CYBERCRIME DETECTION AND FORENSICS
CIS 4930-01
Syllabus — Spring 2010

Instructor

Randolph Langley
Email: langley@cs.fsu.edu
Telephone: 644-4290
Office Location: 208 MCH Building
Office Hours:

Tuesday, Thursday immediately after class in 016 LOV
Wednesday, 9:30 to 11:00 in 208 MCH
Tuesday, Thursday 9:30 to 10:30 in 208 MCH

Class Meetings

Tuesday, Thursday from 2:00pm until 3:15pm in Room 016 Love (the Networking Lab)

Class Home Page

http://www.cs.fsu.edu/~langley/CIS4930r-2010-1

Course Description

Cybercrime activities leave a trail of incriminating evidence. In this course, students will focus on learning tools, techniques, and procedures for detecting cybercrime and analyzing collected data related to past and ongoing cyber offenses. The focus will be on forensic approaches that preserve the legal value of the collected evidence.

Class Prerequisites

CDA 3100, Computer Architecture I
CJE 4610, Crime Detection and Investigation

Objectives

This is a technical class focused on detecting cybercrime and analyzing collected data. In particular, our aims will be to study both traditional "post-mortem" analysis and emerging "live" response techniques.

- Be able to distinguish between post-mortem analysis and live response.
- Be able to carry out post-mortem analysis on Microsoft platforms.
- Be able to carry out effective live response on Microsoft platforms.
- Understand the issues and differences in post-mortem analysis and live response for Unix/Linux platforms and with Microsoft platforms.
- Understand evidentiary issues in both cold and live analyses.

Class Topics

- Introduction to Digital Forensics and Cybercrime
- Technical Introduction to Windows
- Brief Introduction to Unix/Linux
- Windows Live Response: Collecting and analyzing data under Windows
- Unix/Linux Live Response: Collecting and analyzing data under Linux
- Windows Memory Analysis
- Windows Registry Analysis
- Windows File and filesystem analysis
- Unix/Linux File and filesystem analysis
- Windows Executable file analysis
- Unix/Linux Executable file analysis
- (if time permits) Rootkits and Blue Pills

Required Texts

Windows Forensic Analysis, 2nd Edition, by Harlan Carvey. Syngress, 2009. (This will be abbreviated as WFA in class materials.)
Malware Forensics, James Aquilina, Eoghan Casey, and Cameron Malin. Syngress, 2008. (This will be abbreviated as MF in class materials.)

Additional recommended material

- *File System Forensic Analysis*, by Brian Carrier. Addison-Wesley, 2005. (Abbreviated version provided in class materials.)
- *Digital Evidence and Computer Crime*, 2nd edition, by Eoghan Casey. Academic Press, 2004. (Abbreviated version provided in class materials.)
- *Information Warefare and Security*, by Dorothy Denning. ACM Press, 1999. (Abbreviated version provided in class materials.)
- *Fighting Computer Crime*, by Donn Parker. Wiley Computer Publishing, 1998. (Abbreviated version provided in class materials.)

Additionally, throughout the semester, the instructor may add topical material, generally culled from recent news articles. via links from the class home page.

Assessment

ITEM	POINTS
1st Midterm (February 11th)	20
2nd Midterm (March 25th)	20

Final Exam (Thursday, April 29, from 7:30am to 9:30am)	20
Assignments	30
Final Paper (due at the beginning of class on April 22nd)	10

Grades

A	90 - 100
B+	88 - 89
B	80 - 87
C+	78 - 79
C	70 - 77
D	60 - 69
F	0 - 59

Class Policies

Lateness Penalty

Note that **30%** of your grade is determined by the work done in the assignments. Assignments must be submitted on paper on the appropriate day at the beginning of class. Please turn in assignments on time. **There will be a 50% penalty** for late submissions.

Academic Honor Policy

The Florida State University Academic Honor Policy outlines the University's expectations for the integrity of students' academic work, the procedures for resolving alleged violations of those expectations, and the rights and responsibilities of students and faculty members throughout the process. Students are responsible for reading the Academic Honor Policy and for living up to their pledge to "... be honest and truthful and ... [to] strive for personal and institutional integrity at Florida State University. (Florida State University Academic Honor Policy, found at http://dof.fsu.edu/honorpolicy.html.)

Academic dishonesty will **not** be tolerated in this course. Do not turn in other people's work as your own; this includes, but is not limited to, unattributed copying from web pages, other students' work, books, journals, or broadcast media. **Citations and clear delineation of cited material from your own original work is mandatory.**

Attendance

Attendance at all class meetings is expected, and attendance may be taken each class session. **Please extend courtesy in class by arriving on time, staying until dismissed, and refraining from food and drink**.

Excused absences include documented illness, deaths in the family and other documented crises, call to active military duty or jury duty, religious holy days, and official University activities.

These absences will be accommodated in a way that does not arbitrarily penalize students who have a valid excuse. Consideration will also be given to students whose dependent children experience serious illness.

You are responsible for all information explained in class, some of which will not be available in written or electronic form. The instructor is not obligated to repeat announcements of future exams, assignments, schedule changes, question sets, pop quizzes, or hints on assignments. If you are forced to miss a class, it is your responsibility to get class notes from a friend and check with the instructor for handouts. Assignments and general class information will be posted on the class home page.

Communication

You should check your electronic mail frequently for information about this course, as well as the class home page. You are also encouraged to use email to ask questions and report problems. ***If you are experiencing difficulty or are concerned about your progress, please speak with the instructor immediately.***

Americans with Disabilities Act

Students with disabilities needing academic accommodation should:
(1) register with and provide documentation to the Student Disability Resource Center; and
(2) bring a letter to the instructor indicating the need for accommodation and what type. This should be done during the first week of class.

This syllabus and other class materials are available in alternative format upon request.
For more information about services available to FSU students with disabilities, contact the:

Student Disability Resource Center
874 Traditions Way
108 Student Services Building
Florida State University
Tallahassee, FL 32306-4167
(850) 644-9566 (voice)
(850) 644-8504 (TDD)
sdrc@admin.fsu.edu
http://www.disabilitycenter.fsu.edu/

Please advise the instructor at your earliest convenience (within one week) if you have a disability that will require a reasonable accommodation for the successful completion of this course. Also, as indicated above, you should register with the and provide documentation to the Student Disability Resource Center, and provide the instructor a letter indicating the need for accommodation and indicating what type.

Syllabus Change Policy

Except for changes that substantially affect implementation of the evaluation (grading) statement, this syllabus is a guide for the course and is subject to change with advance notice.

Calendar for CIS4930-01 Spring 2010

Month	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Week #	Notes
January	3	4	5	6	7	8	9	01	First week of classes
January	10	11	12	13	14	15	16	02	
January	17	18	19	20	21	22	23	03	January 18th is Martin Luther King Day, no classes
January	24	25	26	27	28	29	30	04	
January/February	31	1	2	3	4	5	6	05	
February	7	8	9	10	11	12	13	06	Midterm #1 will be on February 11th
February	14	15	16	17	18	19	20	07	
February	21	22	23	24	25	26	27	08	
February/March	28	1	2	3	4	5	6	09	
March	7	8	9	10	11	12	13	10	Spring Break, no classes
March	14	15	16	17	18	19	20	11	
March	21	22	23	24	25	26	27	12	Midterm #2 will be on March 25th
March/April	28	29	30	31	1	2	3	13	
April	4	5	6	7	8	9	10	14	
April	11	12	13	14	15	16	17	15	
April	18	19	20	21	22	23	24	16	Last week of classes; final paper due on April 22
April	25	26	27	28	29	30	1	17	Finals week: our final examination is on Thursday, April 29th from 7:30am until

									Room 016.