

## COURSE DESCRIPTION

Dept., Number	<b>CSC 116</b>	Course Title	<b>Cyber Forensics</b>
Semester hours	<b>3</b>	Course Coordinator	<b>Isaac Ghansah</b>
		URL (if any):	<b><a href="http://gaia.ecs.csus.edu/~ghansahi/">http://gaia.ecs.csus.edu/~ghansahi/</a></b>

### Catalog Description

Fundamentals of computer forensics and cyber-crime scene analysis including laws, regulations, and international standards; formal methodology for conducting security incident investigations; categories of electronic evidence. The course includes projects involving digital forensic tools. Prerequisite: At least a C- grade in CSC 114.

### Textbook

Warren G. Kruse and Jay G. Heiser, Computer Forensics: Incident Response Essentials, Addison-Wesley, 2002.

Bill Nelson et al, Guide to Computer Forensics and Investigations, 2<sup>nd</sup> Edition, Course Technology, 2006.

### References

Albert Marcella and Robert Greenfield, Cyber Forensics, Auerbach, 2002.

Chris Davis, Aaron Philipp, and David Cowen, Hacking Exposed: Computer Forensics Secrets and Solutions, McGraw Hill, 2005.

Charles P. Pfleeger, Security in Computing, 3rd Ed., Prentice Hall, 2003.

Chris Smith and Rebecca Gurley Bace, A Guide to Forensic Testimony: The Art and Practice of Presenting Testimony As An Expert Technical Witness, Addison-Wesley, 2003.

Harlan Carvey, Windows Forensics and Incident Recovery, Addison-Wesley, 2005.

Kevin Mandia and Chris Prosise, Incident Response: Investigating Computer Crime, 2nd Ed., Osborne-McGraw Hill, 2003.

Ralph D. Clifford, Cyber Crime: The Investigation, Prosecution and Defense of a Computer-Related Crime, Carolina Academic Press, 2001.

### Course Goals

1. Enhance understanding of the concepts of computer system security models.
2. Study detection and prevention of intrusion and attacks.
3. Gain experience in structured digital evidence collection and evaluation.
4. Understand the legal issues involved in computer forensic analysis.
5. Use commercial and open-source computer forensics tools.

## **Prerequisites by Topic**

### *Thorough understanding of:*

- Information Assurance and Security best practices.
- Threats, risks, and vulnerabilities to information systems; countermeasures available to address these threats.
- Web design and tools.

### *Basic understanding of:*

- Internet security.
- Host security.
- Tools for information security.
- Web client and server software.

### *Exposure to:*

- TCP/IP protocol suite.
- Career paths in information security.
- Ethical issues related to information security.
- Web programming (e.g., Javascript, XML, etc).
- Web protocols (e.g., HTTP, TCP/IP).

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

1. Introduction to forensics, overview of computer security law enforcement and cyber security (3 hours).
2. Computer security policies and guidelines (3 hours).
3. Cyber law and cyber crime (3 hours).
4. Storage device structure and organization (1 hour).
5. Intrusion detection investigation and incident response (5 hours).
6. Detection of covert channels and concealed data (2 hours).
7. Forensic duplication and analysis (3 hours).
8. Auditing and evidence handling (3 hours).
9. Network surveillance (3 hours).
10. Email forensics (3 hours).
11. Toolkits to collect forensic information from Windows/Linux/Unix environments (5 hours).
12. Case studies in Windows/Linux/Unix environments (5 hours).
13. Investigating Router attacks (3 hours).
14. Investigating Web attacks (3 hours).

## 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 forensics toolkits.
- Cyber law and policy.
- Six A's of computer forensics: Assess, Acquire, Authenticate, Analyze, Articulate, and Archive.

### *Exposure to:*

- How data are 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 weeks).
2. Find hidden data in a binary file (image, audio or video) (1 week).
3. Duplicate storage media contents on disk, tape, CD, etc. (2 weeks).
4. Analyze storage media for evidence including erased and/or encrypted files (3 weeks).
5. Use commercial and open source forensics tools (3 weeks).

## Estimated Curriculum Category Content (Semester hours)

<i>Area</i>	<i>Core</i>	<i>Advanced</i>	<i>Area</i>	<i>Core</i>	<i>Advanced</i>
Algorithms			Data Structures		
Software Design			Prog. Languages		
Comp. Arch.					

## 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**

No significant component.

### **Problem Analysis**

Each security incident will be analyzed in a methodical manner with the collection, preservation, and effective use of evidence ensured by addressing the three A's of computer forensics: (a) Acquire the evidence without altering or damaging the original data; (b) Authenticate that the recorded evidence is the same as the original seized data; and (c) Analyze the data without modifying the recovered data.

### **Solution Design**

Students will learn how to compose a computer security incident investigation report that can be used to document the analysis of security incidents.

*/aa*