



The Forensics 5-Day bootcamp consolidates all content from the 3-day DFED an ADFT classes into a succinct yet comprehensive format. In addition to the efficient use of time the student will save about \$1000 over the two-class price structure.

The benefits to law enforcement and the military are obvious. Whereas the corporate IT personnel will use the skills gained to identify and remedy vulnerabilities that have been exploited so as to eliminate the problem. Additionally in many cases the techniques used may help identify the perpetrator for referral to law enforcement for prosecution. In summary, there are many job descriptions that will benefit from this training depending on industry segment - general network administration, law enforcement, insurance investigations, litigation support and criminal defense to name a few.

Student Materials

Students will receive the following items during this course of instruction:

- A 350-page comprehensive computer forensic student guide and investigative resource materials.
- A CD-ROM containing GUI-based Windows data examination software with a “live” case file.
- A CD-ROM containing GUI-based Linux data examination software.
- Upon passing practical and written exams, a Certificate of Completion

Our curriculum was developed by John A. Sgromolo, former Course Director for the Computer Crime curriculum at the Institute of Police Technology and Management at the University of North Florida, located in Jacksonville. Mr. Sgromolo, a pioneer in computer forensics, is a former Special Agent with the Naval Criminal Investigative Service. He was responsible for coordinating all computer crime general investigations at the Norfolk Field Office. In his capacity as Course Director for IPTM, Mr. Sgromolo was responsible for teaching hundreds of law enforcement officers nationwide in the intricacies of computer crime investigations.

Prerequisites

The Computer Forensics Training Bootcamp™ course of instruction is specifically designed for corporate and government personnel who in the performance of their duties may be asked to conduct an advanced digital forensic examination of digital media. Students desiring to attend the Computer Forensics Training Bootcamp™ course of instruction should possess an average knowledge of how to operate a modern personal computer running the MS Windows® operating system. Additionally, the student should possess an average knowledge of how to use e-mail, word-processing, spreadsheet and MS PowerPoint® software programmes. A basic working knowledge of the Linux operating system would also be helpful, but not a requirement. Prior knowledge of the popular automated forensic software tools (EnCase™ and Forensic Tool Kit™) is not required, as students will be exposed to these tools within this course of instruction.

COURSE CONTENTS

What's Included:

Introduction to Computer Crime

An introduction to the field of computer forensics and the basis for gathering electronic digital artifacts. Students are introduced to the concepts, situations and personalities they may encounter while investigating a computer incident. The origins of computer crimes and how they are investigated set the stage for the following lessons.

Disk Storage Concepts

Having a clear understanding of how data is stored is having the upper hand during any investigation. Microsoft operating systems have a systematic way of storing data that is unknown to most end users here you will learn hard drive storage dynamics. Although information may not physically be visible, there are many different approaches to recovering or viewing the data that appears to be lost. DOS, Windows 3.x, 95/98/NT/2000/XP operating systems and file management are covered in this lesson.

Forensic Examination

Techniques and protocols utilized by U.S. computer forensic examiners and laboratories are covered. This is a detailed review of standard and advanced procedures and how you can effectively implement these procedures into your organization. These proven techniques have been the most effective since the inception of computer crimes. Covers the advanced procedures necessary to conduct an accurate and carefully documented computer forensic examination. Advanced methods of computer forensic protocols are implemented, including physical evidence recovery.

Electronic Discovery and Digital Evidence

Students learn recovery methods of digital artifacts from various file structures and gain an overview of different operating systems and file structures that are encountered during a computer forensic examination. The footprints that are left behind with every keystroke are covered. Exercises detail what to look for, as well as the various techniques for retrieving the information in a forensically sound manner.

Tools of the Trade

Multiple software and hardware solutions are covered during this session. Students learn about the numerous tools available to them in a vendor neutral environment. A clear understanding of what the tools do and how they work is presented in layman's terms. Gaining a clear understanding of what forensic tools do and how they work is a crucial part of any investigation, especially if it goes to trial. Students will utilize these tools during practical application exercises to investigate digital media. This is a hands-on lab where innovation and knowledge play a key role.

Seizure Concepts

Proper seizure of digital media is the start of every computer investigation. During this lesson, students learn the correct protocol, as set by the U.S. Department of Justice, to assure proper "Chain of Custody" is followed from the beginning of the investigation. This crucial information can make or break a case. First responders-must properly handle evidence and start the correct chain of custody.

Advanced Artifact Recovery

A hands-on lab where students conduct an advanced forensic examination of digital media. The focus of this lesson is to utilize advanced automated tools for the recovery of digital artifacts that are unattainable by conventional methods. There are several practical exercises that challenge even the senior cyber crime investigator. Focus is placed on using the advanced tools and thinking “outside the box” to try to discover incriminating digital evidence on a live case file.

Crypto and Password Recovery

Covers digital encryption file structures and password-protected data that an investigator may encounter while conducting and exam. Students are exposed to methods to decode and crack passwords that are used to protect potential evidence. They also learn techniques to gain access to encrypted files that may reside within the information.

Specialized Digital Media Analysis and Recovery

Covers state of the art software where students are required to examine digital media in an attempt to recover data pertaining to a civil or criminal offense. The students will present their findings to the class during an evidence presentation exercise. Students will compete to see who completed the most thorough investigation. This exercise is very in-depth and competitive.

Electronic Discovery, Acquisition and Analysis Lab

Students acquire and analyze digital evidence using specialized forensic tools and will conduct a proper “seizure and search” for digital evidence. Proper authentication and analysis skills are taught using advanced forensic utilities and software tools. This is a hands-on lab requiring students to utilize the proper tools and procedures to conduct a forensically sound examination of digital media. Students are required to properly authenticate and analyze digital evidence during this exercise. Students will use their newly attained skills to find evidence that cannot be detected by normal computer forensic investigative methods.

Presentation of Digital Evidence

Students are introduced to aspects of presenting digital evidence in a courtroom environment. They are exposed to the specialized tools necessary to effectively create and present the results of a cyber crime investigation to an administrative body or court of law. Both civil and criminal incidents are covered during this lesson. This is the final exercise where students are faced with the challenge of presenting their findings in a low-tech format where non-technical personnel are able to decipher and understand the results. The students will physically present their findings in “layman’s terms,” which is critical during any investigation. Getting the audience to gain a clear understanding of what occurred on a computer system is sometimes the biggest hurdle in completing an effective investigation. Students will have mastered this critical skill by the end of this exercise.

For information and registration, call 1-888-296-6682 Ext: 267
or email training@novaknowledge.com

