CIS 347 / SOC 395: Digital Forensics

Course Title: CIS 347 Digital Forensics / SOC 395 Digital Forensics

Class Schedule:

CIS 347: Monday and Wednesday 4:00pm – 6:00pm **Location:** SCI B238

SOC 395: Monday 4:00pm – 6:00pm Wednesday 4:00pm – 5:00pm **Location:** SCI B238

Final Exam: Friday, 12/21/2018 10:15am to 12:15pm in SCI B238

Instructor:	Chad Johnson
Office:	ALB 002
Phone:	715-346-2020
Email:	Chad.Johnson@uwsp.edu
Office hours:	Tuesdays 3:00pm - 4:00pm

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 reason, 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.

Course Objectives

- Understand the use of digital forensic tools and techniques.
- Understand the indicators of compromise, chain of custody, and 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

- *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*, 3rd Edition, By Eoghan Casey, ISBN-13: 978-0123742681

Lectures

- Lecture notes MIGHT be posted in D2L. 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
- In general, I do not believe in taking attendance. However, class attendance may be taken in any class without notification in advance.

Grading

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

Final grades will be assigned according to the following scale:

A: score >= 90	A-: 87 <= score < 90	
B+: 83 <= score < 87	B: 80 <= score < 83	B-: 77 <= score < 80
C+: 73 <= score < 77	C: 70 <= score < 73	C-: 65 <= score < 70
D: 60 <= 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 D2L 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.
- Final exam not is 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 and a written explanation along with the supporting documents must be submitted to the instructor.

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 if they are all done <u>to satisfaction</u>. That is the equivalent of 1 regular assignment, or one-quarter an exam.

- 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 will not be accepted.**
- 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 cannot 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 D2L. **I will not take submissions in email, unless the university verifies that D2L 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. 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.

Regrading

Scores of Assignments, Forensic Challenge, and Exams will be posted in D2L, and announcements will be made in D2L. 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.

D2L

The D2L URL is https://uwsp.courses.wisconsin.edu. Use your UWSP NetID and password to login. We use D2L for the following activities:

- Make important announcements.
- Posting assignment instructions and files.
- Students submit assignments electronically.
- Posting scores and grades.

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 collusion. **Any form of academic dishonesty may lead to F grade for this course.**

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.

CIS-347 Assignments

Article Abstracts – A group of articles will be offered. You will select one. The abstract you will write will have two parts: A summary of the article, and your personal critique of the article. No less than two and no more than five pages. Your sources must be cited.

Investigations – A scenario will be provided. The scenario will reproduce a situation outlined in a topical legal case. 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 500 and no more than 2500 words. The paper you will write will be 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: Compare your experiences with the investigation to the topical case this scenario represents. What is your opinion of the outcome of the case, given this?

Process Briefs – A group of topics will be offered. You will select one and write a paper that is no less than two and no more than five pages addressing it.

Pre-Test – Your first assignment is a pre-test to establish the classes base of knowledge. A short exam, which includes an ethics contract, will be given.

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.

SOC-395 Assignments

Article Abstracts – A group of articles will be offered. You will select one. The abstract you will write will have two parts: A summary of the article, and your personal critique of the article. No less than two and no more than five pages. Your sources must be cited.

Case Briefs – A group of cases will be offered. You will select one. Each paper should be no less than 2500 and no more than 5000 words. The legal brief you will write will have these sections:

- The case citation: The name, number and year of the case.
- 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?
- 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.

Policy Briefs – A group of topics will be offered. You will select one and write a paper that is no less than two and no more than five pages addressing it.

Pre-Test – Your first assignment is a pre-test to establish the classes base of knowledge. A short exam, which includes an ethics contract, will be given.

Nomothetic Digital Profile – Throughout the course of the semester, you will select a "toxic community" online. You will write a nomothetic profile of that community.

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

Week	Date	Day	Lecture Topics	Assignment
1	09/05	Wednesday	Syllabus Introduction to Digital Forensics	Assignment 1
2	09/10	Monday	Introduction to Computer Investigations	
2	09/12	Wednesday	Forensic and Investigative Process Introduction to Forensic Data Recovery	
3	09/17	Monday	Role of Computers in Crime	
3	09/19	Wednesday	Warrants, Subpoenas, and Legal Procedure Lab 1: Deductive Reasoning and Establishing Causality	Assignment 2
4	09/24	Monday	Qualities of Evidence	
4	09/26	Wednesday	Qualities of Evidence Acquisition of Evidence – Disk & Data Recovery	
5	10/01	Monday	Forensic Iconography	
5	10/03	Wednesday	Forensic Iconography Lab 2: Preservation, Verification, Authentication	Assignment 3
6	10/08	Monday	Computer Crime Laws	
6	10/10	Wednesday	Computers and Constitutional Law Lab 3: Evidence Analysis - Disk Images	
7	10/15	Monday	Constitutional Law and Internet Law	
7	10/17	Wednesday	m!d-73rm 3x4m	
8	10/22	Monday	Idiographic Digital Profiling	
8	10/24	Wednesday	Idiographic Digital Profiling Forensic Artifacts – Windows Endpoints	Assignment 4
9	10/29	Monday	Creating a Digital Bibliography	
9	10/31	Wednesday	Digital Behavioral Analysis Lab 4: Forensic Analysis of the Windows Registry	
10	11/05	Monday	Correlated Usage Patterns	
10	11/07	Wednesday	Stylometry Acquisition of Volatile Memory	Assignment 5
11	11/12	Monday	Stylometry	
11	11/14	Wednesday	Establishing a Behavioral Profile Lab 5: Forensic Analysis of Volatile Memory	
12	11/19	Monday	Establishing a Behavioral Profile	

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

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

12	11/21	Wednesday	Correlates of Computer Crime Introduction to Mobile Technologies	Assignment 6
13	11/26	Monday	Psychology of Cyber Crime and Interviewing Subjects	
13	11/28	Wednesday	Connecting Computer Crimes to Criminals Lab 6: Evidence Analysis – Mobile	
14	12/03	Monday	Victimology of Cyber-Crime	
14	12/05	Wednesday	Inductive Reasoning and Nomothetic Profiling Counter-Forensics	Assignment 7
15	12/10	Monday	Criminological Theories & Cyber-crime	
15	12/12	Wednesday	Criminological Theories & Cyber-crime Malware and Malware Taxonomy	Assignment 8
16	12/21	Friday	Final Exam (10:15am – 12:15am)	Forensic Challenge

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