IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 21, Issue 4, Ser. II (Jul - Aug 2019), PP 01-07
www.iosrjournals.org

Data Recovery from Hard Disk Independent of Digital Video Recorder

Kananbala Jena
(Scientist, Central Forensic Science Laboratory Kolkata, India)

Abstract: *Digital video recorder (DVR) being popular options for home and organisation security, seizure of DVR in different types of crime scene is increasing constantly. Though the resident operating system of the DVR and the embedded file recovery system can be used for retrieval of footage, difficulty arises due to unavailability and inaccessibility of DVR. In this situation recovery of footage from a DVR hard disk is only available option. But, in majority cases standard data recovery software used for forensic examination/ data recovery of hard disks used in computer and desktop do not show files of DVR hard disk. Though, footages can be carved from raw disk, identification of proprietary file systems requires considerable time and effort.Forensic examination being time bound always benefits from ready tools which do not demand much intervention of examiner. This paper will discuss trial using different tools to recover footage from hard disk of DVR on a window-based computer without much intervention. The recovery output also included files other than video footage thus expanding scope of investigation.The toolsfocused to recovery of only CCTV footage from hard disk deny examiners a view into other type of files. This method can avoid shortcomings in examination of CCTV based evidence oriented to only video footages.*

Keywords: *Closed Circuit television, Digital Video Recorder, Operating System, File System, Hex Editor, DMDE software, Disk Genius software, Encase software, VLC Player, HxD software, Hex Editor.*

Date of Submission: 13-07-2019 Date of acceptance: 29-07-2019

I. Introduction

Digital Video Recorder (DVR) typically contains one circuit board with software burned into the chip. Unlike operating systems of computers with industry standard operating systems installed on the hard disk, the menu and logs of DVR can be accessed in absence of hard disk. It is easy to retrieve footages stored in the hard disk through menu displayed by DVR once it is switched on. Password protection, intentional/ unintentional damage or other circumstances demand deployment of special methods to recover data from DVR hard disk independently.Footage recovered through embedded software of DVR automatically have unique filenames often containing channel name date and time in filename system for ready reference. But standard forensic software do not show any file when bit stream image or clone of the hard disk is mounted. The bit stream image is shown as only unallocated cluster. Carving functions available within the standard forensic software also do not help much. Carving of files from raw disks manually is last option keeping in view long time and tremendous trial and error efforts to understand proprietary file system in a hard disk of capacity between 1TB to 4TB normally found inside DVR. Increasing capacity of DVR hard disk and multiple hard disks within single DVR can make the scenario much more difficult when aim is to deliver within stipulated time and backlogs are also increasing.

The tools, which can search through the disk automatically and recover required data are more practical solution for forensic application. This paper will discuss trials with software namely 'DMDE', 'DISKGENIUS', 'ENCASE' and their applicability to forensic examination of DVR hard disk. During these trials' images, emails, excel files, word files, pdf files has been recovered which is not possible to recover using either backup function of DVR or any tools aimed at only recovery of video footages. Therefore, automatic recovery of added files is a bonusover the current system of CCTV based evidence examination and further study may allow more insight to the problem at hand. This paper has also described details of video footage files recovered by opening these files through HXD hex editor which can be used to reverse engineer recovery of files.

II. Method

2.1 **Tools used**

DMDE, DISKGENIUS, ENCASE 8, VLC PLAYER, HxD Hex Editor

2.2 **Recovery using DMDE software:**

2.2.1 Method:DMDE software is a tool to search, edit, and recover data on disk. Free version of this software DMDE 3.4.4 for windows 64 bit was downloaded from website 'https://dmde.com/download.html' and installed

on workstation with operating system 'WINDOWS 10'.Clone of the DVR hard disk was connected to the workstation and mounted for scanning. The software could not show any partitions. Full scan of the hard disk was selected with option to scan RAW disk. The method was repeated for the hard disks recovered from DVR make DAHUA, HIKIVISION and OPTICOP.

2.2.2. Results:

Scanning recovered different type of files and categorized them under the heading volume. Files of the type jpeg-B and exe-WIN were commonly recovered from hard disks sourcing from all brands. jpeg-B type of files was copied to another location. Some of these files could be played through vlc player configured to play h264 files. These are found to be footages of DVR. Some footages consist of footages of same camera for 02 consecutive dates. Some footages also found to be a mix of different camera footage for same date. Size of files was not constant. The files recovered has size from 569MB to 7GB. Header and footer of the jpeg-B files found to be uniform as 'ff d8 ff' and 'ff d9' respectively irrespective of brand. However, 'exe' extension files could not be executed.

Data recovery output from one of the hard disks contained images, PowerPoint, Excel files, pdf files which could be opened normally in windows 10 computer. These files contained financial data, credit card reports and images relevant to the accused under investigation. The name of the accused and address in credit card statement as well as excel files were consistent with case history. Another hard disk output contained more than 4000 screenshot files with jpg extension of CCTV footage which was consistent with recovered CCTV footages.

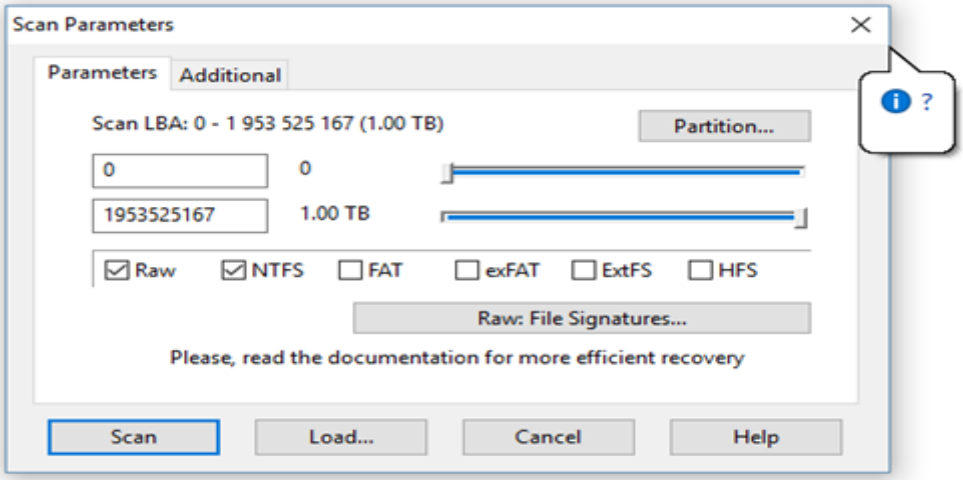

Figure 1 DMDE SOFTWARE SCAN OPTIONS

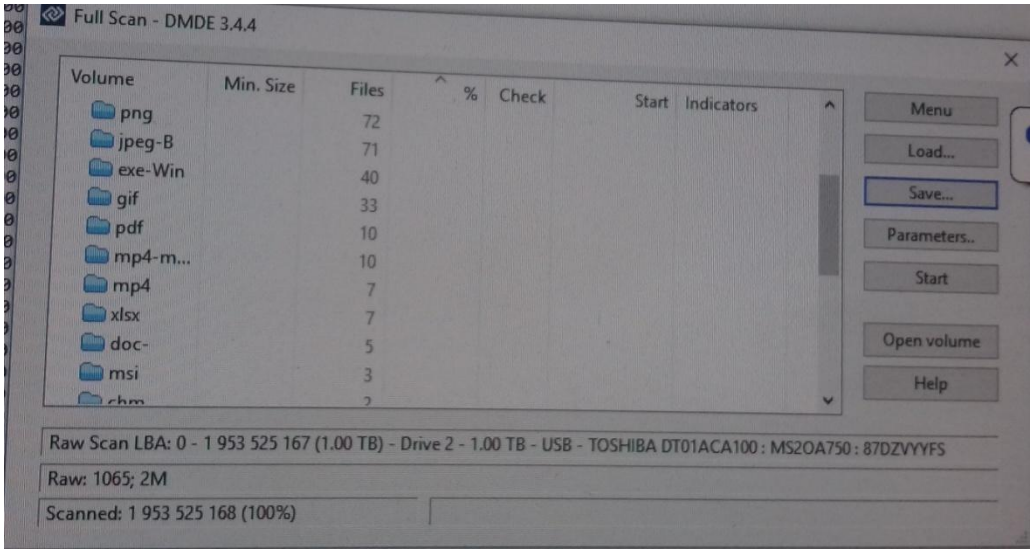

Figure 2 DMDE SCANNING RESULTS

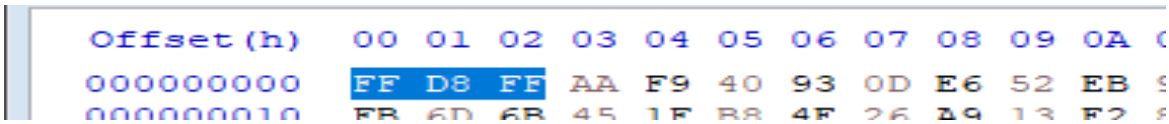

Figure 3 HEADER OF FILES RECOVERED THROUGH DMDE

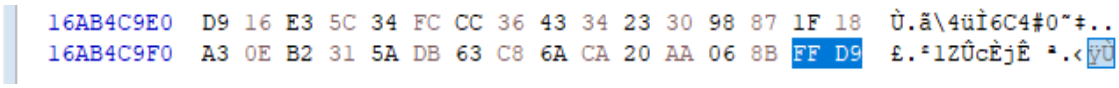

Figure 4 FOOOTER OF FILES RECOVERED THROUGH DMDE

2.3 **Recovery using DISK GENIUS software**

2.3.1 Method:

Disk Genius is software for partition management, back up, restore and recover data on disk**.** Free version of this software could be downloaded from websitehttps://www.diskgenius.com/and installed on workstation with operating system 'WINDOWS 10'. Clone of the DVR hard disk was connected to the workstation and mounted for scanning. The software could not show any partitions. However, recovery option was given and scanning was done. Clone of the hard disk was mounted and raw disk was scanned. The method was repeated for the hard disks recovered from make CPPLUS and DAHUA.

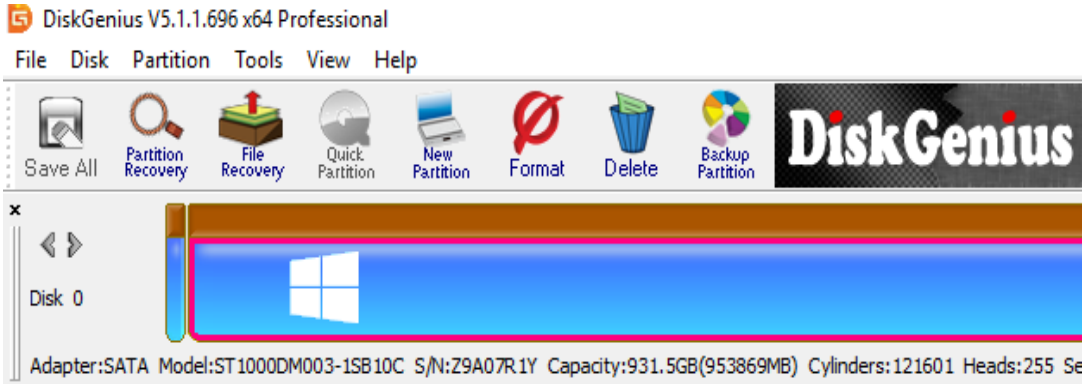

Figure 5 DISKGENIUS

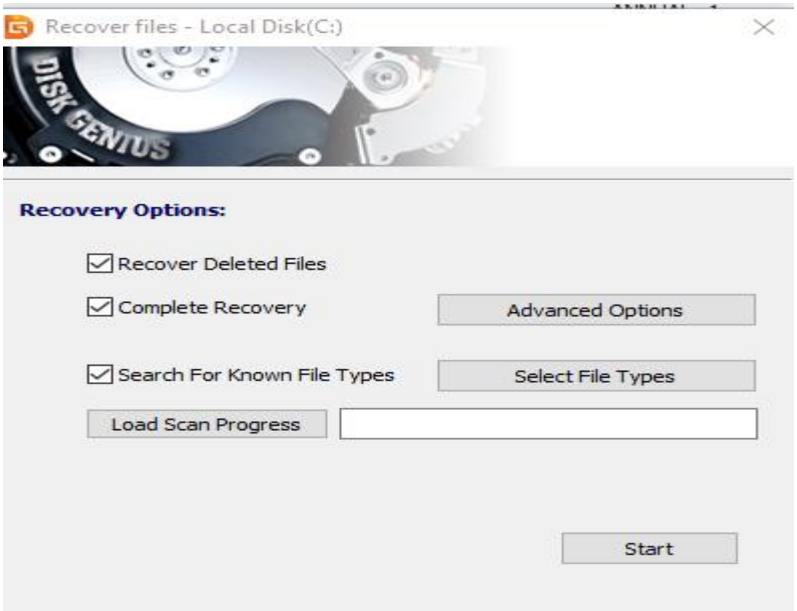

Figure 6 DISKGENIUS RECOVERY OPTION

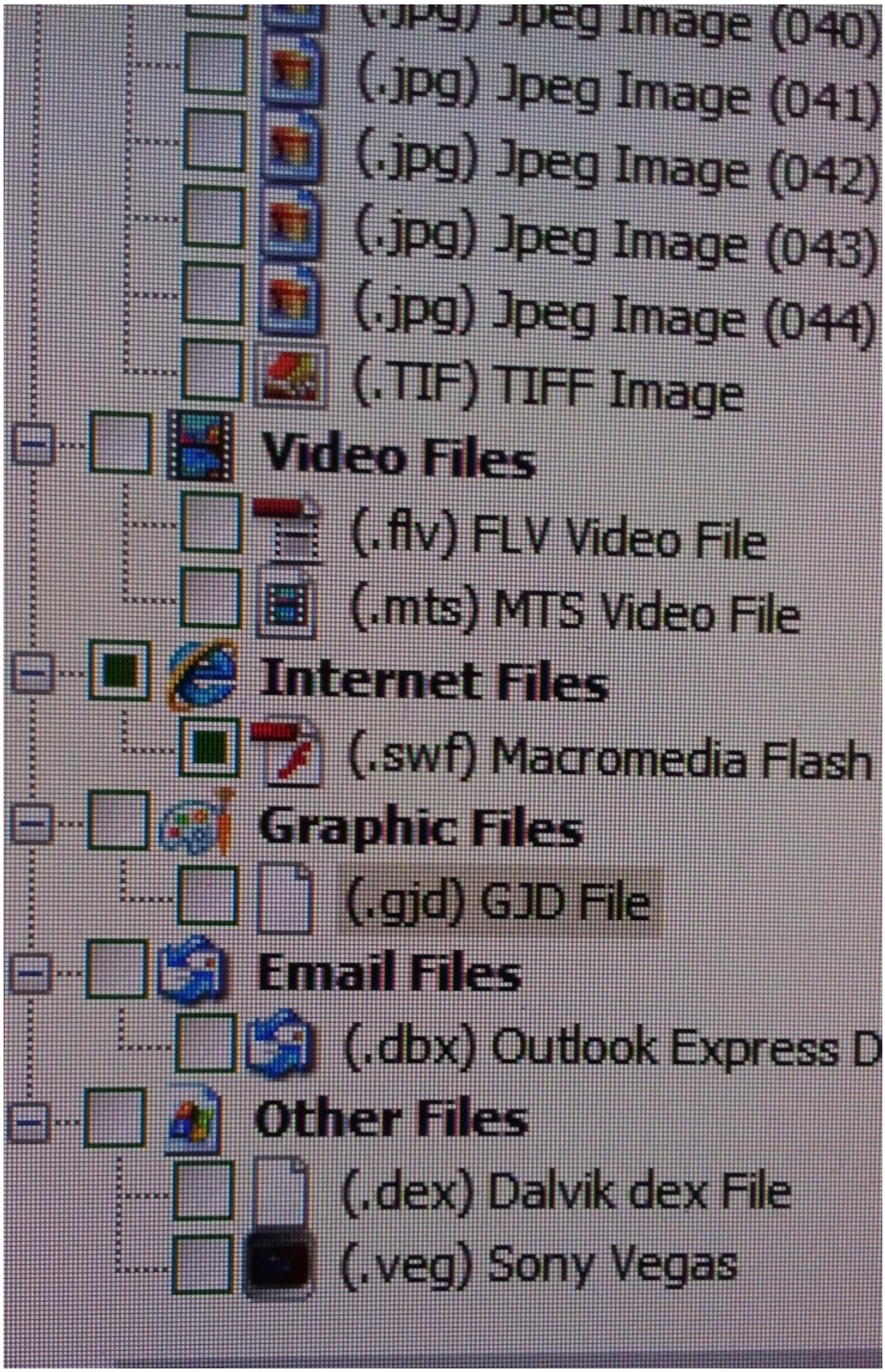

Figure 7 DISKGENIUS RECOVERY RESULTS

2.3.2 Result:

Case 1.

Hard disks of a CPPLUS make DVR has not given any output with inbuilt software and the jpeg-B file recovered through DMDE could not be played. Scanning of the same disk by disk genius has recovered 02 ‘flv’ extension files as output which could be related to area in which CCTV was installed. There were numerous ‘MTS’ extension files derived after scanning each of which was within 1 MB in size. However, none of the ‘MTS’ extension files could be played.

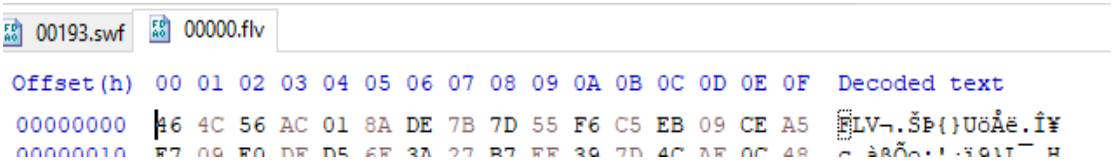

Figure 8 HEADER OF FILE RECOVERED FROM CPPLUS THROUGH DISKGENIUS

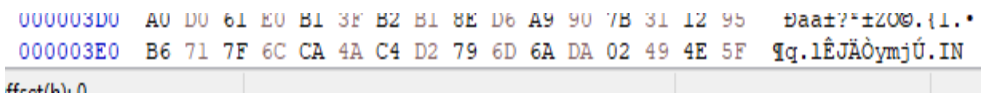

Figure 9 FOOTER OF FILE RECOVERED FROM CPPLUS THROUGH DISKGENIUS

Case 2

Hard disk of DAHUA make DVR which was password protected was examined. The inbuilt menu could not be accessed for recovery of footage. Some CCTV footages and screenshot image of same hard disk could be recovered through DMDE. Scanning with disk genius recovered numerous MTS extension files each of which was within 1 MB in size. These files could not be played. Flash files with 'swf' extension under category 'Internet Files' were also recovered which could be played through vlc player configured to play h264 files. These files are found to be CCTV footage. The files recovered have size from 3.67MB to 3GB. More than 1000 Image files with jpg extension which were screenshot files with jpg extension of CCTV footage and consistent with recovered CCTV footage could be recovered.

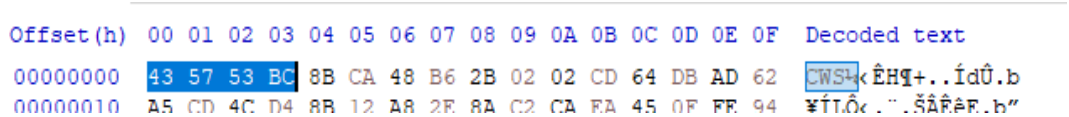

Figure 10 HEADER OF SWF FILE RECOVERED FROM DAHUA THROUGH DISKGENIUS

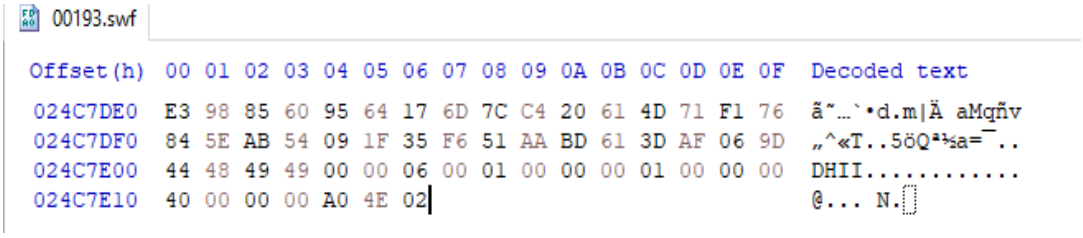

Figure 11 FOOTER OF SWF FILE RECOVERED FROM DAHUA THROUGH DISKGENIUS

Among Other files recovered were email files with extension 'dbx', files with 'dex' extension categorized as dalvikdex files, files with 'veg' extension categorized as 'Sony Vegas' files were recovered.

2.4 **Recovery using ENCASE 8 software**

2.4.1 Method:

Encase is a widely used software forensic examination. Licensed Encase version 8.04 installed on workstation with operating system 'WINDOWS 10'. Bit stream image of the hard disk extracted from OPTICOP make DVR which could not be accessed through embedded system due to password protection was examined. Bit stream image of the hard disk was carved for multimedia. The same method was also repeated with hard disks extracted from DAHUA and CPPLUS make DVR.

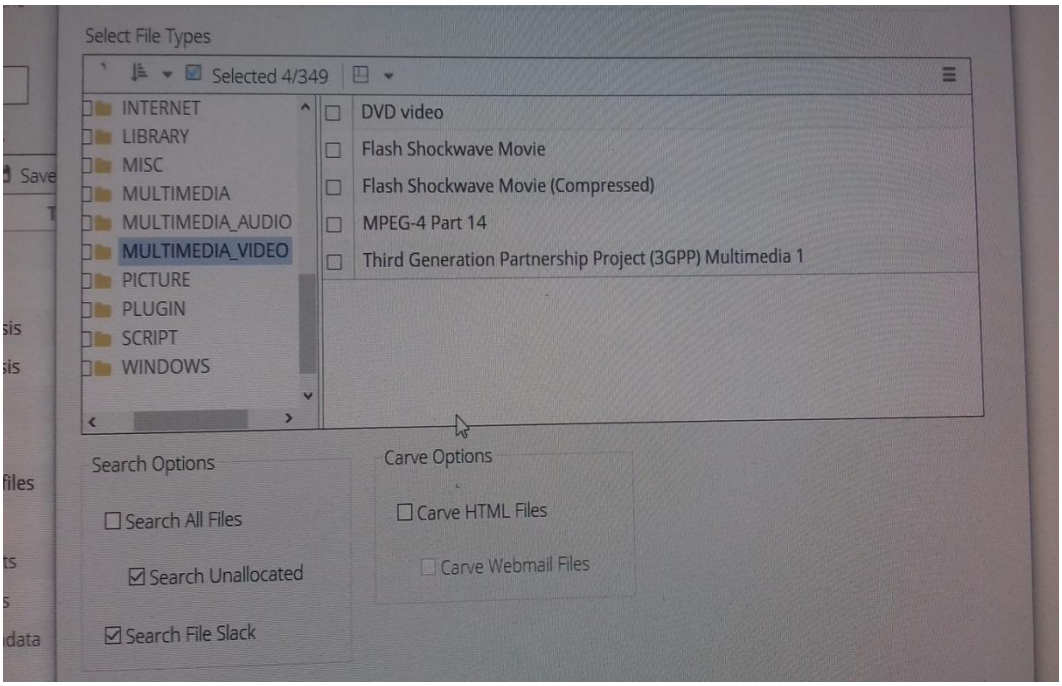

Figure 12 ENCASE CARVING FOR MULTIMEDIA

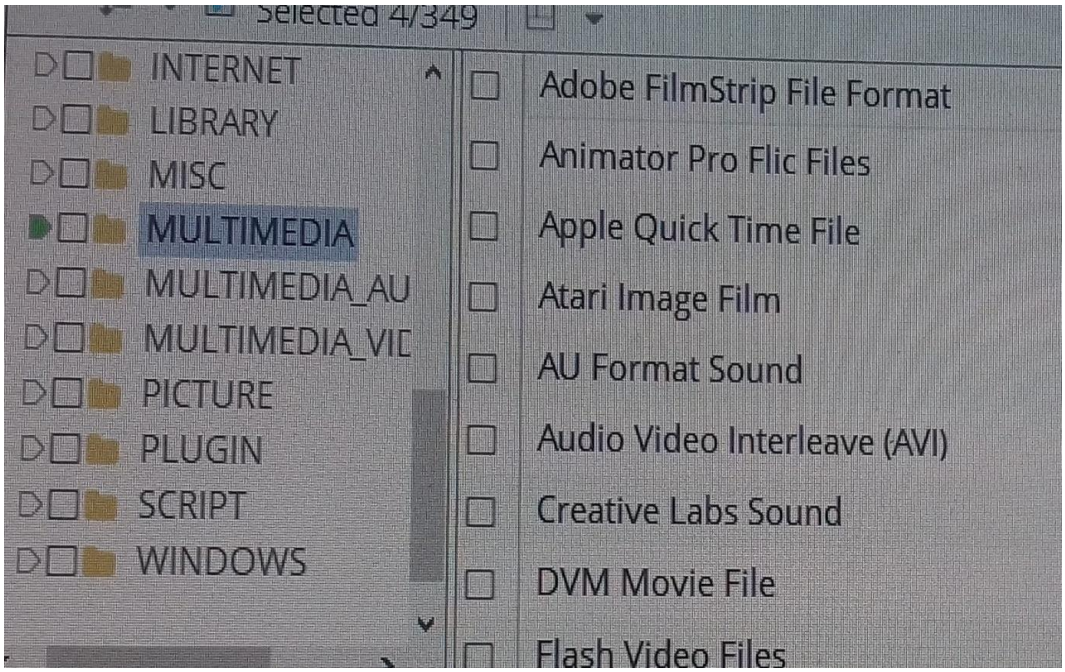

Figure 13 ENCASE CARVING OPTION

2.4.2 Results:

One video with AVI extension was recovered from bit stream image of the hard disk extracted from DVR of OPTICOP make could be played through vlc player configured to play h264 files. One video recovered from same hard disk through DMDE found to be same in content. However, time span for both differed. No files could be recovered from clone of the hard disk extracted from two other brands of DVR (DAHUA and CPPLUS). Some files were recovered by DMDE and DISK GENIUS software from same hard disk.

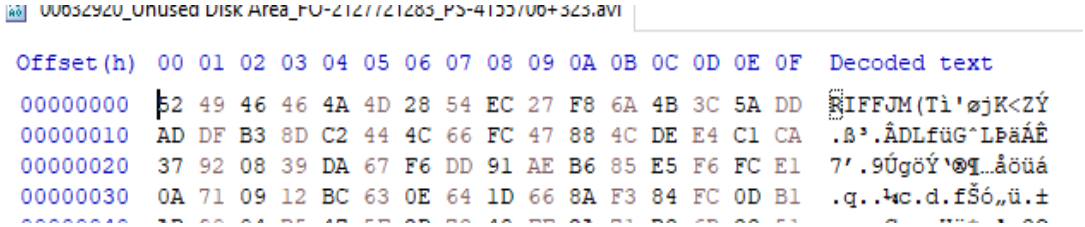

Figure 14 HEADER OF FILE RECOVERED BY ENCASE

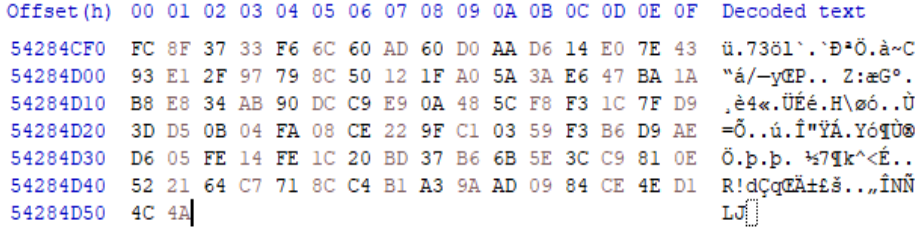

Figure 15 FOOTER OF FILE RECOVERED BY ENCASE

III. Discussion

Though trial was restricted to multimedia files with Encase software, more files may be recovered. However, one of the reasons to such restricted trial is long time taken to process carving option restricted to multimedia file as compared to whole disk scanning by DMDE and DISK GENIUS software both of which took almost same time. Additional option of other files will increase processing time further. Thus, prior knowledge of file types is desirable if Encase is tool of choice.

IV. Conclusion

It is possible to recover the CCTV footages with software for data recovery and hard disk forensic. Moreover, a collection of tools identified and validated for different brand of DVR can be prepared and used. Such collection of tools will save time as well as save examiners from closure of cases without any result. This approach also reveals presence of additional data without prior knowledge.though the study has identified some tools, more appropriate tools may exist which needs more trials with variety of DVR brands and make.

Reference

[1]. Texas instruments 'Hybrid DVR reference designs available based on TI technology' http://www.ti.com/lit/ml/sprm512a/sprm512a.pdf (accessed on 24/06/2019).
[2]. AVI RIFF File Reference DATED 05/31/2018 https://docs.microsoft.com/en-us/windows/desktop/directshow/avi-riff-file-reference (accessed on 02.07.2019).
[3]. Ethan Ace, Dahua OEM Directory Published on Apr 11, 2017https://ipvm.com/reports/dahua-oem (accessed on 02.07.2019)
[4]. Dmitry Sidorov DMDE 3.4.4 Manual (www.DMDE.COM) (accessed on 01.07.2019)
[5]. Lothar kehrer Behavior Research Methods &Instrumentation 1983, Vol. 15(1), 107-108 'A simple system for displaying alphanumeric characters on an oscilloscope using an AIM-65 microcomputer'.
[6]. White paper by altera corporation 2007 'Video Surveillance Implementation Using FPGAs'(accessed on 02.07.2019)
[7]. Thomas Gloea, André Fischera, Matthias Kirchner. Forensic analysis of video file formatsDigital Investigation 11 (2014) S68-S76
[8]. Fan J, Cao H, Kot AC. Estimating EXIF parameters based on noise features for image manipulation detection. IEEE Trans Inf Forensics Security 2013;8:608-18.
[9]. Wang W, Farid H. Exposing digital forgeries in video by detecting double MPEG compression. In: ACM workshop on multimedia and security. ACM Press; 2006. pp. 37-47.
[10]. Wang W, Farid H. Exposing digital forgeries in interlaced and dein- terlaced video. IEEE Trans Inf Forensics Security 2007;2:438-49.
[11]. 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.
[12]. Aswami Ariffin, Jill Slay, Kim-Kwang Choo. Data Recovery from Proprietary Formatted Cctv Hard Disks. 9th International Conference on Digital Forensics (DF), Jan 2013, Orlando, FL, United States. pp.213-223, ff10.1007/978-3-642-41148-9_15ff. ffhal-01460629f
[13]. 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.
[14]. Lim, Kyung-Soo & Lee, Sangjin. (2008). A Methodology for Forensic Analysis of Embedded Systems. 283-286. 10.1109/FGCN.2008.225.
[15]. F2s2: fast forensic similarity search through indexing piecewise hash signatures, Digital Investigation, 10 (4) (2013), pp. 361-371

Kananbala Jena "Data Recovery from Hard Disk Independent of Digital Video Recorder" IOSR Journal of Computer Engineering (IOSR-JCE) 21.4 (2019): 01-07.