

**CS 447 Computer and Network Forensics
Fall 2008 Syllabus**

Catalog Description: Competence in using established forensic methods in the handling of electronic evidence; rigorous audit/logging and data archival practices; prevention, detection, apprehension, and prosecution of security violators and cyber criminals.

Class Meetings: TuTh 9:30 - 10:45 in BEL 118
Course Credits: 3 cr.
Prerequisites: CS 336, Introduction to Information Assurance
Textbook: E. Casey, *Digital Evidence and Computer Crime*, 2nd Edition, 2004
Instructor: Dr. Paul W. Oman, Professor of Computer Science
Office: McClure 409; Phone 885-6899; Email oman@uidaho.edu
Assistants: Katie Smith (katie.smith@vandals.uidaho.edu), Corey Thuen (cthuen@vandals.uidaho.edu), Kris Watts (watt0916@vandals.uidaho.edu)

Course Goals:

1. Familiarize students with the principles of forensics data gathering.
2. Explore and understand legal processes relative to forensics data.
3. Differentiate between computer and network forensics.
4. Recognize operating system nuances with respect to computer forensics.
5. Apply computer and network forensics methodologies to mock situations.

Course Grading: A grading curve will be used based on the cumulative points earned through homework, labs exercises, and exams. Grades will be assigned as follows:

A	$\geq 90\%$	D	65% - 69%
B	80% - 89%	F	< 65%
C	70% - 79%		

There will be two midsemester exams, a final comprehensive exam, and a series of homework and laboratory exercises, assigned as follows:

In-class midsemester exam	100 points	Homework/Lab	70 points
Take-home midsemester exam	100 points	Mock Court	30 points
Final exam	200 points		

CS 447 Guidelines and Rules

1. The purpose of this class is to familiarize students with both the technical and legal aspects of digital forensics. We will study legal issues and become familiar with the process of conducting a forensic investigation. This class is not an overview of specific forensic tool sets. We will not be going over the intricate details of any one software suite, nor will we require you to use any specific tool. You will be required to do some exercises by hand and provide proof (code and/or procedures) that you did so. By the end of the class each student should be able to readily approach a suspect system and conduct a reasonable investigation.
2. There will be homework and lab exercises that count for a substantial part of your grade and you will be hard pressed to pass the hands-on midsemester exam without completing these assignments. The assignments will be accessible via the course website; you will be given login credentials that enable access to the materials.
3. Anyone caught cheating on any work task will receive a zero for that work task and all related work tasks. You are all nearing professional careers and you are expected to act as professionals.
4. If for any reason the class website fails and you are unable to submit your work, we will modify due dates accordingly, but you have to show forensics evidence that backs up your claim that the website failure caused you to miss the original deadline.
5. You will each take part in a mock court where student teams take opposing sides in a case, to “prove” that the defendant either did or did not commit the crime.
6. The second midsemester exam will consist of a complete forensic investigation for you to take home and “solve.” You will be given a hard drive image to investigate; you will report back using a standardized template on which to record your findings.
7. **Unauthorized probing and hacking on any system are not tolerated.** Anyone caught attempting to probe, hack, or crack computer systems or accounts outside of their immediate ownership without the express written approval of the instructor, will be disenrolled or failed from the course and remanded to the appropriate university, state, and federal authorities. All offensive activities, like hacking, cracking, probing, sniffing, snorting, etc., should only be done in isolated or controlled environments with the instructor’s prior approval.
8. **Cheating and plagiarism are not tolerated.** Anyone caught copying or stealing another person’s work will receive a zero for that entire work task, whether it is a test, project, or lab exercise. Anyone caught plagiarizing another person’s work, from printed or electronic sources, will receive a zero for that project or lab exercise. Anyone caught sharing work with other classmates, unless they are working on an approved team project and the sharing is restricted to teammates, will receive a zero for that project. Note that plagiarism is not just copying other people’s writings, it includes all instances of passing off someone else’s work as if it is your own. If you use other people’s work, cite that work in a footnote or reference list.

**CS 447 Computer and Network Forensics
Fall 2008 Tentative Schedule**

Week	Dates	Topic	Readings
1	Aug. 26, 28	Course overview, Digital Evidence, Computer Organization	Ch. 1, 2, 8
2	Sept. 02, 04	Technology and the Law and Investigative Processes	Ch. 3, 4
3	Sept. 09, 11	Forensics Investigations and the Criminal Mind	Ch. 5, 6
4	Sept. 16, 18	Computer and Network Forensics in the Courtroom	Ch. 7, 9
	Sept. 19	Last day to drop without getting a "W."	
5	Sept. 23	Midsemester In-class Exam	
	Sept. 25	Exam Review, Computer Forensic Tools Discussion	Outside reading
6	Sep.30, Oct.2	Unix-based Forensics	Ch. 11
7	Oct. 07, 09	Unix-based Forensics	Ch. 11
8	Oct. 14, 16	Macintosh Forensics	Ch. 12
9	Oct. 21, 23	MS Windows Forensics	Ch. 10
10	Oct. 28, 30	MS Windows Forensics	Ch. 10
11	Nov. 04, 06	Forensics for Hand-held Devices and Embedded Systems	Ch. 13
12	Nov. 11	Do-at-home Midsemester Exam Assignment	
	Nov. 13	Do-at-home Midsemester Exam Review	
13	Nov. 18, 20	Network Forensics and the ISO OSI 7-Layer Model	Ch. 14, 15, 16, 17
14	Nov. 24-28	Thanksgiving Break	
15	Dec. 02, 04	Internet Evidence, Computer Intrusions, Crimes	Ch. 18, 19, 20, 21
16	Dec. 09	Digital Evidence in Support of the Defendent	Ch. 22
	Dec. 09	Last day for all homework and labs	
	Dec. 11	Course Review	
17	Dec. 15-19	Final Exam (Tuesday, Dec. 16, 7:30 – 9:30, BEL 118	Comprehensive