*ANDROID EXTRACTION DEVICES DATA AND INFORMATION*

Based on the research findings of NIST (National Institutes of Standards and Technology), methodology for forensics may be implemented in four stages; device access, acquisition of device data, testing and report [Wayne; et al(May 2007)]. Furthermore, the implementations of custom ROMS that allow modifications to the original system structure, password and device data encryption. Application used are device dependent are all challenges that could hinder or possibly terminate forensic analyses of individual devices.

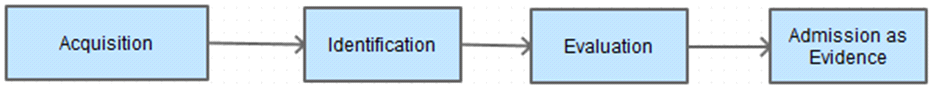
METHODOLOGY

PREPARE FOR AN INVESTIGATION: -

Ensuring that evidence devices are “write protected” in the sense that a mobile forensics analyst must ensure that the mobile device obtained at a crime scene or suspect must be kept in a static state, preventing the device from making changes to a last know record or log. This can be achieved by making sure that the device is kept from accessing any form of settings change or network connections

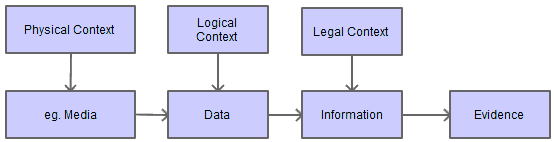
The primary goal of this report is to perform Full forensics analysis of android mobile device and internal memory using Linux Open source forensic tools (Kali-Linux). We will analyze all the partition memory, which is of forensic interest with respect to application, email, contacts , call logs , messaging application data logs etc. We will also perform data recovery from formatted partitions and corrupted partitions. The Process has been divided into three steps which follow the widely accepted procedure for forensic analysis. In this Process, the android device is ‘rooted’ using well known rooting application to obtain the raw image of the phone and the internal memory of the device using the DD command.

We also recommend that more than one forensic tool that perform a particular task is used in each step to ensure accuracy and reproducibility of results



ACQUIRING DATA

This refers to making copies of the evidence device internal storage, system, cache as well as any external S.D cards. The reason for this is that the core foundations of forensics in general is reliability and reproducibility of results without altering the content or state of the evidence device.



Data acquisition is done in 3 forms:

Manual acquisition

Utilizing user interfaces of various devices inorder to browse its available content, Traditionally, the analysts keeps picture record of each screen that contains required data. This process does not involve the use of any tool to perform data acquisition providing access to only content visible to users on the device.

Physical Acquisition

Mirroring or Cloning of the device’s content is done, including deleted data and unallocated spaces.

Logical Acquisition

Data / Information on Android mobile devices is obtained through device synchronization tools (Basically). The tools used for this process is usually free and open source based

Brute force acquisition

Built-in Security

Many modern devices have built-in layers of security protocols in order to protect content. These security layers come in many forms; varying from simple four-digit PINs to more complex and long passcodes as well as pattern-locks, newer versions of mobile device provide a more secure option with fingerprint-locking technology and biometrics to identify user some commercial tools may provide security override and bypasses, but this is may differ from different versions of security features covering every device. Some mobile devices can provide directory and file protection with or without third party applications. Newer Operation systems also provide full-Disk encryption which is quite complex to decrypt, sandboxing which ensures that eat application running is mutually exclusive to other applications running on the same unless specified by the user in the setting up of the applications, thus each application is installed in its own sandbox directory this way data within this up is guaranteed some level of protection

Brute force acquisition which is a sequential key prediction technique that can be performed using third party tools, which send a series of passcodes predictions to the mobile device. This is a time consuming method, but effective nonetheless. Brute forcing tools are connected to the device and will physically send codes onto the device until it hits the correct user keycode.

Physical Acquisition – by Rooting the Android device

In the process, the Android device is rooted while connected to the computer using a USB cable with USB debugging enabled. We ensure that the rooting software used does not make changes to the phone data and avoid data loss. After the rooting process the device enables root user privileges; this will ensure the imaging software acquires the entire phone internal and physical memory content. FTK Imager which is a graphical imaging software is used to create an image file the phone content. Also the Linux command DD is used to create the same image. ( We use two different imaging approaches to ensure data integrity and accuracy of results.) The sizes of the Inage files are recorded together with their hashing value

MD5sum and FTK hashing tools are used to obtain and compare the Hashing values of both images; if the hash values are equal/same then the imaging process was successful.

Android SDK tools can also be used to perform the same process. The target here is to obtain the various file/ memory partitions of Android device (/Cache, /system and /Data)

Physical Acquisition -JTAG

The default interfaces for analyzing data are built into several existing mobile phones eg. Obtaining proximity and geotag information from GPSE devices or to record the rate of deceleration of airbag units. For the physical acquisition of certain android volatile and non-volatile memory the author integrates the JTAG standard using a device called the Riff-Box

Many of the mobile devices in existence do not provide these interfaces or a standard interface for all mobile devices, a major setback for many manufacturers is the Small form Factor of device components which restricts ways in which the functionality and quality of integrated components soldered together can be tested. Therefore, in order to solve this problem, the Joint Test Action Group(JTAG) proposed a testing procedure called the Boundary scan, which then became a standard for testing.

Despite this Standardization, memory recovery of JTAG interfaced devices requires four steps; the processor and memory electronic circuits used and connected to the system bus must be known in order to find the correct bits in the register of boundary scan. If this procedure cannot be accessed externally, the circuit board is used to find test points for the JTAG interface and the signaling pattern for each test point. It is not a necessity to always solder the JTAG port with connectors. An alternative can be to open the device and re-solder the access port. The maximum tolerated voltage and memory reading protocol must be determined before any action is performed to avoid damaging the circuit. The boundary scan provides a complete image of the temporary and permanent memory components in a forensically sound procedure. Thus, reducing the risk of data alterations and prevents de-soldering of the memory chip. Image generation can be slow, different devices come with different interfaces that do not enable JTAG and finally the difficulty in determining the access port are all constraints in this procedure.

ANALYSE DATA

Once the disk image (Bit by bit copy of storage components) of an evidence device is obtained. The Analyst must analyze the content of the disk image e.g. (Conducting a search based on key words.)

Examination and analysis overview

Technology advances continuously; resulting in the alteration and advancement of mobile device structure and features; many of the mobile devices today use a high level file system similar to that of computers, therefore the approach in computer related forensics could be applied to these mobile devices with slight modifications to the original procedures. The NAND memory uses the File Allocation Table file system with the main difference being the block size used which is larger in hard disk and the memory type used. There are many commercial and Open source tools that can be used to extract content from a memory image; automated forensics tools or generic file system viewers (HEX EDITORS) can search the characteristics of file headers. Hex Editors provide an advantage of detailed view of the memory structure and management. But this tool requires a high level of expertise in file system headers and pattern analysis. With this, specialized softwares have been developed to facilitate the search and extraction of memory content though they are limited in the scope of their search. AccessData, Sleuthkit, and EnCase are forensic software products to analyze memory images. Since there is no tool that extracts all possible information, it is advisable to use two or more tools for examination.

Analysis using Linux based tools

The Author of this report begins analysis by implementing at least 2 different data analyzing software and procedures. The first and most important step before any kind of data analysis is conducted is to verify the integrity of the Disk Image before any disk writing process occurs. This is normally done by storing the original Hash value of the disk image; Kali Linux forensics tools provide many Open Source means of obtaining a Disk image or any type of data’s Hashing Value using MD5SUM.

Our next step is to create a report of the Case to be conducted; recording the Date of research, researchers involved, size of Disk image, hashing value of Disk Image and any other Critical information for record keeping. Kali-Linux also provides forensic tools that perform Forensics Case Creation and Report Writing such as ENCASE. As u may have noticed by now, our target tools suite for this Forensics Report is the Kali-Linux Open Source Forensics Tools because we aim at providing the opportunity for not only Professional Forensics Analysts but users and students to perform some kind of Forensics research, also, to allow users to acknowledge the vulnerable nature of their Personal Identifiable Information (PII) on any digital device and take measures to secure their Data.

Next is to Analyze the content of the Disk image present. This is done by two ways:

* Analyze disk image by exploring the Directory/ File system of the Disk image;

This basically refers to gaining access into the Disk Image and viewing the contents of the various directories by using the Kali-Linux Forensics File explorer tools.

* Analyzing the Bitwise Structure of Disk Image or Partitions:

A more advanced form of analysis where the Disk image is opened in a bitwise/ hexadecimal structure. This is the raw format of the data in the Disk image using Kali-Linux HEX-EDITOR tools which enables forensics analysts to study the Hexadecimal structure of the file to identify Bit/Hex trends by implementing advance Bit restructuring techniques (Bit shifts and Key Shifts). This is done in most advance evidence cases because many cyber criminals hide important information in the Phones file structure using hidden partitions and bit-cloning.

Data Recovery and File Carving

Overview:

This Process of Data Access, it is required that a disk Image of the entire device Memory is obtained and the Hashing value is maintained (No form of change is made to the content of the evidence drive). The theory in this is that; many Digital devices in general does not necessarily “Delete” Information that the user wants to remove. Rather, the bit pattern of the file or content is scattered across the entire volume of the disk or the access list identifier for that unique data is remove. Thereby rendering the file or data inaccessible.

This does not mean that the file is completely deleted from the storage device. But a new form of data placed in the previous location of the deleted file may overwrite the hidden/scattered bit pattern of the deleted file. This will reduce the amount of deleted information that can be recovered. Thus we ensure that in performing Digital Forensics in general, the integrity of the evidence device is maintained.

Process:

Our Process of Data recovery also referred to as “File carving” will implement Kali-Linux Forensics tool such as Scarpel and “foremost “, which provides some degree of data recovery for examination purposes only. With many of the Forensics tools in the Kali Linux Forensics Suite, a unique syntax is developed and must be followed.

Syntax:

EVIDENCE PRESENTATION: -

After the analysis of data, the Analyst must conclude and produce the results obtained in the form of a report.

Summary

Over the year’s new models of mobile devices are manufactured with continuous improvements made to their file system structure and form factor. Recent devices have been developed with a closed Operating system making analysis of content with forensic tools much more complex and time consuming. Our aim is to bridge the vast void by giving the forensics community an in-depth sight of mobile forensics techniques using a systematic approach based on widely accepted forensics standards.