Video Data Recovery for A CCTV System by Reverse Engineering

Sai-Chung Law

Abstract— **This paper explains how the detailed data analysis approach of reverse engineering the file system of a commercial Digital Video Recorder (DVR) was performed, without prior CCTV hardware and software, or part of data corrupted. Then a more pragmatic approach of reverse engineering the system, by eavesdropping the data structures of files while running the application software could be employed, to achieve useful outcomes in a more efficient way.**

Keywords: Video, Internet of Things (IoT), CCTV Forensics, Reverse Engineering, Big Data

I. INTRODUCTION

The aim of this work is to show how best use of reverse engineering a CCTV system [1] in two approaches. Approach 1 is by performing detailed analysis of its file system and then extracting video data, without use of manufacturer's application software, and directly playing the video sequences in a standard PC computer. Approach 2 is by using the related CCTV software to perform a task on the data being investigated while the disk I/O is monitored, so that the operation of the CCTV system can be understood in a limited amount of time, without losing forensic rigour [2].

II. METHODS & RESULTS

A typical 4-Channel DVR (AVC760 of AVTECH) with 500GB hard disk storage and network interface was selected as the subject for the investigation, because of its general usage among retail establishments and small offices nowadays.

After studying the specification of the target DVR, and removing the hard disk from the system, the sectors of hard disk were initialized to all zeros. Then the drive was re-installed to the DVR, with video recording under documented conditions for a considerable time span (24h, say). It is beneficial to have just small enough data on the disk in the initial analysis. At the end of the test period, the hard disk was again removed from the system. It was imaged on a forensic workstation. The 500GB image so created was subsequently archived and analyzed in detail by a low-level disk analyzer called WinHex [3]. Deatils on the data structures in different sectors of the memory map of the hard disk were then obtained.

By tracing the respective pointers from master sectors, to entry list sectors, index sectors and finally up to the video data sectors, the recorded video could be located by using WinHex. By direct comparison of extracted video data file and the video recorded, the packaging difference of video data for frame and CIF modes was identified. The format of video data was essentially MPEG4, for the first three bytes of start codes of video data are consistent to that of standard MPEG4 video.

With minor additional processing on the data, the stored video could then be rendered with a standard media player, say, VLC media player. An example CIF video display format for a particular event chosen is shown in Fig. 1.

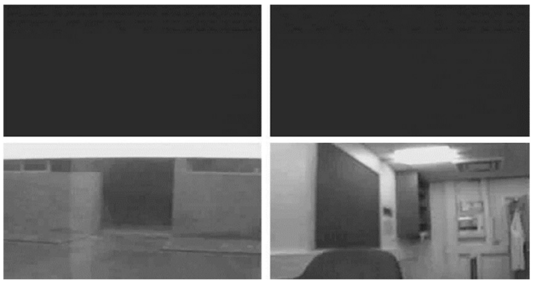

Figure 1. Extracted CIF video rendered with VLC media player [4]

To save time while achieving useful outcome, a more pragmatic approach was adopted. Validation of the results can be done by comparing the entries in the report generated from the reverse engineering process on the disk layout, with the entries from the proprietary software which is necessary.

An application program such as DiskAccess (written in C#) for Windows operating environment was chosen to use for this rather straightforward analysis. The information provided by the reverse engineering process was found to substantially match that obtained from the proprietary software.

In the Internet-of-Things (IoT) and Big Data era, CCTV forensics present challenges and approaches which are very different from traditional CCTV forensics as described above [5]. Further work will include research study in this area.

III. CONCLUSION

By reverse engineering the CCTV system for video data recovery, both approaches are useful. However, the pragmatic approach can extract information quicker than the detailed approach, while maintaining forensic regour and accuracy.

REFERENCES

[1] V. Damjanovski, *CCTV: From Light to Pixels*, 3rd ed. B.H., 2014.

[2] R. Mckemmish, "What is forensic computing?", available from official website of U.S. Department of Justice [accessed 19.8.2023].

[3] X-ways Software Technology AG, WinHex: computer forensics and data recovery software, available from https://www.x-ways.net/winhex/index-m.html; 2023 [accessed 19.8.2023]

[4] L. Tobin, A. Shosha, and P. Gladyshev, "Reverse engineering a CCTV system, a case study", Digital Investigation (D.I.), vol. 11, no. 3, 2014, p.179-p.186.

[5] E. Dragonas, C. Lambrinoudakis,, and M. Kotsis, "IoT Forensics: Analysis of HIKVISION's Mobile App", D.I., vol. 45, 2023.

S. C. Law was with Hong Kong Polytechnic University as a postgraduate student, and is now a veteran electronics and information engineer with Hong Kong government (Corresponding Author Email: s.c.law@connect.polyu.hk)