

COMP2310 Digital Forensics

Alireza Jolfaei, alireza.jolfaei@mq.edu.au

Department of Computing



MACQUARIE
University

Acknowledgement: Guide to Computer Forensics and Investigations, by Bill Nelson, Amelia Phillips, Christopher Steuart, 6th ed., Cengage Learning, 2019.

Table of Contents

- 1 Administrivia
- 2 Forensics
- 3 History
- 4 Tools
- 5 Laws
- 6 Investigations
- 7 Law Investigation
- 8 Corp. Investigations
- 9 Conduct

Welcome to Country

We would like to acknowledge the traditional custodians of this land, the Wattamatagal Clan of the Dharug Nation, and pay our respects to Elders past, present and future.

Welcome to Country

Welcome

■ Staff

- Convenor Dr. Alireza Jolfaei, alireza.jolfaei@mq.edu.au
- Lecturer 1 Dr. Alireza Jolfaei, alireza.jolfaei@mq.edu.au
- Lecturer 2 Dr. Muhammad Ikram, muhhammad.ikram@mq.edu.au
- Workshops Mohamad Ali Mehrabi, mohamadali.mehrabi@mq.edu.au
Saad Hashmi, saad.hashmi@mq.edu.au
Maryam Shahpasand, maryam.shahpasand@mq.edu.au

Unit Guide - Lectures and Readings

Unit Guide

https://unitguides.mq.edu.au/unit_offerings/123670/unit_guide

You should have a careful read as it contains useful information about how the unit is going to run

Lectures

Recordings of lectures (Echo360) will be provided via iLearn

Textbooks/Readings

- Guide to Computer Forensics and Investigations, by Bill Nelson, Amelia Phillips, Christopher Steuart, 6th edition, Cengage Learning, 2019.
- Digital Forensics and Investigations People, Process, and Technologies to Defend the Enterprise, by Jason Sachowski, 1st edition, 2018.

Unit Outline

- The unit provides a theoretical and practical approach to digital forensics organised around 3 modules
- **Module 1 (Weeks 1 to 4):**
 - Computer Forensics and Investigation Processes
 - Understanding Computing Investigations
 - The Investigator's Office and Laboratory
 - Data Acquisitions
 - Processing Crime and Incident Scenes
- **Module 2 (Weeks 4 to 8):**
 - Working with Windows and DOS Systems
 - Computer Forensics Tools
 - File Systems
 - Recovering Graphics Files
 - Recovering data from memory/hardware
 - Digital Forensics Analysis and Validation

Unit Outline

- **Module 3 (Weeks 9 to 13):**
 - Virtual Machines, Network Forensics, and Live Acquisitions
 - E-mail Investigations
 - Cell Phone and Mobile Device Forensics
 - Report Writing for High-Tech Investigations
 - Expert Testimony in High-Tech Investigations
 - Ethics and High-Tech Investigations

Staff

- Alireza will teach the first module (Weeks 1 to 4)
- Ikram will teach the second module (Weeks 5 to 8)
- Alireza and Ikram will share the third module
- Alireza is in charge of the first assignment
- Ikram is in charge of the second assignment
- Ali, Saad, and Maryam will run all the workshops

Unit Guide - Bring Your Own Device

- COMP2310 is a *Bring Your Own Device (BYOD)* unit.
- You should bring your own laptop to the workshops.
- This is to encourage you to incorporate security practices and tools in your daily work

Unit Guide - Assessment Tasks

- Tutorial Submissions and Quizzes
 - Weekly tasks - 10% of unit total marks
- Assignments
 - Assignment 1 - individual assignment - 15% of total marks
 - Assignment 2 - group assignment, report, and presentation - 15% of total marks
- Examinations
 - Module Exam #1 Week 5 – 20% of total marks
 - Module Exam #2 Week 9 – 20% of total marks
 - Module Exam #3 Week 13 – 20% of total marks
- Hurdles
 - You must attempt at least eight (8) of the weekly tutorial tasks

Unit Guide - Disruption to Studies

Special Consideration

- In case of circumstances that have adversely affected your performance (especially in the final examination):
- Make sure you understand the policy of the Department. See <https://students.mq.edu.au/study/my-study-program/special-consideration>
- In particular, if you are granted special consideration, you may be required to sit a Supplementary Examination.

In that case:

Your performance in the final exam will not be considered.

Your grade will be based on the Supplementary Examination only.

Tutorial Tasks

- During the workshop of Week $n + 1$, there will be a task addressing the material covered in Week n
- The task be in the form of a quiz, or a short written answer
- Tasks will be marked in Week $n + 2$
- It is crucial that you submit work regularly as weekly Submission are a hurdle assessment

Unit Guide - Ethics

Infosec Responsibilities

- Infosec professionals have “unusual” skills and capabilities
- Society (represented by professional bodies) expects us to use these:
 - To protect society, shared infrastructure and public resources
 - To act honestly, honourably, justly, responsibly and legally
 - To protect the interests of clients and principals
 - To advance and protect the profession

Unit Guide - Ethics

Specifically:

- You need to be aware of the University's

- Acceptable Use of IT Resources Policy

`https:`

`//staff.mq.edu.au/work/strategy-planning-and-governance/
university-policies-and-procedures/policies/
acceptable-use-of-it-resources`

- Information Security Policy

`http://www.mq.edu.au/about_us/offices_and_units/information_
technology/policies/information_security_policy/`

- Network Policy (currently under review)

`http://www.mq.edu.au/about_us/offices_and_units/information_
technology/policies/network_policy/`

- Especially, do not:

- Sniff network traffic
 - Attempt to crack other users' credentials

Acceptable Use Policy

- All Authorised Users will be lawful, efficient, economical and ethical in their use of the University's Information Technology Resources. Authorised Users, shall so far as possible:
 - respect the rights of all users;
 - ensure Information Technology Resources and related physical resources are used for purposes authorised by the University;
 - ensure the security and integrity of Information Technology Resources; and
 - ensure Information Technology Resources are used in a way which complies with all relevant laws, subordinate legislation of the University, and contractual obligations governing the use of Information Technology Resources.

Introduction

Computer Forensics and Investigation Processes

Objectives

- Describe the field of digital forensics
- Explain how to prepare for 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

Understanding Computer Forensics

■ Computer forensics

- Involves obtaining and analyzing digital information
 - As evidence in civil, criminal, or administrative cases

Understanding Computer Forensics

- **Computer forensics**

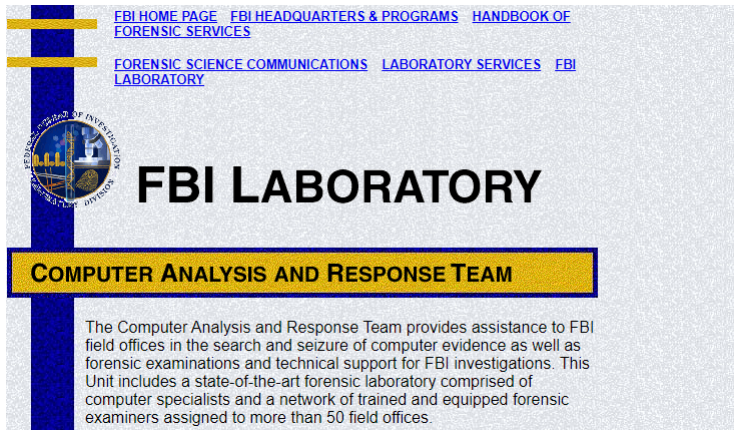
- Involves obtaining and analyzing digital information
 - As evidence in civil, criminal, or administrative cases

- **FBI Computer Analysis and Response Team (CART)**

- Formed in 1984 to handle the increasing number of cases involving digital evidence

FBI CART Website

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



The screenshot shows the FBI Laboratory website. At the top, there are navigation links: [FBI HOME PAGE](#), [FBI HEADQUARTERS & PROGRAMS](#), [HANDBOOK OF FORENSIC SERVICES](#), [FORENSIC SCIENCE COMMUNICATIONS](#), [LABORATORY SERVICES](#), and [FBI LABORATORY](#). On the left, there is a vertical blue bar with a yellow stripe and the FBI Laboratory seal. The seal features a scale of justice, a microscope, and the text "FEDERAL BUREAU OF INVESTIGATION" and "LABORATORY DIVISION". The main heading is "FBI LABORATORY" in large, bold, black letters. Below this, a yellow banner with a black border contains the text "COMPUTER ANALYSIS AND RESPONSE TEAM". At the bottom, a paragraph states: "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."

Understanding Computer Forensics

- **Fourth Amendment** to the U.S. Constitution
 - Protects everyone's rights to be secure in their person, residence, and property
 - From search and seizure
- **Search warrants** are needed

Computer Forensics Versus Other Related Disciplines

■ Computer forensics

- Investigates data that can be retrieved from a computers hard disk or other storage media

■ Network forensics

- Yields information about how a perpetrator or an attacker gained access to a network

■ Data recovery

- Recovering information that was deleted by mistake
 - Or lost during a power surge or server crash
- Typically you know what you are looking for

Computer Forensics Versus Other Related Disciplines

■ Digital forensics

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

■ Disaster recovery

- Uses computer forensics techniques to retrieve information their clients have lost
- Investigators often work as a team to make computers and networks secure in an organization

Computer Forensics Versus Other Related Disciplines

Figure 1-1.



The investigations triad

Computer Forensics Versus Other Related Disciplines

■ Enterprise network environment

- Large corporate computing systems that might include disparate or formerly independent systems

■ Vulnerability assessment and risk management group

- Tests and verifies the integrity of standalone workstations and network servers
- Professionals in this group have skills in **network intrusion detection and incident response**

■ Litigation

- Legal process of proving guilt or innocence in court

■ Computer investigations group

- Manages investigations and conducts forensic analysis of systems suspected of containing evidence related to an incident or a crime

History

A Brief History of Digital Forensics



A History of Digital Forensics

- By the 1970s, electronic crimes were increasing, especially in the financial sector
 - Most law enforcement officers did not 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

A History of Digital Forensics

- 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

A History of Digital Forensics

Figure 1-2.



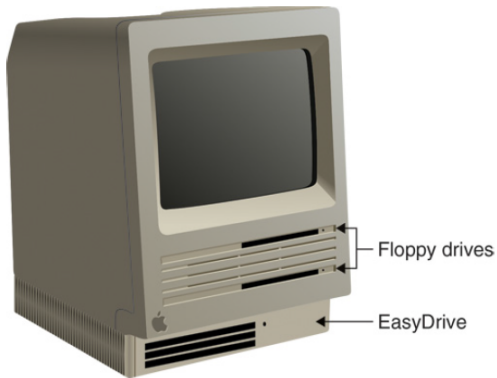
iStock.com/Maxiphoto

© iStock.com/Maxiphoto

An 8088 computer

A History of Digital Forensics

Figure 1-3.



A Mac SE with an external EasyDrive hard disk

A History of Digital Forensics

- 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
 - Recovers deleted files and fragments of deleted files
- Large hard disks posed problems for investigators
- Now
 - iLook
 - Maintained by the IRS, limited to law enforcement
 - EnCase
 - Available for public or private use
 - AccessData Forensic Toolkit (FTK)
 - Available for public or private use

Computer Forensics Tools

Computer Forensics Tools



Most Important Commercial Forensic Software Today

- EnCase



- FTK



- Free demo version (we will use it in this unit)

Open Source Forensic Tools

- Linux-based
 - Knoppix Live CDs
 - Helix
 - Ubuntu
 - Backtrack
- Not commonly used as the main tool, but for special purposes

Laws & Resources

Laws and Resources

Understanding Case Law

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

Developing Computer Forensics Resources

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

Developing Computer Forensics Resources

- **High Technology Crime Investigation Association (HTCIA)**

- Exchanges information about techniques related to computer investigations and security
- User groups can be helpful
- Build a network of computer forensics experts and other professionals
 - And keep in touch through e-mail
- Outside experts can provide detailed information you need to retrieve digital evidence

Public & Private Investigations

Public and Private Investigations



Preparing for Computer Investigations

- Computer investigations and forensics falls into two distinct categories
 - Public investigations
 - Private or corporate investigations
- Public investigations
 - Involve government agencies responsible for criminal investigations and prosecution
 - Organizations must observe legal guidelines
- Law of **search and seizure**
 - Protects rights of all people, including suspects

Preparing for Computer Investigations

Figure 1-4.

Government agencies

Article 8 in the Charter of Rights of Canada

U.S. Fourth Amendment search
and seizure rules



iStock.com/RobinsonBecquart, iStock.com/buzbuzzer

Private organizations

Company policy violations
Litigation disputes



iStock.com/RobinsonBecquart, iStock.com/buzbuzzer

Public-sector and private-sector investigations

Preparing for Computer Investigations

Figure 1-5.

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

The Fourth Amendment

Preparing for Computer Investigations

- 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

Law Enforcement Agency Investigations



Understanding Law Enforcement Agency Investigations

- In a **criminal case**, a suspect is tried for a criminal offense
 - Such as burglary, murder, or molestation
- Computers and networks are sometimes only tools that can be used to commit crimes
 - Many states have added specific language to criminal codes to define crimes involving computers, such as theft of computer data
- Following the legal process
 - Legal processes depend on local custom, legislative standards, and rules of evidence
 - Criminal case follows three stages
 - The complaint, the investigation, and the prosecution

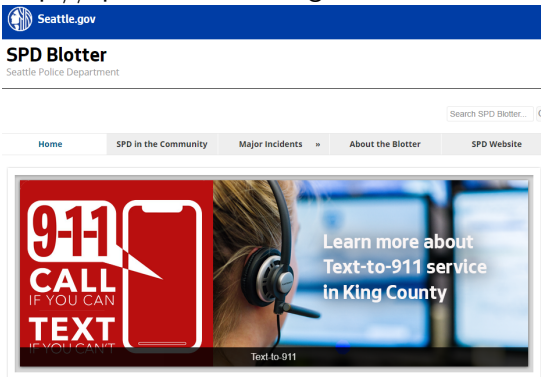


Understanding Law Enforcement Agency Investigations

- Following the legal process (continued)
 - 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

Police Blotter

To see an example of a police blotter, go to <http://spdblotter.seattle.gov>.



Police Seize Narcotics in Investigation at Dearborn Encampment

Written by Public Affairs on January 23, 2020 4:28 pm

Seattle police on Wednesday arrested seven people and seized 19 grams of crack cocaine from a multi-room tent on Dearborn Street, between freeway ramps for Interstate 90 and Interstate 5. Police learned individ[...][Read more »](#)

SPD Channels

 **Facebook**
Like SPD

 **Twitter**
Follow SeattlePD

Categories

- 2019 Homicides (RSS)
- 2020 Homicides (RSS)
- 2018 Homicides (RSS)
- General (RSS)
- Chief of Police (RSS)

Understanding Law Enforcement Agency Investigations

- Following the legal process (continued)
 - After you build a case, the information is turned over to the prosecutor
 - **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

Understanding Law Enforcement Agency Investigations

Figure 1-6.

Date ____

Based on actual inspection of spreadsheets, financial records, and invoices, Joe Smith, a computer forensics expert, is aware that computer equipment was used to generate, store, and print documents used in Jonathon Douglas's tax evasion scheme. There is reason to believe that the computer system currently located on Jonathon Douglas's premises is the same system used to produce and store the spreadsheets, financial records, and invoices, and that both the [spreadsheets, financial records, invoices] and other records relating to Jonathon Douglas's criminal enterprise will be stored on Jonathon Douglas's computer.

Source: *Searching and Seizing Computers and Obtaining Electronic Evidence in Electronic Investigations*, U.S. Department of Justice, July 2002.

Typical affidavit language

Corporate Investigations

Corporate Investigations



Understanding Corporate 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

Understanding Corporate Investigations

■ 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

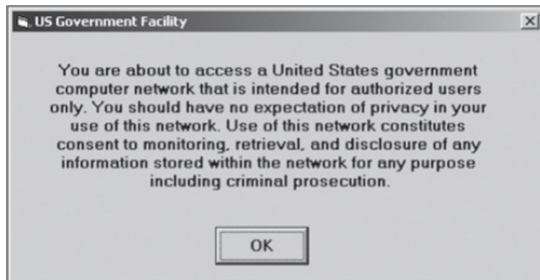
Understanding Corporate Investigations

■ Displaying Warning Banners

- Another way to avoid litigation
- 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

Understanding Corporate Investigations

Figure 1-7.



A sample warning banner

Understanding Corporate Investigations

- **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

Understanding Corporate Investigations

■ Conducting security investigations

■ Types of situations

- Abuse or misuse of corporate assets
- E-mail abuse
- Internet abuse

■ Be sure to distinguish between a companys abuse problems and potential criminal problems

■ Corporations often follow the silver-platter doctrine

- What happens when a civilian or corporate investigative agent delivers evidence to a law enforcement officer

Understanding Corporate Investigations

- **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

Professional Conduct

Professional Conduct

Maintaining Professional Conduct

■ Professional conduct

- Determines your credibility
 - Includes ethics, morals, and standards of behavior
-
- Maintaining objectivity means you must form and sustain unbiased opinions of your cases
 - Maintain an investigations credibility by keeping the case confidential
 - In the corporate environment, confidentiality is critical
 - In rare instances, your corporate case might become a criminal case as serious as murder

Maintaining Professional Conduct

- Enhance your professional conduct by continuing your training
- Record your fact-finding methods in a journal
- Attend workshops, conferences, and vendor courses
- Membership in professional organizations adds to your credentials
- Achieve a high public and private standing and maintain honesty and integrity