Understanding Investigations

CSC 388 – Spring 2021

Introduction

Objectives

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

What is digital forensics?

- The application of computer science and investigative procedures for a legal purpose involving the analysis of digital evidence after proper search authority, chain of custody, validation with mathematics, use of validated tools, repeatability, reporting, and possible expert presentation.
  - In October 2012, an ISO standard for digital forensics was ratified - ISO 27037 Information technology - Security techniques

The Target

- Extracting relevant information for various types of investigations or recovery
  - Administrative / private
  - Criminal / public
  - Data recovery (we'll come back to this)
    - Recovering intentionally or accidentally lost data can be part of any forensics investigation, but can also occur independently (ex: accidentally cleared SD card in camera, damaged phone, etc.)

Elements of an Investigation

- Investigating digital devices includes:
  - Collecting data securely
  - Examining suspect data to determine details such as origin and content
  - Presenting digital information to courts
  - Applying laws to digital device practices
- Forensics investigators often work as part of a team, known as the investigations triad

The Investigations Triad

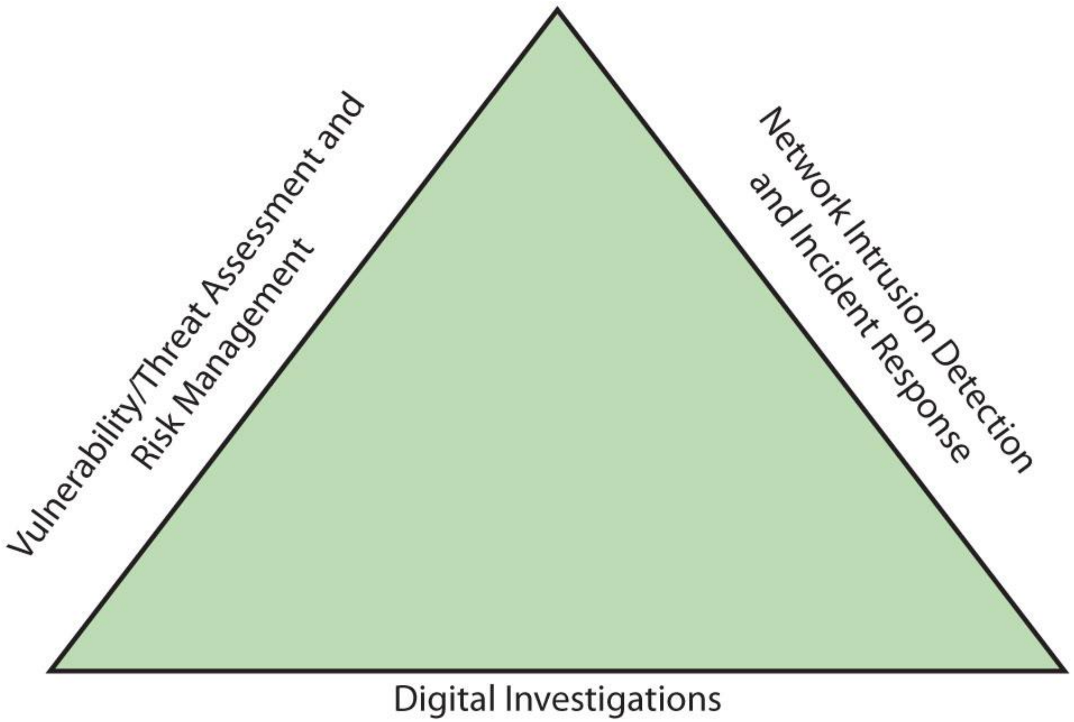
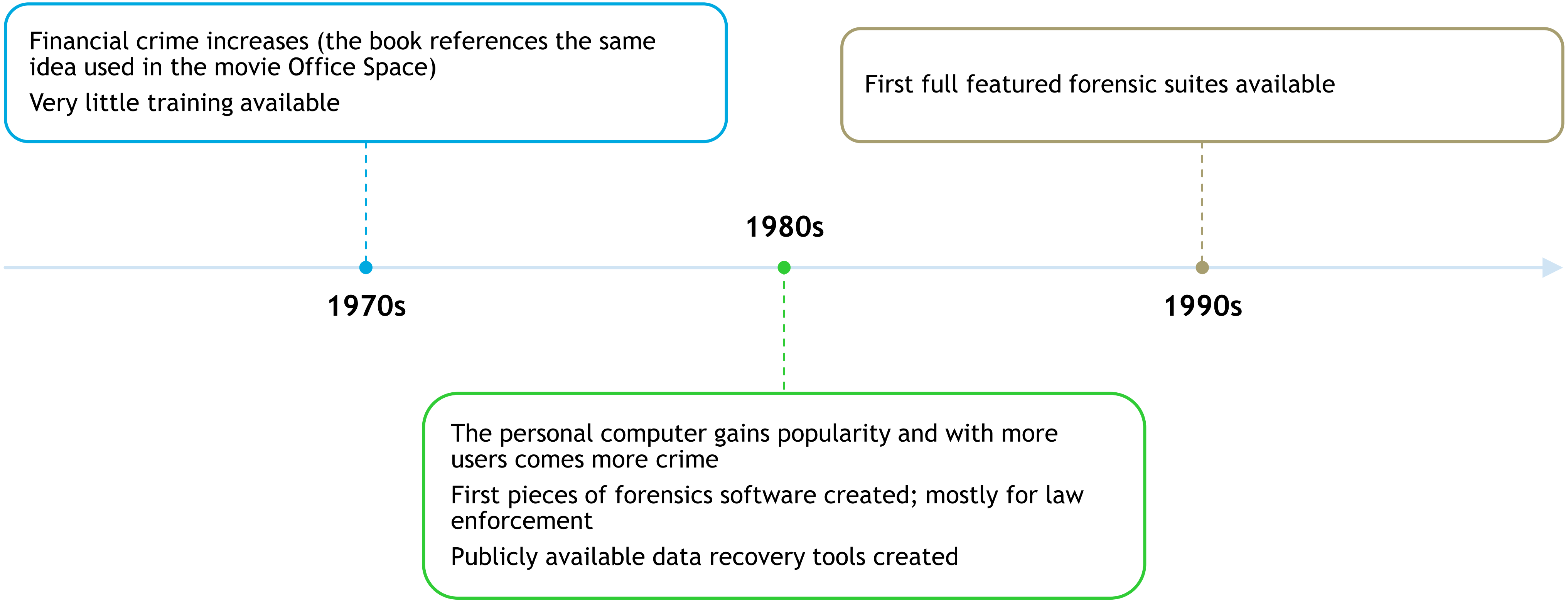

Vulnerability/Threat Assessment and Risk Management
Network Intrusion Detection and Incident Response
Digital Investigations

Figure 1-1 **The investigations triad**

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

Brief History



1970s

Financial crime increases (the book references the same idea used in the movie Office Space)

Very little training available

1980s

The personal computer gains popularity and with more users comes more crime

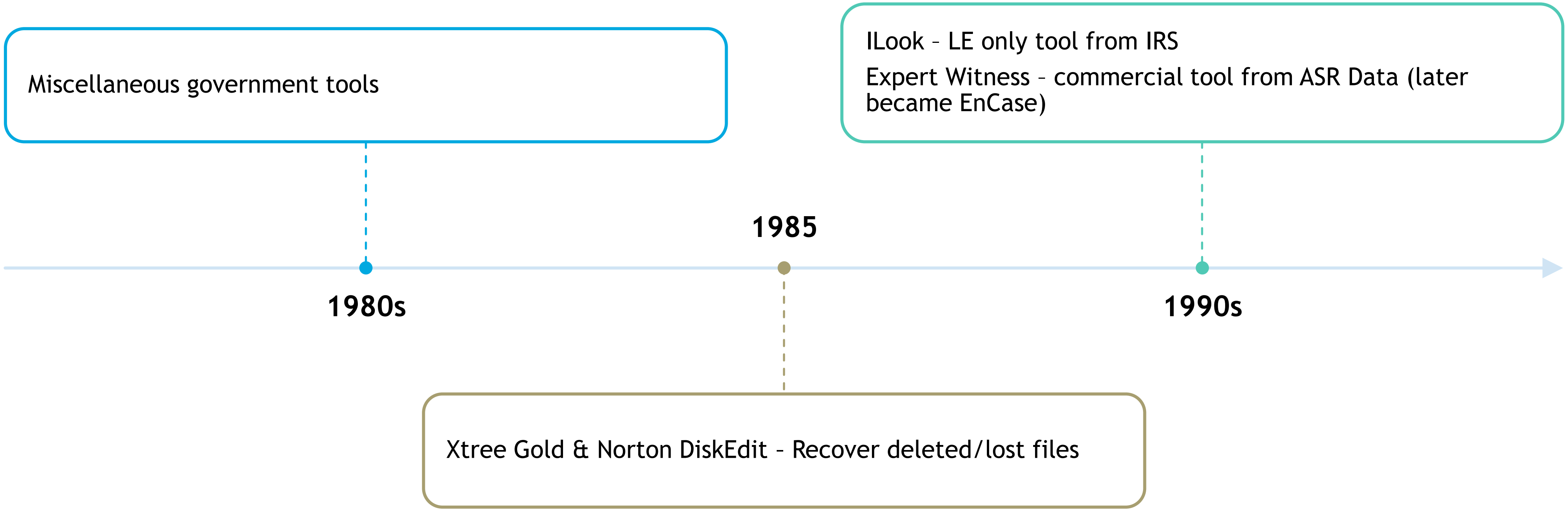
First pieces of forensics software created; mostly for law enforcement

Publicly available data recovery tools created

1990s

First full featured forensic suites available

Some Tool History



Miscellaneous government tools

1980s

1985

Xtree Gold & Norton DiskEdit – Recover deleted/lost files

1990s

ILook – LE only tool from IRS

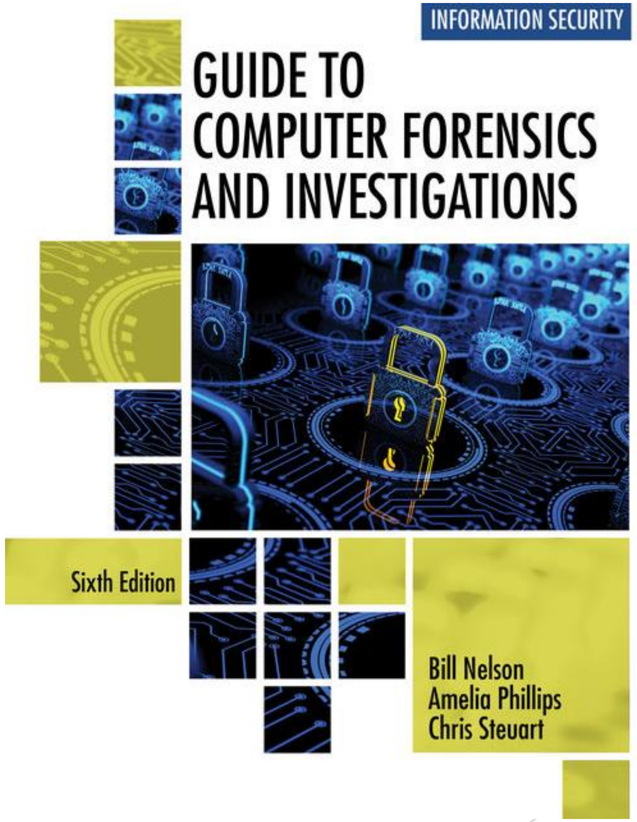
Expert Witness – commercial tool from ASR Data (later became EnCase)

Understanding Case Law

- Existing laws can’t keep up with the rate of technological change
- When statutes don’t exist, case law is used
  - Allows legal counsel to apply previous similar cases to current one in an effort to address ambiguity in laws
- Examiners must be familiar with recent court rulings on search and seizure in the electronic environment

References

- Wikipedia: EnCase / FTK
- *Guide to Computer Forensics and Investigations*
  - *ISBN: 9780357688595*



Preparation

Developing Resources

- To supplement your knowledge:
  - Develop and maintain contact with computing, network, and investigative professionals
  - Join computer user groups in both the pubic and private sectors
  - Consult outside experts
- Focus on continuing education when available:
  - Attend conferences
  - Take professional trainings
- Share your knowledge when appropriate:
  - Document and share what you can publicly for the greater good
  - Document successful processes internally

When can digital evidence be gathered?

- The Fourth Amendment to the U.S. Constitution protects everyone’s right to be secure from search and seizure
  - Separate **search warrants** might not be necessary for digital evidence
  - Rules for organizations are different and depend on how users use their corporate resources and what the users agreed to (even if that agreement is implied)

- Every U.S. jurisdiction has case law related to the admissibility of evidence recovered from computers and other digital devices

Understanding Law Enforcement Agency Investigations

- When conducting public-sector investigations, you must understand laws on computer-related crimes including:
  - Standard legal processes
  - Guidelines on search and seizure
  - How to build a criminal case

- The Computer Fraud and Abuse Act was passed in 1986
  - Specific state laws were generally developed later
  - The text notes Alabama has wording that adjusts qualifications for felony vs misdemeanor crimes

Steps of a Criminal Investigation

- A criminal investigation usually begins when someone finds evidence of or witnesses a crime
  - Witness or victim makes an **allegation** to the police
- Police interview the complainant and writes a report about the crime
- Report is processed and management decides to start an investigation or log the information in a police blotter
  - Blotter is a historical database of previous crimes

Steps of a Criminal Investigation (Cont.)

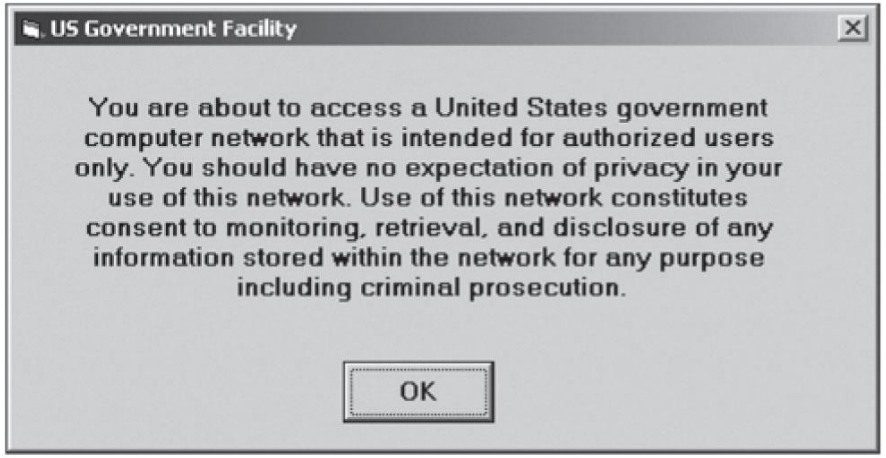
- **Digital Evidence First Responder (DEFR)**
  - Arrives on an incident scene, assesses the situation, and takes precautions to acquire and preserve evidence
- **Digital Evidence Specialist (DES)**
  - Has the skill to analyze the data and determine when another specialist should be called in to assist
- **Affidavit** - a sworn statement of support of facts about or evidence of a crime
  - Must include **exhibits** that support the allegation

Private Sector Investigations

- Private-sector investigations involve private companies and lawyers who address company policy violations and litigation disputes
  - Example: wrongful termination
- Businesses strive to minimize or eliminate litigation
- Private-sector crimes can involve:
  - E-mail harassment, falsification of data, gender and age discrimination, embezzlement, sabotage, and industrial espionage

Private Sector Investigations (Cont.)

- Generally, organizations use an “Acceptable Use Policy” or AUP to define the rules of using company computers
  - This is generally signed at initial access being granted to a network
  - The policy (or a referenced policy) will document who may authorize investigations
- Additionally, warning banners can be used to reinforce the implications of accessing a particular system



You are about to access a United States government computer network that is intended for authorized users only. You should have no expectation of privacy in your use of this network. Use of this network constitutes consent to monitoring, retrieval, and disclosure of any information stored within the network for any purpose including criminal prosecution.

Figure 1-7 A sample warning banner

Private Sector Investigations (Cont.)

- During private investigations, you search for evidence to support allegations of violations of a company’s rules or an attack on its assets
- Three types of situations are common:
  - Abuse or misuse of computing assets
  - E-mail abuse
  - Internet abuse
- A private-sector investigator’s job is to minimize risk to the company

Bring Your Own Device

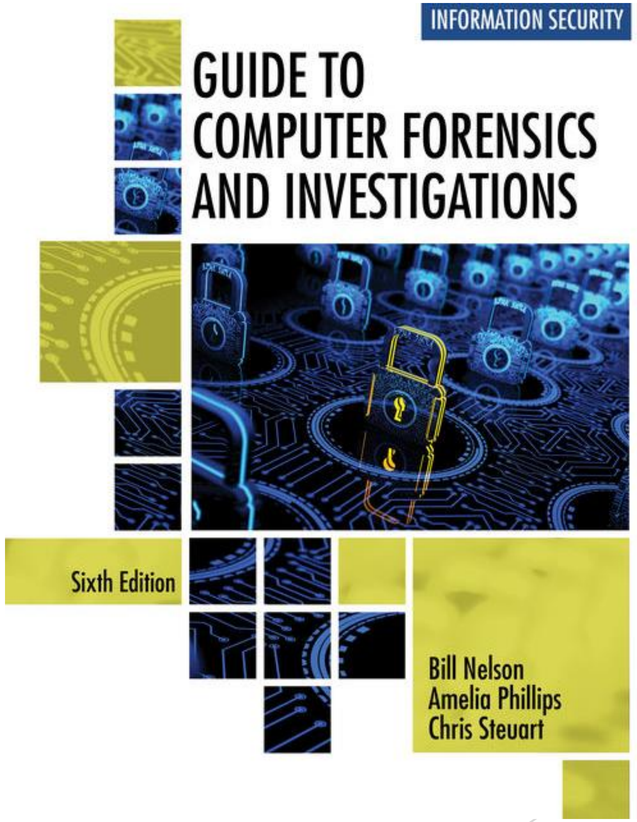
- The distinction between personal and company computer property can be difficult with cell phones, smartphones, personal notebooks, and tablet computers
- Bring your own device (BYOD) environment
  - Some companies state that if you connect a personal device to the business network, it falls under the same rules as company property

Professional Conduct

- **Professional conduct** - includes ethics, morals, and standards of behavior
- An investigator must exhibit the highest level of professional behavior at all times
  - Maintain objectivity
  - Maintain credibility by maintaining confidentiality
- Investigators should also attend training to stay current with the latest technical changes in computer hardware and software, networking, and forensic tools

References

- [Warning Banner Examples from DOJ]()
- *Guide to Computer Forensics and Investigations*
  - *ISBN: 9780357688595*



Gathering Evidence

Getting Started

- The role of digital forensics professional is to gather evidence to prove that a suspect committed a crime or violated a company policy

- Collect evidence that can be offered in court or at a corporate inquiry
  - Investigate the suspect’s computer
  - Preserve the evidence on a different computer

- **Chain of custody**
  - Route the evidence takes from the time you find it until the case is closed or goes to court

Reminders

- 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
- Additionally, computers may include evidence of company misuse

Use a Systematic Approach

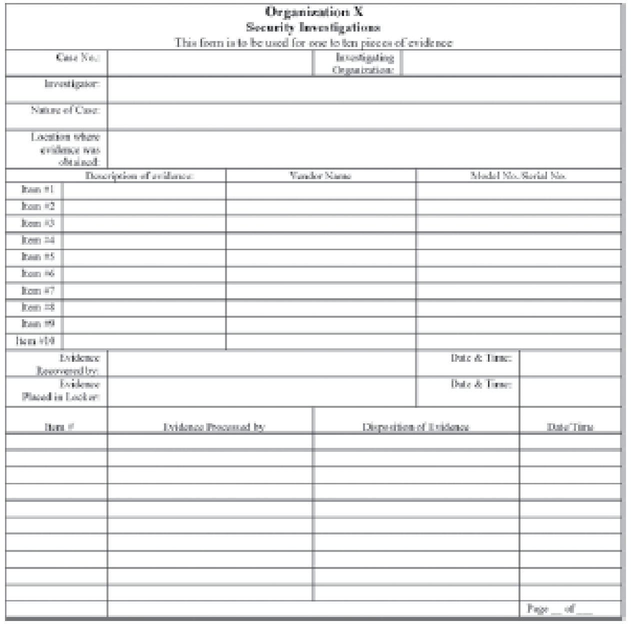
- Make an initial assessment about the type of case you are investigating
- Determine a preliminary design or approach to the case
- Create a detailed checklist
- Determine the resources you need
- Obtain and copy an evidence drive
- Identify the risks
- Mitigate or minimize the risks
- Test the design
- Analyze and recover the digital evidence
- Investigate the data you recover
- Complete the case report
- Critique the case

Planning

- 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**
  - Prepare your **forensics workstation**
  - Retrieve the evidence from the secure container
  - Make a forensic copy of the evidence
  - Return the evidence to the secure container
  - Process the copied evidence with computer forensics tools

Planning (Cont.)

- 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**

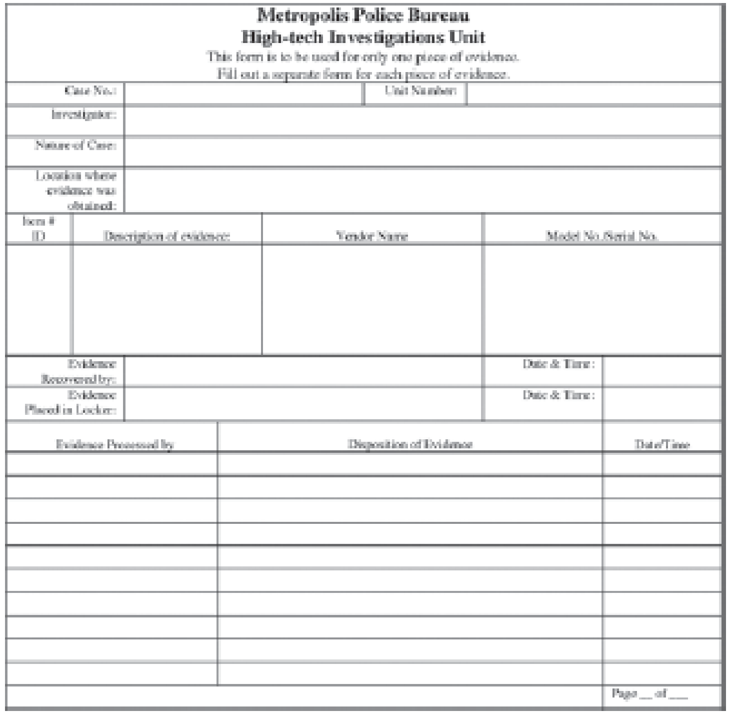


Organization X
Security Investigations
This form is to be used for one to ten pieces of evidence

Case No.:		Investigating Organization:		
Investigator:				
Nature of Case:				
Location where evidence was obtained:				
	Description of evidence:	Vendor Name	Model No./Serial No.	
Item #1				
Item #2				
Item #3				
Item #4				
Item #5				
Item #6				
Item #7				
Item #8				
Item #9				
Item #10				
Evidence Recovered by:			Date & Time:	
Evidence Placed in Locker:			Date & Time:	

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

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



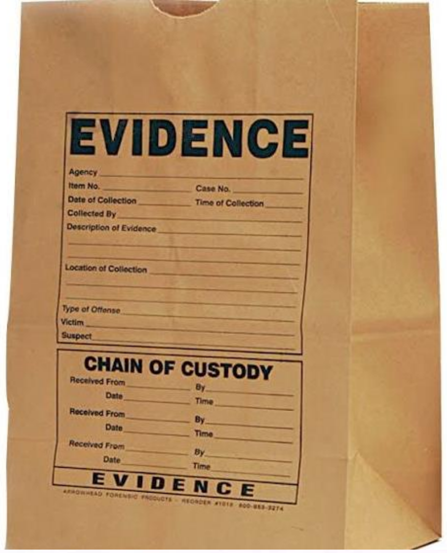
Metropolis Police Bureau
High-tech Investigations Unit
This form is to be used for only one piece of evidence.
Fill out a separate form for each piece of evidence.

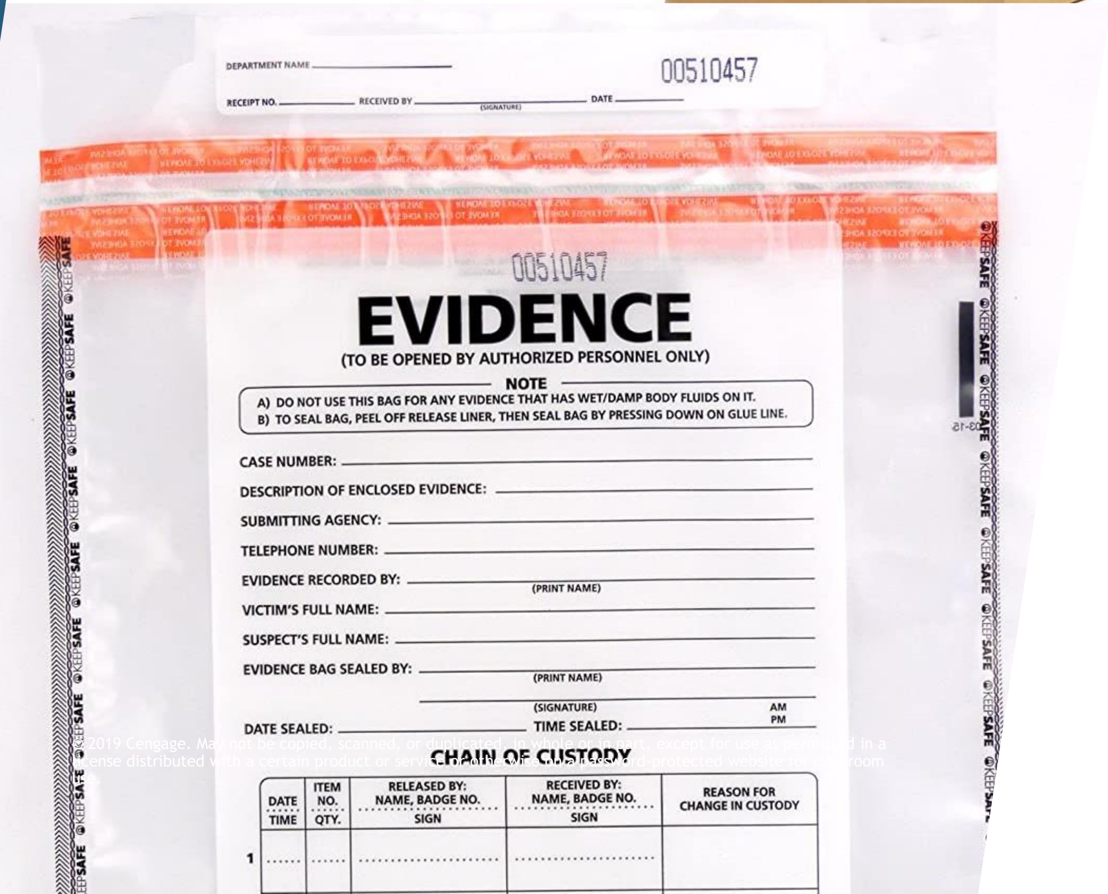
Case No.:		Unit Number:		
Investigator:				
Nature of Case:				
Location where evidence was obtained:				
Item # ID	Description of evidence:	Vendor Name	Model No./Serial No.	
Evidence Recovered by:			Date & Time:	
Evidence Placed in Locker:			Date & Time:	

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

Figure 1-10 A single-evidence form

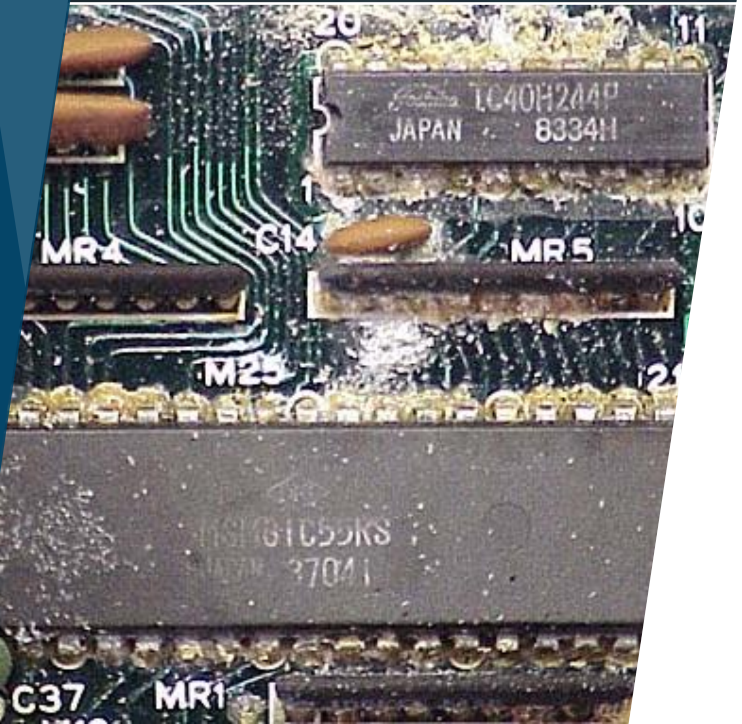
Evidence Forms




DEPARTMENT NAME
00510457
RECEIPT NO.
RECEIVED BY
(SIGNATURE)
DATE
KEEPSAFE
00510457
EVIDENCE
(TO BE OPENED BY AUTHORIZED PERSONNEL ONLY)
NOTE
A) DO NOT USE THIS BAG FOR ANY EVIDENCE THAT HAS WET/DAMP BODY FLUIDS ON IT.
B) TO SEAL BAG, PEEL OFF RELEASE LINER, THEN SEAL BAG BY PRESSING DOWN ON GLUE LINE.
CASE NUMBER:
DESCRIPTION OF ENCLOSED EVIDENCE:
SUBMITTING AGENCY:
TELEPHONE NUMBER:
EVIDENCE RECORDED BY:
(PRINT NAME)
VICTIM'S FULL NAME:
SUSPECT'S FULL NAME:
EVIDENCE BAG SEALED BY:
(PRINT NAME)
(SIGNATURE)
DATE SEALED:
TIME SEALED:
AM
PM
CHAIN OF CUSTODY
DATE
TIME
ITEM NO.
QTY.
RELEASED BY: NAME, BADGE NO. SIGN
RECEIVED BY: NAME, BADGE NO. SIGN
REASON FOR CHANGE IN CUSTODY
1

Securing 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

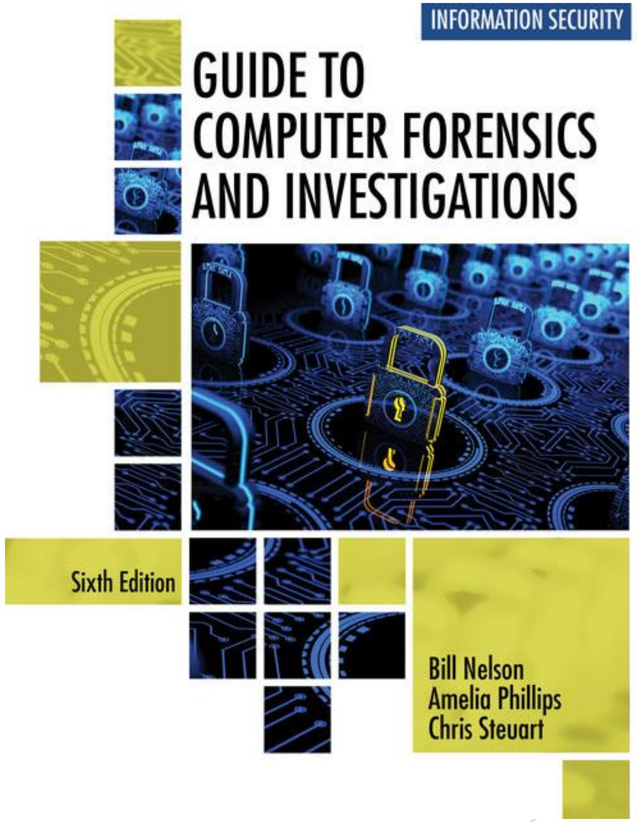


Securing Evidence (Cont.)

- 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

References

- *Guide to Computer Forensics and Investigations*
  - *ISBN: 9780357688595*



Starting the Investigation

Different Scenarios May Require Different Approaches

- 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

Employee Termination Cases

- The majority of investigative work for termination cases involves employee abuse of corporate assets
- Examples of incidents include:
  - Misuse of corporate assets (Time theft, personal gain, etc)
  - Viewing pornography in the workplace
  - Sending inappropriate e-mails
- Organizations must have appropriate policies in place

Internet Abuse Investigations

- To conduct an investigation you need:
  - Suspect computer's IP address
    - IT department should coordinate and document whether this is static or changing, and if so when they can document it changed
  - Corporate traffic logs (proxy logs, archived traffic flow, etc)
  - Suspect computer's disk drive
  - Your preferred computer forensics analysis tool(s)
- Recommended steps
  - Use standard forensic analysis techniques and procedures
  - Use appropriate tools to extract all Web page URL information
  - Compare the data recovered from forensic analysis to the logs

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 logs
  - 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(s)
- Recommended steps
  - 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

Attorney-Client Privilege Investigations

- Under **attorney-client privilege (ACP)** rules for an attorney
  - You must keep all findings confidential

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

Attorney-Client Privilege Investigations (Cont.)

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

- Other guidelines
  - Minimize written communications with the attorney
  - Any documentation written to the attorney must contain a header stating that it’s “Privileged Legal Communication—Confidential Work Product”
  - Assist the attorney and paralegal in analyzing data

Industrial Espionage Investigations

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

Industrial Espionage Investigations (Cont.)

- Guidelines when initiating an investigation
    - Determine whether this investigation involves a possible industrial espionage incident
    - Consult with corporate attorneys and upper management
    - Determine what information is needed to substantiate the allegation
    - Generate a list of keywords for disk forensics and sniffer monitoring
    - List and collect resources for the investigation
    - Determine goal and scope of the investigation
    - Initiate investigation after approval from managementx

Industrial Espionage Investigations (Cont.)

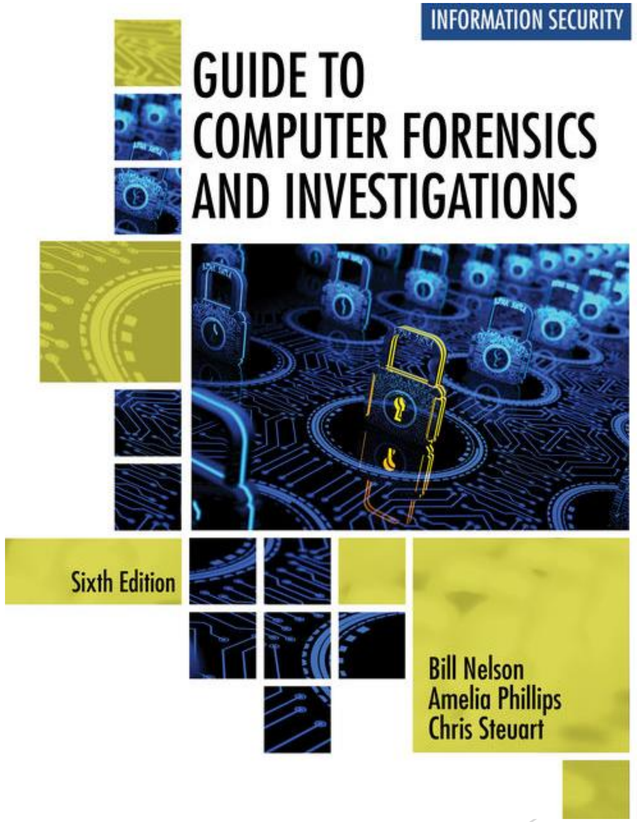
- Planning considerations
  - Examine all e-mail of suspected employees
  - Search Internet newsgroups or message boards
  - Initiate physical surveillance
  - Examine facility physical access logs for sensitive areas
  - Determine suspect location in relation to the vulnerable asset
  - Study the suspect’s work habits
  - Collect all incoming and outgoing phone logs

Industrial Espionage Investigations (Cont.)

- Steps to conducting an industrial espionage case
  - Gather all personnel assigned to the investigation and brief them on the plan
  - Gather resources to conduct the investigation
  - Place surveillance systems at key locations
  - Discreetly gather any additional evidence
  - Collect all log data from networks and e-mail servers
  - Report regularly to management and corporate attorneys
  - Review the investigation’s scope with management and corporate attorneys

References

- *Guide to Computer Forensics and Investigations*
  - *ISBN: 9780357688595*



Your Analysis System

Preparation and initial acquisition

Forensic Workstation Considerations

- Computer Forensics Workstation
  - Specially configured for the tasks of forensic analysis
  - Typically contains extra storage and forensic software suites
  - Critical: should contain or have access to a **write-blocker**
    - Write-blockers prevent writing data to an evidence drive
    - Hardware write-blockers are preferred, but when required software write-blockers can be allowed

Forensic Workstation Considerations (Cont.)

- The OS your workstation uses could vary depending on investigation
  - What OS does the suspect use? Should you use the same?
  - Do the tools you want to use run on your OS?
- You need ways to look at artifacts you’re reviewing

Gathering Evidence

- Avoid damaging the evidence
- Collection steps:
  - Meet the IT manager to interview them
  - Fill out the evidence form, have the IT manager sign
  - Place the evidence in a secure container
  - Carry the evidence to the computer forensics lab
  - Complete the evidence custody form
  - Secure evidence by locking the container

Capturing an Image or Clone

- You want to protect the original evidence and prevent changes to it (this is where the write blocker comes in)
  - Conduct your analysis only on a copy of the data

- There are two options to acquiring copies of evidence to evaluate
  - Bit-stream copies/clones
  - Bit-stream images

- Bit streams are copies of all data on a disk (even data inaccessible by the OS)
  - A typical backup is likely not the same as a bit-stream clone/image

Expert Witness Format (EWF / .E01)

- A compressed image format that contains additional metadata about the acquisition
  - Includes verification for entire disk and blocks within the disk
  - Saves space for drives that contain mostly the same thing (pre-zeroed)

Collecting an Image

References

- Good preview of hardware write blockers

- *Guide to Computer Forensics and Investigations*
  - *ISBN: 9780357688595*