Forensic Analysis of Content Hiding Android Applications

Parag Rughani*
Ph. D., IFS, Gujarat Forensic Sciences University,
Gujarat, India

DOI: 10.23956/ijarcsse/V7I6/0124

Abstract—In this era of smartphones and with the availability of sophisticated anti-forensic applications, it is a big challenge for forensic investigators to retrieve information hidden using anti-forensic techniques. This paper discusses forensic analysis of content hiding android applications. The work mentioned in this paper is carried out to retrieve maximum information related to how these applications store data, whether they encrypt the data or not, how the credentials and patterns are preserved, etc. Outcome of this work will help forensic investigators in handling content hiding android applications, which if not investigated may hide lots of crucial information.

Keywords—Android Applications Forensics, Content Hiding Applications, Vault, Safe Box, Android Anti-Forensic Techniques, Android Forensics, Privacy Applications

I. INTRODUCTION

Evolution in technology has changed the way crime had been committed and solved in the past. Increasing use of Smartphone, Internet and smart gadgets in day-to-day life have become crucial source of information. People all over the world have become smartphone and Internet dependent for all sorts of work. As per Gartner [1] report, “Global sales of smartphones to end users totaled 432 million units in the fourth quarter of 2016”. However, notable change observed in last few years is because of Android OS, which is holding 84.82 % smartphone market share by 2016 mentioned by statista [2].

It is not only android that changed the whole world, but advancement in high speed Internet has also played equal role. As per the statistics from internetlivestats [3], the number of Internet users has crossed over 3 billion in 2014 compared to less than one billion in 2005. In early days when there was less access to Internet, people where using mobile phones mainly for voice communication and messaging. But as both the technologies – smartphones and speed and accessibility of Internet – grew together, they opened a whole new world of smartphones and gadgets which allows them to connect to anything from anywhere at anytime.

However, even if you have mobile device and high speed Internet, you cannot do much until and unless you get interface to do your tasks, this is the reason the main contributors in this domain are application developers.

The developers from all over the world have developed and are still developing variety of applications, ranging from games, utilities, financial apps, wallets and much more. Openness of android and ease of publishing apps to the Google play store has made it possible for developers to develop and publish unlimited apps for android users. As per the statistics published by statista [4], Google Play Store was most recently placed at 2.8 million apps in March 2017. This figure shows how versatile the application market is.

As being an open platform, Google play store hosts applications for various purposes. Though, majority of applications are designed to assist end users in their routine work, many of them are developed with other intentions. One such purpose is to allow users to maintain their privacy. There are hundreds of applications which allow users to hide their contents including multimedia files, messages, and much more. These applications in general, also support locking access to applications.

These content hiding applications are mostly aimed to provide privacy to the end users, but this may not be case in all conditions. If we look at the other side of privacy, then the hidden content by the end user may restrict forensic investigation process, especially when such phone was used by a victim or the suspect. This paper emphasizes on forensic analysis of such content hiding applications to assist forensic investigators in solving a crime.

Following sections of the paper discuss smart phone related crimes, privacy or anti-forensics, role of content hiding applications in forensic investigation, forensic analysis of various factors related to content hiding applications and conclusion.

II. SMARTPHONE RELATED CRIMES

It wouldn't be too much to say that most of the crimes committed these days involve role of smartphone directly or indirectly. Whatever the nature of crime may be but the way smartphones are used in storing and communicating information, they are the crucial source of information. In the early days of mobile phones, only CDR was the key information which was used and considered in solving a crime. But, in today's scenario a smartphone can contain Internet history logs, locations, social network activities, emails, documents, multimedia files and much more.

Direct involvement of smartphones in digital and conventional crimes is always visible and most of the time it becomes important evidence to solve the case. But many times smartphones are involved indirectly and can become instrumental as they can tell what a person does, where the person was, whom he contacted, what were his interests, overall psychology of a person based on the applications and Internet content he accessed, and much more. These small
pieces of information may not directly provide any evidence of a crime but indirectly they can tell overall nature of a person – a victim or a suspect.

As per the report from RSA [5] rise in fraud attempts originating from the mobile channel, increasing 173% increase between 2013 and 2015 compared to a mere one percent in the Web channel. This clear indicates how quickly mobile phones are being targeted and it also depicts that such crimes will increase in near future.

### III. PRIVACY OR ANTI-FORENSICS

As the crimes are increasing, investigative techniques to solve these crimes are also increased and strengthened. However, criminals always find out ways to keep the investigation process complex and lengthy. The anti-forensic techniques like staying anonymous, clearing logs and history are few common methods used by criminals.

Though, these techniques are used in anti-forensics they are equally used by a normal users to assure their privacy. The purposes and intentions may not be criminal in nature but the functionality remains same. Most of the users use incognito mode or private browsing mode while surfing the Internet, they may not be using it for any malicious purpose but still they know that it will allow them not to be tracked. Similarly, cleaning history after web access is also a common habit in end users, may be this is one of the ways by which users ensure their privacy. Aggarwal, G et.al [6] analyzed private browsing modes while Satva K et.al. [7] discussed a forensic approach to retrieve remnants from private browsing.

It is always a debatable point whether the tools and techniques used by users for their privacy are ethical and legal? One of the well known cases is Apple V/S FBI, as mentioned by Timberg, C. & Miller, G. [8], FBI “Director James B. Comey sharply criticized Apple and Google for developing forms of smartphone encryption so secure that law enforcement officials cannot easily gain access to information stored on the devices — even when they have valid search warrants”. While, on another hand Schulze, M. [9] referred to a dual-edge sword: “encryption helps to protect the privacy of individuals and industry, but it also can shield criminals and terrorists importance of privacy.” However Shulze emphasized only on encryption, other privacy related tools and technologies can be treated equally. They do allow normal users in maintaining their privacy, while the same thing can be used by criminals in hiding their identity.

Many researchers have so far worked on anti-forensics related issues, Harris, R. [10] discussed standardized method of addressing anti-forensics, Kessler, G. C. [11] emphasized on time-sensitive anti-forensics, while Garfinkel, S. [12] categorized traditional and recent anti-forensic techniques. Albano, P. [13] on another hand discussed a novel anti-forensic technique for Android OS. Though, sufficient work has been done in this field, but still very less work is done in another approach of content hiding applications which allow to maintain privacy of the user, especially when the device is shared by more than one users. The main objective of these applications is to allow users to hide their documents, files, other content and restrict access to certain applications with help of PIN, password of pattern. Next section discusses forensic relevance of content hiding applications.

### IV. CONTENT HIDING APPLICATIONS

The word content hiding applications refers to two different types of applications. The first type is related to applications which allow to hide textual content in a container, as it is being done in steganography and digital watermaking [14]. The other type has broad coverage as it refers to the applications which allow users to hide files, documents, images, videos, chat messages, and much more. To achieve this objective these type of applications use various folders and applications locking mechanisms and this is the reason they are referred as vault, safebox, locker, app locker, etc.

These applications as other privacy related applications, allow the users to hide content of their interest from other users. As number of smartphones are increased, these type of applications are made available for all the known smartphones. Google play store itself has more than 100 applications which serve the purpose for android users. If it was only privacy then it could not have been a problem, but the same privacy concern leads to many issues for forensic investigators when they need to analyze devices having such content hiding applications.

A common scenario for such problems can be visualized when a forensic investigator acquires a smartphone from a crime scene and at the time of analysis he finds that the phone has an application and document locker app, which restricts access to media files and few social networking related applications on the phone. The investigator has to find out the ways by which he can overcome this issue and can extract maximum possible information from the phone.

As android currently holds almost 85% of smartphone market, the next section discusses important characteristics of these content hiding android applications. This is an attempt to assist forensic investigators by identifying crucial information related to the way these applications act and achieve privacy.

### V. FORENSIC ANALYSIS

To carry out experiment, 10 content hiding and privacy related android applications were selected randomly. The applications were selected from Google Play Store [15] and required apk files for these samples were downloaded from APKPure [16]. All the samples are from free category as most of the end users prefer to download apps for free.

To understand these applications forensically, Permissions, Encryption, Data Recovery and Application Lock Bypass have been considered in this research. Each of these are explained in following subsections.

#### A. Permissions

The first step to understand content hiding applications from forensics' point of view is to understand basic characteristics of the application. Static analysis is the most common and less risky way of analyzing an application.
Christodorescu, M. et.al. [17] explained importance of static analysis in detecting malicious patterns of executable files. Looking at investigation point of view it is necessary to understand permissions used by the application.

As a part of the static analysis the emphasis was given on permissions required by the sample applications. Permissions is one of the important security implementation of android and it allows a user to understand which resources application wants to access. Many researchers including Felt, A. et.al [18], Kelley, P. G. et. al. [19], Sarma, B. P. et. al. [20], Wang, Y. et. al. [21] and many more have published their work on android permissions.

Permissions of all 10 samples were analyzed and results are shown in following figure:

![Permission Analysis](image1)

Above chart clearly indicates that most of the content hiding applications require access to ACCESS_NETWORK_STATE, INTERNET and WRITE_EXTERNAL_STORAGE. These permissions are required mainly for Internet access and write operations on external storage, which are basic functions a content hiding application does. The WRITE_EXTERNAL_STORAGE permission also indicates that the possibilities are there that application stores files to be hidden in the external storage. Permission to access Internet can be used to show advertisements, but it also shows possibilities, that the application may be storing some information on the cloud or server.

**B. Encryption**

Encryption is one of the key components used by content hiding applications. While investigating a phone loaded with any content hiding application, the investigator must confirm whether the application has used any encryption algorithm to encrypt data for hiding it from other users. If it does have encrypted the files then it becomes mandatory to use necessary encryption breaking (decryption) techniques for the retrieval of information. If algorithm used for encryption and keys are stored on the device then it may become very easy for investigators to retrieve the information.

But, if application writer has used any custom algorithm or the keys are stored on any cloud or server then things would become worse for the investigator.

An analysis of the sample applications was done and the results found are shown below:

![Use of Encryption](image2)
The above chart indicates that 70% of the samples used encryption to hide the files. The use of encryption algorithm here varies from application to application. But, it has been observed that though applications use encryption, forensics tools like Cellebrite UFED 4 PC are able to recover majority of the original files. This is an indication that these content hiding applications are not 100% anti-forensic applications as they are not wiping of files which they encrypt.

However, further research can be done in continuation to find out possibilities of decrypting files, this would help the investigators in case if the original files are erased intentionally.

C. Data Recovery

Though recovery of the data hidden by content hiding applications is directly dependent on whether the application has used any encryption mechanism or not, this section mainly discusses capability of automated analysis tools like UFED 4 PC in recovering data from the device.

5 images and 5 video clips were stored on the test device for the experiment. The sample content hiding application was then used to hide these files. Sufficient credentials were given to the application itself so other users cannot see these files.

Dump of the device was taken using Cellebrite UFED 4 PC and then it was analyzed by Cellebrite UFED Physical Analyzer.

With no surprise the results were in the favor of forensic investigators, data locked by the application was available for analysis using the results displayed by physical analyzer. The notable thing here is that the phone used for experiment was rooted and which was main reason it was possible to perform physical acquisition. In case if the phone under investigation is not rooted and rooting is not permitted or possible then the investigator may need to rely on logical acquisition and other manual methods.

Another important observation was location of the hidden data, all applications used external storage media to store / hide files while 2 applications had option to synchronize with cloud for hiding data. The interesting thing here is possibilities of synchronizing data on cloud, if user has done that, then it may become complex situation but not impossible as all the IP addresses and URLs can be recovered from the analysis. But, if the data is stored on external storage device, then irrespective of whether the phone is rooted or not, the information from storage media can easily be accessed and analyzed.

D. Application Lock Bypass

Apart from hiding content, these applications also offer a feature to restrict access to other applications. This is very useful and handy when the mobile is shared among multiple users. In general, users prefer to lock applications like WhatsApp, Viber, Internet Browsers, Movie Players, Galleries, etc. These applications themselves contain crucial information as their data and logs can reveal important information related to user's activities on the device. Some applications support self locking feature, where user requires pin to access the content hiding application itself.

In this section, I tried to understand how these applications manage passwords, pins and patterns used for restricting access to the other applications on the device. The forensic interest is to make it possible to bypass these locks and access the applications to know more about the user.

It has been observed during the experiment that the applications were storing password / pin / pattern in an sqlite db with no encryption. The db was accessible in all cases and it was possible to view it. This could be one of the important vulnerability of these applications. The obvious reason is as the developers are not looking for very secure application, they might not have considered to encrypt the database.

VI. CONCLUSION

Content hiding applications can become an obstacle in forensic investigation, if they are not understood and analyzed properly. The work published in this paper will help forensic investigators in handling devices loaded with such applications. Even if the automated tools fail in retrieving information, the points discussed in this paper may help an investigator in retrieving content and applications hidden/restricted by those privacy applications.

REFERENCES

© www.ijarcse.com, All Rights Reserved


[22] Cellebrite UFED 4 PC, http://www.cellebrite.com/Mobile-Forensics/Products/ufed-4pc