

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/		

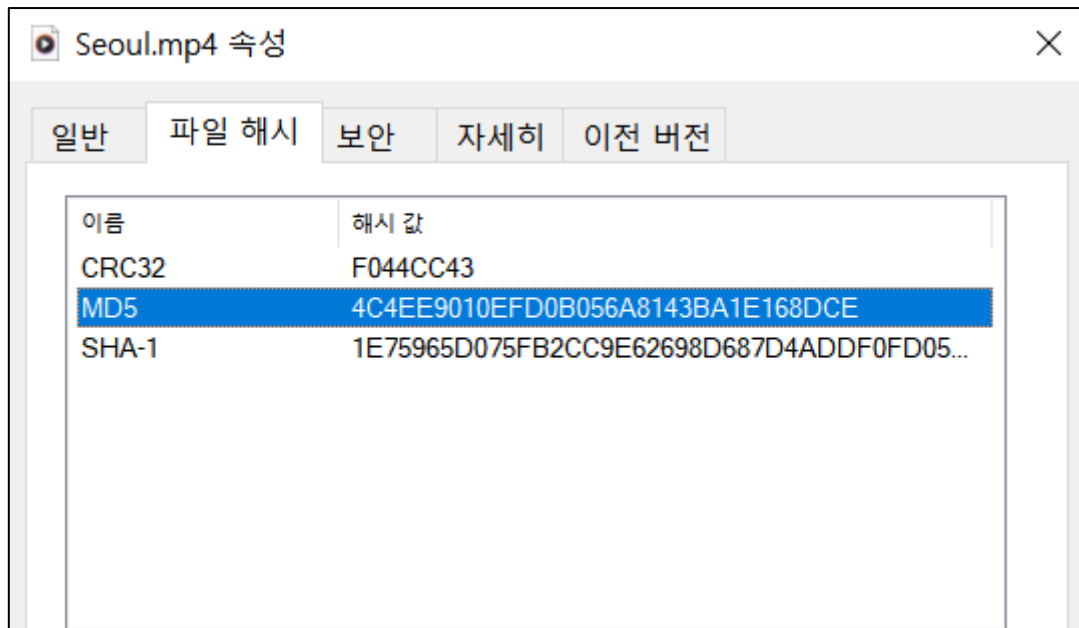
Name:	Mp4 Explorer	Publisher:	CM streaming Technologies
Version:	1.0.1.41163		
URL:	https://mp4-explorer.apponic.com/		

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		

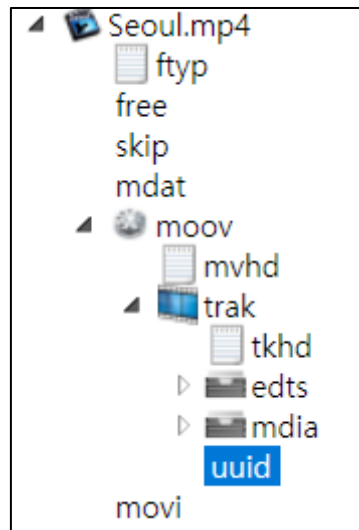
Step-by-step methodology:



[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.

D6E07580	00 00 01 00 00 00 00 00 00 03 BA 75 75 69 64 FF°uui
D6E07590	CC 82 63 F8 55 4A 93 88 14 58 7A 02 52 1F DD 3C	I,cøUJ^^.Xz.R.Ý<
D6E075A0	3F 78 6D 6C 20 76 65 72 73 69 6F 6E 3D 22 31 2E	?xml version="1.
D6E075B0	30 22 3F 3E 3C 72 64 66 3A 53 70 68 65 72 69 63	0"?><rdf:Spheric
D6E075C0	61 6C 56 69 64 65 6F 20 78 6D 6C 6E 73 3A 72 64	alVideo xmlns:rd
D6E075D0	66 3D 22 68 74 74 70 3A 2F 2F 77 77 77 2E 77 33	f="http://www.w3
D6E075E0	2E 6F 72 67 2F 31 39 39 39 2F 30 32 2F 32 32 2D	.org/1999/02/22-
D6E075F0	72 64 66 2D 73 79 6E 74 61 78 2D 6E 73 23 22 20	rdf-syntax-ns#"
D6E07600	78 6D 6C 6E 73 3A 47 53 70 68 65 72 69 63 61 6C	xmlns:GSpherical
D6E07610	3D 22 68 74 74 70 3A 2F 2F 6E 73 2E 67 6F 6F 67	="http://ns.goog
D6E07620	6C 65 2E 63 6F 6D 2F 76 69 64 65 6F 73 2F 31 2E	le.com/videos/1.
D6E07630	30 2F 73 70 68 65 72 69 63 61 6C 2F 22 3E 3C 47	0/spherical/"><G
D6E07640	53 70 68 65 72 69 63 61 6C 3A 53 70 68 65 72 69	Spherical:Spheri
D6E07650	63 61 6C 3E 74 72 75 65 3C 2F 47 53 70 68 65 72	cal>true</GSpher
D6E07660	69 63 61 6C 3A 53 70 68 65 72 69 63 61 6C 3E 3C	ical:Spherical><
D6E07670	47 53 70 68 65 72 69 63 61 6C 3A 53 74 69 74 63	GSpherical:Stitc
D6E07680	68 65 64 3E 74 72 75 65 3C 2F 47 53 70 68 65 72	hed>true</GSpher
D6E07690	69 63 61 6C 3A 53 74 69 74 63 68 65 64 3E 3C 47	ical:Stitched><G
D6E076A0	53 70 68 65 72 69 63 61 6C 3A 53 74 69 74 63 68	Spherical:Stitch
D6E076B0	69 6E 67 53 6F 66 74 77 61 72 65 3E 41 64 6F 62	ingSoftware>Adob
D6E076C0	65 20 4D 65 64 69 61 20 45 6E 63 6F 64 65 72 20	e Media Encoder
D6E076D0	43 43 3C 2F 47 53 70 68 65 72 69 63 61 6C 3A 53	CC</GSpherical:S
D6E076E0	74 69 74 63 68 69 6E 67 53 6F 66 74 77 61 72 65	titchingSoftware
D6E076F0	3E 3C 47 53 70 68 65 72 69 63 61 6C 3A 50 72 6F	><GSpherical:Pro
D6E07700	6A 65 63 74 69 6F 6E 54 79 70 65 3E 65 71 75 69	jectionType>equi
D6E07710	72 65 63 74 61 6E 67 75 6C 61 72 3C 2F 47 53 70	rectangular</GSp

[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.

D6E07940	3E 00 C2 20 A0 6D 6F 76 69 00 00 00	31 33 33 32	>.Å movi...1332
D6E07950	39 30 35 35 38 30 30 30 30 30 30 30	00 00	9055800000000000..

[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.

133290558000000000	Convert 18-digit LDAP to human date/epoch
Epoch/Unix time: 1684582200	
GMT: 2023년 May 20일 Saturday AM 11:30:00	
Your time zone: 2023년 5월 20일 토요일 오후 8:30:00 GMT+09:00	

[그림 5] ldap/Windows File time timestamp 변환

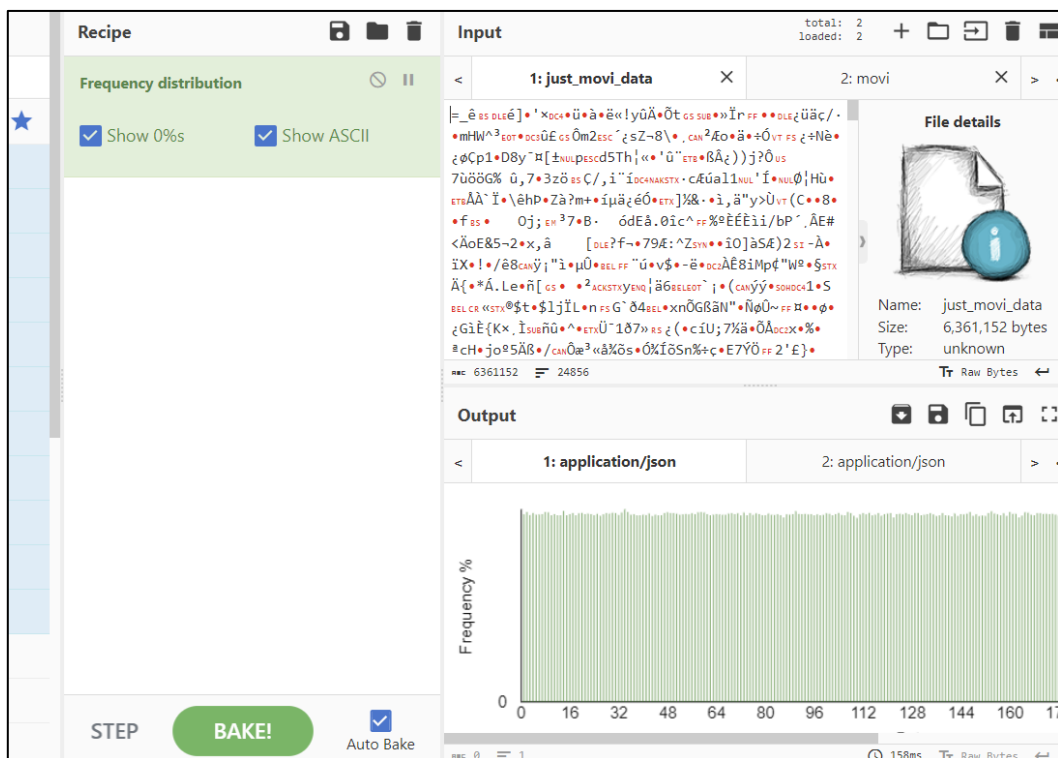
epoch converter online에서 timestamp 변환 결과 계획된 공격 시각은 **2023년 5월 20일 토요일 오후 08:30:00 GMT+09:00** 으로 판단하였습니다.

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

D6E07960	00	33	64	35	66	65	61	30	38	31	30	65	39	35	64	38	.3d5fea0810e95d8
D6E07970	35	32	37	64	37	31	34	38	35	66	63	38	61	65	30	38	527d71485fc8ae08
D6E07980	63	65	62	61	62	32	31	37	39	66	62	63	34	38	30	64	cebab2179fbc480d
D6E07990	35	37	34	31	64	31	61	39	61	62	62	63	66	37	32	30	5741d1a9abbcf720
D6E079A0	63	38	31	39	37	31	30	62	66	66	63	65	34	65	37	32	c819710bfffce4e72
D6E079B0	66	62	37	39	61	36	64	34	38	35	37	35	65	62	33	30	fb79a6d48575eb30
D6E079C0	34	37	66	31	33	66	62	61	33	31	64	64	34	36	64	33	47f13fba31dd46d3
D6E079D0	32	31	62	62	34	62	66	37	33	35	61	61	63	33	38	35	21bb4bf735aac385
D6E079E0	63	38	62	62	38	31	38	62	32	63	36	36	66	37	66	65	c8bb818b2c66f7fe
D6E079F0	34	38	38	66	37	64	33	30	62	31	63	62	66	66	37	34	488f7d30b1cbff74
D6E07A00	65	65	38	38	62	62	66	66	38	63	37	37	30	33	31	39	ee88bbff8c770319
D6E07A10	34	34	34	33	38	37	39	61	66	61	34	35	62	62	31	30	4443879afa45bb10
D6E07A20	30	37	30	31	62	36	34	33	35	35	34	36	38	61	36	61	0701b64355468a6a
D6E07A30	62	38	64	32	37	66	62	61	38	31	37	38	30	64	66	63	b8d27fba81780dfc
D6E07A40	32	62	66	32	39	32	39	36	61	33	66	64	34	31	66	33	2bf29296a3fd41f3
D6E07A50	37	66	39	66	36	66	36	34	37	32	35	32	30	66	62	32	7f9f6f6472520fb2
D6E07A60	63	33	37	38	33	33	33	37	61	66	36	30	38	63	37	32	c3783337af608c72

[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

이더로 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.

000C75A0	00 00 00 00 00 00 00 00 01	6D 64 61 74	00 00 00mdat...
000C75B0	00 D6 C7 B2 5D 00 00 00 02	09 10 00 00 00 18 67	.ÖÇ²].....g	
000C75C0	4D 40 33 96 52 80 78 01 E3	4D 40 40 40 50 00 00	M@3-REx.ãM@@@P..	
000C75D0	3E 90 00 0E A6 08 40 00 00	05 68 E9 09 35 20	>...!.@....hé.5	

[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.

000C75A0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 D6 C7 B2ÖÇ²
000C75B0	55 6D 64 61 74 00 00 00 02 09 10 00 00 00 00 18 67	Umdat.....g
000C75C0	4D 40 33 96 52 80 78 01 E3 4D 40 40 40 50 00 00	M@3-REx.ãM@@@P..

[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)