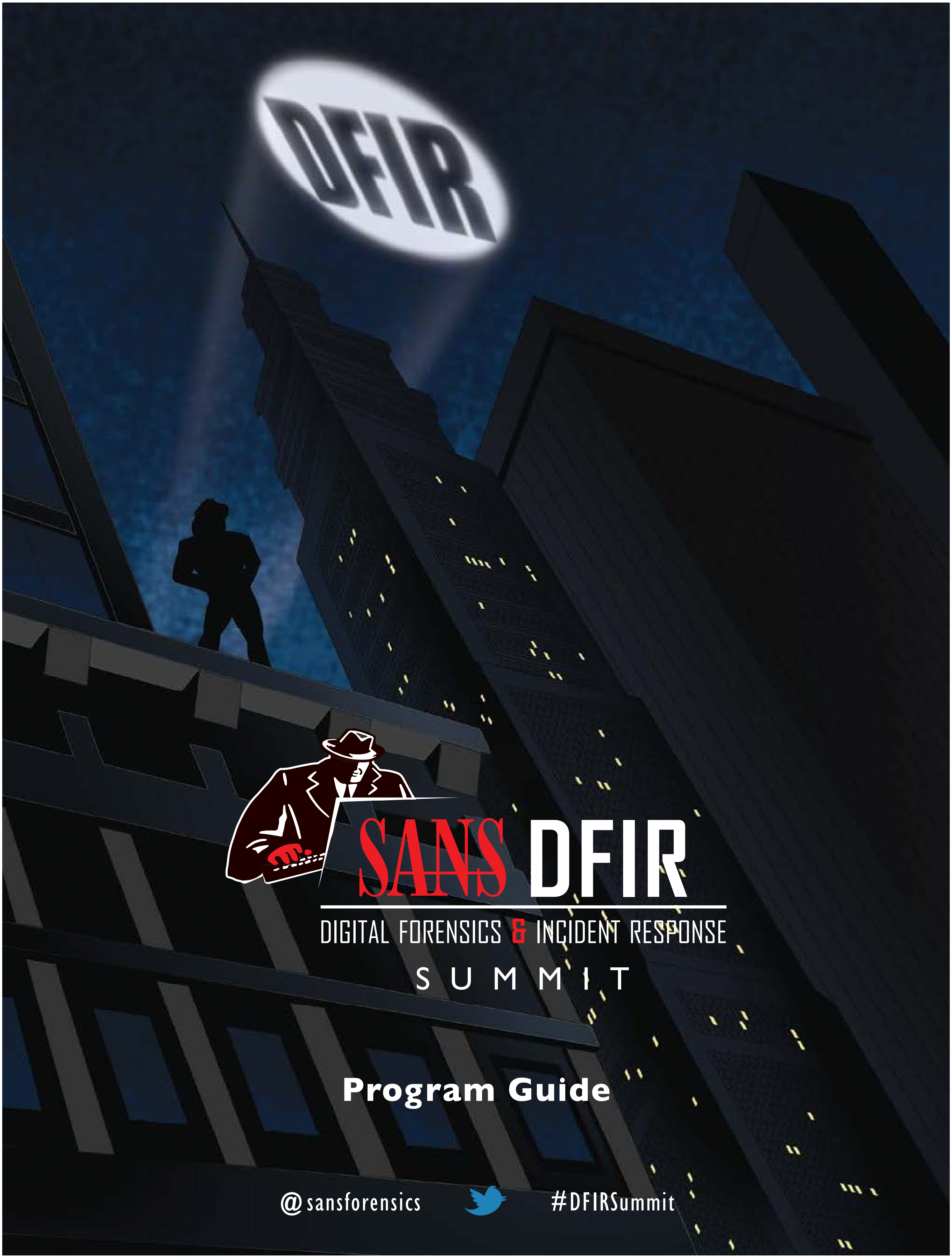

SANS DFIR

DIGITAL FORENSICS & INCIDENT RESPONSE

SUMMIT

Program Guide

@sansforensics #DFIRSummit

Welcome to the Digital Forensics & Incident Response Summit!

Rob Lee

As we come together as a community to discuss and share ideas on all things DFIR, your participation is what makes our Summit the most comprehensive event of its kind. We have nearly 200 members of the DFIR community in attendance this year, including top industry experts sharing their wisdom on the latest trends and most innovative topics the industry has to offer. Our goal is for you to take this information and use it to win the battle against ever-stronger adversaries.

Take this opportunity to introduce yourself to those sitting around you, join one of the many conversations during breaks, and engage with our expert speakers during our many networking events, ask questions during Q&A sessions, and weigh in on Twitter **#DFIRSummit** and **@DFIRSummit**.

Finally, let's have fun and make the next two days count! Put your gaming skills to the test with fellow attendees and Summit speakers at Recess Arcade Bar on Thursday night, June 23rd. Attendees tell us time and again that the greatest value of our Summit is the plethora of newly forged or deepened industry connections they make during their time with us.

Looking forward to a great Summit!

Sincerely,

Rob Lee

Fellow, SANS Institute

Agenda

All Summit Sessions will be held in the Salons AB & C – 4th floor (unless noted).

All approved presentations will be available online following the Summit at
https://digital-forensics.sans.org/community/summits
An e-mail will be sent out as soon as the presentations are posted, typically within 5 business days of the event.

Thursday, June 23

8:00-9:00am

Registration & Coffee (LOCATION: ABC PRE-FUNCTION)

9:00-9:10am

Welcome and Opening Remarks (LOCATION: SALON C)

Rob Lee *(@robtlee), DFIR Lead, SANS Institute*

9:10-10:00am

Defending a Cloud (LOCATION: SALON C)

What makes cloud platforms unique – and uniquely difficult to defend? There are cool and wonderful things a forensics/IR person can do in the cloud, from collecting higher quality evidence from running systems, to interesting analysis that can be done with the event logs from a 1000 identical machines. Get the low-down during this return engagement by one of the DFIR Summit's most popular keynote speakers, back by popular demand to help you make sense of forensicating in the cloud.

Troy Larson *(@troyla), Microsoft Security Response Center | Azure*

10:00-10:30am

Networking Break and Vendor Expo (LOCATION: ABC PRE-FUNCTION)

10:30-11:00 am

(LOCATION: SALON AB)

iOS of Sauron: How iOS Tracks Everything You Do

iOS devices have the ability to track everything the user does – how many steps the user takes, where the user has been, and keeps track of how they use their devices.

This presentation will dive into some of the protected files that keep track of every detail of a user's life that iOS tracks.These databases and files can be used to correlate user activity down to the smallest detail. Methods of analysis as well as some scripts will be shown to help analyze these files.

Sarah Edwards *(@iamevltwin), Mac Nerd, Parsons Corporation; Author & Instructor, FOR518, SANS Institute*

(LOCATION: SALON C)

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

Hunt teams increasingly are building redundancy into their investigations to detect and respond to cyberattacks. Cross-Customer Correlation is a process where hunt teams pivot from one set of indicators from a customer into other customer networks to find threats, anomalies and other attack patterns they may have missed in their initial investigations. In this presentation, Farsight Security CEO Dr. Paul Vixie and ProtectWise CTO Gene Stevens will present a compelling case study focused on how ProtectWise used Farsight's historical passive DNS information to pivot from threat indicators found in one customer's network to uncover a previously undetected attack in a second customer's network.

Gene Stevens*, (@genestevens) CTO, ProtectWise*

Dr. Paul Vixie *(@paulvixie), CEO, Farsight Security*

Thursday, June 23

(LOCATION: SALON AB)

(LOCATION: SALON C)

11:05-11:35am

Hello Barbie Forensics

With the introduction of Hello Barbie, Mattel has brought one of the world's most recognizable toys into the Internet of Things era. The Wi-Fi-connected doll is able to hold real-time conversations by recording audio and uploading it to the cloud for instant processing of artificial intelligence-based responses.

Our research examined the security of the mobile components of Hello Barbie including the mobile app, both iOS and Android versions, developed by Mattel partner ToyTalk as well as communications between the app and its cloud-based servers.

This talk will detail the security issues discovered with the Hello Barbie app, the doll, and the related hosting infrastructure that could allow a malicious user to intercept and collect a child's interaction with the doll. We will also discuss the digital fingerprints left on mobile devices during initial configuration as well as those left by the ongoing parental management and monitoring of their child's interactions.

Andrew Blaich, Ph.D. *(@ablaich), Lead Security Analyst, Bluebox Security*

Andrew Hay *(@andrewsmhay), CISO, Data Gravity*

Start-Process PowerShell: Get Forensic Artifact

The increasing size of Hard Disk Drives presents a growing problem for the digital forensics field. It is no longer feasible to investigate every artifact on every host in the environment when a compromise occurs. Lucky for us, nearly all disk-based artifacts have a timestamp associated with them, which can be used to build a forensic timeline. This timeline can be used to narrow the scope of the investigation, allowing analysts to quickly triage events related to the compromise.

Fortunately, this can all be accomplished without purchasing any expensive tools by leveraging PowerShell and its access to the Windows API and .NET framework. PowerForensics provides Digital Forensics/Incident Response community with an all in one toolset for attack investigation, providing a forensically sound "live" investigation platform without the need to image the hard drive. This presentation will cover the background and overview of PowerForensics, including how its new Forensic Timelining capability can facilitate the investigation of advanced actors at scale. Finally, I'll cap off with a complex demo, showing how PowerForensics can help blue teams investigate the real attacks they're currently facing.

Jared Atkinson *(@jaredcatkinson), Hunt Capability Lead, Veris Group's Adaptive Threat Division*

11:40am-12:10pm

CryptoLocker Ransomware Variants Are Lurking "In the Shadows;" Learn How to Protect Against Them

Recently, attackers employing a CryptoLocker variant have been removing volume shadow copies on systems, disallowing the users from restoring those files, and then encrypting the files for ransom. If a user cannot recover from backups, he/she is at the attacker's mercy.

In this technical session, we'll discuss the ins and outs of shadow copies, reveal how attackers are using them to encrypt files for ransom, and then discuss ways you can quickly - and easily - detect and respond to these kinds of attacks.

Ryan Nolette*, Security Operations Lead, Carbon Black*

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; Fellow, SANS Institute*

Thursday, June 23

12:10-12:25pm

Ken Johnson Memorial Scholarship

Earlier this year, the DFIR community suffered a great loss with the passing of Ken Johnson. In recognition of his many contributions to the community, and with fond memories of the joy he brought to those he met at events like the DFIR Summit, SANS Institute and KPMG is honored to jointly announce the Ken Johnson Memorial Scholarship, which will be awarded each year to one individual so that (s)he may attend the DFIR Summit and a training course.

***Matt Bromiley**, Senior Consultant, Mandiant*
***Rob Lee**, DFIR Lead, SANS Institute*
***David Nides**, Director – Forensic Technology Services, KPMG LLP*

12:25-1:30pm

LUNCH & LEARN

(LOCATION: SALON AB)

Presented by

AccessData
A Pioneer in Digital Investigations Since 1987

Benefit of Enterprise in the IR Plan

***Nick Drehel**, VP of Digital Investigations, AccessData*

In the past, incident response and computer forensics have remained separate entities in the digital investigation world. The time has come to bring the two disciplines together to answer the questions of how the incident occurred, who may have been responsible, and what data may have been accessed. Examiners might come across malware in the form of browser scripts, exploit-ridden documents, or malicious executables. Examining these artifacts to understand their capabilities requires a specialized malware analysis and reverse-engineering skill-set.

Currently, there are six steps to incident response:

- Preparation
- Identification
- Containment
- Eradication
- Recovery
- Review/Debriefing

This collaboration will add in one more step into your incident response program:

- Forensic Investigation: A forensic analysis to determine what actually happened to the systems or network. We need to answer the questions of how the incident occurred, who may have been responsible, and what data may have been accessed.

This presentation will introduce attendees to the AccessData Enterprise software. You will see how to use the tool to remote into end points on your network to determine if users are accessing information that should not be doing or to determine if a system may be compromised. In either case, you can document the issue in a forensically sound manner that can be used in legal proceedings and remediate the problem until further action can be taken.

LUNCH & LEARN

(LOCATION: SALON C)

Presented by

LogRhythm
The Security Intelligence Company

Securing the Internet of All Things: My Fridge is Hacking Me

***Luis Guzman**, Senior Sales Engineer*

A new change in securing the perimeter is being seen by the next wave of the Internet – the Internet of Things (IoT). While creating an incredible opportunity in global communication, this transformation also presents new challenges in securing the organization from previously “dumb” devices like the break-room refrigerator! Previously only holding salmonella in the food it imprisoned, the digital frontier of kitchen appliances and other things is wide open.

(LOCATION: SALON AB)

(LOCATION: SALON C)

1:30-2:00pm

Rising from the Ashes: How to Rebuild a Security Program Gone Wrong… With Help from Taylor Swift

All good security programs have people, process and technology that make them run smoothly. But what happens when your security program has been derailed by a major incident, your company's reputation has taken a hit, or even worse, the security team has lost the trust of the larger organization?

With a little help from Taylor Swift song titles, your security program can rise like a phoenix from the proverbial ashes.

Shelly Giesbrecht *(@nerdiosity), Incident Responder, Cisco*

Mike Hracs *(@bumjubeo), Senior Consultant, Deloitte*

Tracking Threat Actors through YARA Rules and Virus Total

One of the largest challenges in incident response and security operations is tracking changes in campaigns and maintaining an up-to-date list of indicators of compromise. This presentation will detail creating and maintaining YARA rules and leveraging them against the VirusTotal database to track file relationships, subtle changes in campaigns, and generate predictive intelligence using two real-world case-studies. In addition, we will provide several working ideas for tracking and logging this information and automating analysis specific to individual campaigns.

Kevin Perlow*, Senior Consultant, Booz Allen Hamilton*

Allen Swackhamer*, Reverse Engineer, Target*

2:05-2:35pm

All About That (Data)Base

Attackers want it. Your organization uses it every day. Your job is to protect it. It's where all the sensitive stuff sits: the database. As DFIR professionals, our job is to leave no stone unturned. In this talk, we're going to expand your DFIR toolkit and show how to incorporate database forensics in your workflow. Databases contain a wealth of information that may help us determine how the attacker got in and what they took. Through memory, disk, and log analysis, we will cover how analyzing the database in concert with other systems helps to paint a better picture of the breach.

This talk goes beyond simply discussing databases forensics, we're going to get our hands dirty with scripts, memory, and disk analysis. Attendees will learn techniques and methods for performing forensics on MS SQL database systems. We will be releasing new research and tools on carving and analyzing disk- and memory-based artifacts. Attendees will also be exposed to a SQL Database Analysis Framework, which allows them to immediately incorporate these important artifacts into their investigations.

Matt Bromiley*, Senior Consultant, Mandiant*

Jacob Christie*, Consultant, Mandiant*

FLOSS Every Day: Automatically Extracting Obfuscated Strings from Malware

The FireEye Labs Obfuscated String Solver (FLOSS) is an open-source tool that automatically detects, extracts, and decodes obfuscated strings in Windows Portable Executable (PE) files. Malware analysts, forensic investigators, and incident responders can use FLOSS to quickly extract sensitive strings to identify indicators of compromise (IOCs).

Malware authors encode strings in their programs to hide malicious capabilities and impede reverse engineering. Even simple encoding schemes defeat the 'strings' tool and complicate static and dynamic analysis. FLOSS uses advanced static analysis techniques, such as emulation, to deobfuscate encoded strings.

Incident responders and forensic analysts that understand how to interpret the strings found in a binary will understand FLOSS's output. FLOSS extracts higher value strings, as strings that are obfuscated typically contain the most sensitive configuration resources – including malicious domains, IP addresses, suspicious file paths, and other IOCs. FLOSS is more robust than 'strings', so in our technique talk we'll spend some time describing the computer science that powers the tool, and why it works. We'll also show FLOSS in action, as it decodes configurations from a dozen obfuscated malware families.

William Ballenthin *@williballenthin), Reverse Engineer, FireEye*

Moritz Raabe*, Reverse Engineer, FireEye*

Thursday, June 23

(LOCATION: SALON AB)

(LOCATION: SALON C)

2:40-3:10pm

UAV Forensic Analysis – Next Gen

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.

This presentation has been updated from last year to include new analysis options, specifically log and JTAG analysis, along with other enhancements.

***David Kovar** (@dckovar), Consultant*

Plumbing the Depths: Windows Registry Internals

This presentation will explore the low-level structures that comprise Registry hives including key and value records, data cells (including big data), and security records. List records, the glue holding the Registry together, will also be discussed. The Registry contains vast amounts of forensically relevant information and, like file systems, can contain deleted keys and values. By using free, open source tools (Registry Explorer and RECmd), attendees will see how both deleted keys and values are recovered, reconstructed, and made available to examiners to review.

Because analysis of Windows Registry hives is such a common component in forensic reviews, examiners should have a deep understanding of how Registry tools they have used for years work at a low level. By doing so, they will be more competent examiners and can explain how tools work vs. merely consuming tool output.

***Eric Zimmerman** (@EricRZimmerman), Sr. Director, Kroll Cyber Security*

3:10-3:40pm

Networking Break and Vendor Expo (LOCATION: ABC PRE-FUNCTION)

3:40-4:10pm

Trust but Verify: Why, When and How

Ask not what your tools can do for you, but what you should be doing with your tools. How does an examiner know if the tools they are using are providing accurate and trustworthy results? In this talk we will cover the importance of verifying and testing your tools with real world examples of tool fails. We'll also walk through an example of how to verify your tools using several methods.

***Mari DeGrazia** (@maridegrazia), Director, Kroll Cyber Security*

The Incident Response Playbook for Android and iOS

What is your mobile device incident response plan? If you cannot answer that question, you should attend this session. We will cover the challenges in mobile as they pertain to incident response, how and why mobile differs from traditional incident response, and provide you with the building blocks you can use to craft your own mobile incident response plan.

***Andrew Hoog** (@ahoog42), CEO & Co-Founder, NowSecure*

Thursday, June 23

(LOCATION: SALON AB)

(LOCATION: SALON C)

4:15-4:45pm

Analyzing Dridex, Getting Owned by Dridex, and Bringing in the New Year with Locky

Dridex has been running wild for quite a while now. Even with the huge takedown operation conducted by several three-letter agencies from all around the world, Dridex is still here and it's only getting louder - except now the operators have shifted to ransomware which they have named Locky.This talk will go through the timeline of Dridex/Locky, including the technical side of Dridex/Locky, i.e. how infection occurs (IOCs, network & system analysis; overview of the Dridex/Locky network infrastructure currently being utilized; a general overview of how it operates; and an anecdote of how I failed hard which resulted in my having my VPS shut down due to a Dridex infection.

@sudosev

What Does my SOC Do?: A Framework for Defining an InfoSec Ops Strategy

Don't be turned away by the word "strategy." This talk is for SOC practitioners and managers who deal with the day-to-day struggle to improve their day-to-day ops teams.

Using experience from consulting in and/or standing up SOC environments at multiple SMB and large enterprise organizations, Austin has developed a framework for helping a SOC measure their effectiveness and define their objectives.This framework was developed after years of consulting to help with the following problems including the vast gap between how analysts/practitioners and executives communicate; lack of well-defined metrics frameworks; and tying SOC requirements to business objectives.

***Austin Murphy** (@austinjmurphy), Director of Incident Response, CrowdStrike Services*

4:45-5:15pm

Forensic 4cast Awards (LOCATION: SALON C)

***Lee Whitfield** (@lee_whitfield), Director of Forensics, Digital Discovery*

Thursday, June 23

6:30-8:30pm

DFIR Night in Austin

Hosted by

ARBOR® NETWORKS

The Security Division of NETSCOUT

Recess Arcade Bar, 222 E. 6th Street | Austin, TX 78701

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

NOTE: Please wear or bring your Summit badge for admission.

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.

Friday, June 24

8:00-9:00am

Registration & Coffee (LOCATION: ABC PRE-FUNCTION)

9:00-9:45am

The History of Data Forensics, and Get Off My Lawn! (LOCATION: SALON C)

The evolution, current state and direction of Data Forensics as experienced and related by a cranky old man. Andrew Rosen will share 25 years of experience from the front lines of DF/IR. You'll hear insights gleaned from someone who's "been there, done that" and unabashedly shares his perspective.

***Andy Rosen**, President, ASR Data Acquisition & Analysis, LLC*

9:45-10:30am

Puzzle Solving and Science: The Secret Sauce of Innovation in Mobile Forensics (LOCATION: SALON C)

In today's world, technology (especially mobile device technology) moves at a much faster pace than any of us can keep up with, and available training and research doesn't always address the problems we encounter. As forensic examiners we face the daily challenges of new apps, new, updated and obscure operating systems, malware, secure apps, pass code and password protected phones, encoding and encryption problems, new artifacts, and broken hardware in order to obtain the evidence we need in a legally defensible and forensically sound manner. In this session, learn from consistent and experienced innovators in the mobile forensics field the tips, tricks, and mindset that they bring to bear on the toughest problems and how to move beyond cookie cutter forensics towards an approach that allows you to successfully solve and own problems others might consider too hard to even try.

***Heather Mahalik** (@HeatherMahalik), Forensics Lead and PM, Oceans Edge, Inc & SANS Certified Instructor, Author, Course Lead*

***Chris Crowley** (@CCrowMontance), Certified Instructor, SANS Institute*

***Andrew Hoog** (@ahoog42), CEO & Co-Founder, NowSecure*

***Adrian Leong** (@SCheeky4n6Monkey), Research and Development Specialist & Blogger*

***Cindy Murphy** (@cindymurph), Madison (WI) Police Department*

10:30-11:00am

Networking Break and Vendor Expo (LOCATION: ABC PRE-FUNCTION)

Friday, June 24

11:00-11:30pm

(LOCATION: SALON AB)

Using Endpoint Telemetry to Accelerate the Baseline

As the first boots-on-ground in a hostile environment, establishing a baseline or normalcy is a critical but time-consuming task. Traditionally, this has been done by collecting system and network logs, correlating the two and then inferring what is "normal." The problem with this is that logs often lie or tell an incomplete truth, and while network metadata is reliable payloads are easily hidden from view.

The rise of endpoint-based data collection tools can either augment the above or be used in their place to very rapidly collect not only information about network nodes and users, but also detailed information about endpoint activity to include user behaviors, process relationships and behaviors, and how endpoints are interacting with both internal and external hosts.

We present a framework that includes a small number of primary data elements—executable files and the process-level events associated with both—and a similarly small number of attributes and/or rules related to each. The resultant data set can be used to very rapidly and accurately group and triage systems based on these attributes, confirming expected behaviors and allowing unexplainable behaviors to stand out. Most importantly, these groupings can be used as a baseline against which both past and future activity can be compared to detect introduction of new elements, evasion, or even extrication.

Keith McCammon *(@kwm), Co-Founder & VP of Detection Operations, Red Canary*

(LOCATION: SALON C)

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

Is your organization planning to use threat intelligence in incident response but you are struggling with where to start? Are your technology solutions and threat intelligence working together or violently conflicting? Are you getting the most that you can out of your threat intelligence?

77% of organizations report that establishing or improving threat intelligence capabilities is a priority. Ironically, 77% percent also report that excessive false positives from threat intelligence is a problem.

This talk covers how to select and implement a strategy that works in your specific case, avoiding common pitfalls, and developing meaningful metrics for measuring success. We will break down practical strategies for enabling threat intelligence to best support detection, validation, and the investigation of known and unknown threats. Attendees will walk away armed with the knowledge and confidence to evolve their detection and response capabilities.

Rebekah Brown *(@PDXbek), Threat Intelligence Lead, Rapid7*

11:35am-12:05pm

Who Watches the Smart Watches?

Wearable technology use has accelerated over the past 18 months, to the point of where even most fitness devices now have notification capabilities to allow users to use the device as an extension of their mobile phone. This talk will explore two mobile operating system-independent devices: a Pebble Time and Microsoft Band 2. The talk will highlight functionality and the data that is stored on the device, as well as data stored on the mobile phone with which the wearable technology is associated.

Brian Moran *(@brianjmoran), Digital Strategy Consultant, BriMor Labs*

Deleted Evidence: Fill in the Map to Luke Skywalker

This presentation will describe forensic artifacts that track activity on the NTFS file system, and how to leverage these artifacts during investigations when evidence has been deleted or partially stored in a BB-8. We will discuss artifacts such as the $UsnJrnl, INDX, Windows Defender Log, OBJECTS.DATA, and how to use these data artifacts to determine attacker activity, or find hidden Jedi temples.

David Pany *(@DavidPany), Consultant, FireEye*

Mary Singh *(@marycheese), Senior Consultant*

Friday, June 24

(LOCATION: SALON AB)

(LOCATION: SALON C)

12:05-1:15pm

LUNCH & LEARN

(LOCATION: SALON AB)

Presented by

ARBOR® NETWORKS

Out of the Sandbox: Investigating and Proving Threats in Minutes

***Jennifer Glenn**,*
Sr. Product Marketing Manager, Advanced Threats

Breach detection systems like sandboxes and IDS are powerful alerting mechanisms for security concerns. They are also nearly ubiquitous in their deployments across today's enterprise networks. While necessary and already present, these tools lack the necessary information for security teams to take action. Without context or background on attack alerts, these teams can't calculate risk to the business and therefore they do not have the justification to disrupt critical business systems to mitigate attack activity.

Join us for a lunch session to learn how Fortune 1000 organizations are using Arbor Spectrum to get the valuable context necessary to make remediation decisions. See how to thoroughly investigate and definitively prove attacks occurring in your network in just a matter of minutes.

LUNCH & LEARN

(LOCATION: SALON C)

Presented by

ENDGAME.

Left of Boom: Hunting Before a Known Incident

***Mark Dufresne**,*
Director of Malware Research & Threat Intelligence, Endgame

Adversaries compromise at will, penetrating today's signature and IOC dependent detection capabilities. Most incident responders are locked in a cycle of constant reaction to the fraction of activity that is known. Often, undetected attackers remain active in the network as reported incidents are remediated. A new approach is needed to break the cycle of reaction and eradicate the unknown.

An offense-based approach must be adopted. Hunting puts the defender on the offensive within their networks, allowing for rapid detection and remediation of threats. Adversary dwell time can be drastically reduced, reducing business impacts and recovery costs. The Endgame hunt platform enables instant protection, visibility, and precision response across your endpoints and automates detection of known and never before seen adversaries without relying on signatures.

This talk will cover:
- Description and benefits of hunt
- Challenges of hunting
- Solutions and hunting best practices

1:15-1:45pm

Hadoop Forensics

Nowadays it seems that everyone from businesses to product vendors are using Apache Hadoop to store critical data. Hadoop is regarded by many as the miracle solution to big data challenges and it's not uncommon to find Hadoop clusters storing petabytes of information which make it a target for cyber criminals. The world is adopting and supporting Apache Hadoop - so why hasn't the field of forensics? The sheer volume of data and distributed architecture of Hadoop frustrates traditional forensic approaches. Apache Hadoop is a challenge that investigators will continue to face on an increasing basis. Get ready and learn how to tackle Apache Hadoop, the elephant in the room! This session will outline techniques and tools that can be used to investigate incidents on Apache Hadoop, and reduce huge data sets into manageable artifacts that can be analyzed in support of a case.

***Kevvie Fowler** (@kevviefowler), National Leader, Cyber Response Services, KPMG Canada*

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*

(LOCATION: SALON AB)

(LOCATION: SALON C)

1:50-2:20pm

Rocking your Windows EventID with ELK Stack

We have thousands of possible windows events id, split into 9 categories and 50+ subcategories that logs all actions in a windows machine as login/logoff, process creation, modifications, packet filtering and so on. By default Windows only holds those events for a short period (depends on configurations) which makes some aspects forensics impossible. In our deployment, we used the ELK stack and some custom Python scripts in order to optimize data aggregation into a strucured index. This custom process generates revelant intelligence that can be used for historical analysis and telemetry of those millions of daily events.

In this presentation we will share how to configure your Windows Audit policy, ELK stack to process/archive all information and share some tools to analyze your data based on an infection demo and incident case sample.

Rodrigo Ribeiro Montoro *(@spookerlabs), Security Researcher, Clavis Security Brazil*

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 for 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*

2:20-2:50pm

Networking Break and Vendor Expo (LOCATION: ABC PRE-FUNCTION)

2:50-3:20pm

Dive into DSL: Digital Response Analysis with Elasticsearch

In this talk we will take a deep dive into the Elasticsearch DSL using python and how you can use it to go beyond the simple searches you may have been using in Kibana. We will demonstrate how Elasticsearch can be used to speed up and automate your DFIR investigations by grouping multiple queries of artifacts into a "signature of forensics" format to answer common investigator questions. In addition, this talk will explore the full power of elasticsearch's searching and aggregation capabilities that can be utilized with indexed artifacts as well as the visualization functionality of Kibana. Use cases and code samples from real world investigations will be presented showing how you tap into this functionality already built into your ELK stack!

Brian Marks *(@brianDFIR), Senior Associate, KPMG*

Andrea Sancho Silgado*, Associate, KPMG*

Incident Detection and Hunting at Scale: An Introduction to Osquery

Facebook released a host instrumentation framework called osquery as an open source project and it's all the rage. The tool allows you query vital operating system, file system, and network information across your whole fleet and is a critical tool in detecting anomalies, providing both ongoing detection and fast sweeping capability. Even more exciting is osquery is built specifically for OSX & Linux, platforms treated as second tier by most vendors.

It's not as simple as downloading and installing though; osquery is a framework for building robust host monitoring. We have each taken time to deploy osquery in our respective environments, on a variety of hosts, and want to share our experiences. We'll discuss deployment, configuration, and provide example queries for hunting badness in your environment. And we'll discuss other projects that integrate with osquery to build a comprehensive host monitoring system.

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

Kevin Thompson *(@bfist), Senior Incident Responder, Heroku*

Friday, June 24

3:25-3:55pm

(LOCATION: SALON AB)

stoQ'ing Your Splunk

stoQ is an open-source DFIR analysis framework that allows for plug and play automated analysis of threats into a datastore of their choice. When combined with a data exploration tool like Splunk, it allows analysts to simplify the repetitive analytic tasks (running yara signatures, running hashes against virustotal, XOR, ROT13, extracting links from emails, and much more) and quickly correlate against other data sources or threat intelligence offerings to better visualize the threats to their network. In this talk we will cover what stoQ is, how it works, and show a demonstration of how you can leverage it's capabilities with Splunk. We will also be releasing a free Splunk app that will allow anyone with Splunk to start leveraging stoQ today. Attendees will learn: how to streamline the analysis of malicious files and network traffic using a flexible open-source DFIR framework; how to view that data and use it in an incident; and how to install and configure the stoQ and Splunk instance for use when they get back to their own offices.

Ryan Kovar *(@meansec), Staff Security Strategist, Splunk*

Marcus LaFerrera *(@mlaferrera), Director of Development, PUNCH Cyber Analytics Group*

(LOCATION: SALON C)

Accurate Thinking: Analytic Pitfalls and How to Avoid Them

Proper forensic investigation requires more than log review and image examination. To provide useful information, analysis must be approached with an appropriate level of intellectual rigor. This talk examines specific methodologies drawn from fields as widely varied as mathematics and political science, such as falsification and compensation for cognitive bias. Attendees will learn how to apply several frameworks and techniques they can apply immediately to improve the accuracy and reliability of all types of analysis within their organizations.

Kyle Maxwell *(@kylemaxwell), Senior Researcher, Verisign iDefense*

4:00-4:30pm

Leveraging Cyber Threat Intelligence in an Active Cyber Defense (LOCATION: SALON C)

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.

Robert M. Lee *(@robertmlee), Author & Instructor, SANS Institute*

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

4:30pm

Closing Remarks and Wrap-Up (LOCATION: SALON C)

Rob Lee *(@robtlee), DFIR Lead, SANS Institute*

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.

@sansforensics **#DFIRSummit**

DFIR SUMMIT SPEAKER BIOGRAPHIES

Jared Atkinson

(@jaredcatkinson), Hunt Capability Lead, Veris Group's Adaptive Threat Division

Jared Atkinson is the hunt capability lead with Veris Group's adaptive threat division. Before working for Veris Group, Jared spent four years leading incident response missions for the U.S. Air Force Hunt Team, detecting and removing advanced persistent threats on Air Force and DoD networks. Passionate about PowerShell and the open-source community, Jared is the lead developer of the PowerForensics project, an open-source forensics framework for PowerShell, and maintains a DFIR-focused blog.

William Ballenthin

(@williballenthin), Reverse Engineer, FireEye

William Ballenthin is a reverse engineer on the FLARE team that enjoys tackling malware and developing forensic analysis techniques. Willi's favorite beer is La Chouffe.

Andrew Blaich, Ph.D.

(@ablaich), Lead Security Analyst, Bluebox Security

Andrew Blaich is the lead security analyst at Bluebox Security where he is focused on all things mobile. He holds a Ph.D. in Computer Science and Engineering from the University of Notre Dame in enterprise security and wireless network performance. Andrew has worked at both Samsung and Qualcomm Research on next generation access control, kernel security, and indoor location systems for mobile devices.

Matt Bromiley

Senior Consultant, Mandiant

Matt has over four years' experience in incident response, digital forensics, and network security monitoring. He recently joined the team at Mandiant, a FireEye company. His skills include disk, database, and network forensics, incident response/triage, and log analytics. Matt has helped organizations of all sizes with their forensic and IR needs, from local banks to large, multinational conglomerates. He also has a passion for Mac and Linux forensics, as well as building scalable analysis tools utilizing free and open-source software. Matt's passion for DFIR helps him explore new topics with hopes of addressing previously unanswered questions.

Rebekah Brown

(@PDXbek), Threat Intelligence Lead, Rapid7

Rebekah Brown is a former NSA network warfare analyst, U.S. Cyber Command training and exercise lead, and Marine Corps crypto-linguist who has helped develop threat intelligence programs at the federal, state, and local levels as well as in the private sector at a Fortune 500 company. Rebekah currently leads threat intelligence at Rapid7. She has an Associates in Mandarin, a B.A. in International Relations and is wrapping up a M.A in Homeland Security with a cybersecurity focus.

Dr. Brian Carrier

(@carrier4n6), VP, Digital Forensics, Basis Technology

Brian Carrier leads the digital forensics team at Basis Technology, which builds software for incident response, digital forensics, and custom mission needs. He is the author of the book *File System Forensic Analysis* and a developer of several open-source digital forensics analysis tools, including The Sleuth Kit and Autopsy. Brian has a Ph.D. in computer science from Purdue University and worked previously for @stake as a research scientist and the technical lead for their digital forensics lab and incident response team. Brian is the chair person for the Open Source Digital Forensics Conference (OSDFCon) and on the committees of many conferences, workshops, and technical working groups, including the annual DFRWS conference and the *Digital Investigation Journal*.

Jacob Christie

Consultant, Mandiant

Jacob Christie has two years' experience in digital forensics and incident response and a lifetime of involvement in IT. From humble desktop support roots, he has risen to perform roles such as a data analyst, network security monitoring analyst, and forensic analyst – sometimes all within the same day. After working in the Big 4 for a spell, Jacob recently joined Mandiant, a FireEye Company, where he is afforded the opportunity to focus exclusively on incident response at scale. His real passion is herding bits from Point A to Point B using anything within his grasp to help accomplish this task (Python, Ruby, BASH, Visual Basic, etc.) regardless of the source or destination (SQL, NoSQL, flat text, or a forensic image). Jacob has presented at numerous internal trainings, teaching colleagues about various DFIR topics including forensic timelining, data breach identification, and open-source forensic tools.

Chris Crowley

(@CCrowMontance), Certified Instructor, SANS Institute

Chris Crowley has 15 years of industry experience managing and securing networks. He currently works as an independent consultant in the Washington, DC area. His work experience includes penetration testing, computer network defense, incident response, and forensic analysis. Mr. Crowley is the course author for SANS MGT535: Incident Response Team Management and holds the GSEC, GCIA, GCIH (gold), GCFA, GPEN, GREM, GMOB, and CISSP certifications. His teaching experience includes SEC401, SEC503, SEC504, SEC560, SEC575, SEC580, FOR585, and MGT535; Apache web server administration and configuration; and shell programming. He was awarded the SANS 2009 Local Mentor-of-the-Year award.

Mari DeGrazia

(@maridegrazia), Director, Kroll Cyber Security

Mari DeGrazia is a director at Kroll Cyber Security, which provides incident response services on a global scale. Throughout her career in DFIR, Mari has investigated high-profile breach cases, worked civil and criminal cases, and provided testimony as an expert witness. Mari has a Bachelor's of Science in Computer Science from Hawaii Pacific University as well as various certificates related to digital forensics. She is currently pursuing her Masters of Science in Digital Forensics.

Sarah Edwards

(@iamevltwin), Mac Nerd, Parsons Corporation, SANS Institute

Sarah Edwards is a senior digital forensic analyst who has worked with various federal law enforcement agencies. She has performed a variety of investigations including computer intrusions, criminal, counter-intelligence, counter-narcotic, and counter-terrorism. Sarah'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 SANS FOR518: Mac Forensic Analysis.

Kevvie Fowler

(@kevviefowler), National Leader, Cyber Response Services, KPMG Canada

Kevvie Fowler is a partner and national cyber response leader for KPMG Canada and has over 19 years of IT security and forensics experience. Kevvie assists clients in identifying and protecting critical data and proactively preparing for, responding to, and recovering from incidents in a manner that minimizes impact and interruption to their business.

Shelly Giesbrecht

(@nerdiosity), Incident Responder, Cisco

Shelly Giesbrecht is living the dream as an incident responder for Cisco in Calgary, Alberta. In her spare time, Shelly is also a SANS Technology Institute MSISE student, and is currently GREM, GCFA, GFCE, GCIA, GCIH and GSEC certified. Shelly has been working in security operations since 2006 but learned her craft from the ground-up as a helpdesk analyst over 15 years ago. She enjoys imaging servers in candlelight, writing regex to relax, and her favorite registry key is AppCompatCache.

Andrew Hay

(@andrewsmhay), CISO, Data Gravity

Andrew Hay is the CISO at DataGravity where he advocates for the company's total information security needs and is responsible for the development and delivery of the company's comprehensive information security strategy. Prior to that, Andrew was the director of research at OpenDNS (acquired by Cisco) and was the director of Applied Security Research and chief evangelist at CloudPassage, Inc.

DFIR SUMMIT SPEAKER BIOGRAPHIES

Andrew Hoog

(@ahoog42), CEO & Co-Founder, NowSecure

Andrew Hoog is a mobile security researcher, expert witness, and the CEO and co-founder of NowSecure, an enterprise mobile security company. Hoog has one patent issued with two more pending and has authored two books on mobile forensics and security. When not breaking (or fixing) things, he enjoys great wine, running, and science fiction.

Mike Hracs

(@bumjubeo), Senior Consultant, Deloitte

Mike Hracs is currently working as a member of the Deloitte "Purple" team in Calgary, Alberta. He is a senior security operations analyst by day, and aids in pen testing or incident response when help is needed. Mike is currently GREM and GCFA certified, and has held many industry certifications throughout his career. Mike began his career in 2005 as a network engineer eventually making the shift to security, and it's been sunshine and lolly pops since then. Mike enjoys sweet talking pcaps by moonlight and listening to dial-up modems to relax. His favorite routing protocol is BGP.

Dave Hull

(@davehull), Product Engineer, Tanium

Dave Hull is a product engineer at Tanium. Prior to joining Tanium, he was the senior technical lead for security incident response for Microsoft Office 365 and a senior security software developer in Microsoft Azure. He has been a builder, a breaker, a DFIR practitioner, and researcher. He created Kansa, an open-source framework for security incident response in use in organizations around the world. Dave was a leading contributor to and managing editor of the award winning SANS Digital Forensics and Incident Response blog. He has spoken at various security conferences including the SANS DFIR Summit, Microsoft's Blue Hat, and SecTOR.

David Kovar

(@dckovar), Consultant

David Kovar was recently a cybersecurity and incident response leader for a major consulting firm. He shifted focus to disruptive technologies and is currently pursuing a Master's degree in International Affairs while consulting on UAVs. He runs a commercial UAV company that provides disaster response, precision agriculture, surveying and other aerial imaging services. He's also been an entrepreneur, ediscovery consultant, software engineer, search and rescue incident commander, executive protection agent, and lethal forensicator. He's collected images in China, rescued wayward Americans in Australia, fenced with APT actors from all over the world, and led a mission to Tajikistan to evaluate the emergency preparedness of many local agencies. Oh, and he flies sailplanes, fixed wings, helicopters, and drones.

Ryan Kovar

(@meansec), Staff Security Strategist, Splunk

Ryan Kovar worked at the Defense Advanced Research Projects Agency (DARPA) on a team dedicated to detecting and mitigating advanced threats. Ryan moved onto Splunk as a staff security strategist where he helps out with IR, hunting, and solving fun problems. Ryan despises printers.

Marcus LaFerrera

(@mlaferrera), Director of Development, PUNCH Cyber Analytics Group

Marcus LaFerrera worked at the Defense Advanced Research Projects Agency (DARPA) on a team dedicated to detecting and mitigating advanced threats. Marcus now works at PUNCH Cyber as the director of development and builds tools to simplify a security analyst's life.

Troy Larson

(@troyla), Microsoft Security Response Center/Azure

Troy Larson is a true leader in the field of digital forensics and engineer on the Microsoft Security Response Center's Azure team. Troy is focused on building and measuring forensic capabilities in the Azure platform, and executing advanced security investigations. Troy has been on the front lines of critical cases for Microsoft for over 10 years, creator of the Windows Forensic Environment toolkit and is a frequent speaker on Windows and Office incident response and forensics.Troy received his undergraduate and law degrees from the University of California at Berkeley, and has been working in the field of digital forensics since the late 90s.

Rob Lee

(@robtlee), DFIR Lead, SANS Institute

Rob is currently the curriculum lead and author for digital forensic and incident response training at the SANS Institute in addition to owning his own firm. Rob has more than 15 years of experience in computer forensics, vulnerability and exploit discovery, intrusion detection/prevention, and incident response.

Robert M. Lee

(@robertmlee), Author & Instructor, SANS Institute

Robert M. Lee is is a SANS Certified Instructor and the course author of SANS ICS515: Active Defense and Incident Response and the co-author of SANS FOR578: Cyber Threat Intelligence. Robert is also CEO of Dragos Security, a non-resident National Cyber Security Fellow at New America focusing on policy issues relating to the cybersecurity of critical infrastructure, and a PhD candidate at Kings College London. For his research and focus areas, he was named one of Passcode's Influencers and awarded EnergySec's 2015 Cyber Security Professional of the Year. Robert obtained his start in cybersecurity in the U.S. Air Force where he served as a cyber warfare operations officer. He has performed defense, intelligence, and attack missions in various government organizations including the establishment of a first-of-its-kind ICS/SCADA cyber threat intelligence and intrusion analysis mission.

Adrian Leong

(@Cheeky4n6Monkey), Research and Development Specialist & Blogger

Adrian Leong regularly enjoys the forensic analysis/research of computers, mobile devices, and other electronic evidence responsibly. He has several years of commercial software development experience and has also completed post-graduate training in the identification, preservation, analysis, and presentation of electronic evidence. He has completed several U.S.-based computer forensic internships in both the private and law enforcement sectors. His personal blog "Cheeky4n6monkey – Learning About Digital Forensics" (cheeky4n6monkey.blogspot.com) details his various forensic research projects and scripts in a light-hearted manner (typically accompanied by poorly drawn attempts at cartoon humor). In 2014, as part of an international group of current and ex-law enforcement forensic investigators, Adrian developed software tools to extract SMS, call history and contact data for a Windows Phone 8 device that was previously unsupported by existing forensic tools. Subsequently, he co-authored a SANS whitepaper on "Windows Phone 8 Forensic Artifacts" with the group.

Heather Mahalik

(@HeatherMahalik), Forensics Lead and PM, Oceans Edge, Inc, SANS Senior Instructor

Heather Mahalik is leading the forensic effort as a principal forensic scientist and team lead for Oceans Edge, Inc. Heather's extensive experience in digital forensics began in 2003. She is currently a senior instructor for the SANS Institute and is the course lead for FOR585: Advanced Smartphone Forensics.

Erick Mandt

Analyst, Air Force Office of Special Investigations (AFOSI)

Erick Mandt is a 25-year intelligence professional with broad experience in cyber counterintelligence, signals intelligence, intelligence analysis, and language analysis. He currently works as an analyst for the Air Force Office of Special Investigations (AFOSI) open-source intelligence team where he supports a full range of law enforcement and counterintelligence investigations and operations. Erick's research and analytical interests focus on integrating critical thinking and structured analysis processes into active cyber defense operations. Prior to joining AFOSI, Erick served 20 years as a cryptologic linguist for the U.S. Navy. He is proficient in Russian, Bulgarian, Serbian-Croatian, and Macedonian. Erick has an undergraduate degree in Russian Area Studies from Excelsior College and an MS in Cybersecurity from Utica College.

Brian Marks

(@brianDFIR), Senior Associate, KPMG

Brian is a senior associate with KPMG's forensic technology practice in Chicago, IL. Brian has over five years of experience in the information security industry having worked for a Department of Defense contractor before joining KPMG. There he gained experience in intrusion detection, incident response, log analysis, firewall administration, and operating system auditing and hardening. At KPMG, he specializes in providing digital response services including incident response, digital forensics, reverse engineering, and threat intelligence. He has provided these services for clients in many various industries including multinational businesses and Fortune Global 100 organizations.

DFIR SUMMIT SPEAKER BIOGRAPHIES

Kyle Maxwell

(@kylemaxwell), Senior Researcher, Verisign iDefense

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 and 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.

Keith McCammon

(@kwm), Co-Founder & VP of Detection Operations, Red Canary

Keith runs Red Canary's Security Operations Center and leads a group of expert analysts that monitor a continuous stream of potential attacks detected in Red Canary's customers' environments. Keith is a known expert in offensive cyber computing and defensive IT security from his background as director of commercial security at Kyrus and executive director of information technology at ManTech. Keith has taught and spoke extensively during his time as an information operations practitioner and technology executive within the intelligence community and defense industrial base.

Rodrigo Ribeiro Montoro

(@spookerlabs), Security Researcher, Clavis Security Brazil

Rodrigo "Sp0oKeR" Montoro has 15 years experience deploying open-source security software (firewalls, IDS, IPS, HIDS, log management) and hardening systems. Currently he is security researcher/SOC at Clavis. Before that he worked as a senior security administrator at Sucuri, Spiderlabs Researcher where he focuses on IDS/IPS signatures, modsecurity rules, and new detection researches. Author of two patented technologies involving discovery of malicious digital documents and analyzing malicious HTTP traffic. He is currently coordinator and snort evangelist for the Brazilian Snort Community. Rodrigo has spoken at a number of open-source and security conferences (OWASP AppSec, Toorcon (USA), H2HC (São Paulo and Mexico), SecTor (Canada), CNASI, SOURCE Boston & Seatle, ZonCon (Amazon Internal Conference), BSides (Las Vegas e São Paulo), and Blackhat Brazil) and serves as a coordinator for the creation of new snort rules, specifically for Brazilian malware.

Brian Moran

(@brianjmoran), Digital Strategy Consultant, BriMor Labs

Brian is a digital forensic analyst currently residing in the Baltimore, Maryland area. He has approximately 15 years of experience in the cybersecurity field, with 10 of those years focusing on digital forensics incident response (DFIR), both in the United States Air Force and the private sector. His initial exposure to the DFIR field occurred during a six month deployment to Mosul, Iraq in 2004-2005, when he served on a team that provided mobile device analytic information in support of tactical military operations. During his tenure in the Air Force, he has worked with numerous DoD entities and has been invited to speak and share information at several intelligence community events. After his military service ended, he entered the private sector and has worked globally on a wide range of cases. His favorite aspect of this DFIR field is that it is always changing and evolving, and every case has unique problems, questions, and solutions.

Austin Murphy

(@austinjmurphy), Director of Incident Response, CrowdStrike Services

Austin Murphy has over 10 years of computer network security experience in both private sector professional services as well as service in the U.S. Department of Defense. As the director of incident response, Austin leads a team of consultants responsible for delivering trusted advisory services to customers in need of assistance with critical security breaches. Prior to his career in consulting, Austin was a U.S. Air Force cyberspace operations officer where his primary focus was on developing tactics for the deployment of advanced computer network attack and defense capabilities.

Cindy Murphy

(@cindymurph), Madison (WI) Police Department

Cindy Murphy is a detective with 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. Det. Murphy 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 financial crimes, homicides, missing persons, computer intrusions, sexual assaults, child pornography, 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 also helped to develop the digital forensics certificate program at Madison Area Technical College. She is a certified SANS instructor and co-authored and teaches the Advanced Mobile Device Forensics (FOR585) course for the SANS Institute. She has presented internationally on various digital forensics topics and frequently writes articles and whitepapers for the community on various forensics-related topics. She earned her MSc in Forensic Computing and Cyber Crime Investigation through University College, Dublin where she completed her dissertation on the subject of victim-age estimation from child exploitation images. She is also involved with the Wisconsin Association of Computer Crimes Investigators (WACCI) where she served as president for the WACCI West Chapter, Chicago Electronic Crimes Task Force, High Tech Crime Consortium (HTCC), High Tech Crime Network (HTCN), and the International Guild of Knot Tyers (IGKT).

Ryan Nolette

Security Operations Lead, Carbon Black

Ryan Nolette, now the security operations lead, was a senior threat researcher and senior incident response consultant at Bit9 + Carbon Black and draws from more than a decade of intense and active incident response, threat research, and IT experience to add a unique perspective of technical expertise and strategic vision to Bit9 + Carbon Black. Prior to joining Bit9, Ryan was a technology risk analyst for Fidelity Investments, where he was the malware subject-matter expert for their cybersecurity group and focused on signature verification and placement for all IPS across the world, and provided non-signature-based malware detection and prevention through manual auditing and automated tools that he wrote. Ryan earned a bachelor's degree in Information Security and Forensics from the Rochester Institute of Technology and is constantly looking to learn new skills and technologies.

David Pany

(@DavidPany), Consultant, FireEye

David Pany is a consultant in Mandiant's Alexandria, Virginia office. His primary responsibilities include delivering incident response, digital forensic, compromise assessment, and product implementation engagements. Mr. Pany has experience performing forensics analysis using tools such as EnCase and FTK, along with open-source and mobile device forensics tools. He also develops python-based tools that process forensic artifacts and automate repetitive tasks. His scripts and tools have been integrated into the standard investigative methodologies for payment card breaches and Citrix environments. In addition to providing forensic consulting services, Mr. Pany also assisted in the development of FireEye's product implementation and integration services and methodologies.

Kevin Perlow

Senior Consultant, Booz Allen Hamilton

Kevin Perlow is an incident responder and forensic analyst at Booz Allen Hamilton. He is a senior consultant on Booz Allen's strategic innovation group predictive intelligence team where he investigates network intrusions, performs static and dynamic malware analysis, and assists in corporate security policy development for commercial organizations. He has over five years of experience in fields ranging from digital forensics and incident response to system administration. Mr. Perlow holds a Bachelor's of Science in Business Administration from Georgetown University.

DFIR SUMMIT SPEAKER BIOGRAPHIES

Hal Pomeranz

(@hal_pomeranz), Principal, Deer Run Associates; Fellow, SANS Institute

Hal Pomeranz is an independent digital forensic investigator who has consulted on cases ranging from intellectual property theft to employee sabotage, organized cybercrime, and malicious software infrastructures. He has worked with law enforcement agencies in the United States, Europe and global corporations. While equally at home in the Windows or Mac environment, Hal is recognized as an expert in the analysis of Linux and Unix systems. His research on EXT4 file system forensics provided a basis for the development of open-source forensic support for this file system. His EXT3 file recovery tools are used by investigators worldwide. Hal is a SANS faculty fellow, lethal forensicator, and is the creator of the SANS SEC506: Linux/Unix Security course (GCUX). He holds the GCFA and GREM certifications and teaches the related courses in the SANS forensics curriculum. He is a respected author and speaker at industry gatherings worldwide. Hal is a regular contributor to the SANS computer forensics blog and co-author of the Command Line Kung Fu blog.

Moritz Raabe

Reverse Engineer, FireEye

Moritz Raabe is a reverse engineer on the FireEye Labs Advanced Reverse Engineering (FLARE) team. He currently focuses on automating and simplifying malware analysis.

Scott J. 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 900-pound security gorillas, government security giants, boutiques, and financial services security firms, and has 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 third person.

Andy Rosen

President, ASR Data Acquisition & Analysis, LLC

Andrew Rosen has over 25 years of experience in data forensics, litigation support, software development and electronic discovery.

Andrea Sancho Silgado

Associate, KPMG

Andrea is an associate in the Chicago, IL office of KPMG U.S. Andrea has been a member of the forensic technology team since 2014, focusing on providing forensic services, threat intelligence, and incident response to clients, including Fortune 500 organizations. She also assists developers in the forensic technology team with coding between projects. Andrea is constantly aspiring to study and learn more in the DFIR field. In her first year as a professional, Andrea completed the certifications for GCFA and EnCase Certified Examiner. Prior to joining KPMG, she studied telecommunications engineering at Universidad Politecnica de Madrid, Spain. In the fifth year of her studies, she enrolled in a double degree program with Illinois Institute of Technology completing a Master of Science in Electrical Engineering in one year.

Mary Singh

(@marycheese), Senior Consultant, FireEye

Mary Singh is a senior consultant with Mandiant with 14 years of experience in the information security field. Mary specializes in forensic analysis, location of information exposure, and EnCase forensic software. She has experience in information operations, intrusion detection and incident response. While at Mandiant, Mary has investigated over 60 computer intrusions involving the federal government, defense industrial base, and Fortune 500 companies. Prior to joining Mandiant, Ms. Singh conducted attack prevention, detection, and vulnerability assessment in the U.S. Air Force and as a consultant with Booz Allen Hamilton. She shares her experience and knowledge by teaching and presenting at conferences. In 2015, she taught at Black Hat USA and conducted a webinar to share the latest methods to "find evil" with law enforcement, federal government, and industry.

Gene Stevens

Chief Technology Officer, ProtectWise

Gene Stevens drives the technology vision and architecture for ProtectWise. He has more than 20 years experience in software development, cloud computing, security as a service, and distributed systems. Prior to founding ProtectWise, Gene was the founder and CTO at TagLabs, a mobile tagging company. He was a principal software engineer at McAfee, cloud and content security and has also held engineering roles at MX Logic and GDX. Early in his career, Gene developed financial forecasting, market analysis, and service capacity planning software for Hewitt Associates (Aon).

Allen Swackhamer

Reverse Engineer, Target

Allen Swackhamer is a malware reverse engineer at Target Corporation. He is a member of the Cyber Fusion Center's Threat Defense Operations team where he reverse engineers malicious binaries to identify functionality, track crimeware, and APT campaigns, as well as aid incident responders in intrusion investigations. He has over seven years of experience in network security, intrusion detection, digital forensics, and incident response. Mr. Swackhamer holds two Bachelor's of Business Administration in Infrastructure Assurance and Information Systems from the University of Texas at San Antonio.

@sudsev

Network security analyst intern, malware hunter/analyst hobbyist, still at University studying computer and network security.

Kevin Thompson

(@bfist), Senior Incident Responder, Heroku

Kevin Thompson (@bfist) is a senior incident responder and chief snarkitecht at Heroku. He specializes in detecting and responding to security incidents by hunting for anomalies in an environment with tens of thousands of servers. Previously, Kevin was a security researcher and co-author of the *Verizon Data Breach Investigations Report* and is a core developer of several open-source software projects.

Dr. Paul Vixie

(@paulvixie), CEO, Farsight Security

Dr. Paul Vixie is the CEO of Farsight Security, Inc. In 2014, he was inducted into the Internet Hall of Fame for his work related to DNS. Previously, he served as president, chairman and founder of Internet Systems Consortium (ISC), as president of MAPS, PAIX, and MIBH, as CTO of Abovenet/MFN, and on the board of several for-profit and non-profit companies. He served on the ARIN board of trustees from 2005 to 2013, and as chairman in 2008 and 2009. Dr. Vixie is a founding member of ICANN Root Server System Advisory Committee (RSSAC) and ICANN Security and Stability Advisory Committee (SSAC). He has been contributing to Internet protocols and UNIX systems as a protocol designer and software architect since 1980. He is considered the primary author and technical architect of BIND 8. He earned his Ph.D. from Keio University for work related to DNS and DNSSEC.

Lee Whitfield

(@lee_whitfield), Director of Forensics, Digital Discovery

Lee Whitfield 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.

Eric Zimmerman

(@EricRZimmerman), Sr. Director, Kroll Cyber Security

Eric Zimmerman is a senior director at Kroll Cyber Security responsible for research and development as well as developing internal and external training for forensic examiners, law enforcement, and private industry. Prior to joining Kroll, Eric was a special agent with the FBI assigned to the cyber squad of the Salt Lake City field office. Eric has a degree in computer science and has developed many digital forensics related programs related to on scene triage, ShellBags, and online investigations. Eric was the first to be recognized as an X-Ways X-PERT and also holds EnCE, GCFW, GCFE, and GSEC certifications.