

Course Overview & Syllabus

Computer Forensics I **FOR 240-01 and FOR240-51** **Spring 2008**

This course covers topics related to criminal justice and computer technology and is, by its nature, a multi-disciplinary course — which is why this course was originally team developed and taught by a computer guy and a police officer. *Forensics* is the use of science in a court of law; this course looks specifically at how one obtains evidence off of a computer and from network messages and logs, preserving the evidentiary chain, and the legal aspects of the search and seizure of computers and related equipment/information. To that end, we will cover a large set of topics, including:

- Introduction to computer and Internet technology
 - Computer components
 - Computer media
 - The Internet, the Web
 - TCP/IP
- Types of computer and Internet crimes
- Investigations
 - The process of computer forensics and digital investigations
 - Legal methods to obtain the computer
 - Jurisdictions and agencies
 - Internet investigations (e-mail, IRC, chat rooms, etc.)
 - IP addresses and domain names
 - Investigative methods
 - Constitutional law, search and seizure guidelines, case law
 - Privacy Protection Act (PPA)
 - Electronic Communications Privacy Act (ECPA)
 - Seizing electronic evidence
 - Investigative and testimonial challenges
 - CALEA
 - International computer crime laws
- Forensics
 - Types of computers (e.g., laptops, watches, cell phones)
 - Windows and Unix file storage
 - Handling computers and media (seizure and maintaining the integrity of evidence)
 - Searching and retrieving information
 - Encryption and steganography basics
 - Tools (e.g., Sam Spade, ping, traceroute, whois, netstat, EnCase, FTK, WinHex)

This course will present varying levels of detail on the topics above. It is expected that technology students will be more familiar with computers and networks than the Criminal Justice students but less familiar with the legal aspects, and vice versa. Part of the course experience will be the blending of student expertise in the formation of teams. This is intended to be a general, practical course.

Course prerequisite: NET 120 (Computers and Telecommunications)

It is expected that incoming students to this course have basic familiarity with computers, the Internet, and the law.

Student outcomes:

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

- Describe the role of computer forensics in a criminal investigation.
- Demonstrate the ability to perform a basic computer forensic analysis using computer and network-based tools.
- Articulate the laws applying to the appropriation of computers for forensic analysis, citing what laws are relevant and apply under what circumstances.
- Describe the underlying concepts of how data are stored on computers and the general structure of the Internet.
- Apply current industry best-practices to the analysis of some hypothetical and real case scenarios.

Instructor contact information:

Cristian Balan

CHAMPLAIN COLLEGE

Champlain College
West Hall, Room 106
Burlington, VT 05401

Phone: +1 802-865-6477

Fax: +1 802-865-6446

Cell phone:

E-mail: balan@champlain.edu

URL: digitalforensics.champlain.edu

HOME OFFICE

Plattsburgh NY 12901

+1 518-561-5174

(up to 9PM)

+1 518-569-1423

<http://www.nycomputernetworks.com/df>

Texts and supplementary resources:

The first **required text** for this course is *Computer Forensics: Principles and Practices* by Linda Volonino, Reynaldo Anzaldúa, and Jana Godwin (Pearson Prentice-Hall, 2007). This book is a very good — and highly readable — introductory text. It is not **the** complete work on computer forensics, however, and other readings from the Web and handouts will also be assigned to supplement the text. (*Disclosure notice:* Gary C. Kessler is listed as a contributing author of this book largely because the book's authors used some of the papers from the GaryKessler.net Web site. Gary receives no financial incentive to use this book.)

The second **required text** for the course is *First Responder's Guide to Computer Forensics* by Richard Nolan et al. (Carnegie Mellon, 2005) [Source #1](http://www.cert.org/archive/pdf/FRGCF_v1.3.pdf) (http://www.cert.org/archive/pdf/FRGCF_v1.3.pdf) | [Source #2](http://digitalforensics.champlain.edu/download/CERT_FR_Guide_to_Computer_Forensics.pdf) - (http://digitalforensics.champlain.edu/download/CERT_FR_Guide_to_Computer_Forensics.pdf). This volume, a free download from the Internet, contains excellent information about the technical and legal aspects of the computer forensics process.

One of the definitive texts in this field is *Digital Evidence and Computer Crime, 2nd ed.* (<http://www.amazon.com/exec/obidos/ASIN/0121631044>) by Eoghan Casey (Academic Press, 2004). This book provides excellent broad coverage of the field, including computer and network basics, digital investigations, legal issues, and computer crime. While an excellent professional reference and graduate text, the book is a tough read at the introductory level. C&DF majors may wish to eventually purchase this text. (A review of this book can be found at [GaryKessler.net](http://www.garykessler.net).)

These are by no means the only books available on this topic; there are at least a dozen books currently available on computer forensics and each has its own strengths and weaknesses. Students are encouraged to investigate other texts as their studies progress.

[GaryKessler.net](http://www.garykessler.net) has a number of papers and articles on topics related to this course and you should feel free to read and peruse them! In addition, a set of computer forensics URLs, including many to the legal aspects, can be found at <http://www.garykessler.net/library/forensicsurl.html>.

Finally, be sure to download the free Adobe Acrobat reader to be able to view course lecture notes and other course resources.

Attendance, Homework, and Grading:

Active participation in this course is particularly important given the multidisciplinary nature of the subject matter and the multidisciplinary makeup of the students in the class. Students will be assigned to teams comprising at least one criminal justice expert and one computer expert for at least one assignment; these teams will work together so that both "sides" learn about the other. Participation is also important so that you can take notes on the lectures and other activities that will supplement the course instructional material. Also note that the lecture is not intended to replace actually reading the text book!

Homework and other assignments will also be given in this course. *Homework assignments* are generally due the week after they are distributed and *case project assignments* are due two weeks after they are assigned. The *final project* will be assigned approximately a month before it is due.

There is a writing assignment that will be periodically assigned called the "Computer Crime Topic of the Week (TOW)." This is a one- to two-page (single-spaced) assignment, consisting of a summary of the current reading assignment plus a brief piece of independent research — something from a Web site, news report, or other timely item that relates to the reading. I'd like to know what you found important or significant about the week's reading; what interested you, what resonated, what was new, etc., etc. — and *why*? Cite the relevant article or URL, and describe why you chose that article and why you think it important. Think critically about these issues and involve yourself in your writing — e.g., outlawing certain activities to aid law enforcement might sound good at first blush but does it really make sense; why or why not? The TOW needs to relate to the reading but can come from anywhere: a mailing list that you monitor, some security-related site, a friend, the *Burlington Free Press*, an experience from your workplace, etc. Use your imagination and get used to thinking about this.

Each of you will be asked to present at least one of your TOWs to the class. You will prepare a 10 slide Power Point presentation that will present at the beginning of class on your assigned day. Here are some guidelines for your mini-presentation:

- The presentation should be about 10 minutes long.
- Introduce yourself and the topic
- Present an overview
- Summarize your points at the end
- Asks for questions from the class
- Use of humor is encouraged as long as it does not take away from the seriousness of the Digital Forensics content.

. And remember this quote from Herb Caen, former columnist for the *San Francisco Chronicle*: "Any clod can have the facts, but having an opinion is an art." Have an opinion!!!

There will be a final project in this course where you need to do some research on pretty much any computer forensics-related topic of your choice. The project will have two parts; a paper and

a presentation. More detail will be provided during the semester but you can start thinking about topics at any time.

Finally, 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!

Group Work Requirement

From my experience over the past ten years teaching both undergraduate students and adults, I have found that student work improves when accomplished in groups with ample peer review. This mimics a real life work environment where you collaborate on projects. I will split you into groups of 4 students. You will have both Criminal Justice and Digital Forensics students in each group. Before the assignment or project is due, you will meet with your group and review each other's work. You will help your peers by pointing out spelling, grammatical and content issues that they will need to fixed before handing the work in to the instructor. At your group meeting you need to bring in 4 copies of your written work and your peers will "red pen" your assignment. You will hand in your assignment in a folder with your name and group number on it. Your folder will contain both the final work and corrected copies. Your final work will also be posted electronically on the Web so you can easily keep track of your grades. Throughout the semester I will ask the whole group to meet with me during office hours to review your work and discuss your progress.

You need to be able to get along with others, agree on meeting times, and negotiate workloads. I will not grade you on your ability to work successfully as part of a group, but your work and the peer review you will receive will be evident. A student that functions successfully as part of the group, attends all class meeting and lecture, shoulders an equal amount of work and participates at levels that indicate involvement and interest in the subject matter should be looking at receiving the full 15% for participation and attendance

Final course grades will be calculated roughly as follows:

- Homework assignments (10): 20%
- Case project assignments (4): 20%
- Final project paper/"presentation": 10%
- Attendance and participation: 15%
- Presentation of your TOW: 5%
- Midterm: 15%
- Final Exam: 15%

The College's standard numerical scale for calculating final grades is as follows:

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

Applicability of Core Competencies

The Champlain College faculty and administration have committed that our curricula will address these seven critical core competencies:

- Technology
- Critical and Creative Thinking
- Global Awareness
- Oral Communication
- Written Communication
- Quantitative Literacy
- Ethical Reasoning

This course addresses these competencies as outlined below.

Technology: This course covers basic concepts related to computers and networks, the application of this technology to law enforcement and information security incident response, and the relationship of current laws to this technology. Analysis of the contents of computers and network traffic is a growing field affecting business, government, the military, education, and more. This course discusses a wide range of issues related to computer, network, and telecommunications technologies, including hardware, operating systems, software, network applications, and communication protocols.

Critical and Creative Thinking: Due to the broad and highly technical nature of computer and network forensics, the ability to think critically must become second nature to its practitioners. While there are some well-defined processes and procedures for the forensic analysis of computers, every scenario is slightly different and forensic computing remains as much art as it is science. By discussing and analyzing various real and hypothetical case scenarios, students will learn how to determine what needs to be analyzed, what evidence is being sought, what tools are most applicable to the task at hand, and the most efficient way to perform the analysis.

In any computer examination, the individual component must be understood as well as the big picture. Computers are examined as part of a larger investigation; the very nature of this business is critical thinking.

And there is more. A digital forensics examiner must analyze someone else's computer in the context of some event and think like that other person. Everything done on a computer or on the Internet leaves a trace; the digital forensics professional has to find those traces — and that means being able to think like the Bad Guy.

Critical thinking is reinforced by homework assignments and classroom discussions. Rather than focus on bare "facts," the homework and class meetings focus more on how the subject matter integrates with other things that student know and will learn in the future. We also examine how students attitudes change as their level of knowledge — and responsibility — changes.

Global Awareness: International awareness is not a major focus of this course and, in fact, there are few aspects of computer forensics that are geography-specific. The technology is relatively universal and, therefore, the technical solutions are universal. Laws, however, vary country-by-country so that actions that are illegal in some countries are legal in others (such as unleashing a virus). Although not emphasized, the course does describe some of the geographical, political, and cultural differences as they apply to legal aspects, privacy expectations, and cooperation between law enforcement agencies from different countries.

Oral and Written Communication: Computer forensics is a part of the overall criminal justice process and can be made totally useless if the investigator cannot effectively communicate forensics findings both in written form (such as a report or other affidavit) and verbal form (such as a deposition or court testimony). These skills will extend those learned in other classes by use of papers, student presentations, and the demonstration of proper computer forensics techniques.

The digital forensics professional must be able to communicate to many audiences on many levels:

- Communication with peers and managers at the technical level. This requires an understanding of computer, networking, and security concepts, as well as the proper vernacular.
- Communication with attorneys, judges, juries, and users, generally at a non-technical level. A successful technologist must be able to communicate the technical findings in an understandable and compelling way. This is often the most challenging portion of a professional's development.
- Communication with individuals at all levels within an organization with all levels of understanding. This includes upper management and supervisors to peers and subordinates, ranging from the technophobe to the technophile.

This course will provide students with ample opportunity to practice their communication skills through the weekly homework assignments and classroom discussions, but even more so through the research project that is part research paper, part oral presentation, and part presentation graphics. All assignments include grammar and composition as a component of grading.

Quantitative Literacy: Digital forensics professionals have to be able to analyze patterns of activity to differentiate between normal and abnormal activity, as well as to find information within the context of an investigation. Most of the information on computers and networks involves numbers and symbols, and the computer/network analyst needs to be able to find the events that are pertinent to a case — both incriminating and exculpatory. This course will provide students with ample opportunity to practice quantitative literacy through the weekly homework assignments and classroom discussions.

Ethical Reasoning: The use of networks and information often requires ethical considerations — e.g., how to employ individuals' private information that is stored on a computer or Web site, adherence to usage policies and the law, and how to respond to a potentially unethical request by a supervisor. Furthermore, computer forensics managers are involved in the discovery of information that can be used as evidence against them — or to support them. The responsibility

of the computer forensics examiner is high and ethical behavior is a key element in one's credibility. Ethical reasoning is specifically addressed in this course.

Students with 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 your accommodation form, please see me so I can work with you to implement them in a timely fashion.

Contact: Allyson Krings, Coordinator of Support Services for Students with Disabilities (Hauke 007i, 802-651-5961, krings@champlain.edu)

Academic Honesty Policy

The Champlain College Student Handbook (*The Rudder*) describes the College's Academic Honesty policy. If the instructor suspects that a student has plagiarized or otherwise cheated on an assignment — i.e., to either actually or attempt to knowingly give, receive, or use work that is not your own — the instructor can give a 0 on that assignment.

This is not to suggest that the college or the program discourages your collaboration with students and others; in fact, we encourage as much collaboration as possible. The point of this policy is that work that you submit as your own *has* to be your own! If you work with another person or other resource that helps you learn an answer to something, that's fine — but what you turn in should be in your own words and clearly demonstrate **your** understanding. If you're unsure, indicate on your paper that you worked with others.

Don't cheat; there's no margin in it!! If you have a problem, talk to me instead.

This course along with the syllabus has been adapted from Gary Kessler, Director of the Center for Digital Forensics and Professor of Digital Forensics at Champlain College and it is being used with permission.

Course calendar: (Subject to change but you will be notified of changes...)

There is an assignment, project work and reading each week during the semester. During each of the 15 weeks, expect to spend a full 6-10 hours working on course materials outside the classroom.

Week/Lecture No. (Start Date)	Topic	Reading*	Assignment
1 (9/2)	Introduction to computer forensics	VAG Chaps. 1, 2	Lecture 1 Homework
2 (9/8)	Basic computer terms and concepts; Legal principles related to digital investigations (Part 1)	VAG Chaps. 6 (pp. 195-216), 12; CMU § 1.4.1	Lecture 2 Homework Case project #1 Assigned
3 (9/15)	"Computer topics for CJ majors!" Review of basic computer skills, including downloading files, installing programs, accessing the command line, and simple base conversion; WinHex.		Lecture 3 Homework
4 (9/22)	Hard drive basics and file systems; Legal principles related to digital investigations (Part 2)	VAG Chap. 5 (pp. 158-173); CMU § 1.4.2, 2.1, 2.2	Lecture 4 Homework Case project #1 Due Case project #2 Assigned
5 (9/29)	Seizing computers; Computer forensics process and tools	VAG Chaps. 3, 4; CMU § 2.2.12-2.2.17, 2.3, 3	Lecture 5 Homework
6 (10/6)	FAT12; Metadata; File signatures	VAG Chaps. 6 (pp. 216-221), 7; CMU § 2.2.3-2.2.6	Case project #2 Due
7 (10/13)	Computer forensics, privacy, and ethics	VAG Chap. 13	MID-TERM
10/13	October Recess – we have class on Tue 10/14 – it is a Monday schedule		
8 (10/20)	Networking basics; Internet basics, domains, addresses, and TCP/IP	VAG Chaps. 6 (pp. 221-229), 9	Lecture 8 Homework
9 (10/27)	E-mail, headers, and logs; Network/Internet software tools	VAG Chap. 8 (pp. 282-304)	Lecture 9 Homework Case project #3 Assigned
10 (11/3)	Registry information; Browsers; Instant Messaging	VAG Chaps. 7 (pp. 240-251), 8 (pp. 304-307); CMU § 2.2.7 &	Lecture 10 Homework Final Project Assigned

4.7.3			
11 (11/10)	Cell phone forensics	VAG Chap. 5 (pp. 173-188)	Lecture 11 Homework Case project #3 Due Case project #4 Assigned
12 (11/17)	Cryptography and steganography	VAG Chap. 7 (pp. 264-267)	Lecture 12 Homework
13 (11/24)	"The Federal perspective on computer crime." Guest lecturer: TC Fuller, FBI <i>12/26-11/30 Thanksgiving Break NO class on Wed 11/26 – loose participation points if you skip Monday Class</i>		Case project #4 Due
14 (12/01)	STUDENT PRESENTATIONS		Final Project Due
15 (12/08)	STUDENT PRESENTATIONS		FINAL EXAM

(*) NOTE: For the readings, "VAG" refers to Volonino, Anzaldua, & Godwin (*Computer Foresnics*) and "CMU" refers to Nolan et al. (*First Responder's Guide to Computer Forensics*).