
CIS 361: DIGITAL FORENSICS

Instructor:	Chad Johnson
Office:	SCI B231
Phone:	715-346-2021 (CNMT Sept)
Email:	Chad.Johnson@uwsp.edu
Office hours:	Mondays and Thursdays, 2pm to 3:50pm

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.

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

- Students are strongly encouraged to attend each class and actively participate in class discussions. You are also encouraged to participate in discussions and assignments
- 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: 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

- 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

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

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

know to complete it in this class.) Since these are bonus points, the grading will be extraordinarily strict – you will need to do exceptionally well.

- 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.**
- The forensic challenge is due by 11:59pm on its due date. I can't accept it after the deadline.
- 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*).

Investigations – 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:

- 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?

Forensic Challenge – 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.

OFFICE HOURS

- 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

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

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

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.

REGRADES

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 HONESTY:

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

STUDENTS IN NEED OF ACCOMODATIONS:

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.

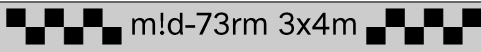
RECORDED LECTURES:

I may record lectures and post them online. I do this as a convenience for students, not as an obligation. Online postings aren't a substitute for regular attendance of class and I make no guarantee that they will be complete or available.

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

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

COURSE OUTLINE:

Week	Lecture Topics	Assignment (Due Sunday)
1	Introduction to Digital Forensics and Computer Investigations	
2	The Role of Computers in Crime	
3	Qualities of Evidence and Forensic Data Recovery	
4	Acquisition of Evidence – Disk Images	Assignment 1
5	Forensic Iconology	
6	Image Forgery Detection	
7		
8	Forensic Artifacts	Assignment 2
9	Computer Crime Laws and Civil Rights	
10	Criminological Theories and Cyber-crime	
11	Stylometry and Adversarial Stylometry	Assignment 3
12	Idiographic Digital Profiling, CLA, and Correlated Usage Patterns	
13	Acquisition of Evidence – Volatile Memory	
14	Cyber-crime Victimology	Assignment 4
15	Forensic Analysis of Mobile Technologies	
16	Final Exam	Forensic Challenge

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