CTC 328: Computer Forensic and Investigation

Fall 2010

Instructor:	K Kowalski. Ph.D.	E-mail:	kkowalski@csudh.edu
Classroom:	Lib C-522	Class time:	MW 5:30PM - 6:30PM
Office:	NSM E-155	Office Hours:	Tuesday 1:00PM - 4:00PM
Phone:	(310) 243-3398	Website	http://mieszko.csudh.edu/ctc328

Catalog Description:

This course presents methods to properly conduct a computer forensics investigation, beginning with a discussion of ethics while mapping to the objectives of the International association of Computer Investigative Specialist (IACIS) certifications

Pre-requisite:

CSC 116: Introduction to Computer Hardware an Tools, or Consent of Instructor

Prerequisites by topic:

Students should have a working knowledge of hardware and operating systems (OSs) to maximize their success on projects and exercises throughout the course.

Text book:

Computer Forensics: Evidence Collection and Management by Robert C Newman. ISBN-13: 9780849305610

Course goals and objectives:

This course will provide the students an introduction to Evidence Collection and Management by examining cyber-crime, E-commerce, and Internet activities that could be used to exploit the internet, computers, and electronic devices. The student will focus on the numerous vulnerabilities and threats that are inherent con the Internet and networking environments. This course will present techniques and suggestions for corporate security personnel, investigators, and forensic examiners to successfully identify, retrieve, and protect valuable forensic evidence for litigation and prosecution.

Learning Outcomes:

Upon completion of this course, students will be able to:

- Understand the basic concepts that make up the filed of computer forensics
- Become familiar with various threats, risks, laws, policies, tools related to computer forensics
- Explore information needed to understand the underlying concepts of computer forensic investigations
- Identify the various crimes and incidents that are involved in electronic forensic investigation
- Understand the importance of security and computer use policies
- Determine and understand the functions and infrastructure requirements of a computer and electronic forensic lab
- Identify the software, hardware, and personnel requirements for lab examinations

Course requirements:

There will be one midterm exams and an in-class final exam. One semester project will be required.

Grading

The weights of the various assignments are given below

Midterm exam: 30%

Final Exam: 30%

Semester Project: 40%

Completion of all exams and projects is required to pass the course.

The following grading table will be used:

Score:	94-100	91-93	88-90	84-87	81-83	78-80	74-77	71-73	68-70	64-67	61-63	0-60
Grade:	A	A-	B+	B	B-	C+	C	C-	D+	D	D-	F

Academic Integrity:

Academic integrity is of central importance in this and every other course at CSUDH. You are obliged to consult appropriate sections of University Catalog and obey rules and regulations imposed by the university relevant to its lawful missions, processes, and functions.

Make up policy:

No make-ups will be given

Projects:

Unless stated otherwise, all projects are individual assignments and are expected to be the student's own work. You may engage in general discussions concerning the solutions, but giving and receiving major sections of the code is considered cheating. Projects must be ready by 3:00 PM on their assigned due date. Late projects will be penalized 5% per 24 hours period of lateness, up to 50%. No projects will be expected 2 weeks after the due date. Software project should be e-mailed as attachments (including source code as well as executable files and documentation - when appropriate) to instructor.

Documentation should contain: algorithm, description, printout of the source code, application discussion, user manual.

Research projects should be e-mailed as attachments (including research essay and PowerPoint presentation) to instructor.

You will need to make a public statement of your results to the class. The overall grade will depend how well you show: **a/** involvement, **b/** exploration, **c/** understanding of the subject, **d/** conclusions communication.

Attendance and drop policy:

Students are expected to attend lectures, study text, and contribute to discussions. It is the student's responsibility to contact the instructor in the event a midterm exam is missed and to make arrangements before returning to class. Drops after (Check Academic Calendar) will reflect student's average. The student must initiate all withdrawal procedure. Non-attendance does not constitute withdrawal and will result in F.

****You will be notified in class of any and all changes to this syllabus****

Tentative schedule (based on 15 weeks/45 hours of study):

Week	Material	Chapter	Meetings
1	Computer Forensic Investigation Basics	1	Tues, Th HW 1 due
2	Policies, Standards, Laws, and Legal Processes	2	Tues, Th HW 1 due
3	Computer Forensic Examinations	3	Tues HW 2 due
3	Computer, Internet, and Electronics crimes	4	Th HW 3 due
4	Computer, Electronics, and Networking Environment	5	Tues HW 4 due
5	Investigate Tools, Technical Training, and Forensic Equipment	6	Tues HW 5 due
6	Midterm	N/A	Tues HW 6 due
7	Managing the Crime/Incident Science	7	Tues
8	Investigating Computer Center Incidents	8	Tues HW 7 due
9	Computer Forensic Examinations	9	Tues HW 8 due
10	The Computer and Electronic Forensic Lab	10	Tues HW 9 due
11	The Computer and Electronic Forensic Lab	10	Tues
12	Extracting Computer and Electronic Evidence	11	Tues

			HW 10 due
13	E-mail and Internet Investigation	12	Tues HW 11 due
13	Mobil Phone and PDA Investigation	13	Th HW 12 due
14	Court Preparation, Presentation, and Testimony	14	Tues HW 13 due
14	Projects due	N/A	Th HW 14 due
15	Project Presentation	N/A	Tues, th

Final Exam: ***Tuesday from 7:00 PM - 9:00 PM***

Project (choose one):

TBA