Original Research Paper

A Forensic Approach for Data Acquisition of Smart Phones to Meet the Challenges of Law Enforcement Perspective

[1]Shalini, [2]Vibhuti Narayan Singh, [3]Mukesh Yadav, [4]Pooja Rastogi

Abstract

As the mobile devices grown popularity in everyday life, they are often vulnerable in security and privacy. Mobile device such as Cell Phones, Personal Digital Assistance (PDA) and Satellite phones have become essential tool in our personal and professional lives. These devices serves for user as Target, Storage and Communication medium by which user can able to perform various tasks such as send and receive SMS, MMS, Email, multimedia files, storing audio, video, text, image files and also make and receive calls. When mobile phone involved in criminal activity extraction of this Electronic/Digital evidence becomes ‘Gold Mine’ of intelligence and evidence about ‘Who knows Who, What has Happened, What is being discussed and even what may happen in the future and the right use of this extracted evidence become important in judicial process that significantly helps in case hearing.

This paper studies extraction of digital evidence from, Nokia Lumia 520, Blackberry Curve 8520 and Samsung Galaxy GT-19082 mobile phones through three widely used mobile forensic devices (Device A, B & C), and it was concluded that no single tool can be exclusively relied upon to collect and present every item of potential evidence from a smart mobile device.

Key Words: Mobile Forensics, Electronic/Digital evidence, Mobile Forensic devices

Introduction:

A great number of mobile phones worldwide used in everyday life & much of them involves in criminal activity and possesses important evidences.

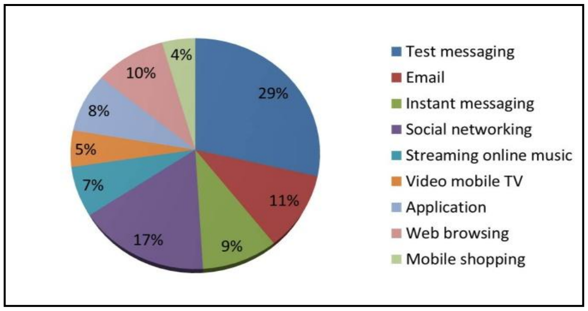
Mobile phones with cellular capability provide users with the ability to perform additional task such as creating phonebook, calendar, Short Messaging Services (SMS), Instant Messaging (IM), Electronic mail (Email), Web browsing, Storing videos, audios, text files, Portable Document Files (PDF), JPEG files etc.

Now days smart phones inbuilt with Global Positioning System (GPS) which is useful for providing location information and extraction of such information is useful by Law Enforcement Agencies to track down kidnappers, criminals and terrorist in real time.

When mobile devices are involved in a crime or other incidents, Mobile forensic analyst assembles this evidence from the crime scene, evaluates and analyse it and present the data in the court. According to the Nielsen Company database (2013) out of 100 Indians 81 Indians use mobile phones in which 80% Indians use feature phone, 10% smart phone and 9% multimedia phone.They further provide a dataset for mobile activities and applications used by Indians. (Fig. 1 and 2)

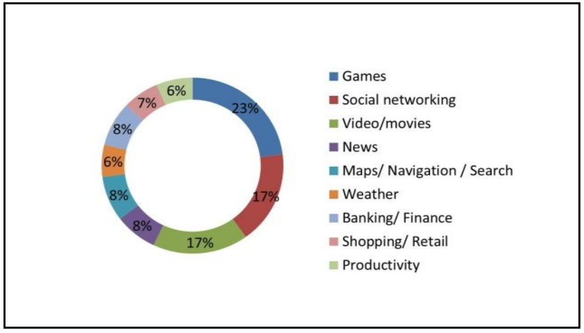
This paper provides a comparative experimental overview of three famous mobile forensic tools on Window, Android and Blackberry OS (Operating System) phones. The technical specifications of both mobile forensic tools and mobile phones are respectively explained in Testing environment and requirement section.

Fig. 1: Dataset of mobile activity uses by Indians



Corresponding Author:
[1]Assistant Professor
Dept. of Forensic Science & Criminology
BBAU, Lucknow, U.P. 226025
E-mail: shalinichauhan89@gmail.com
[2]Handwriting & Fingerprint Expert
[3]Director/Principal/Dean
Siddhant School of Medical Science, Mainpuri, UP
[4]Prof & HOD, Dept. of FMT
SMS &R, Sharda University, Greater Noida, U.P
DOR: 12.12.2014; DOA: 15.01.2015
DOI: 10.5958/0974-0848.2015.00045.7

Fig 2: Dataset of Application uses by Indians



Digital/ Electronic Evidence and Its Present Scenario According to Indian IT Act 2000:

Digital evidence is also known as electronic evidence or E-evidence. After implementation of the Information Technology Act 2000 (IT Act 2000) in India, E-evidences are admissible in the court as Documentary evidence (Section 3, 65A and 65B).

The definition of "Documentary Evidences" has been amended to include all documents including electronic records produced for inspection by the court.

An amendment to the India Penal Code (IPC), 1860, Indian Evidence Act (IEA), 1872 and Banker's Book Evidence Act, 1891 provide the legislative framework for transaction in electronic world.

Section 3 of Indian Evidence Act, 1872 define Evidence as under-

Evidence means and includes:

1. All statement which the court permit or requires to be made before it by witnesses in relation to matters of fact under inquiry, Such statement are called "Oral Evidence"
2. All documents including electronic records produced for the inspection of the court. Such documents are called as "Documentary Evidence".

Testing Requirements:

The purpose of forensically sound evidence is admissibility in a court of law. This is only possible when the testing environment will fulfil a crucial rule of digital forensics, which is to preserve the integrity of the original data and it to prevent from any contamination thus the mobile forensic workstation is designed to capture and process extremely high volume of digital data quickly and efficiently with obsolete assurance data integrity. The required hardware and software for experiment are mentioned below with their specifications.

- **Computer Workstations:** The configuration of workstation is mentioned in Table 1.
- **Mobile phones:** Nokia Lumia 520, Blackberry Curve 8520, Samsung Galaxy GT-19082. The specifications of mobile phones are mentioned in Tabular form. (Table 2)
- **Mobile Forensic Tools:** In the proceeding with above experiment we have used 3 Mobile Forensic Devices, namely Device A, B and C. (Due to some legal issues we didn't mention the name of Mobile Devices used).

Analysis and Results:

Analysis of all three mobiles is done on three Mobile Forensic Devices under forensically sound condition. In this research we carried Logical and Physical extraction of mobile phones.

Logical Extraction:

It includes a bit-by-bit copy of logical storage objects such as call logs, SMS, contacts, pictures etc.

Physical extraction:

It implies a bit-by-bit copy of an entire physical storage. A physical extraction has the advantage of allowing deleted files to be examined. (Table 4)

Conclusion:

In both the extraction we have taken the 13 parameters as mentioned in the table.

Logical Extraction:

The logical extraction appears to be mildly supported across all the mobile forensic devices tested. All the Mobile Forensic Devices A, B and C equally support for the Nokia Lumia 520 and Blackberry Curve 8520 for the extraction of parameters like contacts, call logs, SMS/MMS, image, audio, video etc. But for the Samsung Galaxy 19082 all the three devices are less supportive or we can say it did not support at all. (Table 3)

Physical Extraction:

The physical extraction didn't seem to be strong across all the three mobile forensic devices tested. Device A appears totally unsuccessful for all the parameters of Nokia Lumia 520, whereas for Samsung Galaxy GT-19082 it is somewhat support the physical extraction leaving 4 parameters unsupported. (Table 4) But for Blackberry Curve 8520 it is fully supported for all the parameters except one. Device B is supported only for the Blackberry Curve 8520 for all the parameters but not for the other two mobile phones. Device C results as totally unsupported for physical extraction of all the parameters of all three mobile phones.

Hence, in this analysis both inventive features and limitations were found. These mobile devices represent the three most popular operating systems (Windows, Android & Blackberry).

On the basis of three mobile forensic devices it is concluded that no single tool can be exclusively relied upon to collect and present every item of potential evidence from a smart mobile device.

It should be noted that new releases of forensic tools and mobile operating systems may change the way the data is acquired and the result may vary.

References:

1. Nokia E5–00 Device Details, http://www.microsoft.com/en-in/mobile/phone/lumia-520/specifications
2. Blackberry Curve 8520 Device Details, http://us.blackberry.com/search.html?q=Blackberry+curve+8520#q=Blackberry%20curve%208520
3. SamsungGalaxyGT19082DeviceDetails,http://www.samsung.com/in/consumer/mobile-phone/mobile-phone/smartphone/GT-I9082EWAINU?subsubtype=android-mobiles
4. Data Extraction and Mobile/Cell Phone Forensic, http://www.forensic-pathways.com/products-and-services/mobile-phone-forensics
5. Digital Evidence: An Indian Perspective- International Law Office, http://www.internationallawoffice.com/newsletters/detail.aspx?g=93c76fe9-e156-470b-b84d-3f4cf73da391
6. Electronic Evidence and Cyber Law, www.csi-india.org
7. **Seyed Hossein Mohtasebi, Ali Dehghantanba et.al.** Smart Phone Forensics: A Case Study With Nokia E500 Mobile Phone, IJDIWC, 2011(3): 651-655
8. **John Butler**. Geode Forensics Limited, Forensic Analysis of Mobile Phones 2010.
9. **Igor Mikhaylov**. Extracting Data from Damaged Mobile Devices.2013.
10. **Curran, K., Robinson, A. et.al**. Mobile Phone Forensic Analysis, IJDCF, 2010; Vol. 2, No. 2
11. **Paul Mc Carthy**. Forensic Analysis of mobile Phones, 2005
12. **B. Wiliamson, P. Apeldoorn et.al.** Forensic Analysis of the Contents of Nokia Mobile,2006; http://ro.ecu.edu.au/adf/36
13. **Ibrahim M. Baggilli, Richard Mislan et.al.** Mobile Phone Forensic Tool Testing: A Database Driven Approach, IJDE, 2007; Vol.6, Issue 2
14. **Amjad Zareen, Shamim Baig**. Mobile Phone Forensic: Challenges, Analysis and Tools Classification, International Workshop on Systematic Approaches to Digital Forensic Engineering, 2010;PP. 47-55
15. The Mobile Consumer, www.**nielsen**.com/.../**Mobile**-**Consumer**-Report-**2013**.pdf

Table 1: Specification of Mobile Forensic Workstation

CPU	Intel Core i5
RAM	8 GB
OS	Window 7 Home Basic Service Pack 1 32bit
GPU	NVIDIA 512M 1GB
HDD	500 GB @ 5400 RPM

Table 2
Specification of Mobile Phones

Manufacturer	Nokia	Samsung	Blackberry
Model	Lumia 520	Galaxy GT-	Curve 8520
Operating System	Microsoft window	Android 4.1 (jelly bean)	Blackberry
RAM	512 MB	1 GB	256 MB
Internal Memory	8 GB	8 GB	256 MB
Expendable Memory	84 GB	64 GB	16 GB
CPU	1 GHz Dual core	1.2 GHz Dual core	512 MHz

Table 3
Logical Extraction

S. N.	Data Type	Mobile Forensic Tool (A)			Mobile Forensic Tool (B)			Mobile Forensic Tool (C)		
		Nokia Lumia 520	Blackberry Curve 8520	Samsung Galaxy GT-19082	Nokia Lumia 520	Blackberry Curve 8520	Samsung Galaxy GT-19082	Nokia Lumia 520	Blackberry Curve 8520	Samsung Galaxy GT-19082
1	Contact	250	120	180	250	120	UnSup	250	120	UnSup
2	Call history	133	51	88	133	51	UnSup	133	51	UnSup
3	SMS	44	23	70	UnSup	23	UnSup	44	23	UnSup
4	MMS	0	0	0	0	0	UnSup	0	0	UnSup
5	Email	UnSup	UnSup	UnSup	12	14	UnSup	8	6	UnSup
6	Calendar entry	UnSup	UnSup	0	UnSup	0	UnSup	UnSup	UnSup	UnSup
7	Web history	UnSup	UnSup	UnSup	UnSup	27	UnSup	UnSup	UnSup	UnSup
8	Bookmarks	UnSup	UnSup	UnSup	UnSup	0	UnSup	UnSup	UnSup	UnSup
9	Image	15	25	12	15	25	UnSup	15	25	UnSup
10	Audio	67	157	152	67	157	UnSup	67	157	UnSup
11	Video	2	8	4	2	8	UnSup	2	8	UnSup
12	User PW Extraction	UnSup	UnSup	UnSup	Yes	Yes	UnSup	UnSup	UnSup	UnSup
13	Doc	UnSup	UnSup	UnSup	UnSup	5	UnSup	2	5	UnSup

Unsupported: UnSup, Document: Doc. Password: PW

Table 4
Physical Extraction

S. N.	Data Type	Mobile Forensic Tool (A)			Mobile Forensic Tool (B)			Mobile Forensic Tool (C)		
		Nokia Lumia 520	Blackberry Curve 8520	Samsung Galaxy GT-19082	Nokia Lumia 520	Blackberry Curve 8520	Samsung Galaxy GT-19082	Nokia Lumia 520	Blackberry Curve 8520	Samsung Galaxy GT-19082
1	Contact	250	120	180	250	120	UnSup	250	120	UnSup
2	Call history	133	51	88	133	51	UnSup	133	51	UnSup
3	SMS	44	23	70	UnSup	23	UnSup	44	23	UnSup
4	MMS	0	0	0	0	0	UnSup	0	0	UnSup
5	Email	UnSup	UnSup	UnSup	12	14	UnSup	8	6	UnSup
6	Calendar entry	UnSup	UnSup	0	UnSup	0	UnSup	UnSup	UnSup	UnSup
7	Web history	UnSup	UnSup	UnSup	UnSup	27	UnSup	UnSup	UnSup	UnSup
8	Bookmarks	UnSup	UnSup	UnSup	UnSup	0	UnSup	UnSup	UnSup	UnSup
9	Image	15	25	12	15	25	UnSup	15	25	UnSup
10	Audio	67	157	152	67	157	UnSup	67	157	UnSup
11	Video	2	8	4	2	8	UnSup	2	8	UnSup
12	User PW Extraction	UnSup	UnSup	UnSup	Yes	Yes	UnSup	UnSup	UnSup	UnSup
13	Doc	UnSup	UnSup	UnSup	UnSup	5	UnSup	2	5	UnSup

Unsupported: UnSup, Document: Doc. Password: PW