Northeastern University
Khoury College of
Computer Sciences

Master of Science in Cybersecurity

NSA/DHS Designated Center of Academic Excellence in
Information Assurance/Cyber Defense, Research and Cyber Operations

Information System Forensics

Course Number: CY5210
Total Credit Hours: 4
Course Schedule: 13 September – December 17, 2022
Class Location: Tuesdays 6-920PM EST; Hayden Hall 322 (HA 322)
Instructor: Elton Booker
Email: e.booker@northeastern.edu

Course Description

This course will explore various digital forensic and incident response methodologies, techniques, and legal aspects of examinations of computer systems and networks. Students will be exposed to a variety of forensic tools and technologies used to collect and analyze evidence for case preparation. Particular attention will be given to legal issues and challenges faced by practitioners such as evidence collection, preservation, chain of custody best practices, proper documentation and reporting.

At the end of the course students will understand what it takes to put together a comprehensive digital forensic program including tools, checklists, processes and procedures, as well as the legal issues and standards required to forensically obtain evidence and maintain the integrity of that evidence. Finally, students will learn the steps to gather facts in a timely manner and complete a forensic report that accurately details the investigation for possible use in a legal setting.

Required Textbooks

There are no required textbooks for this course at this time. The instructor will use a combination of open source standards, best practices, published journal articles, public media releases, and personal knowledge to present forensic best practices.

Hardware Requirements

Lab assignments and case studies will require a minimum amount of disk drive space, memory, and processing power. Core labs and case projects will require students to use a virtual machine or to install forensic software on their primary Windows host system.

Hardware requirements include at least 250GB of free hard drive space, 8-16GB of RAM, and at least 2-4 processor cores for forensic labs (or cloud storage). In addition, an external HDD of at least 256GB should suffice for evidence files, output files, and applications used in the course. Students have had success deploying their forensic workstation in AWS or Azure instead of on their personal system, but this would be a trial basis or at their expense.

Course Objectives

Upon successful completion of this course, students will develop abilities to:

- Define processes for the collection, preservation, analysis and reporting of evidence.
- Understand processes for criminal, civil and corporate investigations.
- Acquire a forensically sound image and complete a chain of custody document.
- Assist in the formulation and implementation of policies and procedures.
- Develop a profile of individual user or attacker activity.
- Recover deleted and/or intentionally hidden information.
- Image, process, and analyze a mobile device.
- Complete a network forensic investigation.
- Complete analysis of system RAM for intrusion investigations.
- Determine the manner in which an operating system has been subverted.
- Determine when forensic techniques can support incident response actions.
- Complete analysis of TTPs and utilize industry models for cyber threat intelligence.
- Draft forensic case reports outlining technical analysis and scientific processes.

Course Methodology

Each week, you will be expected to:

1. Review the week's learning objectives.
2. Complete all assigned readings.
3. Complete all lecture material for the week.
4. Complete and submit all assignments by the due date.

Grade Breakdown

Assignment Type	Percent of Grade
Participation (Discussion Board)	10 %
Lab Assignments (6 x 25)	15 %
Case Studies (4 x 100 points)	40%
Research / Technical Short Paper	10 %
Midterm	12.5 %
Final Exam	12.5 %
	100%

Late submissions will result in a 10% penalty per day (e.g. 3 days late results in 30% penalty).

Course Communications

This course is using Piazza as its main method of communication. The use of Piazza is highly recommended for asking questions about the course content and assignments. When communicating with the TAs it is particularly important that you use Piazza, so the Instructor or the TAs can be sure that your questions was answered in less than 24 hours. Your

question may help your classmates and allow them to answer your questions too (those answers will be reviewed by the instructor or the TAs). Remember that Piazza also allows the sending of private messages if needed.

Email communication: students can expect that emails will be answered within 24 hours on week days and 48 hours on weekends.

Class Participation (Discussion Board)

Student participation and the completion of assigned discussion boards is mandatory. There are ten discussion forums scheduled and they will cover topics related to the course material. Each forum will have questions or current event topics that students need to answer or comment on. The discussion forum will be open on Monday and students need to post one "primary response" by Wednesday 11:59pm (two or more paragraphs). Then, between Friday and Sunday 11:59pm, students need to comment/ respond to two "primary responses" from other students (one or more paragraphs). Source links should also be included, when appropriate, and your opinion and experience related to the subject should be in your own words.

Weekly Class Sessions

Weekly class sessions will be held on Tuesday evenings, unless otherwise communicated. The instructor may request input from students regarding topics to cover, will address topics related to current events, and will allow for open discussion and questions from students. If schedule conflicts arise, sessions will be recorded. The majority of topics will also be recorded and posted on Canvas when relevant.

Lab Assignments

Each lab provides an opportunity to demonstrate proficiency with the tools and techniques demonstrated in class. Each student is required to complete all labs and turn in a lab document or the requested output. Collaboration is encouraged and students can request assistance to complete each lab. However, simply copying or providing other students with lab work is inappropriate and will not be tolerated; students must submit their own work. Lab assignments and case studies will provide hands-on training which may include commercial forensic software suites, open source software tools, and labs created by the instructor.

Case Studies

There will be four case studies during the semester that are intended to serve as real examples of actual forensic cases an analyst or examiner may need to analyze in the field. All case reports should be 10-15 pages of text (not including screenshots or tables), single spaced, 12 point font, with one inch margins. The case report should include an executive summary, introduction, analysis and conclusion (at a minimum).

Technical Paper

Each student is expected to complete a short research papers during the course, with 4-5 pages of content, researching and citing public information sources, other than Wikipedia. All papers should be grammatically correct and have proper syntax. The preferred formatting method is the Chicago Manual of Style. A rubric will be available on Canvas.

Academic Integrity

Students must read the Academic Integrity Policy and email the instructor by the end of the first week of class (or upload a file to Canvas) acknowledging that they have read, understand and will adhere to the university's policy requirements which are available at http://www.northeastern.edu/osccr/academic-integrity-policy/.

Student Accommodations

Northeastern University and the Disability Resource Center (DRC) are committed to providing disability services that enable students who qualify under Section 504 of the Rehabilitation Act and the Americans with Disabilities Act Amendments Act (ADAAA) to participate fully in the activities of the university. To receive accommodations through the DRC, students must provide appropriate documentation that demonstrates a current substantially limiting disability.

For more information, visit https://drc.sites.northeastern.edu/.

Class Schedule and Due Dates

Week	Topic	Assignment
1	Introduction to Digital Forensics	AIP Agreement Lab 0
2	Evidence Collection and Acquisition	Lab 1
3	Windows File System and Registry Analysis	Lab 2
4	Windows User Activity Analysis*	Lab 3
5	Linux and macOS Triage and Analysis*	Case Study 1
6	Mobile Device Analysis*	Lab 4
7	**Midterm Exam*** **	-
8	Introduction to Incident Response	Case Study 2
9	Introduction to Network Forensics	Lab 5
10	Introduction to Cyber Threat Intelligence (CTI)	Case Study 3
11	**Thanksgiving Break - NO CLASS**	-
12	E-Mail Forensics and E-Discovery	Case Study 4
13	Memory Analysis and Malware Triage	Lab 6
14	**Final Exam*** **	Technical Paper

**This schedule is subject to change as the instructor sees fit to accommodate for current technologies.
***A complete course schedule with applicable dates will be available on Canvas.