

FOR526: Advanced Filesystem Recovery and Memory Forensics

Course Length: One Day • 6 CPE Credits
Laptop Required

If you understand forensic filesystem fundamentals, then this course is for you. It moves quickly from covering memory forensics to recovering and discovering deleted partitions from hard drives.



This advanced course is perfect for the diligent student familiar with core forensic methodology and techniques.

This course focuses on innovative forensic techniques and methodologies so the seasoned practitioner can keep his skills sharp and up-to-date with the latest research areas in both live and static based disk forensics.

You will receive:

- Forensic analysis workstation VMware machine equipped to investigate forensic data
- Course DVD loaded with case examples, tools, and documentation

Prerequisites

This advanced course is perfect for the diligent student conversant with file system forensic techniques. If you are just beginning in digital forensics, this course is not appropriate for you, as the basics of digital forensics will not be covered.

Who Should Attend

- System administrators and incident handling personnel who are trying to further their knowledge in the latest forensic techniques
- Anyone who wants to learn how file system partitions are structured
- Anyone who wants to learn how to recover lost partitions from a physical disk image
- Anyone who wants to learn how to forensically recover artifacts from memory collected from a machine

SANS Computer Forensic and e-Discovery Website

The learning doesn't end when class is over. SANS Computer Forensic and e-Discovery Web site 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.



<http://computer-forensics.sans.org>

FOR408
Computer Forensic Essentials



FOR508
Computer Forensic Investigations
and Incident Response
GCFA



FOR558
Network
Forensics

FOR563
Mobile Device
Forensics



FOR606
Drive and Data
Recovery Forensics

FOR610
REM: Malware
Analysis Tools &
Techniques
GREM

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.