The Forensic Investigation of Android Private Browsing Sessions using Orweb

Nedaa Al Barghouthy, Andrew Marrington, Ibrahim Baggili
Advanced Cyber Forensics Research Laboratory, College of Technological Innovation
Zayed University
Dubai, United Arab Emirates
m80001432@zu.ac.ae, andrew.marrington@zu.ac.ae, ibrahim.baggili@zu.ac.ae

Abstract— ***The continued increase in the usage of Small Scale Digital Devices (SSDDs) to browse the web has made mobile devices a rich potential for digital evidence. Issues may arise when suspects attempt to hide their browsing habits using applications like Orweb - which intends to anonymize network traffic as well as ensure that no browsing history is saved on the device. In this work, the researchers conducted experiments to examine if digital evidence could be reconstructed when the Orweb browser is used as a tool to hide web browsing activates on an Android smartphone. Examinations were performed on both a non-rooted and a rooted Samsung Galaxy S2 smartphone running Android 2.3.3. The results show that without rooting the device, no private web browsing traces through Orweb were found. However, after rooting the device, the researchers were able to locate Orweb browser history, and important corroborative digital evidence was found.***

Keywords— Orweb; Tor; digital forensics; Android forensics; private web browsing. *(key words)*

I. INTRODUCTION

Small Scale Digital Device forensic (SSDD) evidence is increasingly becoming important. It is difficult to steadily assess the error rates and accuracy of SSDD forensic tools since they are continuously revamped in order to keep up with the technological advancements in SSDDs and their operating systems [1].

Coupled with the lack of tools and research in SSDD forensics, many mobile anonymity applications are making their way to users such as the Orweb browser application that can provide network anonymity while browsing the Internet since it uses Onion Routing.

Briefly, Onion Routing is a distributed overlay network designed to anonymize TCP-based applications like web browsing, secure shell, and instant messaging. Connected clients choose a network path to build a circuit where each connected client becomes a node called an Onion Router (OR). Each OR in the chosen path knows its predecessor and successor but does not know any other ORs in the circuit [2].

Besides its network anonymity, because of its use of Onion Routing, there are claims that Orweb keeps no local history of the websites that are visited [3]. As the use of such applications continues to grow, they will pose ongoing challenges for forensic investigators since they help conceal corroborative digital evidence. This drives the need to examine Orweb related digital evidence that can be acquired from SSDDs. Further, from a privacy perspective, users install and use Orweb with an expectation of anonymity – they believe that the use of this browser will conceal their web activity. The claimed privacy benefits of this browser should be tested.

The aim of this research was to experimentally investigate forensic artifacts that can be recovered from the Android Orweb browser application on a Samsung Galaxy S2 smartphone on both a rooted and non-rooted device. The purpose of recovering those artifacts is to reconstruct a suspect's private browsing session as part of a criminal investigation. The researchers aimed to answer the following questions:

- Is it possible to locate evidence related to the Orweb browser on a non-rooted Samsung S2 Android device?
- Is it possible to locate evidence related to the Orweb browser on a rooted Samsung S2 Android device?
- Is it possible for forensic investigators to locate evidence related to the visited websites when the Orweb browser is used to anonymize network traffic?
- Is it possible for forensic investigators to find evidence related to Facebook instant messaging when used within the Orweb browser?

II. CONTRIBUTION

To the authors' knowledge, this is the first research that investigates the potential of extracting digital evidence from Android devices when Orweb is used to anonymize web traffic, therefore, this research aims to fill a gap in the literature. Furthermore, this work will help digital forensic practitioners in investigating cases where Orweb was used as a web browser on Android devices. The approach demonstrated is straight-forward and easily adapted to the investigation of other private browsers similar to Orweb. The results presented in this paper demonstrate the need for developers of mobile private web browsers like Orweb to be more attentive about artifacts of private browsing sessions left behind on the mobile device, so that their retrieval is far less straight forward.

III. LITERATURE REVIEW

A. Related Work

With respect to Android forensics, a number of studies and books have been published. Most notably, one of the first

published academic research studies that discussed Android forensics examined rooting the device and creating a forensic image of the device [4]. It would also be important to recognize Andrew Hoog's work in his book "Android Forensics: Investigation, Analysis and Mobile Security for Google Android" [5]. In 2011, a paper was published discussing a general methodology for the collection and examination of evidence from Android devices [6]. To discuss all the methodological literature on Android forensics is beyond this paper's scope, as the scope and purpose of this research was to examine Orweb artifacts on Android devices.

Research has been conducted on digital evidence related to Android forensics. A recent paper that was presented in the Digital Forensics Research Workshop examined forensic evidence that could be extracted from social networking applications on mobile devices including Android, Blackberry and iPhone [7]. Other research focused on the reconstruction and examination of facebook instant messaging from a computer system running a windows operating system across different web browsers [8]. Researchers have also studied the forensics of volatile web-enabled instant messaging services [9]. Lastly, researchers have also examined digital evidence that could be reconstructed from iPhones with respect to chat messages sent over AIM, Google Talk and Yahoo! [10].

Even though studies were conducted on the forensic examination of application artifacts on various mobile devices and computers, to date, researchers have not examined the potential impact of Orweb in concealing digital evidence found on mobile devices.

B. *Android Rooting*

Rooting an Android device may be perceived negatively - just like 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 [4]. It is critical to note that one should take extreme caution and prior testing before rooting a device in case of a real investigation.

There are many ways and applications in which an Android device can be rooted. A simple search on the World Wide Web yields numerous results on this topic. To explain all the ways in which devices can be rooted is beyond this paper's scope. However, the method used to root the device in this experimental work is outlined in the methodology section.

Once a device is rooted however, a popular application that can be used to view files on Android is the Root Explorer. In order for Root Explorer to work, the device has to be rooted. Root Explorer is a file system manager for root administrator users that provides access to the device's system files. Features include SQLite database viewer, Text Editor, the creation and extraction of zip or tar/gzip files, extraction of rar archives, multi-selection, script execution, searching, remounting, permission setting, bookmarking, file sending (via email, bluetooth etc) and many other functionalities [11].

IV. RESEARCH METHODOLOGY

In order to address the research questions mentioned above, an experiment was designed. In this experiment, a popular Android smartphone was used to web browse through the Orweb browser. The device was subsequently examined twice, once prior to rooting, and once afterwards. In each examination the researchers searched for evidence of the user's browsing activity. The experiment is described in detail in this section.

A. *Instruments*

The following instruments were used in our experiment:

- Laptop PC running Windows XP SP3 as the forensics workstation
- Samsung Galaxy S2 smartphone running Android 2.3.3
- Orweb v2.28 Android app (includes Orbot)
- Titanium Backup v5.5.2.1 Android app
- Samsung Kies v2, Odin3 and S2 Root software for rooting the smartphone
- SQLite Database Browser v1.2
- Root Explorer v2.19, to be installed on the smartphone
- CF-Root kernel, to be installed on the smartphone
- Micro USB cable to connect the forensics workstation to the smartphone

B. *Procedures*

The experiment consisted of an Orweb browsing session on the Android smartphone followed by two attempts at forensic analysis – one without rooting and one with rooting the device. The steps involved in the experiment are described in this section.

1) *Usage Scenario*

The Orweb browser was installed on the (non-rooted) Samsung Galaxy S2 mobile device. We then performed the following steps which comprise our simulated "suspicious usage" which will be subsequently investigated, all using the Orweb browser:

- We visited the Facebook website (www.facebook.com – not the Android app).
- We logged into Facebook website as "Butti Hamad" – a user profile created specifically for this experiment.
- We started a Facebook Message instant messaging conversation with a Facebook Friend, the user "Hind Rashid" (also a user profile created specifically for this experiment).
- As "Butti Hamad" we sent an image photo file to "Hind Rashid".

Although the user profiles and image file used in our experiment were innocuous, this simple scenario was designed to be deliberately similar, in terms of the actions performed, to a cyber-bullying or harassment scenario.

2) *Examination of the non-Rooted Device*

Two examinations were attempted on the non-rooted Samsung Galaxy S2 device. First, we attempted a logical

acquisition via a back-up utility, similar to the approach employed by Bader and Baggili for the iPhone [12]. To this end, we employed the Titanium Backup application, but were unable to perform a backup as we didn't have root permission (required by the app). Next, we performed a live examination of the device using the Android File Explorer app, but were only able to access the user data files and could identify no evidence of the simulated suspicious browsing activity.

3) Rooting the Android Samsung Galaxy S2 device

The detailed process for rooting Android devices is well-documented on the World Wide Web. We briefly summarize the steps followed for our Samsung Galaxy S2 device here:

- Installed Samsung Kies, Odin3, and S2 Root on the forensic workstation.
- Enabled USB debugging on the device.
- Powered down the device.
- Powered on the device and enabled downloading mode (holding volume down, power switch, and menu switch on the Samsung Galaxy S2).
- Connected the device to the forensic workstation via the USB cable.
- Ran Odin3 on the forensic workstation, loaded the new kernel onto the device, and rebooted.
- Applied the rootkit when the device restarted through the forensic workstation.

Once the device was rooted, we attempted our examination again.

4) Examination of the Rooted Device

After rooting the device, we attempted to perform a logical acquisition of the Android device using the Titanium Backup application. The backup was then copied from the SD card in the device to the forensic workstation for examination. Using SQLite Database Viewer, we examined the contents of the backup, manually searching for artifacts of the browsing activity under investigation. We corroborated our findings with a live examination of the device, by viewing the contents of the database files on the android device. Our findings with both techniques are discussed below.

V. RESULTS

A. Non-Rooted Device

As we were unable to obtain a back-up without rooting the device, we were unable to conduct a logical acquisition of the non-rooted device, and were unable to examine it on the forensic workstation. Our live examination yielded no additional results. Using the Android File Explorer utility on an non-rooted Android Samsung Galaxy S2 mobile device, we were unable to locate any artifacts of the Orweb browsing session. Without rooting the device, the device user lacks sufficient privilege to access anything more than the default user directory "/mount/sdcard" on the device. This directory did not contain any information related to the Orweb browser in our experiment. On an un-rooted device, then, we were unable to retrieve any information relating to the simulated suspicious browsing activity.

B. Rooted Device

In order to perform a logical acquisition through the Titanium Backup utility or to access the contents of the Orweb browser database in a live examination, it was necessary to root the device. We were able to access the Orweb browser's application files (located in "/data/data/info.guardianproject.browser" – see Fig. 1) both through examining the backup on the forensic workstation, and through the Root Explorer app on the Android device. Using the SQLite Database Viewer, we were able to examine the contents of these files and find some traces of the web browsing activity under investigation. Our findings are summarized in Table 1.

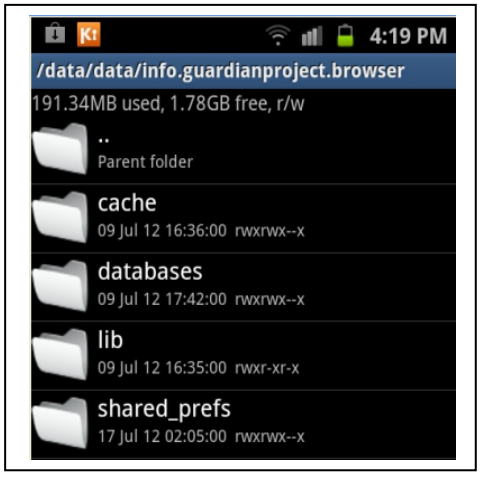

Figure 1. The Orweb application files as seen in Root Explorer on the Android device

TABLE I. ORWEB TOR BROWSER ARTIFACTS RETRIEVED FROM ROOTED GALAXY S2 MOBILE DEVICE

Evidence Description	Contents	Relative path under Orweb directory's "databases" subdirectory
History of Visited URL	Records of the URLs: http://m.facebook.com/ http://m.facebook.com/login.php http://m.facebook.com/login/identify http://m.facebook.com/home.php	webview.db
Chat participant email ID	Email address: engineering989@gmail.com	webview.db/formdata
Chat date and time stamp	Mon, 09 Jul 2012 12:58:48 GMT	webview.db
URL of transferred file	%2Fmessages%2Fattachment%2F%3attach_id%3Dfce … (truncated)	webview.db
Encrypted or encoded conversation between "Butti Hamad" and "Hind Rashid"	Example message (several retrieved): 0N9SS9fwcqauCWffW.AWUL72tT_ujrnYDkFM9h0GED9eg	webview.db

Evidence Description	Contents	Relative path under Orweb directory's "databases" subdirectory
Facebook ID numbers for both accounts	100003379119959 100003400419055	webview.db

VI. FINDINGS AND DISCUSSION

In the previous section, data were analyzed and findings were presented addressing the major research questions in this work. The key finding of this experiment is that rooting the device allows an investigator to uncover a great deal more evidence than they can examining un-rooted devices, as we would expect. With respect to the Orweb browser, our results show that traces of browsing sessions can indeed be located on Android devices. This demonstrates that, despite the perceived privacy benefits of such browsers, a forensic investigator will be able to re-construct a significant proportion of one's secret activities online. Table 2 summarizes the findings of investigating the artifacts of Orweb Tor browser on rooted and non-rooted Android Samsung Galaxy S2 devices:

TABLE II. ORWEB TOR BROWSER ARTIFACTS ON ROOTED AND NON-ROOTED SAMSUNG GALAXY S2 MOBILE DEVICE

Orweb Tor browser Artifacts	Rooted Galaxy S2-Device	Non-Rooted Device
History of Visited URL	Yes	No
Facebook Login account and Password	Login name found only	None
Participants Facebook ID	Yes	No
Participants names	No	No
Participants Image URL	No	No
Participants Profile Image	No	No
Participants email ID	Yes	No
Conversation Text	Yes (encrypted)	No
Time and date of the conversation	Yes	No
File transferred between participants	Yes (only the path)	No

Although we were able to retrieve the Facebook login name on rooted device, we were not able to retrieve the password. In a real investigation into Facebook, this information could be obtained from Facebook by following the right legal processes to obtain or complain about content.

VII. CONCLUSION AND FUTURE WORK

As privacy-enhancing technologies increase in abundance and usage, users can visit web sites, send messages, and interact with applications without revealing their identity. This means that criminals may use private browsers such as the Orweb to take advantage of this anonymity on the web. In this research, examinations were performed on both an un-rooted device and a rooted Android device. The results show that without rooting the device, no private web browsing traces through the Orweb web-browser were found. However, after rooting the device, the researchers were able to locate the Orweb browser history, and important corroborative digital evidence was found.

Future work can be conducted into the forensic reconstruction of Orweb browser sessions on Android devices. Most particularly, similar experiments could be carried out using physical acquisition of the Android device, and using the Vidas technique [6], to compare the data recovered from each approach to the rooting-based approach described in this work.

There are clear lessons to be drawn for the developers of private web browsers like Orweb. It would not appear to be difficult to avoid leaving the artifacts of the browsing session described in this work through relatively minor modifications to the Orweb source code. The approach described in this paper is straight forward and well within the capabilities of most forensic investigators, or highly proficient Android users. Given the rapid pace of development in the field of small scale digital device forensics, it is important for developers of anonymisers like Orbot and private browsers like Orweb to consider not just the privacy of the user against network traffic analysis, but also against forensic analysis of the device.

REFERENCES

[1] I. Baggili, R. Mislan, and M. Rogers, "Mobile Phone Forensics Tool Testing: A Database Driven Approach," *International Journal of Digital Evidence*, vol. 6, no. 2, 2007.

[2] R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The second-generation onion router," Washington D.C., 2004.

[3] The Guardian Project, "Orweb: Proxy+Privacy Browser," 2012. [Online]. Available: https://guardianproject.info/apps/orweb/. [Accessed: 30-Nov-2012].

[4] J. Lessard and G. C. Kessler, "Android Forensics: Simplifying Cell Phone Examinations," *Small Scale Digital Device Forensics Journal*, vol. 4, no. 1, 2010.

[5] A. Hoog, *Android Forensics: Investigation, Analysis and Mobile Security for Google Android*. Syngress, 2011, p. 432.

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

[7] N. Al Mutawa, I. Baggili, and A. Marrington, "Forensic analysis of social networking applications on mobile devices," *Digital Investigation*, vol. 9, pp. S24–S33, Aug. 2012.

[8] N. Al Mutawa, I. Al Awadhi, I. Baggili, and A. Marrington, "Forensic artifacts of Facebook's instant messaging service," in *Internet Technology and Secured Transactions (ICITST), 2011 International Conference for*, 2011, pp. 771–776.

[9] M. Kiley, S. Dankner, and M. Rogers, "Forensic Analysis of Volatile Instant Messaging," in *Advances in Digital Forensics IV*, vol. 285, Boston: Springer, 2008, pp. 129–138.

[10] M. I. Husain and R. Sridhar, "iForensics: Forensic Analysis of Instant Messaging on Smart Phones," vol. 31, Springer, 2010, pp. 9–18.

[11] "Root Explorer (File Manager)," 2012. [Online]. Available: https://play.google.com/store/apps/details?id=com.speedsoftware.rootexplorer&hl=en. [Accessed: 30-Nov-2012].

[12] M. Bader and I. Baggili, "iPhone 3GS Forensics: Logical analysis using Apple iTunes Backup Utility," *Small Scale Digital Device Forensics Journal*, vol. 4, no. 1, 2010.