Computer Forensics Syllabus

Text/Materials:

1. File System Forensic Analysis, Brian Carrier, Addison-Wesley, ISBN 0-321-26817-2.
2. Computer Forensics JumpStart, 2nd Edition, Michael G. Solomon, K Rudolph, Ed Tittel, Neil Broome, and Diane Barrett, ISBN: 978-0-470-93166-0
3. AccessData Forensic Tool Kit User Guide (to be provided on NUoodle).
4. Numerous readings will be on reserve in the library or available in pdf form on Moodle.
5. 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. Students will perform tool testing and critical reviewing of commercial digital forensic tools for publication in *SC Magazine* as the final project.

Prerequisite

None

SESSION		TOPIC	READINGS
1	(Lab)	Intro to the course, lab tool orientation, Bonnie and Clyde orientation, imaging	Pre-Course Reading Assignment: JumpStart Ch 1, 2, 3 and 4, FTK Imager User Guide, "A Career in Forensics"
2	(Lect)	Evidence Management and Triage	JumpStart Ch 5, 6 and 8 and White paper on Triage on Nuoodle
3	(Lab)	Windows file system - Start Bonnie and Clyde case	File System Forensic Analysis Chapter 1 - 5 and 8 - 13, and FTK User Guide Chapter 1, 2, 3, 4, 5, 7, 8, 9
4	(Lect)	Windows file system - Bonnie and Clyde case	
5	(Lecture)	Bonnie and Clyde - Searches	

6	(Lect)	Bonnie and Clyde - Searches	JumpStart Ch 9
7	(Lab)	Bonnie and Clyde - Registry analysis	
8	(Lab)	Bonnie and Clyde - Registry	
9	(Lab)	Bonnie and Clyde - Reporting	
10	(Lab)	Bonnie and Clyde - Reporting	
11	(Lab)	Bonnie and Clyde Final Report	
12	(Lecture)	Forensic tools - project assignments	
13	(Lab and Lecture)	Start project testing - Lab	
14	(Lect)	Project testing - Lab	
15	(Lab)	Project testing - Lab	
16	(Lab)	Project testing - Lab	
17	(Lect)	Complete Project testing - Lab	
18	(Lab)	Linux Basics	File System Forensic Analysis Chapter 14, 15
19	(Lab)	Linux Lab	
20	(Lecture)	Mobile device forensics	
21	(Lab)	Mobile device forensics lab	
22	(Lab)	Mobile device forensics lab	
23	(Lecture)	Mac Forensics	
24	(Lecture)	Encryption	JumpStart Ch 7, FTK User Guide Chapter 11, Readings on NUoodle
25	(Lecture andLab)	Windows analysis and the Registry including shellbag analysis	
26	(Lab)	Windows file/malware analysis with FTK-4 - Lab	
27	(Lecture)	Anti-forensics	Materials on NUoodle
28	(Lab)	Present Projects	

29	(Lab)	Present Projects	