UDC 343.3/.7:340.6 *Pregledni rad*

CHALLENGES IN MOBILE FORENSICS TECHNOLOGY, METHODOLOGY, TRAINING, AND EXPENSE

Edita Bajramović

American University in Bosnia & Herzegovina, BOSNIA & HERZEGOVINA,
e-mail: edita.bajramovic@gmail.com

Abstract: *Mobile devices present special challenges to the digital forensic investigator. Creating a single method or forensic tool to address all scenarios involving the growing number of mobile devices poses an ever-changing challenge [1]. To meet these digital forensics challenges and to allow complete investigation of different mobile devices, the development of new forensics tools and investigative methods is required [2]. Data on mobile devices can be located in different locations, such as on SIM cards, a device's embedded and removable memory. Also, data associated with calls and subscribers is kept by the service provider [3]. Mobile forensic investigators must constantly receive updated training to sustain their level of expertise. Because of the evolving nature of the digital forensic field, a continuous training plan must be in place, based on existing training resources [4]. This paper will present challenges in mobile forensics technologies, methodologies, training, and expenses as well as a proposal example to address these challenges.*

Keywords: *challenges, mobile forensics, training.*

1. INTRODUCTION

Mobile devices such as cell phones, smartphones, and tablets present special challenges to the digital forensic investigator. Copyrighted operating systems, different firmware applications and network communication protocols, and varied data storage systems represent unique issues for the investigator trying to locate data on mobile devices [2]. Mobile forensics investigations—an extremely specific area of digital forensics— require skills and knowledge exceeding basic digital forensic training [4]. First-hand knowledge is required to carry out an effective investigation of mobile devices. Without the appropriate knowledge, expertise, and practice, a forensics investigator is vulnerable to serious mistakes, mistakes that could destroy important data [4]. This paper will present challenges in mobile forensics technologies, methodologies, training, and expenses as well as a proposal to address these challenges.

2. CHALLENGES IN MOBILE FORENSICS TECHNOLOGIES

Mobile device forensic investigators face many challenges, thanks to rapid growth in mobile technology. New types of mobile devices are developed every week. Creating a single method or forensic tool to address all challenges associated with these numerous and evolving mobile devices poses tremendous challenges [1]. Also, mobile device companies do not share the same techniques for storing data. The majority of mobile devices use locked and copyrighted operating systems and interfaces [2]. New forensics tools and investigative methods must be developed to meet digital forensics challenges and to allow complete investigation of different mobile devices [2]. For example, some tools can extract more SMS and other data than other tools. Also, some computer forensic tools have integrated mobile forensic tools. For example, Cellebrite UFED mobile forensic tool investigator is able to pull out, interpret, investigate, and report most technically advanced mobile data [5]. This tool has a built-in SIM reader and can extract physical and logical file systems and passwords even if they are deleted [5]. In addition, an investigator can use Cellebrite UFED on various phones, including smartphones, GPD devices, and tablets [6]. Furthermore, Cellebrite UFED can extract call history, text messages, contacts, calendar, email, chat, etc. Another great feature is its integrated battery that allows an investigator to use the tool for up to five hours [7]. Cellebrite UFED is user friendly and features a simple interface. One of the weaknesses for smaller companies is its price [7]. This tool could be strengthened by using a direct transfer to a media forensic format, for example, dd [7].

The signal of a mobile device is another technological challenge that arises during a mobile forensics investigation. Signals must be blocked to forbid any new access to the mobile device, but blocking signals causes battery power to be used up more quickly than usual [2]. To overcome this weakness, the investigator should perform the mobile device forensics investigation in properly isolated and shielded forensic labs. Also, the investigator can use a Faraday bag [8]. Using this bag limits the spread of digital signals.

Data cables for each mobile device are different. Hence, the identification and collection of such cables necessary for mobile device forensics investigation presents a challenge [2]. Creating databases describing mobile devices and their cables, with labels, helps the investigator identify the appropriate cable for a mobile device [2].

A number of mobile device users employ a personal identification number (PIN). A PIN is used to lock the mobile device [9]. Investigators must be careful while working with a PIN. Continuously entering a wrong PIN, while attempting to unlock the mobile device, causes the system to lock. If the investigator locks the system, only by applying a PIN unblocking key (PUK) will the investigator be able to unlock the mobile device. Another technological challenge in mobile forensics is entering several PUK failures [9]. PUK failures lock and deactivate the mobile device permanently. The PUK is usually kept by the service provider. Also, some mobile device producers use a master lock to prevent mobile devices from connecting to different wireless networks [9]. This master lock can make data undetectable to forensic investigators. Therefore, the only source for retrieving this lock is usually the service provider [9].

Data on active mobile devices is likely to be altered and modified continuously in the absence of write-blocking tools [2]. An investigation must be completed on a device that is turned on. During an investigation, the device should not have incoming calls, SMS, etc. [2]. Performing the investigation in a shielded forensic lab can resolve this problem.

3. METHODOLOGY IN MOBILE FORENSIC INVESTIGATION

Data on mobile devices can be located in different locations such on a SIM card, the device's embedded and removable memory. Also, data associated with calls and subscribers is kept by the service provider [3]. Sources of evidence on mobile devices include:

- Provider information––IMSI, IMEI, and PIN/PUK [8]
- Phone information––Calls, MMS, SMS, and pictures [8]
- SIM card––phone numbers, text messages [8]
- Removable card––pictures [8]

Data extraction on mobile devices can be performed using manual, physical, or logical methods.

A manual method is usually used when investigators need only to extract specific evidence from the mobile device [1]. Sometimes, by performing the manual method on a mobile device, the investigator can easily overlook digital evidence—especially if the investigator is new to mobile device extraction or inexperienced [1]. For example, a digital investigator may overlook a mobile device application, such as one that exchanges secret messages. Overlooking such an application, thus failing to investigate its contents, results in missing digital evidence possibly important to the case. [1] To decrease the possibility of overlooking important data on a mobile device, the investigator should look at each screen and application systematically and document the outcomes [1].

The physical method executes data extraction at a low level while the logical method uses communication protocols obtainable by the mobile device at a higher level [3]. Each of these methods has its strengths and weaknesses. For example, performing an investigation using the physical method, the investigator can gather the contents of the complete device memory as well as deleted items [3]. Furthermore, physical acquisition methods can be used with damaged mobile devices. Also, this method makes fewer modifications to the original device during data acquisition [1]. However, this method takes a long time and involves compound and costly tools. Consequently, the investigator gets a raw image [3]. A raw image is generally encrypted, and, if the investigator is able to decrypt an image, additional investigation can be accomplished only by using particular and sophisticated software tools [3].

On the other hand, using a logical technique, the investigator can gather data instantaneously in a form that is readable. However, the volume of gathered data is considerably lower than in an extraction process using the physical method [3]. Using the logical acquisition method, the investigator may snag evidence such as date and time stamps as well as location inside the file system [1]. In certain scenarios, evidence gathered from a data cable can be different from the evidence pulled out through Bluetooth. The investigator should execute the logical method in various ways to make sure all potential evidence is pulled out [1]. In addition, memory cards are usually investigated using computer forensic tools and methods such as physical image acquisition.

4. TRAINING AND EXPENSES IN MOBILE TECHNOLOGY FORENSIC EXAMINATION

As mobile technology is growing and changing each day, new and upgraded technologies and methodologies, as well as cutting-edge training, are required for the digital forensic

investigator. Mobile forensics investigators must know their roles and duties while performing mobile device forensics and have appropriate training and education on associated forensic tools, policies, instructions, and procedures [4]. In addition, mobile forensics investigators should also discuss thoroughly with legal counsel activities that should and should not be carried out in different situations for a particular case. Furthermore, upper-level management should support forensic abilities, evaluate and approve forensic policies, and investigate and approve rare forensic actions necessary in a specific situation [4].

Last, mobile forensic investigators must constantly receive updated training to maintain their level of expertise. Because of the evolving nature of the digital forensic field, a continuous training plan must be in place, based on existing training resources [4]. Training should focus on tools and equipment used by investigators, on-the-job training, and real-world scenarios. Investigative organizations, colleges, and universities can offer training to investigators working in this field [4]. Clearly, budget approval and required personnel are necessary to perform this type of training. Many expenses, such as ongoing training on updated tools, are reoccurring and should be planned on at least a yearly basis [4]. As new versions of tools are developed, old training methods become obsolete and must be updated. In addition, purchasing new versions of tools is an additional expense for the digital forensic investigator [4]. Also, shielded labs—even at great expense—are required for mobile forensics investigation and training.

5. PROPOSAL EXAMPLE

SUBJECT: Proposal on Technology, Methodology, Training, and Expenses Challenges

This proposal addresses technology, methodology, training, and expenses challenges associated with mobile device forensic investigation.

Mobile device forensic investigators face many challenges. Rapid growth in technology sparks the development of new mobile phones every week. Among the profession's greatest challenges is to develop a single technique or forensic tool to address these challenges [1]. Also, as new mobile devices develop, investigative technologies, methodologies, and training must be kept up to date. All these challenges point to higher training expenses.

The explosion in the development of mobile devices also presents many challenges to investigating mobile device data quickly and successfully. No free tools exists that could investigate every single mobile device on the market. As mobile devices develop, investigation methodologies must develop concurrently.

All these changes point to the need for continuous training of digital forensic investigators and necessarily impose additional expenses for mandatory classes, on-job-training, and training on new tools, at minimum.

To overcome mobile forensics challenges, makers and vendors of mobile forensics investigation tools must continue to develop new tools. Development of new and upgraded tools will enable investigators to perform better quality investigations.

In addition, investigators must be trained to choose appropriate acquisition techniques because related expenses, risks, and benefits can differ considerably. Upper-level management must understand the importance of mobile forensic investigations and provide necessary financial resources so investigators can keep pace with challenges.

6. CONCLUSION

An explosion in the development of mobile devices presents many challenges to forensic experts attempting to investigate mobile device data quickly and successfully. No free tools exists that could investigate every single mobile device on the market. Concurrent with mobile device developments, mobile forensics technologies, methodologies, and training are changing and becoming more expensive. To sustain professional readiness and to perform quality mobile device forensic investigation, investigators must receive appropriate training and have access to adequate budgets.

BIBLIOGRAPHY:

[1] Casey, Eoghan. Digital evidence on mobile devices. In *Digital evidence & Computer Crime: Forensic science, computers, and the Internet* (3rd ed.). London, England: Academic Press. 2011, http://www.elsevierdirect.com/companion.jsp?ISBN=9780123742681

[2] Zareen, Amjad, and ShamimBaig. Mobile phone forensics: Challenges, analysis and tools classification. Proceedings of the 2010 International Workshop on Systematic Approaches to Digital Forensic Engineering. 47-55. *IEEE Computer Society*.2010.

[3] Mobile phone forensics challenges.*eForensics Magazine*. June 15th, 2012. http://eforensicsmag.com/mobile-phone-forensic-challenges/.

[4] Ashcroft, John, Deborah. J.Daniels, and Sarah V. Hart. Forensic examination of digital evidence: A guide for law enforcement. *U.S. Department of Justice*. 2004, https://www.ncjrs.gov/pdffiles1/nij/199408.pdf.

[5] Gogolin, Greg. Digital forensic toolkit. In *Digital forensics explained*. New York, NY: Taylor & Francis.2012.

[6] Physical extraction and decoding from android devices. *Cellebrite*,2013, http://www.cellebrite.com/mobile-forensic-company/the-cellebrite-advantage.html.

[7] Cellebrite UFED Touch Ultimate. *SC Magazine*. May 1st, 2013. http://www.scmagazine.com/cellebrite-ufed-touch-ultimate/review/3870/.

[8] Gogolin, Greg. Mobile forensics. In *Digital forensics explained*. New York, NY: Taylor & Francis. 2012.

[9] Kouns, Tom. Computer forensics in a mobile world. CICS. November 29th, 2009. http://www.cicsworld.org/ blogs/tdkouns/2009/11/computer_forensics_in_a_mobile_3.html.