

## Custom Computer Forensics Training

Our courses were designed to train Corporate Security Personnel and Law Enforcement Agents in electronic discovery and the fundamentals of conducting a proper computer forensic examination.

Our Courses are essential to information security, risk management, loss prevention, corporate security and law enforcement personnel who encounter digital evidence while conducting an investigation.

The training environments are interactive and the students work on case files in a hands-on environment.

Upon completion of our courses, students will have the knowledge to immediately begin using their new skills to conduct a computer forensic examination in the field or in the lab.

### Why Choose GDF for Computer Forensic Training?

- **Real World Training Environment**
- **Use The Latest Techniques Hands On**
- **Experienced Investigators Teach The Courses**
- **Focus On Corporate and Business Issues and Strategies**
- **Small Class Size For A Personalized Experience**
- **Vendor Neutral - Learn To Use Many Forensic Tools**

Students are trained in state of the art training facilities nationwide; each classroom features a workstation for each student, complete case files and limited enrollment to keep classes intimate.

Where most classes are lecture based with limited lab time, GDF students are taken through an investigation using a real case in which the instructor was the actual investigator. Through a combination of lecture, hands-on activities and mentoring; students learn, practice and retain more of the information in each course of instruction.



The question of Relevance is a main concern for GDF in its curriculum development. While the vast majority of courses in Computer Forensics are targeted at "felonious activity" the needs of the corporate investigator are often neglected.

All of GDF's curriculums are designed for corporate clients with the assistance of investigators, technologists and attorneys. They are tailored toward fraud investigation, IP (intellectual property) theft, white collar crime, compliance issues and the discovery of electronic evidence, of course. GDF still covers Identity Theft, Child Pornography and Harassment, but always from a corporate investigators perspective.

### **GDF does not sell forensic software.**

All of our courses introduce students to the tools available from all the major forensic software vendors. Students learn to conduct an investigation using state of the art tools, as well as, the tried and true hands on method.

Knowledge of the newest "do-all-tools" is essential, but a base knowledge of the file system, manual tools and the theories behind them are required to understand the forensic methods and have a thorough grasp of the process behind the tools.

All GDF courses are based on this important principal. Research and Development are an integral part of the GDF philosophy. The GDF team continuously updates and tunes courses to keep up with the changing business and technology environment. Attorneys keep current on case law, technologists stay ahead of the industry trends and that knowledge is continuously passed on to our instructors.

The instructors, combined with their years of experience, then disseminate the knowledge to our students. Through the years the GDF team has worked on leading data recovery tools, system utilities and major IT installations. This insider knowledge of real world environments, continuous research and exceptional, experienced instructors allows GDF to deliver courses that are unmatched in the field.

The Advanced Computer Forensic Techniques (ACFT) course was designed to train corporate and law enforcement investigators in the advanced elements of computer forensics. The main focus of the advanced course is to help digital investigator identify information that is not readily or easily available. The ACFT follows the guidelines set forth in the CFED course and is taught in a hands-on, interactive training environment. This course is designed for the computer forensic savvy investigator that has had previous training or who has been working in the field. Students attending this class

must have a firm understanding of conducting a proper computer forensic examination.

### **Manual Data Carving**

Students will learn to manually carve numerous file types out of digital evidence. In addition to the common image files such as JPEG and GIF, students will learn to identify and successfully carve Word documents, spreadsheets and numerous other file types out of raw data. Students will also learn to visibly identify and include the slack space associated with those files. As well as handle many File Systems like MAC, EXT2, EXT3 and More.

### **Advanced Acquisition**

This section will cover advanced data acquisition techniques in complex networked environments. As a digital investigator you will run across occasions when it is not feasible to shut down a system. Students will learn to map a basic network diagram and create an acquisition plan that will be the least intrusive to the operating environment.

### **Topics Include:**

- Back Up Tapes
- Evidence Preservation
- Testifying on Electronic Evidence
- Acquiring Mail Servers (Notes, Exchange)
- Acquiring Database Servers
- Large Data Stores
- Live Acquisition
- Acquiring Specialized Systems (SAS, PeopleSoft, etc.)
- Mainframe Basics and Acquisition Techniques

### **Computer Forensics Lab Setup**

Students will learn the requirements of setting up, maintaining and operating a computer forensics lab. This section will cover the physical requirements, Standard Operating Procedures (SOP), Access Control List (ACL) and Auditing. This section will also give the students a realistic look at the forensic hardware, software and peripherals to ensure maximum capability. Media storage, safeguards and lab specs are covered to ensure the integrity of digital evidence.

## **Data Hiding and Digital Encryption**

Students will learn the history of encryption and how encryption works in a digital environment today. This section will not only cover the most common forms of encryption, but will also expose students to techniques and tools to decrypt information that has been hidden.

## **Cryptographic Issues and Techniques for the Forensic Examiner**

This section will cover readily available encryption techniques used in email, documents, disks and other information. There are multiple hands on exercises during this section where students will learn how to defeat common encryption schemes. This section will cover password protected items, Encrypted File Systems (EFS) and other common methods of encryption used to protect or hide data. Students will learn the most successful techniques to use when an investigator is confronted with these hurdles.

Topics Include:

- Techniques for PGP
- Handling EFS (Encrypted File System)
- Preparing for WinFS
- Protected Storage Areas
- More..

## **Steganography**

Students will learn the history of steganography and how it is used to hide data in a digital environment today. This section has a number of hands on exercises where the students will learn to hide data and how to detect data that has been hidden. Some of the techniques covered in the lesson will be embedded information in images and sound files and information may be hidden in the Alternate Data Stream (ADS) of the NTFS operating system. These are areas that are not easily detectable and must be reviewed manually by the investigator.

## **Advanced Windows Investigations**

This section will take the students into the heart Microsoft's operating systems. Students will learn how to effectively retrieve valuable information from the Microsoft Windows Desktop and Server operating systems. Students will also learn the value of unique system identifiers that can link a suspect or computer system with an event or a particular object. This section will teach the students what historical data is contained with the system registry and where to locate that information.