INTRODUCTION TO DIGITAL FORENSIC & INVESTIGATION CHAPTER 1

BITS3443

LECTURER

Dr. Siti Rahayu Selamat

Contact info
- B/2-23, SKK, FTMK
- sitirahayu@utem.edu.my
- 012-6249677

2

INSTRUCTIONAL PHILOSOPHY

Would rather discuss than lecture
- Requires student preparation

Hate grading assignments
- Especially LATE assignments

Use class interaction, assignments, quizzes, labs and projects to determine if outcomes are met.

3

BITS 3443 SURVIVAL PRIMER

Read Material BEFORE the class discussion and labs

Check ULearn (E-learning Portal) Often

Use the additional resources identified in syllabus

ASK questions about what you didn't understand in readings

DON'T do assignments and projects at last minute.

REVEIW lectures and notes

Seek HELP if you are having difficulties

OFFER feedback and suggestions to the lecturer in a constructive manner

They only way to learn Forensics is to do investigations
- Expect to be doing a lot of hands-on work in this class
- The hands-on is to develop skills necessary for conducting investigations

4

SPECIAL CONCERN

The course teaches skills and procedures that are intended to be used by law enforcement and security personnel. These same skills and procedures if misapplied or used in improper situations may subject the practitioner to criminal and/or civil penalties. Laws governing these behaviors vary from locality to locality and it is the practitioner's responsibility to be cognizant of local laws pertaining to Computer Forensics and investigative techniques. It is expected that the students in this course use their new found knowledge in legitimate pursuits. Students who do not exhibit the ethical standards required of these professions **will be withdrawn from the course**.

Warning: This lecture will not make you a certified digital forensics technician. This lecture is designed to provide an introduction to this field from both a theoretical and practical perspective. Digital forensics is a maturing scientific field with many sub-disciplines.

5

DEBATE

Is digital forensics a "real" scientific discipline?

- What is digital forensics?
- How do you define a scientific discipline?
- Does it really matter?

6

OBJECTIVES

- Define forensics
- Describe how to prepare for computer investigations and explain the difference between law enforcement agency and corporate investigations
- Explain the importance of maintaining professional conduct

FORENSICS

- Definition of forensics consists of two parts.
  - The first refers to the use of science and technology in investigation
  - The second refers to the requirements of established facts that are presentable in the court of law
- Forensics has three main roles:
  - to facilitate investigations of criminal activities using forensic methodologies, techniques and investigation models
  - to preserve, gather, analyze and provide scientific and technical evidences for the criminal or civil courts of law
  - to prepare proper documentations with relations to the law enforcement.

DEFINITION OF FORENSICS

- Forensic is a field of science dedicated to the methodical gathering and analysis of evidence to establish facts that can be presented in a legal proceeding.
- Forensic is defined as the process of analysis and interpretation of evidence to determine the likelihood of a crime (Michael Y.K. Kwan et al., 2007).
- Gregory and Davis (2005) reported that the connection of forensic discipline with computing appears in two ways: as investigation tools and as evidence
- definition of forensic consists of two parts. The first refers to the use of science and technology in investigation and the second refers to the requirements of established facts that are presentable in the court of law

9

DIGITAL FORENSICS

The Fascinating World of Digital Evidence

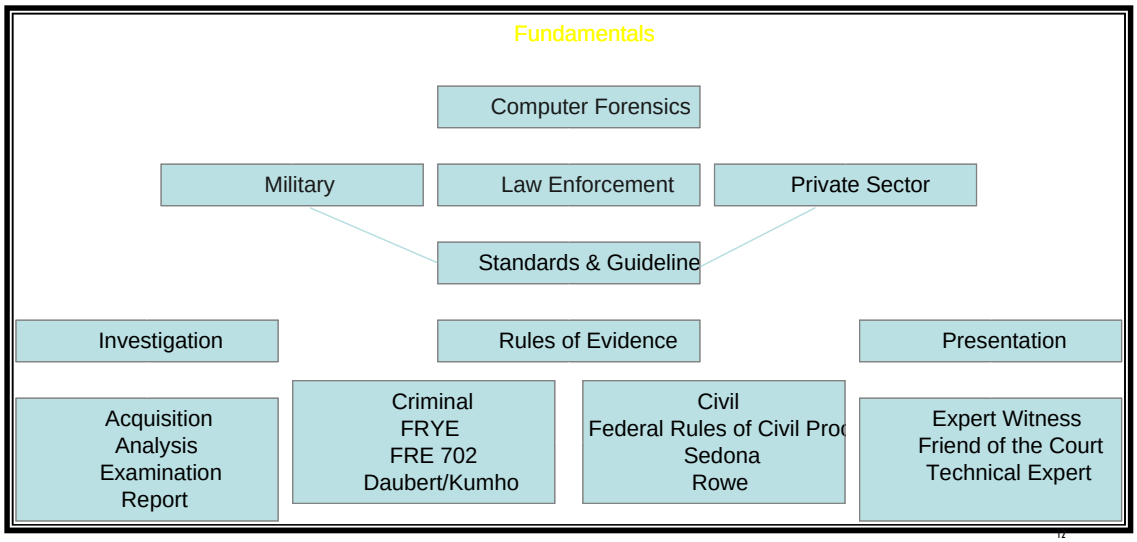
10

DIGITAL FORENSICS

- Digital forensics includes computer forensics, network forensics, software forensics and information forensics (Stephenson, 2003).
- Computer forensics implies a connection between computers, the scientific method, and crime detection.
- Digital forensics is largely used interchangeably with computer forensic.
- It includes devices other than general-purpose computer systems such as network devices, cell phones, and other devices with embedded systems.

11

COMPUTER FORENSICS



12

DIGITAL FORENSIC SCIENCE

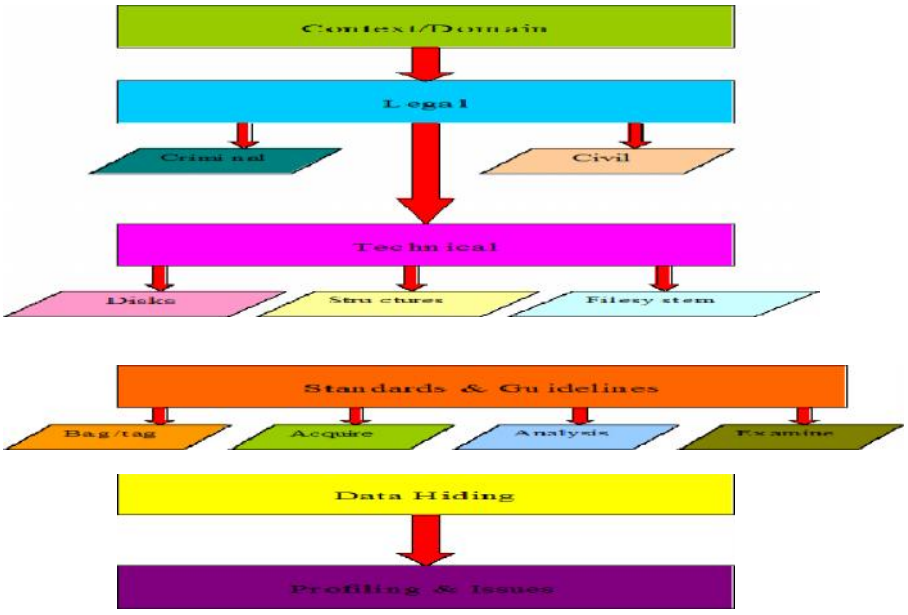
Digital Forensic Science (DFS):

"The **use of scientifically** derived and proven methods toward the **preservation, collection, validation, identification, analysis, interpretation, documentation** and **presentation** of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations."

Source: (2001). Digital Forensic Research Workshop (DFRWS)

13

CONCEPT MAP



14

COMPUTER FORENSICS ACTIVITIES

- Computer forensics activities commonly include:
  - the secure collection of computer data
  - the identification of suspect data
  - the examination of suspect data to determine details such as origin and content
  - the presentation of computer-based information to courts of law
  - the application of a country's laws to computer practice.

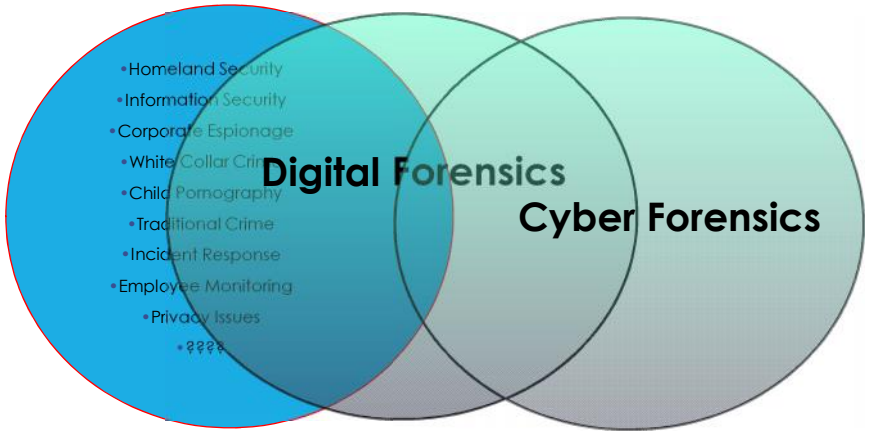
15

THE 3 AS

- The basic methodology consists of the 3 As:
  - ***Acquire*** the evidence without altering or damaging the original
  - ***Authenticate*** the image
  - ***Analyze*** the data without modifying it

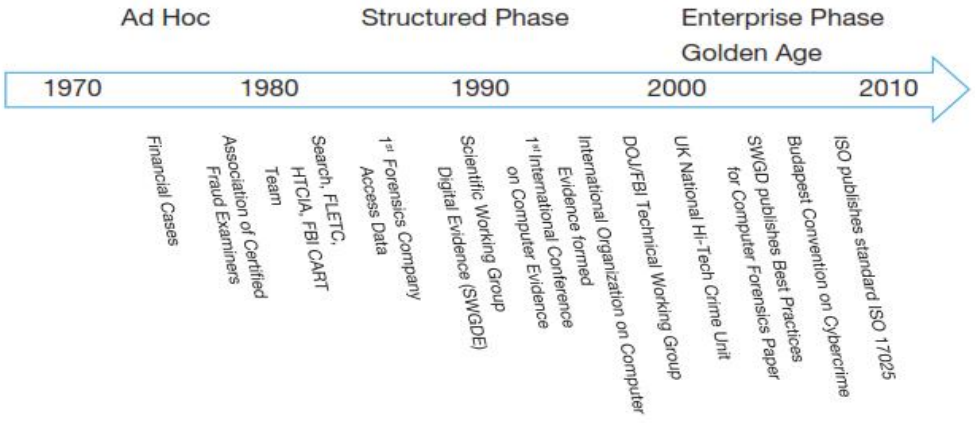
16

CONTEXT OF DIGITAL FORENSICS



17

A BRIEF TIMELINE



(ISACA, 2015)

18

CYBER CRIME REPORTED - STATISTICS

Figure 2: The causes and consequences of cybercrime committed by insiders*

Most adverse consequences	Loss of confidential/proprietary data 11%	Reputational harm 11%	Critical system disruption 8%	Loss of current or future revenue 7%	Loss of customers 6%
Mechanisms used	Social engineering 21%	Laptops 18%	Remote access 17%	E-mail 17%	Copy data to mobile device 16%
Characteristics displayed	Violation of IT security policies 27%	Misuse of organization's resources 19%	Disruptive workplace behavior 10%	Formal reprimands/disciplinary action 8%	Poor performance reviews 7%
Reasons for committing cybercrime	Financial gain 16%	Curiosity 12%	Revenge 10%	Non-financial personal benefit 7%	Excitement 6%

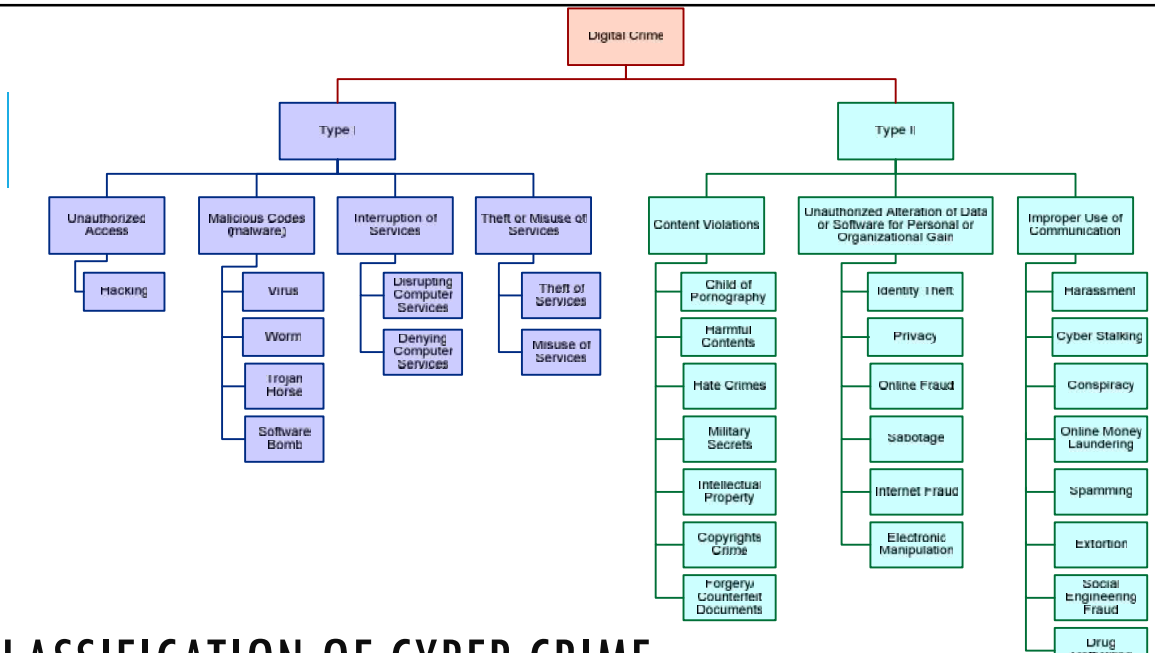
* A current or former employee, service provider, authorized user of internal systems, or contractor

Source: http://www.pwc.com/en_US/us/increasing-it-effectiveness/publications/assets/2014-us-state-of-cybercrime.pdf

"Cybercrime is a clear, present, and permanent danger. While it's a permanent condition, however, the actors, threats, and techniques are very dynamic."

— Tom Ridge, CEO of Ridge Global and first secretary of the US Department of Homeland Security

19



CLASSIFICATION OF CYBER CRIME

20

CRIME SCENES

- Physical Crime Scenes vs. Cyber/Digital Crime Scenes
- Overlapping principals
- The basics of criminalistics are constant across both physical and cyber/digital
- Locard's Principle applies

"When a person commits a crime something is always left at the scene of the crime that was not present when the person arrived"

21

DIGITAL CRIME SCENE

- Digital Evidence
  - Digital data that establish that a crime has been committed, can provide a link between a crime and its victim, or can provide a link between a crime and the perpetrator (Carrier & Spafford, 2003)
- Digital Crime Scene
  - The electronic environment where digital evidence can potentially exist (Rogers, 2005)
  - Primary & Secondary Digital Scene(s) as well

22

FORENSIC PRINCIPLES

- Digital/ Electronic evidence is extremely volatile!
- Once the evidence is contaminated it cannot be de-contaminated!
- The courts acceptance is based on the best evidence principle
  - With computer data, printouts or other output readable by sight, and bit stream copies adhere to this principle.
- Chain of Custody is crucial

23

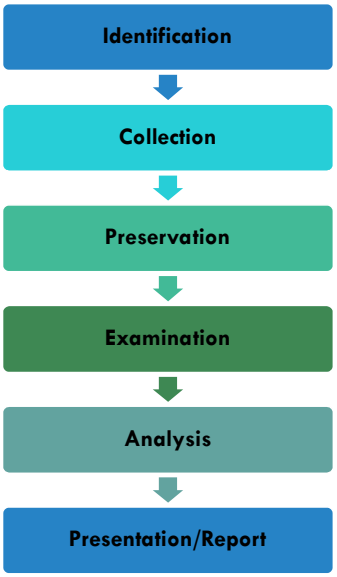
CYBER FORENSIC PRINCIPLES

The 6 Principles are:

1. When dealing with digital evidence, all of the general forensic and procedural principles must be applied.
2. Upon seizing digital evidence, actions taken should not change that evidence.
3. When it is necessary for a person to access original digital evidence, that person should be trained for the purpose.
4. All activity relating to the seizure, access, storage or transfer of digital evidence must be fully documented, preserved and available for review.
5. An Individual is responsible for all actions taken with respect to digital evidence whilst the digital evidence is in their possession.
6. Any agency, which is responsible for seizing, accessing, storing or transferring digital evidence is responsible for compliance with these principles.

24

PROCESS/PHASES



25

IDENTIFICATION

- The first step is identifying evidence and potential containers of evidence
- More difficult than it sounds
  - Small scale devices
  - Non-traditional storage media
  - Multiple possible crime scenes

26

DEVICES IDENTIFICATION











IDENTIFICATION

- Context of the investigation is very important
- Do not operate in a vacuum!
- Do not overlook non-electronic sources of evidence
  - Manuals, papers, printouts, etc.

COLLECTION

Care must be taken to minimize contamination

- Collect or seize the system(s)
- Create forensic image
  - Live or Static?
  - Do you own the system
  - What does your policy say?

29

CRIME SCENE: POTENTIAL EVIDENCE

30

COLLECTION: DOCUMENTATION

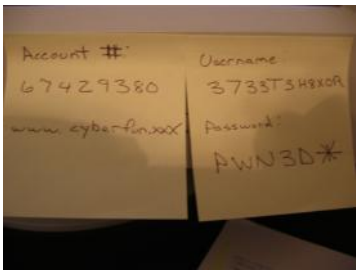



31

COLLECTION: DOCUMENTATION

Take detailed photos and notes of the computer / monitor

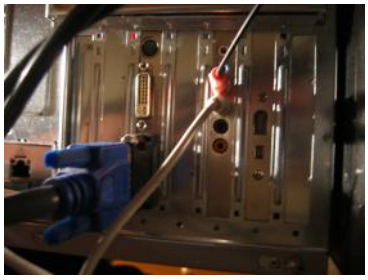
- If the computer is "on", take photos of what is displayed on the monitor – DO NOT ALTER THE SCENE

32

COLLECTION: DOCUMENTATION

- Make sure to take photos and notes of all connections to the computer/other devices



33

COLLECTION: IMAGING

Rule of Thumb: make 2 copies and don't work from the original (if possible)

A file copy does not recover all data areas of the device for examination

Working from a duplicate image

- Preserves the original evidence
- Prevents inadvertent alteration of original evidence during examination
- Allows recreation of the duplicate image if necessary

34

COLLECTION: IMAGING

Digital evidence can be duplicated with no degradation from copy to copy

- This is not the case with most other forms of evidence

35

COLLECTION: IMAGING

- Write blockers
  - Software
  - Hardware
- Hardware write blockers are becoming the industry standard
  - USB, SATA, IDE, SCSI, SIM, Memory Cards
  - Not BIOS dependent
  - But still verify prior to usage!

36

COLLECTION: IMAGING

- Forensic Copies (Bitstream)
  - Bit for Bit copying captures all the data on the copied media including hidden and residual data (e.g., slack space, swap, residue, unused space, deleted files etc.)
- Often the "smoking gun" is found in the residual data.
- Imaging from a disk (drive) to a file is becoming the norm
  - Multiple cases stored on same media
  - No risk of data leakage from underlying media
- Remember avoid working for original
- Use a write blocker even when examining a copy!

37

IMAGING: AUTHENTICITY & INTEGRITY

- How do we demonstrate that the image is a true unaltered copy of the original?
  - Hashing (MD5, SHA 256)
- A mathematical algorithm that produces a unique value (128 Bit, 512 Bit)
  - Can be performed on various types of data (files, partitions, physical drive)
- The value can be used to demonstrate the integrity of your data
  - Changes made to data will result in a different value
  - The same process can be used to demonstrate the image has not changed from time-1 to time-n

38

EXAMINATION

- Higher level look at the file system representation of the data on the media
- Verify integrity of image
  - MD5, SHA1 etc.
- Recover deleted files & folders
- Determine keyword list
  - What are you searching for
- Determine time lines
  - What is the time zone setting of the suspect system
  - What time frame is of importance
  - Graphical representation is very useful

39

EXAMINATION

- Examine directory tree
  - What looks out of place
  - Stego tools installed
  - Evidence Scrubbers
- Perform keyword searches
  - Indexed
  - Slack & unallocated space
- Search for relevant evidence types
  - Hash sets can be useful
  - Graphics
  - Spreadsheets
  - Hacking tools
  - Etc.
- Look for the obvious first
- When is enough enough??

40

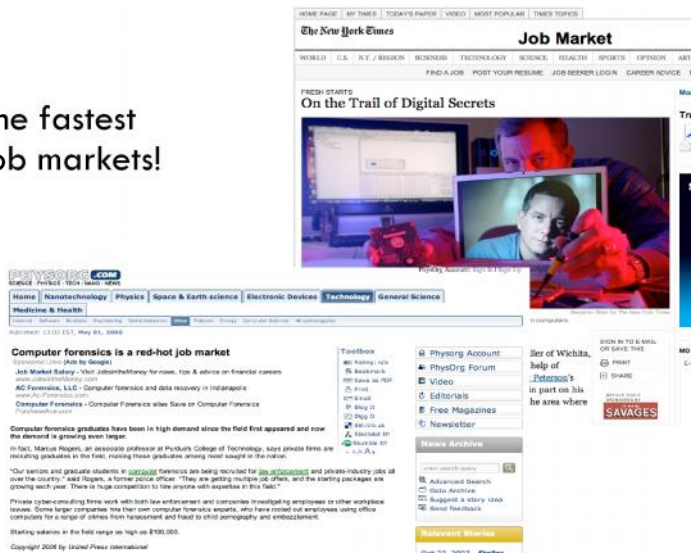
ISSUES

- Lack of certification for tools
- Lack of standards
- Lack of certification for professionals
- Lack of understanding by Judiciary
- Lack of curriculum accreditation
- Rapid changes in technology!
- Immature Scientific Discipline

41

CAREERS

- One of the fastest growing job markets!



42

PATHS TO CAREERS IN CF

- Certifications
- Associate Degree
- Bachelor Degree
- Post Grad Certificate
- Masters
- Doctorate

43

JOB FUNCTIONS

- CF Technician
- CF Investigator
- CF Analyst/Examiner (lab)
- CF Lab Director
- CF Scientist

44

PROFESSIONAL OPPORTUNITIES

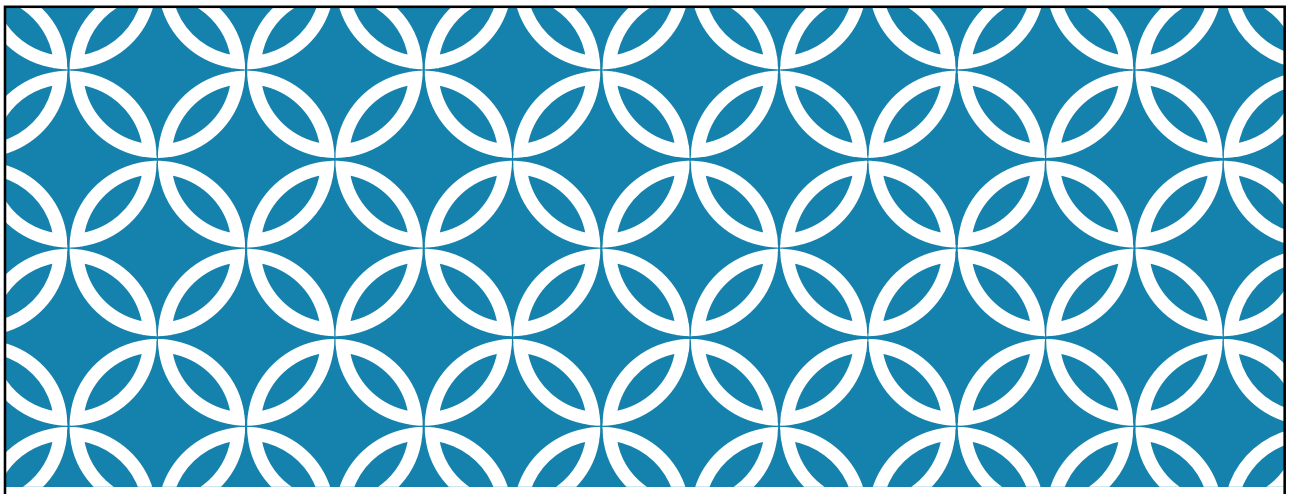
- Law Enforcement
- Private Sector
- Intelligence Community
- Military
- Academia

45

SUMMARY

- Digital/Cyber/Computer Forensics is a maturing forensic Science
- Excellent career opportunities
- Proper education & training is paramount!

46



COMPUTER FORENSICS TOOLS

FORENSIC SOFTWARE

Most Important Commercial Forensic Software Today

- EnCase
- FTK
  - we will use it in this class

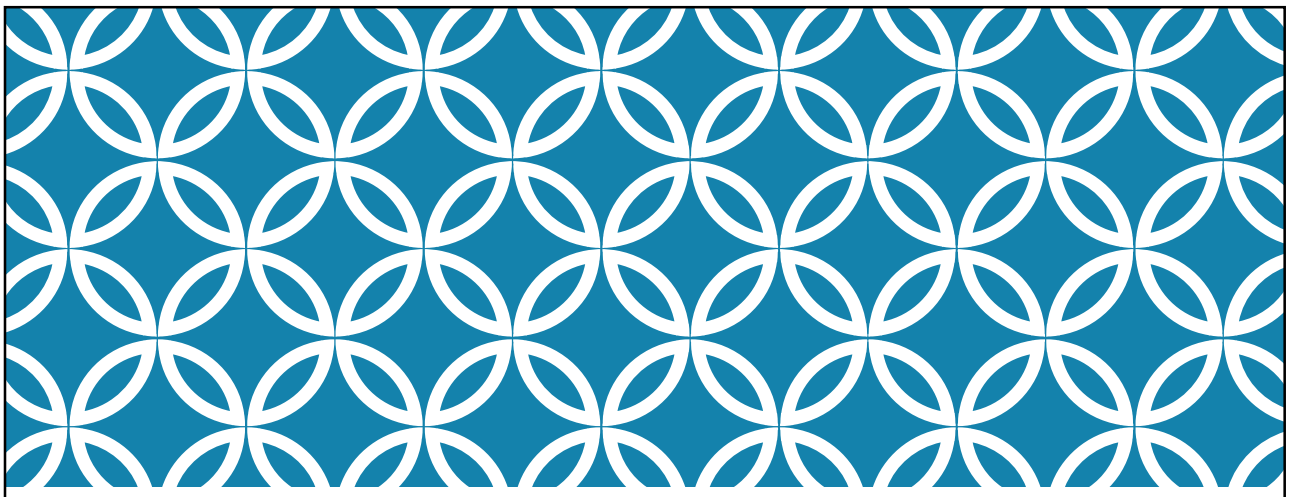
- Open Source Forensic Tools
  - Linux-based
    - Knoppix Live CDs
    - Helix
    - Ubuntu
    - Backtrack
  - Not commonly used as the main tool, but for special purposes

OPEN SOURCE FORENSIC TOOLS

Linux-based

- Knoppix Live CDs
- Helix
- Ubuntu
- Backtrack

Not commonly used as the main tool, but for special purposes



LAWS AND RESOURCES

UNDERSTANDING 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

51

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

52

DEVELOPING COMPUTER FORENSICS RESOURCES (CONTINUED)

High Technology Crime Investigation Association (HTCIA)

- Exchanges information about techniques related to computer investigations and security

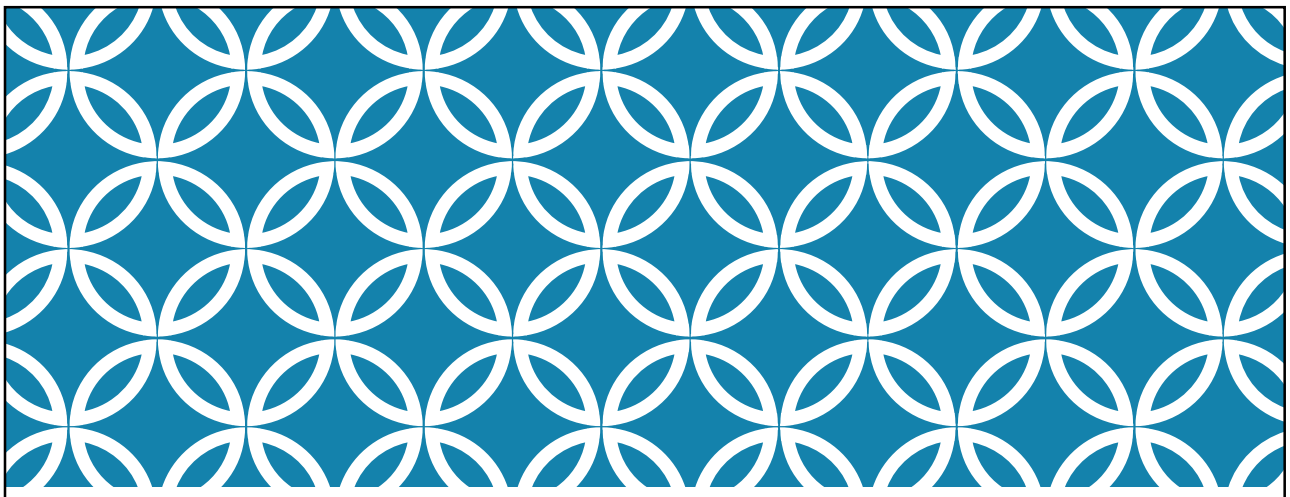
User groups can be helpful

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

53



PUBLIC AND PRIVATE INVESTIGATIONS

54

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

55

PREPARING FOR COMPUTER INVESTIGATIONS (CONTINUED)

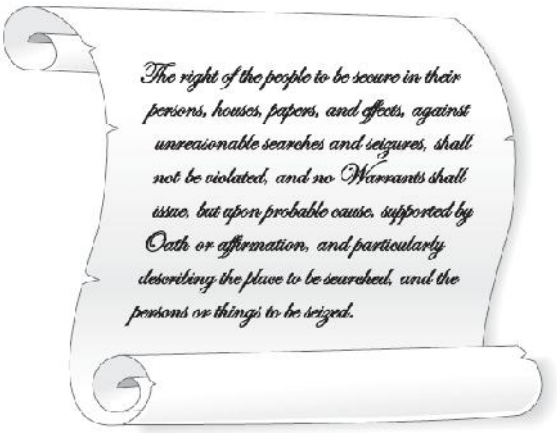


Figure 1-6 The Fourth Amendment

56

PREPARING FOR COMPUTER INVESTIGATIONS (CONTINUED)

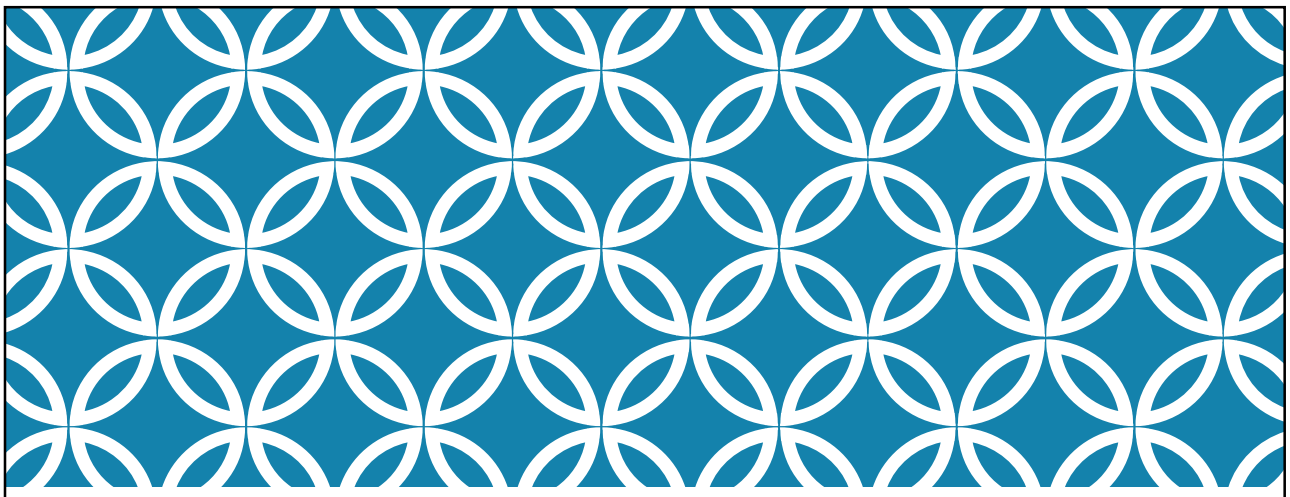
Private or corporate investigations

- 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

57



LAW ENFORCEMENT AGENCY INVESTIGATIONS

58

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

59

UNDERSTANDING LAW ENFORCEMENT AGENCY INVESTIGATIONS (CONTINUED)

Following the legal process (continued)

- Criminal case follows three stages
  - The complaint, the investigation, and the prosecution

Figure 1-7 The public-sector case flow

60

UNDERSTANDING LAW ENFORCEMENT AGENCY INVESTIGATIONS (CONTINUED)

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

61

UNDERSTANDING LAW ENFORCEMENT AGENCY INVESTIGATIONS (CONTINUED)

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

62

UNDERSTANDING LAW ENFORCEMENT AGENCY INVESTIGATIONS (CONTINUED)

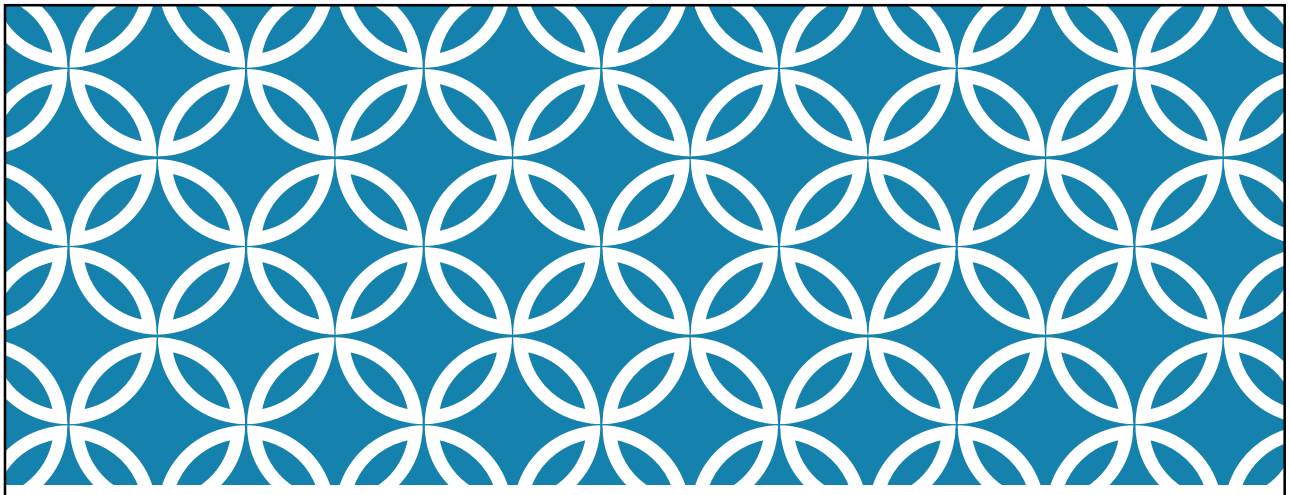
Date ___ ___ ___

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.

Figure 1-8 Typical affidavit language

63



CORPORATE INVESTIGATIONS

64

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**

65

UNDERSTANDING CORPORATE INVESTIGATIONS (CONTINUED)

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

Displaying Warning Banners

- Another way to avoid litigation

66

UNDERSTANDING CORPORATE INVESTIGATIONS (CONTINUED)

Displaying Warning Banners (continued)

- **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

67

UNDERSTANDING CORPORATE INVESTIGATIONS (CONTINUED)

- 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

68

UNDERSTANDING CORPORATE INVESTIGATIONS (CONTINUED)

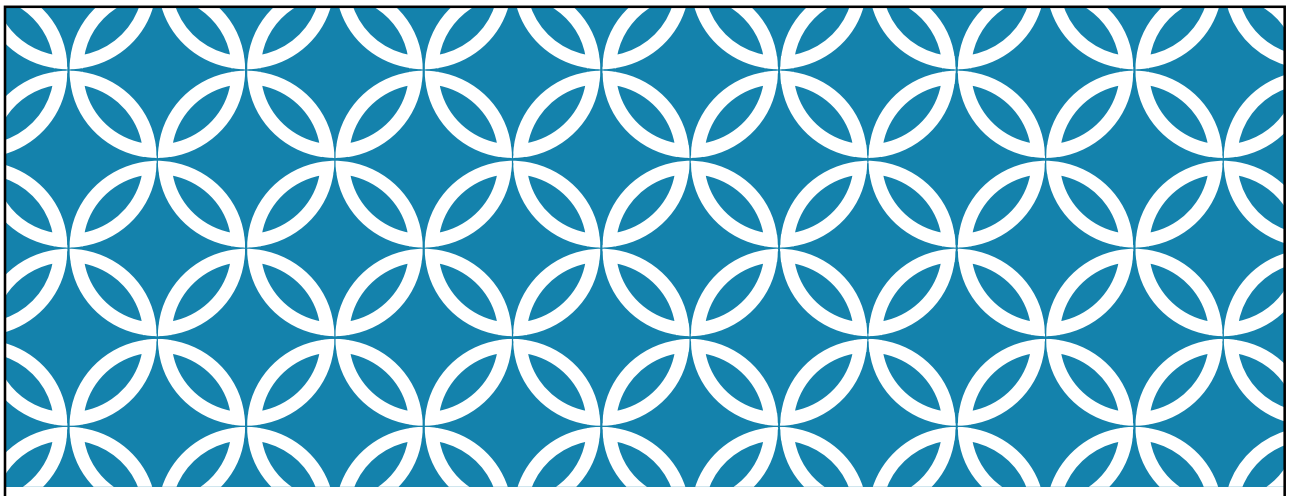
Conducting security investigations

- 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
- 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 (CONTINUED)

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

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 investigation's 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 (CONTINUED)

- 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

DISCUSSION

Describe the three stages of a criminal case.