1-1-2012

Forensic analysis of social networking applications on mobile devices

Noora Al Mutawa
Zayed University

Ibrahim Baggili
Zayed University

Andrew Marrington
Zayed University

Recommended Citation

Al Mutawa, Noora; Baggili, Ibrahim; and Marrington, Andrew, "Forensic analysis of social networking applications on mobile devices" (2012). *All Works*. 1706.
https://zuscholars.zu.ac.ae/works/1706

Digital Investigation 9 (2012) S24–S33

Contents lists available at SciVerse ScienceDirect

Digital Investigation

journal homepage: www.elsevier.com/locate/diin

Forensic analysis of social networking applications on mobile devices

Noora Al Mutawa, Ibrahim Baggili, Andrew Marrington*

Advanced Cyber Forensics Research Laboratory, Zayed University, PO Box 19282, Dubai, United Arab Emirates

Keywords:
Mobile device forensics
Social networking
iPhone
Android
Blackberry

ABSTRACT

The increased use of social networking applications on smartphones makes these devices a goldmine for forensic investigators. Potential evidence can be held on these devices and recovered with the right tools and examination methods. This paper focuses on conducting forensic analyses on three widely used social networking applications on smartphones: Facebook, Twitter, and MySpace. The tests were conducted on three popular smartphones: BlackBerrys, iPhones, and Android phones. The tests consisted of installing the social networking applications on each device, conducting common user activities through each application, acquiring a forensically sound logical image of each device, and performing manual forensic analysis on each acquired logical image. The forensic analyses were aimed at determining whether activities conducted through these applications were stored on the device's internal memory. If so, the extent, significance, and location of the data that could be found and retrieved from the logical image of each device were determined. The results show that no traces could be recovered from BlackBerry devices. However, iPhones and Android phones store a significant amount of valuable data that could be recovered and used by forensic investigators.

1. Introduction

The last several years have witnessed the rapid evolution of a new form of online communication known as social networking. By joining websites that offer these services, users can interact and socialize, share information and ideas, post comments and updates, participate in activities and events, upload files and photos, and engage in real-time instant messaging and conversations. These websites attract millions of people from all over the world. A study estimated that the number of unique users of online social networks worldwide was about 830 million at the end of 2009 (International Telecommunications Union, 2010).

Despite being primarily used to communicate and socialize with friends, the diverse and anonymous nature of social networking websites makes them highly vulnerable to cybercrimes. Phishers, fraudsters, child predators, and other cyber criminals can register to these services with fake identities, hiding their malicious intentions behind innocent-appearing profiles. Social networks also encourage the publication of personal data, such as age, gender, habits, whereabouts, and schedules. The wealth of personal information uploaded to these websites makes it possible for cyber criminals to manipulate this information to their advantage and use it to commit criminal acts. Other abusive activities that can be committed on these websites include uploading illegal or inappropriate material, defaming, and stalking (de Paula, 2009). The large number of criminal acts that can be performed through social networks raises the importance of digital forensics in this area. Electronic evidence retrieved from social networking activities on a suspect's machine can be of great assistance in investigating a criminal case by incriminating or proving the innocence of a suspect.

Besides accessing social networking sites via desktop computers and laptops, subscribers can use their smartphones to tap into these services. A survey conducted by Ruder Finn (a PR agency) showed that "91% of smartphone

* Corresponding author. Tel.: +971 4 402 1199; fax: +971 4 402 1017.
E-mail address: andrew.marrington@zu.ac.ae (A. Marrington).

1742-2876/$ – see front matter © 2012 A. Marrington, N. Al Mutawa & I. Baggili. Published by Elsevier Ltd. All rights reserved.
doi:10.1016/j.diin.2012.05.007

users go online to socialize compared to only 79% of traditional desktop users". It also showed that 43% of smartphone users use them to communicate with people on social networking sites (Finn, 2012). Approximately half of Facebook's users access Facebook through a mobile device, such as a smartphone or tablet. According to Facebook, these users are twice as active as users who do not access Facebook through a mobile device (Facebook, 2011). Given that millions of users access social networks through smartphones and that smartphones provide 24/7 access to these services, there is a high risk of the abuse of these services by users with malicious intentions. Therefore, when a forensic examination is performed on a suspect's smartphone, there might be a chance of finding evidence that supports criminal prosecution.

Forensic examination of smartphones is challenging. Smartphones are always active and are constantly updating data, which can cause faster loss of evidentiary data. Second, the operating systems (OS) of smartphones are generally closed source, with the notable exception of Linux-based smartphones, which makes creating custom tools to retrieve evidence a difficult task for forensic examiners. In addition, smartphone vendors tend to release OS updates very often, making it hard for forensic examiners to keep up with the examination methods and tools required to forensically examine each release. The variety of proprietary hardware of smartphones is another issue faced by forensic examiners (Al Zarouni, 2006).

This paper focuses on conducting forensic analyses on three widely used social networking applications on smartphones: Facebook, Twitter, and MySpace. The tests were conducted on three popular smartphones: BlackBerry Torch 9800, iPhone 4, and the Android-based Samsung Galaxy S, and consisted of installing the social networking applications on each device, conducting common user activities through each application, acquiring a forensically-sound logical image of each device, and performing a manual forensic analysis on each acquired image. The purpose of our analysis was to determine whether activities conducted through these applications were stored on the device's internal memory. If so, the amount, significance, and locations of data that could be found and retrieved from the logical image of each device were determined.

2. Related work

2.1. Mobile device forensics

Initial work in this field has focused on acquisition techniques and general forensic analyses of smart devices. In his paper, Burnette discussed the forensic examination of older versions of the BlackBerry and covered the hardware and software used for acquisition (Burnette, 2002). He also described several methods of examination, including the use of hex editors and emulators. Later research provided foundational concepts on forensic analyses of the new generations of smartphones (e.g., BlackBerry and iPhone). It outlined the technologies used, the handling procedures, and the common evidence storage locations for each device. The data that could be extracted from the internal memory of these devices included call logs, SMS, MMS, emails, webpage bookmarks, photos, videos, and calendar notes (Punja and Mislan, 2008).

Recent scientific research has focused on individual types of smartphones, investigating the methods that could be used to acquire and analyze the internal memory of the device and the data that could be extracted from each device. iPhone data could be acquired by either a physical or a logical method. The physical method requires jailbreaking the system, which causes a slight modification to the system's data (Kubasiak et al., 2009). However, the latest technique developed by Zdziarski acquires a physical-logical image of an iPhone without jailbreaking the phone (Zdziarski, 2010). It is considered the best forensic method for acquiring iPhone and has been evaluated by the National Institute of Standard and Technology (NIST) (National Institute of Standards and Technology, 2010). Similar to iPhones, Android-based smartphones can also be acquired using either a physical or a logical method. The physical technique consists of obtaining a dd image of the phone's memory and requires root access to the device (Lessard and Kessler, 2010). Vidas et al. discuss an acquisition methodology based on overwriting the "Recovery" partition on the Android device's SD card with specialized forensic acquisition software (Vidas et al., 2011).

2.2. Social networking forensic artifacts

Scientific research has also included the investigation of artifacts left by social networking sites on computer systems and tools that assist in the extraction of these artifacts. Zellers has examined the unique data tags created in different MySpace source-code pages and used these tags to create focused artifact keyword searches (Zellers, 2008). Other research discussed the process of recovering and reconstructing Facebook chat artifacts from a computer's hard disk (Al Mutawa et al., 2011).

Because many social networking applications are integrated into new smartphones, in cases involving social networks, forensic examiners may be able to find relevant evidence on a suspect's smartphone. A forensic examination of the iPhone 3GS (via a logical acquisition) showed that a database related to the Facebook application is stored on the phone's memory. The database stores data for each friend in the list, including their names, ID numbers, and phone number (Bader and Baggili, 2010). Two other directories related to the Twitter application were also found. These directories store information about Twitter account data, attachments sent with tweets, user names, and tweets with date and time values (Morrissey, 2010). A forensic examination of an Android phone's logical image showed that basic Facebook friend information is stored in the contacts database (contacts.db) as the device "synchronizes contact's Facebook status updates with the phone book" (Lessard and Kessler, 2010). It also showed that the device stores Twitter passwords and Twitter updates performed through the Twitter application in plain text (Lessard and Kessler, 2010). Forensic research papers on BlackBerry phones and Windows smartphones, however, did not mention finding or recovering any data related to the use of social networking applications.

Similar to computers, smartphones store data that can help determine how the device has been used or misused.

Therefore, activities performed through social networks applications may be stored on smartphones. However, previous research has been limited to the recovery of very basic information related to the use of social networking applications. It is clear that further experiments focusing on the recovery of artifacts related to the use of social networking applications are required to determine whether activities performed through these applications are stored and can be recovered from smartphones.

3. Methodology

The main purpose of this research is to determine whether activities performed through smartphone social networking applications are stored on the internal memory of these devices and whether these data can be recovered. These data can be of high evidentiary value, which can assist in the investigation of criminal, civil, or other types of cases. The goal of this study was achieved by conducting experiments on a number of smartphones. Manual forensic examinations and analyses were performed on three commonly used social networking applications on smartphones: Facebook, Twitter, and MySpace. The experiments were conducted on three popular smartphones: BlackBerrys, iPhones, and Android phones.

In a real investigation, law enforcement agencies may have access to data from the social networking providers. Depending on the nature of the investigation, jurisdictional issues and the degree to which the social networking provider is co-operative with law enforcement, the provider may prove to be a more convenient source of digital evidence about social networking use than the smartphone. However, investigation the smartphone has two-fold value. It is often useful to corroborate evidence from different sources, such as from the provider and then from the smartphone. Moreover, especially in an era of ubiquitous mobile Internet connections, many traditional telephony services (such as text messaging) are provided via social networking sites through their smartphone apps. It may be crucial to the reconstruction of a crime to know whether particular social networking activities (already reflected in data from the service provider) took place on a particular smartphone.

The experiments were conducted using forensically sound approaches and under forensically acceptable conditions to fulfill a crucial rule in digital forensics, which is to preserve the integrity of the original data and to prevent it from any contamination that would interfere with its acceptance in court. The test and examination procedure was derived from the Computer Forensics Tool Testing program guidelines established by the National Institute of Standards and Technology (NIST) to ensure the quality of the testing methods and the reliability and validity of the results (National Institute of Standards and Technology, 2001).

The research aimed to work with realistic data similar to that found in an actual investigation. In a real investigation, suspects may use different social networking applications on smartphones and conduct different activities through each of them. They may also use jailbroken iPhones or rooted Android devices. The experiments were designed accordingly.

3.1. Test environment and requirements

Prior to conducting the experiments, a forensic workstation was set up and configured. Once the forensic workstation was ready, it was isolated from the lab's network. The following is a list of the hardware and software used to conduct the experiment:

- Two Blackberry Torch 9800 phones (software version: 6.0 Bundle 862).
- Two iPhone 4 devices, 32GB (version 4.3.3 8J2).
- One Android phone (Samsung GT-i9000 Galaxy S – Firmware version 2.3.3).
- Facebook, Twitter, and MySpace applications for each tested phones.
- BlackBerry Desktop Software (version 6.1.0 B34).
- Apple iTunes Application (version 10.4.0.80).
- TextPad (version 4.5.2).
- Plist Editor for Windows (version 1.0.1).
- SQLite Database Browser (version 1.3).
- DCode (version 4.02a).
- EnCase (version 6.5).
- A software USB write-blocker (Thumbscrew).
- USB data cables.
- A Micro SD card.
- A Micro SD card reader.
- Odin3 (version 1.3), a tool to upload a root-kit to the Android device.
- MyBackup Rerware, LLC (version 2.7.7).

The configurations of the smartphones were not altered. Temporary storage cache sizes, for instance, were not modified from factory defaults. Changing the default cache size would likely affect the volume of recoverable digital evidence found on the smartphone.

3.2. Test procedure

The test procedure consisted of three stages: scenarios, logical acquisition, and analysis. The following sections describe each stage in details.

3.2.1. Scenarios

This stage involved conducting common user activities on social networking applications on the smartphones. The Facebook, Twitter, and MySpace applications were installed on each device if they were not already integrated with the device. These applications were chosen simply because of their availability as stand-alone applications for each platform. For the purpose of the experiments, fictional accounts with fictional users were created on each social networking website and were logged into and used through the smartphones' applications. For each device, a predefined set of activities were conducted using each application. The activities were chosen to represent common activities, such as uploading photos, posting comments, sending emails within the application, and chatting.

3.2.2. *Logical acquisition*

The second stage involved acquiring a logical image of the internal memory of each device. The acquisitions were performed in a controlled environment using forensically sound techniques to ensure the integrity of the acquired data and its potential admissibility in court. As is always the case with all logical acquisitions, there is the possibility that data remnants of inactive files may be missed in the course of such an acquisition. In computer forensics for example, a logical acquisition may miss data stored in slack space. The same issue exists with all logical acquisition techniques for smartphones.

As the tested phones had three different operating systems, specific tools and configurations were required to manually acquire a logical image of each device. Detailed methods of acquisition are presented later in the paper.

3.2.3. *Analysis*

The third stage involved performing forensic examinations to the acquired logical image of each device, to determine whether the activities conducted through these applications were stored on the device's internal memory. If so, the amount, location, and significance of the data that could be found and retrieved from the logical image of each device were determined. The examinations were conducted manually using a number of tools to view the acquired images, determine the unique headers or signatures in each structure, search for data related to the social networking applications, and determine how these data were stored on each device.

4. Implementation and analysis

The first stage of the experiment involved installing the social networking applications and conducting the predefined activities on each device. This stage was straightforward and general for all of the tested devices. For the two BlackBerry Torch phones, the Facebook, Twitter, and MySpace applications were already preinstalled by the manufacturer. For the two iPhones, Facebook (version 3.4.4), Twitter (version 3.3.5), and MySpace (version 2.0.7) were downloaded from the App Store and installed on the devices. For the Android phone, Facebook (version 1.6.3), Twitter (version 2.1.2), and MySpaceDroid (version 1.0.7) were downloaded from the Android Market and installed on the devices. All of the tested applications were created by the official social networking companies except for MySpaceDroid (the official MySpace application could not be installed on the tested Android phone).

Once the applications were installed on the devices, the predefined activities were conducted on each device. The activities represented common user activities and activities that would of interest to the forensic examiner. These activities included uploading photos, posting comments, sending emails, and chatting. Table 1 represents all activities that have been performed on each application of each tested device.

Table 1
Activities performed on each application of each tested device.

Application	Performed activities	Comments
Facebook	Login with user name: infected.mushroom2011@hotmail.com and password: mushroom77	–
	Post in news feed	–
	Upload photos + captions	–
	Send email messages	–
	Post on friend's wall	–
	Instant messaging (chat)	–
	View profiles of friends	–
Twitter	Login with user name: infected.mushroom2011@hotmail.com and password: mushroom246	–
	Follow people	–
	Post tweets	–
	Upload photos	–
MySpace	Login with user name: infected.mushroom2011@hotmail.com and password: mushroom888	–
	Upload pictures	Did not function for Android
	Add friends	–
	Change status	–
	Check emails	–
	Send emails	–
	Post comments	–
	View profiles	–
	Instant messaging (chat)	Did not function for Android

Similar activities were conducted on each tested phone; however, unique data were used on each application for each phone to reduce redundant data and simplify the analysis phase. After conducting the social networking activities on the tested phones, a logical image of the internal memory of each device was acquired and analyzed for evidence of the conducted activities. Table 2 shows a list of keywords used to search for traces of each social networking application's usage. The following sections describe the procedures used for the acquisition and analysis of each tested smartphone.

4.1. *BlackBerry forensic examination*

This section describes the process of the logical acquisition and forensic analysis of the two tested BlackBerry phones. The processes for both phones were identical, and the analysis results were similar.

Table 2
Keywords for searching for social networking activity.

Application	Keywords
All	infected.mushroom2011@hotmail.com
MySpace	mushroom888, infected mushroom, gloomy, hello myspace
Twitter	mushroom246, ForensicFocus, Jzdiarski, jonathan zdziarski, Sctan, Mushrooom2011, “Amazing how time runs fast!!”, “so hot and humid!!”
Facebook	mushroom77, “craving for shake shack!!”, “hello cheza”, “lets go to the mall”, “hellooooo”, “hey im here”, “what time shall we go?”, “9pm?”, “ok see u later”, Infected, Cheza,

4.1.1. Logical acquisition

The logical acquisition of the BlackBerry phones was performed using BlackBerry Desktop Software (BDS). BDS is a management application that is freely available on the BlackBerry official website. It is designed to synchronize data, applications, and media files between the BlackBerry device and the host computer. It is also used to create backup copies of data from the BlackBerry phone and save them on the host computer. BDS is not designed for forensic acquisition. However, there are several advantages of using it to acquire a logical copy of a BlackBerry device. First, it is produced by the same company which produces the device; thus, more data may be obtained using BDS than with some forensic tools produced by companies with lesser familiarity with BlackBerry. Finally, backup files acquired through BDS can be inspected using a BlackBerry emulator.

A rule of thumb in the field of digital forensics is not to alter the original data acquired from the subject's device. By default, BDS is set to synchronize the phone's date and time with those of the host computer. If this option is not deactivated, it can strongly affect the validity of evidence in a criminal investigation by changing the original dates and times of the subject phones, contaminating the evidence. Therefore, this option must be explicitly disabled before attempting to attach and backup the subject's phone.

After configuring BDS to not synchronize the BlackBerry phone with the host computer, a logical bit-by-bit image of the test device was created using the "Backup" option from the Device menu. The logical image was created manually by performing a full backup of the device. Once the backup process was completed, the device was disconnected from the forensic workstation.

4.1.2. Examination and analysis

Acquiring a logical image of the BlackBerry phones resulted in the creation of a single proprietary IPD file for each phone. The files were stored within the default backup directory and by default had the naming style "BlackBerry model (current date).ipd" (e.g., BlackBerry Torch 9800 (July 30, 2011).ipd). Viewing the IPD file using a text editor showed that it had a unique header that starts with "Inter@ctive Pager Backup/Restore File". The file contained databases of user data and configurations. Examining the contents of the files revealed that they contained user data, such as contacts, SMS messages, MMS messages, and call logs. However, no traces of the social networking activities performed during the test were found.

4.2. iPhone forensic examination

This section describes the process of the logical acquisition and forensic analysis of the two iPhones. The acquisition processes for both phones were identical, and the analysis results were similar.

4.2.1. Logical acquisition

The logical acquisitions of the iPhone 4G devices were performed using the Apple iTunes application (version 10.4.0.80). Similar to BDS, iTunes is a synchronization and management application and is freely available on the Apple official website. It is designed to synchronize data, applications, and media files between Apple devices (e.g., iPhone, iPad, and iPod) and the host computer. It is also used to create backup copies of data from the Apple device and save them on the host computer. iTunes is not designed for forensic acquisition. However, it is an option that forensic practitioners can use to obtain a logical image (backup file) of an Apple device. Backup files may also exist on the suspect's computer if the suspect had previously performed a sync operation or a software update or restored their device to its factory settings.

It is critical for a forensic examiner to ensure the integrity of the acquired evidence. Therefore, the iPhone logical acquisitions were conducted in a forensically sound environment. Before attaching each iPhone to the forensic workstation, it was critical to disable automatic synchronization option from the iTunes application. By default, iTunes automatically syncs the device to the host computer once the device is connected.

Disabling automatic synchronization preserves the integrity of the iPhone's data, as it prevents the user's data from being exchanged between the iPhone and the host computer. Once iTunes was configured, the iPhone was attached to the forensic workstation through a USB data cable. After being detected by the iTunes application, a logical acquisition was manually initiated by right-clicking on the device name and selecting "backup". iTunes created a backup copy of the iPhone, and by default, it placed the backup files in the following directory: *C:\Users\[user]\AppData\Roaming\Apple Computer\MobileSync\Backup\[unique identifier]*. Once the backup process was completed, the iPhone was disconnected from the forensic workstation.

4.2.2. Examination and analysis

Acquiring a logical image of the iPhones using iTunes resulted in the creation of a folder with a unique alphanumeric name (hash value) for each iPhone, which contained the backed-up logical file. Both folders included three plist files, one mbdb file, one mbdx file, and a number of backup files with no apparent extensions. Each of the backup files was distinguished by a unique alphanumeric identifier of 40 characters.

Viewing and examining the backup files in a text editor showed that these files are in binary format or plain text that may contain encapsulated images, SQLite database files, or other plist files. To examine the contents of each file, they had to be decoded and viewed using the appropriate tools. Each file type was determined by the header contained within the file. Files starting with the header "bplist00" contained binary plist data, and files starting with the header "SQLite format 3" contained SQLite databases. A number of tools were used to manually examine the contents of the backup files according to their type. Plist Editor for Windows (version 1.0.1) was used to help read and examine backup files that contained plist data, and SQLite Database Browser (version 1.3) was used to help read and examine backup files that contained SQLite databases.

Manual examination of the backup files showed that they contained a vast amount of user data, including sent and received SMS, calendar events, call history, and address book entries. However, the main focus of this research was to determine whether footprints of social networking applications were stored within these backup files. The Command-line utility was used to manually search the files within the backup directory for keywords that relate to the social networking activities conducted during the experiment. Files containing the keywords were then decoded using the appropriate tools (e.g., Plist Editor and SQLite Database Browser), and their contents were thoroughly examined for traces of the activities that were conducted earlier in the experiment.

4.2.2.1. Facebook artifacts. Examination and analysis of the backup files revealed a number of SQLite and plist files related to the tested social networking applications. Many files contained the strings "Facebook", "Twitter", and "MySpace"; however, only a few contained data of interest to the forensic examiner. Three files contained data related to the iPhone Facebook application. The first two files were SQLite databases with the hashed names *6639cb6a02f32e0203851f25465ffb89ca8ae3fa* and *9f2140d8e87b45a9bb5dfc813fd2299c02851e6b*. Viewing the first file using the SQLite Database Browser showed that it contained a table that stored Facebook friend data. The table stored the friends' profile IDs, first and last names, URLs pointing to their profile pictures on Facebook, phone numbers, and email addresses.

The second file contained traces of the user's previous activities of uploading photos and posting comments through the Facebook application. It stored data such as the user's name, profile ID, the nature of the activity performed (e.g., uploading photos), and timestamps of the performed activities. The timestamps were stored in UNIX numeric values. Comparing the decoded date and times to the date and times of the activities performed on the actual Facebook webpage showed that the pictures were uploaded and the comments were posted within the same period of time. Fig. 1 shows the actual activities as they were presented on the Facebook website. Fig. 2 shows the traces of activities stored in the SQLite database.

The third file that contained data related to the iPhone Facebook application was a plist file with the hashed name *384eb9e62ba50d7f3a21d9224123db62879ef423*. The file stored details about the user, including the last email address used to log into the Facebook account, the unique identifier (ID) that identified the user's profile and user name, and a URL address pointing to the user's profile picture on Facebook.

Further examination of the plist file *384eb9e62ba50d7f3a21d9224123db62879ef423* yielded more interesting results. In addition to the details of the last logged-in user, the plist file contained other information that could be significant to the forensic examiner. It stored a record of all users that have previously logged into their Facebook accounts using the Facebook application. This information included user names, profile IDs, and URL addresses pointing to their profile pictures on Facebook. Furthermore, the plist file stored the details of the friends who had an active chat session with the Facebook user. The details included the user names of the friends, their profile ID, URL addresses pointing to their profile pictures on Facebook, and a timestamp of when the chat session was initiated.

4.2.2.2. Twitter artifacts. The iPhone Twitter application had two plist files that contained data that may be of significance to the forensic examiner: *eb8899d553cf563080453f9a366600de1dcf6286* and *f77282c60c3cee3ffce4a8bba2760fd954d4921f*. The first file held the Twitter application's user information including the user name, URL link pointing to the user's profile picture, tweets posted by the user, and the timestamps of posted tweets. The second file contained the user's details plus some other information. It held records of people followed by the user, their user names, detailed information taken from their profile pages, URL links pointing to their profile pictures, tweets posted by them, and the timestamps of their posted tweets. Fig. 3 show the details of a tweet posted by the user of the iPhone Twitter application recovered from the first iPhone file, and the corresponding tweet extracted from the Twitter website.

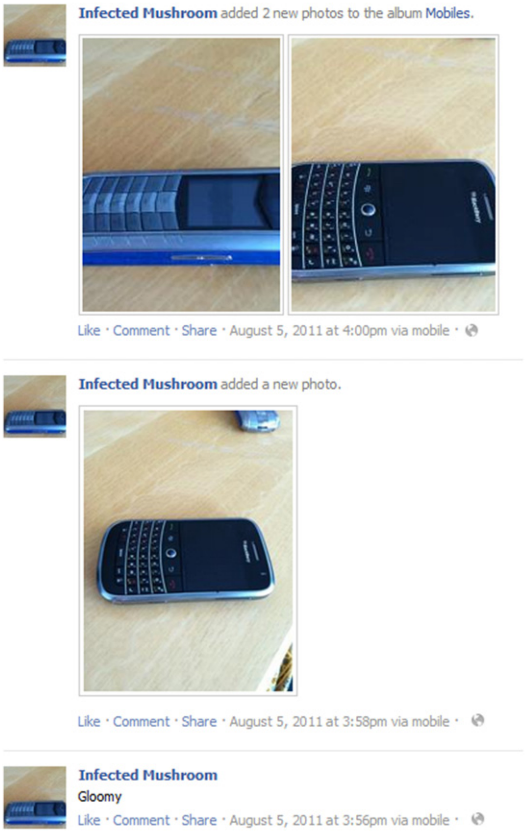
4.2.2.3. MySpace artifacts. The iPhone MySpace application had two files that contained data that may be of significance to the forensic examiner: a SQLite file *48598f280bb577d1e68aaddadccba35c54acbb48* and a plist file *e5cb579c7bdf12b996bd865ecf6290ab94374abd*. The SQLite file contained the user name of the iPhone MySpace application, plus comments that the user had posted in the stream with timestamps encoded in absolute value. Table 3 shows a record of one of the posted comments and its timestamp.

4.2.2.4. Dynamic directory. Another file that held data of interest to this study was *0b68edc697a550c9b977b77cd012fa9a0557dfcb*. Examining the contents of the file in a text editor showed that it started with the header (DynamicDictionary-4) and stored snippets of text that had been typed using the iPhone's keyboard. Performing some tests regarding the contents of this file showed that it stores user keyboard inputs to applications on the iPhone; including social networking applications. Parts of the comments, emails, and chat messages that have been used through the experiment; and were not stored elsewhere on the backup files, were found in this file.

4.3. Android forensic examination

This section describes the process of the logical acquisition and forensic analysis of the Android phone (Samsung GT-i9000 Galaxy S – Firmware version 2.3.3). Unlike other smartphones, unless the Android phone was rooted, many data files could not be accessed or backed up by backup programs. Therefore, the tested Android phone was first rooted using Odin3 (version 1.3) to upload the root-kit (CF Root XW).

Installing a root-kit allows the user to gain privilege control over the Android OS (root access), allowing him to bypass some limitations that the manufacturers put on the device. Having a rooted Android phone also allows the user to access protected directories on the system that hold user data (e.g., */data/data* directory) and backup all of the files in these directories. These data files can hold a significant amount of data that may support an ongoing investigation. The process is not uncontroversial in the forensics literature (see for example, the discussion in Vidas et al. (2011)),



Infected Mushroom added 2 new photos to the album Mobiles.

Like · Comment · Share · August 5, 2011 at 4:00pm via mobile ·

Infected Mushroom added a new photo.

Like · Comment · Share · August 5, 2011 at 3:58pm via mobile ·

Infected Mushroom
Gloomy
Like · Comment · Share · August 5, 2011 at 3:56pm via mobile ·

Fig. 1. The actual photos and comments as presented on the Facebook website.

and ideally, a thorough method of logical acquisition which does not require rooting or other modification of the software running on the Android device will be identified in future research.

4.3.1. Logical acquisition

Unlike Blackberrys and iPhones, Android phones do not have a unified management and backup solution. Various companies have released different backup tools which give the user the option of backing up the device on either the phone's SD Card or the company's server. One such applications is MyBackup.

To acquire a logical backup of the Android phone, MyBackup (v2.7.7) was installed on the test Android phone. A new Micro SD external card was placed into the test phone. The Micro SD card was selected as the location to store the backup files. All three tested social networking applications were selected, and the associated data files were backed up to the external Micro SD card. Once the backup process was completed, the Micro SD external card was removed from the test phone and attached to the forensic workstation to examine the backup files and perform the forensic analysis.

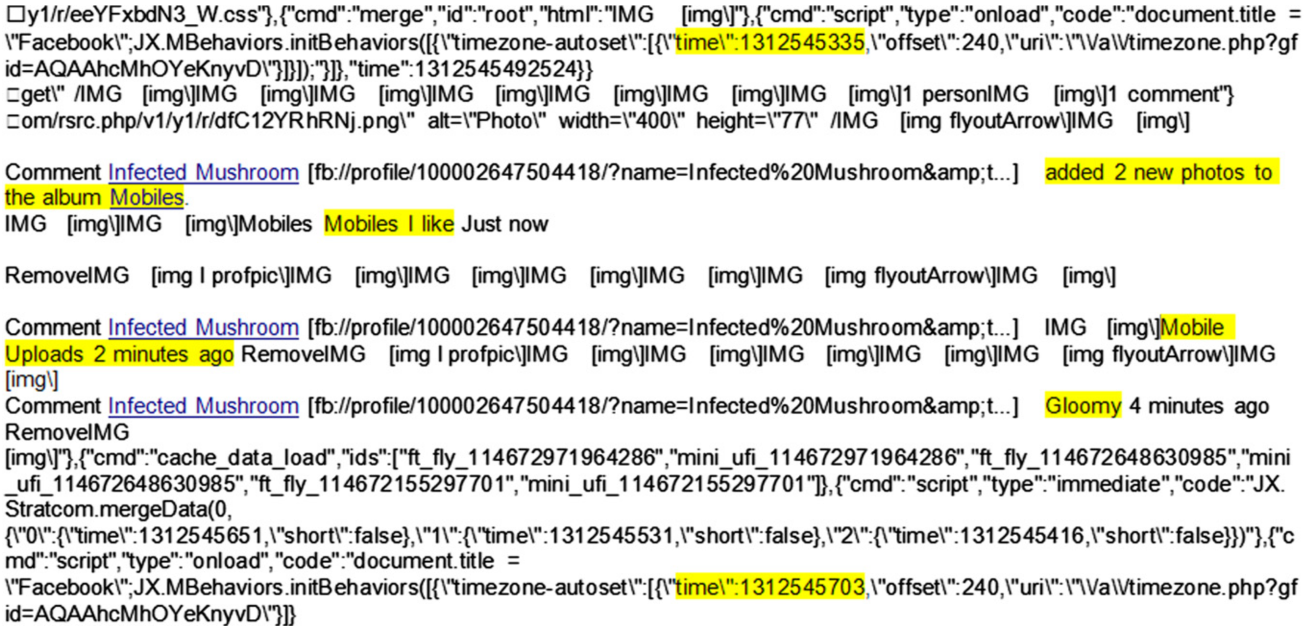
4.3.2. Examination and analysis

Acquiring a logical backup of the data files associated with the Facebook, Twitter, and MySpace applications on the Android phone using MyBackup resulted in the creation of a backup directory on the external Micro SD card. The Directory had the default path *\rerware\MyBackup\AllAppsBackups\[AppsMedia_yyyy_mm_dd]\Apps*. The directory contained three archive (ZIP) files, one for each tested app:

- *com.facebook.katana_4130.zip*
- *com.kozmo.kspace_4.zip*
- *com.twitter.android_134.zip*

4.3.2.1. Facebook artifacts. The three backed up files were copied to the forensic workstation, where each was extracted and thoroughly examined for traces of the social networking activities performed during the tests. The first file *com.facebook.katana_4130.zip* was associated with the Facebook application. It contained three subdirectories: databases, files, and lib, which contained a number of files. The two directories that held relevant data for this study were databases and files.

The databases folder held three SQLite files: fb.db, webview.db, and webviewCache.db. Viewing each file through the SQLite Database Browser and examining its content yielded interesting results. The first file fb.db contained tables that held records of activities performed by the Android Facebook application user, including created albums, chat messages, list of friends, friend data, mailbox



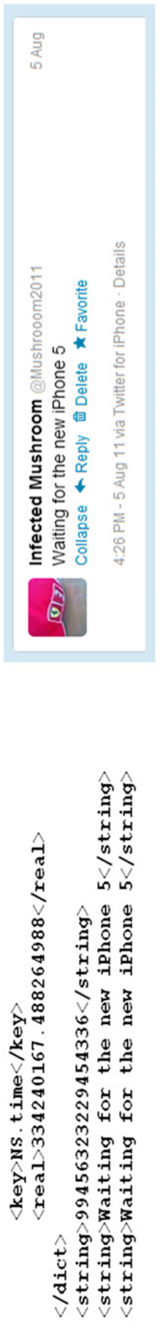
```
□y1/r/eeYFxbdN3_W.css"},{"cmd":"merge","id":"root","html":"IMG    [img\]"},{"cmd":"script","type":"onload","code":"document.title  =
\"Facebook\";JX.MBehaviors.initBehaviors([{\"timezone-autoset\":[{\"time\":1312545335,\"offset\":240,\"uri\":\"\/a\/timezone.php?gf
id=AQAAhcMhOYeKnyvD\"}]}]);"}]},"time":1312545492524}}
□get\" /IMG   [img\]IMG   [img\]IMG   [img\]IMG   [img\]IMG   [img\]IMG   [img\]IMG   [img\]1 personIMG   [img\]1 comment"}
□om/rsrc.php/v1/y1/r/dfC12YRhRNj.png\"  alt=\"Photo\"  width=\"400\"  height=\"77\"  /IMG   [img flyoutArrow\]IMG   [img\]

Comment Infected Mushroom [fb://profile/100002647504418/?name=Infected%20Mushroom&amp;t...]   added 2 new photos to
the album Mobiles.
IMG   [img\]IMG   [img\]Mobiles  Mobiles I like Just now

RemoveIMG   [img l profpic\]IMG   [img\]IMG   [img\]IMG   [img\]IMG   [img\]IMG   [img flyoutArrow\]IMG   [img\]

Comment Infected Mushroom [fb://profile/100002647504418/?name=Infected%20Mushroom&amp;t...]   IMG   [img\]Mobile
Uploads 2 minutes ago RemoveIMG   [img l profpic\]IMG   [img\]IMG   [img\]IMG   [img\]IMG   [img\]IMG   [img flyoutArrow\]IMG
[img\]
Comment Infected Mushroom [fb://profile/100002647504418/?name=Infected%20Mushroom&amp;t...]   Gloomy 4 minutes ago
RemoveIMG
[img\]"},{"cmd":"cache_data_load","ids":["ft_fly_114672971964286","mini_ufi_114672971964286","ft_fly_114672648630985","mini
_ufi_114672648630985","ft_fly_114672155297701","mini_ufi_114672155297701"]},{"cmd":"script","type":"immediate","code":"JX.
Stratcom.mergeData(0,
{\"0\":{\"time\":1312545651,\"short\":false},\"1\":{\"time\":1312545531,\"short\":false},\"2\":{\"time\":1312545416,\"short\":false}})"},{"c
md":"script","type":"onload","code":"document.title  =
\"Facebook\";JX.MBehaviors.initBehaviors([{\"timezone-autoset\":[{\"time\":1312545703,\"offset\":240,\"uri\":\"\/a\/timezone.php?gf
id=AQAAhcMhOYeKnyvD\"}]}
```

Fig. 2. Traces of uploading photos and posting comments using the iPhone Facebook application.



```
        <key>NS.time</key>
        <real>334240167.488264988</real>
</dict>
<string>99456323229454336</string>
<string>Waiting for the new iPhone 5</string>
<string>Waiting for the new iPhone 5</string>
```

Infected Mushroom @Mushrooom2011 5 Aug

Waiting for the new iPhone 5

4:26 PM - 5 Aug 11 via Twitter for iPhone · Details

Fig. 3. The record of a “tweet” from the iPhone file, and the corresponding tweet on the Twitter website.

Table 3
Record of a posted comment in MySpace.

ZTIMESTAMP	ZMESSAGE	Decoded timestamp
338556819.798738	The weather is getting better	Saturday, 24 September 2011 15:33:40 +0400

The plist file contained the user name and password in clear text. For example:

```
<dict>
<key>password</key>
<string>mushroom888</string>
<key>user name</key>
<string>infected.mushroom2011@hotmail.com</string>
</dict>
```

messages, and uploaded photos. The records included significant information for the forensic investigator, such as the users’ IDs, contents of exchanged messages, URL links of uploaded pictures, and timestamps of performed activities.

The files folder contained a number of files with names that consisted of seemingly random letters and numbers and that did not have any extensions. Viewing the files in a text editor and examining their headers showed the (JFIF) marker segment, indicating that these files were (JPEG) image files. Using Windows Photo Viewer to open the files showed the actual image contained within each file. Images contained within these files were either pictures that the user had viewed from within the Android Facebook application or pictures that he uploaded from within the application. Files of uploaded pictures had their names preceded with the word “upload”.

4.3.2.2. Twitter artifacts. The second archive file *com.twitter.android_134.zip* was associated with the Android Twitter application. It contained a folder called databases, which contained three SQLite files. One of the files, *342525691.db*, stored interesting data. It contained tables that stored records of posted tweets, photos, friends, users, and other data associated with activities performed through the Android Twitter application. Besides storing the author IDs, timestamps, and contents of the posted tweets, the records also stored data about the source of the posted tweets, e.g., posting through the website, an iPhone application, or an Android phone application.

4.3.2.3. MySpace artifacts. The third archive file, *com.kozmo.kspace_4.zip*, was associated with the Android MySpace application. It contained a folder called databases, which contained three SQLite files. As mentioned earlier, the tested MySpace application was not the official application created by the MySpace company but a web-based application created by another group. Examining the three SQLite files showed that they stored cookies and cache files associated with navigating the MySpace website. It also showed that the file webview.db stored the user name and the password of the MySpace application in plain text.

4.4. Results summary

Table 4 summarizes the results of our analysis for each application on each device examined.

Table 4
The significant social networking data that could be recovered from the logical image of each smartphone.

Smartphone	Application	Description
BlackBerry	Facebook	Not found
BlackBerry	Twitter	Not found
BlackBerry	MySpace	Not found
iPhone	Facebook	User and friend data incl. contact details and profile picture URLs Photo uploads Comments posted Timestamps All previously logged in users Friends with active chat sessions
iPhone	Twitter	For user and people followed: User names Profile picture URLs Tweets posted Timestamps
iPhone	MySpace	User name/Password Posted comments Timestamps
Android	Facebook	User and friend data incl. contact details and profile Photo uploads Created albums Pictures viewed with app Mailbox/Chat messages
Android	Twitter	For user and people followed: User names Posted tweets and photos Other activity information (e.g., device used to tweet)
Android	MySpace	User name/Password Cookies & cache files

5. Future work

There are several major items of future work leading directly from this study. First, more experimental cases are required to examine a greater variety of smartphones and social networking applications alike. Second, different smartphones employ a variety of techniques to “lock” the device’s interface and encrypt the data stored on the phone while the device is locked, and these privacy measures also serve as anti-forensics techniques to be overcome. Research into this issue would likely require different techniques for each smartphone platform.

6. Conclusions

Few studies have addressed the forensic analysis and recovery of activities performed through social networking applications on smartphones. These studies have also been limited to the recovery of very basic information related to the use of social networking applications. This study focused on the recovery of artifacts and traces related to the use of social networking applications on a variety of smartphones using different operating systems. It aimed to determine whether activities performed through these applications are stored and can be recovered from the internal memory of these smartphones. The tested social networking applications were Facebook, Twitter, and MySpace, which were used on BlackBerry, iPhone, and Android.

The study explored the forensic acquisition, analysis and examination of the logical backup copies of the three smartphones. The tests consisted of installing the social networking applications on each device, conducting common user activities through each application, acquiring a forensically sound logical image of each device, and performing manual forensic analysis on each acquired logical image. The forensic analysis determined the amount, significance, and location of social networking data that could be found and retrieved from the logical image of each device.

The results showed that no traces of social networking activities could be recovered from BlackBerry devices. However, iPhones and Android phones stored a significant amount of valuable data that could be recovered and used by the forensic investigator. The paper documented the nature of the social networking data that could be recovered from each device and their locations from within the backup files. We hope that the paper can inspire the creation of digital forensics tools to extract and reconstruct social networking data from a variety of modern smartphones.

References

Al Mutawa N, Al Awadhi I, Baggili I, Marrington A. Forensic artifacts of Facebook’s instant messaging service. In: Proceedings of the 2011 International Conference for Internet Technology and Secured Transactions (ICITST); 2011. p. 771–6. Abu Dhabi, UAE.

Al Zarouni M. Mobile handset forensic evidence: a challenge for law enforcement. In: Proceedings of the 4th Australian Digital Forensics Conference; 2006. Perth, Australia.

Bader M, Baggili I. iPhone 3GS forensics: logical analysis using apple itunes backup utility. Small Scale Digital Device Forensics Journal September 2010;4(1).

Burnette MW. Forensic examination of a RIM (BlackBerry) wireless device. Retrieved on 18 February 2012 from: http://www.mandarino70.it/Documents/Blackberry%20Forensics.pdf; 2002.

de Paula AMG. Security aspects and future trends of social networks. In: Proceedings of the Fourth International Conference of Forensic Computer Science; 2009. p. 66–77. Natal City, Brazil.

Facebook. Statistics. Retrieved on 26 May 2011 from: http://www.facebook.com/press/info.php?statistics; 2011.

Finn Ruder. New study shows ‘intent’ behind mobile Internet use. Retrieved on 18 February 2012 from: http://www.prnewswire.com/news-releases/new-study-shows-intent-behind-mobile-internet-use-84016487.html; 2012.

International Telecommunications Union. The rise of social networking. Retrieved on 18 February 2012 from: http://www.itu.int/net/itunews/issues/2010/06/35.aspx; 2010.

Kubasiak R, Morrissey S, Varsalone J. Macintosh OS X, iPod, and iPhone forensic analysis DVD toolkit. Burlington, MA: Syngress; 2009.

Lessard J, Kessler GC. Android forensics: simplifying cell phone examinations. Small Scale Digital Device Forensics Journal September 2010; 4(1).

Morrissey S. iOS forensic analysis for iPhone, iPad, and iPod touch. New York: Apress; 2010.

National Institute of Standards and Technology. General test methodology for computer forensic tools. Retrieved on 18 February 2012 from: http://www.cftt.nist.gov/documents.htm; 2001.

National Institute of Standards and Technology. Test results for mobile device acquisition tool. Zdziarski’s Method; 2010.

Punja SG, Mislan RP. Mobile device analysis. Small Scale Digital Device Forensics Journal June 2008;2(1).

Vidas T, Zhang C, Maloof M. Toward a general collection methodology for Android devices. In: Proceedings of the Eleventh Annual DFRWS Conference, vol. 8S; 2011. p. S14–23. New Orleans, USA, published in Digital Investigation.

Zdziarski J. iPhone forensics: recovering evidence, personal data, and corporate assets. Sebastopol, CA: O’Reilly; 2010.

Zellers F. MySpace.com forensic artifacts keyword searches. Retrieved on 18 February 2012 from: http://www.inlanddirect.com/CEIC-2008.pdf; 2008.