National Institute of Standards and Technology

Mobile Forensics Workshop and Webcast

Agenda

June 18, 2014

All times EDT	NIST Gaithersburg Campus with live webcast	
8:30 – 8:45 a.m.	**Introduction**	John Paul Jones II, National Institute of Standards and Technology
8:45 – 9:25 a.m.	**Mobile Forensics Tool Testing at NIST**	Rick Ayers, National Institute of Standards and Technology
	The development of mobile device forensic tools and acquisition techniques continues to grow within the field of digital forensics. Mobile subscribers far outnumber personal computer owners, and studies have shown an increase of mobile device personal data storage compared to personal computers. Over time, mobile devices can accumulate a sizeable amount of information about their users. Data acquired from these devices may be useful in criminal cases or civil disputes. As mobile device usage and sophistication continues to grow, so does the need for tool validation. In order for acquired information to be admissible in a court of law, verification of a tool's behavior and strict forensic acquisition methods are paramount. The Computer Forensics Tool Testing (CFTT) project at NIST has tested numerous mobile device forensic tools capable of acquiring data from mobile devices operating over Global System for Mobile (GSM) communications and Code Division Multiple Access (CDMA) networks. The CFTT project produces specifications, test methods, and test reports that provide a foundation for toolmakers to improve tools, for users to make informed choices, and for interested parties to review any anomalies found. This presentation covers information on the motivation behind testing mobile device forensic tools, the development of specifications and test plans, the creation of a known data set, the population of mobile device data, and the testing of tools.	
9:25 – 10:05 a.m.	**Acquisition Techniques: Mobile Forensics from A to Z**	Sam Brothers, Department of Homeland Security
	The field of mobile device forensics has changed significantly over the last 10 years. The ubiquity of mobile devices has spawned an industry that develops new technology at a dizzying pace. Rules and methods that were developed just 2 – 3 years ago to obtain the data stored inside these devices have been surpassed by even better methods (e.g., Radio Isolation Cards). Level 3 (Joint Test Action Group, or JTAG) extraction methods have revolutionized our industry, and many mobile device vendors are just barely able to keep up with the myriad of Level 3 invasive and non-invasive techniques available. This presentation will cover the evolution of these methods and will discuss some of the latest techniques used in mobile device forensics today.	

10:05 – 10:25 a.m.	**Break**	
10:25 – 11:05 a.m.	**Anybody Seen a Career Path Around Here?**	Kevin Mansell, Control-F Digital Forensics
	Thousands of people around the world examine mobile devices for a living, employed within organizations large and small. Their experience and ability levels differ massively, but we lack an agreed framework with which to measure competency or to recognize and reward ability. The implications of a “framework-free future” look bleak. <INSERT HAPPY ENDING HERE>. (Note: this will be a virtual presentation.)	
11:05 – 11:45 a.m.	**Is Mobile Device Forensics Actually “Forensics”?**	Gary Kessler, Gary Kessler Associates
	Mobile device forensics is fundamentally different from traditional computer forensics, just as digital forensics is fundamentally different from the more traditional forensics in the physical world. In mobile device forensics, we deal with at least three major “standard” operating systems as well as several proprietary ones, we do not necessarily “image” a mobile device as we do a hard drive, and our target devices are powered “on” instead of “off.” It is common, however, to hear a computer forensics examiner say that cell phone forensics are not “real forensics” because we don’t image a phone in the same way that we image a hard drive. This session will examine the premise that mobile device forensics is somehow lesser than traditional computer forensics from the theoretical perspective and from the perspective of the actual practice.	
11:45 – 12:25 p.m.	**BlackBerry® Forensics**	Shafik Punja, Teel Technologies
	Think BlackBerry is no longer relevant? The BlackBerry platform, though it has suffered significant market-share problems, is still in primary use by many government organizations and in the private sector by individuals and companies who value its security features. Significant phone service providers, such as AT&T and Verizon, provide BlackBerry devices as an option for their customers. These smartphone devices are also used by many Federal entities. The presentation will primarily focus on BlackBerry 10 and its backup data structure.	
12:25 – 1:25 p.m.	**Lunch**	
1:25 – 2:05 p.m.	**Open-Source Mobile Forensics**	Heather Mahalik, Basis Technology
	Not everyone has the budget to afford commercial forensic tools in support of smartphone investigations. This talk will provide a brief overview of acquisition methods using open-source tools primarily for Android but applicable to other smartphones. The primary focus of this presentation will be on the analysis and recovery of data residing on Android devices using Autopsy®, the open-source graphical user interface (GUI) based on The Sleuth Kit®. Autopsy will be used as an open-source analytical tool to decode Android data found in standard and third-party applications, including chat, contacts, location information, and more. Sometimes knowing how to use your open-source tool can recover just as much data as the leading commercial kits.	

All times EDT		
2:05 – 2:45 p.m.	**Current State of Mobile Forensics in Academia**	Rick Mislan, Rochester Institute of Technology
	Back in the day, personal digital assistants (PDAs) gave us random-access memory (RAM) and read-only memory (ROM) dumps. After that, simple phones gave us access to contacts, call logs, short message service (SMS), images, and videos. The smartphones of today continue to give us all of the above as well as application and Internet data. As these digital "windows to the world" pervade the very social fabric of our everyday lives, we continue to find more ways to use the digital data to help us solve the crime at hand. Through numerous conferences, journal articles, and other reference materials, academia has played a significant role in pushing these new boundaries. Given the current state of smartphone technologies, this presentation will describe the past and current role that academia is playing in mobile device forensics.	
2:45 – 3:00 p.m.	**Break**	
3:00 – 3:40 p.m.	**Mobile Malware and Spyware Apps: Working Through the Bugs**	Cindy Murphy, Madison, Wisconsin, Police Department
	The proliferation of mobile malware and spyware means that it is likely to exist on some devices that are submitted to your laboratory for examination. Are you looking for malware in your mobile evidence? Can malware and spyware affect your case, and could they potentially help your investigation? This presentation will highlight the various infection vectors for mobile malware and spyware and will provide advice on what to look for in mobile forensic exams, including what should trigger a more in-depth exam for malware or spyware. The demonstration portion of this presentation will show how to unpack and decompile application files using free tools in order to see the suspected malware's underlying programming code and to ascertain what it might be doing.	
3:40 – 4:20 p.m.	**Real-World Mobile Forensics: The Intersection of Research, Academia, and Case Work**	Daren Melson, Wal-Mart
	This talk will first focus on the symbiotic relationship among the major foci (academia and training, research and development, tool testing, and practitioners) within the mobile forensics community and their interconnected workings in the interchange of ideas and processes that drive the practice of mobile forensics. Then, the discussion will look at some unique cases in which an evolution of technique was needed to get to the necessary data that solved the case and how the members of the mobile forensic community played a role in that process. The talk will conclude with a brief discussion of future trends and expectations regarding the mobile forensics community.	
4:20 – 4:50 p.m.	**Q & A Panel Discussion**	Gary Kessler, Heather Mahalik, Daren Melson, Rick Mislan, Cindy Murphy, and Shafik Punja

Speaker Biographies

Richard Ayers, National Institute of Standards and Technology
"Mobile Forensics Tool Testing at NIST"
Mr. Richard Ayers is a computer scientist in the Information Technology Laboratory at NIST in Gaithersburg, Maryland. Mr. Ayers, a participant of the Cyber Corps program, graduated summa cum laude from the University of Tulsa with a BS and MS in computer science and has been in the IT field for more than 15 years. His current research focus is on mobile device forensics tools and proper acquisition techniques. Mr. Ayers's certifications include National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 4011 – Information Systems Security Professional, 4012 – Designated Approving Authority, 4013 – System Administration in Information Security Systems, 4014 – Information Systems Security Officer, and 4015 – Systems Certifier. Mr. Ayers has co-authored numerous mobile device forensic publications and is currently performing formal testing for the Computer Forensic Tool Testing (CFFT) project.

Sam Brothers, Department of Homeland Security
"Acquisition Techniques: Mobile Forensics from A to Z"
Mr. Sam Brothers is a digital forensics specialist working for U.S. Customs and Border Protection. He has been working in the field of mobile forensics since 2006. In late, 2007 he developed the "Cell Phone Tool Classification Pyramid" and presented it at the first Mobile Forensics World 2008 in Chicago, Illinois. Currently, he is not just a digital forensics practitioner, but he is also quite active in the digital forensic community. Mr. Brothers is currently serving as the chair of the Forensic Committee for the Scientific Working Group on Digital Evidence (SWGDE) and the incoming program committee chair for the American Academy of Forensic Scientists' (AAFS's) Digital and Multimedia Section. He also was one of the lead developers for the new International Association of Computer Investigative Specialists (IACIS) Mobile Forensics Training Program for law enforcement. Recently, Mr. Brothers was asked to work with Rick Ayers and Wayne Jansen to re-write NIST's 800-101 Revision 1 "Guidelines on Mobile Forensics."

Kevin Mansell, Control-F Digital Forensics
"Anybody Seen a Career Path Around Here?"
Mr. Kevin Mansell has been teaching people how to get to grips with mobile evidence in order to find the truth since mobile phones had real buttons and batteries that lasted more than a day (circa 2005). Since then, he has taught more than 1,100 delegates how to safely recover and efficiently process evidence from mobile devices. Mr. Mansell's classes typically include personnel from law enforcement and private sector organizations as well as academic institutions.

Mr. Mansell started out teaching digital forensics at the UK's National High Tech Crime Training Centre at Wyboston in Bedfordshire from 2004 to 2006. During that time, Mr. Mansell researched, wrote, and delivered the UK's entry-level mobile phone forensics training course for law enforcement personnel and contributed to European Union and Interpol electronic crime projects. Mr. Mansell founded Control-F in 2007 and delivers vendor-neutral training in mobile device forensics in the UK and overseas. Outside the office and the classroom, Mr. Mansell roams the flatlands of eastern England looking for as-yet-undiscovered peaks to make his mountain bike feel worthy of its name.

Gary Kessler, Ph.D., CCE, CCFP, CISSP, Gary Kessler Associates
"Is Mobile Device Forensics Actually 'Forensics'?"
Dr. Gary C. Kessler is a professor of Homeland Security at Embry-Riddle Aeronautical University (Daytona Beach, Florida) specializing in cybersecurity, and president and janitor of Gary Kessler Associates, a training and consulting company specializing in computer and network security and digital forensics. Dr. Kessler is also a member of the North Florida Internet Crimes Against Children (ICAC) Task Force and an adjunct associate professor at Edith Cowan University (Perth, Western Australia). Dr. Kessler has been performing cell phone examinations since 2006 as a member of the Vermont ICAC, and he was the first such examiner in the Vermont law enforcement community. He is the co-author of two professional texts and more than 70 articles and papers; a frequent speaker at regional, national, and international conferences; and former editor-in-chief of the *Journal of Digital Forensics, Security and Law*. More information about Dr. Kessler can be found at http://www.garykessler.net.

Shafik Punja, BSc, A+, CISSP, Network+, ACE, CCE, GFCE, GFCA, Teel Technologies
"BlackBerry® Forensics"
A senior police officer with the Calgary Police Service for over 18 years, Mr. Shafik Punja has been working in digital forensics since 2003 and has conducted digital forensic examinations on a wide variety of digital data storage devices and operating systems. In 2005, Mr. Punja began researching and developing analytical techniques for mobile devices and smartphone platforms, and he has since become an expert in the analysis of BlackBerry, among other devices.

Mr. Punja has been qualified in the Canadian legal system as an expert in the area of digital forensics numerous times. He also served as an invited guest instructor to assist teaching the Cell Phone Seizure and Analysis Workshop (CSAW) for the Technological Crimes Learning Institute (TCLI) at the Canadian Police College, in Ottawa, Ontario, in 2008 and 2009. Mr. Punja is an instructor and resident smartphone expert for Teel Technologies, with a concentration on the BlackBerry platform, and he is the author of the Advanced BlackBerry Forensics Training class.

Heather Mahalik, Basis Technology
"Open-Source Mobile Forensics"
Ms. Heather Mahalik works with the Digital Forensics Team at Basis Technology and served as the mobile exploitation team lead for more than 5 years. She is the course lead and primary author for the SANS Smartphone Forensics course and co-author of the SANS Mac Forensics course. With more than 11 years of experience in digital forensics, she currently focuses her energy on mobile device investigations, forensic course development, and instruction and research on smartphone forensics. Ms. Mahalik is co-authoring a book, *Practical Mobile Forensics*, which will be released in July 2014.

Prior to joining Basis Technology, Ms. Mahalik worked at Stroz Friedberg and as a contractor for the U.S. Department of State's Computer Investigations and Forensics Branch. She earned her bachelor's degree from West Virginia University. Ms. Mahalik has authored white papers and forensic course material and has taught hundreds of courses worldwide to law enforcement, government, information technology, eDiscovery, and other forensic professionals focused on mobile device and digital forensics.

Rick Mislan, Rochester Institute of Technology
"Current State of Mobile Forensics in Academia"
Dr. Rick Mislan is currently at his alma mater, the Rochester Institute of Technology (RIT), serving in the newly created Computing Security Department within the College of Computing and Information Sciences. At RIT, he is developing the new Mobile Security and Forensics undergraduate and graduate program. He is also a faculty member in the Mobile Information Assurance and Security (MOBIAS) research group.

Prior to his work at RIT, Dr. Mislan made his mark in mobile forensics while a professor at Purdue University. Dr. Mislan's areas of research include mobile device forensics, mobile exploitation, mobile security, and techniques for improving efficiency in mobile forensics. He was also a faculty member with the Center for Education and Research in Information Assurance and Security (CERIAS).

He has authored numerous articles in the area of mobile forensics, he created the *Small Scale Digital Device Forensics Journal* and the Mobile Forensics World Conference, and he acts as a reviewing editor for NIST. As a subject-matter expert, Dr. Mislan supports state and Federal law enforcement, military organizations, and intelligence agencies in mobile device forensics and exploitation.

Cindy Murphy, Madison, Wisconsin, Police Department
"Mobile Malware and Spyware Apps: Working Through the Bugs"
Detective Cindy Murphy works for the City of Madison, Wisconsin, Police Department and has been a law enforcement officer since 1985. She is a certified forensic examiner and has been involved in computer forensics since 1999. She earned her Master's degree in Forensic Computing and Cyber Crime Investigation through University College, Dublin, in 2011. Detective Murphy has directly participated in the examination of many hundreds of hard drives, cell phones, and other items of digital evidence pursuant to criminal investigations including homicides, missing persons, computer intrusions, sexual assaults, child pornography, financial crimes, and various other crimes. She has testified as a computer forensics expert in state and Federal court on numerous occasions, using her knowledge and skills to assist in the successful investigation and prosecution of criminal cases involving digital evidence. She is also co-author of the SANS FOR585 Advanced Smartphone Forensics course and a part-time instructor for the SANS Institute.

Daren Melson, Wal-Mart
"Real-World Mobile Forensics: The Intersection of Research, Academia, and Case Work"
Mr. Daren Melson has been programming computers since he was 9 years old. After teaching for 6 years, he started his information technology career in 2000, during which he worked as a programmer and consultant. Mr. Melson first became interested in forensics in 2002, but he did not formally work in computer forensics until 2005. In 2007, after a year-and-a-half of work in private practice, Mr. Melson joined a statewide law enforcement agency for which he worked as a forensic scientist/digital forensics analyst for 6 years. He currently works for the world's largest retailer as an advanced systems engineer and forensic analyst. Mr. Melson has been an active member of the SWGDE since 2009 and currently serves as the vice chair of the Forensics Subcommittee. He has also served as an invited guest scientist at NIST with the CFTT group working in the areas of file carving and federated testing.