On the Availability of Anti-Forensic Tools for Smartphones

Ioana Sporea *ioana.sporea@port.ac.uk*
School of Computing
University of Portsmouth
Portsmouth PO1 3HE, United Kingdom

Benjamin Aziz *benjamin.aziz@port.ac.uk*
School of Computing
University of Portsmouth
Portsmouth PO1 3HE, United Kingdom

Zak McIntyre *zak.mcintyre@myport.ac.uk*
School of Computing
University of Portsmouth
Portsmouth PO1 3HE, United Kingdom

Abstract

The existence of anti-forensic tools in the context of computing systems is one of the main challenges for forensics investigators in achieving reliable evidence recovery and consequently uncovering crime facts. This is in particular more challenging in emerging smartphone technologies, since data is of highly mobile and volatile nature. In the current paper, we present a brief study of several anti-forensic applications available for smartphones. The applications are ready to use, most of them free, and require no expert technical knowledge. Moreover, these have been proved to be very effective when tested with two commercial forensic tools.

Keywords: Mobile computing, anti-forensics, cryptography, steganography.

1. INTRODUCTION

Mobile devices such as mobile phones and smartphones have emerged as an important part of people personal life. Smartphones, in particular, with increasing storage capacity and computing capabilities, provide a compact mobile computer, and thus, can contain information about call histories and contact lists, but also web history, e-mails, passwords, media files, and credit card numbers.

As a consequence, smartphones have outsold PCs (including pads) for the first time in 2011 [1]. With their extensive functionality, mobile devices can thus provide the richest source of civil and criminal evidence. Mobile forensics has become an important research area, providing the means of extracting critical information to investigators. However, the ever-changing technologies and the lack of standardization means that mobile forensics present some challenges. These will be discussed in more detail in the following section.

Because the field of mobile forensics is relatively new, there is even less research regarding anti-forensics, the process of compromising digital evidence. In this paper, we will focus on testing existing anti-forensics tools for smartphones and their effectiveness against commercial forensic applications. To this extent, two platforms have been used, Android and Apple iOS, and a series of freely available anti-forensic approaches. According to [2], Android and iOS have been in the top of the smartphones market share in 2011 by operating system.

The rest of the paper is organized as follows: the following section contains a short description of most recent advances in the areas of mobile forensics and anti-forensics; a description of the experiments conducted follows and the paper concludes with a short summary.

2. BACKGROUND

Digital forensics refers to the process of digital data acquisition, analysis of data and the extraction of evidence, preservation and presentation of evidence [3]. In the early days of digital forensics, as there were relatively few file formats and operating systems and storage devices with standard interfaces, forensic tools saw a golden age in the late 90s and early 2000s [4]. However, the development and propagation of a multitude of file formats and operating systems, the ever growing storage capacities as well as the use of encryption meant that digital forensics is now more challenging than before [4]. This is especially true for mobile device forensics, as there are thousands of mobile phones models, a lot of them with their own "standard" connectors and chargers, various operating systems (Apple's iOS, Android, Research in Motion's BlackBerry, Microsoft's Windows Mobile, Nokia's Symbian) as well as the now increasing use of embedded flash storage which cannot be easily removed or imaged.

The large number of operating systems, including low-end phones using legacy operating systems, and the fact that these are updated regularly means that mobile forensic tools must also be updated regularly [4]. Moreover, due to the fast technological advances, most people replace their cell phone every two years and some even annually [5].

Although the same forensic principles that apply to computers also apply to mobile devices, the latter involves additional constrains and challenges. Because of the nature of mobile phones, the data is constantly changing and therefore is impossible to obtain a bit-wise copy of the device's memory [6]. Moreover, existing data might be overwritten through wireless network communication [7]. On the other hand, removing the battery may prevent the device communication with the outside world and stop the data from modifications, but may also activate security measures, such as lock codes and encryption, which may restrain further access to the device.

From the access to the mobile device's data point of view, there can be two methods of acquiring data from mobile phones. If the device is powered on, the device must be isolated from networks to avoid the content being altered or even remotely erased and then investigated. This is called an online forensic analysis. If the device is turned off, the analysis of the mobile device is offline [7].

Digital anti-forensics is defined as any attempt of compromising or destroying digital evidence [8] according to the two forensic analysis methods. There is a wide range of anti-forensic techniques, divided into four categories: destroying data, hiding data, manipulating data, and preventing the creation of evidence [8]. Evidence destruction involves making the data unusable or inaccessible to the investigation process. Hiding evidence involves making the data less visible to the investigator. Data can be manipulated by creating a "faked" version with the purpose of appearing to be something else. By eliminating the source of evidence, there is no evidence created [8].

Anti-forensic tools for smartphones, Android phones in particular, have been studied before in order to test their effectiveness [9, 10, 11]. In Distefano et al. [9] an anti-forensic application has been created which makes use of the Android operating system functionality. As such, when installing an Android application, a private folder is created which is inaccessible to any other applications. When such application is uninstalled, the associated folder is also removed. The authors tested whether it is possible to hide data using this private folder mechanism. They used Nandroid, a backup and restore tool, and mobile memory acquisition tool to retrieve data that was logically removed. Although these tools were unable to recover the deleted data, their anti-forensic application was not tested with a specialized forensic tool capable of physical acquisition.

Anti-forensic approaches to data deletion and manipulation have also been investigated in [10, 11]. The authors created their own anti-forensic application which proved to be very effective in compromising the availability of data even when commercial forensic tools were used to retrieve the data.

3. EXPERIMENTS

The current paper presents available commercial anti-forensic tools for smartphones along with studies that reflect how robust and effective are against two commercial forensic applications. The applications were tested on two devices, HTC Desire HD with Android and iPhone 3G with iOS. In order to test how effective the anti-forensic applications are, both devices are tested with two commercial forensic tools, Paraben Device Seizure [12] and Oxygen Forensic Suite [13].

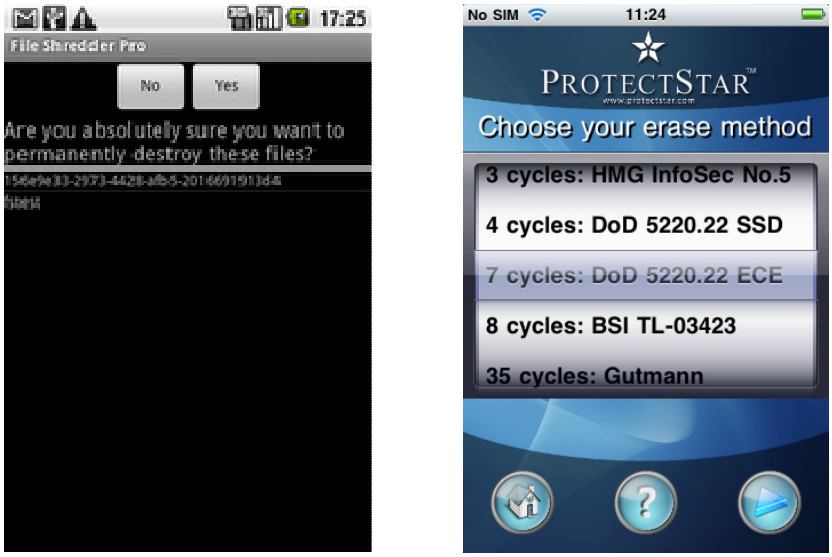
Paraben Device Seizure [12] is a forensic acquisition tool for mobile devices that offers both logical and physical support. In the experiments described in the current paper only logical acquisition was used. Device Seizure offers support for more than 4000 mobile devices, with features which include Google Earth integration, deleted data recovery, hex and text data viewers, exporting of acquired data to a PC.

The Oxygen Forensic Suite [13] is a forensic software suite for mobile devices, which offers strong support especially for smartphones, including logical acquisition of data not accessible to other software products.

In the following we will describe each anti-forensic application along with the results obtained with the two forensic tools.

2.1 File Shredding

File shredding is a popular form of data destruction, where the evidence is rendered unrecoverable after the application of the shredding program. One example is File Shredder [14], an application designed to permanently remove files on mobile devices. The selected files are destroyed by overwriting them with random data. The application was tested on the Android platform. Once the permanent deletion of selected files is completed, neither Device Seizure nor Oxygen Forensic Suite could detect any traces of the deleted files. Figure 1a shows the screen of the File Shredder application on the Android device.



a b

FIGURE 1: (a) FileShredder screen on Android. (b) iShredder screen on iPhone.

File Shredder was used to shred 5 testing files. A range of popular file types where chosen to simulate real life data use, including .pdf, .jpg, .mp3, .docx and 3pg.

ProtectStar iShreder Pro [15] is another such application for iOS platforms. The tool is able to permanently overwrite all free storage space or delete individual files using the U.S. Department of Defense's (DoD's) standards [16] as well as other standards for secure erasure. Again, after

selecting the files to be deleted and the method of overwriting, once the procedure is completed, both forensic tools were unable to find the files. The testing files include three types; namely .jpg, .png and .cvs. With this application, however, it is the user responsible to select all files associated with the unwanted file, such as thumbnail or cache files. Figure 1b shows the screen of iShredder on the iPhone.

2.2 Encryption

Cryptography is the process of hiding information for secure communication in the presence of third parties. LUKS Manager [17] offers encryption to virtual folders on Android devices.

FIGURE 2: LUKS Manager Screen.

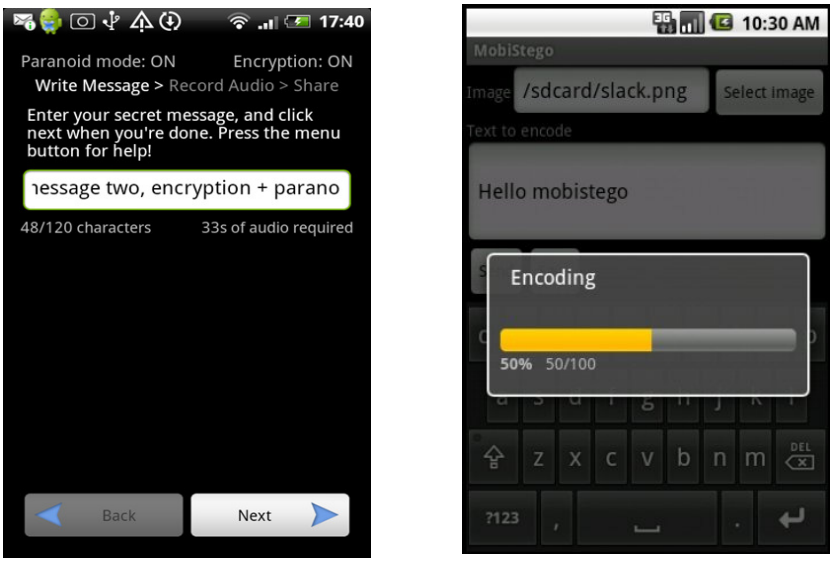
The virtual folder can be dynamically mounted, unmounted, created and deleted as required. After creating and mounting a virtual volume, the forensic tools were used to test the detection and encryption method. Both applications were able to detect the volume created and the encrypted data. The use of LUKS Manager and the encryption method used can also be detected in the file header. However, the contents of files stored within the encrypted volume remain unknown. Figure 2 shows the LUKS Manager with the available encryption methods.

2.3 Steganography

Steganography is the process of hiding digital information inside another carrier file such as media files, document files or executable files. Unlike plain encryption, which can be easily detected, steganography protects both the message and the communicating parties. Media files, such as images, audio and video files, are preferred for this type of encryption because of their large size.

StegDroid [18] offers the option of embedding a secret text message into an audio recording for Android devices. By encrypting the message, the recipient must use the key to read the hidden message. As such, a 60 characters message requires 33 seconds of audio recording. Neither Device Seizure nor Oxygen Forensic Suite was able to detect the hidden message, nor the use of StegDroid. Figure 3a shows the StegDroid screen setting a message using encryption.

MobiStego [19] is another steganography application for the Android platform. The application encodes text messages into an image file. After using the application, again, the forensic tools were unable to find any traces of the hidden message or the use of MobiStego on the image file. Figure 3b shows the MobiStego screen encoding a message.



a b

FIGURE 3: (a) StegDroid screen. (b) MobiStego screen.

2.4 Location Information

Smart phones can provide the richest source of information about the location of the user through the use of media files, social networks and similar applications. Fake Location is an application for iOS platforms that allows the user to set a fake location for desired applications. Fake Location has been tested with Facebook, Google Maps and image Geo positioning tags. The new fake location can be easily set using Google maps. For the first test, a fake location is set using the anti-forensic application; as such status updates on Facebook now show the fake location.

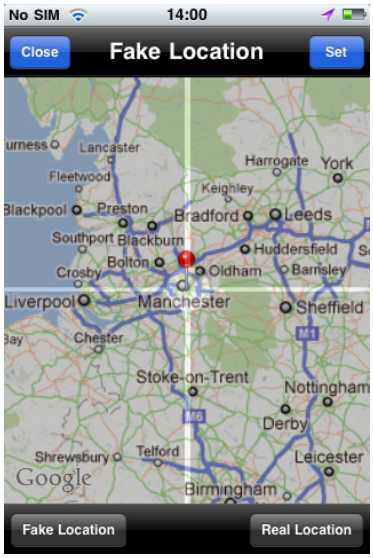


FIGURE 4: Fake Location screen.

Neither Device Seizure nor Oxygen Forensic suite detected the counterfeiting of location information for the social network or Google Maps. In the case of images created with Fake Location, the Geo positioning tags were left empty. Figure 4 shows the screen setting a fake location with Google Maps.

4. SUMMARY

Table 1 shows a summary of the anti-forensic techniques tested on the two platforms classified by their method of counterfeiting digital evidence. While the Android market offers a wide variety of free anti-forensic applications easy to use and very effective, for iOS platforms there is a limited choice and only a few of them are free.

Application	Platform	Anti-forensic Technique	Classification
File Shredder	Android	File Wiping	Destroying Data
iShredder	iOS	File Wiping	Destroying Data
LUKS Manager	Android	Encryption	Hiding Data
StegDroid	Android	Steganography	Hiding Data
MobiStego	Android	Steganography	Hiding Data
FakeLocation	iOS	Spoofing	Counterfeiting Data

TABLE 1: Summary of anti-forensic applications tested on smartphones.

5. CONCLUSION

In [9,10,11] the authors present ways of using anti-forensics techniques on Android devices, these requires technical knowledge of the smartphone's operating system. In this paper, we present several anti-forensic applications for smartphones, for removing, hiding and counterfeiting data. These applications require no technical expertise and most of them are free. The experiments show that these applications are very robust and effective when tested with commercial forensic tools. The results presented here confirm that mobile forensics is a very dynamic field mainly due to the very fast technological advances and the large number of mobile devices and their operating systems. We have shown how easy is to manipulate and destroy information on smartphones which at the moment offers the richest source of evidence.

The current paper presents a systematic study into anti-forensic methods for smartphones. The results show the wide range of methods available to counterfeit digital evidence. Thus, mobile devices can be used by sexual predators to contact victims, by terrorists for coordination, or it can be used to smuggle contraband across borders and steal credit card information [7]. The existence of the presented anti-forensic applications makes it easier for criminals to manipulate or destroy essential digital evidence stored on mobile devices. Although a relatively new research field, mobile anti-forensics reveals the short comings of and challenges of mobile forensics and the implications it has on acquiring digital evidence.

Future work will focus on the development of a decision support environment to aid forensic investigators in dealing with anti-forensic techniques within mobile platforms such as those studied in this paper. Another possible approach would be to develop a knowledge base of the various anti-forensic effects resulting from the application of such tools and the suggested forensic countermeasures that could prevent evidence from being lost or destroyed.

6. REFERENCES

[1.] Canalys Press Release. [Online] http://www.canalys.com/newsroom/smart-phones-overtake-client-pcs-2011 (Accessed 30 August 2012)

[2.] Gartner press release (2011) - Gartner Says Sales of Mobile Devices Grew 5.6 Percent in Third Quarter of 2011; Smartphone Sales Increased 42 Percent [Online] http://www.gartner.com/it/page.jsp?id=1848514 (Accessed 17 September 2012)

[3.] Carrier, B. (2002), 'Defining digital forensic examination and analysis tools', International Journal of Digital Evidence, Vol 1, pp 1-10

[4.] Garfinkel, S. L. (2010), 'Digital forensic research: The next 10 years', in Proceedings of the Tenth Annual DFRWS Conference, pp S64–S73

[5.] Forensic Focus - Challenges of Smart Phone Forensics [Online] http://www.forensicfocus.com/challenges-of-smart-phone-forensics (Accessed 30 August 2012)

[6.] Ahmed, R. and Dharaskar R. V. (2009), 'Mobile Forensics: the roadblocks ahead, proposed solution using Protocol Filtering and SIM programming', International Journal of Computer Science and Applications, Vol. 2(2) pp. 109-116

[7.] Casey, E. And Turnbull, B. (2011) 'Digital evidence on mobile devices', in Casey, E. (Eds.) Digital Evidence and Computer Crime, Academic Press

[8.] Harris, R. (2006), 'Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem', The International Journal of Digital Forensics & Incident Response, Vol 3, pp 44-49

[9.] Distefano, A., Me, G., & Pace, F. (2010, August). Android anti-forensics through a local paradigm. Digital Investigation, 7(Suppl.), pp 83-94

[10] Azadegan, S., Yu, W., Liu, H., Sistani, M., Acharya, S. (2012), 'Novel Anti-forensics Approaches for Smart Phones', in Proceedings of 45th Hawaii International Conference on System Science (HICSS), pp 5424 – 5431

[11] Liu, H., Azadegan, S., Yu, W., Acharya, S. and Sistani, A., (2012), 'Are We Relying Too Much on Forensics Tools?', in Lee, R. (Eds.) Software Engineering Research,Management and Applications 2011, pp 145-156

[12.] Paraben (2012) - Paraben's Device Seizure 5.0 Release Notes [Online] http://www.paraben.com/downloads/ds50.pdf (Accessed 17 September 2012)

[13.] Oxygen (2012) - Oxygen Forensic Suite [Online] http://www.oxygen-forensic.com/en/ (Accessed 17 September 2012)

[14.] File Shredder (2012) - https://play.google.com/store/apps/details?id=net.fizzl.fileshredder&hl=en (Accessed 28 September 2012)

[15.] ProtectStar iShreder Pro (2012) - http://itunes.apple.com/us/app/protectstar-ishredder-pro/id441224022?mt=8 (Accessed 28 September 2012)

[16.] NISP - 'DoD 5220.22-M National Industrial Security Program Operating Manual' [Online] http://transition.usaid.gov/policy/ads/500/d522022m.pdf (Accessed 14 September 2012)

[17.] LUKS Manager (2012) - https://play.google.com/store/apps/details?id=com.nemesis2.luksmanager (Accessed 28 September 2012)

[18.] StegDroid (2012) - https://play.google.com/store/apps/details?id=uk.ac.cam.tfmw2.stegdroid&hl=en (Accessed 28 September 2012)

[19.] MobiStego (2012) - https://play.google.com/store/apps/details?id=it.mobistego&hl=en (Access 28 September 2012)