

## COURSE DESCRIPTION

**Department and Course Number:** CSc 253

**Course Coordinator:** Isaac Ghansah

**Course Title:** Computer Forensics

**Total Credits:** 3

**Proposed Catalog Description:** Structured security incident investigations internal and external; emphasis on analysis of electronic evidence and proper audit; utilization of scientific aids in obtaining information from computing devices; legal electronic evidence. Prerequisite: Fully classified graduate standing in Computer Science, Software Engineering, or Computer Engineering.

### Textbooks

- John Vacca, “Computer Forensics: Computer Crime Scene Investigation”, Charles River Media, 2002
- Warren G. Kruse II & Jay G. Heiser, “Computer Forensics: Incident Response Essentials”, Addison Wesley, 2002
- R. Clifford, Cyber Crime: The Investigation, Prosecution and Defense of a Computer-Related Crime. Carolina Academic Press, 2001

### References

- Kevin Mandia & Chris Prorise “Incident Response: Investigating Computer Crime”, , Second Edition, Osborne McGraw-Hill, 2003
- H. Carvey, Windows Forensics and Incident Recovery, Addison Wesley, 2005
- C. Davis, A. Philipp, and D. Cowen, Hacking Exposed: Computer Forensics Secrets and Solutions, 2005 McGraw Hill
- Albert Marcella & Robert Greefield, “Cyber Forensics”, Auerbach, 2002
- Charles P. Pfleeger, “Security in Computing”, Third Edition, Prentice Hall, 2003

### Course Goals

The goals of this course are to enhance understanding of the concepts of computer system security models, and the detection and prevention of intrusion and attacks; to gain experience in structured digital evidence collection and evaluation, and to understand the legal application issues involved in computer forensic analysis; to expose the student to the conceptual models and the hands-on experience of using open source tools designed for computer forensics.

### Prerequisites by Topic

*Thorough understanding of:*

- Security auditing.
- How to trace domain names and IP addresses.
- Encryption methods

*Basic understanding of:*

- Hard drives and other storage media
- Hostile code

- Unix operating system
- Windows operating system

*Exposure to:*

- Computer crime investigation, legal evidence and ethics.

### **Major Topics Covered in the Course**

- Introduction to Forensics, Overview of Computer Security Law Enforcement and Cyber Security (3 hours)
- Computer Security Policies and Guidelines (3 hours)
- Cyberspace, Cyber Law, and Cyber Crime (3 hours)
- Intrusion Detection and Incident Response. (6 hours)
- Forensic Duplication and Analysis. (3 hours)
- Network Protocols. (3 hours)
- Network Surveillance. (3 hours)
- Advanced Network Surveillance. (3 hours)
- Toolkit to collect forensic information from a Windows environment. (3 hours)
- Toolkit to collect forensic information from Unix/Linux environments. (3 hours)
- Case studies in Windows and Unix environments. (6 hours)
- Investigating Router attacks. (3 hours)
- Investigating Web attacks. (3 hours)

### **Expected Outcomes**

*Thorough understanding of:*

- Structured security incident investigation.
- Preparation of electronic evidence.

*Basic understanding of:*

- Preservation of computer evidence and chain of custody.
- Commercial and open source forensic tool kits.
- Three A's of computer forensics: Acquire, Authenticate and Analyze.

*Exposure to:*

- How data is concealed and how to find such data.
- Presentation of electronic evidence in court.
- Expert witness testimony.

### **Laboratory Projects**

1. Examine logs of: httpd, logon, failed logon, SMTP, system and tcpd.
2. Find hidden data in a binary file (image, audio or video)
3. Duplicate hard drive contents on disk, tape or CD
4. Analyze hard drive for erased and encrypted files
5. Use open source forensic tool kit

## Estimated CSAB Category Content

	CORE	ADVANCED		CORE	ADVANCED
Data Structures	_____	_____ .7 _____	Computer Org & Architecture	_____	_____
Algorithms	_____	_____			
Software Design	_____	_____ 1.0 _____	Concepts of Programming Languages	_____	_____

### Oral and Written Communications

Students will be required to research actual cases where computer forensics was used and give oral presentations and/or written reports.

### Social and Ethical Issues

Class discussions on the information warfare arsenal and tactics of terrorists, criminals and foreign governments such as the “Code Red” worm, possible tactics of private companies to gain access to competitors systems to gain a technological advantage.

### Theoretical Content

Electronic evidence may be encrypted. Therefore different algorithms must be used in the effort to discover the encryption algorithms and keys used by the perpetrators. In the investigation of intrusion the student may also be required to trace back and try to determine the source of the intrusion and reconstruct past events.

### Problem Analysis

Each security incident must be analyzed in a methodical manner and the collection, preserving, and effectively using evidence by addressing the three A’s of computer forensics: Acquire the evidence without altering or damaging the original data. Authenticate that your recorded evidence is the same as the original seized data. Analyze the data without modifying the recovered data.

### Solution Design

Students will learn how to develop a Computer Security Incident Investigation form that can be used to document the analysis of security incidents.

*Course Description for CSC 253  
(Formerly CSC 296P 9/30/05)*