DESCRIPTION: This course discusses identification, extraction, documentation, interpretation, and preservation of computer media for evidentiary purposes and/or root cause analysis as well as methodologies, tools, and technologies for vulnerability assessment. Topics include techniques for discovering digital evidence; responding to electronic incidents; tracking communications through networks; understanding electronic media, crypto-literacy, data hiding, hostile code, and system forensics; discovering new exploits and vulnerabilities; penetrating network perimeters; and the role of forensics and vulnerability assessment in the digital environment.

TOPICS (including Guest Lectures):

1. Computing Basics
   a. File Systems
   b. Operating Systems
   c. Network
2. Computer Forensics Principles
   a. Acquisition/Preparation
   b. Authentication/Identification
   c. Analysis/Examination
   d. Documentation/Presentation
   e. Rules of Evidence
3. Computer Forensics Technologies
   a. Data Forensics
   b. Systems Forensics
   c. Network Forensics
4. Computer Forensics Tools
   a. Commercial Tools
   b. Open Source Tools
5. Incident Responses
   a. Ethical Hacking Techniques
   b. Vulnerability Assessment
   c. Penetration Testing
6. Cybercrime Investigation
   a. Crimes and Violations
   b. Cybercrime Trends
7. Other Issues
   a. Ethics and Legal Issues
   b. Standards
   c. Reporting Requirements

READINGS:


**GRADING POLICY:**
Grades are based on two exams 40% (20% each), class assignments & paper report/presentation 40%, and class project 20%. Graduate students are required to work on additional task (paper presentation). Each assignment and class project should be submitted by the submission deadline or earlier and students must submit their assignments and report via Dropbox at Blackboard.

*Undergraduate Students:* Each student is required to submit a report for a research paper. The report MUST include a brief summary of the paper and critiques and possible enhancements with some research reasoning (at least 4 pages, 12 point, single space) before the submission due or earlier.

*Graduate Students:* Each student is required to present a research paper to the whole class. Class presentation MUST include the concepts of the proposed ideas and approaches in the paper clearly including critiques and possible enhancements with some research reasoning. It will be approximately 30 minutes presentation and the presentation materials should be submitted before the presentation date or earlier. A list of research papers will be available at Blackboard and the research paper should be chosen in mutual agreement.

Students must take initiative to make sure this happens in timely manner. Also, the class attendance will be reflected in the evaluation.

**IMPORTANT DATES:**
First Day of Class: Jan 9, 2012
Exam #1 (Midterm): Feb 27, 2012
Spring Break: Mar 19, 2012 (no class)
Class Project Due: April 23, 2012
Class Presentation: April 16 & 23, 2012
Exam #2 (Final): April 30, 2012

**INFORMATION ASSURANCE LABORATORY:**
The hands-on lab facility will be also available in an isolated teaching lab that is located in BYENG 387. AccessData’s Forensic Toolkit (FTK), Hard Disk Enclosures, and Knoppix VM image are available in the lab.

**ACADEMIC INTEGRITY:**
All students should honor the University Student Academic Integrity Policy and The Student Code of Conduct. Failure to meet these standards may result in suspension or expulsion. Please take some time to read the policy at [http://www.asu.edu/studentlife/judicial](http://www.asu.edu/studentlife/judicial).