



SANS

DFIRCON

EAST

The All Forensics Training Event

November 3-8, 2014

|

Fort Lauderdale, FL

[sans.org/event/dfircon-east-2014](http://sans.org/event/dfircon-east-2014)

## COURSES OFFERED

### CORE



**SEC401**  
Security  
Essentials  
Bootcamp Style  
**GSEC**



**FOR408**  
Windows  
Forensic  
Analysis  
**GCFE**

### ADVANCED AND IN-DEPTH



**New!** **FOR572**  
Advanced  
Network Forensics  
and Analysis  
**GNFA**

### SPECIALIZATION



**New!** **FOR518**  
Mac  
Forensic  
Analysis



**New!** **FOR585**  
Advanced  
Smartphone  
Forensics



NOVEMBER 3-8, 2014

| FORT LAUDERDALE, FL

This unique Digital Forensics and Incident Response (DFIR) 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/event/dfircon-east-2014](http://sans.org/event/dfircon-east-2014)

# Security Essentials Bootcamp Style

Instructor: Tim Garcia

## PREVENTION IS IDEAL BUT DETECTION IS A MUST!

---

*“The flagship SANS course, SEC401 has an exceptional blend of security essential theory and hands-on experience.”*

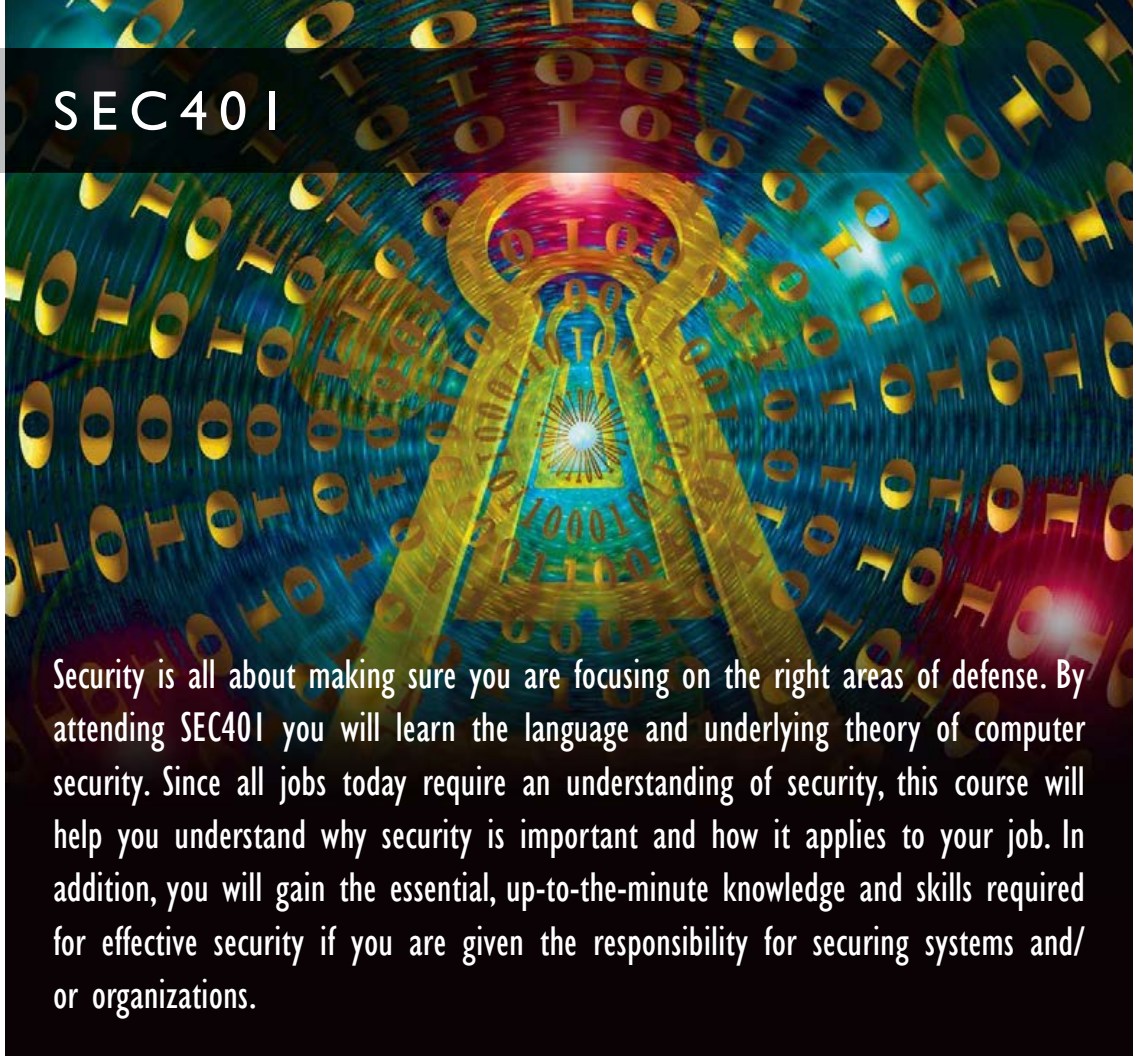
-ED CONCEPCION, USMC

---


- › Design and build a network architecture
- › Learn how to create a security roadmap
- › Build network visibility map for hardening network
- › Develop effective security metrics
- › Analyze systems using Linux and Windows command-line tools
- › Identify vulnerabilities in a system and configure it to be more secure
- › Utilize Wireshark to sniff open protocols to determine content and passwords

[sans.org/sec401](https://sans.org/sec401)

# SEC401



Security is all about making sure you are focusing on the right areas of defense. By attending SEC401 you will learn the language and underlying theory of computer security. Since all jobs today require an understanding of security, this course will help you understand why security is important and how it applies to your job. In addition, you will gain the essential, up-to-the-minute knowledge and skills required for effective security if you are given the responsibility for securing systems and/or organizations.



# FOR408

## Windows Forensic Analysis

Instructors: Rob Lee & David Cowen

**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](https://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.

# NEW! Mac Forensic Analysis

Instructor: Sarah Edwards

## FORENSICATE DIFFERENTLY!

---

*“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.”*

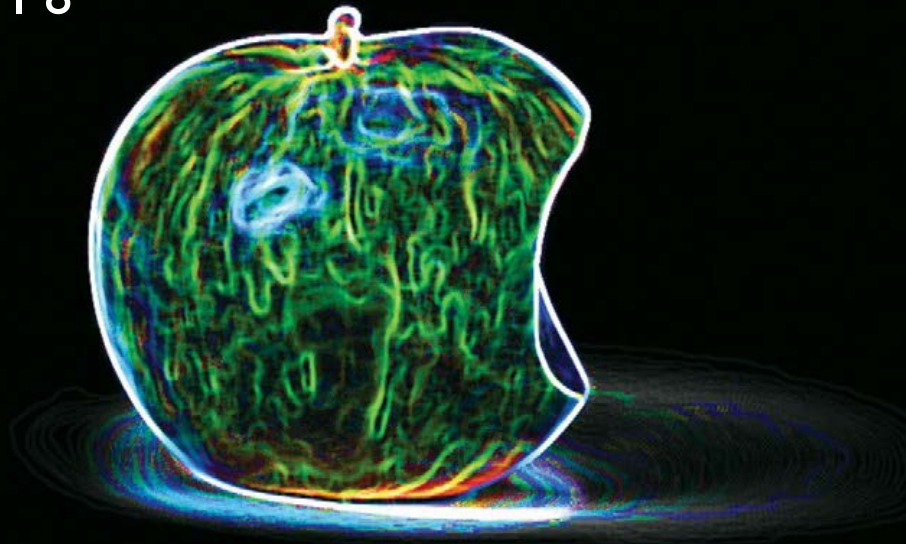
-KEVIN J. RIPA, COMPUTER EVIDENCE RECOVERY, INC.

---

- › 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](https://sans.org/FOR518)

# 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.





# FOR572

## **NEW!** Advanced Network Forensics and Analysis

Instructor: Johannes Ullrich, Ph.D.

### **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

---

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.

- › 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](https://sans.org/FOR572)

# NEW! Advanced Smartphone and Mobile Device Forensics

Instructor: 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 as well as 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

[sans.org/FOR585](https://sans.org/FOR585)

# 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.

# B O N U S   S E S S I O N S

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

## **The Internet of Evil Things**

*Johannes Ullrich, Ph.D.*

Embedded systems are the new target. As our networks grow uncontrolled and unsupervised, forgotten machines will take over and rule us all soon. Analyzing the embedded malware that comes with this presents a number of challenges. Current debuggers and virtualization techniques that mimic these systems are incomplete and will not allow us to completely analyze malware the way we are used to in good old desktop malware environments. These malware blackboxes need different instrumentations and techniques. We will present some ideas on how to analyze these malware samples, and introduce you to embedded system analysis (unless your bot is removing this event from your smart watch's reminder list).

## **DFIR Advanced Smartphone Forensics**

*Cindy Murphy*

Forensic investigations often rely on data extracted from smartphones and tablets. Smartphones are the most personal computing device associated to any user, and can therefore provide the most relevant data per gigabyte examined. Commercial tools often miss digital evidence on smartphones and associated applications, and improper handling can render the data useless. We have created a poster as a cheat-sheet to help you remember how to handle smartphones, where to obtain actionable intelligence, and how to recover and analyze data on the latest smartphones and tablets. This presentation provides an overview of useful data that can be extracted from mobile devices and I will walk through the new **Smartphone Forensics Poster**.

## **When Macs Get Hacked**

*Sarah Edwards*

Computer intrusion cases usually consist of Windows or \*nix systems, if you are lucky. Mac intrusion cases are a rare breed. These cases have the potential to become more popular with the growing market share of Macintosh systems. Many companies and government entities use Macs as their preferred system. This presentation and hands-on lab will introduce you to incident response and intrusion analysis of the Mac.

## **Jumping the Shark**

*Tim Garcia*

Is your security Awareness program like the 10th season of a stale 70's sitcom? Are people just attending to check the box that they completed yearly security awareness training? The Goal of awareness training is to change user behavior. We will discuss some strategies to refresh your security awareness program, ensure people are listening and track its effectiveness. Just like when Fonzie jumped the shark on "Happy Days" your security awareness program will never be the same.

## **Filesystem Journal Forensics**

*David Cowen*

Journalled file systems have been a part of modern file systems for years but the science of computer forensics has only been approaching them mainly as a method of recovering deleted files. In this talk we will outline the three major file systems in use today that utilize journaling (NTFS, EXT3/4, HFS+) and explain what is stored and its impact on your investigations. We will discuss NTFS and new analysis techniques:

- Recover data hidden or destroyed by anti-forensics
- Determine exact deletion times
- Determine what was being accessed and how often





# NETWARS

## T O U R N A M E N T

SANS DFIR NetWars at DFIRCON East 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 Analysis**

**Digital Forensics**

**Packet Analysis**

**Incident Response**

**Memory Analysis**

***NetWars is complimentary for DFIRCON East attendees.***

***Sign up when you register for your course.***

[digital-forensics.sans.org/training/netwars](https://digital-forensics.sans.org/training/netwars)

*“Whether a DFIR newbie or a veteran examiner, DFIR NetWars will make you a better examiner by identifying weaknesses and fine-tuning skill sets.”*

*-BRAD GARNETT,*

*KEMPER CPA GROUP LLP*

# DFIRCON EAST INSTRUCTORS



## David Cowen

Mr. Cowen has more than sixteen years of experience in the areas of integration, architecture, assessment, programming, forensic analysis and investigation. He currently holds the Certified Information Systems Security Professional certification from (ISC)2. He has been trained

in proper forensics practices by the High Tech Crime Investigators Association, ASR Data and Guidance Software, and SANS, amongst others. He is an active contributor within the computer forensics community where he frequently presents and trains on various forensic topics. He has managed, created, and worked with multiple forensics/litigation support teams and associated procedures. His experience spans a variety of environments ranging from high security military installations to large/small private sector companies. He is the author of *Infosec Pro Guide to Computer Forensics, Hacking Exposed: Computer Forensics* (1st and 2nd edition) and the *Anti Hacker Toolkit* 3rd edition all by McGraw Hill. @HECFBlog



## Tim Garcia

Tim has over 10 years of diversified experience in systems engineering and project management as well as information security principles and procedures. His knowledge of security procedures and legislation such as Sarbanes-Oxley, GLBA, CobiT, COSO, and ISO 1779 make

him the perfect mentor for this class. He has taught Information security and project management courses for Keller School of Graduate Management, ITT Technical Institute and Western International University and currently holds his CISSP, GSEC, GCIA, and NSA-IAM certifications. He has worked at Intel, with the military, and currently is employed at Wells Fargo.



## 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; Shmocon, CEC, BSidesNOLA, TechnoSecurity, HTCA, 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. @iameviltwin



## 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. @robtle



## 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



## Johannes Ullrich, Ph.D.

As Dean of Research for the SANS Technology Institute, Johannes is currently responsible for the SANS Internet Storm Center (ISC) and the GIAC Gold program. He founded DShield.org in 2000, which is now the data collection engine behind the ISC. His work with the ISC

has been widely recognized, and in 2004, Network World named him one of the 50 most powerful people in the networking industry. Prior to working for SANS, Johannes worked as a lead support engineer for a web development company and as a research physicist. Johannes holds a PhD in Physics from SUNY Albany and is located in Jacksonville, Florida. His daily podcast summarizes current security news in a concise format.

@johullrich @sans\_isc



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**

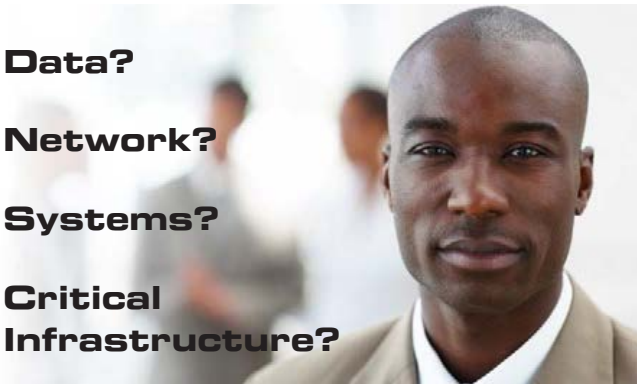
Apply today! Cohorts are forming now.  
**sans.edu**

**info@sans.edu | 855-672-6733**



## How Are You Protecting Your

- **Data?**
- **Network?**
- **Systems?**
- **Critical Infrastructure?**



### 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.



**SEC401: GIAC Security Essentials (GSEC)**  
[giac.org/certification/security-essentials-gsec](http://giac.org/certification/security-essentials-gsec)



**FOR408: GIAC Certified Forensic Examiner (GCFE)**  
[giac.org/certification/certified-forensic-examiner-gcfe](http://giac.org/certification/certified-forensic-examiner-gcfe)



**FOR572: GIAC Network Forensic Analyst (GNFA)\***  
[giac.org/certification/network-forensic-analyst-gnfa](http://giac.org/certification/network-forensic-analyst-gnfa)

\*The GNFA will not be available until November 3, 2014.



# SANS Investigative Forensic Toolkit (SIFT) Workstation Version 3.0

## SANS INVESTIGATIVE FORENSIC TOOLKIT

[digital-forensics.sans.org/community/downloads](https://digital-forensics.sans.org/community/downloads)

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](https://sift.readthedocs.org)**
- › **Expanded Filesystem Support**

# SANS TRAINING FORMATS

## LIVE CLASSROOM TRAINING



### Training Events

*Live Instruction from SANS' Top Faculty, Vendor Showcase, Bonus Evening Sessions, and Networking with Your Peers*  
[sans.org/security-training/by-location/all](https://sans.org/security-training/by-location/all)



### Community SANS

*Live Training in Your Local Region with Smaller Class Sizes*  
[sans.org/community](https://sans.org/community)



### OnSite

*Live Training at Your Office Location*  
[sans.org/onsite](https://sans.org/onsite)



### Mentor

*Live Multi-Week Training with a Mentor*  
[sans.org/mentor](https://sans.org/mentor)



### Summit

*Live IT Security Summits and Training*  
[sans.org/summit](https://sans.org/summit)

## ONLINE TRAINING



### OnDemand

*E-learning Available Anytime, Anywhere, at Your Own Pace*  
[sans.org/ondemand](https://sans.org/ondemand)



### vLive

*Online Evening Courses with SANS' Top Instructors*  
[sans.org/vlive](https://sans.org/vlive)



### Simulcast

*Attend a SANS Training Event without Leaving Home*  
[sans.org/simulcast](https://sans.org/simulcast)



### OnDemand Bundles

*Extend Your Training with an OnDemand Bundle Including Four Months of E-learning*  
[sans.org/ondemand/bundles](https://sans.org/ondemand/bundles)



# FUTURE SANS SUMMIT & TRAINING EVENTS



## SANS **Crystal City** 2014

Crystal City, VA | September 8-13



## SANS **Baltimore** 2014

Baltimore, MD | September 22-27



## **Retail Cyber Security** SUMMIT & TRAINING

Dallas, TX | September 8-17



## SANS **Seattle** 2014

Seattle, WA | September 29 - October 6



## **Security Awareness** SUMMIT & TRAINING

Dallas, TX | September 8-17



## SANS **Network Security** 2014

Las Vegas, NV | October 19-27



## SANS **Albuquerque** 2014

Albuquerque, NM | September 15-20



## SANS **Cyber Defense San Diego** 2014

San Diego, CA | November 3-8

See a complete list of all future SANS training events at [sans.org/security-training/by-location/all](http://sans.org/security-training/by-location/all)

SANS DFIRCON EAST 2014



## Hotel Information

*Training Campus*  
**Riverside Hotel**

**620 East Las Olas Boulevard**

**Fort Lauderdale, FL**

[sans.org/event/dfircon-east-2014/location](http://sans.org/event/dfircon-east-2014/location)

Riverside Hotel is located in the heart of downtown Fort Lauderdale, and is the only hotel on trendy Las Olas Boulevard. Divided by a median of flowers and shady trees, the Boulevard features cool sub-tropical breezeways and courtyards alive with sidewalk cafes, chic boutiques, art galleries, and world class restaurants. Less than two miles from Fort Lauderdale Beach, Riverside Hotel is the perfect location for your time in South Florida. See you on the Boulevard!

### 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 include high-speed Internet in your room and are only available through October 11, 2014. To make reservations, please call 800-325-3280 or 954-467-0671 and ask for the SANS group rate.**

### Top 5 reasons to stay at the Riverside Hotel

- 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 Riverside Hotel, 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 Riverside Hotel that you won't want to miss!
- 5 Everything is in one convenient location!

SANS DFIRCON EAST 2014

## Registration Information

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



Register online at [sans.org/event/dfircon-east-2014/courses](http://sans.org/event/dfircon-east-2014/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	9/17/14	\$400.00	10/1/14	\$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](http://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](mailto:registration@sans.org) or fax: 301-951-0140. Cancellation requests without substitution must be submitted in writing, by mail, or fax, and postmarked by October 15, 2014 — processing fees may apply.



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



[digital-forensics.sans.org/blog](http://digital-forensics.sans.org/blog)



[@sansforensics](https://twitter.com/sansforensics)



[sansforensics](https://www.facebook.com/sansforensics)



[gplus.to/sansforensics](https://plus.google.com/sansforensics)



[lists.sans.org/mailman/listinfo/dfir](mailto:lists.sans.org/mailman/listinfo/dfir)



5705 Salem Run Blvd.  
Suite 105  
Fredericksburg, VA 22407

**Save \$400 when you register and pay by September 17**

**[sans.org/event/dfircon-east-2014](http://sans.org/event/dfircon-east-2014)**

