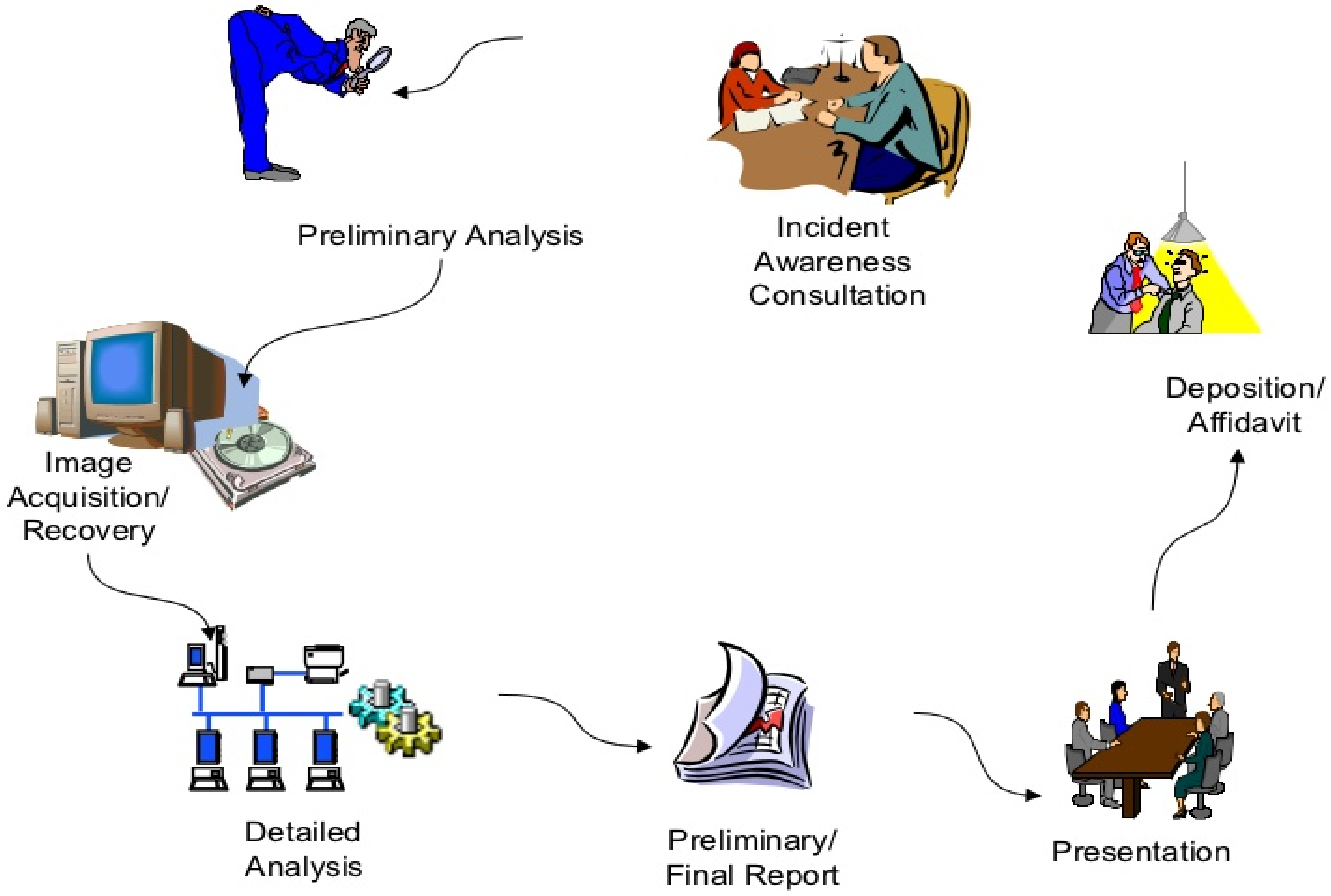
Guide to Computer Forensics and Investigations Sixth Edition

Chapter 2

Understanding Computer Investigations

Objectives

- Describe how to prepare a digital forensics investigation by taking a systematic approach
- Describe procedures for private-sector digital investigations
- Explain requirements for data recovery workstations and software
- Summarize how to conduct an investigation, including critiquing a case



Incident Awareness Consultation

Preliminary Analysis

Image Acquisition/ Recovery

Detailed Analysis

Preliminary/ Final Report

Presentation

Deposition/ Affidavit

Ref : Centre for Development of Advanced Computing

Taking a Systematic Approach

- Steps for problem solving

1. Make an initial assessment about the type of case you are investigating – *i.e Interview people, decide on places to visits and etc*
2. Determine a preliminary design or approach to the case. *i.e when to visit company employees*
3. Create a detailed checklist. *Checklist helps you to stay on track*
4. Determine the resources you need. *i.e s/w n h/w*
5. Obtain and copy an evidence drive

Taking a Systematic Approach

- Steps for problem solving (cont'd)

6. Identify the risks. *i.e unable to access computer due to change of password*
7. Mitigate or minimize the risks *to ensure original evidence is always available*
8. Test the design *like comparing the hash value*
9. **Analyze and recover the digital evidence**
10. **Investigate the data you recover**
11. **Complete the case report**
12. Critique the case *Self-evaluation to improve*

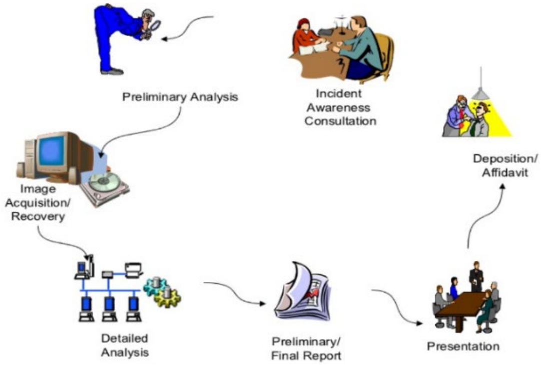
Assessing the Case

- Systematically **outline** the **case details** include:-
  1. Situation : i.e. *employee abuse case*
  2. Nature of the case : *use email for personal matter*
  3. Specifics of the case : *detailed information of case*
  4. Type of evidence : *USB drive*
  5. Known disk format : *FAT*
  6. Location of evidence : *USB recovered from employee's desk*

- Based on these details, you can determine the case requirements

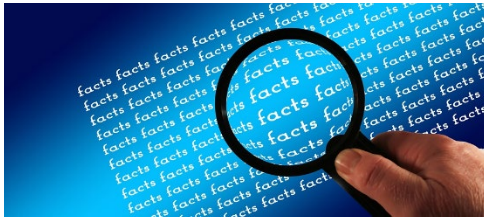
Planning Your Investigation

- A basic **investigation plan** should include the following activities:
  1. Acquire the evidence
  2. Complete an evidence form and establish a chain of custody (*helps show where the file came from, who created it, and the type of equipment that was used*)
  3. Transport the evidence to a computer forensics lab
  4. Secure evidence in an **approved secure container**


Preliminary Analysis
Incident Awareness Consultation
Deposition/ Affidavit
Image Acquisition/ Recovery
Detailed Analysis
Preliminary/ Final Report
Presentation

Planning Your Investigation

5. Prepare your **forensics workstation**
6. Retrieve the evidence from the secure container
    5. *To ensure information is confidential. Container should be a locked, fireproof locker or cabinet that has limited access*)
7. Make a forensic copy of the evidence
8. Return the evidence to the secure container
9. Process the copied evidence with computer forensics tools (*i.e EnCase*)

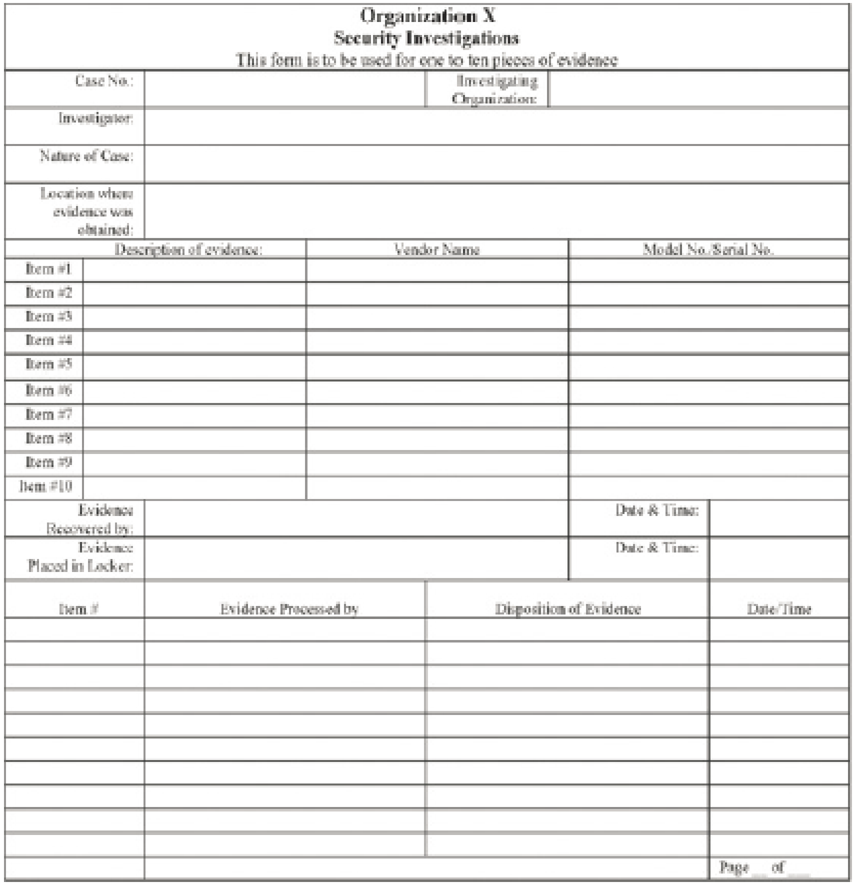


Planning Your Investigation

- An **evidence custody form** helps you document what has been done with the original evidence and its forensics copies
  - Also called a chain-of-evidence form

- Two types
  - **Single-evidence form**
    - Lists each piece of evidence on a separate page
  - **Multi-evidence form**

Planning Your Investigation



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

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

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

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

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

Figure 1-10 A sample multi-evidence form used in a private-sector environment
©Cengage Learning®

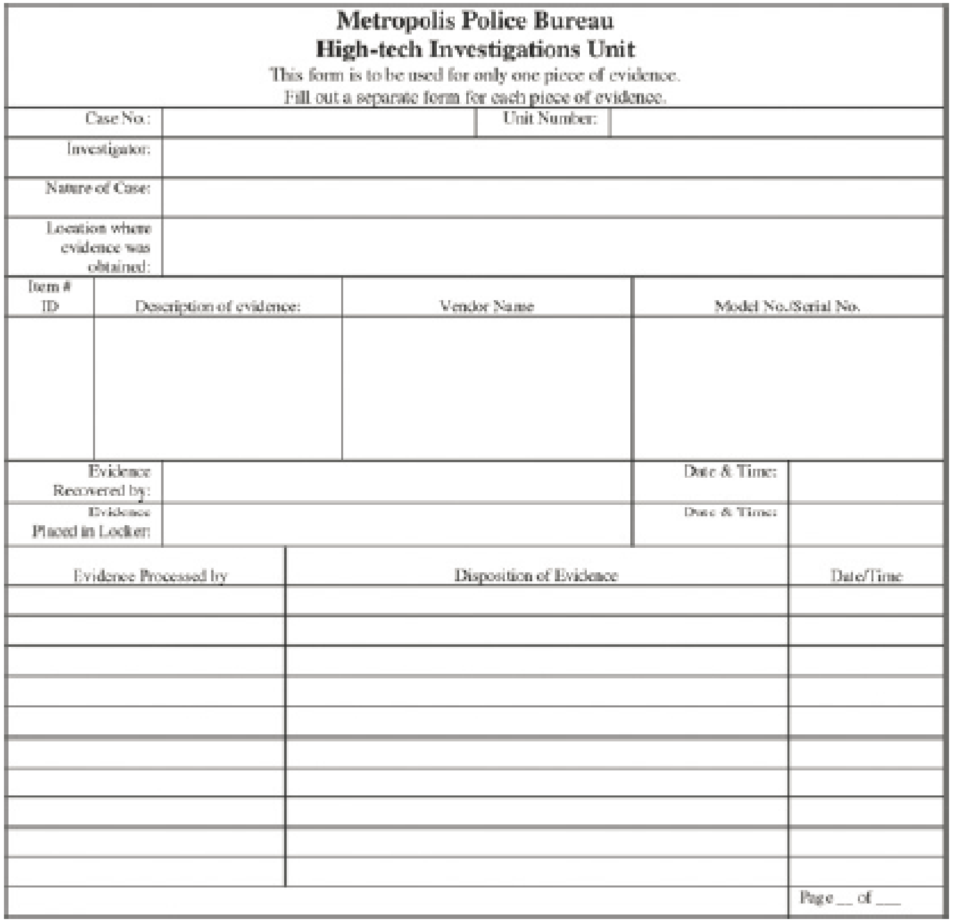
Examples:-

- **Model number or serial number**—List the model number or serial number (if available) of the computer component.

- **Evidence recovered** by—The name of the investigator who recovered the evidence.
The chain of custody for evidence starts with this information. The person placing his or her name on this line is responsible for preserving, transporting, and securing the evidence.

- **Date and time**—The date and time the evidence was taken into custody.

Planning Your Investigation



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

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

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

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

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

Figure 1-11 A single-evidence form
©Cengage Learning®

Securing Your Evidence

- Use **evidence bags** to secure and catalog the evidence

- Use computer safe products when collecting computer evidence
  - Antistatic bags
  - Antistatic pads

- Use well padded containers

- Use evidence tape to seal all openings
  - CD drive bays
  - Insertion slots for power supply electrical cords and USB cables

Securing Your Evidence

- Write your initials on tape to prove that evidence has not been tampered with

- Consider computer specific temperature and humidity ranges
  - Make sure you have a safe environment for transporting and storing it until a secure evidence container is available

Procedures for Private-Sector High-Tech Investigations

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

Example #1: Employee Termination Cases

- The majority of investigative work for termination cases involves employee abuse of corporate assets

- Incidents that create a hostile work environment are the predominant types of cases investigated
  - Viewing pornography in the workplace
  - Sending inappropriate e-mails

- Organizations must have appropriate policies in place – *consult HR department*

Example #2: Internet Abuse Investigations

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

Example : Internet Abuse Investigations

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

Example : E-mail Abuse Investigations

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

Example : E-mail Abuse Investigations (Cont)

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

Example : Industrial Espionage Investigations

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

Example : Industrial Espionage Investigations (Cont)

- **Guidelines** when initiating an investigation
  1. Determine whether this investigation involves a possible industrial espionage incident
  2. Consult with corporate attorneys and upper management
  3. Determine what information is needed to substantiate the allegation
  4. Generate a list of keywords for disk forensics and sniffer monitoring
  5. List and collect resources for the investigation

Example : Industrial Espionage Investigations (Cont)

- Guidelines (cont’d)
  6. Determine goal and scope of the investigation
  7. Initiate investigation after approval from management

- **Planning** considerations
  1. Examine all e-mail of suspected employees
  2. Search Internet newsgroups or message boards
  3. Initiate physical surveillance
  4. Examine facility physical access logs for sensitive areas

Example : Industrial Espionage Investigations (Cont)

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

- **Steps to conducting an industrial espionage case**
  1. Gather all personnel assigned to the investigation and brief them on the plan
  2. Gather resources to conduct the investigation

Example : Industrial Espionage Investigations (Cont)

- **Steps** (cont'd)
  3. Place surveillance systems at key locations
  4. Discreetly gather any additional evidence
  5. Collect all log data from networks and e-mail servers
  6. Report regularly to management and corporate attorneys
  7. Review the investigation's scope with management and corporate attorneys

Interviews and Interrogations in High-Tech Investigations

- Becoming a skilled **interviewer and interrogator** can take many years of experience

Definition:-

- **Interview**
  - Usually conducted to collect information from a witness or suspect
    - About specific facts related to an investigation

- **Interrogation**
  - Process of trying to get a suspect to confess

Interviews and Interrogations in High-Tech Investigations

- Role as a computing investigator
  - To instruct the investigator, who is conducting the interview on what questions to ask
    - And what the answers should be

- Ingredients for a successful interview or interrogation
  - Being patient throughout the session
  - Repeating or rephrasing questions to zero in on specific facts from a reluctant witness or suspect
  - Being tenacious

Understanding **Data Recovery Workstations** and **Software**

- Investigations are conducted on a computer forensics lab (or data-recovery lab)
  - In data recovery, the customer or your company just wants the data back

- **Computer forensics workstation**
  - A specially configured PC
  - Loaded with additional bays and forensics software

- To avoid altering the evidence use:
  - **Write-blockers devices**
    - Enable you to boot to Windows without writing data to the evidence drive

Setting Up Your Workstation for Digital Forensics

- Basic requirements
  1. A workstation running Windows XP or later
  2. A write-blocker device : *prevent writes to storage devices*
  3. Digital forensics acquisition tool
  4. Digital forensics analysis tool
  5. Target drive to receive the source or suspect disk data
  6. Spare PATA (*parallel*) or SATA (*Serial*) ports
  7. USB ports

Ref : www.cru-inc.com

Setting Up your Workstation for Digital Forensics

- Additional useful items
  1. Network interface card (NIC)
  2. Extra USB ports
  3. FireWire (*IEEE 1394*) 400/800 ports
  4. SCSI card
  5. Disk editor tool
  6. Text editor tool
  7. Graphics viewer program
  8. Other specialized viewing tools

Conducting an Investigation

- Gather resources identified in investigation plan

- Items needed
  1. Original storage media
  2. Evidence custody form
  3. Evidence container for the storage media
  4. Bit-stream imaging tool
  5. Forensic workstation to copy and examine your evidence
  6. Securable evidence locker, cabinet, or safe

Gathering the Evidence

- Avoid damaging the evidence : *Important!*
- Steps
  1. Meet the IT manager to interview him
  2. Fill out the evidence form, have the IT manager sign
  3. Place the evidence in a secure container
  4. Carry the evidence to the computer forensics lab
  5. Complete the evidence custody form
  6. Secure evidence by locking the container

Ref : http://www.sirchie.com

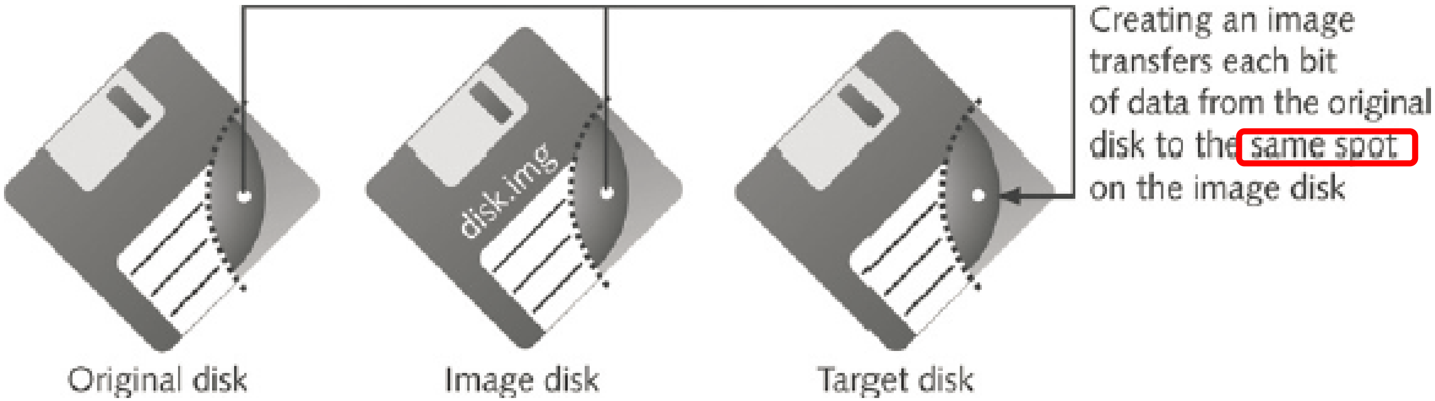
Understanding **Bit-Stream Copies**

- **Bit-stream copy**
  - Bit-by-bit copy of the original storage medium
  - **Exact copy** of the original disk
  - Different from a simple backup copy
    - Backup software only copy known files
    - Backup software cannot copy deleted files, e-mail messages or recover file fragments

- **Bit-stream image**
  - File containing the bit-stream copy of all data on a disk or partition
  - Also known as “image” or “image file”

Understanding Bit-stream Copies

- Copy image file to a target disk that matches the original disk’s manufacturer, size and model



Creating an image transfers each bit of data from the original disk to the same spot on the image disk

Figure 1-12 Transfer of data from original to image to target
©Cengage Learning®

Acquiring an Image of Evidence Media

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

Completing the Case

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

Completing the Case (Cont)

- Keep a written journal of everything you do
  - Your notes can be used in court
- Answer the six **W**s:
  - Who, what, when, where, why, and how
- You must also explain computer and network processes. (*good to identify who is your report reader and write something that is suitable for the reader*)

Critiquing the Case

- Ask yourself the following questions:
  1. How could you improve your performance in the case?
  2. Did you expect the results you found? Did the case develop in ways you did not expect?
  3. Was the documentation as thorough as it could have been?
  4. What feedback has been received from the requesting source?

Critiquing the Case

- Ask yourself the following questions (cont’d):
  - Did you discover any new problems? If so, what are they?
  - Did you use new techniques during the case or during research?

Summary

- Digital forensics involves systematically accumulating and analyzing digital information for use as evidence in civil, criminal, and administrative cases

- Investigators need specialized workstations to examine digital evidence (*must always have the right tools!!*)

- Public-sector and private-sector investigations differ; public-sector typically require search warrants before seizing digital evidence

Summary

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

Summary

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