COMP 5350, Digital Forensics

Credit hours: 3 lecture
Contact hours: 3 lecture

Catalog Description: Computer compromise and forensics, with focus on computer crime and ways to uncover, protect, and exploit digital evidence.

Prerequisites: COMP 2710 or ISMN 3080
Corequisites: None

Selected Elective Course (CSCI, SWEN, WIRS)

Instructor or Course Coordinator: Dr. Tony Skjellum

Required Textbook
Jones and Rose, Real Digital Forensics, 2006.

Reference Materials
Selected current conference and journal articles; other selected resources

Course Outcomes
The student will be able to

Disk Forensics Fundamentals:
• distinguish the basics of NTFS vs. FAT32 vs. UNIX file systems and data storage.
• describe wide varieties of data storage devices, how they operate, and how these devices contain evidence.
• capture critical system information from computer disks.
• capture critical information from a network incident.

Network Forensics Fundamentals:
• describe the basics of good incident response techniques.
• identify the footprint of an attack and how a perpetrator can be identified.
• understand the challenges of network forensics vs. disk forensics.

Security, management, and forensics:
• describe the threats and vulnerabilities to which a computer system and/or network may be exposed.
• design policies and associated controls to assist in providing appropriate incident response.
• identify IP, critical or confidential information from which a computer incident might arise.

Law and ethics:
• discuss the 4th Amendment to the US Constitution and its application to computer / network search and seizure.
• 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.)
• discuss the methods of ensuring the chain of custody of evidence.

Topics Covered
• Introduction to Digital Forensics (3 hours)
• Incident Response in Windows-Based Systems (3 hours)
• Incident Response in Linux-Based Systems (3 hours)
• Network-Based Forensics (3 hours)
• Common Forensic Analysis Techniques (3 hours)
• Web Activity Reconstruction (3 hours)
• Email Activity Reconstruction (3 hours)
• Windows Registry Reconstruction (3 hours)
• Forensic Toolkits (3 hours)
• Forensic Analysis of Mobile Devices (3 hours)
• Forensics and Cryptography (3 hours)
• 4th Amendment / Ethics (3 hours)
• Rules of Evidence / Chain of Custody (3 hours)
• Research paper presentations (3 hours)
• Exams (3 hours)

Course Requirements
• Homework assignments (10%)
• Term projects (20%)
• Research paper (10%)
• Midterm exam 1 (15%)
• Midterm exam 2 (20%)
• Final exam (25%)

Syllabus prepared: Spring 2016