Guide to Computer Forensics and Investigations Fourth Edition pg 28-44

Understanding Computer Investigations

Objectives

- Explain how to prepare a computer investigation
- Apply a systematic approach to an investigation
- Describe ***procedures*** for corporate high-tech investigations
- Explain requirements for ***data recovery*** workstations and software
- Describe how to ***conduct an investigation***
- Explain how to ***complete and critique a case***

Preparing a Computer Investigation

Preparing a Computer Investigation

- Role of computer forensics professional is to gather evidence to prove that a suspect committed a crime or violated a company policy
- Collect evidence that can be offered in court or at a corporate inquiry
  - Investigate the suspect's computer
  - Preserve the evidence on a different computer

Preparing a Computer Investigation (continued)

- Follow an accepted procedure to prepare a case
- **Chain of custody**
  - Route the evidence takes from the time you find it until the case is closed or goes to court

An Overview of a Computer Crime

- Computers can contain information that helps law enforcement determine:
  - Chain of events leading to a crime
  - Evidence that can lead to a conviction
- Law enforcement officers should follow proper procedure when acquiring the evidence
  - Digital evidence can be easily altered by an overeager investigator
- Information on hard disks might be **password protected**

Examining a Computer Crime

Figure 2-1 The crime scene

An Overview of a Company Policy Violation

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

Taking a Systematic Approach

Taking a Systematic Approach

- Steps for problem solving
  - Make an initial assessment about the type of case you are investigating(interview,location,use of computer,evidence)
  - Determine a preliminary design or approach to the case(seize the device in working hrs,law enforcement)
  - Create a detailed checklist-(amt of time)
  - Determine the resources you need(os,sw)
  - Obtain and copy an evidence disk drive(forensic image of devices)

Taking a Systematic Approach (continued)

- Steps for problem solving (continued)
  - Identify the risks(list problems)
  - Mitigate or minimize the risks(eg pass protection)
  - Test the design (compare hash values)
  - Analyze and recover the digital evidence
  - Investigate the data you recover
  - Complete the case report
  - Critique the case(self evaluation)

Assessing the Case

- Systematically outline the case details
  - Situation
  - Nature of the case
  - Specifics of the case
  - Type of evidence
  - Operating system
  - Known disk format
  - Location of evidence

Assessing the Case (continued)

- Based on case details, you can determine the case requirements
  - Type of evidence
  - Computer forensics tools
  - Special operating systems

Planning Your Investigation

- A basic investigation plan should include the following activities:
  - Acquire the evidence
  - Complete an evidence form and establish a chain of custody
  - Transport the evidence to a computer forensics lab
  - Secure evidence in an **approved secure container**

Planning Your Investigation (continued)

- A basic investigation plan (continued):
  - Prepare a forensics workstation
  - Obtain the evidence from the secure container
  - Make a forensic copy of the evidence
  - Return the evidence to the secure container
  - Process the copied evidence with computer forensics tools

Planning Your Investigation (continued)

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

Planning Your Investigation (continued)

Corporation X
Security Investigations
This form is to be used for one to ten pieces of evidence

Case No.:		Investigating Organization:	
Investigator:			
Nature of Case:			
Location where evidence was obtained:			

	Description of evidence:	Vendor Name	Model No./Serial No.
Item #1			
Item #2			
Item #3			
Item #4			
Item #5			
Item #6			
Item #7			
Item #8			
Item #9			
Item #10			

Evidence Recovered by:		Date & Time:	
Evidence Placed in Locker:		Date & Time:	

Item #	Evidence Processed by	Disposition of Evidence	Date/Time
			Page __ of ___

Figure 2-2 A sample multi-evidence form used in a corporate environment

Planning Your Investigation (continued)

Metropolis Police Bureau
High-tech Investigations Unit
This form is to be used for only one piece of evidence.
Fill out a separate form for each piece of evidence.

Case No.:		Unit Number:	
Investigator:			
Nature of Case:			
Location where evidence was obtained:			

Item # ID	Description of evidence:	Vendor Name	Model No./Serial No.

Evidence Recovered by:		Date & Time:	
Evidence Placed in Locker:		Date & Time:	

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

Figure 2-3 A single-evidence form

Securing Your Evidence

- Use **evidence bags** to secure and catalog the evidence
- Use computer safe products
  - Antistatic bags
  - Antistatic pads
- Use well padded containers
- Use evidence tape to seal all openings
  - Floppy disk or CD drives
  - Power supply electrical cord

Securing Your Evidence (continued)

- Write your initials on tape to prove that evidence has not been tampered with
- Consider computer specific temperature and humidity ranges