eForensics Magazine

MAGAZINE

Social Media and Instant Message Forensics

Social Media Cloud Investigations

Forensic analysis of Dating Apps

WhatsApp Forensics

VOL.07 NO.08
ISSUE 08/2018 (85) AUGUST
ISSN 2300 6986

Bluetooth Attacks and Forensics Analysis

by Ummed Meel

Some people with bad intentions could misuse Bluetooth technology to steal data, spamming or sending a payload to hack a mobile device. A hacker can use well known hacking practices, like malware, direct attack or authentication bypass, to hack mobile devices. After the incident, an Incident Responder should seize digital evidences very carefully. Forensics experts can get the Bluetooth device ID, file name, pairing date, file size and path from the victim's device. A Bluetooth attack can happen to mobile, Bluetooth speaker, headphone, screen and laptop, etc. This article will give the complete idea about possible Bluetooth attacks, its forensics and tracing of culprit with practical moves.

Introduction

In the competitive market, mobile manufacturing companies are offering sophisticated applications to attract users. Mobile companies are facilitating users to fulfil their necessity of day to day life. Mobile technology is basically developed to talk with people remotely and share information. Data transfer was one of the primary objects or challenges for mobile companies in the early 90s. Initially, the data was transferred only by cable but later Bluetooth technology was invented by Dutch electrical engineer Jaap Haartsen, working for telecom vendor Ericsson in 1994. Bluetooth is a wireless technology standard for exchanging data over short distances. Consumers adopted this wireless data transfer technology globally and started using it in a very short time. This technology is

getting more popular among users because it does not require any internet data or telecom network to transfer data from device to device. The IEEE standardized Bluetooth as IEEE 802.15.1, but no longer maintains the standard.

Some people with bad intentions could misuse Bluetooth technology to steal data, spamming or sending a payload to hack a mobile device. A hacker can use well known hacking practices, like malware, direct attack or authentication bypass, to hack mobile devices. After the incident, an Incident Responder should seize digital evidences very carefully. Forensics experts can get the Bluetooth device ID, file name, pairing date, file size and path from the victim's device. A Bluetooth attack can happen to mobile, Bluetooth speaker, headphone, screen and laptop, etc. This article will give the complete idea about possible Bluetooth attacks, its forensics and tracing of culprit with practical moves.

Base of the article (Android)

Android is a mobile operating system developed by Google in 2005, based on a modified version of the Linux kernel and other open source software and designed primarily for touchscreen mobile devices such as smartphones and tablets. An Android phone has an open source operating system, which can be modified easily by a device manufacturer as per his requirement. It is very easy to develop custom applications and handle the Android platform.

The Android platform replaced the Java operating system rapidly in between 2010 to 2013. Most Android applications are down-loaded from the play store but users are allowed to develop and install customised application.

Attacks on mobile phones

A hacker can perform attack in two ways, either protected or unprotected. In the unprotected attack, the hacker does not require pairing with target device to exchange data. A protected attack needs to cross a few security levels for pairing with target device. In protected pairing, the target device is relatively safe so the attacker always needs partial interaction of the user (victim) to accept the pairing request.

The hacker can make attacks through the following techniques:

1. BlueBug

BlueBug is a technique in which intrusion can happen through a bug in the stack memory of Bluetooth. By using this vulnerability, a hacker can control the RFCOMM ports of a mobile device and send AT (attention terminal)

commands to the target as per his need. The hacker can exploit this vulnerability and, through AT commands, access Call Logs, Contacts, SMS and set call forwarding. The hacker can also make a call through Bluetooth on any number from the victim's device. An attacker can also add a number to the contact list and change the language.

2. BlueJacking

Normally, Bluetooth devices can share data after pairing but a hacker can perform spamming to engage a user's device or send payload for exploitation. But yes, this is also a question in itself that the spamming has occurred after the pairing or without the pairing. The hacker can perform unprotected pairing or, with the help of social engineering, the user can also accept a pairing request. A forensics investigator should first identify the pairing process to get the right direction of investigation because both protected and unprotected pairing have different directions to investigate.

3. BlueSnarfing

A general attack on Bluetooth is possible when a device is enabled to be viewed publicly or to allow pairing. A BlueSnarfing attack is only possible when the Bluetooth device is not active. A BlueSnarfing attack could give complete access of victim's call log, contacts, SMS, images, video and documents to the hacker. The only requirement of this attack is the MAC address of the target device. Through the MAC address, the hacker can gather much information about the target, like chip (first three bytes) and device manufacturer company name (last three bytes). Similarly, in the case of cyber-crime or attack investigation, an officer can also collect the same information about the hacker's device. Nowadays, with the updated version of Bluetooth, this vulnerability has been patched.

4. BluePrinting

BluePrinting is the technique used to gather information about the target Bluetooth device. This technique aims to collect information like device name, model, Bluetooth version and MAC address anonymously. This technique is called passive scanning because it does not require pairing or user interaction. Through several tools, you can search available Bluetooth devices in the network and gather information about them.

Forensics

A hacker can misuse Bluetooth technology to access a user's device through protected and unprotected connections. Sometimes, a hacker can exploit vulnerabilities in a Bluetooth

application and can steal the user's personal and confidential information. A hacker can also send malicious files to the victim device.

Bluetooth forensics is made in the following steps:

1. Device Seizure

At the incident location, the forensics expert should first complete the seizure memo carefully. The seizure memo includes evidence name, evidence type, model, operating system, other network devices, date and time of incident. The expert should make a detailed report for both software and hardware for the references during investigation.

2. Phone Rooting

To get access to the SQLite database of the Android device, we need root access. Rooting can give us the permission to replace, delete and access applications that require administrator permission. Rooting is also performed to overcome limitations on firmware and hardware of device. After the device rooting, we can get access to the SQLite database of Bluetooth device connectivity logs.

We can root the Android device in the following phases:

Step 01: Download and Install KingRoot apk

There are lots of freeware Android rooting applications available on the internet. We can also root the Android device from the computer by enabling the USB debugging. Here we will use KingRoot application to root the device. You can download and install the latest version of KingRoot application free from the internet.

Step 02: Enable developer mode

To root the Android device, KingRoot application requires developer mode enabled. Normally, developer mode is not visible on the devices. To make "developer mode" option visible, go to Settings > About Phone. Tap the "Build number" seven times to make Settings > Developer options available. Now go to developer mode and enable it as shown in figure 1.0.

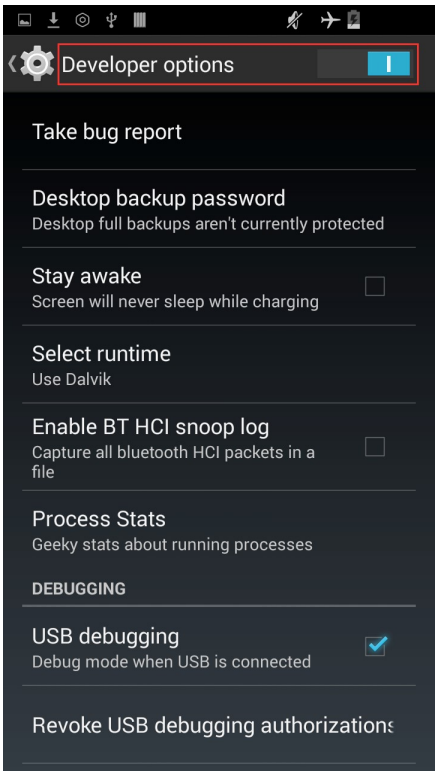
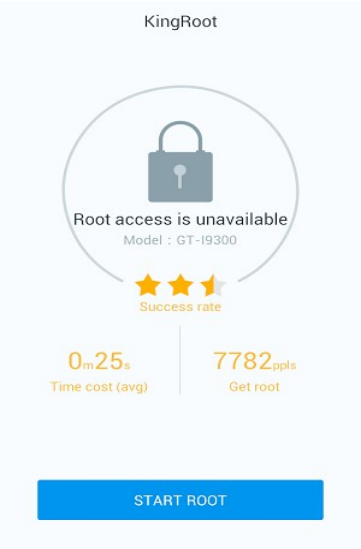


Fig (1.0): Enable Developer Mode

Step 03: Rooting

Open the KingRoot application and click on "Start Rooting" button. This process will take a few minutes to root the Android device. After completion, KingRoot will display a successful rooting message on screen.



Fig(1.1): Start Root

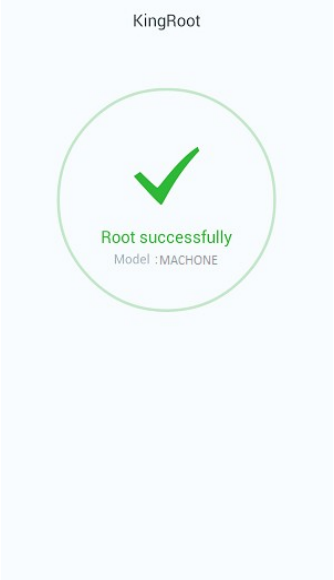


Fig (1.2): Successfully Rooted

Note: You can also across check rooting status of device by using root checker applications. Rooting checking application can also be downloaded from the play store. Here I use "Root Checker" application to verify the root status of device as shown in figure 1.3.

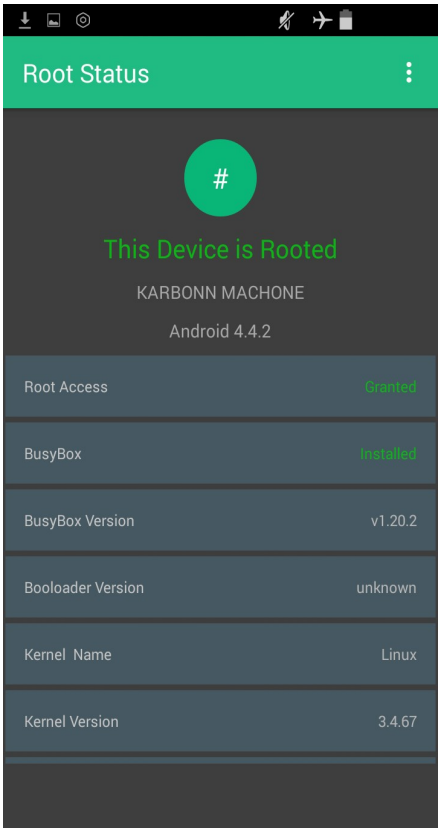
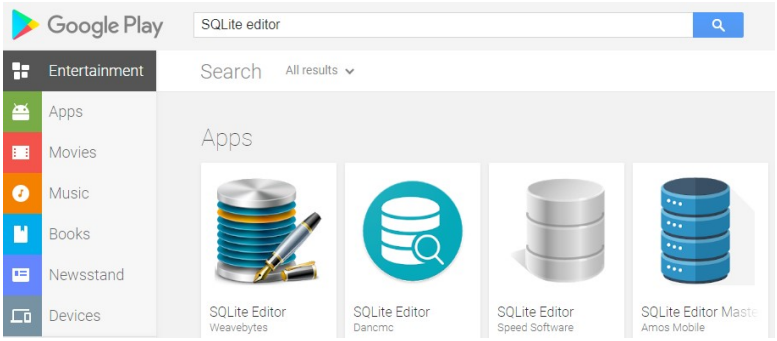


Fig (1.3) Root Status Verification

3. SQLite Editor

To check the Bluetooth connectivity and data transfer logs of a device, you need to analyse the SQLite database of the device. You should download and install "SQLite Editor" application from the play store. After that, you need to browse your application for which you want to

perform forensics. Download and install SQLite editor as shown in the figure below.



4. Logs Analysis

From the SQLite database of an Android device, forensics expert can gather information, like Bluetooth address of destination device, file name, file type, file size, transfer time, storage location. A forensics expert can get more details about device and chip manufacturer company name by using the Bluetooth address. An investigation officer can also search active Bluetooth devices near the incident location and should seize all suspected devices. After the forensics analysis, police can match the destination Bluetooth address with the suspect devices.

Step 01: First open SQLite editor application

Step 02: Now browse BT application to the SQLite editor

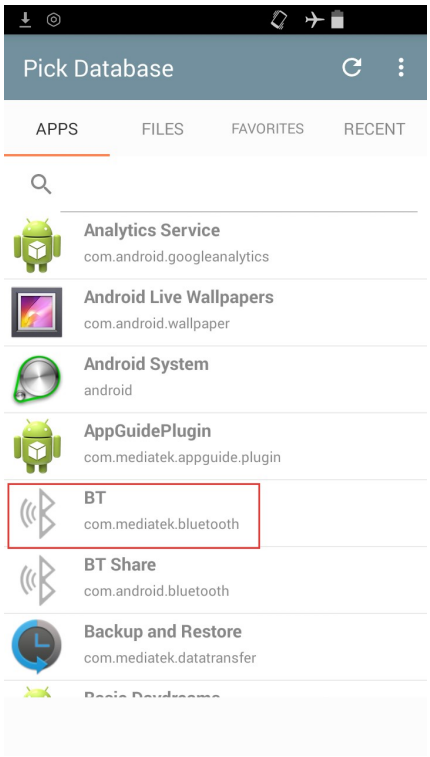


Fig (1.4) Choose BT database

Step 03: Now click on "RECENT" button

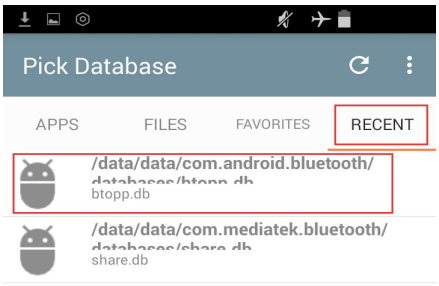


Fig (1.5) Select Database

Step 04: Now click on "btopp"

Here you will find SQLite database named "`/data/data/com.mediatek.bluetooth/database/btopp.db`". Click to open that database

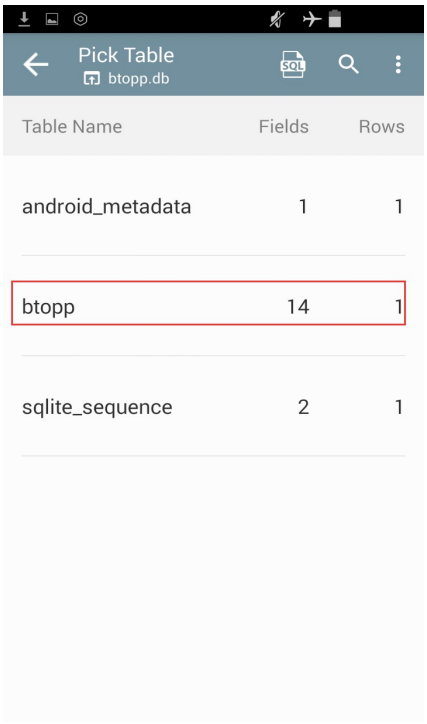


Fig (1.6) Click on btopp

Step 05: Information in the SQLite database

From this database, a forensics analyst can collect information such as Bluetooth address of destination device, file name, file type, file size, transfer time and storage location.

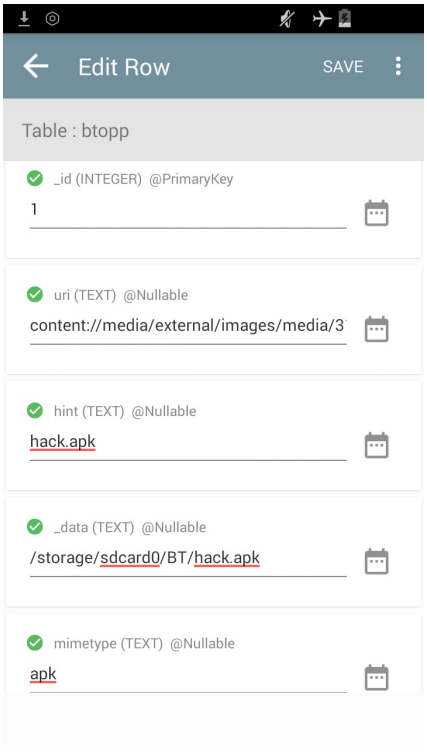


Fig (1.7.1) SQLite database

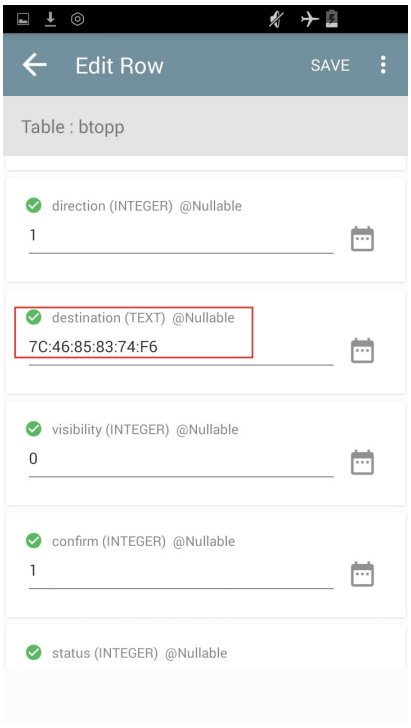


Fig (1.7.2) SQLite database

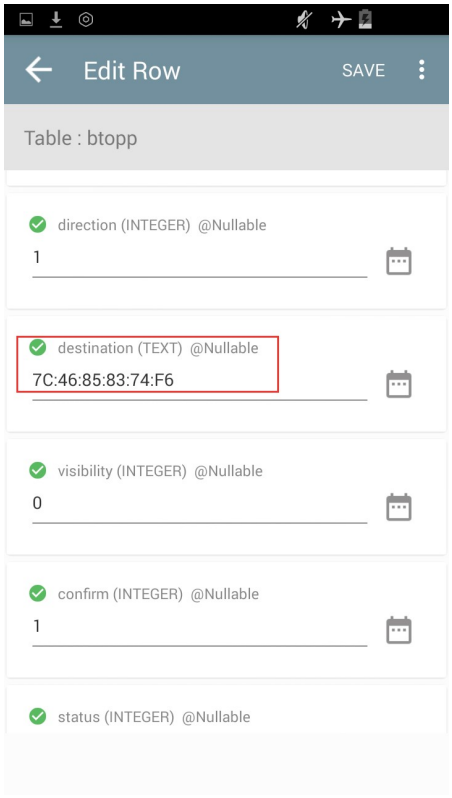


Fig (1.7.3) SQLite database

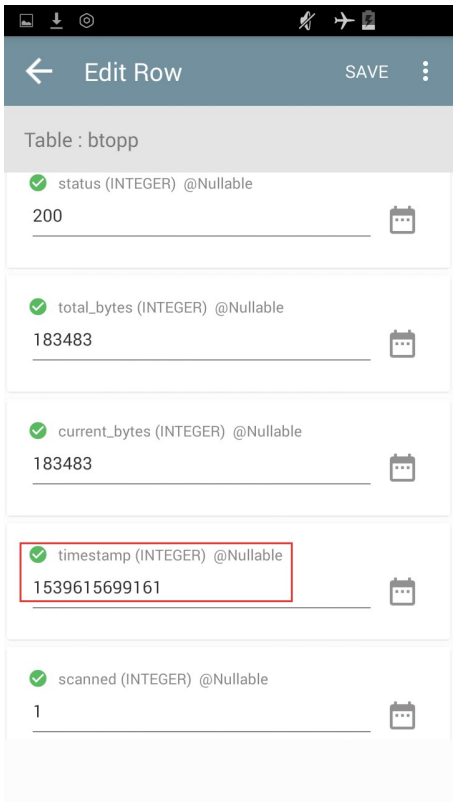


Fig (1.7.4) SQLite database

5. Device Info

The Bluetooth address is unique for every hardware manufacturer company. Through the Bluetooth address, a forensics analyst can gather many pieces of information about a target such as chip (first three bytes) and device manufacturer company name (last three bytes). There are lots of open source databases of Bluetooth addresses and websites to get the manufacturer name from the Bluetooth address.

We can get the device manufacturer name in following phases:

Step 01: Visit https://aruljohn.com/mac/7C4685 website

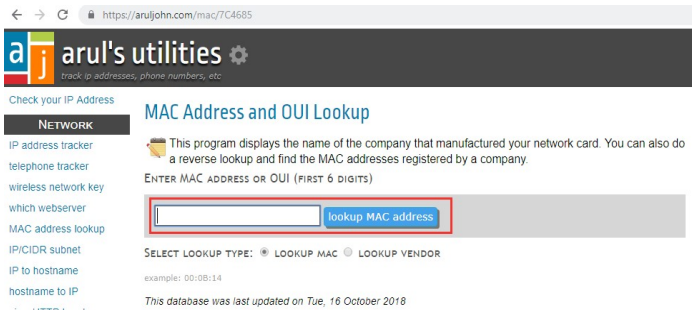


Fig (1.8) Visit Website

Step 02:

Search the first three bytes of your Bluetooth address on this website. Here you will get the device manufacturer name as shown in figure 1.9 below.

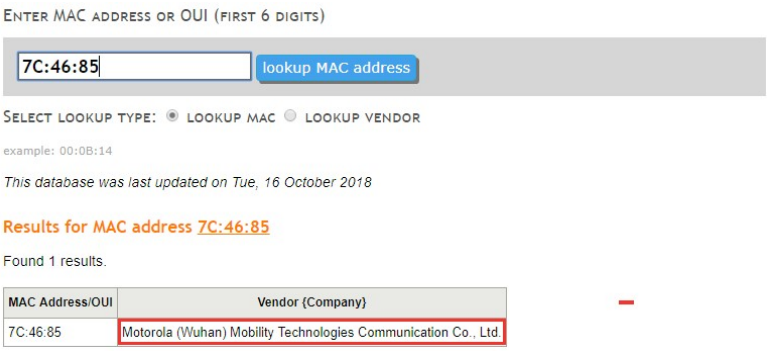


Fig (1.9) Search Bluetooth Address

Here you can see the device manufacturer vendor is Motorola Mobility Technologies Communication Co. Ltd.

Conclusion

In the above example, someone sent hack.apk file to a victim's device anonymously. A forensics officer visited the incident location and seized all suspected devices. During the forensics investigation, he found that the hack.apk file was sent through Bluetooth. Now the forensics officer wanted to get the sender's Bluetooth address and file transfer time. From the SQLite database, the forensics officer collected all required information. After that, you can match this Bluetooth address with the suspect device and catch the owner of the matched device. The forensics officer can also collect additional information such as file size, transfer data and time, file type, status of file transfer, etc.

About the Author

Ummed is closely associated with police, Air Force, BSF, and higher defence authorities in India for the last 5+ years. Ummed has conducted 50+ trainings and workshops for Indian Police and other LEA's. He has also conducted 40+ seminars for government/ non-government organizations, school, colleges and other law enforcement agencies on Cybercrime awareness.

He has 5+ years of experience in Cyber Security, Vulnerability Assessment and Penetration Testing, Cybercrime investigation, Digital Evidence seizure and Digital Forensics. He has been interviewed by several news channels, newspapers and magazines for Cyber Crime Safety and forensics.

Designation: Cyber Security Expert (Police and Defence Trainer)

Education: B Tech (ECE), CEH (EC-Council), Diploma in Cyber Law, LLB (Pursuing)