SANS DFIR
DIGITAL FORENSICS & INCIDENT RESPONSE
SUMMIT & TRAINING
SUMMIT: JUL 25 - 26 | TRAINING: JUL 27 - AUG 1
AUSTIN, TX
LEARN MORE

Thursday, July 25	
9:00-9:15 am	*Opening Remarks* **Phil Hagen @PhilHagen, Senior Instructor, SANS Institute** **Rob Lee @robtlee, Fellow, SANS Institute**
9:15-10:00 am	*Keynote*
10:00-10:30 am	**Networking Break**
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 https://www.ssi.gouv.fr/uploads/2019/01/anssi-coriin_2019-analysis_amcache.pdf. **Blanche Lagny @moustik01, Digital Forensic Investigator@ANSSI_FR ANSSI**
11:05-11:40 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**, Director, Forensic Engineering, ManTech; Senior Instructor and Course Lead for** FOR585: Advanced Smartphone Forensics, SANS Institute
11:40 am- 12:15 pm	**MOICE Sandboxing Behavior** Microsoft Office Isolated Conversion Environment (MOICE) has not been documented since 2007, and OICE folders as they exist today, with copies of documents from outside of trusted zones, are completely undocumented. This talk explores when these files are created and what it means to find documents in these locations. **Lodrina Cherne @hexplates, Security Analyst, Cybereason**
12:15-1:30 pm	**Lunch**
1:30-2:05 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, Digital Forensics Expert, G-C Partners**
2:05-2:40 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 @osardar86, Reverse Engineer, FireEye (FLARE)** • **Blaine Stancill @MalwareMechanic, Reverse Engineer, FireEye (FLARE)**
2:40-3:15 pm	**The DFIR Practitioner's Guide to the Research & 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**
3:15-3:45 pm	**Networking Break**
3:45-4:20 pm	*Talk to be announced*
4:20-6:15 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** ● **Nik Roby trickynik@, Security Engineer, Google**
7:00 pm	*Summit Night Out in Austin*

Friday, July 26	
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**
9:45-10:15 am	**Networking Break**
10:15-10:50 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**

10:50-11:25 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**
11:25 am-noon	**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 @AmanGungor, CEO, Metaspike**
Noon-1:15 pm	**Lunch**
1:15-2:15 pm	*Live Debates* **Matt Bromiley @mbromileyDFIR, Certified Instructor, SANS Institute**
2:15-2:50 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**
3:20-3:55 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**
3:55-4:30 pm	*Talk to be announced*
4:30-5:05 pm	*Forensic 4cast Awards* Nominations are open through May 14th.