

CJ442 Computer Forensics – Spring 2010

Syllabus

Dr. Peter Stephenson
Email: pstephen@norwich.edu

Office Address: Dewey 205
Telephone Number: 485-2007

Text/Materials:

1. File System Forensic Analysis, Brian Carrier, Addison-Wesley, ISBN 0-321-26817-2. Numerous readings will be on reserve in the library or available in pdf form on Moodle.
2. The instructor will provide (via Moodle) course notes that will allow students to follow the course PowerPoint presentations.

Course Description

This course provides the student with an ability to perform basic computer forensic techniques and use appropriate media analysis software as well as an understanding of the digital investigative process. Knowledge of the security, structure and protocols of network operating systems and devices will be covered as students learn to gather evidence in both a networked and single-station environment and to image and restore evidence properly without destroying its value. The students will learn and practice gaining evidence from a computer system while maintaining its integrity and a solid chain of custody. Within the laboratory, the students will gain hands-on experience in the use of current investigative tools.

Prerequisite

IS228 Data Structures , CP337 Operating Systems, or approval of the instructor.

Grading

Exams (2)	30%
Projects/Assignments/Quizzes	40%
Class/Lab Participation and Attendance	15%
Final Project/Presentation	15%
TOTAL	100%

Class Policies

Class Participation: Part of your grade will be based on your participation in the classroom and lab. Your grade will be lowered for the following situations: non-attendance, disruption of the class/lab, non-participation in lab exercises, not being prepared for class/lab.

Quizzes: In preparation for most classes I will assign “study words” and/or readings that you must know for the next class meeting. A quiz will normally take place at the beginning of the following class.

Assignments/Projects: You are required to keep a copy of every item that you submit to me for review or grading. If the assignment does not make it to me (i.e. lost in cyberspace), you need to have a backup.

Academic Dishonesty: Plagiarism and cheating are serious offenses and may be punished by failure on exam, paper or project, failure in course and/or expulsion from the University. For more information refer to the "Academic Dishonesty" policy in the University Undergraduate Catalog.

Assignment Grading: Assignments will be graded on a 10-point scale. All late projects will begin at 5 points and be graded downward – one additional point off for each calendar day late (i.e. an assignment that is five days late will be worth 0 points). Team projects may not receive one grade - if I perceive that one or more individuals did minimal work, they will receive a correspondingly lower grade than others on the team.

Course Department: No hats or any kind will be worn in class or lab. No food of any kind in the lab. The “section marcher” will take attendance prior to my arrival in class. He/she will call the class to attention and report the attendance.

Lab Access (room and software): Students will be provided access to the basement lab facility and will have access to appropriate software. Students are responsible for protecting the key and dongle. Missing keys or dongles are the responsibility of the student and must be replaced.

COURSE CALENDAR (Subject to change based on Dr. Stephenson's travel schedule – students will be notified) – When Dr. Stephenson is off campus, assignments will be conducted via NUoodle.

DATE	TOPIC
Jan 19 (T)	Course Introduction, Forensic and Investigative Basics
21 (R)	Disk Structure Basics – No Class
21 (L)	Removing/Reattaching Disks, Acquiring disk images
26 (T)	Disk Structure, Disk File Structures
28 (R)	Disk File Structures, DOS toolkit commands: dd, netcat, strings, grep
28 (L)	Windows memory imaging, dd, netcat
Feb 2 (T)	Criminal Justice Issues
4 (R)	Criminal Justice Issues
4 (L)	Search, Seizure, Chain-of-Custody
9 (T)	Linux Basics
11 (R)	Linux Basics
11 (L)	Linux Basics
10 (T)	ProDiscover Intro
12 (R)	dd/FastBlock imaging & use of search commands
12 (L)	dd/FastBlock imaging & use of search commands
16 (T)	ProDiscover (basics, search, bookmarking)
18 (R)	ProDiscover (signature analysis, bookmarking)
18 (L)	ProDiscover (search and signatures)
23 (T)	Search analysis
25 (R)	EXAM #1
25 (L)	Search, ProDiscover report generation
Mar 2 (T)	Windows issues
4 (R)	lnk files, pid_guid, registry,
4 (L)	lnk files, pid_guid, registry,
9 (T)	Windows registry
11 (R)	Link Analysis
11 (L)	Link Analysis
===== 13 – 22 Mar – Spring Break =====	
23 (T)	Incident Response Forensics
25 (R)	ProDiscover in Incident Response
25 (L)	ProDiscover in Incident Response

	30 (T)	Steganography
Apr	1 (R)	Steganography
	1 (L)	Steganography
	6 (T)	Investigation Projects
	8 (R)	Investigation Projects
	8 (L)	Investigation Projects
	13 (T)	Gargoyle
	15 (R)	Gargoyle
	15 (L)	Gargoyle
	20 (T)	Passwords
	22 (R)	Passwords
	22 (L)	Passwords
	27 (T)	No Class – Project Prep
	29 (R)	No Class – Project Prep
	29 (L)	No Class – Project Prep
May	4 (T)	Present Projects
	6 (R)	Present Projects
	6 (L)	Present Projects
	2 (T)	Reading Day
May	9 - 14	EXAMS