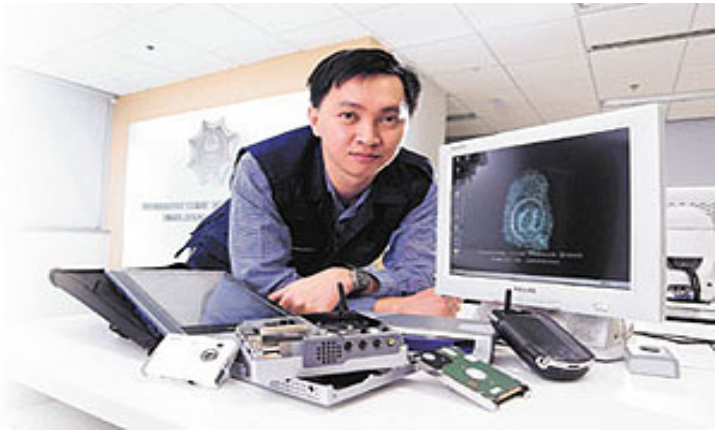
Guide to Computer Forensics and Investigations Fifth Edition

Chapter 1
Intro to Forensics

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

High-tech evidence
Data forensics involves finding, retrieving, analysing and presenting electronic data that may help the police investigate a crime. The data can be retrieved from computers or any other digital device. Files retrieved from his computer (above) with special forensic software were crucial in helping nail Anthony Ler (top).



Note: The teen accomplice of Anthony Ler, now 32 was released on Nov 2nd 2018 after his petition for clemency was granted by President

An Overview of Digital Forensics

- **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.

An Overview of Digital Forensics

- The Federal Rules of Evidence (FRE) was created to ensure consistency in federal proceedings
- FBI Computer Analysis and Response Team (CART) was formed in 1984 to handle cases involving digital evidence
- By late 1990s, CART teamed up with Department of Defense Computer Forensics Laboratory (DCFL)

An Overview of Digital Forensics

- The **Fourth Amendment** to the U.S. Constitution protects everyone's right to be secure from search and seizure. The ultimate goal of this provision is to protect people's right to privacy and freedom from unreasonable intrusions by the government.
  - Separate **search warrants** might not be necessary for digital evidence although "Fourth amendment particularly describe…the things to be seized."
  - Investigator is in position to observe the evidence and its incriminating character is apparent…

Understanding Case Law

- Existing laws can't keep up with the rate of technological change

- When statutes (*a written law passed by a legislative body*) 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

Developing Digital Forensics Resources

- To **supplement** your knowledge:
  - Develop and maintain contact with computing, network, and investigative professionals
  - Join computer user groups in both the public and private sectors
    - Example: **Computer Technology Investigators Network (CTIN)** meets to discuss problems with digital forensics examiners encounter
  - Consult outside experts

Preparing for Digital Investigations

- Digital investigations fall into two categories:
  - Public-sector investigations
  - Private-sector investigations

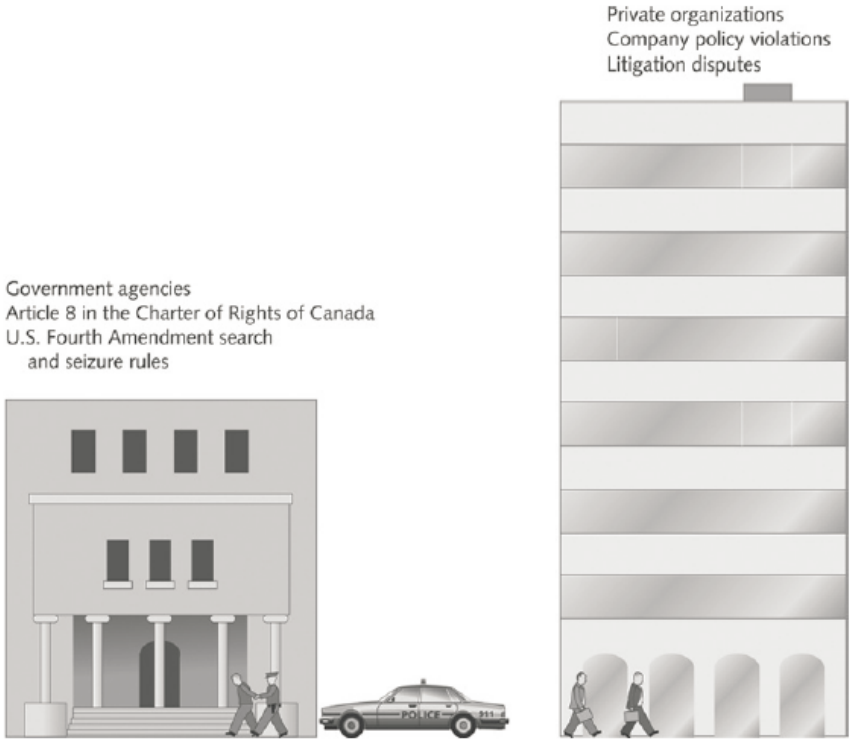


Figure 1-5 Public-sector and private-sector investigations
©Cengage Learning®

Preparing for Digital Investigations

- **Public-sector investigations** involve government agencies responsible for criminal investigations and prosecution

- Be familiar with "Fourth Amendment" to the U.S. Constitution - Restrict government **search and seizure**

- The Department of Justice (DOJ) updates information on computer search and seizure regularly
  - Private-sector investigations focus more on company policy violations

Following Legal Processes

- 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

Following Legal Processes

- **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

Understanding 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

Understanding Private-Sector Investigations

- Businesses can reduce the risk of litigation by publishing and maintaining **policies** that employees find easy to read and follow

- Most important **policies** **define rules for using the company's computers and networks**
  - Known as an "**Acceptable use policy**"

- **Line of authority** - states who has the legal right to initiate an investigation, who can take possession of evidence, and who can have access to evidence

Understanding Private-Sector Investigations

- Business can avoid litigation by displaying a **warning banner** on computer screens
  - Informs end users that the organization reserves the right to inspect computer systems and network traffic at will

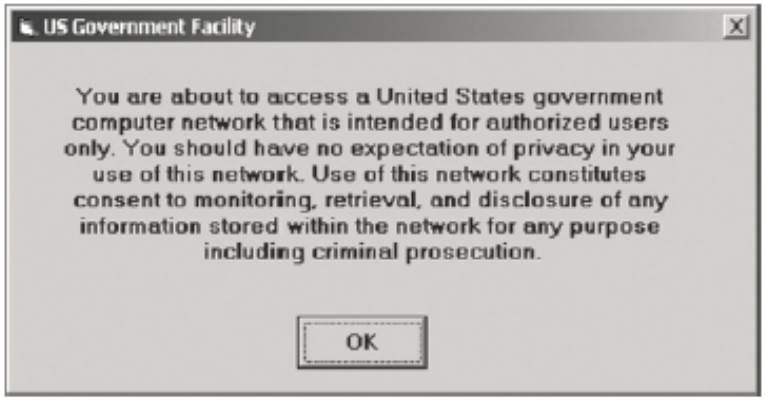


Figure 1-8 A sample warning banner
©Cengage Learning®

Understanding Private-Sector Investigations

- 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**

Understanding Private-Sector Investigations

- 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

Maintaining 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

Preparing a Digital Forensics Investigation

- 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

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

- A potential challenge: information on hard disks might be password protected so forensics tools may be need to be used in your investigation

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

- In general, steps for problem solving include:-
  - 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

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