Data Recovery from Proprietary Formatted Cctv Hard Disks

Aswami Ariffin, Jill Slay, Kim-Kwang Choo

Chapter 15

DATA RECOVERY FROM PROPRIETARY-FORMATTED CCTV HARD DISKS

Aswami Ariffin, Jill Slay and Kim-Kwang Choo

Abstract Digital video recorders (DVRs) for closed-circuit television (CCTV) commonly have an in-built capability to export stored video files to optical storage media. In the event that a DVR is damaged, its contents cannot be easily exported. This renders the forensically-sound recovery of proprietary-formatted video files with their timestamps from a DVR hard disk an expensive and challenging exercise. This paper presents and validates a technique that enables digital forensic practitioners to carve video files with timestamps without referring to the DVR hard disk filesystem.

Keywords: Digital CCTV forensics, video stream, data carving

1. Introduction

Video surveillance and closed-circuit television (CCTV) systems serve as deterrents to crime, and can be used to gather evidence, monitor the behavior of known offenders and reduce the fear of crime [1]. CCTV systems can be broadly categorized into analog, digital and Internet Protocol (IP) based systems. Analog systems have limited abilities to store, replicate and process large amounts of video data, and the quality of images and video files is generally quite low. Digital CCTV systems use digital cameras and hard disk storage media. IP based CCTV systems stream digital camera video using network protocols.

The primary goal of digital CCTV forensics is to ensure the reliability and admissibility of video evidence [4]. To reduce the risk of digital evidence being called into question in judicial proceedings, it is important to have a rigorous methodology and procedures for conducting digital forensic examinations. For example, in a case involving evidence obtained from a digital CCTV system, one of the first activities is to

recover video evidence from the storage media in a forensically-sound manner.

In digital CCTV forensics, it is extremely challenging to recover evidence in a forensically-sound manner without data recovery expertise in a wide range of storage media with different filesystems and video formats. The challenge is compounded if the storage media of a digital video recorder (DVR) is damaged or corrupted. The variety of digital CCTV systems further complicates the digital forensic process, as many of the systems use proprietary technologies. Therefore, digital forensic practitioners need to have an intimate understanding of digital CCTV systems.

This paper describes a forensically-sound technique for carving video files with timestamps without referring to the DVR hard disk filesystem. The technique is validated using a customized DVR with a proprietary file format.

2. Digital CCTV Forensics

The digital forensic framework of McKemmish [2] has four steps: (i) identification; (ii) preservation; (iii) analysis; and (iv) presentation. The proposed digital CCTV forensic technique shown in Figure 1, which extends McKemmish's framework, incorporates four broadly similar steps: (i) preparation; (ii) cloning; (iii) analysis; and (iv) reporting. The following sections discuss the details underlying digital CCTV forensics with respect to the steps in McKemmish's framework.

2.1 Step 1: Identification

The identification step involves a study of the device to understand what evidence is likely to be present, its location and technical specifications. For example, in cases involving a personal computer, the size of the potential evidentiary data can be huge and could include audio and video files, images, Internet browsing histories, emails and GPS data.

The first action that a digital forensic practitioner should take is to conduct a visual inspection of the exhibit to check for damage and, if possible, record the system time offset (difference between the actual time and the device time).

In cases involving a digital CCTV system, a digital forensic practitioner will need to understand its main electronic components. In a digital CCTV system, the camera captures the scene using a charge-coupled device and converts it to electrical signals. The signals are converted to digital data by the DVR using an analog-to-digital converter. The video data is then formatted in a file container with a specific video codec and

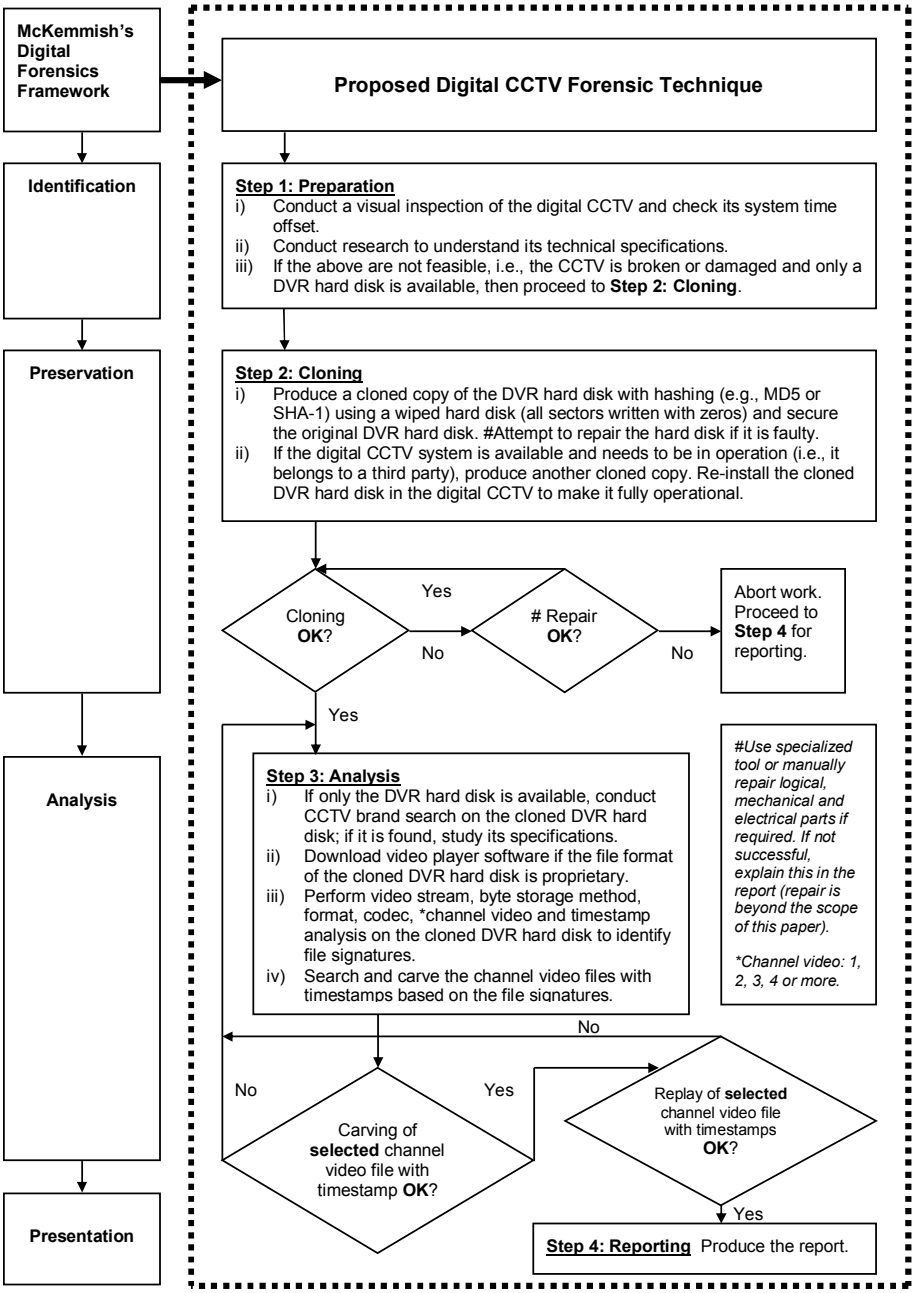

Figure 1. Proposed digital CCTV forensic technique.

other digital data such as timestamps and audio. Finally, the video file is stored on a hard disk.

During the identification step, it may be determined that additional expertise or resources are required to ensure that the forensic team has the requisite knowledge and tools to recover the data. If the digital CCTV system is damaged and it is not possible to conduct a visual inspection and record the time offset, the digital forensic practitioner may proceed to the next step.

2.2 Step 2: Preservation

The preservation step seeks to ensure that the evidentiary data remains unchanged. Given the likelihood of judicial scrutiny, it is imperative that the data be recovered using a forensically-sound method (e.g., it should not write to the original data source). In the event that the storage media is damaged or corrupted, it is necessary to repair the media before the acquisition can commence.

Next, a bit-for-bit copy of the DVR hard disk is created. This copy (image) is hashed and the hash value is retained to prove that it is a duplicate copy of the original media.

A cloned copy of the DVR hard disk may have to be produced if the system belongs to a third party or if the system must remain operational. A digital CCTV system may not belong to the suspect and seizing the system is usually a last resort. Cloning rather than imaging the DVR hard disk is the preferred approach because an imaged hard disk cannot be replayed or made to record video like a cloned copy.

A live cloned copy must also be created if the DVR system has RAID storage. Duplicating the media simplifies the analysis task, eliminating the need for specialized tools and knowledge about the RAID configuration.

2.3 Step 3: Analysis

The third step is to analyze the cloned hard disk, examining the video stream, byte storage method, format, codec, channel and timestamp to identify the file signatures for searching and carving the video files with timestamps. The timestamps of the video files can be obtained from the filesystem using standard recovery procedures. The proposed technique accounts for the possibility that the filesystem is unrecognized by the standard recovery tools and is able to recover the timestamps.

A key challenge to recovering video files with timestamps from a DVR hard disk with a proprietary file format is to analyze the video stream for its internal attributes without the assistance of technical documentation.

However, video file formats have a header and occasionally a footer that provide file metadata, including the format of the video stream. Using this information, a digital forensic practitioner can select the appropriate player and video codec to replay the video files with timestamps. Therefore, we suggest building a database of known file signatures that can be used by a digital CCTV forensic software suite.

For a DVR hard disk that uses a proprietary file format, there are some technical issues that need special attention. First, it is necessary to determine if the byte storage method is little endian or big endian. After the byte storage method has been determined, the file signatures can be derived and this information can be used to correlate each file signature to the channel video that captured the scenes with timestamps.

If the video codec is also proprietary, a proprietary software player must be downloaded from the manufacturer's website. If a player is not available, further research must be conducted on the codec because the carved video files with timestamps cannot be replayed using a standard video player and codec.

2.4 Step 4: Reporting

The fourth step is to ensure that the findings are presented in a manner that is understandable to investigators, prosecutors, members of the judiciary, and other decision makers. When a number of parties are involved in evidence recovery, it is critical that the chain of custody be logged, along with details about the individuals who repaired the device and/or extracted data, and any changes that were made as part of these procedures.

3. Application of the Forensic Process

Table 1 lists the tools and software used in the forensic analysis. Although the CCTV brand was known to be RapidOS, the following use case discusses how brand information can be determined.

3.1 Identification

The first step is to check the DVR time setting and determine the offset from the actual time. The time offset is beneficial for verification against the actual time of the incident. In this particular example, we proceed to the second step (Preservation) given there are no constraints that the device must remain in operation.

Table 1. Tools and software.

Number	Item
1	EnCase 6.7 and FTK 3.0, widely-used commercial digital forensic tools.
2	WinHex 14.5, hexadecimal editor tool commonly used for data recovery and digital forensics.
3	RapidOS T3000-4 Viewer software, proprietary video, audio and timestamp player.
4	MacBook Pro laptop with Windows XP virtual system.
5	500 GB DVR hard disk used in a RapidOS digital CCTV system with a unit of the same size hard disk for cloning purposes (sectors were wiped with zeros).
6	Tableau Forensic Bridge T35es-R2, used to prevent writing on the source hard disk during cloning.
7	DCode v.4.02a, used for Unix 32-bit hexadecimal time conversion.

3.2 Preservation

For preservation purposes, the DVR hard disk was cloned and its hash value was computed using WinHex 14.5. The size of the cloned hard disk was 500 GB and the time taken to create the image was about 27 hours. In a real-world situation, two clones are required – one for forensic analysis and the other for re-installation into the digital CCTV system for continuous operation. The original hard disk is then retained in an evidence preservation facility for future reference.

The MD5 hashing process took approximately nine hours. The image was then verified as accurate.

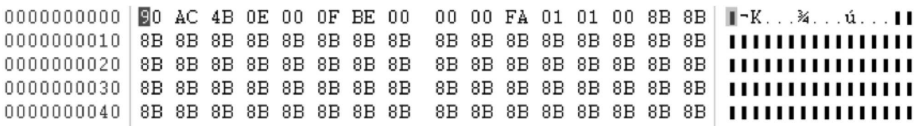

Figure 2. Proprietary file format.

3.3 Analysis

EnCase 6.7 and FTK 3.0 were used to check if the filesystem was readable. Both tools were unable to recognize the filesystem and the video files. Further analysis used WinHex 14.5 to perform byte-level analysis. As shown at offset `0` in Figure 2, the file format was unknown and, therefore, proprietary. Unlike Poole, *et al.* [3], we did not conduct further forensic analysis of the filesystem of the cloned DVR hard disk

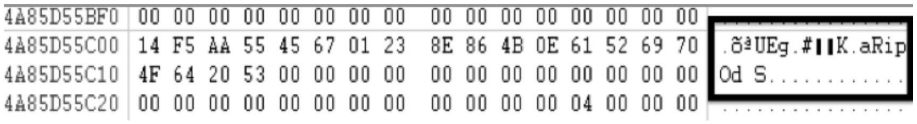

Figure 3. Confirmation of CCTV brand and byte storage method.

because it would have been time consuming. In any case, this was impractical because we did not have access to a complete digital CCTV system.

Next, each sector (512 bytes) of the disk was analyzed to determine the CCTV brand. We found the text string "aRipOd S" at offset `4A85D55C00`, which identified the digital CCTV system brand as RapidOS. The text arrangement was not directly matched because of its byte storage method. The RapidOS system stores data in a reverse 16-bit byte little endian format (Figure 3). This finding was useful for further forensic analysis of the unknown content format.

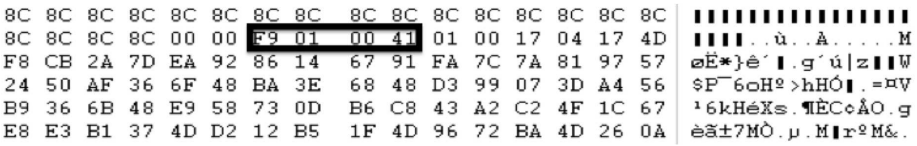

Figure 4. Example of channel video file signature.

Analysis then focused on recognizable file signatures. For this type of CCTV, it involved required searching for repetitive hexadecimal patterns in the channel video (from one to the number of channels) interleaved with timestamp tracks:

- \0xF9\0x01\0x00\0x40\
- \0xF9\0x01\0x00\0x41\ (Example shown in Figure 4.)
- \0xF9\0x01\0x00\0x42\
- \0xF9\0x01\0x00\0x43\
- \0xFA\0x01\0x01\0x00\
- \0xF0\0x7E\0x4B\0x0B\ (According to our findings, the first two bytes change frequently in successive tracks.)

Based on the repetitive hexadecimal pattern, the T3000-4 Viewer software and manual was downloaded to gain additional technical information about the digital CCTV system. Because of the proprietary

nature of the video format, the technical specification did not provide enough details to develop tools for further analysis. Additionally, only the T3000-4 Viewer software played the VVF file format found on the drive. Overall, 50 GB of data for all four channels of CCTV videos with timestamps were extracted from the drive image. Viewing the video confirmed that the cloned DVR hard disk was a four-channel digital CCTV system and allowed for further analysis of the repetitive interleaving hexadecimal signatures. After performing the analysis, the video and timestamp file signatures were interpreted as follows:

- \0x01\0xF9\0x40\0x00\ → Channel 1 video header file signature
- \0x01\0xF9\0x41\0x00\ → Channel 2 video header file signature
- \0x01\0xF9\0x42\0x00\ → Channel 3 video header file signature
- \0x01\0xF9\0x43\0x00\ → Channel 4 video header file signature
- \0x01\0xFA\0x00\0x01\ → Footer file signature
- \0x7E\0xF0\0x0B\0x4B\ → Unix 32-bit hexadecimal timestamp (little endian)

Further forensic analysis was performed on the cloned hard disk content to demonstrate that the proposed technique was capable of searching and carving on selected channel video and timestamps. This can considerably shorten the time required for a forensic examination of a digital CCTV system. The selected channel video and timestamp details were:

- Channel 1 video header file signature → \0x01\0xF9\0x40\0x00\
- Footer file signature → \0x01\0xFA\0x00\0x01\
- Timestamp: 24th November 2009 at 14:41:01 → \0x7D\0xF0\0x0B\0x4B\

We converted the timestamp to Unix 32-bit hexadecimal using DCode v.4.02a in order to search the cloned DVR hard disk.

The Channel 1 video header, footer (file signatures) and Unix 32-bit hexadecimal timestamp were converted to the RapidOS 16-bit byte little endian format:

- \0xF9\0x01\0x00\0x40\ → Channel 1 video header file signature
- \0xFA\0x01\0x01\0x00\ → Footer file signature

Figure 5. Sample channel video file image with timestamp.

- \0xF0\0x7D\0x4B\0x0B\ → Timestamp of November 24, 2009 at 14:41:01

WinHex 14.5 was then used to search and carve out the digital video evidence according to the channel (video header and footer) and timestamp signatures. The channel video file with timestamp was 16-bit byte swapped and converted into VVF file format for replay using the T3000-4 Viewer (Figure 5). Note that some of the video has been intentionally darkened to mask the identities of the individuals.

3.4 Reporting

For the findings of the forensic analysis to be meaningful, they must be reported in a manner that complies with the local court requirements. The report may be verbal or written and should include information on all procedures, tools and software used along with their limitations to prevent false conclusions from being reached.

4. Forensic Analysis of a Customized DVR

A forensic analysis of an AVTECH digital CCTV KPD674 4-Channel DVR customized with a database was conducted as an additional test to provide support for the proposed technique. The AVTECH DVR recordings were made for five days over three months. The database consisted of several records, primarily an image identity number, offset and Unix timestamp records. SQLite Database Browser 2.0b1 and MPlayer 06.9+SVN-r3607 were used as additional software during our analysis.

The DVR file system was intentionally corrupted to demonstrate that video files with timestamps were recoverable. Recovery involved searching for the database file signature: \0x53\0x51\0x4C\0x69\0x74\0x65\0x20\0x66\0x6F\0x72\0x6D\0x61\0x74\0x20\0x33\0x00\ and subsequently extracting the SQLite database file. Concurrently, adjacent raw hexadecimal video streams were analyzed to identify the video codec and then extracted. The video codec was identified as H.264 from the hexadecimal file signature of \0x32\0x36\0x34\. Other video specifica-

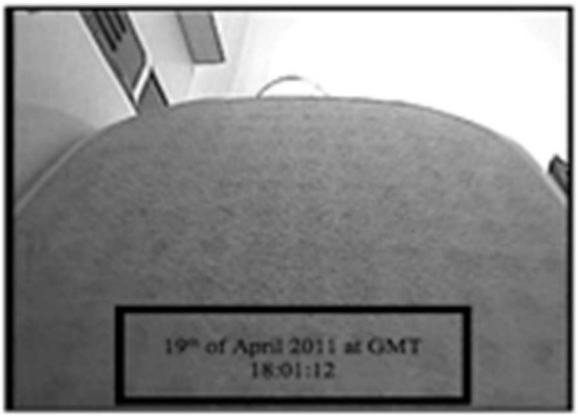

Figure 6. Customized AVTECH DVR video snapshot using MPlayer.

tions such as resolution, aspect ratio and frames per second can also be obtained from the video header data.

MPlayer 06.9+SVN-r3607 was able to replay the H.264 video files. The timestamp was obtained from the database using SQLite Database Browser 2.0b1. Figure 6 shows a snapshot taken from the AVTECH DVR video stream. The timestamp from the database was April 19, 2011 at GMT 18:01:12.

5. Conclusions

The digital CCTV forensic technique presented in this paper enables video files with timestamps to be carved without referring to the filesystem. The technique is designed to be independent of the brand, model, media and filesystem. Moreover, it does not require interaction with the vendor or manufacturer.

Our future work will focus on developing a digital CCTV forensic software suite. A video-carving tool will be included in the software suite. The tool will be intuitive and easy to use. It will help create forensic copies and reference lists for various video headers and footers (file signatures), and will search for and carve video files with timestamps with minimal human intervention.

References

[1] K. Choo, Harnessing information and communications technologies in community policing, in *Community Policing in Australia*, J. Putt (Ed.), Australian Institute of Criminology, Canberra, Australia, pp. 67–75, 2010.

[2] R. McKemmish, What is forensic computing? *Trends and Issues in Crime and Criminal Justice*, no. 118, 1999.

[3] N. Poole, Q. Zhou and P. Abatis, Analysis of CCTV digital video recorder hard disk storage system, *Digital Investigation*, vol. 5(3-4), pp. 85–92, 2009.

[4] G. Porter, A new theoretical framework regarding the application and reliability of photographic evidence, *International Journal of Evidence and Proof*, vol. 15(1), pp. 26–61, 2011.