Lecture Contact Hours: 32-36; Homework Hours: 64-72; Total Student Learning Hours: 96-108
Laboratory Contact Hours: 48-54; Homework Hours: 0; Total Student Learning Hours: 48-54

CUYAMACA COLLEGE
COURSE OUTLINE OF RECORD

COMPUTER AND INFORMATION SCIENCE 265 – COMPUTER FORENSICS FUNDAMENTALS

2 hours lecture, 3 hours laboratory, 3 units

Catalog Description
This course introduces the methods used to properly conduct a computer forensics investigation. Topics include ethics, computer forensics as a profession, the computer investigation process, operating systems boot processes and disk structures, data acquisition and analysis, technical writing, and a review of familiar computer forensics tools. The course prepares students for Computer Hacking Forensic Investigation certification (CHFI ECO 312-46).

Prerequisite
Completion of CIS 264 with grades of "C" or better

Entrance Skills
Without the following skills, competencies and/or knowledge, students entering this course will be highly unlikely to succeed:
1) Evaluate the legal and regulatory requirements of ethical hacking and penetration tests.
2) Produce a penetration test authorization and rules of engagement document.
3) Contrast penetration testing methodologies.
4) Derive system reconnaissance and network scan to detect open ports and vulnerable systems.
5) Elaborate social engineering techniques for a penetration test.
6) Compile penetration test scanning results to exploit vulnerabilities.

Course Content
1) Computer Forensics Investigation Process
2) Searching and Seizing Computers
3) Digital Evidence
4) First Responders Procedures
5) Computer Forensics Lab
6) Understanding Hard Disks and File Systems
7) Window Forensics
8) Data Acquisition and Duplication
9) Recovering Deleted Files and Deleted Partitions
10) Forensics Investigation using Access Data FTK
11) Forensics Investigation Using EnCase
12) Steganography and Image File Forensics
13) Application Password Crackers
14) Log Capturing and Even Correlation
15) Network Forensics, Investigating Logs and Network Traffic
16) Investigation Wireless Attacks
17) Investigation Web Attacks
18) Track Emails and investigating Email Crimes
19) Mobile Forensics
20) Investigative Reports
21) Becoming an Expert Witness

Course Objectives
Students will be able to:
1) Describe the features and operation of modern file systems;
2) Perform elementary forensic analysis and data recovery on the FAT (File Allocation Table) systems, using only a hex editor.
3) Evaluate the strengths and weaknesses of various software tools for data recovery.

Method of Evaluation
A grading system will be established by the instructor and implemented uniformly. Grades will be based on demonstrated proficiency in the subject matter determined by multiple measurements for evaluation, one of which must be essay exams, skills demonstration or, where appropriate, the symbol system.
1) Essay Examinations with open-ended questions reflecting theoretical and applied situations
2) Laboratory exercises
3) Objective Examinations and quizzes
4) Problem Solving Examination (demonstration of skill applied to a specific scenario)

Special Materials Required of Student
Electronic storage media, reliable access to Internet

Minimum Instructional Facilities
Smart computer lab with whiteboards, Internet browser, Internet connectivity, software, printer; network connection not connected to school academic resources Virtual Machine (VM) environment for students to work (Netlab)

Method of Instruction
1) Online computer-based reading assignments
2) Instructor and individual student mentoring
3) Practical application assignments

Out-of-Class Assignments
1) Read the curriculum and assignment instructions
2) Complete Netlab assignments and online quizzes
3) Review online resources, including reference materials and videos

Texts and References
1) Required (representative example): CHFI Computer Hacking Forensic Investigator Certification All-in-One Exam Guide, Charles L. Brooks, September 5th 2014, ISBN: 9780071831550
2) Supplemental: None

Student Learning Outcomes
Upon successful completion of this course, students will be able to:
1) Describe different types of digital evidence, rules of evidence, digital evidence examination processes, and electronic crime and digital evidence consideration by crime category, the roles of a first responder, first responder toolkit, securing and evaluating an electronic crime scene, conducting preliminary interviews, documenting electronic crime scenes, collecting and preserving electronic evidence, packaging and transporting electronic evidence and reporting the crime scene
2) Demonstrate the ability to utilize forensic procedures such as: how to recover deleted files and deleted partitions in Windows, Mac OS X, and Linux; the process involved in forensic investigation using Access Data FTK and Encase Steganography and its techniques, as well as Steganalysis, and image file forensics; password cracking concepts, tools, types of password attacks and how to investigate password protected file breaches; different types of log capturing techniques, log management, time synchronization and log capturing tools; how to investigate logs, network traffic, wireless attacks, and web attacks; how to track e-mails and investigate e-mail crimes.