Forensic Analysis of Wickr Application on Android Devices

Tarun Mehrotra[1, 2], B. M. Mehtre[2]
[1]School of Computer and Information Sciences, Hyderabad Central University, Hyderabad, India
[2]Center for Information Assurance and Management, Institute for Development and Research in Banking Technology (Established by Reserve Bank of India), Hyderabad, India
(tarun4242@gmail.com, bmmehtre@idrbt.ac.in)

Abstract - **As there are many applications that are supported by smartphones, so there is an increasing interest in finding artifacts (digital evidence) created by such applications. Wickr is a free application that allows users to send self-destructing files and messages. It came out as an iOS-only app but now it is launched in "public-beta" for android devices. As claimed by the Wickr app founders, it leaves no traces behind even for forensic investigators. This research focuses on authenticating the claims above. Experiments consisting of various test cases on rooted and non-rooted android devices were performed to investigate whether the traces are left behind or not.**

Keywords - **Wickr, Digital forensics, Android forensics, Artifacts, Forensics Investigation, Anti-Forensics**

I. INTRODUCTION

Smartphone age may have brought us the convenience of instant communication, but it has also left us vulnerable to the prying eyes of corporations and business who may decide to share your text, pictures, audio & video messages with the rest of the world.

To provide secure communication that leaves no traces, a team of security and privacy experts comes up with a mobile application: Wickr. This app was introduced for iOS devices but now it goes multi-platform as it is available for android. This app is different as it gives the user the option to set a self-destruct timer to anything they send so that they can control how long a recipient views their videos, photos or text before it disappears completely. The aim of this research was to investigate forensic artifacts if they can be recovered from the Wickr application on a Samsung smartphone running android on both rooted and nonrooted device. Features of the Wickr application are listed in Table I.

II. RESEARCH METHODOLOGY

The main purpose of this experiment is to find any artifacts or traces during forensic analysis of Wickr application in rooted and nonrooted Android smartphones.

A. Android Rooting

Rooting an Android device may be perceived in a way similar to jailbreaking an iPhone. With that said, the term rooting refers to gaining access to the root directory " / " and having the appropriate administrative permissions to take root actions [2]. Once a device is rooted we can have access to device system files. Without rooting the device, the device user lacks sufficient privilege to access anything more than the default user directory. Table II shows a list of Android phones and their version used:

B. Testing Equipments & Procedures

1) Table III shows a list of hardware's, software's and applications used for experiment and analysis.

2) *Procedures:* The experiment consisted of using a Wickr app on the Android smartphone followed by two attempts at forensic analysis – one with non rooted device (Samsung Galaxy S DUOS GT-S7562) and one with rooted device (Samsung Galaxy S II I9100).

(a) *Creation of Scenario for nonrooted device*: Wickr was installed on the non-rooted Samsung Galaxy S DUOS GT-S7562 device. The following steps were performed:

(i) We entered the username "tarunforensics" to create account on Wickr.
(ii) We started instant messaging conversation with a Wickr friend, the user "piyushhome".

TABLE I
FEATURES OF WICKR APP

Application	General Features
Wickr	1)Text Chats 2)Send and Receive images 3)Send and Receive audios 4)Send and Receive videos

TABLE II
ANDROID PHONES & VERSION USED

Mobile phone maker & model	Rooted/Non Rooted	Android version
Samsung Galaxy S II I9100	Rooted	4.0.3-ICS
Samsung Galaxy S DUOS GT-S7562	Non-Rooted	4.0.4-ICS

978-1-4799-1597-2/13/$31.00 ©2013 IEEE

TABLE III
HARDWARE'S, SOFTWARE'S AND APPLICATIONS USED

List of Hardware's & the Software's used in Experiments	Configuration/Version
A PC running as the forensic workstation	CPU Intel Core i5 -2400M, RAM 4GB DDR3, Hard Disk SATA 500GB, Windows 7 professional SP1.
Android phones	Refer Table II
Titanium Backup Android app	v6.1.1
Helium Backup Android app	v1.1.0.8
Hex Workshop	v6.7
Micro USB cable	U2
Wickr application for testing	Refer Table I

(iii) As "tarunforensics" we sent various messages with some audio clips.
(iv) We set a timer for self destruction of some messages and for others we left default timer which is 5 days. (messages will be automatically destructed after 5 days)
(v) It is to note that messages are destructed from sender side as well as receiver side according to a timer set by the sender.
(vi) We deliberately deleted some messages before the timer expired, then we waited for some messages to be deleted according to a timer expires and some were deleted according to a default timer (5 days)
(vii) We examine the device at various intervals that will be discussed shortly.

Text, audio and picture sent from Wickr user "tarunforensics" to the other Wickr user "piyushhome" is shown in Table IV.

Fig. 1 is showing messages in a Wickr app to Wickr user "piyushhome".

(b) *Examination of the nonrooted device:* We employed Titanium Backup application [6] for logical acquisition, but were unable to perform a backup as we didn't have root permission as required by the app. So, we performed a live examination of the device using the Helium application (formerly known as Carbon*)* for android which does not require root. We were only able to access user data files and could not identify any traces of Wickr messages.

TABLE IV
MESSAGE EXCHANGED BY NONROOTED PHONE

Messages	Timer sets	Action done by sender
Good Morning. Have a nice day.	10 seconds	No action. Message was self destructed
Start the mission fast	5 hours	Deliberately deleted before the timer expires
Audio clip of 20 seconds.	1 minute	No action. Message was self destructed
Picture from gallery with text "enjoy".	No Timer Set	Self destructed after the default timer expires.(5 days)
Work completed boys	No Timer Set	Self destructed after the default timer expires.(5 days)

(c) *Creation of scenario for rooted device:* Wickr was installed on the rooted Samsung Galaxy S II I9100 device. The following steps were performed:
(i) We entered the username "piyushhome" to create account on Wickr.
(ii) We started instant messaging conversation with a Wickr friend, the user "tarunforensics".
(iii) As "piyushhome" we sent various messages with some audio clips.
(iv) We set a timer for self destruction of some messages and for others we left default timer which is 5 days. (messages will be automatically destructed after 5 days)
(v) It is to note that messages are destructed from sender side as well as receiver side according to timer set by the sender.
(vi) We deliberately deleted some messages before the timer expired and then we waited for some messages to be deleted according to timer expires and some were deleted according to a default timer (5 days).
(vii) We examine the device at various intervals that will be discussed shortly.

Text, audio and picture sent from Wickr user "tarunforensics" to the other Wickr user "piyushhome" is shown in Table V.

Fig. 2 shows messages in a Wickr app to Wickr user "tarunforensics".

(d) *Examination of rooted device:* We employed Titanium Backup application for logical acquisition. The backup obtained was copied from SD card in the device to the forensic workstation for examination. Using Hex Workshop, we examined the contents of the backup.

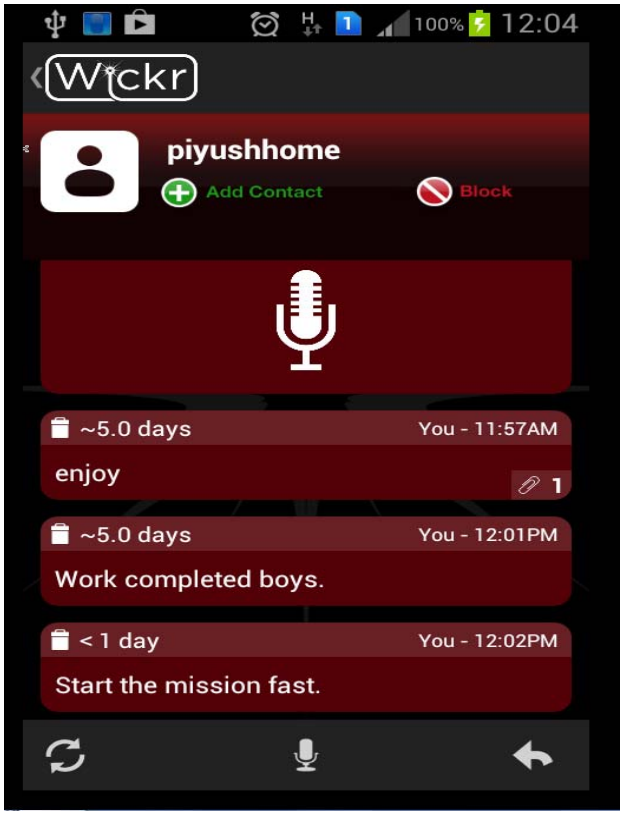

Fig. 1. Messages to user "piyushhome"

III. Results

A. NonRooted Device

At various intervals we took the backup of non rooted device by helium back up android app. Without rooting the device, the device user lacks sufficient privilege to access anything more than the default user directory "/mount/sdcard" on the device. In that directory we found the folder "**com.myWickr.Wickr"**. In that we got two files as shown in Fig. 3.

We analyze ".ab" file with Hex Workshop as shown in Fig. 4.

We tried to find artifacts by "FIND" option available. We put various strings like morning, mission, enjoy, nice etc. that we used in our messages (Refer to Table IV) as shown in Fig. 5.

But we found no artifacts/traces related to our exchanged messages as shown in Fig. 6.

B. Rooted Device

At various intervals we took the back up of rooted device by titanium back up android app. We created a folder in SD card as "tit" to store our titanium back up. We were able to access Wickr application files located in "/sd card/tit/" as shown in Fig. 7.

When we took the backup file in forensic workstation then we got 4(four) folder as shown in Fig. 8.

There was a "Wickr_db" file in database folder as shown in Fig. 9, that we opened in Hex Workshop. We tried to find artifacts by "FIND" option available as done previously. We put various strings like battle, terror, dark, joy etc. that we used in our messages (Refer to Table V). But here also we found no artifacts related to our exchanged messages. Traces found also were not related to our investigation.

IV. Summary

In this research we were not able to found any artifacts /traces related to Wickr app in both rooted and nonrooted android device. Even no information on the users contacted was found. We tried variety of test cases like deleting messages before their expiry, default destruction of messages etc. but not even a single trace related to our exchanged message was found.

TABLE V
MESSAGE EXCHANGED BY ROOTED PHONE

Messages	Timer Set	Action done by sender
Do job when night becomes dark.	30 seconds	No action. The message was self destructed
World is battle field	12 hours	Deliberately deleted before the timer expires.
Audio clip of 15 seconds	4 minutes	No action. The message was self destructed
Picture from gallery with text "joy".	No timer set	Self destructed after the default timer expires. (5 days)
Terror is bad.	No timer set	Self destructed after the default timer expires. (5 days)

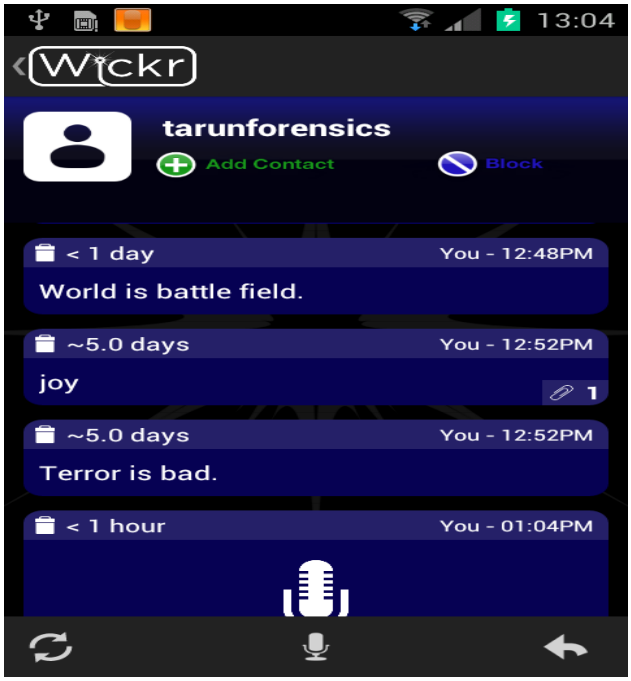

Fig. 2. Messages to user "tarunforensics"

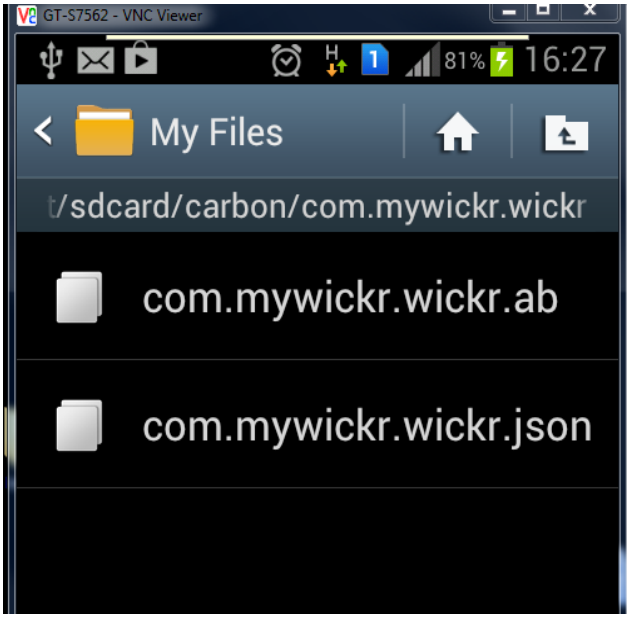

Fig. 3. Files in folder **com.myWickr.Wickr**

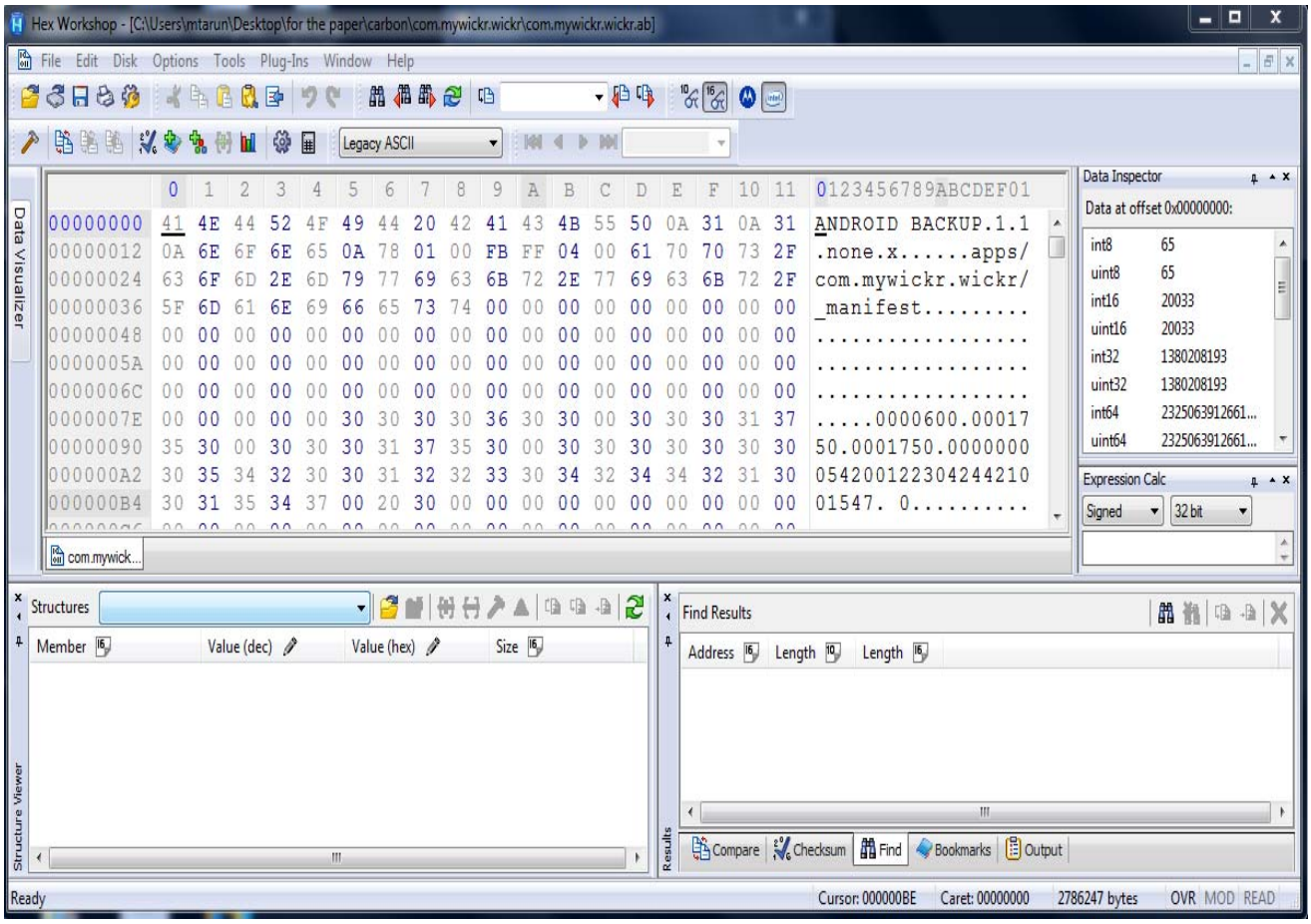

Fig. 4. Backup file ".ab" in Hex Workshop

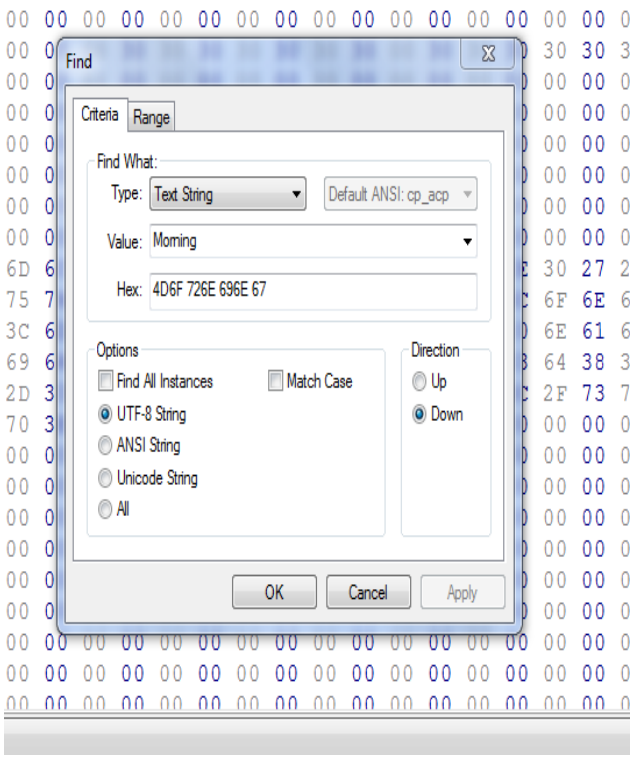

Fig. 5. Strings Searched in "FIND" option

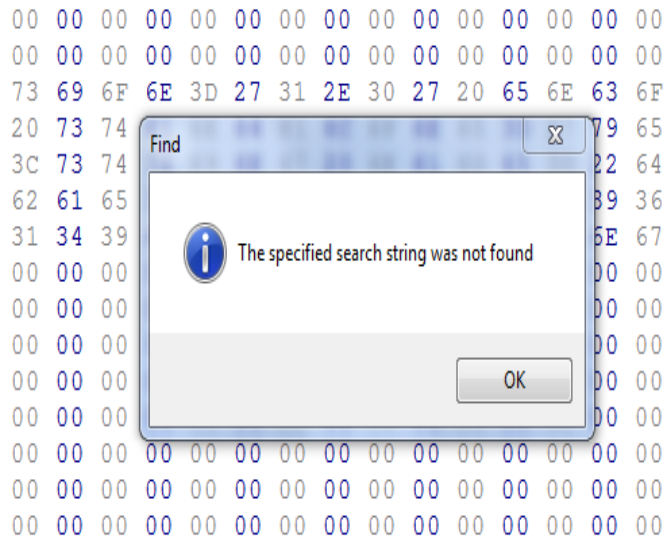

Fig. 6. No artifacts found

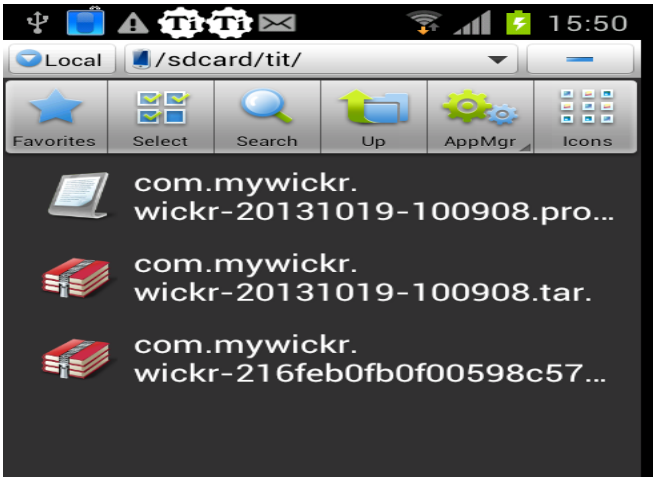

Fig. 7. Wickr application files located in "/sd card/tit/"

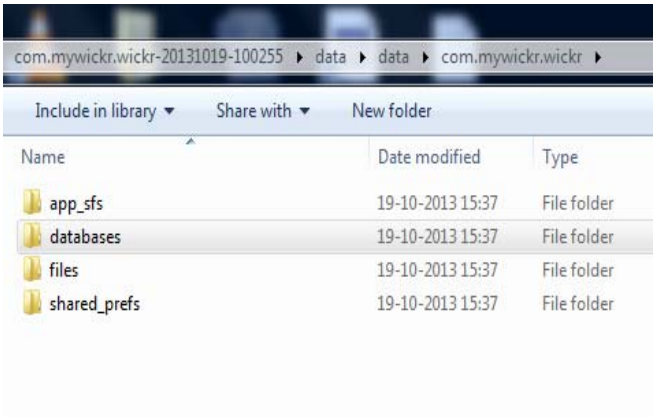

Fig. 8. Folders in backup file

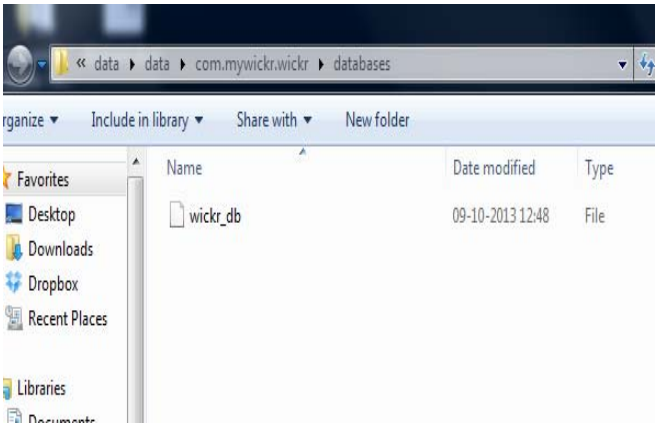

Fig. 9. Wickr_db file in database folder

V. CONCLUSION & FUTURE WORK

As we are unable to finds any traces of Wickr app on android devices, so we can say that this application will allow for everyday users to have control over their privacy. Organizations could utilize the services of this app to safely send client information & other sensitive materials.

There are clear lessons for forensic investigator & law enforcement who will have a tough time investigating the crime in which this application is involved. As there is no traces found so we can infer that this application might be using some techniques which deletes all the information regarding messages exchanged. It seems to be an anti forensic tool which can also be used by criminals to perform their crimes.

We have investigated the backup files of Wickr app for both rooted and non rooted android devices, more advanced forensic investigation can be carried out in future to find any traces possible.

REFERENCES

[1] J. Lessard,G.C.Kessler,"Android Forensics:Simplifying Cell Phone Examinations," Small Scale Digital Device Forensics Journal,vol.4,Sep. 2010

[2] Al Barghouthy, N.; Marrington, A.; Baggili, I., "The forensic investigation of android private browsing sessions using orweb," Computer Science and Information Technology (CSIT), 2013 5th International Conference on , vol., no., pp.33,37, 27-28 March 2013.

[3] Aditya Mahajan, M S Dahiya and H P Sanghvi. Article: Forensic Analysis of Instant Messenger Applications on Android Devices. International Journal of Computer Applications 68(8):38-44, April 2013.

[4] A. Hoog, Android Forensics: Investigation, Analysis and MobileSecurity for Google Android. Syngress, 2011, p. 432.

[5] T. Vidas, C. Zhang, and N. Christin, "Toward a general collection methodology for Android devices," Digital Investigation, vol. 8, pp.S14–S24, Aug. 2011.

[6] "TitaniumBackupRoot"2013[Online].Available: https://play.google.com/store/apps/details?id=com.keramidas.TitaniumBackup&hl=en