



Tuesday, June 26, 2012		
Time	Capital Room	Senate Room
7:00am - 8:00am	Registration	
8:00am - 8:10am	Welcome and Introduction to the 2012 Digital Forensics and Incident Response Summit	
	<ul style="list-style-type: none"> • <i>Rob Lee – Summit Chair Computer Forensic/IR Summits</i> 	
8:10am - 9:10am	Keynote	
	<ul style="list-style-type: none"> • <i>Detective Cindy Murphy, City of Madison, WI</i> 	
9:10am - 10:10am	<p style="text-align: center;">Windows 8 Forensic Artifacts</p> <ul style="list-style-type: none"> • <i>Kenneth Johnson, IT Security Analyst, Principal Financial Group</i> <p>With any new operating system, it is important to understand how it will interact with current technologies, what artifacts from previous versions carry over, and what new artifacts and behaviors are discovered. This presentation will examine new features of Windows 8, including integration and the usability of a Windows Live ID, file history services, the refresh and recover options that are available and the forensic artifacts that are retained on the machine, and explore the implications of these features on digital forensic investigations.</p>	<p style="text-align: center;">Analysis and Correlation of Macintosh Logs</p> <ul style="list-style-type: none"> • <i>Sarah Edwards, Digital Forensics Analyst, Harris Corporation</i> <p>When was this user logged on the system? Where was this system on a given date? What devices were used on the system? How often was the system used? Is the system compromised? - These questions may be answered by viewing the logs provided by Mac OS X. This presentation will cover the variety of logs, tools to read them, and analysis of additional file system files to provide a clear picture of events. User, network, or software activities can provide a timeline that can be used to uncover the clandestine activity on the system - whether or not it was meant to be secret.</p>
10:10am - 10:30am	Networking Break	
10:30am - 11:30am	<p style="text-align: center;">Practical Use of Cryptographic Hashes in Forensic Investigations</p> <ul style="list-style-type: none"> • <i>Pär Österberg Meding, Sr. Incident Response Consultant, McAfee and Foundstone Professional Services</i> <p>Cryptographic checksums can be useful in computer forensic investigations, both for finding</p>	<p style="text-align: center;">Reasons Not to "Stay in Your Lane" as a Digital Forensics Examiner</p> <ul style="list-style-type: none"> • <i>Alissa Torres, Security Researcher, KEYW Corporation</i> <p>Why do examiners need to know offensive and anti-forensics techniques? The answer becomes obvious when you experience your first</p>

	<p>files of interest and for excluding files known to be good. This presentation will show how indexing of hash databases can cut down search time and how the Reference Data Set available from NIST can be edited to include only relevant product codes, separating the infamous "Hacker Tools" from our database with hashes of known good programs. We'll also explore fuzzy hashing and how it can be used to identify both file fragments and establishing relationship with other files. Lastly, learn about Hashdog, a program used to generate custom hash databases. The program will not only traverse directory structures recursively, it will also try to unpack and expand every file it comes across. The output files that hashdog generates are compatible with the internal database structure of the Reference Data Set from NIST, making it easy to import and use custom hash databases in existing forensic frameworks.</p>	<p>investigation of a highly sophisticated computer user. During this session, attendees will gain knowledge of some of the artifacts left behind by SSH tunneling tools, anti-forensic browser plug-ins and open-source offensive tools. In addition, they will leave with justification to attend training that is "outside their lane" of daily tools and techniques.</p>
<p>11:30am-12:40 pm</p>	<p style="text-align: center;">Lunch & Learn Presented By</p> <div style="text-align: center;">  </div> <p>21CT will present a panel of CISOs talking about real world challenges and sharing their insights on topics including:</p> <ul style="list-style-type: none"> • Identifying strategies for responding to sophisticated digital attacks • The role of security intelligence and analytics • State-of-the-art best practices • Key lessons learned by the those who are in the middle of the threat every day. <p>Moderator: Fred Chang, President, 21CT</p> <p>Panelists:</p> <ul style="list-style-type: none"> • Brian Engle, CISO, Texas Health and Human Services Commission • Gary McAlum, SVP & CSO, USAA • Dave Notch, CISO, Thomson Reuters 	
<p>12:40pm - 1:40 pm</p>	<p style="text-align: center;">Digital Forensics for IaaS Cloud Computing</p> <ul style="list-style-type: none"> • <i>Josiah Dykstra, Computer Security Researcher, US Dept. of Defense</i> <p>In this talk, we expose and explore technical and trust issues that arise in acquiring forensic</p>	<p style="text-align: center;">Carve for Records (Not Files)</p> <ul style="list-style-type: none"> • <i>Jeff Hamm, Senior Consultant, Mandiant</i> <p>Traditional file carving is less than perfect when attempting to recover data for PCI investigations, targeted intrusions, insider data theft and destruction, and criminal activity. The</p>

	<p>evidence from infrastructure-as-a-service cloud computing and analyze some potential strategies for addressing these challenges. We first discuss why cloud computing presents new and unique challenges to digital forensics using hypothetical case studies. Then we create a model to show the layers of trust required in the cloud. We then demonstrate, for the first time, an evaluation of popular forensic acquisition tools including Guidance EnCase and AccessData Forensic Toolkit, and show that they can successfully return volatile and non-volatile data from the cloud. We explain, however, that judge and jury must accept a great deal of trust in the authenticity and integrity of the data from many layers of the cloud model. These results lay the foundation for future development of new acquisition methods for the cloud that will be forensically sound and trustworthy. In addition, our work helps forensic examiners, law enforcement, and the court evaluate confidence in evidence from the cloud. The final part of the talk deals with the legal aspects of cloud forensics, exploring why even usually routine discovery, such as search and seizure, is more complicated and troublesome when dealing with the cloud.</p>	<p>header is easy to find with most tools, but fragmentation and no file footer can cause automated carving to fail. These investigations require a methodology that involves carving for individual record entries instead of trying to recover full files. Windows Event Log Entries, Apache Log Entries, IIS Log Entries, ZShell command history entries, wtmp (Linux login log) entries, and others contain structured data. If the data is structured, an analyst can formulate a regular expression not just to parse the data, but to find the data.</p> <p>This presentation will detail specific tools used and/or developed to search for and parse data. Real successes (and failures) illustrate the concepts and techniques.</p>
<p>1:40pm – 2:40pm</p>	<p>Android Memory Acquisition and Analysis with DMD and Volatility</p> <ul style="list-style-type: none"> • <i>Joe Sylve, Senior Security Researcher, Digital Forensics Solutions</i> <p>Physical memory analysis is vital to investigations, since it contains a wealth of information that is otherwise unrecoverable. This evidence includes objects relating to both running and terminated processes, open files, network activity, memory mappings, and more. Lack of such information can make certain investigative scenarios impossible, such as when performing incident response or analyzing advanced malware that does not interact with nonvolatile storage.</p> <p>This presentation will explore the technical issues associated with acquiring physical memory captures from Android-based devices as well as subsequent analysis of the data acquired. We will present a methodology for acquiring complete memory captures from Android, code to analyze</p>	<p>Building and Maintaining a Digital Forensics Lab</p> <ul style="list-style-type: none"> • Panelists: • <i>Chad Tilbury, SANS Instructor</i> • <i>Art Ehaun, Director, Forward Discovery</i> • <i>Jeff Hamm, Senior Consultant, Mandiant</i> • <i>David Nides, Senior Forensic Technology Associate, KPMG</i> • <i>Willy Straubhaar, MS, PMP, Cyber Training Program Manager, Office of Antiterrorism Assistance, U.S. Department of State</i> <p>One of the unique challenges in digital forensics and incident response is building a forensics lab. As more organizations seek to add in-house digital forensic capabilities, they are employing a variety of solutions to meet this need. Common threads exist for sole-practitioners, law enforcement entities, Fortune 500 companies, and even unique environments like deployed locations in Iraq and Afghanistan.</p>

	<p>kernel data structures, and scripts that allow analysis of a number of userland and file system-based activities. We will also demonstrate support for Android memory analysis into the Volatility Memory Analysis framework. Since Volatility is already used extensively in real investigations, in the support of research in memory forensics, and in a number of training courses, we hope our results will generate further interest in the Android platform.</p>	<p>Come hear a diverse panel of experts from both large and small organizations share their experiences, best practices and lessons learned. Receive the latest information on accreditation and regulations, personnel, online storage and disaster recovery, budgets, case tracking and oversight, virtualization, and secure access solutions for outside organizations and remote employees.</p>
<p>2:40pm - 3pm Networking Break</p>		
<p>3:00pm - 4:00pm</p>	<p style="text-align: center;">Sniper Forensics v3: Hunt</p> <ul style="list-style-type: none"> • <i>Christopher Pogue, Managing Consultant, Trustwave SpiderLabs</i> <p>I am a sniper. I hunt malware. Specifically, I hunt malware that is committing a crime. Memory Dumpers, Key Loggers, and Network Sniffers are the enemy. The enemy can take on any form, he deploys stealth to hide from me. To know the enemy, I have to know HOW he works, not just what his goals are.</p> <p>Sniper Forensics v3.0: Hunt will culminate the Sniper Forensics Trilogy. It will bring all of the elements of the previous two Sniper Forensics presentations to bear, and illustrate the hunt. From system preparation, to data gathering, to finally, identifying the primary target of many forensic investigators...malware.</p> <p>Not only will this talk cover how to identify the most common types of criminal malware, but HOW to identify an infected host by WHAT it's doing, not by what has traditionally been known as "malware detection" by hash comparisons, keyword searches, or even just blind luck. This final installment will equip the investigator with the methodology, the tools, and take them on the hunt for cyber criminals in three real world scenarios. I am a sniper. I will find and eliminate my target.</p>	<p style="text-align: center;">Decade of Aggression</p> <ul style="list-style-type: none"> • <i>Christopher Witter, Principal Network Security Engineer, Major Defense Contractor</i> <p>Do you sometimes struggle to find the evidence you need to prove your case? Do you want to process your evidence faster and easier? If you answered yes, then Decade of Aggression is for you. Decade of Aggression is a compilation of tips and lessons learned from responding to incidents over the last ten years. These tips are a mixture of proactive and reactive steps to help you better obtain and handle your evidence. We will cover hardware configuration, software settings, network infrastructure items, as well as policy and procedural details. Examples include minimizing the noise level when recovering deleted files, maximizing the location information present on a laptop, and efficient analysis in the wake of an incident.</p>
<p>4:00pm - 5:00pm</p>	<p style="text-align: center;">Passwords are Everywhere!</p> <ul style="list-style-type: none"> • <i>Hal Pomeranz, Consultant, Deer Run</i> 	<p style="text-align: center;">Recovering Digital Evidence in a Cloud Computing Paradigm</p>

	<p style="text-align: center;"><i>Associates</i></p> <p>Passwords are a valuable artifact for Forensic investigators-- particularly when found in clear-text format and are passwords that are being used by suspects. Not only do they have significant evidentiary value, but because password reuse is just as prevalent in the criminal community as it is among their victims, recovered passwords may provide the key to unlocking otherwise inaccessible data in databases, encrypted files, etc.</p> <p>This talk is based on my experience finding and leveraging password information in real-world investigations. Attendees will learn common places where password data may be found, including:</p> <ul style="list-style-type: none"> -- Scripts, automated tasks, and other applications -- Database access libraries and the databases themselves -- Application configuration files, particularly on mobile devices -- Command-line history <p>Techniques for obtaining and de-obfuscating passwords will be covered. Attendees will also learn how to leverage these passwords to obtain additional information and evidence.</p>	<ul style="list-style-type: none"> • <i>Jad Saliba, Founder & CEO, JADsoftware Inc.</i> <p>Attendees will learn about the methods and techniques used to recover digital evidence from a computer that has been used for cloud based services such as Dropbox, Skydrive, and Google Docs. In addition, as the trend to cloud computing and Solid State Drives leaves less evidence on a hard drive it becomes paramount to effectively recover evidence from live RAM. We will explore the best practices in conducting live triage and RAM captures.</p>
<p>5:00pm – 6:00pm</p>	<p style="text-align: center;">DFIR SANS360</p> <p>In one hour, 10 Digital Forensics and Incident Response experts will discuss the coolest forensic technique, plugin, tool, command line, or script they used in the last year that really changed the outcome of a case they were working. If you have never been to a lightning talk it is an eye opening experience. Each speaker has 360 seconds (6 minutes) to deliver their message. This format allows SANS to present 10 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 6 minutes away.</p> <p>Registry Decoder: Automated Acquisition, Analysis, and Reporting of Registry Contents <i>Andrew Case, Research Engineer, Terremark</i></p> <p>Remote Collection Standardization with Triage in an Immature IR Structure <i>Ken Johnson, IT Security Analyst, Principal Financial Group</i></p> <p>How We Know the Sky is Blue: Child Victim Age Estimation in 360 Seconds <i>Detective Cindy Murphy, Madison (WI) Police Department</i></p> <p>Registry, UserAssist, and VSCs...Oh, My! <i>Harlan Carvey, Chief Forensics Scientist, Applied Security, Inc.</i></p>	

	<p>A Hash is Worth a Thousand Words <i>Hal Pomeranz, Consultant, Deer Run Associates</i></p> <p>Automating Your Timeline Analysis in 360 Seconds <i>Kristinn Gudjonsson, Security Engineer, Google</i></p> <p>Finding Fraudulent Word Documents in 360 Seconds <i>Corey Harrell, Information Security Specialist III, NYS Office of the State Comptroller</i></p> <p>EXIF and Metadata and Geotags, Oh My! Finding Embedded Data Without the Need for Flying Monkeys <i>Melia Kelley, Senior Forensic Consultant, First Advantage Litigation Consulting</i></p> <p>The Analytic That Changed My Life: Who Are We All Talking To? <i>Tim Ray, Subject Matter Expert, 21CT</i></p> <p>The Relevance of Shellbag Artifacts: A 360 Second Soapbox <i>Alissa Torres, Security Researcher, KEYW Corporation</i></p> <p>360 Megabytes of Timeline Data <i>David Nides, Senior Forensic Technology Associate, KPMG</i></p>
<p>7:00 -9:00pm</p>	<p style="text-align: center;">DFIR Night in Austin Sponsored By</p> <div style="text-align: center;">  </div>

Wednesday, June 27, 2012

6:45-7:50am

Networking Breakfast & Security Analytics Demo

Presented By



Time

Capital Room

Senate Room

7:30am - 8:00am

Registration

8:00am - 9:00am

Keynote

- *Harlan Carvey, Chief Forensics Scientist, Applied Security, Inc.*

9:00am - 9:30am

Forensic 4Cast Awards

Forensic 4Cast popular computer forensic and computer crime podcast. Join Lee Whitfield for a session of Forensic4Cast podcast recorded live from the Forensic Summit 2011

- *Lee Whitfield, Director of Forensics at Digital Discovery*
- Show: <http://forensic4cast.com>

9:30am -
10:30am

Anti-Incident Response

- *Nick Harbour, Principal Consultant, Mandiant*

This presentation covers what techniques the bad guys are using to thwart the Incident Response process and which of those techniques actually work. This is a broad category that also encompasses anti-forensics and anti-reverse engineering. The successful use of clever anti-analysis strategies can be the key difference the distinguishes an elite intruder.

Automating File Analysis

Pär Österberg Medina, Sr. Incident Response Consultant, McAfee and Foundstone Professional Services

On a case-to-case basis, the file types that you are interested in examining will differ. When investigating a case involving sexually explicit material, picture files such as JPEGs and PNGs might be of more interest than executable files whereas in an investigation of a suspected computer compromise those executable files are what you might be focusing on. In this presentation I will show how to truly identify which kind of type a file actually is and how to automate the analysis of said files. In order to do this, I will be presenting two programs that I wrote, Classify and Analyze (working names).

By using a database of rules and signatures, Classify will automate the classification process by placing the files into the category they belong. Now when all the files are organized, we will use Analyze to automate the actual analysis. Even if some generic techniques like generating

#DFIRsummit

		<p>a cryptographic checksum of the file and search for it in our databases can be applied to all file types, the rest of the analysis is highly dependent on the file type of the file you are analyzing. This is why Analyze is not only using configuration files to control which modules to use for which file category but also why the program has a easily editable plug-in directory to customize or extend the functionality of the program. The great advantage of utilizing both of these tools together is that it will allow you to cut down on your investigation time and increase the efficiency and effectiveness of your analysis.</p>
--	--	--

<p>10:30am - 10:50am</p>	<p>Networking Break</p>	
--------------------------	--------------------------------	--

<p>10:50am - 11:50pm</p>	<p style="text-align: center;">Mac Memory Analysis with Volatility</p> <ul style="list-style-type: none"> • <i>Andrew Case, Research Engineer, Terremark</i> <p>Memory analysis is becoming a vital part of every digital forensics investigation due to the proliferation of advanced malware, disk encryption, and the plethora of information that is only stored in memory. During this presentation the new Mac memory analysis capabilities of Volatility will be presented. Previously, Volatility had only supported Windows and Linux targets. The new Mac capabilities include recovering and listing processes, memory mapping details and data, network information, open files, filesystem information, and loaded kernel modules. Presentation of newly developed kernel rootkit detection techniques will be also be discussed. The talk will end by showing the capabilities and limitations of performing memory analysis against iOS devices including the iPhone and iPad. Throughout the presentation relevant kernel internals will be discussed as well as the developed Volatility plugins.</p>	<p style="text-align: center;">Digital Dumpster Diving</p> <ul style="list-style-type: none"> • <i>Lee Reiber, Director of Mobile Forensics, AccessData</i> <p>What happens to that data when you turn in your old cellphone? Are you sure you removed it all. Simply doing a factory reset might not be enough.</p> <p>In this presentation Lee Reiber will present a case study that he conducted after purchasing cellular phones from several reselling outlets known to us all and some not. We will look at the methods used, the types of data recovered and possible ways to protect your data from the Digital Dumpster Diver.</p>
--------------------------	--	---

<p>11:50am-1pm</p>	<p>Lunch & Learn Presented By</p> 	
--------------------	---	--

<p>1:00-2:00pm</p>	<p>What Works in Computer Forensics and Incident Response Data Triage Panel</p>	
--------------------	--	--

	<p style="text-align: center;">Solutions Panel: Tips & Tools</p> <ul style="list-style-type: none"> • <i>Moderator: Rob Lee, SANS Institute</i> • <i>David Roskind, Captain, Sandy Springs (GA) Police Department</i> • <i>Christopher Witter, Principal Network Security Engineer, Major Defense Contractor</i> <p>DFIR professionals have a lot of data coming their way and are often under-staffed or otherwise limited by time. How do they prioritize the tasks they are asked to perform? How do they eliminate the "noise" when sifting through evidence and focus on what is meaningful and important? What techniques exist to make this easier to do? What tools--free and commercial ones--might assist with the process? How might a team be staffed and skilled to accommodate the triage process?</p>	
<p>2:00pm – 3:00pm</p>	<p style="text-align: center;">When Macs Get Hacked</p> <ul style="list-style-type: none"> • <i>Sarah Edwards, Digital Forensics Analyst, Harris Corporation</i> <p>Computer intrusions cases usually consist of a Windows boxes or a *nix system, if you are lucky. Mac intrusion cases are a rare breed. These cases have the potential to become more popular with the growing market share of Macintosh systems. Many companies and government entities use Macs as their preferred system. This presentation will introduce you to incident response and intrusion analysis of the Mac.</p>	<p style="text-align: center;">Evidence is Data: Your Secret Advantage</p> <ul style="list-style-type: none"> • <i>Jon Stewart, Big Picture Guy, Lightbox Technologies, INC.</i> <p>It's nothing new to say we're drowning in evidence. Experts and vendors tell us we now must triage evidence to cut down on the amount of data examined, lab managers worry about case backlogs, and investigators spend time watching progress bars creep along their screens. Terabyte-sized cases inspire terror in many. This fear is misplaced.</p> <p>Peter Norvig, Google's Director of Research, has argued that computer scientists should "make use of the best ally we have: the unreasonable effectiveness of data."¹ With the explosion of the Internet and the availability of cheaper hardware and better software systems, researchers have shown how to harness expanding data sets with simple statistical techniques. This presentation will cover the basic principles of such techniques and show how they can be applied to aspects digital forensics, including document analysis, image clustering, facial recognition, and timeline analysis. In addition to a big-picture understanding of how such technologies work, some simple, practical tips for investigators to apply will be demonstrated. Finally, we'll show how results improve as more data is analyzed. This leads us to the conclusion that more evidence is not a curse, but a blessing in disguise.</p>
<p>3:00pm - 3:20pm</p>	<p style="text-align: center;">Networking Break</p>	

3:20pm – 4:20pm	<p>Taking Registry Analysis to the Next Level</p> <ul style="list-style-type: none"> • <i>Elizabeth Schweinsberg, Incident Responder, Google, Inc.</i> <p>Contemporary Registry Analysis involves sifting through a registry hive for a list of keys, subkeys, and values. These lists of keys have been gathered over time from Windows resources and investigators' notes, but are they the right ones for your organization to be looking at? The next level of registry analysis is comparing the registry you have with what's "normal".</p> <p>What is normal? We will share the results of data-mining the malware analysis that AV companies have published to find the common -- and not so common -- places to hide while comparing them to contemporary research. Then, we'll look at using existing tools to find out what keys are normal in your enterprise. From there, you can save analysis time by filtering out the normal, and focusing on the unique.</p>	<p>Tales from the Crypt: TrueCrypt Analysis</p> <ul style="list-style-type: none"> • <i>Hal Pomeranz, Consultant, Deer Run Associates</i> <p>What if you suspect a device you are investigating may contain TrueCrypt volumes? What if you have no passwords or memory image to analyze and cannot access the volumes? Is all hope lost?</p> <p>Based on real-world investigations, this talk starts by covering techniques for detecting TrueCrypt volumes on Windows systems using a combination of specialized tools, registry forensics, and application-specific configuration files. Next we'll look at the information that is available to the investigator about the contents of a TrueCrypt volume, even when the volume itself cannot be decrypted.</p>
4:20pm - 5:20pm	<p>Security Cameras: The Corporate DFIR Tool of the Future?</p> <ul style="list-style-type: none"> • <i>Mike Viscuso, CEO, Carbon Black</i> <p>The evolution of digital forensics closely mimics that of physical forensics in many ways. In the early days of fingerprints, bullet grooves and blood splatters, procedures were new or non-existent and practices were subject to no small amount of skepticism. Today, however, the methodical procedures are captured in academic texts and training regimens and criminalistics is widely accepted in the courts. So too did computer forensics evolve from a niche and poorly understood practice to a highly effective practice widely used in the pursuit of justice. Yet digital forensics, like every crime-fighting technology, is reactive. It depends upon our ability to understand – at a very granular level – operating systems and applications whose authors have no vested interest in cooperating with forensics product developers or practitioners. Both industry and government security experts are in agreement that the <i>prevention</i> approach to security is increasingly untenable. <i>Assumption of breach</i> is the new normal. Unfortunately, since most companies have been slow to adopt this new reality, it is costing</p>	<p>Exfiltration Forensics in the Age of the Cloud</p> <ul style="list-style-type: none"> • <i>Frank McClain, GCFA, GCIH, CHFI, PI, Senior Information Security Analyst, PrimeLending</i> <p>Host-based forensics is dead. How many times have we heard statements like that? In this case, the alleged cause is the cloud, but is it an accurate assessment? There is no doubt that the cloud – with all its different definitions and scenarios – has changed the face of forensics, but the problem is that with its prevalence, it's an easy way to exfiltrate data from a network, and we're not talking about webmail here. Cloud-based storage is very low-cost, and local clients can be used to back up or synchronize systems or files for sharing between computers and mobile devices, accessible from anywhere on the internet. Whether we're dealing with a disgruntled employee or an opportunistic hacker, these backup and synchronization services are a handy target for exfiltration. Theft of intellectual property can occur without much effort if the user has the ability (whether</p>

	<p>data breach victims an average of \$200,000 per incident to identify what happened and how to fix it. We'll discuss log management tools and techniques that enable forensics and incident responders. Much like security cameras in the physical world, these tools and techniques have been proven to reduce 90-99% of the unknowns in incident response and allow digital detectives to focus on the juicy problems versus random imaging and log collection.</p>	<p>authorized or not) to use one of these services. If an attacker can compromise a host with one of these clients installed, or gain physical possession (think lost/stolen laptop or tablet), they have ready access to sensitive files. The good news is that all this activity leaves a footprint on the host system, thanks to the client applications that manage the data transfer.</p>
5:20pm - 5:30pm	Summary & Closing Remarks	