IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 7.12 ⁜ Vol. 9, Issue 11, November 2022

DOI: 10.17148/IARJSET.2022.91102

Data Acquisition Using Andriller and AF Logical

Aishwarya BS[1], Shreya Srinivas[2], Dhruva Anantha Prasad[3]

Student, Computer Science, PES University, Bangalore, India[1]

Student, Computer Science, PES University, Bangalore, India[2]

Student, Computer Science, PES University, Bangalore, India[3]

Abstract: Mobile phones are everywhere, and they hold a lot of information about the owner and their activities. As a result of the widespread adoption of these devices into every aspect of our lives, they will/mostly be involved in almost any crime that occurs/could occur. The aim of the digital forensics of mobiles is to recover potential digital evidence in a forensic manner so that it can be presented and accepted in court. There are various methods to acquire the evidence from mobile phones.

In this report, complete information about two data acquisition tools, Andriller and AF Logical is represented.

Keywords: data acquisition, andriller, aflogical, forensic tools

I. Introduction

The number of Android device users in the third quarter of 2012 is reported to be 181 million. This number represents approximately 75% of smartphone users. The evolution in consumer electronics especially mobiles has caused an exponential growth in the amount of mobile digital data(personal &public).

The majority of mobile phones has a built in camera and is able to record, store, play audio, and video data. Almost all of them have voice recorder which at all times is active. Some countries probably have more memory sticks than the inhabitants. A lot of this data is related to human behavior and might become subject of a forensic investigation in many cases these days

Andriller is software with a collection of forensic tools for smartphones/mobile phones. It performs read-only, forensically sound, non-destructive acquisition from Android phones. It has features, such as Lock screen cracking for Pattern, PIN, or Password; decoders for Apps data from Android, also IOS and Windows databases for decoding. Extraction and decoders produce reports in HTML and Excel formats and also ab files.

AF Logical is an Android forensics logical tool which is distributed free to law enforcement and government agencies. The app, developed by viaForensics. This tool extracts data using Content Providers, which are an important feature of the Android platform.

II. Forensic Process

A. Identification

It is the first step in the forensic process. The identification process includes things like what evidence is present, where it is stored, and how it is stored (in which format).

Electronic storage media can be personal computers, Mobile phones, PDAs, etc.

B. Preservation

In this step, data is isolated, secured, and preserved. It includes preventing people from using the digital device so that digital evidence is not tampered with.

C. Analysis

In this step, investigation agents use the fragments of data and draw conclusions based on evidence found. However, it might take many iterations of examination to support a crime theory.

D. Documentation

A record of all the visible data is created. This helps in recreating the crime scene and reviewing it. It involves proper documentation of the crime scene along with photographing, sketching etc

E. Presentation

This is the last step. Here the case is summarized, and a conclusion is drawn.

III. ANDRILLER

Andriller is software with a collection of forensic tools for smartphones/mobile phones. It performs read-only, forensically sound, non-destructive acquisition from Android phones. It has features, such as Lock screen cracking for Pattern, PIN, or Password; decoders for Apps data from Android, also IOS and Windows databases for decoding. Extraction and decoders produce reports in HTML and Excel formats and also ab files.

A. Features

- Automated data decoding and extraction.
- Data extraction for non-rooted without devices can be done by Android Backup.
- Screen can be captured (device display)
- Lock screen cracking – PIN, Pattern.
- Selection of individual database decoders for Android and Apple.
- Decryption of encrypted WhatsApp archived databases
- Data parsing and decoding for Folder structure, Tarball files and android backup.

B. Database Decoders

- Database decoders helps in importing individual App database files for automated parsing of the data.
- There are decoders for many Android and Apple IOS apps.
- Once the decoding is finished, the reports will be shown on the web browser.
- Databases can be exported from mainstream forensic tools, such as XRY, UFED Cellebite, Oxygen Forensic, and imported into Andriller for individual decoding.
- The output of the Andriller is clear output data.

C. Data Extraction from Androids

Data extraction from Android is carried out very easily using Andriller.
The smartphone should be connected to the device with Andriller using USB cable.
After extracting, decoding the report will be available.

D. Data Parsing

FOLDER STRUCTURE: This will parse the folder structures from the android device and will produce Andriller style reports. These could be exports of filesystem from raw image files, or from 'adb pull /data' extractions, or unpacked '.tar' files content.

E. Reporting

After data extraction is done, the data is saved in the directory which we mention before the extraction process. The main index file is REPORT.html.
It will contain the summary of the device examined and will also list the data which is extracted.
From here we can navigate to any data that is extracted like SMS, call history, location, gallery images etc.

IV. TOOLS

Andriller is a free software which is not only used for data extraction but also decoding and cracking passwords, pins and patterns.
Some of the tools are:
Lock screens Decoding
Andriller has the means of decoding pattern locks, and cracking PIN codes and passwords.
Password, pin and pattern cracking needs more processing power.
The method is: Choose Get Salt From...
(Salt is an integer value which is required to crack the lock screens. The salt value can be both negative as well as positive.)
This value can be obtained by parsing files- setting.db or locksettings.db.

DOI: 10.17148/IARJSET.2022.91102

When the files is fetched successfully, the salt value will be printed on the terminal.

A. Gesture Pattern Decoding

The steps involved in decoding Pattern lock are:

- Click and select the gesture.key file located at /data/system/gesture.key on the Android device.
- Or submit the gesture pattern hash (hexadecimal string of the gesture.key file) and click [Decode].
- When decode is done, the pattern will be shown as a sequence list. When Pattern is filled, click [Draw] and the pattern displayed in a visualized form.
- Right-click on the drawn pattern to save is as a PostScrip file.

B. Pin Code Cracking

Using Andriller, PIN can be decoded very easily.
The steps to crack a PIN code are:

- Select start and max value of the PIN code. By default, the max value is set to 9999, increase if necessary.
- Enter the password.key value
- Enter the salt value (Should be an integer)
- Click on START to begin the cracking of the pin.

After these steps, a percent progress will be displayed.
Andriller also has Samsung cracking of the pin, as Samsung uses different type of password hashing compared to other android devices.

C. Lock Screen Password Cracking

Using Andriller, even the passwords can be decoded.
The steps involved are:

- Click on browse and select a word list file.
- Enter the value of password.key file
- Enter the salt value (as an integer)
- Click on START to begin decoding.

Once Start is clicked, tried password will be displayed while cracking.You can pause and resume cracking at any time, just like with PIN cracking. Also includes Samsung cracking, which uses different type of password hashing than other Android vendors.

D. Lock Screen Password Brute Force

Password can be cracked by brute force method too.
The steps involved are:

- Set the minimum length of the password.
- Select characters believed to have been used in the password. Select combinations of lower/upper case characters, digits, or custom characters.
- Enter the password.key file value.
- Enter the salt value(as an integer)
- Click on START to begin decoding.

This method cannot be resumed or paused like other methods..

E. Decrypt Encrypted Database

Andriller allows decryption of encrypted WhatsApp databases:

- msgstore.db.crypt
- msgstore.db.crypt5
- msgstore.db.crypt7
- msgstore.db.crypt8
- msgstore.db.crypt9
- msgstore.db.crypt10
- msgstore.db.crypt12

Plain Crypt (msgstore.db.crypt) The encrypted database is automatically decrypted into an SQLite3 database. Step Browse and select the encrypted file, Andriller will decode to a new file in the same directory.
msgstore.db.crypt ==> msgstore.db

Crypt5 (msgstore.db.crypt5) To successfully decrypt this type of database, an email address is required, which is synchronised with the Android device. So,Browse and select the encrypted file, then we have to to enter the email address. Once successful, it will decode to a new file in the same directory.
msgstore.db.crypt5 ==> msgstore.db

Crypt7-12 (msgstore.db.crypt7-12) To successfully decrypt this type of database, an encryption key file is required for the following location: '/data/data/com.whatsapp/files/key' <-- absolute path 'apps/com.whatsapp/f/key' <-- from Android backup This file should be automatically extracted during normal Andriller extraction (root and AB), and saved in the 'db' folder of the extraction
Browse and select the encrypted file, you will be prompted to browse and select the key file next. Once successful, it will decode to a new file in the same directory.
msgstore.db.crypt7 ==> msgstore.db

F. Decode and Merge Multiple Database

Facebook This utility will decode multiple Facebook databases and produce combined messages on one report (without duplicates). This is useful if attempting to combine "threads_db2" databases from com.facebook.katana and com.facebook.orca applications directories.
WhatsApp This utility will decode multiple WhatsApp databases and produce combined messages on one report (without duplicates). Use recovered (from /data/data/com.whatsapp) and decrypted backup databases (such as decrypted msgstore.db.crypt8 from /sdcard/WhatsApp/Databases).

G. Conversion Tools

Andriller has a feature to unpack Android backup files from Android versions 4.x and above. **AB to TAR** Converts backup.ab file to Tarball.
backup.ab ==> backup.ab.tar
AB to folder Converts and extracts backup.ab to a folder.
backup.ab ==> backup.ab_extracted/

H. Screen Record / Capture

New Feature for Andriller - take screen captures. Supports Android devices version 4.x and above. Screen captures are saved at same resolution that the device display supports. Generate a report from taken screen captures. Add notes to taken captures.

V. STEPS

Steps for data acquisition using Andriller :-
Pre – requisites

- A suitable version of Andriller downloaded
- An android device Which is on USB debugging and revoke USB debugging authorisations.

Steps for data acquisition:-

1. Install the andriller version from their github or website
2. Connect the android device to the PC
3. Open the andriller tool
4. First enter the output directory location
5. Click on check button to search for suitable device connected
6. Check the boxes “use AB method” and “extract shared data”
7. Click on extract
8. Extracted data can be located on the output directory
9. The output directory contains .ab file called as backup.AB
10. Go to the andriller tool and click on PARSE .ab
11. On doing so we get all the data

DOI: 10.17148/IARJSET.2022.91102

Steps for cracking lockscreen
Files required

- Password.key
- Gesture.key
- Salt integer

These files will be located under the location

- /data/system/password.key under the extracted data

the salt, which is stored in a SQLite database under the lockscreen.password_salt key.

Which is under
/data/data/com.android.providers.settings/databases and is called settings.db
And by keying in the right keys under each lock screen, the lock screen can be cracked
Andriller can be used for acquisition of the following types of data;

- A general report about the device
- Android version
- Account
- Local time
- Wifi mac
- Model
- Serial no
- Wifi passwords
- Download history
- Communication data
- App data like calenders
- Sms snippets
- Call history
- Contacts
- Whatsapp data
- Facebook data

Recently facebook and whatsapp added a new layer of privacy which has made it difficult to acquire data from android devices using tools such as Andriller
In devices which are not rooted andriller can extract only basic data like

- A general report about the device
- Android version
- Account
- Local time
- Wifi mac
- Model
- Serial no
- Calender info

But in devices that are rooted all the information can be extracted and will be stored in our preferred directory
Andriller apart from extracting information can also be used for cracking lock screens

- Gesture Pattern
- Pin cracking
- Password by dictionary

Password by brute force

- Pin (Samsung)
- Pattern(Samsung)

For cracking the following lock screen following files need to be extracted from the devices which can be done by parsing. AB files where we get the keys under settings.db / lockscreen.db which are under data / settings folder

- Gesture pattern – gesture key and salt integer
- Pin cracking – salt integer and password.key
- Password – salt integer
- Pin – salt and password.key
- Pattern – gesture.key and password.key

VI. DISADVANTAGES

- All the data contained in the phone cannot be extracted. Especially some messaging apps which are more secure.
- Cannot extract deleted messages.
- USB debugging should be done before extraction
- Too much information which is not required to the purpose is given out. So may be used illegally.

VII. AFLOGICAL

AF Logical is an open-source Android Forensic Tool released for the use for non-law enforcement.

Using this tool, call logs, contact phones, MMS messages, SMS messages can be extracted from the device.

A. Usage

- To extract data from the Android phone, AF Logical OSE application must be installed.
- After opening the AF Logical OSE application, we need to choose the data that we need to extract, then follow the prompts to complete the extraction of the data.
- The selected data will now be extracted to the SD card, either internal or external.
- To view the data extracted, it can be copied to the computer from the SD card by either connecting it to the computer or by using adb pull.
- The extracted data will be in
- ~/Desktop/AFLogical_Phone_Data directory.

B. Data Extracted Using AFLogical

- Contact
- SMS
- Device Info
- Call Logs
- MMS
- MMS parts

C. Steps – Santoku Linux

- The mobile device from which the data needs to be extracted should be enabled for USB debugging.
  (Settings -> Developer Options)
- Then the mobile is connected to the computer using santoku Linux in Virtual Box.
  (Devices -> USB Devices -> Mobile Device name)
- Next step is to open File Manager in Santoku Linuxafter revealing the interface, and then the mobile files is copied manually to the Santoku Linux or to the host machine.
- In the Santoku Linux Virtual Machine => Device Forensics => AFLogical OSE command

prompt, the command (sudo adb devices) was used to show the serial number of the mobile device before typing the command (adb reboot bootloader) to reboot the mobile device into recovery mode.

After the above steps are completed, the device will be rebooted and will start again after it successfully unlocks.
How AFlogical and andriller are different from each other

- AFlogical APk is installed to the user’s device
- AFlogical doesn't need USB debugging and rooting
- data extracted is stored in user device

- data is extracted very easily in a fraction of a second

Whereas in Andriller

- data is extracted by connecting it to the pc
- data is stored in pc
- usb debugging and rooting is most essential
- Lock screen can also be unlocked

VIII. CONSTRAINTS

collection and extraction of data using andriller is possible only assuming the mobile phones are

1. On USB debugging mode
2. Devices are ROOTed

- Hence it makes it difficult for them to extract data if the devices are not in this state, also now a days the devices are locked securely using lock screens.

These lock screens can be cracked using Andriller, but it required the key files which can be accessed

- provides the data is extracted from the phones but again it is a challenge because this required turning on USB debugging and rooting the device by doing these changes in the phone requires access to phone first.
- Although the problem of rooting can be solved by AFlogical OSE, but installation of app can’t be done without having cracked the screen lock
- Andriller works with just USB debugging also but the data acquired is not very useful, rooting the device makes it more accurate and effective in extracting data.

Hence these 2 factors have a huge dependency on USB debugging because without that both become useless and cannot be used.

Since there were 2 major dependencies we had in this project when we used Andriller and AFlogical OSE

Although when using AFlogical OSE neither of USB debugging nor Rooting was required, a major problem we had to tackle was lock screen because installing App required access to phone but the data we extracted was very quick, easy, and efficient

while using Andriller we had to turn on USB debugging and crack the lock screen in order to have access to device settings, we could retrieve data using just this but most effective data like SMS, MMS , call logs etc were retrieved only when the device was rooted

Extraction of mobile data using Andriller and AFlogical OSE tools

These are the tools we have planned on using, the reason why we are using is

- It is easy to use
- It extracts large amount of data in a short span of time
- It extracts necessary data from a large domain using keywords
- It manages to extract all the necessary data that we require
- Even deleted and erased data can be retrieved
- Cost effective
- Can be used on all devices irrespective of version of device

IX. CONCLUSION

Doing data acquisition by technical methods is very challenging. The forensic tools, Andriller and AF Logical makes the process easier and saves time and has more accurate results.

Before the extraction of data from any device it is very important to understand the Android Architecture, forensic process and tools.

Both Andriller and AF Logical are highly effective tools by which all the information can be extracted from the phones (including location).

Data acquisition has been a huge success in forensic examination of electronic system has undoubtedly been a huge help in the identification of cyber and computer assisted crimes.

DOI: 10.17148/IARJSET.2022.91102

The aim of the digital forensics of mobiles is to recover potential digital evidence in a forensic manner so that it can be presented and accepted in court, and this can be achieved with forensic tools like Andriller and AF Logical.

ACKNOWLEDGMENT

We'd like to thank PES University and ISFCR for providing us an opportunity to work on this project.
We perceive this opportunity as a big milestone in our educational development. We will strive to use gained knowledge in the best way possible and will continue to improve our skills.

REFERENCES

[1]. User Manual – Andriller
https://www.andriller.com/manual/
[2]. AF Logical OSE Forensics Tool – Git Hub
https://github.com/viaforensics/android-forensics/downloads
[3]. Practical Cyber Forensics
(An Incident Based Approach to Forensic Investigations)
-Niranjan Reddy