CS 798: Digital Forensics and Incident Response

Lecture 1 - Introduction

Diogo Barradas

Winter 2025

University of Waterloo

Outline

1. Logistics
2. Overview
3. Our First Case Study

Logistics

Instructors

Diogo Barradas

- diogo.barradas@uwaterloo.ca
- https://cs.uwaterloo.ca/~dbarrada/
- Office hours: Mondays 2:00–3:00 pm (or by appointment)

Lecture times: 9:30–10:50 am in MC 2568
No classes: Feb 17th, 19th (Reading Week)

Course Mechanics

- Campus and CS VPNs: remote working
- LEARN: Assignments, submissions, etc.
- Piazza: Q&A, general discussions
- Course website: syllabus, public materials

Communication Channels

- Important course announcements will be made on Piazza.
  - Please keep up with the information there.
- Use discussion forums in Piazza for all communication
  - Use a private question for questions not of general interest
- Use email only as a last resort and then it must be from your uwaterloo.ca email address
- Some communication might be sent to your uWaterloo email
  - Check your uWaterloo email account regularly or have email forwarded to your regular account

Course Syllabus

- You are expected to be familiar with the course's syllabus
- Available on the course website
- If you haven't read it, read it after this lecture

What is our goal in this course?

- Upon completing this course, students are expected to:
  - Understand the basics of digital forensics principles
  - Acquire hands-on practice on digital forensics investigation
  - Learn how to respond to, remediate, and report a cybersecurity incident
  - Be prepared for active research on the field

What this course will not provide

- Describe how computers and networks work
- Make of you an experienced forensics analyst
  - You'll need "many years turning chicken"
- Cover all existing forensic tools and evidence sources
- Dive (deeply) into the legal aspects involved in digital forensics

Grading Scheme

- Assignments ($3 \times 20\% = 60\%$)
  - Work in pairs (Group formations due Jan 15th 3pm)
- Final Exam (40%)
- See syllabus for late and reappraisal policies, academic integrity policy, and other details

Assignments

- Focus on completing different steps of a digital forensics investigation
- You will interact with (simulated) sources of evidence
- Deliverables:
  - Expect to have 1 assignment every 4 weeks (roughly).
  - Assignments will be due at 3pm Waterloo time.
  - Late submissions will be accepted with a 20% penalty for each day elapsed.

Final Exam

- Covers the entire syllabus
- Must have a minimum of 45% to pass the course
- Don't panic

Plagiarism and Academic Offenses

- We take academic offenses very seriously
- Nice explanation of plagiarism online
  - `https://uwaterloo.ca/math/academic-matters/academic-integrity`
- Read this and understand it
  - Ignorance is no excuse!
  - Questions should be brought to instructor
- Plagiarism applies to both text and code.

Plagiarism (2)

- Common mistakes
  - Excess collaboration with other students
  - Using solutions from other sources
  - Asking public questions containing (partial) solutions
  - Posting (partial) solutions to websites (e.g., github)
- Penalties for graduate students are severe
- More information linked to from course syllabus

Primary Bibliography

- Books:
  - **Digital Evidence and Computer Crime, 3rd edition**, Eoghan Casey, Academic Press, 2011.
  - **File system forensic analysis, 1st edition**, Brian Carrier, Safari Tech Books Online, 2005.
  - **Incident Response & Computer Forensics, 3rd edition**, Jason Luttgens, Matthew Pepe, Kevin Mandia, McGraw-Hill, 2014.

- Digital copies are available via the library website (see Course Reserves on LEARN).
- You are expected to know all the material presented in class, even if it's not in the textbooks.

Secondary Bibliography

- Books:
  - **Practical Mobile Forensics, 4th Edition**, Rohit Tamma, Oleg Skulkin, Heather Mahalik, Satish Bommisetty, Packt Publishing, 2020.
  - **Cloud Storage Forensics, 1st edition**, Darren Quick, Ben Martini, Kim-Kwang Raymond Choo, Syngress, 2014.
  - **Information Hiding: Steganography and Watermarking - Attacks and Countermeasures, 1st edition**, Neil F. Johnson, Zoran Duric, Sushil Jajodia, Springer, 2001.
  - **Information Hiding in Communication Networks: Fundamentals, Mechanisms, Applications, and Countermeasures, 1st edition**, Wojciech Mazurczyk, Steffen Wendzel, Sebastian Zander, Amir Houmansadr, Krzysztof Szczypiorski, Wiley, 2016.

Other readings

- There will be additional assigned readings for each class.
  - These will be linked to from the course web page.
- These will mostly consist of research papers related to the lectures' content.

A Note on the Acquired Skillset

- In this course, you will be exposed to information and tooling on computer and network forensics.
- To be clear, you are not to use this or any similar information to conduct a digital forensic analysis on any device, system, or network without the express consent of the owner.
  - a.k.a., the Spider-Man rule.
- You will comply with all applicable laws and University policies.
- See syllabus for more details.

Outline

1. Logistics
2. Overview
3. Our First Case Study

Overview

Digital Forensics

It's all about following a digital trail

- Personal files and browsing history are stored on your desktop, mobile, and cloud services like Google Drive.
- When you log in to websites with Google Sign-In, your behavior can be linked to your real name or email address.
- Everything you browse and buy on sites like Amazon or you post on Facebook is recorded forever.
- Mobile devices leaves traces: the calls you make, your location, etc.
- Can you think of something else?

It's all about following a digital trail

- Personal files and browsing history are stored on your desktop, mobile, and cloud services like Google Drive.
- When you log in to websites with Google Sign-In, your behavior can be linked to your real name or email address.
- Everything you browse and buy on sites like Amazon or you post on Facebook is recorded forever.
- Mobile devices leaves traces: the calls you make, your location, etc.
- Can you think of something else?

Question:

Can these trails be used as evidence in court of law?

They sure can!

Mashable

Facebook Pic of Police Car Gas-Siphoning Leads to Arrest

6.7k SHARES Share Tweet +

BY TODD WASSERMAN
APR 19, 2012

A Kentucky man landed in jail after posting a picture of himself on Facebook siphoning gas from a police car.

Burglar leaves his Facebook page on victim's computer

September 16, 2009
By Edward Marshall, Journal Staff Writer

Save |

MARTINSBURG - The popular online social networking site Facebook helped lead to an alleged burglar's arrest after he stopped check his account on the victim's computer, but forgot to log out before leaving the home with two diamond rings.

Busted! Cops arrest teenager after she posted a picture of pot on Instagram

2

Computerworld | Sep 9, 2013 6:51 PM PT

"Marijuana" is one of about 400 "hot" keywords that are monitored by government agencies on social media. Social media monitoring is not new, but apparently some people either do not know about open-source intelligence (OSINT), or choose to disregard the list of terms in the Department of Homeland Security National Operations Center Media Monitoring Capability Desktop Reference Binder. So what might happen if you post a picture of big fat bud of pot on Instagram? Busted!

On a more serious note...

We joined Discord, the network where the FBI discovered the young man that planned a murder at the University of Lisbon

João Guerreiro Rodrigues | Nuno Mandeiro

12 Feb 2022, 18:00

An 18-year-old young man, who has since been detained, wanted to kill "as many people as possible" at the Faculty of Science at the University of Lisbon. The plan would be put into practice this Friday, February 11th. It was stopped by the Judiciary Police, who had received an alert from the FBI

Fitbit Used as Key Evidence in Murder Case

September 14th, 2017 | Tags: crime, fitbit, Internet of Things, iot

Connecticut police have used a woman's FitBit data to disprove her husband's story and subsequently charge him in her murder.

Murder solved by Alexa: Domestic abuser who killed his wife is jailed for life with 20-year minimum term - after voice recordings on Amazon device helped bring him to justice

- **Daniel White, 36, murdered Angie White, 45, at her home in Swansea, Wales**
- **Amazon's Alexa saved audio recordings of White at the time of the murder**

By ALEXANDER BUTLER
UPDATED: 16:58 BST, 24 March 2023

On a more serious note... (2)

Child Porn-Filled Hard Drive Flushed Down Toilet Recovered By FBI In Round Hill

Despite his best efforts to cover up his misdeeds, a Virginia man will spend years behind bars after being busted by federal officials with a hard drive filled with child pornography.

NEWS

Insecure wheels: Police turn to car data to destroy suspects' alibis

They returned to French's 2016 black Chevy Silverado pickup truck, which had been stolen around the time he vanished, and discovered time-stamped recordings of someone else's voice using the hands-free system to play Eminem on the radio at the time of French's murder.

The voice, according to the police report obtained by NBC News, belonged to Joshua Wessel, now 32, who used to tinker on cars and motorcycles with French. Wessel's voice was identified by relatives, including his wife, key evidence that allowed investigators to reconstruct his movements and the final hours of French's life, the police report says. In July, Wessel was arrested and charged with French's murder. He has pleaded not guilty and is awaiting trial subject to psychiatric assessment.

Should we always trust digital evidence?

'Deepfake' audio evidence used in UK court to discredit Dubai dad

▶ Doctored recording was intended to deliberately paint Emirates resident as a danger to his family

Byron James, a lawyer at Dubai firm Expatriate Law. Antonie Robertson / The National

People are trying to claim real videos are deepfakes. The courts are not amused

May 8, 2023 · 5:01 AM ET

Heard on All Things Considered

Shannon Bond

A Hacker Group Has Been Framing People for Crimes They Didn't Commit

A recent study shows the tactics and techniques of a cybercrime group that is known for planting incriminating evidence on the devices of activists in India.

By **Lucas Ropek** Published February 11, 2022 | Comments (41)

What is digital forensics?

- Branch of forensic science concerned with the proper acquisition, preservation and analysis of digital evidence, typically after an unauthorized access or use has taken place.

What is digital evidence?

- Digital evidence is any probative information stored or transmitted in digital form that a party to a court case may use at trial.
  - e.g., emails, digital photos, ATM transaction logs, databases, call logs, network traces, social network activity, etc.
- The goal of digital forensics is to explain the current state of a digital artifact.

Relevant actors in the forensics process

- **Forensic analysts / investigators**
  - Collect, preserve, analyze, and present digital evidence
- **Forensic tool developers**
  - Develop forensic tools for investigations
- **Digital forensic researchers**
  - Devise new techniques for investigators and tool developers

Uses of digital forensics

- **Criminal prosecutors**
  - Rely on evidence obtained from a computer to prosecute suspects and use as evidence
- **Civil litigations**
  - Personal and business data discovered on a computer can be used in fraud, divorce, harassment, or discrimination cases
- **Insurance companies**
  - Evidence discovered on computer can be use to lessen costs (fraud, worker's compensation, arson, etc.)

Uses of digital forensics

- **Private corporations**
  - Obtained evidence from employee computers can be used as evidence in harassment, fraud, and embezzlement cases
- **Law enforcement officials**
  - Rely on computer forensics to backup search warrants and post- seizure handling
- **Individual / private citizens**
  - Obtain the services of professional computer forensic specialists to support claims of harassment, abuse, or wrongful termination from employment

Incident Response

What is an incident?

- **Definition by NIST**: An incident is a "violation or threat of violation of computer security policies, acceptable use policies, or standard security practices"

How bad do incidents look today?

- In practice, intrusions are getting more complex over time:
  - May include hundreds of (geographically dispersed) compromised systems
  - Attackers increasingly use anti-forensic techniques
  - Attackers use multiple tactics to access computer systems
- The **goals of an incident response** may vary, depending on:
  - Severity of the incident, the victim's needs, the timing of the incident, the intent of the attack group, the industry or customers impacted, etc.

Why should we care?

- Many attacks now have a broad scope, affecting the private and public sectors, as well as individual citizens
- Cyber-criminals operate with little risks or repercussions
- Digital investigations get increasingly more complex, requiring incident responders to understand how to normalize, parse, and make sense of large amounts of data

What is incident response?

- **Incident response** is a coordinated and structured approach to go from incident detection to resolution. It includes:
  - Confirm whether or not an incident occurred
  - Provide rapid detection and containment
  - Determine and document the scope of the incident
  - Minimize disruption to business and network operations
  - Restore normal operations
  - Manage the public perception of the incident
  - Allow for criminal or civil actions against perpetrators
  - Enhance the security posture of a compromised entity

Course Modules

1. The digital investigation process
2. File system forensics
3. Memory forensics
4. Network forensics
5. Anti-forensic techniques
6. Mobile and cloud forensics
7. Incident response

Our First Case Study

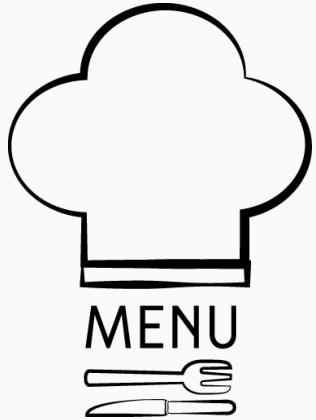
The Tea Room Case [1]

- Natasha Romanov (former secret agent) has retired and opened a new Russian Tea Room in Moscow.

[1] Inspired on Jim Lyle's (NIST) "Overview of Digital Forensics"

The Tea Room Case: A crime suspect

- However, her employee Nick Ulyanov vanished and may have stolen her award winning menu
- The last time he was seen, he was hovering near the computer with a flash drive in his hand
- Natasha suspects that Nick copied her menu to the flash drive and plans to open his own Tea Room with a similar version of the menu



The Tea Room Case: Call the Cops

- Natasha called Andrei Demidov, a digital forensic investigator for the Moscow Police
- Andrei's Chief gives him the department intern, Ivan Durok, with the comment "Be nice to him, try to teach him the skills, and don't let him contaminate the evidence!"
- They get a warrant & storm out to the train station. They catch Nick about to board the express to Saint Petersburg

The Tea Room Case: Call the Cops

- Natasha called Andrei Demidov, a digital forensic investigator for the Moscow Police
- Andrei's Chief gives him the department intern, Ivan Durok, with the comment "Be nice to him, try to teach him the skills, and don't let him contaminate the evidence!"
- They get a warrant & storm out to the train station. They catch Nick about to board the express to Saint Petersburg

Question:

How should Andrei and Ivan proceed?

The Tea Room Case: First Look

- A search of the suspect reveals a flash drive
- The first step was create an exact copy of the flash drive without changing the original
- Bag & Tag - Start chain of custody to document who has the drive forensic image (or copies)

- Ivan wants to take a look, inserts a copy into his laptop and sees no files in it.

The Tea Room Case: First Look

- A search of the suspect reveals a flash drive
- The first step was create an exact copy of the flash drive without changing the original
- Bag & Tag - Start chain of custody to document who has the drive forensic image (or copies)

- Ivan wants to take a look, inserts a copy into his laptop and sees no files in it.

Ivan:

"Looks like there's nothing here..."

Andrei:

"We'll see..."

The Tea Room Case: Caviar, anyone?

- Andrei asks Natasha for menu items that could be searched for
- Ivan uses a forensics tool and searches for "икра" (Caviar)
- The tool returns a hit not located within an allocated file:

```
икра..............................  caviar
```

- Perhaps they can recover the deleted text file with a menu!

The Tea Room Case: Recovered a deleted file!

```
Natasha Romanov's New Little Russian Tea Room
#4 Lubyanka Square, Moscow


ЗАКУСКИ (Appetizers)
икра.............................. caviar
ветчина ..............................ham
грибы ..............................mushrooms
колбаса ..............................sausage
селёдка ..............................herring
-----------------------------------

СУП (Soup)
борщ ..............................borscht
```

The Tea Room Case: Recovered a deleted file!

```
Natasha Romanov's New Little Russian Tea Room
#4 Lubyanka Square, Moscow


ЗАКУСКИ (Appetizers)
икра.............................. caviar
ветчина ..............................ham
грибы ..............................mushrooms
колбаса ..............................sausage
селёдка ..............................herring
-----------------------------------

СУП (Soup)
борщ ..............................borscht
```

Question

What lessons can a novice digital investigator learn from this case?

Lesson #1: We are not judging someone

Ivan:

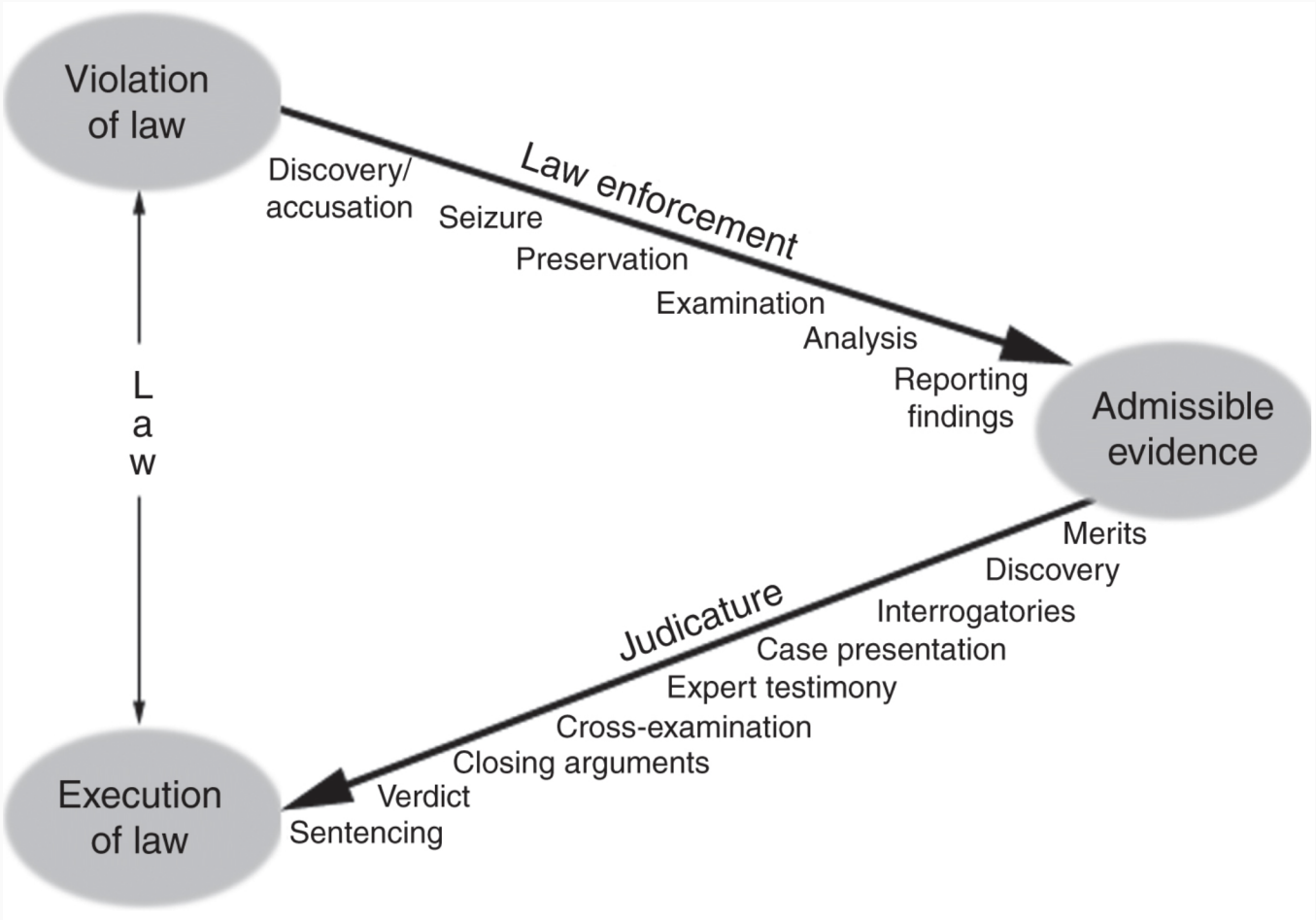
"We have shown that Nick is guilty, right?"

Andrei:

"No, that's not what we do."

- We use our wits and tools to reveal facts. If we try to prove the case one way or the other we will find only what we expect.
- Nick may be guilty or not guilty. This is for the case agent and prosecutor to present to the court. The court decides.
- To be presented before the court, we must follow a rigorous methodology when handling evidence.

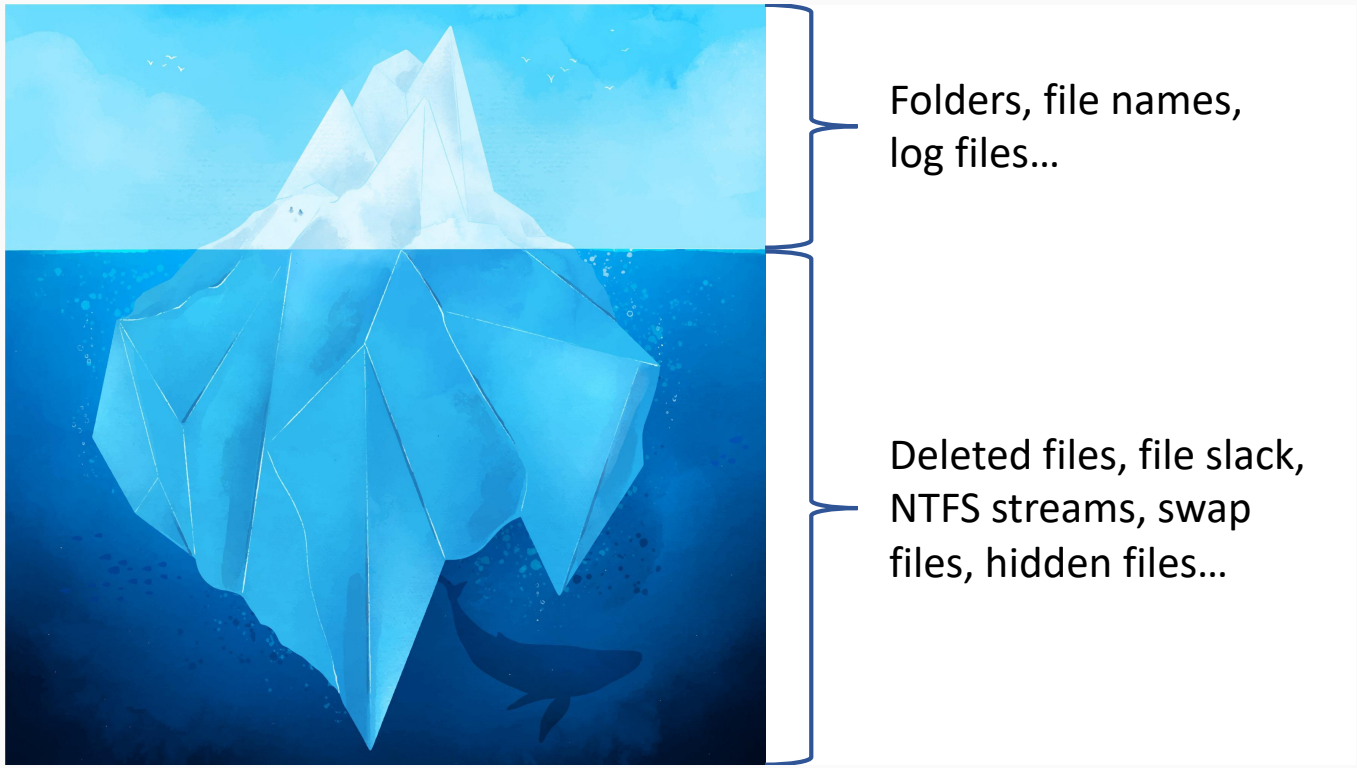
Case/incident Resolution Process



from: Digital Evidence and Computer Crime, Eoghan Casey

Lesson #2: We need to look under the surface

- There's a lot more data contained on a digital artifact than what it may seem at first.



https://www.freepik.com/free-vector/iceberg-illustration-concept_9907610.htm

Lesson #3: We rely on adequate forensic tools

- Use forensic tools to help collect & analyze evidence
  - FTK, foremost, Wireshark, WinHex, Autopsy, Volatility,...

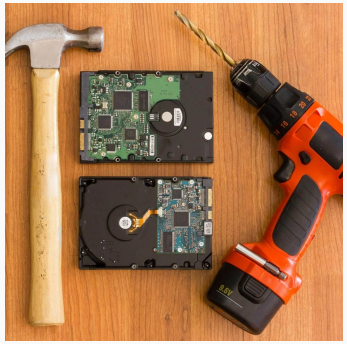
Autopsy® is a digital forensics platform and graphical interface to The Sleuth Kit® and other digital forensics tools. It is used by law enforcement, military, and corporate examiners to investigate what happened on a computer. You can even use it to recover photos from your camera's memory card.

Download Now

- But need to use them right, abiding by the law
  - "With great power comes great responsibility" – Uncle Ben

Lesson #4: Digital forensics is not that easy...

- **Wide variety of devices and types of data**
  - Requires domain expertise
  - Requires techniques for filtering relevant data
- **Data can be incomplete, corrupted, noisy...**
  - Requires know-how to recover and analyze
- **Miscreants make our life harder**
  - Use of steganography, encrypted storage, anonymous communication tools, etc.



Takeaways

- People leave a digital trail everywhere that can be used (in certain circumstances) as evidence in court-of-law.
- Digital forensics is the branch of forensic science concerned with the acquisition, preservation, and analysis of digital evidence.
- Digital forensics requires a systematic investigation procedure which is determined by a legal framework.

Pointers

- **Textbook:**
  - Casey – Chapter 1
- **Other resources:**
  - SWGDE – `https://www.swgde.org/`
  - AAFS – `https://www.aafs.org/`
  - DFRWS – `https://dfrws.org/`
  - SANS – `http://www.sans.org`
- **Acknowledgements:**
  - Slides adapted and extended from Nuno Santos's Forensics Cyber-Security course at Técnico Lisbon