Identification of Fake SMS generated using Android Applications in Android Devices

Aditya Mahajan, Laxmikant Gudipaty, Dr. M. S. Dahiya

Abstract— Mobile phone forensic experts frequently come across forensic verification of SMS messages during investigations. The experts have to verify with the reports that whether the SMS messages or a particular SMS is present or not in the mobile phone. But mobile phones with Android OS (2.2.x Froyo, 2.3.x Ginger Bread and 4.0.x Ice-cream Sandwich) have the vulnerability of generating self-modified fake SMS from any fake Number, Name, text and time-Stamp. These Fake SMS can be Incoming as well as outgoing Fake SMS. So, if the SMS evidence is present on a mobile phone talking particularly about mobile phones with Android operating system versions 2.0.x , 2.3.x or 4.0.x , then a further forensic examination is must required to verify that whether the SMS present in the mobile phone is self-generated or self-modified fake SMS or not. This SMISHING vulnerability was reported to Google in November 2011.Therefore, with the objective to list-out the parameters which can forensically ascertain that the Incoming SMS in question is fake SMS or not, some examinations were conducted. In this paper, we have presented a way to identify those application based self-modified and self-generated Incoming SMS which can be faked in mobile phones with Android OS (versions 2.2.x Froyo, 2.3.x Ginger Bread and 4.0.x Ice-Cream Sandwich).

Index Terms—Android forensics, SMS forensics, FileSystem Extraction, SQLite database browser, Logical extraction, Mobile Devices.

1 INTRODUCTION

Mobile phone forensics is the process of collecting and analyzing the evidence which leads to a crucial role in cyber crime & forensic investigations. Among many sources of information in mobile phones, one is SMS. Also it is one of the most important information that is found in mobile phones is SMS. The total number of SMS sent & received per day in the world exceeds the total population of earth. So, SMS plays a very crucial

role to be presented as evidence in cyber crime investigations. Still a question arises that whether the SMS found as evidence is purely original or not and whether it is possible to generate self-modified fake SMS on a Android phones? Because of this SMISHING vulnerability [1] of generating self modified SMS, the answer automatically becomes "YES".

"Yes", it is possible to generate self-modified fake SMS and then another question arises that "How to forensically differentiate the self-generated and self-modified fake incoming SMS with the original & genuine incoming SMS?" So, in order to forensically examine and identify the self-generated and self-modified fake incoming SMS, we have to investigate SMS logs and the parameters in those logs.

2 FORENSIC EQUIPMENT & METHODOLOGY

Equipment and approach used in cyber investigations and research for extracting the data from the mobile phones should always be acceptable in court of law. If possible, NIST [National Institute of Standards & Technology] **[2]** approved instruments should be used. Forensically sound methodology for extraction of data should also be taken care of as it generates TimeStamp and hash values which play highly evidentiary value to prove the evidence in court of law. In this research, Mobile Hardware Extraction device "Cellebrite UFED (Universal Forensic Extraction Device v1.8.0.0)" **[3]** and software "UFED Physical Analyzer v3.6.1.6" were used for maintaining the integrity of the data and database files to be extracted from Android Devices. Maintaining Integrity of data prevents any kind of contamination on the device so as to get the device & evidence acceptable in court. Cellebrite UFED supports Physical, Filesystem & Logical extraction **[4]** of data from the mobile phones but FileSystem extractions should be conducted in order to analyze the data and database files. Cellebrite UFED v1.1.05 was tested successfully by NIST in January 2009 **[5]**, but in this research v1.8.0.0 was used. However, "XRY" from MicroSysmentation **[6]** and "AFLogical" from ForensicFocus **[7]** are other hardware and software which can also be used for extraction of SMS database file. "AFLogical" is an android application which needs to be installed on the Android Phone and can be used for extracting SMS, Call Logs and Contacts database files which contains all details along with TimeStamps and other parametric Values.

2.1 Hardware Equipments & Software's

Here Android phones are the potential sources of SMS and SMS logs. In this research, experiments were performed on 5 different Android phones covering 3 different versions of Android Operating systems **[8]**. Details of phones along with their versions are given in Table-1. Also, all the 5 phones were non-rooted Android phones. Hardware Extraction device used for extraction of data from Android Device is "Cellebrite UFED Classic Ultimate". "SUPER SMS FAKER (SSF)" &

- *Aditya Mahajan is currently pursuing masters degree program in Digital Forensics in Gujarat Forensic Sciences University, Gujarat.India. E-mail: adityamahajan3@gmail.com*
- *Laxmikant is also currently pursuing masters degree program in Digital Forensics in GFSU, Gujarat, India E-mail: laxmikant.gudiptay@gmail.com*
- *Dr.M.S. Dahiya is Current Deputy Director & Director at Directorate of Forensic Science, Gujarat State, Gujarat and Institute of Forensic Science, GFSU, Gujarat, India. E-mail: msdahiya49@rediffmail.com*

"LogMe" **[9, 10]** are the 2 android applications used for generating Fake Incoming SMS in Android devices and were also helpful for identifying parametric values of Fake SMS. These applications were downloaded and installed from Google Play Store. SQLite database browser **[11]** was used for analyzing the database (.db) files.

Table-1 List of Android Phones Tested

HTC A8181 Desire (Android 2.2 Froyo)
Samsung GT-S5830 Ace (Android 2.2.1 Froyo)
Sony Ericsson Xperia Neo V (Android 2.3.4 Ginger Bread)
Sony Ericsson Xperia Neo V (Android 4.0.4 Ice-Cream Sandwich)
Sony Ericsson Xperia ST 15i Mini (Android 4.0.4 Ice-Cream Sandwich)

2.2 Storage

For every SMS (Incoming, Outgoing, Saved) an entry is added to the "SMS" table of the database file "mmssms.db". This database file maintains the record of every SMS along with TimeStamps, phone numbers, SMS body, and many other values. The location of this database file on the phone is "/data/data/com.android.providers.telephony/databases/" **[12]**. However direct access to this folder is not available in non-rooted android phones.

2.3 Proposed Method

Firstly identify all the protocols which are common and identical in "SMS" table of the database file "smsmms.db" of all the Android phones. Out of those common protocols, again identify those protocols which cannot be altered or modified by the user or by using any application. Protocols
which distinguish between Incoming, Outgoing and draft saved Sms should also be identified. However, in this paper, following protocols were identified:

1. Protocols which identified and distinguished between incoming, outgoing and saved Sms.
2. Protocols which cannot be altered or modified by user or by any application.
3. Protocols which used to identify if a Fake SMS is generated by the user using some Android application.

2.4 Extraction Procedures

FileSystem extractions were carried out on every Android device using Cellebrite UFED Classic Ultimate. FileSystem extraction is an extraction procedure which acquires all the directories, database files, configuration files and all other files stored in the internal memory of the mobile phone. The extraction of SMS database file "mmssms.db" were carried out using UFED and android application "AFLogical" for verifying that the data extracted using both are same.

3 EXPERIMENTS AND RESULTS

In this section, we describe our experiments which were carried out on 5 different Android phones and present our results on identifying the Fake incoming SMS parameters and parametric values generated by some application or by the user using some Android Application.

3.1 Data Collection

A total of 5 Android phones containing more than 15000 SMS which had more than 9000 Incoming SMS were taken into consideration for analysis. In order to analyze SMS details, the "mmssms.db" database file was extracted from each of the Android phone. The location of the database file is"/data/data/com.android.providers.telephony/ databases/". The collection of database file of SMS was conducted through "FileSystem Extraction" using Hardware extraction device UFED from Cellebrite. Android Application "AFLogical" was also used for extraction of same database file for cross-verification of the data.

Steps for extracting data from UFED:

- Enable USB debugging option in settings menu of Android device.
- Connect Android device to UFED Source Port via USB.
- Select "FileSystem Extraction" option in UFED.
- Select Android phone model in UFED and press OK for extraction.

The files and folders will be extracted to the external USB drive attached to the UFED destination port.

Steps for Extracting "mmssms.db" file using "AFLogical":

- Download and Install "AFLogical" application from Google Play Store.
- Open application and check the SMS option.
- Click on Extract Button in the app.

The "smsmms.db" file will be extracted to the external memory card in ".csv" format.

Now "mmssms.db" database file was opened in SQLite database Browser and table "SMS" was selected. In all the 5 "mmssms.db" files extracted from 5 different phones, 5 parameters were found to be common in the "SMS" Table of the database file. Parameters were: "TYPE", "SERVICE CENTER NUMBER", "REPLY-PATH", "PROTOCOL" & "ADDRESS". However, out of these 5 parameters, first four (4) parameters were considered for identifying the Fake incoming SMS with the respective "Address/Mobile Number" which is the last parameter.

3.2 Classification of Genuine SMS parametric Values

This section describes the 4 parameters of an incoming SMS and their Genuine values in those parameters. The 4 parameters: "Type", "Service Center Number", "Reply-Path" and "Protocol" are taken into consideration from the "SMS" table of the database file "mmssms.db" from all 5 Android phones. Table No.2 shows the list of parameters with possible values.

The significance of the parametric values is discussed below:

Table 2: Possible values for 4 parameters of Genuine SMS in Android phones

Type	Service Center Number	Reply-Path Present	Protocol
-1, or 1, or 2, or 3	**Present (number starting with country code)**	**0 Or Empty**	**0, or 52, or 57, or any other numeric value**

Significance of Parameter – "Type" :

The parameter "TYPE" defines the type of SMS, whether Incoming, Outgoing or Saved Draft SMS. There can be one of the 4 possible values in the "TYPE" parameter for any SMS.

The 4 values are:

"-1", this value defines that the SMS is of OUTGOING TYPE but outgoing SMS to a group of people.

"1", this value defines that the SMS is of INCOMING TYPE.

"2", this value defines that the SMS is of OUTGOING TYPE [Outgoing to a single person].

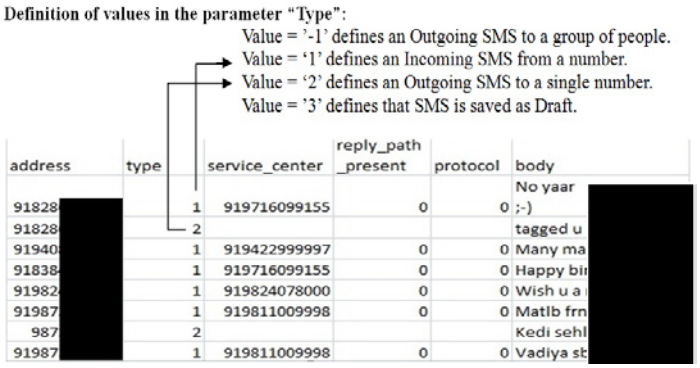
"3", this value defines that the SMS is SAVED AS DRAFT.

Picture No.1 shows the screenshot of data obtained from phone which clearly indicates the parametric values and their definitions.

Significance of Parameter – "Service Center Number":

This parameter describes the address of the service center which forwarded the SMS. The service center number returns the address of the service center that relayed the particular incoming SMS to the user's Android phone. This is a server generated value which cannot be altered or tampered and till now no application is capable of altering this value. Picture No.1 shows the Service center numbers starting the with country code "91" which is allotted by

Picture No.-1



Country, INDIA **[13]**. However the value in this parameter will be generated only for Incoming SMS only. No Service center number value will exist for outgoing or saved SMS.

Significance of Parameter – "Reply-Path":

This parameter returns value='0' only if this parameter is set to true by the service center or network provider. This value also cannot be altered or tampered by the user and till now no application is capable enough to tamper this network generated value. However the value in this parameter will be generated only for Incoming SMS only.

Significance of Parameter – "Protocol":

Protocol stands for protocol identifier. The value for protocol identifier will have at least some numerical value and cannot be empty and the value will be generated by network provider. The values can be '0', '52', '57' or any other numeric value **but not empty**. Picture No.1, the screenshot shows the protocol value='0'. However it will be generated only for Incoming SMS only. For outgoing SMS, it will be empty.

So, Parametric values for Genuine Incoming SMS;

- **Type="1";**
- **Service Center Number="should be Present, with number starting with country code";**
- **Reply Path="0" and;**
- **Protocol="0 or other Numeric value but not empty".**

3.3 Classification of Self or Application Generated FAKE SMS parametric Values Classification

This section describes that several SMS were sent, received and some were generated falsely using Android application "Super SMS Faker (ssf)" and "LogMe". These applications have the capability to generate Fake incoming and Fake Outgoing SMS from any Mobile number in Android phones. These applications also have the feature of generating Fake SMS with Fake Time-Stamps like Fake or modified Date, time and with any self-written text. So, after generating Fake Incoming SMS in all Android phones, FileSystem Extraction

were carried out again using Cellebrite UFED. Again "SMS" table of the file "mmssms.db" was analyzed from every phone. After analysis, some variations were found in the values of some parameters. The parameters showing variable values from the Genuine Values were "Service Center Number", "Reply-Path" and "Protocol". However, parameter "Type" was used to identify Incoming SMS.

According to the values found in 4 parameters of Genuine Incoming SMS, 3 parameters out of 4 are used for identification of self or application based generated Fake incoming SMS, and the 4th (Fourth) parameter is used to identify the Incoming SMS. Table-3 shows the difference between parametric values in Genuine and Fake Incoming SMS, so it cannot be different.

Table-3- Showing Parametric difference in values for Genuine and Fake SMS

Paramter SMS Type	Type	Service Center Number	Reply-Path	Protocol
Genuine	1	Present	0 or **Empty (in case of Android 2.3.X)**	0 or other numeric value but not empty
Fake	**1**	**EMPTY**	**EMPTY**	**EMPTY**

3.4 Version Wise Results of Genuine And Fake SMS Parametric Values

Genuine Incoming SMS Parametric Values

	Mobile phone Make & Model	Android Version	Type	Service Center Number	Reply Path	Protocol
Actual Incoming SMS with Values (Android Versions Tested)	HTC Desire , A8181	2.2 Froyo	1	**(present)**	0	0
	Samsung ACE GT-S5830	2.2.1 Froyo	1	**(present)**	0	0
	Sony Ericsson Xperia Neo V	2.3.4 Ginger-Bread	1	**(present)**	EMPTY	0
	Sony Ericsson Xperia Neo V	4.0.4 Ice-Cream Sandwich	1	**(present)**	0	0
	Sony Ericsson Xperia ST 15i Mini	4.0.4 Ice-Cream Sandwich	1	**(present)**	0	0

FAKE Incoming SMS Parametric Values

	Mobile phone Make & Model	Android Version	Type	Service Center Number	Reply Path	Protocol
Fake Incoming SMS with Values (Android Versions Tested)	HTC Desire A8181	2.2 Froyo	1	**Empty or Absent**	**empty**	**empty**
	Samsung ACE GT-S5830	2.2.1 Froyo	1	**Empty or Absent**	**empty**	**empty**
	Sony Ericsson Xperia Neo V	2.3.4 Ginger-Bread	1	**Empty or Absent**	**empty**	**empty**
	Sony Ericsson Xperia Neo V	4.0.4 Ice-Cream Sandwich	1	**Empty or Absent**	**empty**	**empty**
	Sony Ericsson Xperia ST 15i Mini	4.0.4 Ice-Cream Sandwich	1	**Empty or Absent**	**empty**	**empty**

This above difference in parametric values shown in table-3 was found in all the 3 Android operating systems tested and in all the 5 Android phones which were taken for analysis. However, the value in the "Type" parameter remains unchanged to "1", because the Fake SMS is of incoming TYPE, so for incoming SMS, "Type" parameter value will always be "1".

So, for Fake Incoming SMS;

- **Type="1";**
- **Service Center Number="Absent";**
- **Reply Path="Absent" and;**
- **Protocol="Absent".**

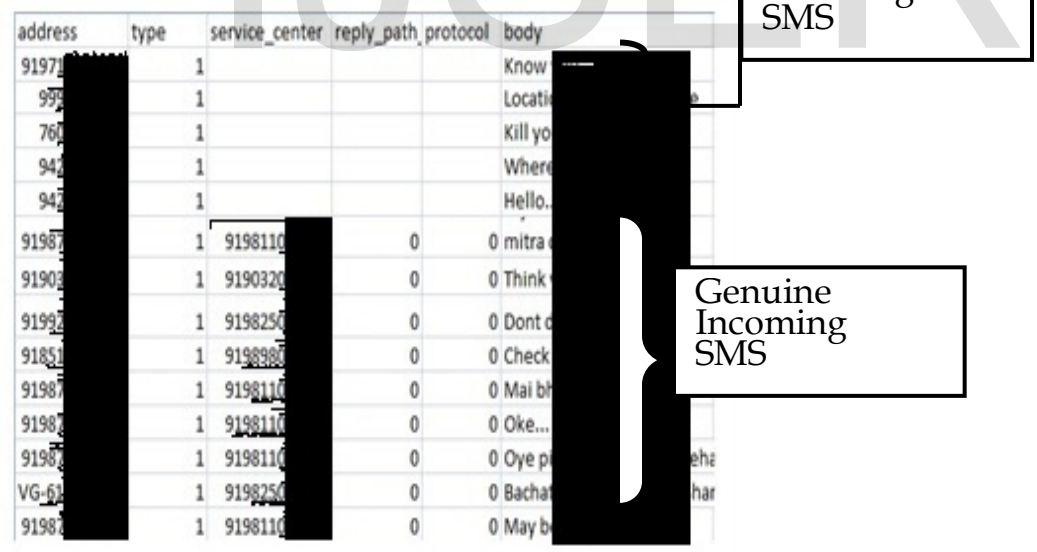
But It should be noted that In case of following situation:

- **Type="2";**
- **Service Center Number="Absent";**
- **Reply Path="Absent" and;**
- **Protocol="Absent"**

The SMS will not be considered Fake because the Value in "TYPE" parameter is "2", which signifies the SMS is of "OUTGOING" Type and is not an Incoming SMS.

Picture-2. Screenshot Showing Fake and Genuine SMS with Fake and Genuine Parametric Values. A Screenshot of Original Values taken from an Android phone.

S.No.	Type	Service Center Number	Reply Path	Protocol
1	1	Not Present	Not Present	Not Present



4 DISCUSSIONS

This research was carried out after the vulnerability of generating Fake SMS was discovered. This vulnerability exits in Android OS (Versions 2.0.x, 2.2.x, 2.3.x, and 4.0.x). Google was reported for this vulnerability in November 2011.

This research will directly benefit and help the investigating agencies, Police and cyber experts if any suspect tries to modify the SMS evidence on his or on any other Android phone by generating Fake SMS with Fake Time-Stamps, modified Fake text and with Modified Mobile Number. This will also be helpful in case if a suspect deleted an Original SMS evidence and generates the Fake SMS with time-stamps matching to Original SMS evidence (Evidence which was deleted), then investigators and cyber experts will be able to detect which SMS is modified and self-generated by the suspect.

In this paper, the parameters along with their Original as well Fake parametric values were identified for identifying the Fake incoming SMS which can be generated using applications like "Super SMS Faker (ssf)" and "LogMe".

5 CONCLUSION'

From section 3.2 and 3.3., we conclude that for Genuine Incoming SMS and for identifying Fake incoming SMS, the parametric values should be as per Table No.2.

So, in this paper, it was identified the fake SMS generated using Android applications and distinguished them from the Genuine SMS. This identification of Fake SMS will help the investigating Agencies and cyber experts if a suspect tries to tamper or modify the Original SMS evidence in Android phones by generating Fake incoming SMS matching with timsstamps of Original Incoming SMS. This will also help cyber experts to identify those Fake SMS which might had been generated through some malware application installed and present on the phone.

REFERENCES

[1] Smishing Vulnerability in Multiple Android Platforms (including Gingerbread, Ice Cream Sandwich, and Jelly Bean) By Xuxian Jiang, Associate Professor, Department of Computer Science,NC State University
Source:
http://www.csc.ncsu.edu/faculty/jiang/smishing.html

[2] Test Results for Mobile Device Acquisition Tool: Cellebrite UFED 1.1.05 by National Institute of Standards and Technology [NIST].
Source: http://www.ncjrs.gov/pdffiles1/nij/228220.pdf

[3] October 2012, Test Results for Mobile Device. Acquisition Tool: Celle Brite UFED 1.1.8.6 -- Report Manager 1.8.3/UFED Physical Analyzer 2.3.0 by National Institute of Standards and Technology [NIST].
Source:
http://ncjrs.gov/pdffiles1/nij/238993.pdf

[4] http://www.cellebrite.com/releases/Mar-2013/Release-Notes-UFED-1.8.6.0.pdf

[5] January 2009, Test Results for Mobile Device Acquisition Tool: Cellebrite UFED 1.1.05 by National Institute of Standards and Technology [NIST]. Source:
http://www.ncjrs.gov/pdffiles1/nij/228220.pdf

[6] Source is: http://www.msab.com/xry/xry-complete

[7] AFLogical Application:
Sources:
1. https://viaforensics.com/android-forensics/aflogical-open-source-edition-free-android-forensics-tooldownload.html
2.https://viaforensics.com/resources/tools/android-forensics-tool/

[8] Android OS versions:
http://en.wikipedia.org/wiki/Android_version_history

[9] Android Super SMS Faker Application.
Google Play Application Source:
https://play.google.com/store/apps/details?id=com.superdroid.ssf&hl=en

[10] Fake Call, SMS and Call Logs Application "Log Me"
Google Play Application Source:
https://play.google.com/store/apps/details?id=org.baole.fakelog&hl=en

[11] SQLite database browser, download source:
http://sqlitebrowser.sourceforge.net/

[12] SMS database file location in Android phones,
http://androidcommunity.com/forums/f4/data-file-storage-location-for-sms-messages-23299/

[13] List of Country calling codes:
http://en.wikipedia.org/wiki/List_of_country_calling_codes