SANS DFIR

DIGITAL FORENSICS & INCIDENT RESPONSE

COURSE CATALOG

SANS DFIR Curriculum

SANS Digital Forensics and Incident Response DFIR 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.

CORE

FOR408
Windows Forensics
GCFE

SEC504
Hacker Techniques, Exploits, and Incident Handling
GCIH

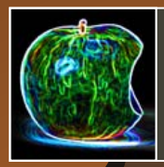
IN-DEPTH

FOR508
Advanced Incident Response
GCFA

FOR572
Advanced Network Forensics and Analysis
GNFA

FOR610
REM: Malware Analysis
GREM

SPECIALIZATION



FOR518
Mac Forensics

FOR526
Memory Forensics In-Depth

FOR585
Advanced Smartphone Forensics

Join The SANS DFIR Community

Blog: dfir.to/DFIRBlog
Google+: gplus.to/sansforensics
Twitter: @sansforensics
Mailing list: dfir.to/MAIL-LIST
Facebook: sansforensics
YouTube: dfir.to/DFIRCast

FIGHT CRIME

Unravel incidents... one byte at a time.

digital-forensics.sans.org

Rob Lee

Dear Colleague,

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
Digital Forensics and Incident Response Lead

Contents

Windows Forensics Analysis

FOR408

Master Computer Forensics.
What Do You Want to Uncover Today?

Every organization will deal with cyber-crime occurring on the latest Windows operating systems. Analysts will investigate crimes including fraud, insider threats, industrial espionage, traditional crimes, and computer hacking. Government agencies use media exploitation of Windows systems to recover key intelligence available on adversary systems. To help solve these cases, organizations are hiring digital forensic professionals, investigators, and agents to uncover what happened on a system.

FOR408: Windows Forensic Analysis focuses on critical knowledge of the Windows OS that every digital forensic analyst must know in order to investigate computer incidents successfully. You will learn how computer forensic analysts collect and analyze data from computer systems to track user-based activity that could be used internally or in civil/criminal litigation.

Proper analysis requires real data for students to examine. The completely updated FOR408 course trains digital forensic analysts through a series of new hands-on laboratory exercises that incorporate evidence found on the latest Microsoft technologies (Windows 8.1, Office365, Skydrive, Sharepoint, Exchange Online, and Windows Phone). This will ensure that students are prepared to investigate the latest trends and capabilities they might encounter. In addition, students will have labs that cover both Windows XP and Windows 8 artifacts.

"FOR408 is based on real scenarios that are likely to occur again. The most up-to-date training I have received."

-Martin Heyde, UK Ministry of Defence

"FOR408 is going to help me obtain my GCFE certification, and will help me in my day-to-day job as a digital forensic associate."

-Christine Casey, Stroz Friedberg

You Will Learn

- Perform in-depth Windows forensic analysis
- Determine which files were stolen during an IP theft
- Track a user's every movement inside the Windows OS
- Identify programs executed by the user
- Examine event logs, registry, jump lists, and more

Who Should Attend

- Information technology professionals
- Incident response team members
- Law enforcement officers, federal agents, and detectives
- Media exploitation analysts
- Anyone interested in a deep understanding of Windows forensics

Hands-On | Six-Day Course | Laptop Required | 36 CPEs | GIAC Cert: GCFE

Course Day Descriptions

408.1 Windows Digital Forensics and Advanced Data Triage

The Windows Forensics course starts with an examination of digital forensics in today's interconnected environments and discusses challenges associated with mobile devices, tablets, cloud storage, and modern Windows operating systems. We will discuss how modern hard drives, such as Solid State Devices (SSD), can affect the digital forensics acquisition process and how analysts need to adapt to overcome the introduction of these new technologies.

408.2 Core Windows Forensics Part 1 – Registry and USB Device Analysis

This day focuses on Windows XP, Windows 7, and Windows 8/8.1 Registry Analysis, and USB Device Forensics. Throughout the section, investigators will use their skills in a real hands-on case, exploring evidence and analyzing evidence.

408.3 Core Windows Forensics Part 2 – E-mail Forensics

You will learn how major forensic suites can facilitate and expedite the investigative process, and how to recover and analyze e-mail, the most popular form of communication. Client-based, server-based, mobile, and web-based e-mail forensic analysis are discussed in-depth.

408.4 Core Windows Forensics Part 3 – Windows 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.

408.5 Core Windows Forensics Part 4 – Web Browser Forensics: Firefox, Internet Explorer, and Chrome

This section looks at Internet Explorer and Firefox Browser Digital Forensics. Learn how to examine exactly what individuals did while surfing via their web browser. The results will give you pause the next time you use the web.

408.6 Windows Forensic Challenge

This section revolves around a Digital Forensic Challenge based on Windows Vista/7. It is a capstone exercise for every artifact discussed in the class. You will use this section to consolidate the skills that you have learned over the past week.

"I have been using forensics tools for years. I never professed to know it all; however, I did not expect to learn as much as I did."

-Jody Hawkins, Cook Childrens Health Care System

giac.org sans.edu digital-forensics.sans.org

Advanced Computer Forensic Analysis and Incident Response

FOR508

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.

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.

SIFT Workstation Training Course

FOR508 trains digital forensic analysts and incident response teams to identify, contain, and remediate sophisticated threats. 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 were stolen and by whom, contain the threat, and provide your organization the capabilities to manage and counter the attack.

"I've already used several of the tools/techniques from the course with past-case evidence to uncover things I didn't previously know."

-Dave Ockwell-Jenner, SITA

"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

You Will Learn

- How to track Advanced Persistent Threats in your enterprise
- Perform forensic analysis and incident response on any remote enterprise system
- Examine memory to discover active malware
- Perform timeline analysis to track the steps of an attacker on your systems
- Discover unknown malware on any system
- Perform deep dive analysis to discover data hidden by anti-forensics

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

Hands-On | Six-Day Course | Laptop Required | 36 CPEs | GIAC Cert: GCFA

Course Day Descriptions

508.1 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 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 APT groups or crime syndicate groups that propagate through thousands of systems.

508.2 Memory Forensics

Critical to many incident response 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.

508.3 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 who pioneered timeline analysis tradecraft. Temporal data are 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 established during advanced incidents and forensic cases.

508.4 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.

508.5 Intrusion Forensics – The Art of Finding Unknown Malware

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.

508.6 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.

GCFA — giac.org

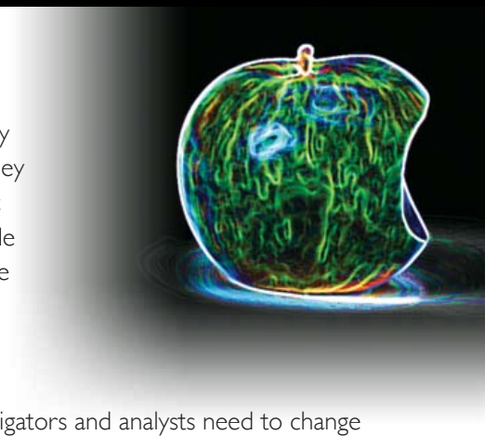
SANS Technology Institute — sans.edu

DFIR — digital-forensics.sans.org

Mac Forensic Analysis

FOR518

Forensicate Differently!



Digital forensic investigators have traditionally dealt with Windows machines, but what if they find themselves in front of a new Apple Mac or iDevice? The increasing popularity of Apple devices can be seen everywhere, from coffee shops to corporate boardrooms, yet most investigators are familiar with Windows-only machines.

Times and trends change and forensic investigators and analysts need to change with them. The new FOR518: Mac Forensic Analysis course provides the tools and techniques necessary to take on any Mac case without hesitation. The intense hands-on forensic analysis skills taught in the course will enable Windows-based investigators to broaden their analysis capabilities and have the confidence and knowledge to comfortably analyze any Mac or iOS system.

FOR518: Mac Forensic Analysis aims to form a well-rounded investigator by introducing Mac forensics into a Windows-based forensics world. This course focuses on topics such as the HFS+ file system, Mac specific data files, tracking user activity, system configuration, analysis and correlation of Mac logs, Mac applications, and Mac exclusive technologies. A computer forensic analyst who successfully completes the course will have the skills needed to take on a Mac forensics case.

"This course gives a top-to-bottom approach to forensic thinking that is quite needed in the profession."

-Naveel Koya, A C-DAC - Trivandrum

"Pound for pound, dollar for dollar, there is no other forensic training I have seen, from FTK to EnCase to anything private, that holds a candle to what was presented in this course."

-Kevin J. Ripa, Computer Evidence Recovery, Inc.

You Will Learn

- Analyze and parse the Hierarchical File System (HFS+) file system
- Recognize the specific domains of the logical file system and Mac-specific file types
- Understand and profile users through their data files and preference configurations
- Determine how a system has been used or compromised
- Analyze numerous Mac-specific technologies

Who Should Attend

- Experienced digital forensic analysts
- Law enforcement officers, federal agents, or detectives
- Media exploitation analysts
- Incident response team members
- Information security professionals
- SANS FOR408, FOR508, FOR526, FOR585, and FOR610 alumni looking to round out their forensic skills

Hands-On | Six-Day Course | Laptop Required | 36 CPEs

Course Day Descriptions

518.1 Mac Essentials and the HFS+ File System

This section introduces the student to Mac system fundamentals such as acquisition, the Hierarchical File System (HFS+), timestamps, and logical file system structure. Acquisition fundamentals are the same with Mac systems, but there are a few Mac-specific tips and tricks that can be used to successfully and easily collect Mac systems for analysis. The building blocks of Mac Forensics start with a thorough understanding of the HFS+. Utilizing a hex editor, the student will learn the basic principles of the primary file system implemented on Mac OS X systems. Students comfortable with Windows forensic analysis can easily learn the slight differences on a Mac system: the data are the same, only the format differs.

518.2 User Domain File Analysis

The logical Mac file system is made up of four domains; User, Local, System, and Network. The User Domain contains most of the user-related items of forensic interest. This domain consists of user preferences and configurations, e-mail, Internet history, and user-specific application data. This section contains a wide array of information that can be used to profile and understand how individuals use their computers.

518.3 Investigating the User via Memory Artifacts

The System and Local Domains contain system-specific information such as application installation, system settings and preferences, and system logs. This sections details basic system information, GUI preferences, and system application data. A basic analysis of system logs can give a good understanding of how a system was used... or abused. Timeline analysis tells the story of how the system was used. Each entry in a log file has a specific meaning and may be able to tell how the user interacted with the computer. The log entries can be correlated with other data found on the system to create an in-depth timeline that can be used to solve cases quickly and efficiently. Analysis tools and techniques will be used to correlate the data and help the student put the story back together in a coherent and meaningful way.

518.4 Advanced Analysis Topics

Mac systems implement some technologies that are available only to those with Mac devices. These include data backup with Time Machine, Versions, and iCloud; extensive file metadata with Extended Attributes and Spotlight; and disk encryption with FileVault. Other advanced topics include data hidden in encrypted containers, Mac intrusion and malware analysis, Mac Server, and Mac memory analysis.

518.5 iOS Forensics

From iPods to iPhones to iPads, it seems everyone has at least one of these devices. Apple iDevices are seen in the hands of millions of people. Much of what goes on in our lives is often stored on them. Forensic analysis of these iOS devices can provide an investigator with an incredible amount of information. Data on these iOS devices will be explored to teach the student what key files exist on them and what advanced analysis techniques can be used to exploit them for investigations.

518.6 The Mac Forensics Challenge

Students will put their new Mac forensics skills to the test by completing the following tasks:

- In-Depth HFS+ File System Examination
- File System Timeline Analysis
- Advanced Computer Forensics Methodology
- Mac Memory Analysis
- File System Data Analysis
- Metadata Analysis
- Recovering Key Mac Files
- Volume and Disk Image Analysis
- Analysis of Mac Technologies including Time Machine, Spotlight, and FileVault
- Advanced Log Analysis and Correlation
- iDevice Analysis and iOS Artifacts

"Best MAC class anywhere."

-Eric Koebelen, Incident Response U.S.

DFIR

digital-forensics.sans.org

Memory Forensics In-Depth

FOR526

Malware can hide, but it must run.

Digital Forensics and Incident Response (DFIR) professionals view the acquisition and analysis of physical memory as critical to the success of an investigation, be it a criminal case, employee policy violation, or enterprise intrusion. Investigators who do not look at volatile memory are leaving evidence on the table. The valuable contents of RAM hold evidence of user actions as well as evil processes and furtive behaviors implemented by malicious code. It is this evidence that often proves to be the smoking gun that unravels the story of what happened on a system.

SIFT Workstation Training Course

FOR526 provides the critical skills necessary for digital forensics examiners and incident responders to deftly analyze captured memory images and live response audits. By using the most effective freeware and open-source tools in the industry today and delivering a deeper understanding of how these tools work, this five-day course shows DFIR professionals how to unravel the real story of what happened on a system. It is a critical course for any serious investigator who wants to tackle advanced forensics, trusted insider, and incident response cases.

Just as it is crucial to understand disk and registry structures to substantiate findings in traditional system forensics, it is equally critical to understand memory structures. Having in-depth knowledge of Windows memory internals allows the examiner to access target data specific to the needs of the case at hand.

Remember: "Malware can hide, but it must run." It is this malware paradox that is the key to understanding that while intruders are becoming more advanced with anti-forensic tactics and techniques, it is impossible for them to hide their footprints completely from a skilled incident responder performing memory analysis. FOR526 will ensure that you and your team are ready to respond to the challenges inherent in DFIR by using cutting-edge memory forensics tools and techniques.

"The training opened my eyes for the need to collect memory images as well as physical images for single computer analysis such as theft of IP or other employee investigations."

-Greg Caouette, Kroll

You Will Learn

- Utilize stream-based data parsing tools to extract AES-encryption keys
- Capture, examine and analyze physical memory image and structures
- Inspect a Windows crash dump
- Conduct Live System Memory Analysis
- Extract and analyze packed and non-packed PE binaries from memory
- Gain insight into the latest anti-memory analysis techniques and how to overcome them

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

Hands-On | Six-Day Course | Laptop Required | 36 CPEs

Course Day Descriptions

526.1 oundations in Memory Analysis and Acquisition

Simply put, memory analysis has become a required skill for all incident responders and digital forensics examiners. Regardless of the type of investigation, system memory and its contents often expose the first hit – the evidential thread that, when pulled, unravels the whole picture of what happened on the target system. Where is the malware? How did the machine get infected? Where did the attacker move laterally? Or what did the disgruntled employee do on the system? What lies in physical memory can provide answers to all of these questions and more.

526.2 Unstructured Analysis and Process Exploration

Structured memory analysis using tools that identify and interpret operating system structures is certainly powerful. However, many remnants of previously allocated memory remain available for analysis, and they cannot be parsed through structure identification. What tools are best for processing fragmented data? Unstructured analysis tools! They neither know nor care about operating system structures. Instead, they examine data, extracting findings using pattern matching. You will learn how to use Bulk Extractor to parse memory images and extract investigative leads such as e-mail addresses, network packets, and more.

526.3 Investigating the User via Memory Artifacts

An incident responder (IR) is often asked to triage a system because of a network intrusion detection system alert. The Security Operations Center makes the call and requires more information due to outbound network traffic from an endpoint and the IR team is asked to respond. In this section, we cover how to enumerate active and terminated TCP connections – selecting the right plugin for the job based on the OS version.

526.4 Internal Memory Structures (PART I)

Day 4 focuses on introducing some internal memory structures (such as drivers), Windows memory table structures, and extraction techniques for portable executables. As we come to the final steps in our investigative methodology, "Spotting Rootkit Behaviors" and "Extracting Suspicious Binaries," it is important to emphasize again the rootkit paradox. The more malicious code attempts to hide itself, the more abnormal and seemingly suspicious it appears. We will use this concept to evaluate some of the most common structures in Windows memory for hooking, the IDTs and SSDTs.

526.5 Internal Memory Structures (PART II) and Memory Analysis Challenges

Sometimes an investigator's luck runs out and he or she does not complete a memory acquisition before the target system is taken offline or shut down. In these cases, where else can system memory captures be found? Hibernation files and Windows crashdump files can be valuable sources of information, regardless of whether or not you find yourself with a current memory capture. This section covers the structure of the hibernation and crashdump files, as well as how to convert both into raw memory images that can easily be parsed using Volatility and other tools in our memory forensics weapons arsenal. In addition, we will analyze a crash dump file, discovering just how Windows responds and what information is captured when a system crashes.

526.6 Final Day Memory Analysis Challenge

This final section provides students with a direct memory forensics challenge that makes use of the SANS NetWars Tournament platform. Your memory analysis skills are put to the test with a variety of hands-on scenarios involving hibernation files, Crash Dump files, and raw memory images, reinforcing techniques covered in the first five sections of the course. These challenges strengthen the students' ability to respond to typical and atypical memory forensics challenges from all types of cases, from investigating the user to isolating the malware. By applying the techniques learned earlier in the course, students consolidate their knowledge and can shore up skill areas where they feel they need additional practice.

"Totally awesome, relevant and eye opening. I want to learn more every day."

-Matthew Britton, Blue Cross Blue Shield of Louisiana

DFIR
digital-forensics.sans.org

Advanced Network Forensics and Analysis

FOR572

Take your system-based forensic knowledge onto the wire. Incorporate network evidence into your investigations, provide better findings, and get the job done faster.

Forensic casework that does not include a network component is a rarity in todays environment. Performing disk forensics will always be a critical and foundational skill for this career, but overlooking the network component of today's computing architecture is akin to ignoring security camera footage of a crime as it was committed. Whether you handle an intrusion incident, data theft case, or employee misuse scenario, the network often has an unparalleled view of the incident. Its evidence can provide the proof necessary to show intent, or even definitively prove that a crime actually occurred.

FOR572: Advanced Network Forensics and Analysis was built from the ground up to cover the most critical skills needed to mount efficient and effective post-incident response investigations. We focus on the knowledge necessary to expand the forensic mindset from residual data on the storage media from a system or device to the transient communications that occurred in the past or continue to occur. Even if the most skilled remote attacker compromised a system with an undetectable exploit, the system still has to communicate over the network. Without command-and-control and data extraction channels, the value of a compromised computer system drops to almost zero. Put another way: Bad guys are talking – we'll teach you to listen.

SIFT Workstation Training Course

This course covers the tools, technology, and processes required to integrate network evidence sources into your investigations, with a focus on efficiency and effectiveness. You will leave this week with a well-stocked toolbox and the knowledge to use it on your first day back on the job. We will cover the full spectrum of network evidence, including high-level NetFlow analysis, low-level pcap exploration, ancillary network log examination, and more. We cover how to leverage existing infrastructure devices that may contain months or years of valuable evidence as well as how to place new collection platforms while an incident is already under way.

"FOR572 taught me how to use different evidence sources to fill in missing gaps. This is critical, as most environments or incidents will not have every type of evidence available."

-Alexander Bond, Mandiant

You Will Learn

- Extract files from network packet captures and proxy cache files
- Use historical NetFlow data to identify relevant past network occurrences
- Reverse engineer custom network protocols
- Decrypt captured SSL traffic to identify attackers actions
- Incorporate log data into a comprehensive analytic process
- Learn how attackers leverage man-in-the-middle tools
- Analyze network protocols and wireless network traffic

Who Should Attend

- Incident response team members
- Law enforcement officers, federal agents, and detectives
- Information security managers
- Network defenders
- Information technology professionals
- Network engineers
- Information technology lawyers and paralegals
- Anyone interested in computer network intrusions and investigations

Hands-On | Six-Day Course | Laptop Required | 36 CPEs | GIAC Cert: GCNA

Course Day Descriptions

572.1 Off the Disk and Onto the Wire

Network data can be preserved, but only if captured directly from the wire. Whether tactical or strategic, packet capture methods are quite basic. You will re-acquaint yourself with tcpdump and Wireshark, the most common tools used to capture and analyze network packets, respectively. However, since long-term full-packet capture is still uncommon in most environments, many artifacts that can tell us about what happened on the wire in the past come from devices that manage network functions. You will learn about what kinds of devices can provide valuable evidence and at what level of granularity. We will walk through collecting evidence from one of the most common sources of network evidence, a web proxy server, then go hands-on to find and extract stolen data from the proxy yourself. The Linux SIFT virtual machine, which has been specifically loaded with a set of network forensic tools, will be your primary toolkit for the week.

572.2 Network Protocols and Commercial Network Forensics

This section covers some of the most common and fundamental network protocols that you will likely face during an investigation. We will cover a broad range of protocols including the Dynamic Host Configuration Protocol, which glues together layers two and three on the OSI model, and Microsoft's Remote Procedure Call protocol, which provides all manners of file, print, name resolution, authentication, and other services.

572.3 Netflow Analysis and Wireless Network Forensics

In this section, you will learn what data items NetFlow can provide, and the various means of collecting those items. As with many such monitoring technologies, both commercial and open-source solutions exist to query and examine NetFlow data. We will review both categories and discuss the benefits and drawbacks of each. Finally, we will address the forensic aspects of wireless networking. We will cover similarities with and differences from traditional wired network examination, as well as what interesting artifacts can be recovered from wireless protocol fields. Some inherent weaknesses of wireless deployments will also be covered, including how attackers can leverage those weaknesses during an attack, and how they can be detected.

572.4 Logging, OPSEC, and Footprint

In this section, you will learn about various logging mechanisms available to both endpoint and network transport devices. You will also learn how to consolidate log data from multiple sources, providing a broad corpus of evidence in one location. As the volume of log data increases, so does the need to consider automated analytic tools. You will learn various solutions that accomplish this, from tactical to enterprise-scale.

572.5 Encryption, Protocol Reversing, and Automation

Encryption is frequently cited as the most significant hurdle to effective network forensics, and for good reason. When properly implemented, encryption can be a brick wall in between an investigator and critical answers. However, technical and implementation weaknesses can be used to our advantage. Even in the absence of these weaknesses, the right analytic approach to encrypted network traffic can still yield valuable information about the content. We will discuss the basics of encryption and how to approach it during an investigation. The section will also cover flow analysis to characterize encrypted conversations.

572.6 Network Forensics Capstone Challenge

This section will combine all of what you have learned prior to and during this week. In groups, you will examine network evidence from a real-world compromise by an advanced attacker. Each group will independently analyze data, form and develop hypotheses, and present findings. No evidence from endpoint systems is available – only the network and its infrastructure.

"Amazing content. Real life and totally relevant to today's network battle space."

-Don Dorey, Dept. of National Defense

GNFA — giac.org

DFIR — digital-forensics.sans.org

Advanced Smartphone Forensics

FOR585

Your texts and apps can and will be used against you

It is rare to conduct a digital forensic investigation that does not include a smartphone or mobile device. Often, the smartphone may be the only source of digital evidence tracing an individuals movements and motives and may provide access to the who, what, when, where, why, and how behind a case. FOR585 teaches real-life, hands-on skills that enable digital forensic examiners, law enforcement officers, and information security professionals to handle investigations involving even the most complex smartphones available today.

FOR585: Advanced Smartphone Forensics focuses on smartphones as sources of evidence, providing the necessary skills to handle mobile devices in a forensically sound manner, understand the different technologies, discover malware, and analyze the results for use in digital investigations by diving deeper into the file systems of each smartphone. Students will be able to obtain actionable intelligence and recover and analyze data that commercial tools often miss for use in internal investigations, criminal and civil litigation, and security breach cases. Dont miss the NEW FOR585!

The hands-on exercises in this class cover the best tools currently available to conduct smartphone and mobile device forensics, and provide detailed instructions on how to manually decode data tools sometimes overlook. The course will prepare you to recover and reconstruct events relating to illegal or unauthorized activities, determine if a smartphone has been compromised with malware or spyware, and provide your organization the capability to use evidence from smartphones. This intensive six-day course will take your mobile device forensics knowledge and abilities to the next level. Smartphone technologies are new and the data formats are unfamiliar to most forensic professionals. Its time to get smarter!

"The topics covered in the course can be considered advanced but are also very practical. Topics such as parsing and searching devices not supported by commercial tools and digging in hex for deleted artifacts are extremely important."

-Matthew Edmondson

"FOR585 is the best out there."

-Andy Nind, British Army

You Will Learn

- Manually parse and decode data from smartphones and smartphone applications
- Detect hidden malware and spyware on smartphones
- Interpret file systems on smartphones
- Recover artifacts and location-based and GPS information
- Perform advanced forensic examinations of data structures and data-carving
- Reconstruct events surrounding a crime
- Decrypt locked backup files and bypass smartphone locks

Who Should Attend

- Experienced digital forensic analysts
- Media exploitation analysts
- Information security professionals
- Incident response teams
- Law enforcement officers, federal agents, or detectives
- IT auditors
- SANS SEC575, FOR408, and FOR508 graduates looking to take their skills to the next level

Hands-On | Six-Day Course | Laptop Required | 36 CPEs

Course Day Descriptions

585.1 Smartphone Overview and Malware Forensics

Although smartphone forensic concepts are similar to those in digital forensics, smartphone file system structures differ and require specialized decoding skills to correctly interpret the data acquired from the device. Today you will apply what you already know to smartphone forensic handling, device capabilities, acquisition methods, and data encoding concepts of smartphone components. You will also become familiar with the forensic tools required to complete comprehensive examinations of smartphone data structures.

585.2 Android Forensics

Android devices are among the most widely used smartphones in the world, which means they will surely be part of an investigation that will come across your desk. Android devices contain substantial amounts of data that can be decoded and interpreted into useful information. Without honing the appropriate skills for bypassing locked Androids and correctly interpreting the data stored on the devices, you will be unprepared for the rapidly evolving world of smartphone forensics. Malware affects not only Androids, but also a plethora of smartphone devices. This section will examine various types of malware, how it exists on smartphones, and how to identify it.

585.3 iOS Forensics

Apple iOS devices are no longer restricted to the United States, but are in use worldwide. iOS devices contain substantial amounts of data, including deleted records, that can be decoded and interpreted into useful information. Proper handling and parsing skills are required for bypassing locked iOS devices and correctly interpreting the data. Without the iOS instruction, you will be unprepared to deal with the iOS device that will likely be a major component in a forensic investigation.

585.4 Blackberry and Backup File Forenics

Blackberry smartphones are designed to protect user privacy, but techniques taught in this section will enable the investigator to go beyond what the tools decode and manually recover data residing in database files of the file system of Blackberry devices. Backup files are commonly found on external media and can be the only forensic acquisition method for newer iOS devices that are locked. Learning how to access and parse data from encrypted backup files may be the only lead to smartphone data relating to your investigation.

585.5 Third-Party Application and Other Smartphone Device Forensics

Given the prevalence of other types of smartphones around the world, it is critical for examiners to develop a foundation of understanding about data storage on multiple devices. Nokia smartphones running the Symbian operating system may no longer be manufactured, but it doesn't mean that they do not exist in the wild. You must acquire skills for handling and parsing data from uncommon smartphone devices. This day of instruction will prepare you to deal with "misfit" smartphone devices and provide you with advanced methods for decoding data stored in third-party applications across all smartphones.

585.6 Smartphone Forensic Capstone Exercise

This section will test all that you have learned during this week. In small groups, you will examine three smartphone devices and solve a scenario relating to a real-world smartphone forensic investigation. Each group will independently analyze the three smartphones, manually decode data, answer specific questions, form an investigation hypothesis, develop a report, and present findings.

"This is the most advanced mobile-device training that I know of and is greatly needed. It is currently the only course being taught at this level!"

-Scott McNamee, DoS/CACI

digital-forensics.sans.org

Reverse-Engineering Malware: Malware Analysis Tools & Techniques

FOR610

This popular course explores malware analysis tools and techniques in depth. FOR610 training has helped forensic investigators, incident responders, security engineers, and IT administrators acquire the practical skills to examine malicious programs that target and infect Windows systems. Understanding the capabilities of malware is critical to an organizations ability to derive threat intelligence, respond to information security incidents, and fortify defenses. This course builds a strong foundation for reverse-engineering malicious software using a variety of system and network monitoring utilities, a disassembler, a debugger, and other tools useful for turning malware inside-out.

The course begins by covering fundamental aspects of malware analysis. You will learn how to set up an inexpensive and flexible laboratory to examine the inner workings of malicious software, and how to use the lab to uncover characteristics of real-world malware samples. Then you will learn to examine the specimens' behavioral patterns and code. The course continues by discussing essential x86 assembly language concepts. You will examine malicious code to understand its key components and execution flow. In addition, you will learn to identify common malware characteristics by looking at suspicious Windows API patterns employed by bots, rootkits, keyloggers, downloaders, and other types of malware.

You will also learn how to handle self-defending malware, bypassing the protection offered by packers, and other anti-analysis methods. In addition, given the frequent use of browser malware for targeting systems, you will learn practical approaches to analyzing malicious browser scripts, deobfuscating JavaScript and VBScript to understand the nature of the attack.

You will learn how to analyze malicious documents that take the form of Microsoft Office and Adobe PDF files. Such documents act as a common infection vector and may need to be examined when dealing with large-scale infections as well as targeted attacks. The course also explores memory forensics approaches to examining malicious software, especially useful if the software exhibits rootkit characteristics.

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

-Don Lopez, Valley National Bank

"I thought I knew reversing. This class taught me so much more and provided easy understandings of complex reversing tasks."

-David Werden, NGIS

You Will Learn

- Build an isolated lab for analyzing malicious code
- Employ network and system-monitoring tools for malware analysis
- Examine malicious JavaScript, VB Script and ActionScript
- Use a disassembler and debugger to analyze malicious Windows executables
- Bypass a variety of defensive mechanisms designed by malware authors
- Derive Indicators of Compromise (IOCs) from malicious executables
- Utilize practical memory forensics techniques to understand malware capabilities

Who Should Attend

- Professionals with responsibilities in the areas of incident response, forensic investigation, Windows security, and system administration
- Professionals who deal with incidents involving malware and would like to learn how to understand key aspects of malicious programs
- Individuals who attended the course have experimented with aspects of malware analysis prior to the course and were looking to formalize and expand their malware forensics expertise

Hands-On | Six-Day Course | Laptop Required | 36 CPEs | GIAC Cert: GREM

Course Day Descriptions

610.1 Malware Analysis Fundamentals

Section one lays the groundwork for malware analysis by presenting the key tools and techniques useful for examining malicious programs. You will learn how to save time by exploring Windows malware in two phases. Behavioral analysis focuses on the program'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 debugger tools such as IDA Pro and OllyDbg. You will learn how to set up a flexible laboratory to perform such analysis in a controlled manner, and you will set up such a lab on your laptop using the supplied windows and Linux (REMnux) virtual machines. You will then learn how to use the key analysis tools by examining a malware sample in your lab – with guidance from the instructor – to reinforce the concepts discussed throughout the day.

610.2 Malicious Code Analysis

Section two focuses on examining malicious Windows 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 section begins with an overview of key code-reversing concepts and presents a primer on essential x86 Intel 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 remaining part of the section discusses how malware implements common characteristics, such as keylogging and DLL injection, at the assembly level. You will learn how to recognize such characteristics in suspicious Windows executable files.

610.3 In-Depth Malware Analysis

Section three builds upon the approaches to behavioral and code analysis introduced earlier in the course, exploring techniques for uncovering additional aspects of the functionality of malicious programs. You will learn about packers and the techniques that may help analysts bypass their defenses. Additionally, you will understand how to redirect network traffic in the lab to better interact with malware to understand its capabilities. You will also learn how to examine malicious websites and deobfuscate browser scripts, which often play a pivotal role in malware attacks.

610.4 Self-Defending Malware

Section four focuses on the techniques malware authors commonly employ to protect malicious software from being examined, often with the help of packers. You will learn how to recognize and bypass anti-analysis measures, such as tool detection, string obfuscation, unusual jumps, breakpoint detection and so on. We will also discuss the role that shellcode plays in the context of malware analysis and will learn how to examine this aspect of attacks. As with the other topics covered throughout the course, you will be able to experiment with such techniques during hands-on exercises.

610.5 Malicious Documents and Memory Forensics

Section five starts by exploring common patterns of assembly instructions often used to gain initial access to the victim's computer. Next, we will learn how to analyze malicious Microsoft Office documents, covering tools such as OfficeMalScanner and exploring steps for analyzing malicious PDF documents with practical tools and techniques. 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 as 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 analyze malware more efficiently.

610.6 Malware Analysis Tournament

Section six assigns students to the role of a malware analyst working as a member of an incident response or forensics team. Students are presented with a variety of hands-on challenges involving real-world malware in the context of a fun tournament. These challenges further a students ability to respond to typical malware analysis tasks in an instructor-led lab environment and offer additional learning opportunities. Moreover, 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 consolidate their knowledge and shore up skill areas where they feel they need additional practice

giac.org

sans.edu

digital-forensics.sans.org

Hacker Techniques, Exploits, and Incident Handling

SEC504

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 challenging course is particularly well suited to individuals who lead or are 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.

"SEC504 should be taken by everyone in your company that has anything to do with security. It is especially valuable for sys admins as well as security personnel."

-Karl Findorff, Xavier University of Louisiana

"SEC504 should be taken by everyone in your company that has anything to do with security. It is especially valuable for sys admins as well as security personnel."

-Karl Findorff, Xavier University of Louisiana

You Will Learn

- Apply incident handling processes in-depth
- Analyze the structure of common attack techniques
- Accomplish operating system and application-level attacks
- Crack passwords and break into web applications
- Learn how to maintain access on a target
- Diagnose specific types of traffic-flooding denial-of-service techniques
- Use built-in command-line tools to detect an attackers presence

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

Hands-On | Six-Day Course | Laptop Required | 37 CPEs | GIAC Cert: GCIH

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.

504.2 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.

504.3 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.

504.4 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.

504.5 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.

504.6 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.

"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

giac.org

DoD 8570 Required
sans.org/8570

sans.org/cyber-guardian

sans.edu

Digital Forensics Resources

digital-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: dfir.to/DFIRBlog
- Google+: gplus.to/sansforensics
- Twitter: @sansforensics
- Mailing list: dfir.to/MAIL-LIST
- Facebook: sansforensics
- YouTube: dfir.to/DFIRCast

Digital 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: digital-forensics.sans.org/community/whitepapers

Webcasts: digital-forensics.sans.org/community/webcasts

Newsletters: sans.org/newsletters

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

Digital Forensics Posters

digital-forensics.sans.org/community/cheat-sheets

SIFT WORKSTATION V3.0

SANS Investigative Forensic Toolkit

dfir.to/SANS-SIFT

An international team of forensics experts, led by SANS Faculty Fellow Rob Lee, created the SANS Investigative Forensic Toolkit (SIFT) Workstation and made it available to the whole community as a public service. The free SIFT toolkit, that can match any modern forensic tool suite, is also featured in SANS' **FOR508: Advanced Computer Forensic Analysis and Incident Response** course. It demonstrates that advanced investigations and responding to intrusions can be accomplished using cutting-edge open-source tools that are freely available and frequently updated.

Offered free of charge, the SIFT 3.0 demonstrates that advanced investigations and responding to intrusions can be accomplished using cutting-edge open-source tools that are freely available and frequently updated.

"Even if SIFT were to cost tens of thousands of dollars, it would still be a very competitive product," says, Alan Paller, director of research at SANS. *"At no cost, there is no reason it should not be part of the portfolio in every organization that has skilled forensics analysts."*

Developed and continually updated by an international team of forensic experts, the SIFT is a group of free open-source forensic tools designed to perform detailed digital forensic examinations in a variety of settings. With over 100,000 downloads to date, the SIFT continues to be the most popular open-source forensic offering next to commercial source solutions.

"The SIFT Workstation has quickly become my 'go to' tool when conducting an exam. The powerful open source forensic tools in the kit on top of the versatile and stable Linux operating system make for quick access to most everything I need to conduct a thorough analysis of a computer system," said Ken Pryor, GCFA Robinson, IL Police Department

Key new features of SIFT 3.0 include:

- **Ubuntu LTS 12.04 Base**
- **64 bit base system**
- **Better memory utilization**
- **Auto-DFIR package update and customizations**
- **Latest forensic tools and techniques**
- **VMware Appliance ready to tackle forensics**
- **Cross compatibility between Linux and Windows**
- **Option to install stand-alone via (.iso) or use via VMware Player/Workstation**
- **Online Documentation Project at sift.readthedocs.org**
- **Expanded Filesystem Support**

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 ANALYSIS TOOLS

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

Mandiant Redline (Windows)
`http://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. @ovie

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. @mikecloppert

Christopher Crowley *SANS Certified Instructor*

Mr. Crowley has 15 years of industry experience managing and securing networks. He currently works as an independent consultant in the Washington, DC area. His work experience includes penetration testing, computer network defense, incident response, and forensic analysis. Mr. Crowley is the course author for SANS MGT535: Incident Response Team Management and holds the GSEC, GCIA, GCIH (gold), GCFA, GPEN, GREM, GMOB, and CISSP certifications. @CCrowMontance

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. @iamevltwin

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 Certified Instructor*

Philip Hagen has over 14 years experience in creating and deploying strategic and ad-hoc IT and information security solutions. Currently, Phil is the CEO at RedCanary, where he oversees the development and growth of their managed threat detection service, which minimizes the time between a compromise and detection. This helps to support faster and more decisive remediation of network-based intrusions. Phil has provided technical services to various government offices covering a variety of exotic requirements in high-threat environments. He served in the U.S. Air Force as a communications officer at the Pentagon and Beale AFB, CA. Phil holds a computer science degree from the U.S. Air Force Academy. @PhilHagen

SANS DFIR Faculty

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 Certified 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. @kleinco

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 Certified 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://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 Senior 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. He blogs at 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 Certified 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 zeltser.com. He blogs at http://blog.zeltser.com @lennyzeltser

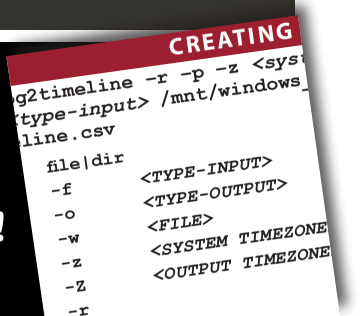
SANS Lethal Forensicator Coin

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

Learn more about the SANS Lethal Forensicator Coin and how to earn one at

digital-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

FOR14

Register using this Promo Code