NYU TANDON SCHOOL OF ENGINEERING

CS GY696 Digital Forensics - Spring 2020
Professor: Mike Berger, (MSc)^2
mb5811@nyu.edu
Teaching Assistants:N/A

COURSE OVERVIEW

This course introduces students to the application of forensic science principles and practices for collecting, examining, analyzing and presenting digital evidence. The course includes selected topics from the legal, forensic, and information technology domains and utilizes lectures, assignments and projects to illustrate these topics. We will explore these topics through the use of various open-source and free forensic tools.

PREREQUISITES

While there may not be prerequisites listed, to be successful you should have a working knowledge of a computer language and a scripting language - preferably Python. You should also have a working knowledge of computer networks and operating systems.

LEARNING OBJECTIVES

By the end of this course students should be able to:

- Understand and describe how forensic science is applied to the cyber realm
- Identify and describe sources of digital evidence
- Develop custom scripts & programs to perform automated forensic analysis
- Understand file systems and their operational artifacts which both aid and hinder forensic analysis
- Conduct forensic analysis of both disk images and network data
- Acquire and analyze volatile memory
- Identify and describe basic legal principles regarding digital forensics
- Understand and perform basic static and dynamic malware analysis
- Describe how the concepts of digital forensics can be applied to aid in threat hunting

IMPORTANT DATES

- January 27, 2020 - Spring 2020 classes begin
- February 17, 2020 - Presidents' Day (No Classes)
- March 1, 2010 - Final Project Proposal Due
- March 16-22, 2020 - Spring Break (No Classes)
- March 30, 2020 - Midterm Released

- April 5, 2020 - Midterm Due
- May 11, 2020 - Final Project Due
- May 12-14, 2020 - Final Presentations
- May 19, 2020 - Semester Ends

COURSE STRUCTURE

This course is conducted entirely online, which means you do not have to be on campus to complete any portion of it. You will participate in the course using NYU Classes located at https://newclasses.nyu.edu.

LEARNING TIME RUBRIC

Learning Time Element	Asynchronous* / Synchronous**	Time on Task for Students (weekly)	Notes
Lecture (Active Module)	(A)synchronous	2 - 3 hours	Live lecture via NYU Classes, also recorded for anyone who can not view at the scheduled time.
Active participation	Asynchronous	0.25 hours	Students discuss weekly lessons or topics related to the course
Reading & Research	Asynchronous	2.5 hour	Students complete recommended readings (textbook and provided materials) and work on their final project.
Assignments	Asynchronous	3 -4 hours	Students independently work on assignments. Answers and/or source code will be submitted to NYU classes.

*Asynchronous learning is defined as any non-real time student learning, such as recorded lecture, podcast, interactive module, articles, websites, etc. This also includes any student-to-student or faculty-to-student communication that may happen with an asynchronous tool, such as discussion board, chatroom, e-mail, text, etc.

**Synchronous learning is defined as any real-time student-to-student and/or faculty-to-student learning, such as a live webinar session or other video/audio communication service.

WEEKLY MEETINGS

We will meet each week through NYU Classes (Zoom) and go over the content listed on the syllabus. Our meeting day and time will vary each week, to try and allow everyone to attend at least some of the meetings live. For anyone who can't attend live, each meeting will be recorded and posted shortly after, for everyone to view. There is no direct grade penalty for not attending live classes.

ASSIGNMENTS

Students should anticipate 6-8 assignments and having between one and two weeks to complete each, based on the particular assignment's level of difficulty. All assignments are to be submitted via NYU-Classes. Code files are to be submitted separately. Documents are to be submitted in PDF Format. Late submissions may be accepted, however a penalty based on the lateness duration will be imposed. Late submissions of more than five days will not be accepted. Late submission of the midterm & final project will not be permitted.

PARTICIPATION

This component will include interacting with your fellow students, as well as the instructor. The chat function of the live meeting software will allow you to ask questions in real time during the lectures. For anyone viewing the recorded lectures, you will be able to post questions in a section on the NYU Classes discussion board. The board will also be a place where topics pertaining to digital forensics can be discussed with your peers and the instructor.

MIDTERM

The midterm will be given as an assignment to work on at home, similar to the other assignments in the course. The format will involve assessing your ability to perform forensic analysis on provided digital evidence. More details will be provided as the date approaches.

FINAL PROJECT

We will be talking extensively about your final project. It is arguably the most valuable teaching tool in this course. Once you identify your topic/focus, we will work together to ensure your success. The final project will be to either create an open-source forensic tool, or contribute to an open-source forensic project. Previous student topics will be provided in order to give you an idea of the types of projects previously completed for this class. You will be required to submit a project proposal, for which I will provide feedback to help guide your progress. At the end of the semester, you will be presenting a live demonstration of your project to your peers.

WEEKLY VIRTUAL OFFICE HOURS

The instructor will be available for weekly virtual office hours by appointment. To schedule an appointment, or to ask any questions about the course content, please email them.

GRADING

Participation: 10%
Assignments: 20%
Midterm: 30%
Final Project: 40%

COURSE MATERIALS

REQUIRED READING MATERIAL

Title: Digital Evidence and Computer Crime:
Forensic Science, Computers, and the Internet, 3rd Edition
Author: Eoghan Casey
Publisher: Academic Press
ISBN: 9780123742681

RECOMMENDED REFERENCE MATERIAL

Title: Violent Python: A Cookbook for Hackers,
Forensic Analysts, Penetration Testers and Security Engineers
Author: TJ O'Connor
Publisher: Syngress: 1 edition (November 22, 2012)
ISBN: 1597499579

Title: The Art of Memory Forensics
Author: Michael Hale Ligh, Andrew Case, Jamie Levy, AAron Walters
Publisher: Wiley
ISBN: 1118825098

Title: File System Forensic Analysis (1st Ed.)
Author: Brian Carrier
Publisher: Addison-Wesley, 2005
ISBN: 0321268172

PROGRAM POLICIES

MOSES CENTER STATEMENT OF DISABILITY

If you are a student with a disability who is requesting accommodations, please contact New York University's Moses Center for Students with Disabilities (CSD) at 212-998-4980 or mosescsd@nyu.edu. You must be registered with CSD to receive accommodations. Information about the Moses Center can be found at www.nyu.edu/csd. The Moses Center is located at 726 Broadway on the 2nd floor.

CODE OF CONDUCT

Integrity is an integral part of the field of Digital Forensics. As such, students are reminded to review the code of conduct (https://engineering.nyu.edu/campus-and-community/student-life/office-student-affairs/policies/student-code-conduct) as it will be strictly enforced.

COURSE SCHEDULE

The readings specified for each week should be completed prior to attending or reviewing the lecture for week.

Week	Date Range	Topic	Readings
1	1/27 ->2/2	General Introductions and Class Administration	

2	2/3 -> 2/9	Forensic Science, Computers and the Internet Language of Computer Crime Investigations	Casey Ch 1-2
3	2/10 -> 2/16	Computer Basics for General Investigations	Casey Ch 15
4	2/17 -> 2/23	Applying Forensic Science to Computers	Casey Ch 16
5	2/24 -> 3/1	Forensic Tools & Imaging Open Source Forensic Tool Review	
6	3/2 -> 3/8	Network Basics for Digital Investigators Applying Forensic Science to Networks Digital Evidence on the Internet	Casey Ch 21 Casey Ch 22 Casey Ch 23
7	3/9 -> 3/15	Python for Digital Forensics	Violent Python
8	3/16 -> 3/22	***Spring Break***	***Spring Break***
9	3/23 -> 3/29	Investigative Reconstruction with Digital Evidence	Casey Ch 8
10	3/30 -> 4/5	Midterm	Take-home
11	4/6 -> 4/12	Digital Evidence on Windows Systems Digital Evidence on Unix Systems Digital Evidence on MacOS Systems	Casey Ch 17 Casey Ch 18 Casey Ch 19

12	4/13 -> 4/19	Volatile Memory	Casey Ch 13 Supplemental Materials
13	4/20 -> 4/26	Malware Analysis	Casey Ch 13 Supplemental Materials
14	4/27 -> 5/3	Network Forensics	Supplemental Materials
15	5/4 -> 5/10	Incident Response / Threat Hunting	Supplemental Materials
16	5/11 -> 5/17	Final Project Presentations	