

Master Course Syllabus
School of Engineering and Computer Science
Washington State University Vancouver

CS 425
Digital Forensics
3 Semester Hours

Catalog Description

A detailed approach to the use of computers and computer technology in the investigation of incidents, both criminal and civil, in which computers or computer technology plays a significant or interesting role.

Prerequisite Courses

CS 360

Prerequisite Topics

Operating system basics and advanced programming concepts

Measured Course Outcomes

Students taking this course will:

1. Investigate the impact of technology related criminal activity on society (via the legal structure). (*Contributes to performance criterion G-2*)
2. Contribute to the formulation of ideas and the implementation of a group project (*Contributes to performance criterion D-1 and D-2*)
3. Present investigation findings in a formal written document. (*Contributes to performance criterion F-1*)

Required Textbooks

Digital Evidence and Computer Crime, by Eoghan Casey, Second Edition, Academic Press, (ISBN 978-0-12-163104-8)

Reference Material

DOJ *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, Computer Crime and Intellectual Property Section Criminal Division United States Department of Justice, July 2002. Available at www.cybercrime.gov/s&smanual2002.pdf

Major Topics Covered in the Course

1. Introduction to crimes, investigations and electronic evidence
2. Law enforcement procedures for preserving, collecting and analyzing digital evidence

3. State laws covering technology and crime; federal guidelines for search and seizure in the digital arena, and the Electronic Communications Protection Act
4. Forensic artifacts maintained in file systems; memory allocation and de-allocation
5. Performing forensic analysis of computer systems; sources of information and tools to extract evidence
6. Location of potential evidence on a variety of digital devices
7. Network forensics and wireless network analysis

Laboratory Projects

In this course, students perform assignments as members of teams. There is one programming project assigned in several phases. The first phase entails developing an “evidence disk”; later phases cover the analysis of an evidence disk.

CSAB Category Content

	FUNDAMENTAL	ADVANCED		FUNDAMENTAL	ADVANCED
Data Structures	0	0	Computer Organization and Architecture	.5	.5
Algorithm & Software Design	0	0	Concepts of Programming Languages	0	0

Oral and Written Communications

There is significant written communication required in this course. The course project has several written documents.

Social and Ethical Issues

This course contains significant coverage of social and ethical issues. Students are required to do several assignments researching state and federal laws pertaining to computer crime and the role of digital evidence in all categories of crime. 6 hours

Theoretical Content

This course contains no significant coverage of theoretical topics.

Problem Analysis

The main project requires student to analyze a systems logical structure and perform an investigation of an “evidence disk”.

Solution Design

Students are assigned to teams to participate in a multi phase project. The project containing various pieces of electronic evidence relating to one or more crimes. The second phase entails swapping evidence disks created in the first phase, and performing an electronic investigation on the disk that the team has received. In the final phase of the project students demonstrate their understanding of the elements of the crime. Student's individual grades on the project will be a function of the success of the project, as well as individual contributions to the project, based on the Professor's observations, the team member's self evaluation, and peer evaluations from the rest of the team. The goal of the project is to exercise skills using forensic tools; exhibit the capacity to identify relevant evidence, and illustrate chain of custody concepts.

CC2001

This course provides coverage of topics in the following areas (hours listed are minimums):

OS8 File systems	2
SP2 Social context of computing	2
SP4 Professional and ethical responsibility	2
SP7 Privacy and civil liberties	2
SP8 Computer crime	10

Course Coordinator:
Last Updated:
Syllabus Version Number:

Sarah Mocas
April 8, 2009 (Approved)
1.3