Journal of
Information Technology & Software Engineering

Aditya et al., J Inform Tech Softw Eng 2013, 3:2
DOI: 10.4172/2165-7866.1000120

Research Article Open Access

Extracting Passwords and User-Related Data from Yahoo Messenger and Mail Client on Android Phones

Aditya Mahajan*, Laxmikant Gudipaty and Mohinder S. Dahiya

Institute of Forensic Science, Gujarat Forensic Sciences University, Gujarat, India

Abstract

The purpose of this paper is to provide a simplified methodology to extract information stored in the internal memory of phone like chat logs, contact history, email history and user login password of a user using a Yahoo Messenger and Yahoo Mail application App on an Android Phone .This will help us classify the fore-mentioned artifacts as per their forensic importance to a forensic investigator depending upon the nature of the digital crime being analyzed.

The introduction of smartphones into the market has opened up a whole new scope of possibilities on how a mobile phone can be used by a user. The modern day smartphones are capable of strongly competing with computers in terms of the functionality and features that they can provide. Some of these features include email support, instant messengers, interactive games, GPS navigation, music player, document viewers and readers. The feature which we intend to primarily focus on in this paper is Yahoo instant messenger applications and Yahoo mail client application that can be freely downloaded and installed on Android Smartphone. The recovery of digital evidence in the form of user names, Passwords, conversations and contacts details on Instant messengers and mail clients may yield valuable information regarding the suspect/victim's chatting and email history or their contacts list details.

Keywords: Android forensics; Yahoo Messenger forensics; Yahoo Mail Client Forensics; FileSystem extraction; SQLite database browser

Introduction

Instant messenger applications are those applications that support instant messaging communication in a bidirectional manner at real time speeds between users who are logged in to the messenger. The more recent instant messengers not only provide text messaging but also audio and video communication at real-time. The modern day smartphones support instant messaging thereby increasing their functionality well beyond the basic call sending/receiving and SMS feature. Instant messengers on smartphones however require the user to be logged on using a unique username and a password. Once logged in to the messenger using a registered username and password, the user can then communicate via text, audio or video with anyone who is added to their contact list and is logged on to the messenger at that instant. Similar to messenger application, an email client allows a logged in user to send or receive emails on the smartphone.

During the research, experiments were conducted on Android phones for discovering the objects of potential evidentiary value such as chat history, contact lists, user login name, password, email history associated with the Yahoo instant messenger application [1] and email clients installed on the smart phone. This discovery may provide substantial information regarding the user and his/her contact details, chat log and most importantly the login password of the user who has signed in to the application. The Yahoo mail client application was downloaded from the Google Play Store and installed onto the phone with Android Version 2.2 (Froyo). However, we found the password stored in plain text form which was easily readable. This forensically relevant information may prove to be very vital in proving a crime or providing a lead to the investigators to further investigate a digital crime and successfully establish the occurrence of a crime. The basic methodology and the purpose behind the research is to try and discover the precise locations on the phone's memory from where forensically relevant information fore mentioned can be retrieved.

Following the steps mentioned below, we were able to successfully extract the user password.

1. Using a forensically approved method to perform file system extraction of Android test devices.
2. Browsing through the filesystem to find the precise location where chat logs, contacts list and passwords related to Yahoo Messenger application are stored (\data\data\com.yahoo.mobile.client.android.im).These artifacts are usually stored in .db (SQLite) database files
3. Analyzing the database files using a database browser such as SQLite Database browser.

Using a forensically approved method maintains the integrity of the data on the device and doesn't alter or change any data on the cell phones [2].

Forensic Equipment and Methodology

The main motive behind this research is to ascertain whether the applications installed or run on the Smartphone leave any artifacts on the device's internal memory or not. This evidentiary data may prove to be very crucial during investigations of any criminal case. The list of possible evidentiary artifacts associated with Yahoo messenger and Yahoo mail client that may be discovered on phone's internal memory are as follows:

1. Contact list
2. Login Username
3. Login Password
4. Instant messaging conversations
5. Mailing history

***Corresponding author:** Aditya Mahajan, Institute of Forensic Science, Gujarat Forensic Sciences University, Gujarat, India, E-mail: adityamahajan3@gmail.com

Received June 09, 2013; **Accepted** August 17, 2013; **Published** August 21, 2013

Citation: M Aditya, G Laxmikant, M.S. Dahiya (2013) Extracting Passwords and User-Related Data from Yahoo Messenger and Mail Client on Android Phones. J Inform Tech Softw Eng 3: 120. doi:10.4172/2165-7866.1000120

The aforementioned objects may help us recreate a scenario that may have occurred at the crime. Further investigation of such objects may provide valuable leads that affect the verdict of a case.

However these evidentiary objects need to be extracted and analyzed in a forensically sound manner to be help admissible in court of law. The integrity of the data should not be compromised with under any circumstances. With this intention, the tests and experiments conducted in this paper have been performed following the guidelines established by NIST [2].

Efforts have been taken to ensure that a realistic crime scenario is replicated and the investigation is performed in a reliable manner. Similar to a real time crime scenario, a suspect or victim may have installed Android applications namely Yahoo Messenger version 1.8.3 [3] and Yahoo Mail Client Version 1.8.1 [4] on their Smartphone. The mobiles used may be rooted or unrooted. Considering all these circumstances, we designed our tests accordingly. A mobile phone was specially rooted [5] for these experiments while keeping others unrooted.

Test environment

A secure workstation devoid of any form of malware was configured and setup. Details of the workstation are as follows:

- Windows7 Professional - SP1
- RAM - 8 GB
- System Type- 64 bit Operating System
- Processor - Intel Core i7- 3770 CPU @3.40 Ghz

This setup was disconnected from any form of network to ensure utmost security from vulnerabilities caused by networks. The experiments were conducted keeping the predefined settings of the devices intact. The internal memory configurations such as cache size were left unaltered. Hash values were also generated prior to experiments. Hash values [6] play very important role in order to submit evidence in court of law. Hash Values calculated for all the phones are given in Table 1. Figure 1 shows the Mobile phones and equipment used for testing and experiments. Following is the list of Hardware's and software's used for testing and conducting experiments:

- 3 Android phones
- Sony Xperia Mt11i – Neo V (version: 4.0.4 – ICS)
- LG P698 F Optimus Dual(version: 2.3.4 – Ginger Bread)
- HTC A8181 Desire (version: 2.2.1 – Froyo)
- Cellebrite UFED Classic Ultimate (version: 1.8.0.0)
- Yahoo Messenger and Yahoo Mail Client
- SQLite Database Browser (version: 2.0)
- USB data cables
- SuperOne Click (Version: 2.3.3)
- Android Commander (version: 0.7.9.11)

However, Cellebrite UFED is not the only tool which extracts this data, *Micro Systemation's XRY* tool can also recover this data and can be used for analysis.

Test procedure

The following scenarios were incorporated as a part of test procedure

1. Rooted Android smartphones
2. Unrooted Android smartphones.

Scenario of rooted smart phones: The following phone was rooted in order to perform the experiments:

- *LG P698F Optimus Dual (Android 2.3.4 Gingerbread)*

Rooting an Android device is a methodology by which we gain root privileges of a device. Acquiring root access of a device allows the user to gain elevated privileges thereby allowing the user to access permissions and rights that are by default not available to the user of unrooted mobile. The main purpose of rooting in our test scenario is to secure access to root folder i.e. internal memory of the smartphone. This will eliminate the need to perform filesystem extraction of the smartphone as the folders & files of the root directory (internal memory) are directly accessible after gaining root privileges. The directories can then be directly copied using freely available tools namely Root Explorer for the device and Android Commander for desktop PC. Acquisition process through Android Commander is later described in this paper.

The Yahoo Messenger and Yahoo Mail client applications were then installed on the device from Android's official application source Google Play Store [3,4]. The evidentiary objects related to these applications that left a trace on the device's internal memory were then located and analyzed without having to use expensive imaging and extraction tools.

Scenario of un-rooted smart phones: Following Unrooted phones were taken in-order to perform tests and experiments:

1. Sony Xperia MT11i – Neo V (version: 4.0.4 – ICS)
2. HTC Desire A8181 (version: 2.2.1 – ICS)

Unrooted Android phones restrict the access to root files and folders residing in the internal memory of the phone. To extract the data from those folders without rooting the phone, mobile data extraction device UFED from Cellebrite was used. Physical, FileSystem and Logical extractions are supported by UFED (Universal Forensic Extraction Device) [7,8] which covers extensive range of phones. However, FileSystem extractions were carried out here for manual analysis of data extracted from both phones. Filesystem extraction extracts all the files and folders which contain database files, log files, login-Id's information, chat logs and other important data.

The major difference of an unrooted Android phones compared to rooted phones is the unavailability of root access. This disallows accessibility to the root folder present on the internal memory of the device. Therefore such devices compulsorily require complete filesystem extractions in order to acquire folders that are otherwise

Android Device	Hash Value (SHA 256)
Sony Xperia Neo V (MT11i)	6A3F63E4EVEB0D036CB9AE25A2183B761C3B79128A59DE92481B68AF4CD2B24
LG P698	A34D8CCCBF53A04198ED0BEB2FF90F34DAAB3B2751474B156815F9EC43CB69
HTC A8181 Desire	23BD7BC18C36A20BC3F07501570A9EF5C787A6701C49E4E4A4EE80D6EFB761A6

Table 1: Hash Values calculated for phones.

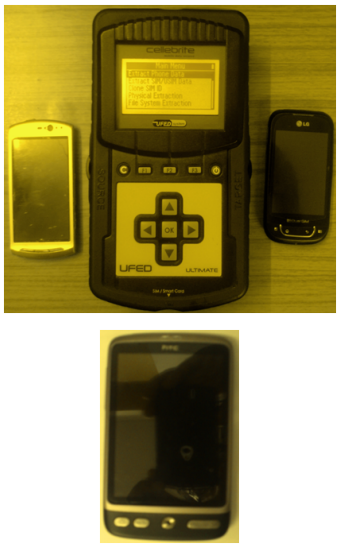

Figure 1: Mobile phones and Equipment Used for Testing and Experiments.

unavailable without root access. The potential evidence related to yahoo can then be accessed by analyzing the output of filesystem extraction tool used via UFED Classic Ultimate. Thereafter we can investigate the potential evidence left behind by the Yahoo Messenger and Yahoo Mail application.

The following operations and activities were performed using both sets of mobiles phones i.e. rooted as well as unrooted:

➢ **Common activities performed:**

- Installing Yahoo messenger and Yahoo mail client applications from Google Play Store.
- Logging into Yahoo Messenger using test username and password.
- Instant Messaging using Yahoo Messenger application
- Logging into Yahoo Mail Client application using test username and password.
- Sending emails via Yahoo Mail Client application
- Receiving emails on device via Yahoo Mail Client application.

File system acquisition

This stage involves acquisition of filesystem located on the internal memory of each smartphone. The unrooted smartphones used in the testing procedure require acquisition [9] using hardware based devices such as UFED Classic Ultimate. This acquisition is performed in a forensically approved manner to ensure that evidences discovered can be admitted in the court. This approach also compulsorily requires enabling USB Debugging [10] from settings menu on each device.

The acquisition of the rooted devices requires no physical hardware device for extraction and could be performed using freely available tools like Oxygen Forensics and MobilEdit. Acquisition can also be done using simple "dd" command in computer after connecting the cellphone to the computer. However, the drawback of such an approach is admissibility in court [2] as it involves rooting an Android phone. The procedure of rooting a device involves certain write operations on the internal memory of the device thereby affecting its integrity.

Experiment and Analysis

After acquisition of filesystem dumps of each of the test devices, a thorough forensic examination of the files and folders extracted was performed. The location of databases associated with Yahoo Messenger and Yahoo Mail apps was determined and evidentiary data was extracted and analyzed using forensically admissible techniques. The manual examination and analysis of databases so found, helped us acquire potential evidences i.e. Instant messaging chat logs, user login names, passwords ,mails sent and received related to Yahoo messenger and Yahoo mail Android applications installed on the test phones.

Implementation and analysis phase

First stage of this experiment involved installation of Yahoo Messenger and Yahoo Mail Client applications on all the test devices. A common set of activities to be performed were decided upon and conducted on each device. The criteria behind deciding these activities was to ensure that the activities could replicate a real time scenario and help provide data that might prove to be crucial as per a digital forensic experts perspective.

The activities performed on the Yahoo Messenger application and Yahoo mail application on each of the test devices are:

- Creation of test user account.
- Logging into the application using test user name and password
- Chatting
- Sending mails
- Receiving mails

Table 2 describes the activities briefly. After thoroughly performing the above mentioned activities, a file system acquisition of each device was acquired using different approaches. The approaches implemented to obtain the required data have been described later in the paper.

Approach for rooted phones

Prerequisites: This approach requires acquiring superuser/root privileges of the following Android Smartphone by rooting the device.

Device: LG P698F Optimus dual (Android 2.3.4 Ginger Bread): A third party tool called SuperOneClick [11] was installed on the forensic workstation.

Under the Settings menu in the Android device >Applications>Development>Enable USB Debugging option is enabled. After downloading and installing the LG USB drivers and other required drivers, the device is connected to the workstation and the "SuperOneClick" application is executed. The Root Device button is clicked upon to begin the rooting of the device. This takes approximately ten minutes to complete followed by a device reboot. After rebooting the device, a SuperUser application is automatically installed on the device which means root privileges for the device have been acquired and the user is now a root user.

Application	Activities Performed
Yahoo Messenger	1) Logging in with username hpsanghvi@yahoo.com
	2) Send instant messages to adityamahajan5@yahoo.com
	3) Receive instant messages from adityamahajan5@yahoo.com
Yahoo Mail Client	1) Logging in with username hpsanghvi@yahoo.com
	2) Send email to adityamahajan5@yahoo.com
	3) Receive email from adityamahajan5@yahoo.com

Table 2: Activities performed using Applications for testing.

Acquisition of rooted phone: As mentioned earlier, file system acquisition on a rooted phone requires no additional hardware based extraction devices. A third party free application like Android commander will allow the user to view the root directory on a rooted device and support pulling and pushing of directories within the internal memory of the mobile device. The folders that are of importance to us from an examiner's perspective are:

1) **\data\data\com.yahoo.mobile.client.android.im\databases** ***(Yahoo Messenger related artifacts)***

2) **\data\data\com.yahoo.mobile.client.android.yahoo\databases** ***(Yahoo mail application related artifacts)***

Since our primary focus is on extraction potential evidentiary data related to Yahoo messenger and Yahoo mail application from Android Devices, we can merely pull or fetch the above mentioned directories leaving rest of the directories intact. An application called Android Commanders that is free for download is downloaded from "www.Androidcommander.com" and installed on forensic workstation being used. This application will provide an elaborate view of all the available folders on the internal memory of the device.

The methodology employed to extract the desired folders is as follows:

1) Enable USB debugging on the device and connect the device to the preconfigured workstation.

2) Launch the Android commander application on the workstation and select the device from the list of devices available list. This will allow us access into the root directories of the internal memory

3) Thereafter we can simply pull the folders of interest and save them on the desired location on the workstation.

File system acquisition of unrooted devices: Steps for Filesystem Extraction from UFED [12]:

1. Under settings menu, go to development and Enable USB debugging option.
2. Connect mobile phone to source port via USB cable.
3. In UFED, Under Filesystem option, select mobile phone model.
4. Press continue for extraction

The files and folders will be extracted into a ".zip" file to the USB drive attached at the destination port of UFED.

Experimental Results

This section focuses on representation of the outcome of the experiments conducted. The results of analysis of each of the applications "Yahoo Mail and Yahoo Messenger", related data has been enlisted below for simplified [13] understanding and concise representation of the study.

Yahoo Chat/IM application examination and results

Following the golden rule of forensics, the acquisition of desired folders from phone's internal memory was performed ensuring complete integrity of data.

The examination of "\data\data\com.yahoo.mobile.client.android.im\databases\" revealed several forensically vital artifacts stores in SQLITE databases (.db files)

These SQLite databases are lightweight databases for mobiles for stories important entries and tuples in tabular form.

The messenger.db found in "\data\data\com.yahoo.mobile.client.android.im\databases\" revealed a lot of forensically important information. The list of ".db" files found present on the internal memory are:

- messenger.db
- share.db
- rest.db
- webview.db

Table 3 shows the different artifacts found in different database files mentioning particular table.

The instant messaging conversations/chats displayed both sender and recipient name along with Timestamps of the conversation. Timestamps are forensically very important as they help in establishing the timeline of when the conversation happened. This may provide valuable leads regarding the time at which the conversation occurred.

Apart from the two databases discussed above, the other three databases did not provide any data that could be important from a forensic investigation perspective.

Yahoo mail client application examination and analysis

Similar approach was followed to analyze the ***"data/data/com.yahoo.mobileclient.androidyahoo"*** folder which yielded far more interesting results related to the mail client used on the devices. We could recover snippets of emails sent or received along with their source and destination email addresses. Such information could come in handy when a case requires proof of the mail being sent or received. The user name or email id used to login to the messenger client and the password associated with that user id could also be recovered on specific devices i.e. Devices running Android version 2.2. The recovery of password on devices running Android versions beyond version 2.2 was not possible. This clearly implies that the Application developers came up with better security mechanism to ensure privacy of user data is not compromised.

The lists of databases found on the Yahoo Mail client application folder are

- Webview.db
- WebviewCache.db

The most important database from a forensic perspective is webview.db. This database file revealed valuable artifacts given in Table 4.

Screenshots of artifacts found on Android devices during experiments and analysis

Figure 2 and 3 shows the list of contacts and friends added in the yahoo account profile of the userfound in the table named as 'Buddies_2'.

Database File Name	Table Name	Artifacts Found
Messenger.db	Users	Usernames of Yahoo application users
	Message_1	Instant Messaging/Chat conversations along with TIMESTAMPS
	Buddies_2	Messenger Contact List
Share.db	Accounts	All Login user names used for application

Table 3: Artifacts found in Yahoo Chat/IM.

Figure 4 shows the list of login-id's used by the cellphone user found in table 'Users'.

Figure 5 is the most important data which is found in table 'password' which stores and shows the password of the respective login-id.

In Figure 6, following is the significance of Values in the "iAmSender" Parameter:

If value='0', Message is Sent by the User

If value='1', Message is received by the User

Also, for every chat message sent by the user, a unique hash value is generated by the application.

Database File Name	Table Name	Artifacts Found
Webview.db	Formdata	1. Sent Email History 2. Received Email History
	Password	1. Email Address of the User 2. Password of the user (in Plain Text)

Table 4: Artifacts found in Yahoo Mail Client.

Table: formdata

	id	urlid	name	value
1	1	2	id	hpsanghvi
2	2	7	to	adityamahajan5@yahoo.com
3	3	9	to	adityamahajan5@yahoo.com
4	4	9	subject	Test sent emails
5	5	15	to	jm [redacted] hotmail.com
6	6	15	subject	FW: ta [redacted] -2012
7	7	17	id	hpsanghvi
8	8	66	to	paku_ [redacted]
9	9	66	subject	FW: Biodata of Reen [redacted]

Figure 2: Email Artifacts with email addresses and Subjects.

Table: Buddies_2

	id	key	displayName	yahooId	network
1	3	hpsanghi:yahoo	Hitesh Sanghvi	hpsanghvi	yahoo
2	4	amin [redacted] yahoo	amin [redacted]	amin [redacted]	yahoo
3	6	djd [redacted] :yahoo	dj [redacted] jsk	dj [redacted] jsk	yahoo
4	7	vyas_ [redacted] :yahoo	pal [redacted]	vy [redacted] 0999	yahoo
5	8	p. [redacted] @ymail.com:yahoo	Maulin [redacted]	p [redacted] @ymail.com	yahoo
6	9	pa [redacted] :yahoo	Pat [redacted]	pa [redacted]	yahoo
7	10	kinu [redacted] :yahoo	Kin [redacted]	kin [redacted]	yahoo
8	12	saa [redacted] :yahoo	Sa [redacted]	saa [redacted]	yahoo
9	13	brij [redacted] @hotmail.com	brij [redacted] @hotn	brij [redacted] @hotmail.com	msn

Figure 3: Screenshot of Contact List of Yahoo users.

Table: Users

	id	data1	data2	data3	data4	data5	data6	data7	data8	data9	yahooId
1	1										hiteshsanghvi
2	2										p [redacted] r
3	3										adityamahajan5

Figure 4: Users Names found in database table "Users".

Table: password

	id	host	username	password
1	11	httpmlogin.yahoo.com	hpsanghvi	hem [redacted]

Figure 5: Screenshot Showing stored PASSWORD and USER NAME found in PLAIN TEXT.

Table: Messages_1

	id	iAmSender	profile_id	buddy_id	message	hash
1	1	0	1	3	hi	ROKl4j1S7ecoS3lu/6jTtWHJJdiqQ==
2	2	0	1	1	bolo	z3RgIU/e6UxxHDC9k3B8mlhC1UZIFQ==
3	3	1		1	Cam [redacted]	
4	4	0	1	1	be an [redacted] athi	aw4U5GL2ZIAYkTFsuGquiuj8u83H2og==
5	5	0	1	1	video calling [redacted] u	QPLxqe7ClZbXrpgUJEDhLyh/WVcdPA==
6	6	1		1	Kem? [redacted]	
7	7	1		1	Me bij [redacted] thay	
8	8	1		1	Sent file	
9	9	0	1	1	nathi [redacted]	tdxNjZRMZXg1eFBtazcy8XGzzHsSGQ==
10	10	1		1	Hm w [redacted] dhi ar	

Figure 6: Chat Message history or Logs Along with automatic Hash generated by application for every message sent by the user.

Conclusion

The Forensic examination of Yahoo Mail and Yahoo Messenger were aimed at determining whether the operations performed by these applications leave any traces on the internal phone memory. The tests conducted provided valuable results that helped us to retrieve forensically vital artifacts such as Chat Logs, Contact list, login name, passwords (password only in Android 2.2). The tests results have been represented in a simplified manner for better understanding of the reader. The password retrieval was the most turning point of this paper as most Android phones store password in encrypted form or in token and not in simple text whereas in this, the password was retrieved in simple text. The artifacts discussed in the paper have tremendous potential to act as a source of evidence and provide valuable leads in a digital crime case. We hope that the paper provides a valuable insight to forensic examiners who deal with cases where Yahoo Mail and Yahoo Messenger are objects of interest.

References

1. Sridhar R, Iftekhar Husain M (2010) iForensics: Forensic Analysis of Instant Messaging on Smart Phones. Digital Forensics and Cyber Crime 31: 9-18.
2. Jansen W, Ayers R (2007) Guidelines on Cell Phone Forensics.
3. Yahoo Messenger for Android. Version: 1.8.3.
4. Yahoo Mail for Android. Version: 1.8.1.
5. Android Rooting.
6. Kumar K (2012) Significance of Hash Value Generation in Digital Forensic: A Case Study. International Journal of Engineering Research and Development.
7. Rose K (2009) Test Results for Mobile Device Acquisition Tool: Cellebrite UFED 1.1.05 by National Institute of Standards and Technology [NIST].
8. Holder EH, Leary ML, Laub JH (2012) Test Results for Mobile Device Acquisition Tool: CelleBrite UFED 1.1.8.6 -- Report Manager 1.8.3/UFED Physical Analyzer 2.3.0. National Institute of Standards and Technology [NIST].
9. de L Simao AM (2011) Acquisition of Digital Evidence in Android Smartphone.
10. Horesh N (2012) USB DEBUGGING Enable for Extraction.
11. Super one click, Android rooting tool.

12. UFED Touch Product Tour - File System Extraction.

13. Kessler GC, Lessard J (2010) Android Forensics: Simplifying Cell Phone Examinations 4: 1941-6164.