COURSE DESCRIPTION

Department and Course Number: COMP 5350
Course Title: Digital Forensics
Total Credits: 3
Required: No
Prerequisites: COMP 2710 or ISMN 3080 or departmental approval
Class meetings per week: 3 hours
Lab meetings per week: 0 hours
Course Coordinator: Dr. Drew Hamilton
Date Prepared: Spring 2010

Current Catalog Description:
Digital forensics encompasses not just computers, but the increasingly pervasive digital devices. There is a growing need for computer science, software engineering and information system graduates with the skills to investigate these crimes. This course will introduce the topics of computer compromises and computer forensics. Students will be required to learn different aspects of computer crime and ways in which to uncover, protect and exploit digital evidence. Students will be exposed to different types of tools, both software and hardware, and be able to use them to perform rudimentary incident analysis and investigation.

Textbooks:

References (Optional):
1. Farmer & Venema, Forensic Discovery, Addison-Wesley.

Course Objectives:
Disk Forensics Fundamentals:
1. Distinguish the basics of NTFS vs. FAT32 vs. UNIX file systems and data storage
2. Describe wide varieties of data storage devices, how they operate, and how these devices contain evidence
3. Capture critical system information from computer disks
4. Capture critical information from a network incident.

Network Forensics Fundamentals:
1. Describe the basics of good incident response techniques.
2. Identify the footprint of an attack and how a perpetrator can be identified.
3. Understand the challenges of network forensics vs. disk forensics.

Security, management, and forensics:
1. Describe the threats and vulnerabilities to which a computer system and/or network may be exposed,
2. Design policies and associated controls to assist in providing appropriate incident response.
3. Identify IP, critical or confidential information from which a computer incident might arise.

Law and ethics:
1. Discuss the 4th Amendment to the US Constitution and its application to computer / network search and seizure,
2. Apply the rules of evidence as they relate to an electronic crime scene and to obtaining digital evidence.
   (i.e. recognize what can and can NOT be seized at an electronic crime scene.)
3. Discuss the methods of ensuring the chain of custody of evidence.

**Prerequisites by Topic:**
1. Computer Fundamentals
2. Basic understanding of operating systems
3. Basic understanding of networks

**Topics Covered:** (specify number of hours on each)
1. Introduction to Digital Forensics (3 hours)
2. Incident Response in Windows-Based Systems (3 hours)
3. Incident Response in Linux-Based Systems (3 hours)
4. Network-Based Forensics (3 hours)
5. Common Forensic Analysis Techniques (3 hours)
6. Web Activity Reconstruction (3 hours)
7. Email Activity Reconstruction (3 hours)
8. Windows Registry Reconstruction (3 hours)
9. Forensic Toolkits (3 hours)
10. Forensic Analysis of Mobile Devices (3 hours)
11. Forensics and Cryptography (3 hours)
12. 4th Amendment / Ethics (3 hours)
13. Rules of Evidence / Chain of Custody (3 hours)
14. Research paper presentations (3 hours)
15. Exams (3 hours)

**Oral and Written Communications:**
Each student writes a research paper on topics related to digital forensics. Graduate students are required to produce a much more extensive and in-depth paper that is publishable as a research article in the field.

**Social and Ethical Issues:**
Contains significant component on law and ethics relating to digital forensics.

**Grading:**
Homework assignments..........................10%
Term projects.....................................20%
Research paper.................................10%
Midterm exam 1.................................15%
Midterm exam 2.................................20%
Final exam......................................25%
Theoretical Content:
None.

Problem Analysis and Solution Design:
None.