SHS Web of Conferences **14**, 02005 (2015)
DOI: 10.1051/shsconf/20151402005

Discuss on the Data Recovery Method of Embedded DVR

Rongrong Li[1,2], Fan Yang[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]The Criminal Investigation Department of Beijing Public Security Bureau, 100054 Beijing, China

Abstract. On condition that the manufacturer keeps the file system and storage mechanism as the secret, this article makes an analysis and comparison of large amount of underlying data, and realize the research of digital video data recovery by researching the head, tail of frame data, passage number, data storage and other methods.

Keywords. embedded DVR; data recovery

1 Importance of surveillance video in public security

With the recently rapid development of computer, network and image treatment technology, the video surveillance technology has significantly developed. Currently, the video surveillance that can directly, accurately and timely reflect the objective facts has an important effect in the public security, and the cases solved by surveillance video has been increased. Meanwhile, more and more suspects also get to know the evidence effect of surveillance video, for example, the suspects will deliberately delete the surveillance video to destroy the evidence in the cases of quarrel in singing hall or other entertaining places or of theft by staff in an enterprise. Thus, the inspection demand of public security bureau 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.

Video surveillance generally includes camera, transmission cable and video surveillance system. Camera collects the front-end video image signal. After collection, the video signal will be transmitted to the host machine by cables and distributed to each monitor. Meanwhile the video and audio signal will be synchronously input in the DVR. 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.

[a] Corresponding author: wucs@sccas.cn

2 Introduction of recovery methods of video data in the embedded DVR

There are many kinds of video recorders, and for the need of technical confidentiality for each manufacturer, the file system specially owned by manufacturer is usually used, and its storage mechanism and structure are unknown, which cause a big trouble in abstraction and play of videos. In daily works, we received a video recorder produced by Streaming Video Corporation, and the surveillance video in the period of crime occurrence is man-made deleted and required for recovery.

2.1 Features of the built-in hard disk storage of embedded DVR

Different from PC type video recorder, the inner operation system and applications of embedded DVR are solidified in the motherboard. As the hard disk has no operation system, so it can be just used to store the video data. As the video that records the actual conditions of the case is stored in the hard disk, there is no doubt that the hard disk will become our main inspection object. By referring to the relevant website, we obtain several important technical parameters. The operation system of this embedded DVR uses Embedded Linux, with the standard of important code H.264. According to the experience of analysis on a large amount of underlying data, the inner hard disk storage of embedded DVR has the following features:

(1) In view of the spatial distribution of hard disk data, it can be roughly divided into system identification area, index area, data area, and the video data we care is in the data area. Similar to FAT32, NTFS and other file systems, the data area occupies a large proportion of the whole hard disk storage space.

(2) The video data in the hard disk data area is stored in frame unit, with each frame of data having symbolic frame head and tail.

(3) The storage space occupied by each frame of data is not fixed, and the size is related to the image content.

(4) The digital video will be stored in a cycling overwriting manner according to time order

(5) The deletion and formatting program of video recorder does not delete the date in the data area, but rewrite the content area, which is our theoretical basis for data recovery.

2.2 Recovery methods of video data in the embedded DVR

We know that the video data is stored in frame unit, and a continuous video is composed of much frame data. To complete the recovery task, the priority is to clarify the structure of frame data. As for this video recorder, as it uses the image code standard H.264, the frame data area is generally added with frame head and tail customized by manufacturer based on 264 raw data flow. The start code of H.264 raw data flow is "0000000161H", therefore "0000000161H" may be used as the key words in Winhex software for searching. To avoid interference, we generally start searching the date in middle section. As shown in Figure 1, the appearance frequency of "0000000161H" is very high in hard disk.

Offset	Result	Time
91F561856	0000000161	2014/09/02 17:46:24
91F561EB7	0000000161	2014/09/02 17:46:24
91F562A65	0000000161	2014/09/02 17:46:24
92E09A71D	0000000161	2014/09/02 17:46:24
92E0BE7B5	0000000161	2014/09/02 17:46:24
9397CDCF5	0000000161	2014/09/02 17:46:24
98E424731	0000000161	2014/09/02 17:46:24
98E5E2911	0000000161	2014/09/02 17:46:24
98FF8078D	0000000161	2014/09/02 17:46:24
98FF824AD	0000000161	2014/09/02 17:46:24
9900B55A2	0000000161	2014/09/02 17:46:24
990C18635	0000000161	2014/09/02 17:46:24

Figure 1. Search results in Winhex.

Then, we shall determine the head and tail of frame data. In the search result "0000000161H", we shall select five sections, and cut out several bytes prior to "0000000161H" in section. By comparing and checking the underlying data, we found that "31337762A800A800 00015200H" repeatedly appears in the middle of each section (as shown in Figure 2 and Figure 3). By preliminary reasoning, "31337762A800A80000015200H" may be the frame head of frame data. For further confirmation, we respectively select several data sections with "0000000161H" in different position in data area for analysis, check and comparison, and find that there are "33337762A800A80000015200H" (as shown in Figure 4), "32337762A800A80000015200H" (as shown in Figure 5) and other bytes that appear, by which we reason that the frame head may be "337762A800A800000 15200H". Use "337762A800A80000015200H" as the key word to search, we found a lot of results. By abstracting several results therein, we found that the key word and "0000000161H" appear in pairs. Therefore, we may confirm that "337762A800A80000015200H" is the head of frame data. According to previous inspection experience, for saving of space, the manufacturer generally leaves little interval among each frame data. So a byte section ahead of the frame head is generally the tail of frame data. By contrasting several data sections, we do not find any bytes with regularity, by which it is reasoned that the manufacturer may not specially define the frame tail. In fact, the determination of frame head, either with frame tail or not, does not greatly affect us to abstract the video data.

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
00007935008	BA	97	F7	1B	32	96	4B	FB	FC	5E	03	8B	45	2D	C1	AF
00007935024	54	C7	FC	DC	0D	9A	96	36	1A	9C	9F	E2	25	C4	78	00
00007935040	31	33	77	62	A8	00	A8	00	00	01	52	00	63	F1	0F	00
00007935056	2B	00	6A	08	07	9B	10	90	4A	1B	29	29	3B	0D	1B	7B
00007935072	3B	11	0A	A7	A0	09	93	93	4F	18	10	81	A9	11	E1	11
00007935088	0D	80	B3	3F	20	91	91	A9	2E	29	2D	29	19	31	29	3A
00007935104	79	10	92	C4	80	D3	8A	3D	0B	11	97	9B	82	A4	9A	03
00007935120	00	03	F1	84	99	91	95	11	89	11	2E	39	0A	2C	B7	99
00007935136	B4	1C	49	A1	80	B6	19	80	9F	19	18	19	A6	A8	19	00
00007935152	0B	79	08	90	81	B1	39	84	8B	01	94	11	1F	91	1A	7A
00007935168	92	A3	1D	29	49	1B	28	79	3D	80	1C	00	C3	9A	31	A9
00007935184	91	93	93	C1	03	B7	BB	51	B1	B1	11	F2	D3	90	19	01
00007935200	80	7B	10	09	4B	10	C2	0C	93	4C	82	C1	2A	10	68	99
00007935216	31	31	64	63	48	32	36	34	B7	12	00	00	00	00	00	00
00007935232	B3	58	1A	F2	1E	01	00	00	00	00	00	01	61	FE	03	91
00007935248	42	B8	FF	36	6F	17	FF	E1	E2	41	4D	2D	E6	E6	22	3F
00007935264	9F	14	48	2C	D2	DF	E8	8B	92	43	9B	28	BC	16	6B	AE

Figure 2. A section of search result "0000000161H".

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
00007950064	E1	2F	80	EB	94	B7	8B	86	6C	4E	1F	31	C7	FF	31	30
00007950080	1C	5C	52	C0	EB	94	B7	8A	8B	52	9B	43	0A	EF	F4	13
00007950096	16	43	62	AE	3D	96	67	B2	88	38	0A	0F	03	67	81	22
00007950112	45	8F	36	26	CB	58	12	7B	13	91	F5	31	C4	FC	0D	FE
00007950128	0C	E5	26	06	CD	4B	78	0A	0F	01	43	26	03	89	A2	96
00007950144	F3	09	7F	FF	04	E4	22	EE	79	7C	07	17	29	66	10	FE
00007950160	3F	3C	4E	7F	11	E2	3A	80	31	33	77	62	A8	00	A8	00
00007950176	00	01	52	00	84	F1	0E	00	2B	3A	3A	A6	A3	99	8A	3A
00007950192	98	4D	32	C2	03	CE	82	11	D0	38	97	8A	82	CB	32	C0
00007950208	21	B1	2A	A5	04	F1	1A	91	4E	20	0A	18	89	39	18	B0
00007950224	53	C9	3A	B1	94	E2	11	F3	90	09	3B	91	3F	09	2E	01
00007950240	3B	0B	2D	00	20	88	B6	98	0B	79	00	98	10	B8	30	88
00007950256	09	48	19	15	B0	97	93	C1	91	99	51	A8	3E	79	09	0B
00007950272	28	90	00	81	1B	49	B1	1F	30	19	9A	D0	13	06	9C	3B
00007950288	13	19	F2	89	19	88	5A	95	80	89	92	B8	70	89	89	06
00007950304	B1	39	A0	A5	09	92	82	F1	89	22	F0	18	02	8B	9A	61
00007950320	AB	60	9B	13	B1	10	81	92	FB	38	1C	90	33	B3	E1	69
00007950336	00	99	01	08	03	0B	F1	88	31	31	64	63	48	32	36	34
00007950352	DC	12	00	00	00	00	00	00	68	2D	1C	F2	1E	01	00	00
00007950368	00	00	00	01	61	E4	03	D1	42	91	B8	DF	E1	86	C4	61
00007950384	13	CF	4E	18	CB	7A	96	8F	8F	34	66	8F	8F	AB	E0	51
00007950400	62	E3	51	9E	B1	9D	93	BB	E0	50	42	E3	6D	4B	50	63
00007950416	D6	62	38	BF	04	EF	9B	05	F8	26	12	50	B9	68	3F	4E

Figure 3. A section of search result "0000000161H".

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
00008009920	F1	A0	89	96	90	0B	2A	03	B8	17	A3	D2	80	81	02	A6
00008009936	D8	91	03	F3	90	09	32	B9	A2	B3	10	AB	7D	10	8C	38
00008009952	18	1A	AB	93	3B	5A	01	C3	C1	A6	80	2F	18	98	09	60
00008009968	8A	10	88	05	B9	82	1A	F3	1C	18	97	2C	2A	A8	01	B1
00008009984	4B	48	91	B9	4B	30	0F	4B	1A	11	10	08	B4	C2	10	B9
00008010000	33	33	77	62	A8	00	A8	00	00	01	52	00	CC	F6	08	00
00008010016	82	A3	72	F0	01	91	3B	89	11	D8	70	1B	8B	09	9A	6B
00008010032	3A	1B	60	88	08	08	9B	31	1E	3A	11	CA	85	08	3D	78
00008010048	09	02	AA	10	81	2C	31	7C	38	1B	A5	98	C9	3A	01	4A
00008010064	2B	11	FA	3A	1B	59	92	A0	B4	90	BF	48	80	80	88	10
00008010080	A7	88	2A	91	29	98	8C	42	09	94	F0	00	8F	81	82	92
00008010096	08	92	21	A7	98	01	99	5C	03	C1	08	14	A3	B8	1E	83
00008010112	D1	10	80	93	2B	4B	52	F9	00	09	28	93	08	E1	0C	39
00008010128	30	00	4E	30	B3	F2	A0	4A	A2	3C	89	18	80	19	78	AA
00008010144	51	A2	B1	85	90	0A	19	2E	82	8A	6A	80	1C	00	D2	18
00008010160	8A	27	C2	00	A9	0A	38	90	B7	98	90	B4	2A	7B	2A	3D
00008010176	33	31	64	63	48	32	36	34	C7	03	00	00	00	00	00	00
00008010192	6D	07	1D	F2	1E	01	00	00	00	00	00	01	61	F0	02	71
00008010208	42	9C	46	22	C9	13	DF	1A	C7	EE	6D	5D	64	8C	EB	93
00008010224	6C	81	00	6D	EA	5E	5B	C6	32	DE	7B	D5	6E	7E	69	31
00008010240	7D	E2	1E	F2	66	BE	EC	23	DD	32	77	C7	B2	DA	D5	D5
00008010256	D3	6C	FB	AD	F7	DA	FE	5E	D5	5E	EB	2F	76	8F	7E	A4
00008010272	CD	4A	41	0E	D2	03	0C	69	BB	E6	E1	D6	5F	3B	FF	5C

Figure 4. A section of search result "0000000161H".

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
00008091104	F5	64	C2	32	8A	90	52	B9	11	D8	8C	EB	E3	25	7D	6A
00008091120	B2	D6	7B	C9	A9	D8	8D	F1	4E	4C	44	58	AD	D4	F9	DE
00008091136	BD	E9	77	11	78	8B	E8	F4	26	5C	47	CB	C8	B9	70	2D
00008091152	7A	AF	11	BB	F5	FC	EF	F6	53	78	AE	6D	C7	CB	88	F4
00008091168	CD	E4	9F	B3	37	9E	47	13	13	E3	70	A4	FE	6E	2B	88
00008091184	15	CA	29	C4	B8	55	DD	EE	F7	2E	48	C5	DC	A2	B6	8F
00008091200	15	8C	F1	55	AE	6B	51	FF	61	0E	6A	34	67	C7	E1	93
00008091216	7F	79	A0	00	00	00	00	00	32	33	77	62	A8	00	A8	00
00008091232	00	01	52	00	C8	F4	0E	00	28	B7	90	99	3B	39	31	F9
00008091248	13	C8	20	0A	49	AC	2C	84	C1	93	9B	7A	18	95	A0	03
00008091264	B9	58	91	8A	B7	B1	01	0A	3C	00	09	89	3A	68	D9	32
00008091280	C2	81	D1	19	93	9B	79	6B	88	20	A3	1D	99	68	19	B3
00008091296	98	92	A2	F1	92	AA	18	21	94	E3	92	B1	B5	A1	82	99
00008091312	48	BB	3D	1B	78	B4	A3	A1	83	C4	98	04	91	8B	79	89
00008091328	18	08	14	D3	A0	8A	58	A0	80	D2	2D	2A	01	4A	99	59
00008091344	A1	3B	6A	92	89	98	27	B8	1B	E2	B1	69	90	92	08	91
00008091360	3C	58	A1	20	98	C3	03	B1	D0	BC	3A	58	99	3A	5C	01
00008091376	85	D4	89	2B	2B	30	9D	5A	01	91	A0	83	B0	92	B9	6A
00008091392	98	13	A5	A0	E0	1D	6A	1A	32	31	64	63	48	32	36	34
00008091408	45	20	00	00	00	00	00	00	F7	7B	21	F2	1E	01	00	00
00008091424	00	00	00	01	61	F6	03	31	42	AF	13	D0	84	4F	8B	D4
00008091440	51	44	6E	11	61	4E	75	A1	02	44	1E	A2	CD	A1	42	C5
00008091456	1E	54	8B	B9	C8	BC	65	0D	C8	92	C6	F7	90	AE	69	44

Figure 5. A section of search result "0000000161H".

Furthermore, we also find another regularity. A byte "30H", "31H", "32H", "33H" with regularity appear ahead of the frame head "337762A800A80000015200H". To clarify the meaning of this byte, we respectively export several frame data starting with "30337762A800A80000015200H", "31337762A800A80000015200H", "32337762A800A80000015200H", "33337762A800A80000015200H" to be stored as a file and checked by a player software provided by manufacturer, in which it is found that the passages displayed in the image are respectively "Passage 1", "Passage 2", "Passage 3" and "Passage 4". For further confirmation of the relation between one byte before the frame head and the passage number, we also select several data section for experiment, and basically confirm that this byte represents the passage number.

We export several sections of continuous data (Note: delete the start section of frame head and export from "0000000161H") to be stored as a file with extension name 264. We try to use video player to play, but unfortunately, Windstorm Image Sound, Perfect Decode and other universal player fail to play the file. By searching on the Internet, we found an exclusive video surveillance player named Hsplayer, which could play the exported file, but the images are switched frequently in each passage, we could not normally watch the video. Therefore, we reasoned that the data storage method of this video recorder may store the video data in each passage with the same time in a same region in order. So we successively copied, matched and exported the data section in the same passage to files to be played by Hsplayer, and the image display was normal.

Generally, the digital video will be stored in a cycling overwriting manner according to time order According to the above storage regularity, we shall search the video data in a certain time section, namely we shall first determine the data area and export the data section in the front, middle and rear part of data area respectively according to the above method to confirm the rough position of video data we wanted to find, and repeated this procedure to reduce the searching scope until we found out the video data in relevant period.

3 Conclusion

The data recovery of surveillance video has always been the problem that the digital evidence inspection faces, especially the embedded surveillance video. As it uses the file system customized by manufacturer, its storage mechanism and storage structure are varied, and there's not any available professional data recovery tools. Generally, we can only depend on the experience and ability of inspector for artificial recovery. This article discusses the data recovery method of embedded DVR, and makes an analysis, comparison of a large amount of underlying data and research on the head and tail of frame data, as well as the passage number and data storage methods to realize the recovery of video data. But, as for the crack of information, such as time, that is conducive for us to rapidly search the video data is subject to further analysis and research.

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, Han Jie, Jia Yongsheng & Song Run. Ideology of taking evidence from digital video[J]. *Criminal Technology*, 2010, 2.
2. Huang Deyi. Application of hard dis storage technology in video surveillance[J]. *Chinese Security and Protection*, 2009, 5.
3. Chen Bo, Shi Xugang, Application of H.264 Standard in video surveillance system[J]. *Chinese Wire Television*, 2008, 11.
4. Zhang Li, Xu Lihong & Xu Shenglin. Design and realization of digital video recorder based on embedded Linux[J]. *Application of Micro Computer*, 2005.
5. Jia Chaoguang & Zou Fengxing. Feature of H.264/AVC and its application in video surveillance[J]. *Measurement and Control of Computer*, 2005, 2.