TÉCNICO LISBOA

Course Overview

Welcome!

CSF: Forensics Cyber-Security

Fall 2019

Nuno Santos

People leave a digital trail everywhere

- Personal files, browsing history, etc. are stored on your desktop, mobile, and cloud services like Dropbox
- When you log in to sites like Gmail, 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.
- Surveillance cameras in subway stations and on city buses watch you board and depart
- …

Is it possible to leverage such trails to be used as evidence in the court of law?

Yes!

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!

More (serious) examples

Anthony trial: 'Chloroform' searched on computer

See show times »

NANCY GRACE

By **Ashley Hayes**, CNN
June 8, 2011 -- Updated 2116 GMT (0516 HKT)

(CNN) -- Someone conducted keyword searches on "chloroform" using a desktop computer located in the home Casey Anthony shared with her parents, a computer examiner testified Wednesday in Anthony's capital murder trial.

The searches were found in a portion of the computer's hard drive that indicated they had been deleted, Detective Sandra Osborne of the Orange County Sheriff's Office testified.

However, she told jurors, deleted material remains on a computer's hard drive and can be retrieved until it is overwritten by new data. It had not been overwritten on the Anthonys' computer, she said, and "a complete Internet history" was obtained.

News › UK › Crime

UK's youngest terrorist convicted of bomb plot

Schoolboy from a respected Muslim family was part of cell that plotted to make explosives and napalm. Jonathan Brown and Michael Savage report

Monday 18 August 2008

A schoolboy who possessed a guide to making napalm on his computer and had notes on martyrdom under his bed became Britain's youngest convicted terrorist yesterday.

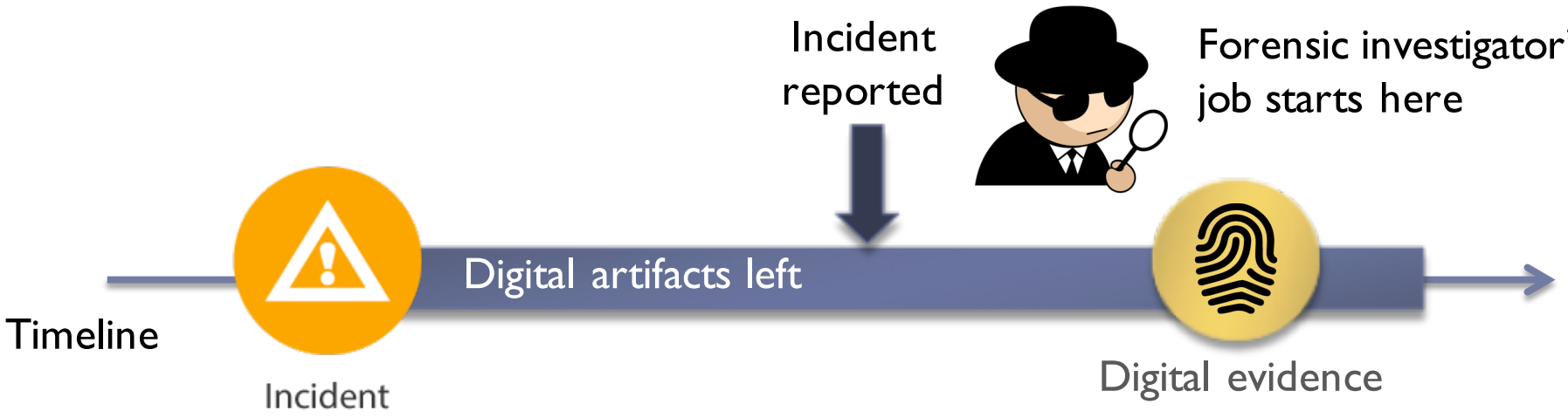
Convicted molester facing child pornography charges

By MATT THACKER
Matt.Thacker@newsandtribune.com Oct 16, 2010

The New Albany Police Department examined the computer hard drives and found “an extremely large amount of obvious child pornography,”

What is digital forensics?

- **Digital forensics (AKA: cyber 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 (PT: prova digital):** 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, backups, etc.
- The **goal of digital forensics** is to explain the current state of a digital artifact

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 mollify 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 to support claims of harassment, abuse, or wrongful termination from employment

Some classic high-profile cases

The BTK Killer

From 1974 to 1991, 10 murders were committed in and around Wichita, Kansas, all by the same criminal dubbed the BTK Killer in the media. Although the killer communicated with police and media regularly, his identity remained a mystery, and investigators had given up hope of solving the case until he reinitiated contact in 2004. He delivered this message on a floppy disk, based on police "assurances" that documents saved on a floppy disk are not traceable. **However, using metadata on a deleted Microsoft Word document, police were quickly able to trace BTK's true identity: Dennis Rader.** Rader is now serving 10 consecutive life sentences in a Kansas prison. BTK's floppy disk error made his trial one of the most famous forensic cases ever.

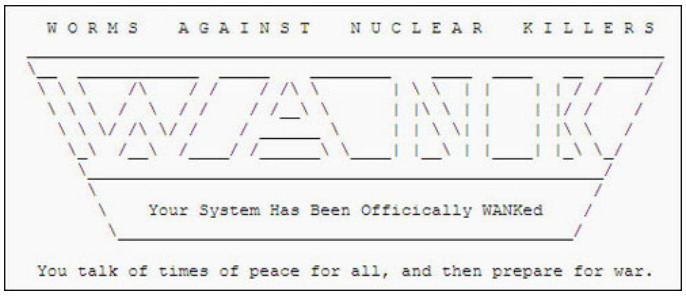
The Corcoran Group

This lawsuit occurred over a fairly insignificant crime; plaintiffs claimed that defendants, including the real estate firm The Corcoran Group, knowingly sold them a condominium that flooded during storms, but failed to disclose this information to the buyers. The court discovered **that the Corcoran Group defendants had deleted many emails relevant to the case once litigation began**. This case changed the legal precedent on storage and deletion of electronically stored information, establishing an obligation to preserve electronically stored information relevant to a lawsuit that is underway or that seems likely to occur in the future.

A few unsolved cases

The WANK Worm (1989)

Possibly the first "hacktivist" (hacking activist) attack, the WANK worm hit NASA offices in Greenbelt, Maryland. WANK (Worms Against Nuclear Killers) ran a banner (pictured) across system computers as part of a **protest to stop the launch of the plutonium-fueled, Jupiter-bound Galileo probe**. Cleaning up after the crack has been said to have cost NASA up to a half of a million dollars in time and resources. To this day, no one is quite sure where the attack originated, though many fingers have pointed to Melbourne, Australia-based hackers.



CD Universe Credit Card Breach (2000)

A blackmail scheme gone wrong, the posting of over 300,000 credit card numbers by hacker Maxim on a Web site entitled "The Maxus Credit Card Pipeline" has remained unsolved since early 2000. Maxim **stole the credit card information by breaching CDUniverse.com**; he or she then demanded $100,000 from the Web site in exchange for destroying the data. While Maxim is believed to be from Eastern Europe, the case remains as of yet unsolved.

Short timeline of digital forensics

- 70's
  - First crime cases involving computers, mainly financial fraud
- 80's
  - FBI Computer Analysis and Response Team (CART) created
- 90's
  - International Organization on Computer Evidence (IOCE)
- 00's
  - USA PATRIOT Act ("Computer Crime") empowered government agencies to crack down on computer crime in the name of combating terrorism
  - FBI CART case load exceeds 6500 cases examining 782 TB of data
  - In Portugal, Lei do Cibercrime (Lei n° 109/2009)

Many (unofficial) digital forensics branches

Digital Forensics

- Computer forensics
  - Flash, HDD, USB device
- Network forensics
  - Monitoring and analyzing network traffic
- Mobile device forensics
  - Collect digital evidence from mobile devices
- Cloud forensics
  - Forensic analysis of cloud infrastructures
- …

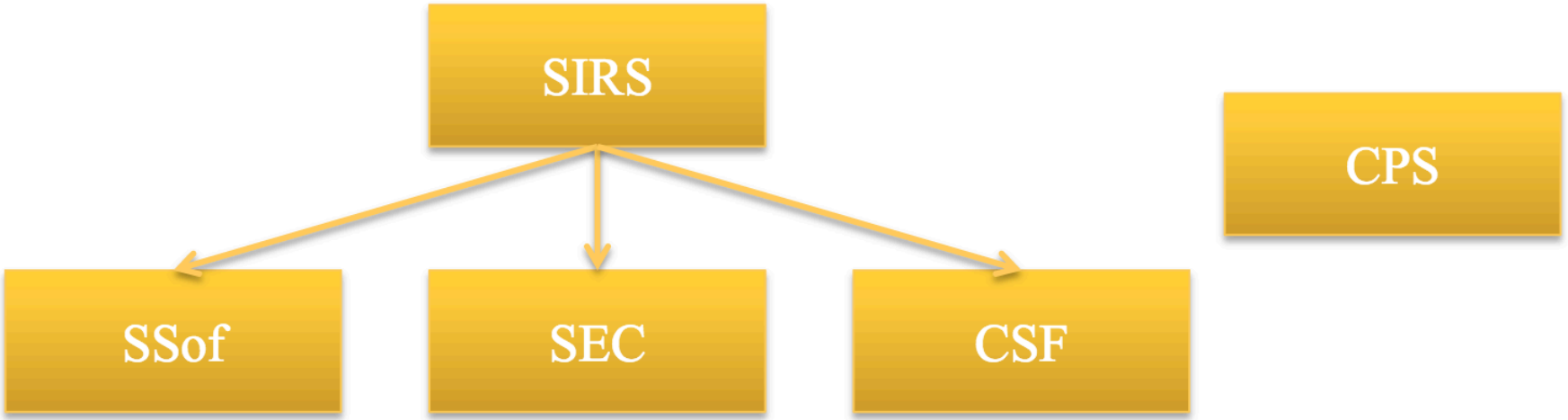
Digital forensics vs. other related disciplines

- **Computer security** main focus concerns with the prevention of unauthorized access, as well as the maintenance of confidentiality, integrity and availability of computer systems

- **Data recovery** is a process of recovering inaccessible data from corrupted or damaged computer systems not necessarily within the scope of a digital investigation

Specialization in cyber-security courses

- Segurança Informática em Redes e Sistemas (SIRS)
- Segurança em Software (SSof)
- Sistemas de Elevada Confiabilidade (SEC)
- **Ciber Segurança Forense (CSF)**
- Criptografia e Protocolos de Segurança (CPS)



Tea Room Case

Natasha Romanov (former secret agent) has retired and opened a new Russian Tea Room on Lubyanka Square in Moscow

Tea Room Case: A crime suspect

- However, her employee Nick Ulyanov vanished and may have stolen her award winning menu

- The last 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 his own version of the menu

Tea Room Case: Call the cops

- Natasha called Andrei Demidov, a crack digital forensic investigator for the Metropolitan 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, don't let him contaminate the evidence!"
- They get a warrant & stake out the Train Station, watch the outbound trains, and catch Nick about to board the express to Saint Petersburg
- Now what…

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 made)
- Ivan wants to take a look, inserts a copy into his laptop and **sees no files in it.**
- Ivan says, "Looks like nothing here…"
- Andrei says, "We'll see…"

Tea Room Case: Looking deeper

- Andrei: "How big is the file system and how big is the device?"
- He uses several **forensic tools** to take a closer look at the data
- Create a **new case** and adds the image of Nick's flash drive
- Notice an **anomaly**: The file system is 1GB, but the device is 2GB
- Could be nothing, or could be something hidden…
- Let's look up for a deleted text file with a menu

Tea Room Case: Caviar anyone?

- Andrew asks Natasha for menu items that could be searched for
- He uses a **forensics tool** and searches for “икра” (Caviar)
- The tool returns a hit **not located within an allocated file:**

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

- Looks like Nick may have deleted a text file with a menu!
- Andrew does a **recover deleted files** from the active file system

Tea Room Case: A deleted file recovered!

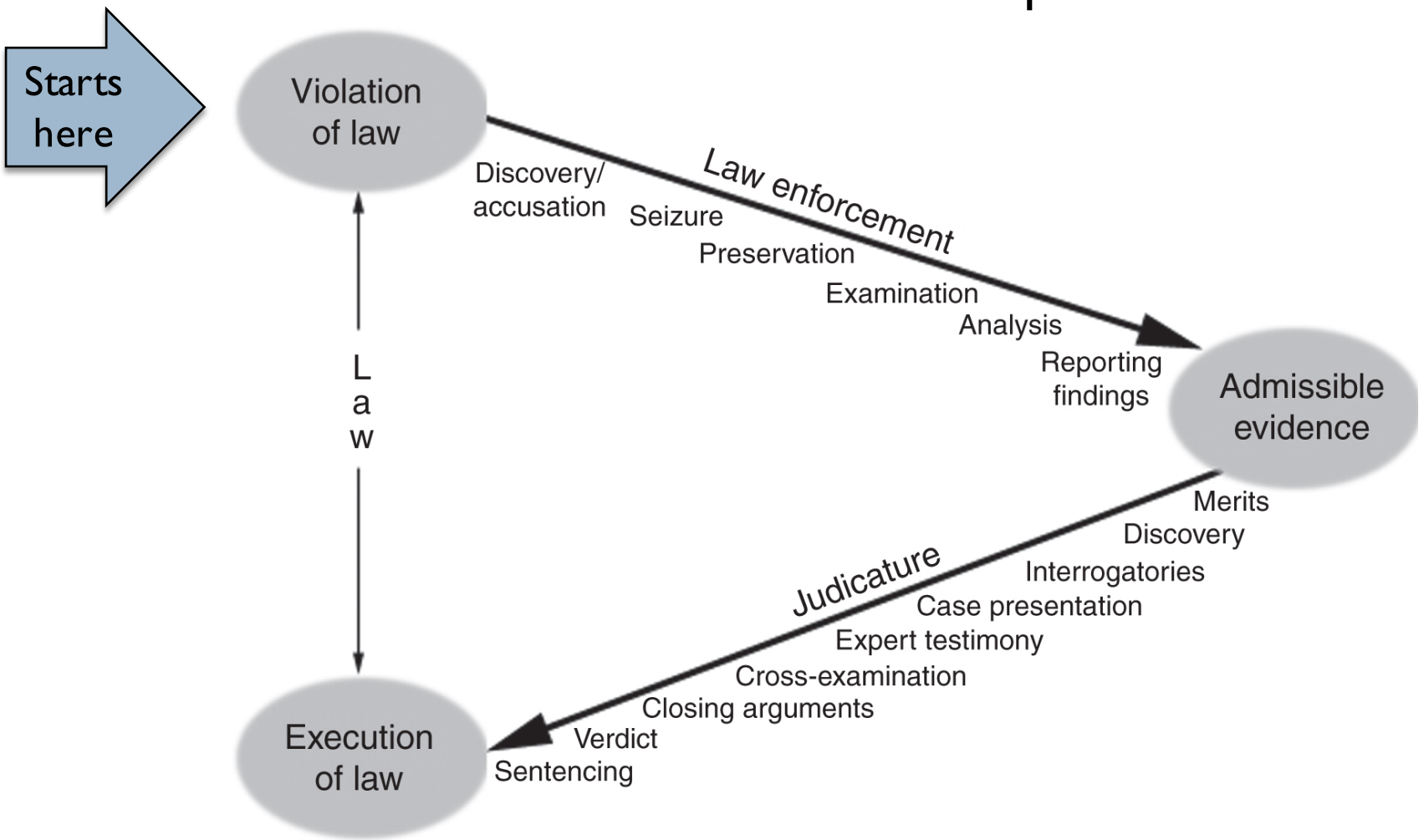
```
Natasha Romanov's New Little Russian Tea Room
#4 Lubyanka Square, Moscow


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

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

What can a novice digital investigator learn from this case about digital forensics (DF)?

Lesson #1: DF is not about judging someone

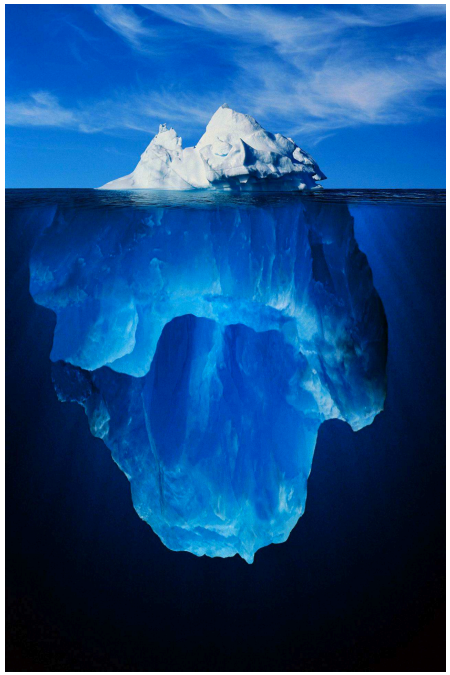
- Ivan: “Have we shown that Nick is guilty?”
- Andrei: “No, that’s not what we do.
- **We use our wits and tools to reveal facts.** If we try to prove the case one way or the other we will find only what we expect
- Nick may be guilty or not guilty. This is for the case agent and prosecutor to present to the court. **The court decides.**
- To be presented before the court, must follow **rigorous methodology** in handling evidence.”

Typical digital forensics workflow



Lesson #2: DF looks deep under the surface

- The "data iceberg": there's a lot more data on a digital artifact than what can immediately be seen



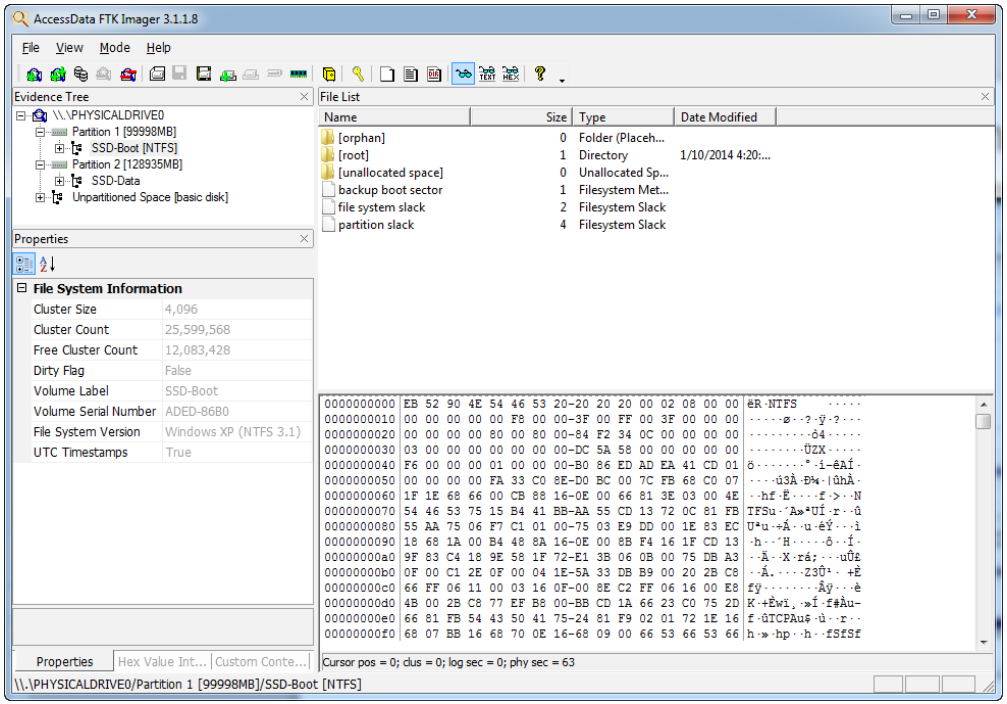
Filenames, folders, log files, …

File and memory slack,
NTFS streams,
deleted files,
swap files,
hidden files,…

- Need to understand technology and where to look for

Lesson #3: DF relies on adequate forensic tools

- Use **forensic tools** to help collect & analyze evidence
  - FTK, Directory Snoop, Wireshark, WinHex, Autopsy, Volatility,…



FTK Imager: saves an image of a hard disk in one file or in segments that may be later on reconstructed

- But need to use them right, abiding by the **law**

Lesson #4: DF faces many technical challenges

- Bad guys use anti-forensic tools
  - Steganography, anonymous communication services, etc.
- Data can be partial, corrupted, noisy, etc
  - Need adequate techniques to recover and analyze such data
- Deluge of technology and data
  - Require techniques for reducing and filtering relevant data

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

Objectives of this course

- Upon completing this course, students are expected to:
  - Understand the basics of digital forensics principles & praxis
  - Acquire hands-on practice on digital forensics investigation
  - Be prepared for active research at the forefront of this area

Course program

- Part I: Foundations of digital forensics
  - Legal framework, digital investigation, evidence acquisition…
- Part II: Basic techniques and tools for digital forensics
  - Files, steganography, storage, file systems, OSes, packet analysis, email, web…
- Part III: Advanced techniques and tools for digital forensics
  - Rootkits, anonymization, botnets, cryptocurrency, cloud forensics…

What this course is not going to do

- Make of you an experienced forensics analyst
  - That requires lot of fieldwork; here you'll learn the basics of the praxis
- Cover all existing forensic tools and computer technologies
  - Impossible! We'll focus on the universal principles underlying them
- Analyze in depth the legal aspects involved in digital forensics
  - This is a computer engineering course, and thus more focused on technology
- Describe how existing computer and networked systems work
  - We assume you have that necessary background from previous courses

Teaching staff

- Theoretical and lab classes:
  - Nuno Santos (theory)
    nuno.santos@inesc-id.pt
    Tagus: 2N3.1 (office hours: Tuesdays, 15h30)
    Alameda: INESC-ID, office 503 (office hours: Thursdays, 9h30)
  - Tiago Brito (labs Alameda)
    tiago.de.oliveira.brito@ist.utl.pt
    Alameda: INESC-ID, office 601 (office hours: TBA)
  - João Tiago (labs Tagus)
    joao.marques.tiago@tecnico.ulisboa.pt
    Tagus: 2N3.1 (office hours: TBA)
- Professor may leave >15min if no students are present
- Extra office hours can be arranged by appointment

Class schedule

- Theoretical classes: 2 classes/week, one and a half hour long
  - Taguspark
    - Class1: Tuesday, 14h00-15h30, Room A5
    - Class2: Wednesday, 11h30-13h00, Room A5
  - Alameda
    - Class1: Wednesday, 8h00-9h30, Room FA3
    - Class2: Thursday, 11h00-12h30, Room FA2

- Lab classes: 1 class/week, one and a half hour long
  - Taguspark:
    - Tuesday, 11h00-12h00, Room 1-27
    - Tuesday, 15h30-17h00, Room 1-29
    - Wednesday, 10h00-11h30, Room 1-15
    - Thursday, 8h00-9h30, Room 1-29
  - Alameda:
    - Thursday, 17h00-18h30, LAB11
    - Friday, 8h00-9h30, LAB11

Selection of the lab shift

- Each lab shift will function with groups of 3 elements each
  - Groups are allowed with elements from both campi (Tagus and Alameda)

- Enrollment through Fenix, according to the following schedule:

  Monday, 24th, 9h:

  enrollment opens for complete groups

  Wednesday, 26th, 9h:

  enrollment opens for groups with two or more elements

  Friday, 28th, 9h:

  no restrictions

- Feel free to choose the lab shift, as long as slots are available
- In the end, we will perform group compacting in each shift

Assessment

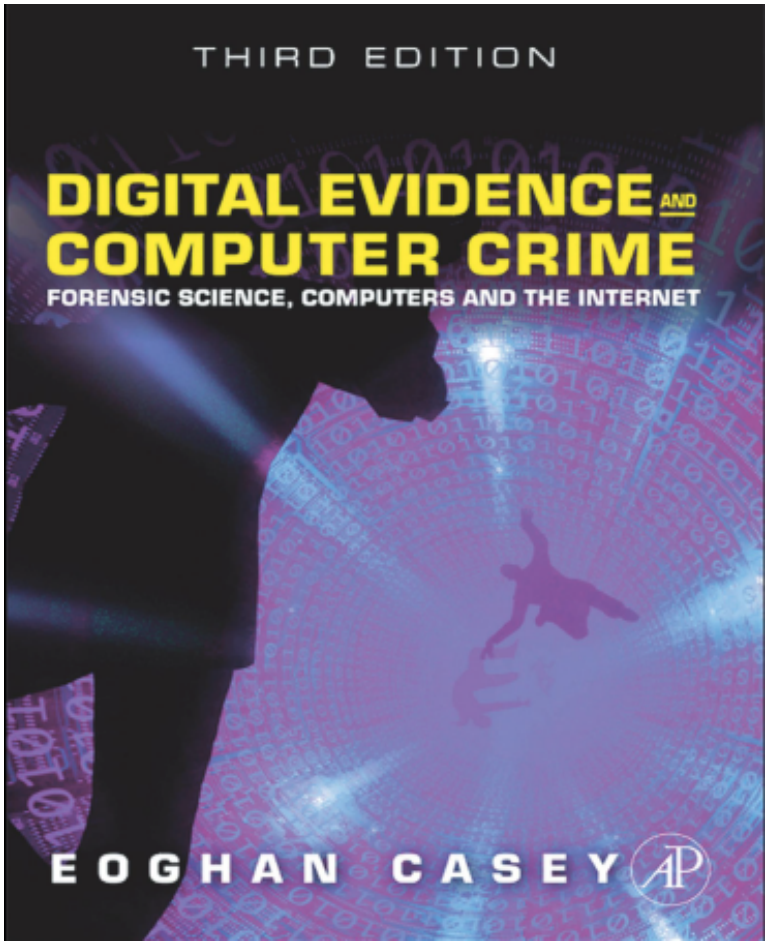
- Lab component (40%) – minimal grade 9
  - Groups of 3 elements
  - 3 lab assignments and defense
  - Lab assignments' submission dates:
    - Lab 1: 25 October
    - Lab 2: 22 November
    - Lab 3: 13 December
  - Lab grade baseline = 30% Lab1 + 35% Lab2 + 35% Lab3
  - Lab grade final: defined individually in the defense at the end of the term
- Exam (60%) – minimal grade 9
  - Final exam, January 8th, 11h30
  - Recovery exam: February 3th, 8h00

Bibliography

- **Primary: Course slides**

- Main book: [Casey11]
  - **Digital Evidence and Computer Crime, Third Edition: Forensic Science, Computers and the Internet, 3 edition**: Eoghan Casey 2011 - May 4 Academic Press

- Secondary bibliography:
  - Papers and other supplemental material to be provided on the course web site



Plan 1/2

week		theory				labs		
#	dates	days	class #	section	topic	class #	topic	observ.
1	16-20 Set	17,18 Set	1	Part I: Foundations of Digital Forensics	Introduction		No class	
		18,19 Set	2		I.1. Legal Framework			
2	23-27 Set	24,25 Set	3		I.2. Digital Investigation Process		Lab enrolment	
		25,26 Set	4		I.3. Evidence Acquisition			
3	30 Set-4 Out	1,2 Out	5	Part II: Basic Techniques and Tools for Digital Forensics	II.1 File Forensics	1	Tutorial I	
		2,3 Out	6		II.2. Steganography and Watermarking			
4	7-11 Out	8,9 Out	7		II.3. Memory Analysis	2	Tutorial II	
		9,10 Out	8		II.4. Storage and Volume Analysis			
5	14-18 Out	15,16 Out	9		II.5. File System Analysis Techniques	3	Lab Assignment 1	Lab 1 published: 14 October
		16,17 Out	10		II.6. File Carving and Timestamp Analysis			
6	21-25 Out	22,23 Out	11		II.7. Operating System Forensics	4	Lab Assignment 1	
		23,24 Out	12		II.8. Traffic Analysis			Lab 1 submission: 25 October
7	28 Out - 1 Nov	29,30 Out	13		II.9. Investigation of Computer Networks	5	Tutorial III	1 Nov holiday, Friday, no labs
		30,31 Out	14		II.10. Email and Web Forensics			

Plan 2/2

8	4-8 Nov	5,6 Nov	15	Part III: Advanced Techniques and Tools for Digital Forensics	III.1. Deep Web and Social Networks	6	Lab Assignment 2	Lab 2 published: 4 November
		6,7 Nov	16		III.2. Online Anonymity			
9	11-15 Nov	12,13 Nov			No class - Trip to conference	7	Lab Assignment 2	
		13,14 Nov						
10	18-22 Nov	19,20 Nov	17		III.3. Botnets	8	Lab Assignment 2	
		20,21 Nov	18		III.4. Rootkits and Malware Analysis			Lab2 submission: 22 November
11	25 Nov - 29 Nov	26,27 Nov	19		III.5. Cryptocoins	9	Lab Assignment 3	Lab 3 published: 26 November
		27,28 Nov	20		III.6. Wireless Networks			
12	2-6 Dez	3,4 Dez	21		III.7. Mobile Forensics	10	Lab Assignment 3	
		4,5 Dez	22		III.8. File System Interpretation			
13	9-13 Dez	10,11 Dez	23		III.9. Case Studies on File System Analysis	11	Lab Assignment 3	
		11,12 Dez	24		III.10. Cloud Forensics and Conclusions			Lab3 submission: 13 December
14	16-20 Dez	17,18 Dez			Discussions		Discussions	
		18,19 Dez						

References

- Primary bibliography
  - [Casey11] Chapter 1

- Fun:
  - "Privacy is dead – get over it"
    https://www.youtube.com/watch?v=DaYn_PkrfvQ

- Resources:
  - SWGDE www.swgde.org
  - AAFS http://www.aafs.org
  - DFRWS http://www.dfrws.org
  - SANS www.sans.org

Next class

- I.1 Legal Framework