Android Mobile Forensics Methods and Challenges

ISLAM ABDALLA MOHAMED ABASS, OMDRAMN, SUDAN
E-mail: islamabdalla32@gmail.com

Abstract
This extraordinary development of mobile communications is a source of new security challenges. Many people use mobile phones in their daily activities, and sometimes, those activities might be criminal in nature.
When a mobile device is encountered during an investigation, many questions arise: What is the best method to retrieve the evidence? What type of data should be retrieved? What software should be used? The key to answering these questions begins with understanding of the hardware and software characteristics of mobile devices. This paper discusses procedures for the preservation, acquisition, examination, and analysis digital evidence in android smartphone, because it’s the most public in smartphone world. I have used MOBILEDIT forensic tool in my example. This paper make it clear that with each new android firmware update, there are initial challenges to the forensic community.

1. INTRODUCTION
Digital forensics is an exciting field that can have a powerful impact on a variety of situations including internal corporate investigations, civil litigation, criminal investigations, intelligence gathering, and matters involving national security. It faces a constant challenge to stay informed of the latest technologies that may be used to expose relevant clues in an investigation.
Mobile devices are commonplace in today’s society, used by many individuals for both personal and professional purposes. Mobile devices vary in design and are continually undergoing change as existing technologies improve and new technologies are introduced[1].
Mobile forensics, arguably the fastest growing and evolving digital forensic discipline, offers significant opportunities as well as many challenges. While the interesting part of Android forensics involves the acquisition and analysis of data from devices, it is important to have a broad understanding of both the platform and the tools that will be used throughout the investigation. A thorough understanding will assist a forensic examiner or security engineer through the successful investigation and analysis of an Android device.

2. Mobile devices being targeted[1, 2, 3, 4]
Cybercrime is most commonly perpetrated through computer viruses and other malware, or via online scams and phishing, in which fraudulent emails are sent asking for personal information.
Michael Legarry, an information security professional based in Winnipeg, said the latest forms of cybercrime can involve a "hybrid attack."

"Attackers understand that we're logged into multiple systems at any given time. You could be on Google, Facebook, LinkedIn, your iTunes accounts all at once," he explained.

"So if an attacker can trick you into doing something on your web browser, they have access to all your online accounts. So we're seeing a lot more sophisticated attacks. They're designed to take money from you quickly".

Such attacks can happen quickly because many people connect their credit card numbers to their various online accounts, Legarry said.

"We are carrying a tiny computer around in our pockets," he said. "All the things we did on our laptop or workstation over the last decade, we now need to do on our phones."

This is how Gordon M. Snow, assistant director of the FBI's Cyber Division ("Statement Before the House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit," on Sept. 14, 2011), explains it:

"Cyber criminals have successfully demonstrated man-in-the-middle attacks against mobile phones using a variation of Zeus malware. The malware is installed on the phone through a link imbedded in a malicious text message, and then the user is instructed to enter their complete mobile information. Because financial institutions sometimes use text messaging to verify that online transactions are initiated by a legitimate user, the infected mobile phones forward messages to the criminal."

Kaspersky Security Bulletin 2013. Overall Statistics for 2013 written by Christian Funk, Maria Garnaeva make it clear that Vulnerabilities in Android In a nutshell, we have seen exploits targeting Android for three purposes: to circumvent Android's app integrity check on installation (also known as master key vulnerability, to gain enhanced rights, and to hinder the analysis of an app.

StatisticsIn terms of the mobile operating systems that are being targeted by malware, nothing has significantly changed in 2013. Android is still target number one, attracting a whopping 98.05% of known malware. No other OS gets anywhere close, as seen below. The reasons for this are Android's leading market position, the prevalence of third party app stores and the fact that Android has a rather open architecture, making it easy to use for both app developers and malware authors alike. We do not expect this trend to change in near future.

3. Mobile device forensics:[5, 6, 7]

It is a branch of digital forensics relating to recovery of digital evidence or data from a mobile device under forensically sound conditions. The phrase mobile device usually refers to mobile phones; however, it can also relate to any digital device that has both internal memory and communication ability, including PDA devices, GPS devices and tablet computers.
Mobile devices can be used to save several types of personal information such as contacts, photos, calendars and notes, SMS and MMS messages. Smartphones may additionally contain video, email, web browsing information, location information, and social networking messages and contacts.

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

- Evidential and technical challenges exist. For example, cell site analysis following from the use of a mobile phone usage coverage, is not an exact science. Consequently, whilst it is possible to determine roughly the cell site zone from which a call was made or received, it is not yet possible to say with any degree of certainty, that a mobile phone call emanated from a specific location e.g. a residential address.

- To remain competitive, original equipment manufacturers frequently change mobile phone form factors, operating system file structures, data storage, services, peripherals, and even pin connectors and cables. As a result, forensic examiners must use a different forensic process compared to computer forensics.

- Storage capacity continues to grow thanks to demand for more powerful "minicomputer" type devices.

- Not only the types of data but also the way mobile devices are used constantly evolve.

As a result of these challenges, a wide variety of tools exist to extract evidence from mobile devices; no one tool or method can acquire all the evidence from all devices. It is therefore recommended that forensic examiners, especially those wishing to qualify as expert witnesses in court, undergo extensive training in order to understand how each tool and method acquires evidence; how it maintains standards for forensic soundness; and how it meets legal requirements.

4. Android OS Architecture

Android is an operating system (OS) developed by the Open Handset Alliance (OHA). The Alliance is a coalition of more than 50 mobile technology companies ranging from handset manufactures and service providers to semiconductor manufacturers and software developers, including Acer, ARM, Google, eBay, HTC, Intel, LG Electronics, Qualcomm, Sprint, and T-Mobile.

- **Linux kernel**[8, 9]
  
  At the bottom of the layers is Linux - Linux 2.6 with approximately 115 patches. This provides basic system functionality like process management, memory management, device management like camera, keypad, display etc. Also, the kernel handles all the things that Linux is really good at such as networking and a vast array of device drivers, which take the pain out of interfacing to peripheral hardware. Its importance because it provides the following functions in the Android system:
  1. Hardware Abstraction
  2. Memory Management Programs
  3. Security Settings
  4. Power Management Software
  5. Other Hardware Drivers (Drivers are programs that control hardware devices.)
  6. Support for Shared Libraries
  7. Network Stack

- **Libraries**[9]
On top of Linux kernel there is a set of libraries including open-source Web browser engine Web Kit, well known library libc, SQLite database which is a useful repository for storage and sharing of application data, libraries to play and record audio and video, SSL libraries responsible for Internet security etc.

- **Android Runtime**[9, 11]
  This is the third section of the architecture and available on the second layer from the bottom. This section provides a key component called Dalvik Virtual Machine which is a kind of Java Virtual Machine specially designed and optimized for Android.
  The Dalvik VM makes use of Linux core features like memory management and multi-threading, which is intrinsic in the Java language. The Dalvik VM enables every Android application to run in its own process, with its own instance of the Dalvik virtual machine.
  The Android runtime also provides a set of core libraries which enable Android application developers to write Android applications using standard Java programming language.
  Unlike the typical desktop operating system, data or other files created by one Android app cannot automatically be viewed by other applications by default.
  The VM nature of Android allows each application to run its own process. Security is permissions-based and attached at the process level by assigning user and group identifiers to the applications. Application cannot interfere with each other without being given the explicit permissions to do so.
  The security mechanisms of the Android OS could impede a forensic examination although some of the basic tools and techniques could allow investigators to recover data from the device. The first, most obvious step is to perform a traditional forensics analysis of the micro SD card from the phone. This is the least effective method as it can only access the data that apps directly store on the SD card. SD cards use the FAT32 file system and are easily imaged and examined using traditional forensics tools.

- **Application Framework**[9]
  This includes the programs that manage the phone's basic functions like resource allocation, telephone applications, switching between processes or programs and keeping track of the phone's physical location. Application developers have full access to Android's application framework. This allows them to take advantage of Android’s processing capabilities and support features when building an Android application. Think of the application framework as a set of basic tools with which a developer can build much more complex tools. The Application Framework layer also provides many higher-level services to applications in the form of Java classes, the important of Application Framework is:

1. **Activity Manager**: Manages the activity life cycle of applications. To understand the Activity component in Android in detail click here
2. **Content Providers**: Manage the data sharing between applications. Our Post on Content Provider component describes this in greater detail
3. **Telephony Manager**: Manages all voice calls. We use telephony manager if we want to access voice calls in our application.
4. **Location Manager**: Location management, using GPS or cell tower
5. **Resource Manager**: Manage the various types of resources we use in our Application.

- **Applications**[^9]
  You will find all the Android application at the top layer. You will write your application to be installed on this layer only. Examples of such applications are Contacts Books, Browser, and Games etc.

![Android Application Stack](image)

Android Application and Forensic Analysis, will examine a number of these apps in detail. A sample of data found on Android devices includes the following:

- Text messages (SMS/MMS)
- Contacts
- Call logs
- E-mail messages (Gmail, Yahoo, and Exchange)
- Instant Messenger/Chat
- GPS coordinates
- Photos/Videos
- Web history
- Search history
- Driving directions
- Facebook, Twitter, and other social media clients
- Files stored on the device
- Music collections
- Calendar appointments
- Financial information
- Shopping history
- File sharing

5. **How Data are Stored**[^1]

Android provides developers with five methods for storing data to a device. Forensic examiners can uncover data in at least four of the five formats. Therefore, it’s important to understand each in detail. Persistent data are stored to either the NAND flash, the SD card, or the network.

Specifically, the five methods are:
1. Shared preferences
2. Internal storage
3. External storage
4. SQLite
5. Network

Beyond the data that app developers store, the Linux kernel and Android stack provide information through logs, debugging, and other standard information services.

5.1 Files on Internal Storage[1, 12]
Files allow developers to store more complicated data structures and are saved in several places on the file internal storage. The files are stored in the application’s /data/data subdirectory and the developer has control over the file type, name, and location. By default, the files can only be read by the application and even the device owner is prevented from viewing the files unless they have root access. The developer can override the security settings to allow other processes to read and even update the file.

The files clearly indicate data that may be of interest to a forensic analyst or security engineer.

5.2 Files on External Storage[1, 12]
While files stored on the internal device’s storage have strict security and location parameters, files on the various external storage devices have far fewer constraints. First, one important motivation (beyond cost) for using a removable SD card is that the data could be used on other devices, presumably upgraded Android devices.

If a consumer purchased a new Android device, inserted their previous SD card containing all of his or her family pictures and videos and found they were unable to access them, they would be quite upset.

In order to facilitate mounting the SD card on desktop computers to share files, SD cards are generally formatted with Microsoft’s FAT32 files system. While the file system is widely supported, it lacks the fine grained security mechanism built into file systems such as ext3, ext4, yaffs2, hfsplus, and more. Thus, by default, the files cannot enforce permissions.

For example, the com.google.android.apps.maps application referenced previously also stores data on the SD card in the Android/data subdirectory. The following is a listing of the files and directories from the reference HTC Incredible SD card, mounted at /mnt/sdcard:

5.3 SQLite[1, 13]
Another NAND/SD card-based storage that developers leverage is a specific type of SQLite database. Databases are used for structured data storage and SQLite is a popular database format appearing in many mobile systems as well as traditional operating systems.

SQLite is popular for many reasons. Notably the entire code base is of high quality, open source, and released to the public domain. The file format and the program itself are very compact and pack significant functionality in less than a few hundred kilobytes. Unlike more traditional relational database management systems (RDBMS), such as Oracle, MySQL, and Microsoft’s SQL Server, with SQLite the entire database is contained in a single cross-platform file.

The Android SDK provides dedicated APIs that allow developers to use SQLite databases in their applications. The SQLite files are generally stored on the internal storage under /data/data/<packageName>/databases. However, there are no restrictions on creating databases elsewhere.
SQLite databases are a rich source of forensic data. The built-in Android browser, based on the Web Kit Open Source Project (http://webkit.org/), provides a great example. In our referenced HTC Incredible, there were 28 SQLite databases located in subdirectories of /data/data/com.android.webkit. In this instance, the five subdirectories were as follows:

- app_icons: database of web page icons.
- app_cache: database containing web application data cache.
- app_geolocation: databases relating to GPS position and permissions.
- app_databases: databases providing local database storage for supporting web sites.
- Databases: databases for the browser and browser cache.

There is very high potential of recovering forensically valuable data from these files.

5.4 Network[1,12]

The final data storage mechanism available to developers is the network, a key benefit of a device designed to be network aware. Initially, very few applications took advantage of the network as a storage option. However, as the SDK, apps, and devices mature, the network storage option is being leveraged more.

The Android Developer web site provides very few details for those interested in network storage. You can use the network to store and retrieve data on your own web based services.

6. Memory Considerations [14]

Mobile devices contain both non-volatile and volatile memory. Volatile memory (i.e., RAM) is used for dynamic storage and its contents are lost when power is drained from the mobile device. Non-volatile memory is persistent as its contents are not affected by loss of power or overwriting data upon reboot. For example, solid-state drives (SSD) that stores persistent data on solid-state flash memory.

Mobile devices typically contain one or two different types of non-volatile flash memory. These types are NAND and NOR. NOR flash has faster read times, slower write times than NAND and is nearly immune to corruption and bad blocks while allowing random access to any memory location. NAND flash offers higher memory storage capacities, is less stable and only allows sequential access.

System and user data are stored in NOR and copied to RAM upon booting for faster code execution and access. This is known as the first generation of mobile device memory configurations.

The arrangement of NOR, NAND and RAM memory is referred to as the second generation. This generation of memory configurations stores system files in NOR flash.

The latest smartphones contain only NAND and RAM memory (third generation), due to requirements for higher transaction speed, greater storage density and lower cost. To facilitate the lack of space on mobile device mainboards and the demand for higher density storage space (i.e., 2GB – 128GB) the new Embedded MultiMedia Cards (eMMC) style chips are present in many of today’s smartphones.
Evidence in Mobile Phones[15]
Mobile phones are digital media. In principle, this means that mobile phones have the same evidentiary possibilities as other digital media, such as hard drives. For example it is, as will be explored in this paper, possible to extract deleted information from a mobile phone, in the same way it is possible on a hard drive. However, mobile phones also suffer from the same evidentiary problems as other digital media. As with a computer, the content of a mobile Phone is fragile and can easily be deleted and overwritten. Mobile phones should therefore be handled with great care and insight, just as any other digital media.

7. Difference between Logical and Physical Techniques[1]
Android forensic techniques are either logical or physical in nature. A logical technique extracts allocated data and is typically achieved by accessing the file system. Allocated data simply means that the data are not deleted and are accessible on the file system. One exception to this definition is that some files, such as a SQLite database, can be allocated and still contain deleted records in the database. While recovery of the deleted data requires special tools and techniques, it is possible to recover deleted data from a logical acquisition. Physical techniques, on the other hand, target the physical storage medium directly and do not rely on the file system itself to access the data. There are advantages to this approach; the most significant is that physical techniques likely provide access to significant amounts of deleted data. File systems often only mark data as deleted or obsolete, and do not actually erase the storage medium unless needed. As physical forensic techniques provide direct access to the storage medium, it is possible to recover both the allocated and the unallocated (deleted or obsolete) data.
Of course, the analysis of an Android physical acquisition is generally far more difficult and time consuming. Also, the physical techniques are more difficult to execute and missteps could leave the device inaccessible. In Android forensics, the most common logical technique does not provide direct access to the file system and operates at a more abstract and less-effective level than the traditional logical techniques.

8. Android Mobile forensic step by step[16, 17, 18]
The type of phone generally dictates the procedure to be followed in a forensic investigation. We have basically divided the present day phones into 3 major categories: General Phones (Nokia, Samsung, and LG), BlackBerry models, Chinese mobile phones and tried to handle each issue in forensic preservation and acquisition with respect to each of them. I will focus on Samsung, Sony, LG, HTC, and Chinese mobile phone because they runs android as OS.
A. The goals of the examination:
I will identify how in–depth the examination needs to be based upon the data requested. The goal of the examination makes a significant difference in selecting the tools and techniques to examine the phone and increases the efficiency of the examination process.
B. Preservation:
Preservation involves the search, recognition, documentation, and collection of electronic-based evidence. In order to use evidence successfully, whether in a court of law or a less formal proceeding, it must be preserved. Failure to preserve evidence in its original state could jeopardize an entire investigation, potentially losing valuable
case-related information [2]. This stage is performed by the first responders who first arrive at the scene. Their first task is to secure and cordon off the scene and ensure the security of all individuals. Next, the entire scene is documented using camera/video. This is done to create a permanent record of the scene. The team then determines whether there is a need for any kind of DNA analysis to be conducted. A number of challenges, as mentioned below, can come up during this stage:

- Phone found in a liquid.
- Identification of Phones.
- On – Off State Challenge.
- Isolation.

The steps taken to meet these challenges are extremely critical for forensic investigators as a small mistake in performing them can lead to loss of crucial evidence.

When a mobile is found at crime scene, it may be in an on or off state. Depending on the power state and model of the phone, different approaches, as described below, are to be followed:

1) General Phones (Sony, HTC, Samsung, LG):

The USSS (United States Secret Service) document [3] lists a set of rules on whether to turn on or off the device:

- If the device is turned “on” do not turn it “off”.
- Turning the device off may activate the lockout feature.
- If the device is turned “off” leave the device “off”.
- Turning it on could alter evidence on device

2) Chinese Devices:

The Chinese phones pose a big challenge for forensic investigators. The Chinese manufacturers do not follow any standards and therefore it is unclear how the device will behave in different scenarios. Analysis of a few Chinese phones, has revealed that in case the battery is removed from the cavity of the phone (for 5-10 minutes), no temporary data such as the date, time and call logs get erased. Therefore on this current issue, it is best advised to treat the phones as a general phone.

C. Acquisition:

Performing acquisition at the scene has the advantage that loss of information due to battery depletion, damage, etc. during transportation and storage is avoided. However, it is difficult to perform acquisition at the scene due to the absence of a controlled environment. In a laboratory setting this is readily achievable. When a mobile is brought to the lab, it is first determined whether the device has been identified. Next, if the device is found to be switched on a different flow is to be followed as compared to a device which is found to be switched off. When a phone is found switched on, the examination is quite straightforward leaving a few minor issues such as PIN/Password bypass.

However in case a phone is found to be switched off, it is required that the SIM be removed and its acquisition done directly. There are various issues that can come up during acquisition:

A. Selection of Correct Acquisition Tool
B. PIN, Password Protection, and Passcode Pattern bypass
C. Issues with Chinese phones

PIN, Password Protection, and Passcode Pattern is one important challenge that is faced by forensic investigators. Common obstructed devices include mobile phones.
with PIN-enabled identity modules, or with an enabled phone lock setting. A number of ways exist to recover data from obstructed devices.

D. The verification phase:
After processing the phone, I need to verify the accuracy of the data extracted from the phone to ensure that data is not modified. The verification of the extracted data can be accomplished in several ways.

- **Comparing extracted data to the handset data**
  Check if the data extracted from the device matches the data displayed by the device. The data extracted can be compared to the device itself or a logical report, whichever is preferred. Remember, handling the original device may make changes to the only evidence—the device itself.

- **Using multiple tools and comparing the results**
  To ensure accuracy, use multiple tools to extract the data and compare results.

- **Using hash values**
  All image files should be hashed after acquisition to ensure data remains unchanged. If file system extraction is supported, the examiner extracts the file system and then computes hashes for the extracted files. Later, any individually extracted file hash is calculated and checked against the original value to verify the integrity of it. Any discrepancy in a hash value must be explainable (for example, if the device was powered on and then acquired again, thus the hash values are different).

E. The document and reporting phase:
Any forensic examiner is required to document throughout the examination process in the form of contemporaneous notes relating to what was done during the acquisition and examination. Once the examiner completes the investigation, the results must go through some form of peer-review to ensure the data is checked and the investigation is complete. The examiner's notes and documentation may include information such as the following:

- Examination start date and time
- The physical condition of the phone
- Photos of the phone and individual components
- Phone status when received—turned on or off
- Phone make and model
- Tools used for the acquisition
- Tools used for the examination
- Data found during the examination
- Notes from peer-review

9. Mobile forensic challenges[18]
One of the biggest forensic challenges when it come to the mobile platform is the fact that data can be accessed, stored, and synchronized across multiple devices as the data is volatile and can be quickly transformed or deleted remotely, more effort is required for the preservation of this data. Mobile forensics is different from computer forensics and presents unique challenges to forensic examiners. Law enforcement and forensic examiner often struggle to obtain digital evidence form mobile device. The following and some of the reason:

- Hardware differences: The market is flooded with different models of mobile phones from different manufacturers. Forensic examiners may come across different types of mobile models, which differ in size, hardware, features, and
operating system. Also, with a short product development cycle, new models emerge very frequently. As the mobile landscape is changing each passing day, it is critical for the examiner to adapt to all the challenges and remain updated on mobile device forensic techniques.

- **Mobile operating systems**: Unlike personal computers where Windows has dominated the market for years, mobile devices widely use more operating systems, including Apple's iOS, Google's Android, RIM's BlackBerry OS, Microsoft's Windows Mobile, HP's Nokia's Symbian OS, and many others.

- **Mobile platform security features**: Modern mobile platforms contain built-in security features to protect user data and privacy. These features act as a hurdle during the forensic acquisition and examination. For example, modern mobile devices come with default encryption mechanisms from the hardware layer to the software layer. The examiner might need to break through these encryption mechanisms to extract data from the devices.

- **Lack of resources**: As mentioned earlier, with the growing number of mobile phones, the tools required by a forensic examiner would also increase. Forensic acquisition accessories, such as USB cables, batteries, and chargers for different mobile phones, have to be maintained in order to acquire those devices.

- **Generic state of the device**: Even if a device appears to be in an off state, background processes may still run. For example, in most mobiles, the alarm clock still works even when the phone is switched off. A sudden transition from one state to another may result in the loss or modification of data.

- **Anti-forensic techniques**: Anti-forensic techniques, such as data hiding, data obfuscation, data forgery, and secure wiping, make investigations on digital media more difficult.

- **Dynamic nature of evidence**: Digital evidence may be easily altered either intentionally or unintentionally. For example, browsing an application on the phone might alter the data stored by that application on the device.

- **Device alteration**: The possible ways to alter devices may range from moving application data, renaming files, and modifying the manufacturer's operating system. In this case, the expertise of the suspect should be taken into account.

- **Passcode recovery**: If the device is protected with a passcode, the forensic examiner needs to gain access to the device without damaging the data on the device.

- **Communication shielding**: Mobile devices communicate over cellular networks, Wi-Fi networks, Bluetooth, and Infrared. As device communication might alter the device data, the possibility of further communication should be eliminated after seizing the device.

- **Lack of availability of tools**: There is a wide range of mobile devices. A single tool may not support all the devices or perform all the necessary functions, so a combination of tools needs to be used. Choosing the right tool for a particular phone might be difficult.

- **Malicious programs**: The device might contain malicious software or malware, such as a virus or a Trojan. Such malicious programs may attempt to spread over other devices over either a wired interface or a wireless one.

- **Legal issues**: Mobile devices might be involved in crimes, which can cross geographical boundaries. In order to tackle these multijurisdictional issues, the
forensic examiner should be aware of the nature of the crime and the regional laws.

10. MOBILEDIT forensic took kit [24]
Most of phone forensic challenges can be solved by using advanced forensics tools like MOBILEDIT forensic. This application can provide an interface between a cell phone and a personal computer. It is designed to help improve productivity and communication by allowing input using the computer to be downloaded into the phone. It used to send photos, SMS messages, documents, and other important data to and from a cell phone. MOBILEDIT has the ability to send SMS messages and phone calls directly from a computer connected to a cell phone, monitor a cell phone's battery life, signal quality, and the current network operator, display everything on a phone to the screen of a computer, allowing easier use of the phone, allow the user to control a phone from a personal computer, synchronize e-mail onto a cell phone with Microsoft Outlook, configure multiple devices to connect to MOBILEDIT, generate secure reports in any language, create specific templates for specific functions and insert gathered data into a template.

11. Using MOBILEDIT:
Now let's try to do some forensic. I will focus on finding image, e-mail, application (APK), sound file, text file, contact name, and web page visited by the victim. I will use my own Samsung android phone jelly bean 4.2 in this forensic.
First:
I will try to extract the data form my phone using USB. MOBILEDIT can support connect your phone using USB, Bluetooth, and Wi-Fi. Most of the recovered documents were not of a real evidentiary value. This operation take around (3-6) hours depending on the data stored in the device. MOBILEDIT has succeeded in collection all the data from my phone and the SD card without changing and data by install small apps in my phone called ME! Forensic connecter.
Second:
Now I will investigate the image recovered. I have notice that MOBILEDIT give me the size of each Image so I can be sure that no image used to cover harmful program. MOBILEDIT have a hex dump that can be used to make sure the image is not been change to another format by change the extinction. The investigator will notice the first two digit (FF D8) which is mean its JPG file.
Third:
MOBILEDIT get all the contact in my phone, message, MMS, File Browser, Call Log, Calendar, and even my WhatsApp contact list which could be useful by reading the text on it. After forensic all the data last thing is the report and MOBILEDID is doing a good job in this field because in support Multilanguage’s and slice the report into category.
12. MOBILEDIT limitation:
   - It can’t do Physical Acquisition which could retrieve deleted apps, messages, text, html pages, etc.
   - It can’t detect virus or malicious apps.

13. CONCLUSION
Mobile phones outsell personal computers and with digital crime rates rising, IT becomes a good host for digital crime. For Android mobile phone forensics must catch up with release cycles of mobile phones, and develop more comprehensive and depth forensic toolkits. Examiners responsible for mobile device must understand the different acquisition methods, and the phase of retrieving data and the weakness in their tools. The operation system, security features, and type of smartphone will determine the amount data retrieved. Tools like MOBILEDIT can solve some challenges but it also have its own weakness.

15. REFERENCES
Android", Syngress USA, 2011.
bulletin-2013-overall-statistics-for-2013/
tablets-say-experts-1.1877058
Examinations", September 2010.
Forensics", May 2011.
Norwegian University of Science and Technology, 2005.
[16] SatishBommisetty, RohitTamma, Heather Mahalik, "Mobile Forensics: Guidelines
[18] SatishBommisetty, RohitTamma (Author), Heather Mahalik (Author), "Practical Mobile