GenCyber2021
Cybercrimes and digital forensics

Claire S. Lee, Ph.D.

July 13, 2021

(11:00 – 11:45 am)

UMASS LOWELL

About me: Dr. Claire S. Lee

- Assistant Professor, School of Criminology and Justice Studies, University of Massachusetts Lowell

- Research interests
  - Cybercrime, human and social factors of cybersecurity

UMASS LOWELL

Overview of GenCyber curriculum

Module 1 Defense in Depth		Domain Separation
Motivating game:	Phishing email	Layering
Lecture 1 with Hands-on lab:	Firewall	Least Privilege
Lecture 2 with Hands-on Lab:	Intrusion Detection System (IDS)	Process Isolation
Special topic talk and discussion:	Cybercrimes and digital forensics	Minimization
Module 2 Confidentiality		Data Hiding
Motivating game:	Messaging with Caesar Cipher medallion encryption	
Lecture 3 with Hands-on Lab:	Symmetric key cryptography	
Lecture 4 with Hands-on Lab:	Asymmetric key cryptography	
Special topic talk and discussion:	Cybersecurity ethics	
Module 3 Integrity		Simplicity
Motivating game:	Man in the middle attack	
Lecture 5 with Hands-on Lab:	Checksum and hash	
Lecture 5 with Hands-on Lab:	Digital signature	
Special topic talk and discussion:	Cybersecurity professions	
Module 4 Availability		Modularity
Motivating game:	Denial of service (DoS)	
Lecture 5 with Hands-on Lab:	Introduction to Metasploit	
Lecture 6 with Hands-on Lab:	Distributed DoS (DDoS)	
Special topic talk and discussion:	Keep it Simple	
Module 5 Think Like an Adversary		Abstraction
Motivating game:	Planting backdoor	Resource
Lecture 7 with Hands-on Lab:	Ethical hacking with Python programming	Encapsulation
Lecture 8 with Hands-on Lab:	Software security	
Student demo:	Ethical hacking	

UMASS LOWELL

Objectives

- To understand the nature of cybercrime
- To learn about cybercrime victimization and offending
- To get to know about digital forensics

AGENDA

Mode	Topic	Tool/platform
Lecture, discussion	Cybercrime * Definitions of cybercrime * Types of cybercrimes - Discussion of the definitions, types, and severity of cybercrimes	jamboard
Lecture, discussion	Cybercrime investigation * A cybercrime scenario - Hands-on: finding evidence - Discussion of the scenario	jamboard
Lecture, discussion, hands-on	Digital forensics * Definition and process of digital forensics - Digital investigation: Search warrant, process - Digital footprint * Digital forensics tools	jamboard
Summary and take-home message	Cybercrime Cybercrime investigation Digital forensics	jamboard FTK Imager

Vocabulary

- Cybercrime
- Cybercrime investigation
- Digital forensics
- Hackers
- Hacking

Cybercrime

Cybercrime

What comes into your mind when you hear about the term “cybercrime”?

- Hacking, identity fraud, Internet auction fraud, Internet piracy
- Online harassment, Digital child pornography
- Cyberstalking
- Cyberterrorism

UMASS LOWELL

Jamboard: Severity of "Cybercrime"

What is the most severe cybercrime among these?
Please choose one and write your thoughts.

Use your breakout room group number

We will be using this Jamboard link to know each other better.

Click sticky note on left hand side menu & put your name on it to answer my questions.

CC & DF: Jamboard (Breakout room groups: 1-3)

1:
https://jamboard.google.com/d/17yrkyFV9UrmmDI8Kj4CzC-msfy1eBgUQiwD_cVL16yA/edit?usp=sharing

2:
https://jamboard.google.com/d/1eYyGIiB36jCVO5AuYXlhJmJyCpi-KSvWPPIqI9ptzJ0/edit?usp=sharing

3:
https://jamboard.google.com/d/1rX09WGci6NvUuL1hcJWfPizFc2JL-OSPDGgsIaQpkaM/edit?usp=sharing

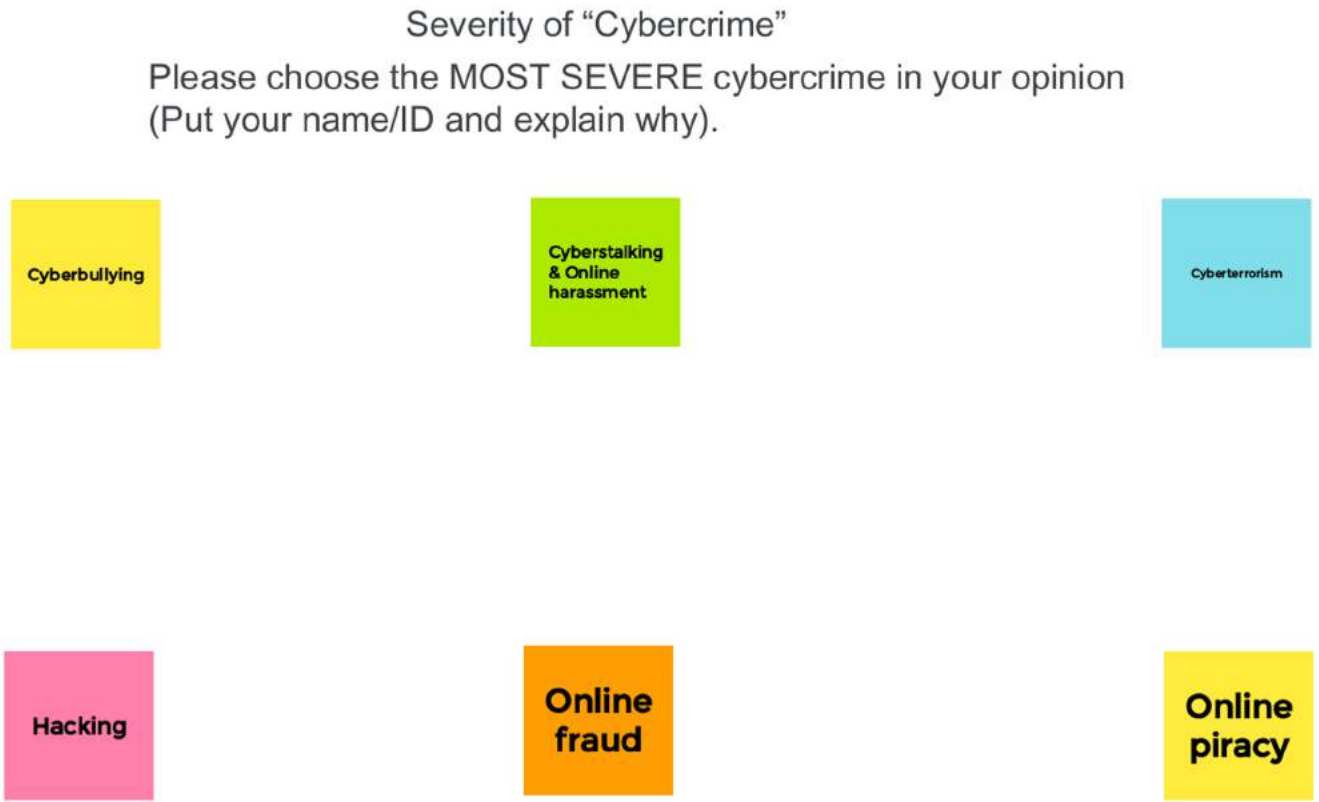
CC & DF: Jamboard (Breakout room groups: 4-6)

4:
https://jamboard.google.com/d/1ljXn21vmnWFgX65bMsSRsgfEAjbzZZyD6XUUFUzLXD8/edit?usp=sharing

5:
https://jamboard.google.com/d/1G3YJncugHVP2uPM2LnEgh5_9Rg9k2iUykEBtG1jL9t8/edit?usp=sharing

6:
https://jamboard.google.com/d/189tFMhjCZAZSRXetZs-HJyXcX6P1Q6zQJnZkVTsjKiA/edit?usp=sharing

Jamboard: Severity of "Cybercrime"



There are types of crimes ...

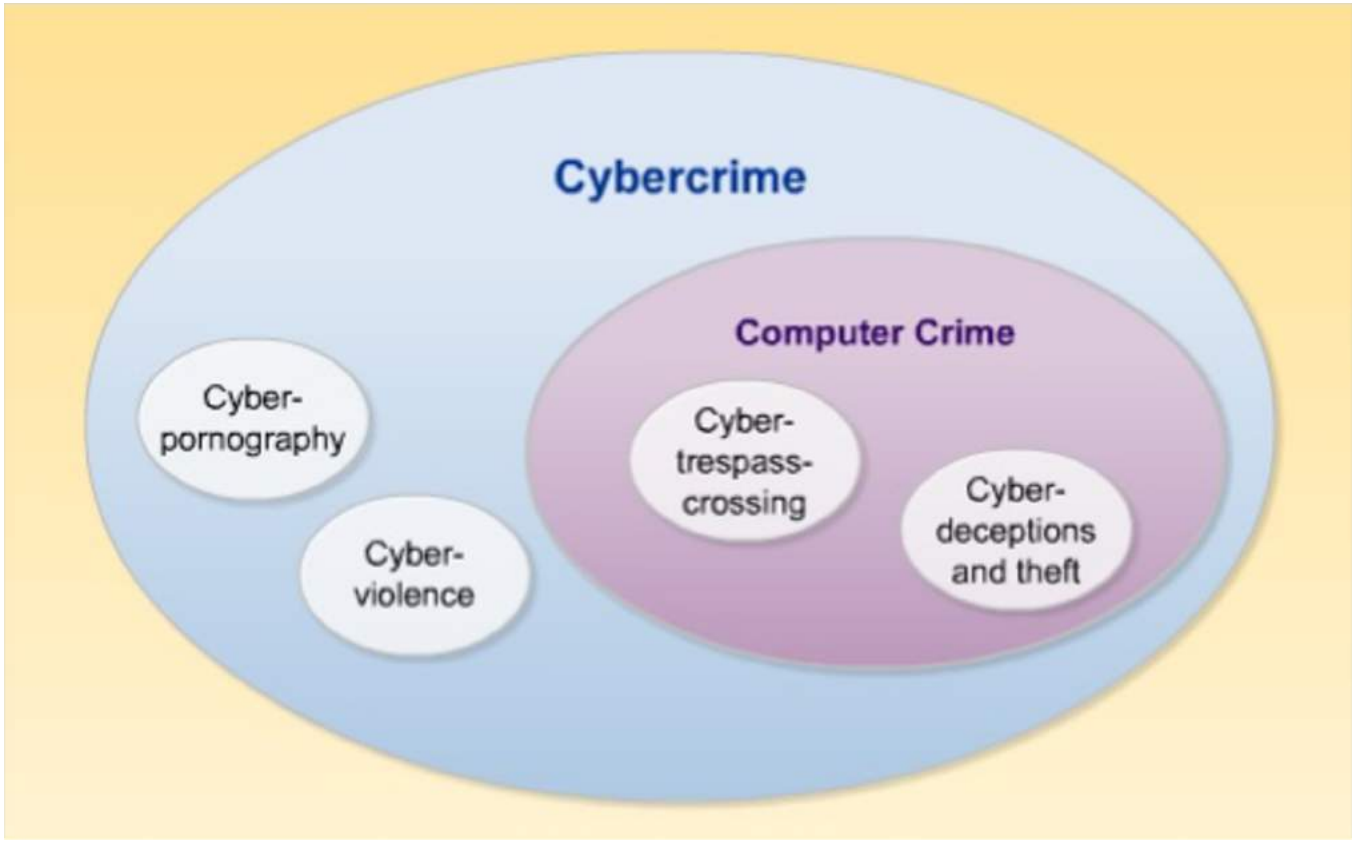
Computer-assisted crimes

Crimes occur offline, but computers/Internet/technology facilitate certain kinds of crimes.

Computer-focused crimes

Crimes that occur due to the existence and presence of computers/Internet/technology.

UMASS LOWELL


Cybercrime
Computer Crime
Cyber-
pornography
Cyber-
violence
Cyber-
trespass-
crossing
Cyber-
deceptions
and theft

Definitions and categories of cybercrime

Computer-assisted crimes

Cybercrime can therefore be viewed as a large umbrella term that encompasses **computer-assisted crime** in which computers and technology are used in a supporting role, such as the use of a computer to send harassing messages.

Computer-focused crimes

The term cybercrime also includes **computer-focused crimes** that are a direct result of computer technology and would not exist without it, such as unauthorized computer system trespassing.

UMASS LOWELL

Cybercrime investigation

(aka Hacking cybercriminals' minds)

How do we find out **who** did **what**?


NORSE
ATTACK ORIGINS
COUNTRY
United States
China
Ukraine
Netherlands
Colombia
South Korea
Switzerland
Turkey
Vietnam
ATTACK TYPES
PORT SERVICE TYPE
312 25 unknown
162 8080 unknown
154 23 telnet
48 3389 unknown
32 5900 unknown
25 445 unknown
25 3306 unknown
20 50864 unknown
18 53413 unknown
12 123 unknown
ATTACK TARGETS
COUNTRY
539 United States
219 United Arab Emirates
55 Spain
26 Singapore
23 Italy
16 Philippines
13 France
8 Russia
8 Belgium
6 Norway
LIVE ATTACKS
TIMESTAMP ATTACKER ATTACKER IP ATTACKER GEO TARGET GEO ATTACK TYPE PORT
16:59:18.841 Microsoft Corporation 207.46.100.245 Redmond, US De Kalb Junctio... unknown 25
16:59:18.469 Microsoft Corporation 207.46.100.253 Redmond, US De Kalb Junctio... unknown 25
16:59:18.268 Microsoft Corporation 65.55.169.253 Washington, US De Kalb Junctio... unknown 25
16:59:18.206 Chinanet Guangxi Province Network 171.107.91.55 Nanning, CN Madrid, ES telnet 23
16:59:17.937 Microsoft Corporation 157.56.110.250 Redmond, US De Kalb Junctio... unknown 25
16:59:17.528 Dslam Infrastructure South 182.180.148.15 Lahore, PK Roseville, US telnet 23
16:59:17.287 Chinanet-Zj Ningbo Node Network 60.178.154.200 Ningbo, CN Lynnwood, US unknown 50864
16:59:16.910 Microsoft Corporation 157.56.111.251 Redmond, US De Kalb Junctio... unknown 25
16:59:16.496 Chinanet Yunnan Province Network 182.243.33.3 Kunming, CN Lynnwood, US unknown 50864
HOME
EXPLORE
WHY NORSE?

How do you find suspects?
How do you find evidence?

Discussion

EVIDENCE

DIGITAL FOOTPRINT

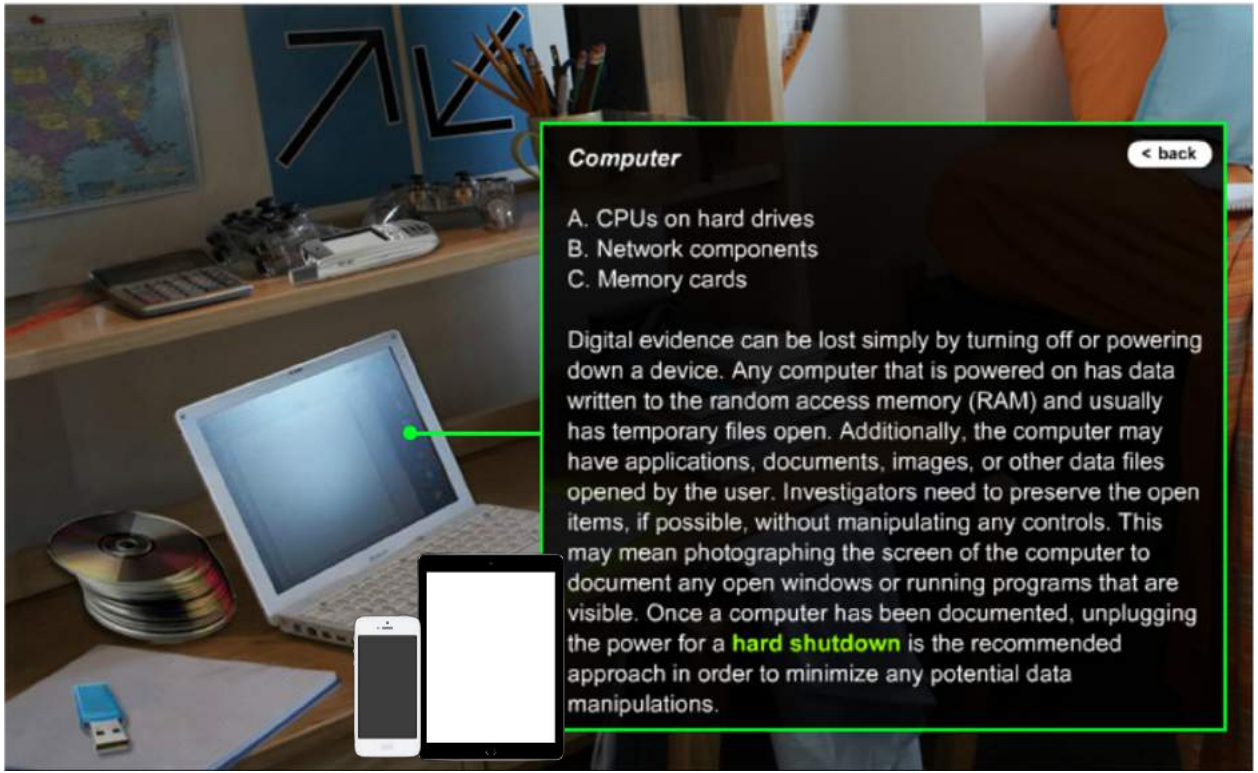
Finding evidence

John davis
(27 years old male)

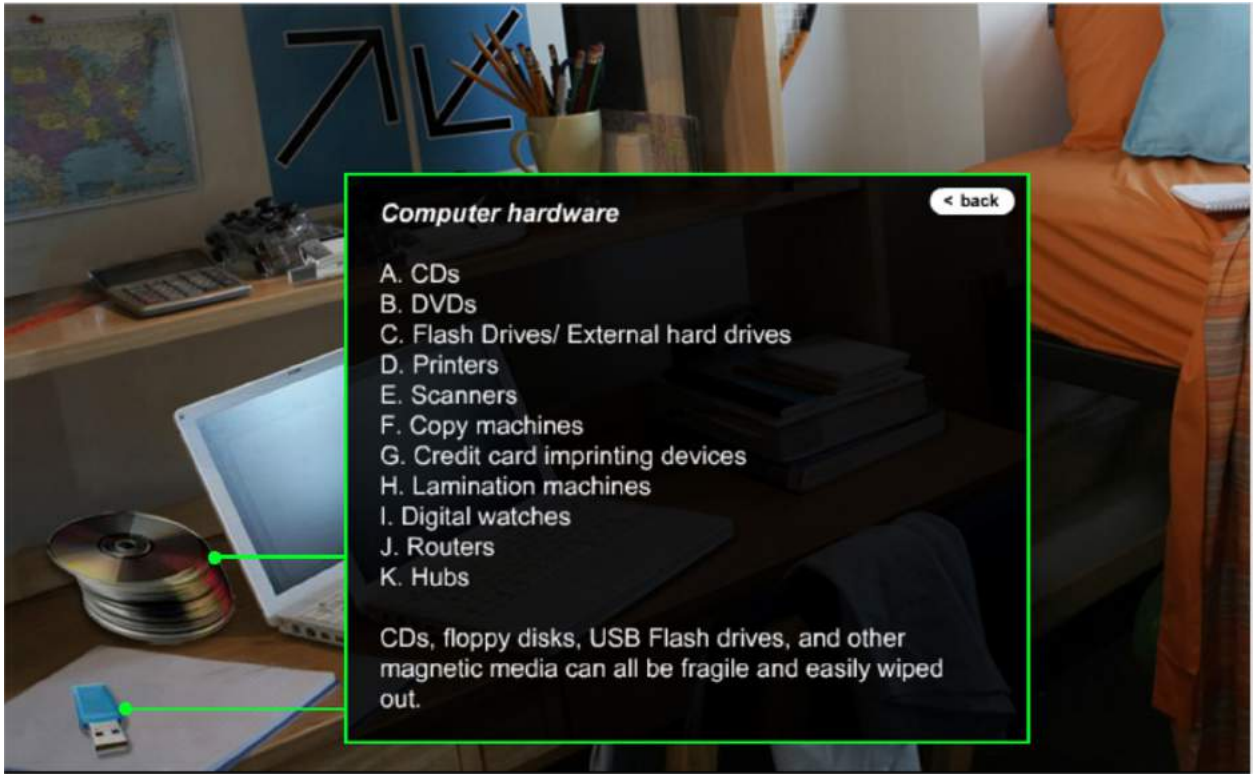
Our suspect

John Davis is suspected of hacking into
a foreign country's computer system.
What items would you collect as evidence?

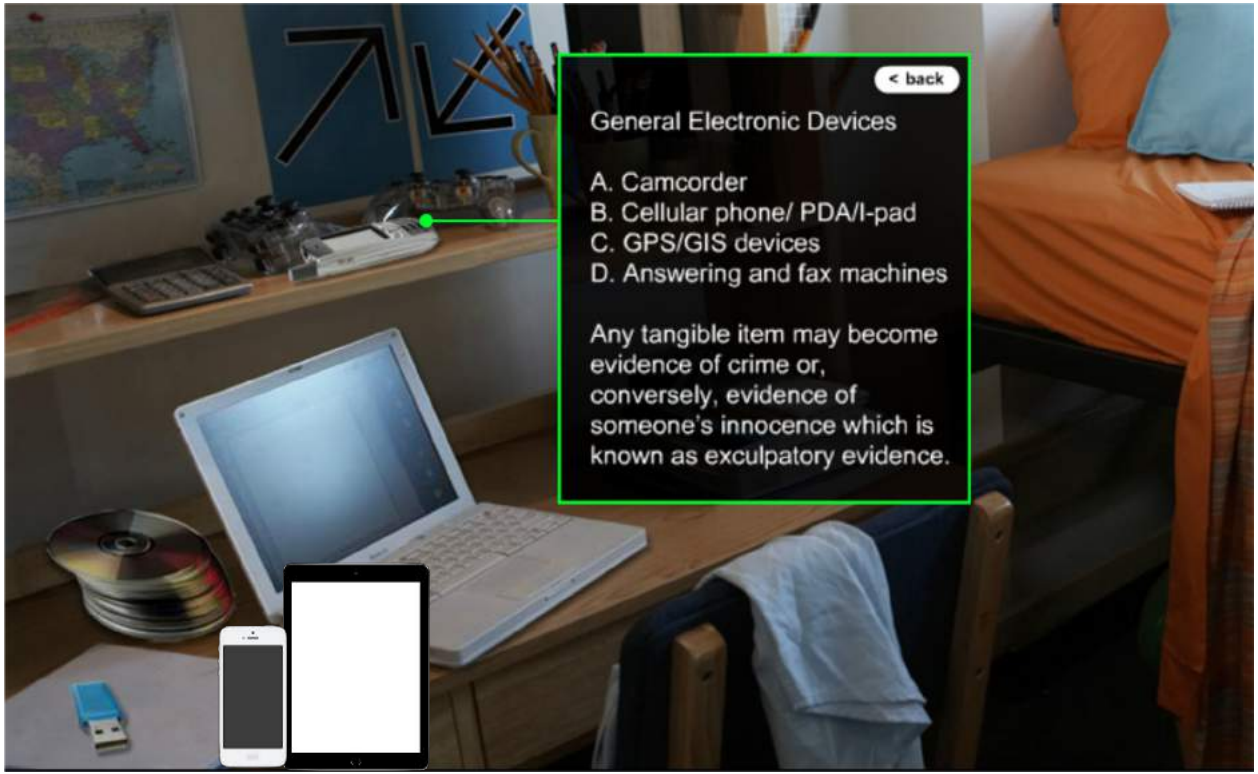
Computer


Computer
< back
A. CPUs on hard drives
B. Network components
C. Memory cards
Digital evidence can be lost simply by turning off or powering down a device. Any computer that is powered on has data written to the random access memory (RAM) and usually has temporary files open. Additionally, the computer may have applications, documents, images, or other data files opened by the user. Investigators need to preserve the open items, if possible, without manipulating any controls. This may mean photographing the screen of the computer to document any open windows or running programs that are visible. Once a computer has been documented, unplugging the power for a hard shutdown is the recommended approach in order to minimize any potential data manipulations.

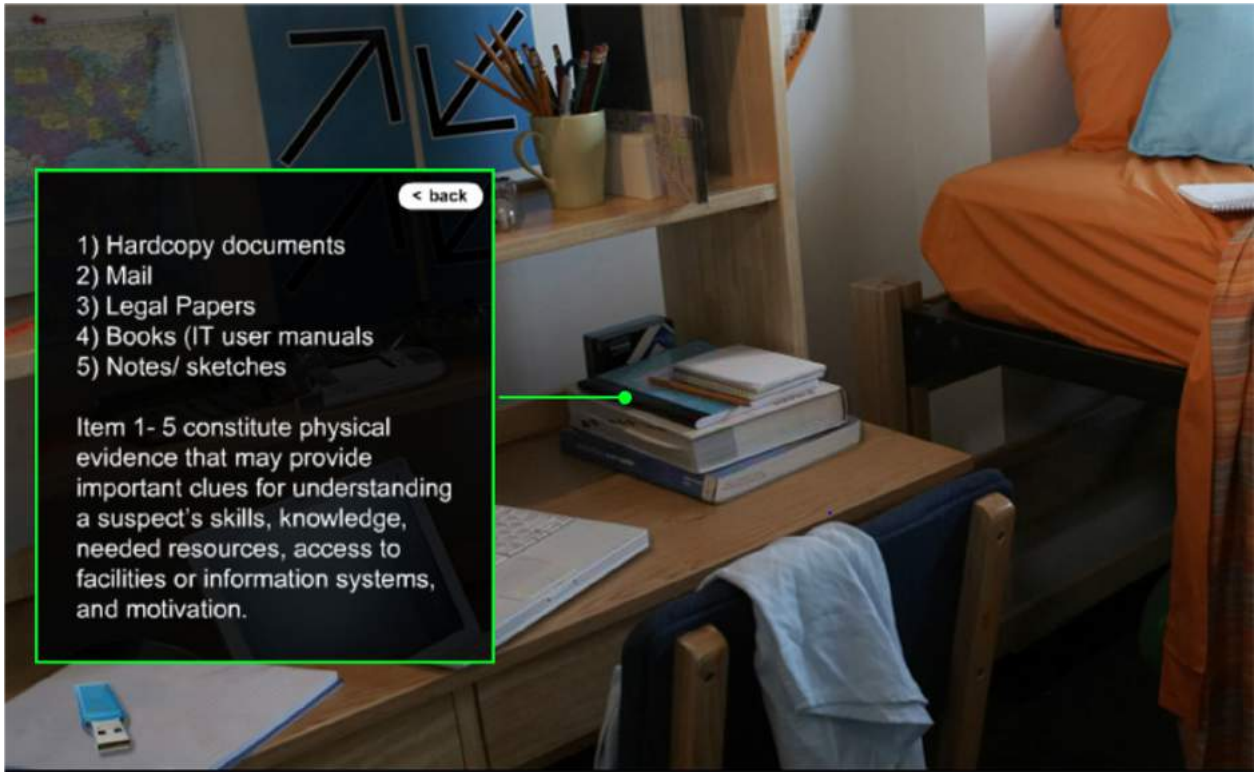
Computer hardware



General Electronic Devices



Papers


< back
1) Hardcopy documents
2) Mail
3) Legal Papers
4) Books (IT user manuals
5) Notes/ sketches
Item 1- 5 constitute physical evidence that may provide important clues for understanding a suspect's skills, knowledge, needed resources, access to facilities or information systems, and motivation.

How do you find cybercriminals' evidence?

These all can be evidence ...

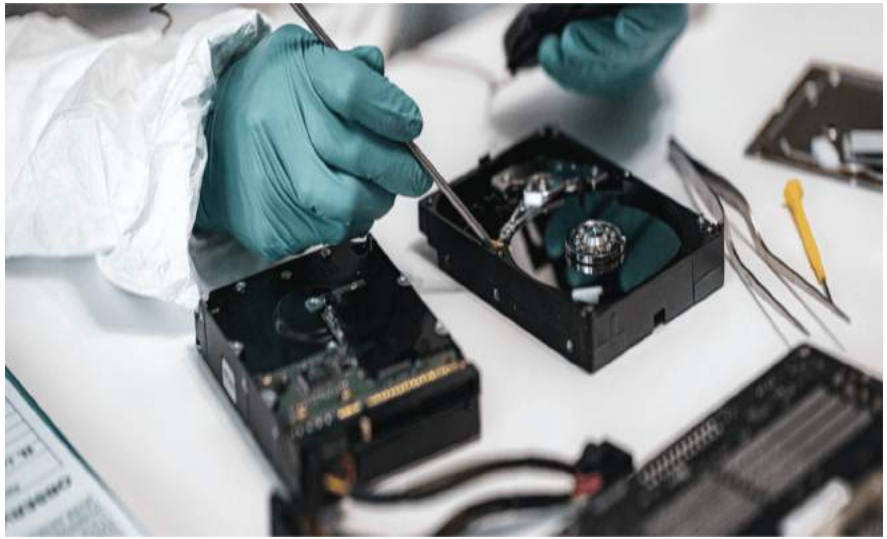
Computer

Computer hardware

Electronic devices

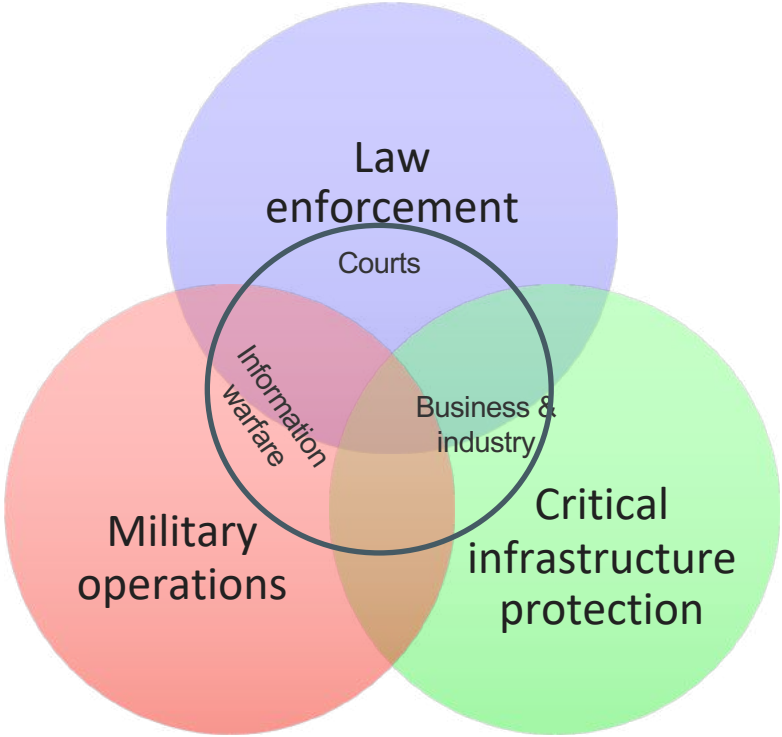
Papers

Digital footprint and digital forensics



Digital Forensics

"The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation presentation of digital digital evidence evidence derived derived from digital 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)

NON-DIGITAL EVIDENCE

Digital evidence

Roadmap of digital forensics

Aim

Methodology and activities

4 basic processes

6 principles

Criminal proceeding requirements

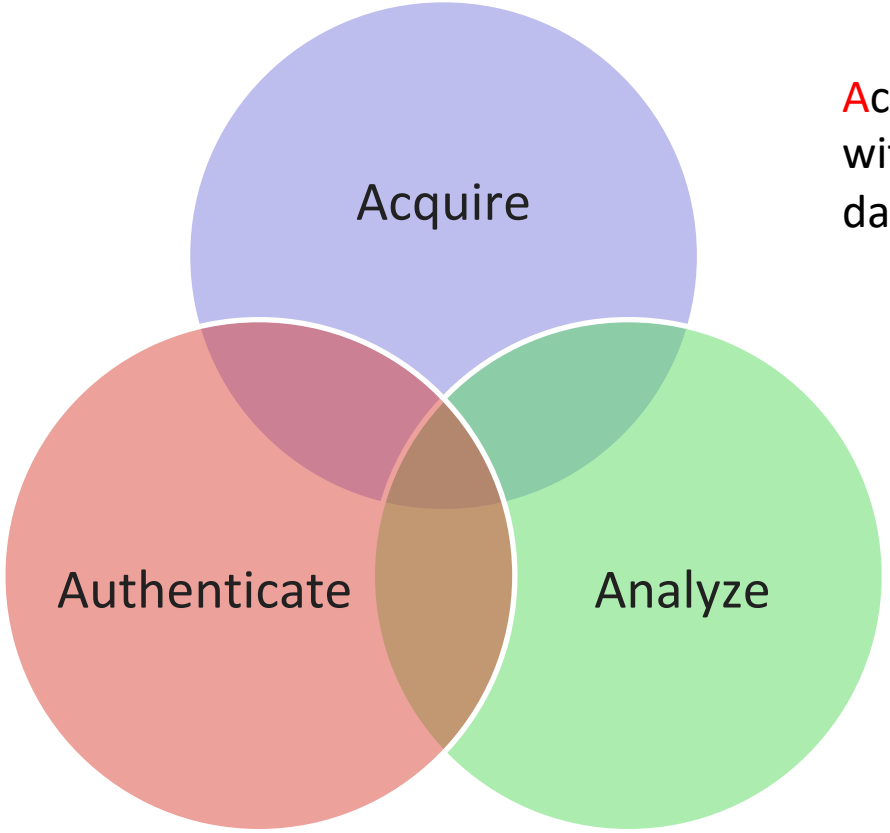
Hands-on practice

Digital forensics

Purpose

- To **search**, **preserve** and **analyze** information on computer systems to find potential evidence for a trial.
    - Many of the techniques detectives use in crime scene investigations have digital counterparts, but there are also some unique aspects to computer investigations.

Digital forensics: basic methodology



Acquire the evidence without altering or damaging the original

Authenticate the image

Analyze the data without modifying it

Types of digital forensics

- **Database forensics: databases** (incl. data & metadata)
- **Email forensics: emails** (incl. schedules & contacts)
- **Malware forensics: malware** (e.g. Trojan horses, viruses, ransomware)
- **Memory forensics:** information a computer's random access memory **(RAM) & cache**
- **Mobile forensics: mobile devices** (incl. contacts, text messages, pictures & video files)
- **Network forensics:** monitoring **network traffic** (e.g. a firewall, intrusion detection system)

Digital forensics: key activities

The secure **collection** of computer data

The **identification** of suspect data

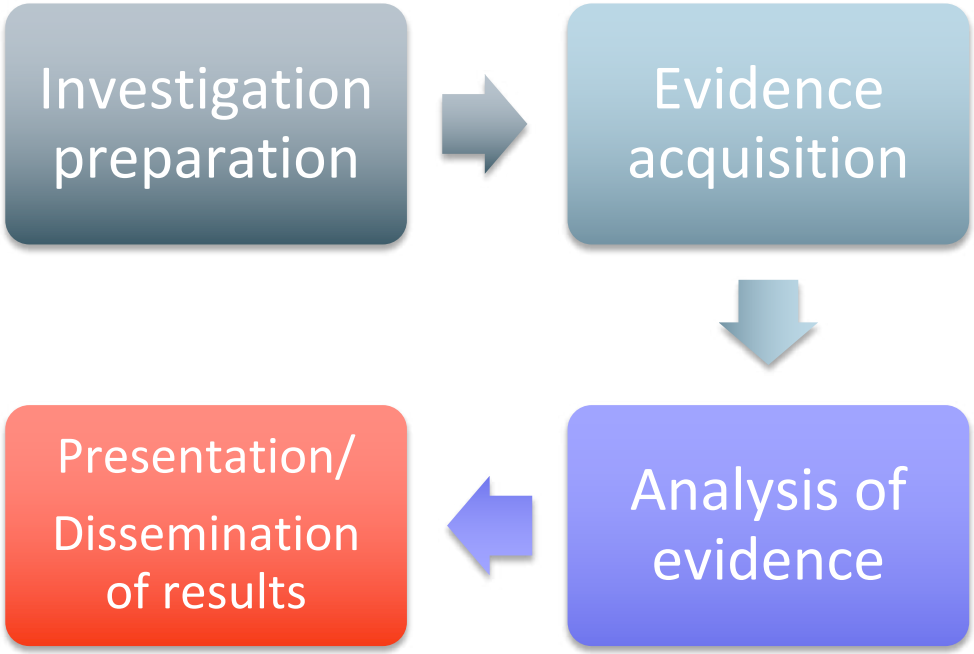
The **examination** of suspect data to determine details (e.g., origin, content)

The **presentation** of computer-based information to courts of law

The **application** of a country's laws to computer practice

Digital forensics: Basic process

- Identify the purpose of investigation
- Identify resources required



- Identify sources of digital evidence
- Capture the evidence

- Report findings
- Present findings

- Identify tools and techniques for further investigation
- Process data
- Interpret and analyze result

6 Principles of digital forensics

1. When dealing with digital evidence, all the general forensic and procedural principles must be applied.

2. Upon seizing digital evidence actions taken should not change that 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 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.

Digital forensics

- Usually, detectives have to secure a **warrant** to search a suspect's computer for evidence.
- The warrant must include where detectives can search digital device (phone, table) and what sort of evidence they can look for.

The 8 Steps of Criminal Proceedings

- Step 1: Arrest
- Step 2: Charges
- Step 3: Arraignment
- Step 4: Pretrial Proceedings
- Step 5: Trial
- Step 6: Verdict
- Step 7: Sentencing
- Step 8: Appeal

Search Warrant

- a legal document authorizing a police officer or other official to enter and search premises

The Search Warrant Requirement

- The Fourth Amendment has generally been interpreted to require that a search warrant contains a complete analysis and description of the place to be searched by law enforcement officers.

Example

- Let's try! What information should a law enforcement officer include during the search for digital evidence?
- Make sure you take into account the 4th Amendment

a legal document authorizing a police officer or other official to enter and search premises

Subpoena

- **Subpoena – basic subscriber information** (name, address, local and long distance telephone connection records, session times and duration, length of service, types of service used, telephone number or IP address, sources of payment, and the content of emails that are older than 180 days and have been previously opened by the owner).
- Benefits: If a suspect has a screen name that indicates the user is an MSN customer, using a subpoena drafted with this online identity the investigator could get the name, address, and billing information for the person who registered that screen name with MSN.

THE SEARCH WARRANTS ARE THE 1ST IMPORTANT STEPS OF CRIMINAL PROCEEDINGS

- In February 2015, the FBI obtained a search warrant to hack into the dark web to catch child pornography viewers and downloaders. Nationally, hundreds of people have been arrested for possessing and distributing child pornography and many motions have already been filed challenging **the validity of the search warrants**.

- Computer hacking forensic investigation is the process of detecting hacking attacks and properly extracting evidence to report the crime and conduct audits to prevent future attacks.

Digital forensics tools

Digital Forensics Tools

Disk imaging software

- It records the structure and contents of a hard drive

Digital Forensics Tools (con't)

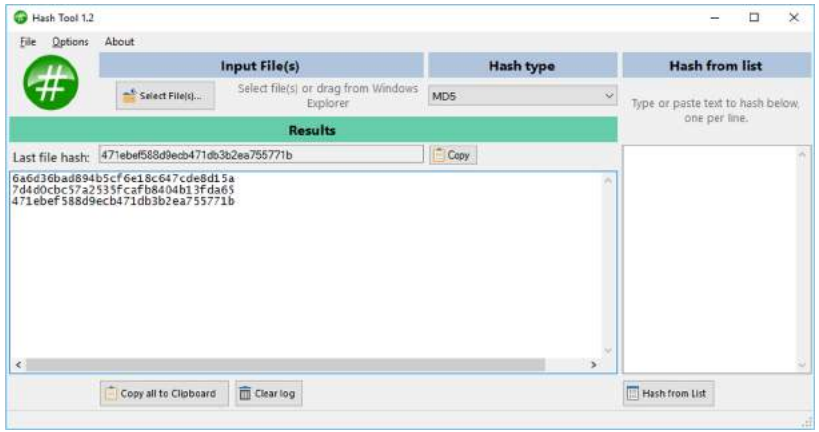
Software or **hardware write tools**

- It can copy and reconstruct hard drives bit by bit.
- Both the software and hardware tools avoid changing any information.

Digital Forensics Tools (con't)

Hashing tools

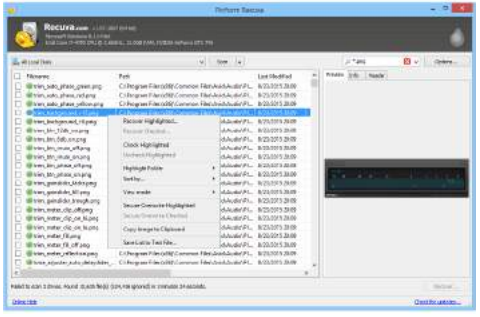
- Used to compare original hard disks to copies

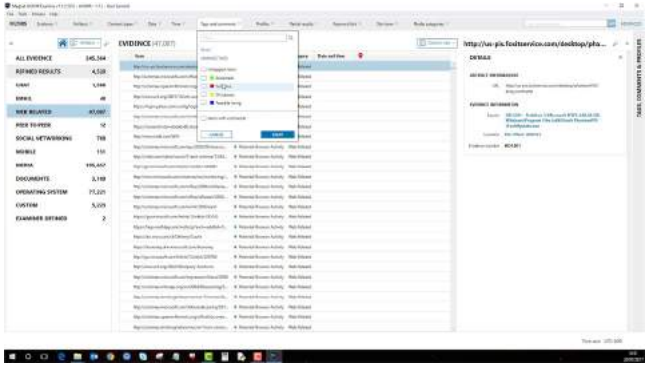


Digital Forensics Tools (con't)

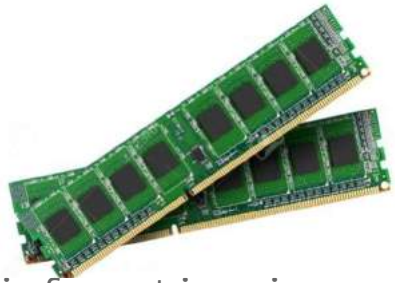
File recovery programs

- Used to search for and restore deleted data





Digital Forensics Tools (con't)

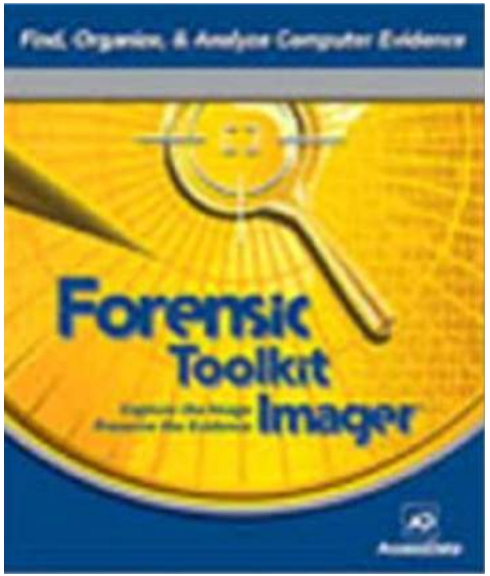


- There are several programs designed to preserve the information in a computer's **random access memory (RAM).**
  - Unlike information on a hard drive, the data in RAM ceases to exist once someone shuts off the computer. Without the right software, this information could be lost easily.
  - Analysis software sifts through all the information on a hard drive, looking for specific content. Because modern computers can hold gigabytes of information, it's very difficult and time consuming to search computer files manually. For example, some analysis programs search and evaluate Internet cookies, which can help tell investigators about the suspect's Internet activities. Other programs let investigators search for specific content that may be on the suspect's computer system.
  - Encryption decoding software and password cracking software are useful for accessing protected data.

Hands-on practice: FTK Imager

INSTALLATION/PREPARATION GUIDE

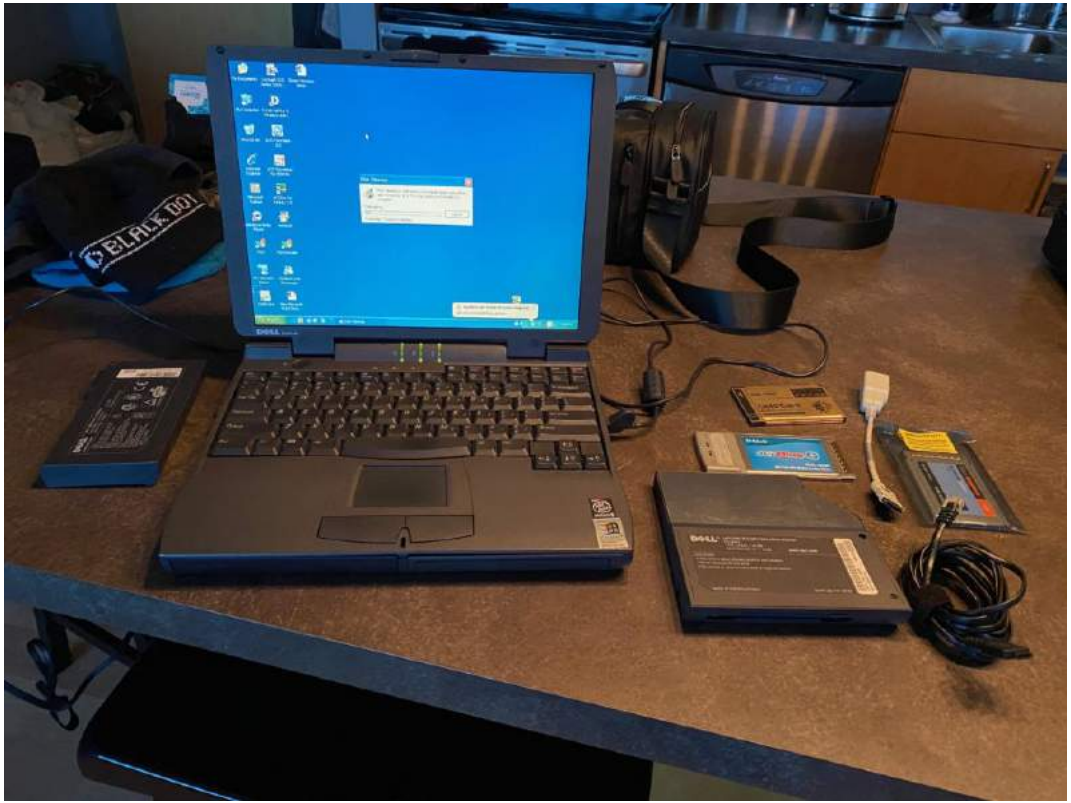
- You should be ready to find the tool (FTK Imager) in your virtual machine via UMass Lowell's CyberRange.



Forensic Toolkit Imager (aka TK Imager)

freeware

Scenario & Step-by-step guide



Source: NIST (2018). https://www.cfreds.nist.gov/Hacking_Case.html.

Handout & demo

Wrap-up: take home message and closing remarks

- Cybercrime
- Cybercrime investigation
- Digital forensics
- Digital forensic tools

Questions
&
Comments

claire_lee@uml.edu

See you in three days!

Main theme: Cybersecurity ethics

Dr. Claire S. Lee

Claire_Lee@uml.edu

E-MAIL

“You never really understand something until you understand how it relates to something you already know”

HOMEPAGE

drclairselee.wordpress.com

UMASS LOWELL