CIS 345 / HTI 345 / SOC 395 Digital Forensics

Course Title: CIS 345 Digital Forensics / HTI 345 Digital Forensics / SOC 395 Digital Forensics

Class Schedule: **CIS 345 & HTI 345 Section 02:** T Th 4:00pm – 6:00pm **Location:** SCI B228

SOC 395 Section 01: T 4:00pm – 6:00pm Th 4:00pm – 5:00pm **Location:** SCI B228

Final Exam: 12/19/2017 5:00pm – 7:00pm in SCI B228

Instructor: Chad Johnson
Office: SCI D260 / ALB 002
Phone: 715-345-2020
Email: Chad.Johnson@uwsp.edu
Office hours: F 3:00pm - 4:00pm

Course Description

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 and forensic accounting, the victimology, profiling, and case law of computer crimes. Finally, to describe the process of acquiring, evaluating, and preserving digital evidence.

Course Objectives

- Master 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.
- Obtain 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
- SOC-395
  - *Cybercrime and Criminological Theory: Fundamental Readings on Hacking, Piracy, Theft, and Harassment*, 1st Edition, By Thomas J. Holt, ISBN-13: 978-1609274962
- CIS-345 & HTI-345
  - *Digital Forensics with Open Source Tools*, 1st Edition, By Cory Altheide and Harlan Carvey, ISBN-13: 978-1597495868

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
- 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: 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.

Assignments and Deadlines

- 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 HTI-345, the other for students enrolled in CIS-345. See the list at the end of the syllabus for guidelines on the different assignments.

Exams

- 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.
- 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.
- Do NOT ask for make-up tests or exams if you missed a test or exam due to travel.

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.

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, I would like to meet with you in the privacy of my office during the first week of the semester to ensure that you are appropriately accommodated.

CIS-345 & HTI 345 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 – 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 partner. Be sure to write a forensic report for all of 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 personal opinion of the court's decision and the case facts.

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 – A short exam, which includes an ethics contract, will be given.

Forensic Challenge – Your role in the forensic challenge will be to examine the evidence provided by your forensic team and prepare a submission of documentary evidence, including forensic report and exhibits. The length of this document depends entirely on the amount of evidence your team has been able to gather.

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

Week	Date	Day	Lecture Topics	Readings	Assignment
1	09/05	Tuesday	Introduction to Digital Forensics	1	Pre-test
1	09/07	Thursday	Introduction to Computer Investigations	15	
2	09/12	Tuesday	Role of Computers in Crime	2	
2	09/14	Thursday	Forensic Process	7	Lab 1
3	09/19	Tuesday	Legal Process and Procedure	3	
3	09/21	Thursday	Preservation, Verification, Authentication	16, 22	Assignment 2
4	09/26	Tuesday	Warrants & Subpoenas	6	
4	09/28	Thursday	Malware & Malware Taxonomy	See D2L	Lab 2
5	10/03	Tuesday	Legality & Ethics	11	
5	10/05	Thursday	Counter-Forensic Techniques	14	Assignment 3
6	10/10	Tuesday	Reconstruction and Reporting	8	
6	10/12	Thursday	Forensic Artifacts – Endpoints	17 (18/19)	Lab 3
7	10/17	Tuesday	Chain of Custody/Evidence Handling	See D2L	
7	10/19	Thursday	Acquisition of Evidence - Disk & Data Recovery	18	Mid-Term Exam
8	10/24	Tuesday	Computer Crime Laws	4	
8	10/26	Thursday	Acquisition of Evidence - Volatile Memory	19	Assignment 4
9	10/31	Tuesday	Constitutional Law	See D2L	
9	11/02	Thursday	Indicators of Compromise – Endpoint & Network Acquisition of Evidence - Network	21 23	Lab 4
10	11/07	Tuesday	Criminal Behavioral Analysis	9	
10	11/09	Thursday	Evidence Analysis – Endpoint & Network	24	Assignment 5
11	11/14	Tuesday	Criminological Theories & Cyber-crime	10	
11	11/16	Thursday	Evidence Analysis – Endpoint & Network	25	Lab 5
12	11/21	Tuesday	Criminological Theories & Cyber-crime	12	
12	11/23	Thursday	** HOLIDAY BREAK – NO CLASS **	-	Assignment 6
13	11/28	Tuesday	Victimology of Cyber-crime	13	
13	11/30	Thursday	Introduction to Mobile Technologies	See D2L	Lab 6
14	12/05	Tuesday	Psychology of Cyber-Crime Profiling Hackers & Cyber-Criminals	14 See D2L	
14	12/07	Thursday	Indicators of Compromise - Mobile Acquisition of Evidence – Mobile	20	Assignment 7
15	12/12	Tuesday	Introduction to Fraud Analysis – Benford's Law	13	
15	12/14	Thursday	Evidence Analysis – Mobile	See D2L	Assignment 8
16	12/19	Tuesday	Final Exam (5pm to 7pm)		Forensic Challenge

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