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 68

DIGITAL FORENSICS FUNDAMENTALS

Effective: Spring 2018

I. CATALOG DESCRIPTION:
CNT 68 — DIGITAL FORENSICS FUNDAMENTALS — 3.00 units

A practical course in Digital Forensics; the detection, and investigation of incidents involving computers, networks, the Internet, and digital information. Case oriented, following the objectives for the CFE Computer Forensics Examiner certification exam and the International Association of Computer Investigative Specialists (IACIS), the class includes understanding and practice in basic computer forensics, methods of investigation, analysis of storage media, logs, and tracking persons and data, using court-approved evidence collection tools. Also covered, computer forensics as a profession; the computer investigation process, and technical writing.

2.50 Units Lecture 0.50 Units Lab

Strongly Recommended
CIS 66 - Networking Fundamentals
with a minimum grade of C

Grading Methods:
Letter or P/NP

Discipline:
- Computer Service Technology

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

II. NUMBER OF TIMES COURSE MAY BE TAKEN FOR CREDIT: 1

III. PREREQUISITE AND/OR ADVISORY SKILLS:

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

A. CIS66
   1. describe and differentiate the devices, protocols, and services used to support communications in data networks and the Internet;
   2. evaluate the importance of addressing and naming schemes at various layers of data networks in IPv4 and IPv6 environments;
   3. explain Ethernet topologies, and relevant IEEE hardware and software specifications;
   4. describe the major functions of LAN hardware protocols such as Ethernet; and WAN protocols such as T-series, DSL, ATM, and Frame Relay;
   5. build a router and switch topology; and configure the devices to communicate with computers;
   6. compose CISCO command-line interface (CLI) commands to perform basic router and switch configration;
   7. identify the responsibilities of a LAN system administrator;
   8. draw typical network diagrams, using software tools such as Microsoft Visio;
   9. monitor the network activity using monitoring tools to view packets and analyze traffic.

IV. MEASURABLE OBJECTIVES:

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

A. define computer forensics.
B. summarize how to prepare for a computer investigation.
C. summarize the certification requirements for computer forensics labs.
D. measure the different ways for proper data acquisition.
E. classify the rules for proper digital evidence handling.
F. analyze how data is stored and managed by an operating system.
G. analyze various computer forensics tools.
H. validate the evidence during the analysis process.
I. identify and reconstruct graphics files.
J. describe the importance of network forensics.
K. analyze email investigations.

L. generate a forensic report.
M. describe guidelines for testifying in court.
N. maintain a high level of ethical behavior in their work.

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. **Discussion** -
B. **Classroom Activity** -
C. **Student Presentations** -
D. **Demonstration** -
E. **Lab** -
F. **Lecture** -
G. **Critique** -

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 5hash vulnerabilities, select three to read.

C. Performing lab esperiments using forensic software

    1. Use FTK to image the target USB drive and search for social security numbers
  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**

1. Exams/Tests
2. Quizzes
3. Projects
4. Lab Activities
5. Other:
    a. Hands-on projects
    b. Examinations
    c. Presentations
    d. Discussions
    e. Problem-solving assignments

B. **Frequency**

1. 6-10 weekly hands-on projects
2. 1 mid-term exam, 1 final exam, and weekly quizzes
3. 1 presentation
4. Weekly class discussions and/or online discussions
5. 1 final project consisting of problem-solving assignments

IX. TYPICAL TEXTS:

1. Luttgens, Jason , and Matthew . *Incident Response & Computer Forensics.* 3 ed., McGraw-Hill Education, 2014.
2. EC-Council . *Computer Forensics: Investigating File and Operating Systems, Wireless Networks, and Storage (CHFI).* 2 ed., Cengage Learning, 2016.
3. Shaaban, Ayman , and Konstantin Sapronov. *Practical Windows Forensics .* 1 ed., Packt Publishing, 2016.

X. OTHER MATERIALS REQUIRED OF STUDENTS:

A. Association of Computing Machinery ACM.org student membership
B. Students require access to a computer connected to the Internet, with word processing and browser software, and an email address.