EEL 4802— Introduction to Digital Forensics

Department of Electrical & Computer Engineering
Florida International University
Spring 2018

Classroom	**:**	EC 3239
Class Time	**:**	8:00 am—12:30 pm
Faculty	**:**	Dr. Luis Galarza
Office Hours	**:**	T & R 10:00-12:00 am or by Appointment
Office	**:**	EC 3944
Phone	**:**	305-348-8464

Catalog Description

This course will give a fundamental foundation for students new to the digital forensics field, discussing, what digital forensics is, the methodologies used, key technical concepts, and the tools needed to perform examinations and media exploitation techniques. The course topics includes the fundamentals of forensic science, laws and regulations relating to digital data, quality assurance and ethics in a digital laboratory, basic terminology, computer hardware and various storage media, software, including operating and file systems, and basics concepts of computer security.. Students will examine various log files, and storage mediums associated with computers, networks, the internet, the cloud, and mobile devices, and different operating systems including Windows and Linux.

Course Objectives:

This course provides students the theoretical and practical concepts to comprehend the details associated what entails Digital Forensics, the requirements in establishing a digital forensics lab and exposures to various tools and techniques to perform data acquisition from different storage mediums and analyze these sources for digital evidence. It will provide students with hands-on exposure to the latest tools and techniques to prepare an investigative plan, understand the common artifacts (from the Windows, Mac, and Linux operating systems) to look for during forensic investigation, and provide exposure to well-known and novel forensic methods using command-line and graphical open-source computer forensics tools for examining a wide range of target systems and artifacts.

Course Student Learning Outcome

- Provide core knowledge necessary for students to have a basic understanding of forensic science, Digital Forensics and the value of digital evidence in solving crimes
- Students will be able to evaluate digital devices for evidence important in solving criminal & civil cases
- Students will gain an understanding of laws governing search and seizure of digital evidence and laws that govern access to stored data will be analyzed. Factors that allow and impact the admissibility of evidence will be explored and debated

- Students will gain an understanding of file format and storage in various operating systems (Linux and Windows)
- Students are exposed to various forensic tools that are used in digital chain of custody
- Student will gain practical application of Digital Forensic Framework, EnCase, HELIX3, X-Ways, FTK Imager, and Hex tools

Topics

- Forensic Science and the Scientific Method
- Managing digital evidence
- Laws regarding digital evidence – acquisition, storage, usage, and preserving
- Understand Forensic Lab requirements
- Windows and Linux file formats
- Logical and physical concepts with regard to storage medium
- Search for deleted files, analyzing data sectors and file content
- Use of Framework for digital chain of custody
- Understand log file and reports from forensic process
- Acquisition of disk image
- Analyze disk images for various artifacts
- Apply forensic analyst tools

Textbooks

Assigned readings and laboratory exercises are an essential component of this course and provide students with a baseline of knowledge that will be expanded upon through more detailed and complex in-class lectures and discussions. Students will be required to complete assigned readings prior to the class period in which the material will be discussed.

(1) Sammons, J. (2015). The Basics of Digital Forensics 2nd Edition. Waltham, MA: Syngress Publishing Inc. ISBN: 978-0-12-801635-0

(2) Supplemental course materials (e.g., handouts, reading assignments, lab exercises, etc.) will be posted to the FIU Online Canvas course shell.

Grading Scheme

Grading Scale: NOTE: There are ***no makeup exams*** offered	
Assignments/labs	30%
Research project	20%
Midterm	20%
Final	30%

Tentative Grading Scale

A	**95-100**	**B+**	**86-89**	**C+**	**76-79**	**D+**	**66-69**	**F**	**0-59**
A-	**90-94**	**B**	**83-85**	**C**	**73-75**	**D**	**63-65**		
		B-	**80-82**	**C-**	**70-72**	**D-**	**60-62**		

University's Code of Academic Integrity

"Florida International University is a community dedicated to generating and imparting knowledge through excellent teaching and research, the rigorous and respectful exchange of ideas, and community service. All students should respect the right of others to have an equitable opportunity to learn and honestly to demonstrate the quality of their learning. Therefore, all students are expected to adhere to a standard of academic conduct, which demonstrates respect for themselves, their fellow students, and the educational mission of the University. All students are deemed by the University to understand that if they are found responsible for academic misconduct, they will be subject to the Academic Misconduct procedures and sanctions, as outlined in the Student Handbook."
More information can be found at http://academic.fiu.edu/academic_misconduct.html

Department Regulations Concerning Incomplete Grades
To qualify for an Incomplete, a student:
1. Must contact (e.g., phone, email, etc.) the instructor or secretary before or during missed portion of class
2. Must be passing the course prior to that part of the course that is not completed
3. Must make up the incomplete work through the instructor of the course
4. Must see the Instructor. All missed work must be finished before last two weeks of the following term.

University policies: on sexual harassment, and religious holidays, and information on services for students with disabilities
http://academic.fiu.edu/
http://drc.fiu.edu

Policies:

- **Academic Misconduct:** For work submitted, it is expected that each student will submit their own original work. Any evidence of duplication, cheating or plagiarism will result at least a failing grade for the course.
- **Unexcused Absences:** Two unexcused absences are permitted during the term. More than two will result in the loss of points from your final grade. (**1 point** per absence above two**, 3 points** per absence above 5).
- **Excused Absences:** Only emergency medical situations or extenuating circumstances are excused with proper documentation. After reviewing documentation you are **required to email** a description of the excuse and absence dates as a written record to aponsr@fiu.edu.
- **On Time:** As in the workplace, on time arrival and preparation are required. Two "lates" are equivalent to one absence. (Leaving class early is counted as tardy.)
- **Deadlines:** Assignments are due at the beginning of the class period on the date specified. Assignments submitted late (within 1 week) will receive **half credit.**
- **DO NOT** send assignments by email.
- Instructor reserves right to change course materials or dates as necessary.

Class Schedule

Week	Weekly Topic
1	Introduction to Forensic Science and the Scientific Method
2	Introduction to Digital Forensics – what is it? Where is it? And what significance does it have?
3	Legal role of the Digital Forensic Analyst
4	Basic practice of Digital Forensics – SOPs/Validation testing/ etc.
5	Hard drive technologies/data storage
6	File systems - FAT
7	File systems – NTFS
8	File systems – EXT3/4, others
9	Deleted data recovery
10	Hashing – what is it? What is it used for?
11	Forensic Imaging – what is a forensic image and why is it important?
12	Forensic Imaging II – tools to acquire and verify media
13	System artifacts – Windows registry
14	System artifacts – Internet History
15	System artifacts – Metadata
16	System artifacts - Linux