DFIR MONTEREY 2015

a REDFIRE Event

The All Forensics and Incident Response Training Event

February 23-28, 2015 | Monterey, CA

sans.org/dfir2015

COURSES OFFERED

CORE

FOR408
Windows Forensic Analysis
GCFE

SEC504
Hacker Tools, Techniques, Exploits & Incident Handling
GCIH

INCIDENT RESPONSE

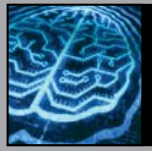
FOR508
Advanced Digital Forensics and Incident Response
GCFA

FOR572
Advanced Network Forensics and Investigations
GNFA

LEARN R.E.M.

FOR610
REM: Malware Analysis Tools and Techniques
GREM

SPECIALIZATION



FOR526
Memory Forensics In-Depth

FOR518
Mac Forensic Analysis

SANS **DFIR MONTEREY** 2015
a REDFIRE Event

FEBRUARY 23-28, 2015 | MONTEREY, CA

Hunt down adversaries in your network using skills needed to respond to breaches.

The Reverse Engineering Digital Forensics and Incident Response Education (REDFIRE) event brings our most popular forensics courses, instructors, and bonus seminars together in one place to offer one of SANS' most comprehensive DFIR training experiences. This is a must-attend event for you and your team as our leading experts focus on building the DFIR skills that will take you to that next level.

Top reasons to attend:

- **DFIR-Focused Training** – The event hosts cutting-edge DFIR training classes, in addition to our new course, **FOR518: Mac Forensic Analysis**.
- **Bonus Talks** – Evenings are packed with bonus talks covering the most innovative DFIR topics.
- **Networking** – One of the few DFIR-only training events on the SANS calendar! Join the most innovative minds in the industry to tackle advanced DFIR issues.
- **DFIR NetWars Tournament** – Free if you sign up for a class: **SANS DFIR NetWars** is a hands-on, interactive learning environment that enables DFIR professionals to develop and master the skills they need to excel in their field.

sans.org/dfir2015

FOR408

Windows Forensic Analysis

Instructor: Chad Tilbury

Windows Forensic Analysis focuses on a comprehensive and deep analysis of the latest Microsoft Windows operating systems. In this intermediate course, you will learn directly how forensic analysts track the second-by-second trail left behind by evildoers used in successful criminal prosecution, incident response, media exploitation or civil litigation.

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

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

-Martin Heyde, MOD

- Perform in-depth Windows forensic analysis
- Learn how to determine files 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

sans.org/FOR408

FOR508

Advanced Digital Forensics and Incident Response

Instructor: Rob Lee

This in-depth incident response course provides responders with advanced skills to hunt down, counter, and recover from a wide range of threats within enterprise networks, including APT adversaries, organized crime syndicates, and hactivism.

GATHER YOUR INCIDENT RESPONSE TEAM – IT'S TIME TO GO HUNTING

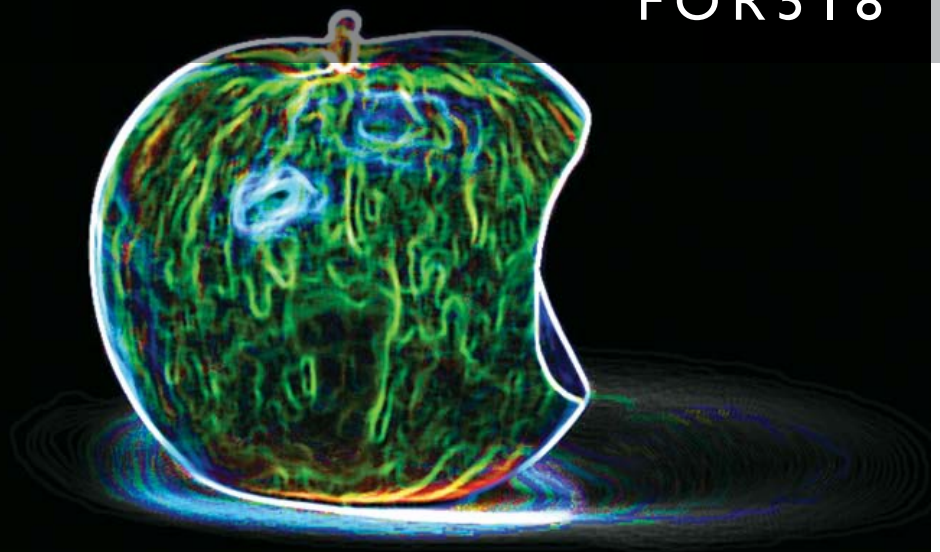
"Best incident response training I've had so far. I thought that some of the other courses were great but, FOR508 is much more current and applicable to the real world."

-Marc Bleicher, Bit9

- Learn how to track Advanced Persistent Threats in your enterprise
- Perform 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

sans.org/FOR508

FOR518



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.

NEW! Mac Forensic Analysis

Instructor: Sarah Edwards

FORENSICATE DIFFERENTLY!

"I have not encountered a Mac class this in-depth that covers the file structure so well."

-Craig Goldsmith, OCSD

- Learn to 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

sans.org/FOR518

FOR526

Memory Forensics In-Depth

Instructor: Alissa Torres

Memory analysis is now a crucial skill for any incident responder who is analyzing intrusions. The malware paradox is key to understanding that while intruders are becoming more advanced with anti-forensic tactics and techniques, it is impossible to hide their footprints completely from a skilled incident responder performing memory analysis.

MALWARE CAN HIDE, BUT IT MUST RUN

"I was able to take the techniques learned in this class and break open a case I was working, even before heading home."

- Anonymous

- Utilize stream-based data parsing tools to extract AES-encryption keys
- Capture, examine and analyze physical memory image and structures
- Windows, Mac, and Linux Memory Analysis Covered
- 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

sans.org/FOR526

FOR572

This course was built from the ground up to cover the most critical skills needed to mount efficient and effective 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.

Advanced Network Forensics and Analysis

Instructor: Philip Hagen

BAD GUYS ARE TALKING – WE'LL TEACH YOU TO LISTEN

"I feel like I have won the lottery with the wealth of information from this week! Very relevant and applicable. I have already started using in our environments with results."

-Don Dorey, Dept. of National Defense

- 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

sans.org/FOR572

FOR610

LEARN REM

This popular malware analysis course has helped forensic investigators, incident responders acquire practical skills for examining malicious programs that target Microsoft Windows. This training also teaches how to reverse-engineer web browser malware implemented in JavaScript and Flash, as well as malicious documents, such as PDF and Microsoft Office files.

REM: Malware Analysis Tools and Techniques

Instructor: Anuj Soni

TURN MALWARE INSIDE-OUT

"It is an excellent course for those who want a hands-on experience understanding an under the hood view of malware and how it works."

-Craig Goldsmith, FBI

- 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

sans.org/FOR610

SEC504

This course addresses the latest cutting-edge insidious attack vectors, 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.

Hacker Tools, Techniques, Exploits, and Incident Handling

Instructor: Neal Bridges

KNOW YOUR ENEMY

"There is no substitute for hands-on hacking experience."

-Andrew Longsworth, Driscoll Strawberry Associates, Inc.

- Apply incident handling processes in-depth
- Analyze the structure of common attack techniques
- Learn how to accomplish operating system and application-level attacks
- Learn how to crack passwords
- Learn how to break into web applications
- Learn how to maintain access on a target

sans.org/SEC504

SANS DFIR MONTEREY BONUS SESSIONS

This concentration of free forensics-themed sessions is only available at this unique event.

Network Forensics: The Final Frontier (Until the Next One)

Philip Hagen

Traditionally, computer forensic investigations focused on data from static data. Now, data from network devices and the wires themselves is becoming necessary to complete our understanding and provide a more comprehensive analysis of an event.

Power-up Your Malware Analysis with Forensics

Anuj Soni

Forensic analysis is invaluable for discovering malicious code, but even after you have that malware in hand, harnessing forensic approaches to support your reverse engineering efforts can prove extremely useful. This talk will use case studies to cover how to use forensic resources, tools, and techniques to perform more robust malware analysis.

DFIReception – Forensicators Unite!

Join us after the first day of class, and immediately before the Keynote event to meet with your fellow digital forensics and incident response professionals for an informal reception. Discuss the latest events with the DFIR community and meet those in the field that you have only seen on Twitter or Google+.

When Macs Get Hacked

Sarah Edwards

Historically computer intrusion cases usually consisted of Windows or *nix systems, but with the growing market share of Macintosh systems, intrusion cases using Mac's are growing. This presentation and hands-on lab will introduce you to incident response and intrusion analysis of the Mac.

Extracting User Credentials using Memory Forensics

Alissa Torres

Though Windows credential extraction and password cracking are often categorized as offensive skills, used by pentesters and sophisticated attackers, digital forensic examiners and incident responders can also put these techniques to use to further their investigations. This talk walks through several practical forensics use cases for Windows credential extraction from memory.

Preparing for PowerShellmageddon – Investigating Windows Command Line Activity

Chad Tilbury

Hackers use command line as it historically leaves far fewer forensics artifacts. This talk will demonstrate how incident responders are countering the command line threat and teach you to identify when it is in play, extract command history, and see what is new on the horizon from Microsoft to make tracking command line and PowerShell activity easier.

DFIR NetWars Tournament

Rob Lee

(See details below.)

DFIR NetWars TOURNAMENT

SANS DFIR NetWars at DFIR MONTEREY 2015 is an incident simulator packed with a vast amount of forensic and incident response challenges that enables Digital Forensics and Incident Response (DFIR) professionals to develop and master the skills they need to excel in their field.

Malware Analysis
Digital Forensics
Incident Response
File and Packet Analysis
Memory Analysis
Host Forensics

Netwars is complimentary for DFIR MONTEREY 2015 attendees. Sign up when you register for your course.

digital-forensics.sans.org/training/netwars

SANS Simulcast

Can't attend DFIR MONTEREY 2015 live?

You don't have to miss out with Event Simulcast!

Event Simulcast allows you to attend a SANS training event without leaving home. Simply log in to a virtual classroom to see, hear, and participate in the class as it is being presented LIVE at the event.

The following courses will be available via SANS Simulcast:

FOR408 | FOR508 | FOR526 | FOR572

Register Now!

sans.org/dfir2015

SANS DFIR MONTEREY INSTRUCTORS

Neal Bridges

Neal Bridges is the Lead Penetration Tester at NetWorks Group with over 20 years of experience in the information technology arena. Neal was hand selected to build and establish the US Air Force's first cyber functional training unit and developed specialized training for thousands of US CYBERCOM students on the latest, advanced offensive cyber techniques. In addition to his vast military experience, Neal has worked extensively in the commercial world in the financial, energy (SCADA/ICS controls), health care, governmental, and R&D arenas conducting in-depth and extensive penetration testing. Neal has also worked closely with the FBI to provide subject matter expertise in adversarial attack tactics. Neal consults with organizations regularly applying his experience in diverse, large-scale enterprise environments. @ITJunkie

Sarah Edwards

Sarah is a senior digital forensic analyst who has worked with various federal law enforcement agencies. She has performed a variety of investigations including computer intrusions, criminal, counterintelligence, counter-narcotic, and counterterrorism. 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, BsidesNOLA, TechnoSecurity, HTCIA, and the SANS DFIR Summit. She has a Bachelor of Science in Information Technology from Rochester Institute of Technology and a Master's in Information Assurance from Capitol College. @iamevltwin

Philip Hagen

Philip Hagen has been working in the information security field since 1998, running the full spectrum including deep technical tasks, management of an entire computer forensic services portfolio, and executive responsibilities. Currently, Phil is an Evangelist at Red Canary, where engages with current and future customers of Red Canary's managed threat detection service to ensure their use of the service is best aligned for success in the face of existing and future threats. Phil started his security career while attending the U.S. Air Force Academy, with research covering both the academic and practical sides of security. He served in the Air Force as a communications officer at Beale AFB and the Pentagon. In 2003, He has provided forensic consulting services for law enforcement, government, and commercial clients prior to joining the Red Canary team. Phil is also a certified instructor for the SANS Institute, and is the course lead and co-author of FOR572, Advanced Network Forensics and Analysis. @PhilHagen

Rob Lee

Rob Lee is an entrepreneur and consultant in the Washington, DC area, specializing in information security, incident response, and digital forensics. Rob is currently the curriculum lead and author for digital forensic and incident response training at the SANS Institute in addition to owning his own firm. Rob has more than 15 years of experience in computer forensics, vulnerability and exploit discovery, intrusion detection/prevention, and incident response. Rob graduated from the U.S. Air Force Academy and served in the U.S. Air Force as a founding member of the 609th Information Warfare Squadron. Later, he was a member of the Air Force Office of Special Investigations (AFOSI) where he led a team conducting computer crime investigations. Prior to starting his own firm, he directly worked with a variety of government agencies in the law enforcement, U.S. Department of Defense, and intelligence communities. @robtlee

Anuj Soni

Anuj Soni is a senior incident responder at a DC-based consulting firm. Anuj manages and executes specialized incident response techniques to detect, respond to, and mitigate sophisticated threat actors across commercial and government networks. He uses his skills in conducting host-based forensics, malicious code analysis, and advanced threat risk assessments to help clients improve their security posture. He has over 8 years of experience in incident response, forensics, malware analysis, penetration testing, and steganalysis. Anuj received his Bachelors and Masters from Carnegie Mellon University and holds the following certifications: GIAC Reverse Engineering Malware (GREM), EnCase Certified Examiner (EnCE), and Certified Information Systems Security Professional (CISSP). @asoni

Chad Tilbury

Chad Tilbury has been responding to computer intrusions and conducting forensic investigations since 1998. 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. @chadtilbury

Alissa Torres

Alissa Torres is a certified SANS instructor, specializing in advanced computer forensics and incident response. Her industry experience includes serving in the trenches as part of the Mandiant Computer Incident Response Team (MCIRT) as an incident handler and working on a internal security team as a digital forensic investigator. She has extensive experience in information security, spanning government, academic, and corporate environments and holds a Bachelors degree from University of Virginia and a Masters from University of Maryland in Information Technology. Alissa has taught as an instructor at the Defense Cyber Investigations Training Academy (DCITA), delivering incident response and network basics to security professionals entering the forensics community. She has presented at various industry conferences and numerous B-Sides events. In addition to being a GIAC Certified Forensic Analyst (GCFA), she holds the GCFE, GPEN, CISSP, EnCE, CFCE, MCT and CTT+. @sibertor

The information security field is growing and maturing rapidly. Are you positioned to grow with it? A Master's Degree in Information Security from the SANS Technology Institute (STI) will help you build knowledge and skills in management or technical engineering.

The SANS Technology Institute (STI) offers two unique master's degree programs:

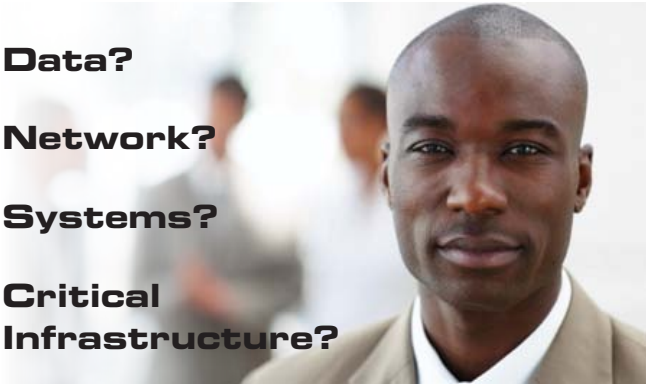
MASTER OF SCIENCE IN INFORMATION SECURITY ENGINEERING

MASTER OF SCIENCE IN INFORMATION SECURITY MANAGEMENT

Apply today! Cohorts are forming now.
sans.edu

info@sans.edu | 855-672-6733

How Are You Protecting Your



Get GIAC certified!

GIAC offers over 26 specialized certifications in security, digital forensics, penetration testing, web application security, IT audit, management, and IT security law.

FOR408: GIAC Certified Forensic Examiner (GCFE)

FOR508: GIAC Certified Forensic Analyst (GCFA)

FOR572: GIAC Network Forensic Analyst (GNFA)

FOR610: GIAC Reverse Engineering Malware (GREM)

SEC504: GIAC Certified Incident Handler (GCIH)

giac.org

FUTURE SANS TRAINING EVENTS

SANS Cyber Defense Initiative 2014
Washington, DC | December 10-19 | #SANSCDI

SANS Security East 2015
New Orleans, LA | January 16-21 | #SecurityEast

SANS Cyber Threat Intelligence SUMMIT & TRAINING 2015
Washington, DC | February 2-9 | #CTISummit

10TH ANNUAL ICS Security SUMMIT – ORLANDO 2015
Orlando, FL | February 23 - March 2 | #SANSICS

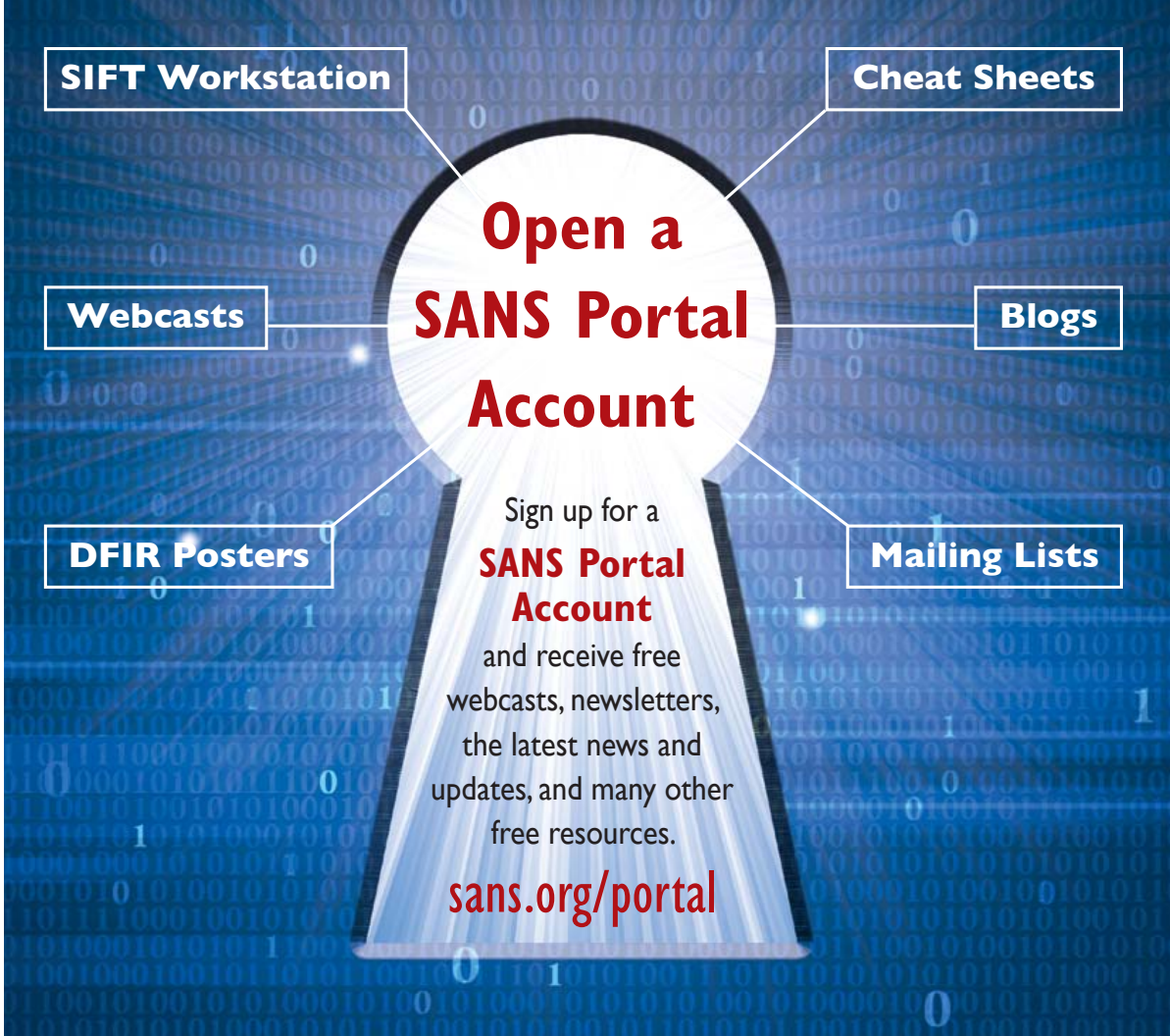
SANS Cyber Guardian 2015
Baltimore, MD | March 2-7 | #CyberGuardian

SANS Northern Virginia 2015
Reston, VA | March 9-14 | #SANSNoVA

SANS 2015
Orlando, FL | April 11-18 | #SANS2015

SANS DFIR SUMMIT & TRAINING 2015
Austin, TX | July 7-14 | #DFIRSummit

Visit sans.org for a complete schedule.



SANS DFIR MONTEREY 2015

Hotel Information

Training Campus
Monterey Marriott

350 Calle Principal
Monterey, CA 93940
sans.org/dfir2015/location

This Monterey hotel near Carmel by the Sea is within walking distance to many of the area's top attractions and family activities. Enjoy shopping and dining or indulge in the various family-fun activities at Cannery Row, just a short drive from the hotel.

Special Hotel Rates Available

A special discounted rate of $162.00 S/D will be honored based on space availability. Government per diem rooms are available with proper ID; you will need to call reservations and ask for the SANS government rate. These rates include high-speed Internet in your room and are only available through February 2, 2015. To make reservations please call (800) 228-9290 or (831) 649-4234.

Top 5 reasons to stay at the Monterey Marriott

1. All SANS attendees receive complimentary high-speed Internet when booking in the SANS block.
2. No need to factor in daily cab fees and the time associated with travel to alternate hotels.
3. By staying at the Monterey Marriott, you gain the opportunity to further network with your industry peers and remain in the center of the activity surrounding the training event.
4. SANS schedules morning and evening events at the Monterey Marriott that you won't want to miss!
5. Everything is in one convenient location!

SANS DFIR MONTEREY 2015

Registration Information

We recommend you register early to ensure you get your first choice of courses.

Register online at sans.org/dfir2015/courses

Select your course or courses and indicate whether you plan to test for GIAC certification.

If the course is still open, the secure, online registration server will accept your registration. Sold-out courses will be removed from the online registration. Everyone with Internet access must complete the online registration form. We do not take registrations by phone.

Register Early and Save

	DATE	DISCOUNT	DATE	DISCOUNT
Register & pay by	**12/31/14**	**$400.00**	**1/28/15**	**$200.00**

Some restrictions apply.

Group Savings (Applies to tuition only)*

10% discount if 10 or more people from the same organization register at the same time
5% discount if 5 - 9 people from the same organization register at the same time

To obtain a group discount, complete the discount code request form at sans.org/security-training/discounts prior to registering.

**Early-bird rates and/or other discounts cannot be combined with the group discount.*

Cancellation

You may substitute another person in your place at any time, at no charge, by e-mail: registration@sans.org or fax: 301-951-0140. Cancellation requests without substitution must be submitted in writing, by mail, or fax, and postmarked by February 4, 2015 – processing fees may apply.

DFIR MONTEREY 2015

a REDFIRE Event

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


digital-forensics.sans.org/blog


@sansforensics


sansforensics


gplus.to/sansforensics


dfir.to/MAIL-LIST

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

Save $400 when you register and pay by December 31

sans.org/dfir2015