Smartphone Forensics Analysis: A Case Study

Mubarak Al-Hadadi and Ali AlShidhani

***Abstract*—Smartphone forensics is a sub-set of digital forensics, and refers to the investigation and acquisition of artefacts in mobile phones. New threats to mobile phones made forensic science a challenging endeavour in the last couple of years. Number of mobile users is increasing worldwide and createstremendous problems and challenges. The literature relevant to Smartphone forensics, as explored in this paper, focuses on the architecture of Smartphone operating systems and anti-forensics techniques. It also addresses the digital evidence of Smartphone applications. In this paper, through a consideration of types of crimes involving Smartphone's, a real case study from the Sultanate of Oman is presented. This case study undertakes practical experiments to identified sources for evidence that can later be used in the judiciary system.**

***Index Terms*—Smartphone forensics, digital forensics, security, Anti-forensic and smartphone security**

I. Introduction

Mobile forensics is a new type of gathering digital evidence where the information is retrieved from a mobile phone. It relies on evidence extraction from the internal memory of a mobile phone when there is the capability to access data. Mobile phone technologies witnessed rapid development in recent years. Different software tools are available to retrieve and analyze smartphone data. Each tool has its set of advantages and limitations. These tools are essential for smartphone forensics to extract digital evidence that can be later used in a legal case [1].

A. The Evolution of Smartphones

Smartphones embodies the continuing evolution of the mobile communications technology. They are not only used for the purpose of messaging and calling, they have many other applications. Smartphones are now used for browsing the Internet and navigating through maps, as well as, for photography, videography and many other use cases. There is an evolution in network connectivity that goes hand-in-hand with the evolution of smartphones. Wireless communications such as Wireless Local Area Networks (WLANs) have developed to become faster and more stable. Cellular communications such as the 3rd Generation (3G) and 4th Generation (4G) Mobile Systems are widely available and offers data speeds in tens of Mbps [2].

B. Architecture of Smartphone Operating Systems

Handful number of smartphone operating systems exists in the market today. Google's Android and Apple's iOS unmistakably are dominating. Smartphone operating systems create major challenges for investigators in the extraction of data because of their complexity [3]. iOS operating system contains four layers on which applications run. Layer one of the operating system provides direct access to memory and OS kernel. The second layer contains basic services written in C programming language. Layer three handles graphics, images, video and audio. Layer four, the last layer,provides an interface between users and applications [4].

Android architecture [5] on the other hand consists of five layers, applications layer, the application framework, libraries, Android runtime and the Linux kernel. The applications layer is written in Java. Applications are usually developed by third party companies and later ported to the device. On the other hand, each set of application programming interfaces available (APIs) that contains some of the capabilities are interesting, such as those that provide the interface with the file system.

C. Smartphone Forensics

Smartphones have become essential to our daily lives. Smartphones are now used as a mobile office or entertainment centre, incorporating basic needs for communicating with friends and relatives. Their storage capacity and processing capabilities are to be equated to low end computers. Smartphones became susceptible to the same and greater vulnerabilities as computers. The data in smartphones such as images, documents, emails, videos and short messages (SMS) can be remotely accessed if the device is connected to the Internet. This reality poses a major challenge for forensics investigators. There are many applications that can run on a smartphone and more are developed every day. Considering the variety of smartphone vendors, mobile applications and networking protocols, the task of forensic analysis on mobile phones is ever challenging.

When dealing with mobile devices such as smartphones, there are three areas where data is stored: the SIM card, which primarily contains contact information and texts; the device memory, which stores user created data such as MMS, text messages, photographs, media...etc, and also contains the phones operating system and settings; and, the device memory which also stores portable application software such as "WhatsApp" and the appropriate logs. There are also portable storage memory devices such as Micro SD cards which again store large amounts of data. Smartphones that have portable applications such as "WhatsApp" store data within the application itself on the specific device.

D. Smartphones Anti-Forensics Challenges

Anti-forensics, generally, is the use of technology to

Manuscript received March 5, 2013; revised June 16, 2013

The authors are with the Department of Electrical and Computer Engineering, Sultan Qaboos University, Sultanate of Oman (Email: alhadadim@gmail.com; alily@squ.edu.om).

defeat forensic investigation. In recent years, anti-forensics for mobiles faces major challenges. Attackers could deliberately mask or hide digital evidence in the smartphone. Anti-forensics practices are currently evolving and spreading, and are not limited to traditional applications. For instance, mobile devices used in the field of forensics medicinestore a significant amount of personal information. The information could be very sensitive and leaking them poses a high risk [6].

Smartphone forensic investigators must understandthe interworking of smartphone operating system layers because layers depend on each other.Applications written by third party developers can access specific OS layers and as a result tamper with the file system and erase digital evidence. Other applications could deliberately delete important artefacts such as messages and logs to hide digital footprint of a crime taken place in a smartphone. This complexity of anti-forensics hardens the job of forensic analysts [5], [7].

There is a spread of applications used to erase evidences that can be used by forensics analysts. Wickr [8], is an application designed to hide digital traces from governments or companies. It supports 256-bit AES symmetric encryption and RSA 4096 encryption and works without relying on their PGP key and the end to end encryption. Such application elevates the challenge faced by mobile forensics scientists.

"Data acquisition from Smartphoneis the process of imaging or otherwise obtaining information from a digital device and its peripheral equipment and media [9]".Acquisition of data imaging from the mobile is critical. Procedures and standards should be observed during data acquisition, transportation and storage. An investigation should also be properly conducted inorder to remedy any loss of information, battery power loss or device self-locking.

Contemporaneous notes should be taken at all times, ensuring that the smartphones are secured within a faraday bag/cage, or ensure that the device's SIM cards have been removed in order to ensure that the device is not receiving or sending data whilst carrying out the tests. Detailed inspection of devices should be carried out to identify their legitimacy and that they are in fact products produced by the said company (There are many fake mobile phones on the market). A dedicated laboratory environment should be available to correctly acquire and handle forensic evidence from the acquisitioned data.

II. SIGNIFICANCEOF THE PAPER

Cybercrime is a serious challenge that harms governments and individuals in today's world. A Symantec report in September 2011 on cybercrime states that the annual cost of cybercrime worldwide now totals $114 billion, affecting more than a million victims a day. The spread of Smartphone, with their rapidly evolving technology, has become inviting to hackers. Smartphones are almost full-fledged computers. Some phones, such as the iPhone, now have over half a million applications, leading to their gradual displacement of traditional computers [10].

The number of mobile phone subscribers in the world in 2011 has increased to almost six billion users of phones that connect to Internet Service Providers (ISPs), according to International Telecommunication Union (ITU) statistics [11]. Moreover, when comparing Internet and fixed line subscriptions, the trend of Global Information and Communications Technology development in 2001 through 2011 shows mobile cellular telephone subscriptions as having the highest increases. All of these reasons and more have helped to spread the emergence of many hacking-based crimes aimed at smartphones.

In this paper, we demonstrate through experiment, the tools that can be used to extract artefacts from a smartphone that is a central piece of evidence in a legal case. A real legal case from the Sultanate of Oman involving smartphone crime is considered. The data in the smartphone will be extracted and analysed to later line-up digital evidences that will help solve a legal case.

III. SMARTPHONE FORENSICS CASE STUDY

Evidence collection from Smartphone is very crucial. Extracting data, preserving them, building hypothesis and presenting digital evidences can all aid in solving legal cases. In this paper, a real legal case from the Sultanate of Oman is considered. A hypothesis will be established and two different software tools will be used to simulate data extraction to help solve a legal case.

Incident summary: an organization (P) received a complaint from a user (Ali) explaining that his mobile phone had been hacked. His contact list has been receiving text messages through a popular chatting application, WhatsApp. However, Ali claims that he has not been sending any messages from his mobile. After accepting the case, the investigators started looking at the logs and records of this incident, and began a trace from Ali's Internet Service Provider (ISP).

In the technical report provided by the ISP, there are two registers of messages for servers of mobile phones: the sender register and the receiver register. The report indicates that the messages were actually received by Ali's contact list. However, there was no record of his mobile having sent any messages. The mobile phone used in this case was an iPhone running on iOS 5.0.1 operating system.

Based on ISP's report, Ali is innocent in this case. However, there is a need to know how was Ali's phone compromised and used to send messages to Ali's contacts. Ali's phone was not available for testing due to legal constraints. There was a need to simulate the events to better understand the ways by which Ali's phone was compromised.

To carry out digital forensics and to better understand how such a compromise can take place, a phone from the same brand as Ali's phone should be examined and WhatsApp data should be extracted. There are many tools used in smartphone's forensics. Two of the most popular tools are the Oxygen Forensic Suite and theUFED physical Analyzer Cellebrite. Both tools are industry leading and widely accepted by forensics experts for providing accurate and verifiable results during forensics analysis. The tools also scored high in Hoog's analysis of smartphone forensics tools [7].

A. Smartphone Testing

The Smartphone was tested usingOxygen Forensic Suite and UFED physical Analyzer. Initial findings show that the smartphone is an iPhone4 runningiOS 5.0.1 "jailbroken". Crucial pieces of information to be extracted are the International Mobile Equipment Identification (IMEI) number, International Mobile Subscriber Identity (IMSI) and Integrated Circuit Card ID (ICCID). These technical details help assuring the subscriber's identity and aid in extracting call logs and history from the service provider.

B. Oxygen Forensic Suite Finding

The investigation with Oxygen forensic suite find the most valued information such as IMEI, IMSI and ICCID in such mobile that used in given crimes scenario. Fig. 1shows the information that will help the investigators to identify the primary evidence that is required.

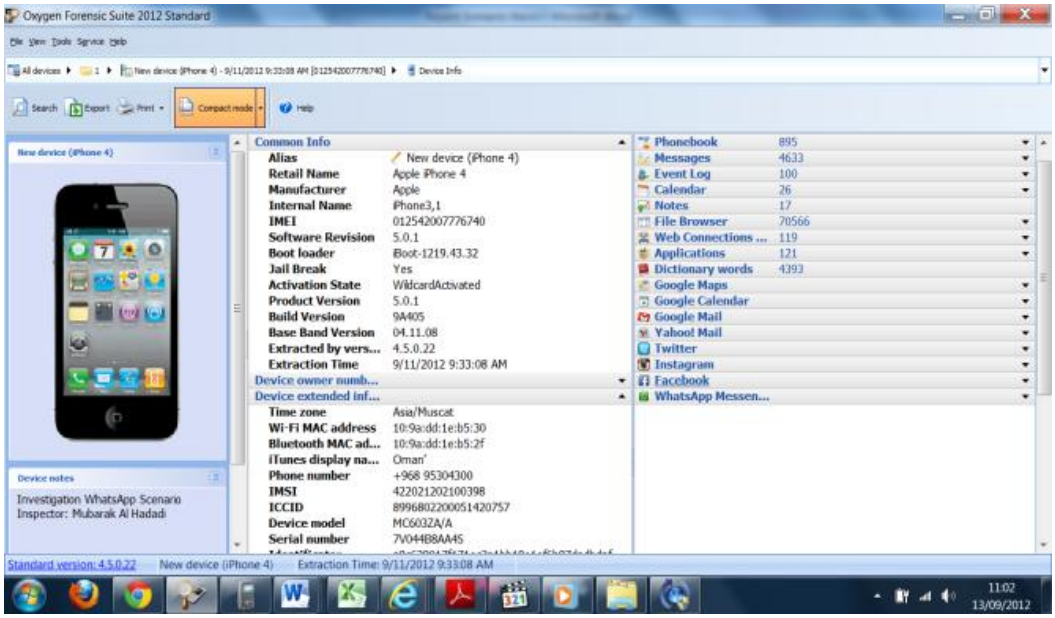

Fig. 1. Oxygen forensic display

The case involves WhatsApp fraud; therefore, information about WhatsApp messages is found. TheOxygen Forensic Suiteused in this experiment is a freeware hence there are limitations in the amount of information that can be extracted.

C. UFED Physical Analyzer Cellebrite Finding

Using a single tool for forensic analysis is not conclusive. Most forensic experts recommend using more than one tool to extract concrete evidences that can be used in the court. The smartphone was tested using UFED physical analyzer cellebriteto widen the search space for evidence.Smartphone data was extracted by the software. The software extracted critical information that can help the forensic analysis such as call logs and message history [12]. The Artefacts showing the installation of WhatsApp application in the smartphone are shown in Fig. 2.

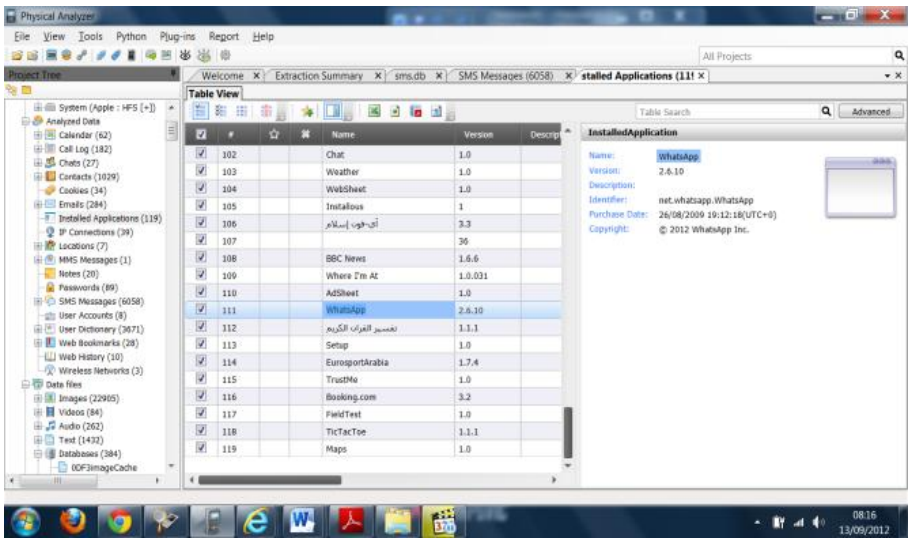

Fig. 2. WhatsApp installed in the mobile

Another artefact that shows the interfaces which have been logged in and which have sent WhatsApp messages gives more insight on the techniques used to send the messages. Fig. 3 shows three Wi-Fi access interfaces that

can act as evidence. Smartphone forensics investigator can make use of information such as connection time and date to generate evidence that can help solve a legal case.

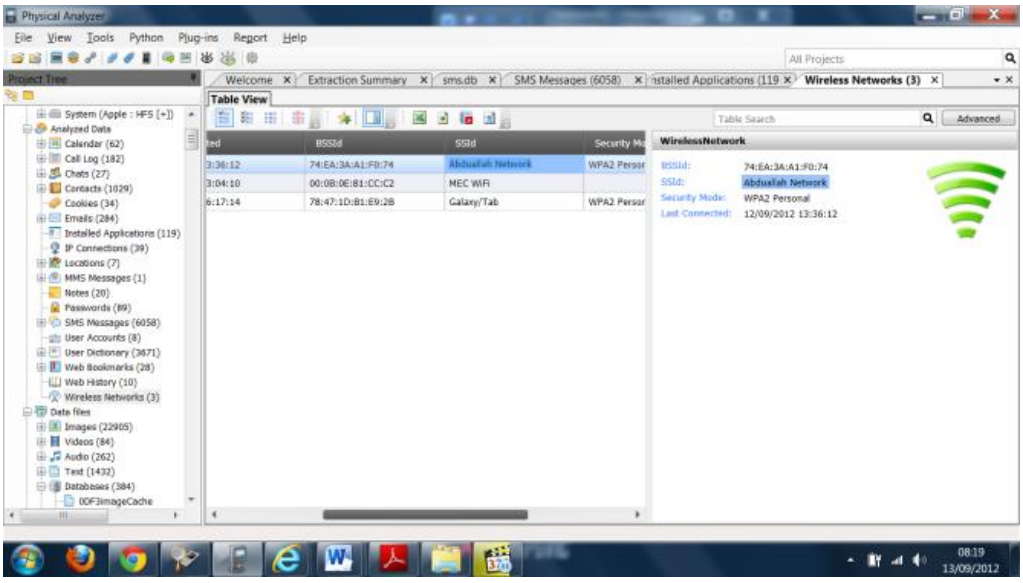

Fig. 3. Interfaces available in the mobile

D. Comparison of Findings for Both Tools

Table I shows a comparison between the artefacts extracted from the smartphone using Oxygen and UFED tools.

TABLE I: COMPARISON OF FINDING FOR BOTH TOOLS

iPhone	**Oxygen Forensic Suite 2012**	**UFED physical analyzerCellebrite**
Phonebook	895	1030 (118 Deleted)
Messages (SMS)	4633	5950 (1649 Deleted)
Event log	100	180 (5 Deleted)
Images	21772	22916
Audio	262	262
Videos	83	84
Database Files	212	388
Web Connection and IP Connections	WiFiconnections 3 IP connections 116	WiFiconnections 3 IP connections 39
Applications	User application 76 System application 45	119
Google Mail	User data 38 Application files 8 Application log 0 Application information 54	299 (118 Deleted)
WhatsApp Messenger	User data 924 Application files 78 Application log 0 Application information 102	42 (3 Deleted) WhatsApp and Viber messages
Web History	-	9
Cookies	-	34
Passwords	-	89
User Account	-	8
Web bookmarks	-	28 (1 Deleted)

Although Oxygen has limited access to the device but it generallygives more information about WhatsApp application compared to UFEDphysical Analyzer. The comparison shows that each tool excels in extracting specific type of information useful for forensic analysis. For example, information like images and contact numbersare better extracted by the UEFS physical Analyzer compared to Oxygen. On the other hand, Oxygen outperforms UFED in extracting data from messaging services such as WhatsApp.

E. Final Findings

The ISP confirmed earlier that Ali did not send WhatsApp messages. On the other hand, Ali's contacts received WhatsApp messages from Ali's phone. To simulate the scenario, a similar device was tested using Oxygen Forensics and UFED physical analyser. It was found that WhatsApp messages do not necessarily require cellular communications to be delivered. WhatsApp messages can also be delivered over Wi-Fi network.

From the abovementioned facts we can derive two possible compromise scenarios. *Scenario A*, the Subscriber Identity Module (SIM) card was removed and the attacker used Wi-Fi network to deliver WhatsApp message. *Scenario B*, Ali sold his smartphone but didn't delete WhatsApp application and the new owner used a Wi-Fi network to deliver WhatsApp messages to Ali's contacts.

IV. CONCLUSION

Procedures for carrying out forensic analysis should be conducted in accordance with appropriate guidelines, particularly for evidence handling.Firstly, regarding the problem of the "WhatsApp" application, the analysis of the suspect device should be carried out using suitable mobile forensic software such as Oxygen Forensic Suite and UFED physical from Cellebrite, within a controlled environment while ensuring that evidential and continuity of evidence is maintained.

Cross examination of all data extracted from testing tools with logs from ISP should be compared and evaluated and the findings reported. Dates and times are relevant in this case; also, the IMEI, IMSI and the ICCID number of the

device and SIM card can be compared with the relevant logs.

Logs from the Network ISP should be obtained and compared with the logs contained within the device. Investigators should provide a report that details their actions and findings and possibly comment on what they consider might have happened. The analysis should be conducted in such a manner that another expert could replicate the work and produce the same findings.If the forensic software is unable to retrieve the specific data, a physical examination may be carried out, providing photographs of the specific requested evidence.

REFERENCES

[1] N. Al Mutawa, I. Baggili, and A. Marrington, "Forensic analysis of social networking applications on mobile devices," *Digital Investigation*, vol. 9, pp. S24-S33, 2012.

[2] L. S. Ashiho. (2003). [Online]. Available: http://www.electronicsforu.com/EFYLinux/efyhome/cover/jun2003/Mobile-tech.pdf.

[3] E. Casey, *Digital Evidence and Computer Crime*, 2011.

[4] A. Hoog, *iPhone and iOS Forensics: Investigation, Analysis and Mobile Security for Apple iPhone, iPad and iOS Devices*, Syngress Publishing, June 2011.

[5] A. Distefano, G. Me., and F. Pace, "Android anti-forensics through a local paradigm," *Digital Investigation*, vol. 7, pp. S83-S94, August 2010.

[6] M. A. Caloyannides, *Computer Forensics and Privacy*, Artech House, 2011.

[7] A. Hoog. (November 2010). Independent research and reviews of iPhone forensic tools. via forensics. [Online]. Available: https://viaforensics.com/resources/white-papers/iphone-forensics/.

[8] K. Jackson. (2012). Dark Reading. [Online]. Available: http://www.darkreading.com/mobile-security/167901113/security/encryption/240002865/free-app-encrypts-destroys-mobile-messages.html.

[9] W. Jansen. (2007). National Institute of Standards and Technology, [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-101/SP800-101.pdf .

[10] Norton. (2011). Symantec. Norton study calculates cost of global cybercrime: $114 billion annually. [Online]. Available: http://www.symantec.com/about/news/release/article.jsp?prid=20110907_02.

[11] International Telecommunication Union. (2012). Key statistical highlights: ITU data release June 2012. [Online]. Available: http://www.itu.int/ITUD/ict/statistics/material/pdf/2011%20Statistical%20highlights_June_2012.pdf.

[12] Cellebrite. [Online]. Available: http://www.cellebrite.com/mobile-forensicsproducts/solutions/ios-forensics.html.

Mubarak Al Hadadi received B.Eng degree in hardware and network from Middle East College, Sultanate of Oman 2008; in 2012 hold Master degree in Science in information Technology (MSc-IT) from Coventry University UK, graduated distinction. A professionally qualified and experienced, Information Security and Chief Information Security Officer (CISO) qualification with a personal passion for achieving results, leading network security team, Sultanate of Oman.His research interest in Smartphone forensic.

Ali Al Shidhani received the B. Eng. degree in electrical and electronics engineering from Sultan Qaboos University, Sultanate of Oman, in 2001; the Master's degree in data communications from Queensland University of Technology, Australia, in 003. He received Ph.D. degree in electrical and computer engineering from the University of British Columbia, Canada, in 2010. He is currently an Assistant Professor at the Department of Electrical and Computer Engineering at Sultan Qaboos University, Sultanate of Oman. His research interest includes authentication in wireless networks.