	65	00	6E	00	32	00	2E	00	72	00	74	00	.B.e.n.2..r.t.	
035B3D00	66	00	00	00	00	00	00	00	40	00	00	00	28	00	00	00	f.....@...{...	
035B3D10	00	00	00	00	00	00	04	00	10	00	00	00	18	00	00	00	
035B3D20	F7	7C	F1	27	DF	E7	DD	11	A8	3F	00	22	15	D5	88	06	+ K'8çY..?..01.	
035B3D30	80	00	00	00	48	00	00	00	01	00	00	00	00	00	03	00	I...H.....	
035B3D40	00	00	00	00	00	00	00	00	02	00	00	00	00	00	00	00	
035B3D50	40	00	00	00	00	00	00	00	00	06	00	00	00	00	00	00	@.....	
035B3D60	78	05	00	00	00	00	00	00	78	05	00	00	00	00	00	00	x.....x.....	
035B3D70	31	03	15	55	01	00	01	00	FF	FF	FF	FF	82	79	47	11	1..U...yyyyyG.	

- 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 6-11 Nonresident file in an MFT record

Skip Pages 216-223

MFT and File Attributes (continued)

- 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

NTFS Data Streams

- **Data streams**
 - Ways data can be appended to existing files
 - Can obscure valuable evidentiary data, intentionally or by coincidence
- In NTFS, a 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

Alternate Data Streams Demonstration

NTFS Compressed Files

- NTFS provides compression similar to FAT DriveSpace 3
- Under NTFS, files, folders, or entire volumes can be compressed
- Most computer forensics tools can uncompress and analyze compressed Windows data

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
 - 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

Error in Textbook

- Page 225
- Only Windows 2000 used the Administrator account as the default EFS Recovery Agent
- Windows XP and later versions have no EFS recovery agent by default
 - Links Ch 6e, 6f

Deleting NTFS Files

- When a file is deleted in Windows XP, 2000, or NT
 - 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

Understanding Whole Disk Encryption

Understanding Whole Disk Encryption

- 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 other handheld devices
- To help prevent loss of information, software vendors now provide whole disk encryption

Understanding Whole Disk Encryption (continued)

- 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
 - A **Trusted Platform Module (TPM)** microchip to generate encryption keys and authenticate logins

Understanding Whole Disk Encryption (continued)

- 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

Examining Microsoft BitLocker

- Available only with Vista/Win 7 Enterprise and Ultimate editions
- Hardware and software requirements
 - A computer capable of running Windows Vista/7
 - The TPM microchip, version 1.2 or newer
 - A computer BIOS compliant with Trusted Computing Group (TCG)
 - Two NTFS partitions; a 1.5 GB or 100 MB partition use just for BitLocker, and the partition containing Windows
 - The BIOS configured so that the hard drive boots first before checking other bootable peripherals

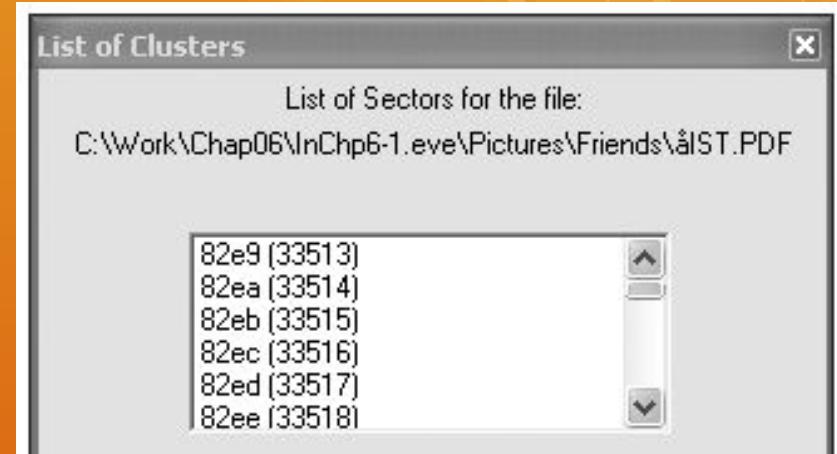
Examining Third-Party Disk Encryption Tools

- Some available third-party WDE utilities:
 - PGP Whole Disk Encryption
 - Voltage SecureDisk
 - Utimaco SafeGuard Easy
 - Jetico BestCrypt Volume Encryption
 - SoftWinter Sentry 2020 for Windows XP
- Some available open-source encryption tools:
 - TrueCrypt
 - CrossCrypt
 - FreeOTFE

iClicker Questions

What is stored in these clusters?

- A. Data run**
- B. Alternate Data stream**
- C. File slack**
- D. Metadata**
- E. Resident file data**



Which of these is a hardware device used to encrypt a hard drive?

- A. PII
- B. EFS
- C. TPM
- D. MFT
- E. FAT

Which of these should never be stored on a laptop without encryption?

- A. PII
- B. EFS
- C. MBR
- D. MFT
- E. FAT

A small file contains only ten bytes of text on an NTFS volume. Where are those ten bytes stored?

- A. MFT**
- B. Data run**
- C. Data stream**
- D. FAT**
- E. Drive slack**

Understanding the Windows Registry

Understanding the Windows Registry

- **Registry**
 - A database that stores hardware and software configuration information, network connections, user preferences, and setup information
- For investigative purposes, the Registry can contain valuable evidence
- To view the Registry, you can use:
 - Regedit (Registry Editor) program for Windows 9x systems
 - Regedt32 for Windows 2000 and XP

Exploring the Organization of the Windows Registry

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

Exploring the Organization of the Windows Registry (continued)

Table 6-6 Registry file locations and purposes

Filename and location	Purpose of file
Windows 9x/Me	
Windows\System.dat	User-protected storage area; contains installed program settings, usernames and passwords associated with installed programs, and system settings
Windows\User.dat Windows\profile\user-account	Contains the most recently used (MRU) files list and desktop configuration settings; every user account created on the system has its own user data file
Windows NT, 2000, XP, and Vista	
Documents and Settings\user-account\Ntuser.dat	User-protected storage area; contains the MRU files list and desktop configuration settings
Winnt\system32\config\Default	Contains the computer's system settings
Winnt\system32\config\SAM	Contains user account management and security settings
Winnt\system32\config\Security	Contains the computer's security settings
Winnt\system32\config\Software	Contains installed programs settings and associated usernames and passwords
Winnt\system32\config\System	Contains additional computer system settings

Exploring the Organization of the Windows Registry (continued)

Table 6-7 Registry HKEYs and their functions

HKEY	Function
HKEY_CLASS_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
HKEY_CURRENT_CONFIG	A symbolic link to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Hardware Profile\xxxx (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

Understanding Microsoft Startup Tasks

Understanding Microsoft Startup Tasks

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

Startup in Windows NT and Later

- All Windows NT 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

Startup Process for Windows Vista

- Uses the new Extensible Firmware Interface (EFI) as well as the older BIOS system.
- NT Loader (NTLDR) has been replaced by three boot utilities
 - Bootmgr.exe—displays list of operating systems
 - Winload.exe—loads kernel, HAL, and drivers
 - Winresume.exe—restarts Vista after hibernation
- See link Ch 6g

Startup Files for Windows XP

- NT Loader (NTLDR)
- Boot.ini
- BootSect.dos
- NTDetect.com
- NTBootdd.sys
- Ntoskrnl.exe
- Hal.dll
- Pagefile.sys
- Device drivers

Startup in Windows NT and Later (continued)

- Windows XP System Files

Table 6-8 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 Win32subsystem
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

Startup in Windows NT and Later (continued)

- 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

Startup in Windows 9x/Me

- System files in Windows 9x/Me containing valuable information can be altered easily during startup
- Windows 9x and Windows Me have similar boot processes
 - With Windows Me you can't boot to a true MS-DOS mode
- Windows 9x OSs have two modes:
 - **DOS protected-mode interface (DPMI)**
 - **Protected-mode GUI**

Startup in Windows 9x/Me (continued)

- The system files used by Windows 9x have their origin in MS-DOS 6.22
 - **Io.sys** communicates between a computer's BIOS, the hardware, and the OS kernel
 - If F8 is pressed during startup, Io.sys loads the Windows Startup menu
 - **Msdos.sys** is a hidden text file containing startup options for Windows 9x
 - **Command.com** provides a command prompt when booting to MS-DOS mode (DPMI)

Understanding MS-DOS Startup Tasks

Understanding MS-DOS Startup Tasks

- Two files are used to configure MS-DOS at startup:
 - **Config.sys**
 - A text file containing commands that typically run only at system startup to enhance the computer's DOS configuration
 - **Autoexec.bat**
 - A batch file containing customized settings for MS-DOS that runs automatically
- Io.sys is the first file loaded after the ROM bootstrap loader finds the disk drive

Understanding MS-DOS Startup Tasks (continued)

- Msdos.sys is the second program to load into RAM immediately after Io.sys
 - It looks for the Config.sys file to configure device drivers and other settings
- Msdos.sys then loads Command.com
- As the loading of Command.com nears completion, Msdos.sys looks for and loads Autoexec.bat

Other Disk Operating Systems

- Control Program for Microprocessors (CP/M)
 - First nonspecific microcomputer OS
 - Created by Digital Research in 1970
 - 8-inch floppy drives; no support for hard drives
- Digital Research Disk Operating System (DR-DOS)
 - Developed in 1988 to compete with MS-DOS
 - Used FAT12 and FAT16 and had a richer command environment

Other Disk Operating Systems (continued)

- Personal Computer Disk Operating System (PC-DOS)
 - Created by Microsoft under contract for IBM
 - PC-DOS works much like MS-DOS

Understanding Virtual Machines

Understanding Virtual Machines

- **Virtual machine**
 - Allows you to create a representation of another computer on an existing physical computer
- 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



Figure 6-32 A virtual machine running on the host computer's desktop

Understanding Virtual Machines (continued)

- In computer 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

Creating a Virtual Machine

- Two popular applications for creating virtual machines
 - VMware and Microsoft Virtual PC
- Using Virtual PC
 - You must download and install Virtual PC first

Creating a Virtual Machine (continued)



Figure 6-33 Creating a new virtual machine

Creating a Virtual Machine (continued)

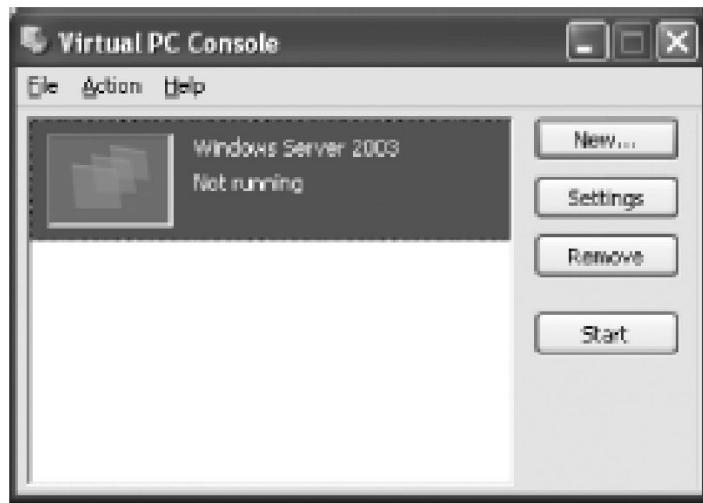


Figure 6-34 The Virtual PC Console with a virtual machine available

Creating a Virtual Machine (continued)

- You need an ISO image of an OS
 - Because no OSs are provided with Virtual PC
- Virtual PC creates two files for each virtual machine:
 - A .vhd file, which is the actual virtual hard disk
 - A .vmc file, which keeps track of configurations you make to that disk
- See what type of physical machine your virtual machine thinks it's running
 - Open the Virtual PC Console, and click Settings

Creating a Virtual Machine (continued)

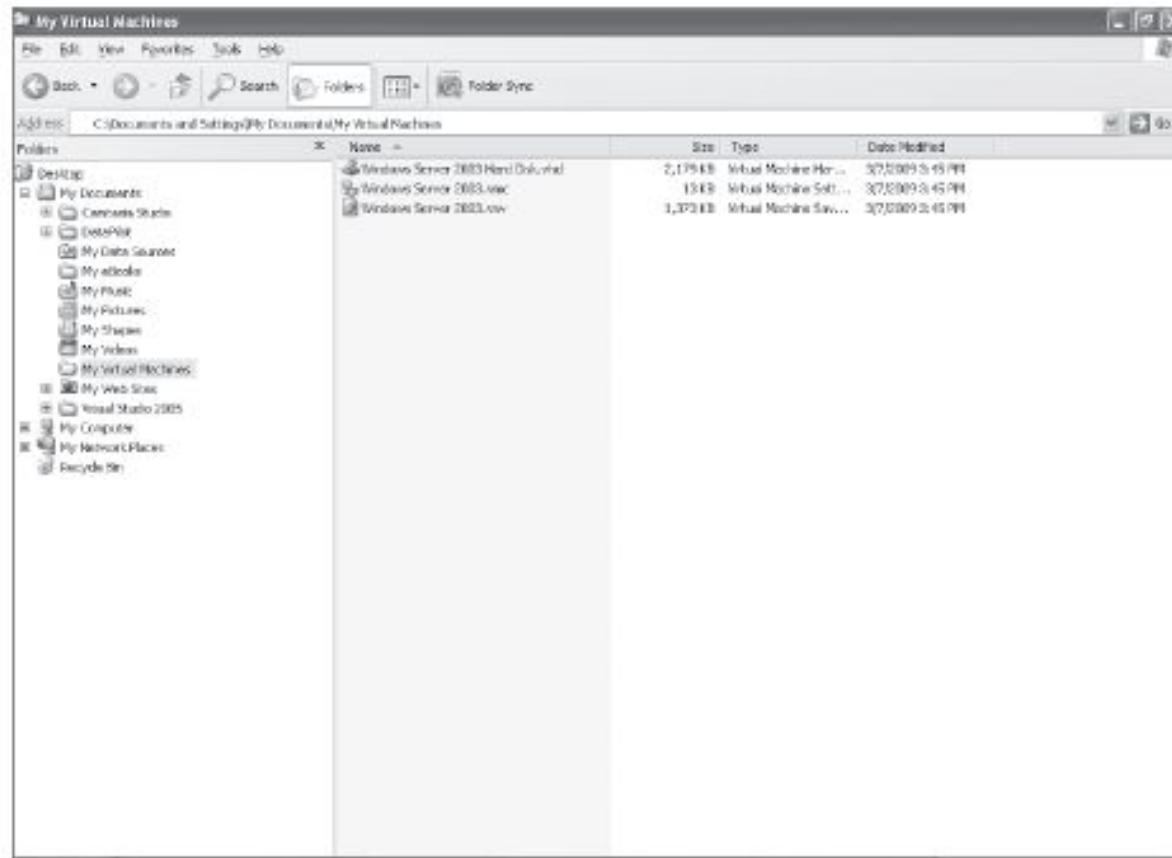


Figure 6-35 Virtual machine configuration files

Creating a Virtual Machine (continued)



Figure 6-36 Properties of a virtual machine

iClicker Questions

What file loads the kernel in Windows 7?

- A. Ntldr**
- B. Bootmgr**
- C. Winload**
- D. Boot.ini**
- E. Io.sys**

Which of these is a new technology to start computers, replacing the BIOS?

- A. **EFI**
- B. **TPM**
- C. **Ntldr**
- D. **HAL**
- E. **Winload**

Which module shows the user a list of available operating systems on a Windows XP machine?

- A. Bootmgr**
- B. Winload**
- C. Hal**
- D. Config.sys**
- E. Ntldr**