SANS DFIR

dē-'fər-'kän

The All Forensics Training Event

March 5-10, 2014 | Monterey, CA

sans.org/event/dfircon-monterey-2014

COURSES BEING OFFERED

CORE

FOR408
Computer Forensic Investigations – Windows In-Depth
GCFE

SEC504
Hacker Techniques, Exploits, and Incident Handling
GCIH

ADVANCED AND IN-DEPTH

FOR508
Advanced Computer Forensic Analysis & Incident Response
GCFA

FOR572
Advanced Network Forensics and Investigations

LEARN REM

FOR610
REM: Malware Analysis Tools and Techniques
GREM

SPECIALIZATION

FOR526
Windows Memory Forensics In-Depth

FOR585
Advanced Smartphone & Mobile Device Forensics

dē-'fər-'kän

MARCH 5-10, 2014 | MONTEREY, CA

This unique Digital Forensics and Incident Response (DFIR) event brings together SANS' most popular forensics courses, top instructors, and bonus seminars for a comprehensive training experience. This is a must-attend event because our leading experts will help you and your team take your DFIR skills to the next level.

Top 5 reasons to attend:

1. **DFIR-Focused Training** – This event offers only SANS' 5-6 day DFIR training classes. In addition, two new courses, Network Forensics (FOR572) and Smartphone Forensics (FOR585), will be making their debut! Be the first to see the new content.
2. **Bonus Talks** – Evenings are packed with bonus talks covering the most ground-breaking DFIR topics.
3. **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.
4. **DFIR NetWar**s –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.
5. **SIFT 3.0** – Brand New Release! We are launching the newest version of SIFT, cutting-edge open source tools that are freely available and frequently updated.

sans.org/event/dfircon-monterey-2014

Hacker Techniques, Exploits, and Incident Handling

Instructor: John Strand

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

More info – sans.org/SEC504

sans.org/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.

sans.org/FOR408

This course focuses on the critical knowledge of the Windows Operating System that every digital forensic analyst needs to investigate computer incidents successfully. You'll cover the methodology of in-depth computer forensic examinations, digital investigative analysis, and media exploitation.

Computer Forensic Investigations – Windows In-Depth

Instructor: Rob Lee

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

More info – sans.org/FOR408

Advanced Computer Forensic Analysis and Incident Response

Instructor: Chad Tilbury

sans.org/FOR508

THE APT IS IN YOUR NETWORK, TIME TO GO HUNTING

> *"I've taken other network intrusion classes but nothing this in-depth. The class is outstanding!"*
>
> -Craig Goldsmith, FBI

- 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

More info – sans.org/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. FOR508 trains teams to identify, contain, and remediate sophisticated threats-including APT groups and financial crime syndicates.

NEW! Advanced Network Forensics and Analysis

Instructor: Philip Hagen

sans.org/FOR572

This course 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.

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

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

More info – sans.org/FOR572

REM: Malware Analysis Tools and Techniques

Instructor: Lenny Zeltser

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

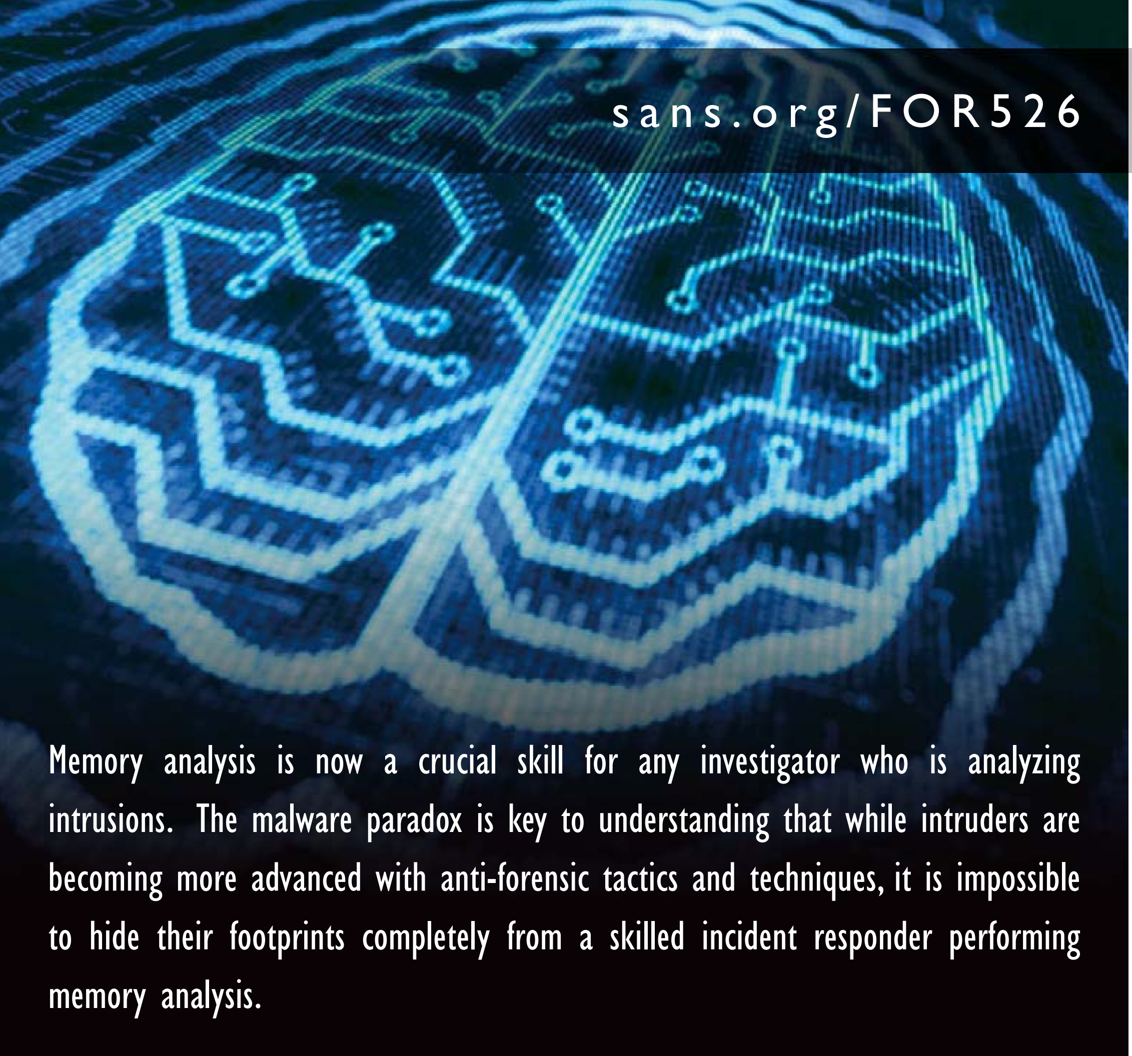
- Build an isolated lab for analyzing malicious code
- Employ network and system-monitoring tools for malware analysis
- Examine malicious JavaScript, VB Script and ActionScript
- Use a disassembler and debugger to analyze malicious Windows executables
- Bypass a variety of defensive mechanisms designed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

More info – sans.org/FOR610

sans.org/FOR610

LEARN R.E.M.

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.



sans.org/FOR526

Memory analysis is now a crucial skill for any investigator 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.

Windows Memory Forensics In-Depth

Instructor: Alissa Torres

MALWARE CAN HIDE, BUT IT MUST RUN

> *"It is entirely possible that key evidence, and perhaps, the only evidence on a system, is resident in memory. This class will really help you develop your memory kung fu."*
>
> - Anonymous

- 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

More info – sans.org/FOR526

NEW! Advanced Smartphone and Mobile Device Forensics

Instructors: Heather Mahalik & Cindy Murphy

YOUR TEXTS AND APPS CAN AND WILL BE USED AGAINST YOU

> *"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

- 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

More info – sans.org/FOR585

sans.org/FOR585

This course 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. The 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.

BONUS SESSIONS

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

KEYNOTE: Have No Fear – DFIR is Here!

Rob Lee, Chad Tilbury, Alissa Torres,
Phil Hagen, and Lenny Zeltser

In less time than it takes you to watch the Avengers, the DFIR hero team will take you through an end-to-end investigation starting with core steps in digital forensics, incident response, memory analysis, and malware analysis.

DFIReception - Forensicators Unite!

Wed, March 5 | 6-7pm

Join us after the first day of class, and immediately before the Keynote event, join 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+.

Panic! Hysteria! No Malware Required!

John Strand

The landscape has shifted. Security is no longer something your organization can have complete control over. In this presentation John Strand will (quickly) demonstrate how most large corporations can be compromised in moments, even without phishing.

Malware Analysis Essentials Using REMnux

Lenny Zeltser

Knowing how to analyze malware has become a critical skill for incident responders and forensic investigators. This practical talk will explain how to you can get started with malware analysis by using free tools installed on the REMnux Linux distribution.

There's *GOLD* in Them Thar Package Management Databases!

Phil Hagen

This presentation will focus on how to leverage RPM in forensic investigations, as it can provide a quick and effective way to find changed files that warrant more in-depth analysis. We'll also discuss potential shortfalls to consider in using this method.

Sick Anti-Forensics Mechanisms in the Wild

Alissa Torres

During this presentation, several of these anti-forensics techniques will be explored, preparing attendees for what they are likely to encounter with increasing frequency - malware that fights back.

Forensic Handling of the iPhone 5c and 5s

Heather Mahalik

This presentation will cover the latest capabilities on iOS devices and will focus on the shortfalls of the tools available and will suggest forensic work-arounds.

A 10 Second Journey: Parsing the structure of the Windows 8 Prefetch Artifact

Jared Atkinson

As Microsoft and other vendors release new Operating System products, forensics researchers must keep up to date with the ever-changing state of available forensic artifacts. This presentation explores the Windows 8 Prefetch file structure, and how the new version of this abundant artifact has become even more potent than ever.

SANS DFIR

dē-'fər-'kän

NETWARS TOURNAMENT

SANS DFIR NetWars at de-'fer-'kän 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 **File and Packet Analysis**

Digital Forensics **Memory Analysis**

Incident Response

Netwars is complimentary for de-'fer-'kän attendees.
Sign up when you register for your course.

computer-forensics.sans.org/training/netwars

SANS Simulcast

Can't attend de-'fer-'kän 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.

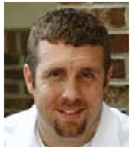
The following courses will be available via SANS Simulcast:

FOR408 | FOR508 | FOR526 | FOR610 | SEC504

Register Now!

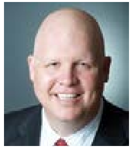
sans.org/event/dfircon-monterey-2014

DFIRCON INSTRUCTORS



Philip Hagen

Philip Hagen has over 14 years of experience in creating and deploying strategic and ad-hoc IT and infosec solutions. He has managed small, tactical projects and large government contracts. Phil started his security career while attending the US Air Force Academy, with research covering both the academic and practical sides of security. He served in the Air Force as a Communications Officer, and was assigned to a base-level Year 2000 project management office. He later managed a team of 85 computer forensic professionals in the National Security sector. Most recently, Phil formed Lewes Technology Consulting, LLC. @PhilHagen

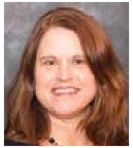


Rob Lee

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

Heather Mahalik

Heather Mahalik is a senior digital forensics analyst at Basis Technology. As the on-site project manager, she uses her experience to manage the cell phone exploitation team and supports media and cell phone forensics efforts in the U.S. government. Heather has worked in digital forensics for over ten years and has performed thousands of forensic acquisitions and examinations on hard drives, e-mail and file servers, mobile devices, and portable media. Previously, Heather worked as a forensic examiner for Stroz Friedberg and the U.S. State Department Computer Investigations and Forensics Lab, where she focused her efforts on high profiles cases. @HeatherMahalik

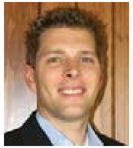


Cindy Murphy

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

John Strand

John Strand is a senior instructor with the SANS Institute. He teaches SEC504: Hacker Techniques, Exploits, and Incident Handling; SEC560: Network Penetration Testing and Ethical Hacking; SEC580: Metasploit Kung Fu for Enterprise Pen Testing; and SEC464: Hacker Guard: Security Baseline Training for IT Administrators and Operations with Continuing Education. John is the course author for SEC464: Hacker Guard: Security Baseline Training for IT Administrators and Operations with Continuing Education and the co-author for SEC580: Metasploit Kung Fu for Enterprise Pen Testing. When not teaching for SANS, John co-hosts PaulDotCom Security Weekly, the world's largest computer security podcast. He is also the owner of Black Hills Information Security, specializing in penetration testing and security architecture services. He has presented for the FBI, NASA, the NSA, and at DefCon. @strandjs

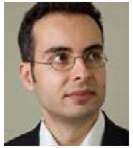


Chad Tilbury

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. 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. 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. In addition to being a GIAC Certified Forensic Analyst (GCFA), she holds the GCFE, GPEN, CISSP, EnCE, CFCE, MCT and CTT+. @sibertor



Lenny Zeltser

Lenny Zeltser is a seasoned business leader with extensive experience in information technology and security. As a product management director at NCR Corporation, he focuses on safeguarding IT infrastructure of small and mid-size businesses world-wide. Before NCR, Lenny led the enterprise security consulting practice at a major IT hosting provider. He also teaches digital forensics and malware courses for the SANS Institute, where he is a senior faculty member. In addition, Lenny is a Board of Directors member at SANS Technology Institute and a volunteer incident handler at the Internet Storm Center. Lenny's expertise is strongest at the intersection of business, technology, and information security practices and includes incident response, cloud services, and product management. Lenny is one of the few individuals in the world who've earned the prestigious GIAC Security Expert designation. He has an MBA degree from MIT Sloan and a Computer Science degree from the University of Pennsylvania. @lennyzeltser

@sansforensics http://computer-forensics.sans.org/blog sansforensics http://gplus.to/sansforensics

FUTURE SANS TRAINING EVENTS

SANS Security East 2014

New Orleans, LA | January 20-25

SECURING SANS 00100111 THE APP

SANS AppSec 2014

Austin, TX | February 3-8

CyberCon
Online Training Event

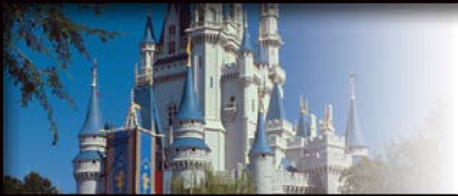
SANS CyberCon Spring 2014

Online | February 10-15

SANS ICS Industrial Control Systems

ICS Security Summit 2014 - Orlando

Lake Buena Vista, FL | March 12-18



SANS 2014

Orlando, FL | April 5-14

SANS Digital Forensics & Incident Response SUMMIT

Austin, TX | June 3-10

SANS Rocky Mountain 2014

Denver, CO | June 7-14

SANSFIRE 2014

Baltimore, MD | June 19-30

See a complete list of all future SANS training events at sans.org/security-training/by-location/all

SANS DFIRCON 2014

Hotel Information

Training Campus
Monterey Marriott

350 Calle Principal
Monterey, CA 93940
sans.org/event/dfircon-monterey-2014/location

Special Hotel Rates Available

A special discounted rate of $159.00 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 are only available through February 11, 2014. To make reservations please call (800) 228-9290 or (831) 649-4234 and ask for the SANS group rate.

The Monterey Marriott Hotel is located in the heart of historic downtown and just steps away from the Monterey Peninsula, making it an ideal choice for any visit to the city. Experience first-class service at the Monterey Marriott Hotel and discover why the property is among the top choices of Monterey Bay hotels for spa vacations, business meetings, and everything in-between.

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 DFIRCON 2014

Registration Information

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

Register online atsans.org/event/dfircon-monterey-2014

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	**1/22/14**	**$400.00**	**2/5/14**	**$250.00**

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 12, 2014 – processing fees may apply.

dē-'fər-'kän

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

- http://computer-forensics.sans.org/blog
- @sansforensics
- sansforensics
- http://gplus.to/sansforensics
- https://lists.sans.org/mailman/listinfo/dfir

5705 Salem Run Blvd.
Suite 105
Fredericksburg, VA 22407

Save $400 when you register and pay by January 22nd

sans.org/event/dfircon-monterey-2014

TAKE THE DFIR CHALLENGE

Win a DFIRCON Simulcast Seat!

bit.ly/DFIRCON