C S 53D: INTRODUCTION TO COMPUTER FORENSICS

Foothill College Course Outline of Record

Heading	Value
Effective Term:	Summer 2021
Units:	4.5
Hours:	4 lecture, 2 laboratory per week (72 total per quarter)
Advisory:	C S 53A.
Degree & Credit Status:	Degree-Applicable Credit Course
Foothill GE:	Non-GE
Transferable:	CSU
Grade Type:	Letter Grade (Request for Pass/No Pass)
Repeatability:	Not Repeatable

Student Learning Outcomes

- A successful student will be able to describe computer forensics and investigations as a profession
- A successful student will be able to use and classify a variety of forensic tools

Description

Provides an overview of the forensic rules-of-evidence, evidence integrity, factual reporting, and the role of expert opinion in legal proceedings. The course is appropriate for students from information technology-related fields. No previous experience in computer forensics is required. All students must agree with and sign the CyberSecurity Institute Code of Ethics and Conduct.

Course Objectives

The student will be able to:
A. Understand computer forensics and investigations as a profession.
B. Perform a computer investigation.
C. Describe the ethical underpinnings of being a computer forensics professionals.
D. Describe how operating system affects the analysis and investigation.
E. Describe various network logs and information sources.
F. Use and classify a variety of forensic tools.
G. Prepare and defend standard forensic reports.
H. Understand the requirements for serving as an expert technical witness.

Course Content

A. Computer forensics and investigations as a profession
1. Computer crime present and future
a. Financial
b. Child pornography
c. Personal and corporate security breaches
2. Scope of computer forensics
3. Preparing for investigations
4. Maintaining professional conduct
B. Computer investigations
1. Preparing an investigation
2. Systematic approach to documentation
3. Understanding data-recovery software
4. Safely seizing/obtaining computers
C. Ethical behavior
1. Signing/agreeing to a code of ethics
2. Privacy and confidentiality
3. Legal requirements and liability
D. Working with operating systems
1. File systems - File Allocation Table (FAT) 32
a. File structures
b. Pure mode DOS
c. Slack space
d. File slack
1) Random Access Memory (RAM) slack
2) Drive slack
3) Unallocated space
4) Data hiding methods
2. Working with other file systems
a. New Technology File System (NTFS)
b. Compact Disk File System (CDFS)
c. Network File System (NFS)
d. Linux file systems
E. Network information sources
1. Internet files
2. Server logs
3. Proxy server logs
4. Firewall logs
5. Email
F. Forensic tools
1. Keyword searches
2. Imaging hard drives
3. Imaging USB drives
4. Restoring erased files and data
5. Using hashing algorithms
6. Restoring erased files and data
7. Using hashing algorithms
8. Best tools
G. Writing investigation reports
1. Understanding the importance of reports
2. Proper documentation methods
3. Expressing an opinion
4. Explaining results
H. Working as an expert technical witness
1. Comparing technical and scientific testimony
2. Preparing for testimony
3. Serving as a consulting witness
4. Preparing for a deposition
5. Testifying in court
6. Forming an expert opinion

Lab Content

A. Introduction to file systems
1. Analyze the structure of:
a. FAT 32 file system
b. FAT 64 file system
c. NTFS file system
B. Common locations of Windows artifacts
1. Analyze the behavior of the direction
C. Hashing data sets
1. Hash data sets to guarantee preservation
D. Perform drive letter assignments in Linux

E. The imaging process - evidence acquisition, preparation and preservation
1. Acquire a data set that is to be used as evidence in a forensics analysis
2. Prepare the data set for imaging
3. Set-up the infrastructure to preserve the image
F. Introduction to single purpose forensic tools
1. Use the following forensics tools:
a. Explore ILooKIX from Perlustro
b. Understand and demonstrate the use of the Digital Forensics Framework
c. Install and configure Wireshark
G. Introduction to Autopsy Forensic Browser
1. Use Autopsy Forensic Browser to analyze NTFS, FAT, UFS1/UFS2, Ext2/Ext3/Ext4 file systems
H. Introduction to PTK Forensics Basic Edition
1. Install and use a analyze a hard disk
I. Analyzing a FAT partition with Autopsy - file and program activity analysis
1. Perform an in-depth analysis of a FAT file system
J. Analyzing a NTFS partition with PTK - file and program activity analysis
K. Browser artifact analysis - browser forensics
1. Exam browser history
2. Exam browser cookies
L. User profiles and the Windows Registry
1. Preserve and analyze User profile
2. Preserve and analyze the Windows Registry
M. Log analysis
1. Preserve and hash the contents of a log file
2. Analyze the log file as part of a forensic investigation
N. Memory analysis - file and program activity analysis
1. Capture a memory image
2. Use the image to analyze the computer state
O. Forensic case capstone - capstone lab covering all objectives
1. Perform a case study using the tools learned during the course

Special Facilities and/or Equipment

A. Access to a network laboratory with current Cisco network equipment host computers required to support the class.
B. A website or course management system with an assignment posting component (through which all lab assignments are to be submitted) and a forum component (where students can discuss course material and receive help from the instructor). This applies to all sections, including on-campus (i.e., face-to-face) offerings.
C. When taught via Foothill Global Access on the Internet, the college will provide a fully functional and maintained course management system through which the instructor and students can interact.
D. When taught via Foothill Global Access on the Internet, students must have currently existing email accounts and ongoing access to computers with internet capabilities.

Method(s) of Evaluation

Tests and quizzes
Written laboratory assignments
Final examination

Method(s) of Instruction

Lectures which include motivation for the architecture of the specific topics being discussed
In-person or online labs (for all sections, including those meeting face-to-face/on-campus), consisting of:
1. An assignment webpage located on a college-hosted course management system or other department-approved internet environment. Here, the students will review the specification of each assignment and submit their completed lab work
2. A discussion webpage located on a college-hosted course management system or other department-approved internet environment. Here, students can request assistance from the instructor and interact publicly with other class members
Detailed review of laboratory assignments which includes model solutions and specific comments on the student submissions
In-person or online discussion which engages students and instructor in an ongoing dialog pertaining to all aspects of designing, implementing and analyzing programs
When course is taught fully online:
1. Instructor-authored lecture materials, handouts, syllabus, assignments, tests, and other relevant course material will be delivered through a college-hosted course management system or other department-approved internet environment
2. Additional instructional guidelines for this course are listed in the attached addendum of CS department online practices

Representative Text(s) and Other Materials

Johansen, Gerard. Digital Forensics and Incident Response, 2nd ed.. 2017.

Types and/or Examples of Required Reading, Writing, and Outside of Class Assignments

A. Reading
1. Textbook assigned reading averaging 30 pages per week.
2. Online curriculum averaging 20 pages per week.
3. Online resources as directed by instructor though links pertinent to networking.
4. Library and reference material directed by instructor through course handouts.
B. Writing
1. Technical prose documentation that supports and describes the laboratory exercises that are submitted for grades.

Discipline(s)

Computer Science