



SACRAMENTO STATE

# Course Change Proposal Form A



<b>Academic Group (College):</b> Engineering and Computer Science	<b>Academic Organization (Department):</b> Computer Science	<b>Date:</b> December 20, 2007
<b>Type of Course Proposal:</b> New <input checked="" type="checkbox"/> Change <input type="checkbox"/> Deletion <input type="checkbox"/>	<b>Department Chair:</b> Du Zhang	<b>Submitted by:</b> Du Zhang
<b>Does this course fulfill a requirement for single-subject or multiple subject credential students?</b> Yes <input type="checkbox"/> No <input checked="" type="checkbox"/>	<b>For Catalog Copy:</b> Yes <input checked="" type="checkbox"/> No <input type="checkbox"/> <b>CCE (Extension):</b> Yes <input type="checkbox"/> No <input checked="" type="checkbox"/>	<b>Semester Effective:</b> Fall <input checked="" type="checkbox"/> Spring <input type="checkbox"/> , 2008

<b>This course replaces experimental course Subject Area (prefix) and Catalog Nbr (course number):</b>	
--	--

### Change from:

<b>Subject Area (prefix) &amp; Catalog Nbr (course no.):</b>	<b>Title:</b>	<b>Units:</b>
--	---------------	---------------

### Change to:

<b>Subject Area (prefix) &amp; Catalog Nbr (course no.):</b> CSC 153	<b>Title:</b> Computer Forensics Principles and Practices	<b>Units:</b> 3
---	---	-----------------

### JUSTIFICATION:

<b>This new course is integral to the creation of the Undergraduate Certificate Program in Information Assurance and Security (Form B in process) and will help Sac State to renew its designation by the NSA/DHS as a Center of Academic Excellence in Information Assurance Education.</b>
--

**NEW COURSE DESCRIPTION:** (Not to exceed 80 words, and language should conform to catalog copy. See <http://www.csus.edu/acaf/univmanual/crspsl.htm> - Guidelines for Catalog Course Description)

Fundamentals of computer forensics, cyber-crime scene analysis and electronic discovery. Technical and formal methodology for conducting security incident investigations; file systems and storage analysis, data hiding techniques, network forensics; projects involving using, understanding, and designing digital forensic tools; anti-forensics; legal issues and standards.	
<b>Note:</b>	
<b>Prerequisite:</b> CSC 138 <b>Enforced at Registration:</b> Yes <input checked="" type="checkbox"/> No <input type="checkbox"/>	
<b>Corequisite:</b> <b>Enforced at Registration:</b> Yes <input type="checkbox"/> No <input type="checkbox"/>	
<b>CAN (California Articulation Number):</b>	
<b>Graded:</b> Letter <input checked="" type="checkbox"/> Credit/No Credit <input type="checkbox"/>	<b>Instructor Approval Required?</b> Yes <input type="checkbox"/> No <input checked="" type="checkbox"/>
<b>Course Classification</b> (e.g., lecture, lab, seminar, discussion): C 04	<b>Title for CMS</b> (not more than 30 characters) COMP FORENSICS PRINC & PRACT
<b>Cross Listed?</b> Yes <input type="checkbox"/> No <input checked="" type="checkbox"/>	<b>If yes, do they meet together and fulfill the same requirement, and what is the other course.</b>
<b>How Many Times Can This Course be Taken for Credit?</b> <u>Once</u>	
<b>Can the course be taken for Credit more than once during the same term?</b> Yes <input type="checkbox"/> No <input checked="" type="checkbox"/>	

**FOR NEW COURSE PROPOSALS OR SUBSTANTIVE CHANGES ONLY:**

**Description of the Expected Learning Outcomes:** Describe outcomes using the following format: "Students will be able to: 1), 2), etc."  
See the example at <http://www.csus.edu/acaf/example.htm>

Students will have a...

*Thorough understanding of:*

- Technical and formal methods of security incident investigation.
- Preparation of electronic evidence.

*Basic understanding of:*

- Preservation of computer evidence and chain of custody.
- Commercial and open source forensics tool kits including design issues.
- Cyber law and policy.
- Six A's of computer forensics process: 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.

\*\*Attach a list of the required/recommended course readings and activities [Note: it is understood that these are updated and modified as needed by the instructor(s).] This attachment should be forwarded only to your Dean's office, not Academic Affairs.

**Assessment Strategies:** A description of the assessment strategies (e.g., portfolios, examinations, performances, pre-and post-tests, conferences with students, student papers) which will be used by the instructor to determine the extent to which students have achieved the learning outcomes noted above:

**Laboratory projects, written reports, and examinations.**

For whom is this course being developed?

Majors in the Dept  Majors of other Depts  Minors in the Dept  General Education  Other

Is this course required in a degree program (major, minor, graduate degree, certificate)? Yes  No

If yes, identify program(s): **Proposed Undergraduate Certificate Program in Information Assurance and Security.**

Does the proposed change or addition cause a significant increase in the use of College or University resources (lab room, computer facilities, faculty, etc.)? Yes  No

If yes, attach a description of resources needed and verify that resources are available.

Indicate which department or programs will be affected by the proposed course (if any). Criminal Justice (possibly)

*The Department Chair's signature below indicates that affected programs have been sent a copy of this proposal form.*

**Approvals:** If proposed change, new course or deletion is approved, sign and date below. If not approved, forward without signing to the next reviewing authority, and attach an explanatory memorandum to the original copy.

**Signatures:**

	Date
Department Chair:	12/21/2007
College Dean or Associate Dean:	12/22/08
CPSP (for school personnel courses ONLY)	
Associate Vice President and Dean for Academic Programs	

Distribution: Academic Affairs (original), Department Chair and College Dean. Dean's office to send original after approval to Academic Affairs, at mail zip 6016. An electronic copy must also be sent.

## COURSE DESCRIPTION

Dept., Number	<b>CSC 153</b>	Course Title	<b>Computer Forensics Principles and Practices</b>
Semester hours	<b>3</b>	Course Coordinator	<b>Isaac Ghansah</b>

### Catalog Description

Fundamentals of computer forensics, cyber-crime scene analysis and electronic discovery. Technical and formal methodology for conducting security incident investigations; file systems and storage analysis, data hiding techniques, network forensics; projects involving using, understanding, and designing digital forensic tools; anti-forensics; legal issues and standards. Prerequisite: CSc 138.

### Textbook

B. Nelson et al., Guide to Computer Forensics and Investigations, Second Edition, Course Technology, 2006.

K. Jones, R. Bejtlich, and C. Rose, Real Digital Forensics, Addison Wesley, 2006.

### References

Brian Carrier, File System Forensic Analysis, Addison-Wesley, 2005.

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

Kevin Mandia, Chris Prosise and Matt Pepe, Incident Response and Computer Forensics, 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, McGraw Hill, 2005.

Albert Marcella & Robert Greefield, Cyber Forensics, Auerbach, 2002.

C. Smith & R. Bace, A Guide to Forensic Testimony: The Art and Practice of Presenting Testimony As An Expert Technical Witness, Addison Wesley, 2003.

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

### Course Goals

1. Understand how to deal with categories of electronic evidence including media, email, and networks.
2. Study detection and prevention of intrusion and attacks.
3. Gain experience in structured digital evidence collection and evaluation.

4. Use and understand commercial and open-source computer forensics tools.
5. Understand the legal issues involved in computer forensic analysis.

### **Prerequisites by Topic**

#### *Thorough understanding of:*

- Distributed computing with client/server programming.

#### *Basic understanding of:*

- TCP/IP suite of protocols and internet technologies.
- UNIX and Windows operating system common services, ports, and sockets.
- How to compile and run programs in Linux and Windows.

#### *Exposure to:*

- File systems.
- Security of computer systems and networks (Firewall, IDS).

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

1. Introduction to forensics: History, categories of forensics, forensic process, cyber laws, and security incidents (3 hours).
2. Overview of hardware, storage organization, operating systems (3 hours).
3. Disk geometry, partitions, boot process, Linux and Windows file systems (3 hours).
4. File signatures, data hiding: deleted file recovery, cryptography, steganography, etc. (3 hours).
5. Local and remote forensic acquisition (3 hours).
6. Hashes, digital certificates, and digital notary and their use in authentication, chain of custody, and evidence handling (3 hours).
7. Use of string searches, pattern matching, regular expressions in computer forensics (3 hours).
8. Network forensics, trapping with honeypots, and log analysis of servers (3 hours).
9. Email forensics: Email protocols, event reconstruction. (3 hours).
10. Web forensics: HTTP protocol analysis, log analysis of web servers. (3 hours).
11. Intrusion investigation and incident response. (3 hours).
12. Forensic toolkits to collect forensic information from a Windows/Linux/Unix environment (3 hours).
13. Forensic investigation involving Windows/Linux/Unix environments including data hiding methods involving cryptography and steganography (6 hours).
14. Recent trends in computer forensics, anti-forensics, reporting (3 hours).

## Outcomes

### *Thorough understanding of:*

- Technical and formal methods of security incident investigation.
- Preparation of electronic evidence.

### *Basic understanding of:*

- Preservation of computer evidence and chain of custody.
- Commercial and open source forensics tool kits including design issues.
- Cyber law and policy.
- Six A's of computer forensics process: 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. Acquisition and authentication of 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).
6. Search and seizure (1 week).
7. Create forensic evidence kit for analysis (1 week).

## 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		0.3	Data Structures		0.4
Software Design		0.2	Prog. Languages		
Comp. Arch.					

## Oral and Written Communications

Every student is required to submit at least one written report (not including exams, tests, quizzes, or commented programs) of typically twenty pages and to make one oral presentation of typically thirty-minute duration.

## **Social and Ethical Issues**

Class discussions on the information warfare arsenal and tactics of terrorists, criminals and foreign governments; tactics of private companies to gain access to competitors' systems to gain a technological advantage. Ethical issues. All the topics are case based. Students typically write a report summarizing what they learned from the discussion. Approximately 2 hours total.

## **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. 4 hours total.

## **Problem Analysis**

Each security incident must be analyzed in a methodical manner by the collection, preservation, and effective use of evidence 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 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.

Status: Approved by Curriculum Committee: 11/19/2007  
Approved by Department: 12/12/2007