Course number and name: ET 339 Computer Forensics

Credits and contact hours: 3 credits, two 50 minute lectures and a 1 hour 40 min. lab

Instructor's or course coordinator's name: Matt Presser

Text book, title, author and year *Guide to Computer Forensics and Investigations 4th Ed*
EBook Incident Response: Computer Forensics Toolkit

other supplemental materials - none

Specific course information

a. **brief description of the content of the course (Catalog Description)** Legal, regulatory, and technical aspects of computer forensics. Topics include current law; privacy legislation; chain of evidence; creating a computer incident response team; and the extraction, preservation, analysis, and presentation of computer-related evidence.
b. **prerequisites or co-requisites E T 182 and (E T 262 or E T 245).**
c. **indicate whether a required, elective, or selected elective (as per Table 5-1) course in the program** This course is required for all IET majors.

Specific goals for the course

a. specific outcomes of instruction, ex. The student will be able to explain the significance of current research about a particular topic.
This course will focus on a subset of skills required to perform forensic analysis on computer systems, with emphasis on the Windows Operating System.

b. explicitly indicate which of the student outcomes listed in Criterion 3 or any other outcomes are addressed by the course.

3. The design techniques, analysis and the building, testing, operation and maintenance of networks, databases, security and computer systems (both hardware and software).
Also ABET 3.b, 3.c, 3.d, 3.f

Brief list of topics to be covered

Basic System Administration and Foundation Concepts

- Computer Hardware
- File Systems
- Windows Operating Systems
- The Windows Registry
- Users and Permissions
- Logs
- Virtual Machines
- Linux/Helix Intro

Forensic Concepts

- Laws and Policies, Criminal vs. Civil
- Chain of Custody
- Established Guidelines
- Incident Identification
- Reporting

Incident Response and Data Acquisition

- Live Analysis of a System
- Encryption
- Live Acquisitions and RAM images
- Static Acquisitions

Windows Forensic Examination

- System Identification and Profiling
- Keyword Searches
- Timeline Analysis
- Recovering Deleted Files
- Internet History
- Email
- Recycle Bin
- Prefetch
- Checking for Viruses/Malware

Network Forensics

- Server Logs
- Packet Sniffing
- NetFlow
- IDS and HIDS

Malware Analysis

- Sandbox Environments, LiveView, VMWare
- Anti-Virus/Anti-Malware
- Online Analysis Tools
- Reverse Engineering Binaries
- Packet Sniffing

Prepared by: Matt Presser June 2, 2011