

Digital Forensics and Computer Criminology

Class Schedule: Monday through Friday - Online

Location: Online - Canvas/Zoom

Final Exam: Due by Sunday of finals week

Instructor: Chad Johnson
Office: ALB 024
Phone: 715-346-2020
Email: Chad.Johnson@uwsp.edu
Office hours: Tuesdays and Thursdays 10:00am - 11:00am

Course Description

This is an introductory course on digital forensics to provide the student with a base of knowledge on the indicators of compromise of various systems, the use of common forensics tools, and a description of the strategies used during digital forensics. There will be a focus on the investigative process, deductive and inductive reasoning, criminal profiling and forensic psychology. The victimology and case law of computer crimes will be introduced. Finally, the course will cover how to describe the process of acquiring, evaluating, and preserving digital evidence, with practical application of forensic techniques used in digital investigations.

Course Objectives

- Understand the use of digital forensic tools and techniques.
- Understand the acquisition, validation, and preservation of digital evidence.
- Gain the ability to determine the authenticity of digital evidence.
- Understand the victimology, profiling, and case law associated with computer crimes.

Textbook

- *Cybercrime and Digital Forensics*, 2nd Edition, By Thomas Holt, et al. ISBN: 978-1138238732

Lectures

- Lecture notes MIGHT be posted in Canvas. Honestly, I make every effort to make my notes available, but I may decline to include them at my discretion.
- Students are strongly encouraged to attend each class and actively participate in class discussions. You are also encouraged to participate in discussions and assignments

Note: Schedule / Syllabus is tentative and subject to change.

- In general, I do not believe in taking attendance. However, class attendance may be taken in any class without notification in advance.

Grading

- 4 Assignments: 30%
- 2 Exams / Papers: 40% (20% each)
- 1 Forensic Challenge / Final Paper: 30%

Final grades will be assigned according to the following scale:

| | | |
|----------------------------|----------------------------|----------------------------|
| A: score \geq 90 | A-: 87 \leq score $<$ 90 | |
| B+: 83 \leq score $<$ 87 | B: 80 \leq score $<$ 83 | B-: 77 \leq score $<$ 80 |
| C+: 73 \leq score $<$ 77 | C: 70 \leq score $<$ 73 | C-: 65 \leq score $<$ 70 |
| D: 60 \leq score $<$ 65 | | |
| F: score $<$ 60 | | |

Scale may be adjusted, depending on the overall performance of the class.

Exams

- Paper exams taken in class are closed book and no-computers/phones, but open-notes - whatever you can write onto the front and back of a single 3" x 5" standard index card. If you print this, use 14pt Times New Roman font, and be double-spaced. I do not often give paper exams these days, but I might so I leave this here.
- Exams taken on Canvas are open-book, and you are free to use all resources at your disposal to complete the exam. Plagiarism and cheating, however, will not be tolerated. NO collaboration is allowed on exams.
- Final exam is NOT comprehensive.
- In general, any test or exam CANNOT be made up.
- If you miss a test or exam due to unavoidable circumstances (e.g., health), you must inform the instructor as soon as possible. A written explanation along with the supporting documents must be submitted to the instructor upon request.

Assignments and Deadlines

- Labs are NOT GRADED, but they are worth bonus points based on effort (not result.) There are 6 labs. 1 is worth 0 bonus points (it's an introductory lab.) The remaining five are worth UP TO 1% each in bonus points, equaling a 5% bump. Since these are bonus points, the grading will be extraordinarily strict - you will need to do exceptionally well.
- There is also a bonus assignment worth UP TO 5%. Note that it will be near impossible to get the full 5% as the challenge has varying difficulty and you will receive no direct instruction on it (though you will learn everything you need to know to complete it in this class.)
- Each assignment must be submitted by 11:59pm on the day it is due. **Late submissions must be submitted to the Late Submissions dropbox. They will be considered in my own time for reduced points.**

Note: Schedule / Syllabus is tentative and subject to change.

Note: Schedule / Syllabus is tentative and subject to change.

- The forensic challenge is due by 11:59pm on its due date. You can still turn in the forensic challenge after the deadline. However, you automatically lose 5 points per hour after the due time, until you get zero. **I will not waive the penalty, unless there is a case of illness or other substantial impediment beyond your control, with proof in documents from the school.**
- You must submit your assignments online through Canvas. **I will not take submissions in email, unless the university verifies that Canvas was malfunctioning or unavailable.**
- All sources should be parenthetically cited and included in a Works Cited list at the end of each paper. Use APA citation. Uncited sources will reduce your grade. Plagiarism will not be tolerated. Case law citations should be done in italics (i.e. *U.S. v. Lopez*).
- All papers should use 1” margins, 12pt Times New Roman font, and be double-spaced.
- This class uses blended assignments and exams. One list is for students enrolled in SOC-395, the other for students enrolled in CIS-347/WD-347. See the list at the end of the syllabus for guidelines on the different assignments.

Office Hours Policy

- I prefer that you contact me via email.
- However, you are still welcome to my office to ask me any questions at any other times.
- I fear the phone.
- For online courses, standing Zoom meetings will be held. You can join them anytime to speak with me. I essentially sit there in the meeting during these times just to be available to students. If I do not let you into the meeting right away, be patient - that means I'm with another student. I will let you into the meeting as soon as I'm free.

Regrading

Scores of Assignments, Forensic Challenge, and Exams will be posted in Canvas, and announcements will be made in Canvas. After the scores are announced, you have 7 days to request for regrading by contacting the instructor (office hours or email). Your grade will be final after 7 days.

Canvas

The Canvas URL is <https://canvas.uwsp.edu>. Use your UWSP NetID and password to login. We use Canvas for announcements, assignments, and exams. You will need to use it.

Academic Integrity

The university cannot and will not tolerate any form of academic dishonesty by its students. This includes, but is not limited to cheating on examinations, plagiarism, or

Note: Schedule / Syllabus is tentative and subject to change.

Note: Schedule / Syllabus is tentative and subject to change.

collusion. **Any form of academic dishonesty may lead to F grade for this course. I assure you I take this extremely seriously.**

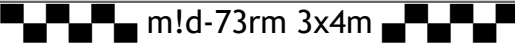
Students with Disabilities

If you require accommodation based on disability, please let me know. I am willing to provide any reasonable accommodations you require. The sooner you inform me the better.

Note: Schedule / Syllabus is tentative and subject to change.

| CIS-347 Assignments | SOC-395 Assignments |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p data-bbox="298 142 847 617"><i>Investigations</i> - A scenario will be provided. The scenario will reproduce the circumstances of an actual investigation. You will follow the directions in the assignment to gather the relevant digital evidence. You will submit this evidence with a short paper. Each paper should be no less than 750 and no more than 4000 words (about 3 to 15 pages.) The paper you will write will include a Forensic Report and a Threshold Assessment, which includes:</p> <ul data-bbox="347 659 834 987" style="list-style-type: none">• A statement of facts: Who are the parties involved, what is being examined, how it the evidence being gathered, and what does the evidence indicate?• Opinion brief: In your opinion as the investigator, what facts do your findings convey? <p data-bbox="298 1029 828 1318"><i>Forensic Challenge</i> - Your role in the forensic challenge will be to gather the digital evidence from a suspect virtual computer and submit that evidence to your group. Be sure to write a forensic report for all the evidence gathered, and that you follow proper procedure.</p> | <p data-bbox="870 142 1406 357"><i>Case Briefs</i> - A group of cases will be offered. You will select one. Each paper should be no less than 1500 and no more than 4000 words (about 6 to 15 pages.) The legal brief you will write will have these sections:</p> <ul data-bbox="919 399 1419 1171" style="list-style-type: none">• A statement of facts: Who are the parties in the case, what is their dispute, how did they get to this point?• Legal issue: What is the basic legal question being determined?• Violations: What law was broken? What facts in the case support this? How does cited precedent support this?• Holding: An overview of the court's opinion. Include concurring and dissenting opinions.• Opinion brief: Finally, your opinion brief of the case where you will provide your opinion of the court's decision and the case facts. Feel free to editorialize. <p data-bbox="870 1213 1419 1759"><i>Case Study</i> - Throughout the course of the semester, you will select a subject that has been convicted of a computer crime. You will write a research paper of that subject wherein you will essentially provide a profile of the subject. Be sure to apply relevant criminological theories and include any relevant information. Include laws for which they were convicted, and the fact surrounding that conviction. Cite case law where applicable. You may speculate provided your assertions are supported.</p> |

Note: Schedule / Syllabus is tentative and subject to change.

| Week | Lecture Topics | Assignment (Due Sunday) |
|-------------|----------------------------------------------------------------------------------------------------------------------------|--------------------------------|
| 1 | Syllabus Introduction to Digital Forensics and Computer Investigations | |
| 2 | Sociological Aspects of Technology Use and the Role of Computers in Crime Lab 1: Introduction to Forensic Data Recovery | |
| 3 | Qualities of Evidence and Forensic Data Recovery | |
| 4 | Acquisition of Evidence - Disk Images | Assignment 1 |
| | Lab 2: Preservation, Validation, Authentication | |
| 5 | Forensic Iconology | |
| 6 | Image Forgery Detection | Assignment 2 |
| | Lab 3: Advanced Image Analysis | |
| 7 |  | |
| 8 | Forensic Artifacts | |
| 9 | Computer Crime Laws and Constitutional Rights on the Internet Lab 4: Evidence Analysis of a Windows Endpoint | |
| 10 | Criminological Theories and Cyber-crime | Assignment 3 |
| 11 | Stylometry and Adversarial Stylometry Lab 5: Authorship Attribution | |
| 12 | Idiographic Digital Profiling, CLA, and Correlated Usage Patterns | |
| 13 | Acquisition of Evidence - Volatile Memory | Assignment 4 |
| | Lab 6: Forensic Analysis of Volatile Memory | |
| 14 | Cyber-crime Victimology | |
| 15 | Forensic Analysis of Mobile Technologies | |
| 16 | Final Exam (Due Sunday of finals week) | Forensic Challenge |

Note: Schedule / Syllabus is tentative and subject to change.