

## **CIS 4000 – Introduction to Computer Forensics**

**Prerequisites:** CIS 2010 and CSP 1, 6, 7.

### **Required Materials:**

Nelson, B., Phillips, A., Enfinger, F., & Steuart, C. (2007). *Guide to Computer Forensics and Investigations* (Third ed.). Boston: Thomson Course Technology.

### **Optional Readings:**

Solomon, M. G., Barrett, D., & Broom, N. (2005). *Computer Forensics Jump Start*. San Francisco: Sybex.

Volonino, L., Anzaldua, R., & Godwin, J. (2007). *Computer Forensics: Principles and Practices*. Upper Saddle River, New Jersey: Pearson Education

### **Course Description**

This course introduces students to the collection, preservation, presentation and preparation of computer-based evidence for the purposes of criminal law enforcement or civil litigation. These activities define the central roles of computer forensic practitioners involved in investigating computer crime scenes and torts involving computers. Students will be prepared to assist in the formulation and implementation of organizational computer forensics preparedness policies, to determine the necessity for forensic procedures, extend governance processes to allow for proper future forensic investigations, and to be contributing members of computer forensics investigation teams.

### **Course Objectives**

Upon successful completion of this course, students will develop abilities to

- Determine whether organizational processes for the collection, preservation, presentation and preparation of computer-based evidence are appropriate for satisfying the requirements of criminal law enforcement and civil litigation.
- Assist in the formulation and implementation of organizational computer forensics preparedness policies.
- Determine the necessity for forensic preparedness procedures and recognize the appropriate moments for instigating an investigation and involving law enforcement.
- Extend organizational due diligence and governance processes to allow for proper future forensic investigations.
- Contribute as a member of a computer forensics investigation team.

- Recognize typical forms of computer crime and abuse and the relevant evidence.
- Assist in determining where and how evidence may be stored in computers, and how this evidence may be extracted without contamination.
- Participate in the selection of appropriate tools for forensic investigation
- Prepare forensic evidence for delivery in adversarial settings.

**Class Policies:**

Assignments & Grading

Labs and Cases :	20%
Forensics Project:	20%
Exams:	40%
Class Participation:	20%
Total:	100

**Special Considerations**

The course web site will be use as a repository for examples of course paper problems, model solutions, examples of projects, and further required course material that arises during the class. Students must arrange for their own access to the World Wide Web (Internet access is available free in the GSU labs). All student work submitted in fulfillment of course requirements is deemed to be granted in the public domain (copyright-free) for the purposes of use as instructional material or examples of student work in future courses. The course syllabus provides a general plan for the course. Deviations may be necessary.

**Lab Preparation**

Students will prepare regular hands-on lab assignments as detailed in the course schedule.

**Forensics Course Project**

Students will complete an assigned Forensics Course Project at the end of the course. While the nature of this project may vary according to availability, an example is the forensic analysis of a computer fixed-disk drive. Students will analyze the drive and compose a forensic analysis report detailing evidence of note. Students will prepare and deliver their report during class in a simulated adversarial setting.

**Deliverable: One forensic analysis report paper in electronic form and a PowerPoint presentation to be used when you deliver your report in session.**

### **Tentative Schedule of Classes**

(Subject to Change)

Week	Topic	Readings	Assignment
1	Computer Forensics and Investigation Processes	Nelson 1	
2	Understanding Computing Investigations	Nelson 2 & 16	Project 2-4
3	Computer Basics	Nelson 6 & 8	Project 6-3
4	Internet Basics Regular Expressions	Nelson 6 & 8	Project 6-4
5	Data Acquisitions	Nelson 4	Project 4-1
6	Processing Crime and Incident Scenes	Nelson 5	Project 5-4
7	Current Computer Forensics Tools Exam Number 1	Nelson 7	Project 7-5
8	Computer Forensics Analysis	Nelson 3 & 9	Project 9-1
9	Recovering Image Files	Nelson 10	Project 10-3
10	Network Forensics	Nelson 11	Project 11-4
11	Email Investigations	Nelson 12	Project 13-6
12	PDA's, Cell Phones, Thumb drives, U3 drives	Nelson 13	TBA
13	High Tech Investigations Report Writing	Nelson 14	TBA
14	Expert Testimony in High Tech Investigations	Nelson 15	TBA
15	Student Presentations		