LECTURE 02: INTRODUCTION CONT'D

DR. ZUNERA JALIL

EMAIL: ZUNERA.JALIL@AU.EDU.PK

18/2/2025

DIGITAL FORENSICS

Digital Forensics is the application of **computer science** and **investigative procedures** for a **legal purpose** involving the **analysis** of **digital evidence** (information of probative value that is stored or transmitted in binary form) after proper **search authority, chain of custody, validation with mathematics** (hash function)**, use of validated tools, repeatability, reporting and possible expert presentation.**

(The former director of the Defense Computer Forensics Laboratory, Ken Zatyko).

DIGITAL FORENSIC (NIST'S DEFINITION)

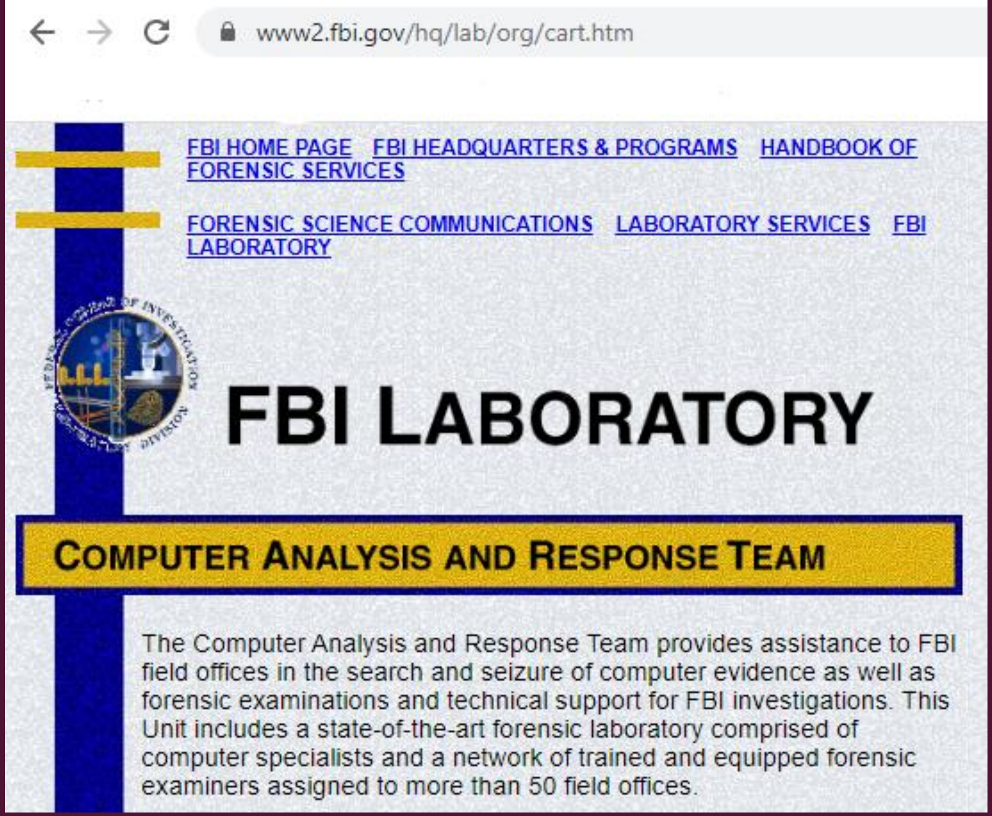
- "The application of science to the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data."
- NIST SP800-86 (Guide to Integrating Forensic Techniques into Incident Response)

https://csrc.nist.gov/publications/detail/sp/800-86/final

DIGITAL FORENSICS STANDARDS

ISO 27037

- “Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence” www.iso.org/standard/44381.html



FBI HOME PAGE FBI HEADQUARTERS & PROGRAMS HANDBOOK OF FORENSIC SERVICES

FORENSIC SCIENCE COMMUNICATIONS LABORATORY SERVICES FBI LABORATORY

FBI LABORATORY

COMPUTER ANALYSIS AND RESPONSE TEAM

The Computer Analysis and Response Team provides assistance to FBI field offices in the search and seizure of computer evidence as well as forensic examinations and technical support for FBI investigations. This Unit includes a state-of-the-art forensic laboratory comprised of computer specialists and a network of trained and equipped forensic examiners assigned to more than 50 field offices.

https://www2.fbi.gov/hq/lab/org/cart.htm

CART

- FBI Computer Analysis and Response Team (CART)
  - Formed in 1984 to handle the increasing number of cases involving digital evidence

THE FOURTH AMENDMENT TO THE U.S. CONSTITUTION

- Protects everyone's right to be secure in their person, residence, and property from search and seizure.
- Continuing development of the jurisprudence of this amendment has played a role in determining whether the search for digital evidence has established a different precedent, so separate search warrants might not be necessary.
- When preparing to search for evidence in a criminal case, many investigators still include the suspect's computer and its components in the search warrant to avoid later admissibility problems.

DIGITAL FORENSICS VS. OTHER RELATED DISCIPLINES

ARCHAEOLOGIST

DIGITAL FORENSICS VS NETWORK FORENSICS

- Digital Forensics:
  - investigate data that can be retrieved from a computer's hard drive or other storage media
  - information retrieved might already be on the drive, but it might not be easy to find or decipher

- Network Forensics
  - yields information about how attackers gain access to a network along with files they might have
    - copied
    - examined
    - or tampered with
  - examiners use log files to determine:
    - when users logged on
    - which URLs users accessed
    - how they logged on to the network
    - and from what location.
  - Determines:
    - what tracks or new files were left behind on a victim's computer
    - what changes were made

DIGITAL FORENSICS VS DATA RECOVERY

- Digital forensics is the task of recovering data that users have hidden or deleted, with the goal of ensuring that the recovered data is valid so that it can be used as evidence
- In digital forensics you are looking for any possible evidence

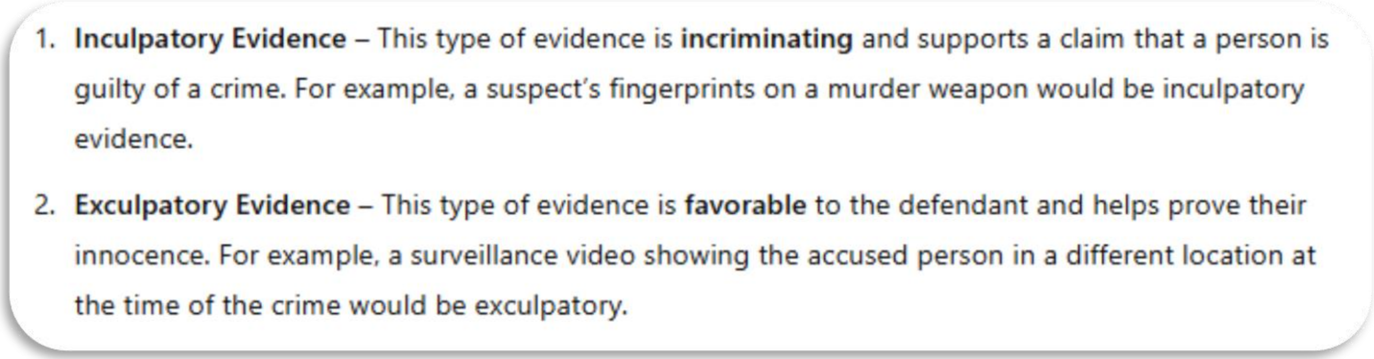
- Data recovery involves retrieving information that was deleted by mistake or lost during a power surge or server crash
- In data recovery you know what you're looking for

DIGITAL FORENSICS VS DISASTER RECOVERY

- Task of recovering data that users have hidden or deleted and using it as evidence
- Evidence can be **inculpatory** (“incriminating”) or **exculpatory**

- For disaster recovery investigator uses digital forensics techniques to retrieve information their clients have lost

CHATGPT



1. **Inculpatory Evidence** – This type of evidence is **incriminating** and supports a claim that a person is guilty of a crime. For example, a suspect’s fingerprints on a murder weapon would be inculpatory evidence.
2. **Exculpatory Evidence** – This type of evidence is **favorable** to the defendant and helps prove their innocence. For example, a surveillance video showing the accused person in a different location at the time of the crime would be exculpatory.

DIGITAL INVESTIGATION

- Investigators often work as a team to make computers and networks secure in an organization
- Each side of the triad represents a group or department responsible for performing the associated tasks
- The digital investigations group manages investigations and conducts forensics analysis of systems suspected of:
  - containing evidence related to an incident or a crime

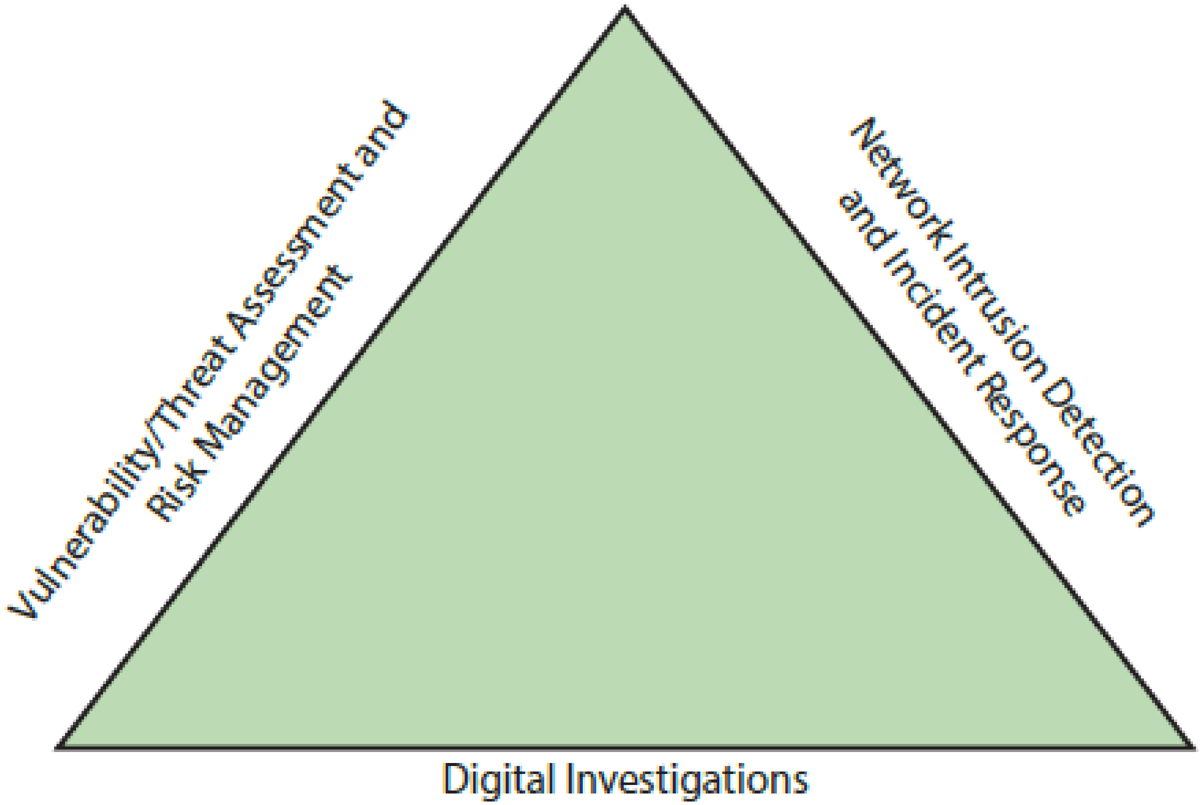

Vulnerability/Threat Assessment and Risk Management
Network Intrusion Detection and Incident Response
Digital Investigations

Figure 1-1 The investigations triad

BRIEF HISTORY OF DIGITAL FORENSICS

HISTORY OF DIGITAL FORENSICS (1/6)

One of the most well-known crimes of the mainframe era is the one-half cent crime. Banks commonly tracked money in accounts to the third decimal place or more.

They used and still use the rounding-up accounting method when paying interest. If the interest applied to an account resulted in a fraction of a cent, that fraction was used in the calculation for the next account until the total resulted in a whole cent. It was assumed that eventually every customer would benefit from this averaging.

Some computer programmers corrupted this method by opening an account for themselves and writing programs that diverted all the fractional monies into their accounts. In small banks, this practice amounted to only a few hundred dollars a month. In large banks with millions of accounts, however, the amount could reach hundreds of thousands of dollars

HISTORY OF DIGITAL FORENSICS (1/6)

- By the 1970s, electronic crimes were increasing, especially in the financial sector
  - Most law enforcement officers didn't know enough about computers to ask the right questions
    - Or to preserve evidence for trial
    - **One-half cent crime**
    - Law enforcement officers didn't know enough about computers to ask the right questions or to preserve evidence for trial

- 1980s
  - PCs gained popularity and different OSs emerged
  - Disk Operating System (DOS) was available
  - Forensics tools were simple, and most were generated by government agencies
  - Mostly written in C or assembly language.
  - US Internal Revenue Service & Royal Canadian Police usage.

HISTORY OF DIGITAL FORENSICS (2/6)

- Mid-1980s
    - Xtree Gold appeared on the market
        - Recognized file types and retrieved lost or deleted files
    - Norton DiskEdit soon followed
        - And became the best tool for finding deleted file

- 1987
    - Apple produced the Mac SE
        - A Macintosh with an external EasyDrive hard disk with 60 MB of storage

Figure 1-2 An 8088 computer

iStock.com/Maxiphoto

Figure 1-3 An 8088 computer

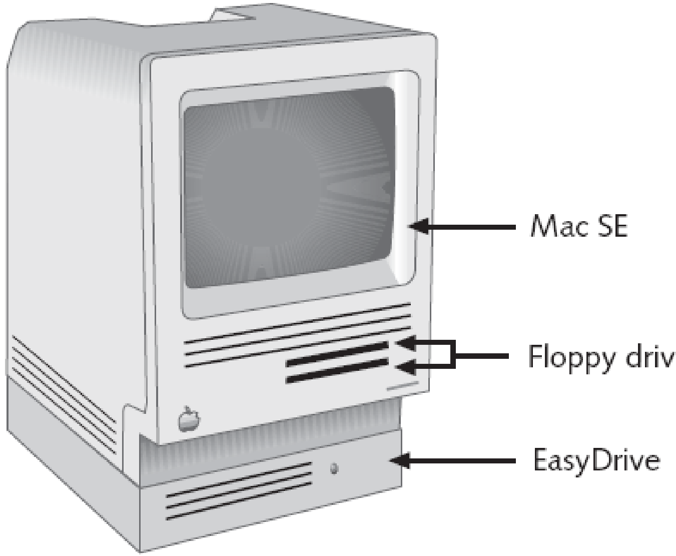


Figure 1-4 A Mac SE with an external EasyDrive hard disk

HISTORY OF DIGITAL FORENSICS (3/6)

HISTORY OF DIGITAL FORENSICS (4/6)

- Early 1990s
  - Tools for computer forensics were available
  - **International Association of Computer Investigative Specialists (IACIS)**
    - Training on software for forensics investigations
  - IRS created search-warrant programs
  - ExpertWitness for the Macintosh
    - First commercial GUI software for computer forensics
    - Created by ASR Data

HISTORY OF DIGITAL FORENSICS (156)

- Early 1990s (continued)
  - ExpertWitness for the Macintosh
    - Recovers deleted files and fragments of deleted files
    - Later one partner of ASR left and developed EnCase
- Large hard disks posed problems for investigators

HISTORY OF DIGITAL FORENSICS (6/6)

- Now
  - iLook
    - Maintained by the IRS, limited to law enforcement
    - Can analyze and read special files that are copies of the disk
  - EnCase
    - Available for public or private use
  - AccessData Forensic Toolkit (FTK)
    - Available for public or private use (Most Popular)

LAWS AND RESOURCES

CASE LAW

- Technology is evolving at an exponential pace
  - Existing laws and statutes can’t keep up change
- Case law used when statutes or regulations don’t exist
- Case law allows legal counsel to use previous cases similar to the current one
  - Because the laws don’t yet exist
- Each case is evaluated on its own merit and issues

DEVELOPING DIGITAL FORENSICS RESOURCES

- You must know more than one computing platform
  - Such as DOS, Windows 9x, Linux, Macintosh, and current Windows platforms/ Mobile OS's

- Join as many computer user groups as you can

- **Computer Technology Investigators Network (CTIN)**
  - Meets monthly to discuss problems that law enforcement and corporations face

PREPARING FOR DIGITAL INVESTIGATIONS

DIGITAL INVESTIGATIONS (1/2)

- Digital investigations and forensics falls into two distinct categories
  - Public investigations
  - Private or corporate investigations

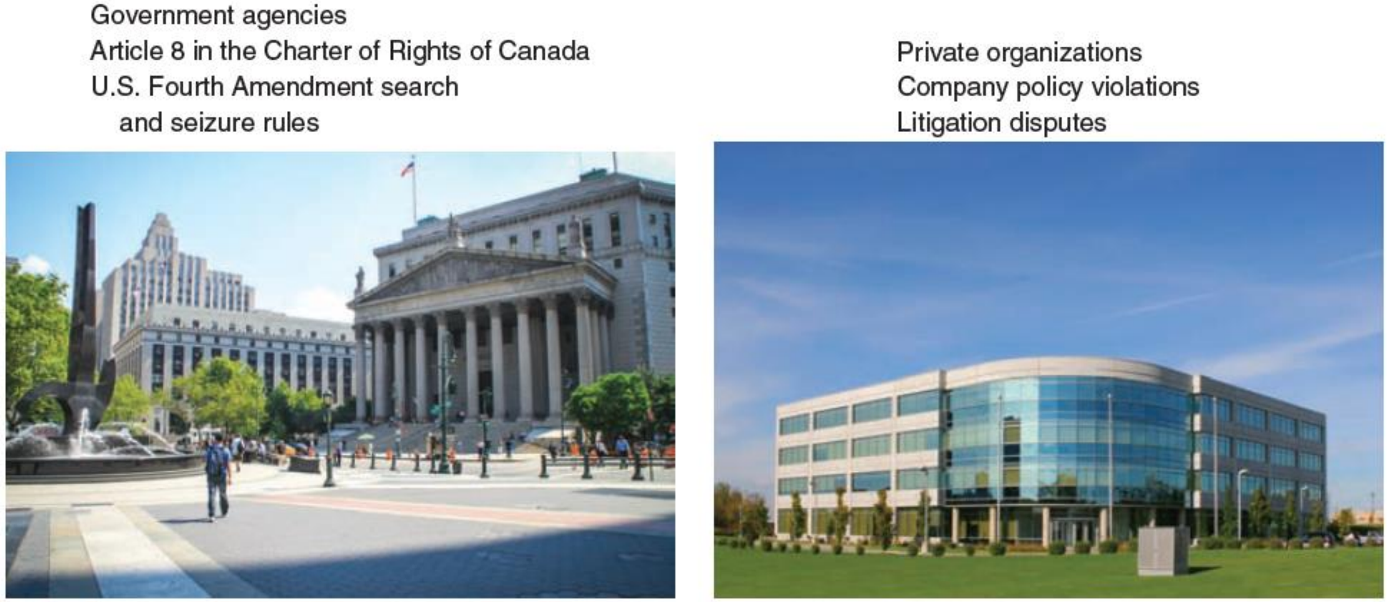

Government agencies
Article 8 in the Charter of Rights of Canada
U.S. Fourth Amendment search
and seizure rules
Private organizations
Company policy violations
Litigation disputes

Figure 1-4 **Public-sector and private-sector investigations**

iStock.com/RobinsonBecquart, iStock.com/buzbuzzer

DIGITAL INVESTIGATIONS (2/2)

- Public investigations
  - Involve government agencies responsible for criminal investigations and prosecution
  - Organizations must observe legal guidelines

- Private or corporate investigations
  - Deal with private companies, non-law-enforcement government agencies, and lawyers
  - Aren’t governed directly by **criminal law** or Fourth Amendment issues
  - Governed by internal policies that define expected employee behavior and conduct in the workplace
- Private corporate investigations also involve litigation disputes
- Investigations are usually conducted in civil cases

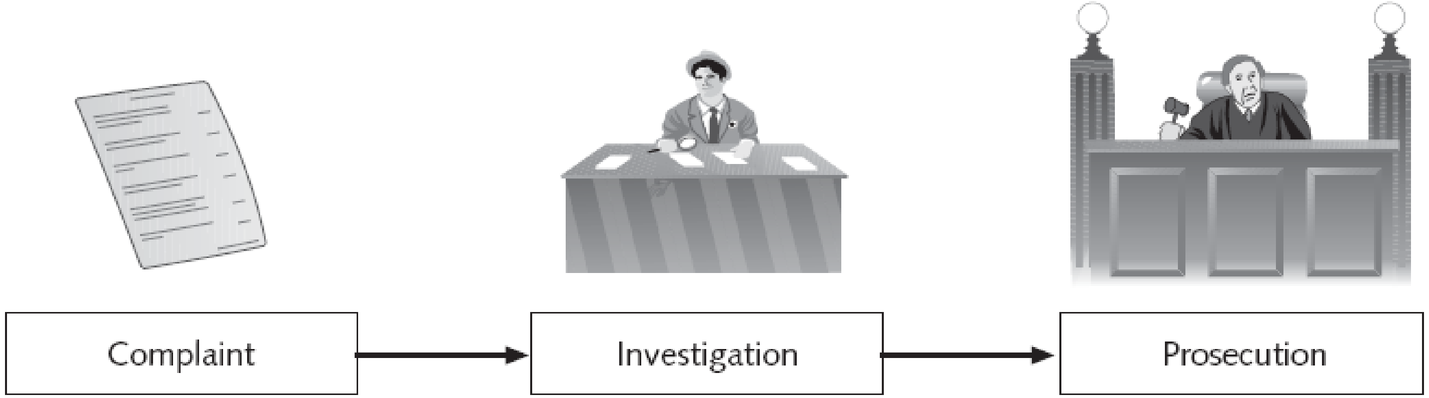
LAW ENFORCEMENT AGENCY INVESTIGATIONS

UNDERSTANDING LAW ENFORCEMENT AGENCY INVESTIGATIONS (1/4)

- In a **criminal case**, a suspect is tried for a criminal offense
  - Such as burglary, murder, molestation or fraud
  - Digital Involvement/Questions
- Computers and networks are sometimes only tools that can be used to commit crimes
  - Not different then lockpick in a burglar case
  - Many states have added specific language to criminal codes to define crimes involving computers, such as theft of computer data
- Following the legal process

FOLLOWING LEGAL PROCESS (1/3)

- Legal processes depend on local custom, legislative standards, and rules of evidence
- Criminal case follows three stages
    - The complaint, the investigation, and the prosecution



Complaint

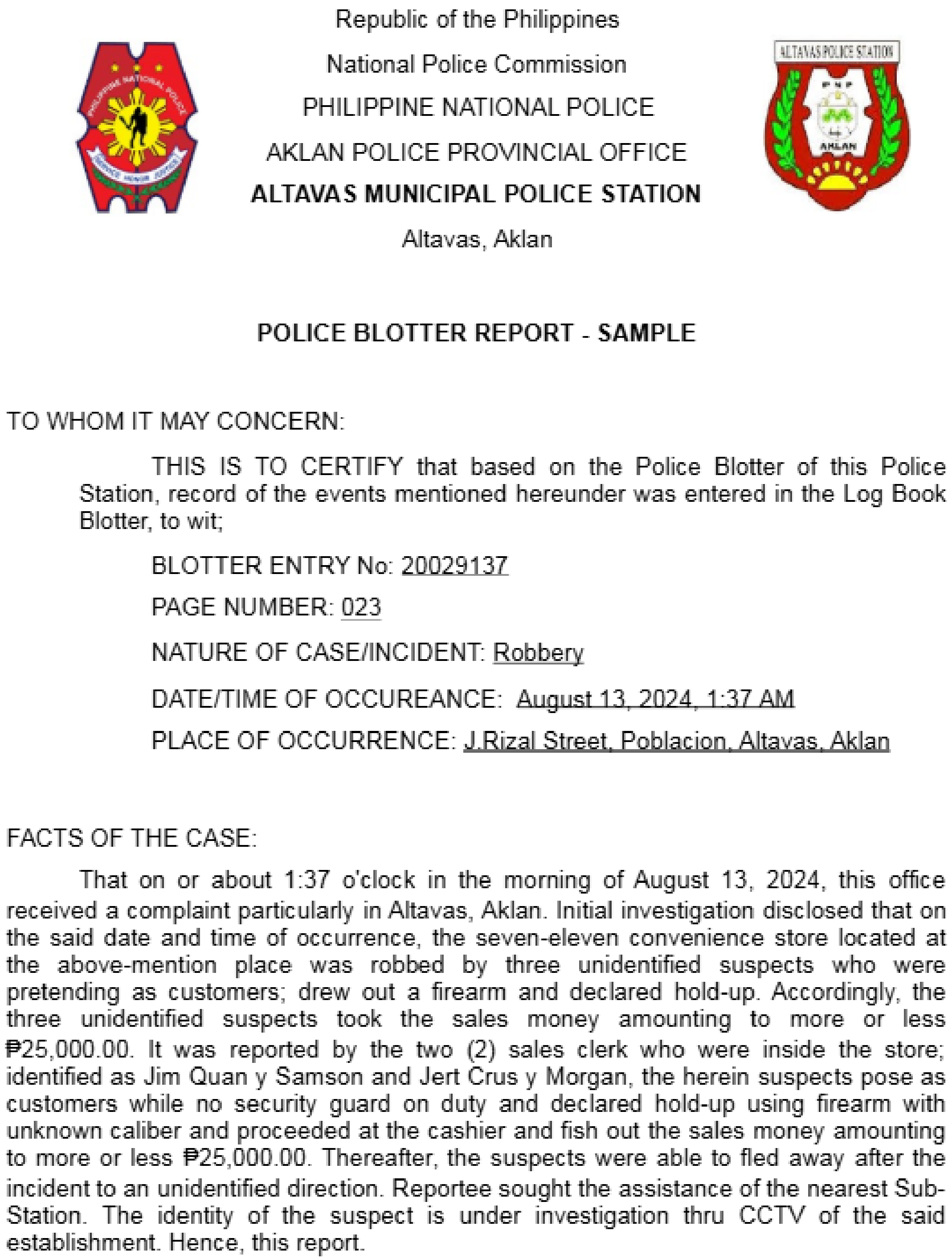
Investigation

Prosecution

Figure 1-7 The public-sector case flow

FOLLOWING LEGAL PROCESS (2/3)

- A criminal case begins when someone finds evidence of an illegal act
- Complainant makes an **allegation**, an accusation or supposition of fact
- A police officer interviews the complainant and writes a report about the crime
    - **Police blotter** provides a record of clues to crimes that have been committed previously
- Investigators delegate, collect, and process the information related to the complaint
- After you build a case, the information is turned over to the prosecutor
- In a criminal case, if you have enough info to support a search warrant, the attorney might ask you to submit an affidavit



Republic of the Philippines

National Police Commission

PHILIPPINE NATIONAL POLICE

AKLAN POLICE PROVINCIAL OFFICE

ALTAVAS MUNICIPAL POLICE STATION

Altavas, Aklan

POLICE BLOTTER REPORT - SAMPLE

TO WHOM IT MAY CONCERN:

THIS IS TO CERTIFY that based on the Police Blotter of this Police Station, record of the events mentioned hereunder was entered in the Log Book Blotter, to wit;

BLOTTER ENTRY No: 20029137

PAGE NUMBER: 023

NATURE OF CASE/INCIDENT: Robbery

DATE/TIME OF OCCUREANCE: August 13, 2024, 1:37 AM

PLACE OF OCCURRENCE: J.Rizal Street, Poblacion, Altavas, Aklan

FACTS OF THE CASE:

That on or about 1:37 o'clock in the morning of August 13, 2024, this office received a complaint particularly in Altavas, Aklan. Initial investigation disclosed that on the said date and time of occurrence, the seven-eleven convenience store located at the above-mention place was robbed by three unidentified suspects who were pretending as customers; drew out a firearm and declared hold-up. Accordingly, the three unidentified suspects took the sales money amounting to more or less ₱25,000.00. It was reported by the two (2) sales clerk who were inside the store; identified as Jim Quan y Samson and Jert Crus y Morgan, the herein suspects pose as customers while no security guard on duty and declared hold-up using firearm with unknown caliber and proceeded at the cashier and fish out the sales money amounting to more or less ₱25,000.00. Thereafter, the suspects were able to fled away after the incident to an unidentified direction. Reportee sought the assistance of the nearest Sub-Station. The identity of the suspect is under investigation thru CCTV of the said establishment. Hence, this report.

FOLLOWING LEGAL PROCESS (3/3)

- **Affidavit**
  - Sworn statement of support of facts about or evidence of a crime
    - Submitted to a judge to request a search warrant
  - Have the affidavit **notarized** under sworn oath

- Judge must approve and sign a search warrant
  - Before you can use it to collect evidence

Rupees 50

SURETY BOND FOR EX. PAKISTAN LEAVE EDUCATION DEPARTMENT

Memorandum of Agreement between W/o, D/o/ S/o Teacher, Govt. High School Tehsil District and the Governor of the Punjab made this ______

Whereas W/o, Teacher, Govt. High School Tehsil District (hereinafter referred to as Employer which expression shall include his/her successors and legal representatives of the First Part) as a result of sanctioning leave by the Governor of the Punjab (hereinafter referred to as the Governor, which expression shall include his successors in office) of the other Part.

NOW, THEREFORE, IN CONSIDERATION FOR THE SAID SANCTION OF LEAVE THE EMPLOYEE AGREES AND UNDERTAKES AS FOLLOWS:-

1. He/ She shall faithfully conform to and abide by the instructions issued with regard to his leave during the period of his/her leave.
2. He/ She will confine his/her leave for the (Umrah) purpose it has been taken/sanctioned and shall not change it without the prior permission of the Governor.
3. Upon the expiry of leave he/she will return to his/her duty in the department.
4. In the event of the breach of any of the aforesaid terms the employee binds herself firmly to pay an amount a sum of Rs. 50,000/- (Rs. Fifty Thousand Only) to the Governor.

In witnesses whereof he/she produces below two sureties who will be responsible and stand bound by this agreement and guarantees that the employee will perform his promise and in case he fails to do so the sureties will pay to the Governor the said amount in default of payment by the Employee.

AND we the sureties below agree to stand bound by this agreement and guarantee the performance of the promise by the employee and for the payment of the said amount in default.

Signed by the above bounded employee
Full Name and Address

AND the Two Sureties and two witnesses

SURETIES

1.______

2.______

WITNESSES

1.______

2.______

CORPORATE INVESTIGATIONS

UNDERSTANDING PRIVATE SECTOR INVESTIGATIONS

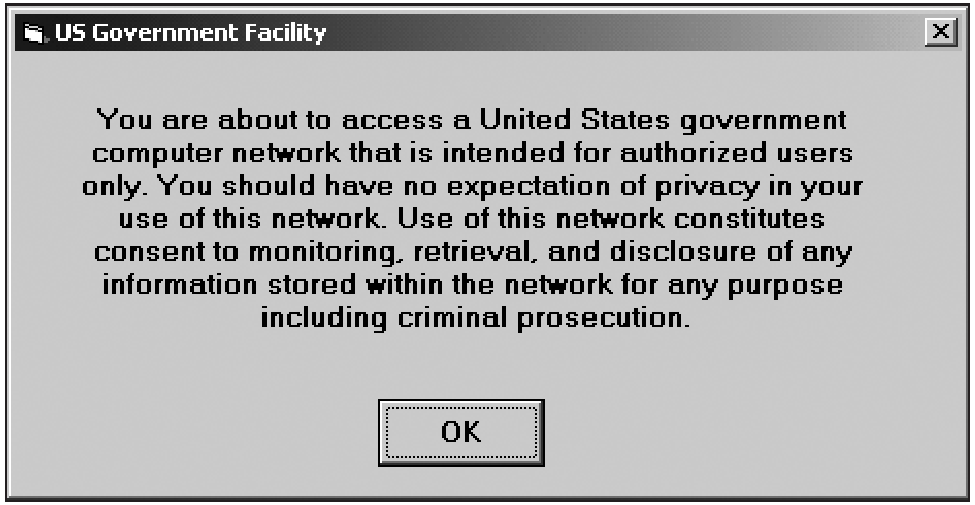
- Private or corporate investigations
  - Involve private companies and lawyers who address company policy violations and litigation disputes

- Corporate computer crimes can involve:
  - E-mail harassment
  - Falsification of data
  - Gender and age discrimination
  - Embezzlement
  - Sabotage
  - **Industrial espionage**

HOW TO REDUCE THE RISK OF LITIGATION ? (1/5)

- Establishing company policies
  - One way to avoid litigation is to publish and maintain policies that employees find easy to read and follow
  - Published company policies provide a **line of authority**
    - For a business to conduct internal investigations
  - Well-defined policies
    - Give computer investigators and forensic examiners the authority to conduct an investigation

HOW TO REDUCE THE RISK OF LITIGATION ? (2/5)



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 1-9 A sample warning banner

- Displaying Warning Banners
  - Another way to avoid litigation
  - **Warning banner**
    - Usually appears when a computer starts or connects to the company intranet, network, or virtual private network
    - Informs end users that the organization reserves the right to inspect computer systems and network traffic at will
    - Establishes the right to conduct an investigation
    - Removes expectation of privacy
  - As a corporate computer investigator
    - Make sure company displays well-defined warning banner

HOW TO REDUCE THE RISK OF LITIGATION ? (3/5)

- Designating an authorized requester
  - Authorized requester has the power to conduct investigations
  - Policy should be defined by executive management
  - Groups that should have direct authority to request computer investigations
  - Corporate Security Investigations
  - Corporate Ethics Office
  - Corporate Equal Employment Opportunity Office
  - Internal Auditing
  - The general counsel or Legal Department

HOW TO REDUCE THE RISK OF LITIGATION ? (4/5)

- Conducting security investigations
  - Types of situations
    - Abuse or misuse of corporate assets
    - E-mail abuse
    - Internet abuse
  - Be sure to distinguish between a company’s abuse problems and potential criminal problems

HOW TO REDUCE THE RISK OF LITIGATION ? (5/5)

- Distinguishing personal and company property
  - Many company policies distinguish between personal and company computer property
  - One area that's difficult to distinguish involves PDAs, cell phones, and personal notebook computers
  - The safe policy is to not allow any personally owned devices to be connected to company-owned resources
    - Limiting the possibility of commingling personal and company data

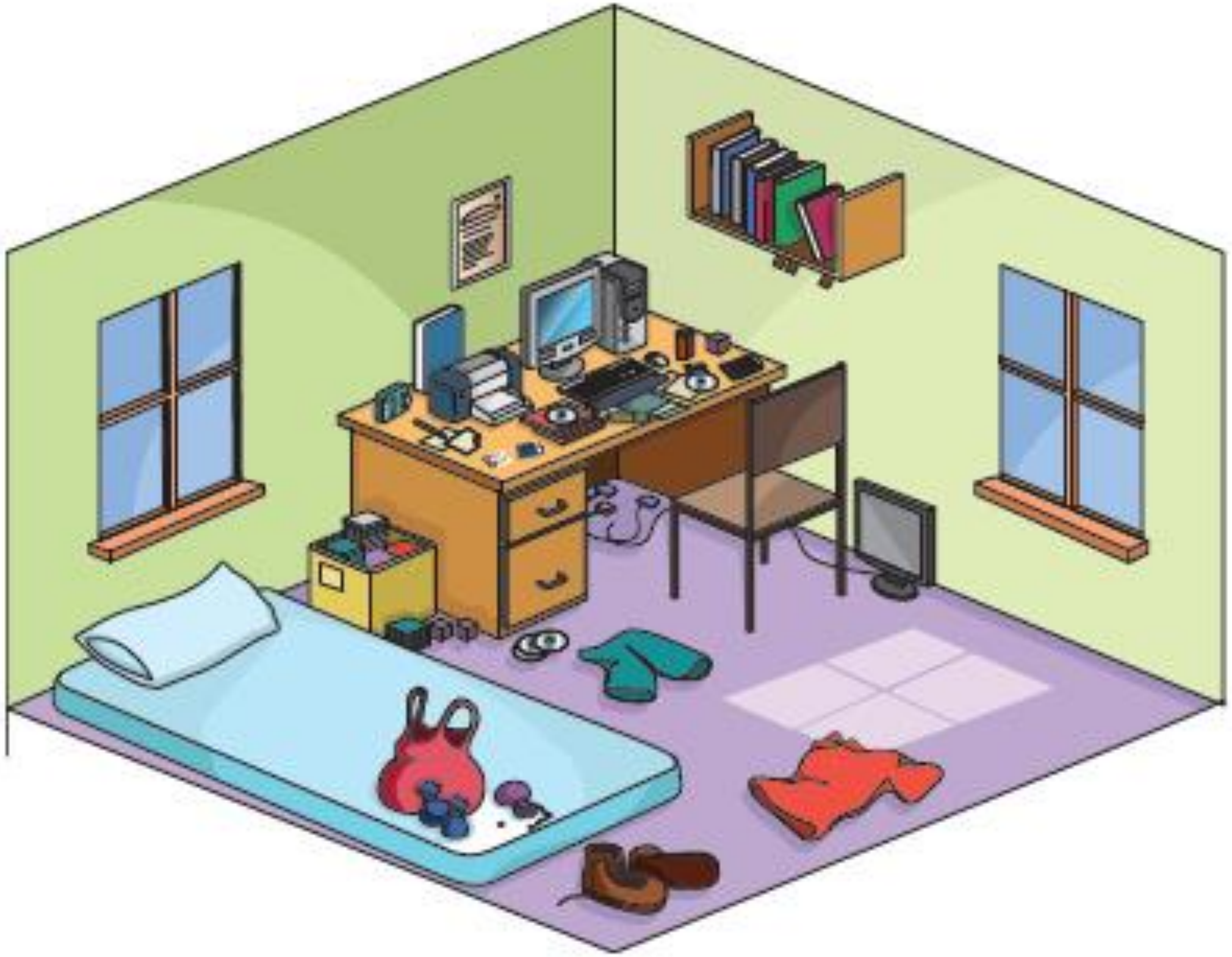


Figure 1-8 The crime scene

PREPARING DIGITAL FORENSIC INVESTIGATION

SYSTEMATIC APPROACH

- When preparing a case,
  - *Make an initial assessment about the type of case you're 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*

EXAMPLE (DIGITAL FORENSICS CASE 1)

Manager Steve Billings has been receiving complaints from customers about the job performance of one of his sales representatives, George Montgomery. George has worked as a representative for several years. He’s been absent from work for two days but hasn’t called in sick or told anyone why he wouldn’t be at work. Another employee, Martha, is also missing and hasn’t informed anyone of the reason for her absence. Steve asks the IT Department to confiscate George’s hard drive and all storage media in his work area. He wants to know whether any information on George’s computer and storage media might offer a clue to his whereabouts and job performance concerns. To help determine George’s and Martha’s whereabouts, you must take a systematic approach to examining and analyzing the data found on George’s desk.

SOLUTION (DIGITAL FORENSICS CASE 1) (1/5)

- **Assessing the case:**
  - Digital investigator talked to George's co-workers
  - Learned that George has been conducting a personal business on the side using company computers
  - Focus of the case has shifted to include possible employee abuse of company resources
  - He can begin assessing this case as follows:
    - Situation—Employee abuse of resources.
    - Nature of the case—Side business conducted on the company computer.
    - Specifics of the case—The employee is reportedly conducting a side business on his company computer that involves registering domain names for clients and setting up their Web sites at local ISPs. Co-workers have complained that he's been spending too much time on his own business and not performing his assigned work duties. Company policy states that all company-owned digital assets are subject to inspection by company management at any time. Employees have no expectation of privacy when operating company computer systems.
    - Type of evidence—Small-capacity USB drive connected to a company computer.
    - Known disk format—NTFS.
    - Location of evidence—One USB drive recovered from the employee's assigned computer.

SOLUTION (DIGITAL FORENSICS CASE 1) (2/5)

Abuse of Company Resources

Looking for evidence

Employee was conducting a side business using office resources

USB drive (from George's computer)

looking for any information related to Web sites, ISPs, or domain names

USB drive uses the NTFS file system

SOLUTION (DIGITAL FORENSICS CASE 1) (3/5)

- Now what does investigator need?

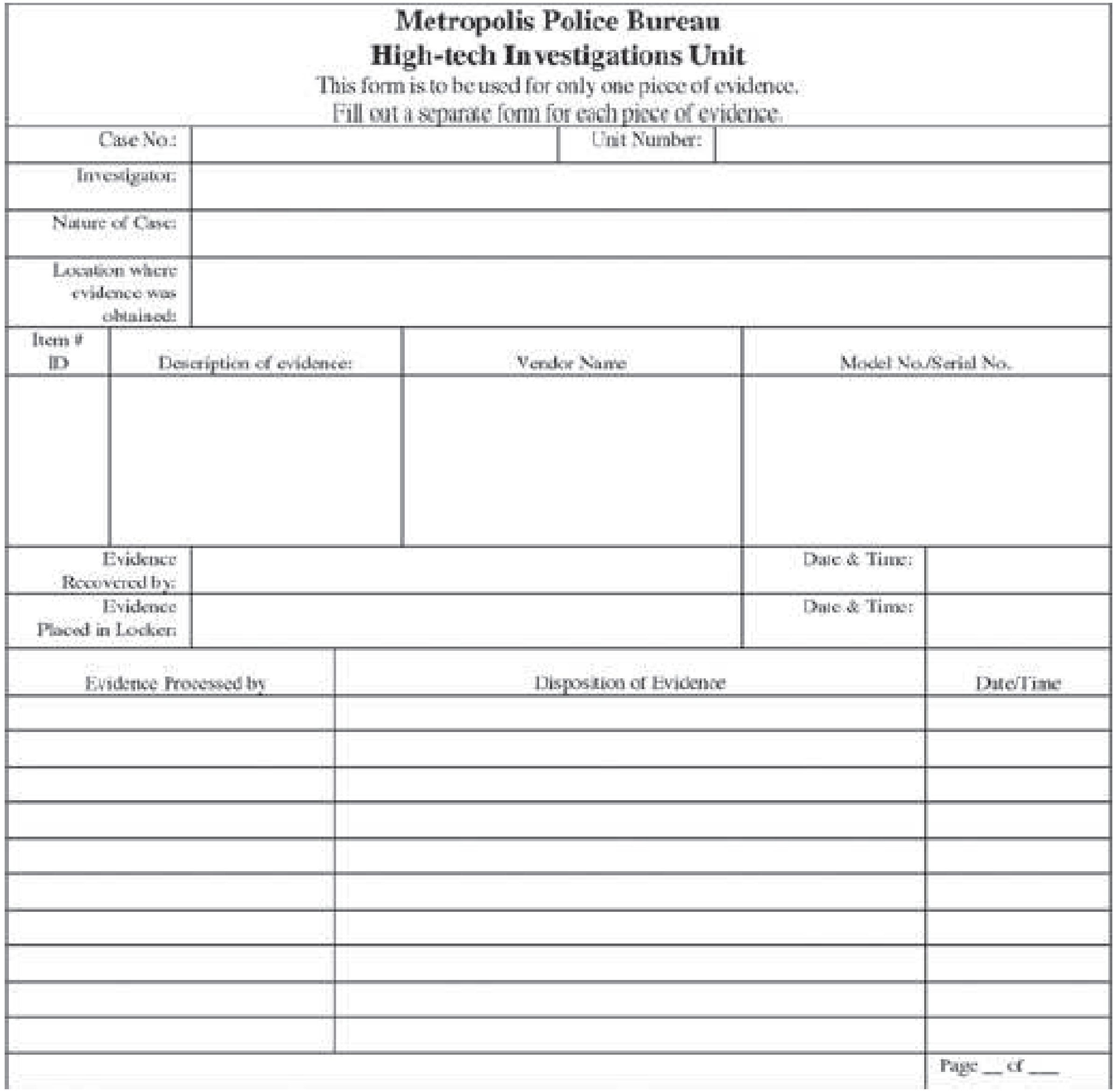
Reliable digital forensic tool for:

- Duplicating USB drive
- Finding deleted and hidden files

SOLUTION (DIGITAL FORENSICS CASE 1) (4/5)

- **Planning your investigation:**
  - Acquire the USB drive from the IT Department, which bagged and tagged the evidence.
  - Complete an evidence form and establish a chain of custody.
  - Transport the evidence to your digital forensics' lab.
  - Place the evidence in an approved secure container.
  - Prepare your forensic workstation.
  - Retrieve the evidence from the secure container.
  - Make a forensic copy of the evidence drive (in this case, the USB drive).
  - Return the evidence drive to the secure container.
  - Process the copied evidence drive with your digital forensics' tools.

- Evidence custody form (chain-of-evidence-form):
  - Single-evidence form
  - Multi-evidence form



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.

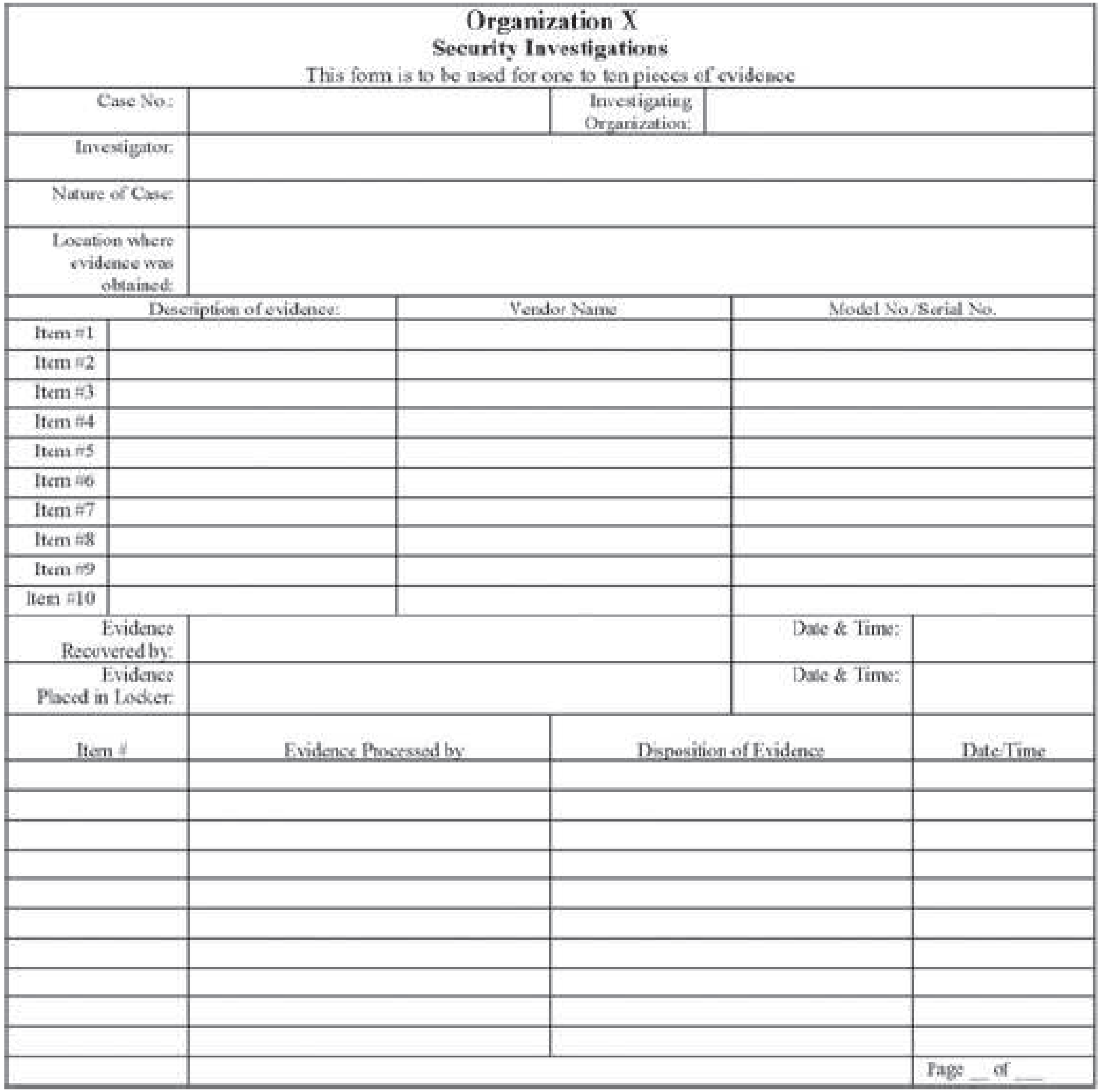
Case No.:		Unit Number:	
Investigator:			
Nature of Case:			
Location where evidence was obtained:			

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



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

SOLUTION (DIGITAL FORENSICS CASE 1) (5/5)

- **Securing your evidence:**
  - You can use large evidence bags, tape, tags, labels, and other products available from police supply vendors or office supply stores
  - Use anti-static bags
  - Place computer evidence in a well-padded container
  - As a standard practice, you should write your initials on the tape before applying it to the evidence
  - If you transport a computer, place new disks in disk drives to reduce possible drive damage while you're moving it

ACTIVITY TIME- 10 MINUTES

Read, Discuss and Be Ready to explain key findings:

- Group A- Employee Termination Cases. Internet Abuse Cases. (Page 32)
- Group B- Email Abuse Investigation (Page 33-34)
- Group C-Attorney Client Privilege Investigation (Page 34-35)
- Group D-Industrial Espionage Investigations (Page 36-37)
- Group E- Interviews and Interrogations in High-Tech Investigations (Page 37-38)

DATA RECOVERY WORKSTATIONS AND SOFTWARE

FORENSIC WORKSTATION (1/2)

- It can use the following operating systems based on the needs:
  - MS-DOS 6.22
  - Windows 95, 98, or Me
  - Windows NT 3.5 or 4.0
  - Windows 2000, XP, Vista, 7, 8, or 10
  - Linux
  - Mac OS X and macOS

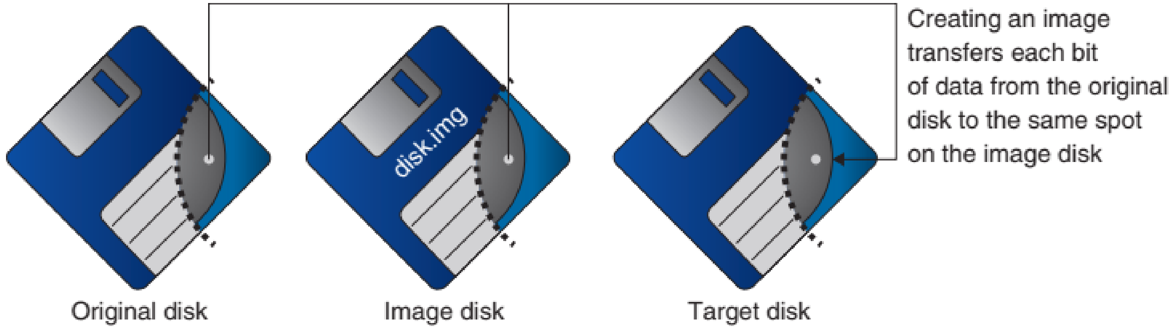
FORENSIC WORKSTATION (2/2)

- Following S/W and H/W is must required:
  - A write-blocker device
  - Digital forensics acquisition tool
  - Digital forensics analysis tool
  - A target drive to receive the source or suspect disk data
  - Spare PATA and SATA ports
  - USB ports
- Additional useful items include the following:
  - Network interface card (NIC)
  - Extra USB ports
  - FireWire 400/800 ports
  - SCSI card
  - Disk editor tool
  - Text editor tool
  - Graphics viewer program
  - Other specialized viewing tools

Wr. Protection
USB
Port 0
ACE LAB
Source

BIT STREAM COPIES

- Bit-by-bit copy (also known as a "forensic copy")
- Process is usually referred to as "acquiring an image" or "making an image"
- A bit-stream image is the file containing the bit-stream copy of all data on a disk or disk partition



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

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

ANALYZING DIGITAL EVIDENCE

- Disk may contain deleted files and fragments
- The files that were deleted are still on the disk until a new file is saved to the same physical location, overwriting the original file
- In the meantime, those files can still be retrieved
- Forensics tools such as Autopsy can retrieve deleted files for use as evidence

https://sourceforge.net/projects/autopsy/files/autopsy/4.3.0/

COMPLETING THE CASE

- At the end of findings, a report needs to be generated
- Basic report writing involves answering the six Ws and one H:
  - **Who, What, When, Where, Why, And How**
- You must also explain computer and network processes
- Some digital forensics tools also generate a log file of all actions taken during your examination and analysis

GUIDE TO COMPUTER FORENSICS AND INVESTIGATIONS

6TH EDITION

CHAPTER 1
UNDERSTANDING THE DIGITAL FORENSICS PROFESSION AND INVESTIGATIONS

READING REFERENCE MATERIAL

FUNDAMENTALS OF DIGITAL FORENSICS

THEORY, METHODS AND REAL-LIFE APPLICATIONS

2ND EDITION

CHAPTER # 1, 2