CS 53D: Computer Forensics
Foothill College Summer, 2020
Online Format
Instructor: Timothy Ryan
Email: ryantimothy@fhda.edu
Office Hours: Sat 10:00AM – 12:00PM (and by appointment)
Website: https://foothillcollege.instructure.com or http://tinyurl.com/gofhda

Required Materials
Textbook: Digital Forensics and Incident Response, 2nd Edition
By Johansen, Gerard (Author). Packt Publishing

Course Description
Provides an overview of computer forensics including retrieving information from computers and data storage systems using browser, email, network and memory forensics. An emphasis will be placed on emerging technologies such as mobile and cellular devices. Legal issues will be explored including rules-of-evidence, evidence integrity, factual reporting, and the role of expert opinion in legal proceedings. Lab exercises will be utilized for hands-on learning including Android OS, Splunk Fundamentals and a Forensic Case Capstone project. The course is appropriate for students from a computer science or information technology-related field, no previous experience in computer forensics is required.

Course Objectives
The student will be able to:

- Understand computer forensics and investigations as a profession.
- Perform a computer investigation.
- Describe the ethical underpinnings of being a computer forensics professional.
- Describe how operating systems affect the analysis and investigation.
- Describe various network logs and information sources.
- Use and classify a variety of forensic tools.
- Prepare and defend standard forensic reports.
- Understand the requirements for serving as an expert technical witness.

Student Learning Outcomes for CS 53C
- 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

Foothill College Student Learning Outcomes:
https://foothill.edu/schedule/outlines.html

Evaluation

Course evaluation is based on the following:

Lab Activities	500 Points
Online Discussions	200 Points
Splunk Certification	100 Points
Quizzes (2)	100 Points
Final Exam	100 Points

1000-900	= A
899-800	= B
799-700	= C
699-600	= D
599-Below	= F

Academic Honesty

Your instructor enforces the Foothill College Academic Honor Code. It is assumed that all students will pursue their studies with integrity and honesty. See course catalogue for details.

Lab Activities

Lab assignments will be completed using the online NetLab+ system which is available at the following URL: https://openlab.bayict.cabrillo.edu. Key features of each assignment will be discussed and emphasized with respect to course objectives. In addition to the nine labs assigned students will complete two elective labs to increase their knowledge on a preferred topic.

Attendance

This class is delivered in an online format. An Instructor presentation will be delivered each week via ConferZoom which allows real-time participation and is recorded for later viewing.

Special Assistance

To obtain disability-related accommodations, students must contact Disability Resource Center (DRC) as early as possible in the quarter. To contact DRC, you may:

- Visit DRC in Room 5400
- Email DRC at adaptivelearningdrc@foothill.edu
- Call DRC at 650-949-7017 to make an appointment

If you already have an accommodation notification from DRC, please contact me privately.

Course Outline
(Note: Subject to Change)

Week	Date	Reading	Assignments
1	6/29	Chapter 1: Incident Response Chapter 3: Digital Forensics	NDG Lab#4: Forensic Linux Tools NDG Lab#5: Analyzing Memory Discussion: Role of Forensics
2	7/6	Chapter 4: Network Evidence Chapter 5: Host-Based Evidence	NDG Lab#6: Linux OS Forensics NDG Lab#7: Windows OS Forensics Discussion: Evidence and Law Quiz 1
3	7/13	Chapter 7: Analyzing Network Evidence Chapter 8: Analyzing System Memory	NDG Lab#9: Browser Forensics NDG Lab#14: Email Forensics Discussion: NIST Guidelines
4	7/20	Chapter 9: Analyzing System Storage Chapter 10: Analyzing Log Files	NDG Lab#16: Intro to Android OS NDG Lab#17: Android Acquisition Discussion: Mobile Forensics Quiz 2
5	7/27	Chapter 12: Malware Analysis Chapter 13: Threat Intelligence	Elective Lab #1 Elective Lab #2 Splunk Certification
6	8/3	Chapter 14: Hunting for Threats	NISGTC Lab#16: Forensic Capstone Final Exam