SANS DFIR

DIGITAL FORENSICS & INCIDENT RESPONSE

SUMMIT 2019

Program Guide

@sansforensics **#DFIRSummit**

Agenda

All Summit Sessions will be held in the Salon C/D/E (unless noted otherwise).

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

Thursday, July 25

7:00-9:00 am	**Registration & Coffee** (LOCATION: SALON A/B
9:00-9:15 am	***Welcome & Opening Remarks*** ***Phil Hagen*** *(@PhilHagen), Senior Instructor, SANS Institute* ***Rob Lee*** *(@robtlee), Fellow, SANS Institute*
9:15-10:00 am	***Keynote: From Tool Building to Scalable Automation*** There are many reasons to write forensics tools, from making it open source, to being free from a vendor for updates, to breaking reliance on APIs. But designing and building tools is not enough. It quickly becomes necessary to run multiple tools in a consistent and efficient manner. Once robust, dedicated tools exist for the most important artifacts, a means to coordinate and automate and run those tools across data is needed. Tools such as KAPE address this need and provide a means for end users to build collection and processing tool chains that makes sense for them. Conceptually, it is a short hop from consistent and efficient "processing tool chains" to scalable, automated processing. The key is reliability and efficacy of the processing tool chain, whether you are concerned with light-weight scans of tens of thousands of disks or more in-depth triage of scores of disks at a time. Tools such as Kape provide a means to simplify the development, testing, and implementation of forensics tasks for automation. Once the automation is reliable, scale is largely a matter of increasing the instances of where the automation runs. In this talk, Eric will explore the development and refinement process of EZ Tools and how KAPE can be used as the "glue" to tie things together. Troy will then provide real world examples of how these tools can and have been used for forensics at scale. ***Troy Larson****, Principal Security Architect, Microsoft* ***Eric Zimmerman*** *(@EricRZimmerman), Senior Director, Kroll Cybersecurity; Certified Instructor & Author, SANS Institute*
10:00-10:30 am	**Networking Break** (LOCATION: SALON A/B)

Thursday, July 25

10:30-11:05 am	***AmCache Investigation*** The AmCache is an artifact that stores metadata related to PE execution and program installation on Windows 7 and Server 2008 R2 and above. Frequently overlooked and understudied, this database is rarely fully exploited when doing incident response. Indeed, its correct interpretation is complex: a lot of special cases can occur that have to be taken into account when performing an analysis. However, the information collected by the AmCache is extremely useful, and the lack of awareness about this artifact makes it very valuable, since it is easily overlooked by attackers erasing their tracks. In this talk we will present the basics of the AmCache and then highlight the relevance of its use through various examples. In one example, an attacker has deleted the malware used to infect a computer, but the AmCache analysis helps the analyst retrieve the hash of the malware. In another example, an attacker has installed a vulnerable driver on a computer and AmCache can help prove this installation. The rest of the examples will focus on what AmCache can bring in more recent versions of Windows 10. This presentation is a follow-up on Blanche Lagny's research on AmCache, which can be accessed at www.ssi.gouv.fr/uploads/2019/01/anssi-coriin_2019-analysis_amcache.pdf. ***Blanche Lagny*** *(@moustik01), Digital Forensic Investigator@ANSSI_FR ANSSI*
11:10-11:45 am	***They See Us Rollin'; They Hatin': Forensics of iOS CarPlay and Android Auto*** Vehicle forensics is still a niche investigative area. It can be difficult to get access to the car, but mobile forensics is still being done every day. More vehicles are coming with iOS CarPlay and Android Auto than ever before. These services allow for anyone to quickly connect their phone and interact with apps on it. What artifacts does this create? Can we tell if users were driving distracted or using "hands-free" services? Do app artifacts such as mapping or messaging look different when used via these services than when they are used on the phones themselves? Does it matter if the user connects via Bluetooth or USB? In this presentation, we will discuss the artifacts left behind on mobile devices and any outlier artifacts. The goal is to determine if there is a standard behavior for connected devices so that you don't have to rent a similar car and connect a device for testing every time CarPlay and Android Auto appear in an investigation. ***Sarah Edwards*** *(@iamevltwin), Forensic Specialist, Parsons; Certified Instructor and Author of SANS FOR518: Mac Forensic Analysis, SANS Institute* ***Heather Mahalik*** *(@HeatherMahalik), Senior Director of Digital Intelligence, Cellebrite; Senior Instructor and Course Lead for FOR585: Advanced Smartphone Forensics, SANS Institute*
11:45 am – 12:00 pm	**Select and find your Lunch & Learn session.**

Thursday, July 25

12:00-1:20 pm

Lunch & Learn Sessions

After the Attack: Automate and Accelerate Your Post-Breach Response
(LOCATION: ROOM 400)

AccessData
A Pioneer in Digital Investigations Since 1987

When dealing with a data breach, minutes could mean the difference between stopping the threat or losing critical company data, revenue and customer trust. The new RESTful API from AccessData enables security teams to seamlessly integrate a company's SIEM platform with its forensic investigation platform, automating collections and dramatically speeding incident response by initiating the immediate preservation of evidence crucial in an investigation. During this presentation, you'll learn how organizations can effectively use automation and forensic analysis solutions to:

- Reduce post-breach analysis time by up to 40 minutes per incident
- Initiate a collection job at a designated endpoint within moments of an attack, immediately preserving data relating to the root cause of the breach
- Reduce the risk and expense of passing data between platforms
- And more

***Shon Harris**, Senior Cloud Engineer*

Incident Response and Investigation Using Shadow Search: A Real-World Example
(LOCATION: ROOM 415 A/B)

digital shadows_

There is no shortage of challenges for today's security analysts – when time is short and the pressure is on – reducing the amount of research required by having all relevant data in one place can make all the difference. This presentation will demonstrate a real-world example of how Shadow Search can help your team in an incident response situation. With instant access to threat data and the open, deep, and dark web when you need it, Shadow Search helps support your incident response with actionable information – rich results with associated observables – allowing analysts to make faster searches and more rapid decisions based on the results.

***Walter Tierney**, Director of Client Engineering*

Domain and DNS-Based Adversarial Threat Intelligence in the SOC/CSIRT
(LOCATION: 412)

DOMAINTOOLS

While external threat intel feeds can be great, most organizations also are sitting on a potential gold mine of useful forensic data. However, making practical and impactful use of the data can be tricky and it doesn't have to be. Corin Imai of DomainTools will demonstrate straightforward methods and data sources to strengthen your security posture without breaking the bank, using real-world examples of DNS-based intelligence that exposed attack campaign infrastructure.

***Corin Imai**, Senior Security Advisor*

Chopping Down a Dense Forest of Teleme-Trees: Making Telemetry Work for You
(LOCATION: ROOM 417 A/B)

ENDGAME.

Security operations teams are increasingly becoming more effective as tools continue to evolve and telemetry increases. Timely interpretation of the data to make actionable decisions is paramount to maximizing successful response and remediation.

However, as telemetry increases, analysts can be overwhelmed and may struggle to interpret signals in the noise. Tuning detections to specific environments reduces problems such as false positives and allows more time to be spent on high-confidence information. Organizations that can effectively baseline their environment, pivot through the relevant telemetry, and incorporate automated workflows, will be more successful at monitoring and defending their environment and assets.

In this lunch and learn, we'll show how to take advantage of Endgame's recently released Reflex™ technology, along with the publicly released Event Query Language (EQL) to alert, hunt, and even respond to activity within your environment.

***Justin Ibarra,** Security Researcher*

Thursday, July 25

1:20-2:05 pm	***MacOS DS_Stores: Like Shellbags but for Macs*** Wouldn't it be nice if there were a Windows shellbags equivalent for MacOS? Turns out there is. Sort of. .DS_Store or Desktop Services Store files are hidden files used by the GUI Finder app which store information related to Finder windows that the user had opened at some point in time. The main purpose of these files is to remember the view settings for each folder the user viewed (like Windows shellbags). They do not exist by default, so their existence in a folder indicates that the folder was opened using Finder. They can be found in any folder on any OS that a Mac user has read/write access to including local drives, shared folders, and attached external devices. This talk will cover what .DS_Store files are, how to parse them, caveats associated with them, and what forensically relevant data they provide. ***Nicole Ibrahim*** *(@nicoleibrahim), Sr. Associate – Cyber Response, KPMG*
2:10-2:45 pm	***Finding Evil in Windows 10 Compressed Memory*** Up until August 2013, a complete Windows memory analysis only required forensic tools to parse physical memory and fill in any missing gaps from the pagefile. In Windows 8.1 Microsoft upended this paradigm with the introduction of memory compression. Pages that had been previously located in a pagefile on disk were now being stored in an undocumented location. As a result, the introduction of compressed memory has led to incomplete memory inspection on major operating systems. To enable a more complete memory analysis on Windows 10, FireEye's FLARE team has analyzed the operating system's memory manager. This presentation discusses the application of that research in finding malware from real investigations that had previously been inaccessible in memory snapshots. The presentation coincides with the release of FireEye's Win10 memory decompression plug-ins for Volatility & Rekall. Attendees can expect to gain an understanding of the issues faced by current forensic utilities; the general algorithm used to locate and decompress pages; and the means to leverage this research in practice via open-source software. An example forensic analysis/investigation of a Windows 10 memory image will demonstrate the additional capabilities the new solutions provide compared to existing tools. ***Omar Sardar*** *(@osardar1), Reverse Engineer, FireEye (FLARE)* ***Blaine Stancill*** *(@MalwareMechanic), Reverse Engineer, FireEye (FLARE)*
2:50-3:25 pm	***The DFIR Practitioner's Guide to the Research and Development Process*** Many practitioners, especially those not from academic backgrounds, may be intimidated by the idea of performing novel research in the field of Digital Forensics and Incident Response (DFIR). Much of this hesitation may stem from these practitioners not being familiar with the research & development (R&D) process. In other instances, practitioners may overestimate the amount of formal training that is required to produce solid, actionable results. Many of the skills that make a qualified DFIR practitioner are also shared by the best researchers in the field, with reverse-engineering, problem-solving, critical analysis, and attention to detail being among the most important. This talk will introduce the DFIR practitioner to the R&D process through a step-by-step approach to answering real-world open digital forensic questions. The hope is that, after attending this talk, practitioners will be interested in becoming more involved in the research community. ***Dr. Joe T. Sylve*** *(@jtsylve), Director of Research & Development, BlackBag Technologies*
3:25-3:50 pm	**Networking Break** (LOCATION: SALON A/B)

Thursday, July 25

3:50-4:25 pm	***Live Response with Ansible*** Jumping almost blindly into a compromised network can be challenging when you don't have standard security tooling available. This presentation reviews how ansible, a open-source configuration management tool, was used to perform DFIR at a small company we acquired. Like many small businesses, and even some very large ones, the environment was lacking meaningful security infrastructure or tooling. The gotcha - 1,000's of Linux servers in multiple colo's completely separated from from the corporate network. This presentation provides an overview of ansible & how it was used for ad-hoc, scalable DFIR including identification of compromised hosts, searching for IOC's and performing remediation with nothing but a single laptop and some creativity. This talk will add another tool to the arsenal of those who don't readily have corporate security tooling available on a moment's notice. ***Brian Olson*** *(@BrianOlsonSec), Sr. Manager, Technical Management, Verizon Media*
4:25-6:15 pm	***Workshop: Practice How You Play: Incident Response War Game*** Experience incident response (IR) through the perspective of multiple stakeholders. This exercise will lead participants through a simulated major incident. The goal is to help participants better understand the IR process and the constraints and needs which may arise during a large-scale incident. The war game will stress-test communications skills, legal challenges, PR, complex trade-offs in completeness vs response speed and rapid triage / forensics skills. Format is a tabletop exercise in teams; laptops are highly encouraged. ***Matt Linton*** *(@0xMatt), Chaos Specialist, Google* ***Adam Nichols*** *(adamjnichols@), Security Engineer, Google* ***Francis Perron*** *(@u269C), Program Manager – Incident Response, Google* ***Heather Smith*** *(@litmoose), Adjunct Professor, Richland College, Senior DFIR Professional, Cylance*
7:00-9:00 pm	**Summit Night Out in Austin** **SPiN Austin | www.wearespin.com** **213 West 5th Street | Austin, TX 78701 | 512-351-7110** Join us for food, drinks, networking and ping pong!

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, July 26

7:00-9:00 am	**Coffee & Tea** (LOCATION: GOVERNOR'S BALLROOM FOYER)
9:00-9:45 am	***Distributed Evidence Collection and Analysis with Velociraptor: Fast, Surgical, at Scale...and Free!*** Having the ability to rapidly collect and examine artifacts across a network is a game changer for any Digital Forensics and Incident Response (DFIR) team. It provides unprecedented visibility into the state of the endpoint and the ability to tailor responses as the investigation evolves. Having this capability in an open-source tool that allows for truly surgical collection – at speed, at scale and free – is a triple bonus. In this talk, we'll present case studies from the Klein & Co. DFIR team on deploying and using Velociraptor in support of DFIR engagements for clients. Despite its young age, Velociraptor builds on the base of Grr (for which Mike Cohen was a lead developer) to feature some outstanding capabilities. Velociraptor introduces a powerful query language (VQL) to flexibly define artifacts to collect and hunt endpoints at scale and without needing to push new client code. This approach allows for truly versatile and rapid response, as investigators are able to adapt queries quickly in response to shifting threats and new information gained through the investigation. We will explore how the Klein & Co. team has used this capability to forensically acquire critical evidence in a range of cases, from investigating the extent of a compromise to performing internal company investigations and carrying out ongoing operational security assessments of client networks – all without affecting endpoint performance. We'll also cover some of the custom endpoint monitoring rules implemented to collect high-value event data in real time, using custom automated response configuration to immediately respond to endpoint events as they occur. In addition to immediate response, we can also query these historical data at a later time to detect past compromise using newly discovered evidence. ***Mike Cohen**, Developer, Velocidex Innovations* ***Nick Klein** (@kleinco), Director, Klein & Co.; Certified Instructor, SANS Institute*
9:50-10:25 am	***Finding Badness: Using Moloch for DFIR*** In this presentation, we will share how the Verizon Media Paranoids use Moloch (molo.ch), Verizon Media's open-source full packet capture system, to perform Digital Forensics and incident Response (DFIR). Moloch augments current security infrastructure by storing and indexing network traffic in standard PCAP format, while also providing fast-indexed access. We will explore several scenarios, including how Verizon Media uses Moloch internally in day-to-day investigations; how Moloch allowed Verizon Media to view the modification to go-pear.phar and build a timeline around its exploitation; how to use Moloch for proactive hunting of badness; how to use Moloch for sustained collection for long-term investigations; and how to correlate Moloch with other data sources such as Suricata, WISE, and others. ***Elyse Rinne**, Software Engineer, Verizon Media* ***Andy Wick**, Senior Principal Architect, Verizon Media*
10:25-10:55 am	**Networking Break** (LOCATION: SALON A/B)

Friday, July 26

11:00-11:35 am	***Pipeline Incident Response*** A customer calls you to investigate a breach in its Industrial Control System (ICS) environment. What can you do? Will your standard processes work? How and why? What questions should you ask? Can you really help at all? Yes, you can help. This presentation will go through the similarities and differences of performing digital forensics and incident response on a SCADA system. It will cover what to ask beforehand to align with your current processes, the tools you will and won't need, and tips for effectively communicating with field staff. ***Terry Freestone*** *(@Smoky_D_Bear), Senior Cybersecurity Specialist, Gibson Energy*
11:40 am – 12:15 pm	***Forensic Investigation of Emails Altered on the Server*** Emails on a cloud email server are often just as vulnerable to tampering as local messages. With a few clicks, an end user can replace the original message on the email server with an altered copy. What can investigators do to detect red flags and authenticate messages acquired from servers? In this session, we'll discuss what data points you need to collect from an email server to authenticate emails, why you should consider preserving emails from multiple sources, and how you can be more confident in your findings by combining server metadata with the information found within the message. ***Arman Gungor*** *(@ArmanGungor), CEO, Metaspike*
12:15-1:25 pm	**Lunch** (LOCATION: SALON A/B)
1:30-2:05 pm	***Tracking Traces of Deleted Applications*** On today's modern smartphones, evidence of absence doesn't always mean a complete absence of evidence. Even though users may delete third-party applications from their iOS and Android devices, there may still be lot of trace evidence points left behind to show that artifacts existed on the device at one time. This talk will discuss ways to track applications that may have been installed previously, and how and when they were used. Artifacts including Google Play searches, installation logs, network connection logs, and usage statistics will be used to timeline the events of applications, even if they are no longer on the device. For both modern versions of iOS and Android operating systems, we'll detail ways to track application usage on a device even when the application has been removed. Insights into how this information can provide unexpected leads into your cases will also be discussed. ***Alexis Brignoni*** *(@AlexisBrignoni), Researcher, Magnet Forensics* ***Christopher Vance*** *(@cscottvance), Manager, Magnet Forensics*
2:10-2:45 pm	***Shedding Light on the macOS Spotlight Desktop Search Service*** The macOS Spotlight desktop search system contains an index of metadata for files and folders on a system. While some of the data it contains duplicate filesystem and exif metadata and their extended attributes, there is also a gold mine of metadata that is unique to this store, including things like use counts and dates for files and folders that can go back years. However, exactly what there is and how to access the data is largely unexplored by the forensics community. In the last year or so forensics tools have surfaced that can parse the Spotlight metadata store, but there are still tons of unanswered questions about what artifacts can be found, where, and how. In addition to reviewing the basics, this session will address a number of specific topics such as recovering deleted metadata stores, what can be done with the iOS version of the Spotlight store, and what data can be found on removable drives that have hopped from machine to machine. These new techniques will better arm investigators to get to actionable data quickly. ***Dr. Vico Marziale*** *(@vicomarziale), Senior Digital Forensics Researcher, BlackBag Technologies*
2:50-3:20 pm	**Networking Break** (LOCATION: SALON A/B)

Friday, July 26

3:30-4:15 pm	***Live Debates*** This fast-paced and spontaneous session will pit forensicator against forensicator to take on hot topics in digital forensics, incident response, and even a little bit of pop culture. *Moderator:* ***Mari DeGrazia*** *(@MariDeGrazia), Senior Vice President, Cyber Risk;* *Instructor, SANS Institute*
4:15-5:00 pm	***Forensic 4cast Awards*** The community has voted! Find out who's been named "Digital Forensicator of the Year," and which books, blogs, and resources your peers chose in this year's awards. ***Lee Whitfield****, Founder, Forensic 4cast*

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.