SANS

Digital Forensics

CURRICULUM

SIFT Workstation Tips and Tricks Plus Free Resources Inside!

Fight Crime.

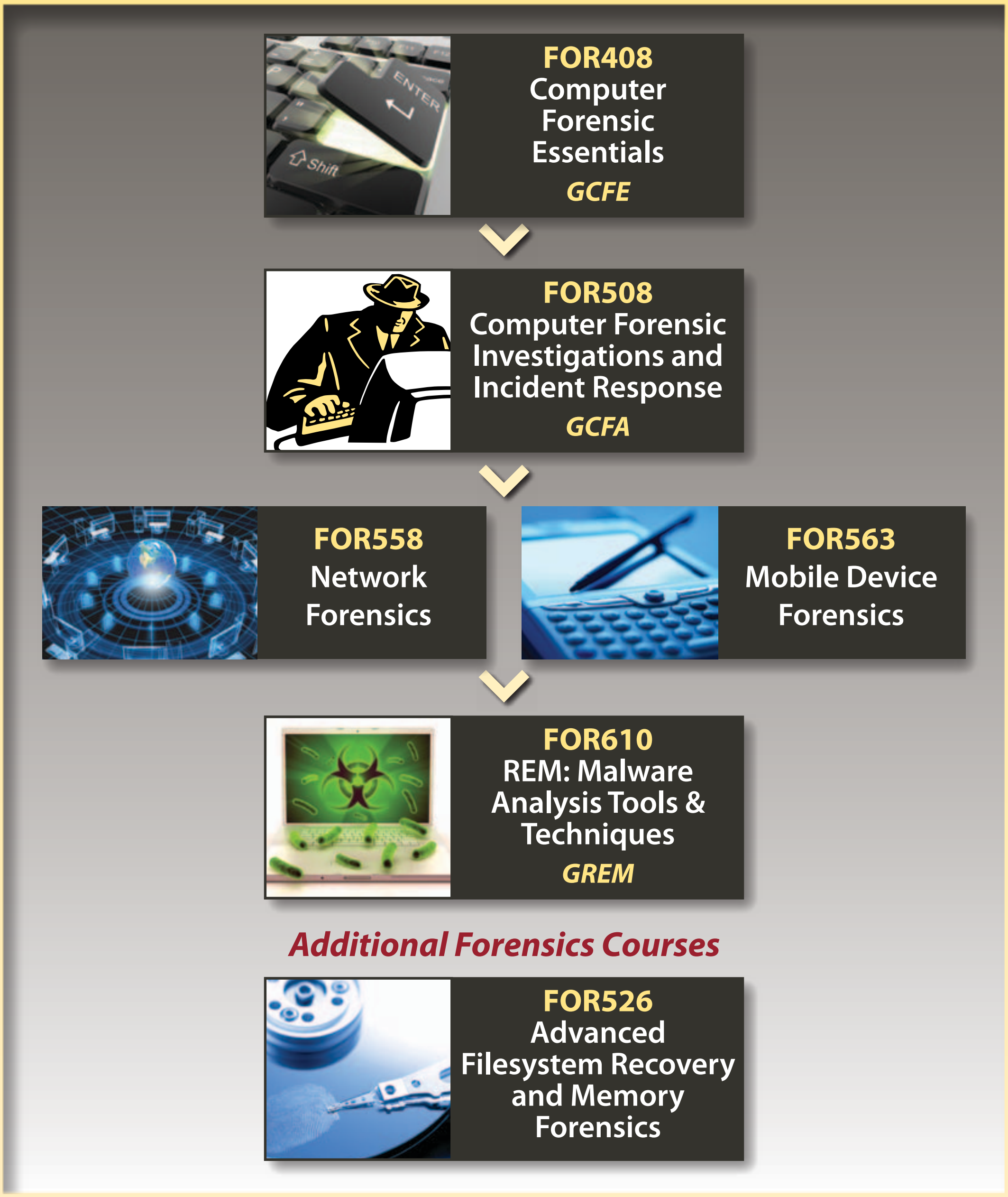
Unravel incidents...

one byte at a time.

http://computer-forensics.sans.org

SANS Forensics Curriculum

SANS forensics 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.



FOR408
Computer Forensic Essentials
GCFE

FOR508
Computer Forensic Investigations and Incident Response
GCFA

FOR558
Network Forensics

FOR563
Mobile Device Forensics

FOR610
REM: Malware Analysis Tools & Techniques
GREM

Additional Forensics Courses

FOR526
Advanced Filesystem Recovery and Memory Forensics

SANS COMPUTER FORENSICS
and e-Discovery with Rob Lee

http://computer-forensics.sans.org

Fight Crime. *Unravel Incidents one byte at a time.*

Dear Colleague,

Rob Lee

With today's ever-changing technologies and environments, it is inevitable that organizations will deal with some form of cyber crime. These forms include, but are not exclusive to, fraud, insider threat, industrial espionage, and phishing. In order to help solve these cases, organizations are hiring digital forensic professionals and calling law enforcement agents to fight and solve these cyber crimes.

Over the past year, digital crime has increased. This clearly indicates that criminal and hacking groups are racking up success after success. Organized crime groups utilizing botnets are exploiting ACH fraud daily. Similar groups are penetrating banks and merchants stealing credit card data. Fortune 500 companies are beginning to detail data breaches and hacks in their annual stockholders reports.

The adversaries are getting better, bolder, and their success rate is impressive, but are we as cyber crime fighters able to keep up?

Bottom line, we can do better. We need to develop a field full of sophisticated incident responders and forensic investigators. We need lethal forensicators that can detect and eradicate advanced threats immediately. A properly trained incident responder could be the only defense your organization has during a compromise. As a forensic investigator, you need to know what you are up against. You need to know what the seasoned experts in the field know. You need to stay ahead, constantly seeking new knowledge and experience, and that's what SANS courses will teach you.

The SANS Digital Forensics Curriculum brings together top professionals that have developed the industry's leading innovative courses for digital forensics and in-depth specialty training. My goal is to continue to offer the most rewarding training to each individual. We will arm you with the tools to fight crime and solve complex digital forensic cases the day after you leave class. I aim to push each investigator's knowledge with advanced skills and techniques to help successfully investigate and defend organizations from sophisticated attacks.

Finally, listed in this catalog are resources to help you stay abreast of the ongoing changes to the industry, recent tool releases, and new research. We have over 70 authors that contribute to the SANS Digital Forensics Blog, so check it often for the latest digital forensics information. We have released the popular SIFT Workstation as a free download available on the SANS Forensics website **computer-forensics.sans.org**. Our aim is to provide not only the best training, but also community resources for this growing field.

Looking forward to seeing you at our conferences and training events.

Best regards,

Rob Lee
SANS Faculty Fellow

CONTENTS

FOR408 Computer Forensic Essentials

Six-Day Course
36 CPE Credits
Laptop Required

Who Should Attend

- Information technology professionals who wish to learn core concepts in computer forensics investigations and e-discovery
- Law enforcement officers, federal agents, or detectives who desire to be introduced to core forensic techniques and topics
- Information security managers who need a digital forensics background in order to manage investigative teams and understand the implications of potential ligation-related issues
- Information technology lawyers and paralegals who need to understand the basics of digital forensic investigations
- Anyone interested in computer forensic investigations with some background in information systems, information security, and computers

@sansforensics
http://blogs.sans.org/computer-forensics

Master Windows-based computer forensics. Learn essential investigation techniques.

With today's ever-changing technologies and environments, it is inevitable that organizations will deal with some form of cyber crime, such as computer fraud, insider threat, industrial espionage, or phishing. As a result, many organizations are hiring digital forensic professionals and are callling cyber crime law enforcement agents to help fight and solve these types of crime.

FOR408: Computer Forensic Essentials 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.

This course covers the fundamental steps of the in-depth computer forensic methodology so that each student will have the complete qualifications to work as a computer forensic investigator in the field helping solve and fight crime. This is the first course in the SANS Computer Forensic Curriculum. If you have never taken a SANS forensics course before, we recommend that you take this introductory course first to set a strong foundation for the full SANS Computer Forensic Curriculum.

With this course, you will receive a FREE SANS Investigative Forensic Toolkit (SIFT) Essentials with a Tableau Write Block Acquisition Kit.

The entire kit will enable each investigator to accomplish proper and secure examinations of SATA, IDE, or Solid State Drives (SSD). The toolkit consists of:

- One Tableau T35es 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
- Fully functioning tools that include working with Access Data's Forensic Toolkit (FTK)
- Course DVD: Loaded with case examples, tools, and documentation

GIAC Certified Forensic Examiner
www.giac.org

STI Masters Program
www.sans.edu

Delivery Methods
Live Events • Mentor • OnSite

SANS Computer Forensic Web site http//computer-forensics.sans.org
The learning does not end when class is over. SANS Computer Forensic 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.

408.1 *Hands On:* Forensic and E-Discovery Fundamentals

Investigations begin with a firm knowledge in proper evidence acquisition and analysis. Digital Forensics is more than just using a tool that automatically recovers data. You must focus on the facts to seek the truth. Digital Forensics requires analytical skills. Today you will learn how the professionals accomplish digital forensics.

Topics: Purpose of Forensics; Discussion Major Case Types; Types of Electronic Stored Information; Location of Electronically Stored Evidence (ESI); Evidence Collection Order of Volatility; Hard Drive Basics; File System Basics; Evidence Fundamentals; Reporting and Presenting Evidence; Forensic Methodology

408.2 *Hands On:* Evidence Acquisition and Analysis

You will learn proper evidence acquisition, integrity, and handling skills of logical, physical, and system memory utilizing the Tableau T35es write blocker. Moving quickly from evidence acquisition, you will begin your investigation using cutting-edge tools that the pros use.

Topics: Evidence Acquisition Basics; Preservation of Evidence; Types of Acquisition; Forensic Field Kits; Full Disk Image Acquisition Tools and Techniques; Network Acquisition; Graphical Forensic Tools; Traditional Tasks Utilized Using the Forensic Tools; Recover Deleted Files

408.3 *Hands On:* E-Mail and Registry Analysis

Beginning with host, server, and webmail forensics the investigator will learn how to recover and analyze the most popular form of communication. The second focus centers on Windows XP, Vista, and Windows 7 Registry Analysis and USB Device Forensics.

Topics: E-mail Forensics; Registry Forensics In-Depth

408.4 *Hands On:* Artifact and Log File Analysis

Hundreds of files are created by actions of the suspect. Learn how to examine key files such as link files, the windows prefetch, pagefile/system memory, and more. The latter part of the day will center on examining the Windows log files and the usefulness in both simple and complex cases.

Topics: Memory, Pagefile, and Unallocated Space Analysis; Forensicating Files Containing Critical Digital Forensic Evidence; Windows Event Log Digital Forensic Analysis

408.5 *Hands On:* Web Browser Forensics

Internet Explorer and Firefox Browser Digital Forensics. Learn how to examine exactly what an individual did while surfing via their Web browser. The results will give you pause the next time you use the Web.

Topics: Browser Forensics

408.6 *Hands On:* Forensic Challenge and Mock Trial

Windows Vista/7 Based Digital Forensic Challenge. There has been a murder-suicide and you are the investigator assigned to process the hard drive. This day is a capstone for every artifact discussed in the class. You will use this day to solidify the skills you have learned over the past week.

Topics: Digital Forensic Case; Mock Trial

FOR508 Computer Forensic Investigations and Incident Response

Six-Day Program
36 CPE Credits
Laptop Required

Who Should Attend

- Incident response team members that respond to complex security incidents/intrusions and need computer forensics to help solve their cases
- Computer forensic professionals who want to solidify and expand their understanding of file system forensics and incident response related topics
- Law enforcement officers, federal agents, or detectives who want to master computer forensics and expand their investigative skill set to include data breach investigations and intrusion cases
- Information security professionals with some background in hacker exploits, penetration testing, and incident response
- Information security managers who would like to master digital forensics to understand information security implications and potential litigation or manage investigative teams

GCFA

ANSI/ISO 17024 Accredited
GIAC Certified Forensic Analyst
www.giac.org

STI Masters Program
www.sans.edu

Cyber Guardian Program
www.sans.org/cyber-guardian

@sansforensics
http://blogs.sans.org/computer-forensics

Upgrade your forensic skills. Learn to investigate and respond to the advanced persistent threat and hackers hired by organized crime.

Sensitive data and intellectual property is stolen from systems that are protected by sophisticated network and host-based security. A motivated criminal group or nation state can and will always find a way inside enterprise networks. In the commercial and government sectors, hundreds of victims responded to serious intrusions costing millions of dollars and loss of untold terabytes of data. Cyber attacks originating from China dubbed the Advanced Persistent Threat have proved difficult to suppress. FOR508 will help you respond to and investigate these incidents.

This course will give you a firm understanding of advanced incident response and computer forensics tools and techniques to investigate data breach intrusions, tech-savvy rogue employees, advanced persistent threats, and complex digital forensic cases.

Utilizing advances in spear phishing, Web application attacks, and persistent malware, these new sophisticated attackers advance rapidly through your network. Incident responders and digital forensic investigators must master a variety of operating systems, investigation techniques, incident response tactics, and even legal issues in order to solve challenging intrusion cases. FOR508 will teach you critical forensic analysis techniques and tools in a hands-on setting for both Windows- and Linux-based investigations.

Attackers will use anti-forensic techniques to hide their tracks. They use rootkits, file wiping, timestamp adjustments, privacy cleaners, and complex malware to hide in plain sight, avoiding detection by standard host-based security measures. Everything will leave a trace; you merely need to know where to look.

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

FIGHT CRIME. UNRAVEL INCIDENTS... ONE BYTE AT A TIME.

Delivery Methods
Live Events • Mentor • OnDemand • OnSite • vLive! • SelfStudy

Computer Forensic Investigations and Incident Response is one of SANS' most advanced and challenging courses. People with GCIA and GCFA certifications often land some of the most challenging jobs in information security. They have solved crimes that have appeared on the evening news.

508.1 *Hands On:* Forensic and Investigative Essentials

Beginning the first day, you will learn the proper methodology of investigating complex and advanced digital crimes and intrusions. Utilizing real-world intrusion scenarios, you will see how to respond to complex attacks through teaching you the background of how data is stored on a variety of operating systems. This knowledge will allow you to see beyond most anti-forensic techniques allowing you to gain the advantage while responding to breaches in your organization.

Topics: Computer Forensics for Incident Responders; Incident Response and Forensics; File System Essentials; Linux/Unix File System Fundamentals; Windows FAT and exFAT File System Fundamentals; Windows NTFS File System Fundamentals

508.2 *Hands On:* Live Response and Complex Evidence Acquisition

Computer Forensic Investigators should be conversant with network and file system forensics in addition to being armed with the latest in incident response tools and methodologies. Day two, you will learn how to respond to complex situations to collect crucial evidence using: Memory Acquisition, Live Response Techniques, and Complex Evidence Acquisition.

Topics: Key Forensic Acquisition/Analysis Concepts; Volatile Evidence Gathering and Analysis; Unix and Windows Live Response; Windows Incident Response Methodology; Evidence Integrity; Complex Forensic Evidence Acquisition and Imaging

508.3 *Hands On – Part 1:* File System Forensic Analysis

Investigating intrusion cases are challenging even for the seasoned investigator. Hackers will try to evade detection and utilize wiping and other anti-forensic techniques to avoid leaving a trail on the host and network. In order to investigate intrusion cases, you have to have a firm grasp of low-level forensic capabilities in both commercial and open-source tools. Understanding of the various layers of the file system will allow you to move beyond being an average investigator into one that could recover data "by hand" if necessary. To accomplish this, we cover the Sleuthkit in the course.

Topics: Filesystem Timeline Analysis; File System and Data Layer Examination, Metadata Layer Examination; File Name Layer Examination; File Sorting and Hash Comparisons; Automated GUI Based Forensic Toolkits

508.4 *Hands On – Part 2:* File System Forensic Analysis

Utilizing advances in spear phishing, Web application attacks, and persistent malware, these new sophisticated attackers advance rapidly through your network. Forensic investigators must master a variety of operating systems, investigation techniques, and incident response tactics to solve challenging cases. Recovering data that was skillfully removed can still be accomplished once an investigator knows the right places to look. This day of the course introduces the investigator to some of the most cutting-edge areas of computer forensics discovered over the past year. Shadow Volume/Restore Point Examinations, Super Timeline Analysis, and Advanced Registry Examinations are all covered during the day.

Topics: Key Windows File System Analysis Concepts; Intermediate/Advanced Windows Registry Analysis; Windows XP Restore Point Analysis; VISTA , Windows 7, Server 2008 Shadow Volume Copy Analysis; Super Timeline Analysis; Recovery Key Windows Files; Finding Unknown Malware; Step-By-Step Methodology to Analyze and Solve Challenging Cases

508.5 *Hands On:* Computer Investigative Law for Forensic Analysts

Legal issues, especially liability, remain foremost in the minds of an incident handler or forensic investigator; therefore, this class has more discussion than any other we offer. Learn to investigate incidents while minimizing the risk for legal trouble. This course is designed not for management, but for the individuals actually performing a computer-based investigation. The content focuses on challenges that every investigator needs to understand before, during, and post investigation. Since most investigations could potentially bring a case to either a criminal or civil courtroom, it is essential for you to understand how to perform a computer-based investigation legally and ethically.

Topics: Who Can Investigate and Investigative Process Laws; Evidence Acquisition/Analysis/Preservation Laws and Guidelines; U.S. Laws Investigators Should Know; E.U. Laws Investigators Should Know; Presenting Data; Forensic Reports and Testimony

508.6 *Hands On:* Advanced Forensics & the Forensic Challenge

Learn how to discover new artifacts using application forensics. Put your new skills to test with a capstone investigation called the Forensic Challenge.

Topics: Application Footprinting and Software Forensics; • The Forensic Challenge

Free SANS Investigative Forensic Toolkit (SIFT) – *See page 2 for contents.*

FOR558

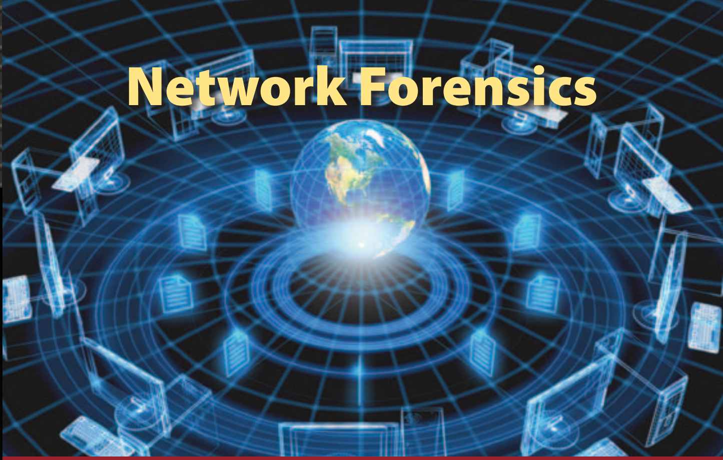
Five-Day Program
30 CPE Credits

Who Should Attend

- Network and/or computer forensic examiners
- Computer incident response team members
- Security architects
- Security administrators
- Law enforcement
- Anyone responsible for orchestrating a corporate or government network for evidence acquisition in the face of a criminal or civil investigation

PREREQUISITE: Students should have some familiarity with basic networking fundamentals, such as the OSI model and basics of TCP/IP. Please ensure that you can pass the SANS TCP/IP & Hex Knowledge quiz. Students should also have basic familiarity with Linux or willingness to learn in a Linux-based environment.

Network Forensics



Recover and Analyze Evidence from Network-based Devices such as Web Proxies, Firewalls, IDS, and Routers: "No hard drive? No problem!"

"CATCHING HACKERS ON THE WIRE." Enterprises all over the globe are compromised remotely by malicious hackers each day. Credit card numbers, proprietary information, account usernames, passwords, and a wealth of other valuable data are surreptitiously transferred across the network. Insider attacks leverage cutting-edge covert tunneling techniques to export data from highly secured environments. Attackers' fingerprints remain throughout the network in firewall logs, IDS/IPS, Web proxies, traffic captures, and more.

This course will teach you how to follow the attacker's footprints and analyze evidence from the network environment. Network equipment, such as Web proxies, firewalls, IDS, routers and switches, contains evidence that can make or break a case. Forensic investigators must be savvy enough to find network-based evidence, preserve it, and extract the evidence. You will gain hands-on experience analyzing covert channels, carving cached Web pages out of proxies, carving images from IDS packet captures, and correlating the evidence to build a solid case. We will dive right into covert tunnel analysis, DHCP log examination, and sniffing traffic. By day two, you'll be extracting tunneled flow data from DNS NULL records and extracting evidence from firewall logs. On day three, we analyze Snort captures and the Web proxy cache. You'll carve out cached Web pages and images from the Squid Web proxy. The last two days, you'll be part of a live hands-on investigation. Working in teams, you'll use network forensics to solve a crime and present your case.

During hands-on exercises, we will use tools, such as tcpdump, Snort, ngrep, tcpxtract, and Wireshark, to understand attacks and trace suspect activity. Each student will be given a virtual network to analyze and will have the opportunity to conduct forensic analysis on a variety of devices. Underlying all of our forensic procedures is a solid forensic methodology. This course complements FOR508: Computer Forensic Investigations and Incident Response, using the same fundamental methodology to recover and analyze evidence from network-based devices.

@sansforensics
http://blogs.sans.org/computer-forensics

Delivery Methods
Live Events • OnSite • Community

558.1 *Hands On:* Passive Evidence Acquisition and Analysis

On the first morning, we'll investigate a rogue system administrator. His colleagues suspect he may be abusing his privileges. There doesn't seem to be any Web surfing activity at all associated with his computers. What could he be up to? To solve the case, we embark together on an extensive analysis of DHCP logs, wireless traffic captures, tcpdump using BPF filters, Wireshark, and the DNS protocol. Along the way, we'll learn about DNS tunneling using iodine, methods of passive evidence acquisition, network taps, hubs, switches, and port mirroring. We'll also use tools, such as ngrep, tcpxtract, and hex editors, to extract the data we need. Underlying all of our forensic procedures is a solid forensic methodology, which includes verification, acquisition, timeline creation, evidence recovery, and reconstruction.

Topics: Case Study: Data Tunneling; The OSI Model for Network Analysis; DHCP & MAC Address Analysis; Passive Evidence Acquisition; Network Evidence Extraction & Analysis

558.2 *Hands On:* Active Evidence Acquisition and Covert Tunnels

We'll begin with covert ICMP and DNS tunnels. You'll extract tunneled TCP and IP packets from DNS NULL records and use active evidence collection methods to uncover the rogue system administrator's secret plot! By the afternoon, we'll conduct hands-on active evidence acquisition. You'll inspect router ARP tables and firewall logs. Volatility and collection methods vary depending on configuration, manufacturer, and the environment. We'll also cover ways that investigators can compensate for less-than-ideal network environments, using publicly available forensic evidence acquisition tools.

Topics: Data Tunneling In-Depth; A Formal Network-Based Investigative Methodology; Active and Interactive Evidence Acquisition

558.3 *Hands On:* Firewalls, IDS, Proxies, and Data Reconstruction

Active evidence acquisition is the focus of day three. We'll analyze IDS/IPS, central logging servers, and Web proxies such as Squid, during hands-on exercises throughout the day. By the end of day three, students will be using hex editors to carve cached evidence out of Web proxies and reconstruct Web surfing histories using only the central Web proxy logs.

Topics: Network Log Analysis In-Depth; Network Intrusion Detection & Analysis with Snort; Web Proxies, Encryption, & SSL Interception

558.4 *Hands On:* Network Forensics Unplugged

At the beginning of the day, we will discuss wireless access point investigations and then learn about techniques for presenting digital evidence in court. After lunch, we will begin our Capstone Case Study in which students will work as investigative teams, presented with a realistic scenario and a virtual network. You will identify sources of evidence, collect the evidence, reconstruct content, solve the crime, and present your analysis in "court."

Topics: Wireless Access Point Investigations; Digital Evidence Court Primer; Capstone Case Study: Investigate a Crime and Present the Evidence

558.5 *Hands On:* Capstone Investigation

Working in investigative teams, students will use forensic analysis tools to build a coherent picture of the crime. We will investigate by carving files out of raw network traffic and extracting sensitive data hidden in ICMP payloads. We will trace the attack to its source by correlating activity with firewall logs, central server logs, IDS logs, and other network-based evidence. Finally, we will identify one of our suspects by reconstructing cached Web content, analyzing DHCP logs, and implementing passive OS fingerprinting techniques. After using this evidence to build a solid case, we will develop a cohesive picture of the crime and discuss techniques for presenting supporting evidence in deposition.

Topics: Capstone Case Study: Investigate a Crime and Present the Evidence, cont.; Trace the Attack to its Source by Correlating: Firewall Logs, Central OS Logs, IDS Logs, and more; Reconstruct Web Histories and Cached Web Content; Analyze DHCP Logs; Fingerprint a Suspect's Computer; Identify the Suspect using Network-based Evidence; Build a Case and Discuss Techniques for Presenting in Court

FOR563 Mobile Device Forensics

Five-Day Program
30 CPE Credits
Laptop Reguired

Who Should Attend

- Information security professionals responsible for investigating misuse of mobile devices by employees and for responding to attacks against and theft of mobile devices
- Forensic investigators who want to process mobile devices in a forensically sound manner and use the resulting evidence in their work
- IT managers who need to understand the relevance of mobile devices in security breaches, policy violations, criminal activities, civil suits, and any resulting proceedings
- IT auditors who need tools and techniques for investigating mobile devices to ensure they are not being misused in a way that puts an organization at risk
- Law enforcement agents who need to extract information from mobile devices in a wide variety of crimes
- Attorneys who need an understanding of the types of evidence that can be extracted from mobile devices, the forensic process, legal issues (e.g., privacy, authentication, integrity), and how the findings can be used to build/strengthen a case

Criminals be warned: Anything you text will be used against you.

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. Using state-of-the art tools, you will learn how to forensically preserve, acquire, and examine data stored on mobile devices and utilize the results for internal investigations or in civil/criminal litigation.

With the increasing prevalence of mobile devices, digital forensic investigators are encountering them in a wide variety of cases. Investigators within organizations can find stolen data and incriminating communications on devices used by rogue employees. In civil and criminal cases, investigators can extract useful evidence from mobile devices, can get a clearer sense of which individuals were in cahoots, and can even show the location of key suspects at times of interest. IT auditors, managers, and lawyers all need to understand the vast potential of mobile device forensics.

By guiding you through progressively more intensive exercises with mobile devices, we familiarize you with the inner workings of these devices and show you the benefits and limitations of various approaches and tools. The combination of teaching skills and knowledge will enable you to resolve investigations. The capstone exercise at the end of this course is designed to hone your mobile device forensics skills and help you apply them to an actual investigation.

Laptops are required for this course. A variety of devices will be available for you to work with during the course. You are also encouraged to bring used mobile devices and SIM cards from home to experiment with using the tools and techniques in this course, but this is not required.

> *"This course was an informative, hands-on, and concise class that changed the way I look at security tools."*
>
> -Richard Salmon,
>
> Louisiana State Employee Retirement System

Delivery Methods
Live Events • OnSite

SANS Computer Forensic Web site http//computer-forensics.sans.org
The learning does not end when class is over. SANS Computer Forensic 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.

563.1 *Hands On:* Fundamentals of Mobile Device Forensics

The first day covers a review of technology from a forensic perspective, forensic handling of mobile devices, and manual examination of mobile devices. In delving into the underlying technology of mobile devices and wireless networks, we show you how the data they contain can be used as evidence. We will cover the core forensic methodology as it relates to mobile devices when conducting a manual triage inspection, logical forensic examination, and in-depth forensic analysis of physical memory. We show you how to interpret and utilize various identifiers and numbers associated with mobile devices, including MEID, IMEI, ICC-ID, and IMSI. Hands-on exercises include how to process mobile devices from a forensic perspective and obtain information that forensic tools may not provide.

Topics: Mobile Network Investigations; Mobile Device Forensics; Forensic Handling of Mobile Devices; Forensic Documentation; Interacting with Mobile Devices; Hands-on Exercises

563.2 *Hands On:* Windows Mobile Forensics

On this day, we'll go through a hands-on exploration of mobile device operating systems and data storage using manufacturer and developer utilities. We will perform forensic acquisitions and examinations of SIM cards to better understand how they store data, how to decode the data, the types of information they contain, and how that information can be useful in an investigation. You will use manufacturer and developer tools to gain a deeper understanding of mobile device internals.

Topics: Accessing Mobile Devices; Mobile Device Operating Systems; Mobile Device File Systems; Forensic Processing of SIM Cards; Forensic Examination of Data; Hands-on Exercises

563.3 *Hands On:* Cell Phone Forensics

We will use forensic tools to acquire and analyze logical data from mobile devices and then compare forensic acquisition tools and validate completeness and accuracy of results. No one tool can accomplish everything, and you need to be able to select the right tool for the job at hand. As day three progresses, we dig deeper into digital evidence on mobile devices, analyzing call logs, SMS/MMS, photos, and associated metadata. In addition, we demonstrate how to utilize e-mail, Web browsing, and other Internet activities on mobile devices in an investigation.

Topics: Forensic Acquisition Tools for Mobile Devices; Forensic Examination of Logical Data; Forensic Analysis of Internet Activities on Mobile Devices; Forensic Reconstruction of Activities on Mobile Devices; Hands-on Exercises

563.4 *Hands On:* Blackberry, Nokia, and iPhone

Acquiring full memory contents is one of the more challenging aspects of mobile device forensics and may not be feasible in all cases. We'll use forensic tools to acquire and analyze physical memory from mobile devices and then delve into memory contents and extract data structures on mobile devices. You'll learn how to confirm key findings by examining them in their original context in hexadecimal form. We demonstrate the various mechanisms for acquiring memory, including Flasher boxes, and assess their strengths and limitations from a forensic perspective. We will step you through the process of acquiring the full contents of physical memory from a mobile device.

Topics: Forensic Acquisition of Physical Memory; Forensic Acquisition of Using Flasher Boxes; Forensic Examination of Physical Memory; Hands-on Exercises

563.5 *Hands On:* Advanced Forensics and the Forensic Challenge

This last day familiarizes you with more complicated and costly forensic acquisition and analysis techniques. For instance, using specialized equipment for accessing circuit boards of mobile devices, it is possible to access data in memory directly. A realistic hands-on investigative scenario brings together lessons and techniques learned throughout the course. Even the most ingenious technical analysis becomes worthless, however, if it is not clearly presented to decision makers -- a manager, lawyer, or jury. We spend the final part of the course discussing effective approaches for presenting your findings to a non-technical audience.

Topics: Advanced Mobile Device Forensics Overview; Bringing It All Together; The Mobile Device Forensic Challenge; Hands-on Exercise

FOR610

Reverse-Engineering Malware: Malware Analysis Tools and Techniques

Five-Day Program
30 CPE Credits
Laptop Required

Who Should Attend

- Anyone whose job requires an understanding of key aspects of malicious programs
- Individuals with responsibilities in incident handling, forensic analysis, Windows security, and system administration
- Individuals responsible for supporting their organization's internal security needs
- Engineers from security product and service companies who are looking to deepen their malware analysis expertise

Prerequisites:

- Students should have a computer system that matches the stated laptop requirements. Some software needs to be installed before you come to class.
- Students should be familiar with using Windows and Linux operating environments and be able to troubleshoot general connectivity and setup issues.
- Students should be familiar with VMware Workstation and be able to create and configure virtual machines.
- Students are recommended to have a high-level understanding of key programming concepts, such as variables, loops, and functions; however, no programming experience is necessary.

GIAC Reverse Engineering Malware
www.giac.org

Malware Analysis, Tools, and Techniques: Turn malware inside-out

This popular five-day course discusses practical approaches to examining Windows malware using a variety of 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 become increasingly important.

By covering both behavioral and code analysis approaches, this unique course provides a rounded approach to reverse-engineering. As a result, the course makes malware analysis accessible even to individuals with a limited exposure to programming concepts. The materials do not assume that the students are familiar with reverse-engineering; however, the difficulty level of concepts and techniques increases quickly as the course progresses.

In the first half of the course, you will learn how to set up an inexpensive and flexible laboratory for understanding inner-workings of malware and demonstrate the process by exploring capabilities of real-world specimens. You will learn to examine the program's behavioral patterns and assembly code and study techniques for bypassing common code obfuscation mechanisms. The course also explores how to analyze browser-based malware.

In the second half of the course, you will review key assembly language concepts. You will learn to examine malicious code to understand its flow by identifying key logic structures, looking at examples of bots, rootkits, key loggers, and so on. You will understand how to work with PE headers and handle DLL interactions. You will also develop skills for analyzing self-defending malware through advanced unpacking techniques and bypassing code-protection mechanisms. Finally, you will discover how to bypass obfuscation techniques employed by browser-based malicious scripts.

You will also learn how to analyze malicious document files that take the form of Microsoft Office and Adobe PDF documents. Such documents act as a common infection vector and need to be understood by enterprises concerned about both large-scale and targeted attacks. The course also explores memory forensics approaches to examining rootkits. Memory-based analysis techniques also help you to understand the context of an incident involving malicious software.

Hands-on workshop exercises are an essential aspect of this course and allow you to apply reverse-engineering techniques by examining malicious code in a carefully controlled environment. When performing the analysis, you will study the supplied specimen's behavioral patterns, and examine key portions of its assembly code.

REM course on YouTube
http://www.youtube.com/watch?v=5AFdZ0v23YA

Delivery Methods

Live Events • Mentor • OnSite • vLive! • SelfStudy

Attention REM Course Alumni: Day five was very recently added to this course. If you've already attended the four-day version of the course (SEC610), you can take the whole five-day class now at a 50% discount or take just day five at one-fifth the full course price. This promotion is only valid in 2010. Please contact tuition@sans.org for details.

610.1 *Hands On:* Malware Analysis Fundamentals

Day one lays the groundwork for the course by presenting the key tools and techniques malware analysts use to examine malicious programs. You will learn how to save time by exploring malware in two phases. Behavioral analysis focuses on the specimen's interactions with its environment, such as the registry, the network, and the file system; code analysis focuses on the specimen's code and makes use of a disassembler and a debugger. You will learn how to build a flexible laboratory to perform such analysis in a controlled manner and will set up such a lab on your laptop. Also, we will jointly analyze a malware sample to reinforce the concepts and tools discussed throughout the day.

610.2 *Hands On:* Additional Malware Analysis Approaches

Day two builds upon the fundamentals introduced earlier in the course, and discusses techniques for uncovering additional aspects of the malicious program's functionality. You will learn about packers and the analysis approaches that may help bypass their defenses. You will also learn how to patch malicious executables to change their functionality during the analysis without recompiling them. You will also understand how to redirect network traffic in the lab to better interact with malware, such as bots and worms, to understand their capabilities. You will also experiment with the essential tools and techniques for analyzing Web-based malware, such as malicious browser scripts and Flash programs.

610.3 *Hands On:* Malicious Code Analysis

Day three focuses on examining malicious executables at the assembly level. You will discover approaches for studying inner-workings of a specimen by looking at it through a disassembler and, at times, with the help of a debugger. The day begins with an overview of key code reversing concepts and presents a primer on essential x86 assembly concepts, such as instructions, function calls, variables, and jumps. You will also learn how to examine common assembly constructs, such as functions, loops, and conditional statements. The second half of the day discusses how malware implements common characteristics, such as keylogging, packet spoofing, and DLL injection, at the assembly level. You will learn how to recognize such characteristics in malware samples.

610.4 *Hands On:* Self-Defending Malware

Day four begins by covering several techniques malware authors commonly employ to protect malicious software from being analyzed, often with the help of packers. You will learn how to bypass analysis defenses, such as structured error handling for execution flow, PE header corruption, fake memory breakpoints, tool detection, integrity checks, and timing controls. It's a lot of fun! As with the other topics covered throughout the course, you will be able to experiment with such techniques during hands-on exercises. The course completes by revising the topic of Web-based malware, showing additional tools and approaches for analyzing more complex malicious scripts written in VBScript and JavaScript.

610.5 *Hands On:* Deeper Malware Analysis

Day five represents the latest addition to the FOR610 course, discussing the more recent malware reverse-engineering approaches adopted by malware analysts. The topics covered during this day include analyzing malicious Microsoft Office and Adobe PDF document files. Exercises that demonstrate these techniques make use of tools, such as OfficeMalScanner, Offvis, PDF-parser, and PDF StructAzer. Another major topic covered during this day is the reversing of malicious Win32 executables using memory forensics techniques. This topic is explored with the help of tools, such as Volatility, malfind, moddump, and others, and brings us deeper into the world of user- and kernel-mode rootkits.

FOR526

Advanced Filesystem Recovery and Memory Forensics

One-Day Program
6 CPE Credits
Laptop Required

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

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 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.

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

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.

Author Statement

One of the most exciting areas in digital forensics is the ability to image and scrutinize physical memory collected from a live system. Starting with discovering basic memory structures, the student will learn how to recover and analyze processes that were seized from a live Windows-based system. Additionally, the student will learn how to discover and recover deleted partitions from hard drives that have corrupted partition tables or that have been formatted. Finally, new techniques in digital forensics will be covered. In the ever-changing world of digital forensics, it is essential that the prepared investigator have the right knowledge combined with new techniques. -Rob Lee

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.

Delivery Methods
Live Events • OnDemand • OnSite

EARN YOUR GIAC CERTIFICATION

GLOBAL INFORMATION ASSURANCE CERTIFICATION

GIAC

The Only Hands-on Information Security Certification

www.giac.org

Top Four Reasons to Get GIAC Certified

1. Promotes hands-on technical skills and improves knowledge retention

"The GIAC certification process forced me to dig deeper into the information that I was taught in class. As a result of this, I integrated this training into my practical skill set and improved my hands-on skills." -Dean Farrington, Information Security Engineer, Wells Fargo

2. Provides proof that you possess hands-on technical skills

"GIAC proves that I have a very solid technical background to support any challenge I deal with every day. There are so many new tools coming up daily, but the underlying background essentially remains the same." -Wayne Ho, Business Information Security Officer, Global Bank

3. Positions you to be promoted and earn respect among your peers

"I think the GIAC certification has definitely helped provide credibility for me in the work place. This, in turn, has helped me be more effective at my job."
-Matt Austin, Senior Security Consultant, Symantec

4. Proves to hiring managers that you are technically qualified for the job

"Hiring managers are always looking for ways to help sort through candidates. GIAC certifications are a major discriminator. They ensure that the candidate has hands-on technical skills." -Chris Schock, Network Engineer, State of Colorado

GCFA is the leading vendor-neutral digital forensic certification. GCFA recipients prove they have a firm understanding of computer forensics tools and techniques to investigate data breach intrusions, tech-savvy rogue employees, nation state threats, and complex digital forensic cases. Sophisticated attackers advance rapidly through networks using advances in spear phishing, web application attacks, and persistent malware. Forensic investigators must master a variety of operating systems, investigation techniques, incident response tactics, and even legal issues in order to solve challenging cases. The GCFA provides a foundation for critical forensic analysis techniques for solving complex Windows- and Linux-based investigations. In addition, an alarming trend has developed in several states regarding legislation of licensing of digital forensic specialists as private investigators without regard to digital forensics qualifications. The GCFA will set apart a true professional from the untrained amateur. Due to the in-depth competency requirements of a digital forensic specialist, a professional will desire to show that they have had their skills tested and accredited.

GIAC CERTIFIED FORENSIC ANALYST

GCFA

ANSI

ANSI Accredited Program
PERSONNEL CERTIFICATION

There are over 2200 certified GCFA holders making it the industry's largest vendor-neutral certification.

Forensic Resources

Digital Forensic Blog - http://blogs.sans.org/computer-forensics

SANS and Rob Lee developed this blog and the related resources at **computer-forensics.sans.org** to provide a "home" for those that are focused on computer forensics, digital investigations, and incident response. Here you will find advice, research, training, and other resources to unravel incidents and fight crime.

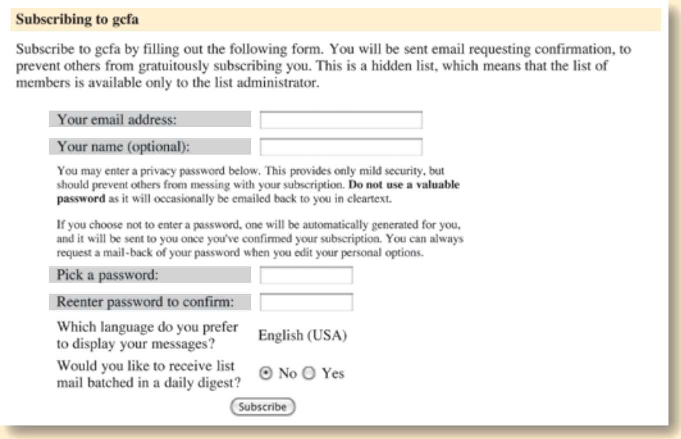
Twitter and LinkedIN

- **http://twitter.com/sansforensics**
- **@sansforensics**

Follow **@sansforensics** for the latest news on Digital Forensics in the community.

Mailing List - https://lists.sans.org/mailman/listinfo/gcfa

Join our mailing list for digital forensic specialists that seek advice from their peers in the field. This list is open to the community and a way for those in the community to join in open discussions on new techniques to solve a variety of crimes.



Subscribing to gcfa

Subscribe to gcfa by filling out the following form. You will be sent email requesting confirmation, to prevent others from gratuitously subscribing you. This is a hidden list, which means that the list of members is available only to the list administrator.

Your email address:

Your name (optional):

You may enter a privacy password below. This provides only mild security, but should prevent others from messing with your subscription. **Do not use a valuable password** as it will occasionally be emailed back to you in cleartext.

If you choose not to enter a password, one will be automatically generated for you, and it will be sent to you once you've confirmed your subscription. You can always request a mail-back of your password when you edit your personal options.

Pick a password:

Reenter password to confirm:

Which language do you prefer to display your messages? English (USA)

Would you like to receive list mail batched in a daily digest? ● No ○ Yes

Whitepapers and Webcasts

- **http://computer-forensics.sans.org/community/whitepapers.php**
- **http://computer-forensics.sans.org/community/webcasts.php**

The SANS Digital Forensics Website is proud to host the hundreds of white papers and webcasts submitted from those in the community that obtained their GCFA Gold Certification. These white papers detail the latest in research by professionals in the digital forensics community.

Challenges

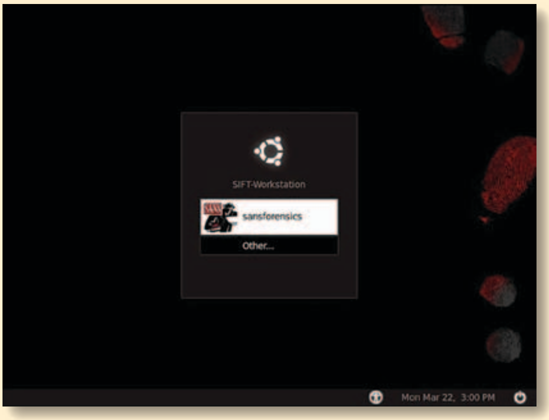
- **http://computer-forensics.sans.org/challenges**
- **http://computer-forensics.sans.org/course/assessment.php**
- **http://digitalforensics.securitytreasurehunt.com**

SANS COMPUTERFORENSICS and e-Discovery with Rob Lee

Understanding how many of these crimes take place is crucial to creating lethal forensicators armed with the knowledge and skills to analyze complex cases. The above challenges and assessments allow an investigator to test their skills to ensure they are prepared for any case they might encounter.

SIFT Workstation

SANS Investigative Forensic Toolkit (SIFT) Workstation - https://computer-forensics2.sans.org/community/siftkit

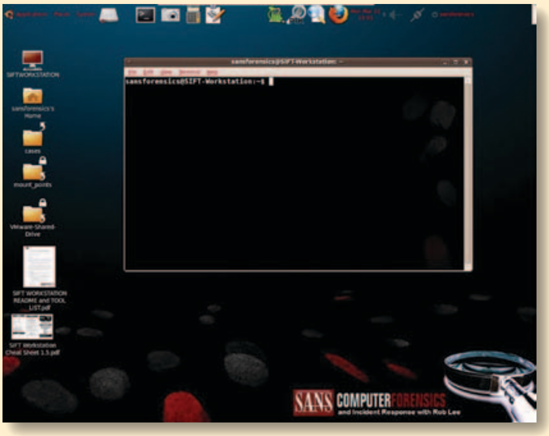


SANS SIFT Workstation Overview

- VMware Appliance
- Ready to tackle forensics
- Cross compatibility between Linux and Windows
- Forensic tools preconfigured
- A portable lab workstation you can now use for your investigations
- Option to install stand-alone via (.iso) or use via VMware Player/Workstation
- Download from **http://computer-forensics.sans.org/community**

Faculty Fellow Rob Lee created the SANS Investigative Forensic Toolkit (SIFT) Workstation featured in the Computer Forensic Investigations and Incident Response course (FOR 508) in order to show that advanced investigations and investigating hackers can be accomplished using freely available open-source tools.

The SANS SIFT Workstation is a VMware Appliance that is pre-configured with all the necessary tools to perform a detailed digital forensic examination. It is compatible with Expert Witness Format (E01), Advanced Forensic Format (AFF), and raw (dd) evidence formats. The brand new version has been completely rebuilt on an Ubuntu base with many additional tools and capabilities that can match any modern forensic tool suite. It has the ability to securely examine raw disks, multiple file systems, and evidence formats. And it also places strict guidelines on how evidence is examined (read-only) verifying that the evidence has not changed.


SIFTWORKSTATION
sansforensics's Home
cases
mount_points
VMware-Shared-Drive
SIFT WORKSTATION README and TOOL LIST.pdf
SIFT Workstation Cheat Sheet 1.3.pdf
sansforensics@SIFT-Workstation: ~
SANS COMPUTER FORENSICS
and Incident Response with Rob Lee

```
sansforensics@SIFT-Workstation:~$
```

File system support

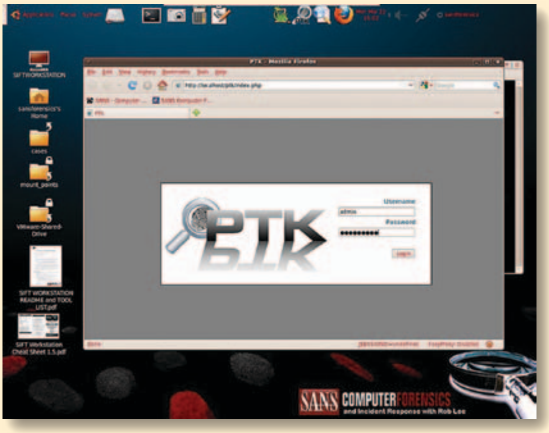
- Windows (MSDOS, FAT, VFAT, NTFS)
- MAC (HFS)
- Solaris (UFS)
- Linux (EXT2/3)

Evidence Image Support

- Expert Witness (E01)
- RAW (dd)
- Advanced Forensic Format (AFF)

Software Includes

- The Sleuth Kit (File system Analysis Tools)
- log2timeline (Timeline Generation Tool)
- ssdeep & md5deep (Hashing Tools)
- Foremost/Scalpel (File Carving)
- WireShark (Network Forensics)
- Vinetto (thumbs.db examination)
- Pasco (IE Web History examination)
- Rifiuti (Recycle Bin examination)
- Volatility Framework (Memory Analysis)
- DFLabs PTK (GUI Front-End for Sleuthkit)
- Autopsy (GUI Front-End for Sleuthkit)
- PyFLAG (GUI Log/Disk Examination)
- and 100's of additional tools



Tips and Tricks

SANS

SIFT WORKSTATION

Tips and Tricks

SANS Forensics

http://computer-forensics.sans.org
http://blogs.sans.org/computer-forensics

Purpose

Forensic Analysts are on the front lines of computer investigations. This guide aims to support Forensic Analysts in their quest to uncover the truth.

How To Use This Sheet

When performing an investigation it is helpful to be reminded of the powerful options available to the investigator. This document is aimed to be a reference to the tools that could be used. Each of these commands runs locally on a system.

This sheet is split into these sections:

- **Mounting Images**
- **Recovering Data**
- **Imaging Systems**
- **Creating Timelines**
- **Integrity Checking**
- **String Searches**
- **Memory Analysis**
- **The Sleuthkit**

The key to successful forensics is minimizing your data loss, accurate reporting, and a thorough investigation.

Imaging Systems

```
#dc3dd if=input file of=output file options
```

Example Input Files (if = *input file*)

LINUX

/dev/hda	(First IDE Physical Drive)
/dev/hda2	(Second Logical Partition)
/dev/sda	(First SCSI Physical Drive)

WINDOWS

\\.\PhysicalDrive0	(First Physical Drive)
\\.\D:	(Logical Drive D:)

Example Output Files (of = *output file*)

\\hostname\share\imagefile.img	(Windows Share)
imagefile.img	(Bit Image File)
/dev/usb	(USB Drive)
/dev/hdb	(2nd IDE Drive)

Useful Options

bs= block size	(sets the block size)
count=N	(copy only N blocks FILE)
skip=N	(skip ahead N blocks FILE)
conv=noerror,sync	(do not stop on errors)
hash=<type>	(md5, sha1, sha256,,sha512)
progress=on	(show progress meter)
hashwindow=0	(hash entire file)
hashlog=filename	(write md5 hash to file)

`mmls` to split out partitions from physical image

```
# mmls physical_imagefile
```

Tips and Tricks

Memory Analysis

volatility ***command -f /path/to/windows_xp_memory.img***

Supported commands

`connscan`	Scan for connection objects
`files`	list of open files process
`hibinfo`	Convert hibernation file
`procdump`	Dump process
`pslist`	list of running processes
`sockscan`	Scan for socket objects

```
# volatility  pslist  -f windows_xp_memory.img
```

Mounting DD Images

mount -t *fstype [options] image mountpoint*

image can be a disk partition or dd image file

Useful Options

`ro`	mount as read only
`loop`	mount on a loop device
`noexec`	do not execute files
`ro`	mount as read only
`loop`	mount on a loop device
`offset=<BYTES>`	logical drive mount
`show_sys_files`	show ntfs metafiles
`\streams_interface=windows`	Use ADS

Example: Mount an image file at mount_location

```
# mount -t fs_type -o loop,ro,show_sys_files
imagefile.dd /mnt/mount_location
```

Mounting E01 Images

# mount_ewf.py ***image.E01 mountpoint***

```
# mount_ewf.py image.E01 /mnt/ewf
```

```
# mount -t ntfs-3g -o loop,ro,show_sys_files
/mnt/ewf/<RAWFILE> /mnt/mount_location
```

Mounting Split Raw Images

# affuse ***image.001 mountpoint***

```
# affuse image.001 /mnt/aff
```

```
# mount -t ntfs-3g -o loop,ro,show_sys_files
/mnt/aff/<RAWFILE> /mnt/mount_location
```

SANS

SIFT WORKSTATION

Tips and Tricks
SANS Forensics

CONTINUED

Creating Super Timelines

```
# mount -t ntfs-3g -o loop,ro,show_sys_files imagefile.dd /
mnt/mount_location
```

```
# timescanner -z <TIMEZONE> -d /mnt/mount_location -w bodyfile
# fls -m mountpoint -r imagefile.dd >> bodyfile
# regtime.pl -m <HIVENAME> -r /path-to/registry_hive >> bodyfile
```

Collect `regtime.pl` for `SYSTEM`, `SAM`, `SECURITY`, `SOFTWARE`, and all `NTUSER.dat` hives on the machine

Create the timeline

```
# mactime -d -b bodyfile > timeline.csv
```

String Searches

`ASCII` string search and list the byte offset

```
# srch_strings -t d imagefile.dd >    imagefile.ascii.str
```

UNICODE string search and list byte offset

```
# srch_strings -e l -t d imagefile.dd > imagefile.uni.str
```

Search for a specific string using grep

GREP Useful Options

`-i`	ignore case
`-f`	`dirty_word_list_filename`

```
# grep -i password -f dirty_words.txt imagefile.ascii.str
```

Registry Parsing - Regripper

# rip.pl –r <*HIVEFILE*> –f <*HIVETYPE*>

Useful Options

`-r`	Registry hive file to parse <HIVEFILE>
`-f`	Use <HIVETYPE> (e.g. `sam`, `security`, `software`, `system`, `ntuser`)
`-l`	List all plugins

```
# rip.pl -r /mnt/windows_mount/Windows/System32/config/SAM -f sam
> /cases/windowsforensics/SAM.txt
```

Recover Deleted Registry Keys

`# deleted.pl` *`<HIVEFILE>`*

```
# deleted.pl /mnt/windows_mount/Windows/System32/config/SAM  > /
cases/windowsforensics/SAM_DELETED.txt
```

Tips and Tricks

Recovering Data

Create Unallocated Image (deleted data) using **`blkls`**

```
# blkls imagefile.dd > unallocated_imagefile.blkls
```

Create Slack Image Using dls (for FAT and NTFS)

```
# blkls -s imagefile.dd > imagefile.slack
```

Foremost Carves out files based on headers and footers

`data_file.img` = raw data, slack space, memory, unallocated space

```
# foremost -o outputdir -c /path/to/foremost.conf  data_file.img
```

Sigfind - search for a binary value at a given offset (-o)

`-o <offset>` start search at byte `<offset>`

```
# sigfind <hexvalue> -o <offset> data_file.img
```

Sleuthkit Tools

File System Layer Tools (Partition Information)

fsstat Displays details about the file system

```
# fsstat imagefile.dd
```

Data Layer Tools (Block or Cluster)

blkcat Displays the contents of a disk block

```
# blkcat imagefile.dd block_num
```

blkls Lists contents of deleted disk blocks

```
# blkls imagefile.dd > imagefile.blkls
```

blkcalc Maps between dd images and blkls results

```
# blkcalc imagefile.dd -u blkls_num
```

blkstat Display allocation status of block

```
# blkstat imagefile.dd cluster_number
```

MetaData Layer Tools (Inode, MFT, or Directry Entry)

ils Displays inode details

```
# ils imagefile.dd
```

istat Displays information about a specific inode

```
# istat imagefile.dd inode_num
```

icat Displays contents of blocks allocated to an inode

```
# icat imagefile.dd inode_num
```

ifind Determine which inode contains a specific block

```
# ifind imagefile.dd -d block_num
```

Filename Layer Tools

fls Displays deleted file entries in a directory inode

```
# fls -rpd   imagefile.dd
```

ffind Find the filename that using the inode

```
# ffind   imagefile.dd inode_num
```

SANS Faculty

Rob Lee *SANS Faculty Fellow*

Rob Lee is a director for MANDIANT (www.mandiant.com). Rob is the curriculum lead for digital forensic training at the SANS Institute (forensics.sans.org). He has over 14 years of experience in computer forensics, vulnerability and exploit discovery, intrusion detection/prevention, and incident response. Rob graduated from the U.S. Air Force Academy and served in the Air Force as a founding member of the 609th Information Warfare Squadron, the first U.S. military unit focused on information operations. Later, as a member of the Air Force Office of Special Investigations, he conducted computer crime investigations, incident response, and computer forensics. Prior to joining MANDIANT, he worked with a variety of government agencies in the law enforcement, U.S. Department of Defense, and intelligence communities as the technical lead for a vulnerability discovery and exploit development team, lead for a cyber forensics branch, and lead for a computer forensic and security software development team. Rob coauthored *Know Your Enemy*, 2nd Edition. He earned his MBA from Georgetown University in Washington DC. Rob was awarded the Digital Forensic Examiner of the Year from the Forensic 4Cast 2009 Awards. He blogs about computer forensic and incident response topics at the SANS Computer Forensic Blog.

http://blogs.sans.org/computer-forensic **@robtlee**

Eoghan Casey *Senior Instructor*

Eoghan Casey is founding partner of cmdLabs, author of the foundational book *Digital Evidence and Computer Crime*, and coauthor of *Malware Forensics*. For over a decade he has dedicated himself to advancing the practice of incident handling and digital forensics. He has been involved in a wide range of digital investigations, including network intrusions, fraud, violent crimes, identity theft, and on-line criminal activity. He has testified in civil and criminal cases and has submitted expert reports and prepared trial exhibits for computer forensic and cyber crime cases. Previously, as a director at Stroz Friedberg, he maintained an active docket of cases, supervised a talented team of forensic examiners, co-managed the company's technical operations, and spearheaded external and in-house forensic training programs. Eoghan has performed thousands of forensic acquisitions and examinations, including cellular telephones and other mobile devices. He has performed vulnerability assessments; deployed and maintained intrusion detection systems, firewalls, and public key infrastructures; and developed policies, procedures, and educational programs for a variety of organizations. In addition, he conducts research and teaches graduate students at Johns Hopkins University Information Security Institute, is editor of the *Handbook of Digital Forensics and Investigation*, and is editor-in-chief of *Elsevier's International Journal of Digital Investigation*.

Lenny Zeltser *Senior Instructor*

Lenny Zeltser leads the security consulting practice at Savvis. He is also a member of the board of directors at the SANS Technology Institute, a SANS faculty member, and an incident handler at the Internet Storm Center. Lenny frequently speaks on information security and related business topics at conferences and private events, writes articles, and has co-authored several books. Lenny is one of the few individuals in the world who has earned the highly-regarded GIAC Security Expert (GSE) designation. He also holds the CISSP certification. Lenny has an MBA degree from MIT Sloan and a computer science degree from the University of Pennsylvania. For more information about his projects, see **www.zeltser.com**. **@lennyzeltser**

Jonathan Ham *Certified Instructor*

Jonathan is an independent consultant who specializes in large-scale enterprise security issues, from policy and procedure, through staffing and training, to scalable prevention, detection, and response technology and techniques. With a keen understanding of ROI and TCO (and an emphasis on process over products), he has helped his clients achieve greater success for over 12 years, advising in both the public and private sectors, from small upstarts to the Fortune 500. He's been commissioned to teach NCIS investigators how to use Snort, performed packet analysis from a facility more than 2,000 feet underground, and chartered and trained the CIRT for one of the largest U.S. civilian federal agencies. He currently holds the CISSP, GSEC, GCIA, and GCIH certifications and is a member of the GIAC Advisory Board. A former combat medic, Jonathan still spends some of his time practicing a different kind of emergency response, volunteering and teaching for both the National Ski Patrol and the American Red Cross.

Michael Murr *Certified Instructor*

Michael has been a forensic analyst with Code-X Technologies for over five years, has conducted numerous investigations and computer forensic examinations, and has performed specialized research and development. Michael has taught SANS SEC504 (Hacker Techniques, Exploits, and Incident Handling), SANS SEC508 (Computer Forensics, Investigation, and Response), and SANS SEC601 (Reverse-Engineering Malware); has led SANS@Home courses; and is a member of the GIAC Advisory Board. Currently, Michael is working on an open-source framework for developing digital forensics applications. Michael holds the GCIH, GCFA, and GREM certifications and has a degree in computer science from California State University at Channel Islands. Michael also blogs about Digital forensics on his Forensic Computing blog.

www.forensicblog.org **@mikemurr**

Chad Tilbury *Certified Instructor*

Chad Tilbury has spent over ten years conducting incident response and forensic investigations. His extensive law enforcement and international experience stems from working with a broad cross-section of Fortune 500 corporations and government agencies around the world. During his service as a special agent with the Air Force Office of Special Investigations, he investigated a variety of computer crimes, including hacking, abduction, espionage, identity theft, and multi-million dollar fraud cases. He has led international forensic teams and was selected to provide computer forensic support to the United Nations Weapons Inspection Team. Chad has worked as a computer security engineer and forensic lead for a major defense contractor and more recently as the vice president of Worldwide Internet Enforcement for the Motion Picture Association of America. In that role, he managed Internet anti-piracy operations for the seven major Hollywood studios in over sixty countries. Chad is a graduate of the U.S. Air Force Academy and holds a BS and MS in computer science as well as GCFA, GCIH, and CISSP certifications. He is currently a consultant specializing in incident response, e-discovery, and computer forensics. **@chadtilbury**

SANS Training Options

Contact SANS today to learn how we can build a custom training package using all of these formats for your organization. Having a variety of training formats allows SANS to develop the most technical and enriching training experience at the best price. We can tailor a program that allows you to take advantage of each delivery method and ensure your team receives not just the training, but the understanding they need to stay secure.

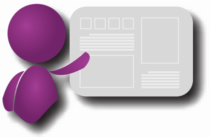
Number of People	Training Options
Individuals	Live Training Events, OnDemand, or vLive!
Groups of 15 or More	OnSite, OnDemand, or vLive!
Large Groups of 50 or More	**Enterprise Solutions:** OnDemand or vLive!

Live Training Events

The Most Trusted Name for Information Security Training

SANS offers classes throughout the year in many major US cities as well as Europe, Australia, Canada, Asia, India, and Dubai. These training events feature anywhere from one to over fifty classes at the same location. SANS events offer much more than just training – this is the place to network with other application security professionals, gain information on new vendor products, participate in onsite/online challenges and contests, and listen to world-class guest speakers.

www.sans.org/security-training/bylocation/index_na.php



SANS OnSite

Your Location - Your Schedule

With the SANS OnSite program you can bring a combination of high-quality content and world-recognized instructors to your location and realize significant savings in employee travel costs. www.sans.org/onsite

SANS vLive!

Live Virtual Instruction

SANS vLive! uses cutting-edge webcast technology to provide a live classroom experience with SANS top instructors, but delivers it over the web to students participating from their homes and offices. vLive! courses are interactive and allow students to share ideas, resources and experiences with their instructors before, during, and after training sessions. Each session is also recorded providing flexibility if a student needs to miss a session or simply wishes to review the material at a later date. www.sans.org/vlive

SANS OnDemand

Online Training and Assessment

SANS OnDemand allows students to access SANS' high-quality training 'anytime, anywhere' using SANS' advanced online delivery system. Students receive training from the same top-notch SANS instructors who teach at our live training events, and the system brings the true SANS experience right to your employees' desktops, which is convenient and saves you travel costs. Plus our integrated courseware, online assessments, hands-on exercises, and online mentor allow students to really grasp the material being taught! www.sans.org/ondemand