Journal of Applied Sciences

ISSN 1812-5654

science alert

ANSInet
an open access publisher
http://ansinet.com

Journal of Applied Sciences 15 (4): 668-674, 2015
ISSN 1812-5654
© 2015 Asian Network for Scientific Information

ansinet
Asian Network for Scientific Information

RESEARCH ARTICLE OPEN ACCESS

DOI: 10.3923/jas.2015.668.674

Multimedia Files Signature Analysis in Blackberry Z10

Aanahita Farjamfar, Mohd. Taufik Abdullah, Ramlan Mahmod and Nur Izura Udzir
Department of Computer Science, Faculty of Computer Science and Information Technology,
Universiti Putra Malaysia (UPM), Serdang, Selangor, 43400, Malaysia

ARTICLE INFO
Article History:
Received: November 20, 2014
Accepted: February 20, 2015

Corresponding Author:
Mohd. Taufik Abdullah,
Department of Computer Science,
Faculty of Computer Science and
Information Technology,
Universiti Putra Malaysia (UPM),
Serdang, Selangor, 43400, Malaysia
Tel: 03-89471724

ABSTRACT

Now-a-days, wide range of Smartphone models are available in the market which have a potentially extensive use in criminal activities. Smartphones as ever present devices, capable of connecting to the Internet and transferring huge amount of multimedia files have been identified as growing challenges to digital forensic investigators. One area of difficulty is to determine whether multimedia files collected form a Smartphone are created locally on the phone under examination or obtained from elsewhere. Using Blackberry Z10 as a case study, study was conducted to determine the system-generated artefacts on multimedia files when created by means of this Smartphone. By determining the metadata on these files, it contributed to a better understanding of the types of artefacts that are likely to be found by digital forensics practitioners and examiners. Potential identified findings include date and time of file creation, Operating System (OS) name and version, device name and other obscure metadata which could relate the file to this specific Smartphone.

Key words: Digital forensics, smartphone, file signature, Blackberry Z10

INTRODUCTION

Digital forensics is a science which concerns identification, collection, preservation, storage, analysis and documentation of digital evidence or data that has been stored, processed or transferred in digital form. As files are the resources for storing information on digital devices, analysis of digital files is critical during a digital forensics investigation. In general, the structure of a digital file consists of three main elements: File name, file header\footer and File content. Each application employs specific file formats to encode data on files with the purpose of preventing extraction of the data by other applications.

The process of identifying and comparing extensions, headers, footers and other metadata of the files is called file signature analysis. File signature analysis is being applied in the digital forensic procedures in the process of an investigation for various purposes such as detecting changes in the filename extensions, detecting deleted files or identifying the source application or the device used to make the files.

Currently, intensive Internet usage affected the way users acquire and use information. The speed and high volume of sharing information are two of the major benefits of Internet. In addition, wide-speared use of Smartphones makes it possible for users to acquire and spread files such as images and videos anywhere and anytime.

This has risen the concerns about unethical activities and dispenses of multimedia files, in particular indecent images of children, among the community. During an investigation, proving whether file was produced on the digital device under examination or obtained from another sources such as Internet can be of very high importance.

To address this issue, file signatures and metadata embedded in computer-generated files has been analyzed and documented for different file types. These documents have been applied in file carvers such as Scalpel developed by Richard and Roussev (2005), to recover files from raw disk images. Digital evidence is not bounded only to those founded on computers. Smartphones are considered valuable sources of information that if collected in a forensically sound manner would be admissible in court of law.

Smartphone's diversity of manufacturers, hardware structures and operating systems provide the opportunities for wide variety of applications to be developed all over the world. Therefore, documenting signatures of files created on Smartphones by means of these applications is not only of value but of high necessity.

In this study, we discuss file carving in the digital forensics process and conduct study into the metadata of multimedia files created by Blackberry Z10 Smartphone. Blackberry Z10 Smartphone was chosen as a case study because of its popularity among corporate and government enterprises. Moreover, since its launch in 2013 there has been no study conducted on the signature analysis of files created by this phone and to the best of our knowledge, so far analysis of BlackBerry Z10 multimedia file signatures is not supported by the available forensics tools such as Encase and Oxygen Forensics Suite. Using file carving technique, this study identifies the digital traces from the Blackberry Z10 mobile device on multimedia files.

File carving is a forensics technique that recovers files based merely on file structure and content, without matching file system metadata. The results demonstrate the presence of special patterns within examined files and by specifying these metadata we contribute to a better understanding of the types of artefacts that are likely to be found by examiners. Using Blackberry Z10 Smartphone as a case study, we attempt to answer:

- What metadata remains on a multimedia file after the file is created on the phone
- Is there any metadata to tie the multimedia files to the phone under study or they were received from another source
- What changes occur on the metadata after the file has been edited

The following discussion firstly explains some background of digital forensics, followed by a brief review of issues related to file signature analysis. Next the scope of the study and preparation is outlined. Following this we discuss for the use of digital forensics method and analysis of multimedia files belong to the Blackberry Z10 Smartphone.

Digital forensics: The Digital Forensics Research Workshop (Palmer, 2001) defined Digital Forensic Science as "The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations".

Regarding this broad definition, the goal of digital forensics is to identify, collect, preserve, analyze and document the digital evidence or data that has been stored, processed or transferred in digital form by using scientifically accepted methods. As Jones and Valli (2011) remark, any items that can be considered evidentially value should be identified and collected.

Digital evidence: According to the Scientific Working Group on Digital Evidence (SWGDE., 2011), digital evidence is "information of probative value that is stored or transmitted in binary form". Based on this definition, digital evidence includes evidence on any digital devices such as portable media players, digital cameras or telecommunication devices and not merely limited to those found on computers.

Moreover, digital evidence has been expanded to include every category of crime where digital evidence can be found and be used as the proof; it is not bounded only to traditional computer crimes like hacking and intrusion (Ghosh, 2004). Digital evidence covers any digital data that can confirm a crime has been committed or can provide a link between a crime and its victim or a crime and its executor. In other words, digital evidence is a sequence of binary digit numbers on transmission or information files stored on the electronic devices. The digital evidence file formats include digital images, text, audio and video, etc.

Digital forensics artifacts: The truth about an event is revealed by forensics investigator through discovering and exposing the remnants of the event, known as artifacts that have been left on the system. While the phrases 'digital artifacts' and 'digital evidence' can be used interchangeably, the first one is preferred to avoid legal connotation overhead of the phrase 'Digital Evidence'.

File signature analysis: Haggerty and Taylor (2007), presented a scheme for the automated analysis of the computer's hard drive for digital pictures or intended files using forensic signatures. The scheme first identifies potential multimedia files of interest and then compares the data to file signatures to make sure whether a malicious file is resident on the computer. This approach made detection of malicious images effective and automated. However, it has been applied only to computer hard disks and for newly emerged mobile phones and extensive multimedia applications no equivalent method has been proposed yet.

Yip (2008) also emphasize on the importance of file signature analysis in the process of computer forensics to find hidden data on the computer either if it is deleted or the related filename extension is changed to deceive the investigator. In the case that the list of predefined file signatures is incomplete, valuable information may be overlooked even by famous forensics tools such as Encase.

File signature analysis can be deployed also in detecting encrypted files as Jozwiak *et al.* (2011) have performed, even though this method cannot detect which encryption mechanism has been used but points that file was created by cryptographic tool. In the technical digital forensic previewing process, developed by Shaw and Browne (2013) in order to triage the digital forensic process, file signature analysis and data carving are conducted as the standard routines during the forensic investigation.

On the other hand, there has been some study conducted on source identification of multimedia files, especially camera source identification; research studies such as those performed by Tsai *et al.* (2007), Li (2010) and Deng *et al.* (2011) which were conducted using other methods such as Sensor Pattern

Noises (SPNs), extracted from digital images to serve as the fingerprints of imaging devices. These methods are not only complicated but also consider camera as a discrete device rather than an application within a mobile device.

MATERIALS AND METHODS

Digital forensics practitioners and law enforcement generally follows accepted procedures, rules and standards such as those of Association of Chief Police Officers (ACPO., 2006) or National Institution of Standard and Technology (Jansen and Ayers, 2007). The NIST guidelines can be used as a starting point for forensic capabilities development rather than legal advice. On the other hand, the ACPO guidelines give the lawful principles and considerations to ensure the integrity of evidence while they need some updated guidance on how mobile devices should be handled by law enforcements during an investigation.

According to Owen and Thomas (2011), guidelines and research into the forensic examination of hard disk drives are much more established compared with those related to mobile devices. A more detailed explanation of various digital forensics process models are outlined in our previous study (Farjamfar *et al.*, 2014). In this study, we adopt the methodology proposed by McKemmish (1999), containing following basic steps of a forensic investigation; identify, preserve, analysis and present.

Our study focuses on identifying metadata remained on the multimedia files by utilizing Smartphone, namely Blackberry Z10, to create those files. Traces that are left behind from the use of an application or from an operating system can be referred to as digital forensic artifacts. The aim is to identify the source of the multimedia files, any dates and times, any device or OS associated information and any other metadata that may assist an investigator.

Research scope: The scope of this study is to determine the artifacts created by the applications without user intervention which are referred to as system-generated digital forensic artifacts. This study is undertaken to determine the artifacts an examiner should search for when Blackberry Z10 is suspected as possible source of a multimedia file, artifacts such as, date and time of creation, Operating System (OS) name and version, device name and other obscure metadata which could relate the file to this specific Smartphone. There is a need to undertake known changes to multimedia files, such as cropping or enhancement in a range of ways including Microsoft picture manager use on a computer PC and Edit option use on the phone.

Research preparation: To gather the data required to answer the study questions in relation to use of Blackberry Z10, twenty pictures were created randomly around the university campus with the blackberry Z10's on-device camera in addition to twenty videos of approximately 20 sec duration. Twenty voice files of 10-20 sec durations were recorded by the user while creating an entry in the "Remember" application as the voice note.

The video and voice duration has not any effect on the metadata though, keeping the size small enough helps in reducing the time to undertake analysis. It was decided to examine any differences while performing some changes to the files on the same phone or on a computer PC and also compare the metadata with those related to multimedia files built by use of other mobile phones, namely BlackBerry Torch running BlackBerry OS 6.0 Bundle 2534 (v6.0.0.570, Platform 6.6.0.212), Samsung galaxy tab2 running Android 4.1.1. and iPhone running iOS 4.3.3.

In our experiments, Hex Workshop 6.7.3 was used to analyze the content of each file and for every file type (image/video/voice) the results were compared to the same file types created by aforementioned mobile devices.

RESULTS AND DISCUSSION

This section discusses the application of the McKemmish method when conducting study into the artefacts remained on a multimedia file and to outline the four steps used to carry out research of Blackberry Z10 usage.

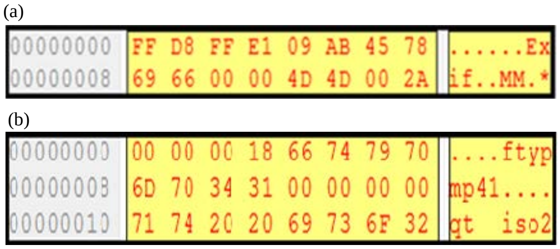
Identification of data: In the context of our study, we identified folders which would contain needed multimedia files to conduct the analysis. Images and videos took by on-device camera will be by default stored in the "Camera" folder while voice files by default will be stored in "Voice" folder. Both these folders are under "File Manager". While connecting the phone to a personal computer using a USB cable and Blackberry Link desktop software, these folder are accessible to the investigator.

Preservation of data: One of the basic rules in digital forensics world is the necessity to conduct analysis on a forensic copy, instead of interacting with the original evidences (ACPO., 2006). For this study, a forensic copy was made of each file using Access Data FTK Imager (AD1) format and MD5 hash values were calculated for each original file and verified with each forensics copy, also to ensure the forensic integrity of the data after conducting analysis.

Analysis of data

Content identification: Content identification concerns validation of a file extension's identity. The file extension of a specific file can be altered by a criminal in order to distract the investigator. Thus a file's integrity needs to be identified by means of file signature analysis. To find a file's particular signature normally the file is analyzed within its first bytes.

Camera images: Figure 1a shows the hexadecimal signatures of the examined images. The figures are copied directly from



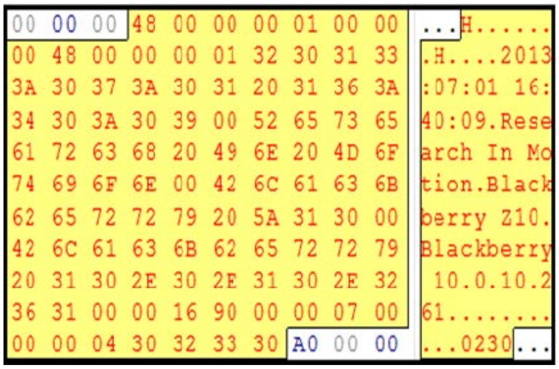
(a)

```
00000000  FF D8 FF E1 09 AB 45 78  ......Ex
00000008  69 66 00 00 4D 4D 00 2A  if..MM.*
```

(b)

```
00000000  00 00 00 18 66 74 79 70  ....ftyp
00000008  6D 70 34 31 00 00 00 00  mp41....
00000010  71 74 20 20 69 73 6F 32  qt  iso2
```

Fig. 1(a-b): Hexadecimal header for (a) Camera images and (b) Camera videos



```
00 00 00 48 00 00 00 01 00 00  ...H......
00 48 00 00 00 01 32 30 31 33  .H....2013
3A 30 37 3A 30 31 20 31 36 3A  :07:01 16:
34 30 3A 30 39 00 52 65 73 65  40:09.Rese
61 72 63 68 20 49 6E 20 4D 6F  arch In Mo
74 69 6F 6E 00 42 6C 61 63 6B  tion.Black
62 65 72 72 79 20 5A 31 30 00  berry Z10.
42 6C 61 63 6B 62 65 72 72 79  Blackberry
20 31 30 2E 30 2E 31 30 2E 32   10.0.10.2
36 31 00 00 16 90 00 00 07 00  61........
00 00 04 30 32 33 30 A0 00 00  ...0230...
```

Fig. 2: Time stamp, device name, OS version in BB Z10 camera images

Table 1: Hexadecimal signature for camera images and camera videos

File type	File extension	ASCII	File signature
Camera image	jpg	ÿØÿá..Exif	FF D8 FF E1 09 AB 45 78 69 66 00
Camera video	mp4	ftypmp41	00 00 00 18 66 74 79 70 6D 70 34 31

the running hex editor. The file extension for these images is jpg, however it is only a suffix illustrating the encoding of a file's content and never can be trusted as it can be renamed to anything else. Therefore, it is wise to focus on the file signature. The various file attributes for camera images are categorized in Table 1. The ASCII section stands for the entry in text readable format. The file signature part on the left side stands for the required entry in hexadecimal format.

This information signify Digital camera's JPG file using Exchangeable Image File Format (EXIF). Every JPG file starts from binary value '0×FF 0×D8' means SOI (Start of image), ends by binary value '0xFF 0xD9' means EOI (End of image). Today, most of new digital cameras use EXIF file format to store images.

EXIF data starts from ASCII character "EXIF" and 2 bytes of 0×00, then EXIF data follows in TIFF format. First 8 bytes of TIFF format are TIFF header. First 2 bytes defines byte align of TIFF data. If it is 0×4949 = "I I", it means "Intel" type byte align. If it is 0×4d4d = "MM", it means "Motorola" type byte align. Next 2 bytes are always 2 bytes-length value of 0×002A. The need of the value of EXIF data, It must check byte align every time. Our findings show the same results for the images taken by the front camera.

Camera videos: Hexadecimal signatures for Camera videos are shown in Fig. 1b. The file extension for these videos are mp4. Table 1 shows various file attributes for camera videos.

MPEG-4 video/QuickTime file is the formats based at the "ISO base media file format". The ISO base media file format should only be used as basis for other specification like "qt", "mp41", "m4v", "3gp6", etc. Mp41 is the MP4 file format version 1. The brand 'iso2' is used to indicate compatibility with the amended version of the ISO Base Media File Format.

Voice files: The results of analyzing voice files reveal that they have the same header as videos created by camera.

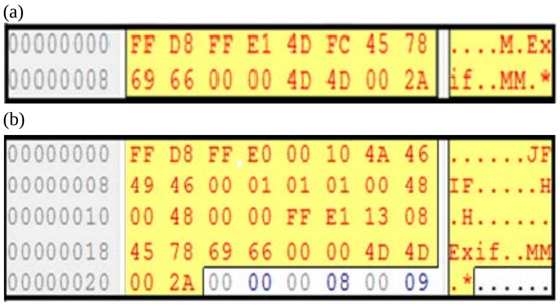
Content examination: Content examination implies verifying the metadata of different application file types. Metadata applies to data about data. It exposes useful information which can be extracted from a specific file thus examining the content is vital during an investigation.

Camera images: As mentioned before jpg is the default file type for images created with BB Z10's camera. The images contain metadata including time stamps, manufacture company name, device name and operating system version, etc. The metadata are mostly recorded within certain offsets from the 0×00-0×BFF. The first significant metadata could be find in the following format: "0×48 0×00 0×00 0×00 0×01 0×00 0×00 0×00 0×48 (Time stamps) (Company name) (Devices name) (OS version) 0×00 0×00 0×16 0×90 0×00 0×00 0×07 0×00 0×00 0×00 0×04 0×30 0×32 0×33 0×30".

These fields have the following meanings:

- **Time stamp:** It is the creation time of the image
- **Company name:** It is the manufacture's company name which was known as "Research In Motion" and now operates globally under the iconic name "BlackBerry"
- **Device name and OS version:** It contains the mobile device brand and version of operating system at the time of taking the image

These three fields appears between the two fixed size hexadecimal strings. It would therefore come into sight that a search for each of the fixed hexadecimal string aforementioned, would reveal the time and date of image creation in addition to the device and the OS used to capture the image. It should be noted that hexadecimal string 0×30 0×32 0×33 0×30 (0230) appears to be related to the EXIF version. Figure 2 shows the file signature and its ASCII exactly as appear in the hex editor.

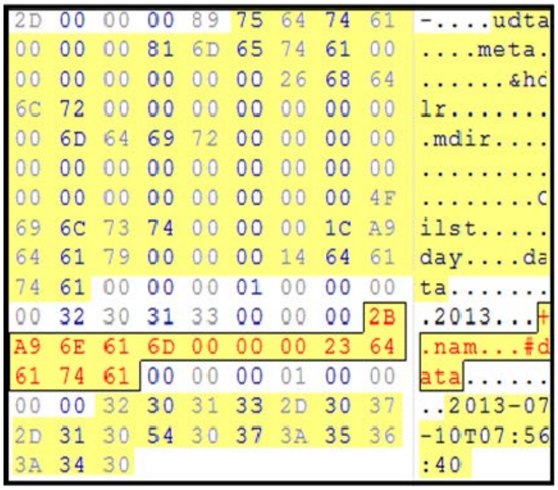

(a)

```
00000000  FF D8 FF E1 4D FC 45 78  ....M.Ex
00000008  69 66 00 00 4D 4D 00 2A  if..MM.*
```

(b)

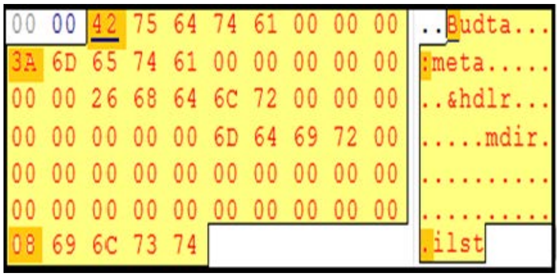
```
00000000  FF D8 FF E0 00 10 4A 46  ......JF
00000008  49 46 00 01 01 01 00 48  IF.....H
00000010  00 48 00 00 FF E1 13 08  .H......
00000018  45 78 69 66 00 00 4D 4D  Exif..MM
00000020  00 2A 00 00 00 08 00 09  .*......
```

Fig. 3(a-b): Hexadecimal header for camera images after being edited on the (a) Same phone and (b) PC



```
2D 00 00 00 89 75 64 74 61  -....udta
00 00 00 81 6D 65 74 61 00  ....meta.
00 00 00 00 00 00 26 68 64  ......&hd
6C 72 00 00 00 00 00 00 00  lr.......
00 6D 64 69 72 00 00 00 00  .mdir....
00 00 00 00 00 00 00 00 00  .........
00 00 00 00 00 00 00 00 4F  ........O
69 6C 73 74 00 00 00 1C A9  ilst.....
64 61 79 00 00 00 14 64 61  day....da
74 61 00 00 00 01 00 00 00  ta.......
00 32 30 31 33 00 00 00 2B  .2013...+
A9 6E 61 6D 00 00 00 23 64  .nam...#d
61 74 61 00 00 00 01 00 00  ata......
00 00 32 30 31 33 2D 30 37  ..2013-07
2D 31 30 54 30 37 3A 35 36  -10T07:56
3A 34 30                    :40
```

Fig. 4: Time stamp in BB Z10 camera videos



```
00 00 42 75 64 74 61 00 00 00  ..Budta...
3A 6D 65 74 61 00 00 00 00 00  :meta.....
00 00 26 68 64 6C 72 00 00 00  ..&hdlr...
00 00 00 00 00 6D 64 69 72 00  .....mdir.
00 00 00 00 00 00 00 00 00 00  ..........
00 00 00 00 00 00 00 00 00 00  ..........
08 69 6C 73 74                 .ilst
```

Fig. 5: Obscure pattern in edited videos

Another noticeable metadata comes in the format of: "0×41 0×053 0×43 0×49 0×49 (DCCver) (Time stamp)". These fields have the following meanings:

- **DCCver:** It is the version of Dynamic Camera Configuration which can be changed when OS updates to a new version
- **Time stamp:** It is the creation time of the image

After the image has been edited on the same mobile phone its hexadecimal header would be "0×FF 0×D8 0×FF 0×E1 0×09 0×AB 0×45 0×78 0×69 0×66 0×00" as shown in Fig. 3a.

In this case the first metadata mentioned before, would be changed to:

- 0×30 0×32 0×33 0×30 (Company name) (Device name) 0×48 0×00 0×00 0×00 0×01 0×00 0×00 0×00 0×48 (OS version) (Time stamp) and the second format to 0×41 0×053 0×43 0×49 0×49 (DCCver)

Any image taken by BB Z10 camera and modified on a computer PC has the hexadecimal header as demonstrated in Fig. 3b.

Then metadata pattern would be as:

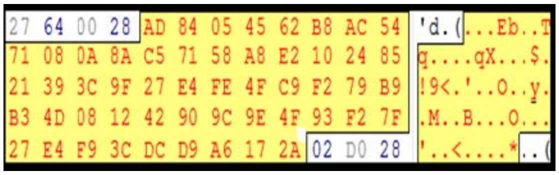
- "(Company name) (Device name) (OS version) (Time stamp) 0×30 0×32 0×33 0×30" And "(DCCver) (Create date) (Creator tool)". Unfortunately there is no indication of the access or modification time or date and the only time and date that was seen refers to the image creation.

Camera video: The videos hold metadata including time stamps but not any indication of manufacturer or device name. The hint for time and date are recorded at the very last offsets where its number depends on the size of the video. It has the style of "0×2B 0×A9 0×6E 0×61 0×6D 0×00 0×00 0×00 0×23 0×64 0×61 0×74 0×61 (Creation Date) (creation Time)". Figure 4 displays that a search for the fixed hexadecimal string shown above would reveal the time and date of the video creation.

Just before this string at the of the file, there is another pattern in the form of "0×89 0×75 0×64 0×74 0×61 0×00 0×00 0×00 0×81 0×6D 0×65 0×74 0×61 0×00 0×00 0×00 0×00 0×00 0×00 0×00 0×26 0×68 0×64 0×6C 0×72 0×00 0×00 0×00 0×00 0×00 0×00 0×00 0×00 0×6D 0×64 0×69 0×72 0×00 0×00 0×00 0×00 0×00 0×00 0×00 0×00 0×00 0×00 0×00 0×00 0×00 0×00 0×00 0×00 0×00 0×00 0×00 0×00 0×4F 0×69 0×6C 0×73 0×74 0×00 0×00 0×00 0×1C 0×A9 0×64 0×61 0×79 0×00 0×00 0×00 0×14 0×64 0×61 0×74 0×61".

The exact meaning of this field is obscure but have been found to be identical for all videos taken. Our experiments show that after editing the video on the same mobile device, file header doesn't change, however, no evidence related to date or time has been detected for the videos after being edited. It means that the first string declared above has not been found on the edited videos while the second one exist at the end of the file with three byte changes from the original video which can be seen in Fig. 5.

0×42 0×75 0×64 0×74 0×61 0×00 0×00 0×00 0×3A 0×6D 0×65 0×74 0×61 0×00 0×00 0×00 0×00 0×00 0×00 0×00 0×26 0×68 0×64 0×6C 0×72 0×00 0×00 0×00 0×00 0×00 0×00



```
27 64 00 28 AD 84 05 45 62 B8 AC 54 'd.(...Eb..T
71 08 0A 8A C5 71 58 A8 E2 10 24 85 q....qX...$.
21 39 3C 9F 27 E4 FE 4F C9 F2 79 B9 !9<.'..O..y.
B3 4D 08 12 42 90 9C 9E 4F 93 F2 7F .M..B...O...
27 E4 F9 3C DC D9 A6 17 2A 02 D0 28 '..<....*..(
```

Fig. 6: Another obscure pattern in the videos

0×00 0×00 0×6D 0×64 0×69 0×72 0×00 0×00 0×00 0×00 0×00 0×00 0×00 0×00 0×00 0×00 0×00 0×00 0×00 0×00 0×00 0×00 0×00 0×00 0×00 0×00 0×00 0×08 0×69 0×6C 0×73 0×74".

There is another ambiguous metadata which is common and exclusive for all videos taken by BlackBerry Z10's camera in the offset between 0×1000 and 0×2000 as it is shown in the Fig. 6. "0×00 0×00 0×00 0×3D 0×27 0×64 0×00 0×28 0×AD 0×84 0×05 0×45 0×62 0×B8 0×AC 0×54 0×71 0×08 0×0A 0×8A 0×C5 0×71 0×58 0×A8 0×E2 0×10 0×24 0×85 0×21 0×39 0×3C 0×9F 0×27 0×E4 0×FE 0×4F 0×C9 0×F2 0×79 0×B9 0×B3 0×4D 0×08 0×12 0×42 0×90 0×9C 0×9E 0×4F 0×93 0×F2 0×7F 0×27 0×E4 0×F9 0×3C 0×DC 0×D9 0×A6 0×17 0× 2A".

This string remains the same in case the video is edited on the phone.

Voice files: The voice files generated in the "Remember" application as the "Voice note", have the similar pattern to edited video files which means there is no date or time detection. In addition, same strings appear at the very end of the file.

"0×42 0×75 0×64 0×74 0×61 0×00 0×00 0×00 0×3A 0×6D 0×65 0×74 0×61 0×00 0×00 0×00 0×00 0×00 0×00 0×00 0×26 0×68 0×64 0×6C 0×72 0×00 0×00 0×00 0×00 0×00 0×00 0×00 0×00 0×6D 0×64 0×69 0×72 0×00 0×00 0×00 0×00 0×00 0×00 0×00 0×00 0×00 0×00 0×00 0×00 0×00 0×00 0×00 0×00 0×00 0×00 0×00 0×00 0×00 0×08 0×69 0×6C 0×73 0×74".

Although, voice files don't include the second pattern: "0×00 0×00 0×00 0×3D 0×27 0×64 0×00 0×28 0×AD 0×84 0×05 0×45 0×62 0×B8 0×AC 0×54 0×71 0×08 0×0A 0×8A 0×C5 0×71 0×58 0×A8 0×E2 0×10 0×24 0×85 0×21 0×39 0×3C 0×9F 0×27 0×E4 0×FE 0×4F 0×C9 0×F2 0×79 0×B9 0×B3 0×4D 0×08 0×12 0×42 0×90 0×9C 0×9E 0×4F 0×93 0×F2 0×7F 0×27 0×E4 0×F9 0×3C 0×DC 0×D9 0×A6 0×17 0×2A".

Presentation of data: In our case study, a variety of artefacts were identified when a Blackberry Z10 Smartphone is used to create multimedia files. This information enables an examiner to conduct keyword searches for multimedia files information. The focus was to determine whether can relate the Blackberry Z10 to multimedia files as the file generator. In total, it has been demonstrate that it is possible to determine device name and OS version for the camera images and times of creation for camera images and videos.

In addition, there are some other obscure artefacts that however are meaningless for us at this time, they can determine if multimedia files manually collected form Blackberry Z10 phone, are created locally on the phone or obtained from elsewhere. Once forensic analysis has determined a Blackberry Z10 as the source of a suspected or unethical multimedia file, the examiner can communicate this to relevant persons to act accordingly.

CONCLUSION

The approach followed in this paper is appreciated in addressing cases where source identification is largely associated with multimedia files collected from Smartphones. In our case study, it was found that an examiner can identify Blackberry Z10 Smartphone as the source of such files by undertaking keyword searches. It can be concluded that File Signature Analysis is an essential preliminary technique in forensic computing.

The findings of this study make it possible for the investigator to determine if multimedia files manually collected form Blackberry Z10 Smartphone are created locally on the phone or not. In addition it facilitates identification of OS version, time stamp, proof of file editing, etc. The outcome from this paper could be applied in existing forensics tools such as EnCase or Oxygen Forensic Suite in order to enable them to support file signature analysis of Blackberry Z10 mobile devices. We believe that future research areas include conducting research into the artefacts of other files types also studying other Smartphone models as the file generator. In the future we will try to conduct same approaches on other file types, still using Blackberry Z10.

ACKNOWLEDGMENT

This study has been supported by the Malaysian Ministry of High Education under the Long Research Grant Scheme LRGS/TD/20/11/UKM/ICT/02/04.

REFERENCES

ACPO., 2006. Good practice guide for computer-based electronic evidence. Association of Chief Police Officers (ACPO), Official Release Version 4.0, pp: 1-66.

Deng, Z., A. Gijsenij and J. Zhang, 2011. Source camera identification using auto-white balance approximation. Proceedings of the IEEE International Conference on Computer Vision, November 6-13, 2011, Barcelona, pp: 57-64.

Farjamfar, A., M.T. Abdullah, R. Mahmod and N.I. Udzir, 2014. A review on mobile device's digital forensic process models. Res. J. Applied Sci. Eng. Technol., 8: 358-366.

Ghosh, A., 2004. Guidelines for the management of IT evidence. Proceedings of the Incident Response and Forensics Workshop, March 21-26, 2004, Hong Kong, China, pp: 1-26.

Haggerty, J. and M. Taylor, 2007. Forsigs: Forensic signature analysis of the hard drive for multimedia file fingerprints. Proceedings of the IFIP TC-11 22nd International Information Security Conference on New Approaches for Security, Privacy and Trust in Complex Environments, May 14-16, 2007, Sandton, South Africa, pp: 1-12.

Jansen, W. and R. Ayers, 2007. Guidelines on cell phone forensics. NIST Special Publication 800-101, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg, MD., USA., May 2007.

Jones, A. and C. Valli, 2011. Building a Digital Forensic Laboratory: Establishing and Managing a Successful Facility. Butterworth-Heinemann, Burlington, MA., ISBN-13: 9780080949536, Pages: 312.

Jozwiak, I., M. Kedziora and A. Melinska, 2011. Theoretical and Practical Aspects of Encrypted Containers Detection-Digital Forensics Approach. In: Dependable Computer Systems, Zamojski, W., J. Kacprzyk, J. Mazurkiewicz, J. Sugier and T. Walkowiak (Eds.). Springer Science and Business Media, New York, ISBN: 9783642213939, pp: 75-85.

Li, C.T., 2010. Source camera identification using enhanced sensor pattern noise. IEEE Trans. Inform. Forensics Secur., 5: 280-287.

McKemmish, R., 1999. What is forensic computing? Trends and Issues in Crime and Criminal Justice No. 118, June 1999, Australian Institute of Criminology, Canberra, Australian, pp: 1-6.

Owen, P. and P. Thomas, 2011. An analysis of digital forensic examinations: Mobile devices versus hard disk drives utilising ACPO and NIST guidelines. Digital Invest., 8: 135-140.

Palmer, G., 2001. A road map for digital forensic research. DTR-T001-01 Final, DFRWS Technical Report, Utica, New York, USA., November 6, 2001. http://www.dfrws.org/2001/dfrws-rm-final.pdf

Richard, G.G. and V. Roussev, 2005. Scalpel: A frugal, high performance file carver. Proceedings of the Digital Forensic Research Workshop, August 17-19, 2005, New Orleans, LA., USA., pp: 1-10.

SWGDE., 2011. Scientific working groups on digital evidence and imaging technology. SWGDE/SWGIT Digital and Multimedia Evidence Glossary Version: 2.4, January 14, 2011, pp: 1-18.

Shaw, A. and A. Browne, 2013. A practical and robust approach to coping with large volumes of data submitted for digital forensic examination. Digital Invest., 10: 116-128.

Tsai, M.J., C.L. Lai and J. Liu, 2007. Camera/mobile phone source identification for digital forensics. Proceedings of the IEEE International Conference on Acoustics Speech and Signal Processing, Volume 2, April 15-20, 2007, Honolulu, HI., pp: 221-224.

Yip, M., 2008. Signature analysis and computer forensics. School of Computer Science, University of Birmingham, UK., December 26, 2008, pp: 1-11.