



작성자	허은정
분석 일자	2024.05.22
작성 일자	2024.05.22
분석 대상	REC_1970_01_01_00_23_05_F.MP4
문서 버전	1.0
작성자 E-mail	dmswjd4315@yonsei.ac.kr

0. 목차

1. 문제3

2. 분석 도구3

3. 환경3


4. Write-Up.....4

5. Flag.....8

6. 별도 첨부9

7. Reference 10

1. 문제

URL	-
문제 내용	<p>A vehicle equipped with a dash cam has recorded the file from the last recorded time zone abnormally due to an accident. Normal files recorded in the previous time zone are recorded with video data and audio data in an Ftyp container with an MP4 extension. However, the video data of abnormal files only records a black screen, while the audio files are recorded normally. Recover audio files of MP4 files recorded due to abnormal termination. Since the mounted dash cam uses a file system with a bank structure, various time zone data remain in the abnormally terminated file due to the file slack phenomenon.</p> <p>Q1. Submit the title of the audio file played from 0 to 20 seconds recorded in the target file. (100 points)</p>
문제 파일	 REC_1970_01_01_00_23_05_F.MP4
문제 유형	file system forensics
난이도	1/ 3

2. 분석 도구

도구명	다운로드 링크	Version
HxD	https://mh-nexus.de/en/downloads.php?product=HxD20	2.5.0

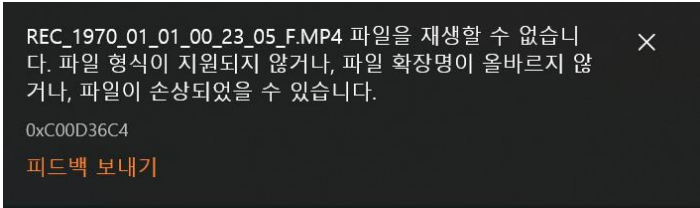
3. 환경

OS
Window 11 64-bit

4. Write-Up

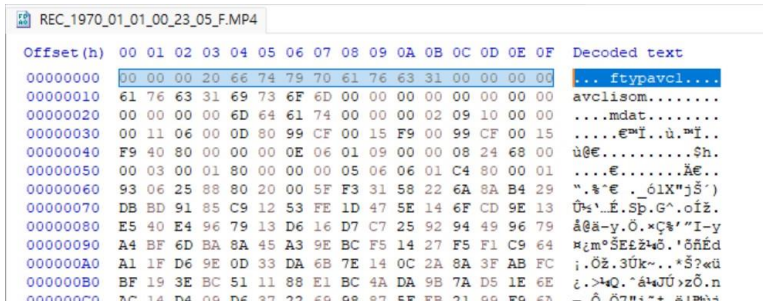
파일명	REC_1970_01_01_00_23_05_F.MP4
용량	80.0MB
SHA256	a7e109f3ba6b70bc7e6d746236823e090cea4fb72a623de3a87c82acdcabcd99d
Timestamp	2023-04-25 9:45:56

Submit the title of the audio file played from 0 to 20 seconds recorded in the target file. (100 points)



[사진 1] 문제 파일을 열어본 결과

다운 받은 문제 파일을 열어본 결과 해당 파일을 재생할 수 없었다.



[사진 2] 문제 파일 확장자 확인

다운 받은 문제 파일을 HxD를 이용하여 확인해보았더니, 모든 mp4 영상에 존재하고 있으며 비디오 데이터의 인덱스 역할을 하는 moov 박스 구조가 파싱되지 않은 것을 알 수 있다. 따라서, 해당 영상을 재생하기 위해서는 moov 박스가 해당 문제 파일 구조에 복구해야 한다.

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	00	00	00	20	66	74	79	70	61	76	63	31	00	00	00	00	... ftypavcl....
00000010	61	76	63	31	69	73	6F	6D	00	00	00	00	00	00	00	00	avclisom.....
00000020	00	00	00	00	6D	64	61	74	00	00	00	02	09	10	00	00	...mdat.....
00000030	00	11	06	00	0D	80	99	CF	00	15	F9	00	99	CF	00	15e"i..u..m"i..
00000040	F9	40	80	00	00	00	0E	06	01	09	00	00	08	24	68	00	ù@e.....\$h.
00000050	00	03	00	01	80	00	00	00	05	06	06	01	C4	80	00	01e.....Åe..
00000060	93	06	25	88	80	20	00	5F	F3	31	58	22	6A	8A	B4	29	".%*e _61X"jŠ")
00000070	DB	BD	91	85	C9	12	53	FE	1D	47	5E	14	6F	CD	9E	13	Ů%'.E.Sp.G^,oİz.
00000080	E5	40	E4	96	79	13	D6	16	D7	C7	25	92	94	49	96	79	â@a-y.O.*Ç% 'I-y
00000090	A4	BF	6D	BA	8A	45	A3	9E	BC	F5	14	27	F5	F1	C9	64	Hzm°SEēZkō.'8ñEd
000000A0	A1	1F	D6	9E	0D	33	DA	6B	7E	14	0C	2A	8A	3F	AB	FC	;.ÖZ.3Ük~..*Š?«ü
000000B0	BF	19	3E	BC	51	11	88	E1	BC	4A	DA	9B	7A	D5	1E	6E	¿.>*Q.^â%UÜ>zÖ.n
000000C0	AC	14	D4	09	D6	37	22	69	98	87	5F	EB	21	99	F9	6A	~.Ö.Ö7"i"+_e!müj
000000D0	D5	2D	8E	C6	D1	EA	CF	89	76	51	09	EE	DF	F6	69	AC	Ö-ZēNēItwQ.iBô1~
000000E0	46	F1	64	DA	33	E0	6F	BB	BB	D9	E2	A4	8B	56	26	E0	FñdÜ3ào»»ÜâH<Vâ~
000000F0	E0	F0	B9	E3	21	E7	99	2E	E4	2A	58	E7	98	2F	90	F9	âô'â!ç™.â*Xç"/.ù
00000100	5E	5B	8B	20	9A	EB	C3	F5	D9	FB	37	96	D9	70	73	99	^[< sēÄöÜ7>Üps™
00000110	33	92	03	F5	F7	0C	14	94	01	28	C7	83	D8	8F	01	89	3/..Ä~.."/.Cfö..k

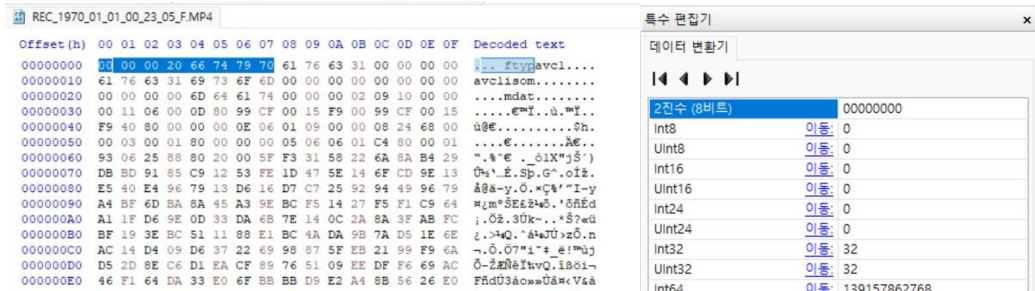
[사진 3] mdat박스의 사이즈 확인

moov 박스 구조가 파싱되지 않는 이유를 찾아보던 중 mdat 박스의 사이즈가 0 으로 지정되어 있는 것을 확인하였고 이를 통해 moov 박스 구조가 파싱되지 않았다는 것을 알 수 있다.

0251ED20	08	06	B2	05	B1	05	41	05	E9	04	F7	04	13	04	42	01	...±.A.e.÷...B.	
0251ED30	47	FE	64	FB	CC	F8	D0	F4	41	F0	83	EB	F3	E6	F0	E2	GpdûIæðöAðfæöæðâ	
0251ED40	77	DF	89	DC	7D	DA	9B	D8	27	D7	FA	D6	83	D8	89	DA	wB%Ů}Ů>Ø'×üÖfØ%Ů	
0251ED50	AC	DC	6E	DF	26	E3	44	E6	5C	E9	24	ED	01	F2	AC	F6	~ŮnB&âDæ\é\$î.ð~ð	
0251ED60	8A	FA	7A	FE	27	03	1A	08	04	0D	6A	12	55	18	39	1E	Šüzp'.....j.U.9.	
0251ED70	84	23	81	28	24	2E	7E	33	26	37	BB	39	5A	3B	7C	3B	„#.(\$.~3&7»9Z; ;	
0251ED80	F0	39	3A	37	46	34	7F	30	B3	2A	EC	22	AD	1A	E6	11	ð9:7F4.0*~i"..æ.	
0251ED90	B4	09	DC	02	70	FC	B8	F5	00	00	7E	E9	6D	6F	6F	76	'Ü.pü,ö...~émoov	
0251EDA0	00	00	00	6C	6D	76	68	64	00	00	00	00	00	7C	25	B5	EA	...lmvhd.... küê
0251EDB0	7C	25	B5	EA	00	00	75	30	00	0B	71	B0	00	01	00	00	küê..u0..q°....	
0251EDC0	01	00	00	00	00	00	00	00	00	00	00	00	00	01	00	00	
0251EDD0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	01	00	
0251EDE0	00	00	00	00	00	00	00	00	00	00	00	00	00	40	00	00@...	
0251EDF0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0251EFF0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00*	

[사진4] moov 박스 존재 확인

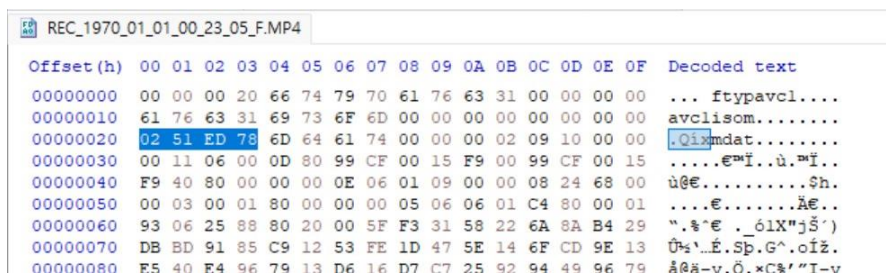
moov 박스가 파일 내에 있는지 확인하기 위해 moov 박스 구조에 포함되어 있는 "moov"문자열을 검색한다. 이를 통해 moov 박스의 존재를 확인할 수 있었고, moov 박스의 시작 위치가 파일의 38923672 번째 바이트 임을 알 수 있다



[사진 5] ftyp 박스의 크기 확인

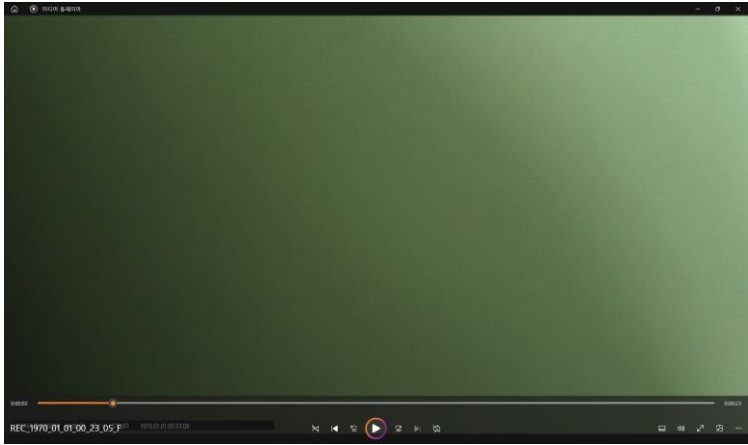
mdat 박스의 사이즈를 구하기 위해 mdat 박스 앞 존재하는 ftyp 박스의 크기를 찾아보았다. [사진 5]에서 보았듯이 ftyp 박스의 크기는 32 바이트임을 알 수 있고, 위에서 찾은 내용을 통해 moov 박스의 시작 지점이 38923672 를 알 수 있다.

이를 통해, moov 박스의 크기를 구할 수 있다. moov 박스의 크기를 구하는 방법은 moov 박스의 시작 지점에서 ftyp 박스의 크기를 빼주는 것이므로 moov 박스의 크기는 $38923672 - 32 =$ **38923640** 바이트이다.



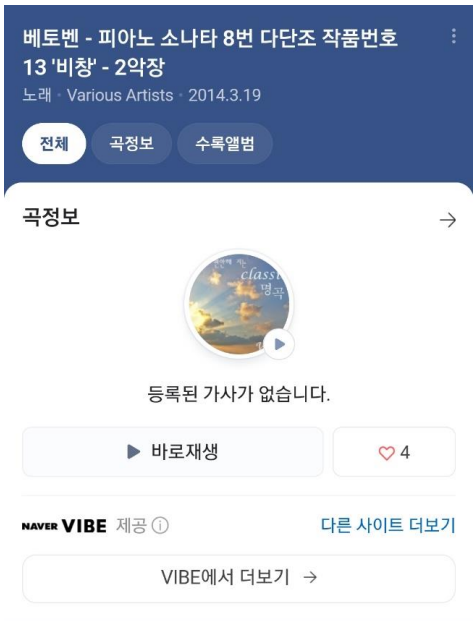
[사진 6] mdat박스의 사이즈를 지정

mdat 박스의 크기를 38923640 으로 설정하면 moov 박스 구조가 정상적으로 파싱되는 것을 확인할 수 있다.



[사진 7] 복구한 영상파일 재생

moov박스를 복구한 영상을 다시 살펴보았더니 정상적으로 재생되는 것을 알 수 있었다.



[사진 8] 영상에 나오는 음악

영상 파일에서 나오는 음악 소리를 네이버 앱을 통해 검색해보면 **베토벤 - 피아노 소나타 8번 다단조 작품번호 13'비창' - 2악장** 곡임을 알 수 있다.

5. Flag

베토벤 – 피아노 소나타 8 번 다단조 작품번호 13'비창' - 2 악장

6. 별도 첨부

7. Reference

- <https://duzi077.tistory.com/118>
- <https://blog.naver.com/yesing1/70096278829?viewType=pc>