

COURSE OUTLINE
CFOR-250
Computer Network Forensic Technology
3 Credits

HOWARD COMMUNITY COLLEGE

Description

This course will cover computer forensics examination process in a network environment. The OSI model, TCP/IP model and IP addressing will be discussed and the relationship and how these layered approaches relate to the computer forensics examination process. Students will determine how various network devices such as servers, hubs, switches and routers create log files that can be used for forensic examination. Students will examine various log files, port scans, and packet sniffers, etc., from network devices for computer forensic analysis. Students will have hands-on experience with actual computer networks in the lab using various forensics tools and devices. Prerequisite: CFOR-210. (2 hours lecture, 2 hours lab)

Overall Course Objectives

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

1. Describe OSI model and the purpose of each layer.
2. Identify physical layer components such as UTP and fiber cables and connectors and their roles.
3. Examine network devices, hubs, switches and routers and servers and their role in network forensic examination.
4. Describe TCP/IP protocols and IP addressing and how they are used to collect forensic evidence.
5. Explain the role of IDS, Firewall, and VPN devices and how these devices play a role in the network forensic examination process on the network.
6. Examine the role of email, web and DNS server and their functions in collecting and analyzing evidence for forensic examination.
7. Examine viruses, worms and Trojan horses and how to mitigate them.
8. Explore password security, weaknesses and disaster recovery methods.
9. Describe the importance of network security and the tools used for computer forensic analysis in a network environment.
10. Examine various log files, port scans, packet sniffers, registry files, etc., for computer forensic evidence.
11. Describe the potential damage associated with compromised computer network systems.

Major Topics

- I. Network Terminology
 - A. OSI layer
 - B. Ethernet Topologies (LAN)
 - C. Physical Layer - copper and fiber
 - D. LAN Protocols
 - E. TCP/IP Protocols
 - F. IP addressing

- II. Server Basics and their Role in Evidence Collection
 - A. DNS servers
 - B. Web servers
 - C. Email servers
 - D. Collecting various log files for evidence

- III. Forensic Examination of Network Vulnerability Issues
 - A. Hubs
 - B. Switches
 - C. Routers
 - D. IDS
 - E. VPN
 - F. Firewalls
 - G. Proxy servers
 - H. Gathering and analyzing evidence

- IV. Vulnerability of Network Security and Network Forensic analysis
 - A. Importance of Physical Security
 - B. Viruses, Worms and Trojan horses
 - C. Password security
 - D. Operating system security
 - E. TCP/IP security
 - F. Computer forensic analysis
 - G. Auditing logs
 - H. Vulnerability assessment
 - I. Compromised network and disaster recovery

Course Requirements

Grading/exams: Grading procedures will be determined by the individual faculty member but will be calculated on the basis of tests, lab reports, project and final exam.

Writing: Each week, students are expected to write a laboratory report after performing that week's assigned experiments.