152 – Detect illegal video

Team Information

Team Name : ISEGYE_IDOL

Team Member : Eungchang Lee, Sojeong Kim, Mingyu Seong, Donghyun HA

Email Address : dfc-isegyeidol@googlegroups.com

Instructions

Description You have obtained a smartphone of a suspect who watched the illegal video. Find traces and information of the video from the smartphone data.

Target	Hash (MD5)
illegal.zip	E5D758041F60F4EC1A7A2C6EBD5CECBF

Questions

Please solve all problems based on UTC+9 time zone.

1) Find the file name of the illegal video. (25 points)

2) Find the time that the suspect watched the illegal video. (25 points)

3) Find a specific time and location where the illegal video was recorded. (100 points)

Teams must:

- Develop and document the step-by-step approach used to solve this problem to allow another examiner to replicate team actions and results.
- Specify all tools used in deriving the conclusion(s).

Tools used:

Name:	SQLite Browser	Publisher:	Digital Ocean
Version:	3.12.2		
URL:	https://sqlitebrowser.org/		

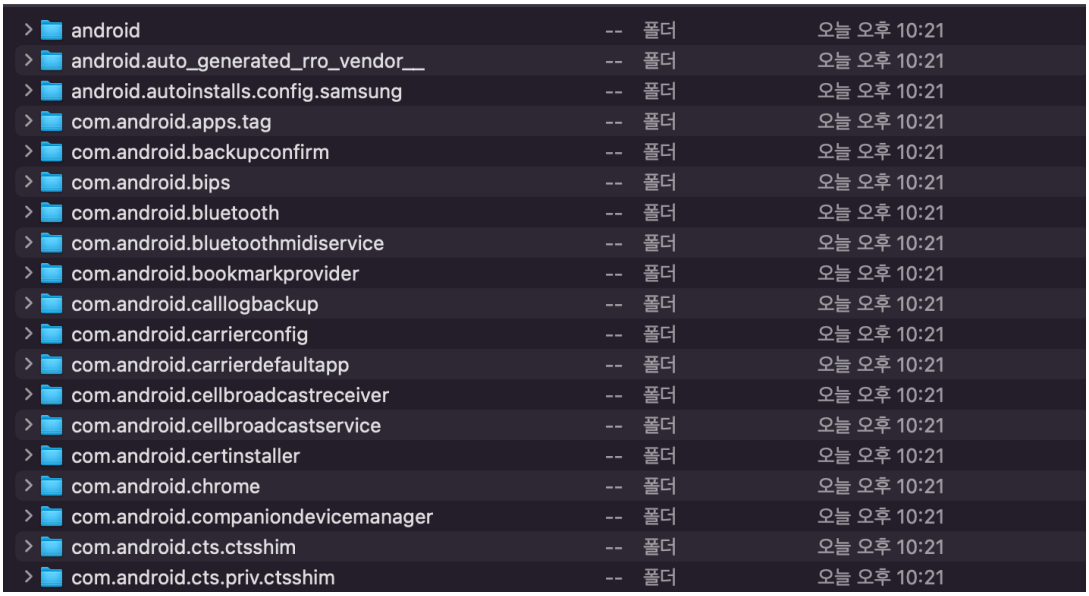
Name:	DCode	Publisher:	Digital Detective
Version:	4.02		
URL:	https://www.digital-detective.net/		

Name:	METADATA2GO	Publisher:	QaamGo Web
Version:	-		
URL:	https://www.metadata2go.com/		

Step-by-step methodology:

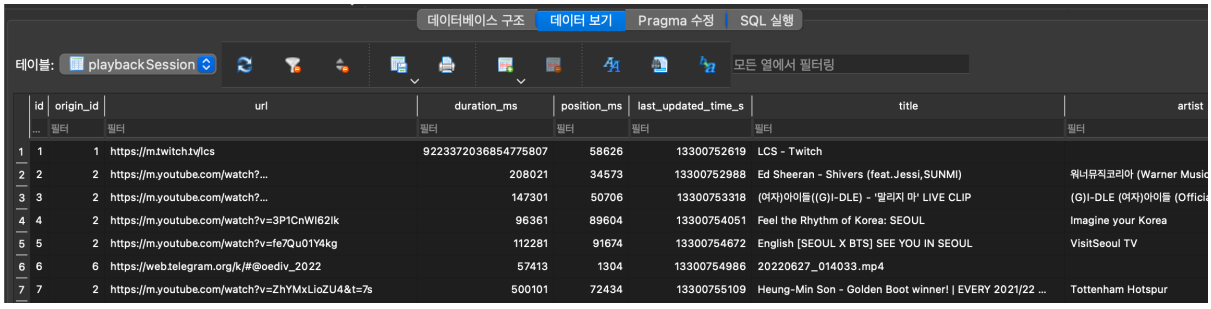
1) Find the file name of the illegal video. (25 points)

주어진 문제를 살펴보게 되면, 안드로이드 어플리케이션 패키지와 그에 대응되는 어플리케이션 사용 데이터가 포함되어 있음을 확인할 수 있다.



[그림 1] 문제 파일 구성

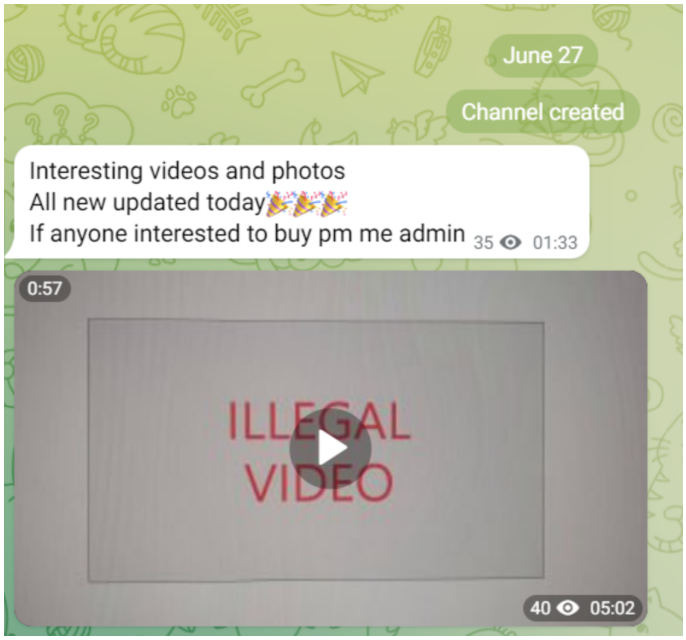
위의 문제에서 언급한 불법적인 비디오의 존재 여부를 탐색하기 위해, 여러 어플리케이션 패키지에 해당하는 아티팩트에 (Android, Google Chrome, Telegram, …) 대해 조사를 수행하였다.



[그림 2] 구글 크롬 미디어 히스토리 파일 조회 결과

그 결과, 구글 크롬에서 사용되는 **"com.android.history\app_chromes\Default\Media History"** 파일, 미디어 히스토리[1]에서 **특정 텔레그램 채널 (@oediv_2022)**에 접속하여 동영상을 시청한 사실을 파악할 수 있었다.

[1] https://kyl3song.github.io/artifacts/NEW-Artifact-of-Chrome-Browser-(Media-History)-part-1/



[그림 3] 텔레그램 채널 접속 결과

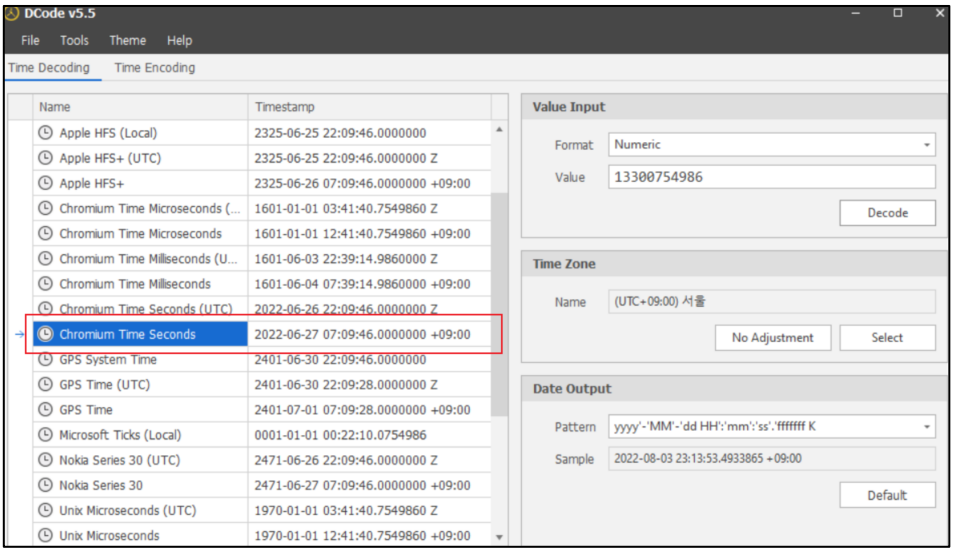
접속한 채널을 방문한 결과, **불법적인 영상이라고 표시된 짧은 영상**을 업로드하고 관심이 있다면 연락을 달라는 취지의 내용이 적힌 것을 확인할 수 있었다.

불법적인 영상이라고 판단된 영상에 대한 이름을 확인하기 위해 채널에 올라온 영상 파일을 다운로드해보고, 크롬 미디어 히스토리에 시청한 것으로 기록된 (“title” 컬럼”) 파일을 교차 검증하였다. 그 결과, 확인된 불법적인 영상의 파일 명은 **“20220627_014033.mp4”**이다.

2) Find the time that the suspect watched the illegal video. (25 points)

용의자가 불법적인 영상을 시청한 시각을 알기 위해서는 위의 사항과 동일하게 구글 크롬의 미디어 히스토리 데이터를 참고해야 한다.

playbackSession 테이블의 last_updated_time_s 컬럼은 마지막으로 업데이트 된 시청 시간을 뜻하며, DB에 저장된 시간은 Chromium Time이므로 이를 DCode 도구로 아래와 같이 변환하였다.

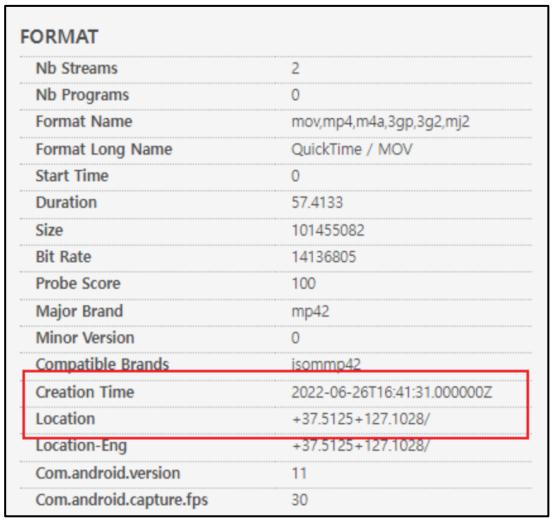


[그림 4] 시간정보 변환

DB에 저장된 원본 값은 13300754986으로 이를 변환하면 “**2022-06-27 07:09:46 (KST)**”이다.

3) Find a specific time and location where the illegal video was recorded. (100 points)

비디오가 촬영된 시각과 장소를 확인하기 위해서는 MP4 파일의 메타데이터를 확인하여야 한다. 불법적인 비디오 파일로 추정되는 파일을 METADATA2GO로 조회한 결과 **"Creation Time"과 "Location"** 데이터를 발견할 수 있었다. 추가로 파일명과 찍은 시간이 58초 가량 차이 나는 이유는 동영상 길이가 58초이기 때문임. 파일명은 동영상을 찍기 시작한 시간이며, 동영상 촬영을 완료한 시간은 MP4 메타데이터인 **"Creation Time"**으로 남는다. 즉 촬영이 완료된 시각은 **"2022-06-27 01:41:31 (KST)"**이다.

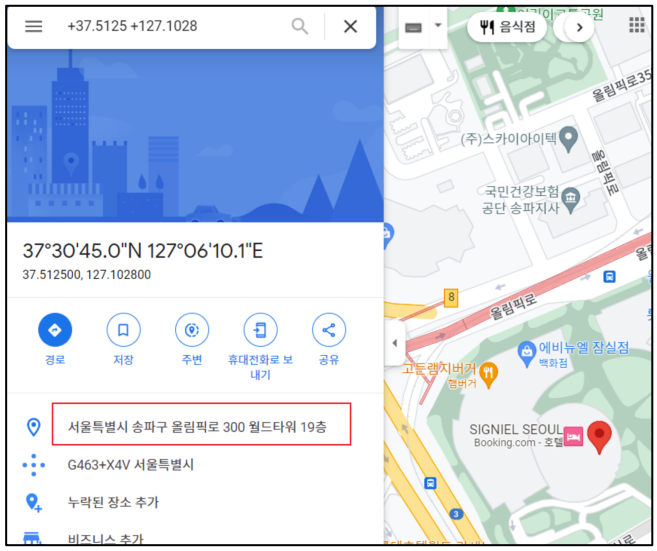


FORMAT

Nb Streams	2
Nb Programs	0
Format Name	mov,mp4,m4a,3gp,3g2,mj2
Format Long Name	QuickTime / MOV
Start Time	0
Duration	57.4133
Size	101455082
Bit Rate	14136805
Probe Score	100
Major Brand	mp42
Minor Version	0
Compatible Brands	isommp42
Creation Time	2022-06-26T16:41:31.000000Z
Location	+37.5125+127.1028/
Location-Eng	+37.5125+127.1028/
Com.android.version	11
Com.android.capture.fps	30

[그림 5] 메타데이터 분석 도구를 통해 조회한 촬영 및 장소 정보

장소는 **"37.5125 / 127.1028"**에 해당하는 좌표 값임을 확인할 수 있었으며, 구글 지도를 통해 위 장소를 검색한 결과, **"서울특별시 송파구 올림픽로 300 월드타워 19층"**임을 확인할 수 있었다.



[그림 6] 좌표에 기반한 위치 정보 조회