



ECS

# Academic Affairs - Course Proposal



Form A

CALIFORNIA STATE UNIVERSITY, SACRAMENTO

Academic Unit: Computer Science		Department Chair: Du Zhang	
Type of Course Proposal: New <input checked="" type="checkbox"/> Change <input type="checkbox"/> Deletion <input type="checkbox"/>		Date: March 9, 2006	
Does this course fulfill a requirement for single-subject or multiple subject credential students? Yes <input type="checkbox"/> No <input checked="" type="checkbox"/>		For Catalog Copy: Yes <input checked="" type="checkbox"/> No <input type="checkbox"/>	CCE: Yes <input type="checkbox"/> No <input checked="" type="checkbox"/>
		Semester Effective: Fall <input checked="" type="checkbox"/> Spring <input type="checkbox"/> 2006	
Prefix & No. CSC 116	Title: Cyber Forensics	Units: 3	

Change to:

Prefix & No.	Title:	Units:
--------------	--------	--------

### JUSTIFICATION:

This course is part of the proposed Minor in Information Security and Computer Forensics, which is intended for students in Criminal Justice and related fields. Information Assurance and Security is an area of emerging significance; the proposed minor is intended to educate future professionals in computer and telecommunications crime investigation and evidence processing. Additionally, Computer Science hopes to reverse its present negative trend in enrollment by taking this interdisciplinary approach.

### NEW COURSE DESCRIPTION: (Not to exceed 80 words, and language should conform to catalog copy.)

See <http://www.csus.edu/acad/univmanual/crspsl.htm> - Guidelines for Catalog Course 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. Projects involving digital forensic tools.

Note:	
Prerequisite: CSC 114	
Corequisite:	
CAN (California Articulation Number):	
Graded: Letter <input checked="" type="checkbox"/> Credit/No Credit <input type="checkbox"/>	Instructor Approval? Yes <input type="checkbox"/> No <input checked="" type="checkbox"/>
Course Classification: 04	Title for SIS+ (not more than 25 characters) CYBER FORENSICS
Cross Listed? Yes <input type="checkbox"/> No <input checked="" type="checkbox"/>	If yes, with what course:
How Many Times Can This Course be Taken for Credit? Once	

ECS

# 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 gain:

*A thorough understanding of:*

- Structured security incident investigation
- Preparation of electronic evidence

*A 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

\*\*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:

Examinations, lab projects, oral presentations and/or written reports

## 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): **Minor in Information Security and Computer Forensics**

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

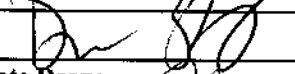
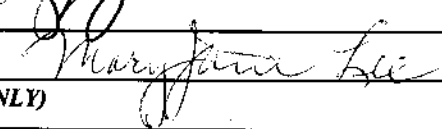
If yes, attach a description of resources needed and verify that resources are available.

Indicate which department or programs will be affected by the proposed course (if any). \_\_\_\_\_

*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: 	3/9/2006
College Dean or Associate Dean: 	04-06-06
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 Jerri McAtee, at zip 6016. An electronic copy must also be sent to [mcateejj@csus.edu](mailto:mcateejj@csus.edu).

## **New Course Proposal**

### **CSC 116 – Cyber Forensics**

By Isaac Ghansah and Dick Smith

This document contains a proposal for a new course in a Minor in Information Security and Computer Forensics. The proposed course covers topics in the field of digital evidence collection and evaluation, as well as legal issues involved in computer systems forensics. Also included are issues in computer crime investigation and electronic evidence discovery.

## COURSE DESCRIPTION

**Department and Course Number:** CSC 116      **Course Coordinator:** Isaac Ghansah

**Course Title:** Cyber Forensics

**Total Credits:** 3

**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: CSC 114

### Textbooks

- B. Nelson et al, *Guide to Computer Forensics and Investigations*, 2nd Ed., Course Technology, 2006
- Warren G. Kruse II and Jay G. Heiser, *Computer Forensics: Incident Response Essentials*, Addison Wesley, 2002

### References

- R. Clifford, *Cyber Crime: The Investigation, Prosecution and Defense of a Computer-Related Crime*, Carolina Academic Press, 2001
- Kevin Mandia and Chris Prosise, *Incident Response: Investigating Computer Crime*, 2nd Ed., 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 and Robert Greenfield, *Cyber Forensics*, Auerbach, 2002
- C. Smith and R. Bace, *A Guide to Forensic Testimony: The Art and Practice of Presenting Testimony As An Expert Technical Witness*, Addison Wesley, 2003
- Charles P. Pfleeger, *Security in Computing*, 3rd Ed., Prentice Hall, 2003

### 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:*

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

*Basic understanding of:*

1. Internet security
2. Host security
3. Tools for information security
4. Web client and server software

*Exposure to:*

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

**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)
- Cyber law and cyber crime (3 hours)
- Storage device structure and organization (1 hour)
- Intrusion detection investigation and incident response (5 hours)
- Detection of covert channels and concealed data (2 hours)
- Forensic duplication and analysis (3 hours)
- Auditing and evidence handling (3 hours)
- Network surveillance (3 hours)
- Email forensics (3 hours)
- Toolkits to collect forensic information from Windows/Linux/Unix environments (5 hours)
- Case studies in Windows/Linux/Unix environments (5 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 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 CSAB Category Content

	CORE	ADVANCED		CORE	ADVANCED
Data Structures	_____	_____	Computer Org & Architecture	_____	_____
Algorithms	_____	_____			
Software Design	_____	_____	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

#### 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.

2/24/06