



SANS DFIR²⁰¹⁵

The Premier Digital Forensics and Incident Response Training and Summit

SUMMIT: July 7-8 | TRAINING: July 9-14 | Austin, TX

COURSES OFFERED

CORE



INCIDENT RESPONSE & ADVERSARY HUNTING



OPERATING SYSTEM & DEVICE IN-DEPTH



TWO-NIGHT CHALLENGE



SANS DFIR 2015

SUMMIT: July 7-8 | TRAINING: July 9-14
Austin, TX

Hear what your peers have said about the SANS DFIR Summit:

“SANS continues to deliver speakers with high caliber content that is in line with current security trends, which is a real need for security practitioners.”

-Daniel García, Baker Hughes

“Cutting-edge research shared by those in the trenches and the front-lines of digital forensics and incident response. A must-attend event for every DFIR professional!”

-Brad Garnett, Kemper CPA Group LLP

“The SANS DFIR Summit is regularly the most technical and highest value forensics-focused training event I've attended. It is always my #1!”

-Alex Bond, Mandiant

Whether you're new to the field or a seasoned professional the DFIR Summit & Training is the premier forensic training event created to tackle advanced DFIR issues. Choose from six DFIR courses taught by industry experts, two days of trending talks at the Summit and opportunities for real discussions with the best leaders in the community.

sans.org/dfirsummit

“The Summit is a great way to get to know leaders, newcomers, and everyone in between. The networking at a smaller event like this is worth it alone – and the presentations make it much more valuable. It's always a great time.”

-Stacey Edwards, The Sylint Group

Windows Forensic Analysis

Instructor: Chad Tilbury @chadtilbury

**MASTER WINDOWS FORENSICS –
YOU CAN'T PROTECT WHAT YOU
DON'T KNOW ABOUT.**

“This is by far the best training I have ever had. My forensic knowledge increased more in the last 5 days than in the last year.”

-Vito Rocco, UNLNY

- > 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



**SIMULCAST
AVAILABLE**
sans.org/simulcast



giac.org

FOR408

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.

FOR508



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.

Advanced Incident Response

Instructor: Rob Lee @roblee

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

“The most in-depth, state-of-the-art IR course I can imagine. It's the first time I think defense can actually gain an advantage.”

-KAI THOMSEN, AUDI AG

- > 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



**SIMULCAST
AVAILABLE**
sans.org/simulcast



giac.org

sans.org/FOR508

FOR526



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.

Memory Forensics In-Depth

Instructor: Alissa Torres @sibertor

MALWARE CAN HIDE, BUT IT MUST RUN

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

-MATTHEW BRITTON, BLUE CROSS BLUE SHIELD OF LOUISIANA

- > 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



**SIMULCAST
AVAILABLE**
sans.org/simulcast

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 @PhilHagen

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

“I research ICS/SCADA environments. I think FOR572 presents a better approach at detecting malware than a more traditional approach does.”

–NIKLAS VILHELM, NORWEGIAN NATIONAL SECURITY AUTHORITY

- > 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

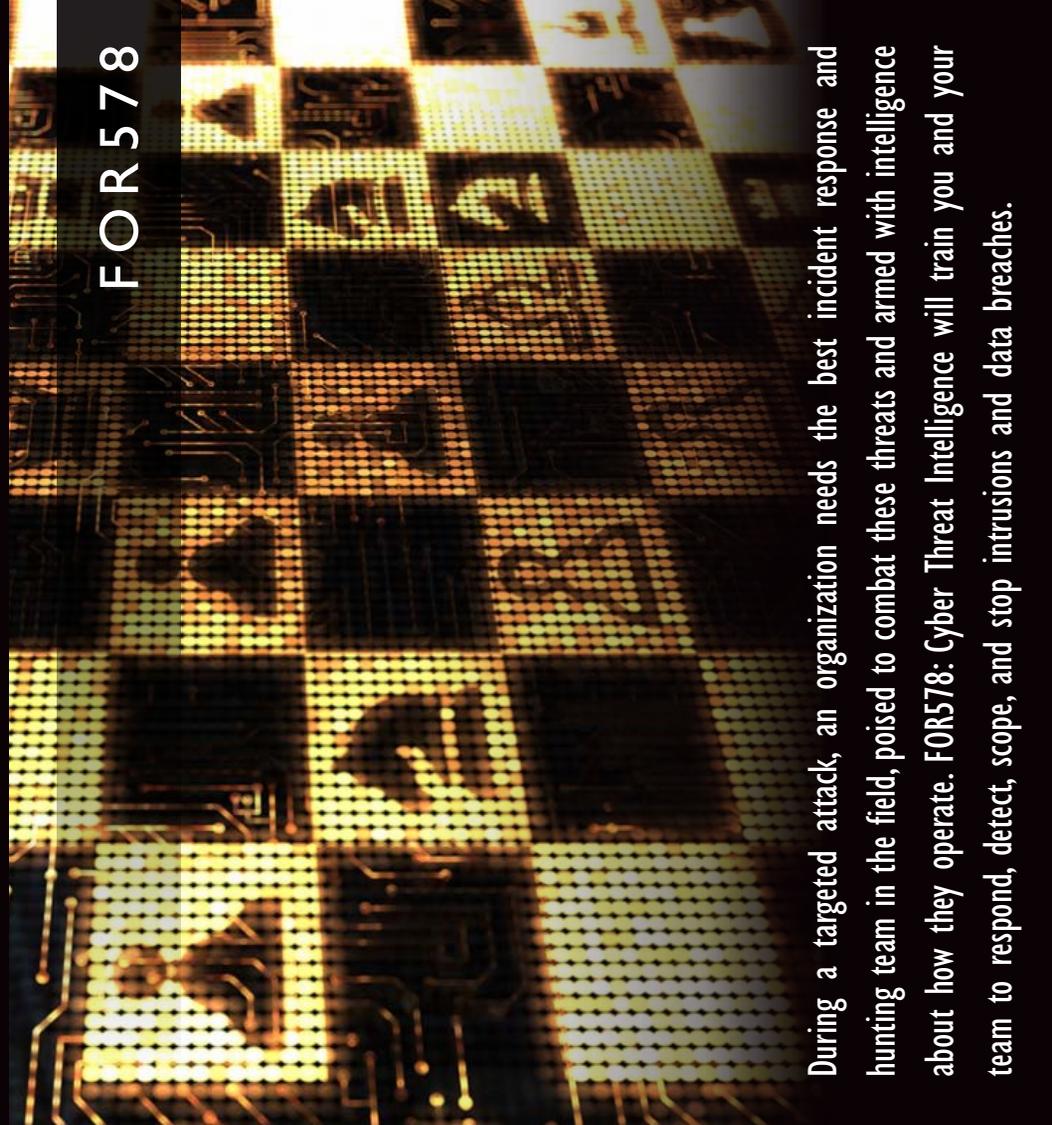


**SIMULCAST
AVAILABLE**
sans.org/simulcast



giac.org

FOR578



During a targeted attack, an organization needs the best incident response and hunting team in the field, poised to combat these threats and armed with intelligence about how they operate. FOR578: Cyber Threat Intelligence will train you and your team to respond, detect, scope, and stop intrusions and data breaches.

Cyber Threat Intelligence

Instructor: Mike Cloppert @mikecloppert

“In teaching this course, my goal is to create a colleague – someone I trust and who understands how to look at defending networks by leveraging the perspective of our adversary.

This course represents my wish list for the baseline knowledge and experience I’d like to see among all the new colleagues I will meet throughout my career.”

–MIKE CLOPPERT, FOR578 COURSE AUTHOR

- > Determine the role of cyber threat intelligence in their jobs
- > Know the analysis of an intrusion by a sophisticated actor is complete
- > Identify, extract, prioritize, and leverage intelligence from advanced persistent threat (APT) intrusions
- > Expand upon existing intelligence to build profiles of adversary groups
- > Leverage collected intelligence to improve success in defending against and responding to future intrusions
- > Manage, share, and receive intelligence on APT actors

sans.org/FOR578

NEW

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.



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.

REM: Malware Analysis Tools & Techniques

Instructor: Hal Pomeranz @hal_pomeranz

TURN MALWARE INSIDE-OUT

“FOR610 should be required training for all forensic investigators. It is necessary for awareness, analysis, and reporting of threats.”

-PAUL GUNNERSON, U.S. ARMY

- > 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



**SIMULCAST
AVAILABLE**
sans.org/simulcast



giac.org

Hacker Tools, Techniques, Exploits, and Incident Handling

Instructor: Bryce Galbraith @brycegalbraith

KNOW YOUR ENEMY

“SEC504 opens your eyes to the real cyberworld.

It encourages thinking about security of data and network access.”

-FRANK MUNSON, VIRGINIA INTERNATIONAL TERMINAL

- > 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



**SIMULCAST
AVAILABLE**
sans.org/simulcast



giac.org

SANS DFIR SUMMIT BONUS SESSIONS

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

CSI and Blackhat Scorpions: From Hollywood to Keyboard

Robert M. Lee

With movies like Blackhat and shows like CSI: Cyber and Scorpion, reality often gets hyped up for a bit of good Hollywood effect; but sometimes the truth is stranger than fiction. This past year there have been a number of high-profile intrusions impacting almost every identifiable sector; from aviation to banking to healthcare. These intrusions have showed creativity, shocked the public, and presented a challenge for forensic analysts in different fields. This talk will take a look at some of the most interesting intrusions faced this past year; where digital forensics excelled, and what we as a community learned – all in the theme of lighthearted Hollywood flair:

Preparing for PowerShellmageddon – Investigating Windows Command Line Activity

Chad Tilbury

There is a reason hackers use the command line, and it isn't to impress you with their prowess. Throughout the history of Windows, the command line has left far fewer forensic artifacts than equivalent operations via the GUI. To make matters worse, the transition to Windows 7 and 8 has spread PowerShell throughout the enterprise. While it makes our lives easier as defenders, it does the same for our adversaries. Every time you marvel at the capabilities of PowerShell, you should fear how your adversaries may use that power against you. This talk will demonstrate how incident responders are countering the command line threat with real-world examples. Learn 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:

The Tap House

Philip Hagen

Packets move pretty fast. The field of Network Forensics needs to move fast, too. Whether you are investigating a known incident, hunting unidentified adversaries in your environment, or enriching forensic findings from disk- and memory-based examinations, it's critical to stay abreast of the latest developments in the discipline. In this talk, Philip Hagen will discuss some of the latest technologies, techniques, and tools that you'll want to know in pursuit of forensication nirvana. Phil is also an avid craft beer fan, so there's a good chance you'll learn something about a new notable national or interesting local beer in the process. This presentation will be helpful for those who wish to keep up-to-date on the most cutting-edge facets of Network Forensics.

The Plinko Board of Modern Persistence Techniques

Alissa Torres

No matter what techniques an attacker employs to hide and persist on compromised remote systems, we must be up for the challenge, to detect, analyze and remediate. This session focuses on the latest techniques modern malware is using to ensure continued presence in your network. As detailed in recently released industry threat intelligence reports, these methods are increasing in sophistication and are often missed by forensics tools developed only to enumerate common autorun and service persistence methods. In this presentation, we will cover advanced detection techniques, pivoting from physical memory analysis to the examination of remnants found on the file system.



DFIR NETWARS

T O U R N A M E N T

SANS DFIR NetWars at the DFIR SUMMIT 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.

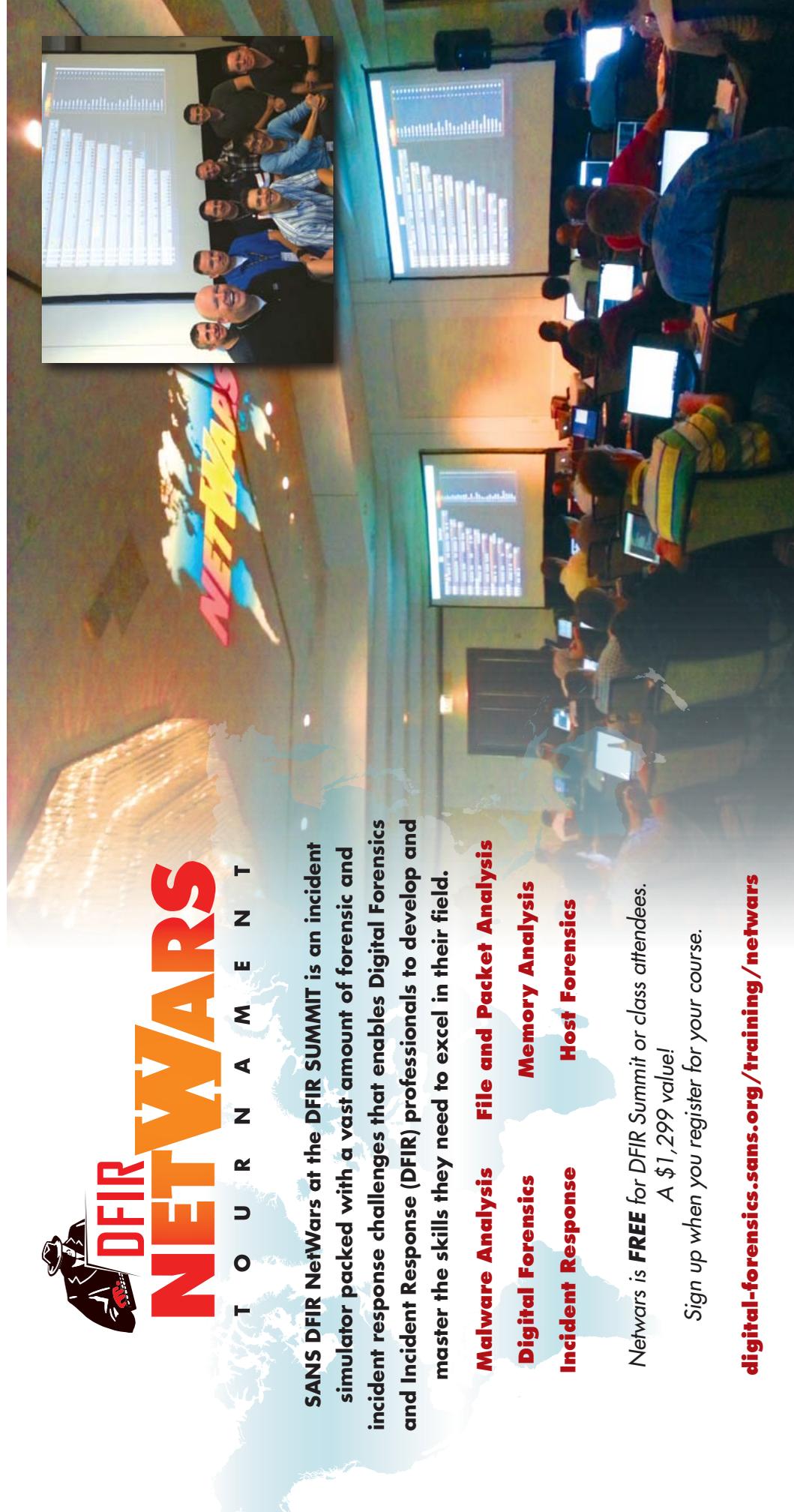
Malware Analysis **File and Packet Analysis**
Digital Forensics **Memory Analysis**
Incident Response **Host Forensics**

NetWars is **FREE** for DFIR Summit or class attendees.

A \$1,299 value!

Sign up when you register for your course.

digital-forensics.sans.org/training/netwars



Can't attend the DFIR SUMMIT 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 | FOR610 | SEC504

Register Now!

sans.org/dfirsummit/attend-remotely



Awesome speakers at DFIR!

SANS DFIR SUMMIT INSTRUCTORS



Bryce Galbraith

As a contributing author of the internationally bestselling book *Hacking Exposed: Network Security Secrets & Solutions*, Bryce helped bring the secret world of hacking out of the darkness and into the public eye. Bryce has held security positions at global ISPs and Fortune 500 companies, he was a member of Foundstone's renowned penetration testing team and served as a senior instructor and co-author of Foundstone's Ultimate Hacking: Hands-On course series. Bryce is currently the owner of Layered Security where he provides specialized vulnerability assessment and penetration testing services for clients. Bryce is an active member of several security-related organizations, he holds several security certifications and speaks at conferences around the world. [@brycegalbraith](https://twitter.com/brycegalbraith)



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



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 where he managed Internet anti-piracy operations for the seven major Hollywood studios in over sixty countries. [@chadtilbury](https://twitter.com/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. [@sibertor](https://twitter.com/sibertor)



Mike Cloppert

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



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



Hal Pomeranz

Hal Pomeranz is an independent digital forensic investigator who has consulted on cases ranging from intellectual property theft, to employee sabotage, to organized cybercrime and malicious software infrastructures. He has worked with law enforcement agencies in the U.S. and Europe and global corporations. While equally at home in the Windows or Mac environment, Hal is recognized as an expert in the analysis of Linux and Unix systems. His research on EXIF4 file system forensics provided a basis for the development of Open Source forensic support for this file system. His EXIF3 file recovery tools are used by investigators worldwide. Hal is a SANS Faculty Fellow and Lethal Forensicator, and is the creator of the SANS Linux/Unix Security course. [@hal_pomeranz](https://twitter.com/hal_pomeranz)

TUESDAY, JULY 7

7:00am	Registration	
8:00am	Welcome to the 2015 Digital Forensics and Incident Response (DFIR) Summit Rob Lee, David Cowen, and Alissa Torres, Summit Co-Chairs	
8:10am	DFIR Opening Keynote James Dunn, Director – Global Investigative and Forensic Services, Sony Pictures Entertainment	
	TRACK I	TRACK 2
9:10am	Ubiquity Forensics - Your iCloud and You Sarah Edwards, Test Engineer, Parsons Corporation	Windows 8 SRUM Forensics Yogesh Khatri, Assistant Professor, Champlain College
10:10am	Networking Break <i>in the Solutions Showcase</i>	
10:30am	Finding the Needle in the Haystack: Triggering Cyber Breach Incident Response by Spotting Even the Most Sophisticated Attacks MODERATOR: Alissa Torres, Certified Instructor, SANS Institute PANELISTS: James Carder, Director of Security Informatics, Mayo Clinic Dr. Sameer Bhalotra, The White House Chris Petersen, Chief Technology Officer, LogRhythm	Bring Your Own Device (BYOD) is Here to Stay: Audit Formulation, Suggestions, and Consequences Josh Chin, Executive Director, Net Force Warren Kruse, Vice President, Altep Inc. Heather Mahalik, Forensics Lead and PM, Oceans Edge, Inc., and SANS Certified Instructor, Author, Course Lead
11:30am	Threat Analysis of Complex Attacks Dmitry Bestuzhev, Head of the Global Research and Analysis Team, Latin America, Kaspersky Lab	Digital Forensics: The Human Cost Lee Whitfield, Director of Forensics, Digital Discovery
	TRACK I	TRACK 2
12:30pm	Lunch & Learn Presented by 	Lunch & Learn To be named
1:45pm	There's Something About WMI Devon Kerr, Senior Consultant, Mandiant, A FireEye Company	Determining Files and Folders Accessed in OS X Sara Newcomer, Computer Forensic Examiner, Lockheed Martin
2:45pm	Solution Provider Sessions	
3:45pm	Networking Break <i>in the Solutions Showcase</i>	
4:05pm	Hardware Keylogger Case Study Steve Gibson, Director, KPMG David Nides, Director, KPMG	Towards Forensicator Pro (Bringing a DevOps Mindset to DFIR to Produce an Assistive Toolchain - CADFIR) Barry Anderson, Security Architect, Cisco Systems
5:00pm	Forensic Artifacts for Cloud-Based Note Applications Mark Hallman, Principal, Digital Discovery	MIG - Mozilla's Distributed Platform for Real-Time Forensics of Endpoints Julien Vehent, Senior Operations Security Engineer, Mozilla
6:00pm	Forensic 4cast Awards Lee Whitfield, Director of Forensics, Digital Discovery	

DFIR Night Out in Austin

Join fellow attendees and DFIR speakers for a night of networking.

WEDNESDAY, JULY 8

7:30am

Registration

	TRACK 1	TRACK 2
8:50am	Windows Phone 8 Forensic Artifacts & Case Study Cindy Murphy, Madison Police Department	Investigation and Intelligence Framework Alan Ho and Kelvin Wong, Valkyrie-X Security Research Group (VXRL)
9:45am	Networking Break <i>in the Solutions Showcase</i>	
10:15am	Crisis Communication for Incident Response Scott J. Roberts, Bad Guy Catcher, GitHub	Forensic Analysis of sUAS aka Drones David Kovar, Senior Manager, Ernst & Young's Advisory Center of Excellence
11:10am	Walk Softly and Carry 26 Trillion Sticks Andrew Hay, Research Lead, OpenDNS Inc.	NoSQL Forensics: What to Do with (No)ARTIFACTS Matt Bromiley, Senior Associate, KPMG
12:00pm	Lunch	
1:20pm	The DFIR Guardians of the Galaxy Rick Holland, Principal Analyst, Forrester Research	Customized Google Chrome Forensics with Python Ryan Benson, Digital Forensic Examiner, Stroz Friedberg
2:10pm	Power(Shelling) Through the Timelin Jon Turner, Security Service Engineer, Microsoft Corp.	This Isn't Your Father's Remediation Wendi Whitmore Rafferty, VP, CrowdStrike
3:00pm	Networking Break <i>in the Solutions Showcase</i>	
3:20pm	Plumbing the Depths: ShellBags Eric R. Zimmerman, Special Agent, FBI	In the Lair of the Beholder: Extrusion Detection in 2015 Kyle Maxwell, Senior Researcher, Verisign



DFIR SANS360

Frank McClain, Information Security Manager, DFIR Team Lead – Premelending

Lee Whitfield, Director of Forensics, Digital Discovery

John Lukach, Security Architect, Pinnacle Bank

Ron Dormido, Senior Security Consultant, Verizon

Matt Linton, Chaos Specialist, Google

Alissa Torres, Certified Instructor, SANS Institute

Rob Lee, Fellow, SANS Institute

David Cowen, Partner, G-C Partners LLC

Hal Pomeranz, Fellow, SANS Institute

Heather Mahalik, Forensics Lead & PM, Oceans Edge Inc.
 and SANS Certified Instructor, Author, Course Lead

Additional speakers to be announced

5:15pm

Conclusion

Rob Lee, David Cowen, and Alissa Torres – Summit Co-Chairs



MEET THE DFIR SUMMIT SPEAKERS



Barry Anderson

Security Architect, Cisco Systems
Barry has over 20 years of experience in IT Security, specializing in Firewalls and Internet Security and Internet Infrastructure. He has provided a wide range of information security, systems and network administration consulting services to the financial and telecommunications sectors of private industry. [@z3ndr4g0h](#)



Ryan Benson

Digital Forensic Examiner, Stroz Friedberg
Ryan previously worked at Mandiant, doing incident response and forensic investigations. In his free time he is the developer of an open source tool called Hindsight, a Google Chrome forensics tool written in Python. [@_RyanBenson](#)



Dmitry Bestuzhev

Head of the Global Research and Analysis Team for Latin America, Kaspersky Lab
With more than 15 years of experience in IT security, Dmitry specializes in the investigation and analysis of complex malware incidents, cyberespionage and APT campaigns, attacks on online banking, and advanced social engineering.



Sameer Bhalotra

Co-Founder & CEO, StackRox
Previously Dr. Bhalotra was at Google, following the acquisition of his first company, Imperium. Dr. Bhalotra has served at the White House, Senate Intelligence Committee, and Central Intelligence Agency, and received degrees from Harvard and Stanford Universities.



Matt Bromley

Senior Associate, KPMG
Matt is a senior associate in KPMG's Forensic Technology Services practice with more than 4 years of digital forensics/incident response, network security monitoring, and threat intelligence experience. He has a strong background in enterprise investigations, assist companies with tackling large data breaches, network intrusions, and insider threats. [@505Forensics](#)



James Carder

Director of Security Informatics, Mayo Clinic
James is the enterprise leader of incident response, threat intelligence, vulnerability management, and penetration testing. Prior to Mayo Clinic, James was a Senior Manager at MANDIANT where he led incident response engagements for the Fortune 500. [@carderjames](#)



Sarah Edwards

Test Engineer, Parsons Corporation
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 counter-intelligence, counter-narcotic, and counter-terrorism. Sarah is also the author of the new SANS FOR518: Mac Forensic Analysis Course. [@jamevtwin](#)



Steve Gibson

Director, KPMG
Steve is a former US Marine infantry sergeant and a former police officer with the Austin Police High Tech Crime Unit. Having worked in DFIR since 1998, a programmer and Linux advocate, Steve currently supports the Forensic Technology practice with custom software and solutions.



Mark Hallman

Principal, Digital Discovery
Mark is the Chief Operating Officer (COO), Vice President and Principal for Digital Discovery. Mark has experience in digital forensics, e-Discovery and as a neutral third party expert with over twenty years of technology experience. Mark has provided expert testimony on both state and federal court.



Andrew Hay

Director of Security, OpenDNS
Andrew is the Director of Research at OpenDNS where he leads the research efforts for the company. [@andrewsmhay](#)



Alan Ho

Valkyrie-X Security Research Group (VXRL)
Alan has experience in development, penetration test, incident response and investigation.



Rick Holland

Principal Analyst, Forrester
Rick works with information security leadership providing strategic guidance on security architecture, operations and data privacy. His research focuses on incident response, threat intelligence, and vulnerability management. Rick likes BBQ [@rickhholland](#)



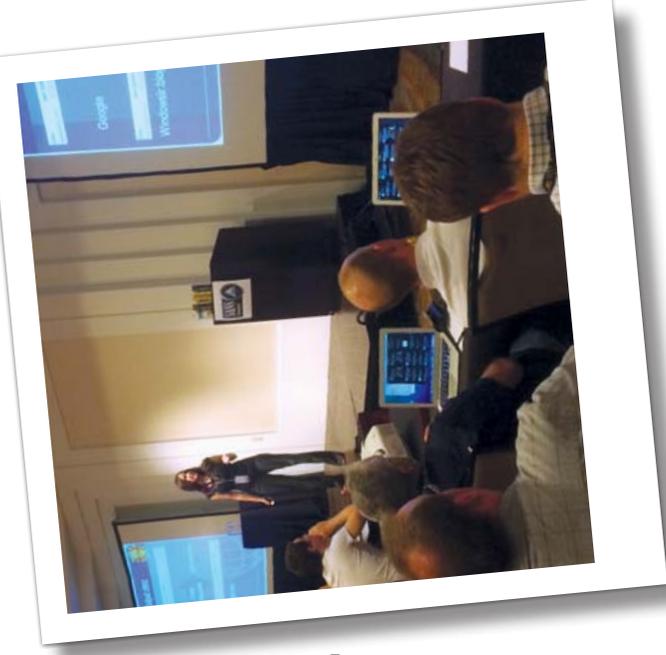
Devon A. Kerr

Principal Consultant, MANDIANT, a FireEye Company
Devon is an enterprise incident response (IR) and remediation lead, and has supported investigations by providing host, network, and log analysis. Mr. Kerr developed and maintains Mandiant methodologies and documentation for the Compromise Assessment service, OpenIOC utilization, and hunting with the FireEye Threat Analytics Platform (TAP). [@_devonkerr_](#)



Yogesh Khatri

Assistant Professor, Champlain College
Yogesh has 10 years of experience practicing Digital Forensics, Incident Response and eDiscovery in North America and Asia. Currently a professor at Champlain College, he has consulted with and trained corporates in many of the Fortune 100 companies, and law enforcement officers on computer forensics, automation of forensic processes, incident response and malware analysis.



Joshua Chin

Executive Director, Net Force
Joshua Chin is a Founding Partner at Net Force. Mr. Chin has a Bachelor of Science in Business Administration: Computer Information Systems from Cal-Poly Pomona and a Master of Science in Business Administration Candidate. He is currently an active member in ISACA and HTCIA.



David Cowen

Partner, G-C Partners
David is the award winning blog author of the Hacking Exposed Computer Forensics blog, the author of *Hacking Exposed: Computer Forensics* (1st, 2nd and upcoming 3rd editions), *Infocsec Pro Guide to Computer Forensics*, and the *Anti Hacker Toolkit* 3rd edition with over 15 years of digital forensic experience. [@HECFBlog](#)



Ron Dormido

Senior Security Consultant, Verizon
Ron is a Senior Security Consultant with the Verizon RISK Team and has over 28 years' experience in investigations and information security. Throughout his career, Ron has worked a number of high-profile data breach investigations, both in the private and government sectors. [@rdormi](#)



James Dunn

Director – Global Investigative and Forensic Services, Sony Pictures Entertainment
For the past year, James Dunn has been the Director of Digital Forensics for Sony Pictures Entertainment. Previously, while working as a consultant, he has worked on numerous high profile investigations involving cyber incident response, FCPA, and large-scale financial fraud. At Sony, James is primarily responsible for conducting investigations in support of network security incidents, fraud inquiries, and other internal issues. [@jamdunnDFW](#)

MEET THE DFIR SUMMIT SPEAKERS (CONTINUED)



John Lukach
Security Architect, Pinnacle Bank
John has nine years of experience focused on digital forensics, litigation support and incident response. His masters is in Network Administration and Security from Dakota State University, SD and bachelors in Computer Information Systems from Valley City State University, ND. John holds the GIAC Certified Forensic Analyst (GCFA) certification. @JohnLukach



Heather Mahalik
Project Manager, Ocean's Edge
Heather's extensive experience in digital forensics began in 2003. She is currently a certified instructor for the SANS Institute and is the course lead for FOR585: Advanced Smartphone Forensics. She is the co-author of Practical Mobile Forensics, currently a best seller from Packt Publishing and technical editor for Learning Android Forensics from Packt Publishing. @HeatherMahalik



Kyle Maxwell
Senior Researcher, Verisign
Kyle is a threat intelligence analyst and malware researcher who has led internal and external incident response teams at multiple organizations. He frequently speaks at conferences around the United States and Latin America. Mr. Maxwell holds a degree in Mathematics from the University of Texas at Dallas. @kylemaxwell



David Kovar
Senior Manager, Ernst & Young
David is a Sr. Manager in Ernst & Young's Advisory Center of Excellence developing and offering operational services in the digital forensics and incident response space. He's also been an entrepreneur, ediscovery consultant, software engineer, search and rescue incident command, executive protection agent, and lethal forensicator. He's collected images in China, rescued wayward Americans in Australia, and fenced with APT actors from all over the world. @dckovar



David Nides
Director, Forensics Technology Practice, KPMG
Currently David is in a national leadership role overseeing innovation and delivery of KPMG's Cyber Investigations services (e.g. network intrusions, POS malware, SCADA). He has worked on countless matters involving insider threats, hacktivist groups and state sponsored adversaries. Additionally he has testified in state court and has experience working in matters as a court appointed neutral. @DAWNADS



Hal Pomeranz
Fellow, SANS Institute
Hal is an independent digital forensic investigator who has consulted on cases ranging from intellectual property theft, to employee sabotage, to organized cybercrime and malicious software infrastructures. He has worked with law enforcement agencies in the US and Europe and global corporations. Hal is a respected author and speaker at industry gatherings worldwide. @hal_pomeranz



Wendi Whitmore Rafferty
Vice President, CrowdStrike Services
Wendi has over 12 years of experience in the computer security industry. As the Vice President of Services for CrowdStrike, Wendi is responsible for all professional services offered by the company. Along with her team, Wendi responds to critical security breaches and provides customers with solutions to complex adversary problems.



Warren G. Kruse II, CISSP, CFE, ENCE, DFCP
Vice President of Data Forensics, Altep, Inc.
Warren has spent the last twenty-five years between law enforcement and as a consultant supporting various agencies with incident response, computer forensics and eDiscovery. Mr. Kruse is President of the Digital Forensics Certification Board (www.DFCB.org), started from a grant by the NIJ and a project of the National Center for Forensic Science, it is now part of the International Association of Financial Crimes Investigators (AFCI). @warren_kruse



Rob Lee
Fellow, SANS Institute
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. @robtee | @SANSForensics



Robert M. Lee
Co-Founder, Dragos Security LLC
Robert gained his start in security in the U.S. Air Force and Intelligence Community and is currently the SANS course author for CS515: Active Defense and Incident Response and Co-Author for FOR578: Cyber Threat Intelligence. @RobertMLee



Matt Linton
Chaos Specialist, Google
Matt is an incident responder with experience throughout the security process, from architecture through penetration. He is formally trained in disaster management and specializes in rapid response, remediation and hardening of compromised environments.



Scott J. Roberts
Bad Guy Catcher, GitHub
Scott J. Roberts makes up his title every time he's asked, so we'll say he's the Director of Bad Guy Catching. He has worked for 900lbs security gorillas, government security giants & boutiques, and financial services security firms and done his best to track down bad guys at all these places. He's released and contributed to multiple tools for threat intelligence and malware analysis.



Cindy Murphy
Detective, Madison Police Department
Detective Cindy Murphy has been a Law Enforcement Officer since 1985 and is a certified forensic examiner who has been involved in computer forensics since 1999. She has directly participated in the examination of 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. @CindyMurph



Sara Newcomer
Computer Forensic Examiner, Lockheed Martin
Sara Newcomer is currently assigned to Defense Computer Forensics Laboratory (DCFL). Her professional background includes seven years as a member of the Defense Cyber Investigations Training Academy (DCITA) staff, as a forensic track instructor and deputy lead technical engineer. Ms. Newcomer also performed incident response and computer forensics at the Centers for Medicare and Medicaid.





Alissa Torres

Certified Instructor, SANS Institute
Alissa 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 an internal security team as a digital forensic investigator. @sibertor



Lee Whitfield

Director of Forensics, Digital Discovery
Lee has several years' experience conducting digital forensic investigations for a variety of cases including child abuse, murder, burglary, drug trafficking, and so on. Lee also has experience as a testifying expert for prosecution, defense, and private clients. @lee_whitfield



Jon Turner

Security Service Engineer, Microsoft Corp.
Jon got his start in security by taking over firewall configuration for a small third-party payroll processing firm, and over the next five years built a comprehensive security program that was the first in the industry to achieve ISO-27001 certification. He currently acts as a subject-matter expert in digital forensics and incident response for Microsoft's Office365 products. @z4ns4su



Julien Vehent

Senior Operations Security Engineer, Mozilla
Julien designs and builds defense systems in the Operations Security team at Mozilla. His background is in risk management, Linux engineering and large web service architecture. At Mozilla, he leads the MIG project, but also performs security reviews and incident response on the infrastructure that serves millions of Firefox users. @jvehent



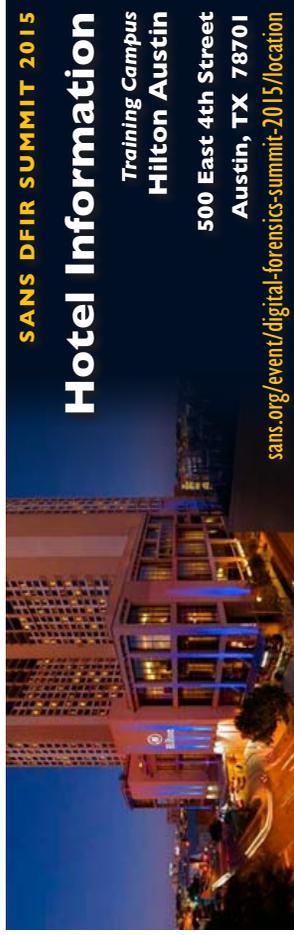
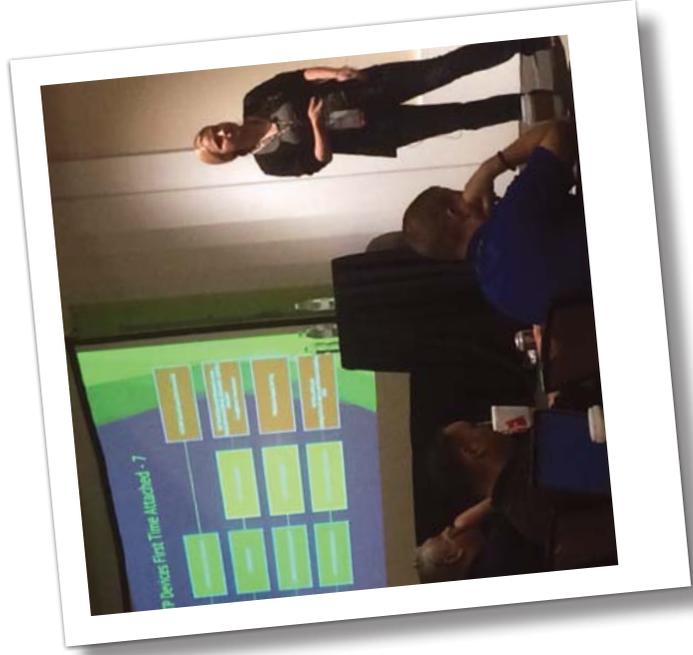
Kelvin Wong

Valkyrie-X Security Research Group (VXRL)
Kelvin (a.k.a. Forensics Ninja) works in a Law Enforcement Agency in HK and has over ten years experience in computer forensics and investigation. He has delivered workshop at DFRWS EU and HTCIA (APAC); presented research studies at DefCON, ATOkyo, HITCON, ICCCF, CeCOS(APWG) & HTCIA (APAC) and published research papers at Digital Forensics Magazine and Hakin9 IT Security Magazine.



Eric Zimmerman

Special Agent, FBI
Eric is an FBI special agent assigned to the Salt Lake City FBI field office since 2007. He is a member of the Utah ICAC and has provided training and assistance to dozens of local, state, federal and international law enforcement agencies.



SANS DFIR SUMMIT 2015

Hotel Information

Training Campus
Hilton Austin

500 East 4th Street
Austin, TX 78701

sans.org/event/digital-forensics-summit-2015/location

The Hilton Austin hotel, situated in downtown Austin adjacent to the Convention Center is surrounded by the city's most vibrant shopping, dining and entertainment scene. The famous 6th Street Entertainment District, Warehouse District, and 2nd Street District are all within walking distance of this downtown Austin hotel.

Special Hotel Rates Available

A special discounted rate of \$189.00 S/D will be honored based on space availability.

Government per diem rooms are available with proper ID; please call reservations and ask for the SANS government rate or online under government rate.

These rates include high-speed Internet in your room and are only available through June 12th. Please contact the hotel directly for availability at (800) 236-1592 or (512) 482-8000 and ask for the SANS Institute 2015 Block or use the group code, **SANS**.

To book online use the following link: resweb.passkey.com/go/SANSInstitute2015

The event hotel historically sells out several weeks prior to the event – so book early!

SANS DFIR SUMMIT 2015

Registration Information

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

Register online at sans.org/dfirsummit

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



SAVE \$400 on any course by paying before May 20th
SAVE \$500 when combining any course with the Summit

Pay Early and Save

Register and pay before	DATE	DISCOUNT	DATE	DISCOUNT
	5/20/15	\$400.00	6/3/15	\$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.

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 June 17, 2015 – processing fees may apply.



SANS DFIR 2015

“Highly focused content plus excellent face-to-networking opportunities is a win!”

-PAUL BOBBY, LOCKHEED MARTIN

“This is truly a wonderful event, with great content, people and just the right amount of crazy. :)”

-FRANK MCCAIN, PRIME LENDING

“A good place to see the new techniques and solutions people are coming up with.”

-JONATHAN TOMOZAK, TZ WORKS



Follow [@sansforensics](https://twitter.com/sansforensics) and join the conversation [#DFIRSummit](https://twitter.com/DFIRSummit) to hear the latest news.



5705 Salem Run Blvd.
Suite 105
Fredericksburg, VA 22407

**Register by May 20th with code DFIRUSB
to receive a free DFIR 64 USB Key.**

sans.org/dfirsummit