

Guide to Computer Forensics and Investigations

CIS285

General Course Information

Instructor:

Office:

Office Hours:

Phone:

E-mail:

Web site:

Classroom:

Class Times:

I. Prerequisites: Instructor Permission

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

III. 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

IV. AIMS AND OBJECTIVES

Learner Outcomes

Measurements

General Education Goals

1.1 Students will know how to work with and configure FTK and retrieve files with regards to:

- Security settings
- Carving
- Saving
- Case Assignment

Given appropriate practical exercises the student will apply their knowledge to finish and complete assigned tasks. These exercises are provided at the end of each module.

DL(3), CT(2), L(2)

1.2 The Students will use prepare and present image diskettes using appropriate discovery methodologies: Outcomes that are measured will include but not be limited to:

- Functionality
- Appearance
- Meeting Standards
- Readability

Students will be measured by how well their images function with regards to readability. Implementation will be measured by their ability to move their images into FTK. Each student will have the opportunity to demonstrate their images to the class at the end of the quarter.

DL(3), L(2), UR(1)

1.3 The students will use hex editors to carve and paste fragmented files in readable objects Outcomes that are measured will include but not be limited to:

- Using HEXEdit properly.
- Using scientific calculators

Measurements will include successful replication of data received from a lab partner. Displaying files and recording files in an evidence file..

DL(4), L(2), UR(2)

*General Education Goals:	Code:
Disciplinary Learning: Knowledge of content in prerequisite or transfer courses, as well as preparation for a career.	DL
Literacy: Skills in reading, writing, speaking, listening, and quantifying, as well a awareness and appreciation of learning styles and lifelong learning options.	L
Critical Thinking: Competency in analysis, syntheses, problem solving, decision making, creative exploration, and formulation of an aesthetic response.	CT
Social and Personal Responsibility: Awareness of and responsiveness to diversity and commonality among cultures, multiplicity of perspectives, ethical behaviors, and heath and wellness issues.	SPR
Using Resources: Skills in accessing, and evaluating information resources including campus resources, awareness of the role of information resources in making sound decisions, and command of the skills required to use appropriate technologies effectively.	UR

Web Site

Supplementary information for the course is available at [URL]. The Web site contains class notes, PowerPoint slides, class announcements, the course syllabus, test dates, and other information for the course.

E-Mail

All students are requested to obtain an e-mail account. If you have any questions about the course or need assistance, please contact me in person or by telephone during office hours; or by e-mail at any time. Also, you may submit the end-of-chapter case project assignments in class on the due date or by e-mail with a date stamp at or before 5:00 PM on the due date. E-mail submissions should be submitted as an attachment in Microsoft Word format.

Grading and Evaluation Criteria

20% of the grade is based on labs and end of chapter exercises.

40% of the grade is based on quizzes. Quizzes are announced one day in advance and may vary from three to five questions that may be in any format.

20% of the grade is based on keeping a project notebook used to create presentations.

20% of the grade is based on final exam.

10-Week Course Outline

Week	Topics	Chapter Readings	Quizzes/Labs/Questions
1	Computer Forensics and Investigation as a Profession Understanding Computing Investigations	Chapter 1 Chapter 2	Questions For Chapter 1 and 2 Due Friday Online Quiz covering Chapters 1 and 2 Thursday In class Quiz covering Chapters 1 and 2 Friday (closed book)
2	The Investigator's Office and Laboratory Data Acquisitions	Chapter 3 Chapter 4	Questions For Chapter 3 and 4 Due Friday Online Quiz covering Chapters 3 and 4 Thursday In class Quiz covering Chapters 3 and 4 Friday (closed book)
3	Processing Crime and Incident Scenes Working with Windows and DOS Systems	Chapter 5 Chapter 6	Questions For Chapter 5 and 6 Due Friday Online Quiz covering Chapters 5 and 6 Thursday In class Quiz covering Chapters 5 and 6 Friday (closed book)
4	Current Computer Forensics Tools Macintosh and Linux Boot Processes and File Systems	Chapter 7 Chapter 8	Questions For Chapter 7 and 8 Due Friday Online Quiz covering Chapters 7 and 8 Thursday In class Quiz covering Chapters 7 and 8 Friday (closed book)
5	Computer Forensics Analysis and Validation	Chapter 9	Questions For Chapter 9 Due Friday Online Quiz covering Chapter 9 Thursday In class Quiz covering Chapter 9 (closed book)
6	Recovering Graphics Files Network Forensics	Chapter 10 Chapter 11	Questions For Chapters 10 and 11 Due Friday Online Quiz covering Chapters 10 and 11 Thursday In class Quiz covering Chapters 10 and 11 Friday (closed book)
7	E-mail Investigations Cell Phone and Mobile Device Forensics	Chapter 12 Chapter 13	Questions For Chapters 12 and 13 Due Friday Online Quiz covering Chapters 12 and 13 Thursday In class Quiz covering Chapters 12 and 13 Friday (closed book)
8	Report Writing for High-Tech Investigations	Chapter 14	Questions For Chapter 14 Due Friday Online Quiz covering Chapter 14 Thursday In class Quiz covering Chapter 14 (closed book)
9	Expert Testimony in High-Tech Investigations	Chapter 15	Questions For Chapter 15 Due Friday Online Quiz covering Chapter 15 Thursday

			In class Quiz covering Chapter 15 (closed book)
10	Ethics for the Expert Witness	Chapter 16	Questions For Chapter 16 Due Friday Online Quiz covering Chapter 16 Thursday In class Quiz covering Chapter 16 (closed book)
11	Final Exam	Hands On	

For students to keep pace with the course and learn all subjects in “CIS285”, emphasis will be placed heavily on them to utilize all the resources available through pageout, the Internet and the instructor. This will involve developing a work habit that you will need to succeed in any career field today, that is being able to work independently, use good research skills and keep on task. There will be no excuses for late assignments--either you have completed them or you haven't. Any student missing more than five instructor contacts, either through email or physically in one term will not receive a grade higher than a “C”.

Tests and quizzes will not be repeated. Students not present for a test without instructor permission will be given a failing grade for that test. Tests will be closed and open book.

DISABILITIES

Students who have documented disabilities that require accommodations in compliance with the Americans with Disabilities Act should contact the Disability Support Services coordinator as well as the instructor of the course in order to insure that together we create an optimal environment for educational achievement.

Holidays and Observances:	Week	Sun	Mon	Tue	Wed	Thu	Fri	Sat
	1		7	8	9	10	11	
	2		14	15	16	17	18	
	3		21	22	23	24	25	
	4		28	29	30			
Holidays and Observances: 26: M. Day	Week	Sun	Mon	Tue	Wed	Thu	Fri	Sat
	4					1	2	
	5		5	6	7	8	9	
	6		12	13	14	15	16	
	7		19	20	21	22	23	
	8		26	27	28	29	30	
Holidays and Observances: 4: Advising Day 16: Last Day Of Classes	Week	Sun	Mon	Tue	Wed	Thu	Fri	Sat
	9		2	3	4	5	6	
	10		9	10	11	12	13	
	11		16	17	18	19	20	