Android Phone Forensic: Tools and Techniques

Nihar Ranjan Roy
GD Goenka University, Gurgaon , India
niharranjanroy@yahoo.com

Anshul Kanchan Khanna
Galgotias University
anshul.khanna@galgotiasuniversity.edu.in

Leesha Aneja
GD Goenka University,Gurgaon, India
leesha_aneja@yahoo.com

Abstract – Today when there are more than 1 billion Android users all over the world, it shows that its popularity has no equal. These days mobile phones have become so intrusive in our daily lives that when they needed can give huge amount of information to forensic examiners. Till the date of writing this paper there are many papers citing the need of mobile device forensic and ways of getting the vital artifacts through mobile devices for different purposes. With vast options of popular and less popular forensic tools and techniques available today, this papers aims to bring them together under a comparative study so that this paper could serve as a starting point for several android users, future forensic examiners and investigators. During our survey we found scarcity for papers on tools for android forensic. In this paper we have analyzed different tools and techniques used in android forensic and at the end tabulated the results and findings.

Keywords –Android Forensic, phone forensics; forensic tools; mobile devices; smart phone forensics; mobile device tools; smart phones.

I. INTRODUCTION

Internet and Information Technology are no more new today as they have become an integral part of everybody's life, but these technologies have given birth to many more technologies which make life further easy. The rapid growth in the Small Scale Digital Devices (SSDD) research and manufacturing has acted as a catalyst for the world of ubiquitous computing. Today Mobile Phones which are part of SSDD have become so pervasive that they rule us in many ways which includes; they not only allow us to make and attend a call but also allow us to do business, online commerce, make financial transactions, social networking, SMS, MMS, video calls, photography, electronic mail, Web browsing, multimedia capturing, basic editing and playback, electronic document previewing, store and manage Personal Information via Persona Information Management (PIM) applications (e.g., contacts, calendar, etc.) [1]. Digital Forensic (DF) came into existence because of the cybercrimes carried out by use of IT infrastructure or technology by cyber criminals. DF has developed several sub-disciplines, including Computer Forensics, Memory Forensics, Multimedia Forensics, Network Forensics, Small Scale Device Forensics or Mobile Device Forensics (MDF) and Android Forensic (AF) depending on attributes of computing and the type of device used [2].

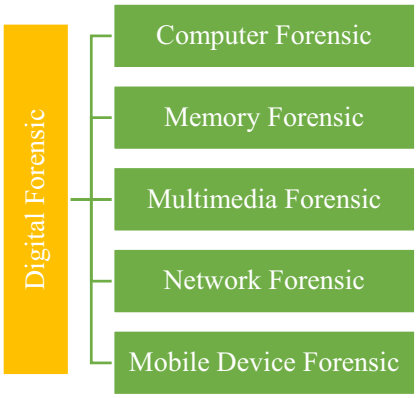

Figure 1: Classification of Digital Forensic

In the past decade the mobile technology (both hard ware and especially software) has obtained phenomenal growth. This growth has not only attracted the common users but also the malware developers and the tradition computer hackers leading to an increased number of cyber-attacks and malware threats. In the past few years the rate of stolen phones have also increased. As these phones contained sensitive personal information, it is risky if they are lost or stolen. Forensic analysis of these phones and devices by app developers and the user themselves can make them more aware on how and which data to store or not to store on these devices. These stored sensitive information can be used by the attacker as a stepping stone to spoof the real identity of a person [3].

II. CHALLENGES IN MDF

The wide spread use of Mobile Phones, makes it inevitable source for forensic analysis both from criminal and non-criminal point of view. According to [4] MF from legal perspective is the science of recovering digital evidence from an non-tampered mobile device under forensically sound conditions using legally accepted methods. Because of the cramming growth of the mobile device manufactures and challenges have also increased because of varying CPU architecture and operating systems. In modern world of competition every day new mobile device manufacturers are coming into the market with the same operating system but with its own variations, in their implementation, resulting in a myriad of file system and structural permutations. These flexibilities offered by the vendors create significant challenges for mobile forensic tool manufacturers and examiners in hunting at the right location and with right technique inside the phone. These variations and changes are so fast that there is

ISBN: 978-1-5090-1666-2/16/$31.00 ©2016 IEEE

always the risk that one forensic tool can be good for a specific version with no guarantee that it will be the same for the successor version. Sometimes the power consumption may lead to vanishing of the information available on these devices as these devices are power constrained. This can occur during one the-fly data acquisition from the volatile memory [5]. Volatility is a frame work designed to retrieve such information irrespective of the platform [6]. Lack of standard hardware and software interface further poses challenge in MDF for the practitioners. Sometimes the storage that is brought to the analyst or recovered by the analyst is damaged or corrupt and taking data out of it is very challenging. Variety of applications for the same task on same mobile platform also puts challenge for example these days web browser forensic in also in demand and there are different types of browsers for android platforms, which are different from each other in many respects [7]. Another challenge to digital forensic analysis with release of every new phone is the growth in the volume of data seized and presented for analysis because of the increased storage and processing capacity on these devices [8]. Because of the presence of dual time stamps (naive and UTC timestamps), timestamps normalization may be required and is a complicated process with an additional possibility of presence of clock skewness [9].

III. Related Work

Very less work has been done by researchers in terms of survey work on Mobile device forensic and Android Forensic in particular. In [10] authors have presented a detailed survey on mobile device forensic assessment and methodologies being followed from 2006-2013 and evolution of MF but as always the technology changes very fast especially mobile technology so there is always scope for further quality work. In [11] authors forensically acquire and analyze the device-stored data and network traffic of 20 popular instant messaging applications for Android. Mostly they were successful in extracting or intercepting data from passwords, screenshots taken by applications, pictures, videos, audio sent, messages sent,
Sketches, and profile pictures. Here the work was carried out using network traffic analysis and server/device storage analysis. In [12] authors have perform forensic work on WhatsApp calling feature which was added to the application in version 2.11.552, which was released 2015-03-05 [13]. During android forensic there are few more parameters that are important such as integrity acquisition speed, and physical dump, these parameters are taken into care in [14] while proposing firmware update protocols of Android smartphones. If the storage is corrupt or damage then the forensic analysts rely on a technique called “file carving”, this technique may recover data after meta data loss also [15]. Web browser based forensic analysis has been done by [16] for five major web browsers, Google Chrome, Internet Explorer, Mozilla Firefox, Opera, and Apple's Safari using a tool called BrowStEx (Browser Storage Extractor).

IV. Tools for Android Forensic

Android forensics focuses on extracting data from android based devices using sound forensic conditions and legally accepted techniques. Primarily there are 3 different methods for the same:

a. Manual Acquisition- In this technique forensic examiner or analyst utilizes the user interface of the mobile device to investigate the available content. While browsing the device, the examiner takes pictures of each screen, containing the required data. The advantage of this technique is that it does not require any tool(s) to perform data acquisition but at the same time disadvantage to this technique is that only data visible to users on the device can be recovered and is time consuming.
b. Physical Acquisition- In this technique cloning of the data available on the phone device is done. This process clones deleted data as well as the unallocated spaces too. After cloning the cloned data is analyzed using different tools.
c. Logical Acquisition- In this technique neither much of manual intervention nor cloning is required. Here data /information available on the phone is acquired using automated tools for synchronizing phone and PC (generally) Most tools available for free perform logical acquisition.

Here we analyze different tools used in android forensic with their limitations.

A. Andriller

For Android forensics Andriller [17] is the most commonly used tool due to its wide functionality and being free of cost. It is software utility with a stack of forensic tools for modern smartphones. The data acquisition process followed by it is read only, non-destructive and forensically sound. It can also crack lock screen for Pattern, PIN code, or Password; and has custom decoders for Apps data from Android databases for decoding communications. The extraction process and the decoder process produce reports that are in Excel and HTML format. It has a large list of decoder for decoding files and databases.

Figure 2: Andriller Lockscreen PIN Cracking screen

B. XRY

XRY [18] performs secure forensic extraction of data from a wide variety of mobile devices, such as smartphones, satellite navigation units, modems, music players and tablets. It is designed to run on the Windows operating. It comes in three versions. XRY-Logical, XRY-Physical and XRY-PinPoint. XRY files are secured files and can be view with XRY-Viewer. Need license for the product. It supports a wide range of apps, its latest version supports 847 apps [19].

XRY-Logical: It extracts/ requests information by communicating with the operating system on the device.

XRY-Physical: It performs extraction of available raw data from the device called 'physical' extraction. It is a two-step process where in the first step raw data is extracted and in the second step its decoded or reconstructed.

XRY-PinPoint: It can be used to extract and decode data from mobiles where the pin-out vary and may not even be known (non-standard devices).

C. UFED TOUCH

Universal Forensic Extraction Device (UFED) Touch is a product from Cellebrite with Graphical User Interface and easy-to-use touch screen. It [20] enables extraction of physical, file system, other data and passwords from the phone device. It can also extract deleted data, from the widest range of mobile devices. For physical extraction it can be run from windows phone running windows 8 or 8.1. Extraction reports can be viewed on screen with the HTML report viewer. No need for PC for data extraction and reports can be viewed in the kit itself. The latest version (4.4) of it promises for physical extraction while bypassing lock from 3,183 devices.

UFED is available in two versions, Ultimate or Logical.

UFED Ultimate- It is used for Physical extraction and decoding while bypassing pattern lock / password / PIN from Android devices including Samsung Galaxy S family, LG, HTC, Motorola, and more.

UFED Logical- is used for Logical extraction of data: Apps data, passwords, IM (instant messaging), contacts, SMS & MMS, emails, calendar, multimedia, call logs, phone details (IMEI/ESN), ICCID and IMSI, SIM location information (TMIS, MCC, MNC, LAC). It also supports forensic cloning of SIM ID to isolate the phone from network activity during analysis.

D. OXYGEN FORENSIC

Oxygen Forensics [21] comes in two versions; Oxygen Forensics-Analyst and Oxygen Forensic-Detective. It promises zero-footprint operation, i.e. leaving no traces and making no modifications to the phone content.

Oxygen Forensic Suite has also capability to detect malicious and spyware apps installed on Android and Apple devices, discover and process their logs and configuration files. It has extensive reporting with variety of graphs, which includes social networking. It has support for more than 11,000 devices and more than 300+apps with 1000+ app versions. Geo-location data extraction from all sources what happened and when.

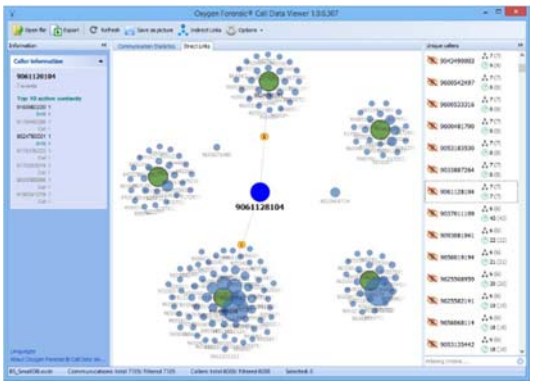

Figure 3: Analyse Call Data Record

E. MOBILEDIT FORENSIC

MOBILedit [22] supports extraction and viewing data from different sources such as; Contact book, call history, text and multimedia messages, files, calendars, notes, reminders, raw application data, IMEI, operating systems, firmware including SIM details (IMSI), ICCID and location area information. Wherever possible MOBILedit based forensic is also able to retrieve data deleted from phone memory and can bypass the passcode, PIN and phone backup encryption techniques too. Number of UNIQUE mobile phones supported by latest version: 3360. Latest version is 8.1. It has also support for physical acquisition of Android phones and memory cards.

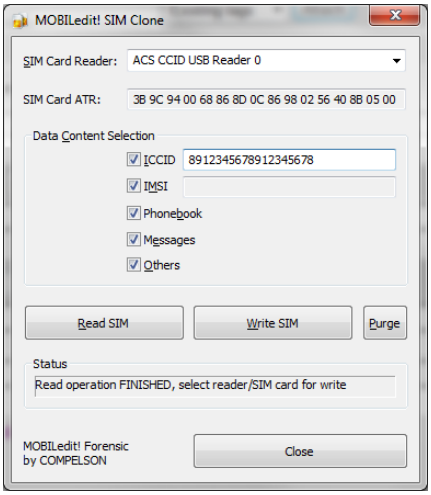

Figure 4: SIM Card Cloning

F. DROIDSPOTTER

DroidSpotter [23] was written entirely in Java. It stores all of its data in a basic SQL database. It is output of academic work and can be used for finding possible locations of location data from unanalyzed android applications. It extracts data form the apk files through a easily available navigation pane as shown in the Figure 5: GUI for DroidSpotter.

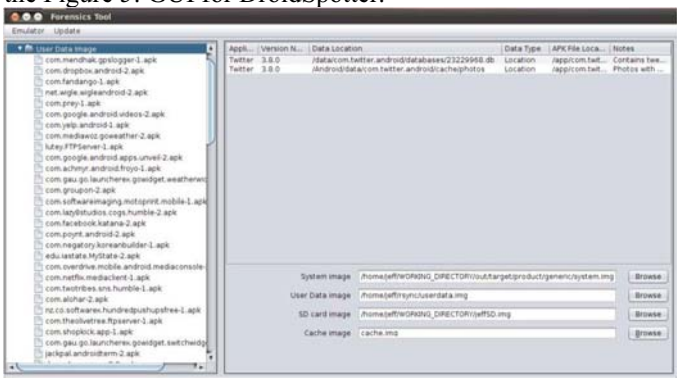

Figure 5: GUI for DroidSpotter

G. VOLATILITY

Volatility [24] is product of Volatility Foundation, which is an independent and non-profit organization that maintains and promotes open source memory forensics with The Volatility Framework. Its most recent version is 2.5, released in October 2015. Its Open Source GPLv2 which means users can use it, copy it and extend it. It is written in Python language. Its vast APIs gives users the power to go beyond and continue innovating. For example user can use volatility to build a their own customized web interface or GUI, drive their malware sandbox, perform introspection on the virtual machine and can also explore kernel memory through automated scripts. Users can add new address spaces, update existing and add new plugins, data structures, and overlays to truly weld the existing framework as per their needs.

The extraction techniques performed by Volatility are independent of the system being investigated but offer indepth visibility into the runtime state of the system. It has capabilities to convert back and forth between various commonly used files systems. It can be used to analyse multiple types of memory dumps such as; raw dumps, crash dumps, hibernation files, VirtualBox core dumps, LiME (Linux Memory Extractor), VMware .vmem, VMware saved state and suspended files (.vmss/.vmsn), , expert witness (EWF), and direct physical memory over Firewire..

H. MOBILE PHONE EXAMINER PLUS (MPE+)

MPE+ [25] has one of the most intuitive and user friendly GUI Interface in the market and includes graphically visualization tools that allows its user to easily see communication relationships among contacts and automatically construct graphical data timelines. MPE+ is also available on a preconfigured touch-screen tablet for on-scene mobile forensics triage. It supports both physical extraction and logical extraction of Android devices, with password bypass capabilities and without the need to know the manufacture or model. MPE+ supports latest mobile device profiles and features advanced carving, deleted data recovery, SQLite database browsing, advanced analysis, filtering options and has inbuilt support for query and script building.

Figure 6: MPE+ On preconfigured tablet for on scene analysis

I. VIAEXTRACT/ NOWSECURE

viaExtract is a powerful analysis and reporting tool for Android smart phones and devices. It supports all the three types of data acquisition; Logical, Physical and File System. viaExtract is now NowSecure and has two versions [26] (Non- Commercial and Commercial). The non-commercial version has features like; Access to Root Exploits, Screen Lock Bypass Tool, Gesture Key Decoding, Automated Data Parsing, Deleted Data Recovery, Artifact Viewer, Timeline, Global Search, Android Logical Extraction, Android ADB Backup Extraction and Android File System Extraction. The commercial version of NowSecure has all the features of Non-Commercial version plus; Android Physical Extraction, iOS Logical Extraction, File Carving and Reporting. Its latest version has enhanced support for html and pdf reports for easier navigation and read, and have now included carved images and recovered data.

V. CONCLUSION

In this paper we survey the techniques in practice for android based cell phone forensic. The survey is primarily based on manual acquisition, physical acquisition and logical acquisition of data from the device. The survey work is tabulated in table 1; which includes characteristics like free or proprietary , number of devices the support is available , and the other platforms apart from android where these tools can support. Free tools like volatility provide lots of existing APIs to forensic experts to used and extend the framework, proprietary tools like OXYGEN Forensic are enriched with lots of features and reporting techniques including GUI based graphs, with highest number of device supports.

Table 1: Comparative Study of Android Forensic Tools

Sl. No	Name of the Tool	Cost	Version	Require PC for Extraction	OS	Developed by	Non-Android OS Support	GUI Support	No of device supported	Cloud Support
1	Volatility	Free	2.5	Yes	Windows/Linux/Mac/ Android	The Volatility Foundation	Almost all file formats	Yes+ Console	--	No
2	DroidSpotter	Free		Yes	Windows/Linux	Jeffrey Alan Kramer	No	Yes	--	No
3	Andriller	Paid	2.5.0.2	Yes	Windows XP/Vista/7/8	Andriller	IOS9,Blackberry10	Yes	--	No
4	XRY	Paid	6.15	YES	Windows	MSAB	IOS,Blackberry,Nokia BB5 devices	Yes	--	No
5	UFED Touch	Paid	4.4	Optional	Windows 8	Cellebrite	BB, iOS, Windows Phones	Touch Screen	--	No
6	Oxygen Forensic	paid	8	yes	windows 8	Oxygen Forensic	IOS,Blackberry,Symbian, Bada OS, Chinese MTK		11600+	Yes
7	*MOBILedit*	paid	8.1	Yes	Windows 7/XP	Compelsion	Android,IOS, Blackberry, Symbian, Bada, Meego, Windows Mobile, Windows Phone, Chinese phones and CDMA phones.		3360+	Yes
8	Mobile Phone Examiner Plus (MPE+)	Paid	5.6.0	Optional	Windows XP/7/8/8.1	AccessData	iOS , Blackberry, Windows Mobile	Yes	10,000+	No
9	viaExtract	Paid	2.3	yes	Windows/Linux/Mac	viaForensics/ NowSecure	iOS	yes	46	No
10	DroidWatch	free		yes	Windows/Linex	Rochester Institute of Technology's Justin Grover	No	Yes	--	No
11	NowSecure (non-comm/Commercial)	Free/ Paid	3.5	Yes	Windows/Linux	NowSecure	iOS	Yes	--	No

References

[1] R. P. Mislan and T. Wedge, "Designing Laboratories for Small Scale Digital Device Forensics," in *ADFSL Conference on Digital Forensics, Security and Law*, 2008.

[2] E. Casey, Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, Academic Press, ELSEVIER, 2011.

[3] A. Chavez, "A jailbroken iPhone can be a very powerfull weapon in the hands of an attacker," Project Report, Purdue University, Calumet's CIT Department, 2008.

[4] R. Ayers, S. Brothers and W. Jansen, "Guidelines on Mobile Device Forensics," NIST Special Publication 800-101: [Online]http://dx.doi.org/10.6028/NIST.SP.800-101r1, May 2014.

[5] V. L. Thing, K.-Y. Ng and E.-C. Chang, "Live memory forensics of mobile phones," *Digital Investigation,* Vols. Volume 7, Supplement, no. ISSN 1742-2876,http://dx.doi.org/10.1016/j.diin.2010.05.010., pp. S74-S82, August 2010.

[6] "The volatility framework: volatile memory artifact," Systems., Volatile, [Online]. Available: http://secxplrd.blogspot.in/2011/10/volatility-framework-volatile-memory.html. [Accessed 9 11 2015].

[7] J. Oh, S. Lee and S. Le, "Advanced evidence collection and analysis of web browser activity," *Digital Investigation http://dx.doi.org/10.1016/j.diin.2011.05.008.,* vol. 8, no. SSN 1742-2876, pp. S62-S70, August 2011.

[8] D. Quick and K.-K. R. Choo, "Impacts of increasing volume of digital forensic data: A survey and future research challenges," *Digital Investigation,* vol. 11, pp. 273-294, 2014.

[9] M. Kaart and S. Laraghy, "Android forensics: Interpretation of timestamps," *Digital Investigation,* vol. 11, p. 234–248, 2014.

[10] K. Barmpatsalou, D. Damopoulos, G. Kambourakis and V. Katos, "A critical review of 7 years of Mobile Device Forensics," *Digital Investigation (2013),* vol. 10, p. 323–349, 2013.

[11] D. Walnycky, I. Baggili, A. Marrington and J. Moore, "Network and device forensic analysis of Android social-messaging applications," *Digital Investigation,* vol. 14, pp. S77-S84, 2015.

[12] F. Karpisek, I. Baggili and F. Breitinger, "WhatsApp network forensics: Decrypting and understanding the WhatsApp call signaling messages," *Digital Investigation,* pp. 1-9, 2015.

[13] N. Arce, "WhatsApp Calling For Android And iOS: How To Get It And What To Know," TECHTIMES, 9 March 2015. [Online]. Available: http://www.techtimes.com/articles/38291/20150309/whatsapp-calling-for-android-and-ios-how-to-get-it-and-what-to-know.htm. [Accessed 9 November 2015].

[14] S. J. Yang, J. H. Choi, K. B. Kim and T. Chang, "New acquisition method based on firmware update protocols for Android smartphones," *Digital Investigation ,* vol. 14, pp. S68-S76, 2015.

[15] J. Wagner, A. R. and J. Grier, "Database forensic analysis through internal structure carving," *Digital Investigation,* vol. 14, pp. S106-S115, 2015.

[16] A. Mendoza, A. Kumar, D. Midcap, H. Cho and C. Varol, "BrowStEx: A tool to aggregate browser storage artifacts for forensic analysis," *Digital Investigation ,* vol. 14, pp. 63-75, 2015.

[17] "Andriller," Andriller, [Online]. Available: http://andriller.com/. [Accessed 9 November 2015].

[18] "XRY," MSAB, [Online]. Available: https://www.msab.com/products/. [Accessed 9 November 2015].

[19] XRY, "https://www.msab.com," [Online]. Available: https://www.msab.com/download/release_notes/en/english_xry_release_notes/XRY_6.15_release_notes_EN.pdf. [Accessed 9 November 2015].

[20] Cellebrite, [Online]. Available: http://www.cellebrite.com/Mobile-Forensics/Products/ufed-touch. [Accessed 9 November 2015].

[21] "oxygen-forensic," http://www.oxygen-forensic.com/en/, [Online]. Available: http://www.oxygen-forensic.com/en/. [Accessed 9 November 2015].

[22] "http://www.mobiledit.com/forensic," MobileEdit, [Online]. Available: http://www.mobiledit.com/forensic. [Accessed 10 November 2015].

[23] J. A. Kramer, "DroidSpotter: A Forensic Tool for Android Location Data Collection and Analysis," Digital Repository, Ames, IA 50011, United States, 2013.

[24] "The Volatility Foundation," The Volatility Foundation, [Online]. Available: http://www.volatilityfoundation.org/. [Accessed 10 November 2015].

[25] "AccessData," http://accessdata.com/solutions/digital-forensics/mpe, [Online]. Available: https://ad-pdf.s3.amazonaws.com/mpe/2015/02/AD-MPEX-BRO-25Feb2015.pdf. [Accessed 10 November 2015].

[26] "NowSecure," NowSecure, [Online]. Available: https://www.nowsecure.com/forensics/community/#viaprotect. [Accessed 10 November 2015].