Las Positas CurricUNET
LAS POSITAS COLLEGE

Las Positas College
3000 Campus Hill Drive
Livermore, CA 94551-7650
(925) 424-1000
(925) 443-0742 (Fax)

Course Outline for CNT 70

COMPUTER FORENSICS II

Effective: Fall 2006

I. CATALOG DESCRIPTION:
CNT 70 — COMPUTER FORENSICS II — 3.00 units

A practical course in the detection, and investigation of incidents involving computers and digital information. Case oriented, following the objectives for the CFE Computer Forensics Examiner certification exam, the class includes understanding and practice in basic computer forensics, methods of investigation, analysis of hard drives, storage mediums, network logs, and investigation reporting utilizing court-approved forensic software and tools.

2.50 Units Lecture 0.50 Units Lab

Strongly Recommended
CIS 50 - Intro to Computing Info Tech
or

-

Grading Methods:
Letter or P/NP

Discipline:

	MIN
Lecture Hours:	45.00
Lab Hours:	27.00
Total Hours:	72.00

II. NUMBER OF TIMES COURSE MAY BE TAKEN FOR CREDIT: 2

III. PREREQUISITE AND/OR ADVISORY SKILLS:

Before entering this course, it is strongly recommended that the student should be able to:

A. CIS50

IV. MEASURABLE OBJECTIVES:

Upon completion of this course, the student should be able to:

A. demonstrate an understanding of basic computer forensic concepts;
B. utilize proper investigative procedures relative to individual, corporate, and criminal rights, responsibilities and law;
C. formulate and execute an investigative plan;
D. perform basic methods and techniques of forensic investigation;
E. use forensic software to secure and analyze various digital media at a basic level;
F. evaluate and effectively implement various forensic utilities and software;
G. access, document and evaluate hidden data;
H. demonstrate the ability to use basic investigative techniques for various operating systems;
I. create and present simple reports and analysis of forensic investigation results;
J. perform the basic skills required by the objectives of the CFE Computer Forensic Examiner certification test.

V. CONTENT:
A. Digital investigation / forensics careers
   1. Computer forensics
   2. History of digital investigation
   3. Forensic training and resources
   4. Code of conduct
B. The lab and forensic tools
   1. Lab certification and standards
   2. Forensic software
   3. Evidence handling and storage
   4. Practical exercises
C. Operating systems and data storage basics
   1. Windows/Macintosh/OSX

        2. Unix / Linux
        3. Hard drive storage concepts
        4. Practical exercises
    D. Laws, regulations and standards
        1. SB 1386
        2. Federal
        3. State and local
        4. Policy and procedures
    E. Network fundamentals
        1. OSI model for forensics
        2. TCP/IP for forensics
        3. Network devices and concepts
        4. Practical exercises
    F. Evidence handling / investigative procedures
        1. Methods, tools and procedures
        2. Measurement and documentation
        3. Practical exercises
    G. Data acquisition & forensic analysis
        1. Evidence seizure / chain of custody
        2. Imaging, Backup and storage
        3. Analyzing files
        4. Procedures and documentation
        5. Practical exercises
    H. Email investigations
        1. Crimes and violations
        2. Messages and logs
        3. Procedure and documentation
        4. Methods, tools, and skills
        5. Practical exercises
    I. Images, files and Steganography
        1. Image file formats
        2. Encryption, Steganography
        3. File, password recovery
        4. Data hiding techniques
        5. Methods, tools and skills
        6. Practical exercises
    J. Forensics and security management
        1. computer and investigative policy
        2. Whitehat hacking
        3. Best Practices
        4. Practical exercises
    K. Reports and documentation
        1. Legal versus technical reports
        2. analysis and conclusions
        3. Layout and presentation
        4. Practical exercises

VI. METHODS OF INSTRUCTION:
    A. **Lecture** -
    B. **Demonstration** -
    C. **Research** -
    D. **Lab** -
    E. Assigned reading
    F. **Discussion** -

VII. TYPICAL ASSIGNMENTS:

A. Reading / listening to presentations and readings 1. Presentations and lectures: Lecture on the use of writeblockers 2. Selected current online reading: Example: http://www.nsrl.nist.gov/ (file hash libraries) B. Search for relevant material and read 1. Students use search engines to find readings relevant for each module Example: Find resources describing MD 5 hash vulnerabilities, select three to read. C. Provide comments regarding curriculum 1. Discussion and response questions accompany each module. Example: Discuss how BIOS limitations affect forensic examinations. D. Answer comments and questions from fellow students and instructor 1. Students must participate in group discussion. Example: Is it possible to recover data inserted in a graphic? Why or why not?

VIII. EVALUATION:
    A. **Methods**

    B. **Frequency**

        1. Frequency
            a. 6-10 module assignments
            b. Weekly discussion of group work
            c. 6-10 module quizzes
            d. 6-10 labs
            e. 1 final project
        2. Typical quiz question
            a. Which method is best for write protecting, hardware or software blockers?
            b. Describe the difference between file copy and bitstream copies.
        3. Final exam

IX. TYPICAL TEXTS:
    1. Nelson, Phillips, Enfinger, Stuart *Guide to Computer Forensics and Investigations.*, Course Technology, 2005.
    2. Kruse & Heiser *Computer Forensics: Incident Response Essentials.*, Pearson Education, 2001.

X. OTHER MATERIALS REQUIRED OF STUDENTS:
    A. Students require access to a computer connected to the Internet, with word processing and browser software, and an email address.