SANS DFIR 2015

SUMMIT

Program Guide

Summit Chairman: Rob Lee

Co-Chairs: Alissa Torres and David Cowen

 # DFIRsummit **@SANSForensics**

Agenda

All Summit sessions will be held in the Governor's Ballroom on the 4th floor (unless noted).

*Summit presentations will be posted via the following URL - **http://digital-forensics.sans.org/community/summits**.*
An email will be sent to all attendees once the slides are live on the website, typically about 5 business days after the event.

Portions of the Summit may be video-recorded. These videos may be used for marketing or other purposes, but will not be available for distribution or viewing on demand at this time.

Tuesday, July 7

7:00 - 8:00am

Registration & Coffee
Breakfast Pastries Provided
(LOCATION: GOVERNOR'S BALLROOM SALON D FOYER)

8:00-8:10am

Welcome to the 2015 Digital Forensics and Incident Response Summit

***Rob Lee**, **David Cowen** & **Alissa Torres**, Summit Co-Chairs*

8:10-9:10am

Beyond the Kill Chain: Lessons in Cyber Crisis Management

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

While popular in incident response and cyber security circles, the kill chain provides too narrow of a viewpoint on the lifecycle of a major intrusion. Namely…it fails to address what happens after an attacker strikes, accomplishes their objectives, and how to handle the ensuing fallout when the extent of the damage is finally uncovered.

By applying crisis management principles to the incident response lifecycle you can find yourself better prepared to identify the precursors that lead a company into an crisis. By understanding how the perceptions of internal and external stakeholders motivate the response process, you can position yourself to be successful when disaster strikes. By understanding the importance of organizational learning, you can adapt your policies and tactics to avert a crisis in the future.

This talk will tell the story of how two different companies chose to handle a cyber-breach from the perspective of their crisis management teams. The speaker will identify the precursors that lead to the eventual crisis, why it is sometimes important to be able to make decisions in a state of ambiguity, how to handle all the moving pieces, and how to prepare for the worst case scenario. ?

9:10-10:10am

(LOCATION: SALON D)

Ubiquity Forensics – Your iCloud and You

***Sarah Edwards**, Test Engineer, Parsons Corporation*

Ubiquity or "Everything, Everywhere" – Apple uses this term describe iCloud related items and its availability across all devices. iCloud enables us to have our data synced with every Mac, iPhone, iPad, PC as well as accessible with your handy web browser. You can access your email, documents, contacts, browsing history, notes, keychains, photos, and more all with just a click of the mouse or a tap of the finger - on any device, all synced within seconds.

Much of this data gets cached on your devices, this presentation will explore the forensic artifacts related to this cached data. Where is the data stored; how to look at it; how is it synced; and what other sensitive information can be found that you may not have known existed!

(LOCATION: SALON E)

Windows 8 SRUM Forensics

***Yogesh Khatri**, Assistant Professor, Champlain College*

Windows 8 has a newly added feature to track system resource usage, specifically process and network metrics over time. Process related information such as process owner, CPU cycles used, data bytes read/written, and network data (sent/received) are continuously recorded by a mechanism called System Resource Usage Monitor (SRUM). The talk explores how this information can be parsed out and utilized for forensic purposes and can be especially useful in incident response.

10:10-10:30am

Networking Break & Vendor Expo

(LOCATION: GOVERNOR'S BALLROOM SALON D FOYER)

10:30-11:30am

(LOCATION: SALON D)

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**, Former Director of Security Informatics, Mayo Clinic; CISO, LogRhythm*

***Dr. Sameer Bhalotra**, Former Director of Cybersecurity, The White House*

***Chris Petersen**, SVP Products, CTO & Co-Founder, LogRhythm*

You cannot respond to an incident unless you know it's happening. Within cybersecurity, detecting security breaches has become a seemingly insurmountable challenge. IT security firm Gartner estimates that eighty-five percent of breaches go completely undetected and ninety-two percent of the detected breaches are reported by third parties.

Cyber criminals are innovating at an accelerating pace and continuously shifting tactics in their execution of advanced attacks. They are utilizing malicious and hard to detect threats by bypassing traditional IT defenses, and their methods are so clever that finding the results of their work is impossible without knowing where to look.

The security industry has responded with new approaches that detect even the most hidden and advanced attacks. They target companies facing a new reality – it's not a question of whether a company will be breached, but rather when. This panel discussion will focus on the very latest approaches to discovering security breaches and triggering incident response. Panelists will discuss the importance of combining comprehensive threat intelligence with advanced security analytics to strengthen cyber defenses and reduce mean-time-to-detect (MTTD) and mean-time-to-respond (MTTR) to breaches and threats, and how exactly organizations can do this.

Panelists will also share real world examples of how they've used threat intelligence and analytics to identify and remedy some of today's most sophisticated cyber threats, which they would have otherwise been blind to.

(LOCATION: SALON E)

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*

Bring Your Own Device is commonly thought to be related to using your own mobile device in the workplace, however this is a false assumption. BYOD pertains to many digital devices, including tablets, laptops and computers. How the data is viewed, saved, and transmitted on these devices is commonly a concern for the employee and the company. If you or your organization participate in BYOD, does this mean your personal information is susceptible to employer review? As and employee, how can you ensure your personal data is safe? As a company, how can you ensure your data isn't compromised and what to do if it is. As an IT professional, what can you do to secure the data and the device. As an IT Auditor, what risks are associated with BYOD? We will cover all of these topics, questions and more during the BYOD: Audit panel discussion.

11:30am-12:30pm

(LOCATION: SALON D)

Threat Analysis of Complex Attacks

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

Despite appearance in-the-wild for the last ten years, targeted attacks only received special attention three years ago. These attacks are usually complex and specifically designed and should not be approached in the same manner one analyzes traditional malware like a banking trojan. There exists an advanced security researcher approach for the analysis of APTs and targeted attacks. This presentation will walk the audience through the essential elements of this advanced approach, ranging from attack attribution and technical indicators to the preparation of a presentable threat intelligence report capable of enhancing the customer's protection. This topic is essential in the evolution of security research and will help prepare practitioners for the oncoming trend of fractured attack groups responsible for the next onslaught of targeted attacks.

(LOCATION: SALON E)

Digital Forensics: The Human Cost

***Lee Whitfield**, Director of Forensics, Digital Discovery*

Do digital forensics professionals truly understand the power that they wield? A single line in a statement or a report can have significant impact on many lives. The results of our investigations can lead to termination of employment, marriage, or freedoms. Targets of our investigations could lose property, businesses, and families. In some instances our findings may lead to the target developing health problems or, in the most drastic of cases, taking their own lives.

We have the power to change lives with only a few words, either written or spoken.

Lee Whitfield will provide case studies showing how digital forensics professionals have gotten it wrong in the past, how those instances caused real-life problems and how you can avoid them in the future.

Further, how are we, as analysts, able to protect ourselves from the adverse effects of the work that we conduct? When many in the field are exposed to graphic material, how does this affect our own behavior? How can we best cope with what we see on a regular basis? This talk will share some interesting points and potential coping mechanisms.

12:30-1:45pm

LUNCH & LEARN

(LOCATION: MEETING ROOM 410)

Presented by

LogRhythm™

Applying Security Intelligence to Detect & Respond to Advanced Threats

***Luis Guzman**, Sales Engineer*

The Security Intelligence Maturity Model™ (SIMM™) provides a systematic guide for an organization to assess and actively achieve a heightened security posture. Today's reality indicates that organizations need to elevate the importance of cybersecurity. CEOs and boards need to be more directly involved in IT security and setting the level of acceptable risk. While CISOs must make a shift of processes and priorities toward detecting and responding to threats as quickly as possible. An agnostic view of where we need to be headed in security intelligence as the industry is shifting into detecting and responding as prevention has failed.

1:45-2:45pm

(LOCATION: SALON D)

There's Something About WMI

***Devon Kerr**, Senior Consultant, Mandiant, A FireEye Company*

This presentation will describe the purpose and components of Windows Management Instrumentation (WMI) from the incident response and forensics perspectives. Attendees will learn how targeted threats are using WMI during each phase of the compromise, case studies and examples, the artifacts generated by those activities, some of the tools used to interact with WMI, using WMI for persistent access that defeats antivirus and application whitelisting, and the benefits of enabling WMI trace logging for additional detection and improved analysis.

(LOCATION: SALON E)

Determining Files and Folders Accessed in OS X

***Sara Newcomer,** Computer Forensic Examiner, Lockheed Martin*

One important component of a digital forensic investigation can be determining what files and folders were accessed and which user account was used for this access. In the OS X operating system, entries are created in a database as users navigate through folders using Finder, the OS X equivalent of Windows Explorer. Using the database, an investigator can look for specific file names of interest, the contents of a directory of interest, the name of files that have been deleted, or files on external media. The information can be attributed a specific user account. The database tracks a user's Finder navigation activities, creating entries as folders are accessed including locally attached storage and network attached storage media. It is located in a hidden operating system directory not typically navigated to by users, inaccessible to non-admin accounts, and not part of the user's profile. Even after a user account is removed from the system this database can be used to provide insight about data accessed in Finder by deleted user accounts. Additional information in the database may also provide information about when the actions occurred, the number of times a folder was accessed, and if files were renamed or moved.

2:45-3:45pm

(LOCATION: SALON D)

Hardware Keylogger Case Study

***Steve Gibson**, Director, KPMG*
***David Nides**, Director, KPMG*

Hardware keyloggers were identified in a client environment. Upon analysis identified the mass storage volume associated with the hardware key logger data was not accessible due password protection at hardware level. Using a teensy (USB-based microcontroller development system) created a hardware based brute force device which was used to emulate a dictionary of keystrokes. Ultimately this device exposed the password for the keylogger allowing sufficient analysis. Upon analysis of the device was able to tie the keylogger back to a hostname and user name with unique and surprising artifacts. Demo of teensy will be provided.

(LOCATION: SALON E)

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

***Barry Anderson,** Security Architect, Cisco Systems*

Advancing the work done in the Forensicator FATE GCFA Gold Paper, this talk will briefly review the work done in that paper integrating Jenkins into the evidence processing chain before moving on to demonstrate how much evidence processing can be automated (for example, the processing of memory and disk images looking for Indicators of Compromise), moving the DFIR professional up the value chain. Also demonstrated will be a fully virtualised DFIR laboratory built in AWS with Cloud Formation scripts, i.e. a DFIR laboratory environment that can be spun up on a per-project basis, and auto-scaled based on workload.

3:45-4:05pm

Networking Break & Vendor Expo

(LOCATION: GOVERNOR'S BALLROOM SALON D FOYER)

4:05-5:00pm

(LOCATION: SALON D)

Think Again: Are We Doing it Wrong?

***Jordi Sanchez**, Red Mage, Google*

As companies trying to defend ourselves and our customers/users against pervasive attackers, are our methods effective? Is the information being shared useful?

Will passively waiting for signals to fire be enough? Or are you completely blind to their actions?

In this talk, Jordi will ponder on the state of affairs on incident response and computer compromises, covering the current defense and detection mechanisms, and present compelling arguments why we may be doing it all wrong. And what can we do about it.

Keywords: state-sponsored attacks, threat data exchange formats (IOCs), massive collection of data, remote incident response, memory forensics.

(LOCATION: SALON E)

MIG: Mozilla's Distributed Platform for Real-Time Forensics of Endpoints

***Julien Vehent**, Senior Operations Security Engineer, Mozilla*

MIG is a platform to perform investigative surgery on remote endpoints. It enables investigators to obtain information from large numbers of systems in parallel, thus accelerating investigation of incidents and day-to-day operations security, while preserving privacy and security

of the infrastructure. It's an army of Sherlock Holmes, ready to interrogate an infrastructure within seconds. This talk will introduce MIG, the problems it solves, its design goals and server-agent model, and how it is used at Mozilla. The audience will learn how Indicators of Compromise (IOCs) can be searched for across thousands of systems within seconds (MIG can query thousands of systems in about 10 seconds on average). During the talk, the audience will be given elements to install and operate MIG in their own environments.

5:00-5:30pm

Forensic 4cast Awards

***Lee Whitfield**, Director of Forensics, Digital Discovery*

Thank you for attending the SANS Summit.

Please remember to complete your evaluations for today.
You may leave completed surveys at your seat or turn them in to the SANS registration desk.

6:30pm

DFIR Night in Austin

Hosted by

Bit9 + CARBON BLACK

ARM YOUR ENDPOINTS.

At

Buffalo Billiards AUSTIN TEXAS

201 E 6th St | Austin, TX 78701

Join fellow attendees and Summit speakers for a night of networking and fun.

Wednesday, July 8

7:30-8:00am

Registration & Coffee
Breakfast Pastries Provided
(LOCATION: GOVERNOR'S BALLROOM SALON D FOYER)

8:00-8:50am

(LOCATION: SALON D)

Windows Phone 8 Forensic Artifacts and Case Study

***Cindy Murphy**, Madison Police Department*

Due to the quick progression of mobile device technology, a need often arises for forensic examination of mobile devices that are not yet supported for data extraction and parsing by commercially available mobile forensic tools. This is particularly the case with less commercially popular (and therefore less supported) mobile operating systems such as Windows Phone 8. This case study will present the challenges that practitioners face with Window Phone 8 devices, practical solutions to those challenges, collaborative strategies that work in a jam, and presents from the practitioners perspective, useful artifact locations from Windows Phone 8 devices.

In February of 2013, a home invasion and sexual assault occurred in the City of Madison, Wisconsin. The home invasion involved a conspiracy, planned by a drug addicted escort who solicited the assistance of her drug dealer in order to rob the man she was temporarily staying with, targeting significant amounts of cash he stored in his home from his tattoo business. Unfortunately, the five people carrying out the armed robbery plan forced entry into the wrong half of the targeted duplex. During the course of the home invasion, a woman who was six months pregnant was sexually assaulted repeatedly in front of her husband by several of the assailants. A Nokia Lumia 520 cell phone running Windows Phone 8 was used extensively during the planning, and aftermath of the robbery. Attend this session to learn how advanced mobile forensics techniques on unsupported devices can take a case from few leads to six convictions based upon the successful examination of a single unsupported phone.

(LOCATION: SALON E)

Investigation and Intelligence Framework

***Alan Ho** and **Kelvin Wong**,*
Valkyrie-X Security Research Group (VXRL)

Digital forensics investigators are facing new challenges every day because there are a large variety of high-tech cybercrimes reported. For instance APT, Hacking, Ransomware and DDOS etc. During the investigation, investigators are often too concentrated on the evidence itself, like reversing the malware for the detailed behaviors or analyzing packets for credential leakage, but seldom or having difficulties to draw out the whole picture of the incident by correlating the seized/acquired evidences for the intelligence purpose. All relevant data from seized media should be utilized and analyzed, later transformed to intelligence so as to build a profile of the potential suspect with the corresponding attributes.

Based on the principle of Zachman Framework, we propose and design an Investigation and Intelligence Framework, which is an automated mechanism to identify the potential suspect at the early stage for the ease of the further investigation, correlating evidence to oversee the entire picture of the cybercrime. Our framework has adopted four of the intersections, i.e. When, Where, Who and How. 4W of the incident should be the concerned factors no matter what type of cybercrimes happened. To fulfill this 4W concept, related artifacts including timeline, location, identity and attack path would be effectively recognized at the earlier phase, and investigators can tackle the cybercrimes more successfully. Analyzing the evidences with intelligence for example VirusTotal, PassiveTotal, PhishTank and MalProfile, the artifacts can be transformed into new pieces of intelligence and build the possible story of the incident/crime for further investigation.

A tool is developed to correlate the evidence (by integrating with Rekall Memory Forensics Framework[3], Pypcap library for pcap extraction, Python Registry and Exif library to extract useful artifacts). Together with intelligence sources, the tool will apply probability model and algorithms to correlate evidence. It will then return the confidence level, risk scores and possible attack path/incident type for the collected evidence and suggest which worth further investigation. This will provide a big picture of the cybercrime story and build a potential profile of the suspect so as to help investigation more effectively.

8:50-9:45am

(LOCATION: SALON D)

Crisis Communication for Incident Response

***Scott J. Roberts**, Bad Guy Catcher, GitHub*

One of the parts of intrusion response that rarely gets attention in DFIR circles, though huge attention outside them, is the customer facing victim companies' communication to their own customers. This is almost always the only real information the public gets of your intrusion and communicating what happened effectively is crucial to minimizing damage, both to customers and to your organizations reputation.

Using lessons pulled from professional public relations specialists combined practical experience in operations and security incident response we'll review the five keys to good crisis communications. We'll walk through multiple examples of good and bad crisis communications and develop an understanding of what information people need to know when and why they should get it from you and not the media. We'll also discuss building a comprehensive incident communications plan.

(LOCATION: SALON E)

Forensic Analysis of sUAS aka Drones

***David Kovar,** Senior Manager, Ernst & Young's Advisory Center of Excellence*

Small Unmanned Aerial Systems (sUAS) aka "drones" are all the rage – they are invading your privacy, they are delivering your packages (and illegal drugs), they are even landing on the White House lawn. Where have they been? Where are they going? Who launched them? Let's find out.

sUAS – emphasis on the final 'S' – are complex systems. The aerial platform alone often consists of a radio link, an autopilot, a photography sub-system, a GPS, and multiple other sensors. Each one of these components might contain a wealth of pieces to the answer to the above questions. Add in the ground control stations, the radio controller, and the video downlink system and you have a very complex computing environment running a variety of commercial, closed source, open source, and home brew software.

And yes, there is already malware specifically targeting drones.

During this presentation, we will walk through all of the components of a representative drone and discuss the forensic process and potential artifacts of each component, along with a presentation of the overall story told by the individual components.

9:45-10:15am

Networking Break & Vendor Expo

(LOCATION: GOVERNOR'S BALLROOM SALON D FOYER)

10:15-11:10am

(LOCATION: SALON D)

Walk Softly and Carry 26 Trillion Sticks

***Andrew Hay**, Research Lead, OpenDNS Inc.*

Malware research community has long spent their expertise in dissecting malware binaries, examining footprints on victims' systems. Instead of studying the diseases themselves, however, at OpenDNS we study the collective behavior of victims (patients) and the behavior of bad actors (diseases).

At OpenDNS Andrew has the privilege of using roughly 71 Billion DNS queries per day (~26 Trillion per year) with which to track bad guys, predict malware outbreaks, and determine opportunistic or campaign-specific botnet infrastructures. In this talk, Andrew will explore some of the key findings in 2014 based on this massive corpus of data. Visualization techniques for assigning attribution based on co-occurring domains and infrastructure will also be discussed.

(LOCATION: SALON E)

NoSQL Forensics: What to Do with (No)ARTIFACTS

***Matt Bromiley**, Senior Consultant, Mandiant*

MongoDB, Elasticsearch, and CouchDB. With the explosive growth of these solutions, it's only a matter of time before you run into them on your next engagement. Wouldn't you like to know what to do with them?

Using a combination of log analytics and an understanding of core functions of these databases, attendees will learn how to examine NoSQL artifacts for user activity and data interaction. We'll begin with basic CRUD operations to understand how information is logged, and then expand upon artifact analysis to trace user sessions, attribute activity to particular users, and even trace sessions to unique IPs. We'll also examine artifacts from RESTful interfaces of NoSQL databases, understanding how users don't need to access a machine to interact with data.

This session promises to offer attendees, both new and experienced, a new perspective on NoSQL databases, artifacts, and forensic analysis.

11:10am-Noon

Live Broadcast

DFIR Summit Forensic Lunch*

*Hosted by **David Cowen** and **Matthew Seyer***

You love Forensic Lunch on YouTube; here's your chance to be part of the live audience for the first-ever DFIR Summit Forensic Lunch! Ask questions and get involved as we dig deeper with our featured speakers about their research and what's next.

**lunch will not be served during the broadcast; lunch break to follow at noon*

Noon-1:20pm

LUNCH & LEARN

(LOCATION: MEETING ROOM 410)

Presented by

Bit9 + CARBON BLACK

ARM YOUR ENDPOINTS.

Gaining control of Incident Costs with Carbon Black

***Jim Raine**, Director, BD Technical Engagement, Bit9, Inc.*

Costs associated with post-breach activities have soared in the past three years. Despite new tools, techniques, and changes in defensive posture, as an industry we still suffer from old traditions in solution design that fail to meet the needs of crisis service teams today. Carbon Black endeavored to break this development cycle with a simple, yet impactful change in "how we do things." Come learn why Carbon Black is the fastest growing solution and how Carbon Black can reduce the costs associated with incident response engagements.

LUNCH & LEARN

(LOCATION: MEETING ROOM 412)

Presented by

cellebrite

delivering mobile expertise

The Power of 3: Combine Artifacts from Mobile, Operator, and Other Data Sources to Focus Your Investigations Program

***Ronen Engler**, Senior Manager, Technology & Innovation, Cellebrite Inc.*

Do you need to extract insights from an increasing number of disparate data sources, but also need to make sense of it in minimal time? In this scenario-based session, find out how to extract forensically sound data from mobile and other data sources. Learn how importing it, together with carrier records, into a unified visual view can help you efficiently contextualize the data to identify leads and make decisions. Finally, understand how these efficiencies can accelerate your investigations, improving both their quantity and their quality.

1:20-2:10pm

(LOCATION: SALON D)

Scaling Incident Response From a One-Person Shop to a Full SOC

***Brian Carrier**, VP of Digital ForensicsBasis Technologye*

This interactive panel will talk about experiences with scaling an incident response program from its initial creation to a mature capability. The panelists will include members of corporate response teams and consultants that advise companies on building a response capability. We'll also be engaging the audience with their experiences while we talk about what situations cause companies to stumble when they try to keep up with the backlog of alerts and determine the scope of incidents.

(LOCATION: SALON E)

Customized Google Chrome Forensics with Python

***Ryan Benson**, Digital Forensic Examiner, Stroz Friedberg*

Hindsight is an open source tool (written in Python) for extracting, interpreting, and reporting on Google Chrome artifacts. It is extensible via "plugin" files that can do very targeted analysis. Example plugins include parsing Google Analytics cookies, extracting Facebook user names from downloaded pictures, or even detecting possible system clock tampering by comparing server-side and local timestamps.

This presentation will show users how to use Hindsight to analyze a user's Chrome installation, how to write custom plugins to parse specific artifacts, how to integrate Hindsight into a complex investigative workflow, and finally, how to explain all this to a manager in a report.

2:10-3:00pm

(LOCATION: SALON D)

Power(Shelling) Through the Timeline

Jon Turner, *Security Service Engineer, Microsoft Corp.*

Timeline analysis is a tried and true method well understood by many investigators, but digging through a spreadsheet can be tedious, especially when an incident's scope expands to dozens, hundreds or thousands of hosts. What if there was a more automated and scriptable way? PowerShell provides the platform and tools necessary to easily identify outliers, filter and highlight the information that is most important, and expand analysis to enterprise scale. **https://twitter.com/z4ns4tsu**

(LOCATION: SALON E)

This Isn't Your Father's Remediation

Wendi Whitmore Rafferty*, VP, CrowdStrike Services*
Christopher Scott*, Director of Remediation, CrowdStrike Services*

Today's incident response team can't just rely on having a whole weekend to remediate. You've also got to be able to start frustrating the attacker earlier and earlier in the response. Suppose an advanced attacker had figured out how to reliably evade your FireEye boxes, your Bit9 endpoint software, your Symantec DLP. And he's using *your* credentials against you. Could you find and frustrate him? Or would you pour a steaming cup of fail in your own lap?

In this talk, you'll learn a few ways that CrowdStrike's hunters lock down authentication credentials during a hot incident, when we're engaging in a running firefight with the adversary on your own network.

We'll show you the tactics and when to apply them. Attendees will learn how to conduct adversary-based hunting operations using existing technology; improve authentication credential protection during live IR and prepare for adversary evolution.

And yeah, we'll use tactics from current incidents we responded to.

3:00-3:20pm

Networking Break & Vendor Expo
(LOCATION: GOVERNOR'S BALLROOM SALON D FOYER)

3:20-4:10pm

(LOCATION: SALON D)

Plumbing the Depths: ShellBags

Eric R. Zimmerman*, Special Agent, FBI*

This presentation will explore the most common ShellBag types (directories, GUIDs, control panel items, etc) and the kinds of data contained therein including timestamps, usernames, changing program associations, file system info, user searches, accessing network resources (UNC paths and FTP), and so on. The discussion will also cover extension blocks and the kinds of data they contain.

The discussion will start at the hex level, work toward higher levels of abstraction, and culminate with examples of using ShellBags Explorer (SBE) to streamline the review of ShellBags data. This will include showing how SBE can be used to accelerate the investigation of unlimited amounts of ShellBag data including working with individual registry hives as well as deduplicating multiple hives for a user. The presentation will also demonstrate how Dan Pullega's research has been incorporated and expanded upon including first and last explored dates.

The information contained in ShellBags and exposed via SBE is relevant to FEs, IR teams, and law enforcement as it quickly and easily provides context around a user's action in addition to their interaction with a computer and its associated resources.

(LOCATION: SALON E)

In the Lair of the Beholder: Extrusion Detection in 2015

Kyle Maxwell*, Senior Researcher, Verisign*

Monitoring external data can detect potential security incidents in your network that other internal systems may have missed. In this session, we will review a number of technologies and techniques for extrusion detection in 2015 such as YARA, Combine, and systems that automate social media monitoring. This will include the review of sample scenarios, lessons learned, and guidance for future development. We will also release all the scripts (including an Ansible playbook) so that attendees can begin deployment in their organizations immediately.

4:15-5:15pm

DFIR SANS360

This session features an array of top Digital Forensics and Incident Response experts discussing the coolest forensic technique, plugin, tool, command line, or script they used in the last year. They'll talk about the approach that really changed the outcome of a case they were working on. If you have never been to a lightning talk, it is an eye-opening experience. Each speaker has 360 seconds (six minutes) to deliver his or her message. This format allows SANS to present 10-12 experts within one hour, instead of the standard one presenter per hour. The compressed format gives you a clear and condensed message eliminating the fluff. If the topic isn't engaging, a new topic is just six minutes away.

Musashi Forensics – ***Frank McClain**, Information Security Manager, DFIR Team Lead – PrimeLending*

TOR: The Dark Web – ***Lee Whitfield**, Director of Forensics, Digital Discovery*

Malware Blocks – ***John Lukach**, Security Architect, Pinnacle Bank*

I Love It When a Plan Comes Together: A Case Study on Using Various Tools Throughout an Intrusion Investigation – ***Ron Dormido**, Senior Security Consultant, Verizon*

Network Disasters: Incident Response When the Bits Hit the Fan – ***Matt Linton**, Chaos Specialist, Google*

Re-"Tension": Tips from a Recovering Job-Hopper – ***Alissa Torres**, Certified Instructor, SANS Institute*

Need for Speed: Malware Edition – ***Anuj Soni**, Booz Allen Hamilton*

Oh, Snap!: Snapshots and Re-creation Testing in VMs – ***David Cowen**, Partner, G-C Partners LLC*

Performing Smartphone Forensics without Commercial Tools – ***Heather Mahalik**, Forensics Lead and PM, Oceans Edge, Inc & SANS Certified Instructor, Author, Course Lead*

The Beauty and the Beast: Threat Intel Done Right...and Wrong – ***Robert M. Lee**, Co-Founder, Dragos Security LLC*

5:15-5:30pm

Summary & Closing Remarks

***Rob Lee**, **David Cowen** & **Alissa Torres**, Summit Co-Chairs*

Thank you for attending the SANS Summit.

Please remember to complete your evaluations for today.
You may leave completed surveys at your seat or turn them in to the SANS registration desk.

SPEAKERS

***Barry Anderson**, Security Architect, Cisco Systems*
Barry has over 20 years of experience in IT Security, specializing in Firewalls, 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. He has BSc Comp Sci, GSEC (Gold, Hons) and GFOR (Gold, Hons) certifications and is a member of AISA and ISACA. **@z3ndrag0n**

***Ryan Benson**, Digital Forensic Examiner, Stroz Friedberg*
Ryan Benson is a Digital Forensic Examiner at Stroz Friedberg's San Francisco office. He 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 Chrome forensics tool written in Python. Ryan holds a Bachelor's degree in Computer Engineering from the University of the Pacific. During his undergraduate studies, he did an internship in the FBI's Silicon Valley Regional Computer Forensics Lab. He is a member of the High Technology Crime Investigation Association (HTCIA) and holds several certifications including the GIAC Certified Forensic Analyst (GCFA) and GIAC Certified Incident Handler (GCIH). **@_ryanbenson**

***Dmitry Bestuzhev**, Head of the Global Research and Analysis Team, Latin America, Kaspersky Lab*
Dmitry Bestuzhev is the Director of the Global Research and Analysis Team (GReAT) for Latin America at 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.

In addition to leading Latin America's team of security analysts, Dmitry is responsible for the development of threat intelligence reports and IT security forecasts for the region. He frequently collaborates with international media as well as public and private entities as an expert source on IT security topics. His vast experience covers everything related to the industry, from online fraud to the use of social networks by cybercriminals, corporate security breaches, cyber war and cyberespionage campaigns. In addition to his professional responsibilities, Dmitry is also involved with several educational initiatives across Latin America that help promote online safety and encourage IT security as a field of study. **@dimitribest**

***Sameer Bhalotra**, The White House*
Sameer Bhalotra is Co-founder & CEO of StackRox, a new startup in Mountain View, CA. Previously he was at Google, following the acquisition of his first company, Impermium. Dr. Bhalotra has served at the White House, Senate Intelligence Committee, and Central Intelligence Agency, and received degrees from Harvard and Stanford Universities. **@sameerbhalotra**

***Matt Bromiley**, Senior Consultant, Mandiant*
Matt has over 4 years experience in incident response, digital forensics, data breaches, and threat intelligence. He recently joined the team at Mandiant where he finds himself working with some of the best and brightest in the industry. His skills include disk, database, and network forensics, malware analysis, network security monitoring, and log analytics. Matt has helped organizations of all sizes with their forensics and IR needs, from local banks to large, multinational conglomerates. He has a passion for Mac & Linux forensics, as well as building scalable analysis tools utilizing free and open source software. Matt's interest in non-traditional forensic topics, such as NoSQL, has stemmed from his experiences in developing tools using NoSQL databases, including MongoDB or Elasticsearch, and the artifacts that are left behind. **@505forensics**

***James Carder**, Director of Security Informatics, Mayo Clinic*
James Carder is the director of security informatics at Mayo Clinic. He is the enterprise leader of incident response (triage, forensics, malware analysis, cyber analytics), threat intelligence, and technical risk (vulnerability management and penetration testing).

Prior to Mayo Clinic, James was a senior manager at MANDIANT. While at MANDIANT, he led professional services and incident response engagements for the Fortune 500. James has responded to, investigated and remediated organizations involved in credit card compromise and intrusions by the advanced persistent threat (APT). He has also led criminal and national security related investigations at the city, state and federal levels. Prior to joining MANDIANT, James was a managing consultant for IBM/ISS X-Force. **@carderjames**

***Josh Chin**, Founding Partner, 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 Cowen 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), Infosec 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 RISK Team*
Ron Dormido 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**

***Sarah Edwards**, Test Engineer, Parsons Corporation*
Sarah is an 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's research and analytical interests include Mac forensics, mobile device forensics, digital profiling and malware reverse engineering. Sarah has presented at many industry conferences including; Shmoocon, CEIC, Bsides*, Defcon and the SANS DFIR Summit. She has a Bachelor of Science in Information Technology from Rochester Institute of Technology and a Masters in Information Assurance from Capitol College. Sarah is the author of the new SANS Mac Forensic Analysis course - FOR518. **@iamevltwin**

***Steve Gibson**, Director – Forensic Technology Practice, 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 is currently a Director with KPMG, supporting the Forensic Technology practice with custom software and solutions.

SPEAKERS

***Andrew Hay**, Research Lead, OpenDNS*
Andrew Hay is the Research Lead & Evangelist at OpenDNS where he leads the research efforts for the company. Prior to joining OpenDNS he was the Director of Applied Security Research and Chief Evangelist at CloudPassage, Inc. Prior to that, Andrew served as a Senior Security Analyst for 451 Research's Enterprise Security Practice (ESP) providing technology vendors, private equity firms, venture capitalists and end users with strategic advisory services – including competitive research, new product and go-to-market positioning, investment due diligence and tactical partnership, and M&A strategy.

Before joining The 451 Group, Andrew worked in the Information Security Office (ISO) of the University of Lethbridge, in Alberta, Canada and at a privately held bank in Hamilton, Bermuda; in each position, he was responsible for strategically designing, driving and executing the goals and objectives of the organization's information security programs. Prior to that, Andrew served in various roles at Q1 Labs, including Engineering Manager, Product Manager and finally as the Program Manager responsible for the entire portfolio of third-party technology partner relationships. **@andrewsmhay**

***Alan Ho**, Valkyrie-X Security Research Group (VXRL)*
- *CeCOS VIII (APWG) 2014 – Best Practice in Network Forensics*
- *DFRWS EU 2014 – Real Network Forensics Kungfu*
- *Hack in Taiwan 2014 – Investigation and Intelligence Framework*
- *IFMTA 2014 - Website Security For Mobile*
- *SANS GWAPT Holder*
- *SANS Gold Paper - Website Security For Mobile*

Experience in development, penetration test, incidence response and investigation

***Rick Holland**, Principal Analyst, Forrester Research*
Rick Holland is a Principal Analyst at Forrester Research where he serves security and risk professionals. 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. Prior to joining Forrester, he was a Solutions Engineer where he architected enterprise security solutions. Previously, he worked in both higher education and the home building industry, where he focused on intrusion detection, incident response and forensics. He is regularly quoted in the media and is a frequent guest lecturer at the University of Texas at Dallas. Rick holds a B.S. in Business Administration MIS from UT Dallas. Rick is also a GIAC Certified Incident Handler (GCIH) as well as a former U.S. Army Intelligence Analyst. **@rickhholland**

***Devon Kerr**, Senior Consultant, Mandiant*
Devon Kerr is a Principal Consultant at Mandiant, 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 Khatri 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.

***David Kovar**, Senior Manager, Ernst & Young*
David Kovar is a senior manager in EY's Cybersecurity practice. He's also been an entrepreneur, ediscovery consultant, software engineer, SAR incident commander, executive protection agent, and lethal forensicator. He has collected images in China, rescued wayward Americans in Australia, and conducted disaster preparedness assessments in Tajikistan. Oh, and he flies sailplanes, fixed wings, helicopters, and drones. **@dckovar**

***Warren Kruse**, VP Data Forensics, Altep, Inc.*
Warren is a vice president with Altep Inc., a national provider of e-discovery and computer forensic services. He 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 the 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).

He is the author of "Computer Forensics: Incident Response Essentials", and has supported incident response projects across a wide range of major U.S. corporations and agencies. In addition: led a team of computer forensic experts in a three-year engagement in support of a fraud investigation task force at the world's largest international cooperative organization. He was the eDiscovery expert for AMD on the AMD versus Intel Antitrust lawsuit; led the forensics on the billion dollar "Comtraid" theft of Intellectual Property and Trade Secrets; and testified as a computer forensic expert for the US Securities and Exchange Commission (SEC). **@warren_kruse**

***Rob Lee**, Fellow, SANS Institute*
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, the first U.S. military operational unit focused on information warfare. Later, he was a member of the Air Force Office of Special Investigations (AFOSI) where he led a team conducting computer crime investigations, incident response, and computer forensics. Prior to starting his own firm, he directly worked with a variety of government agencies in the law enforcement, U.S. Department of Defense, and intelligence communities as the technical lead for a vulnerability discovery and an exploit development team, lead for a cyber forensics branch, and lead for a computer forensic and security software development team. Rob was also a director for MANDIANT, a company focused on investigating advanced adversaries, such as the APT, for four years prior to starting his own business.

Rob co-authored the book *Know Your Enemy*, 2nd Edition. Rob earned his MBA from Georgetown University in Washington DC. He was awarded the Digital Forensic Examiner of the Year from the Forensic 4Cast Awards. Rob is an ardent blogger about computer forensics and incident response topics at the SANS Computer Forensic Blog. Rob is also a co-author of the MANDIANT threat intelligence report M-Trends: The Advanced Persistent Threat. **@robtlee**

SPEAKERS

***Robert M. Lee**, Co-Founder, Dragos Security LLC*
Robert M. Lee is a co-founder at the critical infrastructure cyber security company Dragos Security LLC where he has a passion for control system packet analysis, digital forensics, and threat intelligence research. He is a passionate educator having taught for various organizations including Utica College where he is currently an Adjunct Lecturer in the M.S. Cybersecurity program. He is the SANS ICS 515 - Active Defense course author and co-author for SANS FOR578: Cyber Threat Intelligence. Robert is often confused with the other Rob Lee at SANS who is a SANS Fellow and runs the Forensics track. It is in fact a different Rob Lee who just so happened to have also been in the Air Force and attended the same undergraduate university as Robert – that Rob Lee is more talented although it has cost him his hair.

Robert obtained his start in cyber security in the U.S. Air Force where he currently serves as an active-duty Cyber Warfare Operations Officer. He has been a member of multiple computer network operation teams including his establishing and leading of a first-of-its-kind ICS/SCADA cyber threat intelligence and intrusion analysis mission in the intelligence community. He has published numerous articles and journals for various publications including SC Magazine, Air and Space Power Journal, Control Global, and Control Engineering and is a frequent speaker at conferences having previously presented at events such as SANS, IFRI, BSides, and TROOPERS. Robert received his B.S. from the United States Air Force Academy, his M.S. in Cybersecurity - Digital Forensics from Utica College, and is currently pursuing his PhD at Kings College London with research into cyber conflict and the cyber security of control systems. He is also the author of the book "SCADA and Me." **@robertmlee**

***Matt Linton**, Chaos Specialist, Google*
Matt Linton 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.

***John Lukach**, Security Architect, Pinnacle Bank*
John Lukach 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 Mahalik is leading the forensic effort for Ocean's Edge as a project manager. 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.

Previously, Heather led the mobile device team for Basis Technology, where she focused on mobile device exploitation in support of the U.S. Government. She also worked as a forensic examiner at Stroz Friedberg and the U.S. State Department Computer Investigations and Forensics Lab, where she focused her efforts on high profiles cases. Heather maintains **www.smarterforensics.com** where she blogs and hosts work from the digital forensics community. **@heathermahalik**

***Kyle Maxwell**, Senior Researcher, Verisign*
Kyle Maxwell is a threat intelligence analyst and malware researcher, currently focused on covering DDoS and Latin America. He has contributed to several public reports on data breach analysis and frequently speaks & writes at conferences around the United States and Latin America. Previously, he led the incident response team at a large payment processor and performed digital forensics for clients across the United States at several private investigation firms. Mr. Maxwell holds a degree in Mathematics from the University of Texas at Dallas. **@kylemaxwell**

***Frank McClain**, Information Security Lead, DFIR Team Manager, Prime Lending*
Frank McClain is a military veteran and information assurance practitioner with deep experience in digital forensics, incident response, and eDiscovery. He oversees information security operations for a national financial services firm where he developed and leads their incident response, digital forensics, malware remediation, threat analysis, eDiscovery, and security awareness team. **@littlemac042**

***Cindy Murphy,** Detective, City of Madison, WI Police Department*
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 and has been involved in computer forensics since 1999. She earned her Master's degree in Forensic Computing and Cyber Crime Investigation through University College, Dublin in 2011. She has directly participated in the examination of many hundreds of hard drives, cell phones, and other items of digital evidence pursuant to criminal investigations including homicides, missing persons, computer intrusions, sexual assaults, child pornography, financial crimes, and various other crimes. She has testified as a computer forensics expert in state and federal court on numerous occasions, using her knowledge and skills to assist in the successful investigation and prosecution of criminal cases involving digital evidence. She is also a part time digital forensics instructor at Madison College, and a part time Advanced Mobile Device Forensics instructor for the SANS Institute. **@cindymurph**

***Sara Newcomer**, Computer Forensic Examiner, Lockheed Martin*
Sara Newcomer is a computer forensic examiner for Lockheed Martin. Ms. Newcomer has a Master of Science degree in Information Technology from Towson University and a Bachelor of Science degree in Computer Engineering from Virginia Tech.

***David Nides**, Director – Forensic Technology Practice, KPMG*
David is a Director with KPMG's Forensic Technology practice in Chicago, IL. Currently, he plays a national leadership role overseeing innovation and delivery of KPMG's Cyber Investigations services. **@davnads**

***Chris Petersen**, CTO, LogRhythm*
Chris Petersen is CTO and co-founder of LogRhythm. He combines extensive industry experience in information assurance and network security with an innovative approach to technology to drive LogRhythm's strategic vision as the company delivers the most comprehensive log and event management solution on the market. Chris's past accomplishments include developing the Price Waterhouse (now PriceWaterhouseCoopers) Enterprise Security Architecture System as a senior consultant and leading an engineering group at Ernst & Young that produced one of the first managed security services. He has served on the faculty of the Institute for Applied Network Security, has presented numerous times at information security conferences and events, and is frequently quoted in industry leading publications. **@logrhythm**

SPEAKERS

***Wendi Rafferty**, VP, CrowdStrike Services*
Wendi Rafferty 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 Roberts**, Bad Guy Catcher, GitHub*
Scott J Roberts works for GitHub and 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. Scott is also really good at speaking in the 3rd person.

***Jordi Sanchez**, Red Mage, Google*
Jordi is a member of the Incident Response Team at Google. In the past he's been seen in courts testifying as an expert witness, rocking remote enterprise forensics while solving high-profile fraud and civil cases and penetrating networks to later secure them. He's taught forensics to law enforcement, competed in CTFs and done research and development on virtualization, file format and memory analysis.

Lately, he's been spending some of his spare time developing Rekall, a memory forensics framework, and enjoying the sunny weather of California with his fiancée. **@parkisan**

***Christopher Scott**, Director of Remediation, CrowdStrike*
Christopher Scott has over 17 years experience working with the Department of Defense and Fortune 500 companies to develop business and network security processes and procedures. He has particular expertise in targeted threat detection and prevention. As the Director of Remediation at CrowdStrike Christopher specializes in developing and implementing remediation plans for clients. **@NetOpsGuru**

***Matthew Seyer**, Consultant at G-C Partners, LLC*
Matthew Seyer, is a consultant at G-C Partners, LLC based in Dallas, Texas. He has obtained a Bachelor of Technology in Information Assurance and Digital Forensics at Oklahoma State University Institute of Technology Okmulgee and an Associate in Applied Sciences of Digital Forensics at Richland College. Over the past three years Mr. Seyer has been involved with researching and creating tools for file system journal forensics. Both David Cowen and Matthew Seyer are hosts of the Forensic Lunch, a webcast that covers digital forensics topics Fridays at noon (CST) on Google Hangouts. **@forensic_matt**

***Anuj Soni**, Senior Incident Responder, Booz Allen Hamilton*
Anuj Soni is a Senior Incident Responder at Booz Allen Hamilton, where he leads forensic, malware, and network analysis efforts to investigate security incidents. Since entering the information security field in 2005, Anuj has performed numerous intrusion investigations to help government and commercial clients mitigate attacks against the enterprise. His malware hunt skills and technical analysis abilities have resulted in the successful identification, containment, and remediation of multiple threat actor groups. Anuj has analyzed over 400 malware samples to assess function, purpose, and impact, and his recommendations have improved the security posture of the organizations he supports.

Sought after as a technical thought leader and adviser, Anuj excels not only in delivering rigorous forensic analysis, but also in process development, knowledge management, and team leadership to accelerate incident response efforts. Anuj shares his knowledge and experience often by teaching for SANS and presenting at events including the U.S. Cyber Crime Conference, SANS DFIR Summit, and the Computer and Enterprise Investigations Conference (CEIC). He received his Bachelors and Masters degrees from Carnegie Mellon University. He also holds the following certifications: GIAC Reverse Engineering Malware (GREM), EnCase Certified Examiner (EnCE), and Certified Information Systems Security Professional (CISSP). **@asoni**

***Alissa Torres**, Certified Instructor, SANS Institute*
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. She has presented at various industry conferences and numerous B-Sides events. In addition to being a GIAC Certified Forensic Analyst (GCFA), she holds the GCFE, GPEN, CISSP, EnCE, CFCE, MCT and CTT+. **@sibertor**

***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. Along the way, he collected an alphabet soup of GIAC certifications and is currently a GSE candidate. He currently acts as a subject-matter expert in digital forensics and incident response for Microsoft's Office365 products. **@z4ns4tsu**

***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 perform security reviews and incident response on the infrastructure that serves millions of Firefox users. **@jvehent**

***Lee Whitfield**, Director of Forensics, Digital Discovery*
Lee is director of forensics at Dallas-based Digital Discovery. He 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**

Kelvin Wong
Kelvin Wong (a.k.a Forensics Ninja) works in 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, AVTokyo, HITCON, ICCCF, CeCOS(APWG) & HTCIA (APAC) and published research papers at DigitalForensics Magazine and Hakin9 IT Security Magazine.

***Eric Zimmerman**, Special Agent, FBI*
Eric Zimmerman 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. **@EricRZimmerman**

EXHIBITORS

Atola TECHNOLOGY

BASIS TECHNOLOGY

Bit9 + CARBON BLACK
ARM YOUR ENDPOINTS.

cellebrite
delivering mobile expertise

LogRhythm™