Challenges in Mobile Phone Forensics

Kyle D. Lutes
Associate Professor, Mobile Computing Lab
kdlutes@purdue.edu

Richard P. Mislan
Assistant Professor, Cyber Forensics Lab
rmislan@purdue.edu

Computer & Information Technology
Purdue University

ABSTRACT

As ubiquitous societal components, mobile (or cellular) telephones continue to become increasingly prevalent. With a shrinking footprint and a seemingly ever-increasing storage capacitance, these devices can be warehouses of information about our daily lives. Just as mobile phones permeate our social fabric, they are also becoming more and more crucial as evidentiary devices in civil and criminal investigations. Thus, our law enforcement, intelligence and private investigation communities are grasping for ways to get evidence off each and every mobile device. Some tools and techniques exist for such investigative work; however, there is not yet one good solution. The various manufacturers, models, operating systems, protocols, and cables lend to a combinatorial explosion that leaves most criminal investigators grasping for a cohesive solution.

During a recent project funded by a National Institute of Justice Electronic Crimes Research grant, we experienced these challenges first hand. In this paper, we summarize the issues facing both the criminal investigators hoping to recover evidence from these mobile phone devices as well as the challenges that must be overcome by the technology vendors who are working to develop automated tools to aid the investigators.

Keywords: mobile phones, computer forensics, mobile forensics, pervasive computing

1. RELEVANCE

Mobile phones became part of our world in the late 1990's with the introduction of so-called "bag and brick" phones. The usage of mobile phones has since skyrocketed due to reduced cost, and with the introduction of text messaging features, which launched commercially in 1995. Several key factors that have made the mobile phone so pervasive include the introduction of the pre-paid phones from the second generation networks and the fact that there are over 243.4 million subscribers who can send and receive text messages [6]. By June 2005, estimates of 7.2 billion text messages were exchanged in the US each month, and by 2007 the number has launched to 28.8 billion text messages per month [6]. Other reasons for increased usage of mobile phones include custom ring tones, Internet connectivity, multimedia messaging services, music and video capabilities, games, cameras, and other features.

2. MOBILE PHONE FORENSICS

As daily life and business moves at the speed of electrons through the air, most civil and criminal investigations involve some sort of digital element. As mobile phones become so ubiquitous and play such a large societal role [9], there is a high probability that these same devices will be part of those investigations. There are four ways in which a mobile phone can be tied to crime:

- It can be used as a communication tool in the process of committing a crime.
- It can be a storage device providing evidence of a crime.
- It can contain victim information.
- It can be a means of committing a crime.

Today's criminal investigators must be familiar with mobile phones and understand the intricacies of mobile phone forensics. In other words, acquiring and analyzing the data on the device, attached SIM cards, and inclusive memory cards. These procedures are well documented and should be adhered to in the forensics acquisition and analysis of mobile phone data [1, 2, 3, 4, 5, 10, 11, 12, 18]. However documented, it is well known that there is currently no one examination facilitation tool (hardware or software) that is universally used or recommended to remove the data from each and every mobile phone [17].

Mobile phones can yield an abundance of information. The most obvious kinds of data that can be retrieved from a phone are call logs, contact lists, and text messages. However, in an investigation, other features of a modern mobile phone, such as ring tones, T9 dictionaries, canned responses, video files, still image files, calendar events, miscellaneous documents and data files, and location information can also provide valuable clues. Given the variety of types of information available, it is imperative to examine every single one with utmost precision, especially since it is entirely possible, with the use of specialized tools, to often recover deleted information.

3. CURRENT CHALLENGES

Knowing the importance of the forensics of mobile phone devices, it is essential to understand the current known challenges facing investigators. Using funding from the National Institute of Justice Electronic Crimes Research grant, a survey of the current mobile phone landscape produced six general categories of challenges: 1) carriers and manufacturers, 2) data preservation, 3) power and data connectors, 4) operating systems and communication protocols, 5) security mechanisms, and 6) unique data formats. The following is a realization of these challenges.

Carriers and Manufacturers

In an investigation of a mobile phone, the first action must be the identification of the phone. Given that there are multiple network carriers (at least seventeen in the US alone) and device manufacturers (over thirty in the US), identifying a phone by sight alone is extremely difficult even for trained investigators [8]. A given model from a single hardware manufacturer may be marketed using many different names from the various carriers. A good example of this is the recently popular Motorola RAZR which is marketed under at least 24 different product names. It is not until an investigator removes the device’s battery that the true hardware model can be determined, but removing batteries can cause the phone to lose the information stored in volatile memory, or even worse, force a handset lock code on power up.

Data Preservation

For a mobile phone investigation, it is important to prevent the device from receiving any further data or voice communication. As text messages are stored in a “First In, First Out” order, any new incoming text messages could delete older stored text messages. Likewise, incoming calls could erase call history logs, and some devices (such as the RIM Blackberry) can be wiped of all data remotely if not protected from incoming communications. Therefore, upon initial acquisition, these mobile phones must be placed in some sort of wireless preservation container. Multiple technologies can be used for this with various levels of success. These tools range from three layers of common aluminum foil, to a tri-weave mesh material shield of nickel, silver, and copper [14], to an anodized aluminum shielded enclosure made to withstand wireless devices from radio frequencies [15].

Power and Data Connectors

Another challenge facing investigators is how to preserve power to the phone. If left unplugged for a long enough period of time, a phone’s battery will eventually lose all power. Because many mobile phones store information in volatile memory, a complete loss of power may mean a loss of information, thus a loss of crucial evidence. Therefore, it is desirable to keep a phone in a charging state. Frustratingly, there currently is no standard for power requirements for mobile phones.

This lack of power standards is compounded by the fact that there is also no standard for cable connectors. There are literally hundreds of different mobile phone power connectors currently in use. So even if two phones require the same voltage to remain charged, they likely will not have compatible power connectors.

One group, the OMTP (Open Mobile Terminal Platform) hopes to reduce the number of connectors by recommending the micro-USB standard be adopted across the mobile industry [16]. Even though criminal investigators, and end consumers for that matter, would benefit from such a standard, it is unlikely to happen any time soon as hardware manufacturers are constantly changing designs and will employ whichever connector type helps them achieve their design goals.

Operating Systems and Communication Protocols

Another challenge impeding the development of forensics tools is the various operating systems used on mobile phones. Mobile phones have evolved into full-fledged computing platforms requiring vendors to use sophisticated operating systems so that various software applications can be run on them. Several of the common operating systems in include RIM’s Blackberry, iDEN, Palm, Symbian, Windows Mobile, Macintosh OS X, and various versions of the Linux open-source operating system. Some operating systems are also proprietary to the hardware manufacturer. For example, Nokia has the ISA platform for the Series 30 and 40 phones.

The challenge of having all these operating systems is knowing which protocols to use for communication between the evidentiary mobile phone and the forensic investigator's computer. Some of the more well-known data communication protocols currently in use are AT, BREW, FBUS, IrMC, MBUS, OBEX, and SyncML [4, 13] and are highly dependent on the operating system and restrictions imposed by each carrier.

Often proprietary, sometimes very cryptic, and hardly ever documented [19], these protocols can be used to retrieve information from a mobile phone such as its make and model, telephone number, software revisions, serial number, call logs, contacts, text messages, ring tones, videos, images, and other important pieces of data. Unfortunately, almost every phone implements a different flavor of each of these protocols, seeming never to respond to the same commands the same way. Worse still, several operating systems require the examiner to first copy program files directly to the device in order to open a communications channel so that critical evidence can be retrieved. However, the mere act of copying data to a mobile phone has the potential to erase evidence.

One more note should be made about how protocols may sometimes change data. For example, in some phones, using the built-in protocols to access messages in the message store will mark the message as read even if the user has never seen the message. This necessity to access information on the phone, even if it changes the state of the phone should be seriously considered. In some cases, evidence retrieved from a phone that required changing information on the phone can not be used in a court of law [8].

Security Mechanisms

There are several security mechanisms used on mobile phones to protect data. These securing mechanisms range from manufacturer or user handset locks, to SIM card PINs and PUKs [20]. Whichever type of security is employed, the implications differ depending on the make and model of the device. Many mobile phones have a handset lock code that is either set by the manufacturer (Motorola – 000000, Nokia – 1234), the last four digits of the current phone number, or set by the user which is even more problematic. The handset lock is normally activated upon power-up, which presents a problem for examiners who must attempt to investigate a phone that was found or seized in a powered off state.

One of the most heavily used network technologies the world over, is Global Systems for Mobile communication (GSM). Most GSM phones will contain a SIM card, which contains a light-weight processor chip and a small amount of non-volatile memory. In GSM phones, the SIM card is used as a storage device for subscriber related data. The only purpose of the SIM's processor is to implement the access mechanism and security features. The physical and logical properties of the access mechanism are defined in GSM specifications. [7]

A physical connection can be made by mounting the SIM in a standard smart-card reader attached to a typical PC. Software running on the PC is necessary to logically access the SIM. The software is needed to implement the GSM SIM access mechanism. The contents of the SIM card is organized as a series of files containing binary data that can be transferred to a PC once the user has authenticated himself with a PIN and/or PUK code.

A PIN (Personal Identification Number) is not usually required to gain access to the SIM. Since the phone cannot be used without access to the SIM, this number must be entered whenever the phone is turned on. If the user fails to enter a valid PIN through three attempts, the card becomes blocked, and the user must instead enter an 8-digit code, called a PUK (Personal Unblocking Key), to reopen it. If the user fails to enter the correct PUK after ten attempts, the card becomes permanently blocked and cannot be reopened.

PINs for a card can be changed and deactivated by the user. The PUKs are fixed and cannot be changed. Since the PUK is fixed, the network operator usually keeps track of the PUKs for all of its users. Therefore, the investigator can almost always gain access to a SIM card by asking the network operator for the correct PUK. It might, however, be more efficient to ask the owner of the phone to provide correct PIN or PUK codes. During searches, the PUK might also be recovered, since phone owners sometimes keep the PUK in writing in case they forget the PIN [20].

Even after gaining access to the data on the mobile phone, an additional barrier may be present. Data stored in files on mobile devices are sometimes stored in an encrypted form using proprietary encryption algorithm. This encryption can then make understanding the data much more difficult or even impossible without help from the hardware or operating system vendor.

Unique Data Formats

Assuming that the carrier and manufacturer of a phone can be identified, that the phone can be protected from wireless activity, that the correct power and data connector wiring can be found, and that the information is not stored encrypted, it is then theoretically possible to retrieve information from the phone. However, one more obstacle remains. As with the other components that make up a modern mobile phone, there is neither a standard format nor a standard location, for much of the information desired by an investigator.

Data files might be stored in several places. As mentioned earlier, some information can be stored in the memory located on the phone's SIM card. Mobile phone hardware also contains random access memory (RAM) that can be segmented as volatile (requires an electrical charge to retain information), or non-volatile (retains information without an electrical charge). Investigators and makers of forensic software need to be aware that information might be hiding in all these types of memory. Many mobile phones also contain read-only memory (ROM). However, ROM is typically used to store the phone's operating system and is not easily changed by the end user. Because the contents of ROM are not easily changed, the files stored here are likely of little interest to an investigator.

Textual information such as telephone numbers, address books, email messages, and text messages are stored using proprietary file formats. Makers of forensic software tools will need to be aware of these formats so they can write software that will convert these files to information easily understood by humans. An exception to these proprietary file formats is for image and video files which are typically stored in common JPG and MPEG formats.

4. CONCLUSIONS

Modern mobile telephones are now ubiquitous in our society and have evolved into full-fledge computing platforms. Thus they are also becoming more and more crucial as evidentiary devices in civil and criminal investigations. Mobile phones can yield an abundance of information including call logs, contact lists, text messages, ring tones, T9 dictionaries, canned responses, video files, still image files, calendar events, miscellaneous documents and data files, and location information. However, there is no one tool for investigators to used to retrieve evidence from these devices so that it can aid in investigations.

The most likely deterrents to a vendor of forensic tools from creating one single solution is: the number of carriers and hardware manufacturers; the challenge of preventing a phone from receiving incoming messages while at the same time keeping it powered; the hundreds of electrical and data connectors currently in use; the many operating systems and communication protocols being used; the security mechanisms in place on some phone; and the unique data formats used by vendors for storing relevant information.

5. REFERENCES

[1] Association of Chief Police Officers/National Hi-Tech Crime Unit. (n.d.)The Principles of Computer Based Electronic Evidence. Retrieved September 12, 2007 from http://www.acpo.police.uk/asp/policies/Data/gpg_computer_based_evidence_v3.pdf

[2] Ayers, R., Jansen, W., Cilleros, N., Daniellou, R. (2006). An Overview of Cell Phone Forensic Tools. Retrieved on Sept. 10, 2007 from http://www.techsec.com/TF-2006-PDF/TF-2006-RickAyers-MobileForensics-TechnoForensics.pdf

[3] Ayers, R., Jansen, W., Cilleros, N., Daniellou, R. (2006). Cell Phone Forensic Tools: An Overview and Analysis. Retrieved on Sept. 12, 2007 from http://csrc.nist.gov/publications/nistir/nistir-7250.pdf

[4] Ayers, R., Jansen, R., Moenner, L., Delaitre, A. (2007). Cell Phone Forensic Tools: An Overview and Analysis Update. Retrieved on Sept. 10, 2007 from http://csrc.nist.gov/publications/nistir/nistir-7387.pdf

[5] Ayers, R. P. Jansen, W. A. (2006). Forensic Software Tools for Cell Phone Subscriber Identity Modules. Association of Digital Forensics, Security and Law , April 20-21, 2006 , Las Vegas, NV.

[6] CTIA. (June 2007). Wireless Quick Facts Mid-Year Figures. Retrieved on Sept. 10, 2007 from http://ctia.org/media/industry_info/index.cfm/AID/10323

[7] ETSI (1995). Digital cellular telecommunications system (Phase 2+); Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface (GSM 11.11). Retrieved Sept. 10, 2007 from http://www.ttfn.net/techno/smartcards/gsm11-11.pdf

[8] Gratzner, V., Naccache, D., Znaty, D.(2006). Law Enforcement, Forensics and Mobile Communications. Retrieved on Sept. 10, 2007 from http://www.cl.cam.ac.uk/~fms27/persec-2006/goodies/2006-Naccache-forensic.pdf

[9] Hylton, H. (2007). What Your Cell Phone Knows About You. Time. Retrieved on September 1, 2007 from http://www.time.com/time/health/article/0,8599,1653267,00.html

[10] International Organization on Computer Evidence (2000). Good Practices for Seizing Electronic Devices - Mobile Telephones. Retrieved September 12, 2007 from http://www.ioce.org/fileadmin/user_upload/2000/ioce%202000%20electronic%20devices%20good%20practices.doc

[11] Interpol Mobile Phone Forensic Tools Sub-Group. (2006). Good Practice Guide for Mobile Phone Seizure & Examination. Retrieved September 12, 2007 from http://www.holmes.nl/MPF/Principles.doc

[12] Jansen, W., Ayers,R. (2007). Guidelines on Cell Phone Forensics. Retrieved Sept. 10, 2007 from http://csrc.nist.gov/publications/nistpubs/800-101/SP800-101.pdf

[13] McCarthy, P. (2005). Forensic Analysis of Mobile Phones. Retrieved Sept. 10, 2007 from http://esm.cis.unisa.edu.au/new_esml/resources/publications/forensic%20analysis%20of%20mobile%20phones.pdf

[14] Paraben. (n.d.). Paraben's Wireless StrongHold Bag. Retrieved on September 20, 2007 from http://www.paraben-forensics.com/catalog/product_info.php?products_id=173&osCsid=45231cbd175b01532932e348deac741f

[15] Ramsey Electronics. (n.d.). STE3000B - RF Shielded Test Enclosure. Retrieved on September 20, 2007 from http://www.ramseyelectronics.com/cgi-bin/commerce.exe?preadd=action&key=STE3000B

[16] Ray, B. (2007). One plug to rule them all. The Register. Retrieved on September 21, 2007 from http://www.theregister.co.uk/2007/09/21/omtp_data_standard/

[17] Robinson, G., Smith, G. (2001). Evidence from mobile phones. The Legal Executive. Journal of the Institute of Legal Executives. Retrieved on September 12, 2007 from http://www.ilexjournal.com/special_features/article.asp?theid=284&themode=2

[18] Scientific Working Group on Digital Evidence. (2007). Special Considerations When Dealing With Cellular Telephones. Retrieved September 12, 2007 from http://68.156.151.124/documents/swgde2007/SpecialConsiderationsWhenDealingwithCellularTelephones-040507.pdf

[19] Traud, A. (n.d.). 3GPP TS 27.005 / 27.007 Retrieved Sept. 10, 2007 from http://www.traud.de/gsm/index.html

[20] Willassen, S. (2003). Forensics and the GSM Mobile Telephone System. International Journal of Digital Evidence. Spring 2003 Volume 2, Issue 1. Retrieved Sept. 10, 2007 from http://www.ijde.org/docs/03_spring_art1.pdf