SANS

Digital Forensics AND Incident Response

CURRICULUM

SIFT WORKSTATION

Cheat Sheet

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 Investigations – Windows In-Depth
GCFE

FOR508
Advanced Computer Forensic Analysis & Incident Response
GCFA

FOR558
Network Forensics

FOR563
Mobile Device Forensics

LEARN R.E.M.

FOR610
REM: Malware Analysis Tools & Techniques
GREM

Additional Forensics Courses

FOR526
Windows Memory Forensics In-Depth

Not sure which course to take?
Try our free online assessment at
http://computer-forensics.sans.org/courses/assessment

SANS COMPUTERFORENSICS and Incident Response

http://computer-forensics.sans.org

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

Dear Colleague,


Rob Lee

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

FORENSICS 408

Computer Forensic Investigations – Windows In-Depth

Six-Day Course | 36 CPE Credits | Laptop Required

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

With today's ever-changing technologies and environments, it is inevitable that every organization will deal with cybercrime including fraud, insider threat, industrial espionage, and phishing. In addition, government agencies are now performing media exploitation to recover key intelligence kept on adversary systems. In order to help solve these cases, organizations are hiring digital forensic professionals and calling cybercrime law enforcement agents to piece together what happened in these cases.

FOR408: Computer Forensic Investigations - Windows In-Depth focuses on the critical knowledge of the Windows OS that every digital forensic analyst must know to investigate computer 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 and media exploitation 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. In addition to in-depth technical digital forensic knowledge on Windows Digital Forensics (Windows XP through Windows 7 and Server 2008), you will be exposed to well-known computer forensic tools so such as Access Data's Forensic Toolkit (FTK), Guidance Software's EnCase, Registry Analyzer, FTK Imager, Prefetch Analyzer, and much more. Many of the tools covered in the course are freeware, comprising a full-featured forensic laboratory that each student can take with them.

FOR408: Computer Forensic Investigations - Windows In-Depth is the first course in the SANS Computer Forensic Curriculum. If this is your first computer forensics course with SANS we recommend that you start here.

Who Should Attend:

- Information technology professionals
- Incident Response Team Members
- Law enforcement officers, federal agents, or detectives
- Media Exploitation Analysts
- Information security managers
- Information technology lawyers and paralegals
- Anyone interested in computer forensic investigations

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)**
- **SANS Windows Win7 Forensic Analysis VMware Workstation**
- **Fully functioning tools that include working with Access Data's Forensic Toolkit (FTK) and Guidance Software's EnCase**
- **Course DVD: Loaded with case examples, tools, and documentation**

"I've been doing forensics for almost 4 years. FOR408 is not a newbie course. Without 408, an investigator will be missing an incredible wealth of needed knowledge, and a disciplined methodology. Instead of 'looking for evil' by the time you finish the first run through the taught methodology, you will have found and proven 'the evil.'"

-Bruce D. Meyer, SC-ISAC, State of South Carolina Department of State I.T.

GIAC Certification
www.giac.org

STI Graduate School
www.sans.edu

Delivery Methods

Training Events
Community
OnDemand
vLive
Mentor
OnSite
SelfStudy

SANS Computer Forensic Website http//computer-forensics.sans.org

The learning does not end when class is over. SANS Computer Forensic 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.

Forensics 408 Course Content

408.1 *Hands On:* Digital Forensics Fundamentals and Evidence Acquisition

Securing or "Bagging and Tagging" digital evidence can be tricky. Each computer forensic examiner should be familiar with different methods of successfully acquiring it maintaining the integrity of the evidence. Starting with the foundations from law enforcement training in proper evidence handling procedures, you will learn firsthand the best methods for acquiring evidence in a case. You will utilize the Tableau T35es write blocker, part of your SIFT Essentials kit, to obtain evidence from a hard drive using the most popular tools utilized in the field. You will learn how to utilize toolkits to obtain memory, encrypted or unencrypted hard disk images, or protected files from a computer system that is running or powered off.

Topics: Purpose of Forensics: Investigative Mindset, Focus on the Fundamentals; Evidence Fundamentals: Admissibility, Authenticity, Threats against Authenticity; Reporting and Presenting Evidence: Taking Notes, Report Writing Essentials, Best Practices for Presenting Evidence: Tableau Write Blocker Utilization, Access Data's FTK Imager, Access Data's FTK Imager Lite; Evidence Acquisition Basics; Preservation of Evidence: Chain of Custody, Evidence Handling, Evidence Integrity

408.2 *Hands On:* Core Windows Forensics Part I – String Search, Data Carving, and Email Forensics

You will learn how to recover deleted data from the evidence, perform string searches against it using a word list, and begin to piece together the events that shaped the case. Today's course is critical to anyone performing digital forensics to learn the most up-to-date techniques of acquiring and analyzing digital evidence. Email Forensics: Investigations involving email occur every day. However, email examinations require the investigator to pull data locally, from an email server, or even recover web-based email fragments from temporary files left by a web browser. Email has become critical in a case and the investigator will learn the critical steps needed to investigate Outlook, Exchange, Webmail, and even Lotus Notes email cases.

Topics: Recover Deleted Files: Automated Recovery, String Searches, Dirty Word Searches; Email Forensics: How Email Works, Locations, Examination of Email, Types of Email Formats; Microsoft Outlook/Outlook Express; Web-Based Mail; Microsoft Exchange; Lotus Notes; E-mail Analysis, E-mail Searching and Examination

408.3 *Hands On:* Core Windows Forensics Part II – Registry and USB Device Analysis

Each examiner will learn how to examine the Registry to obtain user profile data and system data. The course will also teach each forensic investigator how to show that a specific user performed key word searches, ran specific programs, opened and saved files, and list the most recent items that were used. Finally, USB Device investigations are becoming more and more a key part of performing computer forensics. We will show you how to perform in-depth USB device examinations on Windows 7, Vista, and Windows XP machines.

Topics: Registry Forensics In-Depth;Registry Basics; Core System Information; User Forensic Data; Evidence of Program Execution; Evidence of File Download; USB Device Forensic Examinations

408.4 *Hands On:* Core Windows Forensics Part III – Artifact and Log File Analysis

Suspects unknowingly create hundreds of files that link back to their actions on a system. Learn how to examine key files such as link files, the windows prefetch, pagefile/system memory, and more. The latter part of the section 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:* Core Windows Forensics Part IV – 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: History, Cache, Searches, Downloads, Understanding of Browser Timestamps, Internet Explorer; Firefox

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

Course Relaunch!
Brand New!

FORENSICS 508
Advanced Computer Forensic Analysis and Incident Response

Six-Day Course | 36 CPE Credits | Laptop Required

Over the past two years, we have seen a dramatic increase in sophisticated attacks against organizations. Cyber-attacks originating from China named the Advanced Persistent Threat (APT) have proved difficult to suppress. Financial attacks from Eastern Europe and Russia obtain credit card, and financial data resulting in millions of dollars stolen. Hackivist groups attacking government and Fortune500 companies are becoming bolder.

FOR508: ADVANCED COMPUTER FORENSIC ANALYSIS AND INCIDENT RESPONSE will give you help you start to become a master of advanced incident response and computer forensics tools and techniques to investigate data breach intrusions, tech-savvy rogue employees, the advanced persistent threat, and complex digital forensic cases.

This course utilizes as uses the popular SIFT Workstation to teach investigators how to investigate sophisticated crimes. The free **SIFT Workstation** can match any modern forensic tool suite. It demonstrates that advanced investigations and responding to intrusions can be accomplished using cutting-edge open-source tools that are freely available and frequently updated.

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

Who Should Attend:

- Incident response team members
- Experienced digital forensic analysts
- Law enforcement officers, federal agents, or detectives
- Media exploitation analysts
- Red team members, penetration testers, and exploit developers
- Information security professionals

This course includes a Free SANS Investigative Forensic Toolkit (SIFT) Advanced

As part of this course you will receive the ***SANS Investigative Forensic Toolkit (SIFT) Advanced***. The SIFT Advanced Toolkit consists of:

- **SIFT Workstation Virtual Machine w/ plenty of hands on exercises in class**
- **F-RESPONSE TACTICAL**
  - **TACTICAL enables investigators to access physical drives and physical memory of a remote computer via the network**
  - **Able to use any tool to parse the live remote system including the SIFT Workstation**
  - **Perfect for Intrusion Investigations and Data Breach Incident Response situations**
- **Best-selling book "File System Forensic Analysis" by Brian Carrier**
- **Course DVD loaded with case examples, tools, and documentation**

"This is a great class and should be mandatory for anyone in the forensic field."

-Mark Merchant, State of Alaska/ State Security Office

GIAC Certification
www.giac.org

STI Graduate School
www.sans.edu

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

Delivery Methods

Training Events
Community
OnDemand
vLive
Mentor
OnSite
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.

Forensics 508 Course Content

508.1 *Hands On:* Windows File Systems – In-Depth

File systems are the core to your understanding of computer forensics. As every forensic tool utilizes this knowledge, you will learn how hard drives are used to store data from the partitioning to how file systems work. 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 Methodology; File System Essentials; Windows FAT and exFAT File Systems In-Depth; Windows NTFS File Systems In-Depth

508.2 *Hands On:* Incident Response and Memory Analysis

The section starts focusing on advanced acquisition techniques teaching you to acquire system memory, volatile data, and a remote live drive images from a compromised systems. Forensic analysts responding to enterprise intrusions must also be able to scale their examinations from the traditional one analyst to one machine examination to one analyst to 1,000 machines. This main section of this section's material will introduce some of the newest free tools available and give you a solid foundation in adding core and advanced memory forensic skills in your security armory.

Topics: Windows Incident Response; Mounting Images for Examinations; Remote and Enterprise Forensic Examinations; Memory Acquisition and Analysis; Memory Analysis Techniques with Redline; Live Memory Forensics; Advanced Memory Analysis with Volatility

508.3 *Hands On:* Timeline Analysis

Over the past 3 years, a renascence has occurred for the tool development for timeline analysis. SANS spearheaded the research and development by sponsoring some of the new tools that have been created recently, specifically log2timeline. As a result of the recent developments, many professionals have turned to timeline analysis as one of their core tools and capabilities. This section will step you through the two primary methods of creating and analyzing timelines created during advanced cases. Exercises will not only show how each analyst how to create a timeline, but key methods on how to use them effectively in their cases.

Topics: Timeline Analysis Overview; Filesystem Timeline Creation and Analysis; Windows Time Rules (File Copies vs. File Moves); Filesystem Timeline Creation using Sleuthkit and fls; Super Timeline Creation and Analysis; Super Timeline Artifact Rules; Timeline Creation with log2timeline; Super Timeline Analysis

508.4 *Hands On:* Filesystem Forensic Analysis

A major criticism of digital forensic professionals surrounds that many tools simply require a few mouse clicks to have the tool automatically recover data for evidence. This "push button" mentality has led to inaccurate case results in the past few years in high profile cases such as the Casey Anthony Murder trial. You will stop being reliant on "push button" forensic techniques as we cover how the engines of digital forensic tools really work. To understand how to carve out data, it is best to understand how to accomplish it by-hand and show how automated tools should be able to recover the same data.

Topics: Windows XP Restore Point Analysis; VISTA; Windows 7; Server 2008 Shadow Volume Copy Analysis; File System and Data Layer Examination; Metadata Layer Examination; File Name Layer Examination; File Sorting and Hash Comparisons; Indicator of Compromise Analysis and Creation

508.5 – Part 1 *Hands On:* Intrusion Analysis

Focus: Finding Unknown Malware, Detecting Anti-Forensics Techniques, Step-By-Step Methodology to Analyze and Solve Challenging Cases

Note this is a half day section. This advanced session will demonstrate techniques used by first responders that they use to discover malware or artifacts related to an intrusion when very little information to their capabilities or hidden location. We will discuss techniques to help funnel the possible candidates down to the most likely candidate for our evil malware trying to hide on the system. The section concludes with a step-by-step approach on how to handle investigations surrounding the most difficult cases. You will learn the best ways to approach intrusion and spear phishing attack cases.

Topics: Step-by-Step Finding Unknown Malware; Anti-Forensics Detection Methodologies; Methodology to Analyze and Solve Challenging Cases

508.5 – Part 2 *Hands On:* Computer Investigative Law For Forensic Analysts

Focus: As a team lead, you will need to know where legal land mines might exist. This half day of material focuses on what a technical lead must know before they begin any digital forensic case to protect you and your team during an investigation.

Note this is a half day section. Learn to investigate incidents while minimizing the risk for legal trouble. This course is designed not for management, but for the Digital Forensic and Incident Response team leaders in charge of an investigation. The content focuses on challenges that every lead 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; Laws Investigators Should Know; Forensic Reports and Testimony

508.6 *Hands On:* The Intrusion Forensic Challenge

This brand new exercise, updated in 2012, brings together some of the most exciting techniques learned from earlier in the week and leverage your new skills in a case that simulates an attack by an advanced adversary such as the APT. You will walk out of the course today with hands-on experience investigating scenarios put together by a cadre of experts who have had hands on experience fighting advanced threats today such as the APT.

Topics: Real-World Compromise Based on APT Tactics and Malware; Timeline Creation , String Searches; Unallocated Space Analysis; Data Recovery And Analysis; Finding Malware; Find Data Exfiltration; Find Evidence of Lateral Movement; Find Evidence of Anti-Forensics

FORENSICS 558
Network Forensics

Five-Day Course | 31.5 CPE Credits | Laptop Required

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 and 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.

Forensics 558: Network Forensics will teach you to how to follow the attacker's footprints and analyze evidence from the network environment. Network equipment such as web proxies, firewalls, IDS, routers and even switches contain 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. Forensics 558: Network Forensics will give you 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.

Who Should Attend:

- Incident response team members
- Network and computer forensic professionals
- Law enforcement officers, federal agents, or detectives
- Information security professionals
- Network security professionals
- Anyone asked to investigate a data breach incident or intrusion case

We will begin by diving 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. For 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 Forensic and Investigative Essentials (508), using the same fundamental methodology to recover and analyze evidence from network-based devices.

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.

Delivery Methods
Training Events
Community
OnDemand
vLive
Mentor
OnSite

Forensics 558 Course Content

558.1 *Hands On:* Covert Tunnels

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.

558.2 *Hands On:* Deep Packet Analysis

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: Network Analysis; Passive Evidence Acquisition; Packet Analysis

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, and 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

FORENSICS 563

Mobile Device Forensics

Five-Day Course | 30 CPE Credits | Laptop Required

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.

Who Should Attend:

- Information security professionals
- Law enforcement officers, federal agents, or detectives
- Media exploitation analysts
- Information security managers
- Information technology lawyers and paralegals
- Anyone interested in mobile device forensics
- Information technology auditors

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.

"After attending 6 phone forensics courses this year – SANS is leading the pack in knowledge and providing real world experience in hands-on practice on the newest software and program capabilities for the student."
-Paul Ehlers, LVMPD

PREREQUISITE:
Students should have an understanding of fundamental principles and processes in digital forensics, including acquisition, examination and presentation of results. In addition, students should be familiar with reading and interpreting data in hexadecimal format.

Delivery Methods
Training Events
OnSite

SANS Computer Forensic Website http//computer-forensics.sans.org

The learning does not end when class is over. SANS Computer Forensic 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.

Forensics 563 Course Content

563.1 *Hands On:* Fundamentals of Mobile Device Forensics

Review of technology from a forensic perspective, forensic handling of mobile devices, and forensic acquisition and analysis methods and techniques. Hands-on introduction to leading mobile device forensic tools, including Cellebrite and XRY. Perform logical acquisitions, physical acquisitions and manual examination of mobile devices. Understand about the types of evidence on mobile devices and how to interpret the various data formats. Learn about the strengths and limitations of mobile device forensic tools, and how to overcome in-field challenges.

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:* Cell Phone Forensics & SIM Card Examination

Perform forensic acquisition and examination of SIM cards. Use mobile forensic tools, including BitPim, to acquire and analyze data from a variety of CDMA and GSM devices, including Motorola, Samsung and LG. Recover deleted data by delving into memory contents and extracting data structures on mobile devices. Compare forensic acquisition tools and validate completeness and accuracy of results.

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:* iPhone and Andriod

Apply forensic principles and tools to some of the most popular smart phones. Hands-on exploration of iPhone and Android operating systems and data storage using developer utilities and forensic tools. Perform logical and physical acquisitions and examinations of iPhone and Android devices. Interpret important data structures, understand usage artifacts and recover deleted data from iPhone and Android devices.

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 and Nokia

Apply forensic principles and tools to Blackberry and Nokia systems. Hands-on exploration of Blackberry and Nokia devices and data storage using various utilities and forensic tools. Perform logical and physical acquisitions and examinations of Nokia devices, including the use of Flasher boxes.

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

563.5 *Hands On:* GPS Forensics/Location Information and the Forensic Challenge

Forensic acquisition and examination of GPS navigation devices, including location information saved on smart phones and EXIF data in multi-media files. Familiarization with other forensic acquisition and analysis techniques. Putting the pieces of a case together and presenting results in reports and testimony. A realistic hands-on investigative scenario bringing together lessons and techniques learned throughout the course.

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

Throughout this course, we provide practical, hands-on exercises to give you ample opportunities to explore mobile devices and the data they contain.

FORENSICS 610

Reverse-Engineering Malware: Malware Analysis Tools and Techniques

Five-Day Course | 30 CPE Credits | Laptop Required

Expand your capacity to fight malicious code by learning how to analyze bots, worms, and trojans.

This popular malware analysis course has helped forensic investigators, malware specialists, incident responders, and IT administrators assess malware threats. The course teaches a practical approach to examining malicious programs-spyware, bots, trojans, etc.-that target or run on Microsoft Windows. This training also looks at reversing Web-based malware, such as JavaScript and Flash files, as well as malicious document files. By the end of the course, you'll learn how to reverse-engineer malicious software using a variety of system and network monitoring utilities, a disassembler, a debugger, and other tools for turning malware inside-out!

Who Should Attend:

- Individuals who found this course particularly useful often had responsibilities in the areas of incident response, forensic investigation, Windows security, and system administration.
- You'll benefit from this course if you deal with incidents involving malware and would like to learn how to understand key aspects of malicious programs.
- The majority of course participants have a strong understanding of core systems and networking concepts and have had a limited exposure to programming and assembly concepts.
- Some individuals who attended the course have experimented with aspects of malware analysis prior to the course and were looking to formalize and expand their malware forensics expertise.

A Methodical Approach to Reverse-Engineering

The course begins by covering fundamental aspects of malware analysis. You'll learn how to set up an inexpensive and flexible laboratory for understanding the inner-workings of malicious software and will understand how to use the lab for exploring characteristics of real-world malware. Then you'll learn to examine the program's behavioral patterns and code. Afterwards, you'll experiment with reverse-engineering compiled Windows executables and browser-based malware.

The course continues by discussing essential x86 assembly language concepts. You'll examine malicious code to understand the program's key components and execution flow. Additionally, you'll learn to identify common malware characteristics by looking at Windows API patterns and will examine excerpts from bots, rootkits, keyloggers, and downloaders. You'll understand how to work with PE headers and handle DLL interactions. Furthermore, you'll learn tools and techniques for bypassing anti-analysis capabilities of armored malware, experimenting with packed executables and obfuscated browser scripts.

Towards the end of the course, you'll learn 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 understand the context of an incident involving malicious software.

LEARN REM

REM course info at
http://REMnux.org

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 Certification
www.giac.org

STI Graduate School
www.sans.edu

Delivery Methods

Training Events
Community
OnDemand
vLive
Mentor
OnSite
SelfStudy

Forensics 610 Course Content

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.

Topics: Configuring the malware analysis lab; Assembling the toolkit; Performing behavioral analysis of malicious Windows executables; Performing static and dynamic code analysis of malicious Windows executables; Intercepting system and network-level activities

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.

Topics: Reinforcing the dynamic analysis concepts; Patching compiled malicious Windows executables; Shortcuts for speeding up malware analysis; Analyzing packed executable files; Redirecting IP address-based network connections; Analyzing JavaScript (getting started) and Flash malware

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.

Topics: Core concepts for reverse-engineering malware at the code level; x86 Intel assembly language primer; Handling anti-disassembling techniques; Identifying key x86 assembly logic structures with a disassembler; Patterns of common malware characteristics at the Windows API level (DLL injection, hooking, keylogging, sniffing, etc.)

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.

Topics: Identifying packers; Working with PE headers of malicious Windows executables; Manual unpacking of protected malicious Windows executables (tips and tricks); Tips and tricks for bypassing anti-analysis mechanisms built into malware; Additional techniques for analyzing browser scripts (handling deobfuscation)

610.5 *Hands On:* Malicious Documents and Memory Forensics

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.

Topics: Analyzing malicious Microsoft Office (Word, Excel, PowerPoint) and Adobe PDF documents; Examining shellcode in the context of malicious files; Analyzing memory to assess malware characteristics and reconstruct infection artifacts; Using memory forensics to analyze rootkit infections

FORENSICS 526

Windows Memory Forensics In-Depth

Two-Day Course | 12 CPE Credits | Laptop Required

FOR526: Windows Memory Forensics In-Depth is a critical course for any serious investigator who wishes to tackle advanced forensic and incident response cases.

Malware can hide, but it must run – The malware paradox is key to understanding that while intruders are becoming more advanced with anti-forensic tactics and techniques, it is impossible to hide their footprints completely from a skilled incident responder performing memory analysis. Learn how memory analysis works through learning about memory structures and context, memory analysis methods, and the current tools used to parse system ram.

Who Should Attend:

- Incident Response Team Members
- Law Enforcement Officers, Federal Agents, or Detectives
- Media Exploitation Analysts
- Red Team Members, Penetration Testers, and Exploit Developers
- Information Security Professionals

Attackers will use anti-forensic techniques to hide their tracks. They use rootkits, file wiping, timestamp adjustments, privacy cleaners, and more to hide in plain sight, avoiding detection by standard host-based security measures. Every action that adversaries make will leave a trace; you merely need to know where to look. Memory analysis will give you the edge that you need in order to discover advanced adversaries in your network.

You Will Learn:

- What resources can be gleaned from memory, how to see through anti-forensic obfuscation techniques, and gather data which cannot be found via traditional means.
- How the operating system internals fit together to form a coherent picture, and how to analyze that picture.
- The underlying techniques used in memory forensics tools. Not just how to press-a-button, get-a-result, but what's happening under the hood.
- How to quickly identify the important data when examining many systems in an enterprise.

Author Statement

A forensic examiner is defined by their understanding of the technologies they work with. Somebody who understands what is happening under the hood will have an inherent advantage over somebody who does not. Peeking at the underlying data, poking at them manually, and coming to understand what they represent, is what this course is all about.

Afterward, there are tools and methods, which can automate many of these processes. But the results of those methods are useless if the examiner doesn't understand what they represent. This class will encourage you to try things out and ask questions. The classroom environment is for learning. If you get everything right the first time, you haven't learned anything! Here you will learn by doing, not listening.

Memory analysis is the latest frontier in our field and presents opportunities we have not seen in some time. Taking this class is a great way to get started in this exciting new domain. The technologies involved will unlock some valuable doors. We haven't reached the limits of memory analysis by a long shot. In the near future there will be more advanced techniques and available data. It's important to build a strong foundation now!

-Jesse Kornblum, Kyrus

PREREQUISITE:
This is an advanced investigations course that requires prior in-depth forensic knowledge as a prerequisite. This course is perfect for those that have already attended FOR508 or FOR610.

Delivery Methods
Training Events
OnDemand
OnSite

The Only Hands-on Information Security Certification

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

GIAC Forensic Examiner (GCFE)

GIAC Certified Forensic Examiner (GCFE) certifies that candidates have the knowledge, skills, and ability to conduct typical incident investigations including e-Discovery, forensic analysis and reporting, evidence acquisition, browser forensics and tracing user, and application activities on Windows systems.

GIAC Forensic Analyst (GCFA)

GIAC Certified forensic analysts (GCFAs) are front line investigators during computer intrusion breaches across the enterprise. They can help identify and secure compromised systems even if the adversary uses anti-forensic techniques. Using advanced techniques such as file system timeline analysis, registry analysis, and memory inspection, GCFAs are adept at finding unknown malware, rootkits, and data that the intruders thought had eliminated from the system.

GIAC Reverse Engineering Malware (GREM)

The GIAC Reverse Engineering Malware (GREM) certification is designed for technologists who protect the organization from malicious code. GREM-certified technologists possess the knowledge and skills to reverse-engineer malicious software (malware) that targets common platforms, such as Microsoft Windows and web browsers. These individuals know how to examine inner-workings of malware in the context of forensic investigations, incident response, and Windows system administration.

Top Four Reasons to Get GIAC Certified

1. **Promotes** hands-on technical skills and improves knowledge retention
2. **Provides** proof that you possess hands-on technical skills
3. **Positions** you to be promoted and earn respect among your peers
4. **Proves** to hiring managers that you are technically qualified for the job

Forensic Resources

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

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.

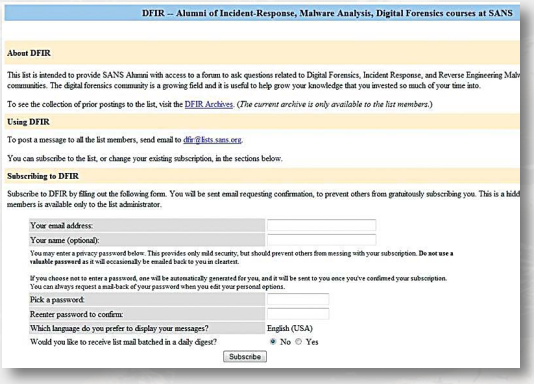
Twitter, Facebook, and LinkedIN

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

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

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

Join our mailing list for digital forensics and incident response 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.


DFIR -- Alumni of Incident-Response, Malware Analysis, Digital Forensics courses at SANS

About DFIR

This list is intended to provide SANS Alumni with access to a forum to ask questions related to Digital Forensics, Incident Response, and Reverse Engineering Malw communities. The digital forensics community is a growing field and it is useful to help grow your knowledge that you invested so much of your time into.

To see the collection of prior postings to the list, visit the DFIR Archives. (*The current archive is only available to the list members.*)

Using DFIR

To post a message to all the list members, send email to dfir@lists.sans.org.

You can subscribe to the list, or change your existing subscription, in the sections below.

Subscribing to DFIR

Subscribe to DFIR by filling out the following form. You will be sent email requesting confirmation, to prevent others from gratuitously subscribing you. This is a hidd 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

Subscribe

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**

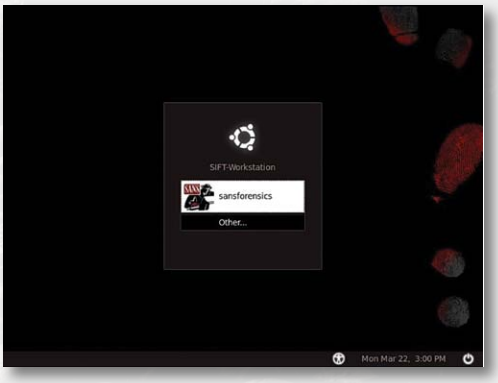
Understanding how many of these crimes take place is crucial to creating lethal forensicators armed with the knowledge and skills to analyze complex cases. The above challenges and assessments allow an investigator to test their skills to ensure they are prepared for any case they might encounter.

SANS COMPUTERFORENSICS and Incident Response

SIFT Workstation

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

SANS SIFT Workstation Overview

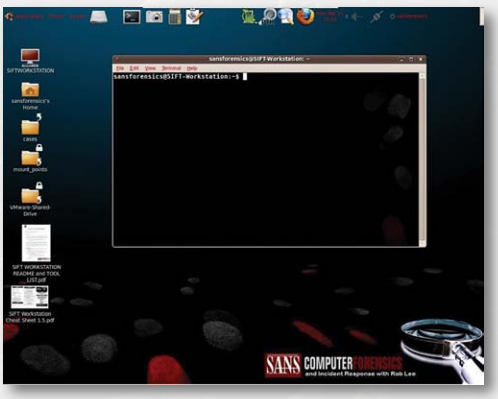


- VMware Appliance
- Ready to tackle forensics
- Cross compatibility between Linux and Windows
- Forensic tools preconfigured
- A portable lab workstation you can now use for your investigations
- Option to install stand-alone via (.iso) or use via VMware Player/Workstation
- Download from **http://computer-forensics.sans.org/community/downloads**

SANS Faculty Fellow, Rob Lee created the SANS Investigative Forensic Toolkit (SIFT) Workstation featured in the Computer Forensic Investigations and Incident Response course (FOR508) 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. It also places strict guidelines on how evidence is examined (read-only) verifying that the evidence has not changed.

File system support

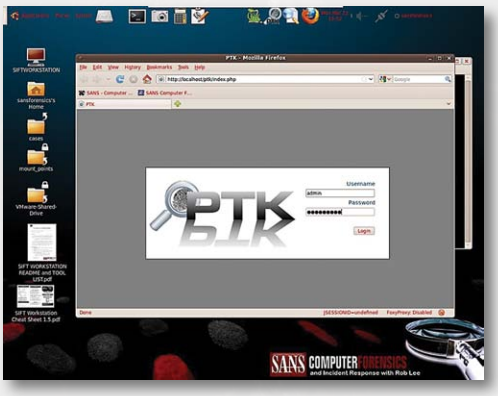


- Windows (MSDOS, FAT, VFAT, NTFS)
- MAC (HFS)
- Solaris (UFS)
- Linux (EXT2/3)

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

SANS SIFT WORKSTATION

Tips and Tricks • SANS Forensics

http://computer-forensics.sans.org • http://computer-forensics.sans.org/blog

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

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

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
```

Cheat Sheet

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 -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 -o loop,ro,show_sys_files
/mnt/aff/<RAWFILE> /mnt/mount_location
```

CREATING SUPER TIMELINES

Step 1 – Find Partition Starting Sector

```
# mmls image.dd – calculate offset ##### (sector *512)
```

Step 2 – Mount image for processing

```
# mount -o ro, noexec,show_sys_files,loop,offset=##### image.dd /mnt/
windows_mount
```

Step 3 – Create Comprehensive Timeline

```
# log2timeline -p -r -f winxp -z CST6CDT /mnt/windows_mount -w
timeline.csv
```

Step 4 – Filter Timeline

```
# l2t_process -b timeline.csv -k keywords.txt MM-DD-YYYY..MM-DD-YYYY
```

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
```

Cheat Sheet

MEMORY ANALYSIS

vol.py [plugin] *-f [image] --profile [PROFILE]*

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

```
# vol.py pslist -f windows_7_memory.img --profile=Win7SP0x86
```

Profiles

VistaSP0x86 - A Profile for Windows Vista SP0 x86
VistaSP1x86 - A Profile for Windows Vista SP1 x86
VistaSP2x86 - A Profile for Windows Vista SP2 x86
Win2K8SP1x86 - A Profile for Windows 2008 SP1 x86
Win2K8SP2x86 - A Profile for Windows 2008 SP2 x86
Win7SP0x86 - A Profile for Windows 7 SP0 x86
WinXPSP2x86 - A Profile for Windows XP SP2
WinXPSP3x86 - A Profile for windows XP SP3

RECOVER DELETED REGISTRY KEYS

 # deleted.pl *<HIVEFILE>*

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

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 Training Formats

Training Events

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

Community

Community Training Events

www.sans.org/community_sans

OnSite

Information Security Training at Your Location

www.sans.org/onsite

Mentor & @Work

Intimate Live Instruction

www.sans.org/mentor

Summit Series

Your IT Security Connection

www.sans.org/summit

OnDemand

Online Training & Assessments Anytime, Anywhere

www.sans.org/ondemand

vLive!

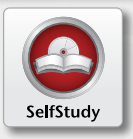
Real-time Access to Your Instructor

www.sans.org/vlive

Simulcast

Live SANS Instruction in Multiple Locations

www.sans.org/virtual-training/event-simulcast
www.sans.org/virtual-training/custom-simulcast



SelfStudy

Books & MP3s

www.sans.org/selfstudy

Ovie Carroll *SANS Instructor*

Ovie Carroll has over 20 years of federal law enforcement experience. Ovie was a special agent for the Air Force Office of Special Investigations (AFOSI) and Chief of the Washington Field Office Computer Investigations and Operations Branch responsible for investigating all national level computer intrusions into USAF computer systems. Following his career with the AFOSI he was the Special Agent in Charge of the Postal Inspector General's computer crimes unit. Ovie is currently the Director for the Cybercrime Lab at the Department of Justice, Computer Crime and Intellectual Property Section (CCIPS) and an adjunct professor at George Washington University teaching computer crime investigations. **@ovie** podcast: **cyberspeak.libsyn.com**

Eoghan Casey *SANS 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. 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*.

Jess Garcia *SANS Certified Instructor*

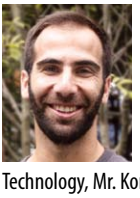
Jess Garcia, founder of One eSecurity, is a Senior Security Engineer with over 15 years of experience in Information Security. During the last 5 years Jess has worked in highly sensitive projects in Europe, USA, Latin America and the Middle East with top global customers in sectors such as financial & insurance, corporate, media, health, communications, law firms or government, in areas such as Incident Response & Computer Forensics, Malware Analysis, Security Architecture Design and Review, etc. Jess holds a Masters of Science in Telecommunications Engineering from the Univ. Politecnica de Madrid.

Jonathan Ham *SANS 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.

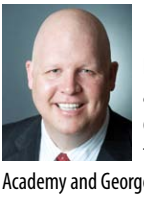
Paul A. Henry *SANS Certified Instructor*

One of the world's foremost global information security and computer forensic experts, with more than 20 years experience managing security initiatives for Global 2000 enterprises and government organizations worldwide. Paul is a principle at vNet Security, LLC and is keeping a finger on the pulse of network security as the security and forensic analyst at Lumension Security. **@phenrycissp**



Jesse Kornblum *SANS Instructor*

Jesse Kornblum is a Computer Forensics Research Guru for the Kyrus Corporation. Based in the Washington, D.C. area, his research focuses on computer forensics and computer security. He has helped pioneer the field of memory analysis and authored a number of computer forensics tools including the md5deep suite of hashing programs and the ssdeep system for fuzzy hashing similar files. A graduate of the Massachusetts Institute of Technology, Mr. Kornblum previously served as a computer crime investigator for the Air Force and with the Department of Justice.



Rob Lee *SANS Faculty Fellow*

Rob Lee is the Curriculum Lead for digital forensic and incident response programs at the SANS Institute and is an entrepreneur in the DC area having recently starting his own consulting firm. Rob has more than 15 years of experience in digital forensics, vulnerability exploitation, threat detection, and incident response working across the DoD, Intel Community, Defense Industrial Base (DIB), and Fortune 500. Rob graduated from the U.S. Air Force Academy and Georgetown University. He served in the U.S. Air Force as a founding member of the 609th Information Warfare Squadron, Chief of the Air Force Office of Special Investigation's Technical Monitoring Team, and reservist at the JTF-GNO. Rob was also a director for MANDIANT, a company focused on investigating advanced adversaries, such as the APT, for four years prior to starting his own business. He was awarded the Digital Forensic Examiner of the Year from the Forensic 4Cast Awards. He blogs about computer forensic and incident response topics at the SANS Computer Forensic Blog. **http://computer-forensics.sans.org/blog** **@robtlee**

orensics Faculty

Heather Mahalik *SANS Certified Instructor*

Heather Mahalik is a Digital Forensics Analyst at Basis Technology. She uses her experience to support media and cell phone forensics efforts in the U.S. Government. Heather has worked in digital forensics for over eight years and has performed hundreds of forensic acquisitions and examinations on hard drives, e-mail and file servers, mobile devices and portable media. She has authored articles, papers and instructed classes focused on Mac Forensics, Mobile Forensics, and Computer Forensics to practitioners in the field.

Michael Murr *SANS 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**

Hal Pomeranz *SANS Faculty Fellow*

Hal Pomeranz is the founder and technical lead for Deer Run Associates, a consulting company focusing on Digital Forensics and Information Security. He is a SANS Faculty Fellow and the creator of the SANS/GIAC Linux/Unix security course (GCUX), as well as being an instructor in the SANS Forensics curriculum. An expert in the analysis of Linux and Unix systems, Hal provides forensic analysis services through his own consulting firm and by special arrangement with MANDIANT. He has consulted on several major cases for both law enforcement and commercial clients. Hal is a regular contributor to the SANS Computer Forensics blog, and co-author of the weekly Command-Line Kung Fu blog.

http://blog.commandlinekungfu.com **http://computer-forensics.sans.org/blog**

@hal_pomeranz

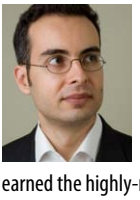
Richard Salgado *SANS Senior Instructor*

Richard P. Salgado is a Senior Legal Director with Yahoo! Inc., where he focuses on international privacy, security and law enforcement compliance matters. Prior to joining Yahoo!, Mr. Salgado served as senior counsel in the Computer Crime and Intellectual Property Section of the United States Department of Justice. As a federal prosecutor, Mr. Salgado specialized in investigating and prosecuting computer network cases, such as computer hacking, illegal computer wiretaps, denial of service attacks, malicious code, and other technology-driven privacy crimes. Mr. Salgado also regularly speaks on the legal and policy implications of searching and seizing computers and electronic evidence, emerging surveillance technologies, digital evidence, and related criminal conduct. Mr. Salgado is a lecturer in law at Stanford Law School, where he teaches a Computer Crime seminar; he previously served as an adjunct law professor at Georgetown University Law Center and George Mason Law School, and as a faculty member of the National Judicial College. Mr. Salgado graduated magna cum laude from the University of New Mexico and in 1989 received his J.D. from Yale Law School.

Chad Tilbury *SANS 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



Lenny Zeltser *SANS 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**. **blog.zeltser.com** **@lennyzeltser**

SANS Lethal Forensicator Coin

The Coin is designed to be awarded to those who demonstrate exceptional talent, contributions, or helps to lead in the digital forensics profession and community. The Coin is meant to be an honor to receive it; it is also intended to be rare. Those who join the Lethal Forensicators Unit will have all privileges and recognition.

Learn more about the SANS Lethal Forensicator Coin and how to earn one at http://computer-forensics.sans.org/community/lethal-forensicator

2012 Forensics and Incident Response Summit

Austin, TX

Pre-Summit: June 20 - 25 | Summit: June 26 - 27

Register Today!

www.sans.org/forensics-incident-response-summit-2012

SANS

5705 Salem Run Blvd.
Suite 105
Fredericksburg, VA 22407

PROMO CODE

FOR12

Register using this Promo Code