Computer Forensics II
IS 236

COURSE LEARNING OUTCOMES

1. Analysis/Problem Solving:
   a. Students evaluate an incident / crime scene as being a possible case.
   b. Students analyze a large amount of digital evidence and identify the most significant data.
   c. Students develop and maintain a precise documentation.

2. Communications
   a. Students discuss the use of different computer forensic tools.
   b. Students formulate a complete and adequate process plan and measure against it.
   c. Students present their conclusion to the rest of the class.

3 Responsibility:
Students are responsible for own work and the securing and handling of digital evidence.

Course Outline

I. Course Introduction
   - a. Overview of class, syllabus, assignments…
   - b. Explanation of textbook, workbook…

II. Forensic Intro Review

III. Computer Forensics Tools – In depth
   - a. DigitalIntelingence
   - b. Access Data FTK
   - c. Data-Sniffer
   - d. EnCase
   - e. Norton Commander v. 5.5
   - f. Norton System Works 2001

IV. Expert Witness – CV
   - a. How to become an expert witness
   - b. Example of expert witness CV

V. Case study: Hard drive
   - a. Intro
   - b. Secure, copy hard drive
   - c. Evidence recovery
   - d. Documentation
   - e. Analysis
   - f. Findings – Affidavit

VI. Other Operating Systems
   - a. Mac
   - b. Unix

VII. Computer Forensics Future