

FOR606:

Drive and Data Recovery Forensics

Course Length: Five Days • 30 CPE Credits

The data recovery world and the forensics world are very close in relation. This class discusses topics valuable to both forensic and data recovery professionals alike and touches on data recovery topics relating to forensics topics where they can be applied.

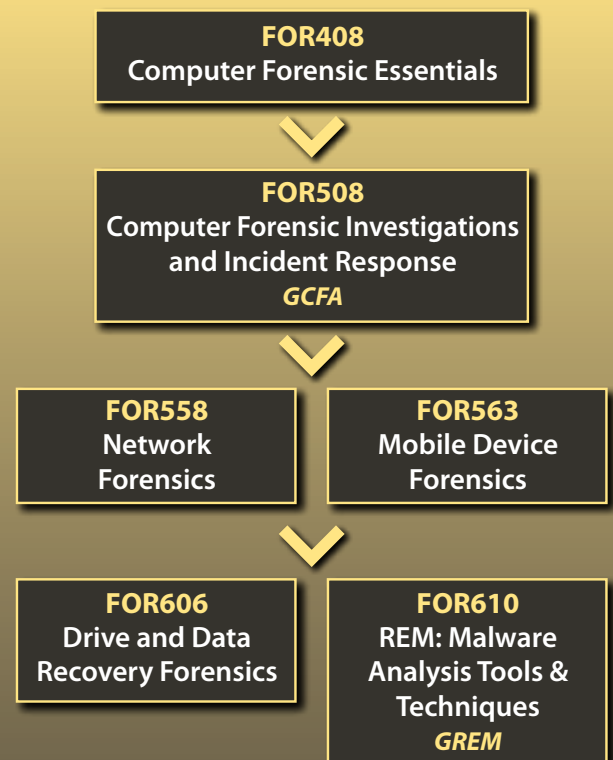


To produce valid disk images and recover the data from marginally operative or defective media for use in data recovery or forensics.

The processes and methodologies taught in this class will train you to collect an image on damaged evidence where standard forensic imaging would have failed. You will learn to understand what kinds of problems hard drives have and what your options are to recover the contents. Specialized data recovery trade secrets that are used in these processes specifically will be discussed so we can acquire data from damaged disks. We will perform some exciting labs, where you will format a hard drive, put data on the drive, disassemble the drive down to the bare metal, and then “successfully” reassemble the drive and recover your data from it.

This class will highlight the tools that work well with corrupted file systems, both in demonstration and in the lab exercises, and students will learn the basics of file systems and logical recoveries. There will be information regarding FAT, NTFS, Mac OSX HFS+ hard drive formats, as well as EXT3 and Reiser recoveries and what to do when there is damage, and there will be examples of each in labs. Students will also perform logical recoveries where we will use software and specialized data recovery equipment to image memory sticks, hard drives, and image files.

If you would like five bootcamp days of training and learning about trade secrets of the data recovery profession, this is the class for you. It will consist of lecture and labs with mentoring on disassembly and reassembly of the hard drives. Usually by the second day, the majority of students are able to rebuild a hard drive and recover data from it. However, this class is about process and methodologies, teaching the techniques used in data recovery labs so that you can understand and build on those skills.



Additional Forensics Courses

FOR526: Advanced Filesystem Recovery & Memory Forensics

SANS Forensic Curriculum

SANS forensic line-up features courses both for those who are new to the field as well as for seasoned professionals. Come learn from true industry experts and experience forensics in a hands-on, immersion style environment. By the time you complete a course, you will be able to put your knowledge to work when you get back to the office.

Fight Crime. Unravel Incidents one byte at a time.

The SANS Investigative Forensic Toolkit (SIFT) Essentials

<http://forensics.sans.org/sift-kit/essentials.php>

The SANS Investigative Forensic Toolkit (SIFT) Essentials are available at an extra cost with purchase of this course. The entire kit will enable each new investigator to accomplish proper and secure examinations of SATA, IDE, or Solid State Drives (SSD).

- **Tableau T35e Write Blocker Kit**
 - One Tableau T35e Write Blocker (Read-Only)
 - IDE Cable/Adapters
 - SATA Cable/Adapters
 - FireWire and USB Cable Adapters
 - Forensic Notebook Adapters (IDE/SATA)
 - HELIX Incident Response & Computer Forensics Live CD
- SANS Windows XP Forensic Analysis VMware Workstation
- Course DVD: Loaded with case examples, tools, and documentation

Who Should Attend

- Anyone that has ever tried to image a hard drive with bad blocks only to have it fail and never be able to get a good image of the drive. This class teaches you what your options are and how to avoid that situation as well as training for the tools.
- Corporations that handle large amounts of data and hard drives.
- Corporation that have a mobile force that uses laptops that have had damaged drives that needed to recover data from.
- Sensitive locations where a drive might not be able to be sent out to a recovery firm and you are required to recover the data from the damaged or corrupt drive.
- System administrators and incident handling personnel who are looking for an understanding of how a hard drive actually works and are interested in reassembling one from the ground up. This will help strengthen your forensic knowledge and give you a fundamental knowledge about how hard drives work and how to fix one.
- Anyone who wants to understand the technical side of hard drives and the data existing on the drive and how to rebuild or put one back together again.
- Anyone who wants to learn how to do data recovery on a damaged hard drive and to collect best evidence.
- To learn the basic tools and functions of data recovery to analyze Windows, Mac OS X and Linux systems with damaged hard drives or corrupt data.
- Anyone who wants to learn how files systems are structured and store their data so that they can understand where evidence exists on any type of hard drive.

Prerequisites

SANS encourages you to attend FOR508 (Computer Forensics Investigation and Incident Response) prior to attending this class.

Extra Items Needed

Digital Camera is helpful for the students to have during disassembly of the Hard Drive. A camera is helpful for documenting the process and knowing how the parts fit together after they are disassembled.

SANS Computer Forensic and e-Discovery Website

The learning doesn't end when class is over. SANS Computer Forensic and e-Discovery Website is a community focused site offering digital forensics professionals a one-stop forensic resource to learn, discuss and share current developments in the field. It also provides information regarding SANS forensics training, GIAC certification, and upcoming events. Visit <http://computer-forensics.sans.org>. New content is added regularly, so please visit often. And don't forget to share this information with your fellow forensic professionals.

FOR408: Computer Forensic Essentials

This course focuses on the essentials that a forensic investigator must know to investigate core computer crime incidents successfully. You will learn how computer forensic analysts focus on collecting and analyzing data from computer systems to track user-based activity that could be used internally or in civil/criminal litigation.

FOR558: Network Forensics

Network equipment such as web proxies, firewalls, IDS, routers and even switches often contain evidence that can make or break a case. A great deal of evidence flows across the network but is never stored on a workstation or server hard drive. In this class, law enforcement and information security professionals will learn how to recover evidence from network-based devices in order to speed up investigations and build stronger cases.

FOR563: Mobile Device Forensics

Mobile device forensics is a rapidly evolving field, creating exciting opportunities for practitioners in corporate, criminal, and military settings. Written for students who are both new to and already familiar with mobile device forensics, this hands-on course provides the core knowledge and skills that a digital forensic investigator needs to process cell phones, PDAs, and other mobile devices.

FOR610: REM: Malware Analysis Tools and Techniques (GREM)

Expand your capacity to fight malicious code by learning how to analyze bots, worms, and trojans. This recently expanded, four-day course discusses practical approaches to examining malware using a variety of system monitoring utilities, a disassembler, a debugger, and other tools useful for reverse-engineering malicious software. You don't have to be a full-time malware searcher to benefit from this course – as organizations increasingly rely on their staff to act as first responders during a security incident – malware analysis skills are becoming increasingly important.