Digital Forensics

Michael Hegarty

Understanding The Digital Forensics Profession and Investigations

Key Points

- Michael Hegarty (TU-Dublin)
  - Born Dublin, Ireland
- Interests……..
- Questions (no such thing as a silly one)

TU-Dublin Blanchardstown

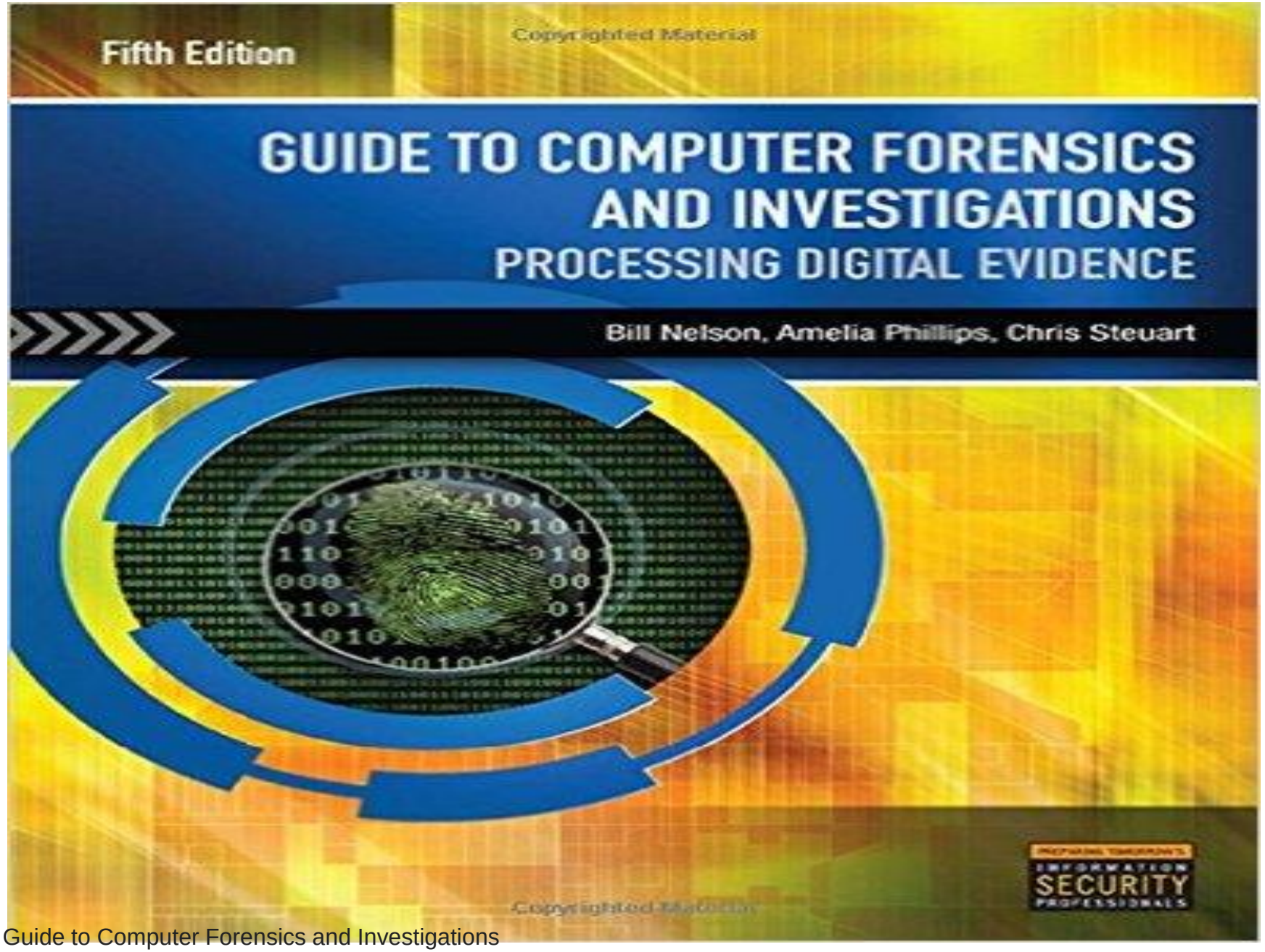
OLLSCOIL TEICNEOLAÍOCHTA BHAILE ÁTHA CLIATH
TU DUBLIN
TECHNOLOGICAL UNIVERSITY DUBLIN
Michael Hegarty

- Bachelor of Science in Computing in Digital Forensics & Cyber Security (TU758)
  - Computer & Network Forensics
  - Mobile Device Forensics
    - Business Communications
    - IT Business Management
- Master of Science in Computing in Applied Cyber Security


tudublincyber
129 Posts
748 Followers
2,111 Following
tudublincyber
Official 📍 TU-Dublin Blanchardstown | Digital Forensics & Cyber Security account.
TUDUBLINCYBER
Instagram


Infinite Possibilities
DUBLIN
BLANCHARDSTOWN
TU-Dublin | Digital Forensics and Cyber Security Graduates
LinkedIn


Michael Hegarty
Lecturer | Information Technology | Digital Forensics | Business
LinkedIn


Fifth Edition
Copyrighted Material
GUIDE TO COMPUTER FORENSICS AND INVESTIGATIONS
PROCESSING DIGITAL EVIDENCE
Bill Nelson, Amelia Phillips, Chris Steuart
INFORMATION SECURITY PROFESSIONALS

Objectives

- Describe the field of digital forensics
- Explain how to prepare computer investigations
- Explain the importance of maintaining professional conduct
- Describe how to prepare a digital forensics investigation by taking a systematic approach

Objectives

- Explain requirements for data recovery workstations and software
- Summarize how to conduct an investigation, including critiquing a case

Global Digital Forensics Market 2022-2030

- Currently estimated to be worth **$5 billion**
- Digital Forensics Market is expected to grow to approx **$23billion** by 2030

- *Cellebrite*
- *AccessData*
- *Guidance Software*
- *FireEye, Inc.*
- *Magnet Forensics*

https://www.globenewswire.com/news-release/2022/04/22/2427044/0/en/Digital-Forensics-Market-to-reach-US-23-62-Bn-by-2030-Comprehensive-Research-Report-by-FMI.html

Defining Digital Forensics

"The application of forensics science techniques to computer-based material"

Oxford English Dictionary

- *legal issues*
- *analysis of digital evidence*
- *search authority*
- *chain of custody*
- *validated tools*
- *repeatability,*
- *reporting and expert presentation*

Defining Computer Forensics

"The application of forensics science techniques to computer based material"

Oxford English Dictionary

The use of science and technology to investigate and establish facts in criminal or civil courts of law.

Computer Forensics is often more of an *art than a science* but as a discipline, it follows clear well defined *methodologies and procedures* however a degree of flexibility is still required when encountering the unusual.

Professional Conduct

- **Professional Conduct** - includes ethics, morals, integrity and standards of behaviour

- ***An investigator must exhibit the highest level of professional behaviour at all times***
  - Maintain objectivity
  - Maintain credibility by maintaining confidentiality

Forensic Process

1. Identify
2. Preserve
3. Acquire
4. Analyse/Discover
5. Document and Present

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 expert presentation.
  - In October 2012, an ISO standard for digital forensics was ratified - ISO 27037 Information technology - Security techniques

Digital Forensics and Other Related Disciplines

- Investigating digital devices includes:
  - Collecting data securely
  - Examining suspect data to determine details such as origin and content
  - Possibly presenting digital information to courts
  - Applying laws to digital device practices

- Digital forensics is different from **data recovery**
  - Which involves retrieving information that was deleted by mistake or lost during a power surge or server crash

Digital Forensics V Cyber Security

- Forensics investigators often work as part of a team, known as the investigation's triad

Figure 1-2 The investigations triad

Understanding Case Law

- Existing laws cannot keep up with the rate of technological change
- Technology moves across borders, laws do not (in most cases) **French** law different to **Irish** law
- 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 (LinkedIn, Twitter)
  - 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
    - **TU-Dublin | Digital Forensics and Cyber Security Graduates** https://www.linkedin.com/groups/8409420/

Preparing for Digital Investigations

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

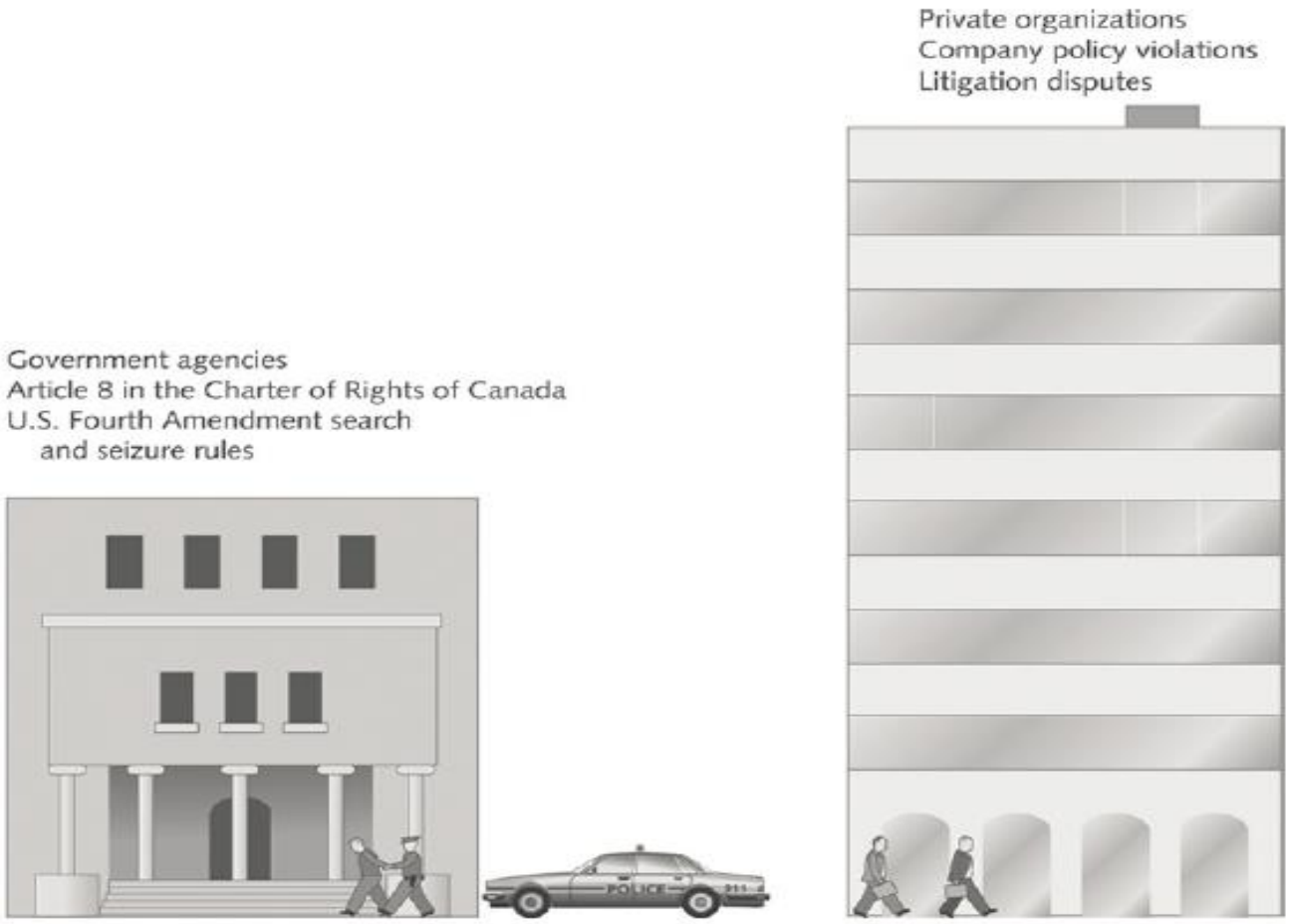


Figure 1-5 Public-sector and private-sector investigations
©Cengage Learning®

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 or HR

- Police/HR/CEO interview the complainant and writes a report about the possible crime

- Report is processed and management decides to start an investigation

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

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

- 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 tablets/iPads*

- 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

Role of Investigator

- The investigator must be impartial and skilled.

- Impartiality
- Neutrality must be maintained, creditability depends on it
- Impartiality in analysis and reporting
- Report evidence of wrong-doing including all the facts
- Role is to deliver the evidence not judge or convict

Preparing a Digital Forensics Investigation

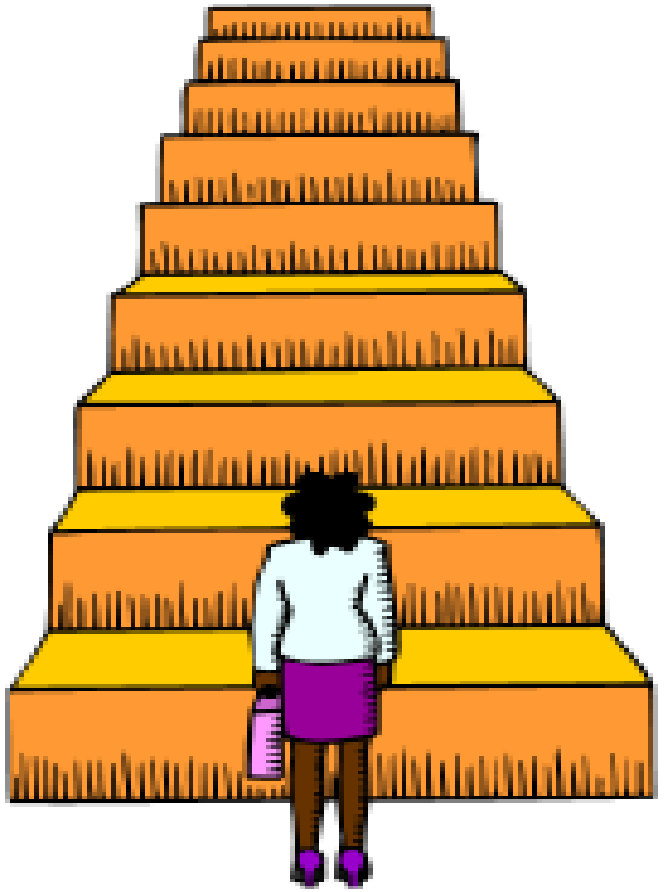
- The role of digital forensics professional is to gather evidence to prove that a suspect did or did not commit a crime or violated a company policy
- Collect evidence that can be offered in court or at a corporate inquiry
  - Investigate the suspect's computer
  - Preserve the evidence on a different 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 determine:
  - Chain of events leading to a crime
  - Evidence that can lead to a conviction

- Digital Forensic Investigators (DFI) should follow proper procedure when acquiring the evidence
  - Digital evidence can be easily altered by an overeager investigator

Steps of a Computer Forensics Methodology



6. Presentation
5. Documentation
4. Discovery
3. Analysis
2. Acquisition
1. Preservation

Document

An Overview of a Company Policy Violation

- Employees misusing resources can cost companies millions of €€€€€€€€'s

- Misuse includes:
  - Using company computers for personal tasks
  - Surfing the Internet
  - Sending personal e-mails

Taking a Systematic Approach

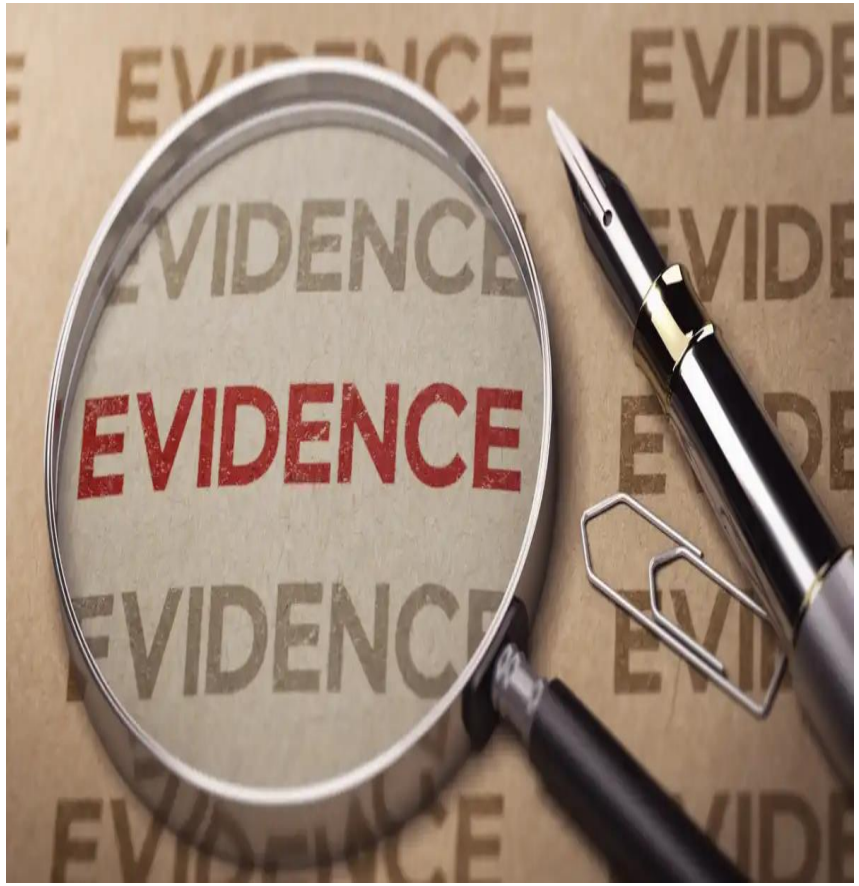
- Steps for problem solving
  - Make an initial assessment about the type of case you are investigating
  - Determine a preliminary design or approach to the case
  - Create a detailed checklist
  - Determine the resources you need
  - Obtain and copy an evidence drive

Planning Your Investigation

- A basic investigation plan should include the following activities:
  - Acquire the evidence (Lab -1 FTK Imager)
  - 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

- A basic investigation plan (cont'd):
  - 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/duplicate evidence with computer forensics tools



E-mail Abuse Investigations

- 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

Industrial Espionage Investigations

- All suspected industrial espionage cases should be treated as criminal investigations
- Staff needed
  - 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

Interviews and Interrogations in High-Tech Investigations

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

Understanding Data Recovery Workstations and Software

- Investigations are conducted in a computer forensics lab (or
  - *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

Conducting an Investigation

- Gather resources identified in investigation plan
- Items needed
  - Original storage media
  - Evidence custody form
  - Evidence container for the storage media
  - Bit-stream imaging tool
  - Forensic workstation to copy and examine your evidence
  - Securable evidence locker, cabinet, or safe

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”, “image file” or “**Forensic Duplicate**”

Understanding Bit-stream Copies

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

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*
- Several vendors provide MS-DOS, Linux, and Windows acquisition tools
  - – Lab 1 in using FTK IMAGER, a tool that creates a Forensic Duplicate

Analyzing Your Digital Evidence

- Your job is to recover (if possible) data from:
  - Deleted files
  - File fragments
  - Complete files

- Deleted files linger on the disk until new data is saved on the same physical location

- Tools can be used to retrieve deleted files
  - FTK Imager
    - https://www.raedts.biz/forensics/forensic-imaging-tools-compared-tested/

Completing the Case

- You need to produce a **final report**
  - State what you did and what you found
- Include forensic tool report to document your work

- **Repeatable findings**
  - Repeat the steps and produce the same result
- If required, use a report template
- Report should show conclusive evidence

Completing the Case

- Keep a written journal of everything you do
  - Your notes can be used in court
- Answer the 5W H:
  - Who, what, when, where, why, and how
- You must also explain computer and network processes

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

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
- Keep track of the chain of custody of your evidence

Summary

- 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
- You should always critique your own work
- THANK YOU!

OLLSCOIL TEICNEOLAÍOCHTA BHAILE ÁTHA CLIATH
DUBLIN
TECHNOLOGICAL UNIVERSITY DUBLIN