International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

A Survey on Forensic Analysis of Android Memory

Kousthubha Balachandra[1], Dr Aravinda C V[2]

[1]M.Tech, CNE, SJBIT, Bengaluru.

[2]Associate Professor, Department of ISE SJBIT, Bengaluru

Abstract: ***Today when there are more than 1 billion Android clients everywhere throughout the world, it demonstrates that its prominence has no equivalent. Nowadays' cell phones have turned out to be so intrusive in our day by day experience that when they required can give colossal measure of data to criminological inspectors. We likewise found that IOS are all the more effective when contrasted with Android working framework. The paper expects to unite them under a similar review with the goal that this paper could fill in as a beginning stage for a few android clients, future criminological analysts and examiners.***

Keywords: Security, Android forensic, verification, Android tools

1. Introduction

Internet and Information Technology are no more new today as they have become an integral part of everybody's life, but these technologies have given birth to many more technologies which make life further simpler. The rapid growth in the Small Scale Industries and manufacturing has acted as a means for the world of computing [2]. Today Mobile Phones which are part of Small scale industry have become so persistent that they rule us in many ways which includes; they not only allow us to make and attend a call but also allow us to do business, online commerce, make financial transactions, social networking, SMS, MMS, video calls, photography, electronic mail, Web browsing, multimedia capturing, basic editing and playback, electronic document previewing, store and manage Personal Information via Persona Information Management (PIM) applications (e.g., contacts, calendar, etc.) [1]. There are many types of android version. To name few of them: cup cake, donut, Eclairs, kitkat, jelly bean, marsh mallow, Naugat. The feature of the latest version naugat is by doing double tap we can switch the apps. It consists of stereo speaker which is 2 times more audible then the previous one. It has toggle button. Notifications are displayed in bundles and need not go to sub menus to check the details. It helps to customize all the things. A new feature called night light mode was added. Updating the apps is easy. Even the IOS has many version. In that iPhone 7 is the latest version. This has the improved design which was in two main color: jet black and just black. It has the ability to resist water and dust, improved display. It has 25% brighter and cinema standard colors. It supports up to 25 multi events, which can maintain 450megabits/sec which is 50% faster than IOS And 3times faster the iPhone6. Battery life is 2 hour longer than iPhone6.

Figure 1.1: Steps for mobile forensic

Figure 1.1 shows that steps for mobile forensic. First step to intake the mobile which is also known as seizure. Further we identify the component which we have seized. Preparations are made to see if they can find any information or evidence from the mobile. We isolate the component. Several steps of processing is carried out. Verification is done to check whether the process is carried out correctly or not. There should a set of copies of report generated to present evidence[3]. Finally the presentation of the evidence or proof is demonstrated. Then the final result is stored in a secure place so that the evidence is not changed. Archiving is to keep the gold copy of the data in the safe place. Keep the data in the common format for future.

2. Architecture

Android working framework is a pile of programming segments which is separated into five section and four primary layers as appeared underneath figure 2.1 in the design chart.

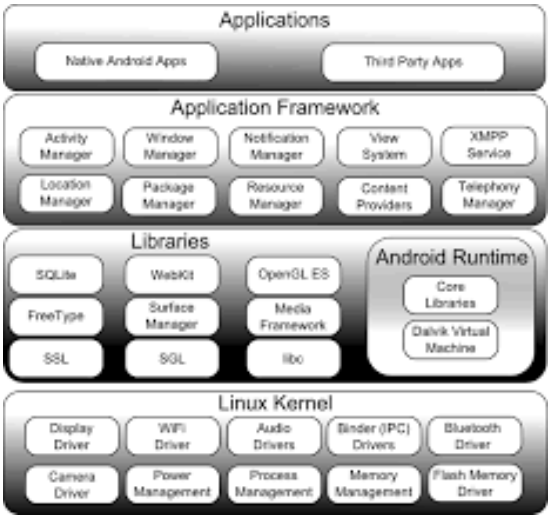

Figure 2.1: Android Architecture

Linux kernel:
At the base of the layers is Linux - Linux 3.6 with roughly 115 patches. This gives a level of reflection between the gadget equipment and it have all the required equipment drivers like camera, keypad, show and so on. Additionally, the piece hold every one of the things that Linux is better than average at, for example, organizing and a variety of gadget drivers, which remove the agony from interfacing to fringe equipment.

Libraries
On top of Linux piece there is an arrangement of libraries including open-source Web program motor WebKit, understood library libc, SQLite database which is a helpful archive for capacity and sharing of use information, libraries to play and record sound and video, SSL libraries in charge of Internet security and so forth.

Android Libraries
This class incorporates those Java-based libraries that are particular to Android advancement. Cases of libraries in this sort incorporate the application structure libraries notwithstanding those that help UI building, representation drawing and database get to. A rundown of some key center Android libraries accessible to the Android engineer is as per the following −
android.app − offers access to the application demonstrate and is the foundation of all Android applications.
android.content − Provides content get to, distributing and informing amongst applications and application parts.
android.database − Used to get information distributed by substance suppliers and incorporates SQLite database administration classes.
android.opengl − A Java interface to the OpenGL ES 3D design rendering API.
android.os − Provides applications with access to standard working framework administrations including messages, framework benefits and between process correspondence.
android.text − Used to convey and control message on a gadget show.
android.view − The basic building squares of utilization UIs.
android.widget − An accumulation of pre-manufactured UI segments, for example, catches, names, list sees, design supervisors, radio catches and so on.
android.webkit − An arrangement of classes proposed to permit web-perusing capacities to be incorporated with applications.

Having secured the Java-based center libraries in the Android runtime, it is presently time to turn our thoughtfulness regarding the C/C++ based libraries contained in this layer of the Android programming stack.

Android Runtime
This is the third area of the engineering and available on the second layer from the base. This segment gives a key part called Dalvik Virtual Machine which is a sort of Java Virtual Machine exceptionally planned and upgraded for Android.
The Dalvik VM makes utilization of Linux center components like memory administration and multi-threading, which is characteristic in the Java dialect. The Dalvik VM encourages each Android application to keep running in its own particular procedure, with its own case of the Dalvik virtual machine.

The Android runtime additionally gives an arrangement of center libraries which gives Android application engineers to compose Android applications utilizing standard Java programming dialect.

Application Framework
The Application Framework layer gives numerous larger amount administrations to applications as Java classes. Application engineers are approved to make utilization of these administrations in their applications. The Android structure incorporates the accompanying key administrations:

- **Activity Manager** − Controls all segments of the application lifecycle and movement stack.
- **Content Providers** − lets applications to distribute and impart information to different applications.
- **Resource Manager** − Provides consent to non-code installed assets, for example, strings, shading settings and UI formats.
- **Notifications Manager** – it let applications to show cautions and notices to the client.
- **View System** − An extensible arrangement of perspectives used to make application UIs.

3. Forensic Process

3.1 Types of evidence

The amount and sorts of information that can be found on a cell phone is continually expanding as cell phone innovation propels. Prove that can be possibly recuperated from a cell phone may originate from a few distinct wellsprings of memory, including handset memory SIM , and appended memory cards, for example, SD cards.

3.1.1Internal memory
There are a wide range of sorts of proof. These days for the most part glimmer memory comprising of NAND or NOR sorts are used for cell phones.

3.1.2 External memory

Outer memory gadgets are SIM cards, SD cards MMC cards, CF cards, and the Memory Stick. The are numerous different gadgets which bolster as an outside memory, for example, remote SSD for IOS gadgets. This incorporates 128 GB of strong stockpiling and rapid USB 3.0 ports. It additionally comprise of in manufactured Wi-Fi transmitter.

3.1.3 Service provider logs

In spite of the fact that non-specialized some portion of cell phone legal sciences incorporates the call detail records (and once in a while, instant messages) from remote bearers frequently fill in as "move down" proof gotten after the cell phone has been held. at the point when the call history as well as instant messages have been erased from the telephone, or when area construct administrations are not handed over light of, these are exceptionally valuable. Call detail records and cell site (tower) dumps can give the telephone proprietor's area, and whether they were pondering around or sitting still in a place (i.e., regardless of whether the telephone bobbed the flag off the comparative side of a solitary tower, or diverse sides of different towers along a specific way of travel)[6]. Bearer information and gadget information together can be utilized to confirm data from different sources, for example, video observation film or onlooker accounts; or to decide the normal area where a non-geotagged picture or video was taken.

The legal sciences handle for cell phones for the most part matches different branches of computerized crime scene investigation; be that as it may, some specific concerns apply. By and large, the procedure can be separated into three principle sorts: seizure, procurement, and examination/investigation. Different parts of the PC scientific process, for example, admission, approval, documentation/revealing, and introduction, filing still apply.

3.1.4 Seizure

Seizing cell phones is secured by an indistinguishable lawful consultations from other advanced media. Mobiles will regularly be recuperated exchanged on; as the point of seizure is to ensure prove, the gadget will as often as possible be transported in a similar state to stay away from a shutdown, which would change records. Moreover, the specialist or person on call would chance client bolt activation[4].

This may get unique information, overwriting proof. To stop an association, cell phones will regularly be transported and analyzed from inside a Faraday confine (or bag)[7]. All things considered, there are two burdens to this strategy. To start with, it causes to be the gadget unusable, as its touch screen or keypad can't be utilized.

Second, a gadget's look for a system association will debilitate its battery all the more rapidly. While gadgets and their batteries can over and over be energized, once more, the specialist hazards that the telephone's client bolt will have enacted. Along these lines, organize confinement is reasonable either through putting the gadget in Airplane Mode, or cloning its SIM card (a procedure which can likewise be valuable when the gadget is feeling the loss of its SIM card completely).The second step in the scientific procedure is procurement, for this situation more often than not alluding to recovery of material from a gadget. Figure 3.1 shows portable process.

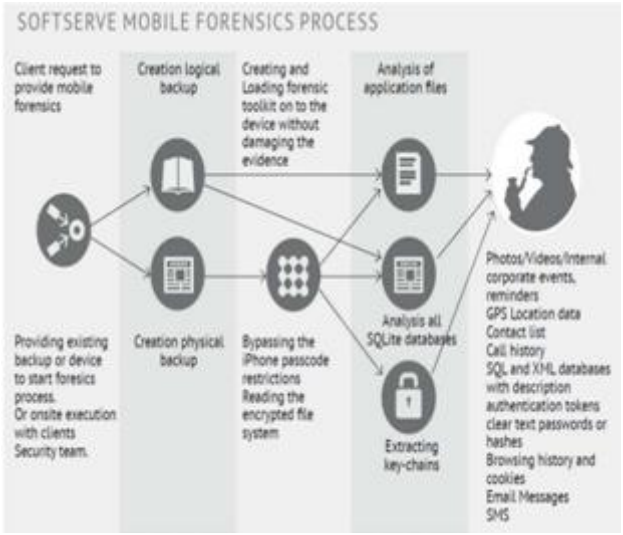

Figure 4.1: Mobile forensic processes

First the client request to provide mobile forensic then they provide existing backup or device to start forensic process or onsite execution with the clients Security team. It creates either logical backup or physical backup. Second step is creating and loading forensic toolkit on to the device without damaging the evidence where as in iPhone passcode restrictions reading the encrypted file system are given. Then the analysis of application files is done. Finally the data is extracted.

Due to the proprietary nature of mobiles it is often impossible to acquire data with it powered down; most mobile device acquisition is performed live[5]. With more superior Smartphone's using advanced memory management, connecting it to a recharger and putting it into a faraday cage may not be good practice.

The mobile device would distinguish the network disconnection and therefore it would change its status information that can trigger the memory manager to write data. Most acquisition tools for mobile devices are profitable in nature and consist of a hardware and software component, often automated.

4. Forensic Tools

4.1 Tools

As of late various equipment or programming apparatuses have risen to recoup consistent and physical proof from cell phones. Most devices contain of both equipment and programming divides. The equipment incorporates various links to interface the telephone to the securing machine; the product exists to take out the confirmation and, incidentally even to examine it[8].

Most recently, cell phone criminological apparatuses have been produced for the field. This is accordingly both to military units' order for quick and exact hostile to

psychological oppression knowledge, and to law authorization interest for measurable reviewing abilities at a wrongdoing scene, court order execution, or critical circumstance. Such portable scientific instruments are regularly ruggedized for unfeeling situations (e.g. the war zone) and harsh treatment (e.g. being dropped or submerged in water).[9]

4.2 Physical instruments

4.2.1 Forensic desoldering

Regularly alluded to as a "Chip-Off" system contained by the business, the last and most meddlesome technique to get a memory picture is to desolder the non-unstable memory chip and append it to a memory chip peruser. This strategy holds the potential threat of aggregate information pulverization: it is conceivable to wipe out the chip and its substance as a result of the warmth required amid desoldering. Prior to the development of the BGA innovation it was conceivable to associate tests to the pins of the memory chip and to recuperate the memory through these tests. The BGA procedure bonds the chips straight onto the PCB through liquid patch balls, with the end goal that it is no longer conceivable to connect tests. Here you can watch that dampness in the circuit board swung to steam when it was subjected to extreme warmth. This delivers the alleged "popcorn impact."

There are for the most part three techniques to dissolve the patch: hot air, infrared light, and steam-staging. The infrared light innovation works with a ready infrared light bar onto a particular coordinated circuit and is utilized for little chips. The hot air and steam strategies can't center as much as the infrared procedure.

4.2.2 JTAG

Existing institutionalized interfaces for perusing information are incorporated with a few cell phones, e.g., to get position information from GPS gadget (NMEA) or to get deceleration data from airbag units.

Not every single cell phone give such a neither institutionalized interface nor does there exists a standard interface for every single cell phone, however all makers have one issue in like manner. The scaling down of gadget segments opens the question how to consequently test the usefulness and nature of the bound coordinated segments. For this issue an industry gathering, the Joint Test Action Group (JTAG), built up a test innovation called limit examine.

Notwithstanding the institutionalization there are four obligations before the JTAG gadget interface can be utilized to recuperate the memory. To find the right bits in the limit filter enroll one must know which processor and memory circuits are utilized and how they are associated with the framework transport. At the point when not accessible from outside one must discover the test focuses for the JTAG interface on the printed circuit board and choose which test point is utilized for which flag. The JTAG port is not generally welded with connectors, to such an extent that it is once in a while important to open the gadget and re-patch the get to port. The convention for perusing the memory must be known lastly the right voltage must be resolved to anticipate mischief to the circuit.

The limit filter creates an aggregate scientific picture of the unstable and non-unpredictable memory. The danger of information change is limited and the memory chip doesn't need to be desoldered. Producing the picture can be moderate and not every cell phone are JTAG empowered. Likewise, it can be entangled to discover the test get to port.[13]

4.3 Command line instruments

4.3.1 System charges

Cell phones don't give the chance to run or boot from a CD, interfacing with a system impart or another gadget to clean devices. Subsequently, framework orders could be the best way to spare the unpredictable memory of a cell phone. With the danger of customized framework summons it must be assessed if the unpredictable memory is truly imperative. A comparable issue emerges when no system association is open and no auxiliary memory can be associated with a cell phone in light of the fact that the unstable memory picture must be saved money on the inside non-unpredictable memory, where the client information is put away and most plausible erased critical information will be lost. Framework charges are the least expensive technique, yet include a few dangers of information misfortune. Each summon custom with alternatives and yield must be reported.

4.3.2 AT charges

AT charges are old modem summons, e.g., Hayes order set and Motorola telephone AT orders, and can therefore be utilized on a gadget that has modem bolster. Utilizing these orders one can just get data through the working framework, with the end goal that no erased information can be extricated.

4.4 Non-scientific business instruments

4.4.1 Flasher instruments

A flasher instrument is customizing equipment as well as programming that can be utilized to program (streak) the gadget memory, e.g., EEPROM or blaze memory. These devices for the most part begin from the maker or administration communities for troubleshooting, repair, or update administrations. They can overwrite the non-unstable memory and a few, contingent upon the maker or gadget, can likewise read the memory to make a duplicate, initially proposed as a reinforcement. The memory can be kept from perusing, e.g., by programming charge or pulverization of wires in the read circuit.

Besides, unique items remove diverse measures of information from various gadgets. This prompts an exceptionally complex scene when attempting to outline the items. When all is said in done this prompts a circumstance where testing an item widely before buy is emphatically suggested. It is very normal to use no less than two items which blend each other.

5. Conclusion

In this report, review the methods by and by for android based PDA scientific. The study is essentially in light of procurement of information from the gadget and apparatuses utilized for android OS. The review work which incorporates qualities like free or restrictive, number of gadgets the support is accessible, and alternate stages separated from android where these devices can bolster. Free instruments give bunches of existing APIs to criminological specialists to utilized and expand the system, exclusive devices like Forensic are enhanced with loads of elements and revealing strategies including GUI based diagrams, with most elevated number of gadget backings.

References

[1] Radicati Group, Inc. “Email Statistics Report, 2014-2018,” 14-April- 2016; http://www.radicati.com/wp/wp-content/uploads/2014/01/EmailStatistics-Report-2014-2018-Executive-Summary.pdf.
[2] Joseph, Neethu, et al. "Volatile Internet evidence extraction from Windows systems." Computational Intelligence and Computing Research (ICCIC), 2014 IEEE International Conference on. IEEE, 2014.
[3] Heriyanto, Andri P. "Procedures and tools for acquisition and analysis of volatile memory on android smartphones." (2013)
[4] Al-Zarouni, Marwan. "Tracing E-mail Headers." Australian Computer, Network & Information Forensics Conference. 2004.
[5] Nurse, Jason RC, et al. "Investigating the leakage of sensitive personal and organisational information in email headers." Journal of Internet Services and Information Security (JISIS) 5.1 (2015): 70-84.
[6] Google. “Ice Cream Sandwich,” 14-April-2016; http://developer.android.com/about/versions/android-4.0- highlights.html#UserFeatures.
[7] Thing, Vrizlynn LL, Kian-Yong Ng, and Ee-Chien Chang. "Live memory forensics of mobile phones." digital investigation 7 (2010): S74-S82.
[8] Leppert, Simon. "Android memory dump analysis." Student Research Paper, Chair of Computer Science 1 (2012).