SANS DFIR

DIGITAL FORENSICS & INCIDENT RESPONSE SUMMIT

Program Guide

@sansforensics #DFIRSummit

Agenda

All Summit Sessions will be held in the Governors Ballroom (unless noted).

All approved presentations will be available online following the Summit at ***https://www.sans.org/summit-archives/dfir***

Thursday, June 7

7:00-9:00 am	**Registration & Coffee** (LOCATION: GOVERNORS BALLROOM FOYER)
9:00-9:15 am	***Welcome & Introductions*** ***Rob Lee*** *(@robtlee), DFIR Lead & Summit Co-Chair, SANS Institute* ***Phil Hagen*** *(@PhilHagen), Senior Instructor & Summit Co-Chair, SANS Institute; DFIR Strategist, Red Canary*
9:15-10:00 am	***Jury-Rigging Democracy: The Crazy, Sad Saga of Election Security in the U.S.*** When Congress passed the Help America Vote Act in 2002 in the wake of the Florida hanging chad debacle, it flung $3.9 billion at states to upgrade their antiquated election technology along with a deadline in which to spend it. States went on a frenzied buying spree, taking voting machine vendors at their word that new electronic voting machines would solve all of their election woes. But instead of solving the nation's election problems, the machines created a host of new ones – including providing an easy way for someone to rig elections without detection. Kim Zetter, who has been writing about the voting machine issue for 15 years – for *WIRED*, *Politico*, and the *New York Times* – will take us through the mad history of elections over the last decade and explain how it set the nation on course for the Russian election hacking scare we face today. ***Kim Zetter*** *(@KimZetter), Journalist, Author of Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*
10:05-10:40 am	***#DFIRFIT or Bust! - A Forensic Exploration of iOS Health Data*** We sit at computers all day long – day in and day out. We make excuses to not take care of ourselves. Sarah's excuse was her long DC commute and Heather's was not having enough time with her kids and travel. Since last year's DFIR Summit, Sarah's workplace location changed, affording her an extra hour a day; and Heather realized the baby weight wasn't going to disappear on its own. We promised ourselves that we would get out from behind our computers (and/or steering wheel/baby carrier) and start sweating! We now have a friendly competition to keep each other honest on how frequently we are sweating at the gym and not just over casework. As the Apple nerds that we are, we started logging lots of data into our iPhones using various apps, the Apple Watch and other gadgets. As the forensic data nerds that we are, we thought - how can this be used forensically? Recently in German courts the iOS Health data was used to determine if an accused person dragged a body down an embankment and walked back up. This activity was recorded as climbing stairs! This presentation will explore the various types of data and sources of data that is stored in the iOS Health databases. By extracting and analyzing this data, we can determine a person's pattern of life as well as any anomalies. When do they get up in the morning, when do they sleep? Where do they take their daily runs? How rigorous are their normal activities, what might have caused the data outliers during a specific time of interest in an investigation? ***Sarah Edwards*** *(@iamevltwin), Mac Nerd, SANS Institute, and Parsons Corporation* ***Heather Mahalik*** *(@heatherMahalik), Principal Forensic Scientist, ManTech; Senior Instructor, SANS Institute*
10:40-11:00 am	**Networking Break** (LOCATION: GOVERNORS BALLROOM FOYER)

Thursday, June 7

11:00-11:35 am	***Windows Forensics: Event Trace Logs*** Looking for a "new" Windows artifact that is currently being underutilized and contains a wealth of information? Event Tracing for Windows (ETW) and Event Trace Logs (ETL) may be your answer. There's nothing new about them, yet they can provide a wealth of information. Event Tracing for Windows was introduced in Windows 2000 and is still going strong in current versions of Windows. ETW is typically used for performance and debugging analysis by the Windows OS and by application developers. ETLs are ETW sessions that are stored to disk. They can be found in numerous locations on a Windows system and carry the extension ".etl." They can contain system configuration information, WiFi connection SSIDs and configuration, Process and Thread information, File and Disk IO, Sleep Session Studies, Boot and Shutdown information, and much more. This talk will cover what ETL files are and where you can expect to find them, how to decode ETL files, caveats associated with those files, and some interesting and forensically relevant data that ETL files can provide. ***Nicole Ibrahim*** *(@nicoleibrahim), Digital Forensics Expert, G-C Partners, LLC*
11:35 am-12:10 pm	***A Planned Methodology for Forensically Sound Incident Response in Microsoft's Office 365 Cloud Environment*** A planned methodology for developing and implementing a forensically sound incident response plan in Microsoft's Office 365 cloud environment must be thoroughly researched and re-evaluated over time as the system evolves, new features are introduced, and older capabilities are deprecated. This presentation will walk through the numerous forensic, incident response, and evidentiary aspects of Office 365. The presentation is based on two years' worth of collection of forensics and incident response data in Microsoft's Office 365 and Azure environments. It combines knowledge from more than a hundred Office 365 investigations, primarily centered around Business Email Compromise (BEC) and insider threat cases. ***Devon Ackerman*** *(@AboutDFIR), Associate Managing Director, Kroll Cyber Security*
12:10-1:30 pm	**Lunch & Learn Sessions**
	DomainTools Lunch and Learn (LOCATION: MEETING ROOM 406) DOMAINTOOLS® ***Advanced Power of the Pivot*** As the threat landscape continues to change, and with more advanced attackers than ever, security teams need all the help they can get to more effectively prevent, detect and respond to threats. Join Taylor Wilkes-Pierce to learn how to better profile adversaries, map their infrastructure and characterize suspicious domains with guided pivots, SSL certificates and historical WhoIs. ***Taylor Wilkes-Pierce,*** *Sales Engineer, DomainTools*
	Guidance Lunch and Learn (LOCATION: MEETING ROOM 400) GUIDANCE SOFTWARE ***Introduction to Efficient Digital Forensic Investigative Workflow*** This talk will focus on describing the attributes of "best-in-class" digital forensic hardware and software, and how to use them in combination to improve case efficiency. Due to the increasing number of devices per case and increasing data storage limits, it is more important than ever for investigators to have the right tools and features available in order to keep case backlogs to a minimum. ***Jeff Hedlesky,*** *Forensic Evangelist and* ***Harp Thukral,*** *Product Manager, OpenText*
1:30-2:05 pm	***Evidence Generation X*** Test evidence lies at the heart of our field. We need to be able to test our tools to make sure that they parse data correctly. New hires and students need to have their knowledge tested and challenged in a controlled environment. How do you create realistic, believable, and effective scenarios to test forensic evidence? After spending several months putting such a scenario together, the presenter will share his experience and insights, as well as the potential "gotchas," of evidence generation. ***Lee Whitfield****, Subject-Matter Expert, SANS Institute*

Thursday, June 7

2:05-2:40 pm	***Efficiently Summarizing Web Browsing Activity*** Reviewing web browsing activity is relevant in a wide variety of DFIR cases. With many users having multiple devices that may need to be analyzed, we need better ways to get answers quickly. This presentation will show how a synopsis of browsing activity can be a starting point before a deep-dive investigation and can help investigators decide whether a device is relevant to their case. We will also examine if a device is relevant to their case, and how this summary can provide quick answers to some common questions that are useful in communicating one's findings to a less technical audience. ***Ryan Benson*** *(@_RyanBenson), Senior Threat Researcher, Exabeam*
2:40-3:00 pm	**Networking Break** (LOCATION: GOVERNORS BALLROOM FOYER)
3:00-3:35 pm	***Mac_apt –The Smarter and Faster Approach to macOS Processing*** macOS forensics has not seen the kind of attention Windows gets. Few tools and documentation exist to specifically address macOS artifact processing needs, so we created the mac_apt - macOS Artifact Processing Tool, a Python, open-source, cross-platform, plugin-based framework with support for Apple File System and High Sierra. We'll show you how mac_apt can process complex artifacts and drastically cut down on manual processing time. We'll talk about mac_apt's design and investigator-friendly features. The presentation will also showcase some of our latest research into Mac artifacts that will eventually be released as mac_apt plugins. ***Yogesh Khatri*** *(@swiftforensics), Assistant Professor, Chaplain College*
3:35-4:10 pm	***Case Study: ModPOS vs. RawPOS – A Nerd's-Eye View of Two Malware Frameworks*** Although merchants and retailers have been implementing more secure technologies within their payment environments, such as Chip and PIN and Point to Point Encryption, they continue to be targeted by cyber criminals intent on stealing payment card data. Popular tools used by hackers in these types of breaches include memory-scraping malware such as RawPOS and ModPOS. This presentation will provide an overview of these two malware variants, exploring the similarities and differences between them. We'll also discuss forensic artifacts and analysis techniques useful in payment card breach investigations. Topics during this session will include an overview of payment card data breaches, comparing and contrasting RawPOS and ModPOS, RawPOS and ModPOS artifacts, and best practices for securing the environment. ***Brandon Nesbit****, Senior Managing Consultant, Kroll* ***Ron Dormido****, Director, Cyber Security and Investigations, Kroll*
4:10-6:15 pm	***Workshop: Practice How You Play: Incident Response War Game*** This exercise will lead the participants through a simulated major incident. The goal is to help participants: better understand the incident response process; better understand the constraints and needs which may arise during a large-scale incident, including communications, legal challenges, PR, complex trade-offs in completeness vs. response speed; experience incident response from the perspective of other stakeholders, including management and legal; gain better insight as to the capabilities, tactics and tools used in other companies to solve security incident related challenges. ***Matt Linton****, (@OxMatt), Chaos Specialist, Google* ***Francis Perron****,(@u269C), Program Manager – Incident Response, Google* ***Ryan Pittman****, Resident Agent-in-Charge, NASA Office of Inspector General's Computer Crimes Division*
7:00-9:00 pm	**DFIR Night Out in ATX!** (LOCATION: 213 W. 5TH STREET) Enjoy an evening of ping pong and networking with fellow attendees at SPiN Austin. *Sponsored by:* CYLANCE DOMAINTOOLS ExtraHop MAGNET FORENSICS

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 8

8:00-9:00 am	**Registration & Coffee** (LOCATION: GOVERNORS BALLROOM FOYER)
9:00-9:15 am	***Day 2 Overview and Opening Remarks*** ***Rob Lee*** *(@robtlee), DFIR Lead & Summit Co-Chair, SANS Institute* ***Phil Hagen*** *(@PhilHagen), Senior Instructor & Summit Co-Chair, SANS Institute; DFIR Strategist, Red Canary*
9:15-10:00 am	***Keynote: Living in the Shadow of the Shadow Brokers*** Most people know the Shadow Brokers leaked (supposedly) stolen NSA cyber tools, which lead to some of the most significant cyber security incidents of 2017. But in addition to targeting NSA, the Shadow Brokers have also targeted a few individuals in our community. Hear about the history of the Shadow Brokers and the implications of their actions for infosec and DFIR from one of the group's targets. Have something you absolutely wanted to know about this great spy vs. spy saga, but were afraid to ask? This is your chance! ***Jake Williams*** *(@MalwareJake), Senior Instructor, SANS Institute*
10:05-10:40 am	***A Process Is No One: Hunting for Token Manipulation*** Does your organization want to start threat hunting but is not certain how to begin? Most people start with collecting ALL THE DATA, but data means nothing if you're not able to analyze them properly. This talk begins with the often-overlooked first step of generating hunt hypotheses that can help guide targeted collection and analysis of forensic artifacts. We will demonstrate how to use the MITRE attack framework and our five-phase hypothesis generation process to develop actionable hunt processes that narrow the scope of your hunt operation and avoid "analysis paralysis." We will then walk through a detailed case study of detecting access token impersonation/manipulation from concept to technical execution by way of the hypothesis generation process. ***Jared Atkinson*** *(@jaredcatkinson), Adversary Detection Technical Lead, SpecterOps* ***Robert Winchester****, Adversary Detection Lead, SpecterOps*
10:40-11:10 am	**Networking Break & Vendor Expo** (LOCATION: GOVERNORS BALLROOM FOYER)
11:10-11:45 am	***$SignaturesAreDead = "Long Live RESILIENT Signatures"*** Signatures are dead, or so we're told. It's true that many items that are shared as Indicators of Compromise (file names/paths/sizes/hashes and network IPs/Domains) are no longer effective. These rigid indicators break at the first attempt at evasion. Creating resilient detections that stand up to attempted evasion by dedicated attackers and researchers is challenging but possible with the right tools, visibility, and methodical approach. As part of FireEye's Advanced Practices Team, we are tasked with creating resilient, high-fidelity detections that run across hundreds of environments and millions of endpoints. In this talk we will share insights on our processes and approaches to developing detection – including practical examples derived from real-world attacks – that you will be able to apply across many common and open-source security tools. ***Matthew Dunwoody*** *(@matthewdunwoody), Principal Applied Security Researcher, FireEye/Mandiant* ***Daniel Bohannon*** *(@danielhbohannon), Senior Applied Security Researcher, FireEye/Mandiant*

Friday, June 8

11:45 am-12:20 pm	***Finding and Decoding Malicious Powershell Scripts*** Malicious PowerShell scripts are becoming the tool of choice for attackers. Although sometimes referred to as "fileless malware", they can leave behind forensic artifacts for examiners to find. In this presentation, learn how to locate and identify activity of these malicious PowerShell scripts. Once located, these PowerShell scripts may contain several layers of obfuscation that need to be decoded. I will walk through how to decode them, as well as some light malware analysis on any embedded shellcode. I will also demonstrate how to use an open source python script to automate the process once you have discovered the MO of the attacker in your case. ***Mari DeGrazia*** *(@maridegrazia), Director of Incident Response, Kroll*
12:20-1:30 pm	**Networking Lunch** (LOCATION: GOVERNORS BALLROOM FOYER) Join us for a networking lunch sponsored by our solution-provider partners.
1:30-2:05 pm	***Logging, Monitoring, and Alerting in AWS (The TL;DR)*** With AWS' ever-increasing number services and ever-growing complexity, individuals and organizations are desperately seeking the "TL;DR" of what services are available to protect them from and respond to attacks, and how to best configure them for effective and efficient monitoring, alerting, and incident response. The first part of this presentation will walk the audience through the core services and capabilities that are critical to logging, monitoring, alerting, and responding to threats. The second part will walk the audience through specific monitoring and alerting configurations that the audience can immediately apply to their infrastructure to begin and/or improve their path toward securing their AWS infrastructure. Whether you're just starting out in AWS or have been using it for years, there is something for everyone to learn or brush up on in ensuring your org is best prepared to monitor for and respond to a compromise. ***Jonathon Poling*** *(@JPoForenso), Managing Principal Consultant, SecureWorks*
2:05-2:40 pm	***Things I Thought Were Ground Truth in Digital Forensics Until I Found Out I Was Totally Wrong – And What to Do About it Now*** In the field of digital forensics we go by a "rulebook" – a set of beliefs that we commonly hold as true. When I recently delved into the world of data recovery though, I found that we were mistaken about some really basic things, like that an SD card that reads all zeros in forensic tools is empty when in fact it can still contain hundreds of pictures, or that we're getting a "full" forensic image of a hard drive with forensic tools when in fact we aren't. This presentation covers the myths of digital forensics I always believed until data recovery techniques proved me wrong. ***Cindy Murphy*** *(@cindymurph), President, Gillware Digital Forensics*
2:40-3:15 pm	***Investigating Rebel Scum's Google Home Data*** After the devastating destruction of the Death Star, Imperial Officers Phill Moore and Courtney Webb were dispatched to Yavin IV to investigate the abandoned Rebel base. Located within the compound were devices that needed to be interrogated for any information about the recent destruction of the Empire's greatest infrastructure project, which cost taxpayers trillions and killed innumerable innocent government workers. A Google Home smart home assistant and an Android device were examined, and the findings will now be presented. Attendees will learn what data can be obtained from the Google Home App, the Google Home device itself, and connected cloud data, and how the Empire intends to bring these terrorists to justice. ***Phill Moore*** *(@phillmoore), Blogger, This Week in 4n6*
3:15-3:35 pm	**Networking Break & Vendor Expo** (LOCATION: GOVERNORS BALLROOM FOYER)

Friday, June 8

3:35-4:10 pm	***Every Step You Take: Application and Network Usage in Android*** Every step you take, every move you make, your device and the network are watching you! We will explore artifacts that demonstrate applications and network usage and how those data points can be used to track activity by a mobile device down to (at times) the millisecond. Our research and presentation will demonstrate and show practical ways to correlate data from the device with network data from a mobile device in order to tell the full story of what happens. The presentation will include case studies, and we'll also debut scripts that can be used to help you utilize these skills on your cases. ***Jessica Hyde*** *(@B1N2H3X) Director, Digital Forensics/Adjunct Professor, Magnet Forensics, George Mason University*
4:10-4:45 pm	***Automating Analysis with Multi-Model Avocados*** In every case you work on, someone is asking you to get answers faster but without introducing more human error. Depending on the case, there are "go to" artifacts that help us to quickly answer basic questions. As the questions get more complicated so can the analysis. Oftentimes, the need arises to correlate multiple artifacts to get a more accurate answer to a complex question. We can sometimes lose the macro focus when reviewing individual artifacts, missing how they all relate to each other to allow for a deeper and faster understanding of a system. This presentation will provide insight into the importance of tool output, and then look at methods and technologies for automated correlation of forensic artifacts to answer more complex questions. A demonstration will introduce you to one method that utilizes the multi-model database, ArangoDB, to correlate artifacts and produce reports of more complicated questions such as "What volume serial number does a shellbag entry relate to?", "What is the timeline of external device usage?", and "What executables are no longer on the system?" ***Matthew Seyer*** *(@forensic_matt), Consultant, G-C Partners, LLC*
4:45-5:20 pm	***DNSplice: A New Tool to Deal with Those Super Ugly Microsoft DNS Logs*** DNS logs can provide a wealth of information to an incident response investigation. Unfortunately, many organizations are not collecting DNS logs and do not have the operational capability to parse or analyze them. Additionally, Microsoft DNS logs, particularly those from Windows 2003–2008R2, are the ugly stepsisters of the log world. (Let's not pretend there aren't DNS servers out there still riding on those platforms!) So how do we efficiently parse these logs into a format we can easily analyze, as well as provide some basic analysis functions that any responder can use? Introducing DNSplice, a new tool to accurately parse Microsoft DNS logs for analysis in Excel (the OG of forensic analysis tools) or ingestion into other analysis platforms. Not only will DNSplice make sense of Microsoft DNS logs from Windows 2003 to 2016, but also allows you to apply your API key from various online threat engines to determine if a domain being requested is considered malicious. Additionally, DNSplice will provide base statistics including client IPs with most requests, domains by least and most frequency, and more! This talk is based on a graduate research paper written for the SANS Technology Institute's Master of Science in Information Security Engineering Program. ***Shelly Giesbrecht*** *(@nerdiosity), Team Lead, Incident Responder, Cisco*
5:20-5:45 pm	***Forensics 4cast Awards***
5:45 pm	***Closing Remarks*** ***Rob Lee*** *(@robtlee), DFIR Lead & Summit Co-Chair, SANS Institute* ***Phil Hagen*** *(@PhilHagen), Senior Instructor & Summit Co-Chair, SANS Institute; DFIR Strategist, Red Canary*