

FOR 340 Computer Forensics II Syllabus

Melodie Woodward

Welcome to Advanced Computer Forensics and the Computer and Digital and Computer Forensics major at Champlain College.

This course is designed to expose students to advanced concepts in digital/computer forensic analysis and Internet Investigations. As with the introductory course, there will be a balance of legal and technical aspects of study to achieve a balance similar to that encountered during common cases in which computer forensics are employed. Toward that end, the following topics will be covered:

- Introduction and Review of Basic Concepts
 - Advanced Legal Concepts
 - Subpoenas and Search Warrants
 - Seizing digital media
 - Imaging & Authentication
 - Forensic Hardware & Software
 - Linux as a forensic platform
 - Analyzing Media with EnCase
 - Analyzing Media with Forensic Toolkit
 - Analyzing Media with ProDiscover
 - File Systems
 - Report Writing for Computer Forensic Analysis

Course Prerequisite: At least 30 credit hours and Intro to Computer Forensics

Student Outcomes:

Upon completion of this course students will be able to:

- Demonstrate an ability to apply computer forensics to practical investigations.
- Perform cyber-research on various forensic topics.
- Analyze case studies involving collaborative investigation.
- Describe the process of computer forensic analysis on an advanced level.
- Articulate legal principles based on current case law and advanced concepts surrounding the 4th Amendment.
- Construct a report of forensic analysis.

Relationship to core competencies:

- **Technology:** This course is about new technologies, including computers and the Internet. Students will be asked to perform some basic research on the Internet in addition to delving into other technologies.
- **Writing:** To enhance the students' writing abilities, homework assignments and the final project will

require students to write about the various forensic technologies and legal cases they learn about in class and through individual research.

- **Communication:** The ability to explain, verbally and in writing, the technical issues to both peers and laypersons is essential in this field. To enhance the student's presentation skills, various projects will be employed requiring students to present the results of their research to the class.
- **Global Perspectives:** Students will review case studies that cross wide geographic boundaries and require collaborative investigation. This aspect of criminal investigation, particularly in crimes involving computers and the Internet, is becoming increasingly important for criminal investigators.
- **Critical Thinking:** The course will introduce students to a variety of tools available to the forensic examiner. Much of the course will teach students to determine what the appropriate tool is for the examination of a given piece of digital evidence. Students also need to apply their own experience and judgment to determine if the results of the examinations seem reliable. This course further introduces students to a thought process that requires logic and creativity.

Instructor contact information:

Melodie Woodward
Champlain College
West Hall
Burlington, VT 05401
802-865-5455
melodie.woodward@champlain.edu
AIM screen name: mwoodward23

Text Books:

We will be utilizing two books for this semester:

- *Computer Evidence Collection and Preservation* by Chris Brown
- *Windows Forensics The Field Guide for Conducting Corporate Computer Investigations* by Chad Steel

Attendance, Homework, and Grading:

Attendance in this course is important, not only because of the breadth of information to be presented but also because interaction with fellow students is critical to the course design. Class discussions will serve as important cornerstones to the learning process to allow students to glean information from their peers not available from other sources.

Homework and exercise assignments will be given.

- Each of these exercises will be conducted during a module. Each paper/exercise is due one week after it is assigned unless otherwise indicated. The assignment details are located in the assignment

section of WebCT which is where they are to be submitted each week.

All assignments have a due date. Late assignments will be accepted only in extraordinary circumstances *and* only with the instructor's permission. Please note that "notifying" me that an assignment will be late is not the same as getting my permission! All homework must be submitted via WebCT. If you have technical problems submitting via WebCT, email me your assignment. If for some reason you can't hand in the homework on time, please make arrangements with me *prior* to the date the assignment is due.

- Class Participation: Weekly interaction with class discussion is expected, and the class participation portion of the grade is based on the level of interaction and contribution to class discussions. At times you will be asked to work in teams on assignments. Your contribution to these assignments also counts toward your class participation.

Grades will be calculated and weighted as follows:

- Each Exercise = **320 points** (20 points each)
- Attendance/Participation = **80 points**
- Final Report= **100 points**
- **TOTAL: 500 points**

The College's standard numerical grading scale will be used for calculating final grades:

A	A-	B+	B	B-	C+	C	C-	D+	D	D-	F
93+	90	87	83	80	77	73	70	67	63	60	59-

Academic Honesty:

The Student Handbook (*The Rudder*) describes the College's Academic Honesty Policy. You should be familiar with that policy, which states simply that if you cheat, you get a 0 (zero). More importantly, in the field of forensics and law enforcement there is quite simply no room for dishonesty. It will destroy a career instantaneously. If you have a problem, simply come and see me and I will help to the greatest extent possible.

Disabilities:

If you believe that you have a disability requiring accommodations in this class, please contact the Coordinator of Support Services for Students with Disabilities as soon as possible. After you receive a letter documenting the appropriate accommodations, please see me so I can work with you to implement them in a timely fashion. It is the student's responsibility to seek and secure accommodations prior to the start of a test or project.

Contact: Janine Allo – office: Hauke 007; phone: 802-651-5961; email: allo@champlain.edu

Course Calendar: Each date is the beginning of the week. Assignments are due at the beginning of the following week – see the modules in WebCT for details.

Date	Week	Topic	Reading	Homework
1/8 1/10	1	Legal	B-Ch 2	Subpoena/2703 Letter
1/15 1/17	2	Seizing Media	B-Ch 4 S-Ch 2	Search Warrant/HW & SW VFT
1/22 1/24	3	Imaging/Previewing	B-Ch 12 S- Ch 9	Convert FTK Image file to DD
1/29 1/31	4	Report Writing-1	B-Ch 10 Appendix A, B, C	Reports- which are good/bad
2/5 2/7	5	FTK	B-Ch 9 S-Ch 13	FTK Case Scenario – part 1
2/12 2/14	6	FTK, RV, PRTK	S- Ch 6	FTK Case Scenario – part 2
2/19 2/21	7	ProDiscover	S- Ch 8	ProDiscover scenario
2/25-2/29		SPRING BREAK		
3/4 3/6	8	EnCase	S-Ch 10	EnCase scenario
3/11 3/13	9	Report Writing-2	S- Ch 11	Create program reports
3/18 3/20	10	File Systems-1	S-Ch 4	Create Helix and Penguin Sleuth CDs

3/24 3/27	11	Helix/Penguin Sleuth	B-Ch 11	Image RAM using Helix
4/1 4/3	12	File Systems-2	S-Ch 5 *See below*	Bootable Helix and Penguin Sleuth
4/8 4/10	13	Volatile data	B-Ch 6	Use FTK to compare image of RAM and hiberfil.sys file
4/15 4/17	14	Misc Stuff	B-Ch 14, 15	Image a CD- session issues, Final Report-comparison of tools
4/21-4/24	Exam Week- Go over final reports			

S= Chad Steel's Windows Forensic B= Chris Brown's Computer Evidence

**Week 12-read documentation on Helix and Penguin Sleuth websites