SANS Forensics and Incident Response SUMMIT

AUSTIN, TEXAS

June 9-10, 2014

PROGRAM GUIDE

Co-Chairs: Rob Lee & Alissa Torres

#DFIRSummit

Agenda

All Summit sessions will be held on the 2nd floor of the Omni Hotel (unless noted).

All approved presentations will be available online following the Summit at ***http://digital-forensics.sans.org/community/summits****.*
An e-mail will be sent out as soon as the presentations are posted, typically within 5 business days of the event.

Monday, June 9

7:00 - 8:00 am

Registration – *Location: 2nd Floor Foyer*

8:00 - 8:10 am

Welcome to the 2014 Digital Forensics and Incident Response Summit

Location: Lone Star Room

***Rob Lee** & **Alissa Torres** – Summit Co-Chairs*

8:10 - 9:00 am

KEYNOTE: ***Don't Let Your Tools Make You Look Bad***

Location: Lone Star Room

Good tools make forensics work possible. Bad tools invite disaster. All tools have limits. All tools have bugs. Any tool can misrepresent, omit, or shade the evidence at hand. Thus, even the best of tools, used well, can make one look bad. Forensics has consequences, so forensic professionals must be able to recognize errors, omissions, and inadequacies when they occur in their work. To do this, they must understand what it is that they are investigating. Proficiency with forensics tools is not the same as proficiency in computer forensics. Good forensics professionals understand what they are investigating.

***Troy Larson**, Principal Network Security Analyst, Microsoft Corp.*

9:00 - 10:00 am

So You Want to Write a Forensics Book?

Location: Lone Star Room

If you have ever entertained the idea of writing a forensics book, here is your chance to talk with published authors who have already done it. Find out how they were able to get their book deals, what the process of writing was like for each of them, how they assembled their writing team, and what they learned from it all. The authors will share practical tips from their experience with the process and the publishing houses.

Moderator: ***Suzanne Widup**, Author of Computer Forensics and Digital Investigation with EnCase Forensic, (McGraw-Hill)*

Panelists: ***David Cowen**, Author of Hacking Exposed: Computer Forensics, Anti Hacker Toolkit 3rd Edition and The Computer Forensics Infosec Pro Guide, (McGraw-Hill)*
***Andrew Hay**, Author of The OSSEC Host-based Intrusion Detection Guide, (Syngress); Nagios 3 Enterprise Network Monitoring; Nagios, Nokia Firewall, VPN; and IPSO Configuration Guide, (Syngress), and co-author of The OpenStack Security Guide, (OpenStack Foundation)*
***Heather Mahalik**, Co-author of Practical Mobile Forensics, (Packt Publishing)*
***Joseph Shaw**, Author of Unified Communications Forensics, (Syngress)*
***Warren Kruse**, Author of Computer Forensics: Incident Response Essentials, (Addison Wesley)*

NOTE: Publishers above noted in parentheses

10:00 - 10:30 am

Networking Break and Vendor Expo – *Location: Capital Ballroom Foyer*

10:30 - 11:15 am

TRACK 1 – Capital Ballroom A

Reverse Engineering Mac Malware

Dynamic malware reverse engineering helps forensic analysts and reverse engineers gather quick data points such as callout domains, file download URLs or IP addresses, and dropped or modified files. These methods have long been used on Windows malware...so why not on Mac malware? This presentation introduces the audience to methods, tools, and resources to help reverse Mac binaries with a Mac. Topics include Mach-O file format, virtualization, analysis VM setup, and various analysis tools (native and third-party). This presentation is intended for those familiar with dynamic analysis (with a touch of static thrown in) or for reverse engineering masters of the Windows executable who want to learn how to start analyzing Mac malware.

Speaker: ***Sarah Edwards,*** *Senior Digital Forensics Analyst*

TRACK 2 – Capital Ballroom B

BlackBerry Forensic Nuggets

Do you think BlackBerry is no longer relevant? Though the BlackBerry platform has suffered a significant market share loss, it is still in primary use by many government organizations and in the private sector by individuals and companies who value its robust security features. Significant phone service providers such as AT&T Sprint, T-Mobile, and Verizon provide BlackBerry devices as an option for their customers. If you've decided that Blackberry is a smartphone platform that you can ignore, or if you've been unable to find good information about forensic artifacts and techniques for BlackBerry devices and BES servers, this presentation is for you. We'll cover the following areas:

- BlackBerry Data Acquisition: Physical vs Logical
- Locked BlackBerry devices
- BlackBerry artifacts related to dat/key files, dat files, and bbm.db files
- BlackBerry Event Log
- BES and BlackBerry
- BlackBerry Malware case study
- BlackBerry 10

Speakers: ***Detective Cynthia A. Murphy,*** *MSc, EnCE, CCFT, Computer Forensics Unit, Madison Police Department*
Shafik Punja, *Police Officer, Calgary Police Service*

11:15 am - Noon

TRACK 1 – Capital Ballroom A

Mach-O Binary Data Analysis

As the popularity of OS X increases, malware written for this platform is increasing as well. Our talk will start by discussing how to extract various artifacts from the Mach–O file format. We will then explore this data using statistics, data analysis, and machine learning. Finally we investigate how to use these techniques to distinguish between malicious and non-malicious files. We will use a set of analysis techniques based on popular packages such as iPython, Scikit - learn, pandas, and statistical packages.

Speaker: ***David Dorsey,*** *Lead Security Researcher, Click Security*

TRACK 2 – Capital Ballroom B

10 Ways To Make Your SOC More Awesome

Security operations analysts are frequently classed as "generalists." The scope of their job description is split into a broad range including incident response, risk assessments, vulnerability management, awareness training, security tool selection, deployment and management, and general troubleshooting. The ability to keep track of and prioritize each day's tasks is a challenge, to say the least, and teams are often are asked to "do more with less." This session will highlight 10 ideas my small team has used to help us make more sense of our days, maximize our success and sanity, and improve our interactions with other IT groups in the organization.

Speaker: ***Shelly Giesbrecht,*** *Senior Security Operations Analyst, Nexen Energy ULC*

Noon - 1:15 pm

Lunch & Learn – *Location: Lone Star Room*

Presented by

cellebrite
delivering mobile expertise

Dealing With Persistent Smartphone Forensic Challenges

Advancements in mobile device hardware and operating systems, developments in data protection, prepaid devices, and app proliferation continue to challenge mobile forensics examiners. This session will cover available workarounds, from limited support from vendors, to advanced methodologies. Learn not only what can be retrieved, but how to analyze it.

Speaker: ***Ronen Engler,*** *Senior Manager, Technology & Innovation, Cellebrite*

1:15 - 2:00 pm

TRACK 1 – Capital Ballroom A

Supersize Your Internet Timeline with Google Analytic Artifacts

The goal of this presentation is to demonstrate how the timestamp information inside Google Analytical Artifacts can help an examiner build out a timeline that cannot be created with traditional tools. This presentation will provide an overview of how Google Analytics works and will also cover:

- Artifacts created on the user's computer by Google Analytics
- How to carve for deleted cookies and cache entries
- How to use parse the artifacts with free python and Windows tools
- How to build out a timeline by using the embedded Google analytic data

Several browsers will be covered, including Internet Explorer, Firefox, Chrome, and Safari.

Speaker: ***Mari DeGrazia****, Senior Security Consultant, RISK Team – Verizon*

TRACK 2 – Capital Ballroom B

Automating Linux Memory Capture for Analysis

Volatility has included support for Linux memory analysis since v2.2. However, practitioners have faced two obstacles:

1) Acquiring memory from a Linux system requires building, loading, and correctly using a third-party kernel module (such as LiME) for each system encountered; and
2) Creating a system-specific volatility "profile" for each system. Even for experts, these tasks are non-trivial and error-prone if performed manually. Fortunately, the Linux environment makes scripting and automation straightforward.

This session presents a tool to capture actionable information from Linux systems. The tool, which has been tested and used many times, was created to be a simple, automated collection agent that can be installed on a portable USB device. The user should be able to insert the USB device into a system and execute a single command to capture the memory of the system and produce a Volatility profile for use in later analysis. This session covers the basics of Linux memory capture and Volatility profile creation as a manual process, and then looks at how to install and use the tool as a portable agent. Using the Volatility framework, the session will also demonstrate some of the valuable information that can only be obtained via memory analysis.

Speaker: ***Hal Pomeranz****, Independent Digital Forensic Investigator*

2:00 - 2:45 pm

Best Finds for 2014

Location: Lone Star Room

After another year of research into all things DFIR, we've walked away with a lot of new tools and artifacts to look at. This presentation will go through what we think are the most useful and relevant of those:

- Detecting writes to NTFS disks with the ntfs-3g driver
- Recovering MTP access
- Outlook attachment access
- Artifacts from renaming accounts in Windows 7
- Using task scheduler logs to recover past logins

Speaker: ***David Cowen****, Partner, G-C Partners LLC*

2:45 - 3:15 pm

Networking Break and Vendor Expo – *Location: Capital Ballroom Foyer*

3:15 - 4:00 pm

TRACK 1 – Capital Ballroom A

Excel at Forensics

We work for an accounting firm crunching digits and pushing pivots, importing text to Excel, and parsing cells. Filter and sort adds class to reports. If you don't vlookup, your skills are weak so come open a sheet to learn the technique.

This presentation will help you increase efficiency and manipulate data using excel. Skills covered include:

- Data Imports – Suggestions and best practices
- Vlookups – QC and combining reports
- Pivot Tables – Reporting and deduplication
- Adding VB modules – Parsing paths, filenames, and extensions
- Database Connectors – Reporting from DB tools

Speakers: ***Anthony Gawron****, Manager, KPMG LLP*
David Nides*, Manager, KPMG LLP*

TRACK 2 – Capital Ballroom B

Public Research: Influencing Change in DFIR Tools

Forensic investigators on the clock usually have to get things out the door as soon as possible, so we often put a significant amount of trust in our tools. Sometimes time doesn't permit for thorough testing of every single bit of forensic evidence. However, an issue arises when comfort sets in and we become all too used to the automatic nature of these tools. We lose sight of what the tools are actually showing us and simply accept their output at face value. This talk will focus on the success story of improving two widely used DFIR tools through the proliferation of public research. By accessing the blog post Shellbags Forensics: Addressing a Misconception and examining follow-up community research, attendees will get a glimpse of how effective, helpful, and rewarding public research can be.

Speaker: ***Dan Pullega*** *(@4n6k), Forensic Investigator – 4n6k.com, KPMG LLP*

4:00 - 4:45 pm

TRACK 1 – Capital Ballroom A

Peeling the Application Like an Onion

Smart devices use not only SQLite databases but also text files, cache folders, and more. Uncovering and piecing together the data is imperative to a successful examination. The data requested are no longer contained in standard locations on a mobile device. It is crucial that the examiner understands what type of data can be found among the onion peels and, more importantly, how to put this together. In this talk we will build powerful SQL queries to quickly extract useful data and build python scripts to scrape the metadata, carve the fat, and uncover the hidden gold.

Speaker: ***Lee Reiber****, Vice President of Mobile Forensic Solutions, AccessData*

TRACK 2 – Capital Ballroom B

Windows 8 File History Analysis

File History is a backup service introduced in Windows 8. This new feature is based on the idea of tracing the USN journal to keep a record of older versions of files. The aim is to reinforce the importance of File History examination by analyzing different artifacts and co-relating them to connect the dots. This session examines the USN Journal file of NTFS at the byte level to better understand the USN change logging and records. It also looks at various artifacts of File History, including registry, configuration files, and event logs. We discuss an important aspect of File History—caching feature in detail—and examine how it stores information and why it could be critical in any forensic examination. Finally, we address several questions that might be raised in any investigation, such as the current state of service, external media or network storage used to save backup files, the time when the service last ran, the time limit (if any) for the backup files, retention policy, etc.

Speakers: ***Kausar Khizra*** *and* ***Nasa Quba****, Paranoid Yahoos, Yahoo! Inc.*

4:45 - 5:30 pm

Forensic 4cast Awards *– Location: Lone Star Room*

Presenter: ***Lee Whitfield****, Director of Forensics, Digital Discovery*

Please remember to complete your evaluation for today. You may leave completed surveys at your seat or turn them in to the SANS registration desk.

All Summit sessions will be held on the 2nd floor of the Omni Hotel (unless noted).

All approved presentations will be available online following the Summit at ***http://digital-forensics.sans.org/community/summits****.*

An e-mail will be sent out as soon as the presentations are posted, typically within 5 business days of the event.

Tuesday, June 10

7:30 - 8:30 am

Registration – *Location: 2nd Floor Foyer*

8:30 - 9:30 am

KEYNOTE: ***Barbarians at Every Gate: Responding to a Determined Adversary***

Location: Lone Star Room

In the last six months, Mandiant has helped an organization repel targeted attackers that utilized an increasingly sophisticated set of tactics to re-compromise their environment. These tactics included:

- Leveraging interfaces from third-party networks
- Use of the heartbleed exploit to bypass VPN authentication
- Phishing attacks using a zero-day exploit in IE

This presentation will focus on how Mandiant kept pace with a determined adversary, followed the breadcrumb trails from new attack vectors, and helped the client repel and remediate these attacks.

Speaker: ***Christopher Glyer****, Technical Director, Mandiant*

9:30 - 10:00 am

Networking Break and Vendor Expo – *Location: Capital Ballroom Foyer*

10:00 - 10:45 am

TRACK 1 – Capital Ballroom A

USB Devices and Media Transfer Protocol: Identifying the Existence of Data Exfiltration Artifacts

The prolific use of mobile phones in general and the use of these devices within corporate environments has started changing the ways examiners approach these kinds of cases. When it comes to questions surrounding potential data exfiltration, a mobile phone can be used to steal data. Mobile phones connected via USB to a workstation can provide an easy way to copy data. At present, Android devices occupy approximately 80% of the market share. These devices use Media Transfer Protocol (MTP) as the default for interfacing with the Windows workstations to which they are connected. The artifacts generated on a Windows OS when using MTP devices (Android phones and tablets running Android 3.0 +) are different from Mass Storage Class (MSC) USB device artifacts generated (thumb and external drives). Therefore, when identifying whether data exfiltration took place from a machine, it is important to understand the differences between the artifacts generated for the aforementioned USB protocols.

Speaker: ***Nicole Ibrahim****, Digital Forensics Researcher, G-C Partners, LLC.*

TRACK 2 – Capital Ballroom B

Closing the Door on Web Shells

While many attackers install malware on end-user workstations to accomplish their goals, external-facing servers continue to be prime targets of attack. In many of these cases, web shell backdoors are used by the adversary to download/upload files, execute arbitrary commands, and access back-end databases and other resources. Web shells are often heavily customized and obfuscated to evade detection. They may be only several lines of code, and they can be deployed on a variety of platforms. Every incident responder should be familiar with this dangerous category of malware so it is not overlooked during an investigation. This talk will discuss how web shells work, dive deep into several specimens, discuss approaches to detect related activity, and touch on some best practices to reduce the likelihood of seeing them on your systems.

Speaker: ***Anuj Soni****, Lead Associate, Booz Allen Hamilton*

10:45 - 11:30 am

TRACK 1 – Capital Ballroom A

The Evolution of Incident Response: How IR Will Change as it Becomes Part of Day-to-Day Information Security Operations

Information security programs have traditionally focused on protecting their networks. When compromised, programs would outsource some or all of the incident response to external experts. Dedicated intrusion response teams have been a luxury only the largest enterprises could afford. But the increasing volume of attacks repeatedly demonstrates the inevitability of compromise, painfully exposing the difficulties of managing outsourced IR. More and more enterprises are building internal IR programs. During program design, the tendency for both engineering and management is to replicate the tools, technologies, and procedures of traditional intrusion response, but internal intrusion response is sufficiently different from traditional intrusion response to demand different approaches. This talk will explore intrusion response as part of day-to-day information security operations and how it's different from traditional incident response.

Speaker: ***Jeffrey J. Guy****, Director - Operations, Carbon Black*

TRACK 2 – Capital Ballroom B

To Silo, or Not to Silo: That is The Question

Have you ever heard someone say they do network forensics and don't need a host computer to know what happened (or vice versa)? Or an incident handler analyzing RAM make a comment about disk imaging being unnecessary and outdated? These types of mindsets are problematic because they are limiting—to the investigator, the evidence, and our profession—and manifest themselves through incomplete analysis and inaccurate conclusions. If the limitation is real and tangible—for instance, if firewall logs are the only available evidence—then we make the most of what we have. Otherwise, incident response should be based on all of the information available to us as investigators, including firewall logs, packet captures, system alerts, RAM, filesystems, malicious executables, and so forth. If these are available, but are ignored or overlooked, analysts are missing out on potentially valuable information. When that happens, the conclusions drawn and recommendations made will be incomplete or just plain wrong. To paraphrase Hamlet, "Ay, there's the rub."

Speaker: ***Frank McClain****, GCFA, GCIH, CHFI, Information Security Manager, DFIR Team Lead, PrimeLending*

11:30 am - 12:45 pm

Lunch & Learn – *Location: Capital Ballroom B*

Presented by

GENERAL DYNAMICS
Fidelis Cybersecurity Solutions

Facing The New Frontier: A Real Case Study In Performing Computer Forensics Without The Evidence

In most modern investigations the computer forensics expert witness has access to all of the data and is able to develop their opinion based on hard evidence. Times are now changing in computer forensics just as if there is a missing body in a murder trial. Now, experts need to provide testimony to support his or her expert opinions on computer systems he or she did not have to examine. Would such a scenario be considered pure speculation, baseless and unethical for the expert to complete? Mr. Jones was able to convince a judge of his opinions without the actual evidence present. Would you like to find out how it was accomplished within the confines of Federal Civil law? Attend this presentation and learn the techniques.

Speaker: ***Keith Jones****, Lead Cybersecurity Engineer, General Dynamics Fidelis Cybersecurity Solutions*

11:30 am - 12:45 pm

Lunch & Learn – *Location: Lone Star Room*

Presented by

CLICK SECURITY

Operational Data Analysis

Do we have the full story? What other data can we look at and what intel can we glean? In this talk we will take a look at several data sources to help understand an incident, and also look at tools for data analysis.

Speaker: ***Eric Chavez****, Security Analyst, Click Security*

12:45 - 1:30 pm

TRACK 1 – Capital Ballroom A

Incident Response Patterns: The "Now What?" to the DBIR and VCDB

Today's network defenders focus largely on incident prevention to the detriment of detection. The Verizon Data Breach Investigations Report (DBIR) and VERIS Community Database (VCDB) contain lots of information explaining how attacks happen at a strategic level. This session will analyze some common incident types identified in our research, isolate relevant tactics, techniques, and procedures (TTPs) based on this real-world data, and discuss how to hunt intrusions matching these very common patterns in modern networks. We will also include standardized representations of our data in STIX and VERIS formats.

Speakers: ***Kyle Maxwell,*** *Senior Researcher, Verisign*
Kevin Thompson, *Senior Researcher, Verizon*

TRACK 2 – Capital Ballroom B

Targeted Campaign Analysis and Tracking

We have all seen those emails pretending to be missed delivery notices from USPS, FedEx, UPS; the counterfeit Amazon orders; or the fake bank or credit card notifications. Then there are the more serious fraudulent emails that masquerade as someone you know encouraging you to visit an interesting link or open an attachment. How do you determine whether these emails arrived in your inbox by chance or by circumstance? During this talk you will learn how to determine the methods of targeting, learn the attacker's motivation, and understand the purpose behind a greater campaign.

Speaker: ***Christopher Witter,*** *Senior Strategic Intrusion Analyst, CrowdStrike, Inc.*

1:30 - 2:15 pm

TRACK 1 – Capital Ballroom A

Pillars of Incident Response: The Calm in the Storm

Incident response is not for the faint of heart, and regardless of what you might think, not just anyone can do it successfully. This session will start with the anatomy of a "day in the life" of a breached company as the information security team moves through the P.I.C.E.R.L steps of incident response. From common notification avenues through technology controls, we'll take a look at common decisions, knee-jerk and otherwise, which are often made while in panic mode. Along with gotchas from past experience and client observation, this session will cover long-term remediation considerations when you need to move beyond immediate incident response into investigations and more extensive and coordinated clean-up. Correctly or not, many consider incident response a rapid-handling, rapid-resolution methodology, and organizations are often not prepared with the budget, technology, or staff resources for the demands of long-term incident response requirements. This session will look at ways to address those issues.

Speaker: ***Brandie Anderson,*** *Senior Manager Production Management, Hewlett Packard*

TRACK 2 – Capital Ballroom B

The Life Cycle of Cyber Crime

Credit card breaches are increasing in alarming numbers. The mainstream media and blogosphere seem to cover a new breach almost daily. From small businesses to large corporations, these attacks are coordinated, sophisticated, and strike without warning, with no signs of slowing down.

Who is committing these breaches? How are they getting in? Why is payment card data being targeted? What do they do with the data once they steal it? After this presentation, you will have an increased understanding of how and why payment card data is stolen, by whom, and how the subsequent financial fraud is being used to fuel organized crime.

Speaker: ***Jonathan Spruill,*** *Senior Security Consultant, Trustwave*

2:15 - 2:45 pm

Networking Break and Vendor Expo – *Location: Capital Ballroom Foyer*

2:45 - 3:30 pm

TRACK 1 – Capital Ballroom A

Why Hunt When You Can Seine?

Mature Computer Incident Response Teams can't afford to sit idly by watching glass and waiting for signatures to trip alerts. Incident response teams have to be proactive, arm themselves with knowledge of attacker TTPs, and engage in intelligence-driven hunts for the adversary. Hunting works great for smaller-scale enterprises or specific targets, but what if your enterprise is comprised of thousands or hundreds of thousands of hosts? This talk explores techniques and tools prepared by the presenter that will allow small and large enterprises to scale up their hunts in Windows environments, enabling them to seine for evil in a scalable way using free and open-source tools.

Speaker: ***Dave Hull****, Senior Security Service Engineer, Microsoft Corp.*

TRACK 2 – Capital Ballroom B

Don't Drop that Table: A Case Study in MySQL Forensics

Digital forensic practitioners are likely to encounter databases in their practice. Databases may have been used by criminals or compromised by attackers. Additionally, many applications function as databases or store information in database files. Chrome, Firefox, Internet Explorer, Skype, ICQ, and many more common communications applications, for example, store data in a database format. A common database format that examiners may encounter is SQL. MySQL is an open source database that has been incorporated into many products – both open source and commercial applications.

This presentation will demonstrate how I rebuilt and queried a database to extract evidence during an actual examination I conducted. Specifically, I examined a MySQL database, rebuilt database tables, and used simple BASH scripts to generate queries on the tables to acquire the information to support an investigation. The ability to create, read, and query database tables will provide an examiner additional skills. These skills can assist when reading logs, determining if a database was compromised, and correlating relational data.

Speaker: ***Jeff Hamm****, Principal Consultant, FireEye*

3:30 - 4:30 pm

DFIR SANS360

Location: Lone Star Room

This session features an array of top Digital Forensics and Incident Response experts discussing the coolest forensic technique, plugin, tool, command line, or script they used in the last year. They'll talk about the approach that really changed the outcome of a case they were working on. If you have never been to a lightning talk, it is an eye-opening experience. Each speaker has 360 seconds (six minutes) to deliver his or her message. This format allows SANS to present 10-12 experts within one hour, instead of the standard one presenter per hour. The compressed format gives you a clear and condensed message eliminating the fluff. If the topic isn't engaging, a new topic is just six minutes away.

Presentations:

- ***Wanted: Dead or Alive (Use Cases and Reminders for Live and Dead Box Imaging)*** *– J. Jewitt, KPMG LLP*
- ***The E-Discovery and Forensics Balancing Act*** *– Stacey Randolph Edwards, The Sylint Group*
- ***How Bad Guys Steal Stuff*** *– Jonathan Spruill, Senior Security Consultant, Trustwave*
- ***DNS Hunting Like a Boss*** *– Pete Hainlen, Threat Analyst, Mayo Clinic*
- ***Internet of Perjury (IoP): Asset Identification and Confirmation*** *– Andrew Hay, Research Lead, OpenDNS*
- ***False Positive: The Eye of the Biased Examiner*** *– Alissa Torres, Certified Instructor, SANS Institute*
- ***Forensics Survivor: Key Artifacts That Aren't Being Voted off the Island*** *– Jake Williams, Certified Instructor, SANS Institute*
- ***Getting up to Speed on Rekall*** *– Elizabeth Schweinsberg, Incident Responder, Google*
- ***The Need for Network Security Monitoring (a.k.a. Capture all the Things)*** *– JP Bourget, Syncurity Networks*

4:30 - 4: 45 pm

Summary & Closing Remarks – *Location: Lone Star Room*

Rob Lee & Alissa Torres*– Summit Co-Chairs*

Thank you for attending the Digital Forensics & Incident Response Summit.

Please remember to complete your evaluation for today. You may leave completed surveys at your seat or turn them in to the SANS registration desk.

Exhibitors

cellebrite
delivering mobile expertise

Since 2007, the Cellebrite UFED has provided mobile forensics solutions to investigative professionals worldwide. The UFED enables extraction, decoding and analysis of data and passwords from thousands of legacy and feature phones, smartphones, portable GPS devices, and tablets. Visit the Cellebrite exhibit or online at www.ufedseries.com to learn more.

CLICK SECURITY

Click Security, runs real-time stream processing analytics against pre-computed log, network, and file/artifact data sources; automatically produces analyst start points with automated actor/event / relationship views; and provides a full attack activity framework – where analysts can interactively visualize, prune, and augment big security data. Now, security teams can rapidly identify early stage attack patterns.

GENERAL DYNAMICS
Fidelis Cybersecurity Solutions

General Dynamics Fidelis Cybersecurity Solutions provides organizations with a robust, comprehensive portfolio of products, services, and expertise to combat today's sophisticated advanced threats and prevent data breaches. Our customers can face advanced threats with confidence through use of our Network Defense and Forensics Services and Fidelis XPS™ Advanced Threat Defense Products.