The information contained on this page is designed to give students a representative example of material covered in the course. Any information related to course assignments, dates, or course materials is illustrative only.

NYU | TANDON SCHOOL OF ENGINEERING

Course Syllabus

Computer Science and Engineering

CS-6963-Digital Forensics

Course Information

Course Prerequisites

- While there may not be prerequisites listed, students should have a knowledge level equivalent to an undergraduate or higher level course in Operating Systems, and an undergraduate or higher level course in Networking. Additionally, students should be comfortable scripting in Python and familiar with programming in C/C++.

Course Description

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 programming projects to illustrate these topics. We will explore these topics through the use of various open-source forensic tools.

Upon completion of this course you will have acquired the following knowledge:

- 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
- Understand how digital evidence artifacts can aid in an intrusion investigation

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.

Grading Breakdown

- 40% Forensic Analysis Assignments
- 25% Programming Assignments
- 15% Quizzes
- 15% Technical Writing Assignment
- 5% Participation

Course Schedule

Module #	**Topic**
1	Introduction to Digital Forensics
2	Acquiring Evidence
3	Filesystems

4	Open-Source Forensic Tools
5	Windows / Mac / Linux Forensics
6	Advanced Windows Forensics
7	Programming for Digital Forensics
8	Application & Database Forensics
9	Network Forensics
10	Volatile Memory Analysis
11	Malware Analysis
12	Threat Hunting & Incident Response
13	Intrusion Analysis
14	Timeline Analysis

Learning Time Rubric

Learning Time Element	**Asynchronous* / Synchronous****	**Time on Task for**	**Notes**

		Students (weekly)	
Lecture (Active Module)	Asynchronous	1-2 hours	Live lecture via NYU Classes / Zoom, also recorded for anyone who can not view at the scheduled time.
Active Participation	Asynchronous	.25 hours	Students discuss weekly lessons or topics related to the course
Reading	Asynchronous	1-2 hours	Students complete required readings for each module to help reinforce lecture content and prepare for the weekly quiz
Assignments	Asynchronous	4-5 hours	Students independently work on assignments
Quizzes	Asynchronous	1 hour	Students complete the weekly quiz

*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, chat room, 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.

Course Communication

Weekly Meetings

We will meet each week through NYU Classes (Zoom) and go over the content listed on the syllabus. 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, although students should make an effort to attend live whenever possible. Notice will be sent via email if the day/time changes for a specific week.

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.

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.

Announcements

Announcements will be posted on NYU Classes on a regular basis (and automatically emailed to you by default). You can locate all previous class announcements under the Announcements tab of our class. Be sure to check the class announcements regularly as they will contain important information about class assignments and other class matters.

Email

You are encouraged to post your questions about the course in the Forums discussions on NYU Classes. This is an open forum in which you and your classmates are encouraged to answer each other's questions. But, if you need to contact me directly, please email me. You can usually expect a response within 24 hours.

Assignments & Quizzes

Reading Material

Students should expect reading material to be provided each week, to supplement the material presented in the lecture, usually in the form of journal articles and research papers. When provided, this material should be read and understood prior to taking the weekly quiz.

Assignments

Students should anticipate weekly assignments in the class, with work generally being assigned Monday morning, and being due Sunday @ 11:55pm EST. These assignments will help to reinforce the concepts covered in the lectures and the readings, and help build your practical analysis skills. Late submissions will not be accepted.

Forensic Analysis Assignments

These assignments will serve to help students learn practical digital forensic analysis techniques, and are thus one of the most important aspects of the overall class. Most assignments will be found under the "Tests & Quizzes" section of NYU Classes, however there will be no set time limit for the assignment, other than the previously mentioned due date.

Programming Assignments

These assignments will help you apply your programming skills to common challenges you will encounter performing digital forensic analysis which are best served by being able to write a custom script or tool. They will also help to further your understanding of what happens “under the hood” of standard forensic tools, in an effort to elevate your knowledge past the level of “pushing buttons in a tool”. These assignments will be submitted via Gradescope for automated evaluation and feedback. Students will have unlimited submissions up through the due date of the assignment, in order to utilize the feedback provided to improve their submission.

Quizzes

Students should expect a quiz each week, which will cover the content in the lecture, as well as the reading material assigned when applicable. You may take the quiz whenever you are ready, prior to the week ending on Sunday evening @ 11:55pm EST. The quiz is “open-book”, however you should not take it until you have attended/watched the lecture, and read the material, as you will not have enough time to look up every question. These are designed as more of a knowledge check, to ensure you are keeping up with the weekly content and understanding the material. Quizzes will generally have a time limit of about an hour once you start.

Technical Writing Assignment

This assignment involves reading the “The Cuckoo’s Egg”, and writing a comparative technical analysis of forensic techniques used in the book vs. what is currently available today. The book tells the true story of one of the first known instances of a foreign adversary based cyber intrusion, and the subsequent investigation undertaken by the victim entity. The assignment serves as an opportunity for students to develop their abilities to write about advanced technical analysis in order to inform the reader, a fundamental skill within the world of digital forensics.

For this assignment, you will be submitting your paper to Peergrade. As an additional part of the assignment, once papers are submitted, you will be tasked with reading and providing feedback on three of your peer’s assignments. This process allows the assignment to also help you develop skills pertaining to reviewing and providing feedback on technical documents. The feedback process will be anonymous on both sides (you will not know whose papers you are grading, and you will not know who provides the feedback to you), and I will be overseeing the process.

Course Materials

Required Reading Material

1. *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*

   Author: Cliff Stoll

   ISBN: 1416507787

Recommended Reference Material

1. *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, 3rd Edition*

   Author: Eoghan Casey

   Publisher: Academic Press

   ISBN: 9780123742681

2. *The Art of Memory Forensics*

   Authors: Michael Hale Ligh, Andrew Case, Jamie Levy, AAron Walters

   Publisher: Wiley

   ISBN: 1118825098

3. *File System Forensic Analysis (1st Ed.)*

   Author: Brian Carrier

   Publisher: Addison-Wesley, 2005

   ISBN: 0321268172

University Policies

Moses Center Statement of Disability

Academic accommodations are available for students with disabilities. Please contact the Moses Center for Students with Disabilities (212-998-4980 or mosescsd@nyu.edu) for further information. Students who are requesting academic accommodations are advised to reach out to the Moses Center as early as possible in the semester for assistance.

NYU Tandon School of Engineering Policies and Procedures on Academic Misconduct[1]

A. Introduction: The School of Engineering encourages academic excellence in an environment that promotes honesty, integrity, and fairness, and students at the School of Engineering are expected to exhibit those qualities in their academic work. It is through the process of submitting their own work and receiving honest feedback on that work that students may progress academically. Any act of academic dishonesty is seen as an attack upon the School and will not be tolerated. Furthermore, those who breach the School's rules on academic integrity will be sanctioned under this Policy. Students are responsible for familiarizing themselves with the School's Policy on Academic Misconduct.

B. Definition: Academic dishonesty may include misrepresentation, deception, dishonesty, or any act of falsification committed by a student to influence a grade or other academic evaluation. Academic dishonesty also includes intentionally damaging the academic work of others or assisting other students in acts of dishonesty. Common examples of academically dishonest behavior include, but are not limited to, the following:

  a. Cheating: intentionally using or attempting to use unauthorized notes, books, electronic media, or electronic communications in an exam; talking with fellow students or looking at another person's work during an exam; submitting work prepared in

[1] Excerpted from the Tandon School of Engineering Student Code of Conduct

advance for an in-class examination; having someone take an exam for you or taking an exam for someone else; violating other rules governing the administration of examinations.

b. Fabrication: including but not limited to, falsifying experimental data and/or citations.

c. Plagiarism: intentionally or knowingly representing the words or ideas of another as one’s own in any academic exercise; failure to attribute direct quotations, paraphrases, or borrowed facts or information.

d. Unauthorized collaboration: working together on work that was meant to be done individually.

e. Duplicating work: presenting for grading the same work for more than one project or in more than one class, unless express and prior permission has been received from the course instructor(s) or research adviser involved.

f. Forgery: altering any academic document, including, but not limited to, academic records, admissions materials, or medical excuses.