302 – Do not blink

Team Information

Team Name : ForensicGPT

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

Email Address : forensicgpt@googlegroups.com

Instructions

Description Analyze the video and prevent a terrorist attack!

Target	Hash (MD5)
Seoul.mp4	4c4ee9010efd0b056a8143ba1e168dce

Questions

1) When is the attack scheduled? (50 points)
2) What is the cryptographic key is needed to identify the location of the attack? (125 points)
3) Where is the attack scheduled? (125 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:	HxD	Publisher:	Maël Hörz
Version:	2.5.0.0		
URL:	http://www.mh-nexus.de/		

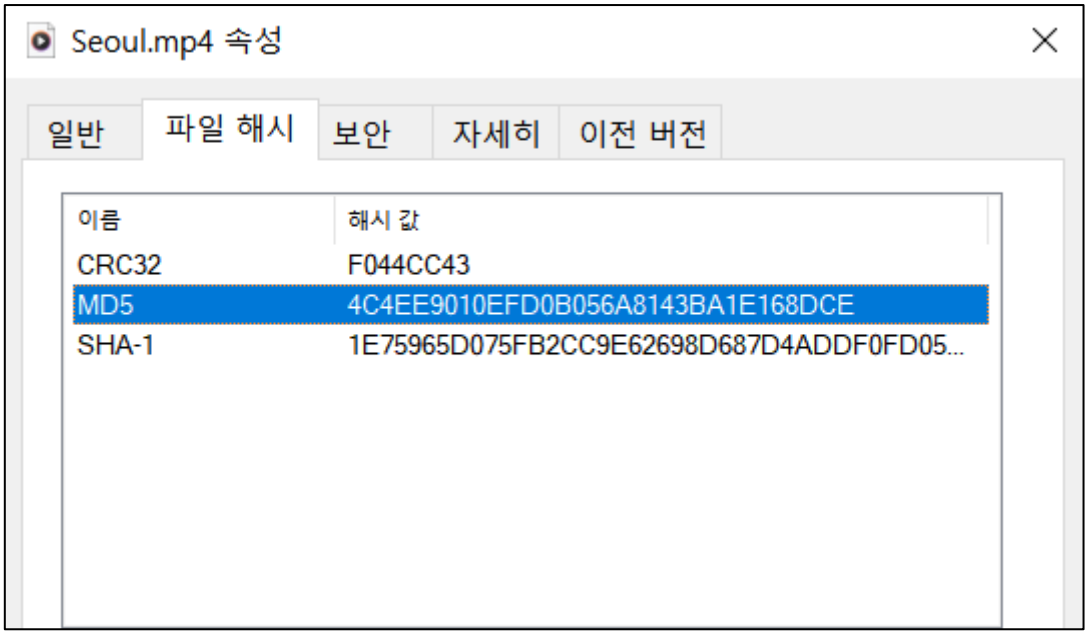
Name:	Mp4 Explorer	Publisher:	CM streaming Technologies
Version:	1.0.1.41163		
URL:	https://mp4-explorer.apponic.com/		

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

Name:	epochconverter	Publisher:	-
Version:	-		
URL:	https://www.epochconverter.com/ldap		

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

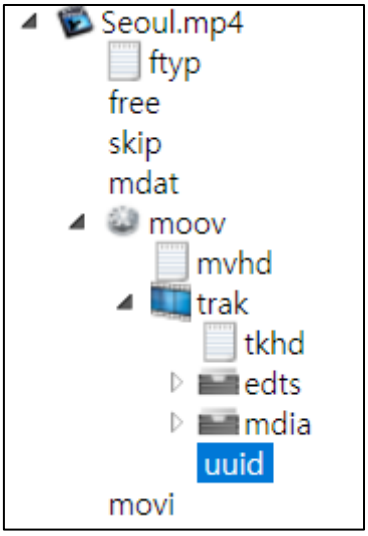
Step-by-step methodology:



[그림 1] 해시 값 확인

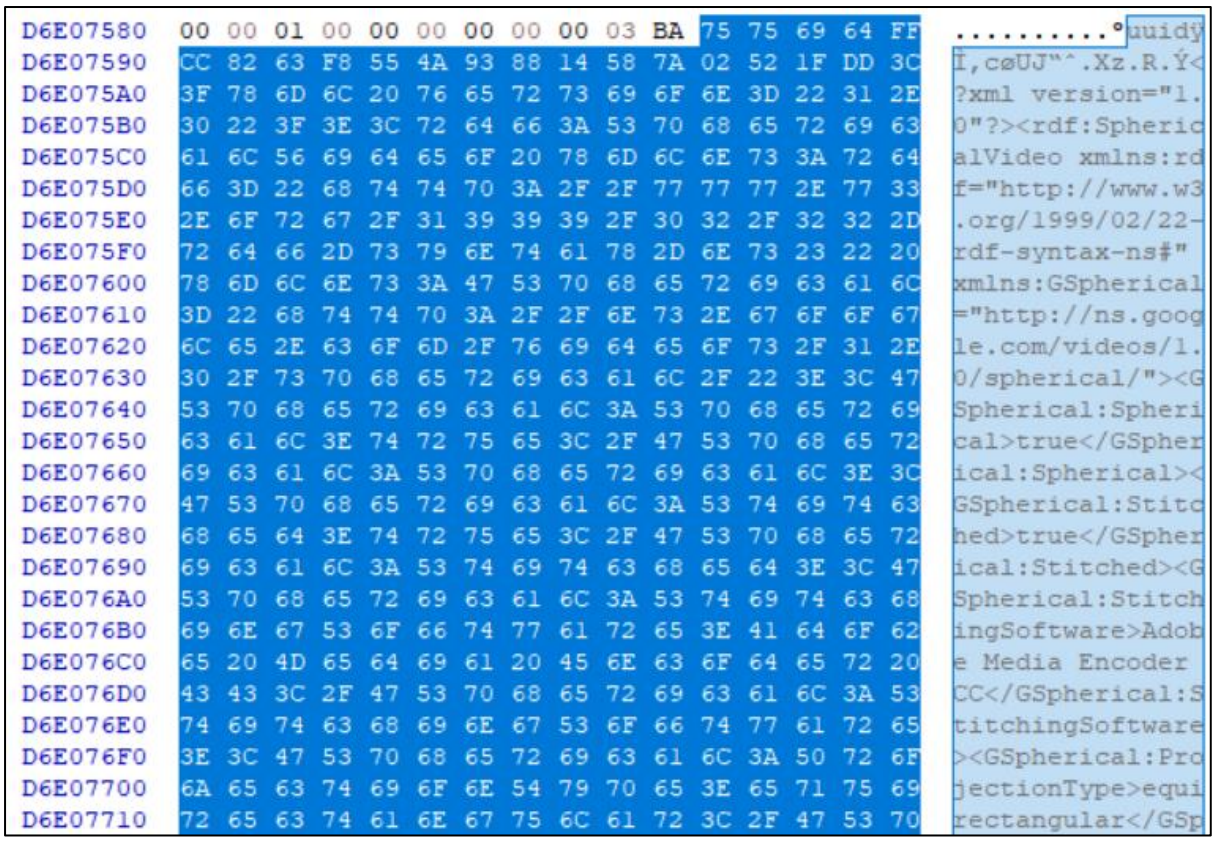
분석에 앞서 주어진 파일의 hash값 비교를 통해 Target 파일 원본임을 확인하였습니다.

1) When is the attack scheduled? (50 points)



[그림 2] Seoul.mp4의 mp4 structure

해당 Seoul.mp4파일은 mp4 explorer로 열어보았을 때 위 그림과 같은 구조를 가지고 있습니다. moov box에 uuid data와 moov box 뒤에 존재하는 movi 데이터가 정상적인 mp4 와 다른 구조라고 생각되어 hxd로 살펴보았습니다.



[그림 3] Seoul.mp4의 uuid 영역

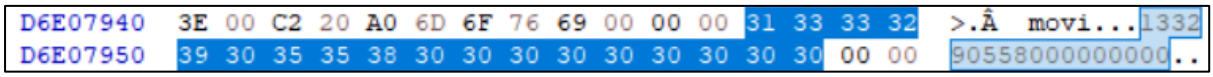
16byte uuid와 특정 XML 메타데이터를 포함하고 있었습니다.

uuid FF CC 82 63 F8 55 4A 93 88 14 58 7A 02 52 1F DD

<?xml version="1.0"?><rdf:SphericalVideo xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"
xmlns:GSpherical="http://ns.google.com/videos/1.0/spherical/"><GSpherical:Spherical>true</GSpherical:Spherical><GSpherical:Stitched>true</GSpherical:Stitched><GSpherical:StitchingSoftware>Adobe Media Encoder CC</GSpherical:StitchingSoftware><GSpherical:ProjectionType>equirectangular</GSpherical:ProjectionType><GSpherical:StereoMode>mono</GSpherical:StereoMode><GSpherical:FullPanoWidthPixels>3840</GSpherical:FullPanoWidthPixels><GSpherical:FullPanoHeightPixels>1920</GSpherical:FullPanoHeightPixels><GSpherical:CroppedAreaImageWidthPixels>3840</GSpherical:CroppedAreaImageWidthPixels><GSpherical:CroppedAreaImageHeightPixels>1920</GSpherical:CroppedAreaImageHeightPixels><GSpherical:CroppedAreaLeftPixels>0</GSpherical:CroppedAreaLeftPixels><GSpherical:CroppedAreaTopPixels>0</GSpherical:CroppedAreaTopPixels></rdf:SphericalVideo>

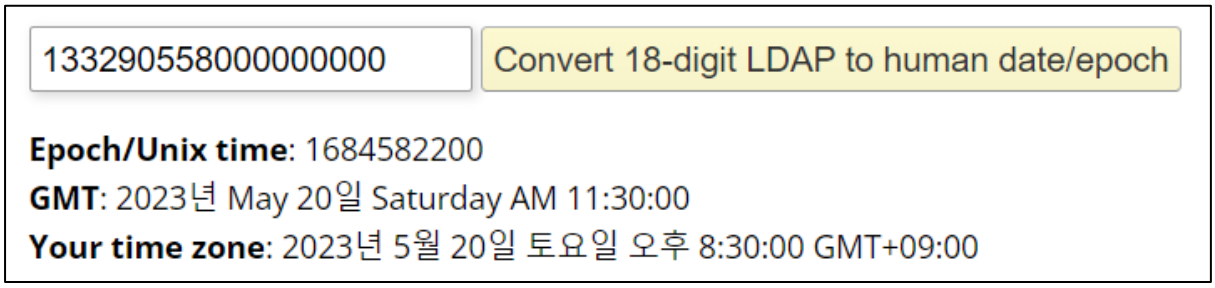
해당 구조는

https://github.com/google/spatial-media/blob/master/docs/spherical-video-rfc.md 에서 확인할 수 있었으며, spherical-video-rfc.md에서도 uuid ffcc8263-f855-4a93-8814-587a02521fdd 형태를 가진다는 것을 알 수 있습니다.



[그림 4] suspicious 18 bytes hex value

uuid와 특정 xml 메타데이터 이후에 존재하는 data에서는 movi라는 파일 시그니처와 특정 18byte data를 확인할 수 있습니다. 이 값은 문제에 기반하여 시간 값 관련 데이터라고 판단하였습니다.



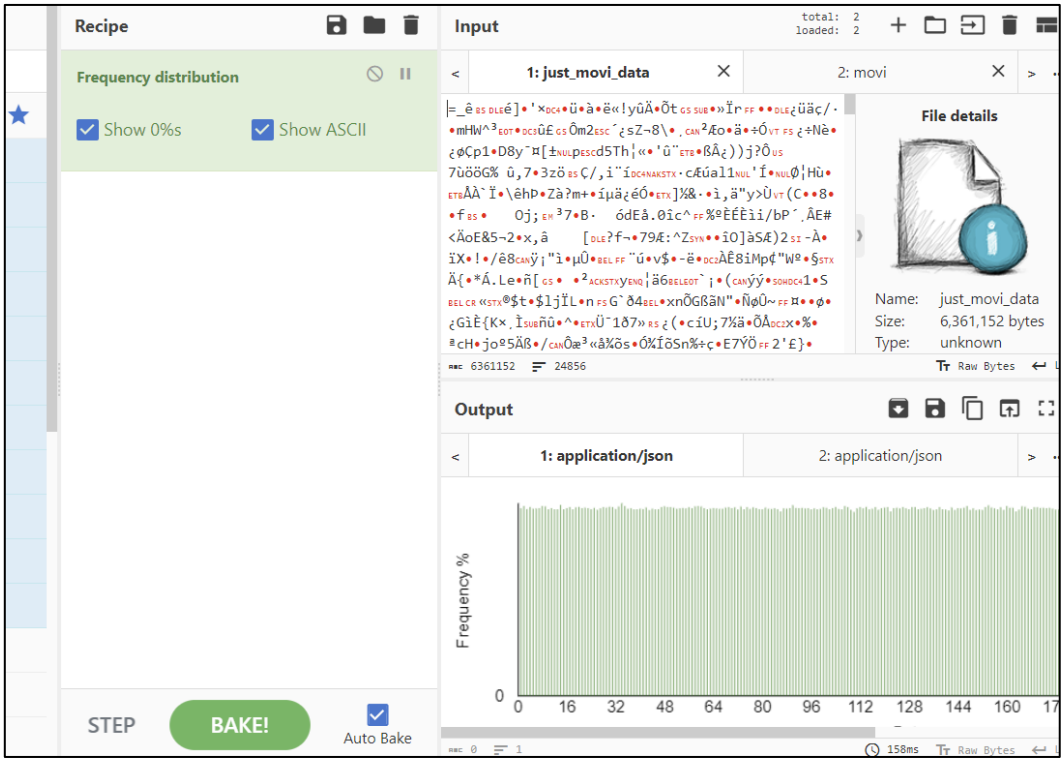
[그림 5] ldap/Windows File time timestamp 변환

epoch converter online에서 timestamp 변환 결과 계획된 공격 시각은 **2023년 5월 20일 토요일 오후 08:30:00 GMT+09:00** 으로 판단하였습니다.

2) What is the cryptographic key is needed to identify the location of the attack? (125 points)

[그림 6] movi file signature 이후 주어진 ascii 값

timestamp 값 뒤에 존재하는 12,722,304 바이트의 ascii data가 의심스럽다고 판단하였습니다.

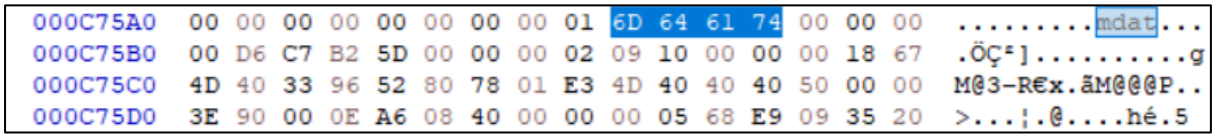


[그림 7] data frequency distribution

일반적으로 데이터 히스토그램을 살펴볼 때 균일한 분포를 이루고 있으면 암호화되어 있는 데

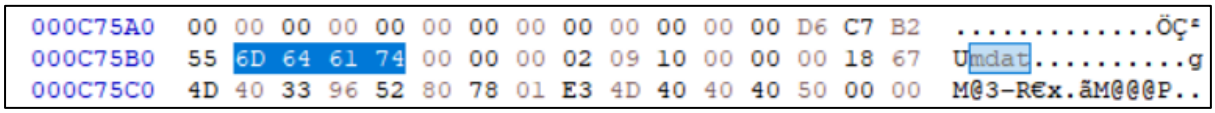
이터로 유추해볼 수 있습니다. 이를 토대로 암호화 키를 찾기 위한 분석을 진행하였습니다.

우선, 주어진 Seoul.mp4의 moov box에서 stco 영역에서 가르키고 있는 첫 mdat offset이 816,565(hex : C75B5)인 것을 확인했습니다.



[그림 8] 원본 Seoul.mp4의 mdat box구조

해당 offset을 따라가면, 0xC75B5 앞에 mdat이 위치하지 않는 것을 확인하였고, 다음 그림과 같이 사이즈와 mdat signature 위치를 수정해주었습니다.



[그림 9] offset 수정 후 mdat box 구조

하지만, 이후 본 팀은 cryptographic key를 찾는 과정에서 tcsteg, frame 추출(fps 변경 후 추출 등), avi변경 등의 다양한 방법을 시도해보았지만 key 값을 찾지 못해서 아쉽게도 분석을 마무리하였습니다.

3) Where is the attack scheduled? (125 points)