CS 4320 : COMPUTER AND MOBILE FORENSICS

Semester Hours:	3.0	*Contact Hours:* 3
Coordinator:	Sankardas Roy	
Text:	Handbook of Digital Forensics and Investigations	
Author(s):	CASEY, E. (ED.)	
Year:	2010	

SPECIFIC COURSE INFORMATION

Catalog Description:

Overview of computer forensics. Computer forensic procedures: identification and collection of potential evidence; reverse engineering; analysis and reporting. Hands-on experience with forensics tools. Forensic mechanisms for mobile devices. Analysis of synthetic and real datasets. Prerequisites: Corequisite of CS 3080 or CS 3270, and a Grade of C or better in CS 3320. Credit cannot be earned for both CS 4320 and CS 5320.

Course type: **ELECTIVE**

SPECIFIC COURSE GOALS

- I can compare and contrast tools used in computer and smartphone forensics.
- I can explain the organization of file system structures in computers.
- I can plan how to securely acquire data from devices under the forensic examination.
- I can articulate mechanisms for recovering encrypted datasets.
- I can create a timeline of events and identify linkage b/w subjects and objects for synthetic and real datasets.

LIST OF TOPICS COVERED

- Course Overview (~8%)
    - Computer security vs. computer forensics
    - Legal and ethical issues in forensics
- Introduction to digital forensics (~28%)
    - Computer attacks

        - Malware, attack vectors, vulnerability, exploits, intrusion schemes
    - Concepts of memory and hard disk management
        - Swap space, hibernation files, disk sectors, deleted files
    - Forensic artifacts acquisition
        - Reliable acquisition: write-blocking, image duplication
    - Preliminary investigation: User accounts, files, logs, timeline analysis
- Forensic Analysis for Computers (~30%)
    - Forensic artifacts: temp file, link file, etc.
    - Reading Windows Registry offline
    - Windows malware reverse engineering
    - Use of forensic tools, for example: EnCase, Sleuth Kit.
- Forensic Analysis for Smartphones (~27%)
    - Specialty of smartphone forensic procedures
    - Different classes of data acquisition process (and tools) and the tradeoff
    - Additional forensic artifacts, such as contact list, call logs, SMS messages
    - Platform specific issues and forensic methodologies: Android vs. iOS;
    - Use of forensic tools, for example: Flasher Box, BlackLight.
- Reporting (~7%)
    - How to document forensic investigation procedures and report the analysis results
        - Elements & organization