

University of Washington, Tacoma
Computer Forensics Certificate Program (Non-Credit)

Course Two: Computer Forensics

Course Description:

A computer forensics case, as in most investigations, begins with a crime or an allegation of wrong doing. The computer forensic examiner may review hundreds if not thousands of bytes of data to prove or disprove the case. Before the first bit of data is examined, it must first be identified, collected, acquired, and verified. The forensic examiner must be prepared to gather evidence both in the field and in the lab. The proficient computer examiner must be familiar with a wide variety of operating systems, networks, software, and hardware configurations.

Textbook: *Guide to Computer Forensics and Investigations, Second Edition: Phillips, Nelson, Enfinger, Steuart*

Class 1 – Class Orientation/Crime Scene Evaluation

Today's mobile work force carries with them the computing capabilities of their office workspace. Laptops and various storage media bring new challenges to field acquisitions. Students will review office and field evidence gathering issues and solutions.

Class 2 – Hardware/Hard Disk Structure/Operating Systems File Management

Hardware incompatibility can lead to many frustrations and possible errors during evidence acquisition. Hardware miscalculations can lead to the destruction of the device and the evidence they contain. The student will review various hardware and solutions to obtaining a forensic exact copy (image) of the device(s). An overview of hardware and a computer system BIOS will be discussed and demonstrated. The following topics will be covered:

Hard Disk Structures

- Logical/Physical
- Logical Block Addressing
- Sector/Cluster
- Binary and Hexadecimal Values

Interface

- IDE/ATA
- SCSI
- USB
- IEEE-1394
- Parallel and Serial ATA

Operating System Formatting

- Windows Based
- Unix Based

Class 3 – Operating System Limitations/Imaging Techniques

Operating systems have limitations when viewing or accessing data from other files systems. Relevant evidence, such as Metadata, may not be interpreted correctly. Additionally, an uncontrolled boot process can alter evidence. Students will become familiar with these issues and solutions by using a Windows system to access files from Macintosh and Linux systems.

The acquisition (imaging) of evidence is a critical component of any forensic examination. Students will create a boot disk to control a systems boot process and successfully create an image. Students will verify the image by using hash computing software and comparing hash values. Hardware and software write blocking tools will also be discussed and used.

Class 4 – Continuation of Operating System Limitations/Imaging Techniques

Class 5 – Forensic Software

Forensic software is available for Windows and Unix based systems. The benefit of each will be discussed. Students will become familiar with forensic software by installing and using several versions of forensic software. The software will be used to recover and analyze data from the evidence images created earlier in class. The following information will be reviewed:

- Date and Time Stamps
- Directory and Folder Structures
- Links
- Master File Table Attributes
- Registry
- Data Clustering
- Keyword Searching

- Data Mining in Unallocated Space

Class 6 – Encryption, Passwords, and Data Hiding

Corporations and home users share a common concern for privacy and security. Powerful encrypting and data hiding software are readily available for both business and home use. It is unlikely true encryption can be defeated. However, students will learn methods in obtaining passwords and possible solutions to recovering encrypted and password protected files. Students will install and use Windows and Open Source software to extract password-protected and hidden data. The following topics will be discussed.

- Steganography
- Hidden Partitions
- Encrypted File System
- File Header Information
- Public and Private Key Encryption
- Compressed Files
- Unicode

Class 7 – Financial and Text Documents, Internet, and E-mail Examinations

Computers accomplish many tasks in the business environment and in the home. On average, computers are used for word processing, financial management, research, and communicating with others via the Internet. These are also the areas of focus for most forensic investigations. Gaining access to the files created by programs used is the most common task and can be challenging. In this block of instruction, the students will gain knowledge in accessing those data files. The following topics and associated data files will be reviewed:

- Chat Logs
- News Groups
- Microsoft Office Documents
- Word Perfect
- Open Office
- Quicken Files
- MS Money Files
- Document Metadata
- Internet Protocol (IP) Tracking
- Hypertext Markup Language (HTML) Documents
- Internet History
- WebPages

- Virtual Storage

Class 8 – Continuation of E-mail Recovery

Much business is conducted through e-mail. E-mail can contain documents, images, and programs as attachments. All or part of these items may be the focus of an investigation. The student will recover e-mail from both web based e-mail clients and Post Office Protocol (POP) Mail accounts. Students will track e-mail through its delivery process. The following topics will be discussed.

- UUE
- Web Mail
- IP Spoofing
- E-mail Headers
- Routers
- E-mail Clients

Class 9 – Presenting the Evidence

At the conclusion of an examination the forensic examiner may have recovered hundreds of files and thousands of e-mail documents. The forensic findings must be organized and presented in a manner that can be clearly understood. The students will review methods of displaying and organizing their findings.

Class 10 – Review

The final day of instruction will include an overview of the forensic process. Students will have an exercise in which they will demonstrate proficiency in identifying, acquiring, validating, and problem solving.