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

Course Outline for CNT 68

INTRODUCTION TO COMPUTER FORENSICS

Effective: Fall 2006

I. CATALOG DESCRIPTION:
CNT 68 — INTRODUCTION TO COMPUTER FORENSICS — 3.00 units

A survey course in the detection, prevention and investigation of incidents involving computers and digital information, including cyber attacks and the use of computers to investigate crimes. The program will include introduction to computer forensics, incident response, methods of investigation, tracking persons and data, the secure analysis of hard drives and storage mediums, and IT security utilizing court-approved forensic software and tools.

3.00 Units Lecture

Strongly Recommended
CIS 50 - Intro to Computing Info Tech
or

-

Grading Methods:
Letter or P/NP

Discipline:

	MIN
Lecture Hours:	54.00
Total Hours:	54.00

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. evaluate proper investigative procedures relative to individual, corporate, and criminal rights, responsibilities and law;
C. formulate a basic incident response plan;
D. discuss the methods and techniques of forensic investigation;
E. use forensic software to secure and analyze various digital media;
F. evaluate and compare various forensic utilities and software;
G. describe and evaluate methods of hiding and accessing hidden data;
H. demonstrate an understanding of investigative techniques for various operating systems;
I. describe methods of reporting and presenting an analysis in a legal setting.

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. Physical requirements
    3. Workstation components
    4. Forensic software
    5. Evidence handling and storage
C. Operating systems and data storage basics
    1. Windows
    2. Macintosh/OS X
    3. Unix / Linux

4. Hard drive storage concepts
5. Investigation methods, tools and skills

D. Laws, regulations and standards
1. SB1386
2. Federal
3. State and local
4. Policy and procedures

E. Network fundamentals
1. OSI model for forensics
2. TCP/IP for forensics
3. IP addressing for forensics
4. Network devices and concepts

F. Evidence handling / investigative procedures
1. Methods, tools and procedures
2. Site plan
3. Reception / Coverage
4. Measurement and documentation

G. Data acquisition & forensic analysis
1. Evidence seizure / chain of custody
2. Imaging
3. Backup and storage
4. Analyzing files
5. Procedures and documentation

H. Email investigations
1. Internet fundamentals
2. Crimes and violations
3. Messages and logs
4. Procedure and documentation
5. Methods, tools, and skills

I. Images, files and Steganography
1. Image file formats
2. Encryption
3. Steganography
4. File recovery
5. Password recovery
6. Data hiding techniques
7. Methods, tools, and skills

J. Forensics and security management
1. Computer and investigative policy
2. Disaster planning / business continuity
3. Whitehat hacking
4. Best Practices
5. Intrusion detection
6. Backup / data integrity
7. Network monitoring / threat management

K. Reports and documentation
1. Legal versus technical reports
2. Analysis and conclusions
3. Layout and presentation
4. Verbal and written reports
5. Fact versus opinion

VI. METHODS OF INSTRUCTION:

A. **Lecture** -

VII. TYPICAL ASSIGNMENTS:

A. Reading / listening to presentations and readings 1. Presentations and lectures Lecture on 802.2 standards 2. Selected current online readings Example: www.iana.org/ipaddresses.html (Domain names) B. Search for relevant material and read 1. Students use search engines to find readings relevant for each module Example: Find resources describing Man in the Middle attacks, select 3 to read C. Provide comments regarding curriculum 1. Discussion and response questions accompany each module Example: “Discuss how ARP cache poisoning threatens web servers. D. Answer comments and questions from fellow students and instructor 1. Students must participate in group discussion Example: Is California SB1386 sufficient to protect personal data rights? 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 making a forensic copy - file copy, or bitstream?
   b. Describe the difference between PING and TRACEROUTE
   c. 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.