We strive 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 22, 2017	
9:00-9:15 am	*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**
9:15-10:00 am	*Opening Keynote* **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***
10:05-10:40 am	**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**
10:40-11:05 am	**Networking Break & Vendor Expo**
11:05-11:40 am	**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**
11:40-12:15 pm	**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 and researcher at G-C Partners, LLC**
12:15-1:30 pm	**Networking Luncheon**
1:30-2:05 pm	**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**
2:10-2:45 pm	**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 utilised. 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**
2:45-3:15 pm	**Networking Break & Vendor Expo**
3:15-3:50 pm	**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**
3:55-4:30 pm	**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 a identifying a Locky affiliate's infrastructure, attributing the Shark/Atom ransomware, and identifying "bitcoin exchanges" on the blockchain. **Kevin Perlow, Associate, Booz Allen Hamilton**
4:35-5:10 pm	**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**
5:15-5:45 pm	**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**
5:45-6:45 pm	**Networking Reception**
6:45-???	**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. Drinks, snacks, and games are all compliments of the DFIR Summit sponsors. 

Friday, June 23rd, 2017	
9:00-9:15 am	*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**
9:15-10:00 am	*Session description to come* **Johan Berggren (@jberggren), Senior Security Engineer, Google**
10:05-10:40 am	**Alexa, Are you Skynet?** This is not yet another internet of things (YAIOT) 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**
10:40-11:10 am	**Networking Break & Vendor Expo**
11:10-11:45 am	**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**

11:50 am – 12:25 pm	**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**
12:25-1:30 p.m.	**Lunch & Learn Sessions**
1:30-1:45 pm	**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 o Setup a CCF-VM DFIR toolkit for each analyst o 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**
1:45-2:20 pm	**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**
2:20-2:55 pm	**Japanese Manufacturing, Killer Robots, & Effective Incident Handling** Every incident is unique, but there are some core competencies that are a 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 vs 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 Toyota's just in time manufacturing practices. In this talk, we'll share those practices with you along with some new tools & 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**
2:55-3:25 pm	**Networking Break & Vendor Expo**
3:25-4:00 pm	**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**
4:00-4:35 pm	**Boot What? Why Tech Invented by IBM in 1983 is Sill 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**
4:35-5:05 pm	**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**
5:05-5:30 pm	**Forensic 4cast Awards**
5:30 pm	*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**

Speaker Biographies

Tim Ball, PhD, Southern Utah University
PhD in Computer Science, Graduate Certificate in Digital Forensics. Former lead Information System Security Engineer at the Naval Undersea Warfare Center and In-house Research Lead for Cyber Operations at the Air Force Research Lab. Currently an Assistant Professor of Computer Science and Information Systems at Southern Utah University.

Ryan Benson (@_RyanBenson), Senior Threat Researcher, Exabeam
Ryan Benson is a Senior Threat Researcher at Exabeam and 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 and blogs about DFIR topics.

Johan Berggren (@jberggren), Senior Security Engineer, Google
Johan is an Incident Responder and Senior Security Engineer at Google. He has been a member of Google's Global Incident Response team for over four years with a focus on developing open source digital forensics software. When he's not responding to incidents, he spends time developing Timesketch, an open source forensic timeline analysis tool.
Johan grew up in Stockholm, Sweden. He spent most of his time tinkering with computers and racing motorbikes without brakes, a.k.a Speedway.

Sarah Edwards (@iamevltwin), Mobile Forensic Engineer, Parsons
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.

Christopher Glyer (@cglyer), Chief Security Architect, FireEye
Christopher Glyer is the Chief Security Architect at FireEye with over ten years of experience in computer forensics and information security. Prior to that Mr. Glyer led Mandiant investigative teams performing enterprise-wide incident response and forensic analysis at some of the most high profile breaches in the news.

Phil Hagen (@PhilHagen), Summit Co-Chair, SANS Institute
For Phil Hagen, a career in information security chose him even before the movies War Games and Sneakers spurred his broader interest in the field. Phil has been captivated since the early days, working on information security projects since the mid-1990s, but networking grabbed his attention even before that.
"Since installing a 2400bps modem into an Apple //e around 1988, every computer I've used has been able to communicate with others," he says. "Of course the systems themselves are becoming more and more varied, making network analysis a critical component of the investigative process today."
Phil began his studies at the U.S. Air Force Academy's Computer Science Department, where he focused on network security and was an inaugural member of the computer security extracurricular group. He served in the Air Force as a communications officer at Beale AFB and the Pentagon. In 2003, Phil moved over to a position with a government contractor, providing technical services for various IT and information security projects.

Today, Phil's career has spanned the full attack life cycle - tool development, deployment, operations, and the investigative aftermath - giving him rare and deep insight into the artifacts left behind. Phil has covered deep technical tasks, managed an entire computer forensic services portfolio, and handled executive responsibilities. He's supported systems that demanded 24x7x365 functionality, managed a team of 85 computer forensic professionals in the national security sector, and provided forensic consulting services for law enforcement, government, and commercial clients. All of that brings Phil to his role today as the DFIR strategist at Red Canary, where he supports the firm's managed threat detection service.
Phil is also a certified instructor for the SANS Institute, and is the course lead and author of FOR572: Advanced Network Forensics and Analysis. This six-day course provides a hands-on curriculum to learn the skills necessary to perform investigations of network-based incidents, where the hard drives or memory of compromised systems are often missing.

Stephen Hinck (@stephenhinck), Senior Technical Account Manager, ICEBRG
With over 10 years in IT operations, security operations, and incident response roles, Stephen has a strong background in networking, systems administration, and incident response from both a business continuity and security perspective. Stephen is experienced with building and running Security Operations Centers (SOCs), including program implementation, signature creation and tuning, incident response and threat hunting.

Ashley Holtz (@thec0dem0nkey), Senior Services Engineer, CrowdStrike
Ashley Holtz is a programmer and consultant specializing in forensic and security tools and automation. In her free time she helps to improve access to quality security education to underrepresented groups through teaching at free or affordable programs like the Cyber Advantage Program at Montgomery College.

Jessica Hyde (@B1N2H3X), Director of Forensics, Magnet Forensics; Adjunct Professor, George Mason University
Jessica is an experienced forensic examiner in both the commercial and government sectors. She is currently the Director, Forensics at Magnet Forensics and an Adjunct Professor at George Mason University teaching Mobile Forensics. Previously, she performed forensic examinations for American Systems and EY. Jessica is a Marine Corps veteran.

Fred Kaplan (@fmkaplan), National Security Columnist, *Slate* & Author, *Dark Territory: The History of Cyber War*
Fred Kaplan is the national security columnist for *Slate* and the author of five books—*Dark Territory: The History of Cyber War* (Simon & Schuster, 2016), as well as *The Insurgents: David Petraeus and the Plot to Change the American Way of War* (Simon & Schuster, 2013, which was a Pulitzer Prize Finalist and a New York Times Best-Seller), *1959: The Year Everything Changed* (Wiley, 2009), *Daydream Believers: How a Few Grand Ideas Wrecked American Power* (Wiley, 2008), and *The Wizards of Armageddon* (Simon & Schuster, 1983, which, in its reissue by Stanford Univ. Press, is still in print and taught in several universities and academies). He has also written for many other publications, including the *New York Times*, *Washington Post*, *The New Yorker, The Atlantic, Foreign Affairs, MIT Technology Review*, and others. For 20 years, he was a staff reporter for the *Boston Globe*, working as the paper's military correspondent (1982-91, during which time he was a lead member of the team that won a Pulitzer Prize for a special series on the nuclear arms race), Moscow bureau chief (1992-95), and New York bureau chief (1995-2002). He has a Ph.D. in political science from M.I.T. For more information, feel free to browse his website, http://fredkaplan.info

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.
Rob 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 prior to starting his own business.
Rob co-authored the book *Know Your Enemy, 2nd Edition*. Rob earned his MBA from Georgetown University in Washington DC. Rob is also a co-author of the MANDIANT threat intelligence report M-Trends: The Advanced Persistent Threat.

Heather Mahalik (@heatherMahalik), Principal Forensic Scientist, ManTech & Senior Instructor, SANS Institute
To say that digital forensics is central to Heather Mahalik's life is quite the understatement. 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.
These days Heather is the Director of Forensic Engineering at ManTech CARD. At the SANS Institute she is a senior instructor and the course lead for FOR585: Advanced Smartphone Forensics. As if that isn't a full enough schedule, Heather also maintains www.smarterforensics.com, where she blogs and hosts work from the digital forensics community. She 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 is passionate about digital forensics because she loves always having to learn something new. "This field moves so quickly. It is literally impossible to get bored," she says. "If you find yourself bored, branch into another realm of digital forensics. The possibilities are endless and so is the fun! I love digging for artifacts and solving the puzzle."
Heather particularly likes working on mobile and third-party applications, a focus of her work. "I love cracking and hacking into apps that are supposed to be secure," she explains.
She cites her role as a SANS instructor as one of the most fulfilling achievements of her career. Heather loves it when students reach out to tell her that, thanks to her course, they put a criminal away for many years. As she says: "Nothing compares to knowing that the effort you put into writing and maintaining a course makes the world a better and safer place. SANS gives me the opportunity to share that with others."
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.

Brian Moran (@brianjmoran), Digital Strategy Consultant, BriMor Labs
Brian is a digital forensic analyst currently living near Baltimore, Maryland. He has been in the cyber security field for nearly two decades and has spent over a dozen years focusing on digital forensics/incident response (DFIR), both in the United States Air Force and the private sector.

Cindy Murphy (@cindymurph), President, Gillware Digital Forensics; Certified Instructor, SANS Institute
Cindy Murphy served in law enforcement for more than thirty years. For twenty-five of those years, she worked at the Madison Police Department (MPD) in Wisconsin. While at MPD, she had the opportunity to serve as a detective and as a certified digital forensics examiner for over seventeen years. During her time as an investigator, she saw firsthand the emergence of mobile devices as the primary source of evidence in investigations. This pushed her to grow into the mobile forensics expert she is today and enabled her to co-author the SANS FOR585 Advanced Smartphone Forensics course. Just recently, Cindy took a leave of absence from the Madison Police Department to launch Gillware Digital Forensics, where she is co-owner and serves as president and lead examiner. As a life-long police officer, Cindy knows the transition from the public to the private sector to private will present new challenges, but she's looking forward to broadening her professional experience even further, which will benefit both Cindy and her students.

Alan Orlikoski (@alanorlikoski), Senior Manager, Incident Response & Threat Protection Team, Oracle
A former Mandiant employee, Orlikoski now works for Oracle's Incident Response & Threat Protection (IRTP) team. As a lead for the IRTP team, he provides emergency services when a security incidents occurs.

David Pany (@DavidPany), Senior Consultant, Mandiant
David Pany is a Senior Consultant in Mandiant's Alexandria, Virginia office. His primary responsibilities include leading and delivering incident response and digital forensics engagements. Mr. Pany enjoys using open source forensic tools and developing python utilities to process forensic artifacts and automate tedious tasks.

Kevin Perlow, Associate, Booz Allen Hamilton
Kevin Perlow is an associate at Booz Allen Hamilton where he investigates network intrusions and performs host-based forensics and malware analysis in support of his firm's managed Cyber Threat Intelligence service, Cyber4Sight. He previously led a threat-hunting project for a public-sector client. Mr. Perlow holds a Bachelor's of Science in Business Administration from Georgetown University.

Ryan Pittman, Resident Agent-in-Charge, NASA Office of Inspector General's Computer Crimes Division
Ryan Pittman is a Resident Agent-in-Charge (RAC) with the NASA Office of Inspector General's Computer Crimes Division, continuing a career of over 20 years in Law Enforcement practicing, teaching, researching and writing about Digital Forensics. He plays the banjo, upright bass, dobro, harmonica, and cajon with the Gilroy Jam Band.

Jonathon Poling (@JPoForenso), Principal Consultant / Future Operations, SecureWorks
Jonathon Poling has over a decade of experience in Network Security Monitoring, Digital Forensics, and Incident Response. Serving in a variety of roles within the government, contractor, and private sectors, he has built and honed his DFIR expertise in all major operating systems, most recently focusing on AWS.

Hal Pomeranz (@halpomeranz), Principal, Deer Run Associates
Hal Pomeranz is an independent digital forensic investigator who has consulted on cases ranging from intellectual property theft, to employee sabotage, to organized cybercrime and malicious software infrastructures. He has worked with law enforcement agencies in the United States and Europe, and with global corporations.

Scott J. Roberts, SIRT Lead, GitHub
Scott is the CIRT Manager at GitHub. He is an incident responder, threat intelligence analyst, and developer. He's also the author of O'Reilly's Intelligence Driven Incident Response and frequent speaker for SANS, BSides, & Shmoocon. Kevin leads the Security Operations Team at Heroku and specializes in Incident Response/Blue-Teaming and automating security operations to run efficiently at scale.

Chad Tilbury (@chadtilbury), Technical Director, CrowdStrike; Senior Instructor, SANS Institute
Chad has nearly 20 years of experience working with government agencies, defense contractors, and Fortune 500 companies. And his case list looks like it's been pulled straight from those spy novels he grew up reading: murder, abduction, espionage, fraud, hacking, intellectual property theft, child exploitation, terrorism, and computer intrusions.
He has served as a Special Agent with the Air Force Office of Special Investigations, where he investigated and conducted computer forensics for a variety of crimes and ushered counter-espionage techniques into the digital age. Chad has also led international forensic teams and was selected to provide computer forensic support to the United Nations Weapons Inspection Team.
In addition, Chad has worked as a computer security engineer and forensic lead for a major defense contractor and served as the vice president of worldwide Internet enforcement for the Motion Picture Association of America. In that role, he managed Internet anti-piracy operations for the seven major Hollywood studios in over 60 countries.

Courtney Webb, Team Leader, Electronic Evidence, New South Wales Police Force
Courtney has been working in Australian Law Enforcement for 12 years and specialising in Digital Forensics for 6 years. He is a lifelong tinkerer and has attended hacking conferences in Australia and the United States. He has

previously built 'Battlebots' as a hobby, but the last 4 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. He has worked on prosecution, defence, and in the corporate arena both in the US and the UK. He is best known for holding the annual Forensic 4:cast Awards.