101 – Where is the starting point of the audio?

Team Information

Team Name : ForensicGPT

Team Member : Eungchang Lee, Donghyun HA, Hyunwoo Shin, Jinhyeok Son

Email Address : forensicgpt@googlegroups.com

Instructions

Description 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.

Target	Hash (MD5)
REC_1970_01_01_00_23_05_F.MP4	82395B3B85E5AF23AEEE50DBB6AE2072

Questions

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

Teams must:

- Describe step-by-step processes for generating your solution.
- Specify any tools used for this problem.

Tools used:

Name:	010 Editor	Publisher:	SWEETSCAPE
Version:	13.0.1 (64-bit)		
URL:	http://www.010editor.com/		

Name:	VLC Media Player	Publisher:	VideoLAN
Version:	3.0.18 (64-bit)		
URL:	https://www.videolan.org/vlc/		

Step-by-step methodology:

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

다운로드 받은 파일은 [REC_1970_01_01_00_23_05_F.MP4]이고, md5 hash를 비교해 동일 파일이라는 것을 확인할 수 있었습니다.

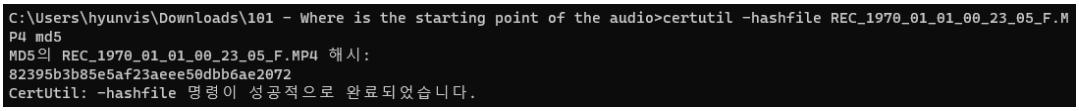


그림 1 MD5 Hash 확인

먼저, 해당 영상을 재생하려고 시도하면 재생되지 않는 문제가 발생합니다.

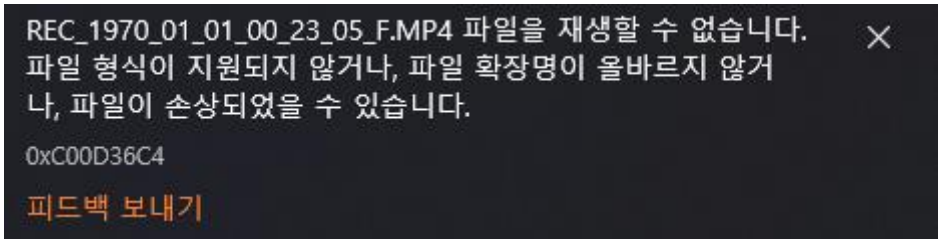


그림 2 재생 불가 확인

010 Editor를 이용해 파일을 확인해보면 다음과 같이 mdat 영역의 사이즈가 0으로 지정된 것을 확인할 수 있습니다.

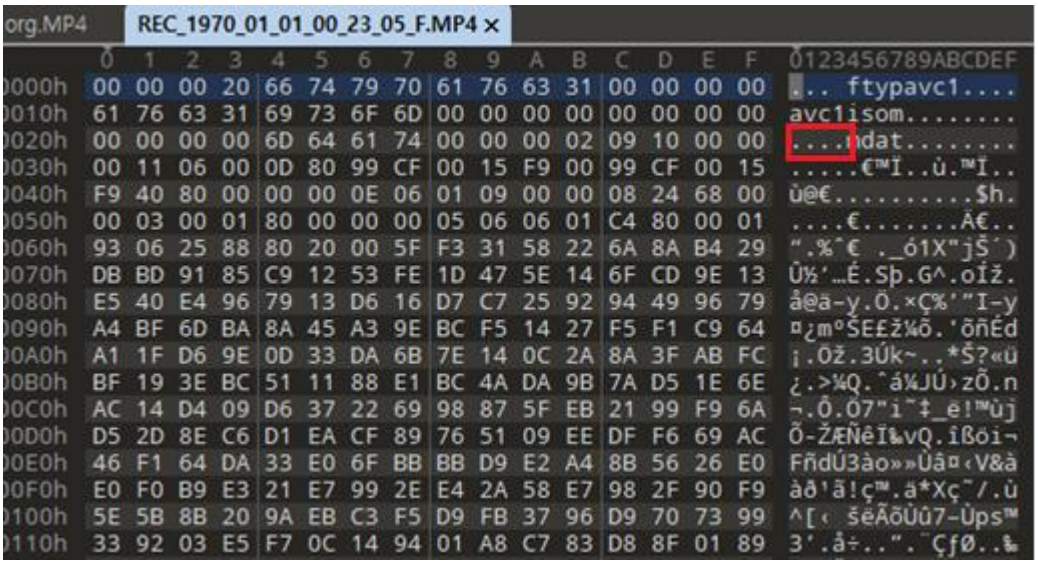
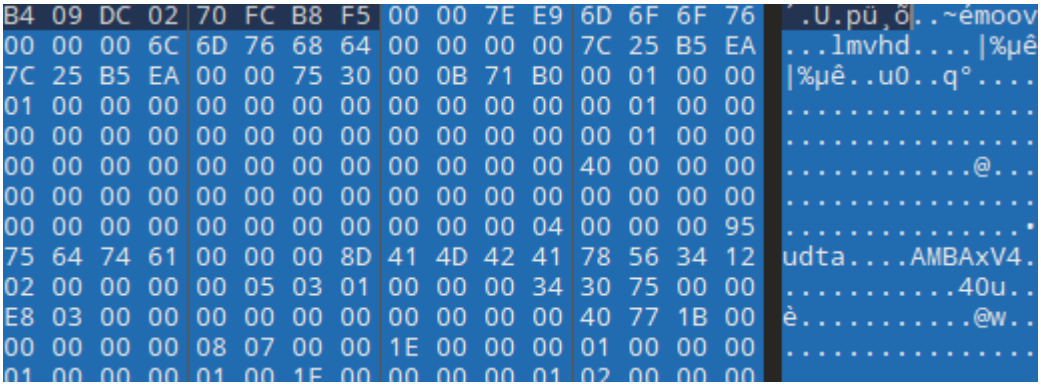


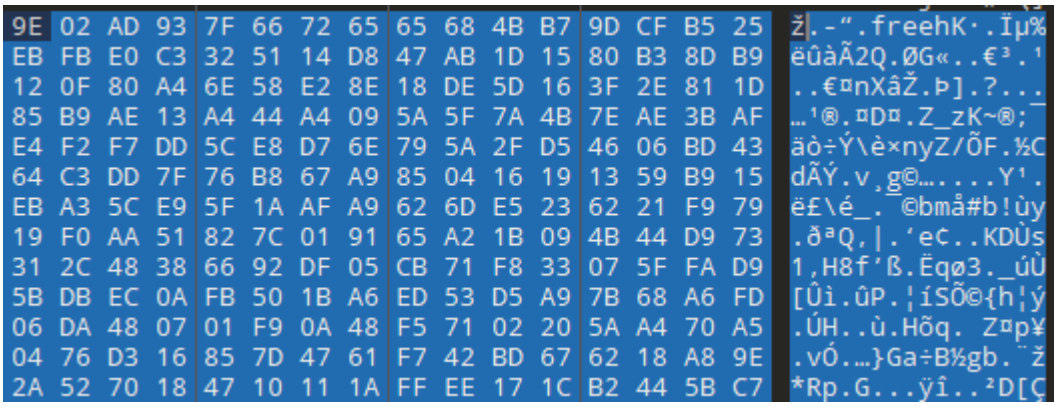
그림 3 mdat 사이즈

반대로 moov 및 free 영역은 아래 사진과 같이 정상적인 것을 확인할 수 있습니다.



B4	09	DC	02	70	FC	B8	F5	00	00	7E	E9	6D	6F	6F	76
00	00	00	6C	6D	76	68	64	00	00	00	00	7C	25	B5	EA
7C	25	B5	EA	00	00	75	30	00	0B	71	B0	00	01	00	00
01	00	00	00	00	00	00	00	00	00	00	00	00	01	00	00
00	00	00	00	00	00	00	00	00	00	00	00	00	01	00	00
00	00	00	00	00	00	00	00	00	00	00	00	40	00	00	00
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00	00	04	00	00	00	95
75	64	74	61	00	00	00	8D	41	4D	42	41	78	56	34	12
02	00	00	00	00	05	03	01	00	00	00	34	30	75	00	00
E8	03	00	00	00	00	00	00	00	00	00	00	40	77	1B	00
00	00	00	00	08	07	00	00	1E	00	00	00	01	00	00	00
01	00	00	00	01	00	1F	00	00	00	00	01	02	00	00	00

그림 4 moov 영역



9E	02	AD	93	7F	66	72	65	65	68	4B	B7	9D	CF	B5	25
EB	FB	E0	C3	32	51	14	D8	47	AB	1D	15	80	B3	8D	B9
12	0F	80	A4	6E	58	E2	8E	18	DE	5D	16	3F	2E	81	1D
85	B9	AE	13	A4	44	A4	09	5A	5F	7A	4B	7E	AE	3B	AF
E4	F2	F7	DD	5C	E8	D7	6E	79	5A	2F	D5	46	06	BD	43
64	C3	DD	7F	76	B8	67	A9	85	04	16	19	13	59	B9	15
EB	A3	5C	E9	5F	1A	AF	A9	62	6D	E5	23	62	21	F9	79
19	F0	AA	51	82	7C	01	91	65	A2	1B	09	4B	44	D9	73
31	2C	48	38	66	92	DF	05	CB	71	F8	33	07	5F	FA	D9
5B	DB	EC	0A	FB	50	1B	A6	ED	53	D5	A9	7B	68	A6	FD
06	DA	48	07	01	F9	0A	48	F5	71	02	20	5A	A4	70	A5
04	76	D3	16	85	7D	47	61	F7	42	BD	67	62	18	A8	9E
2A	52	70	18	47	10	11	1A	FF	EE	17	1C	B2	44	5B	C7

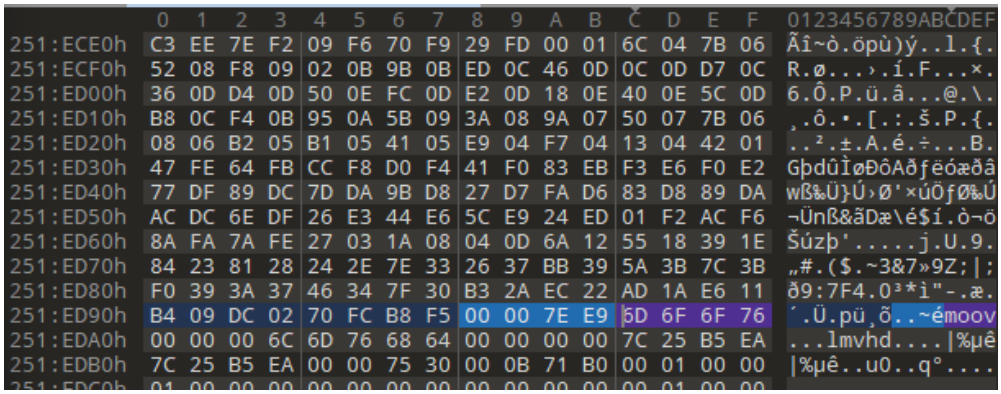
그림 5 free 영역

손상된 mdat영역의 size를 수정하기 위해서 size의 크기를 알아야 합니다.

Mdat의 size를 구하는 공식은 다음과 같습니다.

Mdat Size = [MOOV Size] – [ftyp_END]

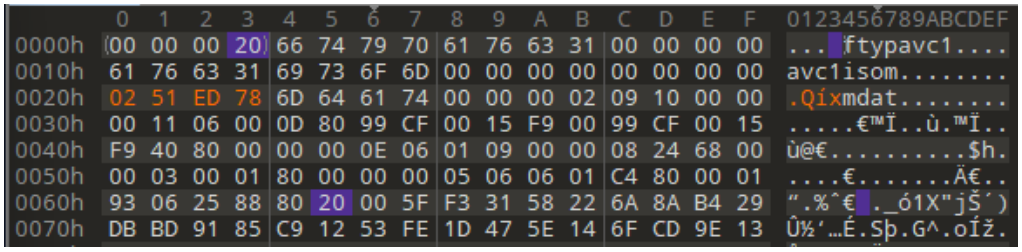
이 공식에 현재 파일을 대입해 보면 moov size는 0x251ED98, ftyp_END 값은 0x20 이기 때문에 mdat size는 0x251ED78인 것을 알 수 있습니다.



	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
251:ECE0h	C3	EE	7E	F2	09	F6	70	F9	29	FD	00	01	6C	04	7B	06	Ãî~ò.öpù)ý..l.{.
251:ECF0h	52	08	F8	09	02	0B	9B	0B	ED	0C	46	0D	0C	0D	D7	0C	R.ø...›.í.F...×.
251:ED00h	36	0D	D4	0D	50	0E	FC	0D	E2	0D	18	0E	40	0E	5C	0D	6.Ô.P.ü.â...@.\.
251:ED10h	B8	0C	F4	0B	95	0A	5B	09	3A	08	9A	07	50	07	7B	06	¸.ô.•.[.:.š.P.{.
251:ED20h	08	06	B2	05	B1	05	41	05	E9	04	F7	04	13	04	42	01	..².±.A.é.÷...B.
251:ED30h	47	FE	64	FB	CC	F8	D0	F4	41	F0	83	EB	F3	E6	F0	E2	GþdûÌøÐôAðƒëóæðâ
251:ED40h	77	DF	89	DC	7D	DA	9B	D8	27	D7	FA	D6	83	D8	89	DA	wß‰Ü}Ú›Ø'×úÖƒØ‰Ú
251:ED50h	AC	DC	6E	DF	26	E3	44	E6	5C	E9	24	ED	01	F2	AC	F6	¬Ünß&ãDæ\é$í.ò¬ö
251:ED60h	8A	FA	7A	FE	27	03	1A	08	04	0D	6A	12	55	18	39	1E	Šúzþ'.....j.U.9.
251:ED70h	84	23	81	28	24	2E	7E	33	26	37	BB	39	5A	3B	7C	3B	„#.($.~3&7»9Z;|;
251:ED80h	F0	39	3A	37	46	34	7F	30	B3	2A	EC	22	AD	1A	E6	11	ð9:7F4.0³*ì"-.æ.
251:ED90h	B4	09	DC	02	70	FC	B8	F5	00	00	7E	E9	6D	6F	6F	76	´.Ü.pü¸õ..~émoov
251:EDA0h	00	00	00	6C	6D	76	68	64	00	00	00	00	7C	25	B5	EA	...lmvhd....|%µê
251:EDB0h	7C	25	B5	EA	00	00	75	30	00	0B	71	B0	00	01	00	00	|%µê..u0..q°....

그림 6 moov size

해당 Size를 기반으로 mdat의 size를 아래와 같이 수정하면 정상적으로 동영상이 재생되는 것을 확인할 수 있습니다.



	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
0000h	00	00	00	20	66	74	79	70	61	76	63	31	00	00	00	00	... ftypavc1....
0010h	61	76	63	31	69	73	6F	6D	00	00	00	00	00	00	00	00	avc1isom........
0020h	02	51	ED	78	6D	64	61	74	00	00	00	02	09	10	00	00	.Qíxmdat........
0030h	00	11	06	00	0D	80	99	CF	00	15	F9	00	99	CF	00	15	.....€™Ï..ù.™Ï..
0040h	F9	40	80	00	00	00	0E	06	01	09	00	00	08	24	68	00	ù@€..........$h.
0050h	00	03	00	01	80	00	00	00	05	06	06	01	C4	80	00	01	....€........Ä€..
0060h	93	06	25	88	80	20	00	5F	F3	31	58	22	6A	8A	B4	29	“.%ˆ€ ._ó1X"jŠ´)
0070h	DB	BD	91	85	C9	12	53	FE	1D	47	5E	14	6F	CD	9E	13	Û½'…É.Sþ.G^.oÍž.

그림 7 mdat size 수정

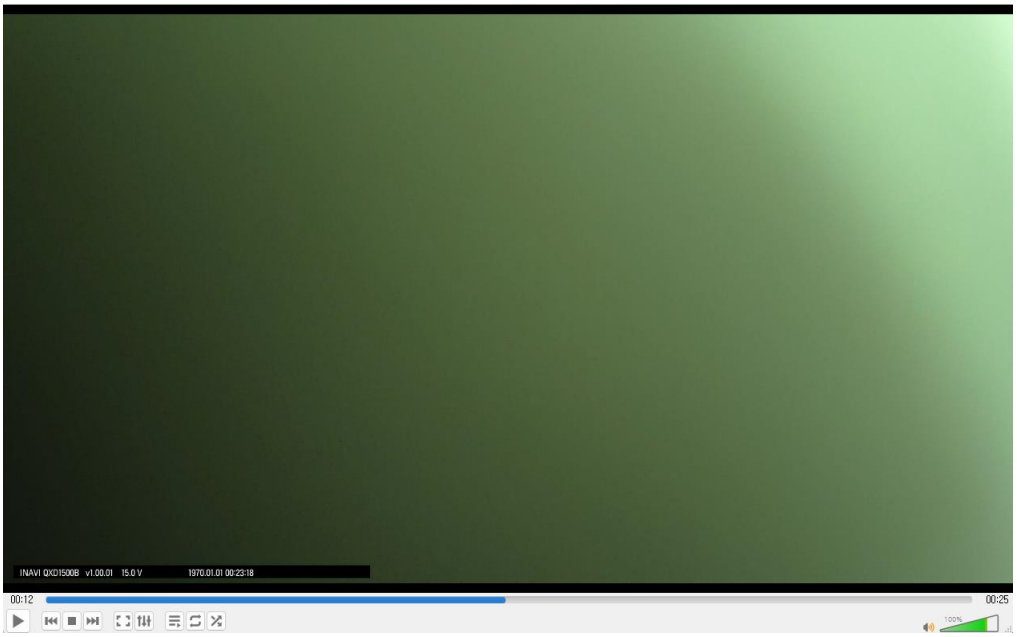


그림 8 영상 재생 확인

녹화된 영상에서는 음악이 재생되고 있으며, 해당 노래는 다음과 같습니다.

Piano Sonata no.8 in C minor, Op. 13 "Pathetique":II. Adagio cantabille