SANS strives to present the most relevant, timely and valuable content. As a result, this agenda is subject to change. Please check back frequently for changes and updates.

Thursday, June 7, 2018	
9:00-9:15 am	**Welcome & Introductions** ● **Rob Lee (@robtlee), DFIR Lead & Summit Co-Chair, SANS Institute** ● **Phil Hagen (@PhilHagen), Certified Instructor & Summit Co-Chair, SANS Institute, and DFIR Strategist, Red Canary**
9:15-10:00 am	***Opening Keynote*** *To Be Announced*
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 about 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 that keeps one another 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. Extracting and analyzing this data we can determine a person's pattern of life as well as its 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, and Senior Instructor, SANS Institute**

10:40-11:00 am	**Networking Break**
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	**Networking Luncheon**
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**

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**
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, Chaos Specialist, Google**
7:00 pm - ???	**DFIR Night Out in ATX!**

Friday, June 8, 2018	
9:00-9:15 am	**Day 2 Overview and Opening Remarks** • **Rob Lee (@robtlee), DFIR Lead & Summit Co-Chair, SANS Institute** • **Phil Hagen (@PhilHagen), Certified Instructor & Summit Co-Chair, SANS Institute, and 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 two of those targeted by the group - Jake Williams and Matt Suiche. 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** • **Matt Suiche (@msuiche), Founder, Comae Technologies**
10:05-10:40 am	**A Process Is No One: Hunting for Token Manipulation** Does your organization want to start threat hunting but not certain how to begin? Most people start with collecting ALL THE DATA, but data mean 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**
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**
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, Kroll Cyber Security**
12:20-1:30 p.m.	**Networking Lunch & Vendor Expo**
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. **Jonathan 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. **Cynthia 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*** **Courtney Webb (@courtneyjjjwebb), Team Leader, Independent Researcher**
3:15-3:35 pm	**Networking Break & Vendor Expo**
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** ● **Kim Thomson (@ArdJect), Digital Forensic Examiner, H11 Digital Forensics**
4:10-4:45 pm	**Automating Analysis with Multi-Model Avocados** In every case you work 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 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), Certified Instructor & Summit Co-Chair, SANS Institute, and DFIR Strategist, Red Canary**

Speaker Biographies

Devon Ackerman (@AboutDFIR), Associate Managing Director, Kroll Cyber Security
Devon Ackerman is an Associate Managing Director with Kroll's Cyber Security and Investigations practice. He is an authority on matters involving digital forensic science, cybercrime, and related incident response. He has extensive experience in the investigation and remediation of cyber-related threats from his years with the Federal Bureau of Investigation and in the private sector.

Jared Atkinson (@jaredcatkinson), Adversary Detection Technical Lead, SpecterOps
Jared Atkinson is the Adversary Detection Technical Lead at SpecterOps and specializes in DFIR. Jared spent two years in the Veris Group's Adaptive Threat Division (ATD) and four years with the U.S. Air Force Hunt Team. Passionate about PowerShell and the open-source community, Jared is the lead developer of the PowerForensics Project, Uproot, and PSReflect Functions.

Ryan Benson (@_RyanBenson), Senior Threat Researcher, Exabeam
Ryan Benson is a researcher at Exabeam. He previously held DFIR roles at Stroz Friedberg, Mandiant, and Kaiser Permanente. He has experience investigating insider threats, responding to intrusions, and performing digital forensics in support of legal proceedings. He is the author of Hindsight, an open-source web browser forensics tool, and researches DFIR topics with a focus on browser forensics.

Daniel Bohannon (@danielhbohannon), Senior Applied Security Researcher, FireEye/Mandiant
Daniel has over seven years of operations, security, and incident response consulting experience. He is the author of Invoke-Obfuscation, Invoke-CradleCrafter, and Invoke-DOSfuscation, and co-author of the Revoke-Obfuscation Detection Framework. He has presented at numerous conferences, including Black Hat USA, DEF CON, DerbyCon, and BlueHat. Daniel has a master of science degree in information security from the University of Georgia. His primary research areas include obfuscation, evasion, and methodology-based detection techniques for endpoint and network applied at scale.

Mari DeGrazia (@maridegrazia), Director, Kroll Cyber Security
Throughout her career, Mari has investigated high-profile breach cases, worked civil and criminal cases, and provided testimony as an expert witness. She has written and released numerous programs and scripts to the forensics community, is a published author in *eForensics* magazine, and was technical editor for Windows Registry Forensics S.E.

Ron Dormido, Director, Cyber Security and Investigations, Kroll
Ron is a 26-year veteran of the U.S. Army, having served as a Counterintelligence Special Agent. During his military career, Ron developed extensive expertise in digital forensics/incident response, conducting sensitive national security investigations involving nation-state cyber threats. On his last tour of duty, Ron was assigned to the Army's Intelligence and Security Command in Hawaii, where he established the computer forensics/digital evidence recovery lab for an Army counterintelligence unit. In that role, he supervised a team responsible for providing digital forensics support to U.S. Army investigations and operations within the Pacific region. His duties included serving as the primary U.S. Army Intelligence representative to the FBI Honolulu counterintelligence/counterterrorism cyber threat working group and as liaison to the U.S. Army Computer Emergency Response Team. Additionally, Ron developed and implemented an in-house program to train U.S. Army counterintelligence personnel deploying to Iraq on tactical digital evidence collection.

Matthew Dunwoody (@matthewdunwoody), Principal Applied Security Researcher, FireEye/Mandiant
Matthew is responsible at FireEye for researching attacker activity and developing effective detection signatures and processes, among other tasks. Prior to his current role, he worked for five years as an incident response consultant with FireEye's Mandiant Consulting, where he supported and led numerous incident response engagements and high-tech crime investigations. Matthew has authored posts for FireEye's threat research blog and has spoken at conferences including DerbyCon, BlueHat, ShmooCon. and BruCON.

Sarah Edwards (@iamevltwin), Mobile Forensic Engineer, Parsons, Author & Certified Instructor, SANS Institute
A self-described Mac nerd, Sarah Edwards is a forensic analyst, author, speaker, and both author and instructor of SANS FOR518: Mac Forensic Analysis. She has been a devoted user of Apple devices for many years and has worked specifically in Mac forensics since 2004, carving out a niche for herself when this area of forensics was still new. Although Sarah appreciates digital forensics in all platforms, she has a passion for working within Apple environments and is well known for her work with cutting-edge Mac OS X and iOS, and for her forensic file system expertise. Sarah's dynamic classroom and presentation skills have been heralded by both her students and colleagues. She keeps students interested and engaged. Sarah has more than 12 years of experience in digital forensics, and her passion for teaching is fueled by the ever-increasing presence of Mac devices in today's digital forensic investigations. Given the complexity of most cases and the high probability that an OS X or iOS will be a part of an investigation, deep knowledge of these Operating Systems is crucial to ensure that forensic analysts grasp all the information required in a case and not omit valuable data.

Shelly Giesbrecht (@nerdiosity), Team Lead, Incident Responder, Cisco
Shelly is a Team Lead, Incident Response with Cisco Security, and a graduate student in the SANS Technology Institute's Master of Science in Information Security Engineering Program. She has been focused on SecOps and Incident Response both as an employee and a consultant for the past 13 years. She is a contributor to the Cisco Security Blog and writes her own blog at nerdiosity.com. Shelly tries to learn one new thing every day and is a firm believer in the bow tie.

Phil Hagen (@PhilHagen), Certified Instructor & Summit Co-Chair, SANS Institute, and DFIR Strategist, Red Canary
Phil is a SANS Certified Instructor and course lead for FOR572: Advanced Network Forensics and Analysis. He is also the DFIR Strategist for Red Canary, where he guides endpoint threat detection and response efforts to best meet customer's needs for fast and complete remediation

Jessica Hyde (@B1N2H3X), Director, Digital Forensics/Adjunct Professor, Magnet Forensics, George Mason University
Jessica Hyde is currently the Director, Forensics for Magnet Forensics and an Adjunct Professor at GMU where she teaches Mobile Forensics. Previously, Jessica performed forensics for Basis Technology, EY, and American Systems. She is also a veteran of the United States Marine Corps.

Nicole Ibrahim (@nicoleibrahim), Digital Forensics Expert, G-C Partners, LLC
Nicole Ibrahim is a digital forensics expert and researcher at G-C Partners, LLC, based in Dallas, Texas. She has a bachelor's degree in technology in information assurance and digital forensics. Nicole has presented many times at digital forensics conferences detailing her research and findings. She is also actively involved in the creation of open-source digital forensics tool.

Yogesh Khatri (@swiftforensics), Assistant Professor, Chaplain College
Yogesh Khatri has been a developer, researcher, and DFIR guy for 13 years. Currently both an assistant professor and program director at Champlain College, he teaches DFIR to the next generation of enthusiasts. He enjoys researching new artifacts (like SRUM, Amcache, APFS, DARWIN folders) and automating forensic tasks. His work can be found on his blog at swiftforensics.com and github.com/ydkhatri.

Rob Lee (@robtlee), DFIR Lead & Summit Co-Chair, SANS Institute
Rob Lee is an entrepreneur and consultant in the Boston area, specializing in information security, incident response, threat hunting, and digital forensics. 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 18 years of experience in digital forensics, vulnerability and exploit discovery, intrusion detection/prevention, and incident response. He graduated from the U.S. Air Force Academy and served in the U.S. Air Force as a founding member of the 609th Information Warfare Squadron, the first U.S. military operational unit focused on information operations. Later, he was a member of the Air Force Office of Special Investigations (AFOSI) where he led a team conducting computer crime investigations, incident response, and computer forensics. Prior to starting his own firm, he directly worked with a variety of government agencies, U.S. Department of Defense, and intelligence communities as the technical lead for a vulnerability discovery and an exploit development team, lead for a cyber forensics branch, and lead for a digital forensic and security software development team. Rob was also a director for Mandiant, a company focused on investigating advanced adversaries such as the APT, for five years. Rob co-authored *Know Your Enemy, 2nd Edition* and is also a co-author of the Mandiant threat intelligence report *M-Trends: The Advanced Persistent Threat.* He earned his MBA from Georgetown University.

Matthew Linton, Senior Security Engineer, Google
Matt is an incident responder with experience throughout the security process, from architecture through penetration. He is formally trained in disaster management and specializes in rapid response, remediation, and hardening of compromised environments.

Heather Mahalik (@heatherMahalik), Principal Forensic Scientist, ManTech, and Senior Instructor, SANS Institute
Heather has worked on high-stress and high-profile cases, investigating everything from child exploitation to Osama Bin Laden's media. She has helped law enforcement, eDiscovery firms, and the federal government extract and manually decode artifacts used in solving investigations around the world. All told she has more than 14 years of experience in digital forensics, including eight years focused on mobile forensics –there's hardly a device or platform she hasn't researched or examined or a commercial tool she hasn't used. At SANS, Heather is the course lead forFOR585: Advanced Smartphone Forensics. She also blogs and hosts work from the digital forensics community at www.smarterforensics.com. Heather is the co-author of *Practical Mobile Forensics* (1st and 2nd editions), currently a best seller from Pack't Publishing, and the technical editor for *Learning Android Forensics* from Pack't Publishing. Heather's background in digital forensics and e-discovery covers smartphone, mobile device, and Windows forensics, including acquisition, analysis, advanced exploitation, vulnerability discovery, malware analysis, application reverse-engineering, and manual decoding, as well as instruction on mobile devices, smartphones, and computers covering Windows, Linux and Macintosh operating systems.

Phill Moore (@phillmoore), Blogger, *This Week in 4n6*
Phill Moore is a senior digital forensic analyst in an Australian law enforcement lab. GCFE/CFCE/MsCyber (Digital Forensics). This Week in 4n6. ThinkDFIR.

Cynthia Murphy (@cindymurph), President, Gillware Digital Forensics
Cindy Murphy spent 31 years in law enforcement before founding Gillware Forensics in 2016. She has been investigating computer-related crimes since 1998 and is well known not only for her experience in the field but for her thirst for new, challenging problems to solve, and for her passion for forensics. She holds a master's degree in forensic computing and cyber crime investigation from University College, Dublin.

Brandon Nesbit, Senior Managing Consultant, Kroll
Brandon Nesbit is based at Kroll's Cyber Security and Investigations practice in Portland, Oregon. Brandon has over 10 years of experience in the areas of incident response, digital forensics, and malware analysis, and has conducted hundreds of cyber investigations for a variety of corporate clients across the globe.

Jonathan Poling (@JPoForenso), Managing Principal Consultant, SecureWorks
Jonathon Poling has 10+ years of experience in network security monitoring, digital forensics, and incident response. With a career spanning the government, contracting, and private sectors, he serves as a DFIR subject-matter expert in all major operating systems (Windows, Linux, Mac), including Cloud (Amazon Web Services). He is most at home on the *nix command line, performing most DFIR analysis using FOSS tools.

Matthew Seyer (@forensic_matt), Consultant, G-C Partners, LLC
Matthew Seyer is a consultant at G-C Partners, LLC based in Plano, Texas. He has obtained both bachelor's and associates degrees in digital forensics at Oklahoma State University and Richland College. Mr. Seyer enjoys research and development, and is currently interested in large data systems for storing forensic artifacts for the purpose of correlation, analysis, and analytics. Currently he codes primarily in Rust and Python.

Kim Thomson (@ArdJect), Digital Forensic Examiner, H11 Digital Forensics
Kim is a mobile device examiner and trainer, and lover of all things, as long as they're hexadecimal. He's a retired soldier, and enjoys spending time with his wife and three sons.

Courtney Webb (@courtneyjjjwebb), Team Leader, Independent Researcher
Courtney has been working in Australian Law Enforcement for 12 years and has been a Digital Forensics expert for six years. He is a lifelong tinkerer and has attended hacking conferences in Australia and the United States. He previously built "Battlebots" as a hobby, but during the last four years has focused on the intersection of DFIR and data recovery and hopes to pass on some of this knowledge.

Lee Whitfield (@lee_whitfield), OnDemand Subject-Matter Expert - Forensics Lead, SANS Institute
Lee has varied experience in forensic investigations and has worked on prosecution, defense, and in the corporate arena both in the United States and the United Kingdom. He is best known for holding the annual Forensic 4:cast Awards.

Robert Winchester, Adversary Detection Lead, SpecterOps

Robby Winchester is an experience threat hunter and pen tester. Over the course of his career, he's developed and supervised penetration testing, physical security, and breach assessments for several private sector and government clients. Previously, Robby worked for the U.S. Air Force Information Aggressors, providing full-scope network and physical red team operational assessments, and worked to integrate security operations within traditional military operations for the U.S. Air Force's RED FLAG exercise.