International Journal of Engineering, Science and Mathematics
Vol. 7Issue 4,April 2018,
ISSN: 2320-0294 Impact Factor: 6.765
Journal Homepage: http://www.ijesm.co.in, Email: ijesmj@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

ANALYSIS OF WHATSAPP LOG FILE FOR INFORMATION RETRIEVAL

Harjinder Singh*
Mr.Ashwani Kumar**

Abstract

Smartphones have increasingly become a part of our daily life. Further, in recent years, we have witnessed a rapid increase in the use of social networking applications as an online communication method on mobile devices. One of the most popular apps which everybody seems to be using is WhatsApp messenger. People share a huge amount of data, including their personal and sensitive information using this particular App. However, as with any other App, WhatsApp leaves a significant trail of artifacts on the mobile device on which it is used. This information is stored at many locations on the phone. The same can be used by any investigating forensic agency to reconstruct the event timeline of WhatsApp.

This paper attempts to analyze the forensic artifacts left by WhatsApp in one of its key artifact file called "WhatsApp.log".

Keywords:

WhatsApp;
WhatsApp Log;
Forensic Analysis of WhatsApp;

Author correspondence:

Harjinder SinghAshwani Kumar
M. Tech (CSE) Assistant
Professor (Dept of CSE)
K.R. Mangalam University K.R. Mangalam
University
Sohna Road, Haryana, IndiaSohna Road, Haryana, India

*M. Tech (CSE), K.R. Mangalam University, Sohna Road, Haryana, India
** Assistant Professor, Dept Of CSE, K.R. Mangalam University, Sohna Road, Haryana, India

1. Introduction

In recent years, we have witnessed an explosive increase in the usage of smartphones worldwide. Nearly 95% of Americans are now smartphone owners [1]. India has nearly 300 million smartphone owners [2]. It has been predicted that by 2019 the number of smartphone users will be more than five billion [3]. Smartphones have been in use since approximately year 2007. From that time to now, smartphones are no more a luxury but have become a necessity of life. These days people use their smartphone devices not only for making voice calls / SMS, entertainment, gaming but also for using several services available on Internet, such as mobile banking, and location-based services such as Google Maps. Meantime, the use of instant messaging applications has enabled people to share information, communicate and remain connected with each other socially with ease.

The following is a summary of some interesting facts about mobile phones as per Pew Research Center [4]

- About three-quarters of U.S. adults (77%) say they own a smartphone.
- Mobile devices aren't just for calling or texting.
- Growing shares of Americans – income – rely on smartphones to access the internet.
- While smartphones are becoming more integrated into our lives, *many users aren't taking the necessary steps to secure their devices.*

The following figure shows number of WhatsApp users from Apr 2013 to Dec 2017 (in Millions) [5].

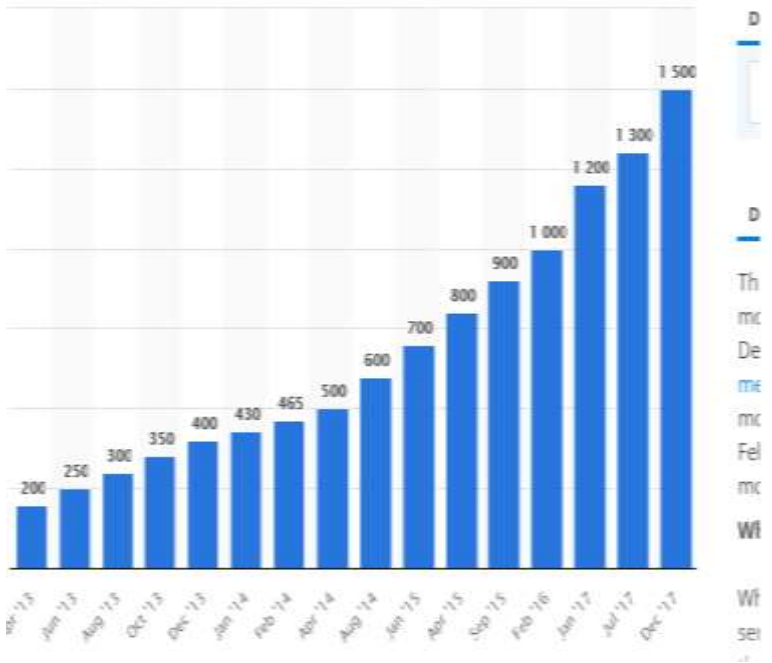

Figure 1 : Number of WhatsApp Users

The above data conveys the rapid popularity, usage and growth of WhatsApp. It has become the de-facto tool to share photos, messages, videos etc. However the same

App is misused by some people to send unwanted, inappropriate messages and also to copy sensitive data from workplace and send it to someone. The culprit then deletes all messages from his phone and claims innocence.

Thus there is a need to carry out a study on various forensic artifacts left behind on the phone by WhatsApp usage.

2. Related Work

2.1 WhatsApp Database - Hardware Acquisition

"Forensic Analysis of Instant Messenger Applications on Android Devices." [6]. A UFED physical analyzer was used to analyze instant messenger applications (WhatsApp and Viber) on Android devices. In the case of WhatsApp, chat message artifacts, timestamps and names of files sent and received were found, however the storage locations of those files were not found. In manual examination of "WhatsApp" application after the File System Extraction, database files (msgstore.db and wa.db) were found with details of chat sessions. Mainly the database extraction and a good detailed analysis was done for existing messages.

2.2 WhatsApp Forensic Analysis of Volatile Memory

"Forensic Analysis of WhatsApp on Android Smartphones" [7]. This paper forms an outline on how forensic investigators can extract useful information from WhatsApp and from similar applications installed on an Android platform. The area of focus is extraction and analysis of application user data from non-volatile external storage and the volatile memory (RAM) of an Android device.

3. Objective

- To analyse the forensic evidence contained in "WhatsApp.log"
- To relate evidence contained in the file with real world events.

4. Experimental Setup

Proposed work will be carried out by using following methodology:

- Obtain a used smartphone. In our case we will use Samsung GT-I19001T.
- Format the phone by doing a factory reset.
- Install fresh copy of WhatsApp.
- Exchange messages, photos with known phone numbers.
- Delete some messages.
- Obtain the "WhatsApp" log.
- Study the log and corelate with the actual sending / deleting of data.

5. Technologies Used

Table I: Technologies Used

Tool	Version	Detail
Android Phone	Samsung GT-I9100T Android v 4.1.2	Mobile device to carry out the study.
Dr.Fone	V 9.0.5	Phone Rooting tool
WhatsApp	V 2.18.46	Application to be investigated
ADB Andriod Debug Bridge [8]	-	Command Line Utilty

6. Testing Procedure

- We obtained a used Samsung phone Model GT-L19001T.
- Factory reset the phone by using the built in functionality. We took care to format the USB storage which is nothing but the internal storage memory of the phone.
- Next we installed WhatsApp v2.18.46 via Google play store.

The following table shows the set of random activities which were carried out on WhatsApp

Table II: Activity Sequence

Sl. No.	Activity	Date / Time Done (Approx)
1	Installed WhatsApp on phone number 9654xxxx02	Feb 19, 2018 / 1950 hrs
2	Added contact number 9711xxxx07	Feb 19, 2018 / 1955
3	Received photo from 9711xxxx07	Feb 19, 2018 / 2000 hrs
4	Sent text message to 9711xxxx07	Feb 19, 2018 / 2000 hrs
5	Sent my location message to 9711xxxx07	Feb 19, 2018 / 2000 hrs
6	Added new contact number 965xxxxxx5	Feb 20, 2018 / 1055 hrs

7	Sent text message to 965xxxxxx5. Message was not seen by this contact.	Feb 20, 2018 / 1055 hrs
8	Made a whatsapp voice call to 9711xxxx07. Call duration	Feb 20, 2018 / 1605 hrs
9	Deleted a message at random.	Feb 24, 2018 / 1045 hrs

- Next we need to root the phone. This is required because the log file is in a protected area and the Android OS will not let us access it otherwise. To root the phone, connect it to laptop via USB cable. Next run the Dr Fone [9] utility on the laptop which roots the phone.
- Go to the directory where the file ADB.exe exists. In that directory open a CMD terminal. Execute "adb devices". The phone ID should show up as attached. Refer following figure.

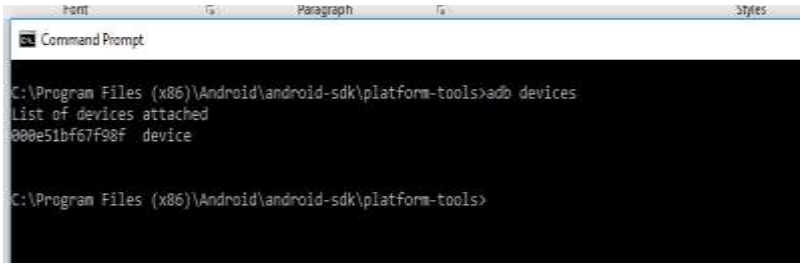

Figure 2 : Obtaining Phone ID

- Execute "adb -d shell". To check whether your phone is rooted execute "su". This should get you the following figure.

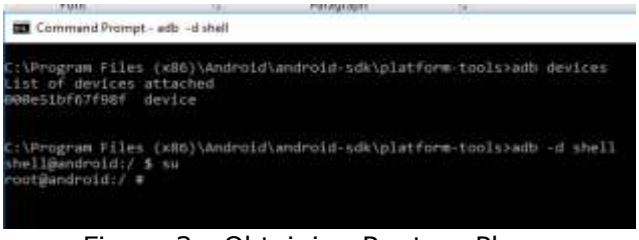

Figure 3: Obtaining Root on Phone

- As can be seen we have got the system prompt "root@android:/#". To make one more check execute "ls /data". This gets the contents of "/data" directory. This is possible only if the device is rooted else the command would not be executed.
- Execute following cmd: "cd /data/data/com.whatsapp/files/Logs". Next list the directory. The following is obtained. We can see that "Logs" directory contains one log file and two zipped files. This might be different in different cases. We need to pull these files from the phone and onto our PC for analysis.

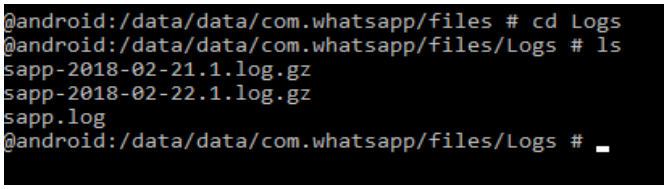

Figure 4: Listing of "Logs" Directory

- This is done by exiting ADB shell and going back to the DOS prompt. Execute following command "adbpull /data/data/com.whatsapp/files /Logs/whatsapp.log g:\". This will pull the file to your G: drive. Similarly repeat for the other two files.
- Now we unzip the files and open the same in any word processor for analysis against the known events mentioned at Table II.

7. Analysis

The following table shows detailed analysis of the WhatsApp log file:

Table III: Analysis of WhatsApp.log

Sl No	**WhatsApp.log (Certain text have been highlighted in bold for attention)**	**ANALYSIS**	**CO-RELATION WITH TABLE:II**
1.	**2018-02-19 19:53:34.410** LL_I D Buildinfo a=com.whatsapp; vc=452170; **vn=2.18.46**; b=release; p=consumer; f=play; d=false; v=2.18.46-play-release; e=180; g=75392c760bb2-dirty; **t=1518113290560**	1. This entry is created in the log file when WhatsApp was installed on the phone. 2. The first highlighted text displays the time /date at which this event took place. It shows that the App was installed on this phone on 19 Feb, 2018 at **19:53:34.410** hrs. (Note that the time stamp is accurate to milliseconds). 2. It shows the version number of installed software which is **2.18.46.** This was physically verified by checking the same in the actual phone**.** 3. The number **t=1518113290560** is the epoch time and tells the date & time at which this version was updated by the developers. We developed a small Java utilty to decode the epoch time in human readable form. The decoded value is Feb 08, 2018.	1. Refer Sl No:1 of Table II. 2. Entry relates to the fresh installation of WhatsApp on the phone.
2.	2018-02-19 19:53:34.890 LL_I W [583:WhatsApp Worker #3] media-state-manager/refresh-media-state/**internal-storage available:1,679,187,968**	1. Shows the total device memory of phone which is 2113732608 bytes or 1.97GB. The same was verified by actually checking	1. Refer Sl No:1 of Table II. 2. Entry relates to the fresh

Sl No	WhatsApp.log (Certain text have been highlighted in bold for attention)	ANALYSIS	CO-RELATION WITH TABLE:II
	total:2,113,732,608 2018-02-19 19:53:34.890 LL_I W [583:WhatsApp Worker #3] media-state-manager/refresh-media-state/writable-media/**external-storage available: 12,348,653,568 total: 12,353,372,160**	the internal memory of the phone. 2. Shows the total USB storage memory of the phone which is 12353372160 bytes or 11.5 GB. It is to be noted that technically this is also part of the internal memory only. **This is not the external SDcard.**	installation of WhatsApp on the phone.
3.	2018-02-19 19:55:03.874 LL_I W [1:main] register/phone/suggested/cc/91 pn=**96xxxxxx02** suggest=9196xxxxxx02 s=+9196xxxxxx02 disp=9196xxxxxx02 same=false	1. User Phone number is recorded in the log at the time of registration.	1. Refer Sl No:1 of Table II. 2. Entry relates to the fresh installation of WhatsApp on the phone.
4.	2018-02-19 19:56:06.454 LL_I W [610:ReaderThread] xmpp/reader/read/**profilephotoreceived** 9196xxxxxx02@s.whatsapp.net id:nulltype:previewhas_url:**false**has_data:**false**	1. Shows that we have not set the profile photo at the displayed event time.	1. Refer Sl No:1 of Table II. 2. Entry relates to the fresh installation of WhatsApp on the phone.
5.	2018-02-19 19:56:16.599 LL_I W [608:WriterThread] xmpp/writer/write/push-name; pushName=**Ficky1**	1. WhatsApp has recorded the user name as typed at the time of registration.	1. Refer Sl No:1 of Table II. 2. Entry relates to the fresh installation of WhatsApp on the phone.
6.	2018-02-19 19:56:24.079 LL_I W [1:main] **unknown contact added**: row_id=27 jid=status@broadcast key=(null) phone=null iswa=true | time: 582	1. WhatsApp has recorded that we have added a new contact.	1. Refer Sl No:2 of Table II. 2. Entry relates to adding of a new contact in WhatsApp.
7.	**2018-02-19 19:59:48.721** LL_I W [601:Signal Protocol] **msgstore/add/recv**; key=Key[id=**66C0DDEA65EDB701DDE89D46F688553D**, **from_me=false**, remote_jid=**9197xxxxxx07**@s.whatsapp.net]; **media_wa_type=1**; status=0	1. Shows that WhatsApp received a message from phone number 9197xxxxxx07 At 19:59 hrs. 2. "**from_me=false**" indicates that it is an incoming message. 3. The most important part of	1. Refer Sl No:3 of Table II. 2. Entry relates to the phone receiving a photo from 9197xxxxxx07

Sl No	WhatsApp.log (Certain text have been highlighted in bold for attention)	ANALYSIS	CO-RELATION WITH TABLE:II
		this entry is the Key ID which is a unique 32 digit number for each message sent or received. ***This ID is very useful in tracing deleted messages.*** 4. Media_wa_type=1 indicates that the message type was image	
8.	**20:00:18.280** LL_I W [1:main] **msgstore/setchatseen/9197xxxxxx07@s.whatsapp.net/1/1/0/null/0** 2018-02-19 **2018-02-19 20:00:17.493** LL_I W [1:main] **conversations/click/jid 9197xxxxxx07**@s.whatsapp.net pos=2	1. Shows that at 2000 hrs we have clicked on the conversation started by 9197xxxxxx07.	1. Refer Sl No:3 of Table II. 2. Entry relates to the phone receiving a photo from 9197xxxxxx07
9.	**2018-02-19 20:01:38.858** LL_I W [543:Messages Async Commit Thread] **msgstore/add/send**; key=Key[id=**A4C305BBA2712278D382B942B6921F5C,from_me=true**, **remote_jid=9197xxxxxx07**@s.whatsapp.net]; **media_wa_type=0**; status=0	1. Indicates that at 20:01 hrs we have sent a message to phone 97xxxxxx07. 2. **media_wa_type=0** indicates that the message was of text.	1. Refer Sl No:4 of Table II. 2. Entry relates to us sending a text message to 9197xxxxxx07
10.	**2018-02-19 20:01:49.276** LL_I W [610:ReaderThread] **xmpp/reader/read/status-update-from-target** Key[id=**A4C305BBA2712278D382B942B6921F5C**, from_me=true, **remote_jid=91971xxxxxx07**@s.whatsapp.net] null 13 1519050710000	1. By correlating the key ID we deduce the fact that the sent message has been seen by the target.	1. Refer Sl No:4 of Table II. 2. Entry relates to we sending a text message to 9197xxxxxx07
11.	**2018-02-19 20:02:59.672** LL_I W [543:Messages Async Commit Thread] **msgstore/add/send**; key=Key[id=**67448C8F6024BE81EC33EB8995B9F8BC**, **from_me=true**, **remote_jid=9197xxxxxx07**.@s.whatsapp.net]; **media_wa_type=5**; status=1	1. Indicates that at 20:02 we have sent a message to 9197xxxxxx07. 2. M**edia_wa_type=5** indicates that the message was of type **location.** 3. This is confirmed by another entry with the same	1. Refer Sl No:5 of Table II. 2. Entry relates to we sending a location message

Sl No	WhatsApp.log (Certain text have been highlighted in bold for attention)	ANALYSIS	CO-RELATION WITH TABLE:II
	2018-02-19 20:03:00.846 LL_I W [608:WriterThread] xmpp/writer/write/message-encrypted; key=Key[id=**67448C8F6024BE81EC33EB8995B9F8BC**, **from_me=true**, remote_jid=9197xxxxxx07@s.whatsapp.net]; originalTimestamp=0; participant=null; groupParticipantHash=null; **mediaType=location**;	key number in which media_type is confirmed as location.	
12.	1. 2018-02-20 10:50:05.723 LL_I W [1:main] **com.whatsapp.ContactPicker.onCreate** 2. 2018-02-20 10:54:15.824 LL_I W [124:sync] **added 1 contacts** (1 whatsapp) 3. 2018-02-20 10:54:15.840 LL_I W [124:sync] updated contact status jid=**9196xxxxxx85**@s.whatsapp.net **status_timestamp=1491321349000status=Enjoy your power**	1. Shows that the user has activated contacts picker. 2. Shows that at 10:54 hrs we have added a new contact. 3. Shows the phone number of the added contact. Status_timestamp in epoch time shows at what time the added contact has joined WhatsApp. In this case the decoded time is Apr 04, 2017 at 2125 hrs. The status line indicates the displayed status of the added contact.	1. Refer Sl No:6 of Table II. 2. Entry relates to us adding a new contact.
13.	1. 2018-02-20 10:54:44.771 LL_I W [113:Messages Async Commit Thread] **msgstore/add/send**; key=Key[id=**642527E642D5482E8582B9F8A2031BE9**, from_me=true, **remote_jid=9196xxxxxx85**@s.whatsapp.net]; **media_wa_type=0;** status=0 2. 2018-02-20 10:54:48.381 LL_I W [169:ReaderThread] **xmpp/reader/read/status-update-from-target** Key[id=642527E642D5482E8582B9F8A2031BE9, from_me=true, remote_jid=9196xxxxxx85@s.whatsapp.net] **null 5**	1. Shows that we have sent a text message to 9196xxxxxx85. 2. Shows that the target has received the message. But the words " **null 5**" indicate that ***target has not yet read the message.*** 3. Receipt of this entry now	1. Refer Sl No:7 of Table II. 2. Entry relates to us sending a text message. But the message was not instantaneously read by the target. The message was only read at a later time which has been confirmed by the logfile entries.

Sl No	WhatsApp.log (Certain text have been highlighted in bold for attention)	ANALYSIS	CO-RELATION WITH TABLE:II
	1519104288000 3. 2018-02-20 16:04:51.951 LL_I W [249:ReaderThread] **xmpp/reader/read/status-update-from-target** Key[id=642527E642D5482E8582B9F8A2031BE9, from_me=true, remote_jid=91965xxxxxx85@s.whatsapp.net] **null 13** 1519117400000 4. 2018-02-20 16:04:52.061 LL_I W [162:WriterThread] **xmpp/writer/write/read-receipt-received;**stanzaKey=[StanzaKey from=9196xxxxxx85@s.whatsapp.net cls=receipt id=642527E642D5482E8582B9F8A2031BE9 type=read]; disable=false	confirms that the target has read at 1604 hrs. 4. Further confirmed by this entry.	
14.	1. 2018-02-20 16:06:22.487 LL_I W [113:Messages Async Commit Thread] **msgstore/add/send**; key=Key[id=call:78CF9F7FA54B6E98669624382E25230D, **from_me=true**, **remote_jid=91971xxxxxx07**@s.whatsapp.net]; **media_wa_type=8**; status=6 2. 2018-02-20 16:06:35.496 LL_I W [268:VoIPSignaling Thread] wa_call_utils. 16:06:35 **EVENT: Call accept received** 3. 2018-02-20 16:06:35.500 LL_I W [268:VoIP Signaling Thread] wa_transport_p 0: **Local: 192.xxx.x.7:50839, Remote: 100.xxx.xxx.5:58358**, priority: 0x202 4. 2018-02-20 16:07:06.535 LL_I W [268:VoIP Signaling Thread] **wa_call_signal Call**	1. Indicates that we have initiated a WhatsApp voice call at 16:06 hrs to 9197xxxxxx07. Note from_me=true &&media_wa_type=8. 2. Indicates that the other party has picked our call. 3. WhatsApp records the IP addresses of the called &&callee. This is undeniable forensic evidence. 4. Indicates the call duration in milliseconds. This was confirmed actually by noting the call time in WhatsApp which showed **31 seconds**.	1. Refer Sl No: 8 of Table II. 2. Relates to the fact that we made a WhatsApp call that lasted 31 seconds.

Sl No	WhatsApp.log (Certain text have been highlighted in bold for attention)	ANALYSIS	CO-RELATION WITH TABLE:II
	end, duration: 31151, video call: 0, call side: caller, call_id: 78CF9F7FA54B6E98669624382E25230D, peer_jid: 9197xxxxxx07@s.whatsapp.net, test bucket:		
15.	**2018-02-24 10:42:06.973** LL_I W [821:Messages Async Commit Thread] thumbnailmsgstore/**deleteMessageThumbnail/0BECD78CED03B8F2448380C02AA82007**/0	1. Indicates that we have deleted a message at the displayed time. 2. The unique message id is also recorded.	1. Co-relates to Sl. No. 9 of Table II.

8. Summary of Analysis

The detailed analysis of the WhatsApp log file is placed at Table III. However, the summary of the analysis is as follows:

- WhatsApp log file contains real time information of all events happening in the app.
- The events are time stamped in Unix epoch time format. The precision of the time stamp is accurate to milliseconds.
- Interesting events are :
  - Incoming / Outgoing messages (Text, Image, Video)
  - Incoming / Outgoing Voice & Video calls.
  - Installation time and version of WhatsApp on the phone.
  - Summary of various types of massages sent / received at fixed intervals of time.
  - Record of total memory available and used at fixed intervals of time.
  - Record of O.S. version of the phone.
  - Record of whether profile photo set or not at the time of registration.
  - Record of user name entered at time of registration of the App.
  - Record of whether a given message is incoming or outgoing.
  - Record of media type of all messages (Text, Image, Video, Geo-location).
  - Addition of new contact.
  - Record of whether the third party has read the message sent by us along with time of reading.
  - Record of call durations.

- Events of following types are marked with a **unique***32 digit "key id "* :
  - All incoming and outgoing messages (Text, Image, Video)
  - All voice and video calls made on WhatsApp. (Incoming and outgoing).

The unique id can be then used to search for deleted messages in the log file. The

exact time of deletion of any given message can be determined.

9. Conclusion

This paper shows that the ***WhatsApp.log*** is a logfile which is automatically updated by the application. We have further shown that *WhatsApp* records all the real time events which happen when one uses the application in the subject log file. We have shown how the entries in the log file can be co-related with the real life events. This information can be used in future by any forensic agency which is interested in tracing the WhatsApp usage time line of a given smartphone.

10. Future Work:

Recently WhatsApp has been allowed to make online payments by using India's Unified Payment Interface (UPI). The forensic evidence left behind by this new feature in the log file is a potential area of research.

11. References

[1] "Mobile Fact Sheet." Internet: http://www.pewinternet.org/fact-sheet/mobile/, [Apr. 12, 2018]

[2] "India Poised For Smart Phone Revolution." Internet: http://money.cnn.com/2017/09/26/technology/india-mobile-congress-market-numbers/index.html, [Apr. 12, 2018]

[3] "Number of smartphone users worldwide from 2014 to 2020 (in billions)." Internet: http://www.statista.com/statistics/ 30695/ number-of-smartphone-users-worldwide/, [Apr. 12, 2018]

[4] "10 facts about smartphones as the iPhone turns 10." Internet: http://www.pewresearch.org/fact-tank/2017/06/28/10-facts-about-smartphones/, [Apr. 12, 2018]

[5] "Number of monthly active WhatsApp users worldwide from April 2013 to December 2017." Internet: https://www.statista.com/statistics/260819/number-of-monthly-active-whatsapp-users/, [Apr. 12, 2018]

[6] Mahajan, Aditya, M. S. Dahiya, and H. P. Sanghvi. (2013) "Forensic Analysis of Instant Messenger Applications on Android Devices." International Journal of Computer Applications (0975 – 8887) Volume 68– No.8, April 2013

[7] Neha S. Thakur (2013) . "Forensic Analysis of WhatsApp on Android Smartphones". University of New Orleans ScholarWorks@UNO.

[8] "Android Debug Bridge." Internet: https://developer.android.com/studio/command-line/adb.html, [Apr. 12, 2018]

[9] "dr-fone- Recover." Internet: https://drfone.wondershare.com/android-data-recovery.html, [Apr. 12, 2018]

[10]"WhatsApp Messenger." Inernet:https://play.google.com/store/apps/details?id=com.whatsapp, [Apr. 12, 2018]