CPS 301 Issues in Criminal and Forensic Computing

Spring 2012

TR: 2:00 – 3:15 pm (Dailey 203)

Instructor: Wensheng Shen
Department of Computational Science
207 Dailey Hall
Phone: (585)395-5182
Email: wshen@brockport.edu
Web: http://www.cps.brockport.edu/~shen

Office hour: TR 10:00 am – 12:00 pm or by appointment

Prerequisites: none

Textbook: Guide to Computer Forensics and Investigations, Third Edition.
Bill Nelson, Amelia Phillips, Frank Enfinger, Christopher Steuart.
Course Technology Incorporated, 2008.
ISBN 10: 1-4180-6733-4 or ISBN-13: 978-1-4180-6733-5

Course Objectives

This course introduces students to the techniques and tools of computer forensics investigations. Students will receive step-by-step explanations on how to use the most popular forensic tools. The course maps to the objectives of the International Association of Computer Investigative Specialists (IACIS) certification to provide credible, standards-based information. Topics include coverage of the latest technology including PDAs, cell phones, and thumb drives. Many hands-on activities are included, which allow students to practice skills as they are learned.

Specific topic coverage includes:

- Computer Forensics and Investigation as a Profession
- Understanding Computing Investigations
- The Investigator's Office and Laboratory
- Data Acquisitions
- Processing Crime and Incident Scenes
- Working with Windows and DOS Systems
- Current Computer Forensics Tools
- Macintosh and Linux Boot Processes and File Systems
- Computer Forensics Analysis and Validation
- Recovering Graphics Files
- Network Forensics
- E-mail Investigations
- Cell Phone and Mobile Device Forensics
- Report Writing for High-Tech Investigations
- Expert Testimony in High-Tech Investigations
- Ethics for the Expert Witness

Web Site

Supplementary information for the course is available at http://www.cps.brockport.edu/~shen/cps301/cps301. The Web site contains class notes, PowerPoint slides, class announcements, the course syllabus, and other information for the course.

Grading and Evaluation Criteria

20% of the grade is based on a midterm and a final examination. Both examinations are cumulative and given in a varied format. An in-class review will be held prior to each examination.

10% of the grade is based on class participation.

35% of the grade is based on the lab participation

35% of the grade is based on homework assignments and projects.

Average	95.0 – 100	90.0 – 94.9	87.0 – 89.9	83.0 – 86.9	80.0 – 82.9	77.0 – 79.9
Grade	A	A-	B+	B	B-	C+
Average	73.0 – 76.9	70.0 – 72.9	67.0 – 69.9	63.0 – 66.9	60.0 –62.9	<60.0
Grade	C	C-	D+	D	D-	E

Assignment policy: Homework and project assignments given in class will be due in one week after they are assigned. Late assignments can be accepted with a penalty at a rate of 10% per day. ***No makeup tests and no incompletes. A missed test will receive 0 points.*** Exceptions to these rules, at instructor's discretion, apply to cases of illness, personal tragedy, or extraordinary circumstances beyond a student's control, if it is documented to instructor's satisfaction. Arrangement for such an exception needs to be discussed with the instructor.

Attendance: Students are expected to attend all classes. Some of the material may not be contained in the textbook. If a student misses a class, it is his/her responsibility to get class notes and handouts. Absences will be excused for documented illness, official representation of the College, an unfortunate death of a close relative, religious holiday, and other circumstances beyond student's control**.**

Authorship: Students are allowed to discuss ideas and help others by explaining concepts and possible solutions. All the work that is submitted, however, must be performed by individual students independently. Students must provide appropriate citations for any text fragments in books, journals, conference proceedings, web-based resources, etc. that have been used in their assignments. Students also need to acknowledge any help from others. A student is considered cheating if he/she submits materials as his/her own work that is not entirely his/her own work, or if he/she intentionally provides an answer to another person. If cheating has been detected, the student will receive a zero grade for that assignment. Further disciplinary procedures may also be considered.

Disability Statements: Students with documented disabilities may be entitled to specific accommodations. SUNY Brockport's Office for Students with Disabilities makes this determination. Please contact the Office for Students with Disabilities at 395-5409 to inquire about obtaining an official letter to the course instructor detailing approved accommodations. The student is responsible for providing the course instructor with the official letter. Faculty and staff work as a team with the Office for Students with Disabilities to meet the needs of students with disabilities.

16-Week Course Outline

Week	Topics	Chapter Readings	Exams
1	Computer Forensics and Investigation as a Profession Basics about Computers	Chapter 1	
2	Understanding Computing Investigations	Chapter 2	
3	The Investigator's Office and Laboratory	Chapter 3	
4	Data Acquisitions	Chapter 4	
5	Processing Crime and Incident Scenes	Chapter 5	
6	Working with Windows and DOS Systems	Chapter 6	
7	Current Computer Forensics Tools	Chapter 7	Midterm Exam
8	Computer Forensics Analysis and Validation	Chapter 9	
9	Recovering Graphics Files	Chapter 10	
10	Network Forensics	Chapter 11	
11	E-mail Investigations	Chapter 12	
12	Cell Phone and Mobile Device Forensics	Chapter 13	
13	Report Writing for High-Tech Investigations	Chapter 14	
14	Expert Testimony in High-Tech Investigations	Chapter 15	
15	Ethics for the Expert Witness	Chapter 16	
16			Final Exam

Labs	Topics	Chapter Readings	Time	Location
1	Understanding Computing Investigations	Chapter 2	Feb. 9	Drake #30
2	Data Acquisitions	Chapter 4	Feb. 16	Drake #30
3	Processing Crime and Incident Scenes	Chapter 5	Feb. 23	Drake #30
4	Working with Windows and DOS Systems	Chapter 6	Mar. 1	Drake #30
5	Current Computer Forensics Tools	Chapter 7	Mar. 8	N/A
6	Computer Forensics Analysis and Validation	Chapter 9	Mar. 22	Drake #53
7	Recovering Graphics Files	Chapter 10	Mar. 29	Drake #53
8	E-mail Investigations	Chapter 12	Apr. 5	N/A
9	Report Writing for High-Tech Investigations	Chapter 14	Apr. 12	Drake #53