ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2015

Anti-forensic: Design and Implementation of an Android Forensic Analyzer

Walter. T. Mambodza[1], Nagoor Meeran A.R[2]

PG Student, Information Security and Computer Forensics, SRM University, Chennai, India[1]

Assistant Professor, Information Security and Computer Forensics, SRM University, Chennai, India[2]

ABSTRACT: In incident response the Computer Emergency Response Team (CERT) or Computer Incident Response Team (CIRT) investigates an incidence in order to have a detailed description on how a crime was conducted, who was responsible and ways of making sure that the incident will not happen in future. In order for an investigation to commence there is need for someone to report the incident. The forensic expert or investigatorquarantines the crime scene, takes a photograph of the area and seizes the evidence in a forensically sound manner whilst preserving the integrity of data. The evidence media is taken to the forensic lab or workstation where an investigation is conducted. In most cases the investigator is qualified and skilled to perform the operation. The investigation process consists of two sub processes which are Data Collection and Data Analysis. Data collection is the process of acquiring the data that will assist in the investigation process for example through the use of Incident Response Toolkit. Data Analysis is the process of examining the collected data by using various forensic tools that follow the Association Chief of Police Officers (ACPO) principles in order to obtain results. The goals of information security are to protect the confidentiality, integrity and availability of data.Hackers compromise the information security and use anti- forensic techniques to make it difficult for investigators to detect and prove the existence and involvement in the crime. The aim of this paper is to design and implement an application that will provide a solution to some of the anti-forensic data hiding techniques.

KEYWORDS: Incident, Anti-forensic, CERT, CIRT, Data collection, Data analysis, Evidence

I. INTRODUCTION

Anti- forensics is a technique that makes it hard for investigators to find a perpetrator for crime and impossible to prove if they find the criminal. They are various anti-forensic techniques such as artifact wiping, trail obfuscation, attacks against computer forensics processes, tools and data hiding. [1] Data hiding techniques can be classified as Encryption or Steganography. When the two are combined they make a forensic investigation difficult if not impossible. Encryption is the process of converting plain text into cipher text through the use of algorithms and keys. Steganography is the process of hiding data or files within another file it can be video, image or audio that is used as a cover media. The Association of Chief Police Officers produced the "Good Practice Guide for Computer Based Electronic Evidence" which states 4 principles which are that no one should change or modify data that is termed as evidence, if original data is accessed the person must be competent to do so and give evidence at the end, All the processes should be recorded during investigation and a third party should be able to follow the steps and produce same results.[2] The fourth principle of the ACPO is that the person performing the investigation should accept full responsibility and ensure that all principles are adhered to. Android forensics has been a major concern due to the increase of the number of people accessing and using android phones. When an incident is reported fig 1.0 shows the steps that are done in incident response methodology. The main goal is to investigate the incident. The process of investigation comprises of two operations which are Data Collection and Data Analysis. The research proposes an application that will collect and analyze data on an android device by preserving the integrity of data and performing all the processes in a forensically sound manner.

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2015

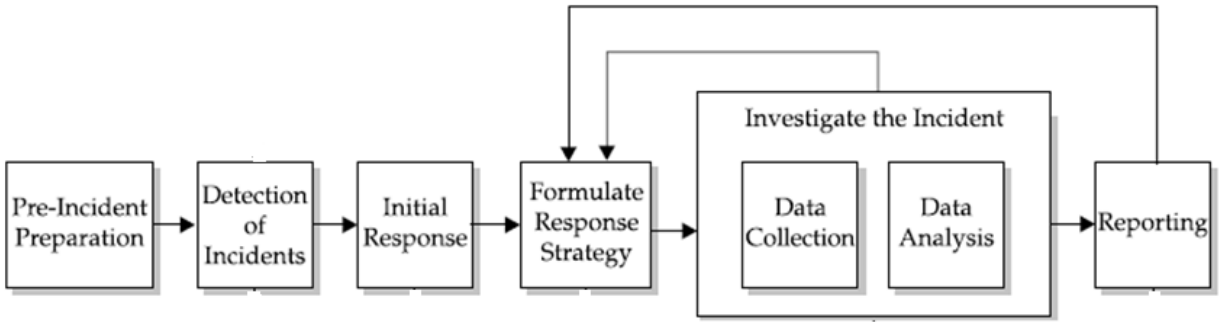

Fig 1.0 Incident Response Methodology diagram

II. RELEVANT WORK

Cellebrite is a mobile forensic product produced in 2007. The product is a Universal Forensic Extraction Device (UFED). It is a portable device that extracts mobile device data to a flash drive or SD card. The UFED can acquire hidden, deleted data, decipher and break codes. The UFED supports various cellular protocol and different operating systems like android, iOS, Symbian and Blackberry. The device can be used to collect both volatile and non-volatile data. [3]

XRY is a mobile and digital forensic product by Micro Systemation. It is used to recover, analyzer data on smartphones. Has a hardware and software component used for extraction. All the operations are conducted in a forensic manner. It allows both logical and physical examinations. It supports android, iOS and Blackberry devices. [4]
EnCase is a multi-purpose forensic tool by Guidance Software. The software is designed for cyber security, forensics and security analytics. The evidence extracted using the software can be admissible in the court of law. It contains tools for data acquisition, data analysis and reporting. Forensic images of suspect media can be created. [5]
Oxygen Forensic Suite is proprietary software used for smartphones. The suite acquires data, parses data, imports device backups and images, recovers deleted data and performs data analytics. Supports various operating systemsuch as Android, iOS, Blackberry and Windows phone. [6]
SteganosPrivacy Suite is a package that includes 9 data protection mechanism such as the safe, the portable safe, the password manager, the internet trace destructor, the email encryption, the shredder, tha anti-theft protection, the private favorites and the steganography trick. [7]

MOBILedit forensic is a toolkit that analyzes phones via WIFI, Bluetooth or USB cable. It provides information of phone status, has a SIM Analyzer, SIM clone tool, Report generator. It performs physical extraction for Android phones. MOBILedit forensic supports Android, Symbian, iOS, Blackberry and Windows phone [8]
Joint Test Action Group (JTAG) forensics is a data acquisition method that test access ports on device by instructing processor. Used to extract physical image were normal tools fail. It is appropriate when device is damaged logically and on pattern locked android phones. They are various steps that are done for a JTAG forensic examination [9]

III. DESIGN

The proposed system is supposed to detect an android device if connected with a USB cable. It has a menu with 3 options which is Images, Audio or video. Depending on the option selected the application is supposed to hash, scan and extract files from an android device. The proposed system at the end of all the process should generate reports. The application should observe all the ACPO principles. Fig 2.0 shows the flow diagram of the proposed system. Fig 3.0 shows an analysis model for use case helps to understand how the user will operate the application. Fig 4.0 shows a sequence diagram of the Android Mobile forensic analyzer and Fig 5.0 is a screenshot of the main interface of the analyzer.

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2015

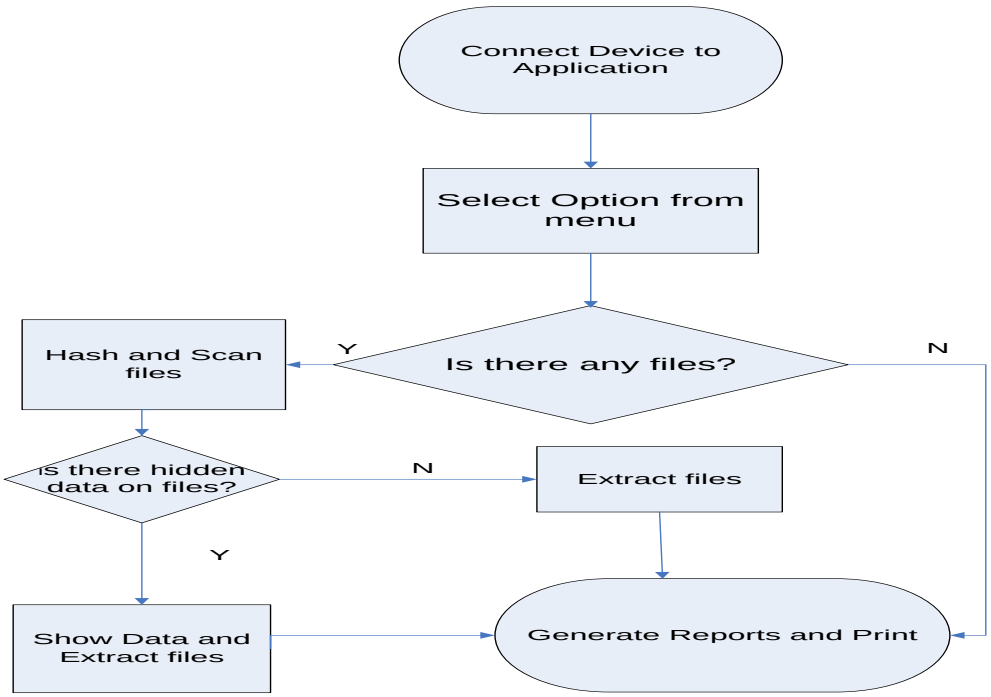

Fig 2.0 Flow chart of proposed system

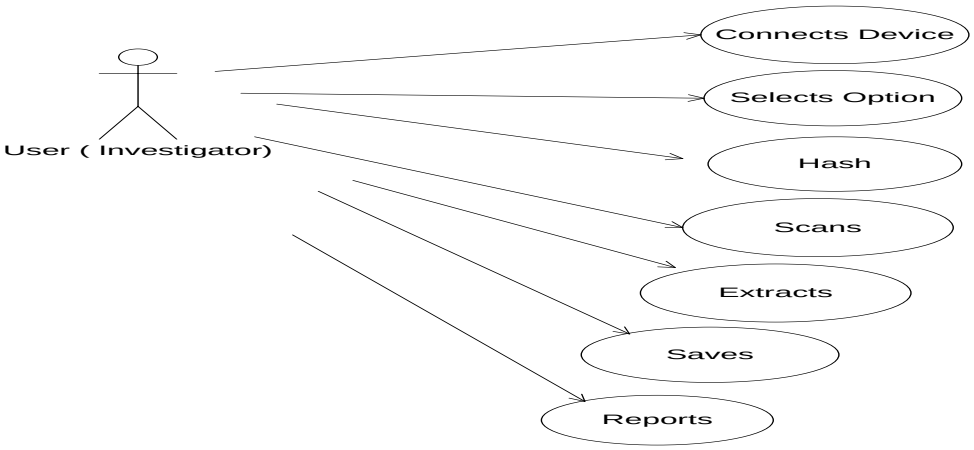

Fig 3.0 Use Case of Android Mobile Forensic Analyzer

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2015

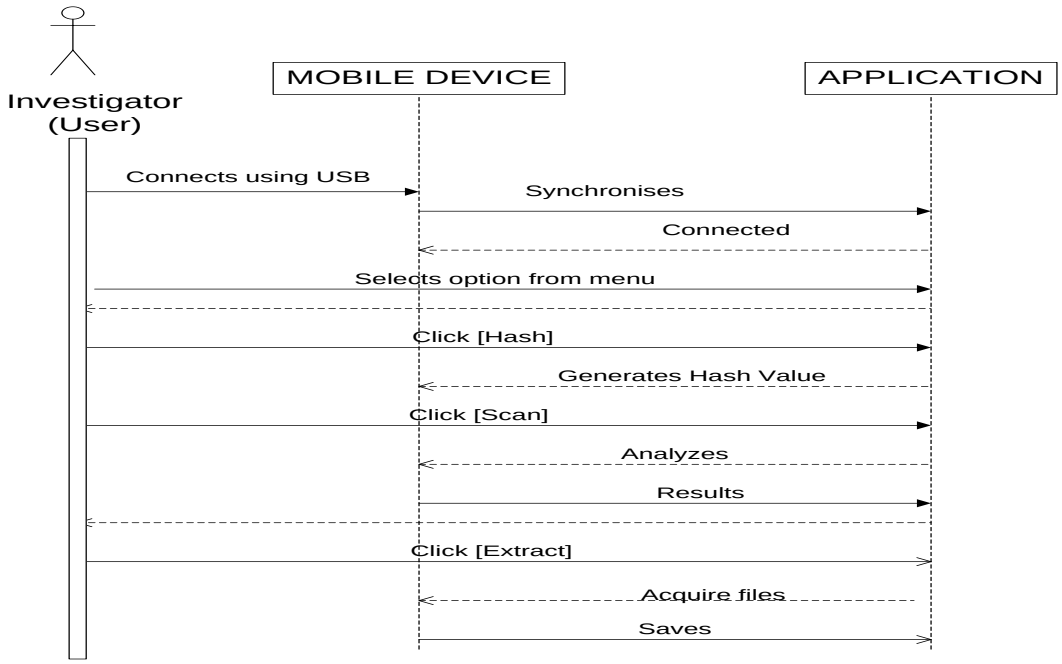

Fig 4.0 Sequence Diagram for Android Mobile Forensic Analyzer

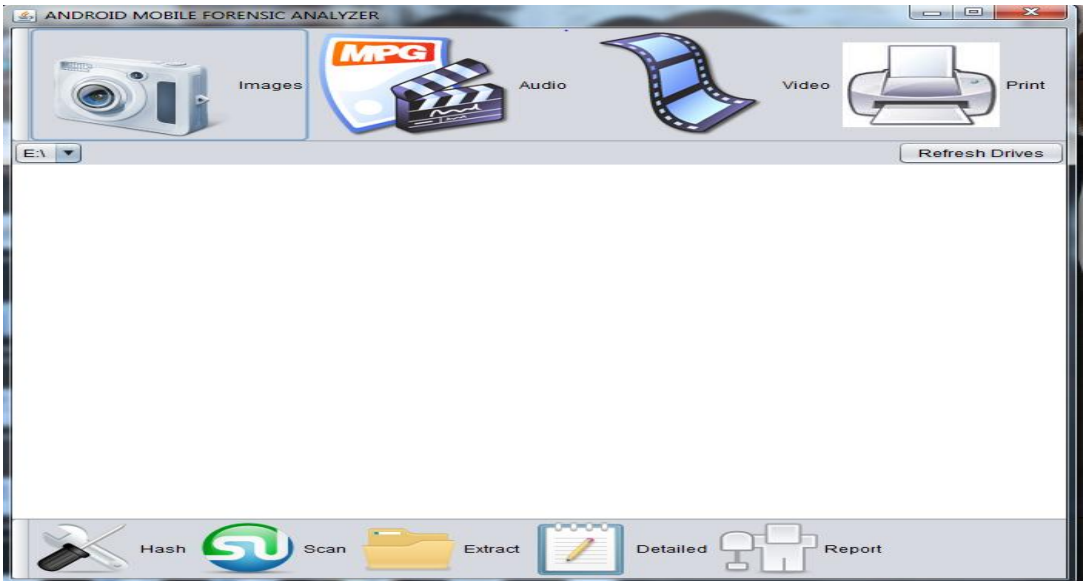

Fig 5.0 Screen shot of Main Interface

IV. IMPLEMENTATION

The designed application was able to detect a rooted Samsung Galaxy 2 running on Jelly bean and images, audio and video files on the android devices were easily retrieved in a forensically sound manner. Each file was hashed using MD5 hash function as a way of preserving the integrity of data and also details of the meta-data of the files could be seen and information such as last accessed and modified can be seen. The scan module was able to detect files embedded with data using least significant bit steganography. The files can be classified as carrier or free files and

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2015

depending on the option selected and embedded data can be revealed. Fig 6 and fig 7 below show screenshots of the classification of the files i.e. free file or carrier file. Files can also be extracted to a flash disk or pen drive to create an evidence media.

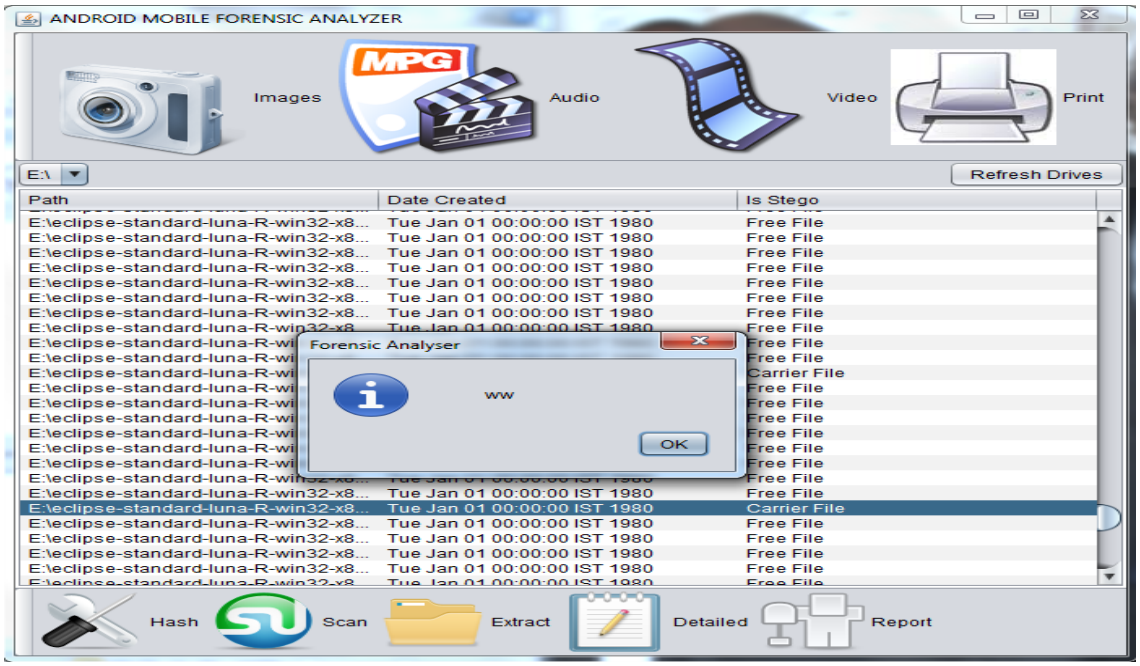

Fig 6.0 Screenshot for Carrier file

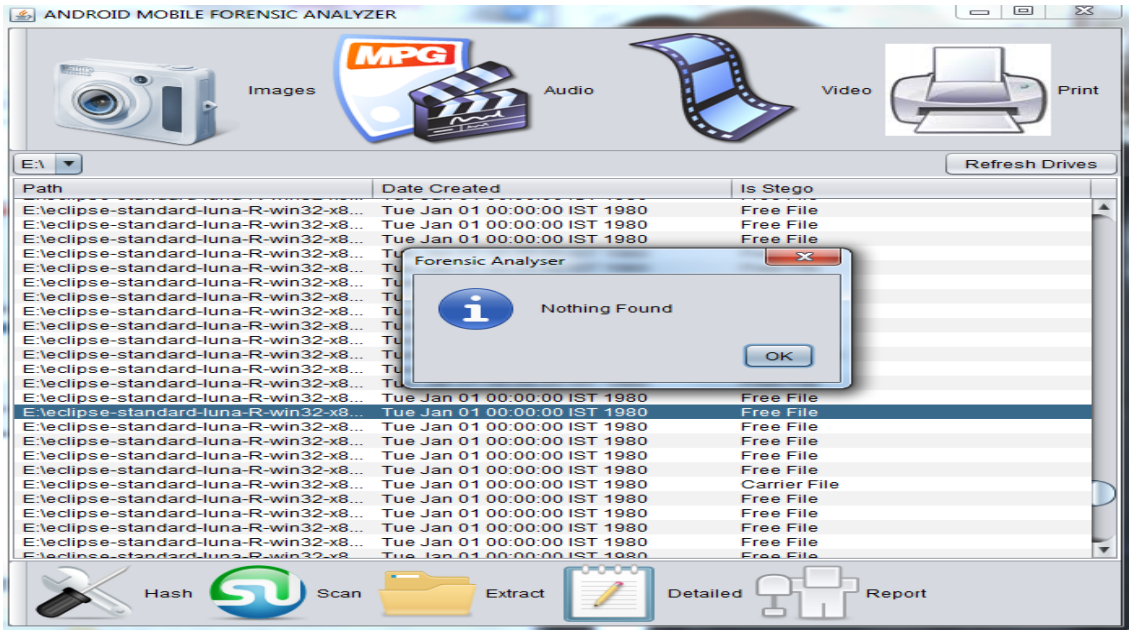

Fig 7.0 Screenshot for free file

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2015

V. RESULTS

The application was able to perform all the functional requirements and this can be shown by the screenshot Fig 8.0. Test data was inserted to an android device and the application generated the reports with all the information

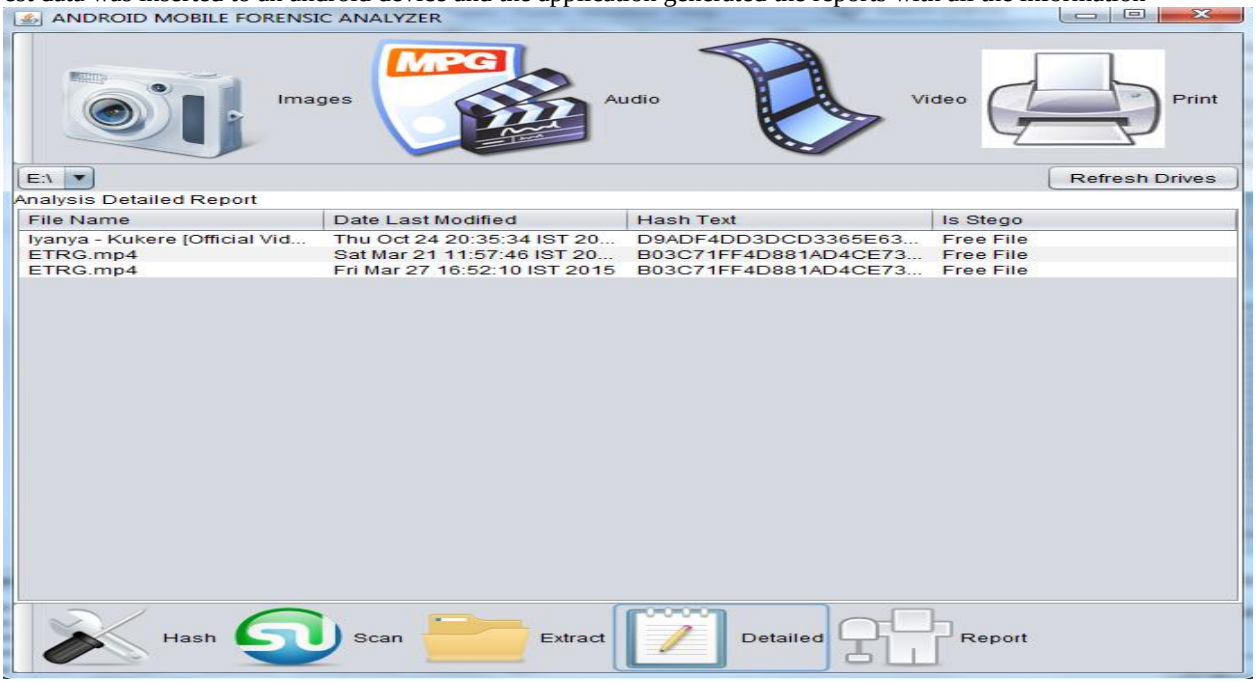

Fig 8.0 Screenshot for Analysis Detailed Report

The table below fig 9.0 shows a summary of the test cases or experiments that were conducted using the designed application

	HASH	SCAN	EXTRACT	REPORT
IMAGES	Each file was hashed	Analysis was successfully done	Evidence media was created	Report generated
AUDIO	Each file was hashed	Analysis was successfully done	Evidence media was created	Report generated
VIDEO	Each file was hashed	Analysis was successfully done	Evidence media was created	Report generated

Fig 9.0 Table for Experiments done

VI. CONCLUSION

The designed application provides a solution to the anti- forensic technique of data hiding on least significant bit steganography. The application serves as proof of concept and can be used on all android devices that can be viewed as removable disks not portable devices. All the ACPO principles are observed and it preserves the integrity of data. The application can be upgraded to detect the latest Android OS like kit kat and lollipop. In future there is need to create a forensic application that can detect a combination of the two data hiding techniques which is encryption and steganography.

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2015

REFERENCES

[1] Karlsson, K.J., and Glisson, W.B., "Android Anti-forensics: Modifying Cyanogen Mod", System Sciences (HICSS), 2014
[2] Jansen, W., and Scarfone, K., "Guidelines on Cell Phone Forensics", National Institute of Standards and Technology (NIST) Special Publication 800-101
[3] Cellebrite UFED- Mobile Forensics, www.**cellebrite**.com/mobile-forensics, accessed 18/01.2015
[4] XRY Mobile Forensic Tool, https://www.msab.com, accessed 18/01.2015
[5] Digital Forensic, https://www.guidancesoftware.com, accessed 18/01.2015
[6] Mobile Forensic Solutions, www.**oxygen-forensic**.com, accessed 18/01.2015
[7] Data Security and Privacy, https://www.**steganos**.com, accessed 18/01.2015
[8] MOBILedit Forensic, www.**mobiledit**.com/**forensic**, accessed 18/01.2015
[9] JTAG Forensic, www.binaryintel.com/services/**jtag**-chip-off-**forensics**/**jtag-forensics**, accessed 18/01.2015
[10] Chris Prosise.., and Kevin Mandia.., "Incident Response and Computer Forensics", Second Edition, McGraw-Hill, 2003
[11] Gloe, T., Fischer, A., and Kirchner, M., "Forensic Analysis of Video File Formats", Digital Investigation, 2014
[12] Quach, T.T., "Extracting Hidden Messages in Steganographic Images", Digital Investigation, 2014
[13] 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.
[14] Android Debug Bridge, http://developer.android.com/tools/help/adb.html , accessed 24/01, 201