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.

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 Garcia, 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

“This is a meeting of the greatest minds in DFIR. I was so impressed with the supportive community and feel I have made long-lasting friends plus fellow security partners.”
- Pete Hainlen, Mayo Clinic

“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

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

FOR408

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, UNLV

- 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
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.

FOR 508
Advanced Incident Response
Instructor: Rob Lee @robtlee

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

sans.org/FOR508

FOR 526
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

sans.org/FOR526
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.

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.

For572

FOR572

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

Cyber Threat Intelligence

FOR578

FOR578

“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
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.

FOR610

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

SEC504

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
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.
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

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, and speaks at conferences around the world. @brycegalbraith

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. @roblee

Chad Tilbury

Chad Tilbury has been responding to computer intrusions and conducting forensic investigations since 1993. 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

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 an internal security team as a digital forensic investigator. She has extensive experience in information security, spanning government, academic, and corporate environments and holds a Bachelor's degree from the University of Virginia and a Masters from the University of Maryland in Information Technology. Alissa has taught as an instructor at the Defense Cyber Investigation Training Academy (DCITA), delivering incident response and network basics to security professionals entering the forensics community. @alissatorres

Hal Pomeranz

Hal Pomeranz is an independent digital forensic investigator who has consulted on cases ranging from intellectual property theft, 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 EXT4 file system forensics provided a basis for the development of Open Source forensic support for this file system. His EXT3 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

Mike Cloppert

Mike Cloppert is the lead analyst for Lockheed Martin CIRT's Intel Fusion team, charged with collecting and analyzing evidence 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

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 he engages with current and future customers of Red Canary’s managed threat detection service to ensure their use of the services 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

Hal Pomeranz

Hal Pomeranz is an independent digital forensic investigator who has consulted on cases ranging from intellectual property theft, 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 EXT4 file system forensics provided a basis for the development of Open Source forensic support for this file system. His EXT3 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

Mike Cloppert

Michael is the lead analyst for Lockheed Martin CIRT’s Intel Fusion team, charged with collecting and analyzing evidence 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
Welcome to the 2015 Digital Forensics and Incident Response (DFIR) Summit

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

**DFIR Opening Keynote**

James Dunn, Director – Global Investigative and Forensic Services, Sony Pictures Entertainment

**Networking Break**

in the Solutions Showcase

**Solution Provider Sessions**

Networking Break

in the Solutions Showcase

**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.

**TRACK 1**

9:00am - 10:10am

Ubiquity Forensics - Your iCloud and You

Sarah Edwards, Test Engineer, Parsons Corporation

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

Panels:

- James Dunn, Director of Security Informatics, Mayo Clinic
- Dr. Sameer Bhalotra, The White House
- Chris Petersen, Chief Technology Officer, LogRhythm

Threat Analysis of Complex Attacks

Dmitry Bestuzhev, Head of the Global Research and Analysis Team, Latin America, Kaspersky Lab

**TRACK 2**

10:30am - 11:30am

Windows 8 SRUM Forensics

Yogesh Khatri, Assistant Professor, Champlain College

**TRACK 1**

11:30am - 12:30pm

There’s Something About WMI

Devon Kerr, Senior Consultant, Mandiant, A FireEye Company

**TRACK 2**

12:30pm - 1:30pm

Determining Files and Folders Accessed in OS X

Sara Newcomer, Computer Forensic Examiner, Lockheed Martin

**TRACK 1**

1:45pm - 2:45pm

There’s Something About WMI: Determining Files and Folders Accessed in OS X

Devon Kerr, Senior Consultant, Mandiant, A FireEye Company

**TRACK 2**

2:45pm - 3:45pm

Market Stats and Forensics: A Brief Look at the Future

Lee Whitfield, Director of Forensics, Digital Discovery

**TRACK 1**

3:45pm - 4:05pm

Hardware Keylogger Case Study

Steve Gibson, Director, KPMG

David Nides, Director, KPMG

**TRACK 2**

4:05pm - 5:00pm

Forensic Artifacts for Cloud-Based Note Applications

Mark Hallman, Principal, Digital Discovery

Julien Vehent, Senior Operations Security Engineer, Mozilla

**TRACK 1**

5:00pm - 6:00pm

Towards Forensicator Pro (Bringing a DevOps Mindset to DFIR to Produce an Assistive Toolchain - CADFIR)

Barry Anderson, Security Architect, Cisco Systems

**TRACK 2**

6:00pm - 7:00pm

Forensic Night Out in Austin

Lee Whitfield, Director of Forensics, Digital Discovery
# DFIR SUMMIT AGENDA

**WEDNESDAY, JULY 8**

<table>
<thead>
<tr>
<th>Time</th>
<th>Track 1</th>
<th>Track 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>7:30am</td>
<td>Registration</td>
<td></td>
</tr>
<tr>
<td>8:50am</td>
<td><strong>Windows Phone 8 Forensic Artifacts &amp; Case Study</strong></td>
<td><strong>Investigation and Intelligence Framework</strong></td>
</tr>
<tr>
<td></td>
<td><em>Cindy Murphy</em>, Madison Police Department</td>
<td><em>Alan Ho and Kelvin Wong</em>, Valkyrie-X Security Research Group (VXRL)</td>
</tr>
<tr>
<td>9:45am</td>
<td><strong>Networking Break</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><em>in the Solutions Showcase</em></td>
<td></td>
</tr>
<tr>
<td>10:15am</td>
<td><strong>Crisis Communication for Incident Response</strong></td>
<td><strong>Forensic Analysis of sUAS aka Drones</strong></td>
</tr>
<tr>
<td></td>
<td><em>Scott J. Roberts</em>, Bad Guy Catcher, GitHub</td>
<td><em>David Kovar</em>, Senior Manager, Ernst &amp; Young’s Advisory Center of Excellence</td>
</tr>
<tr>
<td>11:10am</td>
<td><strong>Walk Softly and Carry 26 Trillion Sticks</strong></td>
<td><strong>NoSQL Forensics: What to Do with (No)ARTIFACTS</strong></td>
</tr>
<tr>
<td></td>
<td><em>Andrew Hay</em>, Research Lead, OpenDNS Inc.</td>
<td><em>Matt Bromiley</em>, Senior Associate, KPMG</td>
</tr>
<tr>
<td>12:00pm</td>
<td><strong>The DFIR Guardians of the Galaxy</strong></td>
<td><strong>Customized Google Chrome Forensics with Python</strong></td>
</tr>
<tr>
<td></td>
<td><em>Rick Holland</em>, Principal Analyst, Forrester Research</td>
<td><em>Ryan Benson</em>, Digital Forensic Examiner, Stroz Friedberg</td>
</tr>
<tr>
<td>2:10pm</td>
<td><strong>Power(Shelling) Through the Timelin</strong></td>
<td><strong>This Isn’t Your Father’s Remediation</strong></td>
</tr>
<tr>
<td></td>
<td><em>Jon Turner</em>, Security Service Engineer, Microsoft Corp.</td>
<td><em>Wendi Whitmore Rafferty</em>, VP, CrowdStrike</td>
</tr>
<tr>
<td>3:00pm</td>
<td><strong>Networking Break</strong></td>
<td><em>In the Lair of the Beholder: Extrusion Detection in 2015</em></td>
</tr>
<tr>
<td></td>
<td><em>in the Solutions Showcase</em></td>
<td><em>Kyle Maxwell</em>, Senior Researcher, Verisign</td>
</tr>
<tr>
<td>3:20pm</td>
<td><strong>Plumbing the Depths: ShellBags</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><em>Eric R. Zimmerman</em>, Special Agent, FBI</td>
<td></td>
</tr>
<tr>
<td>4:15pm</td>
<td><strong>DFIR SANS360</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><em>Frank McClain</em>, Information Security Manager, DFIR Team Lead – PrimeLending</td>
<td></td>
</tr>
<tr>
<td></td>
<td><em>Lee Whitfield</em>, Director of Forensics, Digital Discovery</td>
<td></td>
</tr>
<tr>
<td></td>
<td><em>John Lukach</em>, Security Architect, Pinnacle Bank</td>
<td></td>
</tr>
<tr>
<td></td>
<td><em>Ron Dormido</em>, Senior Security Consultant, Verizon</td>
<td></td>
</tr>
<tr>
<td></td>
<td><em>Matt Linton</em>, Chaos Specialist, Google</td>
<td></td>
</tr>
<tr>
<td></td>
<td><em>Alissa Torres</em>, Certified Instructor, SANS Institute</td>
<td></td>
</tr>
<tr>
<td></td>
<td><em>Rob Lee</em>, Fellow, SANS Institute</td>
<td></td>
</tr>
<tr>
<td></td>
<td><em>David Cowen</em>, Partner, G-C Partners LLC</td>
<td></td>
</tr>
<tr>
<td></td>
<td><em>Hal Pomeranz</em>, Fellow, SANS Institute</td>
<td></td>
</tr>
<tr>
<td></td>
<td><em>Heather Mahalik</em>, Forensics Lead &amp; PM, Oceans Edge Inc. and SANS Certified Instructor, Author, Course Lead</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Additional speakers to be announced</td>
<td></td>
</tr>
<tr>
<td>5:15pm</td>
<td><strong>Conclusion</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><em>Rob Lee, David Cowen, and Alissa Torres</em> – Summit Co-Chairs*</td>
<td><strong>DFIR SANS360</strong></td>
</tr>
</tbody>
</table>
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. @zndragn

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. @iamevltwin

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 API campaigns, attacks on online banking, and advanced social engineering.

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.

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.

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 HYGA.

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.

Andrew Hay
Director of Security, OpenDNS
Andrew is the Director of Research at OpenDNS where he leads the research efforts for the company. @andrewsmhay

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. @SO5Forensics

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), Infotecs Pro Guide to Computer Forensics, and the Anti Hacker Toolkit 3rd edition with over 15 years of digital forensic experience. @HECBlog

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 API campaigns, attacks on online banking, and advanced social engineering.

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.

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

Yogesh Khatri
Assistant Professor, Champlain College
Yogesh has 10 years of experience in 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.

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. @rickholland

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_
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 (GCF) 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 Pack’t Publishing and technical editor for Learning Android Forensics from Pack’t 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 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. @DAVND5

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.

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.

Warren G. Kruse II, CISSP, CFE, EnCE, DFEC
Vice President of Data Forensics, Alep, 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 (IAFCI). @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. @roblee | @SANSforensics

Frank McClain
Information Security Manager, DFIR Team Lead, Primelending
Frank is an accomplished cyber investigator and information assurance practitioner who manages the information security operations team for a national financial services firm where he has developed and leads their internal practices for incident response, digital forensics, malware remediation, threat analysis, eDiscovery, and security awareness. @littlemac042

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 the 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.

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 ICS515: Active Defense and Incident Response and Co-Author for FOR578: Cyber Threat Intelligence. @RobertM_Lee

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.
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 or visit the following link:

resweb.passkey.com/go/SANSInstitute2015

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!
san.org/dfirsummit

To receive a free DFIR 64 USB key, register by May 20th with code DFIRUSB.

Follow @sansforensics and join the conversation #DFIRSummit to hear the latest news.

To be removed from future mailings, please contact unsubscribe@sans.org or (301) 654-SANS (7267). Please include name and complete address.