Journal of Engineering and Applied Sciences 14 (20): 7490-7494, 2019
ISSN: 1816-949X

Mobile Forensic: JPEG Recovery with EXIF Metadata

Wan Hazimah binti Wan Ismail, Herny Ramadhani Mohd Husny,
Mohammad Noramin Bin Basri and Norhaiza Ya Abdullah
Malaysian Institute of Information Technology, Universitiy Kuala Lumpur,
Kuala Lumpur, Malaysia

Abstract: Mobile devices are becoming a more popular tool to use and have changed the way we live in our daily lives. Mobile devices are being used for many activities such as social networking, conducting business transactions and others. Therefore, it become one of the most popular medium of communication in the world. Besides of these good and advanced capabilities of mobile technology, it can also be used to perform various activities that may be of malicious intent or criminal in nature. Due to this, mobile devices can be a valuable source of digital evidence, since, it can accumulate a sizeable amount of information, if the device is involved in a crime. The Android smartphone has been used to store an enormous amount of data that can be stored locally or remotely and enable a forensic analyst to acquire the data and evidence as for collecting this valuable information with regard to the investigation. In this study, we present a new mobile forensic application based on Android smartphone that able to extract and recover the data. File carving technique has been used to recover corrupted or deleted files from the mobile devices. File carving is the technique that can help the investigator to retrieve and acquire the data from unallocated space. This application performs as a digital forensic tool in order to guide basic forensic analysis on Android by focusing on extraction and analysis of JPEG image files from either digital cameras or smart phones. JPEG is the most widespread loss compression formats used by digital cameras or smart phones. The result of this application is where it able to analyze the content of the memory card or secure digital card by extracting JPEG image files and visualize the image as soon as image are extracted. Then, it reveals the EXIF metadata information as well as translating some of the metadata content into GPS tag if available. It is very significant to have this application as it can help the forensic investigator for investigating the evidence on Android applications, since, its mobility and convenience to users.

Key words: Digital forensic, mobile forensic, file carving, JPEG, carving, data recovery

INTRODUCTION

Smartphones are rapidly replacing computers in functionality and popularity as more and more people use them for day-to-day activities. The Android operating system is rapidly gaining a large market share and is being deployed on wide range of devices including smartphones and tablets. There is a great need to be able to extract and analyze data from these devices in a forensically sound manner. In smartphone there are Secure Digital (SD) card that contains many information such as video, image, music, games and etc. Where in images files there are contain picture which comes by taking from camera or by downloaded that use extension JPEG format. JPEG compression is the name given to an algorithm developed by the Joint Photographic Experts Group (JPEG) whose purpose is to minimize the file size of photographic image files (Rathore, 2014). JPEG compression is an impressive tool and with great power comes great responsibility. While JPEG compression can help greatly reduce the size of an images file, it can also compromise the quality of an image.

MATERIALS AND METHODS

Mobile forensic: Mobile forensic is a new type of gathering digital evidence where the information is retrieved from a mobile phone. It relies on evidence extraction from the internal memory of a mobile phone when there is the capability to access data. Mobile phone forensics is the science of recovering digital evidence from a mobile phone under forensically sound conditions using accepted methods (Burrows and Zadeh, 2016). Mobiles are used in all sorts of communications such as

Corresponding Author: Wan Hazimah binti Wan Ismail, Malaysian Institute of Information Technology, Universiti Kuala Lumpur, Kuala Lumpur, Malaysia

Table 1: Types of evidence

Evidences	Descriptions
Contacts	User-created information
Call logs	Phone-created information
Text message	User-created information
Audio/video files	User-created information
Images files	User-created information
Internet history	Internet-related information
SIM card	Identifiers, usage nformation

making calls, sending text messages, sending emails, connecting with friend and family through different social network or instant messaging applications. Mobile phone usage is not limited to basic communication but also heavily used in airline check-in, mobile banking, navigating the location and many other features. Mobile devices are dynamic systems that present challenges from forensic perspective. Additionally, new models of phones are being developed globally with some experts postulating that five new phone models are released every week (Mambodza and NagoorMeeran, 2015).

Type of evidence: The forensic benefit of mobile devices in an investigation varies depending on the criminal acts being investigated, the capability of the mobile device and how it has been used. Data associated with mobile phones is found in a number of locations such as embedded memory, attached removable memory and the Subscriber Identity Module (SIM) card. Not all of these components will be available or necessary for all investigations but in some cases there may be multiple SIM cards, removable media or even more than one mobile device (Vidas *et al*., 2011). The types of evidences that can be extracted from mobile phone shown at Table 1 below (Chen *et al*., 2011).

These artifacts can be extracted in logical or physical methods. Logical is extracting data from the file system by directly interacting device with some special tools. The software's or tools that extract these artifacts (evidences) are limited. So, forensic examiners find it difficult to execute this job in a timely fashion (Chen *et al*., 2011).

Forensic best practice: Mobile forensic involves the same methods of the normal forensic investigation. There are some best practices that need to be followed. Though there are not much standardized format of investigation in mobile forensic the methods of investigation involved is more or less same as digital investigation. The phases of investigation processes that normally follow are (Li *et al*., 2016).

Collection: This is the first and foremost step involved in the investigation. The main purpose here is to collect the potential sources of evidences like mobile, SIM card and other accessories.

Identification: This is focused on the recognition by labeling the potential sources of digital evidence.

Acquisition: This mainly involved in the extraction of data or potential evidence from different sources that have been captured.

Preservation: One of the important steps involved in the investigation is preservation 4 of evidence where adequate measures should be taken to secure the integrity of the evidence.

Examination and analysis: It involves searching, filtering, examining and evaluation of evidence.

Reporting: As like any digital investigation reporting is the final part of documented proof of conclusive evidence.

Data carving: Data carving is the process of extracting a collection of data from a larger data set. Data carving techniques frequently occur during a digital investigation when the unallocated file system space is analyzed to extract files (Li *et al*., 2016). The files are "carved" from the unallocated space using file type-specific header and footer values. File system structures are not used during the process. The most common general file carving techniques are (Uzun and Sencar, 2015).

Header-footer or header-"maximum file size" carving:

- Recover files based on known header and footers or maximum file
- If the file format has no footer, a maximum file size is used in the carving program
- Known header footers carvers are ExifTool, Exiv2, foremost and scalpel

File structure based carving:

- This technique uses the internal layout of a file
- Elements are header, footer, identifier strings and size information

Content based carving:

- Content structure
- Content characteristics

Magic number: The term magic number has different meanings but here, we are focusing on file, hence, the magic number is a constant used to identify a file format. Detecting such constants, basically every file has a header and a footer in order to get correctly recognized, for example, especially, in this project scope was JPEG,

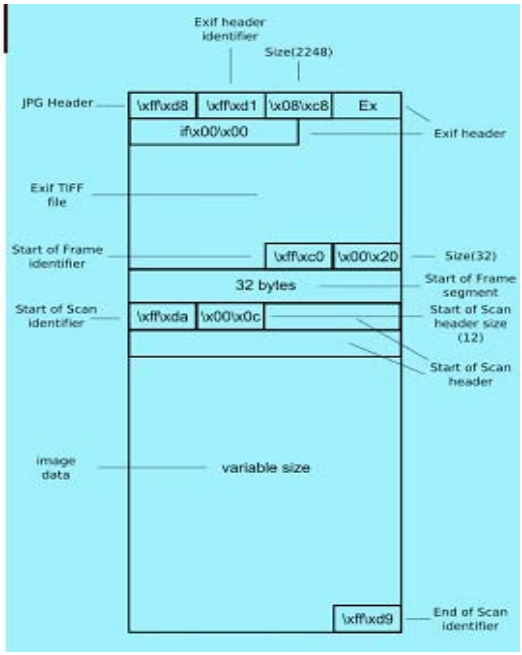

Fig. 1: JPEG structure with magic number

therefore, a JPEG image file begins with "0×FFD8" and ends with "0×FFD9". These constant are called magic numbers (Hadi, 2016). Figure 1 shows the JPEG structure with magic numbers.

Android analysis: Android devices typically have memory card storage such as Secure Digital (SD), Mini SD or Micro SD capability. The file and folder structure of the smartphones included folders for audio, video, photographs, cache data and application data (De Bock and de Smet, 2016). Information located on the SD card used in this project references to the make and model of the device. JPEG pictures taken with the device contained EXIF data relating to the make and model (Ravi *et al*., 2016). The information on an SD card can vary, so, traditional forensic analysis methods are recommended for different devices. There are 2 ways to analyze the Android as stated below (Mumba and Venter, 2014).

Physical without the spare data: Analysis of the extracted data which did not have the spare information of reviewing the hex data for object headers and file data. Data carving was undertaken with WinHex, scalpel and other carving software and all produced similar results.

Physical with the spare data: To undertake analysis of the physical image which included the spare information, an operating system or software to interpret YAFFS is required. Native support for YAFFS is not included with

Fig. 2: Architecture system of JREM Apps

the Linux kernel, however, a kernel can be compiled to include YAFFS and then mounting of YAFFS images to view files and folders. Microsoft Windows or any current forensic analysis software does not support the YAFFS file system, however, it is understood support for YAFFS is being developed, for AccessData's Forensic ToolKit and also for the SleuthKit.

Development of the application: For the development, identifying software and hardware requirement are the basic steps that the developer need to ensure it available in a working machine before the development process of the application started. The software that was used for this application are Android Studio Android Software Development Kit, Java Runtime Environment, Java Development Kit and Genymotion that used as an Android emulator for the developer to test the application. The name of this application is JPEG Recovery with EXIF Metadata (JREM) (Table 2).

The overall system architecture for the JREM Apps is depicted in Fig. 2. According to Fig. 2, it shows the process flow of the JREM Apps on how investigator uses the application and what the developer needs to create on the application. For the investigator, the first step that needs to do is to load the evidence that was found in home file on Android by choosing the disk image or electronic image that contains JPEG file formats. The application will start data carving process after the load evidence was chose by the investigator. Once the image was found and recovered, the image will appear in a row that possibilities contains a lot of information that is called EXIF metadata. Figure 3 shows the results page in the application when user click the 'view report' button. In this page, consists of several images that user had selected with the EXIF metadata information from the

Table 2: Results of functional testing

Text part	Taxt condition	Exparted results	Actual results
Imaging avidence SD card	To done avidence to become disk image img/dd	The avidence was successfully captured	PASS
Integnity avidence file	To make sure integrity of avidence is genuine before extract and after extract	The integrity file avidence file was verified using MDS/SHAL value	PASS
Data carving methods	To know how the porcess recovery image	The carving was successfully by display the picture after recounting the disk image in row	PASS
Bookmarks	To test by selecting multiple images to view the recvoery image	The bookmarks was successfully tick multiple image	PASS
EXIF metadata	To know whether the image was contains picture information	The EXIF metadata appearing	PASS
GPS tag	To cheak whether the each images provide goo-tag when click the image	The geo-tag depend on user preferences	PASS

Fig. 3: Results page

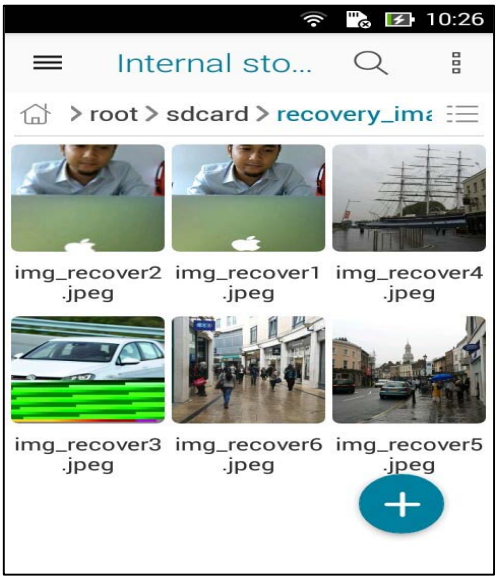

Fig. 4: List of recovery image

image. If user clicks the image that contains GPS tag, it will directed to the maps application, according to the location provided.

All the recovered images were stored in the folder. The user able to view details of the image, edit the image and delete the image by clicking on the image. Figure 4 shows a list of images that successfully recovered by using the application.

RESULTS AND DISCUSSION

For this application, the testing method that has been conducted was functional testing. The purpose of this testing process was to check any defects or errors that were made during the development phases and to gain confidence regarding program functionality. It is also to ensure the functionality and operations meet the objectives. In this testing process, there were seven modules that were tested. The modules are imaging evidence, integrity evidence, data carving, bookmarks, EXIF metadata, GPS tag and Android version. The results according to functional testing were shown in Table 2. This testing process was conducted by the developer of the application. Based on Table 2, it shows that all components were performed as expected.

CONCLUSION

Mobile forensic: JPEG recovery with EXIF metadata has been developing successfully using the Android platform. The application is capable of helping and allows investigators to recover and analyze images in easy way. As a conclusion, the result of this study will be an Android application that makes forensic field becomes more advanced. The findings of this study are important to help the investigators to find out the data extraction and recovery in new ways to investigate or analyze evidence file on Android applications.

REFERENCES

Burrows, C. and P.B. Zadeh, 2016. A mobile forensic investigation into steganography. Proceedings of the 2016 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), June 13-14, 2016, IEEE, London, UK., ISBN:978-1-5090-0710-3, pp: 1-2.

Chen, S.W., C.H. Yang and C.T. Liu, 2011. Design and implementation of live SD acquisition tool in Android smart phone. Proceedings of the 2011 5th International Conference on Genetic and Evolutionary Computing, August 29-September 1, 2011, IEEE, Xiamen, China, ISBN:978-1-4577-0817-6, pp: 157-162.

De Bock, J. and P. de Smet, 2016. JPGcarve: An advanced tool for automated recovery of fragmented JPEG files. IEEE. Trans. Inf. Forensics Secur., 11: 19-34.

Hadi, A., 2016. Reviewing and evaluating existing file carving techniques for JPEG files. Proceedings of the 2016 International Conference on Cybersecurity and Cyberforensics (CCC), August 2-4, 2016, IEEE, Amman, Jordan, ISBN:978-1-5090-2658-6, pp: 55-59.

Li, Z., B. Xi and S. Wu, 2016. Digital forensics and analysis for Android devices. Proceedings of the 2016 11th International Conference on Computer Science and Education (ICCSE), August 23-25, 2016, IEEE, Nagoya, Japan, ISBN:978-1-5090-2219-9, pp: 496-500.

Mambodza, W.T. and A.R. NagoorMeeran, 2015. Android mobile forensic analyzer for stegno data. Proceedings of the 2015 International Conference on Circuits, Power and Computing Technologies [ICCPCT-2015], March 19-20, 2015, IEEE, Nagercoil, India, ISBN:978-1-4799-7075-9, pp: 1-8.

Mumba, E.R. and H.S. Venter, 2014. Mobile forensics using the harmonised digital forensic investigation process. Proceedings of the 2014 International Conference on Information Security for South Africa, August 13-14, 2014, IEEE, Johannesburg, South Africa, ISBN:978-1-4799-3384-6, pp: 1-10.

Rathore, N., 2014. JPEG image compression. Intl. J. Eng. Res. Appl., 4: 435-440.

Ravi, A., T.R. Kumar and A.R. Mathew, 2016. A method for carving fragmented document and image files. Proceedings of the 2016 International Conference on Advances in Human Machine Interaction (HMI), March 3-5, 2016, IEEE, Doddaballapur, India, ISBN:978-1-4673-8810-8, pp: 1-6.

Uzun, E. and H.T. Sencar, 2015. Carving orphaned JPEG file fragments. IEEE. Trans. Inf. Forensics Secur., 10: 1549-1563.

Vidas, T., C. Zhang and N. Christin, 2011. Toward a general collection methodology for Android devices. Digital Invest., 8: S14-S24.