Syllabus

ITMS 538: Cyber Forensics – v1

Don Nelson, Fall 2022

Faculty Information

Professor: Don Nelson
Address: 201 E Loop Rd., Wheaton, IL 60189
Telephone: 630.474.5218
Office Hours: By appointment
Email: dnelson@iit.edu

Lab (RADISHng) Manager: Phil Matuszak
<fill out trouble ticket and contact me regarding any RADISH issues>

Course Description

This course will address methods to properly conduct a computer and/or network forensics investigation including digital evidence collection and evaluation and legal issues involved in network forensics. Technical issues in acquiring court admissible chains-of-evidence using various forensic tools that reconstruct criminally liable actions at the physical and logical levels are also addressed. Technical topics covered include detailed analysis of storage media, files systems (including FAT, NTFS and EXT), mobile devices, databases and applications; mechanisms for hiding and detecting hidden information; and the hands-on use of powerful forensic analysis tools.

Prerequisites

A basic knowledge of computer and Internet components and architecture and operating system internals. Ability to do some scripting and/or coding.

Course Objectives and Outcomes

These objectives and outcomes should be considered close to but not exhaustive. Because of rapidly changing technology, a modest amount of material will likely be added or modified.

Each successful student in this course will be able to:

- Demonstrate knowledge of cyber forensic analysis at levels ranging from professional to executive levels including applicable legal issues.
- Apply this knowledge to planning and executing specific cyber forensic analyses. This includes the use of cyber forensic tools.
- Conduct basic DFIR (Digital Forensics and Incident Response) corporate, civil and criminal investigations.

Students satisfactorily completing this course will have the knowledge, ability and tools to perform cyber forensic analysis; similar to the computer investigations shown on the *CSI* series. This class will provide an excellent preparation for students hoping to go into the field of Digital Forensics.

At the successful completion of this course each student should be able to:

- Demonstrate knowledge of cyber forensic procedures, planning of analyses and the use of common tools for analysis
- Describe several file systems including FAT, EXT, YAFFS and NTFS.
- Describe several common booting procedures.
- Describe how to find file system objects that have been deleted or obfuscated.
- Describe how to track past computer and Internet activity and to establish time lines for this activity.
- Describe techniques for inserting covert information in various text, document and image carrier files.
- Demonstrate the ability to use tools such as WinHex, SleuthKit and Autopsy. Also, several forensic imaging, carving and discovery tools.

Session Days, Time and Location

Wednesdays from 6:30 - 9:00 pm U.S. central time via Zoom (online).
Lectures and Labs will be conducted in an integrated fashion during class lecture.
Lectures will be recorded and posted on Blackboard

Course Deliverables

Course deliverables will include assignments and exams. Assignments will be made on a week-by-week basis. All assignments will be submitted via Blackboard in pdf format. Also, unless otherwise specified, assignments will be due on or before 11:55 pm on the 2nd Sunday following the date that they were assigned. This should accommodate most extenuating circumstances that students may encounter.

Grading

Short quizzes may be included depending upon the needs of the class in areas such as those listed in the *Prerequisites* section. The grading breakdown is:

Midterm Exam:	30%
Final Exam:	30%
Assignments and Labs	40%

Grading scale:
A: >= 90%
B: >= 80% and < 90%
C: >= 65% and < 80%
E: <65%

Exams will include a 2-part midterm and final.

Texts

B. Nelson, A. Phillips, C. Steuart, ***Guide to Computer Forensics and Investigations, 6th edition***
Cengage Learning
ISBN: 978-1-337-56894-4
Includes 1 DVDROM
Publication date: 2019

B. Carrier, ***File System Forensic Analysis,*** *Addison Wesley*
ISBN-13: 978-0321268174; ISBN10: 0-32-126817-2
Publication date: 2005

Assignments & Take-Home Labs

Assignments will generally correspond to the lecture topics, which in turn will correspond to the texts, modified by rapidly evolving technology. The evolving nature of operating systems, data networks and cyber forensics requires continual upgrading of labs and assignments.

Class and Lab Resources

Lecture and lab assignments will make use of *RADISHng* (**R**emotely **A**ccessible **D**ynamic **I**nternet for **S**tudents to **H**ack **n**ext **g**eneration). *RADISHng* allows students to do hands-on labs remotely and provides extended classroom capability. (*RADISH* was developed by forensic and security students and faculty at IIT, *RADISHng* was developed by the faculty and staff with student help; it is near completion.) However, all assignments and exams will be submitted via Blackboard unless otherwise specified.

RADISHng is the result of a grant from the U.S. National Security Agency (NSA). *RADISHng* evolved from the original *RADISH* system funded by IIT's School of Applied Technology.

Internet students can attend class in real or delayed time via two streaming videos that are identified for each class session in the ***Course Schedule***.

Arrangements have been made with several cyber forensic vendors for the use of expensive forensic analysis tools and software in the ForSec Lab and on *RADISHng*. These tools and software are limited to ForSec Lab and *RADISHng* use.

You will need good Internet access to make remote use of RADISHng. Up to and including the autumn 2019 semester, Internet access via Comcast and WOW in the Chicago metro area has been sufficient.

Academic Honesty

Plagiarism:

All work you submit in this course must be your own. You must fully attribute all material directly quoted in papers and you must document all sources used in the preparation of the paper using complete, APA or ACM-style bibliographic entries. Including directly quoted material in an assignment without attribution is always plagiarism and will always be treated as such by me. No more than thirty-three percent of material included in any paper may be direct quotes. If you submit plagiarized material, you WILL receive a grade of ZERO for the assignment, an Academic Honesty Violation Report will be filed, and it may result in your expulsion from the course with a failing grade as per the IIT and ITM academic honesty policies. There is no excuse for not understanding this policy and if you do not understand it, please let me know and I will be happy to discuss it with you until you do.

Collaboration:

Students may only collaborate on assignments or projects that are explicitly designated as group assignments or projects. Students submitting work that is identical or in some cases even substantively the same will be asked to discuss the assignment with the instructor. If one student admits to having copied the work, or if there is clear evidence who is guilty, the guilty student will be assigned a grade of zero. If no one admits to the offense or a reasonable determination of guilt cannot be made, each student involved will be assigned a grade of zero. In either case, an Academic Honesty Violation Report will be filed, and it may result in your expulsion from the course with a failing grade as per the IIT and ITM academic honesty policies.

Disabilities

Reasonable accommodations will be made for students with documented disabilities. To receive accommodations, students must obtain a letter of accommodation from the Center for Disability Resources and make an appointment to speak with me as soon as possible. My office hours are listed on the first page of the syllabus. The Center for Disability Resources (CDR) is located in 3424 S. State St., room 1C3-2 (on the first floor), telephone 312.567.5744 or disabilities@iit.edu.

Contract

This syllabus is a contract between the students and the instructor. It defines what the instructor will deliver and what the instructor expects from the students. It may be necessary to make changes to the syllabus as the course progresses; this is especially true of the Course Schedule. The latest version will be posted to Blackboard as quickly as possible. Revisions to readings and assignments will be communicated via Blackboard.

Course Schedule

Session	*Topics*
01 Wed 24aug22	Course Introduction. ForSec Lab Discussion. Introduction to Network & Computer Forensics.
02 Wed 31aug22	Computer Investigations. Forensic Tools and Tool systems
03 Wed 07sep22	Certification: Investigators and Laboratories. Proc. Crimes & Incidents.
04 Wed 14sep22	Data Acquisition & Image Creation. Mass storage. Solid state (flash) and rotating magnetic drives.
05 Wed 21sep22	Volumes & Partitions. MBR Partitions. GPT Partitions.
06 Wed 28sep22	Linux Boot & Disk & Partitions. File Systems (FAT, NTFS, EXT).
07 Wed 05oct22	Sleuthkit. Autopsy. FTK Imager. Linux forensic tools. Midterm review.
08 Wed 12oct22	**Midterm Exam** (2 parts). 1. Exam taken on Blackboard. 2. Forensic examination of forensic drive image. No online streaming.
09 Wed 19oct22	File carving. File carving analysis & lab.
10 Wed 26oct22	ADS. ADS Lab.
11 Wed 02nov22	Email and Social Media Investigations. Email and Social Media forensic lab.
12 Wed 09nov22	Mobile Device Forensics. Cloud Forensics.
13 Wed 16nov22	Digital Image Forensics.
Wed 23nov22	**Thanksgiving Break.** No class.
14 Wed 30Nov22	Virtual machine forensics. Live acquisitions. Network forensics.
15 Wed 07dec22	**Final Exam** (2 parts). 1. Exam taken on Blackboard. 2. Forensic examination and report. No online streaming.

Text and verbal communication between viewer and instructor are available during the actual lecture.

Recordings of all videos will be available for review on Blackboard until the end of the semester.

Labs will accompany many class sessions and assignments. Labs will be discussed or demonstrated in class. Lab reports will be required as part of assignments.

The "**Topics**" column (the larger right column of the class schedule) is subject to change, especially toward the end of the semester.