
DFIR
SANS DFIR
DIGITAL FORENSICS & INCIDENT RESPONSE
SUMMIT & TRAINING
JUNE 23-30 | AUSTIN, TEXAS

TRAINING COURSES:

FOR408
Windows Forensic Analysis
GCFE

FOR508
Advanced Digital Forensics and Incident Response GCFA

FOR518
Mac Forensic Analysis

FOR526
Memory Forensics In-Depth

FOR572
Advanced Network Forensics and Analysis GNFA

FOR578
Cyber Threat Intelligence

FOR585
Advanced Smartphone Forensics
GASF

FOR610
REM: Malware Analysis Tools and Techniques GREM

MGT535
Incident Response Team Management

Here's a Small Sampling of the 30+ DFIR Summit Talks...

To Automate or Not To Automate; That Is the Incident Response Question

We all know that the number of security incidents is increasing at alarming rates and automation is often brought up as a critical part of the solution. Automation promises faster and consistent responses, but are the responses better? Does automation solve all incident response problems?

In this talk, we address these questions (spoiler alert: sometimes automation is great and sometimes it isn't). We'll talk about the phases of incident response, what can and should be automated, and the associated risks. We'll also talk about the kinds of tools needed to automate those phases.

This talk will, hopefully, be interactive. We'll be looking to the audience to share their positive and negative experiences with automation during their responses. Come to this talk to learn about automating your response and to share your automation experiences.

Dr. Brian Carrier *@carrier4n6, VP – Digital Forensics, Basis Technology*

Leveraging Cyber Threat Intelligence in an Active Cyber Defense

Two useful disciplines are cyber threat intelligence and active cyber defense. However, there is confusion around both of these areas that leads to a perception of hype and cost instead of vital tools for defenders to use. In the case of threat intelligence, many security companies have offered a range of threat intelligence products and feeds but there is confusion in the community as a whole as to how to maximize the value out threat intelligence. With active defense, there has been an attempt to brand this strategy as a hack-back or otherwise offense based practice whereas the strategy for an active defense has existed long before the word 'cyber' and is focused around practices such as incident response. This presentation will examine the current state of cyber threat intelligence and active cyber defense as well as provide strategies for leveraging proven cyber intelligence models within active cyber defense operations.

Erick Mandt*, Analyst, Air Force Office of Special Investigations (AFOSI)*
Robert M. Lee *@robertmlee, Author & Instructor, SANS Institute*

Seeing Red: Improving Blue Teams with Red Teaming

Red teaming: maybe your company or organization is doing it and you'd like to compare notes, or maybe you've heard of it and want to know more. This talk will look at why an organization should consider adding red team engagements to their security program, when red teaming is a good fit, and when it's not.

Dave Hull *@davehull, Product Engineer, Tanium*

You Don't Know Jack About .bash_history

The .bash_history file tracks a user's command history and is an important artifact in Linux and Mac forensics. But many investigators don't understand the rules for how and when they are written and can make wrong investigative assumptions. Suspects may attempt anti-forensic techniques to corrupt or remove .bash_history content. In other words, "It's complicated."

Using both disk and memory based forensics, Hal Pomeranz will shine a little light on some of the darker corners of bash behavior.

What does "normal" look like? What artifacts besides the .bash_history itself can we use to achieve certainty about user behavior? How does a combination of disk and memory forensics help us when interpreting a user's command history?

Hal Pomeranz *@hal_pomeranz, Principal, Deer Run Associates*

DFIR SUMMIT EXPERT SPEAKERS

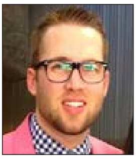
@robtlee
@sansforensics

Rob Lee
SANS Instititute, SANS Fellow, DFIR Summit Chair

@CCrowMontance

Chris Crowley
SANS Institute, Certified Instructor

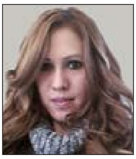
TALK TITLE:
Puzzle Solving and Science: The Secret Sauce of Innovation in Mobile Forensics



@jaredcatkinson

Jared Atkinson
Veris Group's Adaptive Threat Division, Hunt Capability Lead

TALK TITLE:
Start-Process PowerShell: Get-ForensicArtifact



@maridegrazia

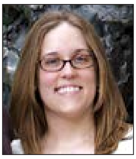
Mari DeGrazia
Verizon RISK Team, Senior Security Consultant

TALK TITLE:
Trust but Verify: Why, When and How

@williballenthin

William Ballenthin
FireEye Labs Advanced Reverse Engineering (FLARE) Team, Reverse Engineer

TALK TITLE:
FLOSS Every Day: Automatically Extracting Obfuscated Strings from Malware



@iamevltwin

Sarah Edwards
Parsons Corp., Mac Nerd

TALK TITLE:
The iOS of Sauron: How iOS Tracks Everything You Do

@ablaich

Andrew Blaich
Bluebox Security, Lead Security Analyst

TALK TITLE:
Hello Barbie Forensics

@KevvieFowler

Kevvie Fowler
KPMG Canada, National Leader, Cyber Response Services

TALK TITLE:
Hadoop Forensics

@505Forensics

Matt Bromiley
Mandiant, Senior Consultant

TALK TITLE:
All About That (Data)Base

@andrewsmhay

Andrew Hay
DataGravity, CISO

TALK TITLE:
Hello Barbie Forensics

@PDXbek

Rebekah Brown
Rapid7, Threat Intelligence Lead

TALK TITLE:
What Would You Say You Do Here?: Redefining the Role of Intelligence in Investigations

@ahoog42

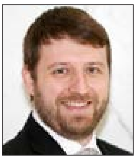
Andrew Hoog
NowSecure, CEO & Co-founder

TALK TITLE:
The Incident Response Playbook for Android and iOS

@carrier4n6

Brian Carrier
Basis Technology, VP Digital Forensics

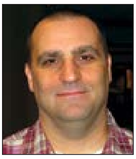
TALK TITLE:
To Automate or Not To Automate; That is the Incident Response Question



Jacob Christie
Mandiant, Consultant

TALK TITLE:
All About That (Data)Base

D F I R S U M M I T E X



@davehull

Dave Hull
Tanium, Product Engineer

TALK TITLE:
Seeing Red: Improving Blue Teams with Red Teaming

@dckovar

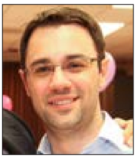
David Kovar
Independent Consultant

TALK TITLE:
UAV Forensic Analysis – Next Gen

@meansec

Ryan Kovar
Splunk Inc., Chief Security Strategist

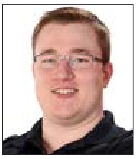
TALK TITLE:
stoQ'ing your Splunk



@mlaferrera

Marcus LaFerrera
PUNCH Cyber Analytics Group, Director of Development

TALK TITLE:
stoQ'ing your Splunk



@RobertMLee

Rob M. Lee
SANS Institute, Author & Instructor

TALK TITLE:
Leveraging Cyber Threat Intelligence in an Active Cyber Defense

@cheeky4n6Monkey

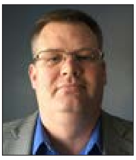
Adrien Leong
State Electronic Branch, New South Wales Police Force, Research and Development Specialist

TALK TITLE:
Puzzle Solving and Science: The Secret Sauce of Innovation in Mobile Forensics

@HeatherMahalik

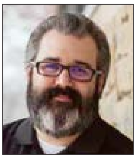
Heather Mahalik
Ocean's Edge/SANS Institute, Project Manager/Certified Instructor

TALK TITLE:
Puzzle Solving and Science: The Secret Sauce of Innovation in Mobile Forensics



Erick Mandt
Air Force Office of Special Investigations (AFOSI), Analyst

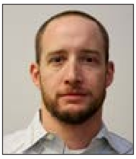
TALK TITLE:
Leveraging Cyber Threat Intelligence in an Active Cyber Defense



@kylemaxwell

Kyle Maxwell
Verisign iDefense, Senior Researcher

TALK TITLE:
Accurate Thinking: Analytic Pitfalls and How to Avoid Them



@kwm

Keith McCammon
Red Canary, Co-Founder & VP of Detection Operations

TALK TITLE:
Using Endpoint Telemetry to Accelerate the Baseline

@brianjmoran
@brimorlabs

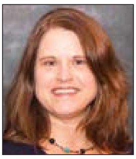
Brian Moran
BriMor Labs, Digital Strategy Consultant

TALK TITLE:
Who Watches the Smart Watches?

@austinjmurphy

Austin Murphy
CrowdStrike Services, Director of Incident Response

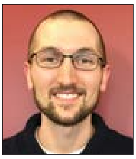
TALK TITLE:
What Does My SOC Do?: A Framework for Defining an InfoSec Ops Strategy



@CindyMurph

Cindy Murphy
Madison Police Department, Detective

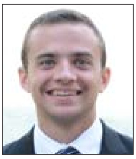
TALK TITLE:
Puzzle Solving and Science: The Secret Sauce of Innovation in Mobile Forensics



David Pany
Mandiant, A FireEye Company, Consultant

TALK TITLE:
Deleted Evidence: Fill in the Map to Luke Skywalker

@DavidPany



Kevin Perlow
Booz Allen Hamilton, Incident Responder and Forensic Analyst

TALK TITLE:
Tracking Threat Actors through YARA Rules and Virus Total

@KevinPerlow

Hal Pomeranz
Deer Run Associates, Principal, SANS Faculty Fellow

TALK TITLE:
You Don't Know Jack About .bash_history

@hal_pomeranz

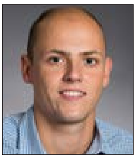
"This is truly a wonderful event, with great content, people and just the right amount of crazy. :)"

-Frank McClain, Prime Lending

Kevin Thompson
Heroku, Senior Incident Responder & Chief Snarkitecht

TALK TITLE:
Incident Detection & Hunting @ Scale: An Introduction to osquery

@bfist



Moritz Raabe
FireEye Labs Advanced Reverse Engineering (FLARE) Team, Reverse Engineer

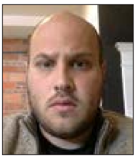
TALK TITLE:
FLOSS Every Day: Automatically Extracting Obfuscated Strings from Malware

@m_r_tz

James Treinen
ProtectWise, Inc, VP of Security Research

TALK TITLE:
Expanding The Hunt: A Case Study in Pivoting Using Passive DNS and Full PCAP

@jamestr



Scott Roberts
GitHub, Bad Guy Catcher

TALK TITLE:
Incident Detection & Hunting @ Scale: An Introduction to osquery

@sroberts

Paul Vixie
Farsight Security, Inc., CEO

TALK TITLE:
Expanding The Hunt: A Case Study in Pivoting Using Passive DNS and Full PCAP

@PaulVixie

Mary Singh
Mandiant, A FireEye Company, Senior Consultant

TALK TITLE:
Deleted Evidence: Fill in the Map to Luke Skywalker

@marycheese

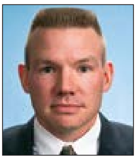
Lee Whitfield
Digital Discovery, Director of Forensics

TALK TITLE:
Forensic 4cast Awards

@lee_whitfield

Allen Swackhamer
Booz Allen Hamilton, Incident Responder and Malware Analyst

TALK TITLE:
Tracking Threat Actors through YARA Rules and Virus Total



Eric Zimmerman
Kroll Cyber Security, Senior Director

TALK TITLE:
Plumbing the Depths: Windows Registry Internals

@EricRZimmerman

FOR408: **Windows Forensic Analysis**

Instructors:
Rob Lee @robtlee & @sansforensics; Carlos Cajigas

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 and use it in successful criminal prosecution, incident response, media exploitation or civil litigation.

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

giac.org

FOR508: **Advanced Incident Response**

Instructor:

Mike Pilkington @mikepilkington

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.

THE ADVANCED PERSISTENT THREAT IS IN YOUR NETWORK – 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

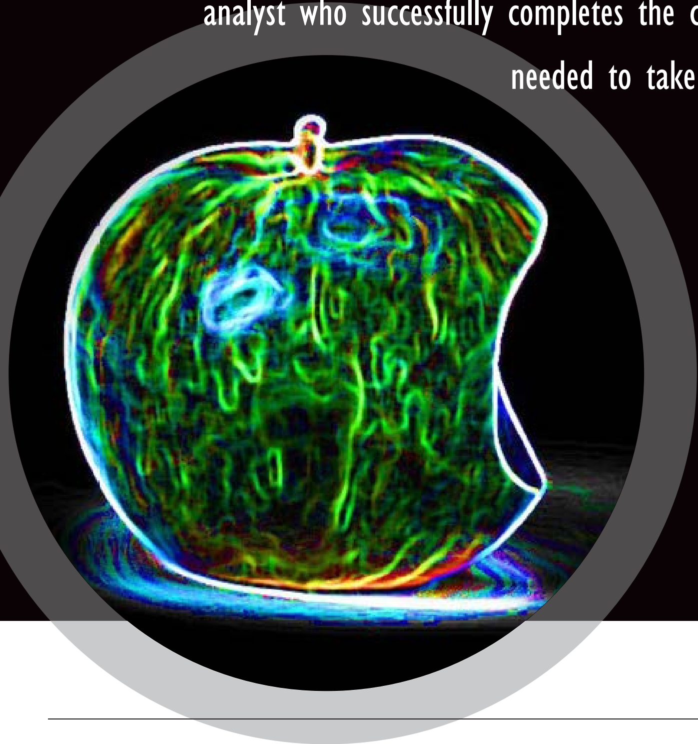
sans.org/FOR508

giac.org

FOR518: Mac Forensic Analysis

Instructor:
Sarah Edwards @iamevltwin

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.



FORENSICATE DIFFERENTLY!

"The most comprehensive Mac class I've taken."
-Daniel Mills, NASA

- Analyze and parse the Hierarchical File System (HFS+) file system by hand and 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 by using the system and user data files in correlation with system log files.
- Understand and analyze many Mac-specific technologies, including Time Machine, Spotlight, iCloud, Versions, FileVault, AirDrop, and FaceTime.

sans.org/FOR518

FOR526: Memory Forensics In-Depth

Instructor:
Alissa Torres @sibertor

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

MALWARE CAN HIDE, BUT IT MUST RUN

"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

FOR572: Advanced Network Forensics and Analysis

Instructor: Philip Hagen @PhilHagen

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.

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

GIAC NETWORK FORENSIC ANALYST GNFA

sans.org/FOR572

giac.org

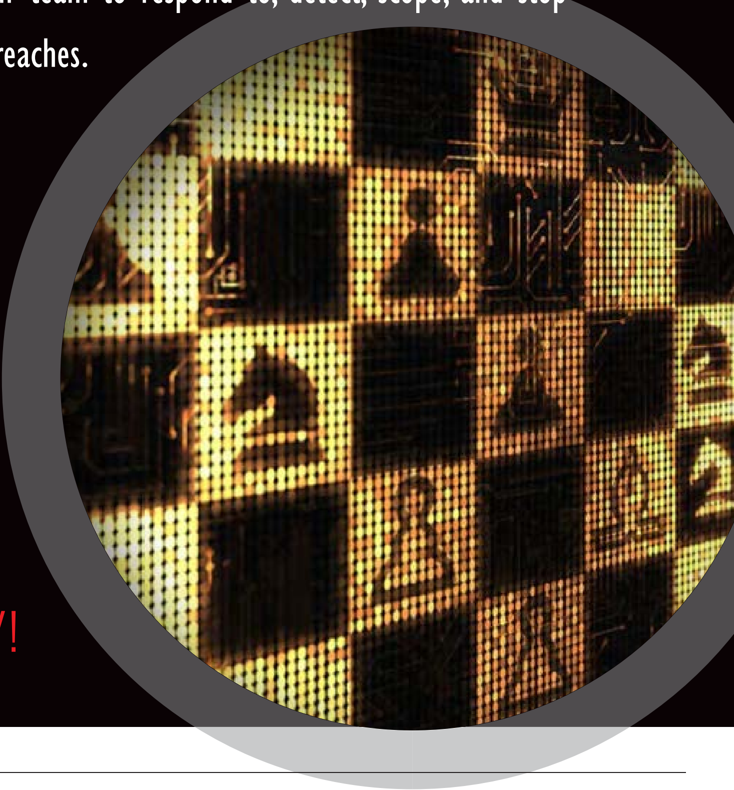
NEW

FOR578: Cyber Threat Intelligence

Instructor:

Robert M. Lee @RobertMLee

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 to, detect, scope, and stop intrusions and data breaches.



THERE IS NO TEACHER BUT THE ENEMY!

"What is threat intelligence? When am I ready for it? How do I use it? This class answers these questions and more at a critical point in the development of the field of threat intelligence in the wider community."

-ROBERT M. LEE, FOR578 CO-AUTHOR

- Determine the role of cyber threat intelligence in your job
- Know when 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 be more successful in defending against and responding to future intrusions
- Manage, share, and receive intelligence on APT actors

sans.org/FOR578

FOR585: **Advanced Smartphone Forensics**

Instructor:
Cindy Murphy @cindymurph

Mobile devices are often a key factor in criminal cases, intrusions, IP theft, security threats, and more. Understanding how to leverage the data from the device in a correct manner can make or break your case and your future as an expert. FOR585: Advanced Smartphone Forensics will teach you those skills.

SMARTPHONE DATA CAN'T HIDE FOREVER – IT'S TIME TO OUTSMART THE MOBILE DEVICE!

"FOR585 provides forensics with the mentality and set of tools required to forensically examine most types of devices."
-Steve Bone, MOD

- Select the most effective forensic tools, techniques, and procedures for critical analysis of smartphone data
- Reconstruct events surrounding a crime using information from smartphones, including timeline development and link analysis (e.g., who communicated with whom, where, and when)
- Understand how smartphone file systems store data, how they differ, and how the evidence will be stored on each device
- Interpret file systems on smartphones and locate information that is not generally accessible to users

sans.org/FOR585

giac.org

MGT535: Incident Response Team Management

Instructor: Christopher Crowley @CCrowMontance

This course discusses the often-neglected topic of managing an incident response team. Given the frequency and complexity of today's cyber attacks, incident response is a critical function for organizations. Incident response is the last line of defense.

YOU ARE THE TEAM CALLED UPON AT THE WORST TIME, BE PREPARED TO WIN THE BATTLE

"This course brings hands-on and very relevant information for everyone establishing or being part of an incident response team."
-GEIR LOSSIUS, SPAREBANKEN VEST

- Incident response – 6 steps
- Creating incident response requirements
- Developing incident handling capabilities
- Reporting, SLAs, cost of incidents
- Setting up operations
- Managing daily operations
- Navigating executive management

sans.org/MGT535

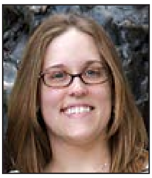
SANS DFIR INSTRUCTORS

Carlos Cajigas

As a retired detective, incident responder, cybercrimes investigator, and digital forensics trainer, Carlos has amassed a wealth of experience in high-technology crime investigations. Carlos holds Bachelor and Master Degrees from Palm Beach Atlantic University. He also holds various certifications in the digital forensics field.

Christopher Crowley

Christopher Crowley has 15 years of industry experience managing and securing networks. He currently works as an independent consultant in the Washington, DC area. Christopher is the course author for SANS MGT535: Incident Response Team Management, and holds several information security certifications. @CCrowMontance



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 cases, counter-intelligence, counter-narcotics, and counter-terrorism. She has a Bachelor of Science in Information Technology from Rochester Institute of Technology and a Master's in Information Assurance from Capitol College. @iamevltwin

Philip Hagen

Philip Hagen has been working in the information security field since 1998, running the full spectrum including deep technical tasks, management of an entire computer forensic services portfolio, and executive responsibilities. Phil started his security career while attending the U.S. Air Force Academy. He served in the Air Force as a communications officer at Beale AFB and the Pentagon. @PhilHagen

Rob Lee

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 graduated from the U.S. Air Force Academy and served in the USAF 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. @robtlee

Robert M. Lee

Robert obtained his start in cybersecurity serving as a Cyber Warfare Operations Officer in the U.S. Air Force. He is a SANS Certified Instructor, the course author of SANS ICS515: Active Defense and Incident Response, and the co-author of SANS FOR578: Cyber Threat Intelligence. @RobertMLee

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.

Mike Pilkington

Mike Pilkington is the technical incident response lead for a Fortune 500 company in the oil & gas industry. He currently teaches FOR408: Windows Forensic Analysis and FOR508: Advanced Digital Forensics and Incident Response. He holds a Bachelor of Science in Mechanical Engineering, as well as numerous IT security certifications. @mikepilkington

Anuj Soni

Anuj Soni is a Senior Incident Responder at Booz Allen Hamilton, where he leads forensic, malware, and network analysis efforts to investigate security incidents. He received his Bachelors and Masters degrees from Carnegie Mellon University and holds several information security certifications. @asoni

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 holds a Bachelors degree from University of Virginia and a Masters from University of Maryland in Information Technology. @sibertor

Are you one of the top

Digital Forensics & Incident Response Professionals?

2 Nights of DFIR NetWars at SANS DFIR SUMMIT 2016!

MON, JUNE 27 – TUE, JUNE 28 6:30-9:30 PM

Come and join us for this exciting event to test your skills in a challenging and fun learning environment. Registration for DFIR NetWars is **FREE OF CHARGE TO ALL STUDENTS AT SANS DFIR SUMMIT 2016**. External participants are welcome to join for an entry fee of $1,450.

SANS DFIR NetWars Tournament is an incident simulator packed with a vast amount of forensic and incident response challenges for individual or team-based "firefights." It is developed by incident responders and forensic analysts who use these skills daily to stop data breaches and solve complex crimes. DFIR NetWars Tournament allows each player to progress through multiple skill levels of increasing difficulty, learning first-hand how to solve key challenges they might experience during a serious incident. DFIR NetWars Tournament enables players to learn and sharpen new skills prior to being involved in a real incident.

sans.org/dfirsummit

Walking distance to:

- 6th Street Entertainment District
- Warehouse District
- 2nd Street District

SANS DFIR SUMMIT 2016

Hotel Information

Training Campus

Hilton Austin

500 East 4th Street
Austin, TX 78701

sans.org/event/digital-forensics-summit-2016/location

Special Hotel Rates Available

A special discounted rate of $199.00 S/D will be honored based on space availability until May 24, 2016.

A limited number of government per diem rate rooms are available with proper ID upon requesting the SANS per diem rate.

These rates include high-speed Internet in your room and are only available through May 24th. Please contact the hotel directly for availability at 1-800-236-1592 or 512-482-8000 and ask for the SANS Institute 2016 Block or use the group code, **SANS**.

To book online use the following link: **https://aws.passkey.com/g/54653385**

In the past, the event hotel has sold out several weeks prior to the event – so book early!

SANS DFIR SUMMIT 2016

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. 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.

Use code **EarlyBird16** when registering early

Pay Early and Save

	DATE	DISCOUNT	DATE	DISCOUNT
Pay & enter code before	**5-5-16**	**$400.00**	**5-24-16**	**$200.00**

Some restrictions apply.

Bundle and Save

SAVE $500 off **your Summit registration fee when purchased in conjunction with a full-priced 5-6 day course!** Does not qualify with EarlyBird discount

Group Savings (Applies to tuition only)

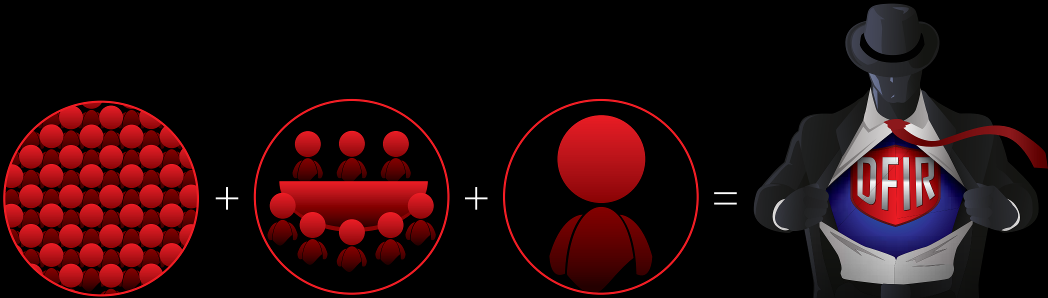
To obtain a group discount, complete the discount code request form at sans.org/security-training/discounts prior to registering.

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 May 31, 2016 – processing fees may apply.

SANS DFIR

DIGITAL FORENSICS & INCIDENT RESPONSE

Digital Forensics & Incident Response Summit



Over 30 Expert Talks + 9 Courses + You = DFIR Superhero in 8 Days

Austin, TX | June 23-30 | sans.org/dfirsummit