SANS DFIR

DIGITAL FORENSICS & INCIDENT RESPONSE

COURSE CATALOG

SANS Forensics Curriculum

SANS Digital Forensics and Incident Response 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.

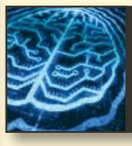
Digital Forensic Analyst

FOR408 Computer Forensic Investigations – Windows In-Depth **GCFE**

FOR508 Advanced Computer Forensic Analysis & Incident Response **GCFA**

FOR585 Advanced Smartphone & Mobile Device Forensics — COMING SOON!

FOR559 Cloud Forensics and Incident Response — COMING SOON!



FOR526 Windows Memory Forensics In-Depth

FOR518 MAC and iOS Forensics — COMING SOON!

FOR610 REM: Malware Analysis Tools and Techniques — New Content Added **GREM**

Incident Responder

SEC504 Hacker Techniques, Exploits, and Incident Handling **GCIH**

Network Analysis | System Analysis | Malware Analysis

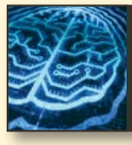
FOR572 Advanced Network Forensics and Investigations — COMING SOON!

FOR408 Computer Forensic Investigations – Windows In-Depth **GCFE**

FOR610 REM: Malware Analysis Tools and Techniques — New Content Added **GREM**

FOR559 Cloud Forensics and Incident Response — COMING SOON!

FOR508 Advanced Computer Forensic Analysis & Incident Response **GCFA**



FOR526 Windows Memory Forensics In-Depth

FIGHT CRIME

Unravel incidents... one byte at a time.

http://computer-forensics.sans.org

Dear Colleague,

Rob Lee

Over the past few years, digital crime and intrusions have increased indicating that criminal, hacking groups and nation-state adversaries 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. We can do better. We need to develop of sophisticated incident responders and forensic investigators. We need adversary hunter, incident responders, and 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 and Incident Response (DFIR) Curriculum brings together top professionals that have developed the industry's leading innovative courses for digital forensics, incident response, and in-depth specialty training. Our goal is to continue to offer the most rewarding training to each individual. We will arm you with the tools to solve complex incidents 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 and cheat sheets 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 and Incident Response Blog; 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

SEC504 Hacker Techniques, Exploits & Incident Handling 2
FOR408 Computer Forensic Investigations – Windows In-Depth 4
FOR508 Advanced Computer Forensic Analysis and Incident Response 6
FOR526 Windows Memory Forensics In-Depth 8
FOR610 REM: Malware Analysis Tools & Techniques 10
Upcoming DFIR Courses 12
Computer Forensics Resources 14
SIFT Workstation 15
SIFT Workstation Cheat Sheet 16
Memory Forensics Cheat Sheet 19
SANS DFIR Faculty 22
GIAC Cerification 25
NetWars 25

SECURITY 504

Hands-On | Six Days | Laptop Required | 37 CPE/CMU Credits | GIAC Cert: GCIH

SEC504: Hacker Techniques, Exploits, and Incident Handling

If your organization has an Internet connection or one or two disgruntled employees (and whose doesn't!), your computer systems will get attacked. From the five, ten, or even one hundred daily probes against your Internet infrastructure to the malicious insider slowly creeping through your most vital information assets, attackers are targeting your systems with increasing viciousness and stealth.

By helping you understand attackers' tactics and strategies in detail, giving you hands-on experience in finding vulnerabilities and discovering intrusions, and equipping you with a comprehensive incident handling plan, the in-depth information in this course helps you turn the tables on computer attackers. This course addresses the latest cutting-edge insidious attack vectors and the "oldie-but-goodie" attacks that are still so prevalent, and everything in between. Instead of merely teaching a few hack attack tricks, this course includes a time-tested, step-by-step process for responding to computer incidents; a detailed description of how attackers undermine systems so you can prepare, detect, and respond to them; and a hands-on workshop for discovering holes before the bad guys do. Additionally, the course explores the legal issues associated with responding to computer attacks, including employee monitoring, working with law enforcement, and handling evidence.

"This online conference for the course is awesome. Instructors are excellent. Being able to do it from anywhere is sweet."
-Giovanni Navarrette, TDS Telecom

"When I get back to the office, I will use the knowledge I gained here to better defend my organization's network."
-Joshua Anthony, West Virginia Army National Guard

This challenging course is particularly well suited to individuals who lead or are a part of an incident handling team. Furthermore, general security practitioners, system administrators, and security architects will benefit by understanding how to design, build, and operate their systems to prevent, detect, and respond to attacks.

You Will Be Able To

- Apply incident handling processes in-depth, including preparation, identification, containment, eradication, and recovery, to protect enterprise environments
- Analyze the structure of common attack techniques to be able to evaluate an attacker's spread through a system and network, anticipating and thwarting further attacker activity
- Utilize tools and evidence to determine the kind of malware used in an attack, including rootkits, backdoors, and trojan horses, choosing appropriate defenses and response tactics for each
- Use built-in command-line tools such as Windows tasklist, wmic, and reg as well as Linux netstat, ps, and lsof to detect an attacker's presence on a machine
- Analyze router and system ARP tables along with switch CAM tables to track an attacker's activity through a network and identify a suspect
- Use memory dumps and the Volatility tool to determine an attacker's activities on a machine, the malware installed, and other machines the attacker used as pivot points across the network
- Gain access of a target machine using Metasploit, and then detecting the artifacts and impacts of exploitation through process, file, memory, and log analysis
- Analyze a system to see how attackers use the Netcat tool to move files, create backdoors, and build relays through a target environment
- Run the Nmap port scanner and Nessus vulnerability scanner to find openings on target systems, and apply tools such as tcpdump and netstat to detect and analyze the impacts of the scanning activity
- Apply the tcpdump sniffer to analyze network traffic generated by a covert backdoor to determine an attacker's tactics
- Employ the netstat and lsof tools to diagnose specific types of traffic-flooding denial-of-service techniques and choosing appropriate response actions based on each attacker's flood technique
- Analyze shell history files to find compromised machines, attacker-controlled accounts, sniffers, and backdoors

Who Should Attend

- Incident handlers
- Penetration testers
- Ethical hackers
- Leaders of incident handling teams
- System administrators who are on the front lines defending their systems and responding to attacks
- Other security personnel who are first responders when systems come under attack

"The course covers almost every corner of attack and defense areas. It's a very helpful handbook for a network security analysis job. It upgrades my knowledge in IT security and keeps pace with the trend."
-Anthony Liu, Scotia Bank

Course Day Descriptions

504.1 Incident Handling Step-by-Step and Computer Crime Investigation

This session describes a detailed incident handling process and applies that process to several in-the-trenches case studies. Additionally, in the evening an optional 'Intro to Linux' mini-workshop will be held. This session provides introductory Linux skills you'll need to participate in exercises throughout the rest of SEC504. If you are new to Linux, attending this evening session is crucial.

Topics: Preparation; Identification; Containment; Eradication; Recovery; Special Actions for Responding to Different Types of Incidents; Incident Record Keeping; Incident Follow-Up

504.2 Hands On: Computer and Network Hacker Exploits – Part 1

It is imperative that system administrators and security professionals know how to control what outsiders can see. Students who take this class and master the material can expect to learn the skills to identify potential targets and be provided tools they need to test their systems effectively for vulnerabilities. This day covers the first two steps of many hacker attacks: reconnaissance and scanning.

Topics: Reconnaissance; Scanning; Intrusion Detection System Evasion; Hands-on Exercises for a List of Tools

504.3 Hands On: Computer and Network Hacker Exploits – Part 2

Computer attackers are ripping our networks and systems apart in novel ways while constantly improving their techniques. This course covers the third step of many hacker attacks – gaining access. For each attack, the course explains vulnerability categories, how various tools exploit holes, and how to harden systems or applications against each type of attack. Students who sign an ethics and release form are issued a CD-ROM containing the attack tools examined in class.

Topics: Network-Level Attacks; Gathering and Parsing Packets; Operating System and Application-Level Attacks; Netcat: The Attacker's Best Friend; Hands-on Exercises with a List of Tools

504.4 Hands On: Computer and Network Hacker Exploits – Part 3

Attackers aren't resting on their laurels, and neither can we. They are increasingly targeting our operating systems and applications with ever-more clever and vicious attacks. This session looks at increasingly popular attack avenues as well as the plague of denial of service attacks.

Topics: Password Cracking; Web Application Attacks; Denial of Service Attacks; Hands-on Exercises with a List of Tools

504.5 Hands On: Computer and Network Hacker Exploits – Part 4

Once intruders have gained access into a system, they want to keep that access by preventing pesky system administrators and security personnel from detecting their presence. To defend against these attacks, you need to understand how attackers manipulate systems to discover the sometimes-subtle hints associated with system compromise. This course arms you with the understanding and tools you need to defend against attackers maintaining access and covering their tracks.

Topics: Maintaining Access; Covering the Courses; Five Methods for Implementing Kernel-Mode RootKits on Windows and Linux; the Rise of Combo Malware; Detecting Backdoors; Hidden File Detection; Log Editing; Covert Channels; Sample Scenarios

504.6 Hands On: Hacker Tools Workshop

In this workshop you'll apply skills gained throughout the week in penetrating various target hosts while playing Capture the Flag. Your instructor will act as your personal hacking coach, providing hints as you progress through the game and challenging you to break into the laboratory computers to help underscore the lessons learned throughout the week. For your own attacker laptop, do not have any sensitive data stored on the system. SANS is not responsible for your system if someone in the class attacks it in the workshop. Bring the right equipment and prepare it in advance to maximize what you'll learn and the fun you'll have doing it.

Topics: Capture the Flag Contest; Hands-on Analysis; General Exploits; Other Attack Tools and Techniques

www.giac.org

DoD 8570 Required
www.sans.org/8570

www.sans.org/cyber-guardian

www.sans.edu

FOR408:
Computer Forensic Investigations – Windows In-Depth

Master computer forensics. Learn critical investigation techniques. With today's ever-changing technologies and environments, it is inevitable that every organization will deal with cybercrime including fraud, insider threats, 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.

"Hands down the BEST forensics class EVER!! Blew my mind at least once a day for 6 days!"
-Jason Jones, USAF

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 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 8 and Server 2008) you will be exposed to well known computer forensic tools 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 students can take with them.

"This is a very high-intensity course with extremely current course material that is not available anywhere else in my experience."
-Alexander Applegate, Auburn University

You Will Be Able To

- Perform proper Windows forensic analysis, determine how and who placed an artifact on the system by applying key analysis techniques covering Windows XP through Windows 8
- Use full scale forensic tools and analysis methods to detail every action a suspect accomplished on a Windows system – and determine program execution, file/folder opening, geo-location, browser history, USB devices, and more
- Uncover the exact time that a specific user last executed a program through Registry analysis, Windows artifact analysis, and e-mail analysis. Over time that is key to proving intent in many cases such as intellectual property theft, hacker breached systems, and traditional crimes
- Demonstrate every time a file has been opened by a suspect through IE browser forensics, shortcut file analysis (LNK), e-mail analysis and Registry parsing
- Use automated analysis techniques via AccessData's Forensic ToolKit (FTK)
- Identify key words searched for by a specific user on a Windows system that can be used to identify files that the suspect was interested in finding
- Use shellbags analysis tools to articulate every folder and directory that a user opened up while he was browsing through the hard drive
- Determine each time a unique and specific USB device is attached to the Windows system, the files and folders that were accessed on it, and who plugged it in via tools parsing key Windows artifacts such as the Registry and log files
- Examine how a user logged into a Windows system through a remote session, at the keyboard, or simply unlocking their screensaver by viewing the logon types in the Windows security event logs
- Use FTK Registry Viewer, pinpoint geo-location of a Windows system through the examination of the networks they have connected to, browser search terms, and cookie data to determine where a crime was committed
- Use Webhistorian and parse raw SQLite databases to profile Internet usage and even recover browser history of suspects attempting to clear their trail using privacy cleaners and in-private browsing through session recovery and flash cookies

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

Course Day Descriptions

408.1 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 while 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 WiebeTech Forensic UltraDock V5 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 E-mail 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. E-mail Forensics: Investigations involving e-mail occur every day. However, e-mail examinations require the investigator to pull data locally, from an e-mail server, or even recover web-based e-mail fragments from temporary files left by a web browser. E-mail has become critical in a case and the investigator will learn the critical steps needed to investigate Outlook, Exchange, Webmail, and even Lotus Notes e-mail cases.

Topics: Recover Deleted Files: Automated Recovery, String Searches, Dirty Word Searches; E-mail Forensics: How E-mail Works, Locations, Examination of E-mail, Types of E-mail 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, Firefox, and Google Chrome Browser Forensics. Learn how to examine exactly what an individual did while surfing via their Web browser, even if "private browsing" is enabled. 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: Digital Forensics Challenge

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

GCFE — www.giac.org

SANS INSTITUTE — www.sans.edu

SANS DFIR
DIGITAL FORENSICS & INCIDENT RESPONSE
http://computer-forensics.sans.org

FORENSICS 508

Hands-On | Six Days | Laptop Required | 36 CPE/CMU Credits | GIAC Cert: GCFA

FOR508:
Advanced Computer Forensic Analysis and Incident Response

This course focuses on providing incident responders with the necessary skills to hunt down and counter a wide range of threats within enterprise networks, including economic espionage, hactivism, and financial crime syndicates. The completely updated FOR508 addresses today's incidents by providing real-life, hands-on response tactics.

DAY 0: A 3-letter government agency contacts you to say that critical information was stolen from a targeted attack on your organization. Don't ask how they know, but they tell you that there are several breached systems within your enterprise. You are compromised by an Advanced Persistent Threat, aka an APT – the most sophisticated threat you are likely to face in your efforts to defend your systems and data.

"The examples in the course relate to what I need to know to deal with real-world threats"
-Tim Weaver, Digital Mtn. Inc.

Over 90% of all breach victims learn of a compromise from third party notification, not from internal security teams. In most cases, adversaries have been rummaging through your network undetected for months or even years. Gather your team—it's time to go hunting.

FOR508: Advanced Computer Forensic Analysis and Incident Response will help you determine:

- **How did the breach occur?**
- **What did they take? What did they change?**
- **What systems were compromised?**
- **How do we remediate the incident?**

The updated FOR508 trains digital forensic analysts and incident response teams to identify, contain, and remediate sophisticated threats—including APT groups and financial crime syndicates. A hands-on lab—developed from a real-world targeted attack on an enterprise network—leads you through the challenges and solutions. You will identify where the initial targeted attack occurred and which systems an APT group compromised. The course will prepare you to find out which data was stolen and by whom, contain the threat, and provide your organization the capabilities to manage and counter the attack.

"The SANS FOR508 course exceeded my expectations in every way. It provided me the skills, knowledge, and tools to effectively respond to and handle apts and other enterprise-wide threats."
-Josh Moulin, NSTEC/NNSA/DOE

During a targeted attack, an organization needs the best incident responders and forensic analysts in the field. FOR508 will train you and your team to be ready to do this work.

You Will Be Able To

- Apply incident response processes, threat intelligence, and digital forensics to investigate breached enterprise environments from Advanced Persistent Threat (APT) groups, organized crime syndicates, or hackivists
- Discover every system compromised in your enterprise utilizing incident response tools such as F-Response and digital forensic analysis capabilities in the SIFT Workstation to identify APT beachhead and spear phishing attack mechanisms, lateral movement, and data exfiltration techniques
- Use the SIFT Workstation's capabilities, perform forensic analysis and incident response on any remote enterprise hard drive or system memory without having to image the system first, allowing for immediate response and scalable analysis to take place across the enterprise
- Use system memory and the Volatility™ toolset to discover active malware on a system, determine how the malware was placed there, and recover it to help develop key threat intelligence to perform proper scoping activities during incident response
- Detect advanced capabilities such as Stuxnet, TDSS, or APT command and control malware immediately through memory analysis using least frequency of occurrence techniques and Redline's Malware Rating Index (MRI) to quickly ascertain the threat to your organization and aid in scoping the true extent of the data breach
- Track the exact footprints of an attacker crossing multiple systems and observe data they have collected to exfiltrate as you track your adversary's movements in your network via timeline analysis using the log2timeline toolset
- Begin recovery and remediation of the compromise via the use of Indicators of Compromise (IOC), Threat Intelligence, and IR/Forensics key scanning techniques to identify active malware and all enterprise systems affected by the breach
- Perform filesystem surgery using the sleuthkit tool to discover how filesystems work and uncover powerful forensic artifacts such as NTFS $I30 directory file indexes, journal parsing, and detailed Master File Table analysis
- Use volume shadow snapshot examinations, XP restore point analysis, and NTFS examination tools in the SIFT Workstation, recover artifacts hidden by anti-forensic techniques such as timestomping, file wiping, rootkit hiding, and privacy cleaning
- Discover an adversary's persistence mechanisms to allow malware to continue to run on a system after a reboot using command-line tools such as autorunsc, psexec, jobparser, group policy, triage-ir, and IOCFinder

Who Should Attend

- Information security professionals
- Incident response team members
- Responders investigating the APT across an enterprise network
- Experienced digital forensic analysts
- Federal agents and law enforcement
- Red team members, penetration testers, and exploit developers
- SANS FOR408 and SEC504 graduates
- Leaders of incident handling teams

Course Day Descriptions

508.1 Hands On: Enterprise Incident Response

Incident responders should be armed with the latest tools, memory analysis techniques, and enterprise scanning methodologies in order to identify, track and contain advanced adversaries, and remediate incidents. Incident response and forensic analysts responding must be able to scale their examinations from the traditional one analyst per system toward one analyst per 1,000 or more systems. Enterprise scanning techniques are now a requirement to track targeted attacks by an APT group or crime syndicate groups which propagate through thousands of systems.

Topics: SIFT Workstation Overview; Incident Response Methodology; Threat and Adversary Intelligence; Intrusion Digital Forensics Methodology; Remote and Enterprise IR System Analysis; Windows Live Incident Response

508.2 Hands On: Memory Forensics

Critical to many IR teams detecting advanced threats in the organization, memory forensics has come a long way in just a few years. It can be extraordinarily effective at finding evidence of worms, rootkits, and advanced malware used by an APT group of attackers. While traditionally solely the domain of Windows internals experts, recent tools now make memory analysis feasible for anyone. Better interfaces, documentation, and built-in detection heuristics have greatly leveled the playing field. This section will introduce some of the newest free tools available and give you a solid foundation in adding core and advanced memory forensic skills to your incident response and forensics armory.

Topics: Memory Acquisition and Analysis; Memory Analysis Techniques with Redline; Live Memory Forensics; Advanced Memory Analysis with Volatility™

508.3 Hands On: Timeline Analysis

Timeline Analysis will change the way you approach digital forensics and incident response… forever. Learn advanced analysis techniques uncovered via timeline analysis directly from the developers that pioneered timeline analysis tradecraft. Temporal data is located everywhere on a computer system. Filesystem modified/access/creation/change times, log files, network data, registry data, and, internet history files all contain time data that can be correlated into critical analysis to successfully solve cases. New timeline analysis frameworks provide the means to conduct simultaneous examinations of a multitude of time based artifacts. Analysis that once took days now takes minutes. This section will step you through the two primary methods of creating and analyzing timelines created during advanced incidents and forensic 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: Deep Dive Forensics and Anti-Forensics Detection

A major criticism of digital forensic professionals is 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; Deep Dive Forensics Analysis; Data Layer Analysis; Stream-Based Data Carving; File-Based Data Carving; NTFS Filesystem Analysis; FAT/exFAT Filesystem Overview

508.5 Hands On: Intrusion Forensics

The adversaries are good, we must be better. Over the years, we have observed that many incident responders have a challenging time finding malware without effective indicators of compromise (IOCs) or threat intelligence gathered prior to a breach. This is especially true in APT group intrusions. This advanced session will demonstrate techniques used by first responders to discover malware or forensic artifacts when very little information exists about their capabilities or hidden locations. We will discuss techniques to help funnel possibilities down to the candidates most likely to be evil malware trying to hide on the system.

Topics: Windows XP Restore Point Analysis; VISTA , Windows 7, Server 2008 Shadow Volume Copy Analysis; Deep Dive Forensics Analysis; Data Layer Analysis; Stream-Based Data Carving; File-Based Data Carving; NTFS Filesystem Analysis; FAT/exFAT Filesystem Overview

508.6 Hands On: The Incident Response & Intrusion Forensic Challenge

This brand new exercise brings together some of the most exciting techniques learned earlier in the week and tests your newly acquired skills in a case that simulates an attack by an advanced adversary such as an APT. This challenge brings it all together using a simulated intrusion into a real enterprise environment consisting of multiple Windows systems. You will be asked to uncover how the systems were compromised in the initial intrusion, find other systems the adversary moved to laterally, and identify intellectual property stolen via data exfiltration. You will walk out of the course with hands-on experience investigating realistic scenarios, which were put together by a cadre of individuals with many years of experience fighting advanced threats such as an APT group.

www.giac.org | www.sans.edu | SANS DFIR DIGITAL FORENSICS & INCIDENT RESPONSE http://computer-forensics.sans.org

FOR526: Windows Memory Forensics In-Depth

FOR526 - Memory Analysis In-Depth is a critical course for any serious investigator who wishes to tackle advanced forensic and incident response cases. Memory analysis is now a crucial skill for any investigator who is analyzing intrusions.

"The presentation, exercises, labs, and data provided are the best in the computer forensics industry."
-Rebecca Passmore FBI

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 by learning about memory structures and context, memory analysis methods, and the current tools used to parse system ram.

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. 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.

"This is the best SANS course I have taken so far with the best instructor. I hope to take more classes in the future."
-Jonathan Hinson, Duke Energy

FOR526 - Memory Analysis In-Depth is one of the most advanced courses in the SANS Digital Forensics and Incident Response Curriculum. This cutting-edge course covers everything you need to step through memory analysis like a pro.

You Will Be Able To

- Utilize stream-based data parsing tools to extract AES-encryption keys from a physical memory image to aid in the decryption of encryption files & volumes such as TrueCrypt & BitLocker
- Gain insight into the current network activity of the host system by retrieving network packets from a physical memory image and examining it with a network packet analyzer
- Inspect a Windows crash dump to discern processes, process objects and current system state at the time of crash through use of various debugging tools such as kd,WinDBG, and livekd
- Conduct Live System Memory Analysis with the powerful SysInternal's tool, Process Explorer, to collect real-time data on running processes allowing for rapid triage
- Use the SIFT workstation and in-depth knowledge of PE File modules in physical memory, extract and analyze packed and non-packed PE binaries from memory and compare them to their known disk-bound files
- Discover key features from memory such as the BIOS keyboard buffer, Kernel Debugging Data Block (KDBG), Executive Process (EPROCESS) structures, and handles based on signature and offset searching, gaining a deeper understanding of the inner workings of popular memory analysis tools
- Analyze memory structures using high-level and low-level techniques to reveal hidden and terminated processes and extract processes, drivers, and memory sections for further analysis
- Use a variety of means to capture memory images in the field, explaining the advantages and limitations of each method

Who Should Attend

- Incident response team members
- Law enforcement officers
- Forensic examiners
- Malware analysts
- Information technology professionals
- System administrators
- Anybody who plays a part in the acquisition, preservation, forensics, or analysis of Microsoft Windows computers

Course Day Descriptions

526.1 Hands On: Unstructured Memory

Memory forensics is the study of operating systems, and operating systems, in turn, work extensively with the processor and its architecture. Before we can begin a meaningful analysis of the operating system, we must therefore understand how the underlying components work and fit together. This section explains a number of technologies that are used in modern computers and how they have evolved to where they are today. Computer memory is a fantastic resource for the forensic investigator even without considering any operating system structures. There are data in memory that are simply not found anywhere else. Without even knowing which operating system was being used, an examiner can glean information that could be critical to a case. These data are generated by the underlying architecture or standards outside of the operating system. In particular, we focus on encryption keys and network packets. These two resources are not part of traditional forensics, but can provide invaluable data to the memory forensics investigator! While conducting brute force searches for these structures, we are also starting to gather data for examining the operating system later on. Unlike disk forensics, there is no volume header to parse in memory. Instead, we must find values created by the operating system by searching for them manually. There are a number of structures that we can search for which will help us determine what operating system was being used, and the values particular to this execution.

Topics: Computer Architectures; Virtual Memory Models; Implementing the Virtual Memory Model; Process Memory; System Memory; BIOS Keyboard Buffer; Encryption Keys; Network Packets; Traditional Data; Preparing for Structured Analysis; The SIFT Workstation; Pool Memory; Walking vs. Scanning

526.2 Hands On: User Visible Structures

Most users are familiar with processes on a Windows system, but not necessarily with how they work under the hood. In this section, we will talk about the operating system components that make up a process, how they fit together, and how they can be exploited by malicious software. We will start with the basics of each process, how it was started, where the executable lives, and what command line options were used. Next will be the Dynamic Link Libraries (DLLs) used by a program and how they are found and loaded by the operating system. Finally, we will talk about the operating system structures involved with threads, the actual blocks of executing code that make up the interactive portion of every process.

Topics: Processes; Dynamic-link Libraries (DLLs); Drivers; Sockets; Kernel Objects; Threads

526.3 Hands On: Operating System Internals

There are a tremendous number of structures used in Microsoft Windows. To understand what the operating system is doing, we have to understand these components. In this section we will begin to explore the complex web of interconnected data structures which make up the operating system. To that end we start with a basic introduction to C structures and how they are put together. From there we talk about which of them are used in Windows and the documentation Microsoft publishes about them. In this section we will explore, in-depth, all of the components which constitute Microsoft Windows operating systems. We will start with processes and all of the data they contain. From there we will discuss DLLs, drivers, sockets, kernel objects, threads, modules, and virtual address descriptors. For each of these areas we will talk about how these systems work, what data the operating system maintains, which of those are relevant for forensics, and how to determine if there is something suspicious occurring.

Topics: Introduction to C Structures; Microsoft Structures; Tools for Structures; Modules; Injected and Unpacked Code; Finding hidden DLLs; Finding Hidden Processes; Driver Hooking

526.4 Hands On: Memory Forensics in the Real World

Knowing the basics of memory forensics allows us to begin doing it in the real world. First, we must acquire memory images. On any given system there may already be memory images, from the machine's past, which contain highly valuable information. In this section we will discuss how to find and recover such memory images. We'll also cover some of the tools to capture memory images and how to choose the one which is best for you.

Topics: The Windows Registry; Hibernation Files; Crash Dump Files; Memory Imaging; Traditional Imaging Programs; Suspended Virtual Machine; USB; Firewire; Cold Boot Method

526.5 Hands On: Memory Challenges

This section will present a number of challenges for the memory forensic examiner. We do not want to spoil all of the surprises by listing them in the outline, but we can give you a sense of what you will be working on. These memory images may contain some kind of malicious software or data of interest. Each challenge will provide a little information to go on. (As with real-world examinations, of course, it's never enough information!) Your job will be to determine if there is anything of interest, and if so, what it is.

"Totally awesome, relevant and eye opening. I want to learn more every day."
-Matthew Britton,
Blue Cross Blue Shield of Louisiana

SANS DFIR
DIGITAL FORENSICS & INCIDENT RESPONSE
http://computer-forensics.sans.org

New Content Added

FORENSICS 610 LEARN

Hands-On | Six Days | Laptop Required | 36 CPE/CMU Credits | GIAC Cert: GREM

FOR610:

Reverse-Engineering Malware: Malware Analysis Tools & Techniques

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!

"The exercises and examples are very good and useful to get a better understanding of code analysis. Definitely one of the best courses I've attended on this topic."

-Thor Olsen, Norwegian Police Security Services

The malware analysis process taught in this class helps incident responders assess the severity and repercussions of a situation that involves malicious software and plan recovery steps. Forensics investigators also learn how to understand key characteristics of malware discovered during the examination, including how to establish indicators of compromise (IOCs) for scoping and containing the incident.

"This class gave me essential tools that I can immediately apply to protect my organization."

-Don Lopez, Valley National Bank

Hands-On Training for Malware Analysis and Reversing

Hands-on workshop exercises are a critical aspect of this course and allow you to apply reverse-engineering techniques by examining malware in a controlled environment. When performing the exercises, you'll study the supplied specimen's behavioral patterns and examine key portions of its code. You'll examine malware on a Windows virtual machine that you'll infect during the course and will use the supplied Linux virtual machine REMnux that includes tools for examining and interacting with malware.

Complexity of the Course: Formalizing and Expanding Your Malware Analysis Skills

While the field of reverse-engineering malware is in itself advanced, the course begins by covering this topic from an introductory level and quickly progresses to discuss tools and techniques of intermediate complexity. Overall, the goal of the course is to act as a practical way for the motivated technologists to enter the field of malware analysis and reversing.

Neither programming experience nor the knowledge of assembly is required to benefit from the course. However, you should have a general idea about core programming concepts, such as variables, loops and functions. The course spends some time discussing essential aspects of Intel assembly to allow malware analysts to navigate through malicious executables using a debugger and a disassembler.

You Will Be Able To

- Build an isolated laboratory environment for analyzing code and behavior of malicious programs
- Employ network and system-monitoring tools to examine how malware interacts with the file system, the registry, the network and other processes on Microsoft Windows
- Uncover and analyze malicious JavaScript, VB Script and ActionScript components of web pages, which are often used as part of drive-by attacks
- Control some aspect of the malicious program's behavior through network traffic interception and code patching
- Use a disassembler and a debugger to examine inner-workings of malicious Windows executables
- Bypass a variety of defensive mechanisms designed by malware authors to misdirect, confuse and otherwise slow down the analyst
- Recognize and understand common assembly-level patterns in malicious code, such as DLL injection
- Assess the threat associated with malicious documents, such as PDF and Microsoft Office files in the context of targeted attacks
- Derive Indicators of Compromise (IOCs) from malicious executables to contain and recover from the incident
- Utilize practical memory forensics techniques to examine capabilities of rootkits

Who Should Attend

- Incident response team members
- Law enforcement officers
- Forensic examiners
- Malware analysts
- Information technology professionals
- System administrators
- Software Engineers
- Ethical Hackers

Course Day Descriptions

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 for malware forensics; Performing behavioral analysis of malicious Windows executables; Performing static and dynamic code analysis of malicious Windows executables; Additional learning resources for reverse-engineering malware

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. And you'll 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 learned in 610.1; Patching compiled malicious Windows executables; Analyzing packed malicious executable files; Intercepting network connections in the malware lab; Analyzing Web browser malware implemented in JavaScript and Flash

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 malicious Windows executables.

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; Manual unpacking of packed and otherwise protected malicious Windows executables; Tips and tricks for bypassing anti-analysis mechanisms built into malware; Additional techniques for analyzing obfuscated browser scripts using tools such as SpiderMonkey

610.5 Hands On: Malicious Documents and Memory Forensics

Day five starts by exploring common patterns of assembly instructions often used to gain initial access to the victims computer. Next, we will learn how to analyze malicious Microsoft Office documents, covering tools such as OfficeMalScanner and explore steps for analyzing malicious PDF documents with utilities such as Origami and PDF Tools. Another major topic covered in this section is the reversing of malicious Windows executables using memory forensics techniques. We will explore this topic with the help of tools such the Volatility™ Framework and associated plug-ins. The discussion of memory forensics will bring us deeper into the world of user and kernel-mode rootkits and allow us to use context of the infection to reverse-engineer malware more efficiently.

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

610.6 Hands On: Malware Reverse-Engineering Challenge

Day six assigns students to the role of a malware reverse engineer, working as a member of an incident response and malware analysis team. Students are presented with a variety of challenges involving real-world malware. These challenges validate students ability to respond to typical malware reversing tasks in an instructor-led lab environment and offer additional learning opportunities. The challenges are designed to reinforce skills covered in the first five sections of the course, making use of the hugely popular SANS NetWars tournament platform. By applying the techniques learned earlier in the course, students solidify their knowledge and can shore up skill areas where they feel they need additional practice.

Topics: Behavioral Malware Analysis; Dynamic Malware Analysis (using a debugger); Static Malware Analysis (using a disassembler); JavaScript Deobfuscation; PDF Document Analysis; Office Document Analysis; Flash File Analysis; Memory Analysis

GIAC Reverse Engineering Malware GREM

www.giac.org

SANS Technology Institute Knowledge for Peace

www.sans.edu

SANS DFIR

DIGITAL FORENSICS & INCIDENT RESPONSE

http://computer-forensics.sans.org

SANS DFIR

DIGITAL FORENSICS & INCIDENT RESPONSE

Upcoming Courses

FOR518: MAC and iOS Forensics

Hands-On | 6 Days | Laptop Required | 36 CPE/CMU Credits

This course is intended to form a well-rounded investigator with the introduction of Mac forensics into a Windows forensics world. This course will focus on Macintosh basics, the HFS+ file system, analysis and correlation of Mac logs and data files and tracking user activity. Completion of the course will allow a computer forensic analyst the skills needed to take on a Mac forensics case.

Course Topics:

- In-depth Hierarchical File System Examination
- File System Timeline Analysis
- Advanced Computer Forensics Methodology
- Mac-specific Acquisition and Incident Response Collection
- Mac Memory Acquisition and Analysis
- File System and Data Layer Examination
- Metadata and File Name Layer Examination
- Recovering Key Mac Files
- Volume and Disk Image Analysis
- Analysis of Mac Technologies including Time Machine and FileVault
- dvanced Log Analysis and Correlation
- iDevice Backup Analysis and Artifacts
- Forensic Artifacts of Mac OS X Server

FOR559: Cloud Forensics & Incident Response

Hands-On | 6 Days | Laptop Required | 36 CPE/CMU Credits

This course will focus on both the collection of evidence in a sound manner from a Private and Public Cloud environment for external analysis as well as performing the complete evidence collection, IR and Forensics Analysis "within" a Private and Public Cloud environment (all work is performed within the Cloud).

Course Topics:

- Forensics In "End-user / Retail" Cloud Storage
- Cloud Forensics Challenges – Incident Response Perspective
- IR & Forensics - VMware & HyperV Private Clouds
- Cloud Forensics Organizational Structure
- SLA Considerations
- Cloud Models – IAAS, PAAS, SAAS
- Key Issues In Cloud Forensics
- Cloud IR & Forensics – Amazon, Azure, OpenStack and RackSpace
- Cloud Forensics Challenge

FOR572: Advanced Network Forensics and Analysis

Hands-On | 6 Days | Laptop Required | 36 CPE/CMU Credits

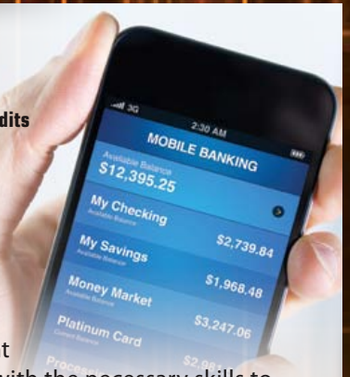
The network is a common domain for almost all modern attacks. Even if a savvy attacker effectively hides their tracks on a compromised system, or the system has long been wiped, the network evidence remains - and is usually more than needed to conduct a thorough investigation. This course will teach students to follow an attacker's footprints and analyze evidence from a networked environment. During hands on exercises, you will use tools such as tcpdump, Wireshark, Snort, tcpxtract. You'll analyze netflow data, logging servers, as well as pcap files to understand the attacks and reconstruct the incident without ever using an endpoint's hard drive. Students will build and use skills from across the forensic and investigative domains using a modified Linux SIFT Workstation VM.

Course Topics:

- Carve files from packet capture
- Wireless Networking
- tcpdump and wireshark hands-on
- Network Architectural Challenges and Opportunities
- HTTPS / SSL Inspection
- Netflow Analysis
- Visualization tools and techniques
- Log data collection, aggregation and analysis
- Encrypted traffic flow analysis (SSL, IPSEC, PPTP, etc)
- Automated tool exercises

FOR585: Advanced Smartphone & Mobile Device Forensics

Hands-On | 6 Days | Laptop Required | 36 CPE/CMU Credits



Since smartphones and other mobile devices can contain details about who was doing what, where and when, their usefulness as a source of information in any investigation should never be underestimated.

This course focuses on smartphones as sources of evidence, providing forensic practitioners, incident responders, and computer security professionals with the necessary skills to handle smartphones and other mobile devices in a forensically sound manner, to acquire and examine digital evidence from these devices, and to analyze the results for use in digital investigations. Students will be able to recover and analyze data for use in internal investigations, criminal and civil litigation, investigation and resolution of security breaches, and to obtain actionable intelligence. FOR585 addresses today's smartphone technologies and threats by providing real-life, hands-on investigative scenarios.

Additional New Courses!

- Cyber Threat Intelligence
- Offensive & Anti- Forensics

Find complete info on all DFIR courses at http://computer-forensics.sans.org

Computer Forensics Resources

http://computer-forensics.sans.org/community/links

SANS Forensic Community provides analysts with a variety of forensic resources. Interact with your fellow analysts and forensic experts on the SANS Forensic Blog, discover solutions to forensic related issues with a multitude of White Papers, or peruse a variety of industry related news and blog sites. SANS is continually updating and adding information to this site, so check back often to see what's new.

Join The SANS DFIR Community

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

Twitter: @sansforensics

Facebook: sansforensics

Google+: Search SANS Digital Forensics and Incident Response

Mailing list: https://lists.sans.org/mailman/listinfo/dfir

Computer Forensic News

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.

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

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

Newsletters:
http://www.sans.org/newsletters

- **SANS NewsBites**
- **@RISK: The Consensus Security Alert**
- **Ouch!**

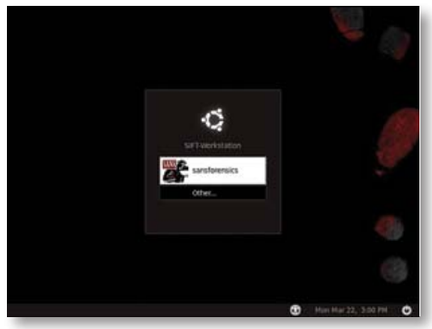
Computer Forensics Poster

SIFT Workstation

SANS Investigative Forensic Toolkit

http://computer-forensics.sans.org/community/downloads

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 **FOR408: Computer Forensic Investigations - Windows In-Depth**, **FOR508: Advanced Computer Forensic Analysis and Incident Response**, and **FOR526: Windows Memory Forensics In-Depth** courses 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 100s of additional tools**

SANS SIFT WORKSTATION CHEAT SHEET V3.0

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
- Stream Extraction
- Shadow Timeline Creation
- Creating Supert Timelines
- Mounting Volume Shadow Copies
- String Searches
- Memory Analysis
- Sleuthkit Tools

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
`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 -o
loop,ro,show_sys_files,streams_interface=windows
imagefile.dd /mnt/windows_mount
```

MOUNTING E01 IMAGES

```
# ewfmount image.E01 mountpoint
```

```
# mount -o
loop,ro,show_sys_files,streams_interface=windows
/mnt/ewf/ewf1 /mnt/windows_mount
```

MOUNTING VOLUME SHADOW COPIES

Stage 1 – Attach local or remote system drive

```
# ewfmount system-name.E01 /mnt/ewf
```

Stage 2 – Mount raw image VSS

```
# vshadowmount ewf1 /mnt/vss/
```

Stage 3 – Mount all logical filesystem of snapshot

```
# cd /mnt/vss
# for i in vss*; do mount -o
ro,loop,show_sys_files,streams_interface=
windows $i /mnt/shadow_mount/$i; done
```

RECOVER DELETED REGISTRY KEYS

 # deleted.pl <*HIVEFILE*>

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


CREATING SUPER TIMELINES

```
# log2timeline -r -p -z <system-timezone>
-f <type-input> /mnt/windows_mount -w
timeline.csv
```

file|dir		artifact target
-f	<TYPE-INPUT>	input format
-o	<TYPE-OUTPUT>	output format: default csv file
-w	<FILE>	append to log file
-z	<SYSTEM TIMEZONE>	
-Z	<OUTPUT TIMEZONE>	
-r		recursive mode
-p		preprocessors

```
# mount -o
loop,ro,show_sys_files,streams_interface=windows
imagefile.dd /mnt/windows_mount
```

```
# log2timeline -z EST5EDT -p -r -f win7
/mnt/windows_mount -w /cases/bodyfile.txt
```

```
# l2t_process -b /cases/bodyfile.txt -w
whitelist.txt 04-02-2012 > timeline.csv
```

STREAM EXTRACTION

```
# bulk_extractor <options> -o output_dir image
```

[Useful Options]	
`-o outdir`	
`-f <regex>`	regular expression term
`-F <rfile>`	file of regex terms
`-Wn1:n2`	extract words between n1 and n2 in length
`-q nn`	quiet mode
`-e scanner`	enables a scanner
`-e wordlist`	enable scanner wordlist
`-e aes`	enable scanner aes
`-e net`	enable scanner net

```
# bulk_extractor -F keywords.txt -e net
-e aes -e wordlist -o /cases/bulk-
extractor-memory-output /cases/
memory-raw.001
```

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
```

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
```

SHADOW TIMELINE CREATION

Step 1 – Attach Local or Remote System Drive

```
# ewfmount system-name.E01 /mnt/ewf
```

Step 2 – Mount VSS Volume

```
# cd /mnt/ewf
# vshadowmount ewf1 /mnt/vss
```

Step 3 – Run fls across ewf1 mounted image

```
# cd /mnt/ewf
# fls -r -m C: ewf1 >> /cases/vss-
bodyfile
```

Step 4 – Run fls Across All Snapshot Images

```
# cd /mnt/vss
# for i in vss*; do fls -r -m C: $i
>> /cases/vss-bodyfile; done
```

Step 5 – De-Duplicate Bodyfile using sort and uniq

```
# sort /cases/vss-bodyfile | uniq >
/cases/vss-dedupe-bodyfile
```

Step 6 – Run mactime Against De-Duplicated Bodyfile

```
# mactime -d -b /cases/vss-dedupe-
bodyfile -z EST5EDT MM-DD-YYYY..MM-
DD-YYYY > /cases/vss-timeline.csv
```

MEMORY ANALYSIS

```
vol.py command -f
/path/to/windows_xp_memory.img  --
profile=WinXPSP3x86
```

[Supported commands]

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

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`

TIME TO GO HUNTING

SANS MEMORY FORENSICS CHEAT SHEET V1.1

PURPOSE

This cheat sheet supports the SANS FOR508 Advanced Forensics and Incident Response and SANS FOR526 Memory Analysis courses. It is not intended to be an exhaustive resource of Volatility™ or other highlighted tools. Volatility™ is a trademark of Verizon. The SANS Institute is not sponsored or approved by, or affiliated with Verizon.

HOW TO USE THIS DOCUMENT

Memory analysis is one of the most powerful tools available to forensic examiners. This guide hopes to simplify the overwhelming number of available options.

Analysis can be generally broken up into six steps:

1. **Identify Rogue Processes**
2. **Analyze Process DLLs and Handles**
3. **Review Network Artifacts**
4. **Look for Evidence of Code Injection**
5. **Check for Signs of a Rootkit**
6. **Dump Suspicious Processes and Drivers**

We outline the most useful Volatility™ plugins supporting these six steps here. Further information is provided for:

- **Memory Acquisition**
- **Converting Hibernation Files and Crash Dumps**
- **Memory Artifact Timelining**
- **Registry Analysis Volatility™ Plugins**
- **Memory Analysis Tool List**

MEMORY ACQUISITION

Remember to open command prompt as Administrator

Win32dd / Win64dd (x86 / x64 systems respectively)

`/f` Image destination and filename

```
C:\> win32dd.exe /f E:\mem.img
```

Mandiant Memoryze MemoryDD.bat

`-output` image destination

```
C:\> MemoryDD.bat -output E:\
```

Volatility™ WinPmem

`-` (single dash) Output to standard out

`-l` Load driver for live memory analysis

```
C:\> winpmem_<version>.exe E:\mem.img
```

CONVERTING HIBERNATION FILES AND CRASH DUMPS

Volatility™ **`imagecopy`**

`-f` Name of source file (crash dump, hibernation file, etc.)

`-O` Output file name

`--profile` Source OS from `imageinfo`

```
# vol.py imagecopy -f hiberfil.sys -O
hiber.img --profile=Win7SP1x64

# vol.py imagecopy -f Memory.dmp -O
memdmp.img --profile=Win7SP1x64
```

LOOK FOR EVIDENCE OF CODE INJECTION

`malfind` - Find injected code and dump sections

`-p` Show information only for specific PIDs

`-o` Provide physical offset of single process to scan

`--dump-dir` Directory to save extracted memory sections

```
# vol.py malfind --dump-dir ./output_dir
```

`ldrmodules` - Detect unlinked DLLs

`-p` Show information only for specific PIDs

`-v` Verbose: show full paths from three DLL lists

```
# vol.py ldrmodules -p 868 -v
```

MEMORY FORENSICS Cheat Sheet CONTINUED

MEMORY ANALYSIS TOOLS

Volatility™ (Windows/Linux/Mac)
`http://code.google.com/p/volatility/`

Mandiant Redline (Windows)
`http://www.mandiant.com/resources/download/redline`

Volafox (Mac OS X and BSD)
`http://code.google.com/p/volafox/`

GETTING STARTED WITH VOLATILITY™

Getting Help

```
# vol.py -h                  (show general options and supported plugins)
# vol.py plugin -h           (show plugin usage)
# vol.py plugin --info       (show available OS profiles)
```

Sample Command Line

```
# vol.py -f image --profile=profile plugin
```

Identify System Profile

```
imageinfo                    - Display memory image metadata
# vol.py -f mem.img imageinfo
```

Using Environment Variables

Set name of memory image (takes place of **-f**)

```
# export VOLATILITY_LOCATION=file:///images/mem.img
```

Set profile type (takes place of --profile=)

```
# export VOLATILITY_PROFILE=WinXPSP3x86
```

IDENTIFY ROGUE PROCESSES

pslist	- High level view of running processes	`# vol.py pslist`
psscan	- Scan memory for EPROCESS blocks	`# vol.py psscan`
pstree	- Display parent-process relationships	`# vol.py pstree`

CHECK FOR SIGNS OF A ROOTKIT

psxview - Find hidden processes using cross-view `# vol.py psxview`

driverscan - Scan memory for _DRIVER_OBJECTs `# vol.py driverscan`

apihooks - Find API/DLL function hooks
- **-p** Operate only on specific PIDs
- **-k** Scan kernel modules instead of user-mode objects

```
# vol.py apihooks
```

ssdt - Hooks in System Service Descriptor Table

```
# vol.py ssdt | egrep -v '(ntoskrnl|win32k)'
```

driverirp - Identify I/O Request Packet (IRP) hooks
- **-r** Analyze drivers matching REGEX name pattern

```
# vol.py driverirp -r tcpip
```

idt - Display Interrupt Descriptor Table `# vol.py idt`

ANALYZE PROCESS DLLS AND HANDLES

dlllist - List of loaded dlls by process
- **-p** Show information only for specific process identifiers (PIDs)

```
# vol.py dlllist -p 4,868
```

getsids - Print process security identifiers
- **-p** Show information only for specific PIDs

```
# vol.py getsids -p 868
```

handles - List of open handles for each process
- **-p** Show information only for specific PIDs
- **-t** Display only handles of a certain type {Process, Thread, Key, Event, File, Mutant, Token, Port, … }

```
# vol.py handles -p 868 -t Process,Mutant
```

filescan - Scan memory for FILE_OBJECT handles `# vol.py filescan`

svcscan - Scan for Windows Service information `# vol.py svcscan`

MEMORY FORENSICS Cheat Sheet CONTINUED

REVIEW NETWORK ARTIFACTS

connections	- [XP] List of open TCP connections	`# vol.py connections`
connscan	- [XP] ID TCP connections, including closed	`# vol.py connscan`
sockets	- [XP] Print listening sockets (any protocol)	`# vol.py sockets`
sockscan	- [XP] ID sockets, including closed/unlinked	`# vol.py sockscan`
netscan	- [Win7] Scan for connections and sockets	`# vol.py netscan`

DUMP SUSPICIOUS PROCESSES AND DRIVERS

dlldump - Extract DLLs from specific processes
- **-p** Dump DLLs only for specific PIDs
- **-b** Dump DLLs from process at physical memory offset
- **-r** Dump DLLs matching REGEX name pattern (case sensitive)
- **--dump-dir** Directory to save extracted files

```
# vol.py dlldump --dump-dir ./output -r metsrv
```

moddump - Extract kernel drivers
- **--dump-dir** Directory to save extracted files
- **-o** Dump driver using offset address (from `driverscan`)
- **-r** Dump drivers matching REGEX name pattern (case sensitive)

```
# vol.py moddump --dump-dir ./output -r gaopdx
```

procmemdump - Dump process to executable sample
- **-p** Dump only specific PIDs
- **-o** Specify process by physical memory offset
- **--dump-dir** Directory to save extracted files

```
# vol.py procmemdump --dump-dir ./out -p 868
```

memdump - Dump every memory section into a file
- **-p** Dump memory sections from these PIDs
- **--dump-dir** Directory to save extracted files

```
# vol.py memdump -dump-dir ./output -p 868
```

MEMORY ARTIFACT TIMELINING

The Volatility Timeliner plugin parses time-stamped objects found in memory images. Output is sorted by:

- **Process creation time**
- **Thread creation time**
- **Driver compile time**
- **DLL / EXE compile time**
- **Network socket creation time**
- **Memory resident registry key last write time**
- **Memory resident event log entry creation time**

timeliner
- **--output-file** Optional file to write output
- **--output=body** body for mactime

```
# vol.py -f mem.img timeliner --output-file out.csv
  --profile=Win7SP1x86
```

REGISTRY ANALYSIS VOLATILITY™ PLUGINS

hivelist - Find and list available registry hives `# vol.py hivelist`

hivedump - Print all keys and subkeys in a hive
- **-o** Offset of registry hive to dump (virtual offset from hivelist)

```
# vol.py hivedump -o 0xe1a14b60
```

printkey - Output a registry key, subkeys, and values
- **-K** "Registry key path"
- **-o** Only search hive at this offset (virtual offset from hivelist)

```
# vol.py printkey -K
"Software\Microsoft\Windows\CurrentVersion\Run"
```

userassist - Find and parse userassist key values
- **-o** Only search hive at this offset (virtual offset from hivelist)

```
# vol.py userassist
```

hashdump - Dump user NTLM and Lanman hashes
- **-y** Virtual offset of SYSTEM registry hive (from hivelist)
- **-s** Virtual offset of SAM registry hive (from hivelist)

```
# vol.py hashdump -y 0x8781c008 -s 0x87f6b9c8
```

Steve Armstrong *SANS Certified Instructor*

Steve began working in the security arena in 1994 whilst serving in the UK Royal Air Force. He specialized in the technical aspects of IT security from 1997 onward, and before retiring from active duty, he lead the RAF's penetration and TEMPEST testing teams. He founded Logically Secure in 2006 to provide specialist security advice to government departments, defense contractors, the online video gaming industry, and both music and film labels worldwide. When not teaching for SANS, Steve provides penetration testing and incident response services for some of the biggest household names in gaming and music media. To relax Steve enjoys playing Battlefield3 to the music of the Muppets.
@Nebulator

Ovie Carroll *SANS Certified 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. podcast: **cyberspeak.libsyn.com**

Mike Cloppert *SANS Instructor*

Michael is the lead analyst for Lockheed Martin CIRT's Intel Fusion team, charged with collecting and managing intelligence on adversaries intent on stealing the organization's intellectual property, and development of new detection and analysis techniques. Michael has worked as a security analyst in various sectors including the Financial, Federal Government, and Defense industries. He has an undergraduate degree in Computer Engineering from the University of Dayton, an MS in Computer Science from The George Washington University, has received a variety of industry certifications including SANS GCIA, GREM, and GCFA, and is a SANS Forensics and IR blog contributor. Michael's past speaking engagements include the DC3 Cybercrime Conference, IEEE, and SANS amongst various others.

Sarah Edwards *SANS Instructor*

Sarah is an senior digital forensic analyst who has worked with various federal law enforcement agencies. She has performed a variety of investigations including computer intrusions, criminal, counter-intelligence, counter-narcotic, and counter-terrorism. Sarah's research and analytical interests include Mac forensics, mobile device forensics, digital profiling and malware reverse engineering. Sarah has presented at the following industry conferences; Shmoocon, CEIC, TechnoSecurity and the SANS DFIR Summit. She has a Bachelor of Science in Information Technology from Rochester Institute of Technology and a Masters in Information Assurance from Capitol College.

Jess Garcia *SANS Certified Instructor*

Jess Garcia is the founder and technical lead of One eSecurity, a global Information Security company specialized in Incident Response and Computer Forensics. With near 20 years in the field, Jess has led the response and forensic investigation of some of the the world's biggest incidents in recent times. An active researcher in the Computer Forensics & Security fields, Jess is also a top-rated regular speaker in international conferences. Jess started his professional career as a Space Engineer after obtaining his MSc in Telecommunications Engineering, but soon changed fields to the even more exciting world of Information Security. **@j3ssgarcia**

Philip Hagen *SANS Instructor*

Philip Hagen has over 14 years experience in creating and deploying strategic and ad-hoc IT and information security solutions. He currently provides computer forensic, information security, and technology support to law enforcement, large and small corporate clients, as well as non profit organizations. In the past, he led a team of 85 computer forensic professionals supporting national security and law enforcement missions. Phil has provided technical services to various government offices covering a variety of exotic requirements in high-threat environments. He served in the US Air Force as a communications officer at the Pentagon and Beale AFB, CA. Phil holds a computer science degree from the US Air Force Academy.

Paul A. Henry *SANS Senior 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**

Nick Klein *SANS Instructor*

Nick is the Director of Klein & Co. Computer Forensics, the leading independent computer forensic team from Sydney, Australia. He has over fifteen years of IT experience, specialising in forensic technology investigations and presenting expert evidence in legal and other proceedings. Nick and his team have been engaged as an expert in hundreds of cases including commercial litigation and electronic discovery, criminal prosecution and defence, financial fraud, corruption, employee misconduct, theft of intellectual property, computer hacking and system intrusion.

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.
http://jessekornblum.livejournal.com **@jessekornblum**

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**

Heather Mahalik *SANS Certified Instructor*

Heather Mahalik is the Lead Digital Forensics Analyst at Basis Technology. She currently conducts advanced acquisitions and investigations on media and mobile devices supporting efforts in the U.S. Government. She earned her BS is Forensic and Investigative Science from West Virginia University in 2002. Heather is a certified forensic examiner (CFCE, EnCE and MFCE) and has worked in digital forensics since 2002 and has performed hundreds of forensic acquisitions and examinations on hard drives, e-mail and file servers, mobile devices and portable media related to criminal and civil investigations, e-discovery, intrusions and other crimes. She has authored articles, papers and instructed classes focused on Mac Forensics, Mobile Forensics, and Computer Forensics to practitioners in the field. **@HeatherMahalik**

Cindy Murphy *SANS Instructor*

Detective Cindy Murphy works for the City of Madison, WI Police Department and has been a Law Enforcement Officer since 1985. She is a certified forensic examiner (EnCE, CCFT, DFCP), and has been involved in computer forensics since 1999. She earned her MSc in Forensic Computing and Cyber Crime Investigation through University College, Dublin in 2011. She has directly participated in the examination of many hundreds of hard drives, cell phones, and other items of digital evidence pursuant to criminal investigations including homicides, missing persons, computer intrusions, sexual assaults, child pornography, financial crimes, and various other crimes. She has testified as a computer forensics expert in state and federal court on numerous occasions, using her knowledge and skills to assist in the successful investigation and prosecution of criminal cases involving digital evidence. She is also a part time digital forensics instructor at Madison College, and a part time Mobile Device Forensics instructor for the SANS Institute. **@cindymurph**

Mike Pilkington *SANS Instructor*

Mike Pilkington is a Senior Security Consultant for a Fortune 500 company in the oil & gas industry. He has been an IT professional since graduating in 1996 from the University of Texas with a B.S. in Mechanical Engineering. Since joining his company in 1997, he has been involved in software quality assurance, systems administration, network administration, and information security. Outside of his normal work schedule, Mike has also been involved with the SANS Institute as a mentor and instructor in the digital forensics program. **@mikepilkington**

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://www.deer-run.com/~hal **@hal_pomeranz**

SANS DFIR Faculty

Christian Prickaerts *SANS Instructor*

Christian's background stems from the academic world where he held a position as senior sysadmin for several years. During this time he also actively performed CERT duties. Christian has been active as a forensic IT investigator since 2004. He leads and actively participates in (digital) forensic IT investigations. Christian has a broad knowledge-base of operating systems and network protocols. He regularly gives presentations on the subject of IT security and IT forensics. As a teacher he also lectures on the subject of open-source intelligence using Internet sources. As an expert witness he is called upon to provide expert testimony in court on occasion. Working for both law enforcement and the private sector his experience in Forensic IT is broad.

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 twelve years responding to computer intrusions and conducting 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 and conducted computer forensics for a variety of 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 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 B.S. and M.S. in Computer Science as well as GCFA, GCIH, GREM, and ENCE certifications. He is currently a consultant specializing in incident response, corporate espionage, and computer forensics. http://forensicmethods.com @chadtilbury

Alissa Torres *SANS Certified Instructor*

Alissa Torres is a certified SANS Instructor and Incident Handler at Mandiant, finding evil on a daily basis. She previously worked as a security researcher at KEYW Corporation, leading research and development initiatives in forensic and offensive methodologies and is co-founder of Torrora, LLC, a forensics consulting company. Prior to KEYW, Alissa performed digital forensic investigations and incident response for a large contractor in the Defense Industrial Base. Alissa began her career in information security as a Communications Officer in the United States Marine Corps and is a graduate of University of Virginia and University of Maryland. As an accomplished instructor, Alissa has taught for various government agencies on topics to include digital forensics, incident response, and offensive methodologies, and is a frequent speaker at industry conferences. In addition to being a GIAC Certified Forensic Analyst (GCFA), she holds the GCFE, GPEN, CISSP, EnCE, CFCE, MCT and CTT+. @sibertor

Jake Williams *SANS Instructor*

Jake Williams is a technical analyst with the Department of Defense (DoD) where he has over a decade of experience in systems engineering, computer security, forensics, and malware analysis. Jake has been providing technical instruction for years, primarily with HBGary, where he was the principal courseware developer and instructor for their products. He also maintains malware reverse engineering courses for CSRgroup Computer Security Consultants. Recently, he has been researching the application of digital forensic techniques to public and private cloud environments. Jake has been involved in numerous incident response events with industry partners in various consulting roles. Jake led the winning government team for the 2011 and 2012 DC3 Digital Forensics Challenge. He has spoken at numerous events, including the ISSA events, SANS @Night, the DC3 conference, Shmoocon, and Blackhat. @MalwareJake

Lenny Zeltser *SANS Senior Instructor*

Lenny is a seasoned business and tech leader with extensive experience in information technology and security. His areas of expertise include incident response, cloud services and product management. Lenny focuses on safeguarding customers' IT operations at NCR Corporation. He also is also a senior faculty member at SANS. Lenny frequently speaks at conferences, writes articles and has co-authored books on forensics, malware and network security. He has earned the prestigious GIAC Security Expert designation, has an MBA from MIT Sloan and a Computer Science degree from the University of Pennsylvania. You can explore Lenny's projects on www.zeltser.com.
http://blog.zeltser.com @lennyzeltser

GIAC certified professionals are sought by global industries, governments, and the Department of Defense.

Get Certified!

www.giac.org

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 incident responders 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

DFIR NetWars

SANS DFIR NetWars is a hands-on, interactive learning environment that enables Digital Forensics and Incident Response (DFIR) professionals to develop and master the skills they need to excel in their field.

DFIR NetWars is designed to help participants develop skills in several DFIR critical areas:

- **Malware Analysis**
- **Incident Response**
- **Digital Forensics**
- **File and Packet Analysis**

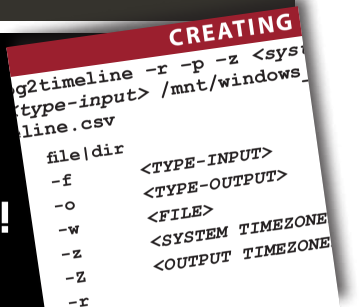
http://computer-forensics.sans.org/training/netwars

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

SIFT Workstation & Memory Forensics Cheat Sheets Inside!



SANS
5705 Salem Run Blvd.
Suite 105
Fredericksburg, VA 22407

PROMO CODE

FOR13

Register using this Promo Code