Digital Camcorder Forensics

Aswami Ariffin[1,2], Kim-Kwang Raymond Choo[1], Jill Slay[1]

[1] Information Assurance Research Group, Advanced Computing Research Centre,
School of Computer and Information Science,
University of South Australia, Mawson Lakes Campus, SA 5095, Australia

[2] CyberSecurity Malaysia,
Level 8, Block A, Mines Waterfront Business Park, No 3 Jalan Tasik, The Mines Resort City,
43300 Seri Kembangan, Selangor Darul Ehsan, Malaysia

Email: aswamifadillah@gmail.com, Raymond.Choo@unisa.edu.au, Jill.Slay@unisa.edu.au

Abstract

Digital camcorders commonly have an in-built capability to export entire video files or a single image to storage media such as a digital versatile disc (DVD). In the event that a DVD is not properly finalised, its contents might not be easily readable. It is generally accepted that recovering video evidence from an unfinalised DVD in a forensically sound manner is an expensive and a challenging exercise. In this paper, we propose a digital camcorder forensics technique that allows digital forensics examiners to carve video files with timestamps without referring to a file system (file system independent technique). We then conduct a forensic analysis to validate our proposed technique.

Keywords: Digital camcorder forensics, unfinalised digital versatile disc, video stream, format, timestamp, file signature, data carving.

1 Introduction

The declining cost of electronic data recording devices (e.g. digital camcorders) and storage media will continue to lower entry barriers for digitization of information, particularly multimedia contents. Choo et al. (2007) explained that the proliferation of information and communication technology (ICT) has not just spawned a new domain of criminal activities but the ability to commit traditional crimes is being enhanced by the use of such technologies. For example, the creation and the dissemination of child abuse/exploitation materials have long been in existence and with ICT have made it much easier and quicker to disseminate and share such illicit materials in real-time.

The presence of digital evidence is central to the digital forensics discipline (see Porter (2011) where some of the early cases included photos and videos submitted as evidence in a court of law). For example, in a case involving a digital camcorder and a digital versatile disc (DVD), one of the first activities is to recover the video evidence from the DVD in a forensically sound manner.

Although multimedia forensics research is not new (see Bijhold et al., 2007), there are still worthwhile contributions, particularly on content analysis of video, audio and biometric (see Battiato et al., 2012; Porter, 2011). However, without recovering the multimedia evidence, it would not be possible to analyse its contents.

In multimedia forensics, it is extremely challenging to recover multimedia evidence in a forensically sound manner without data recovery expertise in a wide range of storage media (optical, magnetic and semiconductor) with different file systems and video file formats. The challenge is compounded if the storage media of digital video recorder (DVR; the core electronic component of digital camcorder and closed-circuit television (CCTV)) is physically damaged or logically corrupted. Seek (2010: 51), for example, explained that 'not all exhibits come to [the Singapore Police Force's Technology Crime Forensic Branch] physically sound. Some exhibits are deliberately damaged by criminals in a bid to destroy evidence while others are already in poor physical conditions resulting in read-sector errors during the acquisition process or lengthened acquisition time'.

Thus, to recover evidence from damaged (electrical or mechanical failure) or corrupted (file system or video) storage media of DVR, digital forensics examiners need to have an intimate understanding of the underlying DVR systems (Sobey et al., 2006). It is highly infeasible for digital forensics examiners in law enforcement agencies (LEAs) to seek assistance from DVR manufacturers (our technique is vendor independent) as the latter is likely to be located in overseas jurisdictions. In some instances, forensic and multimedia specialists from abroad may have to be engaged to recover digital evidence. For example in the incident involving the murder of a taxi/cab driver in Melbourne, it was reported that 'MELBOURNE cabbies are demanding answers after the hi-tech camera in murdered driver Stephen Seymour's taxi had to be sent overseas to try to retrieve images of his killer ... [as] the CCTV manufacturer was "unable to access the footage"' (Thom 2012: np). These challenges will impede digital forensics examiners and potentially prevent LEAs from recovering and analysing multimedia evidence in a timely fashion.

There is, clearly, an urgent need for digital forensics examiners and researchers to adapt and augment technical and procedural digital forensics responses as criminals or otherwise, who are often early adopters, use new technologies in different ways to facilitate crime activities, both traditional criminal (e.g. drug trafficking

and murder) and cybercriminal (e.g. production of child abuse materials).

In this paper, we propose a forensically sound technique that conforms to digital forensics principles and framework, which would allow digital forensics examiners to carve[1] video files with timestamps[2] from an unfinalised DVD (file system independent technique). We then conduct a forensic analysis on a digital camcorder (a DVD based SONY Camcorder model DCR-DVD605E) to validate our proposed technique. This technique would serve both as a technical reference to digital forensics examiners (for expert witness, Aswami et al., 2008) and a scientific reference to legal practitioners (e.g. deputy public prosecutors and defence attorneys).

The digital camcorder was chosen due to its popularity among end users and, possibly, criminals (e.g. newer camcorders are designed to fit in the palm of the user's hand). A Gartner research estimated that the worldwide production of digital camcorders in 2011 was 16.6 million units and expected to grow by 2.4% in 2012 (Shimizu, 2012).

The remainder of this paper is structured as follows: Section 2 provides a general overview of the digital forensics principles, framework and our proposed technique. We then demonstrate how our forensic analysis can be used in digital camcorder investigations (repair work on logical, mechanical and electrical is beyond the scope of this paper). The last section concludes the paper and outlines potential future research opportunities.

2 Derivation of digital camcorder forensics from digital forensics principles and framework

2.1 Digital forensics overview

Digital forensics, often interchangeably known as computer forensics and forensic computing, is a relatively new sub-discipline of forensic science when compared to DNA forensics. The development of digital forensics processes is built on sound scientific principles so that recovered evidential data can be demonstrated to be trustworthy – one of the pillars/requirements in digital forensics.

Digital forensics is increasingly used in civil and criminal (traditional crime and cybercrime) cases involving digital evidence; and has been extensively used in court to inculpate or exculpate suspects (Aswami et al., 2012). A widely used digital forensics framework is that of the US National Institute of Standards and Technology (NIST) comprising (1) Collection: identifying relevant data, preserving its integrity and acquiring the data; (2) Examination: uses automated and manual tools to extract data of interest while ensuring preservation; (3) Analysis: concern with deriving useful information from the results of the examination; and (4) Reporting: the preparation and the presentation of forensic analysis (Kent et al., 2006, p.ES-1).

The NIST framework is similar to that of McKemmish (1999) – see Martini & Choo (2012) for a comparison between these two frameworks and Slay et al. (2009) for a general review of the digital forensics development of principles, procedures, models, guides and standards. Digital forensics frameworks differ primarily in how granular each phase of the processes is and in the terms used for specific phases, but they generally reflect the same basic principles and the same overall processes.

A key component of digital forensics is data recovery involving logical, mechanical and electrical repair work of storage media (see examination phase of the NIST framework and analysis phase of McKemmish (1999)'s framework). The latter is an intricate process as it may involves repairing a wide range of storage media (magnetic, optical and semiconductor) before digital evidence can be analysed for forensic investigations and understanding of the underlying storage media technologies (Agrawal et al., 2009), file systems and data formats is essential. As such, recovering video files from a DVR with proprietary file system can be exceptionally complex; digital forensics examiners can instead analyse the data format for signature as each video file has its own unique structure that could be carved during the data recovery work.

In this paper, we adopt McKemmish (1999)'s digital forensics framework as the overarching framework for our technique, which comprises (1) identification, (2) preservation, (3) analysis and (4) presentation of digital evidence – also see Figure 1.

- Identification is a detailed study of digital evidence to understand what evidential data is present, its possible location, the type of storage media and format.
- Preservation is an important rule that ensures digital evidence remains unchanged. A forensic copy of the digital evidence (storage media) is created to protect and maintain the digital evidence in its pristine state so that forensic analysis is conducted on a forensic copy. In the event that the storage media of digital evidence is physically damaged or logically corrupted, it would be necessary to repair the storage media before the preservation and analysis work could commence.
- Analysis is conducted on a forensic copy (i.e. a bit-by-bit copy) using specialised technique and digital forensics tools. The time taken in the forensic analysis varies depending on the storage media capacity and the technicality involved.
- Presentation is to report all findings including the work of preservation and forensic analysis in a court of law.

2.2 Our proposed technique

Figure 1 outlines our proposed technique and how it aligns with McKemmish (1999)'s digital forensics framework.

[1] Data carving is a commonly used technique in digital forensics to extract a collection of data from a larger data set (see http://www.dfrws.org/2006/challenge/).

[2] The date of the crime committed is important to charge the offender or suspect. It is obtained by correlating the recording time with the actual time of incident.

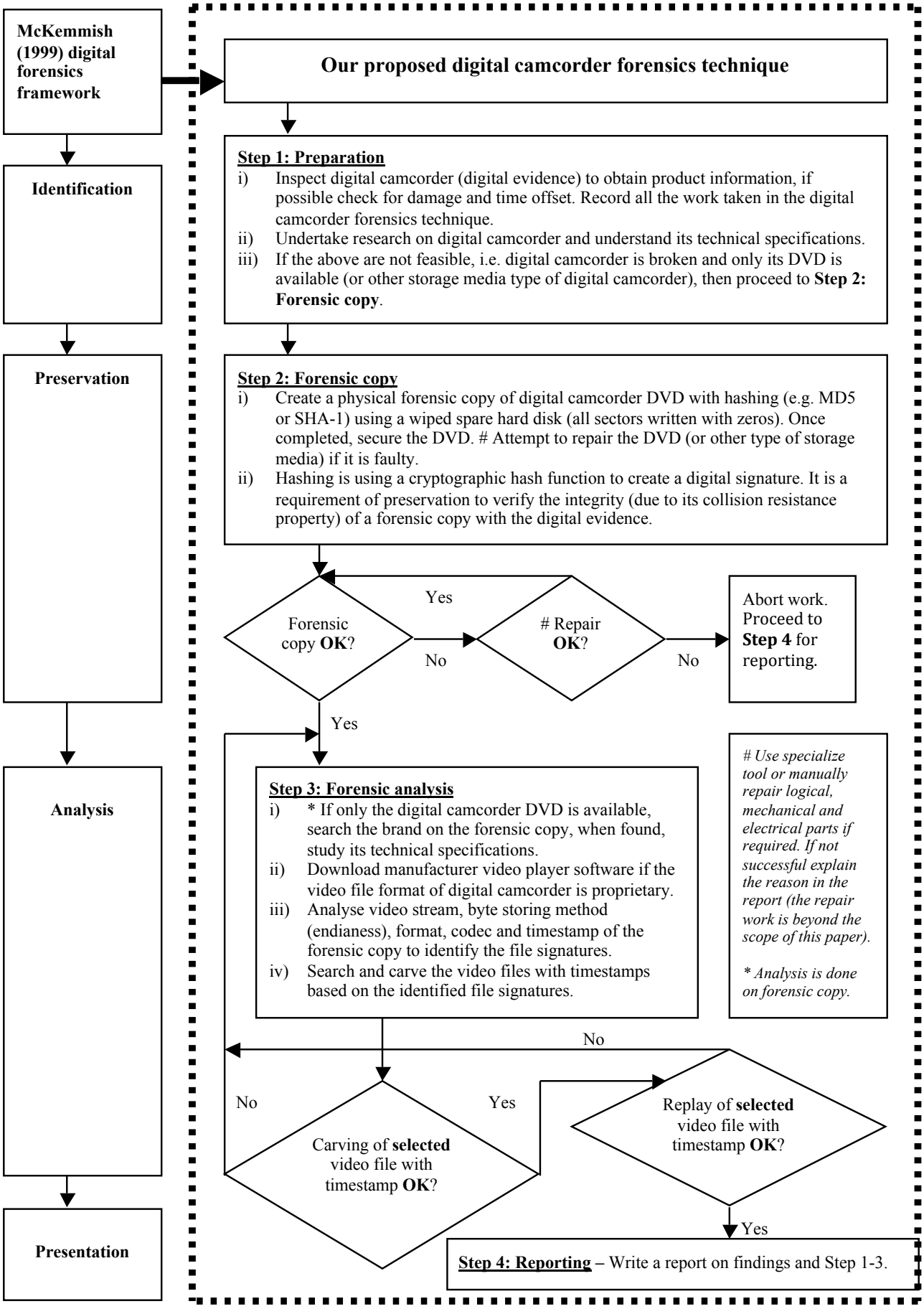

Figure 1: Flowchart illustrating McKemmish (1999) digital forensics framework and our proposed digital camcorder forensics technique

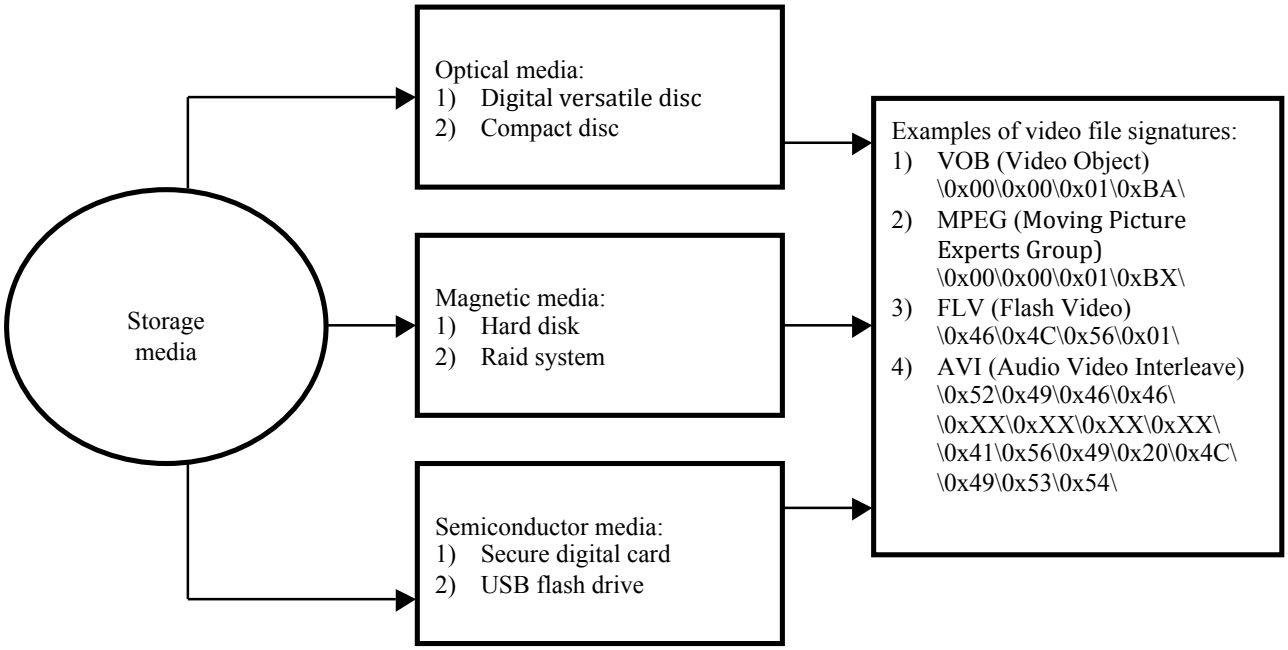

Figure 2: Storage media and video file signatures

Step 1: Preparation

The preparation step plays a fundamental role to determine the possible location, type of storage media and format of digital evidence. As an example, in cases involving mobile devices, the likely digital evidence includes video files, internet browsing histories and GPS (Global Positioning System) locations. It is, therefore, crucial that during the preparation step, digital forensics examiners inspect the digital evidence to obtain product information, if possible check for damage and time offset (the difference between actual and digital evidence time, this is for legal purpose) and record all the work performed in the digital camcorder forensics technique. Then it is essential to undertake research on the digital evidence in order to gain better understanding of its specifications during forensic analysis. If the digital camcorder is broken and only its DVD is available (or other storage media type of digital camcorder), then proceed to Step 2: Forensic copy.

In digital camcorder forensics, digital forensics examiners would need to understand the main electronic components of a digital camcorder (namely, camera, DVR and storage media) and how it works. The camera captures the scene through the charge-coupled device and converts it to electrical signal. The signal is converted to digital within the DVR's system using an analogue to digital converter. The video data is then formatted in a file container with specific codec and other digital data such as audio or subtitle (timestamp). Finally, the video file is stored to a DVD (or other storage media, depending to its specification), which can be played on a compatible DVD player or desktop computer.

This first step would allow digital forensics examiners to seek additional expertise, if deemed necessary, to ensure he/she has the requisite knowledge and tools to recover the evidential data (such as in the case involving the murder of the taxi/cab driver in Melbourne – see Thom 2012).

Step 2: Forensic copy

The second step of the proposed technique is creating a forensic copy of the digital camcorder DVD with hashing (using a cryptographic hash function to create a digital signature) using a wiped spare hard disk (all sectors written with zeros) and, once completed, secure the DVD. Hashing, using MD5 (Message Digest 5) or SHA-1 (Secure Hash Algorithm-1), is a requirement in the preservation step to verify the integrity (due to its collision resistance property) of a forensic copy.

It should be noted that digital evidence to be processed may not be received in working condition (e.g. hard disk with head or firmware faults), and creating a physical forensic copy of digital evidence (storage media) can be challenging. Failing which, we will not be able to preserve and analyse the digital evidence as forensic analysis needs to be conducted on a forensic copy.

We would need to repair the hard disk to be able to do a bit-by-bit copy (i.e. making a forensic copy of the storage media). Repairing a faulty head of hard disk (beyond the scope of this paper) require a clean facility to avoid any particles contaminating the platter and for firmware problem, replace the printed circuit board assembly of the hard disk. For a scratched and scuffed DVD, a refinishing machine and a repair kit would be able to repair the DVD.

Step 3: Forensic analysis

In this step, digital forensics examiners are able to determine the video file format from the DVD forensic copy based on its file signature. Depending on the outcome of Step 1, digital forensics examiners may be able to know the video file format and its file signature in advance based on the specifications of the digital camcorder. Knowing which video file format will enable digital forensics examiners to analyse, search, carve and choose the appropriate player with the right codec to replay the video files with timestamps.

If only the digital camcorder DVD is available, search the brand on the forensic copy, when found, study its technical specifications. Download the video player software of the manufacturer if the video file format of the digital camcorder is proprietary.

The forensic analysis is to analyse the video stream, byte storing method (endianess), format, codec and file signature of the DVD forensic copy to carve the video files with timestamps. Even though the timestamp of a video file could only be obtained from a file system in standard recovery, we choose not to include a reference to a file system (e.g. when the digital camcorder DVD is not properly finalised – as we described in our forensic analysis phase (see Section 2.3.3)) as it is possible to recover the timestamp using our specialised technique.

The challenge of recovering video files with timestamps (supplementary important data to prove time and date of incident) from an unfinalised DVD is by analysing the video stream for its internal unique format. This forensic analysis will determine the video file signature in hexadecimal value for data searching, carving and replay. Note that all video files have their own format and the header/footer of a file has a unique identity (file signature) – see Figure 2 for examples of known video file signatures and storage media. Hence, having a database of known file signatures is useful for forensic analysis and a customised tool to carve digital camcorder videos.

Step 4: Reporting

The challenge of presenting digital evidence in a court of law is aptly summarised by the former South Australia's Director of Public Prosecutions: 'for the prosecutor, the challenge is to have the data translated into a form that is acceptable as evidence to the courts … Assuming that the fragile and elusive evidence can be gathered together, the prosecutor must keep in mind that he or she will 1 day need to be able to prove the chain of evidence. All processes will need to be appropriately documented in a way that can be understood by the layman and the prosecutor must be prepared if necessary to demonstrate that the 'original' digital material has not been changed or tampered with in any way' (Pallaras 2011: 80).

The fourth and final step is to ensure that the findings are explained in a manner that is understandable to investigators, judiciary (including juries), prosecutors and other decision makers. The report must cover the whole digital camcorder forensics technique from Step 1 to Step 3 (as per the record of work performed in the digital camcorder forensics technique). In addition, when a number of parties have been involved in the possession of the digital evidence, it is critical that the chain of custody log records the details of the individuals (e.g. digital forensics examiners and LEAs).

2.3 Forensic analysis of a SONY camcorder

In our forensic analysis, we used a DVD based SONY camcorder model DCR-DVD605E as the forensic investigation item (Figure 3). The DVD was double sided totalling 2.8Gbytes but only one side of the DVD was analysed (the other side was blank). The tools and software of our forensic analysis are outlined in Table 1.

Figure 3: SONY DCR-DVD605E Camcorder

No.	Item
1.	EnCase 6.7, digital forensics tool.
2.	WinHex 14.5, storage media hexadecimal editor tool commonly used for data recovery and digital forensics.
3.	VLC Version 1.0.2, video, audio and subtitle player software.
4.	ImgBurn 2.5.5.0, DVD software for forensic copy.
5.	MacBook Pro laptop with Windows XP virtual system for Windows based software.

Table 1: Digital forensics tools and computer application software

2.3.1 Preparation phase

According to the SONY camcorder features and manual, the DVD needs to be finalised for it to be recognised by operating systems such as Windows XP. If finalised, the DVD's file system would be in UDF (Universal Disk Format) that defines the overall disc structure such as the volume. The UDF is read by the operating system so that installed DVD applications would be able to view the DVD contents.

As explained in earlier section, we choose an unfinalised DVD to demonstrate that we are able to recover the evidential data (video files with timestamps) by carving. As per Step 1 described in Section 2.2 (and in Figure 1), we conducted an inspection of the forensic investigation item and undertook the background research to have an in-depth understanding of its technical specifications (i.e. video file format). Concurrently, the time of the digital camcorder was checked to determine the offset[3] with the actual time (atomic or server time) and it was found to be lagging by approximately five minutes (due to manual time setting as there was no automatic synchronization). From this point onwards until completion, the work performed in the digital camcorder forensics technique was recorded for reporting.

2.3.2 Forensic copy phase

As anticipated, neither the Windows XP operating system nor EnCase 6.7 (a widely used commercial digital forensics tool that is accepted by courts) could read the

[3] In a court case, time offset is important for verification against the actual time of event. If not, the video file's timestamp of the DVD could be used.

unfinalised DVD as there was no file system. We then used ImgBurn 2.5.5.0 to create a one sided physical forensic copy of the DVD for forensic analysis (no repair work was required).

The size of the DVD forensic copy was about 1.4 Gbytes and the hash of the DVD forensic copy was taken as part of the preservation requirement using WinHex 14.5. The MD5 hash value (digital signature) was 3d35cee476e23fb72911d5f5d7cedb14 with 2,048 bytes per sector and 694,688 total sectors.

2.3.3 Forensic analysis phase

The video stream of the DVD forensic copy was analysed for its byte storing method (endianess) and any recognisable video file format using WinHex 14.5. In this case, the hexadecimal value of \0x00\0x00\0x01\0xBA\ was searched in the DVD forensic copy based on Step 3 and 1 of our proposed technique; this is Video Object (VOB) file header (signature) and VOB file format is commonly used for DVD video.

We found a few hexadecimal file signatures of the VOB header (see Figure 4), which was one of the known video file signatures outlined in Figure 2. In total, four VOB files were found, whose maximum size not exceeding 1Gbytes (note that the size limitation is specified in the VOB specification). The video, audio and timestamp tracks were interleaved in the DVD forensic copy of the unfinalised DVD. Three tracks were (track 0: video, track 1: audio and track 2: timestamp) contained in a single VOB file, multiplexed together as a stream.

Offset	0	1	2	3	4	5	6	7
00000000	00	00	01	BA	44	00	EC	89
00000020	5E	AF	87	50	99	82	CD	0A
00000040	69	11	45	0C	41	35	B1	C2
00000060	01	02	1A	E2	06	33	EB	76
00000080	01	76	B3	84	D9	EC	B0	F8
000000A0	BF	B0	FF	E0	07	DD	18	02
000000C0	37	AB	B2	80	94	43	46	1A
000000E0	8C	1E	70	B8	9A	49	18	20
00000100	00	A4	F7	71	7D	52	40	FE
00000120	21	F7	30	56	88	45	17	B9
00000140	87	0E	39	AD	80	C6	04	EF
00000160	BE	38	77	D9	77	F8	0D	D2

Figure 4: File signature of VOB

We then carved four VOB files from the DVD forensic copy based on its file signature, arrangement (Table 2), size and padding (0x00s and 0xFFs) using WinHex 14.5 for replay. The four VOB files were located at offsets 0x4B8000, 0x1850000, 0x423C0000 and 0x52788000 of the DVD forensic copy.

No.	Logical Block Address (LBA)	Offset	File	Size
1.	2304	0x480000	IFO 1	14Kbytes
2.	2416	0x4B8000	VOB 1	19Mbytes
3.	12160	0x17C0000	IFO 1 (BUP 1)	14Kbytes
4.	12288	0x1800000	IFO 2	30Kbytes
5.	12448	0x1850000	VOB 2	1Gbytes
6.	542416	0x42368000	IFO 2 (BUP 2)	30Kbytes
7.	542432	0x42370000	IFO 3	14Kbytes
8.	542592	0x423C0000	VOB3	27Mbytes
9.	556208	0x43E58000	IFO 3 (BUP 3)	14Kbytes
10.	675568	0x52778000	IFO 4	36Kbytes
11.	675600	0x52788000	VOB 4	36Mbytes
12.	694496	0x54C70000	IFO 4 (BUP 4)	36Kbytes

Table 2: VOB and IFO files

From the VOB file specification, Moving Picture Experts Group (MPEG) codec was used for its video compression. Since the type of the codec was known, there was no further need to analyse the codec of the VOB files. The recovered VOB files with timestamps were replayed using VLC 1.0.2 player with MPEG codec.

Two snapshots were taken from the VOB second file (at offset 0x1850000) using VLC 1.0.2 player. As shown in Figures 5 and 6 respectively, there was no timestamp on the first snapshot (subtitle feature was disable in the VLC 1.0.2 player) but the second snapshot suggested that the video was taken on 31 May 2009 at 20:54:04 (subtitle feature was enable in the VLC 1.0.2 player). It showed that we managed to recover the evidential data (all video files with timestamps) by carving and without referring to the underlying file system.

Figure 5: Snapshot of recovered video without timestamp

Figure 6: Snapshot of recovered video with timestamp

We also verified the reliability of the timestamp in Figure 6 by checking the first info (IFO) file; an IFO file is always in front of a VOB file and contains all DVD information for navigation purposes including the brand. By searching the IFO file signature of \0x44\0x56\0x44\ (Figure 7) beginning from sector 0, the first IFO data was located at offset 0x480000. According to the IFO data, the brand was a SONY MOBILE and the DVD format date was on 29 May 2009 at 20:53 (Figure 8) and was progressively in sequence with the timestamp in Figure 6.

This verification was important to reaffirm the validity of all video timestamps; the importance of timestamp is explained in a report by UNODC (2012: 92): 'time and date stamps on digital files can be a compelling method of linking the defendant to the relevant device at times material to the commission of a crime'.

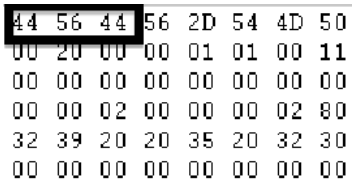

Figure7: File signature of IFO

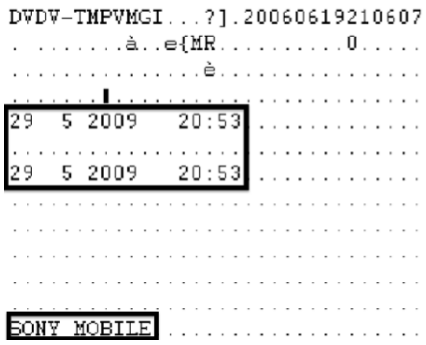

Figure 8: IFO data on DVD format date and brand

We also managed to recover an 'old' VOB file (video remnant) from the previous recording at offset 0x52788000 (Figure 9), and pursue to this, we took a snapshot (using VLC 1.0.2 player) of the video remnant with timestamp on 11 June 2008 at 18:19:54, as shown in Figure 10. We consequently demonstrated that the same data carving method was used to recover video remnant (in unallocated space) that would not be logically shown if there was a file system.

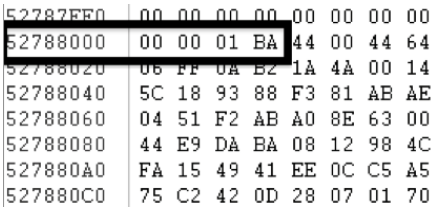

Figure 9: Offset location of an 'old' VOB file

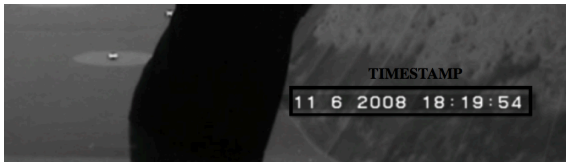

Figure 10: Snapshot of video remnant with timestamp

According to the timestamps of the first three recovered VOB files and IFO data, the recordings of our forensic investigation item were in year 2009 but the timestamp of the video remnant was in year 2008. Such information on VOB files will help digital forensics examiners to distinguish between active (logical) and remnant (physical) data. The 'old' VOB file might also contain incriminating evidential data.

2.3.4 Reporting phase

The findings of the forensic analysis must be reported in a legally acceptable manner and compliant with the local court requirements. The report shall include all the work performed in the digital camcorder forensics technique including any limitations to prevent false conclusions from being reached.

3 Conclusions and future work

With the prevalence of devices capable of recording video (e.g. digital camcorders and CCTVs, mobile phones and other smart devices) and advent of more complex data storage and dissemination technologies, digital forensics examiners face an increasingly difficult task in digital forensics investigations.

The lack of recent understanding of the complexity and the challenges in keeping pace with rapid advancement in ICT further hinder digital forensics examiners in criminal and civil cases, and in national security investigation. Porter (2011: 27–28), for example, warned that 'the technological developments have also increased the dangers associated with inaccurate or unreliable photographic evidence [including] (1) images sourced from witnesses photographing a criminal event using portable digital cameras or mobile phones; (2) CCTV recordings; (3) images recovered from computer hard drives; and (4) images posted on social networking sites'.

The development of digital forensics techniques needs to be built on sound scientific principles to ensure that the digital evidence is trustworthy and admissible in a court of law (Barrett and Kipper, 2010; Manes, 2010). Research on multimedia forensics (including digital camcorder forensics) is continuing, and as highlighted by Porter (2011: 56) – 'the question regarding the reliability of photographic evidence [such as video] is a poignant one that has had little discussion in the forensic science, criminology and law literature'.

Using a digital camcorder as a forensic investigation item, we demonstrated how our proposed technique can be used by digital forensics examiners to carve video files with timestamps without referring to a file system (file system independent). The recovered data (video snapshot in Figure 6) can then be analysed to identify the suspect's vehicle (e.g. enhance the video clip to identify the vehicle registration number) and be used as proof of criminal activity. This specialised technique is generally applicable to other brands of digital camcorders with different types of storage media because it was technically devised and not based on certain brand/product.

Our proposed technique (see Figure 1) can also be adopted in a digital forensics laboratory's standard operating procedure (SOP) as per the requirements of the American Society of Crime Laboratory Directors Laboratory Accreditation Board (ASCLD/LAB-International) and ISO/IEC 17025:2005 (general requirements for the competence of testing and calibration laboratories). To further advance understanding in digital camcorder forensics, the following potential future research is proposed.

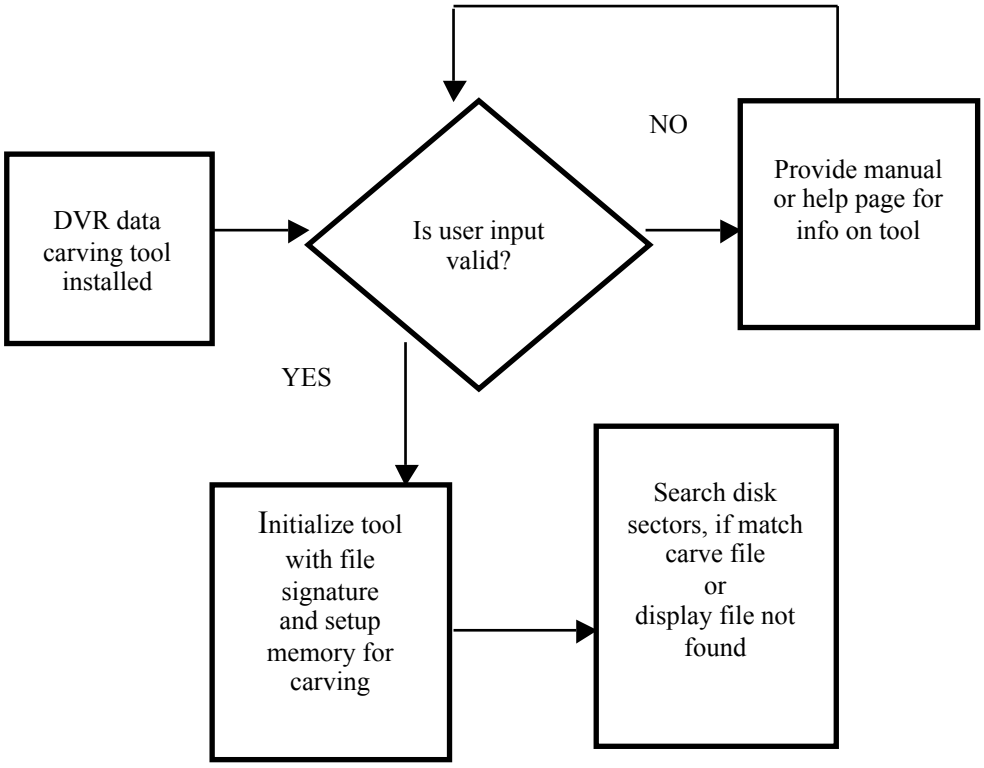

Figure 11: Potential research – development of a DVR data carving tool (DVRDCT)

The need for a customised DVR data carving tool

Digital forensics processes are often misconstrued as entirely automated, but in reality, the forensic analysis of digital evidence is a time consuming manual process undertaken by qualified digital forensics examiners (Seek 2010).

It is unlikely that we will have sufficient policing resources to investigate all cases involving digital evidence and is it unrealistic to expect that LEAs have the capacity to forensically examine the ever increasing size of electronic data. For example, NCMEC's Child Victim Identification Program has reportedly analysed more than 10.5 million child pornography images in 2009 alone to identify the child victims – a 432% increase over 2005 (NCMEC 2009). Digital forensics investigations can often exceed the resources available to digital forensics examiners in LEAs, particularly at a state and local level. Backlogs in the forensic analysis of digital evidence can delay or hinder criminal investigations.

Therefore to improve the efficiency of digital camcorder forensics and to speed up the recovery process, we propose that a DVR data carving tool (DVRDCT) be developed – see Figure 11. For example, the handling of byte arrangement (endianess), the signature search (such as a database of known video file signatures in Figure 2) and offset calculation[4] could be translated into an algorithm. The latter can then be coded to create the DVRDCT that conforms to digital forensics principles and framework.

As well as being user friendly (presenting the user with the tool manual or suggestion on input command to use), the tool should ideally have functions such as:

- The ability to create a reference list for all possible video headers and footers (file signatures) with minimal human intervention;
- The ability to process the input command and check for error with minimal human intervention; and
- The ability to search and carve video files with timestamps within a specified time frame with minimal human intervention.

[4] An offset is the difference in bytes between the position of a header and footer or the next file header.

Acknowledgments

The views and opinions expressed in this article are those of the authors alone and not the organisations with whom the authors are or have been associated/supported. The authors thank the reviewers for providing constructive and generous feedback. Despite their invaluable assistance, any errors remaining in this article are solely attributed to the authors.

References

[All URLs were last accessed (and correct on) 6 August 2012.]

Agrawal, V., Bhattacharyya, C., Niranjan, T. and Susarla, S. (2009): Discovering Rules from Disk Events for Predicting Hard Drive Failures. *International Conference on Machine Learning and Applications*.

Aswami, A., and Izwan, I. (2008): Digital Forensics in Malaysia. *Digital Evidence and Electronic Signature Law Review* **5.** http://www.deaeslr.org/2008.html.

Aswami, A., Slay, J. and Husin, J. (2012): Digital Forensics Institute in Malaysia: the way forward. *Digital Evidence and Electronic Signature Law Review* ***9***. http://www.deaeslr.org/2012.html.

Barrett, D. and Kipper, G. (2010): *Cloud Computing and the Forensic Challenges*. Virtualization and Forensics, Syngress, Boston.

Battiato, S., Emmanuel, S., Ulges, A. and Worring, M. (2012): Multimedia in Forensics, Security and Intelligence. *IEEE Multimedia Magazine* **19**(1):17-19.

Bijhold, J., Ruifrok, A., Jessen, M., Geradts, Z., Ehrhardt, S. and Alberink, I. (2007): Forensic audio and visual evidence 2004-2007: A Review. *15th INTERPOL Forensic Science Symposium*, Lyon, France.

Choo, K.K.R., Smith, R.G. and McCusker, R. (2007): *Future directions in technology-enabled crime: 2007-2009*. Research and public policy No 78, Canberra: Australian Institute of Criminology.

Kent, K., Chevalier, S., Grance, T., and Dang, H. (2006): Guide to integrating forensic techniques into incident response. *SP800-86*, Gaithersburg: U.S. Department of Commerce.

Manes, G.W. (2010): A Digital Forensics Primer, in Innovations and Advances in Computer Sciences and Engineering. Springer Netherlands, pp. 369-372.

Martini, B. and Choo, K.K.R (2012): An integrated conceptual digital forensic framework for cloud computing. *Digital Investigation*.

http://dx.doi.org/10.1016/j.diin.2012.07.001.

McKemmish R. (1999): What is forensics computing?. *Trends and issues in crime and criminal justice* **188**:1-6.

National Center for Missing and Exploited Children (NCMEC) (2009): *2009 annual report*. Alexandria, VA: NCMEC.

http://www.missingkids.com/en_US/publications/NC171.pdf.

Pallaras, S. (2011): New technology: opportunities and challenges for prosecutors. *Crime, Law and Social Change* **56**(1): 71-89.

Porter, G. (2011): A new theoretical framework regarding the application and reliability of photographic evidence. *International Journal of Evidence & Proof* **15**(1): 26-61.

Seek, C. (2010): Technology Crime Forensic Branch: Hitting the Hard Drives. *Home Team Journal* **2010**(2): 47-57.

Shimizu, H., Market Trends: Digital Camcorders, Worldwide, 2011-2016.

http://www.gartner.com/id=1958317.

Slay, J., Lin, Y.C., Turnbull, B., Beckett, J. and Lin, P. (2009): Towards a Formalization of Digital Forensics. *The Advances in Digital Forensics V*, IFIP Advances in Information and Communication Technology **306**:37.

Sobey, C.H., Orto, L. and Sakaguchi, G. (2006): Drive-Independent Data Recovery: The Current State-of-the-Art. *The IEEE Transactions on Magnetics* **42**(2): 188-193.

Thom, G. (2012): Camera 'fails' to identify cab killer. The Advertiser: 6 August.

United Nations Office on Drugs and Crime (UNODC) (2012). The use of the Internet for terrorist purposes. New York, US: United Nations.