FORENSIC ANALYSIS OF DIGITAL EVIDENCE FROM ANDROID DEVICES

A

DISSERTATION SUBMITTED TO

GUJARAT UNIVERSITY

FOR

THE DEGREE OF

MASTER OF SCIENCE

IN

FORENSIC SCIENCE

BY

PARTH LAKHLANI

DEPARTMENT OF FORENSIC SCIENCE

SCHOOL OF SCIENCES

GUJARAT UNIVERSITY

AHMEDABAD-380009

INDIA

APRIL-2016

FORENSIC ANALYSIS OF DIGITAL EVIDENCE FROM ANDROID DEVICES

BY

PARTH LAKHLANI

DEPARTMENT OF FORENSIC SCIENCE

SCHOOL OF SCIENCES

GUJARAT UNIVERSITY

AHMEDABAD-380009

INDIA

APRIL-2016

DEPARTMENT OF FORENSIC SCIENCE,

SCHOOL OF SCIENCES, GUJARAT UNIVERSITY,

AHMEDABAD – 380009,

INDIA

CERTIFICATE

This is to certify that **Mr. Parth Lakhlani** worked under my guidance during the Fourth Semester from February to April, 2016 for his dissertation entitled

"FORENSIC ANALYSIS OF DIGITAL EVIDENCE FROM ANDROID DEVICES"

The dissertation submitted here is the outcome of the above mentioned work which is original and has not been submitted for any diploma or degree of this university or any other university.

Dr. Priyanka Sharma,

Professor in IT,

Raxa Shakti University,

Ahmedabad, Gujarat.

DEPARTMENT OF FORENSIC SCIENCE,

SCHOOL OF SCIENCES, GUJARAT UNIVERSITY,

AHMEDABAD – 380009,

INDIA

CERTIFICATE

This is to certify that **Mr. Parth Lakhlani** worked for his dissertation in M.Sc. Forensic Science as a bonafide student in the Forensic Science, Department of forensic science, School of science, Gujarat University, Ahmedabad-380009, during the fourth semester from February to April 2016.

Prof. (Mrs.) Shobhana K. Menon,
Hon, Coordinator,
Department of Forensic Science,
School of Science, Gujarat University,
Ahmedabad-380009, India.

ABSTRACT

Android operating system for mobile phones is rapidly gaining market, with billions of smart phones, tablets and other devices. Digital forensic investigators have an increasing need to examine android device memory. In this dissertation, I present the methodology and toolset for acquisition and deep analysis of volatile and non volatile memory of Android devices. The aim of this dissertation is to contribute as knowledge base and technique sharing to cyber investigator from forensic perspective.

ACKNOWLEDGEMENTS

Man's quest for knowledge never ends. Theory and practice are essential and complimentary to each other. I am thankful for the assistance receiver from various individuals in making this project a successful.

My sincere thanks to the fine people around me who helped me in completing this project work. Their wisdom, clarity of thought and support motivated me bring this project to its present state. First, I wish to thanks Dr. Shobhana K. Menon, Head of the Dept., Forensic Science, Gujarat University, Ahmedabad for her constant efforts and perpetual patience throughout the dissertation work. The Direction and inspirations helpful me always.

My heartfelt thanks go to, Dr. Priyanka Sharma, Professor in IT, Raxa Shakti University, Ahmedabad and Bhadreshsinh Gohil, Asst. Professor, GTU PG school, Gandhinagar for their invaluable guidance and opportunity to work on this project in at Raxa Shakti Univesity. The continued support, guidance and vision have helped me in this project and it has truly been a pleasure working with them.

My special thanks to, Mr. Nishant Bhatt, Computer expert, Digital marketer and social media analyzer at Aaryavrat for their invaluable guidance, which not only enabled me to sort out the technical issues but also helped me in updating my knowledge.

I wish to express my deep gratitude towards Mr. Kapil Kumar and all Ph. D. students at Dept. of Forensic Science, Gujarat University, Ahmedabad who taught the fundamental essentials to undertake such a project. Without their valuable guidance it would have been extremely difficult to grasp and visualize the project theoretically.

Finally, I would like to thank my parents, my Sister and all my Classmates for their constant love and support for providing me with the opportunity and the encouragement to pursue my goals.

Parth Lakhalani

CONTENT

CHAPTER 1

AIM AND SCOPE

AIM

Forensic analysis of digital evidence from Android devices.

SCOPE

Nowadays Android devices have largest market all around the world. Due to open source market the misuse of these devices are increasing day by day. Aim of this project is to contribute knowledge of memory acquisition tools and software to forensic investigator from forensic perspective.

The study only limits to find out evidence of activities on android devices.

CHAPTER 2

INTRODUCTION

INTRODUCTION

2.1 Digital Forensic

Digital forensics also known as digital forensic science) is a branch of forensic science encompassing the recovery and investigation of material found in digital devices, often in relation to computer crime. The term digital forensics was originally used as a synonym for computer forensics but has expanded to cover investigation of all devices capable of storing digital data.

The technical aspect of an investigation is divided into several sub-branches, relating to the type of digital devices involved.

- Computer forensics
- Network forensics
- Forensic data analysis
- **Mobile device forensics**

The typical forensic process encompasses the seizure, forensic imaging (acquisition) and analysis of digital media and the production of a report into collected evidence.

2.2 Mobile Device Forensic

Mobile device forensics is a branch of digital forensics relating to recovery of digital evidence or data from a mobile device under forensically sound condition. The phrase mobile device usually refers to mobile phones. It can also relate to any digital device that has both internal memory and communication ability, including PDA devices, GPS devices and tablet computers.

The use of phones in crime was widely recognized for some years, but the forensic study of mobile devices is a relatively new field, dating from the early 2000s. A proliferation of phones (particularly smart phones) on the consumer market caused a demand for forensic examination of the devices, which could not be met by existing computer forensics techniques.

Mobile devices can be used to save several types of personal information such as contacts, photos, calendars and notes, SMS and MMS messages. Smart phones may additionally contain video, email, web browsing information, location information, and social networking messages and contacts.

There is growing need for mobile forensics due to several reasons and some of the prominent reasons are:

- Use of mobile phones to store and transmit personal and corporate information
- Use of mobile phones in online transactions
- Law enforcement, criminals and mobile phone devices

Mobile device forensics can be particularly challenging on a number of levels.

2.3 Android

Android is a mobile operating system (OS) currently developed by Google, based on the Linux kernel and designed primarily for touch screen mobile devices such as smart phones and tablets. Android's user interface is mainly based on direct manipulation, using touch gestures that loosely correspond to real-world actions, such as swiping, tapping and pinching, to manipulate on-screen objects, along with a virtual key board for text input. In addition to touch screen devices, Google has further developed Android TV for televisions, Android Auto for cars and Android Wear for wrist watches, each with a specialized user interface. Variants of Android are also used on notebooks, game consoles, digital cameras, and other electronics.

Android has the largest installed base of all operating systems of any kind. Android has been the best selling OS on tablets since 2013, and on smart phones it is dominant by any metric.

Initially developed by Android Inc., which Google bought in 2005, Android was unveiled in 2007, along with the founding of the Open Handset Alliance – a consortium of hardware, software, and telecommunication companies devoted to advancing open standards for mobile devices. As of July 2013, the Google Playstore has had over one million Android applications ("apps") published, and over 50 billion applications downloaded. An April–May 2013 survey of mobile application developers found that 71% of developers create applications for Android, and a 2015 survey found that 40% of full-time professional developers see Android as their priority target platform, which is comparable to Apple's iOS on 37% with both platforms far above others. At Google I/O 2014, the company revealed that there were over one billion active monthly Android users, up from 538 million in June 2013.

Android's source code is released by Google under open source licenses, although most Android devices ultimately ship with a combination of open source and proprietary software, including proprietary software required for accessing Google services. Android is popular with technology companies that require a ready-made, low-cost and customizable operating system for high-tech devices. Its open nature has encouraged a large community of developers and enthusiasts to use the open-source code as a foundation for community-driven projects, which add new features for advanced users or bring Android to devices originally shipped with other operating systems. At the same time, as Android has no centralized update system most Android devices fail to receive security updates: research in 2015 concluded that almost 90% of Android phones in use had known but unpatched security vulnerabilities due to lack of updates and support. The success of Android has made it a target for patent litigation as part of the so-called "smartphone wars" between technology companies.

2.4 Android Memory Forensic

Android Memory forensics is forensic analysis of a android device's memory. Its primary application is investigation of data leaving data on the Android's memory. The leaving memory must be analyzed for forensic information.

Android memory refers to the android devices used to store information for immediate use. Android memory can be categorized into two different types.

2.4.1 Non-volatile Memory

Non-volatile memory (NVM) is a type of memory that has the capability to hold saved data even if the power is turned off. Nonvolatile does not require its memory data to be periodically refreshed. It is commonly used for secondary storage or long-term consistent storage.

Non-volatile memory is highly popular among digital media; it is widely used in memory chips for USB memory sticks and digital cameras. Non-volatile memory eradicates the need for relatively slow types of secondary storage systems, including hard disks. Non-volatile memory is also known as non-volatile storage.

Non-volatile data storage can be classified into two types:

- Mechanically addressed systems
- Electrically addressed systems

Mechanically addressed systems make use of a contact structure to write and read on a selected storage medium. The amount of data stored this way is much larger than what's possible in electrically addressed systems. A few examples of mechanically addressed systems are optical disks, hard disks, holographic memory and magnetic tapes.

Electrically addressed systems are categorized based on the write mechanism. They are costly but faster than mechanically addressed systems, which are affordable but slow. A few examples of electrically addressed systems are flash memory, FRAM and MRAM.

Some examples of NVM include:

- All types of read-only memory
- Flash memory
- Most of the magnetic storage devices, such as hard disks, magnetic tape and floppy disks
- Earlier computer storage solutions, including punched cards and paper tape
- Optical disks

2.4.2 Volatile Memory

Volatile storage is a type of computer memory that needs power to preserve stored data. If the computer is switched off, anything stored in the volatile memory is removed or deleted.

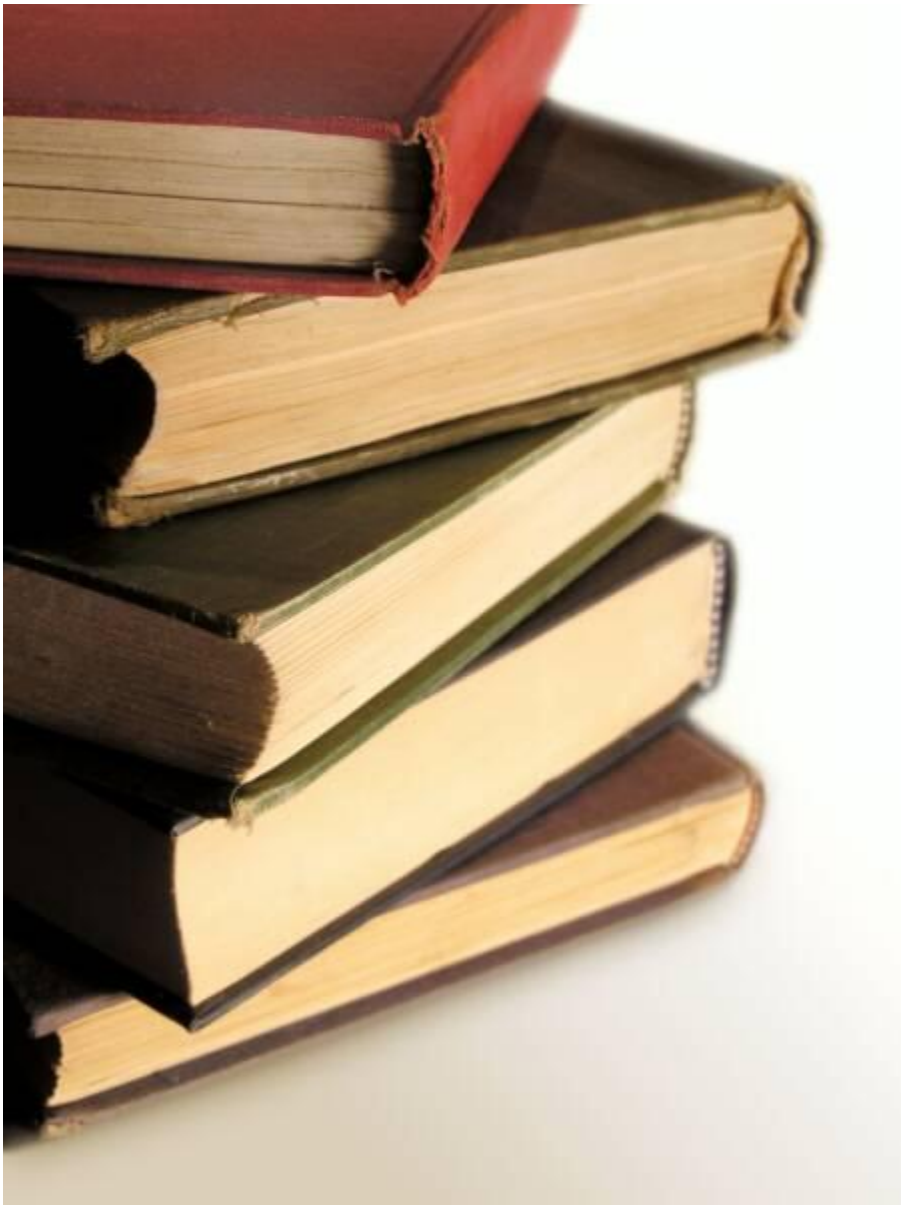
All random access memory (RAM) other than the CMOS RAM used in the BIOS is volatile. RAM is typically used as a primary storage or main memory in computer systems. Since the primary storage demands extreme speed, it mainly uses volatile memory. Due to the volatile nature of RAM, users often need to save their work to a nonvolatile permanent medium, such as a hard drive, in order to avoid data loss. Volatile storage is also known as volatile memory or temporary memory.

The physical structure and electronic properties of volatile memory makes it faster compared to electro-mechanical storage devices such as hard drives, which makes it an ideal candidate as the computer's main form of memory.

In terms of security, volatile memory is very secure since it does not retain any record at all after power is removed, so no data can be salvaged. However, this is a double-edged sword since all data is lost if there is power interruption.

CHAPTER 3

LITERATURE SURVEY



Literature Survey

1. Acquisition and analysis of volatile memory from android devices

By Joe Sylve
Journal of Digital Investigation
mailto:golden@cs.uno.edu

Abstract

The Android operating system for mobile phones, which is still relatively new, is rapidly gaining market share, with dozens of smart phones and tablets either released or set to be released. In this paper, we present the first methodology and toolset for acquisition and deep analysis of volatile physical memory from Android devices. The paper discusses some of the challenges in performing Android memory acquisition, discusses our new kernel module for dumping memory, named *dmd*, and specifically addresses the difficulties in developing device-independent acquisition tools. Our acquisition tool supports dumping memory to either the SD on the phone or via the network. We also present analysis of kernel structures using newly developed Volatility functionality. The results of this work illustrate the potential that deep memory analysis offers to digital forensics investigators.

2. A Novel Anti-Forensics Technique for the Android OS

By Pietro Albano,
pietro.albano@gmail.com
2011 International Conference on Broadband and Wireless Computing

Abstract

In recent years traditional mobile-phones, used only to make calls and send text messages, have evolved into even more versatile and powerful devices (smart phones, tablets, etc.). These devices use a NAND flash memory type to store data, due to it being a memory that has been optimized for the fast updating of data. These flash memory drives usually contain sensitive data that could be a possible danger to the user's privacy. This paper proposes a new anti-forensics technique for mobile devices with the Android OS. The technique makes it possible to modify and erase, securely and selectively, the digital evidence on an Android device without having to use any cryptographic primitives or make any file system changes. While the use of cryptographic primitives or changes to the file system create considerable suspicion in a forensic analysis, the proposed techniqueuses simple software tools commonly used in *nix-like OSes such as the Android OS.

3. Using Smart phones as a Proxy for Forensic Evidence contained in Cloud Storage Services

By George Grispos

g.grispos.1@research.gla.ac.uk

2013 46th Hawaii International Conference on System Sciences

Abstract

Cloud storage services such as Drop box, Box and Sugar Sync have been embraced by both individuals and organizations. This creates an environment that is potentially conducive to security breaches and malicious activities. The investigation of these cloud environments presents new challenges for the digital forensics community. It is anticipated that smartphone devices will retain data from these storage services. Hence, this research presents a preliminary investigation into the residual artifacts created on an iOS and Android device that has accessed a cloud storage service. The contribution of this paper is twofold. First, it provides an initial assessment on the extent to which cloud storage data is stored on these client-side devices. This view acts as a proxy for data stored in the cloud. Secondly, it provides documentation on the artifacts that could be useful in a digital forensics investigation of cloud services.

4. Towards a General Collection Methodology for Android Devices

By Timothy Vidas

tvidas@cmu.edu

Journal of Digital Investigation

Abstract

The Android platform has been deployed across a wide range of devices, predominately mobile phones, bringing unprecedented common software features to a diverse set of devices independent of carrier and manufacturer. Modern digital forensics processes differentiate collection and analysis, with collection ideally only occurring once and the subsequent analysis relying upon proper collection. After exploring special device boot modes and Android's partitioning schema we detail the composition of an Android bootable image and discuss the creation of such an image designed for forensic collection. The major contribution of this paper is a general process for data collection of Android devices and related results of experiments carried out on several specific devices.

5. Dump and Analysis of Android Volatile Memory on Wechat

By Fan Zhou
yutruth123@gmail.com
Communication and Information Systems Security Symposium

Abstract

With the popularity of smart phones, various types of mobile crimes emerge endlessly. Evidence from mobile phones is mostly obtained by non-volatile physical memory dump and file system analysis. The two methods can extract lots of private data, but often invalid for encrypted and deleted data. In this paper, we discuss the Android volatile memory and introduce some methods to dump the memory. Analysis on the Android volatile memory is also presented using software tools. At last the paper provides an in-depth analysis of Android memory structures to extract the encrypted chats and deleted messages on a popular social network application called Wechat. The results show that all chats can be extracted in the form of plaintext, including some deleted messages.

6. Reliable and Trustworthy Memory Acquisition on Smart phones

By He Sun
IEEE Transactions on Information Forensic and security

Abstract

With the wide usage of smart phones in our daily life, new malware is emerging to compromise the mobile OS and then steal or manipulate sensitive data from mobile applications. Forensic analysis tools demand a reliable and trustworthy memory acquisition of the operating systems running on the smart phones for further digital forensic analysis. However, a compromised OS may launch denial of service attacks to prevent a valid memory acquisition by forensic examiners. In this paper, we develop a Trust Zone-based memory acquisition mechanism called Trust Dump that is capable of reliably and securely obtaining the RAM memory and CPU registers of the mobile OS even if the OS has crashed or been compromised. Trust Dump is isolated from the mobile OS by Trust Zone. Instead of using a hypervisor tonsure the isolation between the OS and the memory acquisition tool, we rely on ARM Trust Zone to achieve a hardware-assisted isolation with a small trusted computing base (TCB). Trust Dump can include basic online analysis modules to catch mare in an early stage. Moreover, the acquired memory and register data can be sent to a remote server through a fast Micro-USB port for real-time forensics analysis when the OS runs or a slow serial port for further forensic analysis when the OS has crashed. A trusted GUI is integrated in the Trust Zone to authenticate the user and prevent the misuse of our memory acquisition tool.

7. Live memory forensics of mobile phones

By Vrizlynn L. L. Thing

Journal of Digital Investigation

Abstract

In this paper, we proposed an automated system to perform a live memory forensic analysis for mobile phones. We investigated the dynamic behavior of the mobile phone's volatile memory, and the analysis is useful in real-time evidence acquisition analysis of communication based applications. Different communication scenarios with varying parameters were investigated. Our experimental results showed that outgoing messages (from the phone) have a higher persistency than the incoming messages. In our experiments, we consistently achieved a 100% evidence acquisition rate with the outgoing messages. For the incoming messages, the acquisition rates ranged from 75.6% to 100%, considering a wide range of varying parameters in different scenarios. Hence, in a more realistic scenario where the parties may occasionally take turns to send messages and consecutively send a few messages, our acquisition can capture most of the data to facilitate further detailed forensic investigation.

8. Design and Implementation of Mobile Forensic Tool for Android Smart Phone through Cloud Computing

By Yenting Lai,

Design and Implementation of Mobile Forensic Tool

Abstract

As time progresses, smart-phone features and wireless availability highlight the inner-mobile security issue. By detailed process of inner-mobile acquisition, analyzed result and reporting will be regarded as significant proof on the court. In this paper, researcher forensics implements system of Android smart-phone and delivers the acquisition data through cloud computing to get the forensic analysis and reporting. According to the forensic procedure of National Institute of Standards and Technology (NIST), forensics examiner acquires the inner-data when mobile turns on and then instantly sends it through the clouds. Results will be displayed immediately.

9. Visualization in testing a volatile memory forensic tool

By Hajime Inoue

Journal of Digital Investigation

Abstract

We have developed a tool to extract the contents of volatile memory of Apple Macs running recent versions of OS X, which has not been possible since OS X 10.4. This paper recounts our efforts to test the tool and introduces two visualization techniques for that purpose. We also introduce four metrics for evaluating physical memory imagers: correctness, completeness, speed, and the amount of "interference" an imager makes to the state of the machine. We evaluate our tool by these metrics and then show visualization using dot-plots, a technique borrowed from bioinformatics, can be used to reveal bugs in the implementation and to evaluate correctness, completeness, and the amount of interference an imager has. We also introduce a visualization we call the density plot which shows the density of repeated pages at various addresses within an image. We use these techniques to evaluate our own tool, Apple's earlier tools, and compare physical memory images to the hibernation file.

CHAPTER 4

TOOLS AND TECHNOLOGY

4. Tools and Technology

4.1Tools for Non volatile Memory

During analysis of Non volatile Memory of android device there are numbers of tools are use during analysis of different android devices. List of tools and software are given below which are used during android analysis.

1) **EaseUS Mobisaver for Android**

   http://www.easeus.com/android-data-recovery-software/free-android-data-recovery.html

2) **FonePaw Android Data Recovery**

   http://www.fonepaw.com/android-data-recovery/

3) **Moboedit**

   http://www.mobiledit.com/forensic-guide?CHAPTER=02.02

4) **AF Logical (Linux based)**

   https://santoku-linux.com/howto/howto-use-aflogical-ose-logical-forensics-android/

5) Oxygen Forensic tool

   http://www.oxygen-forensic.com/en/download/33-english-category/download/forensictools/76-forensictools

6) Wondershare Dr.Fone

   http://www.wondershare.net/data-recovery/iphone-data-recovery.html?gclid=Cj0KEQjwxI24BRDqqN3f-97N6egBEiQAGv37hAGNCH4lSV4b4KohPDkNjSGfW3T-3a6nR4gcvXkGWB8aAiph8P8HAQ

7) Android Data Recovery

   http://www.recovery-android.com/android-data-recovery.html

8) Potato share Android Data Recovery

   http://potatoshare-android-data-recovery.en.softonic.com/

9) 7-Data Recovery
   http://7datarecovery.com/

10) Tenoreshare android data recovery trial
http://www.any-data-recovery.com/product/data-recovery-for-android.html
11) Free Any Android data recovery
http://any-android-data-recovery.en.softonic.com/
12) AnyMp4 Android data recovery
http://www.anymp4.com/android-data-recovery/
13) Remo Recover for Android Device
http://www.remorecover.com/android/
14) Johosoft Android phone Recovery
http://www.jihosoft.com/android/android-phone-recovery.html
15) Samsung Data Recovery
http://samsung-data-recovery.en.softonic.com/

During my practical work these all tools we used for analysis for android memory. But some tools were not working properly; some tools are complicated processing step which takes long time and proper knowledge for working with those tools, some tools not analyze valuable information. Among all tools I found some fantastic tools which can be helpful in digital investigation as below.

4.1 Non volatile Memory

1) EaseUS Mobisaver for Android
2) FonePaw Android Data Recovery
3) Moboedit
4) AF Logical (Linux based)

4.2 Volatile Memory

1) LiME (Linux Memory Extractor)

(A)Non volatile Memory

1) EaseUS Mobisaver for Android

EaseUS MobiSaver for Android Free is the most powerful free Android data recovery software. It is quite efficient to recover deleted or lost files from Android devices. Coupled with its user-friendly interface, it can be said the best choice to get back lost Android data for all the users including both home users who have little technical skills or data recovery experience and professional data recovery service supplier. Only takes three simple steps: Scan, preview and recover, the software can bring you what you want.

- **Download link:**
  http://www.easeus.com/android-data-recovery-software/free-android-data-recovery.html
- **Features**

1) Recover lost files from Android devices.
2) Support all the popular Android OS and most Android devices, such as Samsung, LG, HTC, Motorola, Sony, Google etc.
3) Preview all recoverable data and selectively recover what you want.
4) Rock solid support for Android 6.0 Marshmallow/5.

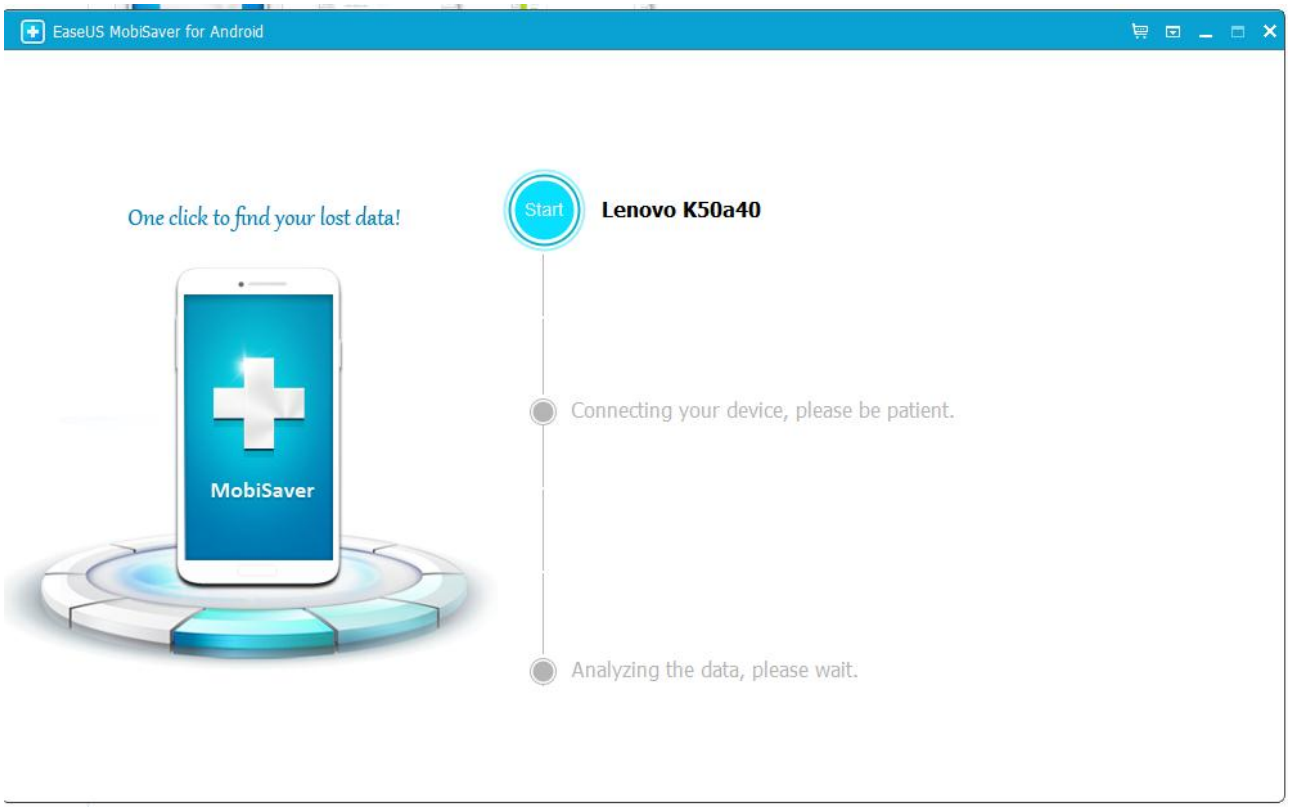


Figure 4.1 EaseUS MobSever for Android

2) FonePaw Android Data Recovery

FonePaw Android Data Recovery is an effective piece of software that can detect and recover deleted or lost files from Android devices, all within a user-friendly interface that's trouble-free and pleasing to navigate. Coupled with its powerful data recovery capacity and multiple Android OS version and devices compatibility, it could be the must-have tool to get back your Android data.

- **Download link:**

  http://www.fonepaw.com/android-data-recovery/

- **Features**

Recover deleted & lost photos, videos, audios, text messages, contacts, call logs and documents from your Android phone & tablet and SD card easily.

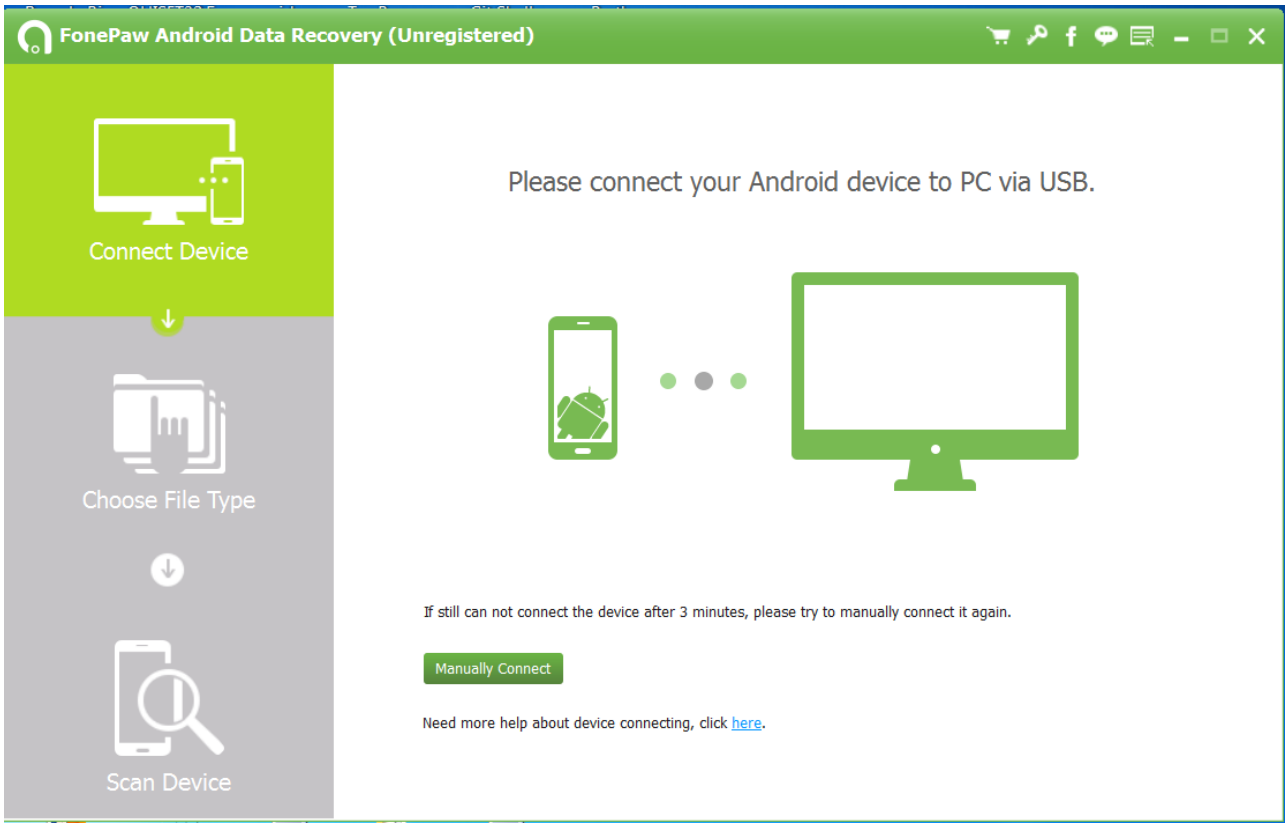


Figure 4.2 FaonePaw Android Data Recovery

3) Moboedit

MOBILedit Forensic you can view, search or retrieve all data from a phone with only a few clicks. This data includes call history, phonebook, text messages, multimedia messages, files, calendars, notes, reminders and raw application data. It will also retrieve all phone information such as IMEI, operating systems, firmware including SIM details (IMSI), ICCID and location area information. Where possible MOBILedit Forensic is also able to retrieve deleted data from phones and bypass the passcode, PIN and phone backup encryption.

- **Download link:**

  http://www.mobiledit.com/downloads.htm

- **Features**

1) Product Highlights
   - Analyze phones via USB cable, Wi-Fi, Bluetooth or IrDA
   - Analyze phonebook, last dialed numbers, missed calls, received calls, SMS messages, multimedia messages, photos, files, phone details, calendar, notes, tasks, SIM cards, applications, application data including those deleted and more
   - Support for Android, iOS, Symbian, Blackberry, Windows Phone, Windows Mobile, MediaTek, Bada, MeeGo and other feature phones covering more than 3000 fully tested devices
   - Complete driver pack with device drivers for all major phone manufacturers included

2) Full Phone Status Information Displayed
   - Picture of the phone
   - Name of the phone, manufacturer and model
   - IMEI
   - Signal strength, battery status
   - Current network operator, connection type, hardware and software revision
   - Remaining storage space
   - Phone display resolution
   - Phone platform/OS
   - Copy IMEI and other information to clipboard with just a double-click of the mouse

3) Powerful SIM Analyzer
   - Direct SIM analysis using SIM card readers
   - Access to SIM card status information (IMSI, ICCID, LAI, PIN, PUK, call costs)
   - Acquire ICCID without knowing the PIN number
   - Extract Location Area Information/Identity

- Retrieve SIM phonebook, sent-received-draft SMS, call log
- PC/SC SIM card reader support
- Support for the connection of multiple readers
- Reads deleted messages from the SIM card
- Review and export of SIM card applications

4) Physical Extraction of Phones and Memory Cards
    - Physical extraction for Android phones
    - Built-in tool for low level physical acquisition of digital media, such as memory card, flash memory and hard disk
    - HEX Dump plug-in optimized for ultra large files of any size

5) Extensive Support for Android Devices
    - Connect Android phones through Wi-Fi using the special forensic version of the connector app
    - Access an application's media and user files
    - Complete support of accounts. Filter contacts according to their sources including Exchange, Facebook, Gmail or Skype
    - Physical extraction available
    - List of installed Android applications
    - Make a screenshot of the current phone display

Figure 4.3 MOBILedit home screen

4) AF Logical

AFLogical is a linux based forensics tool developed by viaForensics that allows logical acquisition of data from Android devices. The tool is free of charge to law enforcement personnel.

- **Download link:**

  https://github.com/viaforensics/android-forensics/downloads

- **Features**
  - AFLogical was the only method capable of extracting text messages from either device.
  - This method was able to identify many of the images and videos, this was by design as these exist on the SD card, which is removed for this method and analyzed separately using well-establish procedures and forensic software to analyze the FAT32 partition.

Figure 4.5 AFLogical home screen

4.3Tools for volatile Memory

Analysis of volatile Memory of android device is big challenge in digital forensic. It also known as Live memory Forensic of android devices. Each and every process run of throw the RAM of that android device. Some data like buffers, sockets, encryption keys reside only in RAM. So it's very important to capture REM data which can play important role during digital investigation of android devices.

During research I found many tools for capture volatile memory. In this dissertation we analyze one linux based the popular tool known as LiME (Linux Memory Extractor). LiME is most effective tool which can be useful during digital investigation.

1) LiME (Linux Memory Extractor)

A Loadable Kernel Module (LKM) which allows for volatile memory acquisition from Linux and Linux-based devices, such as Android. This makes LiME unique as it is the first tool that allows for full memory captures on Android devices. It also minimizes its interaction between user and kernel space processes during acquisition, which allows it to produce memory captures that are more forensically sound than those of other tools designed for Linux memory acquisition.

- **Download link:**

  https://github.com/504ensicslabs/lime

- **Features**

- Full Android memory acquisition
- Acquisition over network interface
- Minimal process footprint

CHAPTER 5

Practical Work

Practical work

My practical work carried out on android memory analysis tools like.

5.1 Tools for Non volatile Memory

5.2.1 EaseUS Mobisaver for Android

5.2.2 FonePaw Android Data Recovery

5.2.3 Moboedit

5.2.4 AF Logical (Linux based)

5.2 Tools for Volatile Memory

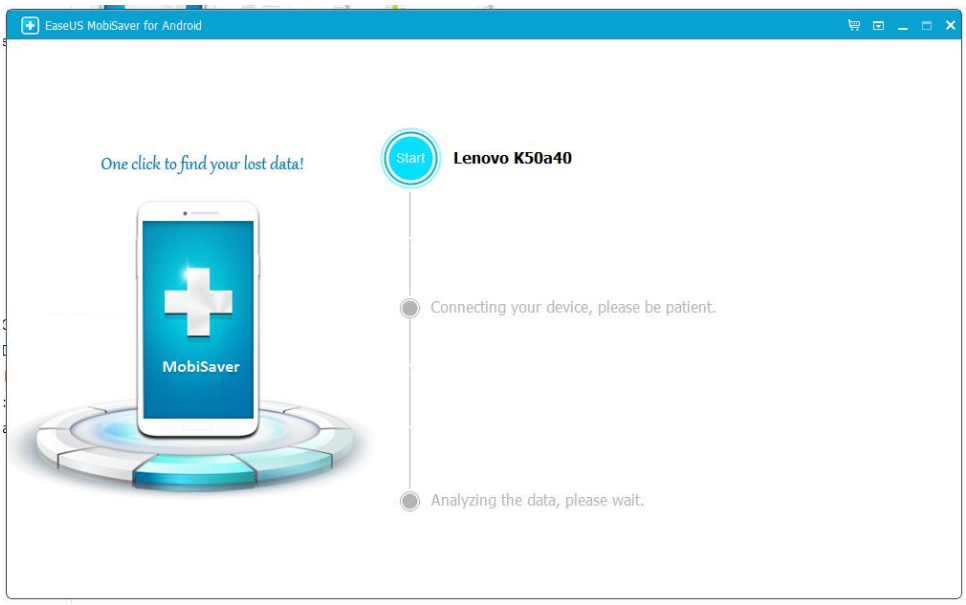
5.2.1 LiME (Linux Memory Extractor)

5.1 Tools for Non volatile Memory

5.1.1 EaseUS Mobisaver for Android

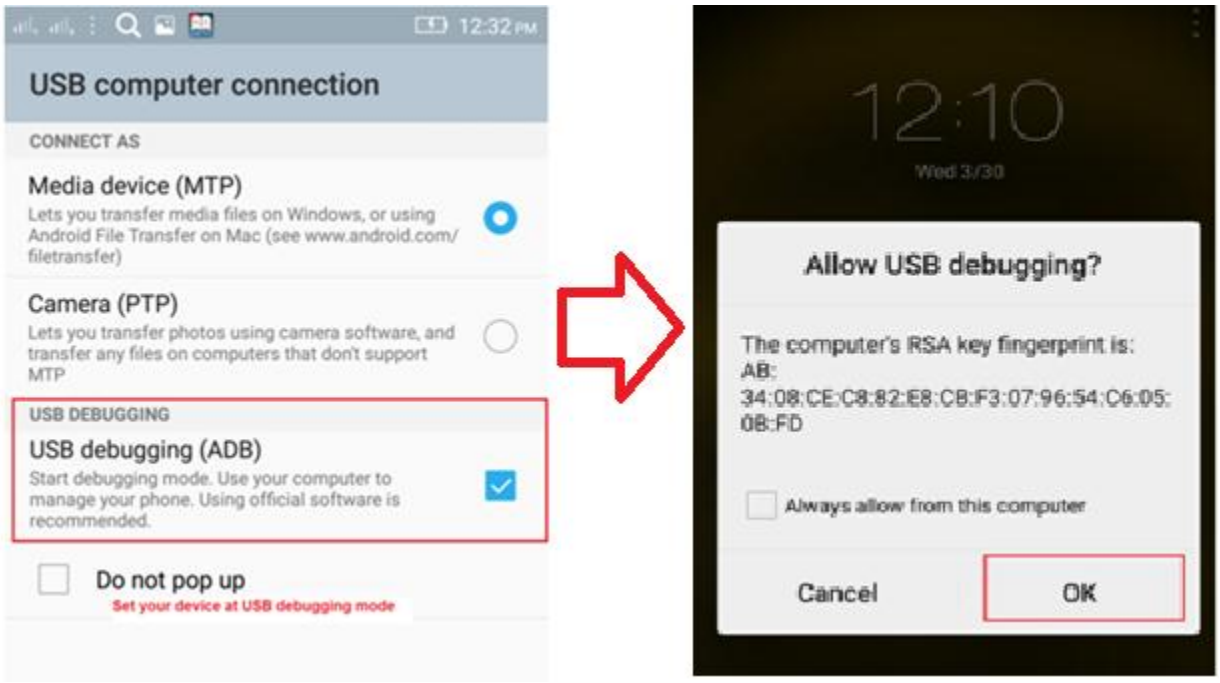
Step 1 Connect Your Android Device to Computer

Connect your Android device to computer using a USB cable. Then click "Start" button and next the software will quickly try to recognize and connect your device.



Step 2 set your mobile at debugging mode

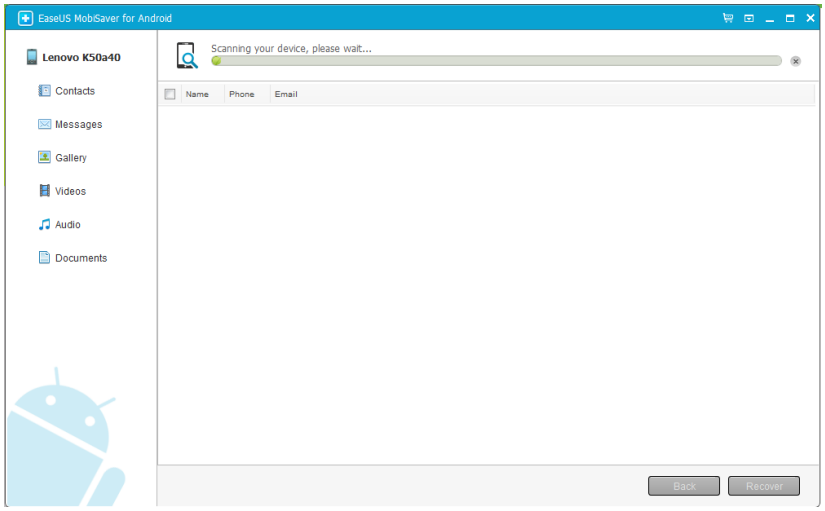
Before connect device set your mobile at debugging mode.



Go to mobile Settings > Developer Options > USB Debugging

Step 3 Scan Your Android Device to Find Lost Data

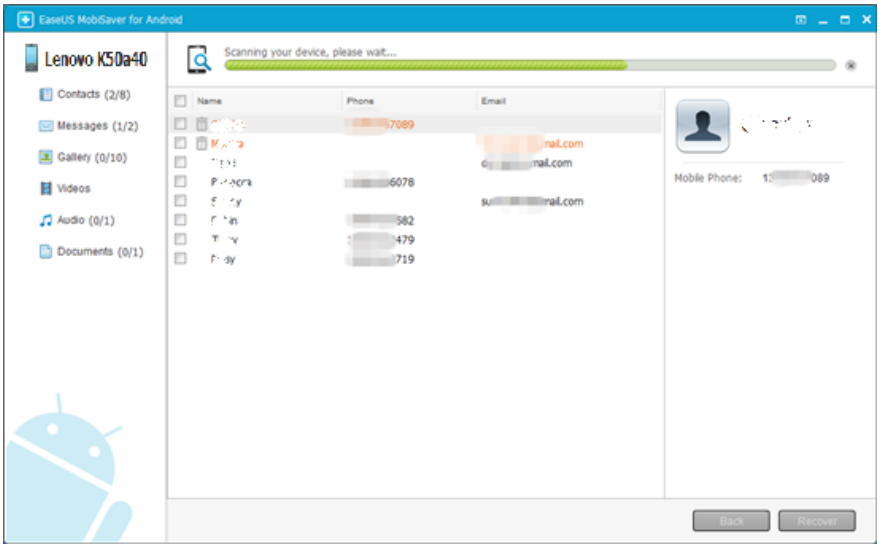
After connecting your Android device, EaseUS MobiSaver for Android Free will automatically scan your device and analyze the data. Then it can help you fully find out all your lost files. During the scanning process, the software will display the tally of found files in real-time.



Note: Before scanning, please make sure that the battery of your device is more than 20%, to ensure a complete scan.

Step 4 Preview the Recoverable Data on Android Device

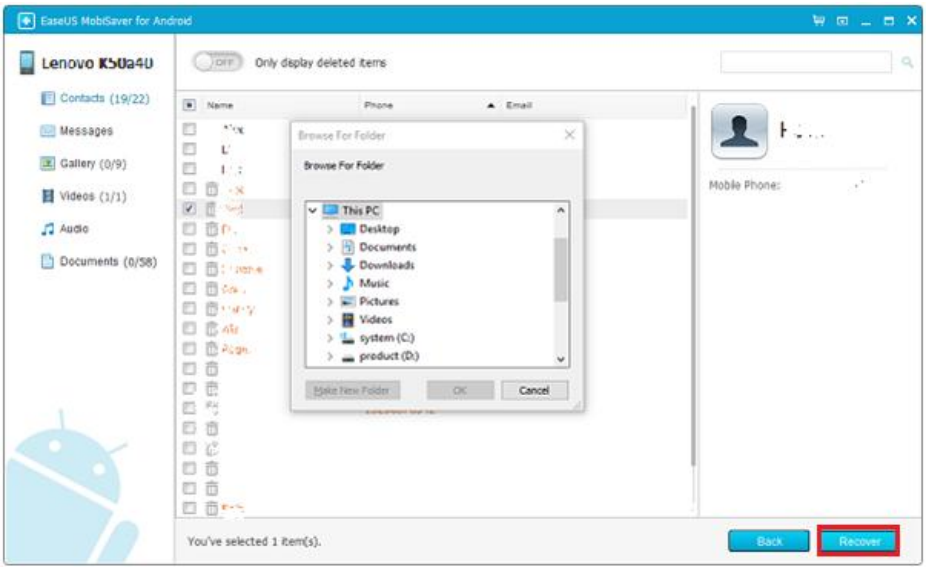
The scanning will take you a while and after that, the program can find and list all the recoverable files on your Android devices. To help you easily find your lost data, all these found file are classified into well-organized categories according to different file types. You can choose any type of file to preview them on the right side of the window one by one.



Note: Deleted SMS and contacts are shown in red. You can separate them by the color.

Step 5 Recover Lost Data from Your Android Device

While previewing the recoverable data, you can easily pick out the files you want to get back. Then mark those selected files and click "Recover" button to retrieve them from your Android device. Finally, you need to specify a folder on your computer to save all the recovered data.

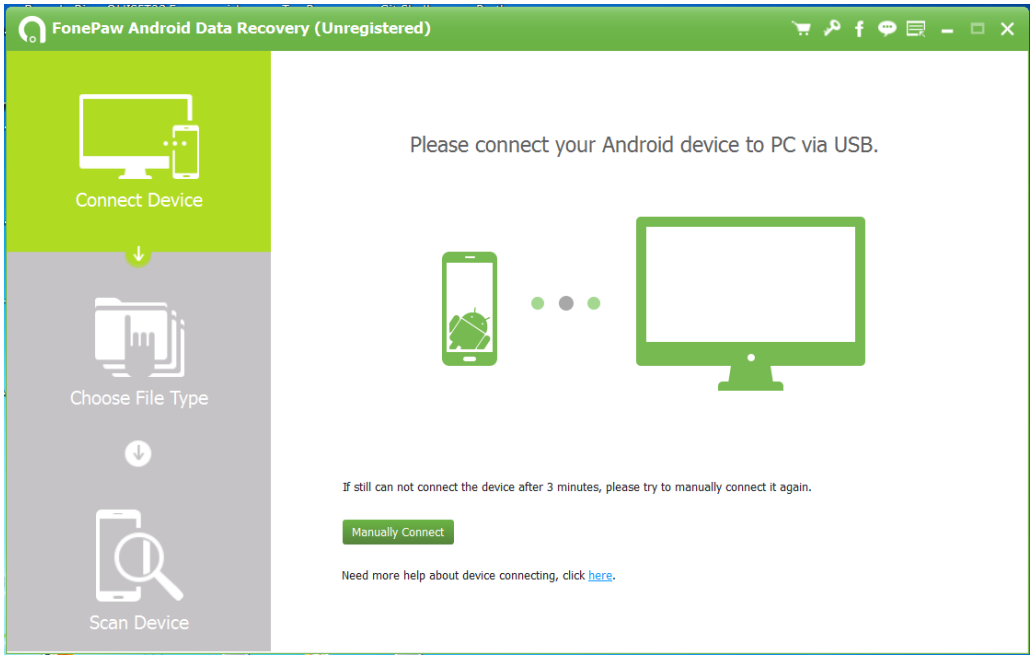


Note: Please don't save the recovered files on your Android device until you make sure that you have get back all your lost data. Otherwise, some of your lost data that have not been retrieved maybe overwritten and you cannot get them back forever.

5.2.2 FonePaw Android Data Recovery

Step 1: Connect your Android device

Launch FonePaw Android Data Recovery and connect your Android device to computer using a USB cable. Wait for seconds before the device is detected. Please note that if this is the first time you connect your phone to PC, drivers should be installed for the program to recognize your Android.

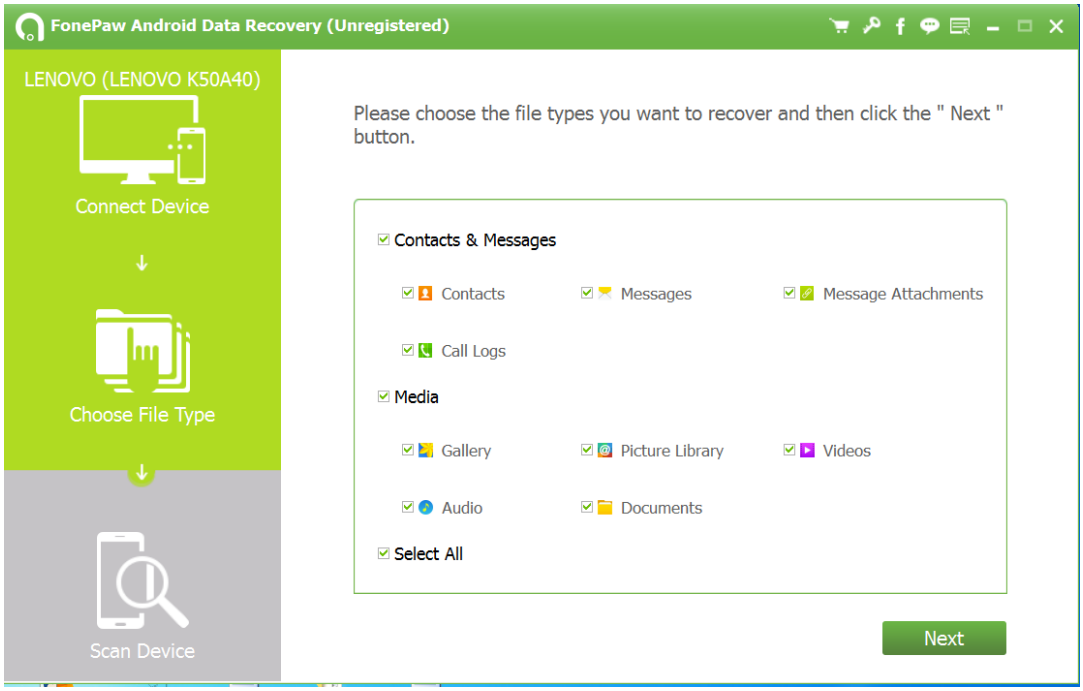


Step 2: Authorize your device

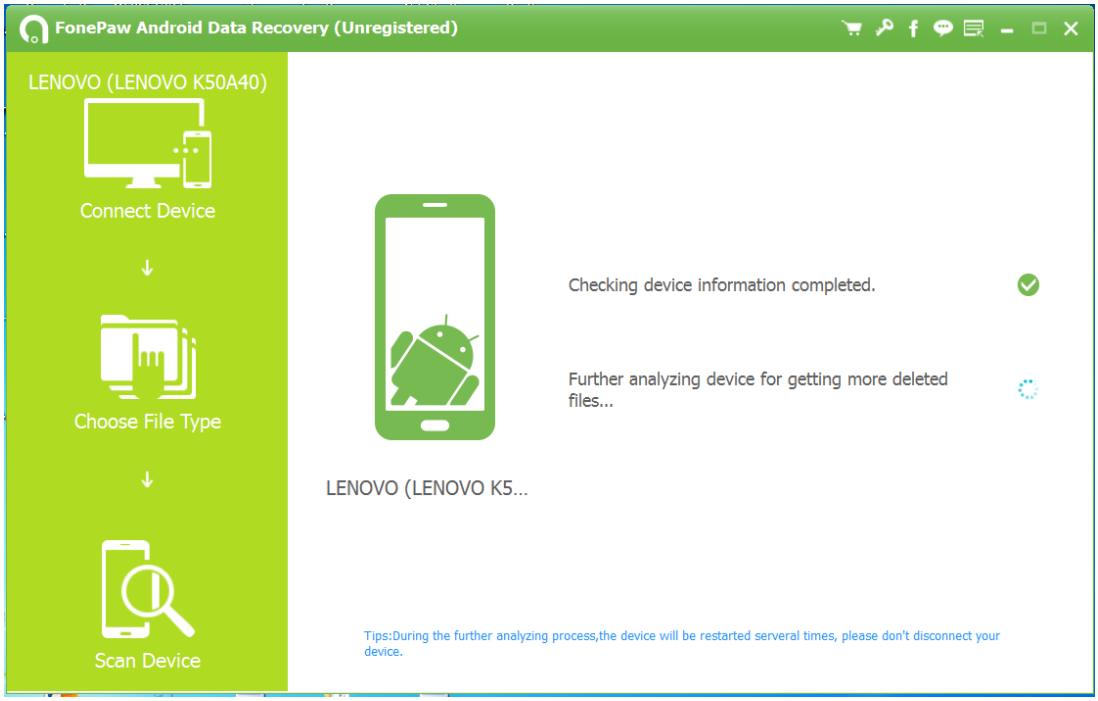
If you don't open the USB debugging on your phone, Android Data Recovery will prompt you to enable USB debugging on your phone.

Step 3: Select the data types to scan

After the Android phone being detected by the program successfully, click the file types you want to recover and click "Next" to begin scanning.



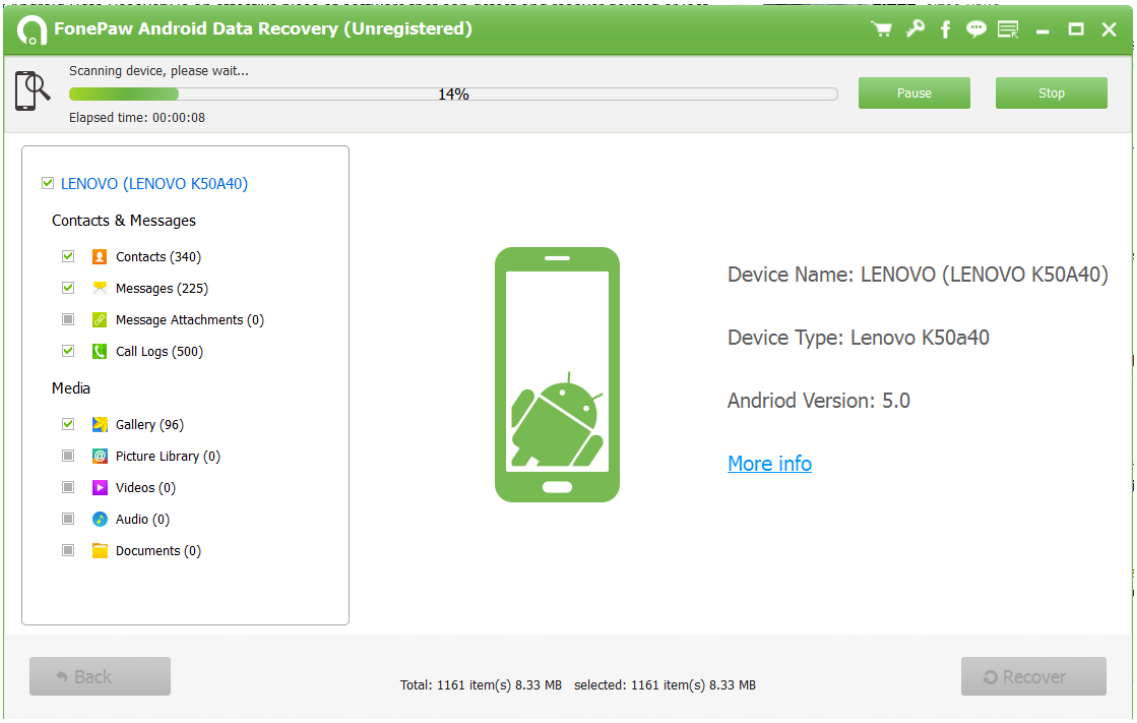
Note: Before scanning, please make sure that the battery of your device is more than 20%.



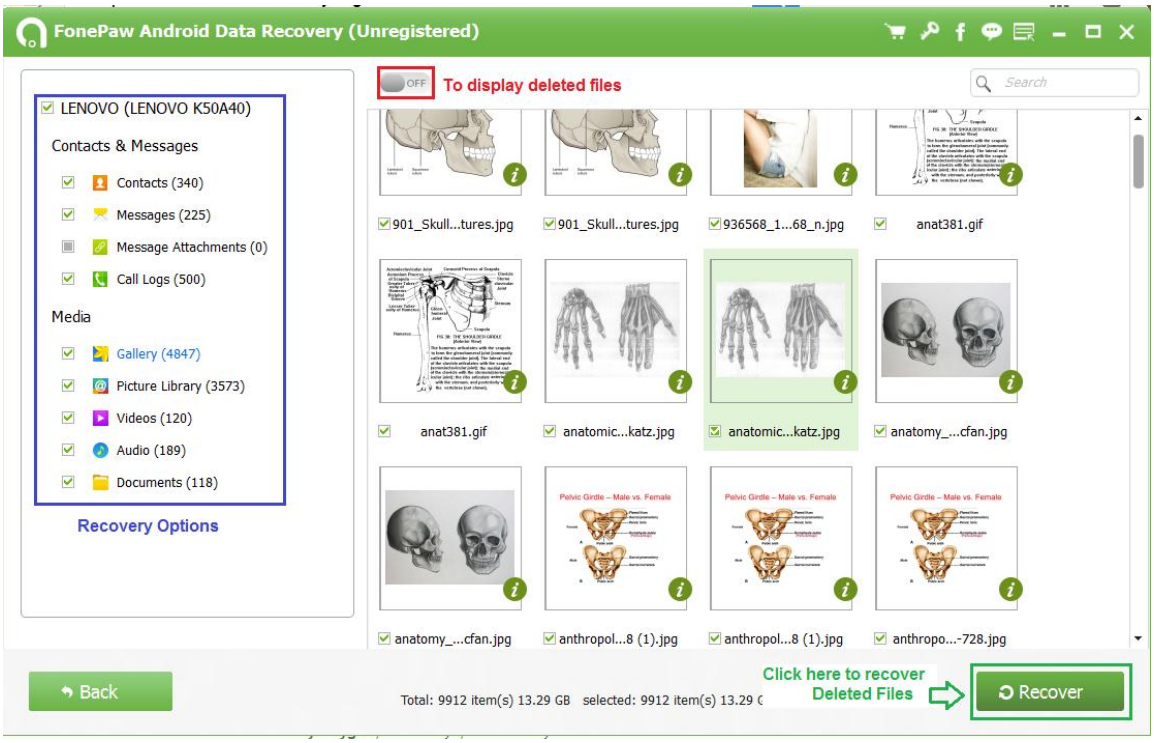
Recovery Process

Step 4: Choose files to recover

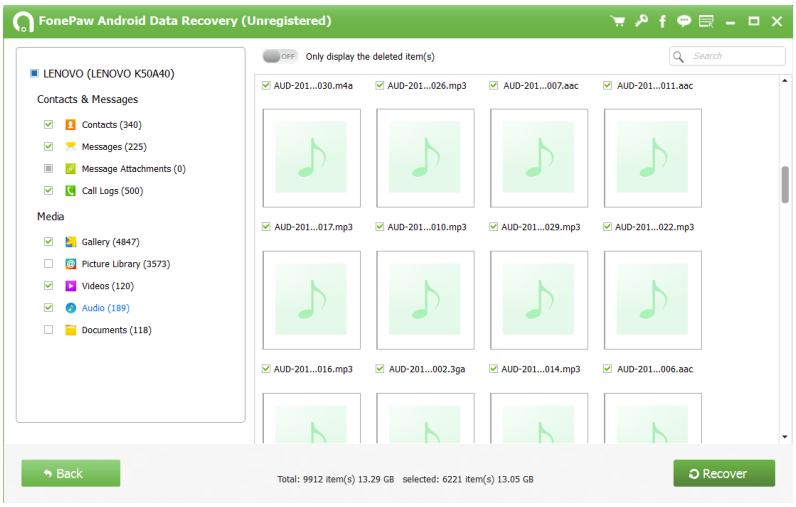
The scanning will take you a while and after that, the files under types you chose will be listed in detail.



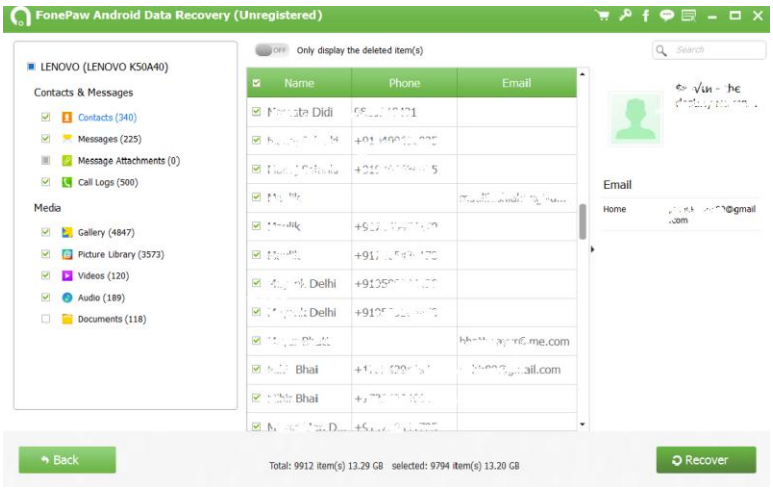
While previewing these files, you can mark down the files you need and click "Recover" button to retrieve them from your Android device to the computer.



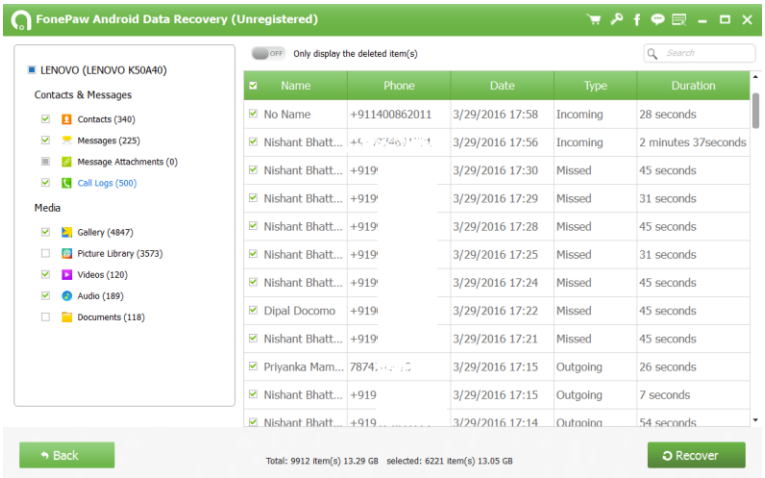
Step 4: Recovery of deleted files



Recovery of Audio files



Recovery of contact information



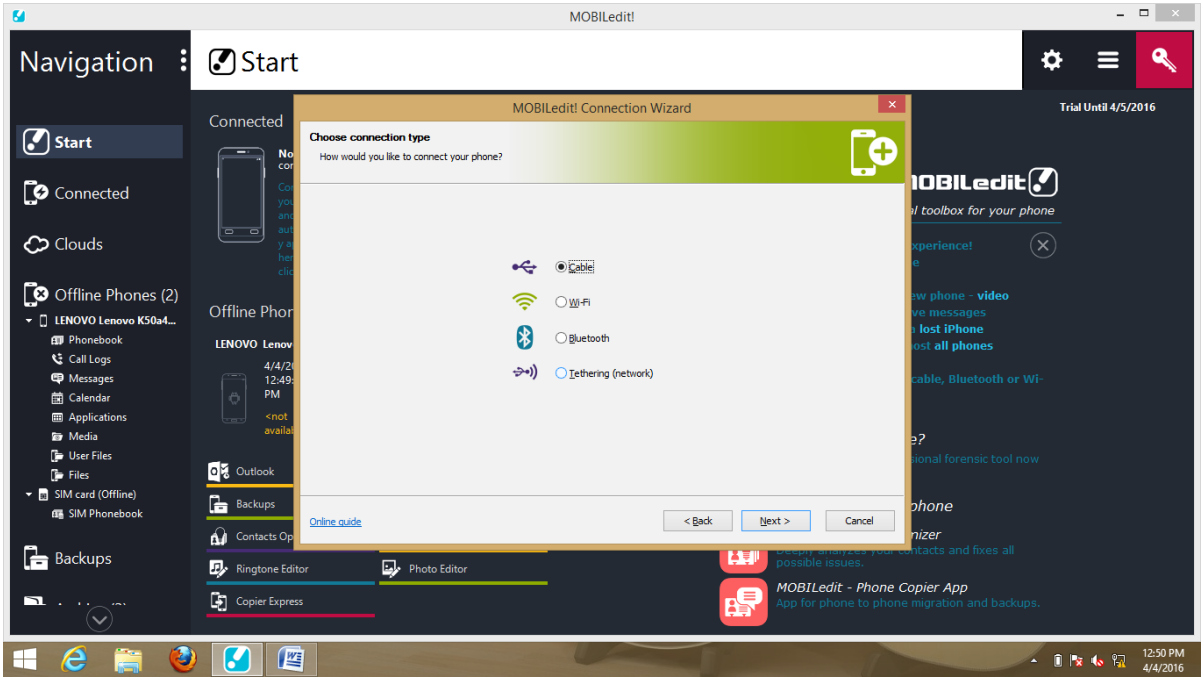
Recovery of Contact details

5.2.3 MOBILedit

Step 1: Connect your Android device

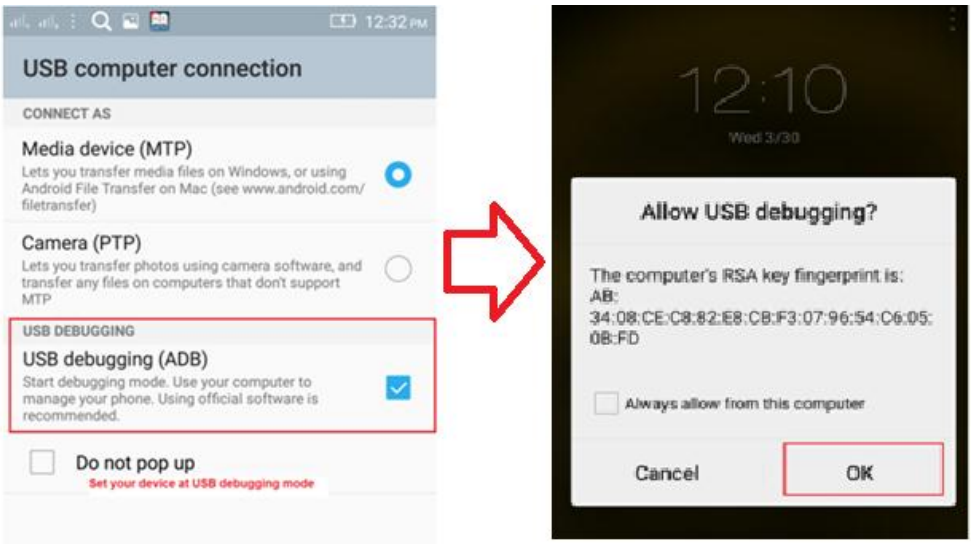
Launch MOBILedit and connect your Android device to computer using a USB cable. Wait for seconds before the device is detected. Please note that if this is the first time you connect your phone to PC, drivers should be installed for the program to recognize your Android.

MOBILedit also provide facility to connect your Android device with wifi, Bluetooth and Tethering (network) connectivity.



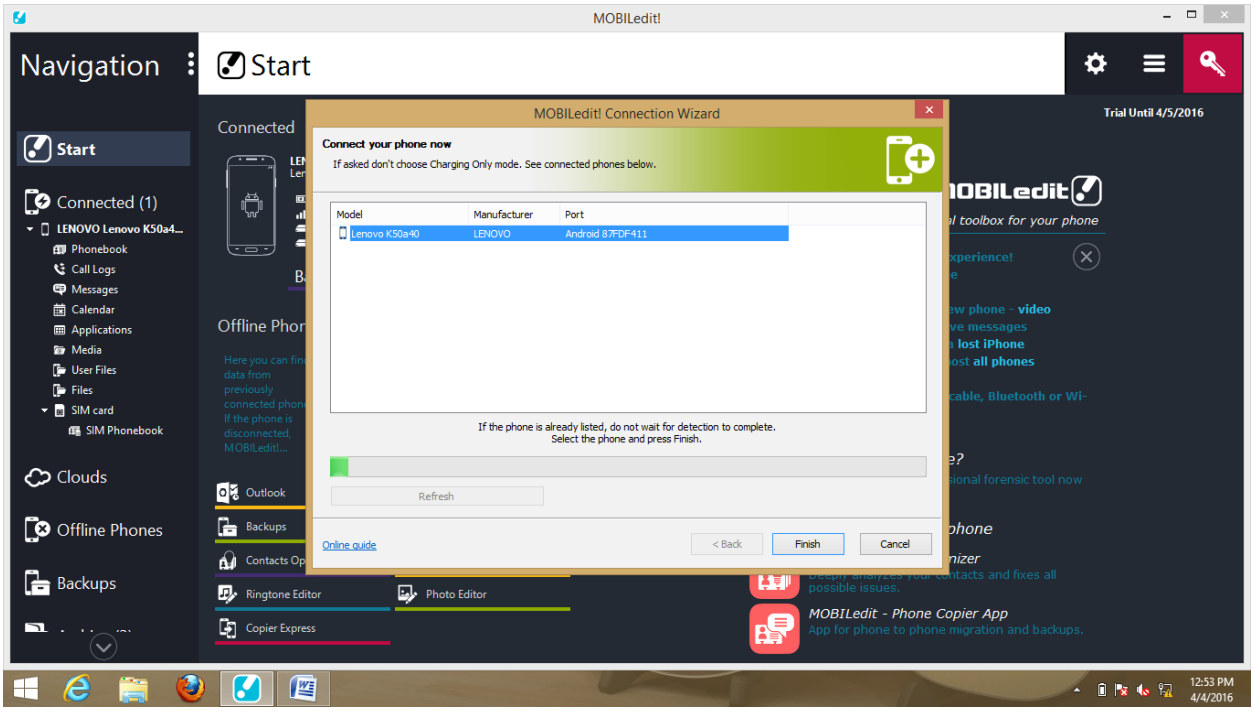
Step 2 Set your mobile debugging mode and allow MOBILedit to analyze your device

set your mobile at debugging mode.



Go to mobile Settings > Developer Options > USB Debugging

Step 3 Select device to scan and wait until device fully analyze



Scanning device for extract internal storage details

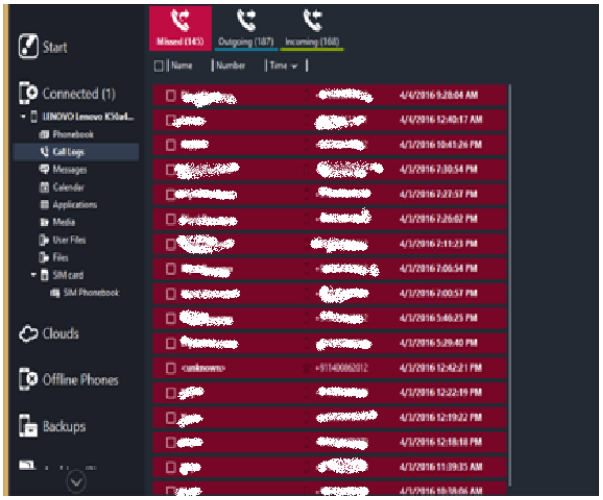
Step 4 Select device to scan and wait until device fully analyze

After device fully scan Red highlight shows devices which are connected and ready to analyze, In green highlight shows call logs and other internal information of device and in blue highlight shows different features.

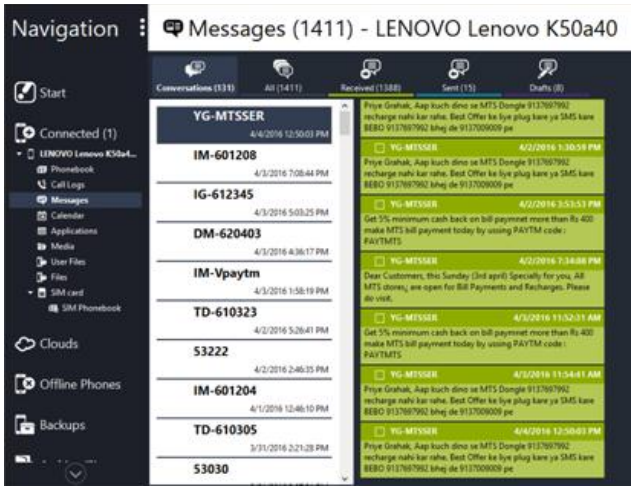
Step 5 Extract storage details

After the full scan of device you can easily extract the user's device storage details and save on your computer.

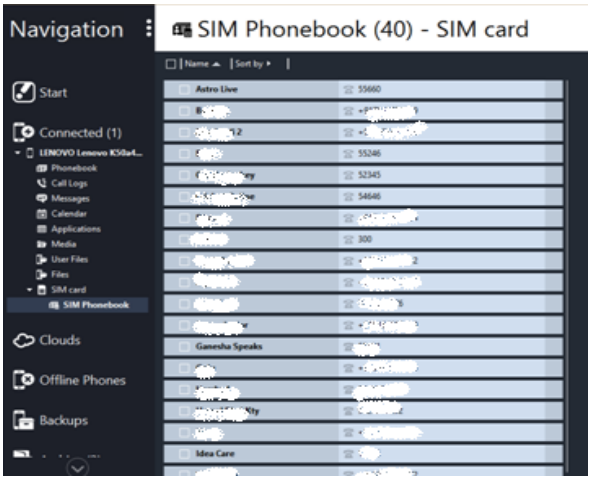
Phonebook



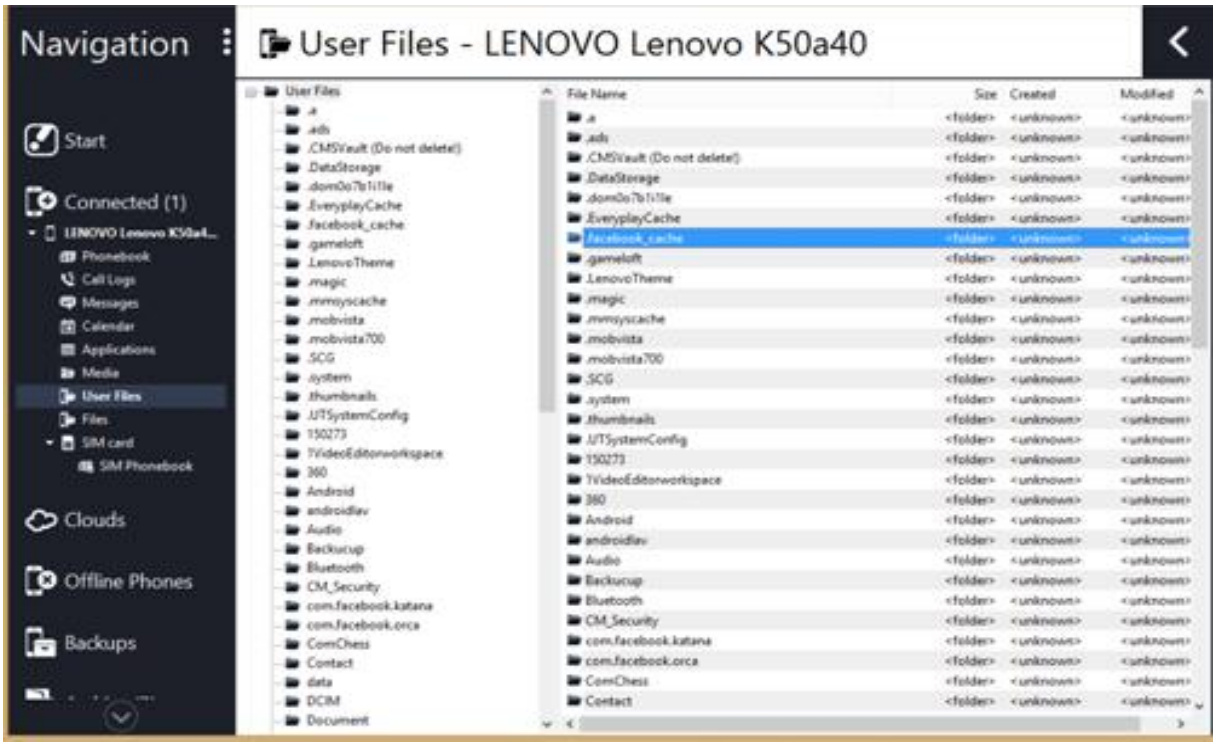
Call logs



Message Details



SIM card phonebook



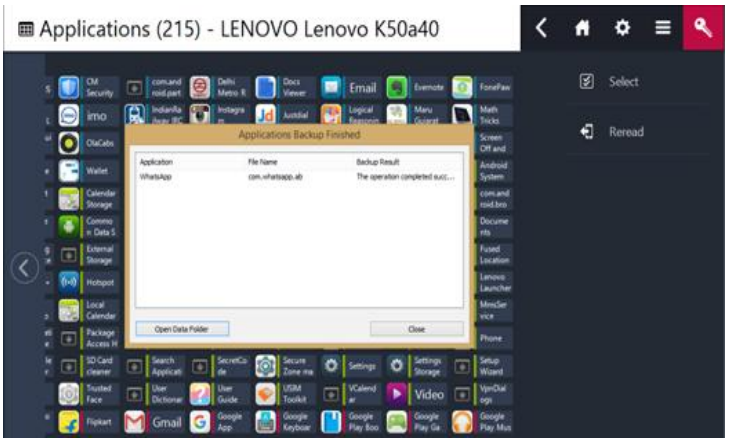
User Files

User file is very important information found from internal storage. Basically these files have encrypted application details which are very useful during investigation.

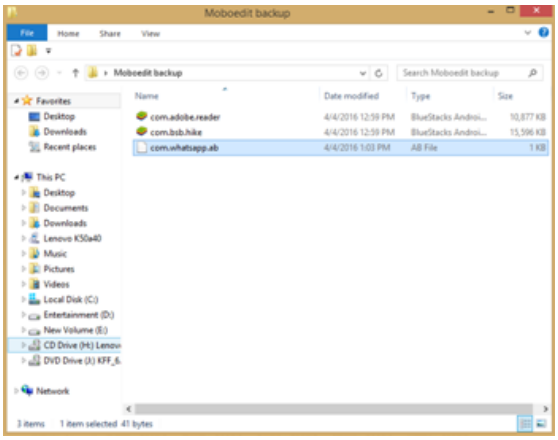
Application Details

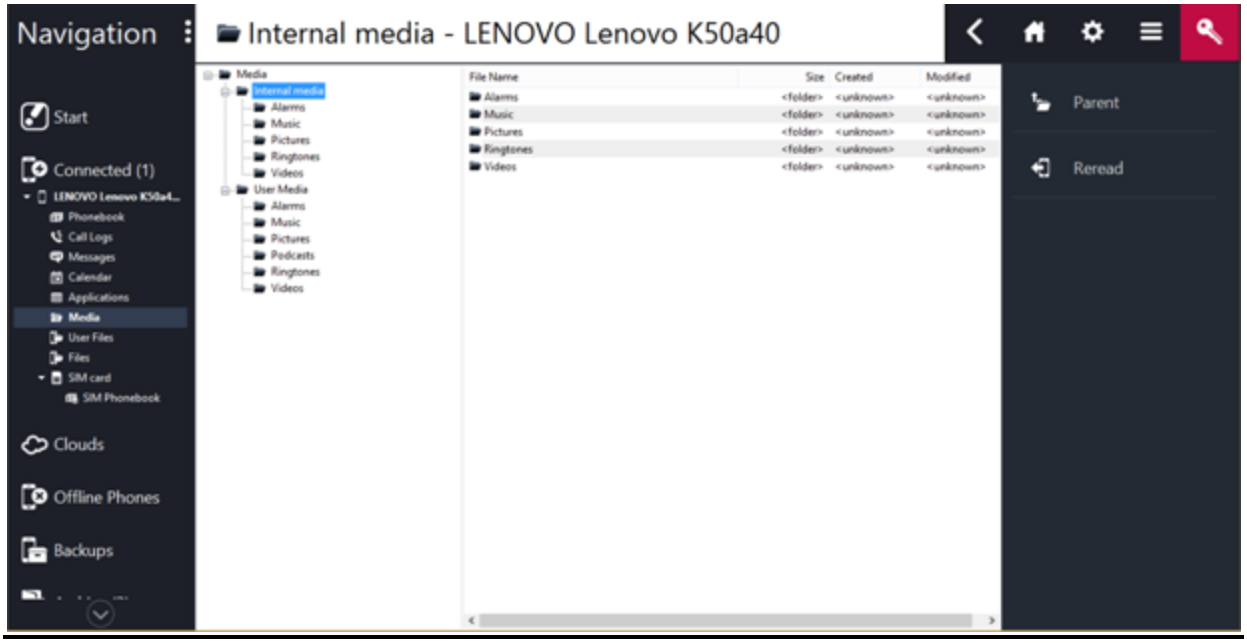
This is another fantastic feature of this software. You can extract application detail and backup all information in your PC or laptop by few simple steps as shown below.

Creating backup of WhatsApp

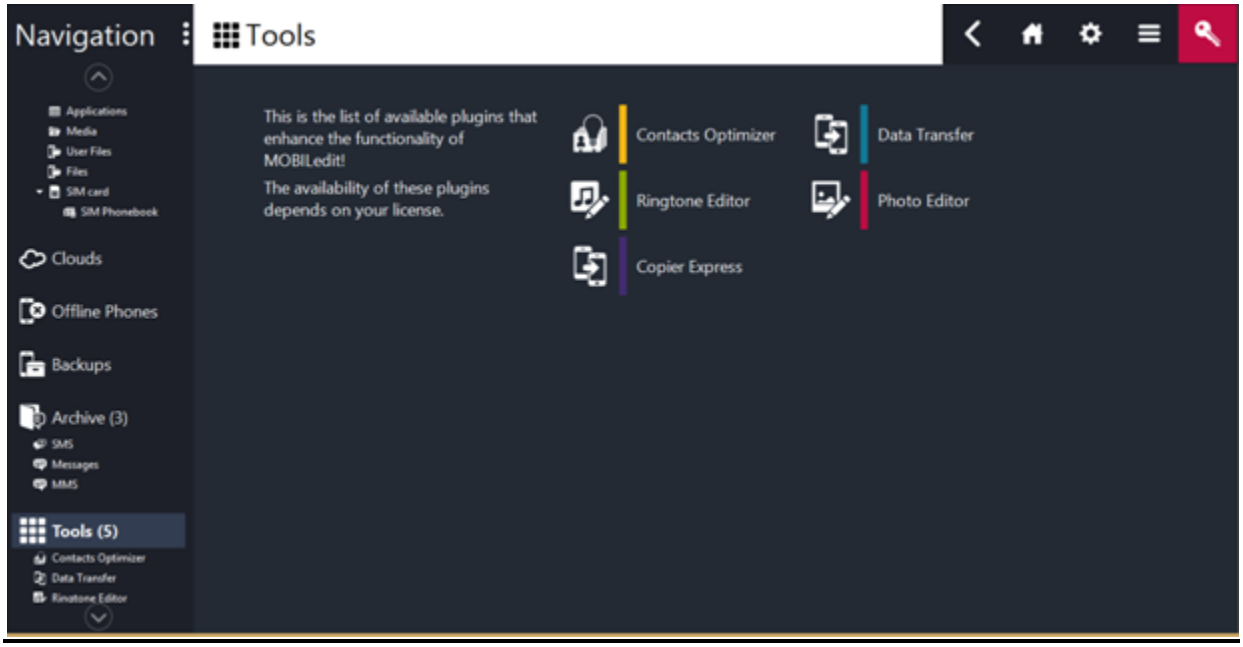


Select application **>>>>** **Backup Folder**





Internal and External media backup



Different tools which can be useful to digital investigator

MOBILedit is one of the best tool among all other to extract the contact detail and backup data. This tool provides all the information and very user-friendly tool to analyze android device.

5.2.4 AFLogical

AFLogical is tool of Santoku Community Edition, which runs in the lightweight Lubuntu Linux distro. It can be run in VirtualBox (recommended) or VMWare Player, both available free and run on Linux, Mac or Windows. The Lubuntu download is large because it is a full .iso. We recommend you download on a fast connection. Which is available open source and available at:

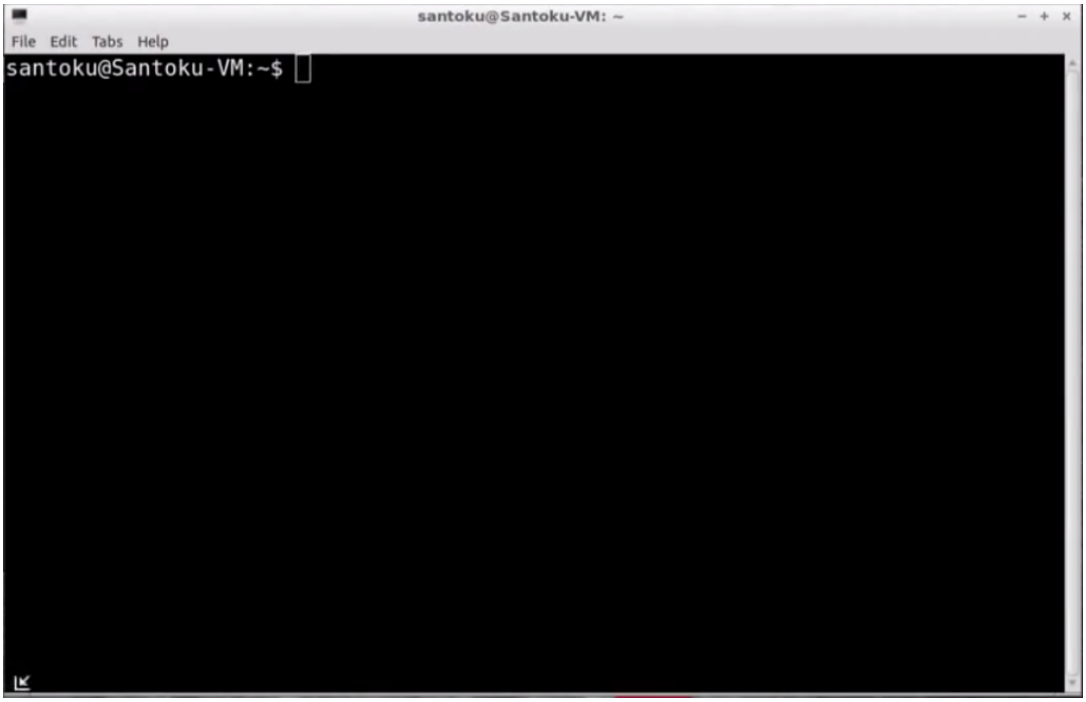
https://santoku-linux.com/download/

After download full version run Santoku-Linux on VMware Workstation.

Home screen of Santoku-Linux

After running home screen follow instructions as below.

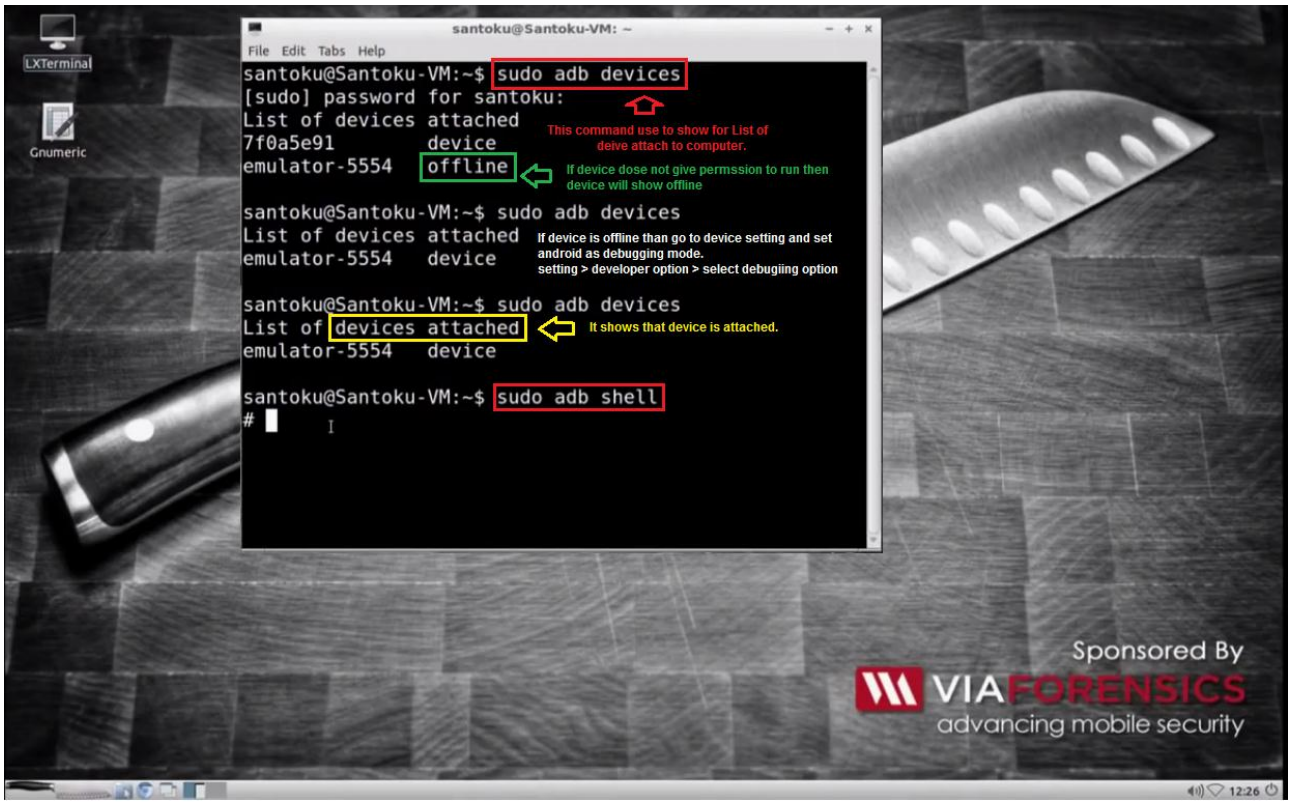
Step 1 Select AF Logical OSE



This terminal screen will shown on desktop

Step 2 Type command as shown in terminal screen

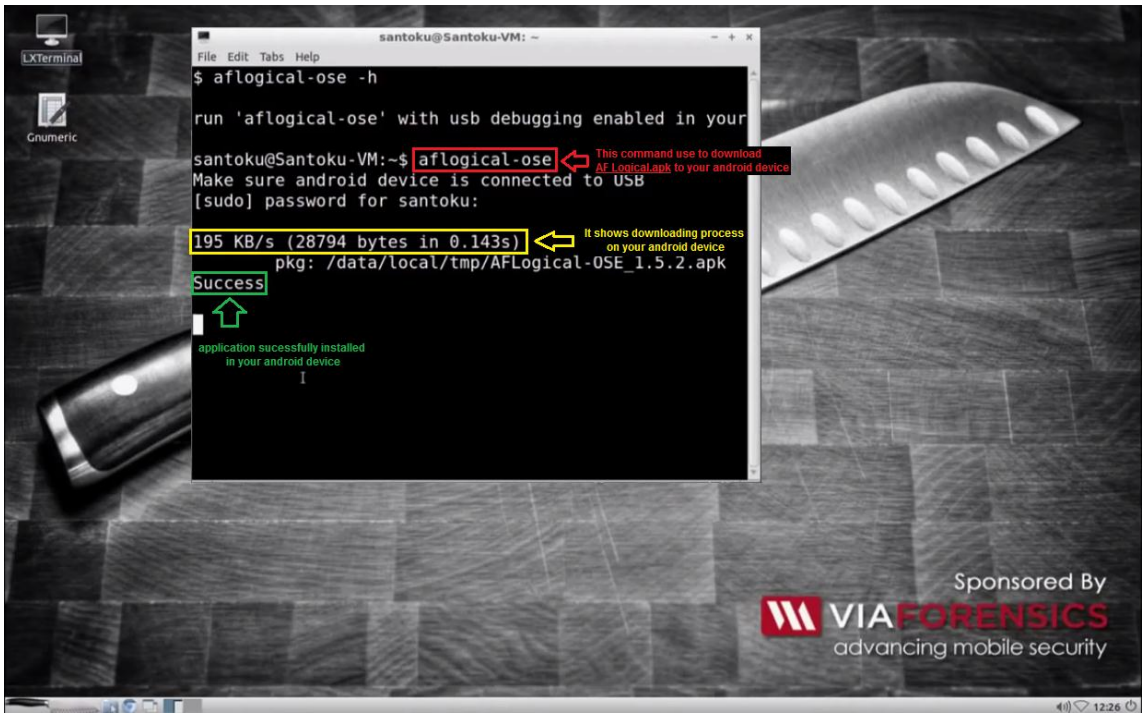
- Command **"Sudo adb devices"** used to find device attached to system.

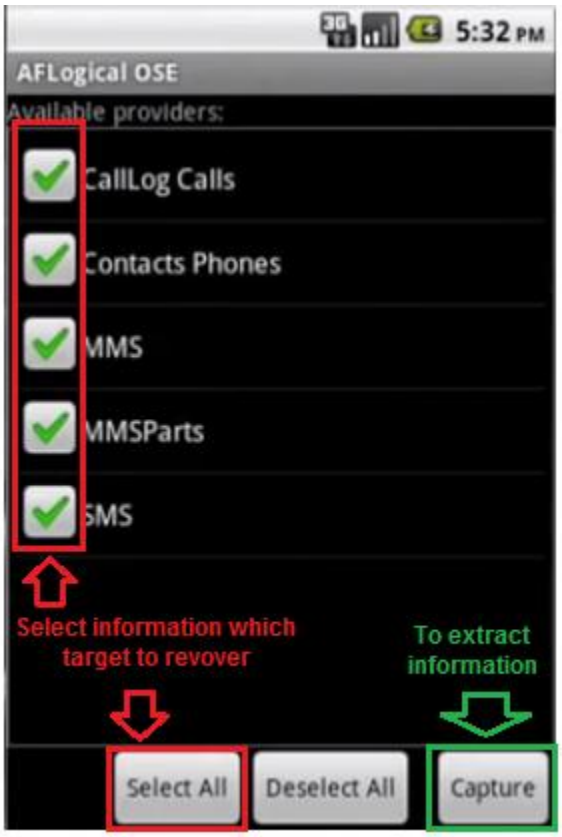


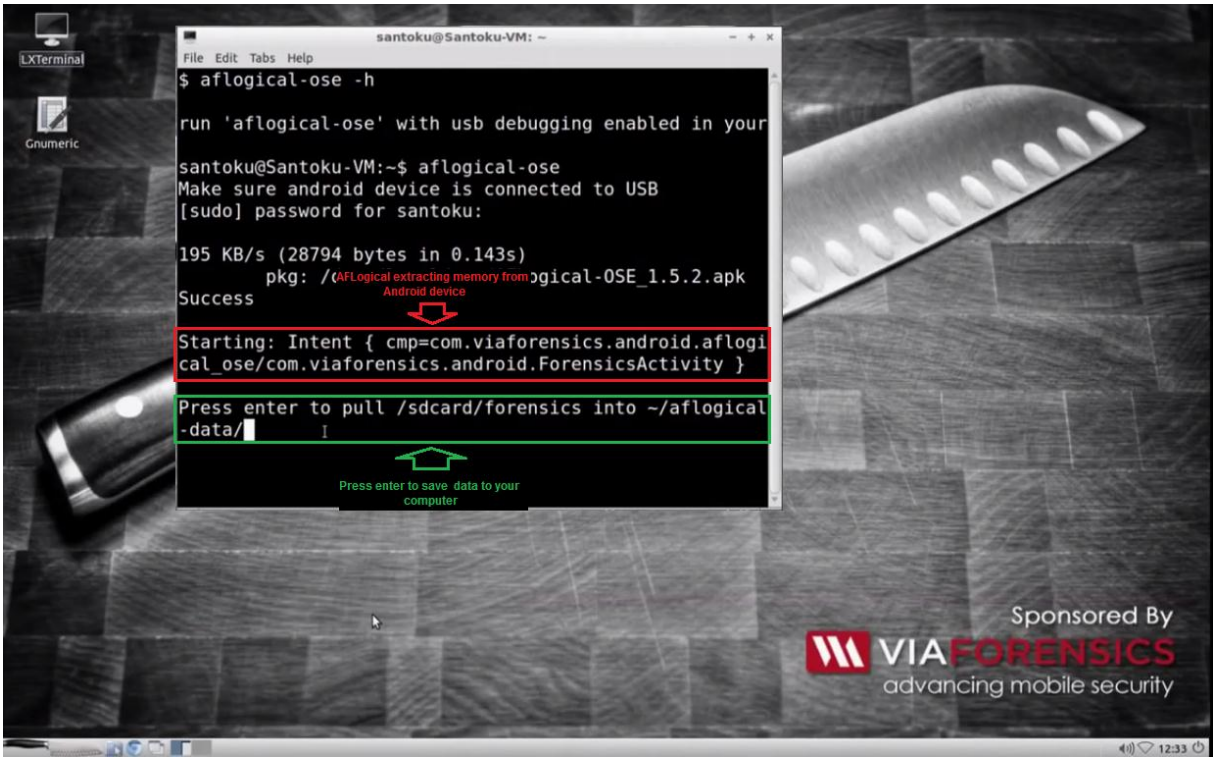
After device attached exit to the terminal and again follow **Step 1** to open new terminal.

Step 3 Type command as shown in terminal screen

- Command **"aflogical-ose"** used to download and install AFLogical-OSE_1.5.2.apk to your android device.

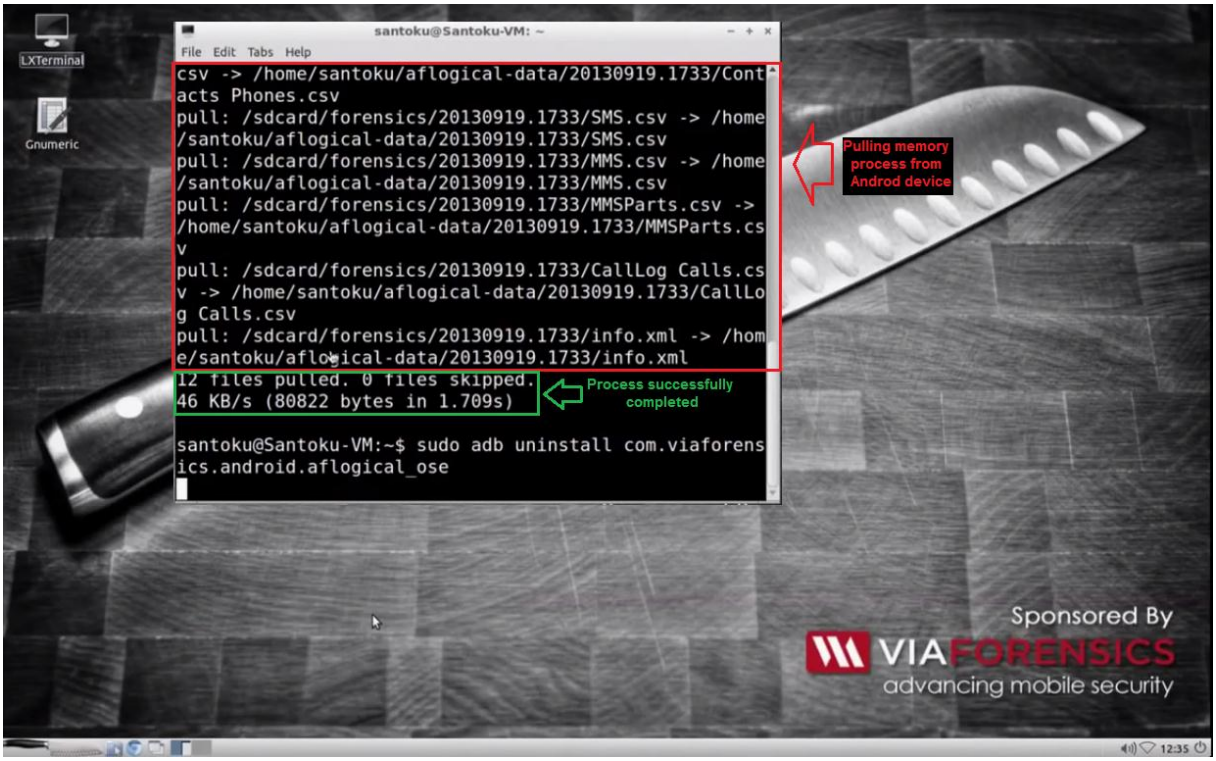




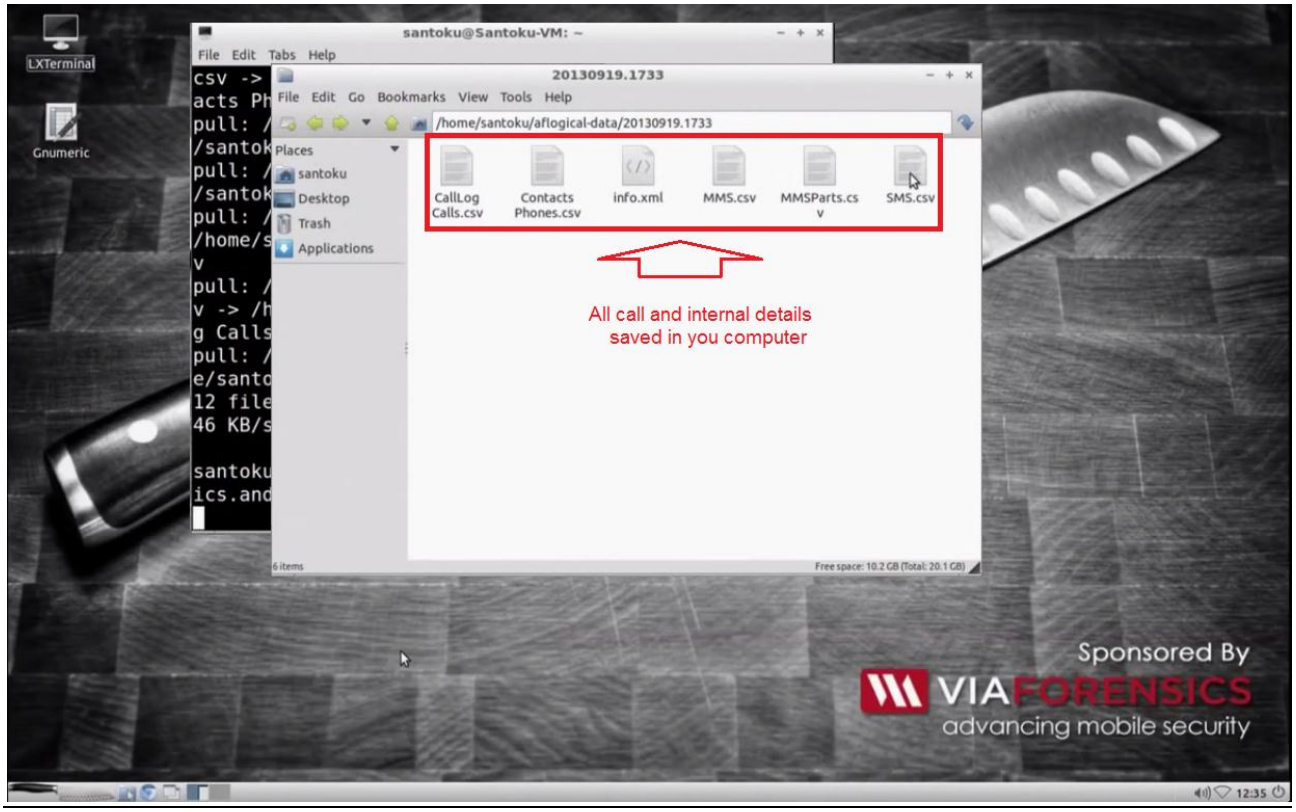


Capturing memory from android device

Step 4 Extracted detail successfully completed



Red box shows that details is successfully saved to your computer



Internal details of Android device