152 – Find video and time info.

Team Information

Team Name : ForensicGPT

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

Email Address : forensicgpt@googlegroups.com

Instructions

Description A movie file, but there is an unknown file that does not play normally in the playback viewer. Video, voice, and time information are recorded in this file, and many books are recorded in the video file. We need to restore the video and find the time information.

Target	Hash (MD5)
problem-final.img	CB91D34E37E31561079909945B4E287E

Questions

1. Submit a book title for a video file with different time information recorded between the video and the video frame data. (50 points)
2. Submit the title of the book containing recorded video time with time information from the year 2024 (The time information of the video is located at the beginning of the video data). (100 points)

Teams must:

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

Tools used:

Name:	HxD	Publisher:	Maël Hörz
Version:	2.5.0.0		
URL:	https://www.mh-nexus.de		

Name:	HashTab	Publisher:	Implbits Software
Version:	6.0.0		
URL:	https://implbits.com		

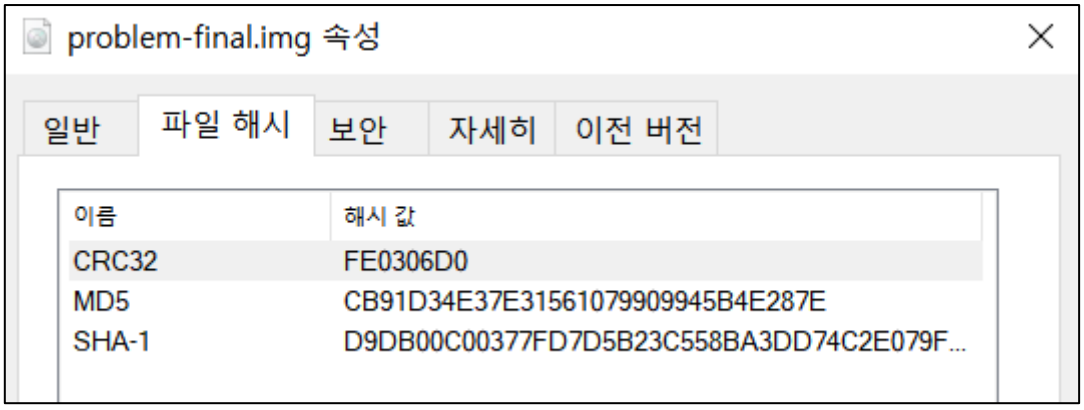
Name:	Dcode	Publisher:	Digital Detective
Version:	5.5		
URL:	https://www.digital-detective.net/dcode/		

Name:	ffmpeg	Publisher:	FFmpeg developers
Version:	6.0		
URL:	https://ffmpeg.org/download.html		

Name:	ffplay	Publisher:	FFmpeg developers
Version:	6.0		
URL:	https://ffmpeg.org/download.html		

Name:	kmplayer	Publisher:	PandoraTV
Version:	4.2.2.68		
URL:	https://www.kmplayer.com/kr/home		

Step-by-step methodology:

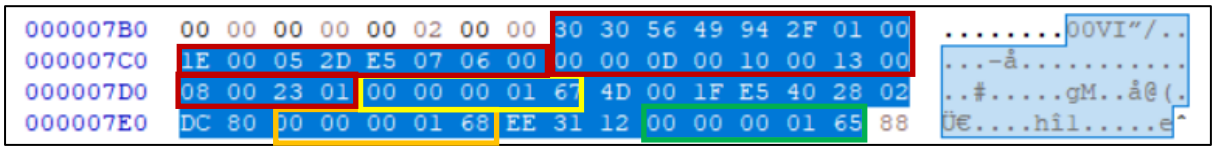


[그림 1] 해시 값 확인

분석에 앞서, 주어진 파일에 대한 해시 값을 산출하여 MD5 해시 값이 일치함을 확인하였습니다.

1. Submit a book title for a video file with different time information recorded between the video and the video frame data. (50 points)

h264(avc) codec의 구조에 따라 SPS, PPS, IDR, non-IDR 등을 구성하는 NAL 단위로 주어진 파일을 분석하였습니다.

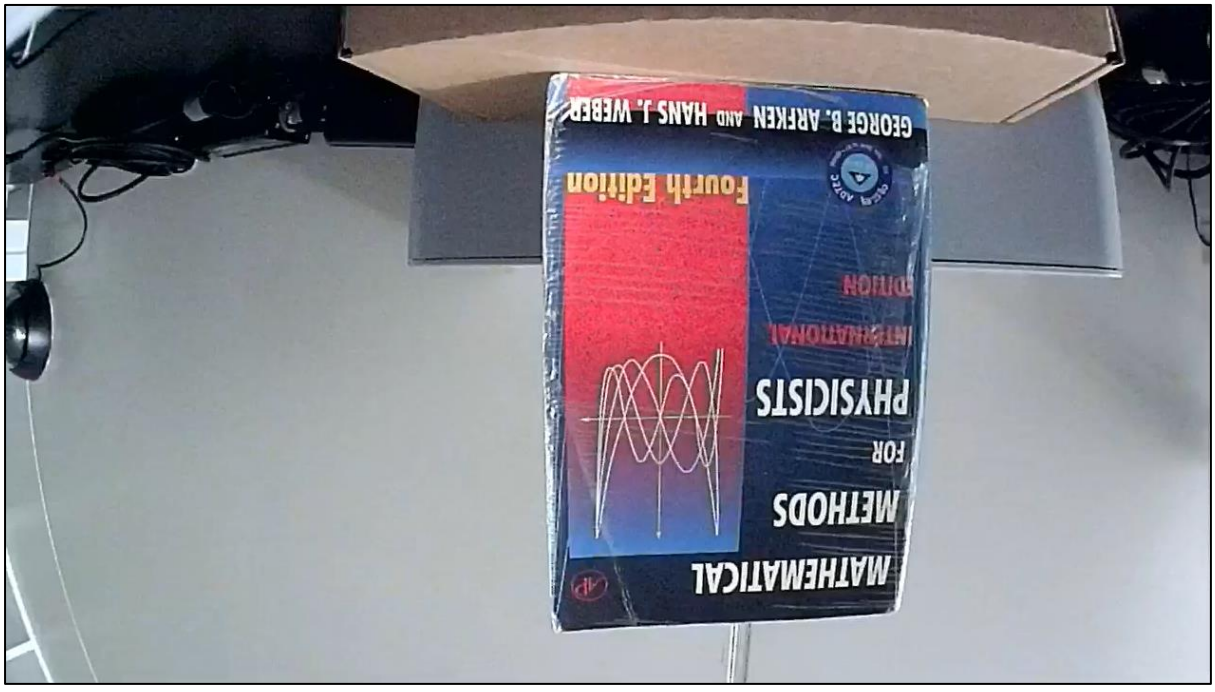


[그림 2] 메타정보 및 NAL 구조 예시

노란색 박스에 해당하는 SPS, 주황색 박스에 해당하는 PPS, 그리고 초록색 박스에 해당하는 IDR NAL Unit들이 존재하는 것과 더불어, 00VI부터 SPS까지 존재하는 데이터에 주목할 수 있었습니다.

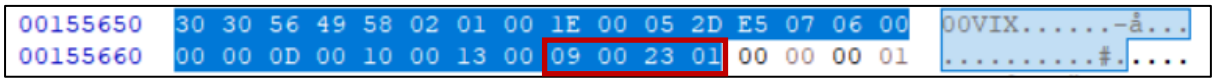
빨간색 박스에 해당하는 데이터 구조의 특징을 각각 살펴보았습니다.

먼저, 00VI에 해당하는 특정 시그니처는 주어진 파일에서 이 외에도 01VI, 00VP, 01VP, 00AD, 00SE 등으로 존재하였습니다. 따라서, 위 그림 2에 해당하는 데이터를 00VI 부터 다음의 특정 시그니처인 00VP 전까지 카빙해서 살펴보면, 다음과 같이 비디오 데이터가 나오는 것을 확인하였습니다.

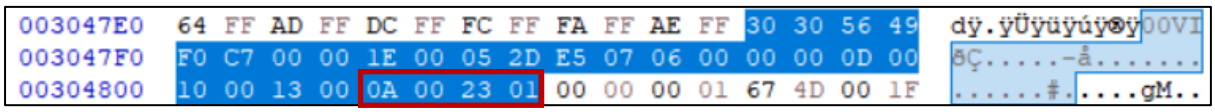


[그림 3] 00VI에 해당하는 청크 예시 카빙

또한, 01VI도 카빙을 진행해보면 위 그림과 같이 비디오 영역의 데이터임을 확인할 수 있었습니다.



[그림 4] 시간 추정 데이터 - 1

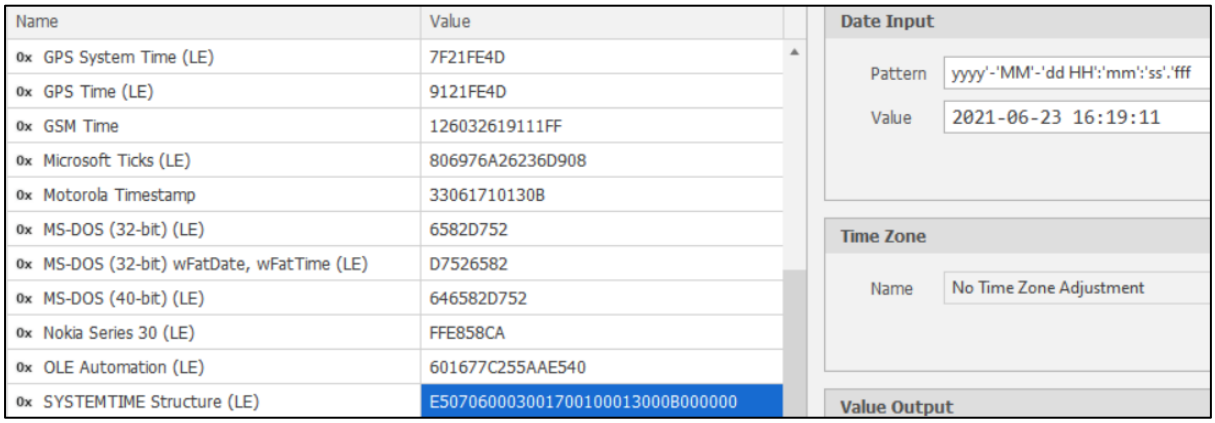


[그림 5] 시간 추정 데이터 - 2

그리고 그림 4와 그림 5를 통해 다음 00VI 청크를 확인할수록 특정 영역의 값이 1씩 증가함을 확인하였고, 시간 관련 데이터라고 판단하였습니다.

[그림 6] 예시 시간 정보

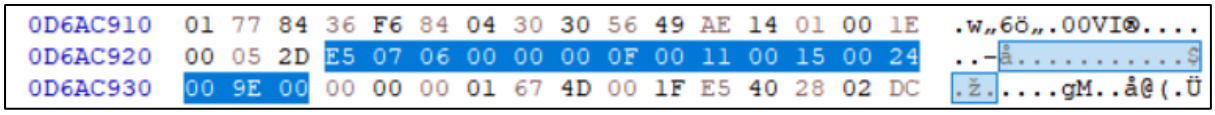
교차 검증을 위해 ffmpeg를 통해 주어진 파일을 mp4로 변환하고, kmplayer로 해당 mp4 영상을 살펴보았습니다. 그 이유는 주어진 img 파일은 프레임이 교차되어 있기 때문에 플레이어로 재생하면 화면이 깨지기 때문입니다. 따라서, 일시정지하고 이동하여 화면 왼쪽 하단에 보이는 시간정보를 토대로 Dcode에서 time encoding을 수행해보았습니다.



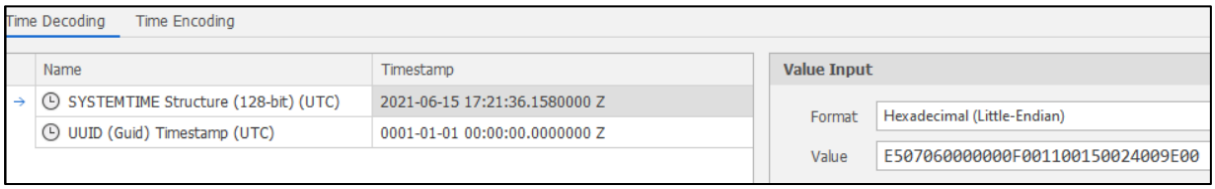
[그림 7] SYSTEMTIME 포맷 확인

위 그림을 통해 SPS NAL unit 이전에 존재하던 데이터는 SYSTEMTIME 구조를 가진 시간 정보였으며, 그림4, 그림5에서 살펴본 데이터는 초에 해당하는 시간정보임을 확인하였습니다.

이를 통해, 00VI 그리고 01VI 시그니처를 가진 데이터 중에서, 1번 문제에서 요구하는 다른 시간 정보를 가진 데이터를 찾을 수 있었습니다.

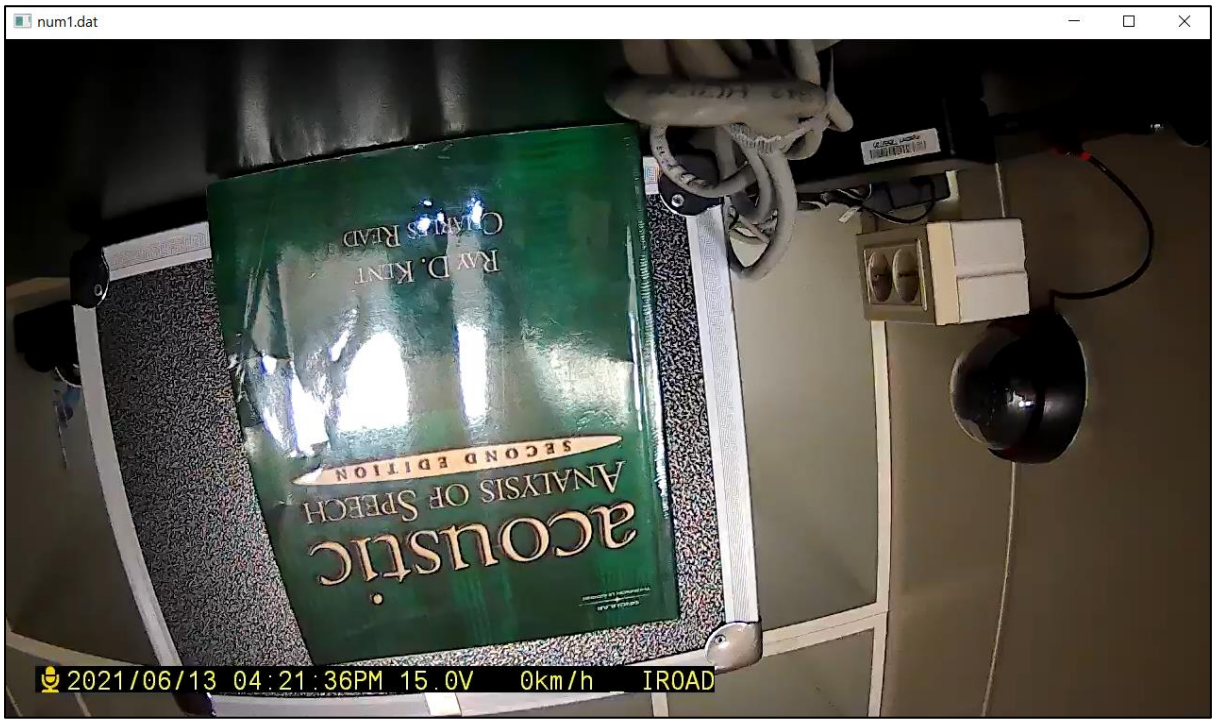


[그림 8] video와 video 프레임 데이터 사이에 기록된 다른 시간 정보



[그림 9] SYSTEMTIME 확인

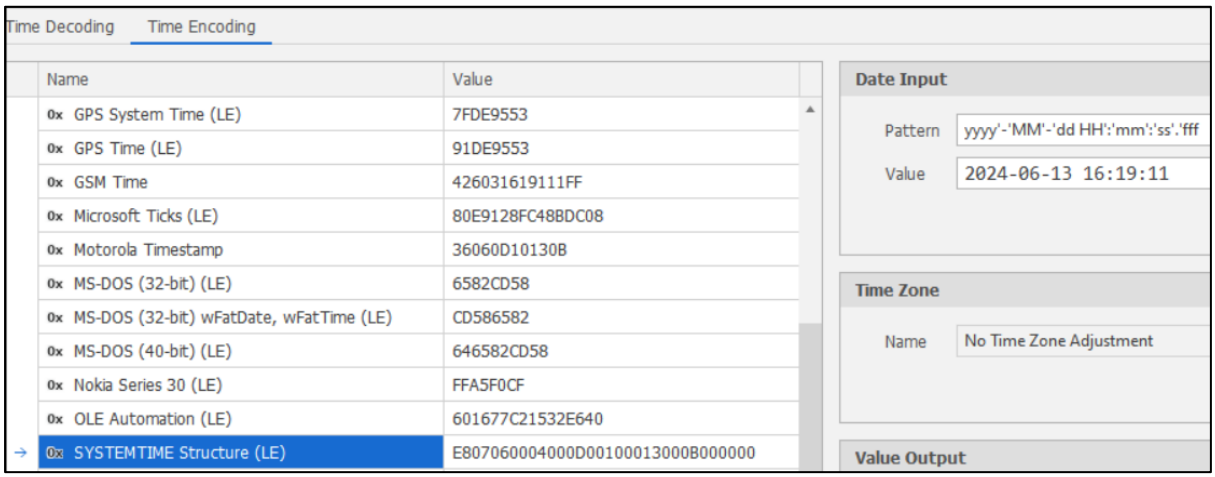
영상에서 확인한 2021-06-14와 달리 해당 시간 정보는 2021-06-15라는 다른 날짜 정보를 가지고 있었음을 확인하였습니다.



[그림 10] 다른 시간 정보를 가진 video file의 책 정보

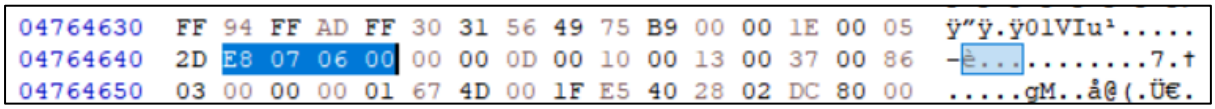
따라서, ffplay를 통해 다른 날짜 정보를 가진 video frame data를 카빙해서 확인해보면 1번에서 요구하는 책 제목은 **"acoustic ANALYSIS OF SPEECH second edition – RAY D. KENT(Charles READ)"**임을 파악할 수 있습니다.

2. Submit the title of the book containing recorded video time with time information from the year 2024 (The time information of the video is located at the beginning of the video data). (100 points)

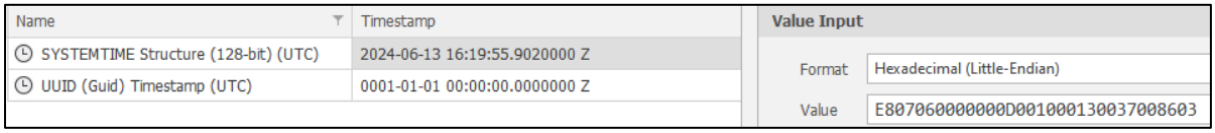


[그림 11] 2024년에 해당하는 SYSTEMTIME Structure 확인

2번 문제도 1번 문제와 유사하게 해결이 가능했습니다. Dcode를 통해 time encoding에 넣는 연도를 2024로 설정하고 보면, SYSTEMTIME에서 0x7E8(2024) 값이 설정된 것을 확인할 수 있습니다. 따라서, 주어진 img 파일에서 "E8 07 06" 에 해당하는 hex값을 검색해서 보았습니다.

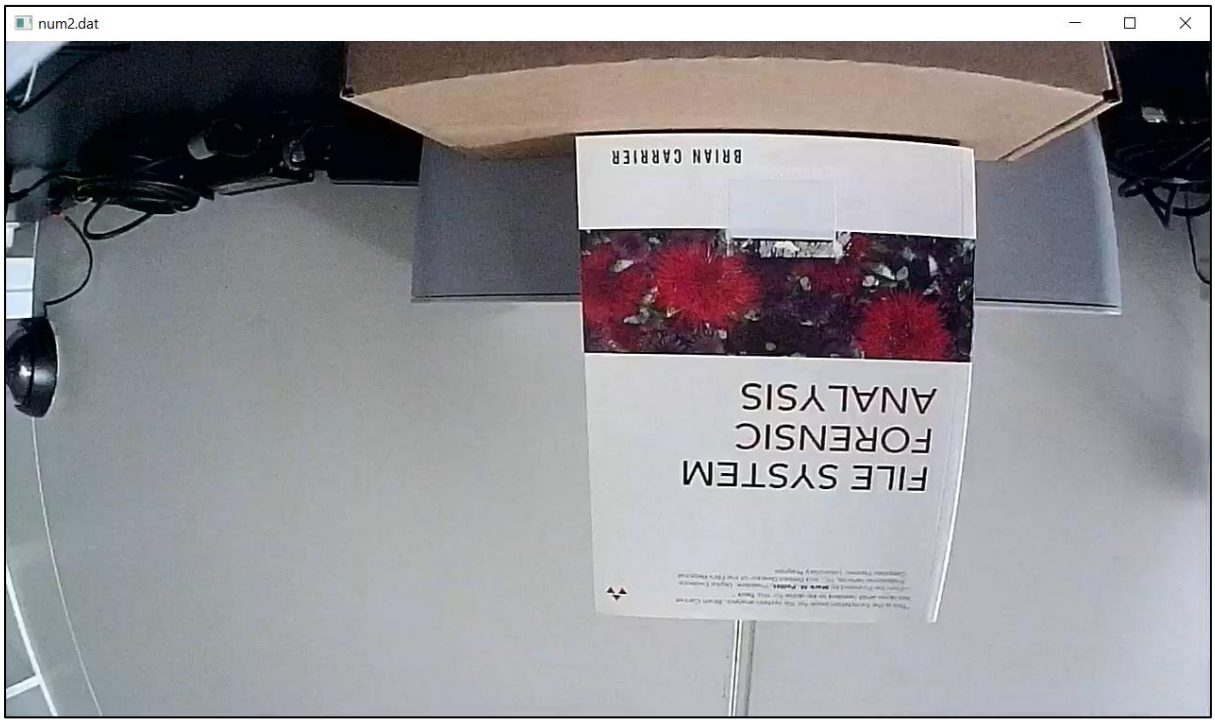


[그림 12] "E8 07 06"으로 시작하는 데이터 확인



[그림 13] 시간 정보 확인

0x4764635에 해당하는 01VI 시그니처를 가진 video frame data에서 "E8 07 06"으로 시작하는 time information을 확인할 수 있었고, 이는 2024-06-13 16:19:55.902 라는 시간 정보를 나타내고 있었습니다.



[그림 14] 2024년 시간 정보를 가지는 video file의 책 정보

따라서, 카빙을 통해 해당 video frame data에서 확인가능한 책의 **제목은 "FILE SYSTEM FORENSIC ANALYSIS – BRIAN CARRIER"**임을 파악할 수 있습니다.