D38 Acquisition Techniques of Mobile Devices and Associated Media

Richard P. Ayers, MS, National Institute of Standards and Technology, 100 Bureau Drive, Mail Stop 8970, Gaithersburg, MD 20899-8970*

The goal of this presentation is to provide an overview on mobile device forensics and suggested procedures during the acquisition phase of GSM devices and associated media.

This presentation will impact the forensic science community by providing a brief overview on mobile device forensics and suggested procedures during the acquisition phase of GSM devices and associated media.

Mobile devices incorporating cellular capabilities are ubiquitous and contain a wealth of personal information useful in criminal cases, civil disputes, employment proceedings and recreation of incidents. Data acquisition performed on cellular devices operating over Global System for Mobile Communications (GSM) and non-GSM networks has proven not only frustrating but extremely tedious due to the rapid rate of new cellular devices appearing on the market. Software vendors specializing in cellular forensics are forced to continuously provide updates to software and associated hardware in order to maintain support and provide examiners with solutions for the latest technologies. Multiple hardware and software solutions exist which provide acquisition solutions for various makes and models of cellular devices and associated media. Forensic examination of mobile devices is a small part of computer forensics, in general. Consequentially, tools possessing the ability to acquire data from these devices are slowly maturing and continually expanding. This paper provides a brief overview on mobile device forensics and suggested procedures during the acquisition phase of GSM devices and associated media.

Introduction: Cellular devices continue to expand in storage space (on the order of gigabytes) via associated removable media (e.g., Multi- Media Card [MMC], Secure Digital [SD], memory sticks) and internal hard drives allowing mobile devices to double as mp3 players and personal organizers. Additionally, the intelligence of these devices continues to advance. Personal Information Management (PIM) applications provide functionality comparable to those present on older desktop personal computers. The combination of ever-increasing storage capacities, built-in camera and video functionality alongside faster processing and Internet ready devices, provide users with the ability to store an abundance of personal information. Consequentially, the advancement in technology has escalated the richness of data contained on cellular devices. Therefore, cellular devices are often the key component to solving an incident or bringing justice to involvement in criminal activity.

Data acquisition of mobile devices entails availability of appropriate hardware and associated drivers used to establish connectivity with a software application capable of interpreting and presenting acquired data in a human readable format. Forensic manufacturers are challenged with producing new hardware (i.e., data interface cables) and software (i.e., drivers) which provide forensic examiners with an acquisition solution for emerging technologies. Unlike hard disks whose interface (e.g., Advanced Technology Attachment [ATA], Serial Advanced Technology Attachment [SATA], Small Computer System Interface [SCSI], Universal Serial Bus [USB], Firewire [FW400/800]) standards are nominal, cellular devices do not have a pre-defined interface standard and vary based upon manufacturer and specific models. Non-standardization of mobile device interfaces often times forces examiners to borrow cables from another source (i.e., mobile device acquisition toolkit) in order to acquire the device. The worst-case scenario forces examiners to physically "thumb" the device while recording the process via video camera, where screenshots are used to create a finalized report.

The evolution of forensic software and associated hardware capable of acquiring data from cellular devices is continuous, due to the turnover rate of mobile devices available on the market today. A lack of interface standards often times leads to acquisition complexities involving multiple toolkits yielding a successful acquisition. Therefore, quality control and rigorous testing of mobile device acquisition tools is paramount, in order to provide examiners with a sound application.

Characteristics: Forensic examiners, specialists and associated team members involved with the task of investigating mobile devices should encompass a general understanding of the mixed variety of architectural layouts contained within low to high end cellular devices, smart phones and PDAs (Personal Digital Assistants) embedding cellular technology. Knowledge of mobile device design architecture plays a significant role in device management throughout the life cycle of the investigation or incident. The type of memory present in a device is quite significant in terms of data preservation related to power conservation during transportation to a protected laboratory setting. Generally, mobile devices are comprised of the following elements: a micro-processor, memory, radio-module, digital signal processor, microphone, speaker and a variety of hardware keys that provide application functionality.[3] However, differences in memory layout between low to high-end cellular devices compared to smart device determine the seizure and transit techniques minimizing the possibility of data loss.

Cellular devices (i.e., low to high-end cell phones), designed with the primary purpose of placing and receiving calls, maintain data in flash memory. Typically, the first part of flash memory is filled with the operating system and the second part is allocated for user data. Due to the design of these devices the conservation of power is not as critical as it is for smart devices. Cellular devices that maintain data within non-volatile memory are not subject to data loss via battery depletion. While the criticality of power maintenance

Copyright 2008 by the AAFS. Unless stated otherwise, noncommercial *photocopying* of editorial published in this periodical is permitted by AAFS. Permission to reprint, publish, or otherwise reproduce such material in any form other than photocopying must be obtained by AAFS.

is lessoned, low to high-end cellular devices face the possibility of data loss via network connectivity overwriting recoverable deleted data or the possibility of a key-chord acting as a device restore feature.

The internal memory of smart phones is classically divided into two regions: Flash Read Only Memory (ROM) and Random Access Memory (RAM). Data stored in Flash ROM, such as the operating system (OS) and pre-loaded applications supplied by the manufacturer are hard-coded and protected against erasure during the event of a hard-reset or battery exhaustion. RAM is generally divided into two areas, program memory and an object store. Program memory (used for program execution, loading drivers, and storage for processing information) is cleared much like RAM on a personal computer. The object store retains data during active and quiescent states, but risks data loss in the event of battery exhaustion or a hard reset. Manufacturers may provide users of smart devices with an allocated safe-store folder for sensitive data that the user would like to protect against erasure in the event of a hard reset or battery depletion. Additional sources of memory storage present on high end devices are external memory (e.g., Secure Digital [SD], MicroSD, Multi-media Card [MMC], Memory Sticks) cards which provide users with a non-volatile storage solutions. Smart phones are high maintenance during transit to a protected laboratory setting due to the memory configuration and must be either shut down or powered while protected in a radio-isolated bag lessening the chance of data modification.

SIM Characteristics: The Subscriber Identity Module (SIM), a smart card that contains a processor, read only memory (ROM) and random access memory (RAM), is an essential element combined with the Mobile Equipment (ME) providing users the ability to authenticate and gain access to subscribed services for devices operating over a GSM network. In addition to providing users with extended non-volatile memory storage for personal information SIMs provide users with the ability to port their identity to multiple devices.[3] The GSM 11.11 standard provides useful information related to SIM characteristics, protocols and data elements. The SIM is approximately the size of a postage stamp and is typically located in the battery cavity area of mobile devices. Often times, multiple SIMs are used with a single device, therefore, it is important to carefully search surrounding areas and confiscate all related media or devices. Devices found without the SIM present may cause difficulty in acquiring the internal memory of the related device. Fortunately, tools exist that provide specialists with the ability to create an access card that allows internal memory acquisition to be completed without interruption.

SIMs provide subscribers with a layer of security via a 4-8 digit Personal Identification Number (PIN). Proper authentication is essential for network connectivity. Three incorrect successive authentication attempts lock the card forcing the correct PIN Unblocking Key (PUK) to be entered; if ten consecutive attempts are entered incorrectly the SIM is rendered useless. Therefore, it is advantageous for SIM acquisition tools to present the number of authentication attempts remaining if examiners are forced to attempt to crack the PIN. SIMs are generally pre-programmed with a default PIN, often documented on the manufacturers' site, which may serve as a starting point when alternative means of PIN discovery are not available. Acquiring the contents of the SIM are extremely limited without proper authentication, therefore knowledge of the PIN is invaluable. An abundance of useful information is stored on the SIM such as Abbreviated Dialing Numbers (ADNs), Last Numbers Dialed (LND), Short Message Service (SMS) messages, Enhanced Messaging Service (EMS), subscriber information (i.e., IMSI), and location (i.e., LOCI, GPRSLOCI) information providing additional data separate from the internal memory acquisition of the ME.

A number of forensic software tools have emerged that deal exclusively with SIMs independently of their handsets. The SIM must be removed from the phone and inserted into an appropriate reader (e.g., Personal Computer/Smart Card [PC/SC] reader) for acquisition. The majority of SIM only tools concentrate on a subset of data (e.g., subscriber information, Abbreviated Dialing Numbers [ADNs], Short Message Service [SMS] text messages, call logs, location information [LOCI]) considered most useful as forensic evidence. Tools have begun implementing support for the creation of a radio-isolation card providing examiners with the ability to acquire devices without network interruption, via writable SIM cards. The ability to create an access card of a SIM provides "radio silence" during acquisition eliminating incoming data overwrites of potentially recoverable deleted information. Additionally, the creation of radio-isolation cards or access cards provides examiners with the ability to acquire the internal memory of GSM devices found without the SIM present.

Currently, Universal Subscriber Identity Modules (USIMs) are on the rise. The third generation (3G) card carries out the same functions as it 2G cousin (i.e., SIM) and offers users with greater bandwidth allowing for enhanced multi-media, communication, wireless Internet access and strengthened security mechanisms.

State of the Art Snapshot: The variety of cellular technologies present on the market today has given rise to a multitude of forensic toolkits providing forensic specialists with the ability to acquire data present on various makes and models of mobile devices and related removable media. A considerable number of software tools and toolkits exist, but the range of devices over which they operate is typically narrowed to distinct platforms for a manufacturer's product line, a family of operating systems, or a type of hardware architecture. Although, the majority of toolkits support a full range of acquisition, examination, book-marking and reporting facilities, some tools focus on a subset that provide examiners with the ability to only acquire and produce a final report. Information present on a cell phone may vary depending on several factors such as the capabilities of the phone implemented by the manufacturer, network services subscribed to, or modifications made to the phone by the service provider and/or the user.[1]

Tools capable of acquiring data from cellular devices may provide

Copyright 2008 by the AAFS. Unless stated otherwise, noncommercial *photocopying* of editorial published in this periodical is permitted by AAFS. Permission to reprint, publish, or otherwise reproduce such material in any form other than photocopying must be obtained by AAFS.

examiners with the ability to perform both a logical and physical acquisition. Often times this is dependent upon the device being acquired. Physical acquisition implies a bit-by-bit copy of an entire physical store, a memory chip), while logical acquisition implies a bit-by-bit copy of logical storage objects (e.g., directories and files) that reside on a logical store (e.g., a file system partition). Physical acquisition has advantages over logical acquisition, since it allows deleted files and any data remnants present to be examined, which otherwise would go unaccounted. A logical acquisition, though more limited than a physical acquisition, has the advantage that the system data structures are normally easier for a tool to extract and provide a more natural organization to understand and use during examination. If possible, doing both types of acquisition is preferable – a physical acquisition before a logical acquisition.[2] Additional features of various mobile device forensic tools often protect case files or individual files from modification via encryption or SHA/MD5 hash functions.

Digital Evidence: The amount and richness of data contained on mobile devices varies considerably dependent upon device type and personal usage. Higher end devices such as smart phones or PDAs doubling as cell phones provide users with enhanced applications, capable of storing multiple file types while providing enhanced network connectivity. However, a core set of user data can be defined that remains somewhat consistent on all device types (i.e., low to high-end cellular device vs. smart devices) with cellular capabilities. GSM devices provide two areas of data storage, the internal memory of the device and the SIM. The following data elements stored on the SIM provide useful investigative or incident-solving information.

- Service Provider Name (SPN): The SPN provides examiners with the name of the provider useful for contact information in the event of needing additional SIM assistance.
- Integrated Circuit Card Identifier (ICCID): The ICCID (useful for obtaining the Pin Unlocking Key [PUK]) is the SIM serial number, which is imprinted on the outside of the card or can be acquired with the use SIM acquisition tool.
- International Mobile Subscriber Identity (IMSI): The IMSI is a unique number that identifies the phone/subscription to the GSM network.
- Mobile Subscriber International ISDN Number (MSISDN): The MSISDN is a number that identifies the phone number used by the headset.
- Abbreviated Dialing Numbers (ADNs) – ADNs are phone book entries that may contain a contact name in addition to the phone number.
- Last Dialed Numbers (LDN) – LDNs are a log of the last numbers dialed from the handset.
- Short Message Service (SMS) – SMS or text messages contain incoming messages sent to the device.
- Enhanced Message Service (EMS) – EMS messages are text messages over 160 characters or messages that contain either Unicode characters or a 16x16 to 32x32 black and white image.
- Location Information (LOCI) – LOCI information provides information relative to cell towers communicated with on the network.
- General Packet Radio Service (GPRS) location – GPRSLOCI contains the routing area information for data communications over the general packet radio service.

The following data elements stored in the device's internal memory provide useful investigative or incident-solving information.

- International Mobile Equipment Identifier (IMEI) – A unique 15- digit number that serves as the serial number of the GSM handset useful for determining statistics on fraud or faults.
- Personal Information Management (PIM) data – Data that is associated with the Address book (e.g., name, phone number, email address, address, website) and Calendar entries (e.g., details such as contact name, time, and address, relating to previous and upcoming appointments), To-Do lists, Memos, etc.
- Call Logs – Incoming and outgoing calls in addition to the SIM are found in the internal memory of the device.
- SMS text Messages – Depending upon the device or user setup SMS messages may be stored on either the internal memory of the device or the SIM. Often times, once the maximum limit has been reached for incoming SMS messages on the SIM they will be stored on the internal memory of the device. Additionally, dependent upon the device and user-setup, outgoing messages may be stored in the devices internal memory in a sent folder.
- Multi-media Messages (MMS)/email – MMS messages/email messages are found in the internal memory of the device and have an audio, graphic or video clip associated with them.
- File Storage – Files types such as audio (.mp3), graphic (.jpg) video clips (.avi) are often supported for many cellular devices (mid-level to high-end) and provide an excellent investigative source to examiners.

Preservation: Proper evidence preservation techniques must be strictly observed lessening the chance of data modification or deletion during the life cycle of the examination (i.e., initial seizure to final reporting). Maintaining the present state of mobile devices during transit to a laboratory setting can be problematic and challenging. For instance, a disposable or portable battery charger for the specific make and model of the device seized must be readily available. Maintaining power to the device eliminates the possible triggering of

Copyright 2008 by the AAFS. Unless stated otherwise, noncommercial *photocopying* of editorial published in this periodical is permitted by AAFS. Permission to reprint, publish, or otherwise reproduce such material in any form other than photocopying must be obtained by AAFS.

authentication mechanisms and loss of data contained in volatile memory as discussed earlier in Section 2.

Live devices require eradicating network connectivity via a radio- isolated container or radio-isolation card protecting against incoming or outgoing communication with the network. Incoming data alters the state of the device and potentially may overwrite recoverable deleted data. Additionally, any exposed cables used for maintaining power must be completely isolated to counteract the cable acting as an antenna negating the effect of the radio-isolated container. The Netherlands Forensic Institute (NFI) has developed in in-depth flow chart of preservation techniques when transporting seized mobile devices.

Data Acquisitions: Retrieving data from cellular devices and associated media must be approached methodically following specific techniques in order to preserve data present on the device. As mentioned earlier, cellular devices must be contained in radio-isolated containers or simply turned off during transit to eliminate the possibility of overwriting potentially recoverable deleted data. Turning off the device may trigger authentication mechanisms and prolong the acquisition process, therefore, use extreme caution when using this technique if radio-isolation is not optional. Deleted data elements such as: address book, calendar entries, text messages, and MMS messages can be recovered from the internal memory of the cellular device dependent upon the tool and type of allowable acquisition (physical vs. logical). Furthermore, data elements stored on the SIM are recoverable if proper seizure, transit and acquisition techniques are strictly followed. Contact with the network can potentially destroy data stored either in the internal memory of the device or data stored on the SIM. Tools that traverse and report data stored on the SIM during internal memory acquisition have been noted to change the status of text messages. For instance, one traversal of the data present on the SIM will report an unread SMS message as unread; the second read due to the first traversal changes the status to read. The slight modification could have significant bearing on resolving an incident or criminal activity. Therefore, a thorough understanding of proper acquisition techniques and operations will lessen the chance of modifying existing data. Additionally, data elements that need to be handled carefully to defend against modification or deletion are the call logs (i.e., last numbers dialed). The SIM should never be removed from the phone before internal memory acquisition and additional SIMs found should not be inserted into the target device. Switching out SIMs alters the data stored in the internal memory of the device.

Conclusions: Forensic examination of cellular devices is a growing subject area in computer forensics. Therefore, cell phone forensic tools are a relatively recent development and in the early stages of maturity. Acquisition of data contained on mobile devices is effected by numerous variables such as the type of device being acquired (i.e., low-end versus high-end) and the techniques used during seizure, transit, acquisition, and storage throughout the life-cycle of the investigation or incident.

The goal of this paper is to provide a brief overview of variables and situations to consider when acquiring a mobile device and associated media. Accurate acquisition techniques and methodologies must be adhered to, yielding optimum results. Moreover, continuous education of executing proper forensic techniques and possessing a profound understanding of the examined mobile device and associated application is paramount when handling digital evidence tied to an incident or criminal investigation.

References:

[1] Ayers, R., Jansen, W., 2007, NISTIR 7387, Cell Phone Forensic Tools: An Overview and Analysis Update URL: http://csrc.nist. gov/publications/nistir/nistir-7387.pdf.

[2] Jansen, W., Ayers, R., 2007, SP800-101, Guidelines on Cell Phone Forensics, URL: http://csrc.nist.gov/publications/nistpubs/ 800-101/SP800-101.pdf.

[3] Jansen, W. Ayers, R. 2006, Forensic Software Tools for Cell Phone Subscriber Identity Modules, Conference on Digital Forensics, Association of Digital Forensics, Security, and Law (ADFSL), <URL: http://csrc.nist.gov/mobilesecurity/Publications/JDFSL-proceedings2006-fin.pdf.

Mobile Device Forensics, Cellular Forensics, Digital Forensic Tools

Copyright 2008 by the AAFS. Unless stated otherwise, noncommercial *photocopying* of editorial published in this periodical is permitted by AAFS. Permission to reprint, publish, or otherwise reproduce such material in any form other than photocopying must be obtained by AAFS. ** Presenting Author*