

# Digital Forensics and Computer Criminology

---

**Course Title:** CIS 347 Digital Forensics / SOC 395 Digital Forensics / WD 345 Digital Forensics

**Class Schedule:**

**CIS 347/WD345:** Monday and Wednesday 3:00pm – 5:00pm    **Location:** SCI B238

**SOC 395:** Monday 3:00pm – 5:00pm Thursday 3:00pm – 5:00pm    **Location:** SCI B238

**Final Exam:** Friday, 12/19/2019 8:00am to 10:00am in SCI B238

**Instructor:** Chad Johnson  
**Office:** ALB 024  
**Phone:** 715-346-2020  
**Email:** Chad.Johnson@uwsp.edu  
**Office hours:** Tuesdays 2:00pm - 3:00pm

## 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 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*, 3<sup>rd</sup> Edition, By Eoghan Casey, ISBN-13: 978-0123742681

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

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

### Grading

- 4 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 $\geq$ 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 if they are all done to satisfaction.
- 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 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-345. See the list at the end of the syllabus for guidelines on the different assignments.

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

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

### **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 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 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.

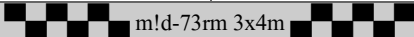
**Note:** Schedule / Syllabus is tentative and subject to change.

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

<b>CIS-347 Assignments</b>	<b>SOC-395 Assignments</b>
<p data-bbox="298 149 837 470"><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="347 520 837 772" style="list-style-type: none"><li>• 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?</li><li>• Opinion brief: In your opinion as the investigator, what facts do your findings convey?</li></ul> <p data-bbox="298 821 837 1031"><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="873 149 1427 289"><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="922 338 1427 856" style="list-style-type: none"><li>• A statement of facts: Who are the parties in the case, what is their dispute, how did they get to this point?</li><li>• Legal issue: What is the basic legal question being determined?</li><li>• Violations: What law was broken? What facts in the case support this? How does cited precedent support this?</li><li>• Holding: An overview of the court’s opinion. Include concurring and dissenting opinions.</li><li>• 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.</li></ul> <p data-bbox="873 905 1427 1255"><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.

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

<b>Week</b>	<b>Lecture Topics</b>		<b>Assignment (Due Friday)</b>
<b>W 1</b>	Syllabus Introduction to Digital Forensics		
<b>Th 1</b>	Syllabus Introduction to Computer Investigations		
<b>M 2</b>	Forensic and Investigative Process		
<b>W/Th 2</b>	Lab 1: Preservation, Verification, Authentication	Lab 1: Sociological Aspects of Technology Use	
<b>M 3</b>	Qualities of Evidence		
<b>W/Th 3</b>	Lab 2: Introduction to Forensic Data Recovery	Lab 2: Role of Computers in Crime	
<b>M 4</b>	Forensic Iconology		Assignment 1
<b>W/Th 4</b>	Lab 3: Forensic Iconology	Lab 3: Forensic Iconology	
<b>M 5</b>	Computer Crime Laws		
<b>W/Th 5</b>	Lab 4: Acquisition of Evidence - Disk Images	Lab 4: Deductive and Inductive Reasoning	
<b>M 6</b>	Constitutional Law and the Internet		
<b>W/Th 6</b>	Lab 5: Mid-Term Study Session	Lab 5: Mid-Term Study Session	
<b>M 7</b>			
<b>W/Th 7</b>	Lab 6: Evidence Analysis - Disk Images	Lab 6: Correlates of Computer Crime	
<b>M 8</b>	Criminological Theories & Cyber-crime		Assignment 2
<b>W/Th 8</b>	Lab 7: Forensic Artifacts – Windows Endpoints	Lab 7: Idiographic Digital Profiling	
<b>M 9</b>	Digital Behavioral Analysis		
<b>W/Th 9</b>	Lab 8: Forensic Analysis of the Windows Registry	Lab 8: Establishing a Behavioral Profile	
<b>M 10</b>	Stylometry		
<b>W/Th 10</b>	Lab 9: Acquisition of Volatile Memory	Lab 9: Connecting Computer Crimes to Criminals	
<b>M 11</b>	Correlated Usage Patterns		
<b>W/Th 11</b>	Lab 10: Malware and Malware Taxonomy	Lab 10: Case Linkage Analysis	
<b>M 12</b>	Victimology of Cyber-Crime		Assignment 3
<b>W/Th 12</b>	Lab 11: Forensic Analysis of Volatile Memory	Lab 11: Nomothetic Profiling	
<b>M 13</b>	Introduction to Mobile Technologies		
<b>W/Th 13</b>	Lab 12: Evidence Analysis – Mobile	NO CLASS – Thxgving Break	
<b>M 14</b>	Counter-Forensics		Assignment 4
<b>W/ Th 14</b>	Working day to finish Forensic Challenge	Working day to finish Case Study	
<b>15</b>	In-class exercise		
<b>15</b>	Working day to finish Forensic Challenge	Working day to finish Case Study	
<b>16</b>	Final Exam (12/19 8:00am – 10:00am)		Forensic Challenge

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