Integrated Economy and Society: Diversity, Creativity, and Technology
16–18 May 2018
Naples • Italy

make learn
TIIM

Management, Knowledge and Learning
International Conference 2018
Technology, Innovation and Industrial Management

A DIGITAL FORENSIC TOOL FOR MOBILE DEVICES: PARABEN

Hitesh Sachdev
Georgia Southern University, United States
hs02955@georgiasouthern.edu

Hayden Wimmer
Georgia Southern University, United States
hwimmer@georgiasouthern.edu

Lei Chen
Georgia Southern University, United States
lchen@georgiasouthern.edu

Chaza Fares Abdul-Al
Robert Morris University, United States
cfast353@mail.rmu.edu

Loreen M. Powell
Bloomsburg University, United States
lpowell@bloomu.ed

Abstract:
Digital forensics is a growing field with many career opportunities within the Accounting, Information Systems and related fields. As a result, many accounting, information system and technology related degree programs are integrating digital recovery, fraud examination or digital forensic courses into their curriculum. However, this are a limited amount of teaching resources available on this topic. This paper adds to the body of knowledge and teaching resources regarding a popular digital forensic tool, the extraction process, and types of data recovered.

Keywords: Digital Forensics, Accounting Forensics, Paraben, Mobile Phone Forensics Analysis, Forensics Tools

1. INTRODUCTION

Digital forensics is relatively new science that is vastly growing due to cloud storage and mobile devices ubiquitous influence. Currently, there is an increasing number of employment opportunities in this field (Edward, 2012; Kearns, 2015, Mishra, & Singh, 2017). As such, many accounting, information systems (IS) and technology related degree programs are developing digital forensic courses within their course offerings (Fleming, Pearson, & Riley, 2008; Henry & Venkatraman, 2015; Kearns, 2015; Seda & Kramer, 2008).

Additionally, the digital forensic/fraud examining field is a vast field with numerous application tools available In an effort to create a real-world learning environment, many educators seek to supplement the text with cases, articles and other teaching resources. (Harron, Langdon, Gonzalez, & Cater, 2017; Namin, Aguirre-Muñoz, & Jones, 2016). However, there is a limited amount of academic resources available for educators within the digital forensic area. Many resources available explain are very technical in nature, explore the digital forensic tools typologies, and explain the benefits of the forensic analysis tools. However, the resources lack concrete evidence for students to see and understand. This paper seeks to explain the need and increase usage of digital forensic tools in general, the Parben, tool, and specific examples of data. This paper also seeks to add to the academic knowledge base of teaching resources for accounting, IS and related educators teaching digital forensic, or fraud related courses. Implications include an overview of the state of the art and knowledge for practitioners and academics as a teaching resource regarding Paraben. The remainder of this paper is structured as follows: review of the literature, Paraben, and conclusion.

2. REVIEW OF LITERATURE

In today's modern world mobile phones are omnipresent containing people's daily life. Thus, mobile phones have become a digital repository, which includes all the basic information about the user from their daily scheduled meetings to personal information. As such, the ubiquitous presence of mobile phones has led the smart/mobile phones to be present in all the illegal activities from child pornography to terrorism (Rakočević,, Pavlović, & Ivanović, 2017). In 2013, a 24-year-old man was arrested by Racine police because child pornography was discovered on his mobile phone (Fox, 2013). This is just one example of child pornography, there are millions of people arrested and data was recovered using mobile phone forensics analysis. Similarly, in the recent Paris terrorist attacks, mobile phones played a vital role and facilitated the terrorists to elude intelligence services. As an article in *The New York Times* reports: "the three teams in Paris were comparatively disciplined. They used only new phones that they would then discard, including several activated minutes before the attacks, or phones seized from their victims" (Moody, 2016).

Researchers have introduced multiple tools and frameworks for mobile phone forensic analysis. Curran, Robinson, Peacocke, and Cassidy (2012) explain the actual meaning of mobile phone forensic analysis: what it means, who avails of it, and the software tools used for the analysis. For maximum data recovery for forensic analysis this paper explains guidelines for it. Al-Zarouni (2006) talks about how computational power of the mobile devices and the data present in it has turned them into evidence in civil and criminal cases. The paper examines some newer information found on the phone that can become potential evidence. It explains some differences between computer and mobile forensics like operating system and file systems, hardware, forensic tools and tool kits available etc. It also covers some weakness of mobile forensic toolkits and procedure and finally it shows how mobile forensic evidence needs more in depth examination (Al-Zarouni, 2006). SIM (subscriber identity modules) can also be used for retrieving information. Curran et al. (2012) explain different types of SIM available in the market and the different types of analysis on it. In the last part, the authors explain the different types of tools available for forensic research.

There are multiple ways/tools to analyze the mobile phone forensic data and there are multiple sources of it. Tassone, Martini, Choo, and Slay (2013) used three different tools and they used them on three different platforms: Apple, Android and RIM's BlackBerry. They identify where each tool can be best used. They also gave the limitations of all the three tools in accessing different information like web history, SMS, Email, images, and other data (Tassone et al., 2013). The most common mobile phone used is Android. Vidas, Zhang, and Christin (2011) talk about the Android platform forensic analysis. Authors have explored special device boot mode, android's partitioning system schema and discussed composition of an Android bootable image for forensic analysis. It describes a general process for data collection of Android devices and results of experiments on different Android devices. Digital forensic tools could be used for analyzing the data from social websites like Facebook, Twitter etc. Al Mutawa, Baggili, and Marrington (2012) use different tools for forensic analysis of this data from mobile devices. iPhone, Android and Blackberry phones were used to recover the data from the internal memory in their forensic test. All the smartphones used different tools for forensic analysis: BlackBerry used BlackBerry Desktop Software, iPhone used iTunes application, and unlike the other two devices, android does not have a software to manage and or backup applications. So, they rooted the android phone using Odin3 which gave them the access to protected directories on the system. The results show that nothing could be recovered from BlackBerry devices. On the other hand, iPhone and Android store a significant amount of data which can be used for forensic research.

Privacy in application is a big concern and there are several aspects that are considered when trying to assess the privacy level of an application. According to Stirparo and Kounelis (2012) data can exist in various forms: data at rest, data in use, and data in transit. All the different aspects use different methodologies and technologies. Stirparo and Kounelis (2012) talk about the data at rest. Their paper mainly demonstrates how this data can be retrieved using free open source tools.

Klomklin and Lekcharoen (2016) talk about how law enforcement agencies in each country are using mobile phones in order to obtain information against criminals. They also talk about how improperly managing and collecting of evidence can impact the investigation. This paper studies the mobile phones forensic procedure and existing behavioral performance of law enforcement agency in Thailand. Authors divided the study into 3 main steps: 1) studying general mobile phone forensics processing and procedures. 2) Qualitative research using Focus group included 20 experts from law enforcement agencies. 3) Quantitative research using 200 questionnaires. At the end, they provided a new framework of mobile phone forensics processing and procedures for Thai law enforcement agencies. Quick and Choo (2016) developed a framework for data volume reduction which focuses on the registry, documents, spreadsheets, email, internet history, communications, logs, pictures, videos, and other relevant file types. When this framework was applied to the Australian Law Enforcement Agency, the data volume was slightly reduced leaving only the main evidential files and data.

Table 1: RCFL From Their Various Regions Adopted From FBI (2010)

RCFL	Data Process
Chicago	585
Greater Houston	306
Heart of America	335
Intermountain West	420
Kentucky	153
Miami Valley	138
New Jersey	227
New Mexico	225
North Texas	410
Northwest	145
Orange County	436
Philadelphia	470
Rocky Mountain	180
San Diego	590
Silicon Valley	347
Western New York	93

The computer Analysis Response Team (CART) is the Federal Bureau of Investigation's (FBI) go-to force. Almost 500 highly trained and certified special agents and other professional personnel work for CART at FBI headquarters. During 2012, CART examined almost 10,400 investigations and conducted more than 13,300 digital forensic examinations with more than 10,500 terabytes (1012) of data (FBI, 2013).

In year 2009, on 10-year mark of the Regional Computer Forensics Labs (RCFL), they examined various media type devices producing terabytes (1012) of information. These consist of computer hard drives (15,630); CD/DVDs (14,028), floppy disks (4,104); flash media (2,820); cell phones and smart phones (1,953); CPUs (684); digital cameras (148); digital media players (95), and navigation systems (54). From New Jersey, RCFL confiscated approximately 600 gigabytes (109) of information from a man who was maintaining a website dedicated to child pornography and child sex (FBI, 2010). Table 1 below shows the amount of data collected by RCFL from there various regions in the United States (US)

2.1.Conceptual Framework of Digital Forensics

According to the Digital Forensic Research Workshop in 2001, Digital Forensic Science is defined by Carrier (2003) as:

> *"The use of scientifically derived and proven methods towards the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital source for the purpose of facilitating or furthering the reconstruction of events to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations".*

Computer forensic is relatively young discipline as comared to other forenisc sciences. Computer Crime and Intellectual Property Section (CCIPS) designed some steps for digital analysis methdology. It was designed referring various for computer forensic experts and federal agensices.

There are multiple elements in the process but there are three main steps for the analysis of computer forensic data i.e. Data Extraction, Identifications and Analysis.

1. *Data Extraction*

   Examiners see if there is sufficient data then they start the process. The examiners duplicate the forensic data and integrity of the data is analyzed. A plan is developed to extract the data and the examiner should know what they are looking for in the forensic image. After fetching the data, they add in into a list known as "Extracted Data List".

2. *Identification*

   After the extraction process the examiners analyze the data and see if the data is relevant. If the data is relevant, then the examiner document it into a document list known as Relevant Data List. If they find something outside the scope of the original search warrant, then it is recommended that the examiner immediately stops all activity, notify the appropriate individuals, including the requester, and wait for further instructions.

3. *Analysis*

   Examiners in this phase try to answers all the questions like who/what, where, when, how. For each relevant data found the examiners tries to explain when it was created, accessed, modified, received, sent, viewed, deleted, and launched. After the examiner has analyzed the relevant items, they move to the reporting phase where all the finding is documented so that the layman can understand and use them in the case.

3. PARABEN

Paraben is in the digital forensic industry since 2001. It is one of the leading tools available for digital forensic in the market. Paraben allows forensic experts to optimize time and get the most data possible. A wide range mobile investigations tools are provided by Paraben. Table 2 explains these tools.

3.1 Paraben for Android

This research employed the Paraben forensic tool for extracting the forensic data from mobile devices. The data was extracted from a ZTE phone, model number Z812, android version 5.1 (Lollipop). For extracting the data new case was created with the name of “Workspace.ds”.
The process utilized followed the standard digital forensic process. For step 1, the data extraction phase, we used the smartphone to fetch the information. Using Paraben recovery stick we duplicated the smartphone data. We created an image of the phone and stored it into the workspace we created using the stick. For the identification phase we aimed to recover the phone data and see what valuable information is available in it. In the last phase we tried to answer all questions like what kind of data was available, whether some questionable/useful data was present in the phone or not.
The paraben stick helps recovering multiple options like contacts, messages, call history, applications etc. We will discuss each part one-by one.

Table 2: Types of forensic tools offered by Paraben

Paraben Tool	Description
E3: Universal	Process all types of evidence.
E3: DS	Support of all mobile devices, smartphones, GPS, eReaders, drones
E3: Viewer	Case agent and attorney review platform for digital data
PAP Flex	Flexible camera system for taking pictures of mobile devices, tablets, and other items.
Mobile Field Kit	Field deployable system that lets you get all types of mobile data.
Hawk Monitoring	Active mobile monitoring and capture of data from Android and iOS

Figure 2 shows recovered contact information. It showed all the contacts that were saved in the cell phone. It also showed the information which was from 2005 linked to “Orkut” account which was linked with a Gmail account. It

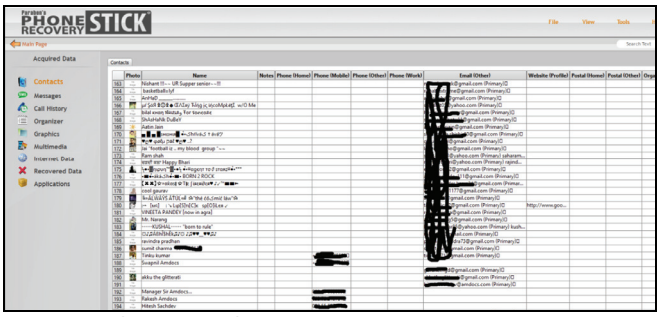

Figure 2: Contact Information

Figure 3 represents the message information of the user. It includes “MMS and SMS’s” from different users. In the recovered data you can see different fields like “data, address (from and to), type, subject” etc.

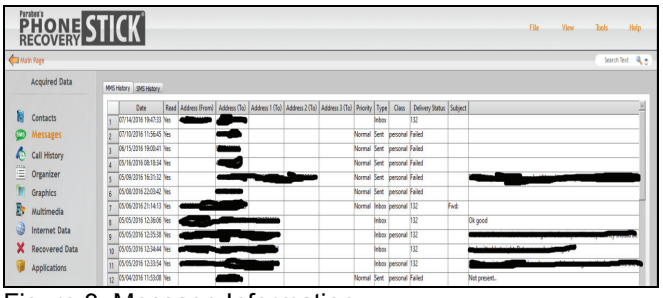

Figure 3: Message Information

This tool gives you the entire call history including type of call, duration of call etc. It can be viewed in figure 4.

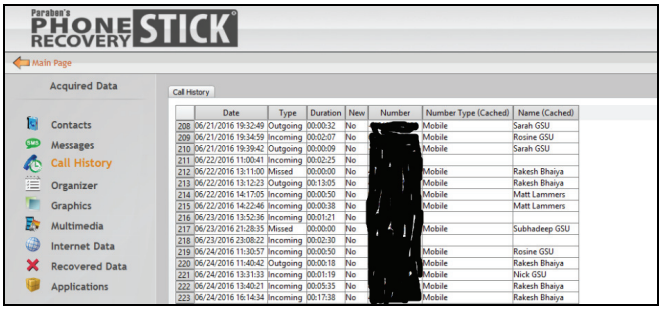

Figure 4: Call History Information

Paraben forensic stick has the capability to recover even the different events which were associated with the person. Figure 5 shows all the organizer/events information about the user.

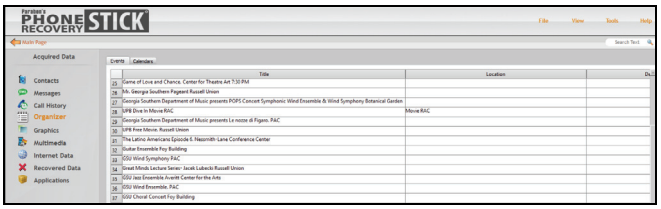
Figure 5: Organizer Information

Graphics information shows all the pictures which were received/sent from different applications like “WhatsApp”, “MMS” etc. by the user. Figure 6 shows the graphics information of the user.

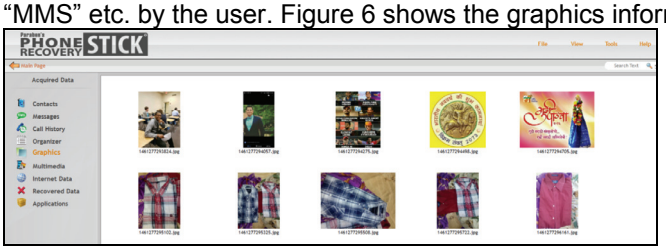
Figure 6: Graphics Information

Similarly, multimedia represents the information like “.mp4”,”.mp3”,”.mov” received/sent by the by the user. Multimedia information for the user is shown in figure 7.

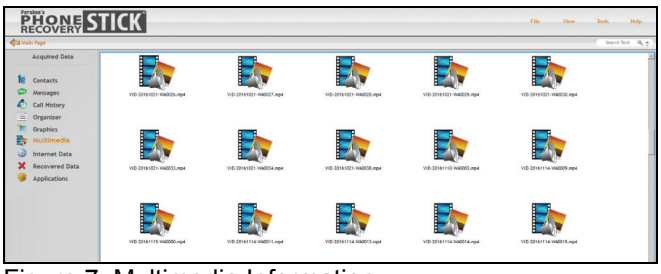
Figure 7: Multimedia Information

Figure 8 represents internet data history of the user. It includes information like “url”,”search history”.

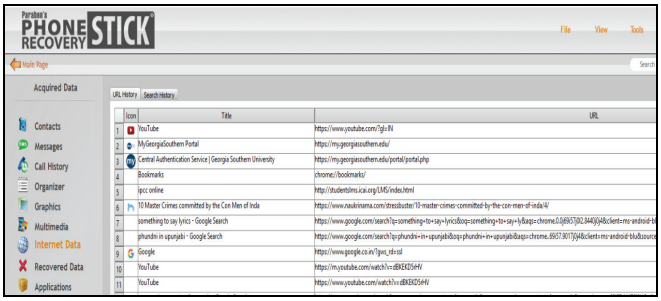

Figure 8: Internet Data Information

In an Android phone is rooted. The person can access the system files, by rooting the phone one can recover the deleted files or can get the system files. But in our case the phone was not rooted so we were unable to recover these kind of data from the tool. Figure 9 shows that no data was recovered by the stick.

Figure 9: Recovered Data Information

Another good feature of this tool is that it shows us the application which were installed in the phone along with the version number and all the basic information. Figure 10 represents all the application installed in the user's cell phone.

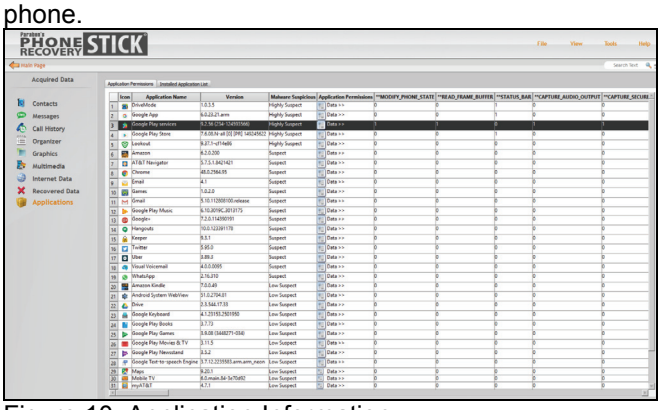

Figure 10: Application Information

3.2 Summary of Paraben

The Paraben tool recovered the 10-12 year old data described above (8 gigabits of data) in just 2-clicks and approximately 35 minutes. It also provided information about the user and the applications installed. However, Paraben didn't provide hex values or any internal system data without rooting. Nevertheless, this tool can be very useful in framework creation so that the recovered data can be used and manipulated.

4. CONCLUSION

Today, digital forensic careers are in demand. As such, many accounting, IS and technology related programs are developing digital forensic courses into their curriculum. Teaching resources for forensic tools are limited (Fleming, Pearson, & Riley, 2008; Henry & Venkatraman, 2015; Kearns, 2015; Seda & Kramer, 2008).

This paper highlighted the importance of digital forensic tools and explained a digital forensic data recovery via the Paraben tool. This paper can aid educators as an academic literature resource to expose student to the field of digital forensics.

Future research will include further exploring implementations of additional digital forensic tools, comparison of digital forensic tools, a digital forensic case study, as well as providing a hands-on teaching exercise.

REFERENCE LIST

1. Al-Zarouni, M. (2006). Mobile handset forensic evidence: a challenge for law enforcement. Available from: OAIster, Ipswich, MA. Accessed March 12, 2018
2. Al Mutawa, N., Baggili, I., & Marrington, A. (2012). Forensic analysis of social networking applications on mobile devices. *Digital Investigation, 9*, S24-S33.
3. Curran, K., Robinson, A., Peacocke, S., & Cassidy, S. (2012). Mobile phone forensic analysis. *Crime Prevention Technologies and Applications for Advancing Criminal Investigation*, 250.
4. *Edward, T. (2012). Following the Evidence. Itnow, 54(4), 12-13.*
5. FBI. (2010). Regional Computer Forensics Labs Mark 10 Years. Retrieved from https://archives.fbi.gov/archives/news/stories/2010/october/RCFL-report/RCFL
6. FBI. (2013). Piecing Together Digital Evidence
7. The Computer Analysis Response Team. Retrieved from https://www.fbi.gov/news/stories/piecing-together-digital-evidence
8. Fleming, A. S., Pearson, T. A., & Riley Jr., R. A. (2008). West Virginia University: Forensic Accounting and Fraud Investigation (FAFI). *Issues In Accounting Education*, 23(4), 573-580.
9. Fox. (2013). Man arrested after child pornography found on smart phone. Retrieved from http://fox6now.com/2013/09/13/man-arrested-after-child-pornography-found-on-smart-phone/
10. Harron, J., Langdon, J., Gonzalez, J., & Cater, S. j. (2017). Digital Forensics: Using smartphones to explore metadata in a simulated criminal case. *Science Teache*r, 84(8), 31-36.
11. Kearns, G. S. (2015). Computer Forensic Projects for Accountants. *Journal Of Digital Forensics, Security & Law*, 10(3), 7-34.
12. Klomklin, S., & Lekcharoen, S. (2016). A development of mobile phone forensics procedures for law enforcement agencies in Thailand. *The Computer Science & Education (ICCSE).*
13. Mishra, S., & Singh, G. (2017). Forensic Accounting: An Emerging Approach to Deal with Corporate Frauds in India. *Global Journal Of Enterprise Information System*, 9(2), 104-109.
14. Moody, G. (2016). Paris terrorists used burner phones, not encryption, to evade detection. Retrieved from https://arstechnica.com/tech-policy/2016/03/paris-terrorist-attacks-burner-phones-not-encryption/
15. Namin, A. S., Aguirre-Muñoz, Z., & Jones, K. S. (2016). Teaching Cyber Security through Competition. *Annual International Conference On Computer Science Education: Innovation & Technology*, 98-104.
16. Quick, D., & Choo, K.-K. R. (2016). Big forensic data reduction: digital forensic images and electronic evidence. Cluster Computing, 1-18.
17. Rakočević, V., Pavlović, Z., & Ivanović, A. R. (2017). Knowledge Driven Framework for realization of proactive criminalistics investigation in Combating Terrorism and Organized Crime in Montenegro with special focus on interception, collection and recording computer data. *Journal Of Eastern European Criminal Law,* (1), 155-180
18. Seda, M., & Kramer, B. P. (2008). The Emergence of Forensic Accounting Programs in Higher Education. *Management Accounting Quarterly*. p. 15.
19. Stirparo, P., & Kounelis, I. (2012). *The mobileak project: Forensics methodology for mobile application privacy assessment. The Internationa Conference for Internet Technology And Secured Transactions*.
20. Tassone, C., Martini, B., Choo, K.-K. R., & Slay, J. (2013). Mobile device forensics: A snapshot. *Trends and Issues in Crime and Criminal Justice*(460), 1.
21. Vidas, T., Zhang, C., & Christin, N. (2011). Toward a general collection methodology for Android devices. *Digital Investigation, 8*, S14-S24.