ISA 785

Research in Digital Forensics

Class Mechanics

Angelos Stavrou, George Mason University
Prerequisites

- **CS 571 (Operating Systems):**
  - We will be analyzing Files and Logs

- **CS 555 (Computer Networks):**
  - We will analyze Network Traces

- **ISA 562 (Information Security Theory & Practice):**
  - Basics of Systems and Log Analysis

- Some Working knowledge of C/C++/Java/C#/Python
  - More on the next slides
Prerequisites: Programming Background

- Must have completed a course on Data Structures and Program Design (e.g. CS 310, INFS 519)
- Has working knowledge of C, C++, Java, Python, C#, …
- Why do I need programing?
  - To understand the Digital Forensic Tools
  - To automate and understand the output of the analysis
  - To create your own tools (optional)

- In an nutshell: you need to be able to understand programming
  - You can CHOOSE which language you will work with Java, C, …
- I am fairly reachable via email, contact me or the TA
- There are no stupid questions
Textbook

- **Required:** [TextBook available online for GMU students]
  File System Forensic Analysis by Brian Carrier.
  [Online for GMU] [Pearson] [Amazon]

- **Recommended:** [TextBook available online for GMU students]
  System Forensics, Investigation, and Response
  by John R. Vacca; K. Rudolph.
  [Jones & Bartlett Learning] [Amazon]
Class Mechanics: Readings

Check the Website for Readings:

- Assigned readings from on-line articles
- Law opinions
- Research publications.

I will also have supplementary materials on reserve or handed out during class. Although we will not read the entire Carrier book, and we will use it for only a portion of the class, it cannot be replaced with other materials.
Class Mechanics: Contacts

Instructor:
- Angelos Stavrou, astavrou@gmu.edu
- Office Hours: Wednesday 4:30pm - 6:30pm and by appointment
- Office: Research I, Room 437

Teaching Assistant:
- Chen Liang, cliang1@gmu.edu
- Office Hours: Monday, 4:00 – 6:00pm
- Office: Engineering building 4456
Class Mechanics: Grading

Grading

- Class Projects: 80%
- Class Presentations: 15%
- Class Participation: 5%
- No Midterm or Final

- Some Projects are going to be Collaborative
- You are responsible to choose your team
Class Mechanics: Accounts & Lectures

Accounts & Lectures:

- Computer Accounts on mason.gmu.edu or zeus.ite.gmu.edu
  Check if you have one!

- E-mails with additional info on lectures and assignments will be sent to students’ GMU e-mail addresses

- All Class material will be posted at the class web page

- Discussion Board (Piazza or BlackBoard)
Accounts & Lectures:

- Computer Accounts on mason.gmu.edu or zeus.ite.gmu.edu. Check if you have one!

- E-mails with additional info on lectures and assignments will be sent to students’ GMU e-mail addresses

- All Class material will be posted at the class web page

- Discussion Board (Piazza or BlackBoard)
Other Useful Resources

HONOR CODE:

- University's Academic Honesty Page
- GMU Honor Code.

Writing Center: A114 Robinson Hall; (703) 993-1200; http://writingcenter.gmu.edu

University Libraries: “Ask a Librarian” http://library.gmu.edu/mudge/IM/IMRef.html

Counseling and Psychological Services (CAPS): (703) 993-2380; http://caps.gmu.edu

University Policies: The University Catalog, http://catalog.gmu.edu, is the central resource for university policies affecting student, faculty, and staff conduct in university affairs
Why Digital Forensics

Why study Digital Forensics?

Computer forensics investigators are “detectives of the digital world.”

However, before becoming that, we need to understand:

- How electronic evidence differs from physical evidence
- What computer forensics tools and techniques can reveal and recover
- Explain the process of discovery and electronic discovery
- Basic steps in a computer forensics investigation
- Legal & Ethical issues
  - Evidence Search and Seizure
- Types of challenges to the admissibility of e-evidence
Class Topics

- Principles and Techniques for Digital Forensics
- Understand the established procedures in Digital Evidence Identification, Extraction, Preservation, Correlation, Analysis and Presentation
- Apply Existing Tools to conduct Forensics Duplication and analysis
- Understand the specific technical challenges in conducting Digital Forensics
- Countermeasures and Caveats of Digital forensics
- Common Legal and Ethical issues in Digital Forensics