Program Guide

SANS DFIR

DIGITAL FORENSICS & INCIDENT RESPONSE SUMMIT

AUSTIN, TX | JUNE 22-23

@sansforensics

#DFIRSummit

Agenda

All Summit Sessions will be held in Salon ABC (unless noted).

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

Thursday, June 22	
8:00-9:00am	**Registration & Coffee** (LOCATION: GOVERNOR'S BALLROOM PRE-FUNCTION)
9:00-9:15am	***Welcome & Introductions*** ***Phil Hagen*** *(@PhilHagen), Certified Instructor & Summit Co-Chair, SANS Institute & DFIR Strategist, Red Canary* ***Rob Lee*** *(@robtlee), DFIR Lead & Summit Co-Chair, SANS Institute*
9:15-10:00am	***The Secret History of Cyber War*** Author and journalist Fred Kaplan provides historical, political, and strategic context to the problems of cyber security and cyber conflict, exploring the origins of hacking, the spread of cyberspace as a domain of combat, and why this is a never-ending war, but how it might be better managed. ***Fred Kaplan*** *(@fmkaplan), National Security Columnist, Slate & Author, "Dark Territory: The History of Cyber War"*
10:00-10:35am	***The Cider Press: Extracting Forensic Artifacts from Apple Continuity*** Apple Continuity allows us to move between our devices without disruption in activity. Just think of the ultimate handoff where you can start browsing the Internet on your iPhone, continue on your Mac without the hassle of having to type a search a second time. Essentially, your devices work together enabling you to do less. Imagine how this looks on a Mac, iPhone or Apple Watch. What will the forensic artifacts look like? Will you be able to tell which device the user conducted an activity on? What if it makes or breaks your investigation? ***Sarah Edwards*** *(@iamevltwin), Mobile Forensic Engineer, Parsons & Certified Instructor, SANS Institute* ***Heather Mahalik*** *(@heatherMahalik), Principal Forensic Scientist, ManTech & Senior Instructor, SANS Institute*
10:35-11:05am	**Networking Break & Vendor Expo** (LOCATION: GOVERNOR'S BALLROOM PRE-FUNCTION)

Thursday, June 22

11:05-11:40am	***The Forensics of Plagiarism: A Case Study in Cheating*** From time to time, and for a variety of reasons, students will engage in the act of plagiarism. Whether it is intentional or through ignorance, plagiarism is the act of taking another person's work and using it without permission or proper credit. Regardless of intent, plagiarism is cheating, and when it occurs, it is often the onus of the educator to prove the case. The purpose of this presentation is to provide instructors with the knowledge and means of gathering proof necessary to defend accusations of plagiarism and cheating. To this end, a case study will be used to demonstrate these tools and techniques. The following account is based on real events. The names have been changed to protect the guilty, but the events occurred as described. ***Tim Ball**, PhD, Southern Utah University*
11:40am - 12:15pm	***Mac Forensics: Looking into the Past with FSEvents*** Have you even wished that you could turn back time and see file and folder events that occurred in the past on a Mac computer and even an iPhone? Good news. You can! FSEvents or File System Events are log files created by OS X and iOS that contain historical events related to file creations, deletions, renames and more. Learn how to parse and interpret the data contained within these logs to glean information about files that previously existed on a system but have since been deleted, original names of files that have been renamed, mount events, websites visited, files sent to the Trash, and much more. Understand how FSEvents work, its caveats and limitations, and how you can use them to enhance you investigation and tap into an invaluable resource that may become one of your primary artifacts when conducting Mac forensics. ***Nicole Ibrahim** (@nicoleibrahim), Digital Forensics Expert & Researcher, G-C Partners, LLC*
12:15-1:30pm	**Networking Luncheon** (LOCATION: GOVERNOR'S BALLROOM PRE-FUNCTION)
1:30-2:05pm	***Google Drive Forensics*** This talk will cover the applicable features of Google Drive and GSuite including the administrator console, reports, API's, host side logs, and more importantly the things that are less documented that are of forensic value. We did the troubleshooting, Googling, and frantic support calls/bug reports for you. Come hear anecdotes from real cases including: "that time I was super admin," "that time we couldn't export revisions on Slides," "that time we had to correlate activity to deleted users" and "that time the guy didn't really download the thing." Finally, I'll use (and release!) code to demonstrate authentication, JSON API return structure, and differences between API versions. ***Ashley Holtz** (@thec0dem0nkey), Senior Services Engineer, CrowdStrike*

Thursday, June 22

2:10-2:45pm	***Your Eyes Can Deceive You: Implications of Firmware Trickery in Metamorphic Hard Drives*** What if I told you that you could be missing Terabytes of data from your investigations? This presentation will explain how, through the manipulation of the Firmware of a Hard Drive, a significant amount of data could be made beyond reach to an investigator/user, as well as being inaccessible to any traditional detection or security measures. Conventional digital-forensic tools and even data-recovery tools are not able to detect the manipulation, as this method goes far beyond changing HPA and DCO values that are usually detected. This presentation will cover some of the implications to digital forensics and incident response if such techniques were being utilized. Public disclosure of techniques by certain three-letter agencies has drawn public attention to this potential method of hiding data. This talk will explain how this type of manipulation has been possible for a number of years, as well as how it is possible to be achieved without the need for expensive tools or extensive research and reverse engineering. As with other hacking techniques, this can be achieved for the cost of parts and using freely available software. A number of difficulties with detecting and exposing this manipulation will be presented, as well as exploring the likelihood of its existence. If all this wasn't scary enough, a perfect storm scenario will demonstrate how to make a perfect metamorphic hard drive that would trick even the most keen-eyed investigator, including the presenter. On a happier note, ideas for further research and possible solutions will also be explored. ***Courtney Webb**, Team Leader, Electronic Evidence, New South Wales Police Force*
2:45-3:15pm	**Networking Break & Vendor Expo** (LOCATION: GOVERNOR'S BALLROOM PRE-FUNCTION)
3:15-3:50pm	***Boot What? Why Tech Invented by IBM in 1983 is Still Relevant Today*** Starting in Windows 8, Microsoft introduced UEFI and Secure Boot to help ensure that the computer boots using only software that is trusted by the manufacturer. If malware can load into memory prior to the execution of the operating system, it can bypass a number of the security controls of the operating system. Although the transition of most organizations to Windows 10 is planned and has started for some, the vast majority of enterprise PCs and servers (97.5% in FireEye's experience as of December 2016) still run pre-Windows 8 operating systems that do not have UEFI and/or Secure Boot. These older operating systems leverage legacy technologies such as a non-UEFI BIOS, a Master Boot Record (MBR), and a Volume Boot Record (VBR) to load the operating system – each of which can be easily modified to load malicious code. While there has been a significant amount of prior work discussing MBR or VBR bootkits (e.g. TDL4, Carberp, KINS, Necurs, Rovnix) we are still finding new attack methods and discovering new ways to detect MBR and VBR modifications. What techniques can incident responders use to investigate intrusions that leverage bootkits – both on individual systems and at scale? Are there additional techniques for offensive teams to implement that have yet to be disclosed? ***Christopher Glyer** (@cglyer), Chief Security Architect, FireEye*

Thursday, June 22

3:55-4:30pm	***Tracking Bitcoin Transactions on the Blockchain*** Bitcoins are a commonly-used currency among cyber criminals for exchanging goods and services and receiving payments from ransomware. While cryptocurrency claims to promote anonymity, the nature of the blockchain's public ledger means that criminal activities can be traced and correlated. This presentation will cover a brief high-level overview of how transactions on the blockchain work and will focus on how to apply this knowledge in order to both manually and automatically map out transactions, associate bitcoin addresses, and identify potential cybercriminal-owned bitcoin wallets with the goal of providing context to the scale and duration of a campaign impacting your enterprise. Examples will include identifying a Locky affiliate's infrastructure, attributing the Shark/Atom ransomware, and identifying "bitcoin exchanges" on the blockchain. ***Kevin Perlow**, Associate, Booz Allen Hamilton*
4:35-5:10pm	***MAC Times, Mac Times, and More*** How well do you really understand the times you see during an investigation? Are you confident in testifying that something happened at a specific time, or on a specific date? This presentation will revisit the file times found on Windows computers and what they mean. It will also focus on the dates and times recorded by MacOS computers, including timestamps found outside of the normal places. ***Lee Whitfield** (@lee_whitfield), OnDemand Subject Matter Expert - Forensics Lead, SANS Institute*
5:15-5:45pm	***Beats & Bytes: Striking the Right Chord in Digital Forensics (OR: Fiddling with Your Evidence)*** We will speak observationally and based in current brain research (and also demonstrate instrumentally) about the benefits and correlations of music in forensics and incident response practice. We will cover brain plasticity research, music and it's benefits to mental health, skills that translate from music to technology (and visa versa), and collaboration and team building through music for forensicators. ***Cindy Murphy** (@cindymurph), President, Gillware Digital Forensics; Certified Instructor, SANS Institute* ***Ryan Pittman**, Resident Agent-in-Charge, NASA Office of Inspector General's Computer Crimes Division*
5:45-6:45pm	**Networking Reception** (LOCATION: GOVERNOR'S BALLROOM PRE-FUNCTION)
6:45pm-???	**DFIR Night Out in ATX!** All work and no play makes for dull forensicators! Give your overloaded brain the night off and get a taste of Austin's storied Sixth Street. Buffalo Billiards, at 201 E. 6th Street, is a quick walk from the hotel. Everyone is invited; just wear your Summit badge for entry. ***Attendees will be scanned - contact info provided to Night Out sponsors.*** DFIR Night Out is sponsored by: DOMAINTOOLS ENDGAME. Carbon Black. VMRAY

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 23

9:00-9:15am	***Day 2 Overview & Opening Remarks*** ***Phil Hagen*** *(@PhilHagen), Certified Instructor & Summit Co-Chair, SANS Institute & DFIR Strategist, Red Canary* ***Rob Lee*** *(@robtlee), DFIR Lead & Summit Co-Chair, SANS Institute*
9:15-10:05am	***A Million Little Wizards: Scaling Forensics Isn't Magic*** As a global company which is often targeted by sophisticated adversaries, Google measures its response time to incidents in minutes, not hours or days. To achieve this, our incident response team must effectively collaborate across multiple time zones and with many responders. This talk explores how Google has advanced our response velocity, scale, and transparency by integrating self-developed open-source tools such as GRR Rapid Response, Plaso (log2timeline), and Timesketch into an end-to-end pipeline of response tooling. Through this efficiency, we are ready for any trouble which finds its way to our door. ***Johan Berggren*** *(@jberggren), Senior Security Engineer, Google*
10:05-10:35am	***Alexa, Are You Skynet?*** This is not yet another internet of things presentation. Our talk will discuss our research journey as we took an in-depth forensic dive into the data that is stored, transmitted, and can be recovered, from the Alexa portion of the Amazon ecosystem. Our primary focus is on the data that can be recovered across a variety of Amazon devices and how it can benefit a forensic analyst. We explore the use of different hardware in the Alexa portion of the Amazon ecosystem, which includes Fire TV/Fire Stick, Echo, and explore how they all integrate with the Alexa app. If the Alexa-powered Echo is always listening, what information is actually stored, what is transmitted to the Amazon ecosystem, and can this information help during an investigation? ***Jessica Hyde*** *(@B1N2H3X), Director of Forensics, Magnet Forensics; Adjunct Professor, George Mason University* ***Brian Moran*** *(@brianjmoran), Digital Strategy Consultant, BriMor Labs*
10:35-11:00am	**Networking Break & Vendor Expo** (LOCATION: GOVERNOR'S BALLROOM PRE-FUNCTION)
11:00-11:35am	***Incident Response in the Cloud (AWS)*** Moving from on-premises deployments to the cloud can offer incredible benefits to many organizations, including a plethora of capabilities to build, scale, modify, monitor, and tear down infrastructure with never-before-seen speed and agility. But, how do you monitor for, and respond to, attackers that leverage those same capabilities against you? In this session, we will compare and contrast performing digital forensics and incident response (DFIR) within AWS versus that as traditionally performed within on-premises environments. Learn the major differences in performing DFIR within AWS, along with the benefits it provides over traditional response within on-premises environments. ***Jonathon Poling*** *(@JPoForenso), Principal Consultant / Future Operations, SecureWorks*

Friday, June 23

11:35am - 12:10pm	***EXT File System Recovery*** The standard Linux fsck utility does a good job recovering damaged file systems. But can a deeper understanding of EXT file system structures yield better results? Superblocks and directory files plus other file system artifacts will come under the scrutiny of our trusty hex editor as we develop tools and methods to help us in Linux data recovery and forensics. ***Hal Pomeranz*** *(@halpomeranz), Principal, Deer Run Associates*
12:10-1:15pm	**Lunch & Learn Sessions**

Identifying and Eliminating Blind spots for Targeted Attacks (LOCATION: ROOM 415A)

ENDGAME.

Enterprises are hit by targeted attacks which are sophisticated and unique. Your exploit prevention and malware prevention has been circumvented by increased use of legitimate credentials, ROPless exploits, and in-memory attacks. Your threat intelligence is stale. Your SOC is already overwhelmed and anxious of missing attacks, and now you are being asked to build a "hunt team" when IR can't even keep up.

Endgame is a converged endpoint security product that stops targeted attacks and its components, at the earliest and all stages of the attack lifecycle. Join Endgame customer Texas A&M and Endgame's Director of Research to learn how to stop targeted attacks and remove blind spots in memory and in forensic data during detection and response.

Chris Delarosa*, SOC analyst, Texas A&M*

Mark Dufresne*, Director of Research, Endgame*

DNS Shadowing and RIGEK Malware (LOCATION: ROOM 415B)

DOMAINTOOLS®

Join DomainTools for lunch as they investigate some of the recent breaches involving DNS shadowing and how criminals are using that attack to distribute RIG Exploit Kit malware. We will also be digging into the use of Domain ownership with regards to illegal gambling operations shutdown in Canada. These incident response examples will demonstrate how to get behind privacy, and show how Passive DNS information can be used to find additional compromised domains.

Steve Butt*, Technical Sales Engineer*

Friday, June 23

1:15-2:20pm	***Open-Source DFIR Made Easy: The Setup*** A common challenge in the digital forensics and incident response (DFIR) community has been creating a DFIR toolkit that is cheap, simple to setup, scalable, and easy to use. Frequently, DFIR teams do not have the money to purchase, nor the time needed to develop a DFIR toolkit solution themselves. Although many open-source solutions exist, they typically require an advanced level of skill to setup and maintain. Alternatively, custom solutions present risk should the maintainer leave or become otherwise unable to maintain it. Another common issue faced by DFIR teams is the requirement for another agent constantly running on each host, exponentially consuming resources in already over-subscribed virtualized environments. This leads to the creation of custom scripts with varying levels of fidelity, based on the experience of the individual or team. This presentation will introduce and demonstrate the use of the "CyLR, CDQR Forensics – Virtual Machine" (CCF-VM). The CCF-VM was designed to provide an all-in-one solution to one of the most common issues facing DFIR teams. It provides a conveniently packaged, easy-to-use platform, designed from the ground up to enable teams to collect, process, and analyze critical forensics artifacts to triage and investigate intrusions both large and small. Including built-in, commonly used searches and dashboards, CCF-VM enables searching of both single or multiple hosts simultaneously based on analyst or incident needs. After completing this session, attendees will understand how to: collect data with CyLR; process forensic artifacts easily with CDQR; use Kibana (as setup in CCF-VM) for DFIR purposes; setup the CCF-VM; set up a CCF-VM DFIR toolkit for each analyst; and scale CCF-VM to the enterprise level. ***Stephen Hinck*** *(@stephenhinck), Senior Technical Account Manager, ICEBRG* ***Alan Orlikoski*** *(@alanorlikoski), Senior Manager, Incident Response & Threat Protection Team*
2:20-2:55pm	***The Audit Log Was Cleared*** "The Audit Log was cleared." The event that is sure to generate a loud groan from any forensicator. Annoying, but reassuring, you know for sure someone was here doing things they shouldn't have. However, some attackers are a little more subtle when it comes to the event logs they leave behind. In this talk, we will highlight some of the techniques real attackers have used to manipulate and remove event logs without leaving a "BAD GUY WUZ HERE" sign. In addition to discussing some Windows-native and custom tools to accomplish this goal, we discuss the challenges of identifying these activities and what DFIR professionals can apply, if any, to crack their case. ***Austin Baker****, Consultant, Mandiant* ***Jacob Christie****, Incident Responder, Mandiant*

Friday, June 23

2:55-3:30pm	***Japanese Manufacturing, Killer Robots, and Effective Incident Handling*** Every incident is unique, but there are some core competencies that are part of every response, such as communication, coordination, and documentation. Your ability to execute in those areas means the difference between a chaotic and confused response versus a smooth and efficient response. In their quest to improve their incident response processes, GitHub and Heroku independently landed on the same set of practices based on Toyota's just-in-time manufacturing practices. In this talk, we'll share those practices with you along with some new tools and hard-earned pearls of wisdom to help move your incident response process from good to great. ***Scott J. Roberts**, SIRT Lead, GitHub* ***Kevin D. Thompson**, Security Operations Lead, Heroku*
3:30-3:45pm	**Networking Break & Vendor Expo** (LOCATION: GOVERNOR'S BALLROOM PRE-FUNCTION)
3:45-4:20pm	***Deciphering Browser Hieroglyphics*** There are many valuable artifacts in modern browsers and not all are as easy to read as SQLite databases or JSON files. We will walk through deciphering web artifacts from popular websites and applications that many forensic tools (or a simple keyword search) would miss. Attendees will learn how to read these modern 'hieroglyphics' using open-source tools and integrate the results into their cases. What have your web browser investigations been missing? ***Ryan Benson** (@_RyanBenson), Senior Threat Researcher, Exabeam*
4:20-4:55pm	***Processing PCI Track Data with CDPO*** Investigating Payment Card Industry (PCI) breaches usually results in the recovery of credit and debit card data such as primary account numbers, expiration dates, cardholder names, and often full magnetic track data. A common challenge investigators often face is organizing and counting this recovered data, especially when dealing with hundreds of millions of records. Traditionally, investigators have had to create their own scripts or databases to process, validate, de-duplicate, count, organize, and query recovered track data, which resulted in inconsistent tools, formats, and methodologies. Say goodbye to weeks spent writing scripts to parse track data, validate account numbers with a Luhn check, and gather statistics. I will be introducing an open source tool, Card Data Processor and Organizer (CDPO), to quickly and efficiently process and validate millions of recovered PCI track records! This tool automatically generates useful information and statistics that victims and card brands require. This presentation highlights the need for a standardized card processing procedure, useful features of CDPO, performance metrics, and a demonstration. ***David Pany** (@DavidPany), Senior Consultant, Mandiant*

Friday, June 23

4:55-5:30pm	***Know Your Creds, or Die Trying*** Windows credentials are arguably the largest vulnerability affecting the modern enterprise. Credential harvesting is goal number one post-exploitation, and hence it provides an appealing funnel point for identifying attacks early in the kill chain. Unfortunately, credentials are diverse and numerous in Windows, and so are the attacks. With significant credential theft mitigations released in Win8.1, Win10 and Server 2012/2016, both red and blue teams require an enhanced understanding of Windows credentials. Red teamers may suddenly find their favorite techniques obsolete, while the blue team needs to take advantage of available mitigation techniques as soon as possible. Credential types, attack tools, and mitigation will all be discussed, giving insight into both sides of the equation. ***Chad Tilbury*** *(@chadtilbury), Technical Director, CrowdStrike; Senior Instructor, SANS Institute*
5:30-6:00pm	***Forensic 4cast Awards***
6:00pm	***Closing Remarks*** ***Phil Hagen*** *(@PhilHagen), Certified Instructor & Summit Co-Chair, SANS Institute & DFIR Strategist, Red Canary* ***Rob Lee*** *(@robtlee), DFIR Lead & Summit Co-Chair, 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**