IFS4102: Digital Forensics

Lecture 1: Module Introduction & Administration, Digital Forensics

Ungraded Pre-Lecture Quiz

- What are key **differences** among: Digital Forensics, Penetration-Testing/Hacking, and Incident Response?
- Some relevant **characteristics**:
  - Offensive
  - Defensive
  - Investigative
  - Reactive
  - Retrospective
  - Preservative

Outline

- Module information
- Module administration & logistics
- Ice breaker

- What is Digital Forensics?
- Digital evidence and Locard's Exchange Principle
- Theories of Digital Forensics & digital investigation
- Role of hardware & information in a crime/breach
- Applications of Digital Forensics: sample cases
- Digital forensic careers

What is IFS4102 (Digital Forensics)?

- **Module description** (from CORS):

  "Digital forensics encompasses the recovery and investigation of material found in digital devices in relation to cyber crime and other crimes where digital evidence is relevant. This module gives an *introduction to principles*, *techniques*, and *tools* to perform digital forensics. Students will gain a good understanding of the *fundamentals* of digital forensics; *key techniques* for performing evidence extraction and analysis on UNIX/Linux systems, Windows systems, networks, Web applications, and mobile devices; and gain exposure to *available tools*. Some *legal aspects* of digital forensics will also be discussed."

- Modular credits: 4
- Pre-requisite: CS3235
- Preclusion: Nil
- Module workload (A-B-C-D-E)*: 2-0-1-2-5 (note the lab component)

* Please refer to CORS for the workload description

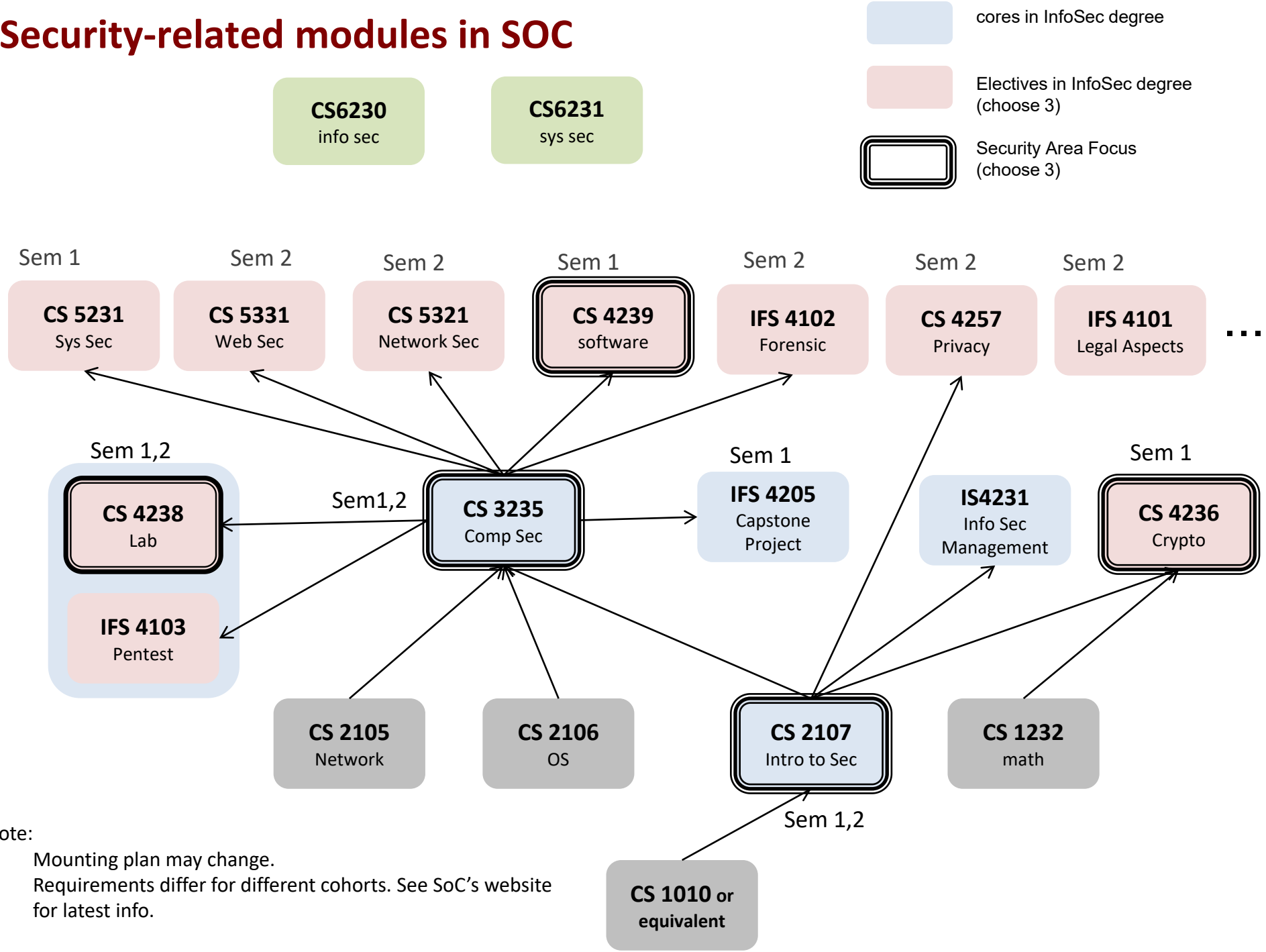
Module Learning Outcomes (MLOs)

- After completing the module, students should be able to:
  - **Understand** the digital forensics fundamentals
  - **Conduct** investigative process and digital evidence handling
  - **Apply** key techniques for performing data extraction and analysis
  - **Report** and **present** investigation findings
  - **Describe** important legal aspects of digital forensics

Module Coverage

- This module thus covers the following **aspects** of digital forensics:
  - **Procedural**: on *digital evidence handling* to meet admissibility requirements
  - **Technical**:
    - The ***main*** focus of this module
    - Includes: digital evidence acquisition, analysis, reporting, and presentation
  - **Legal** (some): just to highlight the role that digital forensic techniques play in solving legal cases (via case studies), admissibility requirements

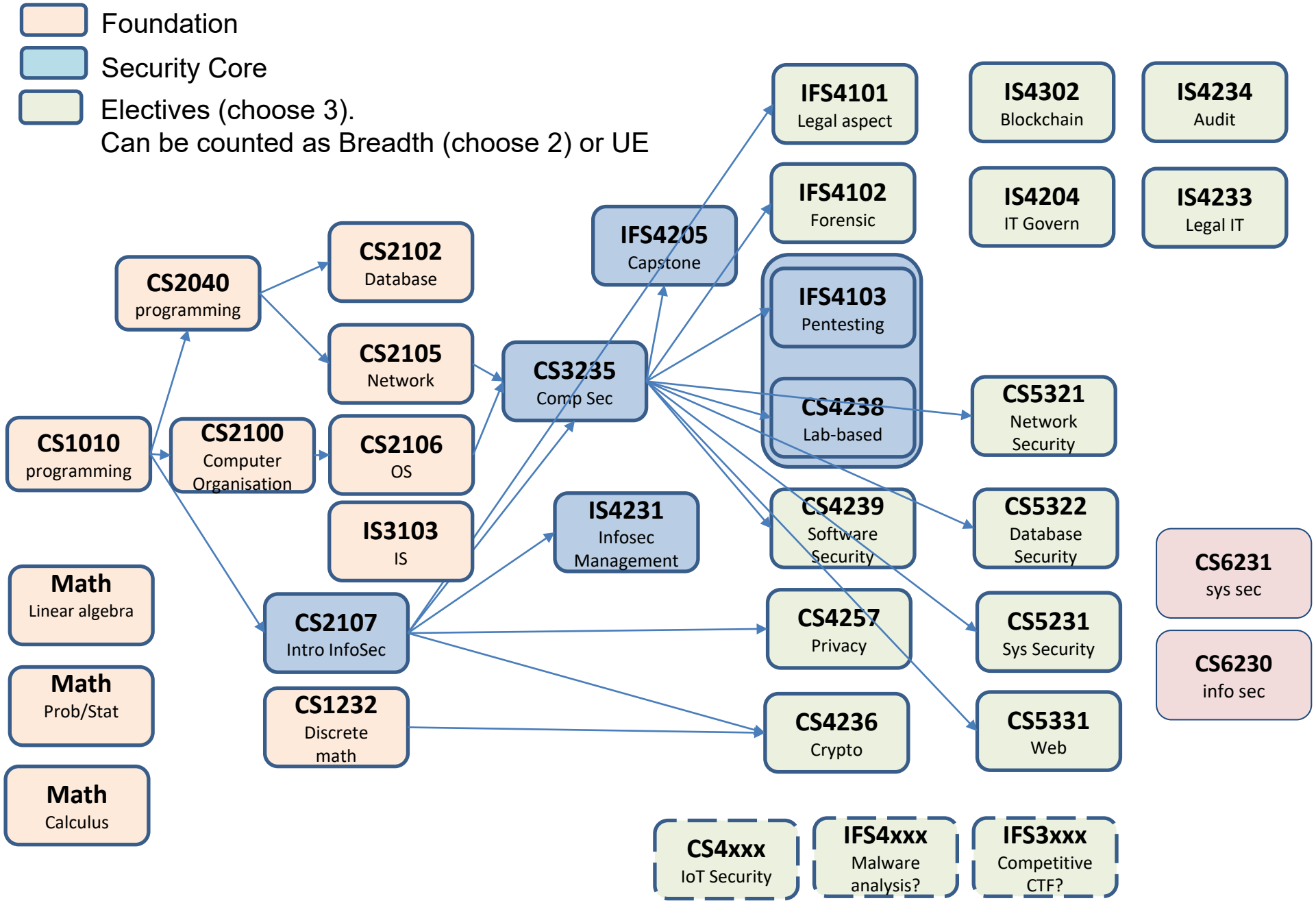
Security-related modules in SOC



Note:

1. Mounting plan may change.
2. Requirements differ for different cohorts. See SoC's website for latest info.

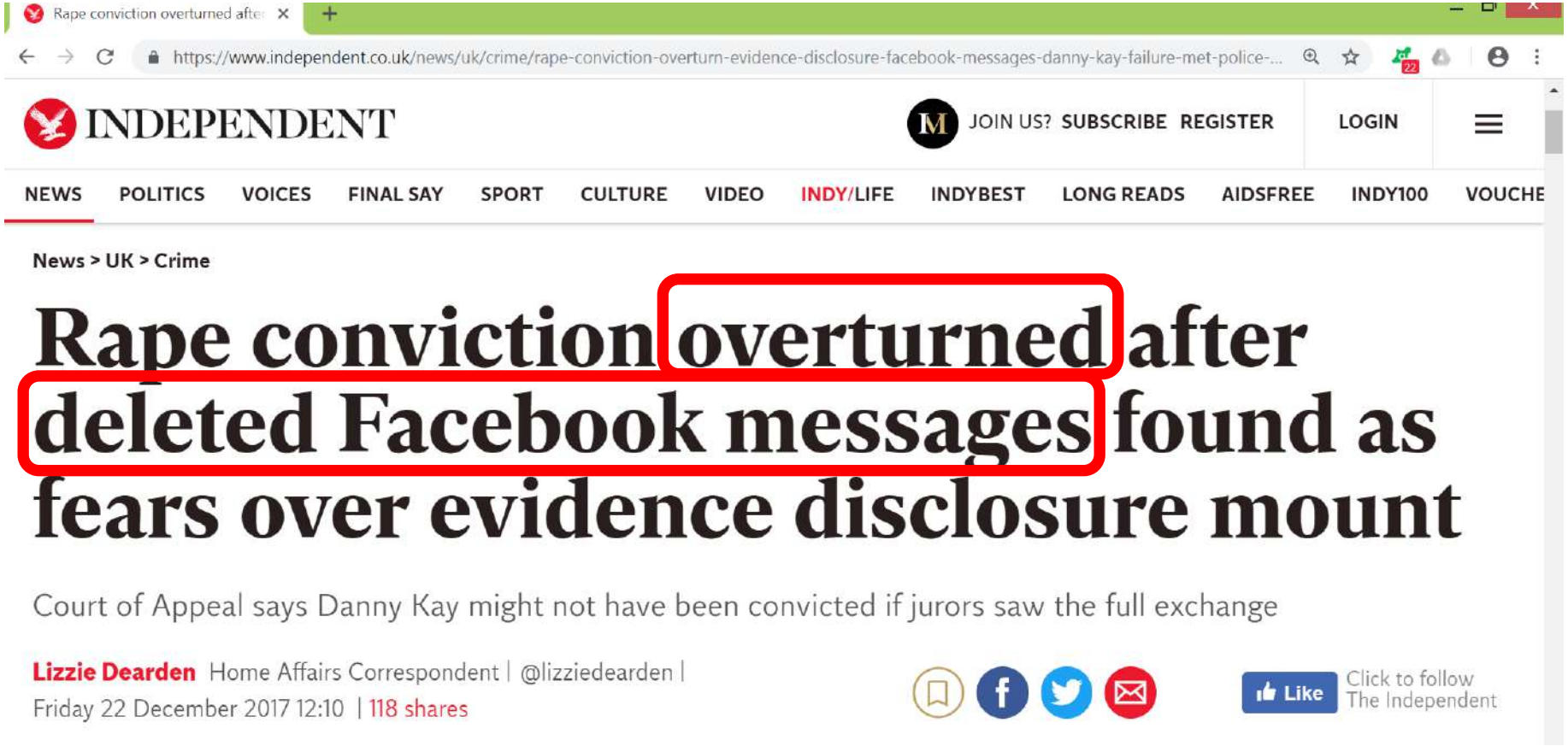
Security-related modules and BCOMP InfoSec requirements



Why Digital Forensics Field?

- Cyber crime and crimes where ***digital evidence*** is required/relevant are on the rise: a *worrying trend*
  - From Henry Lee's ***Crime Scene Handbook***, 1st Edition, 2001:
    "Within the past few years, a new class of crime scenes has become more prevalent, that is, crimes committed **within electronic or digital domains, particularly within cyberspace**. .... Even in investigations that are not primarily electronic in nature, at some point in the investigation **computer files or data** may be discovered and further analysis required."
  - In short: many crimes nowadays have a ***digital dimension***
  - Even if digital data **do *not* provide a (direct) li**nk between a crime and its victim or a crime and its perpetrator, they **can be useful** in an investigation

An Interesting Real Case as Motivation



From: https://www.independent.co.uk/news/uk/crime/rape-conviction-overturn-evidence-disclosure-facebook-messages-danny-kay-failure-met-police-a8124241.html

An Interesting Real Case as Motivation

Danny Kay, 26, spent more than two years in jail for a rape he did not commit had his conviction quashed after a relative took only a minute to uncover a series of bombshell Facebook messages – missed by police – that proved his innocence (pictured with sister-in-law Sarah Maddison)

"Mr Kay asked Ms Maddison to log in to his account. '**I couldn't believe how easy it was to find the messages**,' she said. 'I've just worked in admin all my life and am no social media expert. **It only took me a minute to find them so how trained police couldn't is beyond me**.'"

From: https://www.dailymail.co.uk/news/article-5223567/Man-rape-conviction-quashed-police-blunder.html

Why Digital Forensics *Module*?

- Digital forensics vs other cybersecurity modules/fields (e.g. hacking, Incident Response):
  - Different goal/**nature**, approach, tools
- We feel that *every* information security professional nowadays should also know **digital forensics principles** and **key techniques**
- This module provides you with the basics in performing **evidence extraction** and **analysis**: useful when getting involved in a digital forensics investigation
- The knowledge and techniques are also useful for **incident response**

A Case as Motivation for Digital Forensics Module

- **Roger Lee Sanders v. The State of Texas (Trial Court No. 0940303R):**
  - "Roger Sanders was sentenced to life in prison after his conviction on ten counts of aggravated sexual assault of a child under the age of fourteen."
  - "Jessie Lee, the State's **forensic computer examiner** who recovered the child pornography from computer media found in Sanders's apartment …. His training included **software programs like EnCase and Forensic Toolkit**."
  - "Lee explained that when he takes a **hard drive** from a computer, he uses a program like EnCase to automate the task of searching and finding the files on it:
    - An **image** of the drive is taken.
    - The **files** are copied, and EnCase **validates** the copy by an MD5 hash.
    - EnCase indexed the files, and Sanders was able to **retrieve deleted files** containing child pornography from Sanders's computer."
  - Source: https://law.justia.com/cases/texas/tenth-court-of-appeals/2006/7374.html

Teaching Mode & Grading

- **Lecture**:
  - Friday 12:00-14:00 F2F + Zoom option, with no recordings
  - 12 lectures (due to 1 public holiday: Good Friday, 7 Apr 2023)
- **Lab**:
  - Friday 14:00-15:00 (with some **graded** questions)
  - 9 lab sessions, including *self-exercised* Lab 1 in **Week 1**
- **Assessment**: 100% CA, with the following weightage:
  - 2 individual assignments (15%+15=**30%**): technical tasks
  - Short questions related to lab tasks (**10%**): continual practice!
  - In-class written + practical tests (**25%**): in Week 8
  - Group-project assignment (2 cases), including its presentation in Weeks 11 & 13 (**35%**) → *In a group of 4, group marks are shared (but with possible moderation!)*
- *No final exam, yay!*

Tentative Schedule

1. Module info & admin, digital forensics background & methodologies (+ self-lab Lab 1)
2. Digital evidence & handling, investigative process, static acquisition (+ Lab 2)
3. Live acquisition, storage media, automated disk-image analysis (+ Lab 3)
4. Disk and file analyses (+ Lab 4)
5. Windows forensics (+ Lab 5)
6. Windows forensics, Linux forensics (+ Lab 6)

Recess week

7. Network and Internet forensics, group-project briefing (+ Lab 7)
8. **Written + practical tests**: F2F
9. Forensics case management (report writing & presentation), Incident Response (+ Lab 8)
10. Mobile Forensics (+ Lab 9)
11. **Project presentation 1**
12. *Public holiday*
13. **Project presentation 2**, module review

Tentative Schedule

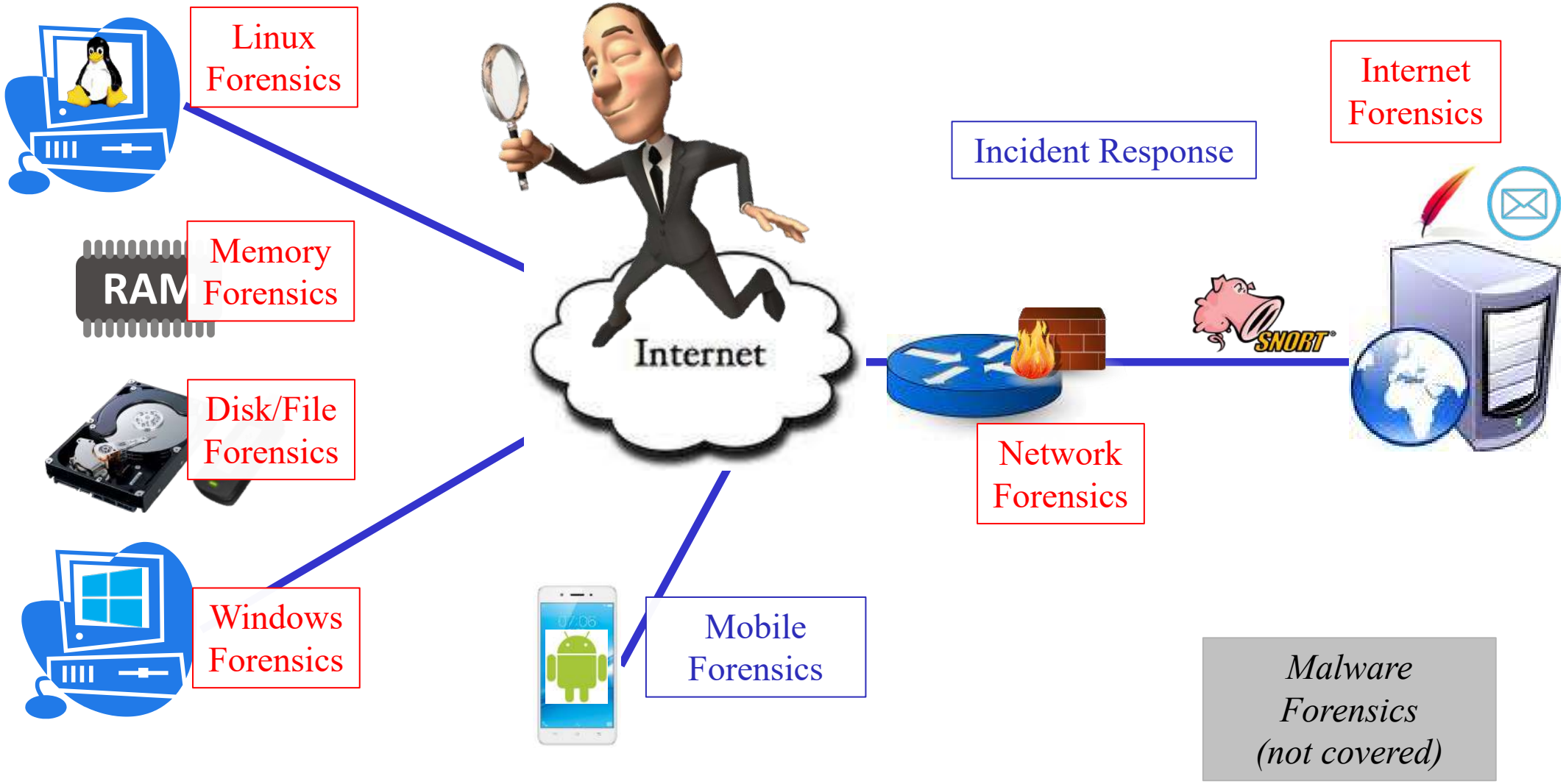
IFS4102 Tentative Schedule: Semester 2 AY-2022/23 (Jan - April 2023)					
Week No	**Date (Fri)**	**Agenda**	**Lab**	**CA Activities**	
				Assignment	**Group Project**
1	13-Jan	Module info & admin, digital forensics	*(Lab 1)*		
2	20-Jan	Digital evidence & handling, investigative process, static acquisition	Lab 2		
3	27-Jan	Live acquisition, storage media, automated disk-image analysis	Lab 3	A1	
4	03-Feb	Disk and file analyses	Lab 4		
5	10-Feb	Windows forensics	Lab 5		
6	17-Feb	Windows forensics, Linux forensics	Lab 6		
Recess Week					
7	03-Mar	Network and Internet forensics, group-project briefing	Lab 7	A2	Project Cases 1 & 2 (Case 1 present in W-11, Case 2 present in W-13)
8	10-Mar	**In-class written + practical tests**			
9	17-Mar	Forensics case management, Incident Response	Lab 8		
10	24-Mar	Mobile Forensics	Lab 9		
11	31-Mar	**Project presentation 1**			
12	07-Apr	*Good Friday*			
13	14-Apr	**Project presentation 2**, module review			

Teaching Staff and Lecture Materials

- Lecturer: Sufatrio (Rio)
- TA: Ryan Kwok

- **Some lecture slides** are based on past year's version co-developed with **Dr. Stephen McCombie** (then an Adjunct Lecturer):
  - Worked in the military, police and IT security industry for over 30 years
  - Been involved in digital forensics and cybercrime investigation for ~15 years
  - Holds a Ph.D. in computer science, a master's of IT and a B.A. in international relations
  - Taught at Macquarie University in Australia

Looking Forward: Covered Topics



What Are *Not* Covered In This Module

- Some cybersecurity aspects ***not*** covered in this module:
  - **Deep legal aspects** of Information Security (in Singapore context): See & take IFS4101 (Legal Aspects of Information Security)
  - **Malware forensics/analysis**: Take CS4238 (Computer Security Practice)
  - **Software vulnerability** discovery and assessment: Check CS4239 (Software Security)
- The following aspect is **covered briefly**:
  - **Incident Response (IR)**: attack detection & response

Popular Forensics Software Suites

- Some popular **commercial forensics** software ***suites***:
  - EnCase (Guidance Software)
  - Forensic Toolkit or **FTK** (AccessData)
  - X-Ways Forensics (X-Ways)
  - Oxygen forensic Suite (Oxygen Forensics)
  - ProDiscover Forensic Edition (the ARC Group of NY)
- Comprehensive and integrated tools
- A **free** & **open-source** alternative: ***Autopsy***

Other Forensics Tools

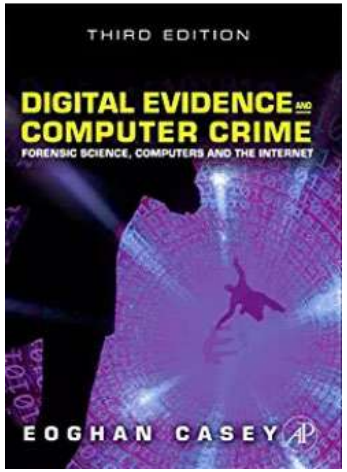
- ***Specialized* software tools/utilities**:
  various tools are available: many are covered in the module
- **Hardware tools**:
  - **Forensics workstation**: a fast machine with large memory+disk capacity
  - **Field-kit**: portable for use at crime scenes, laptop or specialised device
- Other **supporting tools**:
  - Anti-static evidence bags, signal-blocker bags, hardware write blocker, cables, cameras, flashlights, etc.

Forensics Tools Used in the Module

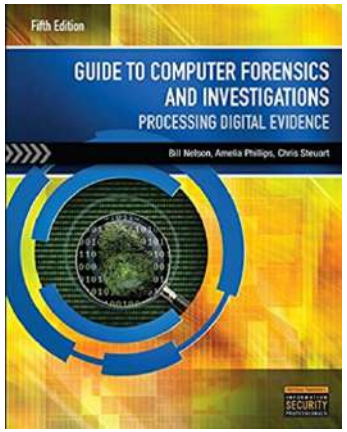
- You will set-up your **forensic workstation**:
  - Some **Linux distros** (Kali Linux, SIFT) can help with tool installations: *See Lab 1*
  - Nevertheless, a **Windows-based forensic** workstation is sufficient
  - VMM/hypervisor is possible: *See Lab 1*
- **Autopsy** suite + various stand-alone **free software tools**, including: FTK Imager, dd/dcfldd, Volatility, The Sleuth Kit (TSK), RegEdit, RegRipper, Scalpel, Bulk Extractor, ExifTool, Wireshark, Log2Timeline/Plaso, several NirSoft utilities, …
- **Emphasis** is put more on: forensics methodology, tasks, techniques, and problem solving
- ***Independent*** of particular products/tools/vendors, specific technologies

Recommended General References

- Eoghan Casey, "*Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*", 3rd Edition, Academic Press, 2011



- Bill Nelson et al., "*Guide To Computer Forensics and Investigations*", 5th Edition, Cengage Learning, 2015



Other References for *Specific* Topics

- **Disk & file analysis**:
  Brian Carrier, "*File System Forensic Analysis*", 1st Edition, Addison-Wesley Professional, 2005
- **Windows forensics**:
  Harlan Carvey, "*Windows Registry Forensics: Advanced Digital Forensic Analysis of the Windows Registry*", 2nd Edition, Syngress, 2016
- **Network forensics**:
  Ric Messier, "*Network Forensics*", 1st Edition, Wiley, 2017
- **Android Forensics**:
  Oleg Skulkin et al., "*Learning Android Forensics*", 2nd Edition, Packt Publishing, 2018

Notes on Group Project & Assignments

- The goal of university study is to encourage **reasoning**, **critical thinking** & **originality**
- For the assignments and group project,
  it is important you understand the required standard
- We are looking for **original thought** but backed up by existing **facts and opinions**
- Look **beyond** the supplied material

NUS' Latest Plagiarism Policy

- You should be aware of the consequence: F
- Importance of **academic honesty**
- The module recognizes that **some interactions** with classmates/others can facilitate understanding of the course's material
- The key is: "**be reasonable**"
- We will adopt a policy similar to Harvard CS50's: https://cs50.harvard.edu/x/2020/honesty/
- Next are rules of thumb that (inexhaustively) lists acts that the module considers **reasonable** (based on https://cs50.harvard.edu/x/2020/honesty/)

Still Reasonable in Our Module

- **Discussing** the course's material or assignment task with others in order to understand it better
- Whiteboarding solutions with others using diagrams but ***not*** actual code/commands
- Turning to the web or elsewhere for instruction beyond the course's own, for references, and for solutions to technical difficulties, but ***not*** for outright solutions to assigned work

Additionally…

- Properly **reference** others work you use
- Do not use slabs of text **cut and pasted** from elsewhere unless in direct quotes, and even then sparingly
- You can **paraphrase** but its not a license to copy, and you must give credit
- Use others to support your statements (multiple sources is great)
- Use a recognized **referencing style** like Harvard or APA

Notes on Lectures and Labs

- Attendance will not be taken during lectures and labs:
  - But please do *attend* them still
  - Please pay attention and participate in class and labs
  - And do submit **graded lab questions**!
- Canvas **forum/discussion**:
  - For group formation
  - For assignment and project discussions
    - You can ask questions and share ideas
    - *But* don't reveal your answers!
  - Please be courteous, even when disagreeing with others

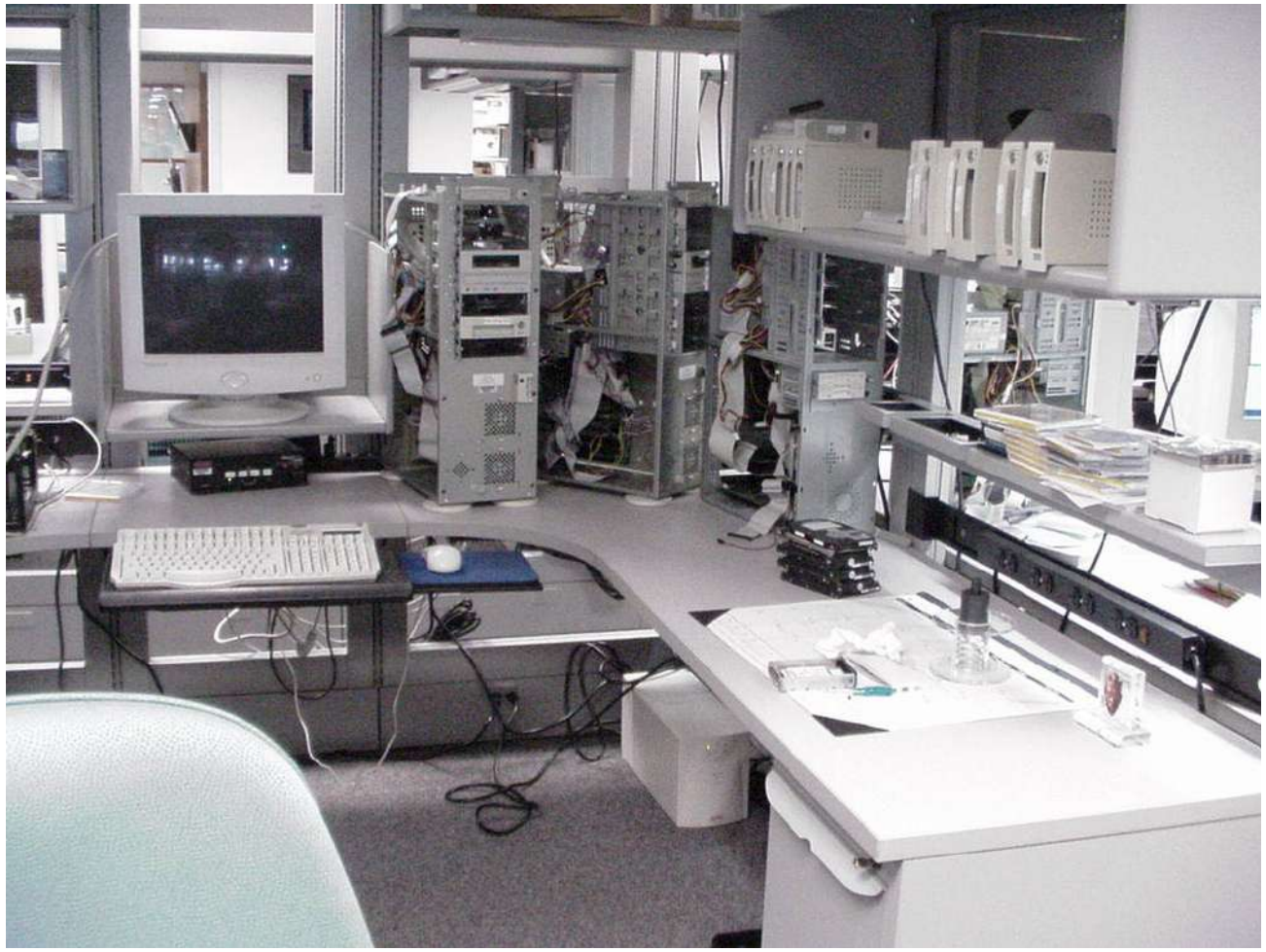
Ice Breaker!

- Tell us about your **background**
- Tell us what you would like to **get out of the course**
- *And…*
- You can start **forming your group** after this lecture later!
- Or even during the **break** right after this

Source: PowerPoint

Break!

Digital Forensic Lab (For Illustration)



US Dept of Defense Computer Forensic Workstation (http://www.dcfl.gov/photo.html)

Mobile Digital Forensic Lab (For Illustration)

Orange County Mobile Digital Forensic Lab: http:// fbiretired.com

What is Digital Forensics?

What is Digital Forensics?

- There are **various** definitions, including the two ones below
- **McKemmish(1999):**
  "The process of **identifying**, **preserving**, **analysing** and **presenting** digital evidence in a manner that is **legally acceptable**"
- **Farmer and Venema (1999):**
  "Gathering and analysing data in a manner as **free from** distortion or bias as possible **to** reconstruct data or what has happened in the past on a system"

What is Digital Forensics?

- Numerous ***other* definitions**
- Often reflect the background of authors

- Sometimes referred to as "**computer forensics**", but nowadays **computer forensics** $\subset$ ***digital forensics***
- The key element is **forensics**

- ***What is forensics anyway?***

Oxford Dictionary Definition of Forensic & Forensics

- ***adjective (forensic)***
  1 relating to or denoting the application of scientific methods to the investigation of crime.
  2 of or relating to courts of law.
- ***noun (forensics)***
  forensic tests or techniques.
- **ORIGIN** Latin *forensis* 'in open court, public'

- Contrast it with **Casey (2011)**:
  Forensic: "a characteristic of evidence that satisfies its **suitability for admission** as fact and its ability to **persuade** based upon proof (or high statistical confidence)"

So, What is Digital Forensics?

- At its **simplest**:
  "Bringing **computer/digital information** using **scientific techniques** (if necessary) **to a court of law or tribunal**"

- Also another commonly-referred definition from **US-CERT** (www.us-cert.gov/sites/default/files/publications/forensics.pdf):
  "The discipline that combines **elements of law and computer science** to **collect** and **analyze** data from **computer systems**, **networks**, **wireless communications**, and **storage devices** in a way that is ***admissible as evidence in a court of law***"

Digital Evidence & Locard's Exchange Principle

Some Definitions: Digital & Electronic Evidence

- ***Digital evidence*** (Chisum, 1999):
  any **data stored** or **transmitted** using a computer that support or refute a theory of how **an offense occurred** or that address **critical elements of the offense** such as intent or alibi

- In short: "any information of *probative value that* is either stored or transmitted in a digital form" (Casey 2011)

- **Digital evidence** (information) vs ***electronic* evidence** (hardware)
- Also the **roles** of information and hardware in a crime/breach: *more later in today's lecture*

Sources of Digital Evidence

- The sources are usually categorized into **three groups**:
  1. **Open computer systems**: computers including their storage
  2. **Communication systems**: traditional telephone systems, wireless telecommunication systems, the Internet, and networks in general
  3. **Embedded computer systems**: mobile devices, smart cards, and many other systems with embedded computers

Locard's Exchange Principle

- By Edmond Locard, who built the first police lab in Lyon, France, in 1910:
  - "**Every contact leaves a trace**"
  - "Anyone/anything entering a crime scene always **leaves something behind** or **takes something with him** when he leaves, no matter how small"

- ***Question*:** Is it applicable to **digital forensics** as well?

- Evidence transfer occurs in **both** the physical and digital realms and can provide **links** between them (Casey 2011):
  - **Digital/cyber footprint** as possible digital evidence
  - An **ever-increasing** digital footprint production per person
  - *Why is that so? Any possible reasons?*

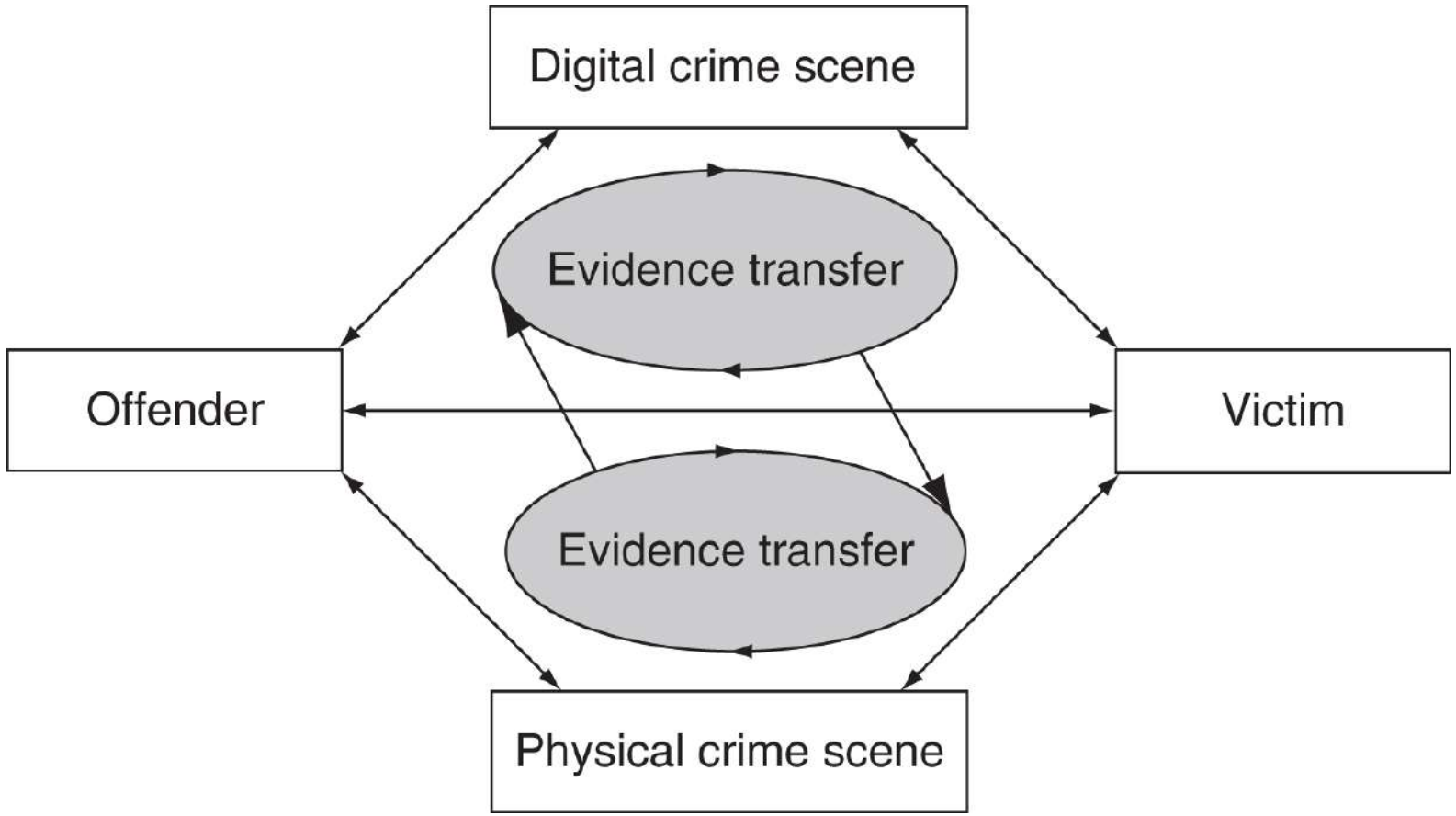


FIGURE 1.1 Evidence transfer in the physical and digital dimensions helps investigators establish connections between victims, offenders, and crime scenes.

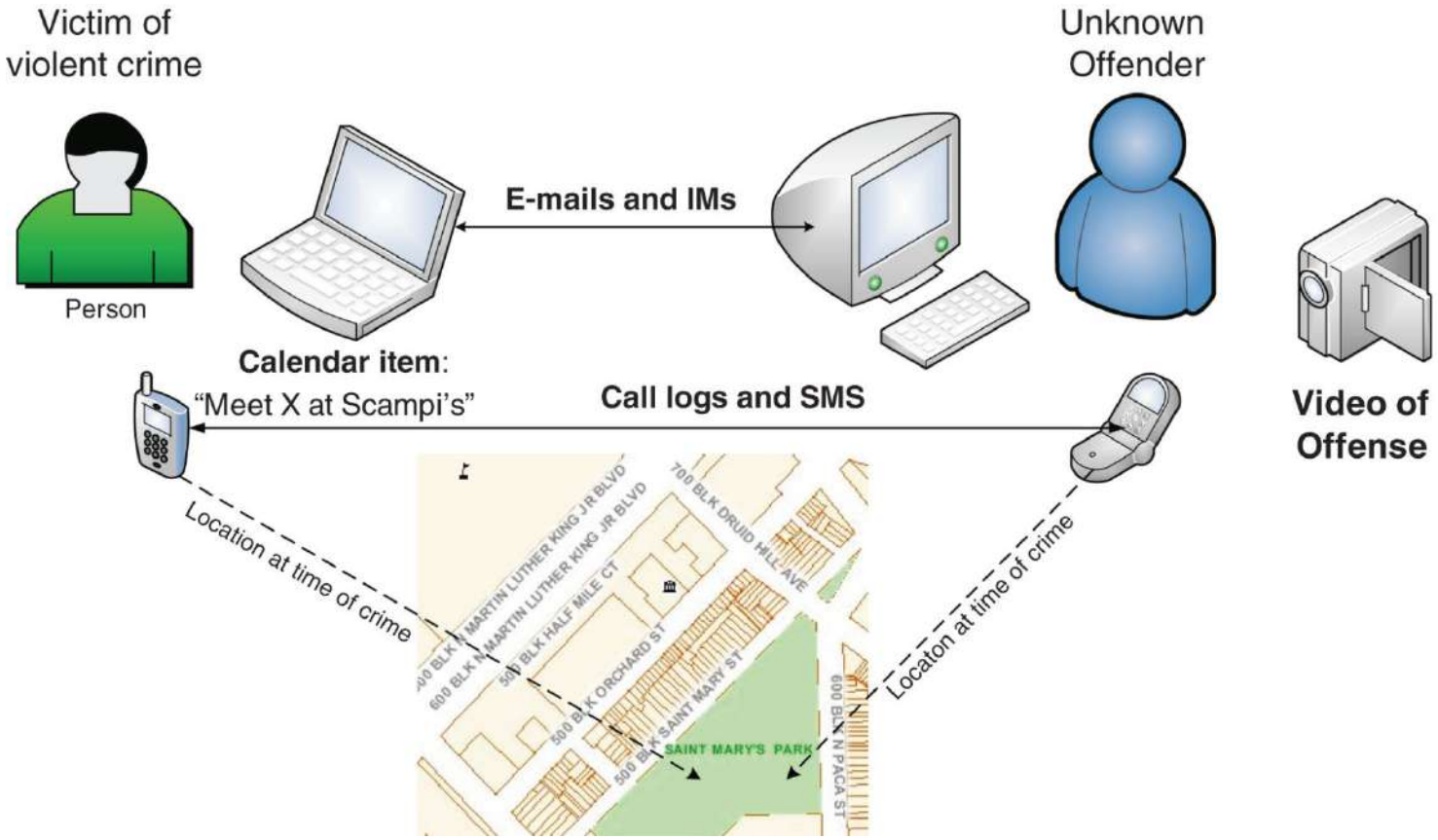


FIGURE 10.1 Diagram depicting potential sources of digital evidence linking the victim of a violent crime with the offender and crime scenes.

Increased Digital Footprint In Our Age

- **Evidence digitalization** (e.g. text, image, audio, video) → evidence is digitally processable, transferable, copiable
- Ubiquitously-available and highly-portable **digital sensors** (e.g. camera, audio/video recorder, geolocation sensor) → increased sensor-created personal digital evidence
- Increased storage capacity & usage: **computer-stored records**
- **Online & connected world** (e.g. online shopping/transaction records, cloud-based email and storage) → abundant user-generated online data
- ***Computer*-generated data** (e.g. telephony logs, network logs, computer logs) → additional user-related online records

So, Is Internet Separate from the Physical World?

- ***No?!*** **(Casey, 2011)**
- Crime on the Internet is usually **closely tied** to crime in the physical world:
  - A **crime on the Internet** usually reflects a crime in the physical world
  - We can learn more about the criminal activities that exist in the physical world by observing **online activities** of offenders
  - When a crime is committed in the physical world, **the Internet often contains related digital evidence**: the evidence should be considered as an **extension** of the crime scene
- ***"In our digital world, our digital actions leave digital evidence"***: while criminals may feel safe on the Internet, they actually can be **observable** and therefore vulnerable

Locard's Exchange Principle in Sample Cases

- **E-mail harassment** case:
  - Sent **threatening *messages***
  - **Traces** due to **the act of sending** via a web-based e-mail service: *files*, *links*, and other stored by the web browser
  - **Web server** *access logs*, *IP addresses*, and possibly *the entire message* in the sent mail folder of the offender's e-mail account
- **Computer intrusion** case:
  - Multiple **traces** of their presence throughout the environment, including in the **file systems**, **registry**, **system logs**, and **network-level logs**
  - **Transferred elements** of the crime scene back with them, e.g. *stolen user passwords*, *PII* in a file or database

How About Tech-Savvy Offenders?

- Even tech-savvy offenders often make ***basic errors***
- An example: going to some lengths to keep their **browsing anonymous** (e.g. with **Tor**), but then using their ***clear*** **home/work connection** to check a web page or send an email
- A sample actual case: **J. Oquendo (a.k.a. "Bobby" or "Sil")**
  - A **computer security specialist**
  - Installed **a sniffer** program to find out a user's password
  - Then used the **user's credential** to break into the **second target system**, grabbed the password file, **deleted the company database**, and left the message: "*Hello, I have just hacked into your system. Have a nice day.*"
  - Was sentenced to 27 months and ordered to pay $96,385 in restitution

Theories of Digital Forensics & Digital Investigation

Theories of Digital Forensics & Digital Investigation

- Palmer
- McKemmish
- Dittrich/Brezinski
- DFRWS
- NIST
- Casey
- Martini, Choo
- …

Palmer (2001)

- The digital forensic information must possess the following **characteristics**:
  - **Relevant** and/or **material**:
    Will this information assist decision-makers in their tasks?
  - **Credible** and/or **competent**:
    Is the information believable, trustworthy, and true and, if so, by what measure?

McKemmish (1999)

- The **identification** of digital evidence
- The **preservation** of digital evidence
- The **analysis** of digital evidence
- The **presentation** of digital evidence

- Rule 1 — **Minimal handling** of the original
- Rule 2 — Account for **any change**
- Rule 3 — Comply with the **rules of evidence**
- Rule 4 — Do not exceed your knowledge

Dittrich/Brezinski (2000)

- Formulate **plan**
- Approach and **secure** the digital crime scene
- **Document** digital crime scene layout
- **Search** for digital evidence
- **Retrieve** digital evidence
- **Process** digital evidence

Digital Forensics Research Workshop Model (Palmer 2001)

DFRWS' **investigative model**:

- Identification
- Preservation
- Collection
- Examination
- Analysis
- Presentation

NIST Digital Forensics Process (Kent et al. 2006)

NIST's **digital forensics process**:

- Collection
- Examination
- Analysis
- Reporting

(Reference: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-86.pdf)

Casey (2004)

Casey's **digital investigation process model**:

- Preliminary & considerations
- Planning
- Recognition
- Preservation, collection & documentation
- **Examination**: the process of *extracting* and *viewing* information from the evidence, and making it available for analysis
- **Analysis**: the application of the scientific method and critical thinking to address the fundamental questions of 5WH in an investigation
- Classification, comparison & individualization
- Reconstruction
- Reporting

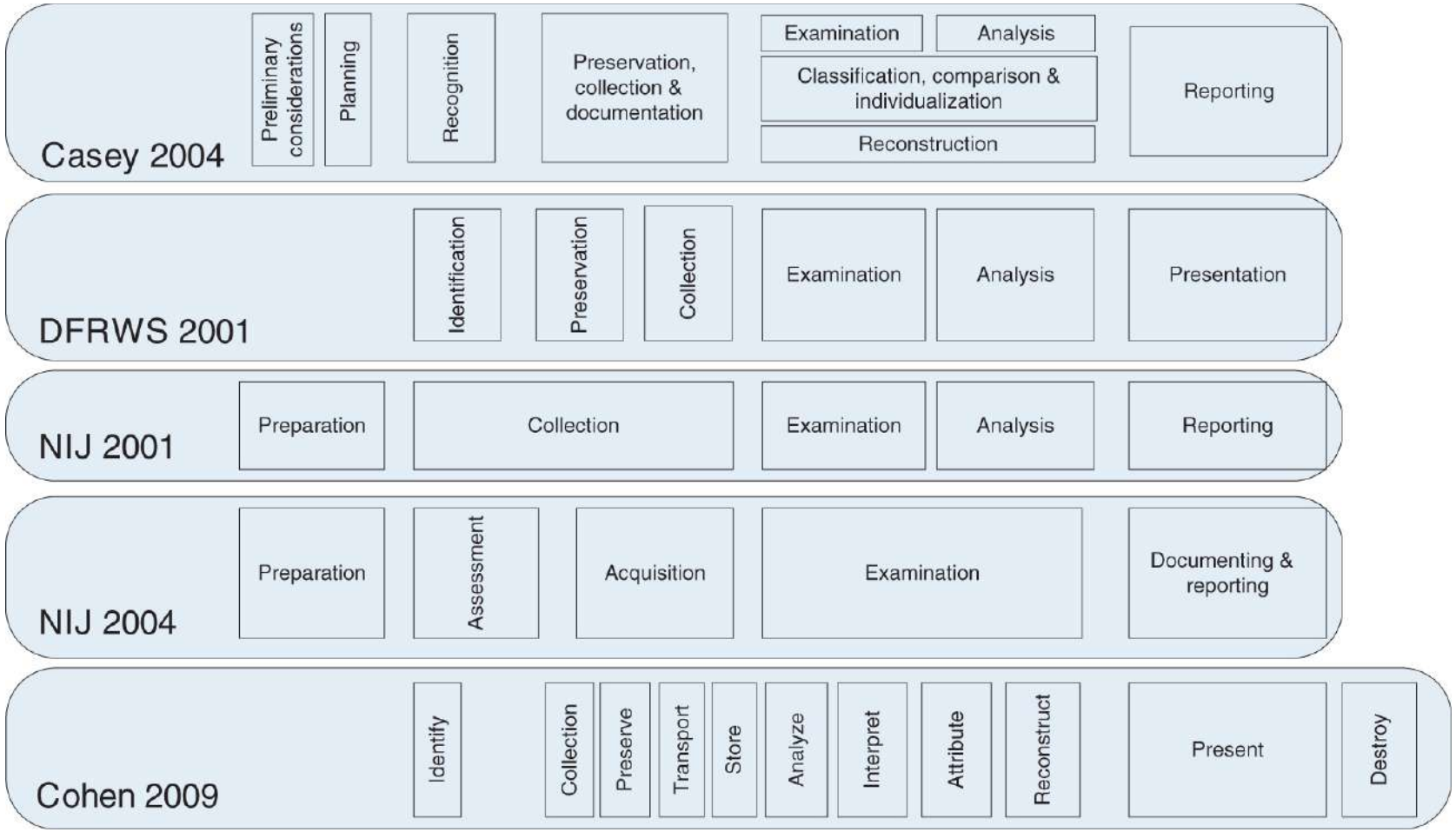


FIGURE 6.1 A comparison of terminology related to digital investigation process models.

Digital Forensics for Cloud (Martini, Choo 2017)

Table 1
Digital forensic framework comparison.

Our proposed framework	NIST framework (Kent et al., 2006)	McKemmish (1999) framework
1. Evidence source identification and preservation	1. Collection	1. Identification 2. Preservation
2. Collection		3. Analysis[a]
3. Examination and analysis	2. Examination 3. Analysis	
4. Reporting and presentation	4. Reporting	4. Presentation

Iterative

Your Tasks as a Digital Forensics Expert Witness

Usually, as a digital forensics expert witness, you are asked to perform the **following tasks**:

- Perform **digital investigation**: to confirm or refute the existence of an incident
- **Testify** the scientific basis of findings, analyses, and conclusions in court: need to follow the procedures of the court

These tasks, including those listed in previous digital forensics **process models**, are only *parts* of a ***case/incident resolution process***: see the next slide

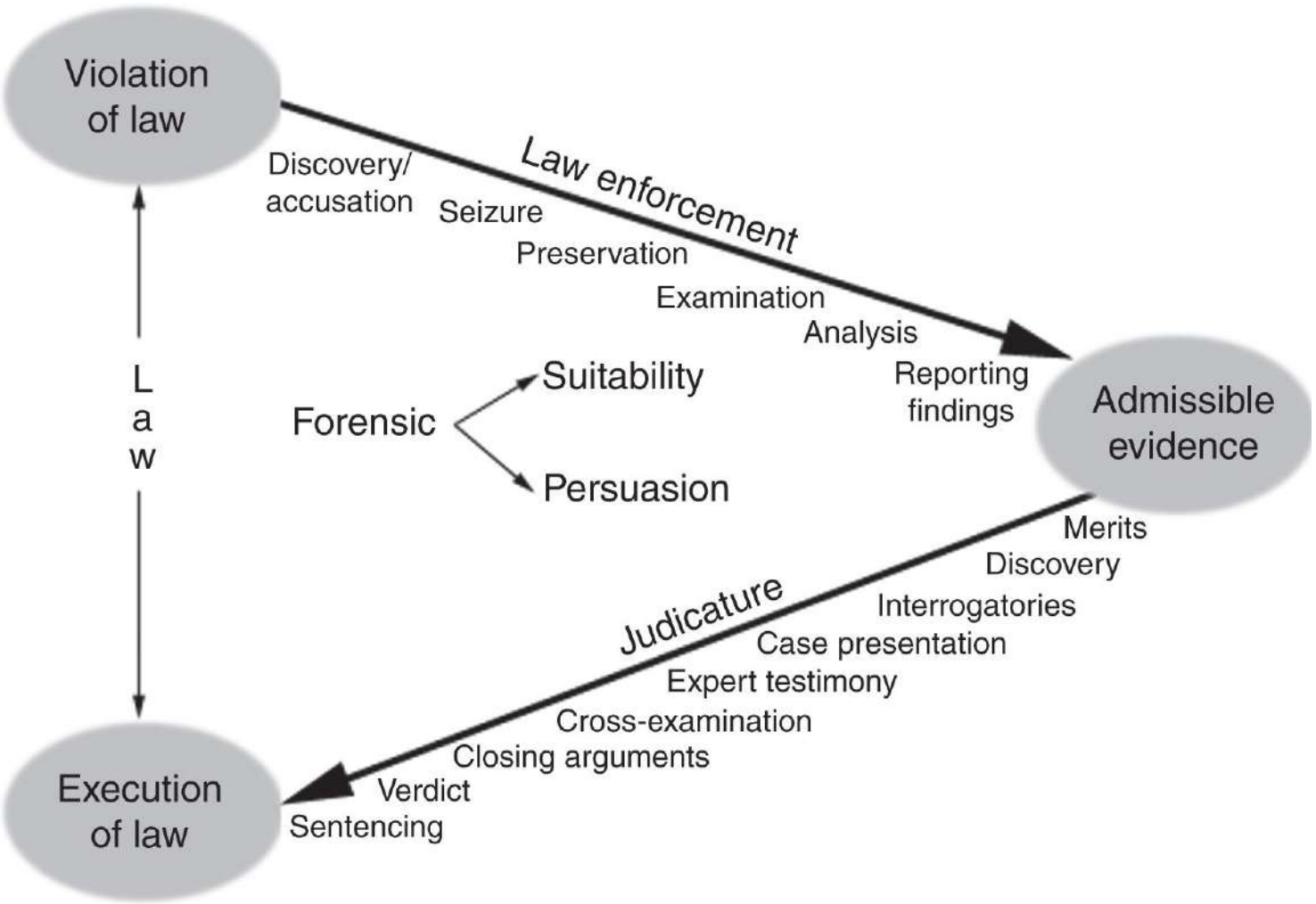


FIGURE 3.1 Overview of case/incident resolution process.

DF Investigation Goal: Crime Reconstruction

- **Crime (scene) reconstruction**:
  the process of determining **the most likely hypothesis**, or **sequence of events**, through the application of the **scientific method**
- **5WH** defines the objectives of an investigation as:
  Who, What, Where, When, Why, How
- Some **main aspects** of analysis:
  - **Temporal** (related to time)
  - **Relational** (relationships of people and objects)
  - **Functional** (conditions necessary for the crime to occur)
  - **Victimology** (victim's characteristics)
  - Crime scene **characteristics**

Types of Digital Forensics Investigations

- **Public/criminal** investigation:
  - A violation of state/federal/international law
  - **Examples**: homicide, drug dealing, child pornography, sexual exploitation
  - **Conducted** by: law enforcement team
  - **Based on**: the applicable criminal law
  - **Supported by**: a warrant
- **Private/corporate** investigation:
  - A violation of company/organization policy
  - **Examples**: IP theft, industrial espionage, sabotage, asset embezzlement, data falsification, email harassment
  - **Conducted by**: corporations, institutions/organizations
  - **Based on**: the applicable civil law, organizational policies
- The **boundary** between the two ***can*** *be* blurry:
  a private investigation can become, or lead to, a public investigation
- Reference: "Prosecuting Computer Crimes",
  https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf

Notes on Private/Corporate Investigation

- The need for "***line of authority***" in conducting an investigation
- An ***investigation request*** can be issued by some designated units: corporate ethics office, internal auditing, legal department
- ***Authorized requester*** (e.g. Chief Information Security Officer): has the power to **initiate** an investigation in a **company**
- Corporate investigations can often turn into **criminal investigations**
- The ***Federal Rules of Evidence*** **(FRE)**:
  - A collection of laws that determine **what can or cannot be admitted** into evidence in a **federal courtroom**
  - Applies to **both types** of investigations
  - References: https://www.law.cornell.edu/rules/fre, https://en.wikipedia.org/wiki/Federal_Rules_of_Evidence

Enterprise Theory of Investigation (ETI)

- When looking at a crime incident, the ***ETI*** can be useful
- Looks at **each separate incident** as possible **part of *an ongoing series of activities*** by a particular enterprise or organization
- A **criminal organization**: a group of individuals with an identified hierarchy engaged in significant criminal activity
- Rather than viewing criminal acts as isolated crimes, the ETI attempts to show that **individuals** commit crimes in furtherance of the **criminal enterprise** itself
- Encourages a **proactive attack** on the structure of the criminal enterprise

Role of Hardware & Information in a Crime/Breach

Computer Crime

- Several possible **terms**:
  - *Computer crime*
  - *Computer-related crime*
  - *Cybercrime*:
    any conduct proscribed by legislation or common law that involves **the use of**, **or against**, **digital technologies** is in general classified as ***cybercrime*** (Smith, Grabosky, & Urbas, 2004)
  - Reference: https://eprints.qut.edu.au/43400/1/Ali_Alkaabi_Thesis.pdf
- *Question*: a computer is related to a crime, but how exactly?
- It comes down to ***role of hardware or information*** in the crime/breach

Electronic & Digital Evidence

- **Hardware** (***electronic evidence***):
  all of the physical components of a computer
- **Information** (***digital evidence***):
  the **data** & **programs** that are stored on and transmitted using a computer

- ***How are hardware and information used in a crime/breach?***
- ***What are their <u>roles</u>?***

Role of Hardware & Information in a Crime/Breach

- Possible **roles**:
  - **Contraband**: a property that the private citizen is **not** permitted to **possess**
  - **Fruits of crime**: property that was **obtained** by criminal activity
  - **Instrumentality**: Hardware/information that has played a **significant role** in a crime to **victimize** someone or other computers/devices
  - **Evidence**: Hardware/information is or captures **evidential information**
- Note that the roles are ***not*** intended to be mutually exclusive:
  - E.g., when a computer is instrumental in committing a crime, it usually contains evidence of the offense
  - See also Casey's *Digital Evidence and Computer Crime*, 2011
  - Yet, it's probably **good/clearer** to **separate** computer/mobile and its storage!

Role of Hardware

- Hardware as **contraband**:
  e.g. a computer that is a repository of data that is contraband (such as child pornography), cloned cellular phones and the equipment used to clone them, *hardware for intercepting communications*
- Hardware as **fruits of crime**:
  e.g. computer equipment stolen/purchased using stolen credit card numbers, stolen microprocessors
- Hardware as an **instrumentality**:
  e.g. computer used as a tool to hack into websites, distribute copyrighted videos, or produce illegal pornography;
- Hardware as **evidence**:
  e.g. a *scanner* used to digitize child pornography, which has **unique scanning characteristics** that link the hardware to the digitized images

Role of Information

- Information as **contraband**:
  e.g. banned encryption software, child pornography images
- Information as **fruits of crime**:
  e.g. illegal copies of computer programs, stolen trade secrets & passwords, and any other information that was obtained by criminal activity.
- Information as an **instrumentality**:
  e.g. programs that computer intruders use to break into computer systems (exploits), keyloggers
- Information as **evidence**: all forms of relevant digital trails

Role of Hardware or Information - Casey (2004)

	Contraband	Fruits of Crime	Instrumentality	Evidence
Hardware	Cloned mobile telephones, or hardware for intercepting communications	Stolen computers, or equipment purchased with stolen credit card	Printer used to produce counterfeit banknotes, or scanner used to produce child pornography	Mobile phone may be evidence of parole violation even if it was not used to deal drugs
Information	Digital photographs or videos of child exploitation, or strong encryption in some countries	Valuable data stolen from computers such as bank account details	Programs used to break into computers and capture passwords	A personal diary on a computer describing details of a crime, or log files showing criminal activity

Pop Quizzes!

Pop Quiz 1

An instrumentality of a crime (in general Forensics) is:

a) An instrument used to commit a crime
b) A weapon or tool designed to commit a crime
c) Anything that is plays a significant role in committing a crime
d) All of the above

Pop Quiz 2

Contraband can include:

a) Child pornography
b) Devices or programs for eavesdropping on communications
c) Illegal encryption devices or applications
d) All of the above

Pop Quiz 3

A cloned mobile telephone is an example of:

a) Hardware as Contraband or Fruits of Crime
b) Hardware as an Instrumentality
c) Hardware as Evidence
d) Information as Contraband or Fruits of Crime
e) Information as an Instrumentality
f) Information as Evidence

Pop Quiz 4

Digital photographs or videos of child exploitation is an example of:

a. Hardware as Contraband or Fruits of Crime

b. Hardware as an Instrumentality

c. Hardware as Evidence

d. Information as Contraband or Fruits of Crime

e. Information as an Instrumentality

f. Information as Evidence

Pop Quiz 5

Computer equipment purchased with stolen credit card information is an example of:

a) Hardware as Contraband or Fruits of Crime
b) Hardware as an Instrumentality
c) Hardware as Evidence
d) Information as Contraband or Fruits of Crime
e) Information as an Instrumentality
f) Information as Evidence

Pop Quiz 6

Stolen bank account information is an example of:

a. Hardware as Contraband or Fruits of Crime

b. Hardware as an Instrumentality

c. Hardware as Evidence

d. Information as Contraband or Fruits of Crime

e. Information as an Instrumentality

f. Information as Evidence

Pop Quiz 7

A network sniffer program is an example of:

a. Hardware as Contraband or Fruits of Crime

b. Hardware as an Instrumentality

c. Hardware as Evidence

d. Information as Contraband or Fruits of Crime

e. Information as an Instrumentality

f. Information as Evidence

Pop Quiz 8

A printer used for counterfeiting is an example of:

a. Hardware as Contraband or Fruits of Crime

b. Hardware as an Instrumentality

c. Hardware as Evidence

d. Information as Contraband or Fruits of Crime

e. Information as an Instrumentality

f. Information as Evidence

Pop Quiz 9

Phone company records are an example of:

a. Hardware as Contraband or Fruits of Crime

b. Hardware as an Instrumentality

c. Hardware as Evidence

d) Information as Contraband or Fruits of Crime

e) Information as an Instrumentality

f) Information as Evidence

Pop Quiz 10 (*Rather Interesting!*)

A "mobile phone" that was used to record upskirt videos and also store the videos is an example of:

a. Hardware as Contraband or Fruits of Crime

b. Hardware as an Instrumentality

c. Hardware as Evidence

d) Information as Contraband or Fruits of Crime

e) Information as an Instrumentality

f) Information as Evidence

Looking at Applications of Digital Forensics: Sample Cases

Applications of Digital Forensics: Sample Cases

- Digital forensics is used in ***varied situations*** & environments: industry, government, law enforcement
- Let's look at some case studies of the use of digital forensics to get a better picture of that ***diversity***
- Also to see some **applications** of **Locard's Exchange Principle** to cases involving digital evidence

Case 1: Microsoft Anti-Trust Case (Cir. 2001)

- Microsoft was accused of **holding a monopoly** and engaging in ***anti-competitive practices***
- The plaintiffs alleged that Microsoft had abused monopoly power on Intel-based PCs in its handling of **OS and web browser sales**
- See: https://en.wikipedia.org/wiki/United_States_v._Microsoft_Corp

From: Paul Maritz
Sent: Tuesday, July 29, 1997 5:29 PM
To: Jim Allchin (Exchange)
Subject: FW: Security as a lock in

fyi

----Original Message----
From: Yacov Yacobi
Sent: Wednesday, July 23, 1997 5:29 PM
To: Nathan Myhrvold; Bill Gates
Cc: Paul Maritz; Butler Lampson; Dan Ling; Rick Rashid; Gregory Faust
Subject: RE: Security as a lock in

Shipping every NT with a unique identifying smart card will do. Else, we can challenge whoever claims to be NT to tell the content of some random line of the NT code – that'll force him to have a complete NT. Real life is messier (different versions, etc.). Will look into it.

Yacov

----Original Message----
From: Nathan Myhrvold
Sent: Wednesday, July 23, 1997 3:52 PM
To: Bill Gates
Cc: Paul Maritz; Butler Lampson; Yacov Yacobi; Dan Ling; Rick Rashid; Gregory Faust
Subject: RE: Security as a lock in

I agree that this seems very possible. There are many customer benefits to having system components that can interact after establishing trust via authentication. We will look into it.

Nathan

----Original Message----
From: Bill Gates
Sent: Wednesday, July 23, 1997 2:53 PM
To: Nathan Myhrvold
Cc: Paul Maritz
Subject: Security as a lock in

I believe as we evolve our security capabilites there must be some way to set this up so that our operating systems have shared secrets with each other that make them work better with each other than with otheroperating systems - whether its JAVAOS layered on top of us or clones or anything else.

I think we need to make this an explicit goal of our security strategy.

Email as a Cross Examination Tool

- "It's like the gift that keeps on giving," said Tom Greene, a deputy attorney general in California, one of the states suing Microsoft Corp. in an antitrust case built largely on **computer messages**. "*People are so chatty in e-mail.*" (CBS News 2001)

- Gates was shown **an email** sent to him by Brad Chase, a Microsoft vice president, on March 13, 1997, that said, "*We need to continue our jihad next year. … Browser share needs to remain a key priority for our field and marketing efforts.*" (CNN 1998)

Bill’s Video Testimony

“Early rounds of his deposition showed him offering obfuscatory answers and saying 'I don't recall' so many times that even the presiding judge had to chuckle.
Worse, many of the technology chief's denials and pleas of ignorance have been **directly refuted** by prosecutors **with snippets of E-mail Gates both sent and received**."
(Business Week 2008)

Case 2: Brad Cooper Murder Trial

- In 2008, Brad Cooper (a Cisco engineer) and his wife were having marital problems
- One morning in 2008, **Nancy** went out running and **never came back**
- She had been strangled, and the police found her body in a nearby park
- Artefacts indicating **a Google map search** showing the location of body was found **on Cooper's work laptop**
- The handling of that laptop was challenged by defense Digital Forensic experts

Case 3: Collar Bomb

- On 3 August 2011 **a hooded man** walked into the $12 million Sydney home of 18-year-old **Madeleine Pulver** and tied a **black metal box** around her neck with a bike chain and a note saying it was a **bomb**
- A Google **Gmail account** dirkstraun1840@gmail.com was placed on a note attached to Ms Pulver's neck
- The account was created as a way of Ms Pulver's family **contacting the attacker** to hand over a sum of money and was set up

Case 3: Collar Bomb

- The account had been established on 30 May 2011 from **an IP address** linked to Chicago Airport
- The **first access** took place at 4.09pm on 3 August from an **IP address** registered to **Kincumber Library in NSW**
- The next two times it was accessed was at 5.25pm and again at 5.51pm, from an **IP address** registered to the Avoca Beach Video Shop

Even More Interesting/Strange Cases

- Cyber attack on **court computer system** (Sullivan, 2003):
  - **William Grace** and **Brandon Wilson** broke into **court systems** in Riverside, California, **to alter records** relating to previous charges filed against him that the charges had been dismissed
  - They could recall warrants, change court records, dismiss cases, and read e-mail of county employees in most departments, including the Board of Supervisors, Sheriff, and Superior Court judges
  - They were sentenced to **9 years in jail**
- **Virtual-world attack**:
  - A Japanese woman was charged with illegal computer access, after she gained **unauthorized access** to a **coworker's online account to destroy his online avatar** (Yamaguchi, 2008)

Applications of Digital Forensics: Summary

- As can be seen, digital forensics is **not** just the domain of law enforcement
- Our **increasing digital/cyber footprint** and the ubiquity of the Internet are seeing to that
- Also the application of **Locard's Exchange Principle** involving digital evidence

Digital Forensic Career Options

Digital Forensic Career Options

- **Digital Forensic (DF) Investigator** in:
  - Law enforcement
  - Government departments
  - Other investigative agencies
  - Forensic consulting firms
  - Large/medium sized banks
  - Large/medium sized organisations with high reliance on IT
  - Organsiations in high risk industries (defence, high tech, etc.)

http://fbi.gov

Digital Forensic Investigator: Specialization

- Identification, preservation, collection and acquisition of digital evidence can be quite complex
- A degree of **specialization** of **Digital Forensics Investigators**
- ***Digital Evidence First Responder (DEFR)***:
  - Has the skill and training to **arrive on an incident scene**, assess the situation, and take precautions to **acquire and preserve evidence**
  - May need to deal with possible hostile work environment, including relevant possible hazmat (hazardous materials)
- ***Digital Evidence Specialist (DES)***:
  - Has the skill to **analyse** the data, and also to determine when additional specialists are needed

Digital Forensic Career Options

- **Incident Responder (IR)** in:
  - National CERT teams: SingCERT
  - Mid range to large IT divisions within organizations
  - Specialist IR firms (i.e. Mandiant)
  - Managed security service providers
  - Consulting firms
  - Independent security contractors

CERT Australia

Digital Forensic Career Options: Related Roles

- **IT security management or IT risk management**
- **Corporate security**
- **Litigation support**

ESPN LOG IN

NFL Home News Scores Schedule Standings Stats Teams Playoffs More

NFL hiring a new director of digital forensic investigations

Darren Rovell
ESPN Senior Writer

30 Jun, 2015

Looking to bolster how it handles off-the-field incidents, the NFL is adding a new position: Director of Digital Forensic Investigations.

The job description, posted online by the league late last week, says that the new position within the security department will include "conducting or coordinating, supervising and managing detailed and complex investigations involved alleged impropriety or criminal conduct by League and Club personnel." The specific position will focus on dealing with "evidence concerning social media, computers, telephones and mobile devices."

NFL spokesman Brian McCarthy acknowledged that the position was newly created as "part of our enhanced personal conduct policy that includes more robust internal investigative procedures."

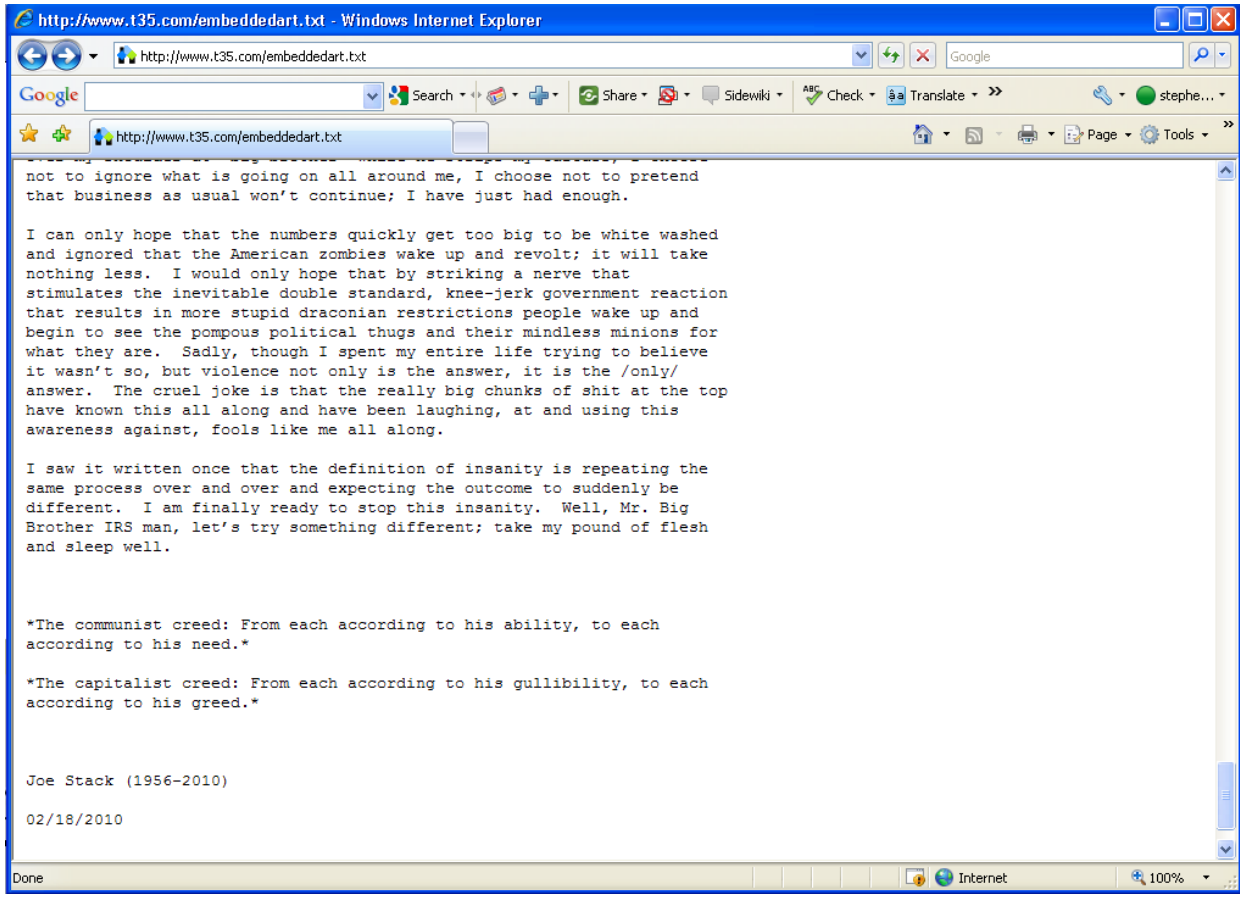
Your Post-Lecture Reading

For Your Offline Reading before Lecture 2

- **Case**: "*2010 Austin suicide attack*" (https://en.wikipedia.org/wiki/2010_Austin_suicide_attack#Suicide_note)
- **Andrew Joseph Stack III** deliberately crashed his single-engine Piper Dakota light aircraft into Building I of the Echelon office complex in Austin, Texas, killing himself and IRS manager Vernon Hunter
- Watch this **video**: https://www.youtube.com/watch?v=utPdWo3vpnE

For Your Offline Reading before Lecture 2

- Prior to the crash, **Stack had posted a note** referring to "greed", "insanity", and the IRS, dated February 18, 2010, to his business website embeddedart.com



For Your Offline Reading before Lecture 2

- Some questions to ponder and answer:
  1. What issues do you think **digital evidence might assist** to establish in this incident?
  2. What are the ***potential sources*** of that digital evidence?

Lab 1: Setting up Your Forensic Workstations

(Please refer to your **Lab 1** and uploaded **"Lecture 1 Supplement**" slide deck)

Your TO-DO for Lab 2:

Get a USB thumb drive with 1-4GB capacity for your next week's lab!

Questions?
See you next week!