



## Computer Forensics II (FOR 340)

Gary C. Kessler, Ed.S., CCE, CISSP  
Melodie Woodward, B.S., CCE

---

Welcome to Computer Forensics II!

This course is designed to expose students to advanced concepts in digital/computer forensic analysis. As with Computer Forensics I, there will be a balance between legal and technical aspects, although this course will focus a lot more on the use of specific tools than you saw earlier. 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:** Computer Forensics I (FOR 240)

---

### 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 technology, including computers and the Internet. Students will be asked to perform some basic research on the Internet in addition to delving into technologies with which to examine computer media.
  - *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 students 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**

Gary C. Kessler  
Champlain College  
West Hall  
163 S. Willard St.  
Burlington, VT 05401

Office: 802-865-6460  
E-mail:  
[gary.kessler@champlain.edu](mailto:gary.kessler@champlain.edu)  
Skype name: gary.c.kessler

Melodie Woodward  
Champlain College  
West Hall  
163 S. Willard St.  
Burlington, VT 05401

Office: 802-865-5455  
E-mail:  
[melodie.woodward@champlain.edu](mailto:melodie.woodward@champlain.edu)  
AIM screen name: mwoodward23

---

## Required Textbooks



There are two required texts for this course, both of which make excellent additions to the computer forensics professional's bookshelf:

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

---

## 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. Each week you will be required to post two *substantive* discussion postings. The first will be your response to the question for that week and the second will be your reaction from what your peers wrote. That's where *substantive* comes into play; do not simply reply that you agree or disagree, but explain your opinion. As Charlie McCabe of the *San Francisco Chronicle* used to say, "Any clod can have the facts but having an opinion is an art."

You are most welcome — and invited! — to respond to more than one posting; don't target for the minimum to get by! The more discussion, the better! Have fun with this!

Homework assignments will be given and timely execution of assignments is important to your success and keeping the workflow smooth and predictable.

- Assignment details are located in the Assignment Tool section. Assignments will be picked up and dropped off via the Assignment Tool. Please be familiar with the assignment release and due dates!!

**All assignments have a due date. Late assignments will be accepted only in extraordinary circumstances and only with the instructor's permission, prior to the due date. Please note that *notifying* the instructor that an assignment will be late is not the same as getting permission! All homework must be submitted via WebCT's Assignment Tool (unless you are advised differently). If you have technical problems submitting via WebCT, send a WebCT mail or external e-mail as soon as possible, and include your assignment.**

- **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. There will be opportunity to work in small groups, which will also count towards your class participation grade. Each week's subject matter builds on the knowledge from the previous weeks, so active participation is very important.

Grades will be calculated and weighted as follows:

- Homework Assignments/Exercises = 320 points (53%) [See Course Calendar below for point breakdown]
- Attendance/Participation = 180 points (30%)
- Final Report = 100 points (17%)
- **TOTAL: 600 points (100%)**

The College's standard numerical grading scale will be used for determining 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 [Champlain College Student Handbook](#) 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 can destroy a career instantaneously. For that reason, there is a zero-tolerance policy in this class for cheating, plagiarism, and other forms of academic dishonesty. If you have a problem, simply contact an instructor and we will help to the greatest extent possible. Also, don't wait until the last minute to do homework assignments; last-minute panic is the primary cause of people making poor decisions!

---

### **Students with Disabilities**

If you believe that you have a disability requiring accommodations in this class, please contact Julie Reville, Coordinator of Services for Students with Disabilities, as soon as possible. After you receive your accommodation form, please contact the instructor ASAP to insure that all accommodations are implemented in a timely fashion. *It is the student's responsibility to seek and secure accommodations prior to the start of a test or project. Accommodations cannot be provided until you supply the instructor with a form from the Counseling Office.*

Julie Reville

Counselor/Coordinator of Services for Students with Disabilities

Phone: 802-651-5961

Fax: 802-860-2764

[jreville@champlain.edu](mailto:jreville@champlain.edu)

Student Life Office- Hauke Building Office 007

## Course Calendar

See the Assignments Tool in WebCT for assignment availability and due date information, and assignment details.

Date	Week	Topic	Reading*	Homework
9/2/2008	1	Legal Issues	B-Chap. 2	Subpoena (25 pts) 2703 Letter (10 pts)
9/7/2008	2	Seizing Media	B-Chap. 4 S-Chap. 2	Search Warrant (25 pts) H/W & S/W VFT (20 pts)
9/14/2008	3	Imaging/Previewing	B-Chap. 12 S-Chap. 9	Convert FTK image file to DD (20 pts)
9/21/2008	4	Report Writing 1	B-Chap. 10; App. A, B, C	Reports template (20 pts)
9/28/2008	5	FTK	B-Chap. 9 S-Chap. 13	FTK case scenario, part 1 (30 pts)
10/5/2008	6	FTK, RV, PRTK	S-Chap. 6	FTK case scenario, part 2 (20 pts)
10/12/2008	7	ProDiscover	S-Chap. 8	ProDiscover case scenario (20 pts)
10/19/2008	8	EnCase	S-Chap. 10	EnCase case scenario (30 pts)
10/26/2008	9	Report Writing 2	S-Chap. 11	Create program reports (20 pts)
11/2/2008	10	File Systems 1	S-Chap. 4	Create Helix and Penguin Sleuth CDs (20 pts)

11/9/2008	11	Helix/Penguin Sleuth	B-Chap. 11	Image RAM using Helix (20 pts)
11/16/2008	12	File Systems 2	S-Chap. 5 Additional reading	Bootable Helix and Penguin Sleuth (20 pts)
11/23/2008	<i>THANKSGIVING BREAK</i>			
11/30/2008	13	Helix - RAM, hiberfil.sys	B-Chap. 6	Use FTK to compare image of RAM and hiberfil.sys file (20 pts)
12/7/2008	14	Linux Forensics	B-Chaps. 14, 15	Final report (100 pts)
12/4/2008	15	<i>Finals week</i>	Review class final reports	

\* S = Steel, *Windows Forensics*; B = Brown, *Computer Evidence*

---