SHS Web of Conferences **14**, 02010 (2015)
DOI: 10.1051/shsconf/20151402010

Basic Principle and Application of Video Recovery Software for "Dahua" and "Hikvision" Brand

Fan Yang[1,2], Rongrong Li[1,2] and Chunsheng Wu[1,2,a]

[1]Key Laboratory of Evidence Science (China University of Political Science and Law), Ministry of Education, 100088 Beijing, China
[2]General Division of Criminal Investigation, Beijing Public Security Bureau, 100054 Beijing, China

Abstract. This article describes the basic principle of mainstream video recovery software in "Dahua" and "Hikvision" brand for the current market, and introduces a practical method to use this software to abstract the digital video, especially the detailed description of application experience of carrying out video abstraction for hard disk with part of damaged sector, and finally make a summary.

Keywords. digital video; file head; data abstraction; sector export; WinHex

1 Introduction of video recovery software

With the wide application of video surveillance, the supporting effect of surveillance video for case solution is increasingly obvious. The inspection and appraisal demand of primary sectors on the surveillance video is gradually increased. In the inspection and appraisal of digital evidence, the recovery and access of digital video are increasingly related. All of the current video surveillance systems use the video surveillance as the basic framework. DVR is also called the Digital Video Recorder, and commonly called as video recorder. As all of the videos are digitally stored in the video recorder, the video recorder is not only the core of video surveillance system, and also the object of digital evidence inspection. The corresponding digital video products are various, with different storage structure and encoding method of video flow, which bring a lot of difficulties for abstraction and playing of video. Currently, there's no inspection device for video. As most of the storage of digital video use the cycling overwriting method, the video will not be maintained for a long time, and the video file with longer history will be more likely to be overwritten. Once the video file is deleted, overwritten, it is hard to be recovered by current device and technology. Even if a part of data can be recovered, the video cannot almost be recovered due to special structure of video file and incomplete file information. So it is very hard to successfully recover the video file, and even harder to recover the (part of) the video file, and even harder to recover the (part of) overwritten video file, which is right the technical problem in urgent need to be solved for current recovery and evidence taking of digital video.

To solve the above technical problem, in February of 2012, our unit set up a project and undertook the concentrated research planning project Research on Recovery Technology of Video. Through recent two years of research, the project had been accepted in 2013. One of the important results of this project "video recovery software" realizes the recovery abstraction for currently domestic mainstream video recorder of "Dahua" and "Hikvision" brand, which solved the actual problem of complex steps and excessive workload to carry out artificial inspection for this work, and obtained a desirable actual application effect.

2 Basic principle of video recovery software

Traditional file systems, such as Microsoft FAT, NTFS and EXT2 file system of Linux, use multilevel index to create and retrieve the files. They have the problems of inability to support the oversize storage file capacity and significant reduce of performance and stability of file system due to fragments from repeated file creation, deletion. In the actual work, the surveillance video system will constantly read and write the hard disk and video file for a long time, which is required to be retrieved according to camera code, video time, alarm time and other searching conditions. So the professional surveillance manufacturer generally will use "pre-format" and fast read and write method to cross the traditional file

[a] Corresponding author: wucs@sccas.cn

system to form a sole file system with video surveillance system feathers in file searching, large-capacity file storage and file division. Professional surveillance manufacturer, when using the video hard disk, will use its own format tool to pre-partition the hard disk, and the a continuous series of sector will be considered as a complete video partition according to the preset size of partition. By recording the relevant information of "partition" in the main sector of hard disk, such as surveillance camera index, creation time corresponding to this video partition and relative deviation address of key frame of video flow in this partition, we can simply read the relevant information in the main sector in the retrieval process to obtain the relevant video file position by the information in the index form, and carry out the recovery. Due to majority of surveillance device manufacturer at home and aboard, and the difference of the key information organization method of video file system, we realize the understanding of the storage method of these two video surveillance by analysis on the file partition index method and features of video file frame in domestic mainstream manufacturer and repeated verification of devices in these two mainstream brands Dahua and Hikvision.

The video file systems of Dahua and Hikvision brand use the pre-format method for video storage. By pre-format the empty hard disk, a large amount of index content may be found in the main sector, including: file path, section deviation, start time, end time, server ID, etc.. By analysis on the difference of large amount of partition storage file system in the hard disk, we could obtain the featured code with regularity, such as surveillance video information and time information, by which we can abstract the real video file from the data area stored in the hard disk.

The video file of Dahua and Hikvision generally uses the MP4 or standard H264 encapsulation format for storage. The abstraction of original data flow in the disk is the operation for the physical disk drive. By obtaining the handle of physical disk drive, the basic information of disk can be obtained (such as: cylinder number of disk, magnetic track number of each cylinder, sector number of each magnetic track and byte number of each sector). To reduce the time complexity, one cylinder of disk will be read each time. In case of failure to read the data by the current cylinder, it will be transited to the next cylinder position and continue to recover the data. Most of the data flow of Dahua bears ES stream of Dahua private data (Elementary Stream, also called basic code stream, a kind of continuous code stream that contains video, audio or data). Each frame data starts with 44 48 41 56 FC, and ends with 64 68 61 76, as shown in Figure 1, 2:

```
00000000h: 44 48 41 56 FC 00 00 00 9F 2E 58 00 09 10 00 00 ;
00000010h: 50 23 75 36 43 34 08 FA 88 FE 36 9E 10 00 00 00 ;
00000020h: 00 00 00 01 61 EE 02 B1 42 82 51 18 EE 79 93 B0 ;
00000030h: 98 3D 83 F9 EB A0 BF E7 AE DF FC F8 99 74 0F B0 ;
00000040h: BC FA EC 21 50 B6 17 CF AF 15 0B FC F5 CE 5C 58 ;
00000050h: 5E B9 EB 8B 08 58 5D 85 E7 AE 81 FF CF 5D 05 D0 ;
```

Figure 1. Start key words of Dahua.

```
00001000h: C9 64 68 61 76 09 10 00 00 44 48 41 56 FC 00 00 ;
00001010h: 00 A0 2E 58 00 53 2C 00 00 50 23 75 36 6B 34 08 ;
00001020h: 89 88 B5 FF BB 42 00 00 00 00 00 00 01 61 F0 03 ;
00001030h: 31 42 88 BA DB 8A 97 6A 4F 61 58 4B 33 D7 BB C9 ;
00001040h: 4B A4 BD 46 ED EB 4F 5C C2 30 11 FE 1A 13 60 FF ;
```

Figure 2. End key words of Dahua.

After abstracting the original data from the hard disk, we shall first retrieve the key words 44 48 41 56 FC. After successful retrieval, we shall mark a start for one frame data and start to analyze. Firstly, we shall analyze the passage, time stamp and other information in the data head, and then discard the private Dahua data head to abstract the H.264 data. In case of 64 68 61 76, it indicates that this frame data is finished, and it may be simply saved.

Similarly, most of Hikvision data carries PS stream with Hikvision private data. Each frame data of Hikvision with PS stream starts with 00 00 01 BA, while each PS package may contain multiple PES (Packet Elementary Stream, named packaged basic code packet). PES packet starts with 00 00 01 E0. After abstracting the original data from the hard disk, we shall first retrieve the key words00 00 01 BA. After successful retrieval, we shall mark a start for one frame data and start to analyze multiple PES packets in each PS packet to be reconstructed as a complete frame. Finally, we just simply save it.

Timing diagram of storage module of video data for these two brands is as shown in Figure 3:

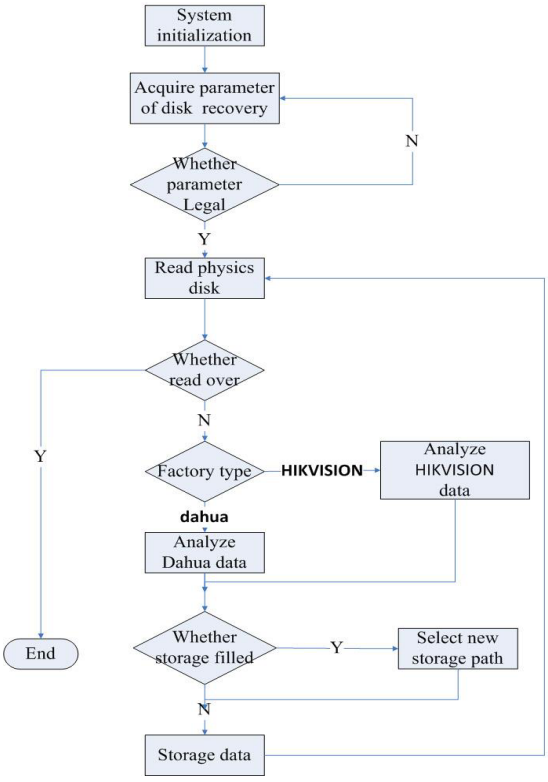

Figure 3. Timing diagram of storage module.

3 Application of video recovery software

The video recovery software independently developed by our unit was successfully accepted and put into practical inspection. This software is installed and operated in the environment of Windows series operation system By August 2014, I have used this software to inspect 12 relevant cases, involving over 20 hard disks with storage capacity over 10 TB. In the routine inspection, we shall simply finish it in accordance with the operation steps, which will not be further clarified herein. Now, I will

introduce the review of inspection work for a hard disk with a damaged sector in a certain case.

The inspection material in this case is one Dahua embedded DVR with one built-in Seagate hard disk with capacity of 2000G and an interface of SATA. Connect the hard disk to copier for copying. The copying progress is just 1% after 4 hours of operation due to many damaged sectors in this hard disk. Then we exited the system for re-copy, changing copier to re-copy and other methods, but failed to finish the copying due to a large amount of damaged sectors. Connect the inspection material hard disk to the inspection and analysis computer through a read-only interface, start the video recovery software, select this physical hard disk letter, and the software will implement the parameters. Click the "Start saving" according to default set Dahua content, and the software will start reading the hard disk data and carry out the transfer. In case of damaged sector after saving several video files, it is required to be skipped by artificial selection. After multiple skipping confirmations, the system will fail to skip for a long time, and the video recovery abstraction will not be successfully implemented due to damaged sector. Until now, the inspection is in difficulty. So could we use some auxiliary means to better utilize the video recovery software to abstract the video in this hard disk and seek valuable clues for the case? The answer is positive! Of course, it also requires assistance of two kinds of tool software we often use in digital evidence inspection work: Hard disk clone and virtual mirror image. There are many brands and versions for these two kinds of software. What we used in this case are respectively WinHex 15.8 and Mount Image Pro v3.26。

Firstly, we use hard disk clone function of WinHex software to copy the data sector from the source disk to mirror image file. In this process, the "wish to ignore the bad partition" shall be checked, and the ignored data shall be written in with "UNREADABLESECTOR" mark. This clone copy function is flexible and convenient, and we may select to copy all the sectors completely, or copy a certain amount of data by setting the number of starting sectors and copied sectors. Due to large capacity of source disk (2TB), we use multiple copies method to generate multiple mirror image file and carry out video recovery for each mirror image file. Use WinHex software to open a certain mirror image file that we generated, and we may see that the data file in the hard disk has been copied to the mirror image file, as shown in Figure 4:

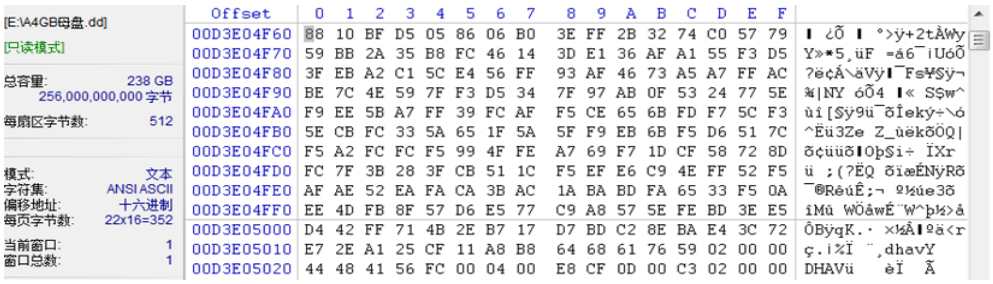

Figure 4. Hexadecimal data of mirror image file.

Continue to browse the hexadecimal data below, and find that the data in bad sector has been filled with "UNREADABLESECTOR". Then, we may carry out video abstraction for mirror image file. Firstly, we shall virtualize the mirror image file as logic disk by Mount Image Pro software, as shown in Figure 5, and virtualize the mirror image file "A4GB mother disk 3. dd" to logic disk "I:" :

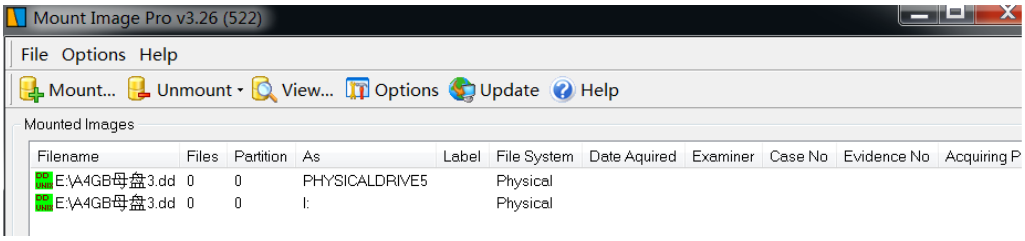

Figure 5. Load the mirror image file.

Thereafter, we may carry out video recovery abstraction for this logic disk according to general operation method of video recovery software, as shown in Figure 6 below:

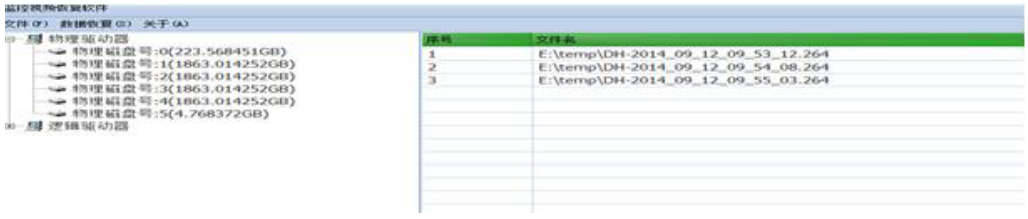

Figure 6. Use video recovery software to carry out video abstraction.

After successful generation of video file, the rest work is to play the generated video file and seek the content that we care.

4 Conclusion

In summary, the key of recovery and abstraction of surveillance video in the hard disk is to obtain the data storage specification from different manufacturers, but the fact is that each manufacturer will not provide the relevant information often due to technical confidentiality or other similar reasons. So it requires us to make research and analysis on a large amount of examples, and obtain this kind of information by experiment. The analysis on the data of Dahua and Hikvision brands is our first step to solve the recovery and abstraction of digital video. In this kind of inspection work, there are still many important contents required to be deeply researched and discussed, for example, the retrieval and fast positioning of video according to time section and the data storage format of video recorder in other brands. I hope that our research fruits will provide a certain reference for research and solution of relevant problems.

Acknowledgement

Supported by the Opening Project of Key Laboratory of Evidence Science (China University of Political Science and Law), Ministry of Education.(2012KFKH03).

References

1. Yao Bo, Jia Yongsheng & Song Run. Underlying recovery of digital video by application of key words searching method [J]. *Criminal Technology*, 2012, 5.
2. Lv Jinna, Zhou Bing & Zhang Zhijun. Universal storage and retrieval plan for embedded digital video surveillance system [J]. *Computer Engineering and Design*, 2009, 21.
3. Zhang Chaowei & Zhou Bing. Design and realization based on H.264 embedded video surveillance [J]. *Application of Micro Computer*, 2009, 8.
4. Zhang Li, Xu Lihong & Xu Shenglin. Design and realization of digital video recorder based on embedded Linux [J]. *Application of Micro Computer*, 2005, 6.
5. Huang Deyi. Application of hard dis storage technology in video surveillance [J]. *Chinese Security and Protection*, 2009, 5.
6. Yao Bo, Han Jie, Jia Yongsheng & Song Run. Ideology of taking evidence from digital video [J]. *Criminal Technology*, 2010, 2.