CYBERCRIME DETECTION AND DIGITAL FORENSICS
CIS 4385
Syllabus

Delivery Mode: Traditional

Class Description

"This course discusses tools, techniques, and procedures for detecting cybercrime and analyzing collected data related to past and ongoing cyber offenses, along with preserving the legal value of the collected evidence."

Objectives

This is a technical class focused on the forensic identification, collection, and analysis of digital evidence which can be used in the detection of criminal activity including but not limited to cybercrime. At the end of the course, students will

1. be able to distinguish between post-mortem analysis and live response;
2. be able to perform analysis using approved forensic tools;
3. be able to perform effective collection of digital evidence, including creating forensic images;
4. be able to describe the issues and challenges associated with the collection and analysis of digital evidence and the tools used to perform these tasks;
5. be able to describe basic legal issues in digital forensics.

Class Topics

- Introduction to Digital Forensics and Cybercrime
- Technical Introduction to Operating Systems
- Forensic collection of digital evidence
- Maintaining data integrity - Hashing
- Operating System forensic artifact analysis

- Meta Analysis
- File and filesystem analysis

Required Text

Digital Forensics, Investigation, and Response, 4th edition, 2022, Chuck Easttom

Prerequisites

You are required to have passed CIS4360 and CJE3110 in order to take this class.

Additional recommended material

Digital Archaeology, by Michael Graves, 2013. (Abbreviated DA in class materials.)

Digital Forensics for Handheld Devices, by Eamon P. Doherty. CRC Press, 2013. (Abbreviated DFHD in class materials.)

Computer Forensics: Cybercriminals, Laws, and Evidence, by Marie-Helen Maras. Jones & Bartlett, 2012. (Abbreviated CFCLE in class materials.)

Malware Forensics Field Guide for Windows Systems, by Cameron H. Malin, Eoghan Casey, and James Aquilina. Syngress, 2012. (Abbreviated MFFGWS in class materials).

Digital Forsensics with Open Source Tools, by Cory Altheide and Harlan Carvey. Syngress, 2011. (Abbreviated DFOST in class materials)

**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.)

**File System Forensic Analysis,* by Brian Carrier. Addison-Wesley, 2005. (Abbreviated FSFA in class materials.)

Digital Evidence and Computer Crime, 2nd edition, by Eoghan Casey. Academic Press, 2004. (Abbreviated DECC in class materials.)

Information Warfare and Security, by Dorothy Denning. ACM Press, 1999. (Abbreviated IWS in class materials.)

Fighting Computer Crime, by Donn Parker. Wiley Computer Publishing, 1998. (Abbreviated FCC in class materials.)

Additionally, throughout the semester, I may add topical material, generally culled from

recent news articles. I will add links to this material on the class home page.

Assessment

ITEM	POINTS
1st Midterm	20
2nd Midterm	20
Final Exam	30
Assignments	30
Class participation. You are expected to attend all classes and participate in this class.	20
TOTAL	**120**

Grades

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

Class Policies

Problem Solving Assignments

Please turn in assignments on time. **No late submission will be accepted.**

In the event of an excused absence, you may request an extension for the assignment.

Attendance

Attendance at all class meetings is expected, and attendance may be taken each class session in the form of a sign-in roster. **Please extend courtesy in class by arriving on time, staying until dismissed, and refraining from food and drink.** You are responsible for all information explained in class, some of which will not be available in written or electronic form. I will not feel 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 also your responsibility to get class notes from a friend and check with me for handouts. I will use the class home page to give out assignments and general class information. You are expected to participate in the class, and this participation makes up 20 points of the 120 points of your graded activities (that is, about 16.7% of your final grade.)

If you are not present when attendance is checked you will be considered absent. Each unexcused recorded absence will result in a reduction of the class participation grade.

University Attendance Policy

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.

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; however, all email correspondence must be done via an email account from Florida State University, and not via third party providers.

Academic Dishonesty

There is no group work in this class. All assignments must be done solely by you. Do not solicit help from your fellow students or from any other source.

Academic dishonesty will **not** be tolerated. 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 as distinguished from your own original work is mandatory.**

The Florida State University academic honor policy is at http://dof.fsu.edu/content/download/21140/136629/AHP2010Revision.pdf

Official FSU statement on the Academic Honor Policy:

```
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://fda.fsu.edu/Academics/Academic-Honor-Policy)

University ADA statement

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.

Please note that instructors are not allowed to provide classroom accommodation to a student until appropriate verification from the Student Disability Resource Center has been provided.

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:

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
http://www.disabilitycenter.fsu.edu/

Please advise me 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 and provide documentation to the Student Disability Resource Center, and provide me a letter indicating the need for accommodation and indicating what type.

Summary

If you are experiencing difficulty or are concerned about your progress, please speak with me immediately.

Syllabus changes

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.