CSCE 517: COMPUTER CRIME AND FORENSICS

Catalog Description:
517 -- Computer Crime and Forensics. (3) (Prereq: CSCE 311) Methodical approaches for collecting and preserving evidence of computer crimes. Foundational concepts such as file system structures, MAC times, and network protocols; tools for extracting evidence; general legal issues.

Prerequisite(s) By Topic:
Programming and data structures
File systems

Textbook(s) and Other Required Material:
Kevin Mandia and Chris Prosise, *Incident Response: Investigating Computer Crime,* Osborne/McGraw-Hill, 2001, ISBN: 0-07-213182-9.

Eoghan Casey, *Handbook of Computer Crime Investigation: Forensic Tools and Technology*, Academic Press, Boston, MA, 2002, ISBN: 0-12-163103-6.

We use the F.I.R.E. Forensic and Incident Response Environment Bootable CD as our forensic environment. http://fire.dmzs.com/

Computing Platform:
Both Unix and Windows; forensics investigations are carried out in each domain.

Course Objectives: {Assessment Methods Shown in Braces}
1. Describe forensic techniques {assignments, tests}
2. Perform forensic analysis {projects, tests}
3. Understand capabilities and use of forensic toolkits. {projects, tests}

Topics Covered:
1. Handling Evidence, Chain of Custody, Admissibility
2. The Forensic Process - Initial Assessment
3. The Forensic Process – Methodologies (Drop/Add deadline)
4. The Forensic Process – Evaluating Tools
5. Windows NT/2000 Forensics
    a. Windows NT/2000 Registry Basics, File System Structure, Processes, Accounts
    b. Windows NT/2000 Forensics Tools and Toolkits
    c. Initial Response to a Windows NT/2000 Incident - Volatile Data Collection
    d. Windows NT/2000 Incident Investigation - Collecting Evidence
6. UNIX Forensics
    a. UNIX File System Structure, Inodes, MAC times, Processes, Accounts
    b. UNIX Forensics Tools and Toolkits
    c. Initial Response to a UNIX - Volatile Data Collection
    d. UNIX Incident Investigation - Collecting Evidence
7. Review of UDP, TCP, ICMP, and IP and Investigating Routers

8. Internet Research, Tracing Ip, MAC, E-Mail addresses
9. Network Forensics
10. Wireless Networking
11. Routers
12. PDAs and Embedded Devices
13. Examining Malicious Programs and Code

Laboratory Projects:
Three fairly extensive forensic analysis projects; one in UNIX, one in Windows and one network analysis.

Syllabus Flexibility: High. The instructor approves the choice of textbook and syllabus.

Relationship of Course to Program Outcomes:
The contribution of each course objective to meeting the program outcomes is indicated with the scale:
3 = major contributor, 2 = moderate contributor, 1 = minor contributor. Blank if not related.

	Program Outcomes										
Course Objectives	1. Logic & Math	2. Computing Fundamentals	3. Apply Computing Principles	4. Work on teams	5. Communicate Effectively	6. Liberal arts & Soc. Sciences	7. Basic Science and Lab Procedures	8. Learn New Tools & Processes	9. Employed upon Graduation	10. Application Area	11. Electronics and Digital Sys Design
1. Describe forensic techniques			3		2			2	2		
2. Perform forensic analysis			3		2			3	2		
3. Understand capabilities and uses of forensic toolkits			3		2			3	2		

Estimated Computing Category Content (Semester hours):

Area	Core	Advanced	Area	Core	Advanced
Algorithms			Data Structures		
Software Design		2	Programming Languages		
Computer Architecture		1			

Estimated Information Systems Category Content (Semester hours):

Area	Core	Advanced	Area	Core	Advanced
Hardware and Software		1	Networking and Telecommunications		
Modern Programming Language			Analysis and Design		1
Data Management			Role of IS in an Organization		1
Quantitative Analysis			Information Systems Environment		

Oral and Written Communication: Three written forensic analysis reports**.**

Social and Ethical Issues: A major component of the course is legal issues relating to computing and computer crime.

Theoretical Content:
None.

Analysis and Design:
No program analysis, but extensive analysis of systems for forensics evidence.

Collaborative Work:
Some projects may be done in teams.

Course Coordinator: Manton Matthews

Class/Laboratory Schedule:
Lecture: 3 periods of 50 minutes or 2 periods of 75 minutes per week

Modification and Approval History
Course approved Spring 2004
New description June 2005 by Manton Matthews and Caroline Eastman.