universidade
de aveiro

Computer Systems Forensic Analysis
AFSC

Course Presentation

Artur Varanda

School Year 2021-2022

AGENDA

I. Context

II. Objectives

III. Syllabus

IV. Evaluation

V. Resources

VI. Bibliography

COURSE CONTEXT

Computer Systems Forensic Analysis:

Optional – 1st year, 1st Semester – 39 contact hours

Lecturer:

Artur Varanda (`artur.varanda@sapo.pt`)

Office hours:

send an email first to schedule a meeting (VTC)

COURSE DESCRIPTION

This class aims to provide students with sound knowledge of digital forensics such as

- ✓ the collection, identification, preservation, documentation, analysis and presentation of digital evidence;
- ✓ digital evidence acquired from computers, cell phones and other electronic devices;
- ✓ this knowledge will be taught in the various areas of forensic discipline, forensic computing and forensic data analysis.

COURSE DESCRIPTION

This course aims to address the transversal concepts to all areas of digital forensics such as:

- ✓ the scientific method of digital forensic investigation;
- ✓ the different types of digital forensic evidences: data, computers, mobile devices, ...
- ✓ the students will apply the knowledge acquired in the classroom to several laboratory assignments and will be able to produce a digital forensic report

LEARNING

Upon completion of this course, students should be able to:

- ✓ identify the different types of digital forensic evidence
- ✓ know the terminology, techniques and processes of a digital forensic investigation
- ✓ collect digital evidence from storage media
- ✓ know the limitations of digital forensics current techniques
- ✓ understand the scientific method and the need for its use
- ✓ apply the scientific method in a digital forensics investigation
- ✓ use digital some forensic tools and techniques
- ✓ comprehend forensic analysis reports

1 **- Overview of cybercrime investigation**

- ✓ Information security principles
- ✓ AAA Services concept
- ✓ Cybercrime vs Computer Crime
- ✓ Penal framework of cybercrime
- ✓ Applicable legislation

2 - **Introduction to digital forensics**

- ✓ Digital investigation
- ✓ Digital evidence
- ✓ Investigation process
- ✓ Digital evidence handling
- ✓ Ethical code

3 - **Obtaining evidences**

- ✓ Boot process
- ✓ Forensic boot tools
- ✓ Forensic sorting tools
- ✓ Forensic acquisition tools
- ✓ *FTK Imager* overview

SYLLABUS

4 – **Data organization**

- ✓ Data storage devices
- ✓ File system analysis
- ✓ Binary and hexadecimal numbers
- ✓ Endianess
- ✓ Character encoding
- ✓ Data structures

5 -**Autopsy**

- ✓ *Autopsy* workflow
- ✓ Create cases and add data sources
- ✓ Automated processing with ingest modules
- ✓ Manual content analysis
- ✓ Report generation

6 – **Storage devices**

- ✓ Hard disk geometry
- ✓ ATA and SCSI interfaces
- ✓ Flash memory drives
- ✓ Solid State Drives (SSD)

7 – **Volumes and partitions**

- ✓ Partition tables
- ✓ Logical addresses
- ✓ Volume analysis
- ✓ Common partitions
- ✓ Volume partition tools

SYLLABUS

8 – **RAM Analysis**

- ✓ General computer architecture
- ✓ Memory acquisition tools
- ✓ Memory analysis tools
- ✓ *Volatility* overview

9 - **Mobile Forensics**

- ✓ Mobile devices
- ✓ SIM cards
- ✓ Forensic value and potential evidence
- ✓ Mobile data acquisition
- ✓ Hardware and Software tools
- ✓ *XRY* and *XAMN* overview

SYLLABUS

10 – **OSINT (Open-source Intelligence)**

- ✓ History of OSINT
- ✓ Information sources
- ✓ Information to intelligence cycle
- ✓ Open-source possibilities
- ✓ Automated processing
- ✓ Social media OSINT
- ✓ Dark Net OSINT

11 – **Documentation and Reporting**

- ✓ Physical examination
- ✓ Computer examination
- ✓ Media examination
- ✓ What to report
- ✓ Windows forensic report
- ✓ Forensic report structure

COURSE

Learned knowledge will be evaluated through one individual written test and 1 team project.

Final grade = 50% Individual written test + 50% Team Project

Dates:

2021-01-15 09:00 – Individual written test

2021-01-08 23:59 – Team Project submission (Moodle)

2021-01-15 13:00 – Team Project presentation

Classes

Dates:

16/10/2020 – Class 1 (via zoom)

23/10/2021 – Classes 2 and 3

06/11/2021 – Classes 4 and 5

20/11/2021 – Classes 6 and 7

04/12/2021 – Classes 8 and 9

18/12/2021 – Classes 10 and 11

15/01/2022 – Test and Team Project Presentation

October			
16	23	30	
November			
6	13	20	27
December			
4	11	18	
January			
8	15	22	

TEAMS FORMATION

Teams:

- Three (3) students per Team
- Exceptions must be approved by the teacher

1 week to create the teams

- random pool if needed

PROJECT PROPOSAL

Each team will choose just a **different** topic about digital forensic analysis:

1 - Computer Networks

2 - IoT devices

3 - Android devices

4 - RAM

5 - OSINT techniques

6 - Malicious software

7 - Dark Net

8 - Virtual Machines

Organization:

- ✓ create and discuss a plan with the team members and the teacher
- ✓ check the available resources on the Internet
- ✓ class resources will be available on Moodle

PROJECT PROPOSAL

1 - Submit one PDF file, named `TeamX-report1.pdf`, with a maximum of 10 pages

- write and introduction and the state of the art about the chosen topic, as well as the experimental part, results, conclusion and bibliography with IEEE citation style.
- the document should be written like a research paper:
  - must follow the IEEE template (for A4 two columns)

2 – The PDF file will be published on Moodle for all students

3 - Prepare a presentation of up to 20 minutes

- all team members must participate
- present an overview of the state of the art
- the presentation should focus on the experimental part, results and conclusions

PROJECT PROPOSAL : Evaluation

Project Team Evaluation

50% – Presentation

explanation of the concepts and technical details

clarity and communications skills

argumentation in the discussion phase

50% – Report

description of concepts and procedures

expected results and tested results of forensic interest

description and usage of tools and techniques

document formatting and references

VERY IMPORTANT

Do not commit any crime for the purpose of this project

Do not include images or videos that may violate someone's privacy

- instead, use fake images

Do not use illegal content or software to achieve your goals

Do not hack any computer without written permission

- use only virtual machines that you control and setup for this purpose

If you have any doubt about the legality of an action, ask **first**

NOTES VERY IMPORTANT

Think thoroughly

In a real-world case, your conclusions will influence the outcome of a trial.

Write clearly

Digital forensic reports are meant to be read by nontechnical individuals:

lawyers, judges, etc.

Always follow the digital forensics investigator code of ethics

Your team should

split tasks among the team members in a fair way, but

all team members have the responsibility to review the report before delivery

REQUIRED RESOURCES FOR THE PRACTICAL CLASSES

Software:

- Virtual machines (VMware or Virtual Box)
  - Windows and Linux VMs
- Windows Software
  - Free: FTK Imager, Autopsy 4, Volatility, XAMN Viewer

Hardware:

- Computers
  - RAM: 8GB or more recommended
  - Lots of disc space
- Large capacity USB HDD or SSD drive (≥ 250 GB)
- Low capacity USB Pen drive (≥ 8GB)
- USB, SATA and IDE write blocker (can be simulated by software)
- Camera and graduated set square (for scale purposes when taking pictures of equipment)

COURSE BIBLIOGRAPHY

Main Bibliography

- **Mário Antunes**, **Baltazar Rodrigues**, Introdução à Cibersegurança - A Internet, os aspetos legais e a análise digital forense, FCA, 2018, ISBN: 978-972-722-861-4
- John Sammons, The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics, 2nd edition. Amsterdam ; Boston: Syngress, 2014.
- B. Carrier, File System Forensic Analysis, 1st edition. Boston, Mass.; London: AddisonWesley Professional, 2005.
- Cory Altheide and Harlan Carvey, Digital Forensics with Open Source Tools, 1st edition. Burlington, MA: Syngress, 2011.
- Brett Shavers, Placing the Suspect Behind the Keyboard: Using Digital Forensics and Investigative Techniques to Identify Cybercrime Suspects, 1st edition. Waltham, MA: Syngress, 2013.
- Barrett, D., & Kipper, G. (2010). Virtualization and forensics: A digital forensic investigator's guide to virtual environments. Syngress.
- Davidoff, S., & Ham, J. (2012). Network forensics: tracking hackers through cyberspace (Vol. 2014). Upper Saddle River: Prentice hall.
- Polstra, P. Linux Forensics CreateSpace Independent Publishing Platform, 2015
- Ligh, M. H., Case, A., Levy, J., & Walters, A. (2014). The art of memory forensics: detecting malware and threats in windows, linux, and Mac memory. John Wiley & Sons.
- Mahalik, H., Tamma, R., & Bommisetty, S. (2016). Practical Mobile Forensics. Packt Publishing Ltd.
- Ligh, M., Adair, S., Hartstein, B., & Richard, M. (2010). Malware analyst's cookbook and DVD: tools and

PLEASE DOWNLOAD

Please Download:

"Bandido" Virtual Machine Disk	bit.ly/3aEmj9n
Ubuntu Bionic	releases.ubuntu.com/bionic

Please Install:

VirtualBox 6.1	virtualbox.org
7-Zip 19.0	7-zip.org
FTK Imager 4.5.0	accessdata.com

ANY QUESTIONS?