

COURSE OUTLINE

COURSE TITLE: COMPUTER FORENSICS II

COURSE NUMBER: IA-559

CREDIT HOURS: 3 Graduate

PREREQUISITE: IA – 558 Computer Forensics I

CATALOG DESCRIPTION

Comprehension of network forensic investigations and application of investigative framework methodologies. Students will apply Linux for forensic analysis, and Access Data Forensic Tool Kit. Evaluation of Steganography tools and field acquisition of electronic media will be presented. Students subject to background investigation prior to admittance.

COURSE OBJECTIVES

At the conclusion of this course, the student will be able to:

1. Analyze network hardware involved in intrusion detection.
2. Comprehend the variables in network search warrant requirements.
3. Apply the necessary methodologies to conduct a computer forensic examination.
4. Application of Linux operating system for forensic analysis of seized media.
5. Evaluate password recovery tools (PRTK) and Distributed Network Attack Software.
6. Analyze hidden information from pictures and digital audio files utilizing Steganography software.
7. Describe field acquisition problems and solutions of image acquisition issues in hardware and software.

COURSE OUTLINE

- I. Forensic Network Investigations
 - a. Network Computer Components
 - b. Working with Network Administrators
 - c. Search Warrant Issues Related to Network Centers

- II. Investigative Framework Methods
 - a. Cybercrime Methodologies
 - b. Structure of Cybercrime Investigations
 - c. Case Management – Pursue or Drop

- III. Linux for Forensic Analysis
 - a. Introduction of Linux Operating Systems
 - b. Various Types of Linux
 - c. Unix Networks
 - d. Linux Forensic Tools

- IV. Access Data – Password Recovery Tool Kit Software
 - a. Password Recovery Issues / Investigations
 - b. Profile of the Suspect / Password Database
 - c. Password Recovery Toolkit
 - d. Distributed Network Attack Software

- V. Steganography
 - a. Explanation and Usages
 - b. How Steganography Applies to Computer Forensics

- VI. Field Acquisition Kit and Methodology
 - a. Field Acquisitions of Electronic Media
 - b. Hardware Requirements
 - c. Methodology of Field Acquisitions

GRADING REQUIREMENTS

- 1) Quiz 1..... 15%
 - 2) Quiz 2..... 15%
 - 3) Research Paper..... 30%
- See Attachment for Research Paper Guidelines
- 4) Final Examination..... 40%

100-91 = A
81 – 90 = B
71 – 80 = C
65 and below = F