

SEC508: Computer Forensics, Investigation, and Response

Course Length: Six Days • 6 CPE Credits/Day
Laptop Required

SEC508: COMPUTER FORENSICS, INVESTIGATION, AND RESPONSE will give you a firm understanding of computer forensics tools and techniques to investigate data breach intrusions, tech-savvy rogue employees, and complex digital forensic cases.



Unpatched, unprotected computers connected to the internet are compromised in less than three days!

Forensic investigators must master a variety of operating systems, investigation techniques, incident response tactics, and even legal issues in order to solve challenging cases.

SEC508: COMPUTER FORENSICS, INVESTIGATION, AND RESPONSE will teach you critical forensic analysis techniques and tools in a hands-on setting for both Windows- and Linux-based investigations.

We will examine various investigation methodologies and techniques, discovering new places to find evidence and discover the tracks of a cyber criminal or hacker, who is trying to stay hidden on your systems

Learning more than just how to use a forensic tool, you will be able to demonstrate how the tool functions step-by-step. You will become skilled with new tools, such as the Sleuthkit, Foremost, and the HELIX3 Pro Forensics Live CD. This SANS hands-on technical course arms you with a deep understanding of the forensic methodology, tools, and techniques to solve advanced computer forensics cases.



<http://forensics.sans.org>

SEC408
Computer Forensic
Essentials



SEC508
Computer Forensics,
Investigation,
and Response
GCFA



SEC558
Network
Forensics

SEC563
Mobile Device
Forensics



SEC606
Drive and Data
Recovery Forensics

SEC610
REM: Malware
Analysis Tools &
Techniques
GREM

Additional Forensics Courses

SEC526: Advanced Filesystem Recovery &
Memory Forensics *STAR*

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.

Free SANS Investigative Forensic Toolkit (SIFT) Advanced

As a part of this course you will receive a SANS Investigative Forensic Toolkit (SIFT) Advanced, you will gain first-hand experience in collecting and analyzing evidence recovered from a system under investigation. The toolkit consists of:

- Hard Drive USB mini adapter kit for SATA/IDE hard drives 1.8"/2.5"/3.5"/5.25" (Read and Write)
- SANS VMware based Forensic Analysis Workstation
- Course DVD loaded with case examples, tools, and documentation
- Best-selling book "File System Forensic Analysis" by Brian Carrier
- New Addition! The SIFT Kit Advanced will now include a single version Helix3 Pro that will be individually licensed to each student.
 - Works on Mac OS X, Windows, and Linux.
 - Simplified Live Analysis with both Memory and Disk Acquisition
 - Built in Memory Analysis
 - Boots most Intel x86 machines including Mac OS X

Prerequisites

It is strongly recommended that each student attend SEC408: Computer Forensic Essentials prior to taking this course. This course is a perfect follow on for those that have already attended SEC408: Computer Forensic Essentials. If you are just beginning in computer forensics or information security, then this course is not appropriate for you as the basics of computer forensics, system administration, and hacker techniques will not be covered.

Who Should Attend

- **Law enforcement officers, federal agents, or detectives** who want to master computer forensics and expand their investigative skillset to include data breach investigations, intrusion cases, and tech-savvy cases
- **Incident response team members** who are responding to complex security incidents/intrusions and need to utilize computer forensics to help solve their cases
- **Computer Forensic professionals** who want to solidify and expand their understanding of file system forensic and incident response related topics
- **Information security professionals** with some background in hacker exploits, penetration testing, and incident response
- **Information security managers** who would like to master digital forensics in order to understand information security implications and potential litigation related issues or manage investigative teams
- **Anyone with a firm technical background** who might be asked to investigate a data breach incident, intrusion case, or WHO investigates individuals that are considered technically savvy

Course Topics

- Data Breach Cases, Intrusion Analysis, and Advanced Investigative Strategy
- Evidence Acquisition/Analysis/Preservation Laws and Guidelines
- U.S. Laws Investigators Should Know
- E.U. Laws Investigators Should Know
- Forensic Reports and Testimony
- Computer Forensics Methodology
- File System Essentials
- Linux/Unix File System Examination
- Windows FAT File System Examination
- Windows NTFS File System Examination
- Key Forensic Acquisition/Analysis Concepts
- Volatile Evidence Gathering and Analysis
- Image File Conversion (E01, Raw, AFF)
- Windows System Restore and Shadow Volume Copy Exploitation
- Evidence Integrity and Chain of Custody
- Forensic Evidence Acquisition and Imaging
- File System Timeline Analysis
- Forensic Analysis Key Methods
- File System and Data Layer Examination
- Metadata and File Name Layer Examination
- File Sorting and Hash Comparisons
- Live Response and Volatile Evidence Collection
- Key Windows File System Analysis Concepts
- Windows Registry Analysis
- Windows Internal File Metadata
- Application Footprinting and Software Forensics
- Automated GUI Based Forensic Toolkits

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://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.



GIAC Certified Forensics Analyst (GCFA)

GIAC Certified Forensic Analysts (GCFAs) have the knowledge, skills, and abilities to handle advanced incident handling scenarios, legally collect and secure evidence, conduct incident investigations, perform Electronic Evidence Discovery (EED), write forensic reports that can be utilized in litigation, and legally carry out forensic investigation of computers, networks, and hard drives.

Top Four Reasons to Earn a GIAC GCFA Certification

1. GCFA certification has been recognized and accepted in courts around the world for expert witness testimony.
2. GCFA certification helps Forensic personnel get promoted faster and earn more money.
3. GCFA certification reinforces and affirms your 'hands-on' forensic knowledge.
4. GCFA certified personnel know how to respond to and perform Electronic Evidence Discovery using their forensic skills.

Learn more about GIAC at www.giac.org.