ECE 8496: Computer Forensics

Class Meetings

Sections 8496-001, 8496-DL1: Thursday, 6:10-8:50PM, CEER 307

Instructor

Name: Dr. James Solderitsch

Office location: Tolentine Hall Rm 404

Office phone number: (610) 519-4975; Cell phone number: (484) 612-5500

Email: james.j.solderitsch@villanova.edu

Office Hours

Wed. 11:00 am – 12:00 pm, Thurs 4:00 pm – 5:00 pm, other times by appointment (Zoom Teleconferencing Enabled)

Course Objectives

The main instructional areas that will be covered in this course include:

- Digital forensic investigations
- Forensic environments and tools
- Evidence collection and handling
- Forensic reporting
- Solving business challenges with forensic investigations
- Tactical Digital Forensics and Incident Response (DFIR)

In covering tactical DFIR, the course will introduce and apply various open source tools and techniques.

After taking this course, you should be able to:

- Summarize the basic principles of computer forensics.
- Summarize important laws regarding computer forensics.
- Describe various computer crimes and how they are investigated.
- Describe digital forensic methodology and labs.
- Outline the proper approach to collecting, seizing, and protecting evidence.
- Explain techniques for hiding and scrambling information as well as how data is recovered.
- Summarize various types of digital forensics.
- Explain how to perform a network analysis.
- Describe incident and intrusion response.
- Identify trends in and resources for digital forensics
- Become familiar with modern methods in tactical DFIR

Class topics for this course include:

Anti-forensics	Attacks	Chain of Custody

Computer Forensics	Cryptography	Cybercrime
Digital Forensics	E-mail Forensics	Evidence
Expert Testimony	Forensic Investigation	Forensics
Incident Recovery	Incident Response	Laws
Linux Forensics	Macintosh Forensics	Malware
Mobile Forensics	Network Analysis	Privacy Laws
Steganography	System Forensics	Windows Forensics

Grading Policy

Your final grade will be determined based on a percentage score out of 400 points where the points will be based on the following course activities:

Virtual Labs

- All labs required (15) – must have lab access token: acquire ASAP
- Contributions will be graded based on submitted materials as required per lab
- 10 points per lab (total points: 150)

Quizzes – 4 over the semester – use as Final Exam preparation

- 10 points per quiz (total: 40 points)
- Short answer/multiple choice or one long answer
- Questions from text material and topics covered in class or selected readings

Final Exam

- Conducted through Blackboard
    - Comprehensive over semester
    - Short answer and objective questions
- 80 points

Research Presentation

- Course project or research presentation: Expected Focus on Tactical Digital Forensics and Incident Response (DFIR)
- Delivered as VoiceThread submission via Blackboard (details to be provided)
- Topic must be approved by instructor
- 50 points

Presentation Peer Review

- Peer review of 2 Presentations as VoiceThread comments: 10 points (5 per review)

Other

- Class Participation on Yellowdig site: 70 points

Total points for course: 400

The scale used to assign letter grades is:

Letter Grade	Numerical Grade	Letter Grade	Numerical Grade
A	94 to 100	C+	77 to 79
A-	90 to 93	C	73 to 76
B+	87 to 89	C-	70 to 72
B	83 to 86	F	Less than 70
B-	80 to 82		

Attendance

The following paragraph on attendance, along with the list of excused absences, comes from the College of Engineering and is a required element of the syllabus.

Where possible, students should inform their instructors if they plan to be late or absent from class. In all cases, students should be prepared to provide documentation to petition for *excused* absences to the appropriate Associate Dean. The form for requesting an *excused* absence can be found here (http://www1.villanova.edu/villanova/engineering/resources/policies/forms/studentAbsence.html). Excused absences do not count toward a failure in the course for first year students. Absence from class does not release the student from work assigned. Students who miss an in-class obligation (exam, presentation, etc.) due to an excused absence will not be penalized - the instructor may offer a make-up test, arrange an alternative time for a presentation, exempt a student from the assignment, or provide another arrangement.

The University's list of excused absences for all students includes the following:

- participation in NCAA athletic competitions
- participation in special academic events (e.g., conferences, field trips, project competitions)
- participation in official university business (e.g., student representatives attending meetings related to university governance)
- attendance at significant events involving the immediate family (e.g., funerals, weddings)
- religious holidays - see the University's policy on Religious Holidays
- college-approved participation in placement activities (e.g., job interviews, graduate school interviews, attending job fairs)
- documented serious illness or disability (see below how to document)

This course is available as both an in-class section (001) offered in CEER 307 and as a distance learning section (DL1). DL1 students are encouraged, if their schedule permits, to attend in person at the regularly scheduled class time. 001 students may elect to attend the class remotely just like the DL1 students. However, it is highly recommended that students keep up with the class on a weekly basis. If circumstances, such as a work assignment or illness, cause a student to miss the weekly class, it is expected that an email is sent to the instructor documenting the nature and length of the class disconnect. Assignments will have due dates and normally a student is expected to complete all assignments on or before the posted due date. Please review the Deadlines section later in this syllabus.

Students are expected to (virtually) attend every class. Slides used in class and saved on Blackboard may have some of the material covered, but not all or even most. Students may contribute insightful information during class that you can learn from. **You are responsible for everything covered in class, regardless of whether the material is addressed in the readings or handouts or on Blackboard.**

Course Materials

There is a text book for this course:

Easttom, Chuck. *System Forensics, Investigation, and Response, 3rd* Edition., Burlington, MA: Jones & Bartlett Learning, 2019, ISBN: 978-1-284-12184-1

The Virtual Labs are from the InfoSec Security Digital Forensics Fundamentals Lab Sequence. Information on acquiring a token to access these labs will be provided in class.

In addition, the class will feature numerous resources that will be posted on Blackboard.

Academic Integrity

The College of Engineering is committed to creating an environment of academic integrity and ethical decision-making that we hope is reflected in the actions of our students and graduates. As Villanova students, integrity is central to the University mission. As engineers, our code of conduct requires us to place honor and integrity at the forefront of everything we do. As engineering students, it is expected that you will begin to adopt these values and instill them into your work habits. Students violating the academic integrity policy will receive a zero on that assignment or exam and the violation will be reported to the Associate Dean for Academic Affairs.

The University's academic integrity policy can be found here: https://www1.villanova.edu/villanova/provost/resources/student/policies/integrity.html.

The College of Engineering has adopted the following exam guidelines:

- Students must arrive before the start of the exam. Under exceptional circumstances a student may need to arrive late, but he/she can enter the exam no later than 5 minutes after the start of the exam.
- All cell phones must be turned off and stored away until the student exits the exam room.
- The official Villanova class attendance policy must be followed when requesting excuses for absences or lateness to an exam.
- Each student must write and sign the following statement, "*I have neither given nor received any unauthorized assistance in the completion of this exam.*"

The statement given above about exam protocol is meant for in-class exams that will not be part of this course.

Don't be evil

The knowledge you gain in class is for educational purposes only. You may gain powers in this class that you are duty and honor bound not to misuse. You will promise not to scope out, attack, subvert or disrupt Villanova ECE, Villanova, corporate, county, US state or federal computer systems. US State and Federal law does not take these things lightly - prison and $10,000s of fines. Foreign students will probably lose their visa and be deported. Be careful with what you do and where and how you do it.

Students with Disabilities

It is the policy of Villanova to make reasonable academic accommodations for qualified individuals with disabilities. If you are a person with a disability please contact me after class or during office hours to make arrangements.

If you have a non-physical disability you need to register with the Learning Support Office by contacting 610-519-5176 or at learning.support.services@villanova.edu as soon as possible. Registration is needed to receive accommodations.

The Office of Disability Services collaborates with students, faculty, staff, and community members to create diverse learning environments that are usable, equitable, inclusive and sustainable. The ODS provides Villanova University students with physical disabilities the necessary support to successfully complete their education and participate in activities available to all students. If you have a diagnosed disability and plan to utilize academic accommodations, please contact and register with Gregory Hannah, advisor to students with disabilities @ 610-519-3209 or visit the office on the second floor of the Connelly Center.

Schedule

The following calendar of the course is tentative. The first 8 weeks will emphasize material drawn from the class text. Subsequent weeks will not cover text-based material at all, allowing more time to focus on tactical Digital Forensics and Incident Response. Thursday, April 18 is not a class day.

DATES AND TOPICS ARE SUBJECT TO CHANGE

January 17:	Overview of Course; Lab access and expectations; *Lab 1*; Introduction to Forensics (ch 1); Overview of Computer Crime (ch 2)
January 24:	Forensics Methods and Labs (ch 3); *Lab 2*; SANS SIFT Forensics Platform
January 31:	Collecting, Seizing and Protecting Evidence (ch 4); *Lab 3*; *Quiz #1*; More on DFIR; Case Study
February 7:	Techniques for Hiding and Scrambling Information (ch 5); Recovering Data (ch 6); *Lab 4*; More DFIR Case Study
February 14:	Email Forensics (ch 7); Windows Forensics (ch 8); Linux Forensics (ch 9); *Lab 5*
February 21:	Macintosh Forensics (ch 10); Mobile Forensics (ch 11); *Lab 6*, DFIR Case Study
February 28:	Performing Network Analysis (ch 12); *Lab 7*; DFIR Memory Analysis; [*Lab 8*; *Quiz #2* (leading into Spring Break)]
March 14:	Incident and Intrusion Response (ch 13); Trends and Future Directions (ch 14); Systems Forensics Resources (ch 15); *Lab 9*; Hands-On with NetWitness and OSForensics
March 21:	REMnux and Malware Analysis; Google GRR; Memory Analysis; *Lab 10*; *Quiz #3*; Research Presentation topic submitted and approved
March 28:	Registry Forensics; Docker Technology for Forensics; Docker Examples; Elastic Stack with Docker; Log Analysis Application; *Lab 11*; *Quiz #4*
April 4:	Docker Continued including Elastic Stack with Docker; Kubernetes for SOC/Forensics Platform; UEBA: User Entity Behavioral Analytics; Incident Response; *Lab 12*
April 11:	UEBA: User Entity Behavioral Analytics; Cymmetria Maze Runner for Active Defense; Incident Response and

	Orchestration; Hands-On with Phantom platform; *Labs 13 and 14*; Research Presentations submitted
April 25:	*Lab 15* Forensic Case Capstone; Legal Forensics Re-Cap; Splunk Intro and Hands-On; Research Presentation peer reviews
May 2:	Semester Wrap-Up; *Final Exam due May 11*

Assignments

Assignments and Labs for this course will be distributed throughout the course and typically be due within 1 to 2 weeks from the class at which they are assigned. Detailed preparation and submission instructions will be provided when the assignment is made available.

Virtual Labs

A link to enroll in the InfoSec Security Labs offering will be provided in the first class. There are 15 labs in all and to some degree later labs build on the skills acquired in the earlier labs. Lab reports will be required for each lab that will include screen shots captured while you are taking the lab along with answers to questions about what you learn/discover while executing the lab instructions.

Quizzes

Material for quizzes (4 in all) will be drawn from the text book's topics as well as additional material brought to your attention throughout the semester. Recent emerging events and approaches related to forensics are often made available through recorded webinars. At least one quiz will ask for your reaction and opinion after watching one of these webinars.

Semester Presentation Project

The instructor must approve presentation topics. Suggestions will be given during the semester. You will submit a recorded presentation via the VoiceThread mechanism on Blackboard of your research results. An outline of the expected content for the presentation will be described shortly after all topic proposals have been made and approved. You will also perform at least 2 peer reviews of other student presentations.

Final Exam

While the exam will not include a large number of questions, it will be comprehensive.

Deadlines

Submissions of exam and assignment response are done via Blackboard by midnight of the posted due or completion date. Late submission of any lab or assignment may be subject to a deduction of 2 percentage points from the grade for the late lab or assignment per business day per offense. For example, for a lab worth 10 points, 0.2 points could be deducted per day. This penalty will be deducted from the lab/assignment grade as determined by the other course requirements.

Prerequisites

There are two catalog-noted pre-requisites for ECE 8496. They are ECE 8484: Cybersecurity Threats and Defense, and ECE 8476: Cryptography and Network Security. I have been inclined to routinely waive ECE 8476 for the initial offerings of this course but students should not begin their Cybersecurity course program

with a course such as Computer Forensics – ECE 8484 is a good beginning course. Future versions of this course may require stricter enforcement of the noted prerequisites. Consultation with the instructor is always a good idea if either of the prerequisites (or related) courses are missing from a student's background.