Android Mobile Forensic Analyzer for Stegno data

Walter. T. Mambodza
Department of Information Technology
SRM University
Chennai, India
wales4000@gmail.com

NagoorMeeran A.R
Department of Information Technology
SRM University
Chennai, India
nagooris@gmail.com

***Abstract* -The advancement of technology has led to better and improved service in mobile communication networks. Smartphones are being used by people for social networking, conducting business transactions as well as committing crime. Anti-Forensic compromises the availability of evidence to the forensic process causing problems to the investigator. The aim of this paper is to provide a solution to the anti-forensic technique of steganography by designing and implementation of an application that will scan, hash and analyze for any hidden information on an image, video or audio file on an android device and collect data for digital profiling or investigation.**

Keywords: Anti-forensics, Steganography, Android, Investigation

1.INTRODUCTION

Smartphones are no longer a necessity but a style of living. They can be used for communication, social networking and daily consumption. Statistics indicate that 51% of users in the world are using devices with Android OS [23]. The increase in the usage of smartphones has led to the rise of crime related to mobile devices. Smartphones are a great source of forensic evidence. Android forensics is a field in digital and mobile forensic, an investigation comprises of two parts which are Data Collection and Data Analysis. In Data acquisition collection of information can be performed in two ways which are logical or physical acquisition.

A logical technique extracts allocated data by accessing the file system. Allocated data means that the data is not deleted and is accessible on the file system except some files, such as a SQLite database, they can be allocated but still contain deleted records in the database. Recovering the deleted data requires special tools and techniques. A logical acquisition can recover deleted data [22].Physical techniques target the physical storage medium directly and do not rely on the file system itself to access the data. The advantage is that physical techniques 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. Physical forensic techniques provide direct access to storage medium; it is possible to recover both the allocated and the unallocated data [22].The analysis of an Android physical acquisition is 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 even provide direct access to the file system and it really operates at a more abstract and less effective level than traditional logical technique which can acquire all non-deleted data directly from the file system. This technique, which relies on the Content Providers built into the Android platform and SDK, is effective in producing some important forensic data, but only a fraction of the data available on the system. They are various tools and different methodologies that can be used to acquire the data but most of them they do not preserve the integrity of data. The Association of Chief Police Officers produced the “Good Practice Guide for Computer Based Electronic Evidence” which lays down 4 principles of handling and processing digital device [10] When performing data acquisition or analysis in a forensically sound manner, digital contamination has to be avoided by all means and the investigator has to record all the details. However they are various Anti- forensic techniques that are available that makes it difficult for an Investigator or Forensic Analyst to acquire reliable data. Some of the anti-forensic techniques can be classified as Data Hiding (Encryption, Steganography), Artifact wiping, Trail obfuscation and Attacks against processes and tools [1].

978-1-4799-7075-9/15/$31.00 ©2015 IEEE

This research proposes a solution to the anti-forensic technique of steganography by designing and developing an application that will detect the presence of stegno data within the android device and then perform logical data acquisition of images, videos and audio files.

2. LITERATURE REVIEW

Mobile devices on android are conducive to anti-forensic activities. Researchers modify CyanogenMod community distribution of Android OS. To prevent data extractions, blocked the installation, created extraction delays and presented false data. They classified anti-forensics as Data hiding, Artifact wiping, Trail obfuscation and attacks against processes and tools. The authors used a 5 step methodology to execute experiment; investigate OS modifications, consult Android documents, modified the content providers, created and entered a data set into the phone and performed forensic extractions using Cellebrite and XRY. Used both USB debugging on and off through the use of Android Debugging Bridge [1].

File formats leave room for interpretations. They explored AVI and MP4 of mobile phones & camera. Customized parsers to extract file format structures for 19 digital cameras, 14 mobile cameras and 6 video editing toolboxes. They concluded that videos employ different container formats and compression codecs. The structure of AVI and MP4 containers not strictly defined. The research helps to authenticate original &post processed videos. It is also important in verifying source & identify device used for acquisition [2] Steganography means hidden writing i.e. hiding of data in image, video or audio file. They created a formula which is: cover medium+hiddeninformation+stegokey=stego medium. Steganography is important when protecting private information where cryptograhy is not allowed. Two techniques of steganography are used are watermarking and cover channel. Steganalysis is discovering hidden data. Two techniques to detect hidden data are steganography signatures and visual detection. Steganalysis is an effective tool for protecting information. Steganography hinders law enforcement to gather evidence to stop illegal activities [3].

The researchers explored methods of getting access to, extracting and initial analyzing non-volatile stored data from smart phones taking into considerations forensic principles like evidence dynamics, chain of custody, evidence integrity and order of volatility. The aim was to present current work on extraction methods and how to do initial analysis of the extracted data for comparison with known methods between devices. Mobile smart devices have various versions, they have evolved. Some reasons for trying to get access to data on mobile devices are to install pirated software, circumvent restrictions, install malicious code, perform backups, restore incidental deleted files, verifying security features or extracting data for forensic analysis. The integrity of preserved data must be assured by applying hashing algorithms. A recent market survey indicates more than 60% of Android phones do not support native encryption in the OS. The researchers concluded that in terms of security Android OS has optional encryption in newer OS. The file system is YAFFS, EXT4 or FAT [4].

Data acquisition is crucial in mobile forensics. The researchers elaborate on a concept Live SD that makes use of data recovery to perform physical data acquisition in Android smart phones. The data acquisition methodology differs from most mobile forensics software. Live SD is therefore proposed to utilize the Recovery mode in Android platform to ensure data integrity by copying data from the database. Physical acquisition drives the internal mobile system service and copy the bit content in physical memory with specific communication protocols connecting the targeted mobile phones and professional forensic hardware via cables. Logical acquisition alternatively can access internal information logically with specific software. Researchers concluded that Android is a fast developing and popular smart phone operating system, is capable of software augmentation and contains very important personal information. Tool helps to acquire information from victim's phone after an incident happens. The forensic software does not need to be installed to prevent potential issue of modifying the crime scene [5].

The researchers proposed an automated system to perform a live memory forensic analysis for mobile phones. They investigated the dynamic behavior of the mobile phone's volatile memory. The analysis is useful in real-time evidence acquisition analysis of communication based application. The digital forensic procedure involves acquiring data from the static media, analyzing and correlating the data to retrieve the relevant evidence in a forensic sound manner. The forensic investigation procedure prevents contamination of potential evidence, is well documented and is reliable and accepted by the law enforcement agencies. Live analysis of the current state of the system and its application allows an efficient forensic process. Techniques to protect the privacy and confidentiality of user data such as encryption, steganography provides counter forensic means to technologically aware criminals [6].

Smartphones and mobile devices are being used by hackers to spread malware. There is need to have a secure forensic analyst system which can examine, divide and correlate mobile applications. In this paper they presented to design and implement a signature based analytic system that automatically collect, manage, analyze and extract android malware. They demonstrated the efficiency of the application using various Android applications and discovered lots of zero- day malware. Malware on smartphones is also increasing at unprecedented rate and Android OS based systems being the most popular platform for mobile devices [7].

The aim of steganalytic forensic is to extract hidden messages embedded in stenographic images. A technique that partially addresses the problem is the stenography payload location it reveals the message bits, not their logical order. Functions by finding modified pixels, residuals, as an artifact of the embedding process. The technique is successful against least significant bit steganography and group parity steganography. The researchers establishes an important result addressing this shortcoming, they show that the expected mean residuals have enough information to logically order the located payload if the size of the payload in each stego image is not fixed [8].

3. OBJECTIVES

Objective of the project work is to provide a solution to the Anti-Forensic technique of steganography by designing and developing an application that will hash, scan, analysestegno data in images, audio and video files and extract files in a forensically sound manner from an Android device

4. SCOPE

- The application will only provide a solution to anti-forensic technique of steganography
- The hashing algorithm used will be MD5
- Analysis of stegno data will be on png, mp3 and mp4 file formats
- Implementation of solution is going to be done on mobile device with Android OS.

5. METHODOLOGY

This research aims to provide a solution to the Anti-Forensic technique of steganography on mobile devices running on Android OS. The following steps were executed

The **first step** was to investigate on Digital and Mobile forensics. In order to achieve this information from various sources were gathered. The Association of Chief Police Officers produced the “Good Practice Guide for Computer Based Electronic Evidence” which lays down 4 principles of handling and processing digital device [10].

The **second step** consulted Android documents for procedures on carrying out Android forensics [22]. The use of USB debugging connection to extract data from Android phones. While a USB device (Android phone) must identify itself to the host (i.e. a forensic analysis system). This means there has to be a mechanism that provides a link between the devices such as the use of Android Debugging Bridge (ADB) [17].

The **third step** is designing the Android mobile forensic analyzer as a forensic tool. This application performs a hash function to the option selected to preserve the integrity of data. The application has a module for scanning to check if there is any data hidden within the files on the Android device. The application has an extraction and report button.

The **fourth step** is entering a data set on the phone. This is achieved by using an application developed by the researchers which uses the least significant bit steganography to embed data on the images, audio or video file on the phone.

The **fifth step** is to perform analysis and extractions using the Android Mobile Forensic Analyzer designed. The analysis is conducted with a phone running on Android OS connected to the application via a USB connection and making use of the USB debugging connection and Android Debugging bridge (ADB). A report is generated to aid in further analysis and decision making.

It should be noted that this research is intended to be a proof of concept that enables Forensic Investigators to examine mobile phones running on Android OS and ensures the availability of potential evidence.

6. Proposed Solution

We proposed an Android Mobile Forensic Analyzer that can be used for detecting hidden data on an image, video or audio file and extracting files from the mobile device in a forensically sound manner. To achieve these the Android Mobile Forensic Analyzer has to preserve the integrity of data and perform the following;

- ➢ Hash function
- ➢ Scan
- ➢ Extract files

- Hash function is very crucial in hashing of the image, audio or video file to ensure that there is no digital contamination.
- An MD5 hash function is used to generate a 16 digit hash value.

- Scanning and analysis of the files on the Android device will ensure that data acquisition is reliable and all data on device is made available to investigation process.

The process entails the discovery of detection of stegno data if there is any. It provides a thorough analysis of embedded data.

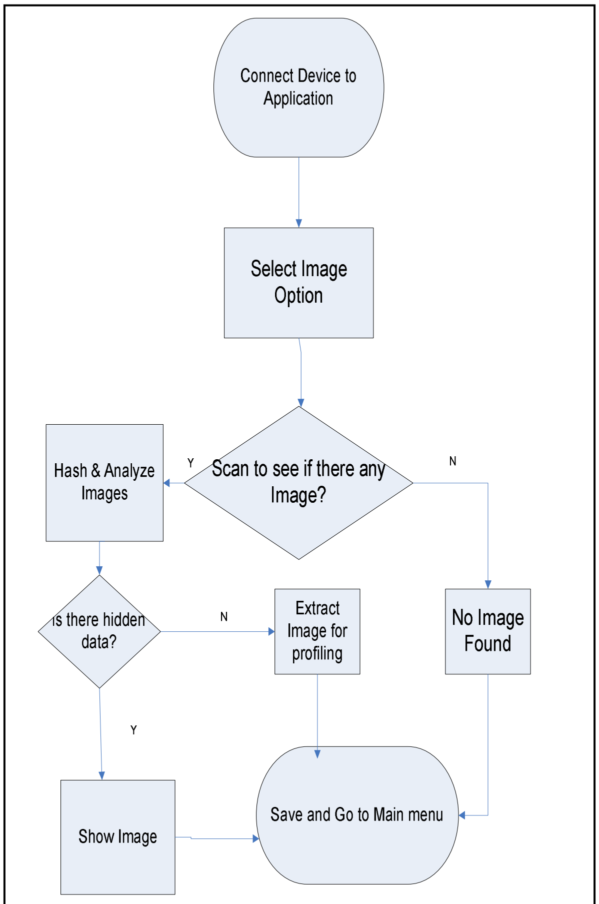


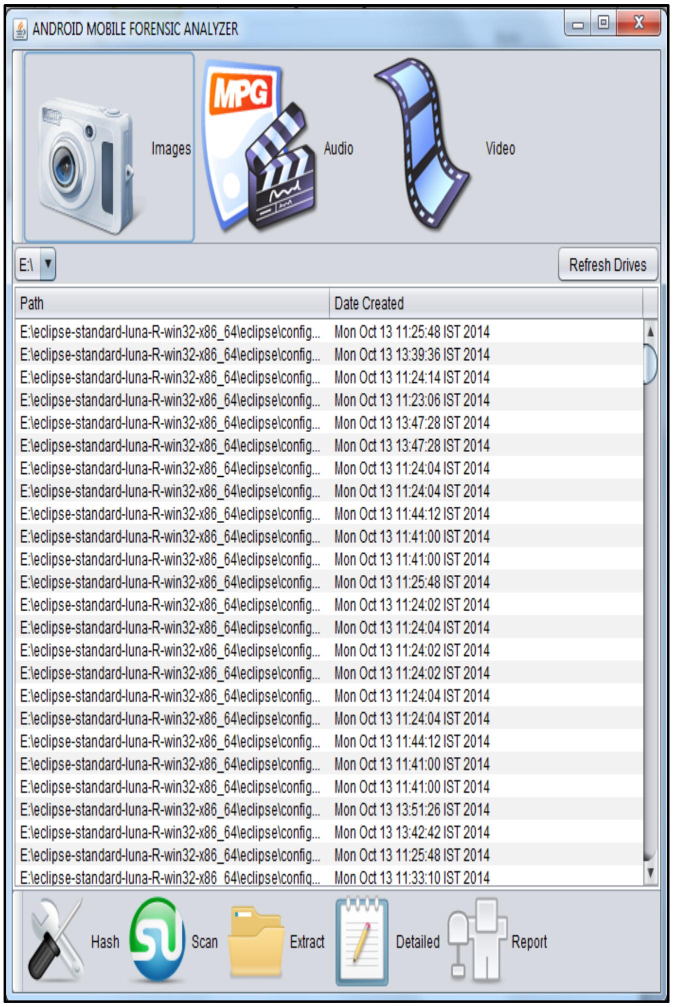
Fig 1- Flow chart of proposed solution

7. IMPLEMENTATION AND RESULTS

The Android Mobile Forensic Analyser developed by the author has 3 main functions which are hashing, scanning and extraction. A Moto G (2nd generation) running on Android 4.4.4 version (Kitkat) was used as an experiment. The Application was connected the Android device through the use of a USB connection when USB debugging was on.

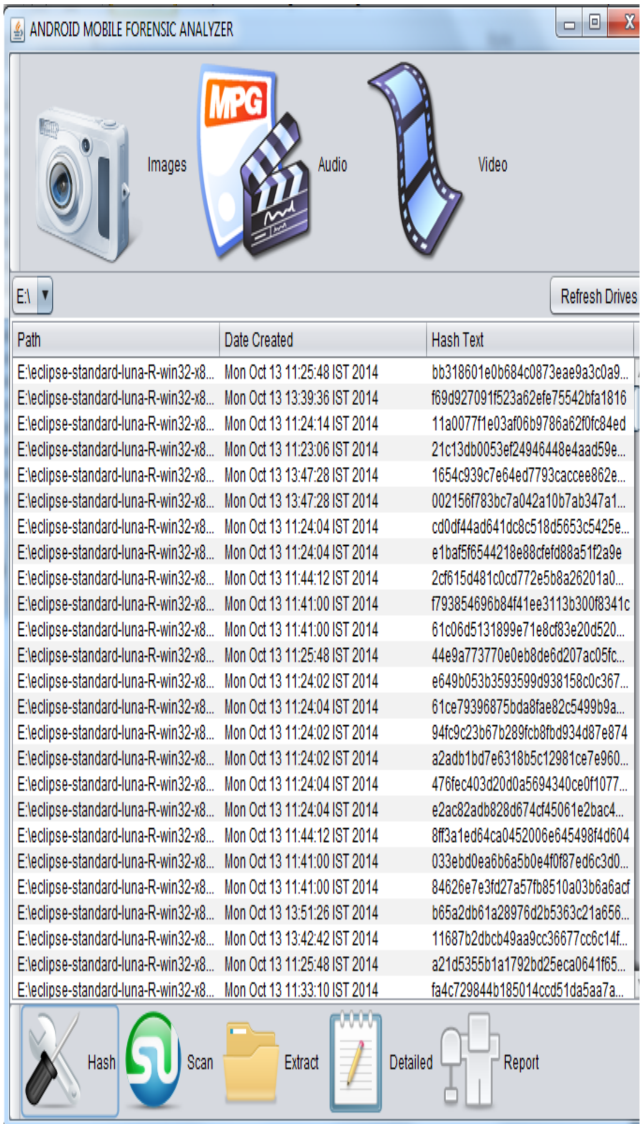
7.1HASHING

Is used in producing hash values for data integrity and security, a hash value, also called a message digest, is a number generated from a string of text. The hash plays a crucial role in Android Mobile Forensic Analyzer because they ensure that files have not been tampered with. The MD5 message-digest algorithm produces a 128-bit (16-byte) hash value, typically expressed in text form. MD5 has been used to verify data integrity. Fig 2.0 shows images that have been retrieved by the application developed and Fig 3.0 shows hash text for images retrieved.



Path	Date Created
E:\eclipse-standard-luna-R-win32-x86_64\eclipse\config...	Mon Oct 13 11:25:48 IST 2014
E:\eclipse-standard-luna-R-win32-x86_64\eclipse\config...	Mon Oct 13 13:39:36 IST 2014
E:\eclipse-standard-luna-R-win32-x86_64\eclipse\config...	Mon Oct 13 11:24:14 IST 2014
E:\eclipse-standard-luna-R-win32-x86_64\eclipse\config...	Mon Oct 13 11:23:06 IST 2014
E:\eclipse-standard-luna-R-win32-x86_64\eclipse\config...	Mon Oct 13 13:47:28 IST 2014
E:\eclipse-standard-luna-R-win32-x86_64\eclipse\config...	Mon Oct 13 13:47:28 IST 2014
E:\eclipse-standard-luna-R-win32-x86_64\eclipse\config...	Mon Oct 13 11:24:04 IST 2014
E:\eclipse-standard-luna-R-win32-x86_64\eclipse\config...	Mon Oct 13 11:24:04 IST 2014
E:\eclipse-standard-luna-R-win32-x86_64\eclipse\config...	Mon Oct 13 11:44:12 IST 2014
E:\eclipse-standard-luna-R-win32-x86_64\eclipse\config...	Mon Oct 13 11:41:00 IST 2014
E:\eclipse-standard-luna-R-win32-x86_64\eclipse\config...	Mon Oct 13 11:41:00 IST 2014
E:\eclipse-standard-luna-R-win32-x86_64\eclipse\config...	Mon Oct 13 11:25:48 IST 2014
E:\eclipse-standard-luna-R-win32-x86_64\eclipse\config...	Mon Oct 13 11:24:02 IST 2014
E:\eclipse-standard-luna-R-win32-x86_64\eclipse\config...	Mon Oct 13 11:24:04 IST 2014
E:\eclipse-standard-luna-R-win32-x86_64\eclipse\config...	Mon Oct 13 11:24:02 IST 2014
E:\eclipse-standard-luna-R-win32-x86_64\eclipse\config...	Mon Oct 13 11:24:02 IST 2014
E:\eclipse-standard-luna-R-win32-x86_64\eclipse\config...	Mon Oct 13 11:24:04 IST 2014
E:\eclipse-standard-luna-R-win32-x86_64\eclipse\config...	Mon Oct 13 11:24:04 IST 2014
E:\eclipse-standard-luna-R-win32-x86_64\eclipse\config...	Mon Oct 13 11:44:12 IST 2014
E:\eclipse-standard-luna-R-win32-x86_64\eclipse\config...	Mon Oct 13 11:41:00 IST 2014
E:\eclipse-standard-luna-R-win32-x86_64\eclipse\config...	Mon Oct 13 11:41:00 IST 2014
E:\eclipse-standard-luna-R-win32-x86_64\eclipse\config...	Mon Oct 13 13:51:26 IST 2014
E:\eclipse-standard-luna-R-win32-x86_64\eclipse\config...	Mon Oct 13 13:42:42 IST 2014
E:\eclipse-standard-luna-R-win32-x86_64\eclipse\config...	Mon Oct 13 11:25:48 IST 2014
E:\eclipse-standard-luna-R-win32-x86_64\eclipse\config...	Mon Oct 13 11:33:10 IST 2014

Fig2 - Images retrieved from Android Device

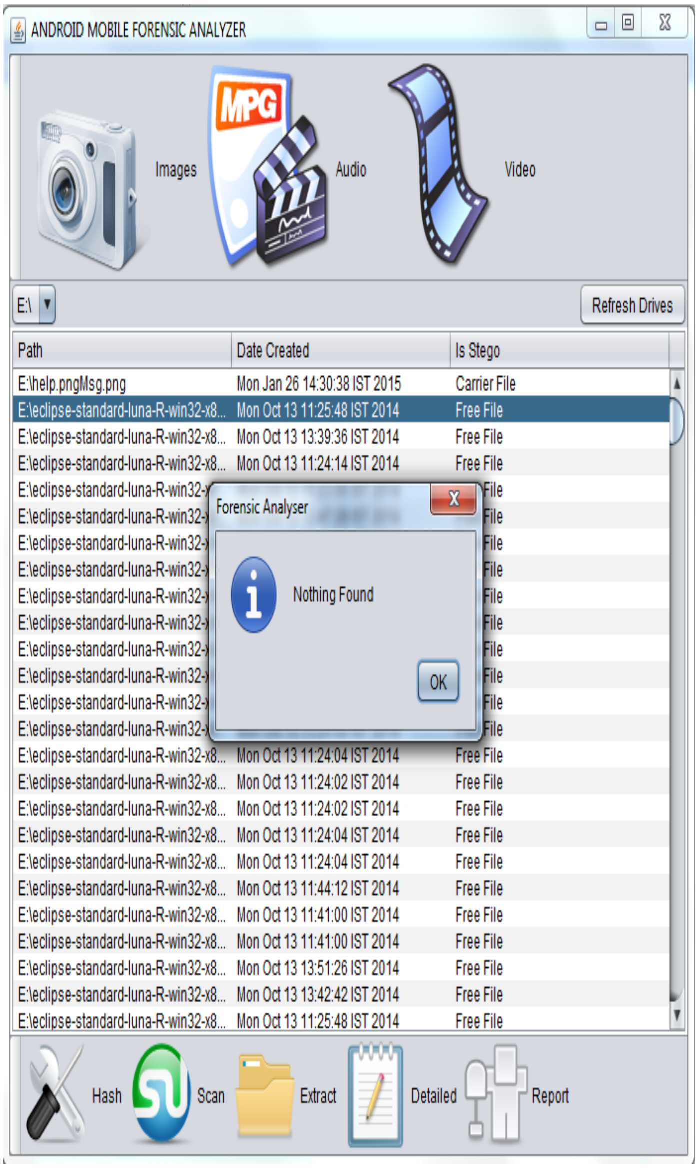


Path	Date Created	Hash Text
E:\eclipse-standard-luna-R-win32-x8...	Mon Oct 13 11:25:48 IST 2014	bb318601e0b684c0873eae9a3c0a9...
E:\eclipse-standard-luna-R-win32-x8...	Mon Oct 13 13:39:36 IST 2014	f69d927091f523a62efe75542bfa1816
E:\eclipse-standard-luna-R-win32-x8...	Mon Oct 13 11:24:14 IST 2014	11a0077f1e03af06b9786a62f0fc84ed
E:\eclipse-standard-luna-R-win32-x8...	Mon Oct 13 11:23:06 IST 2014	21c13db0053ef24946448e4aad59e...
E:\eclipse-standard-luna-R-win32-x8...	Mon Oct 13 13:47:28 IST 2014	1654c939c7e64ed7793caccee862e...
E:\eclipse-standard-luna-R-win32-x8...	Mon Oct 13 13:47:28 IST 2014	002156f783bc7a042a10b7ab347a1...
E:\eclipse-standard-luna-R-win32-x8...	Mon Oct 13 11:24:04 IST 2014	cd0df44ad641dc8c518d5653c5425e...
E:\eclipse-standard-luna-R-win32-x8...	Mon Oct 13 11:24:04 IST 2014	e1baf5f6544218e88cfefd88a51f2a9e
E:\eclipse-standard-luna-R-win32-x8...	Mon Oct 13 11:44:12 IST 2014	2cf615d481c0cd772e5b8a26201a0...
E:\eclipse-standard-luna-R-win32-x8...	Mon Oct 13 11:41:00 IST 2014	f793854696b84f41ee3113b300f8341c
E:\eclipse-standard-luna-R-win32-x8...	Mon Oct 13 11:41:00 IST 2014	61c06d5131899e71e8cf83e20d520...
E:\eclipse-standard-luna-R-win32-x8...	Mon Oct 13 11:25:48 IST 2014	44e9a773770e0eb8de6d207ac05fc...
E:\eclipse-standard-luna-R-win32-x8...	Mon Oct 13 11:24:02 IST 2014	e649b053b3593599d938158c0c367...
E:\eclipse-standard-luna-R-win32-x8...	Mon Oct 13 11:24:04 IST 2014	61ce79396875bda8fae82c5499b9a...
E:\eclipse-standard-luna-R-win32-x8...	Mon Oct 13 11:24:02 IST 2014	94fc9c23b67b289fcb8fbd934d87e874
E:\eclipse-standard-luna-R-win32-x8...	Mon Oct 13 11:24:02 IST 2014	a2adb1bd7e6318b5c12981ce7e960...
E:\eclipse-standard-luna-R-win32-x8...	Mon Oct 13 11:24:04 IST 2014	476fec403d20d0a5694340ce0f1077...
E:\eclipse-standard-luna-R-win32-x8...	Mon Oct 13 11:24:04 IST 2014	e2ac82adb828d674cf45061e2bac4...
E:\eclipse-standard-luna-R-win32-x8...	Mon Oct 13 11:44:12 IST 2014	8ff3a1ed64ca0452006e645498f4d604
E:\eclipse-standard-luna-R-win32-x8...	Mon Oct 13 11:41:00 IST 2014	033ebd0ea6b6a5b0e4f0f87ed6c3d0...
E:\eclipse-standard-luna-R-win32-x8...	Mon Oct 13 11:41:00 IST 2014	84626e7e3fd27a57fb8510a03b6a6acf
E:\eclipse-standard-luna-R-win32-x8...	Mon Oct 13 13:51:26 IST 2014	b65a2db61a28976d2b5363c21a656...
E:\eclipse-standard-luna-R-win32-x8...	Mon Oct 13 13:42:42 IST 2014	11687b2dbcb49aa9cc36677cc6c14f...
E:\eclipse-standard-luna-R-win32-x8...	Mon Oct 13 11:25:48 IST 2014	a21d5355b1a1792bd25eca0641f65...
E:\eclipse-standard-luna-R-win32-x8...	Mon Oct 13 11:33:10 IST 2014	fa4c729844b185014ccd51da5aa7a...

Fig.3. - Hash Text generated from Images

7.2 SCANNING

Is the process of discovering hidden data within files on an Android device. This module checks the presents of any files and analyzes each file on the mobile device running on Android OS for stegno data. It provides a solution to the Anti-Forensic technique of least significant bit (LSB) steganography by exposing hidden information that compromises the security goal of availability of information to the investigator. The scanning process follows the ACPO principles i.e. maintains data integrity, it does not tamper with data. After scanning the file is categorized as a free file or carrier file. A free file is a file that has no embedded or hidden data as shown in fig 4.0. And a Carrier file is a file that has embedded or hidden data as shown in fig 5.0.



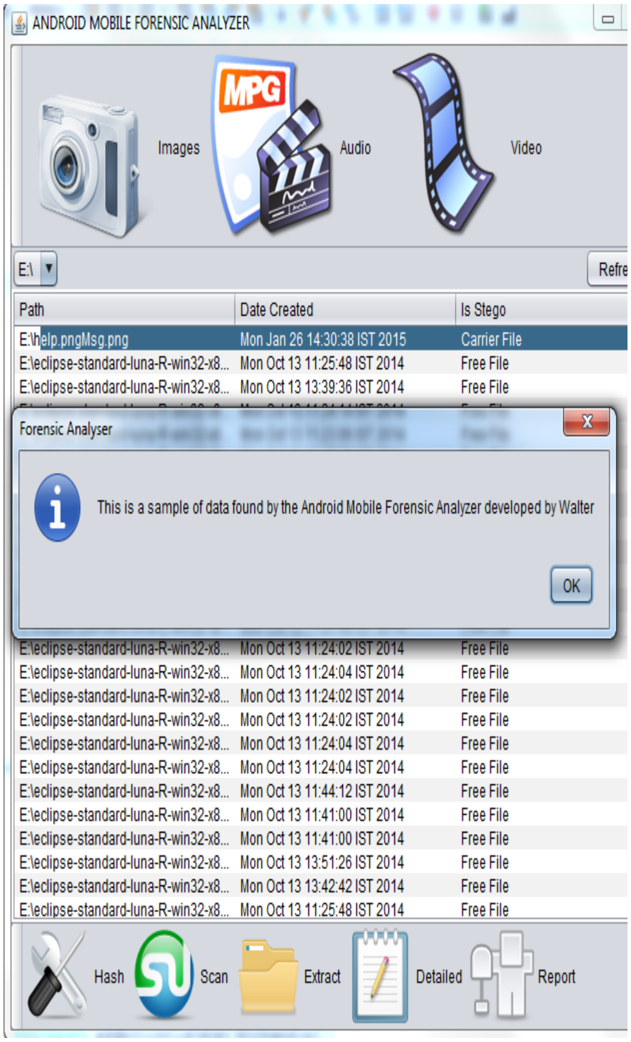
Path	Date Created	Is Stego
E:\help.pngMsg.png	Mon Jan 26 14:30:38 IST 2015	Carrier File
E:\eclipse-standard-luna-R-win32-x8...	Mon Oct 13 11:25:48 IST 2014	Free File
E:\eclipse-standard-luna-R-win32-x8...	Mon Oct 13 13:39:36 IST 2014	Free File
E:\eclipse-standard-luna-R-win32-x8...	Mon Oct 13 11:24:14 IST 2014	Free File
E:\eclipse-standard-luna-R-win32-		File
E:\eclipse-standard-luna-R-win32-		File
E:\eclipse-standard-luna-R-win32-		File
E:\eclipse-standard-luna-R-win32-		File
E:\eclipse-standard-luna-R-win32-		File
E:\eclipse-standard-luna-R-win32-		File
E:\eclipse-standard-luna-R-win32-		File
E:\eclipse-standard-luna-R-win32-		File
E:\eclipse-standard-luna-R-win32-		File
E:\eclipse-standard-luna-R-win32-		File
E:\eclipse-standard-luna-R-win32-x8...	Mon Oct 13 11:24:04 IST 2014	Free File
E:\eclipse-standard-luna-R-win32-x8...	Mon Oct 13 11:24:02 IST 2014	Free File
E:\eclipse-standard-luna-R-win32-x8...	Mon Oct 13 11:24:02 IST 2014	Free File
E:\eclipse-standard-luna-R-win32-x8...	Mon Oct 13 11:24:04 IST 2014	Free File
E:\eclipse-standard-luna-R-win32-x8...	Mon Oct 13 11:24:04 IST 2014	Free File
E:\eclipse-standard-luna-R-win32-x8...	Mon Oct 13 11:44:12 IST 2014	Free File
E:\eclipse-standard-luna-R-win32-x8...	Mon Oct 13 11:41:00 IST 2014	Free File
E:\eclipse-standard-luna-R-win32-x8...	Mon Oct 13 11:41:00 IST 2014	Free File
E:\eclipse-standard-luna-R-win32-x8...	Mon Oct 13 13:51:26 IST 2014	Free File
E:\eclipse-standard-luna-R-win32-x8...	Mon Oct 13 13:42:42 IST 2014	Free File
E:\eclipse-standard-luna-R-win32-x8...	Mon Oct 13 11:25:48 IST 2014	Free File

Forensic Analyser

Nothing Found

OK

Fig 4 - Free file



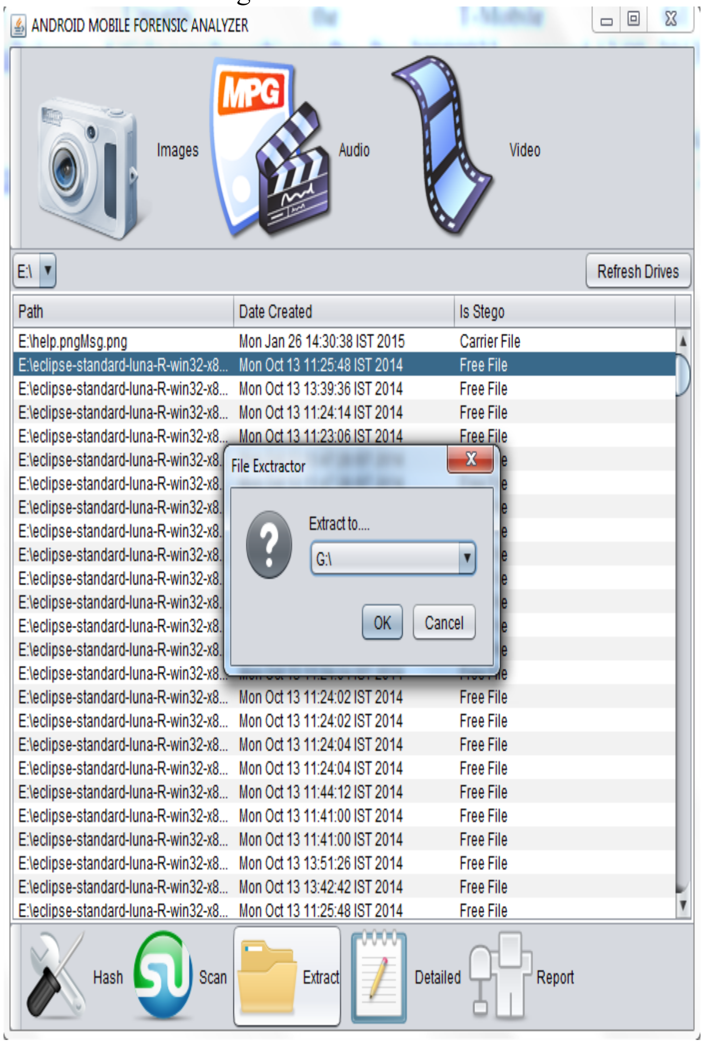
Path	Date Created	Is Stego
E:\help.pngMsg.png	Mon Jan 26 14:30:38 IST 2015	Carrier File
E:\eclipse-standard-luna-R-win32-x8...	Mon Oct 13 11:25:48 IST 2014	Free File
E:\eclipse-standard-luna-R-win32-x8...	Mon Oct 13 13:39:36 IST 2014	Free File
E:\eclipse-standard-luna-R-win32-x8...	Mon Oct 13 11:24:02 IST 2014	Free File
E:\eclipse-standard-luna-R-win32-x8...	Mon Oct 13 11:24:04 IST 2014	Free File
E:\eclipse-standard-luna-R-win32-x8...	Mon Oct 13 11:24:02 IST 2014	Free File
E:\eclipse-standard-luna-R-win32-x8...	Mon Oct 13 11:24:02 IST 2014	Free File
E:\eclipse-standard-luna-R-win32-x8...	Mon Oct 13 11:24:04 IST 2014	Free File
E:\eclipse-standard-luna-R-win32-x8...	Mon Oct 13 11:24:04 IST 2014	Free File
E:\eclipse-standard-luna-R-win32-x8...	Mon Oct 13 11:44:12 IST 2014	Free File
E:\eclipse-standard-luna-R-win32-x8...	Mon Oct 13 11:41:00 IST 2014	Free File
E:\eclipse-standard-luna-R-win32-x8...	Mon Oct 13 11:41:00 IST 2014	Free File
E:\eclipse-standard-luna-R-win32-x8...	Mon Oct 13 13:51:26 IST 2014	Free File
E:\eclipse-standard-luna-R-win32-x8...	Mon Oct 13 13:42:42 IST 2014	Free File
E:\eclipse-standard-luna-R-win32-x8...	Mon Oct 13 11:25:48 IST 2014	Free File

This is a sample of data found by the Android Mobile Forensic Analyzer developed by Walter

Fig 5 - Carrier File

7.3EXTRACTION

This module of the forensic analyzer is responsible for data acquisition. An investigation comprises of two parts that is Data Collection and Data Analysis. The extraction module performs logical acquisition of data from the mobile device running on Android OS. Images, audio and video files are extracted to the application or removable disk or evidence media in a forensically sound manner. The extraction module also maintains the data integrity. Figure 6.0 shows files being extracted.

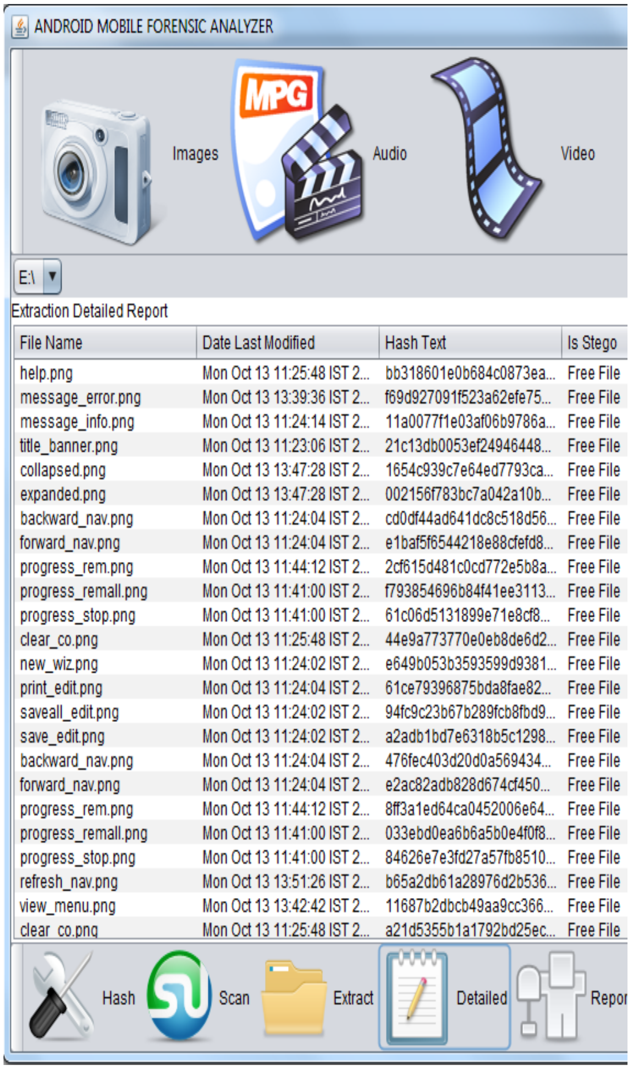


Path	Date Created	Is Stego
E:\help.pngMsg.png	Mon Jan 26 14:30:38 IST 2015	Carrier File
E:\eclipse-standard-luna-R-win32-x8...	Mon Oct 13 11:25:48 IST 2014	Free File
E:\eclipse-standard-luna-R-win32-x8...	Mon Oct 13 13:39:36 IST 2014	Free File
E:\eclipse-standard-luna-R-win32-x8...	Mon Oct 13 11:24:14 IST 2014	Free File
E:\eclipse-standard-luna-R-win32-x8...	Mon Oct 13 11:23:06 IST 2014	Free File
E:\eclipse-standard-luna-R-win32-x8.		e
E:\eclipse-standard-luna-R-win32-x8.		e
E:\eclipse-standard-luna-R-win32-x8.		e
E:\eclipse-standard-luna-R-win32-x8.		e
E:\eclipse-standard-luna-R-win32-x8.		e
E:\eclipse-standard-luna-R-win32-x8.		e
E:\eclipse-standard-luna-R-win32-x8.		e
E:\eclipse-standard-luna-R-win32-x8.		e
E:\eclipse-standard-luna-R-win32-x8.		e
E:\eclipse-standard-luna-R-win32-x8...		e
E:\eclipse-standard-luna-R-win32-x8...	Mon Oct 13 11:24:02 IST 2014	Free File
E:\eclipse-standard-luna-R-win32-x8...	Mon Oct 13 11:24:02 IST 2014	Free File
E:\eclipse-standard-luna-R-win32-x8...	Mon Oct 13 11:24:04 IST 2014	Free File
E:\eclipse-standard-luna-R-win32-x8...	Mon Oct 13 11:24:04 IST 2014	Free File
E:\eclipse-standard-luna-R-win32-x8...	Mon Oct 13 11:44:12 IST 2014	Free File
E:\eclipse-standard-luna-R-win32-x8...	Mon Oct 13 11:41:00 IST 2014	Free File
E:\eclipse-standard-luna-R-win32-x8...	Mon Oct 13 11:41:00 IST 2014	Free File
E:\eclipse-standard-luna-R-win32-x8...	Mon Oct 13 13:51:26 IST 2014	Free File
E:\eclipse-standard-luna-R-win32-x8...	Mon Oct 13 13:42:42 IST 2014	Free File
E:\eclipse-standard-luna-R-win32-x8...	Mon Oct 13 11:25:48 IST 2014	Free File

Figure 6 - Data Extraction

7.4RESULTS

The Android Mobile forensic analyzer produces a detailed report of the analysis that was done on the seized mobile device. Fig 7.0 shows a detailed report generated by the analyzer



Extraction Detailed Report

File Name	Date Last Modified	Hash Text	Is Stego
help.png	Mon Oct 13 11:25:48 IST 2...	bb318601e0b684c0873ea...	Free File
message_error.png	Mon Oct 13 13:39:36 IST 2...	f69d927091f523a62efe75...	Free File
message_info.png	Mon Oct 13 11:24:14 IST 2...	11a0077f1e03af06b9786a...	Free File
title_banner.png	Mon Oct 13 11:23:06 IST 2...	21c13db0053ef24946448...	Free File
collapsed.png	Mon Oct 13 13:47:28 IST 2...	1654c939c7e64ed7793ca...	Free File
expanded.png	Mon Oct 13 13:47:28 IST 2...	002156f783bc7a042a10b...	Free File
backward_nav.png	Mon Oct 13 11:24:04 IST 2...	cd0df44ad641dc8c518d56...	Free File
forward_nav.png	Mon Oct 13 11:24:04 IST 2...	e1baf5f6544218e88cfefd8...	Free File
progress_rem.png	Mon Oct 13 11:44:12 IST 2...	2cf615d481c0cd772e5b8a...	Free File
progress_remall.png	Mon Oct 13 11:41:00 IST 2...	f793854696b84f41ee3113...	Free File
progress_stop.png	Mon Oct 13 11:41:00 IST 2...	61c06d5131899e71e8cf8...	Free File
clear_co.png	Mon Oct 13 11:25:48 IST 2...	44e9a773770e0eb8de6d2...	Free File
new_wiz.png	Mon Oct 13 11:24:02 IST 2...	e649b053b3593599d9381...	Free File
print_edit.png	Mon Oct 13 11:24:04 IST 2...	61ce79396875bda8fae82...	Free File
saveall_edit.png	Mon Oct 13 11:24:02 IST 2...	94fc9c23b67b289fcb8fbd9...	Free File
save_edit.png	Mon Oct 13 11:24:02 IST 2...	a2adb1bd7e6318b5c1298...	Free File
backward_nav.png	Mon Oct 13 11:24:04 IST 2...	476fec403d20d0a569434...	Free File
forward_nav.png	Mon Oct 13 11:24:04 IST 2...	e2ac82adb828d674cf450...	Free File
progress_rem.png	Mon Oct 13 11:44:12 IST 2...	8ff3a1ed64ca0452006e64...	Free File
progress_remall.png	Mon Oct 13 11:41:00 IST 2...	033ebd0ea6b6a5b0e4f0f8...	Free File
progress_stop.png	Mon Oct 13 11:41:00 IST 2...	84626e7e3fd27a57fb8510...	Free File
refresh_nav.png	Mon Oct 13 13:51:26 IST 2...	b65a2db61a28976d2b536...	Free File
view_menu.png	Mon Oct 13 13:42:42 IST 2...	11687b2dbcb49aa9cc366...	Free File
clear_co.png	Mon Oct 13 11:25:48 IST 2...	a21d5355b1a1792bd25ec...	Free File

Fig 7 - Detailed Reports from Analysis

8. CONCLUSION

In conclusion the designed application provides a solution to the Anti- Forensic technique of steganography. It enables the Investigator to detect and discover hidden data within a stego image, audio or video file on Android device. The application preserves the integrity of data through the use of a powerful hash function, scan and extraction method. Though steganography is very old technique, it is a major concern especially in the domain of Android forensics. The application observes all the ACPO principles that enable the investigation process that comprises of Data collection and Data analysis to be performed in a forensically sound manner

REFERENCES

[1] Karlsson, K.J., and Glisson, W.B., “Android Anti-forensics: Modifying Cyanogen Mod”, System Sciences (HICSS), 2014

[2] Gloe, T., Fischer, A., and Kirchner, M., “Forensic Analysis of Video File Formats”, Digital Investigation, 2014

[3] Richer, P., “Steganalysis: Detecting Hidden Information with Computer Forensic Analysis”, SANS, 2003

[4] Abalenkovs, D., Bondarenko, P., Kumarraju, V., and Rekdal, J.E., “Mobile Forensics: Comparison of Extraction and Analyzing Methods of iOS and Android”, 2012

[5] Chen, S.W., Yang, C.H., and Liu, C.T., “Design and Implementation of Live SD Acquisition Tool in Android Smart Phone”, Genetic and Evolutionary Computing (ICGEC), 2011

[6] Thung, V.L.L., Ng, K.Y., and Chang, E.C., “Live Memory Forensic of Mobile Phones”, Digital Investigation, 2010

[7] Zheng, M., Sun, M., Lui, J., “Droid Analytics: A signature Based Analytic System to Collect, Extract, Analyse and Associate Android Malware”,Trust, Security and Privacy in Computing and Communications (TrustCom), 2013

[8] Quach, T.T., “Extracting Hidden Messages in Steganographic Images”, Digital Investigation, 2014

[9] Jansen, W., Scarfone, K., “Guidelines on Cell Phone and PDA Security”, National Institute of Standards and Technology (NIST) Special Publication 800-124

[10] Jansen, W., Scarfone, K., “Guidelines on Cell Phone Forensics”, National Institute of Standards and Technology (NIST) Special Publication 800-101

[11] Albano, P., Castiglione, A., Cattaneo, G., De Maio, G., and De Santis, A., “On the Construction of a False Digital Alibi on the Android OS”, Intelligent Networking and Collaborative Systems (INCoS), 2011, pp 685 – 690

[12] Albano, P., Castiglione, A., Cattaneo, G., and De Santis, A., “A Novel Anti-Forensics Technique for the Android OS”, Broadband and Wireless Computing, Communication and Applications (BWCCA), 2011, pp. 380 – 385.

[13] Image and Video analysis, http://articles.forensicfocus.com/2014/07/28/

the-complete-workflow-of-forensic-image and-video-analysis/, accessed 24/08, 2014

[14] Digital evidence, http://www.fbi.gov/news/stories/2013/january/piecing-together-digital-evidence.html , accessed 24/08, 2014

[15] Android Forensics, http://bits.rahilparikh.me/2012/08/18/android-forensics.html, accessed 24/08, 2014

[16] Recovery, http://blog.avast.com/2014/07/09/android-foreniscs-pt-2-how-we-recovered-erased-data.html , accessed 24/08, 2014

[17] Android Debug Bridge, http://developer.android.com/tools/help/adb.html , accessed 24/08, 2014

[18] Android Forensics, http://resources.infosecinstitute.com/android-forensics.html, accessed 24/08, 2014

[19] Usb Host and Accessory, http://developer.android.com/guide/topics/connectivity/usb/index.html, accessed 24/08 2014

[20] Cyanogenmod, http://www.cyanogenmod.com/, accessed 24/08, 2014

[21] Android Usage Statistics, http://techland.time.com/2013/04/16/ios-vs-android.html, accessed 24/08, 2014

[22] Logical and Physical acquisition, https://viaforensics.com/resources/reports/android-forensics/introduction.html, accessed 23/10, 2014