105 – Where were you

Team Information

Team Name : LuckyVicky

Team Member : Eungchang Lee, Hyun Yi, Juho Heo, Dongkyu Lee

Email Address : dfc_luckyvicky@googlegroups.com

Instructions

Description The given file is a video submitted by the suspect as evidence to prove an alibi of being in Naju, South Korea, at the time of the incident.

Target	Hash (MD5)
IMG_9649.MOV	d68435d4607a5c58c13763292fd857b1

Questions

- Prove the authenticity of the submitted video. (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).

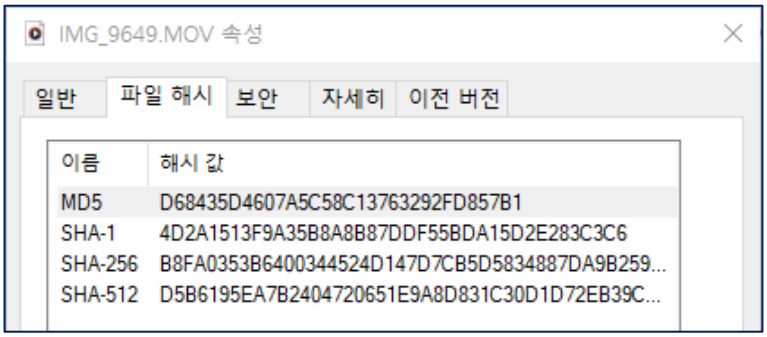
Tools used:

Name:	Hashtab	Publisher:	Implbits Software
Version:	V6.0.0		
URL:	http://implbits.com		

Name:	ExifTool	Publisher:	Phil Harvey
Version:	12.96		
URL:	https://exiftool.org/		

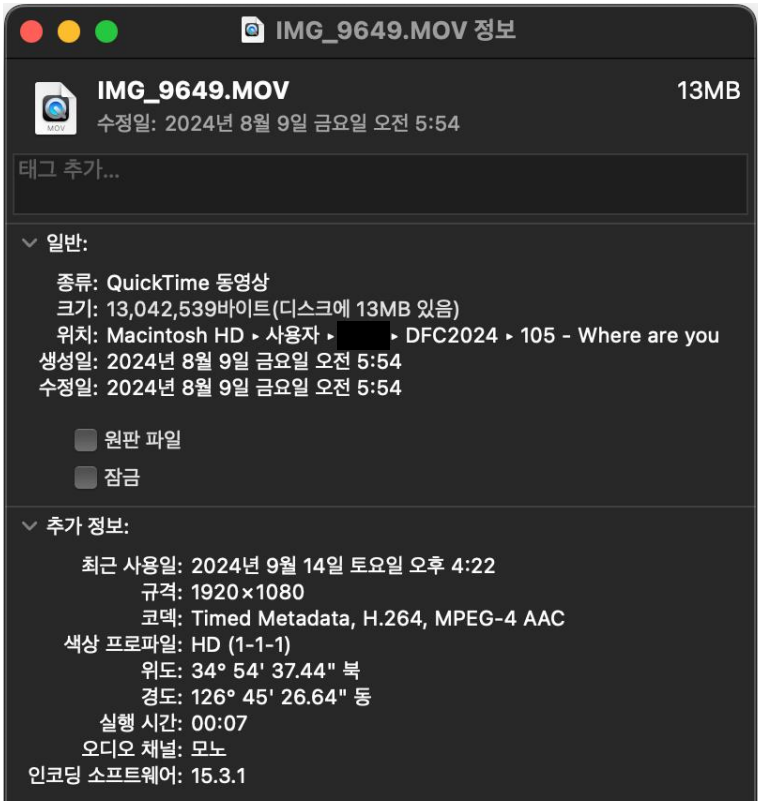
Name:	Kaleidoscope	Publisher:	Leitmotif
Version:	5.1 (6583)		
URL:	https://kaleidoscope.app/		

Step-by-step methodology:



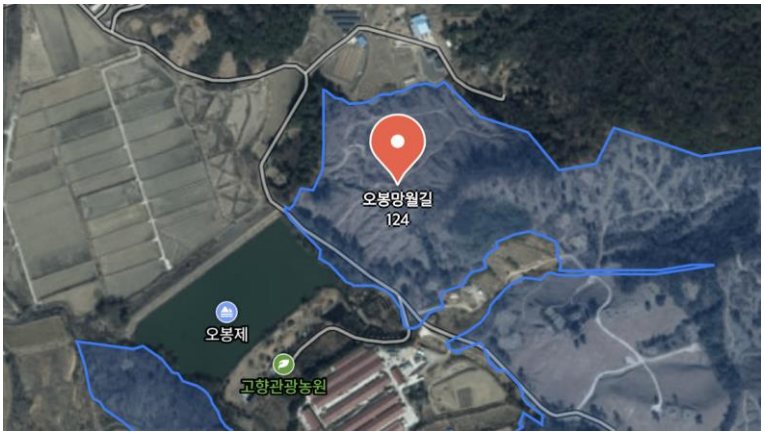
[그림 1] IMG_9649.MOV 파일의 해시 값

분석 대상 파일에 대한 MD5 해시 값이 일치함을 확인하였습니다.



[그림 2] IMG_9649.MOV 파일 정보

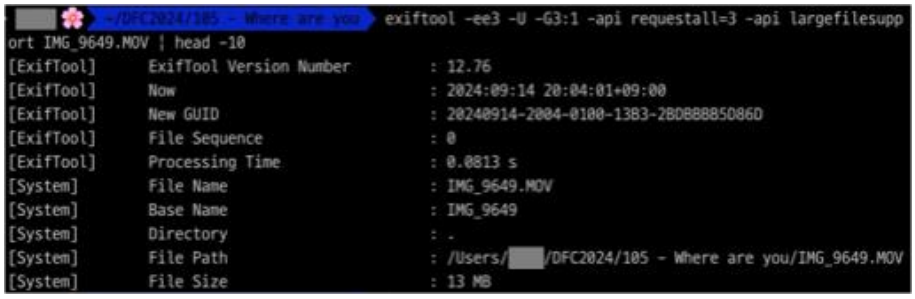
분석 대상 파일은 "IMG_9649.MOV"라는 이름의 QuickTime 동영상 파일이며, 위치 정보를 포함한 메타데이터가 포함되어 있음을 확인할 수 있습니다.



[그림 3] 메타데이터에 기록된 위치 정보의 실제 위치

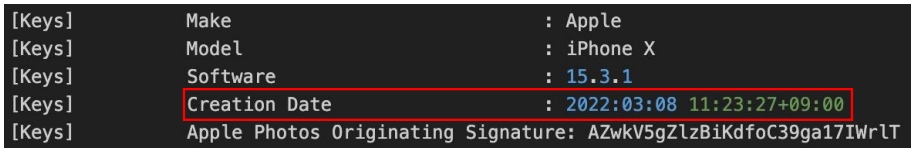
메타데이터에 포함된 위치 정보를 네이버 지도로 검색한 결과, 해당 주소는 '전라남도 나주시 세지면 오봉망월길 124'로 확인되었습니다.

다음부터는 파일 내 메타데이터에 기록된 정보의 진위여부에 대해 서술합니다.

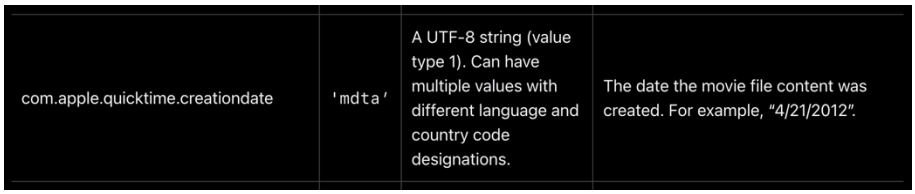


[그림 4] ExifTool를 사용하여 메타데이터 추출

우선 ExifTool을 사용하여 파일에서 추출 가능한 모든 메타데이터를 수집하였습니다.

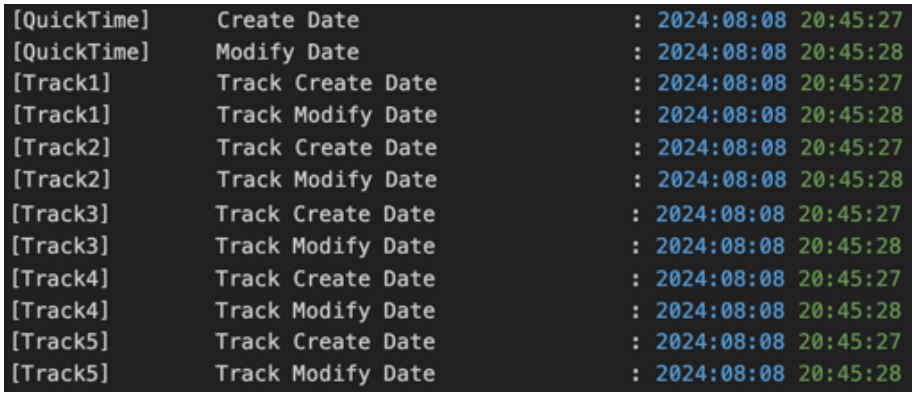


[그림 5] IMG_9649.MOV 영상 생성 시각



[그림 6] Creation Date에 대한 Apple Developer Documentation 설명[1]

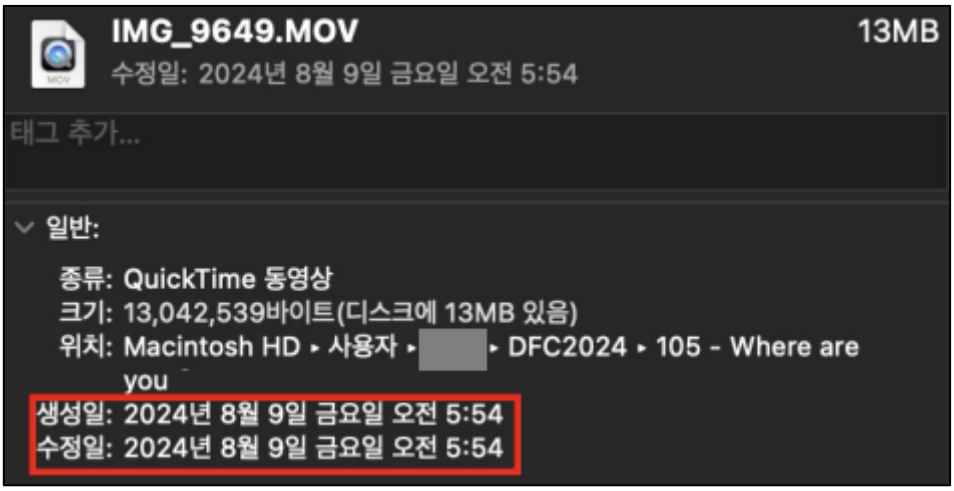
Apple의 QuickTime 파일 형식 문서에 따르면, com.apple.quicktime.creationdate 메타데이터 키는 QuickTime 영상이 생성된 날짜를 기록하는 데 사용됩니다. 즉, 해당 영상은 2022년 3월 8일 11시 23분 27초(KST)에 iPhone X로 촬영된 영상임을 알 수 있습니다.



[그림 7] QuickTime 및 각 Track 생성 시각

위 그림을 통해 해당 영상이 사용자의 iPhone에서 공유를 위해 인코딩된 시점이 2024년 8월 9일 05시 45분(KST)임을 확인할 수 있습니다.

[1] https://developer.apple.com/documentation/quicktime-file-format/quicktime_metadata_keys



[그림 8] IMG_9649.MOV 파일의 시간 정보

그러나 IMG_9649.MOV 파일의 생성일 및 수정일은 2024년 8월 9일 05시 54분으로 나타납니다. 이는 인코딩 완료 시점과 약 9분의 시간 차이가 있으며, 사용자가 해당 시간 동안 파일을 수정했을 가능성을 시사합니다.

또한, IMG_9649.MOV 파일의 위치 정보에서 몇 가지 주목할 만한 사항을 발견하였습니다. 다음은 이러한 위치 정보의 주목 사항에 대한 설명입니다.

```
[Keys]          Location Accuracy Horizontal    : 4000.000000
```

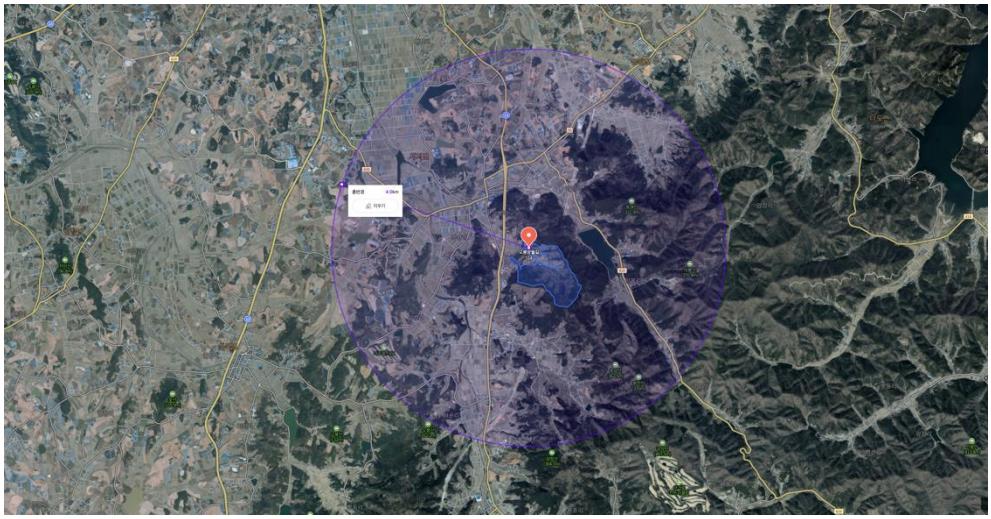
[그림 9] IMG_9649.MOV의 수평 정확도 정보

[그림 10] 수평 정확도 메타데이터 정보[2]

해당 파일에는 위치 정보의 수평 정확도를 나타내는 com.apple.quicktime.location.accuracy.horizontal 메타데이터가 포함되어 있으며, 이를 통해 위치 정보의 오차 범위를 확인할 수 있습니다.

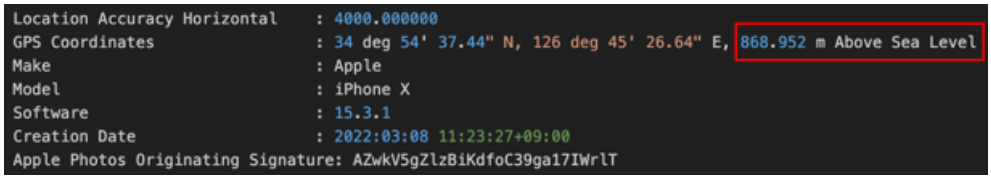
이 영상의 위치 정보의 수평 정확도는 4,000m로 큰 오차 범위를 가지고 있습니다.

[2] https://developer.apple.com/documentation/avfoundation/avmetadataidentifierquicktimemetadatalocationhorizontalaccuracyinmeters?language=objc



[그림 11] 지도상 오차범위

앞서 확인한 위치 정보 값 (+34.9104, +126.7574)을 기준으로 수평 정확도를 적용하면, 위 그림과 같은 결과를 얻을 수 있습니다.



[그림 12] IMG_9649.MOV에 기록된 해발고도

또한, IMG_9649.MOV 파일의 위치 정보에는 해발 고도(Above Sea Level)도 기록되어 있으며, 영상에 기록된 해발 고도는 약 868m입니다.

[그림 13] V-WORLD에서 측정한 절대고도

국토교통부의 공간정보 오픈플랫폼 지도 서비스인 V-WORLD에서 영상의 위치 정보에 기반하여 절대 고도를 측정한 결과, 위 그림과 같이 약 89m임을 확인할 수 있습니다.

영상의 메타데이터에 기록된 해발 고도는 868m로 나타나지만, 지도를 통해 확인한 절대 고도는 약 89m입니다. 일반적으로 해발 고도와 절대 고도는 큰 차이가 나지 않기 때문에, 이러한 큰 차이는 비정상적입니다.

해발 고도는 평균 해수면을 기준으로 측정된 고도이며, 절대 고도는 지표면을 기준으로 측정됩니다. 절대 고도가 89m라면 해당 지점의 해발 고도도 비슷한 값이어야 합니다. 그러나 868m라는 해발 고도는 실제 지형과 일치하지 않으므로, 메타데이터에 기록된 값이 GPS 신호 수신 오류 또는 기기 설정 오류로 인한 잘못된 값일 가능성이 있습니다.

따라서, 지도를 통해 확인한 절대 고도 89m가 더 정확한 수치로 판단되며, 해당 위치로부터 반경 4km 이내에는 절대 고도가 800m 이상의 지형이 존재하지 않습니다. 이에 따라, 메타데이터에 기록된 해발 고도는 신뢰할 수 없는 정보로 간주됩니다.

[그림 14] 비교용 영상의 위치 정보

[그림 15] V-WORLD에서 측정한 비교용 영상의 절대고도

비교를 위해 촬영한 영상의 위치 정보를 기반으로 V-WORLD에서 절대 고도를 측정한 결과, 위와 같은 차이를 확인할 수 있습니다. 영상에서 기록된 메타데이터와 지도상의 절대 고도 간의 차이는 크게 발생하지 않음을 알 수 있습니다.

현재의 분석 결과를 바탕으로 미루어 볼 때, 해당 비디오의 메타데이터 신뢰성은 매우 낮다고 평가되므로 용의자가 제출한 증거에 대한 진정성 성립이 어렵다고 판단됩니다.