

102 – No more ransom

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 received files encrypted by ransomware for your clients. There are some text files created on PCs infected by ransomware.

Target	Hash (MD5)
enc_files.zip	8591307d3b9a87e7561cb3f2422a839b

Questions

- 1) What are the names of the ransomware that infected clients' PCs? (20 points)
- 2) Decrypt the encrypted files and check the contents of the files. (40 points)
- 3) Calculate the MD5 hash of the decrypted files. (40 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:	AuroraDecrypter	Publisher:	Bleeping Computer
Version:	1.0.2.4		
URL:	https://www.getcryptostopper.com/ransomware-decryptors/		

Name:	BDGandCrabDecryptTool	Publisher:	BitDefender
Version:	-		
URL:	https://www.getcryptostopper.com/ransomware-decryptors/		

Name:	Avg_decryptor_Crypt88	Publisher:	AVG
Version:	1.0.0.86		
URL:	https://www.getcryptostopper.com/ransomware-decryptors/		

Name:	RakhniDecryptor	Publisher:	Kaspersky
Version:	1.32.0.0		
URL:	https://www.getcryptostopper.com/ransomware-decryptors/		

Name:	Exiftool	Publisher:	Phil Harvey
Version:	12.43		
URL:	https://exiftool.org/		

Name:	Hashtab	Publisher:	Implbits Software, LLC
Version:	6.0.0.34		
URL:	https://hashtab.softonic.kr/		

Step-by-step methodology:

- 1) What are the names of the ransomware that infected clients' PCs?
(20 points)

고객들의 PC에 랜섬웨어로 인해 암호화된 파일을 분석하고, 분석을 통해 랜섬웨어의 이름을 파악하고 파일을 복호화 해야 한다.

📄	#RECOVERY_FILES#.txt	2022-05-26 오후 5:52	텍스트 문서 1KB
📄	211104_121252.jpg.Nano	2022-05-26 오후 5:52	NANO 파일 3,869KB
📄	211104_121305.jpg.Nano	2022-05-26 오후 5:52	NANO 파일 3,883KB
📄	211104_121307.jpg.Nano	2022-05-26 오후 5:52	NANO 파일 3,959KB
📄	211104_121321.jpg.Nano	2022-05-26 오후 5:52	NANO 파일 3,768KB
📄	IMG_0210.JPG.KRAB	2022-05-25 오후 2:32	KRAB 파일 1,272KB
📄	IMG_1095.JPG.KRAB	2022-05-25 오후 2:32	KRAB 파일 6,263KB
📄	KRAB-DECRYPT.txt	2022-05-25 오후 2:09	텍스트 문서 8KB
ZIP	Lock.plaque.zip	2022-05-25 오후 3:52	압축(ZIP) 파일 1,945KB
📄	Lock.query.txt	2022-05-25 오후 3:52	텍스트 문서 1KB
JPG	Lock.w_8723.jpg	2022-05-25 오후 3:52	JPG 파일 5,264KB
JPG	Lock.w_8724.jpg	2022-05-25 오후 3:52	JPG 파일 4,011KB
JPG	Lock.w_8725.jpg	2022-05-25 오후 3:52	JPG 파일 3,824KB
JPG	Lock.w_8726.jpg	2022-05-25 오후 3:52	JPG 파일 4,156KB
JPG	origin.jpg	2021-11-04 오후 3:25	JPG 파일 3,869KB
📄	Read@My.txt	2022-05-25 오후 4:09	텍스트 문서 1KB
MP4	tree.mp4.Yatron	2022-05-25 오후 4:09	YATRON 파일 3,577KB
JPG	w_8732.jpg.Yatron	2022-05-25 오후 4:09	YATRON 파일 2,898KB
JPG	w_8733.jpg.Yatron	2022-05-25 오후 4:09	YATRON 파일 2,274KB

[그림 1]. 랜섬웨어로 암호화된 파일 목록

origin.jpg라는 원본 파일을 제외하고, 파일들은 총 4가지의 랜섬웨어에 각각 감염되어 있다.

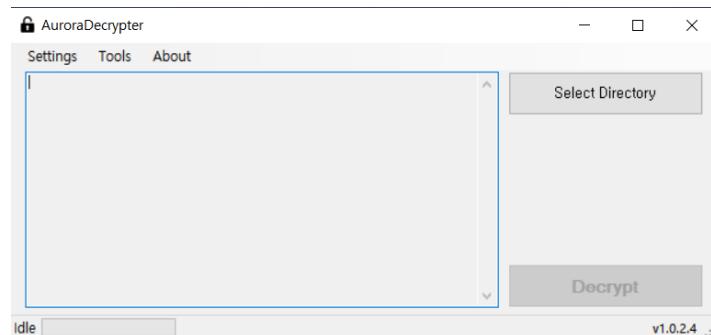
Encrypted File	Ransomware	Ransomnote
211104_121252.jpg.Nano 211104_121305.jpg.Nano 211104_121307.jpg.Nano 211104_121321.jpg.Nano	Aurora	#RECOVERY_FILES#.txt
IMG_0210.JPG.KRAB IMG_1095.JPG.KRAB	Gandcrab	KRAB-DECRYPT.txt
Lock.plaque.zip Lock.query.txt Lock.w8723.jpg Lock.w8724.jpg Lock.w8725.jpg Lock.w8726.jpg	MIRCOP(a.k.a Microcop, Crypt888)	-
tree.mp4.Yatron w_8732.jpg.Yatron w_8733.jpg.Yatron	Yatron	Read@My.txt

[표 1]. Ransomware에 감염된 파일, Ransomware명, Ransomnote

- 2) Decrypt the encrypted files and check the contents of the files. (40 points)

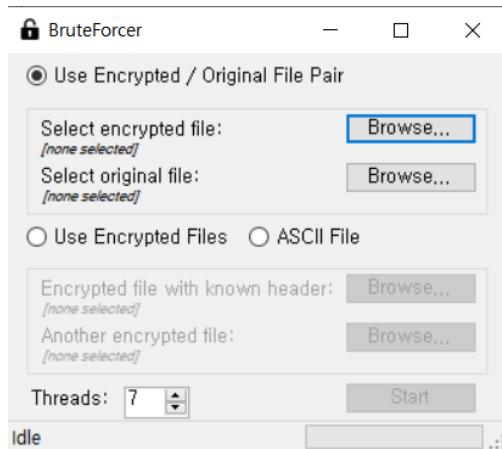
2-1) Aurora Ransomware Decrypt Process

먼저 순서대로 “Nano” 확장자로 암호화된 파일을 복호화 하는 것을 진행했다.



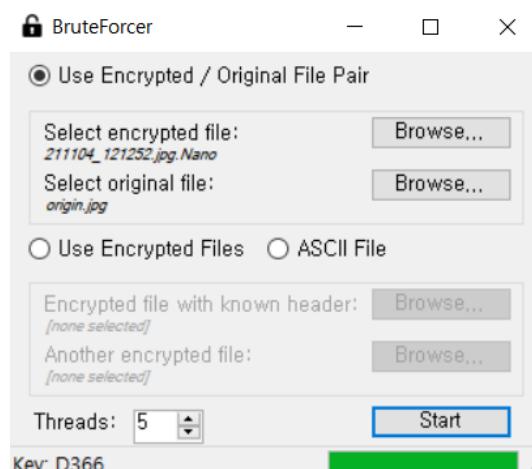
[그림 2]. AuroraDecrypter Tool

암호화된 Nano 파일 복호화를 위해 사용한 상용화 된 툴은 다음과 같다.

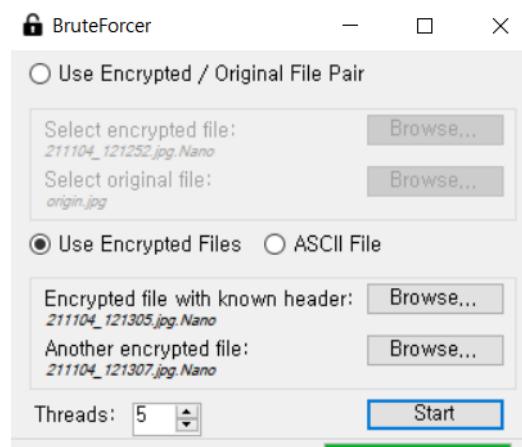


[그림 3]. 키 생성을 위한 BruteForce 기능

Aurora Ransomware을 통해 암호화된 파일을 Decrypt하기 위해서는 Decryption Key가 필요하다. Decryption key를 생성하고 세팅하기 위해서는 Decryptor Tool내에 내장된 Brute force기능을 사용 할 수 있다. 키를 생성하는 방법에는 두 가지의 방법이 존재하는데, 전자의 방법에는 Encrypted 파일과 Original 파일을 이용해서 Brute forcing을 진행한 뒤 key generation이 가능하다. 후자의 방법에는 Encrypted된 두 파일을 통해서 Brute forcing을 진행한다.

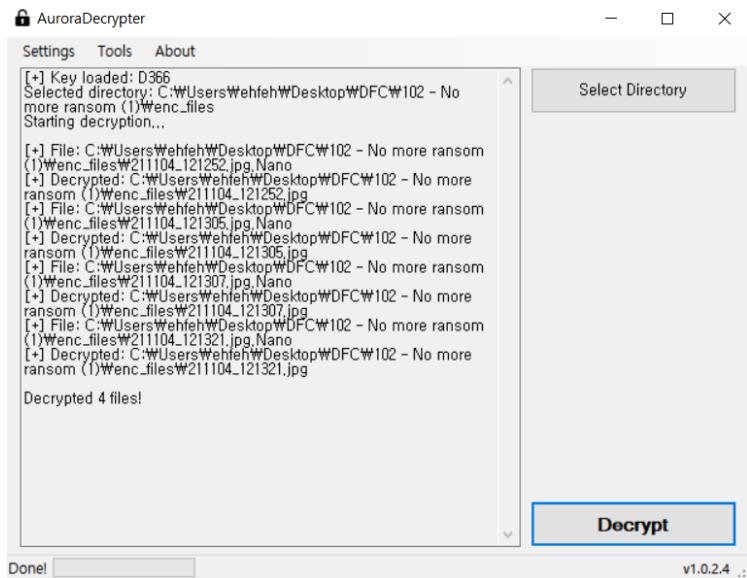


[그림 4]. Encrypted/Original File Pair Bruteforce



[그림 5]. Use Both Encrypted Files Bruteforce

주어진 enc_files 폴더에 origin.jpg라는 원본 파일과 랜섬웨어로 암호화된 파일을 통해 brute forcing한 경우와 랜섬웨어로 암호화된 두 개의 파일을 통해 brute forcing한 경우의 Key 값은 "D366"으로 동일하게 나온다.



[그림 6]. Aurora Ransomware Decrypt 과정

해당 Key를 load해주고 Decrypt를 실행해준다. 해당 문제에서의 Aurora 랜섬웨어에서는 랜섬노트를 따로 복호화 과정에 사용하지 않는다.

이름	수정한 날짜	유형	크기
#RECOVERY_FILES#.txt	2022-05-26 오후 5:52	텍스트 문서	1KB
211104_121252.jpg	2022-07-12 오후 8:16	JPG 파일	3,869KB
211104_121252.jpg.Nano	2022-05-26 오후 5:52	NANO 파일	3,869KB
211104_121305.jpg	2022-07-12 오후 8:16	JPG 파일	3,883KB
211104_121305.jpg.Nano	2022-05-26 오후 5:52	NANO 파일	3,883KB
211104_121307.jpg	2022-07-12 오후 8:16	JPG 파일	3,959KB
211104_121307.jpg.Nano	2022-05-26 오후 5:52	NANO 파일	3,959KB
211104_121321.jpg	2022-07-12 오후 8:16	JPG 파일	3,768KB
211104_121321.jpg.Nano	2022-05-26 오후 5:52	NANO 파일	3,768KB

[그림 7]. Decrypt된 파일 확인

복호화 된 4개의 파일을 확인할 수 있다.

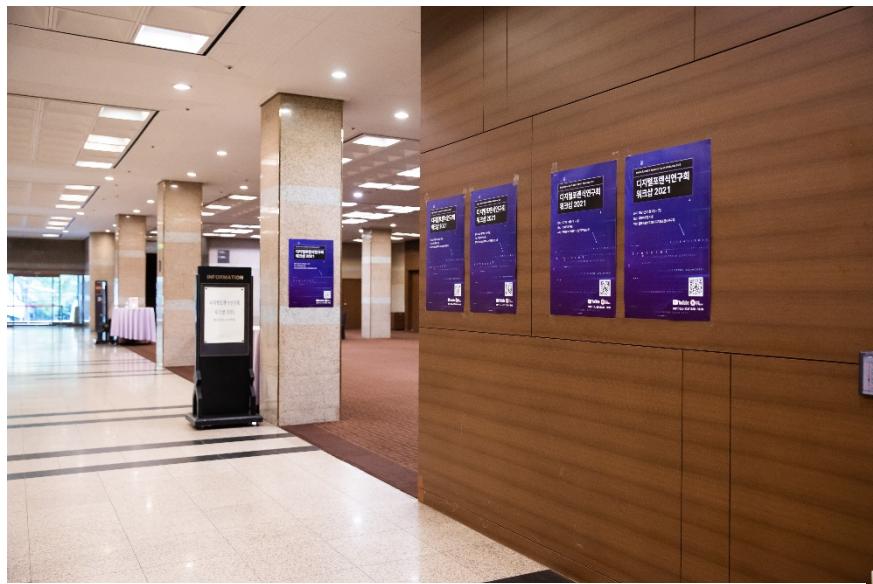


[그림 8]. 복호화 된 211104_121252.jpg 파일

```
root@ubuntu:/home/tobecert/ExifTool# ./exiftool check_file/211104_121252.jpg
ExifTool Version Number          : 12.43
File Name                        : 211104_121252.jpg
Directory                         : check_file
File Size                         : 4.0 MB
File Modification Date/Time     : 2022:07:12 07:04:17-07:00
File Access Date/Time            : 2022:07:12 07:09:00-07:00
File Inode Change Date/Time     : 2022:07:12 07:04:31-07:00
File Permissions                 : -rw-rw-r--
File Type                         : JPEG
File Type Extension              : jpg
MIME Type                         : image/jpeg
Exif Byte Order                  : Little-endian (Intel, II)
Make                             : Canon
Camera Model Name                : Canon EOS 6D Mark II
X Resolution                      : 240
Y Resolution                      : 240
Resolution Unit                  : inches
Software                          : Adobe Photoshop Lightroom Classic 10.0 (Windows)
Modify Date                       : 2021:11:04 15:25:48
Exposure Time                    : 1/125
F Number                          : 3.2
Exposure Program                 : Manual
ISO                               : 2000
Sensitivity Type                 : Recommended Exposure Index
Recommended Exposure Index       : 2000
Exif Version                     : 0231
Date/Time Original               : 2021:11:04 12:12:52
```

[그림 9]. 211104_121252.jpg에 대한 메타데이터

다음은 복호화 된 파일 중 하나인 211104_121252.jpg의 이미지와 파일에 대한 메타데이터 정보이다.



[그림 10]. 복호화 된 211104_121305.jpg 파일

```
root@ubuntu:/home/tobecert/ExifTool# ./exiftool check_file/211104_121305.jpg
ExifTool Version Number      : 12.43
File Name                   : 211104_121305.jpg
Directory                   : check_file
File Size                    : 4.0 MB
File Modification Date/Time : 2022:07:12 07:05:30-07:00
File Access Date/Time       : 2022:07:12 07:15:23-07:00
File Inode Change Date/Time : 2022:07:12 07:05:30-07:00
File Permissions            : -rw-rw-r--
File Type                   : JPEG
File Type Extension         : jpg
MIME Type                   : image/jpeg
Exif Byte Order              : Little-endian (Intel, II)
Make                         : Canon
Camera Model Name           : Canon EOS 6D Mark II
X Resolution                 : 240
Y Resolution                 : 240
Resolution Unit              : inches
Software                      : Adobe Photoshop Lightroom Classic 10.0 (Windows)
Modify Date                  : 2021:11:04 15:25:48
Exposure Time                : 1/80
F Number                      : 3.2
Exposure Program             : Manual
ISO                           : 2000
Sensitivity Type             : Recommended Exposure Index
Recommended Exposure Index   : 2000
Exif Version                 : 0231
Date/Time Original           : 2021:11:04 12:13:05
```

[그림 11]. 211104_121305.jpg에 대한 메타데이터

다음은 복호화 된 파일 중 하나인 211104_121305.jpg의 이미지와 파일에 대한 메타데이터 정보이다.



[그림 12]. 복호화 된 211104_121307.jpg

```
root@ubuntu:/home/tobecert/ExifTool# ./exiftool check_file/211104_121307.jpg
ExifTool Version Number      : 12.43
File Name                   : 211104_121307.jpg
Directory                   : check_file
File Size                    : 4.1 MB
File Modification Date/Time : 2022:07:12 07:05:44-07:00
File Access Date/Time       : 2022:07:12 07:05:41-07:00
File Inode Change Date/Time : 2022:07:12 07:05:44-07:00
File Permissions            : -rw-rw-r--
File Type                   : JPEG
File Type Extension         : jpg
MIME Type                   : image/jpeg
Exif Byte Order             : Little-endian (Intel, II)
Make                         : Canon
Camera Model Name           : Canon EOS 6D Mark II
X Resolution                : 240
Y Resolution                : 240
Resolution Unit             : inches
Software                     : Adobe Photoshop Lightroom Classic 10.0 (Windows)
Modify Date                 : 2021:11:04 15:25:48
Exposure Time               : 1/80
F Number                     : 3.2
Exposure Program             : Manual
ISO                          : 2000
Sensitivity Type            : Recommended Exposure Index
Recommended Exposure Index   : 2000
Exif Version                : 0231
Date/Time Original          : 2021:11:04 12:13:07
```

[그림 13]. 211104_121307.jpg에 대한 메타데이터

다음은 복호화 된 파일 중 하나인 211104_121307.jpg의 이미지와 파일에 대한 메타데이터 정보이다.



[그림 14]. 복호화 된 211104_121321.jpg

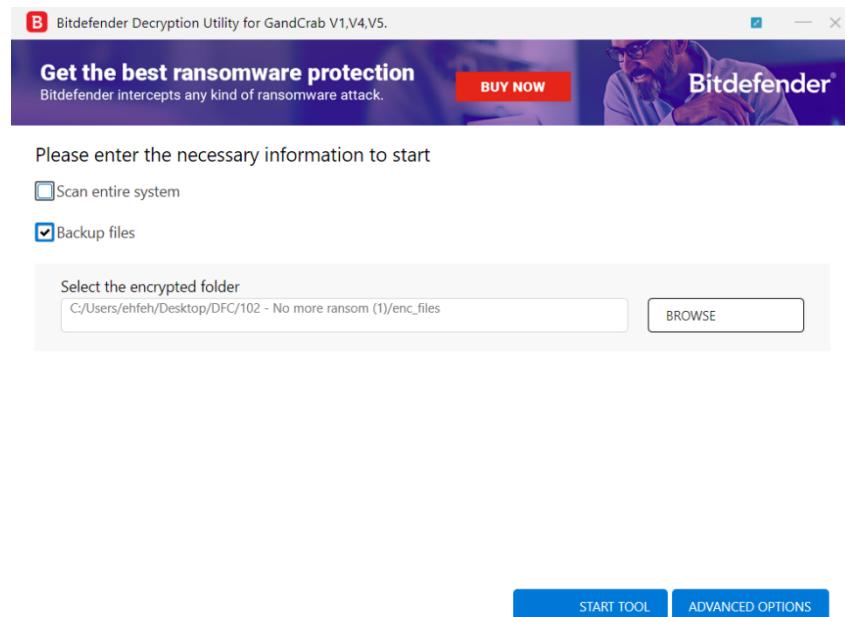
```
root@ubuntu:/home/tobecert/ExifTool# ./exiftool check_file/211104_121321.jpg
ExifTool Version Number      : 12.43
File Name                   : 211104_121321.jpg
Directory                   : check_file
File Size                    : 3.9 MB
File Modification Date/Time : 2022:07:12 07:05:54-07:00
File Access Date/Time       : 2022:07:12 07:05:54-07:00
File Inode Change Date/Time: 2022:07:12 07:05:54-07:00
File Permissions            : -rw-rw-r--
File Type                   : JPEG
File Type Extension         : jpg
MIME Type                   : image/jpeg
Exif Byte Order             : Little-endian (Intel, II)
Make                         : Canon
Camera Model Name           : Canon EOS 6D Mark II
X Resolution                : 240
Y Resolution                : 240
Resolution Unit             : inches
Software                     : Adobe Photoshop Lightroom Classic 10.0 (Windows)
Modify Date                 : 2021:11:04 15:25:48
Exposure Time               : 1/80
F Number                     : 3.2
Exposure Program            : Manual
ISO                          : 2000
Sensitivity Type            : Recommended Exposure Index
Recommended Exposure Index  : 2000
Exif Version                : 0231
Date/Time Original          : 2021:11:04 12:13:21
```

[그림 15]. 211104_121321.jpg에 대한 메타데이터

다음은 복호화 된 파일 중 하나인 211104_121321.jpg의 이미지와 파일에 대한 메타데이터 정보이다.

2-2) GandCrab Ransomware Decrypt Process

이번에는, GandCrab 랜섬웨어 복호화를 진행했다.



[그림 16]. GandCrab 복호화 과정

```
--BEGIN GANDCRAB KEY--  
IAQAAAG+hoYkXgNi2k8ZvIcgBnegusk6uaqq0DVhxw5SAXtBqLgW/k0rUuHl/OYKKG/+6XuEuwlJN/XFbSeOoU5aqMGo52M6sb6k556IMVQNoot4hF+a0y01Hvp0opdpbkjy4Mi  
WvghpEgiBjmjDimLm0FDPnETD7b0Fl6ioUsfkr8v8c2Gi6/D7nCLlv61IWctsyR9V86+X+/WaZv7ZHkllk07QHNTB6uxV2BVbUK+7KtBa2yu4v6SG1Jvk6nRkPaxuyyjoYsv9jlM3e2FO1  
7AUhMvV2U9YGKBqEiYNKSsdca/RzkGKfcUaCbWztvcEHGTM/IBJYcdXlnSgvWA6cYUGVTEXvVpp11Cpg3fbvoeBU3L9uHbS+wYxaNvLpnKhkB0dD2YspLoW+oYeFGTfsCY8l/KVjyS  
--END GANDCRAB KEY--  
  
--BEGIN PC DATA--  
wfKD6iudumBkmpL8IR4U7KxEFa2OW/tiDxwOqf191YnvOeWPx5OYfxdxJZStoRRtXYL7ndWtbe4TGuh5h4sBLzz2NMx7/76G0GXDCriMpJ288/FKv/amF6obpAeLpej5fxw2X3xAZKu  
--END PC DATA--
```

[그림 17]. GandCrab Ransomnote(KRAB-DECRYPT.txt)

Bitdefender사에서 제공하는 GandCrab Decrypt Tool을 이용해서 복호화를 수행했다. 이 도구는 GandCrab Ransomnote가 존재하는 폴더를 encrypted folder로 지정하고 복호화를 수행하면 정상적으로 진행된다.

IMG_0210.JPG	2022-07-12 오후 9:15	JPG 파일	1,272KB
IMG_0210.JPG.KRAB	2022-05-25 오후 2:32	KRAB 파일	1,272KB
IMG_1095.JPG	2022-07-12 오후 9:15	JPG 파일	6,263KB
IMG_1095.JPG.KRAB	2022-05-25 오후 2:32	KRAB 파일	6,263KB

[그림 18]. 복호화된 GandCrab 암호화 파일

다음은 GandCrab tool을 통해 복호화를 진행한 후 얻은 IMG_0210, IMG_1095 파일이다.



[그림 19]. 복호화 된 IMG_0210.JPG

```

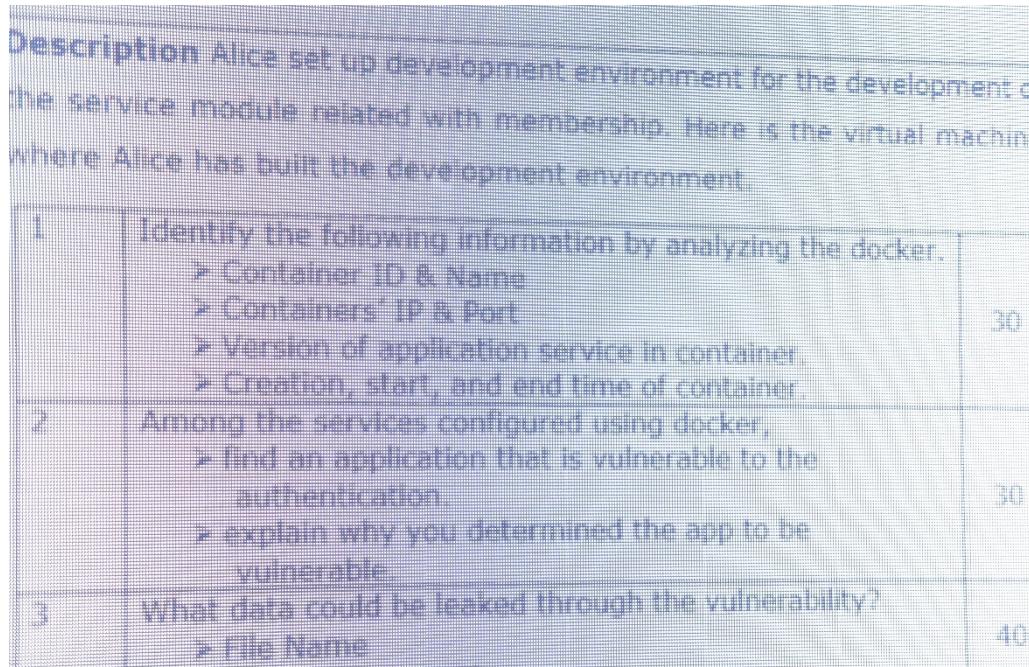
root@ubuntu:/home/tobecert/ExifTool# ./exiftool check_file/IMG_0210.JPG
ExifTool Version Number      : 12.43
File Name                   : IMG_0210.JPG
Directory                   : check_file
File Size                    : 1302 kB
File Modification Date/Time : 2022:07:12 07:22:59-07:00
File Access Date/Time       : 2022:07:12 07:22:59-07:00
File Inode Change Date/Time: 2022:07:12 07:22:59-07:00
File Permissions            : -rw-rw-r--
File Type                   : JPEG
File Type Extension         : jpg
MIME Type                   : image/jpeg
Exif Byte Order              : Little-endian (Intel, II)
Make                         : Canon
Camera Model Name           : Canon EOS 6D Mark II
Orientation                  : Horizontal (normal)
X Resolution                 : 72
Y Resolution                 : 72
Resolution Unit              : inches
Modify Date                  : 2021:11:04 13:57:49
Artist                        : HYUNWOO
Y Cb Cr Positioning          : Co-sited
Copyright                     : HBW100@HANMAIL
Exposure Time                : 1/160
F Number                      : 3.2
Exposure Program              : Manual
ISO                           : 2500
Sensitivity Type              : Recommended Exposure Index
Recommended Exposure Index    : 2500
Exif Version                  : 0230
Date/Time Original            : 2021:11:04 13:57:49

```

[그림 20]. IMG_0210.JPG에 대한 메타데이터

다음 [그림 19], [그림 20]은 IMG_0210.JPG에 대한 사진과 메타데이터를 나타낸다.

해당 복호화 된 파일은 다른 복호화 된 이미지 파일과는 다르게 아티스트가 지정되어 있고 Copyright가 존재하는 파일이다. Artist는 "HYUNWOO"이고, Copyright는 "HBW100@HANMAIL"이다. (수정필요?)



[그림 21]. 복호화 된 IMG_1095.JPG

```
root@ubuntu:/home/tobecert/ExifTool# ./exiftool check_file/IMG_1095.JPG
ExifTool Version Number      : 12.43
File Name                   : IMG_1095.JPG
Directory                  : check_file
File Size                   : 6.4 MB
File Modification Date/Time : 2022:07:12 07:23:10-07:00
File Access Date/Time       : 2022:07:12 07:23:10-07:00
File Inode Change Date/Time: 2022:07:12 07:23:10-07:00
File Permissions            : -rw-rw-r--
File Type                   : JPEG
File Type Extension         : jpg
MIME Type                   : image/jpeg
Exif Byte Order              : Little-endian (Intel, II)
Make                         : Canon
Camera Model Name           : Canon EOS 6D Mark II
Orientation                 : Horizontal (normal)
X Resolution                : 72
Y Resolution                : 72
Resolution Unit             : inches
Modify Date                 : 2021:11:05 14:36:02
Artist                       : HYUNWOO
YCbCr Positioning          : Co-sited
Copyright                   : HBW100@HANMAIL
Exposure Time               : 1/160
F Number                     : 3.2
Exposure Program             : Manual
ISO                          : 2000
Sensitivity Type            : Recommended Exposure Index
Recommended Exposure Index   : 2000
Exif Version                 : 0230
Date/Time Original           : 2021:11:05 14:36:02
```

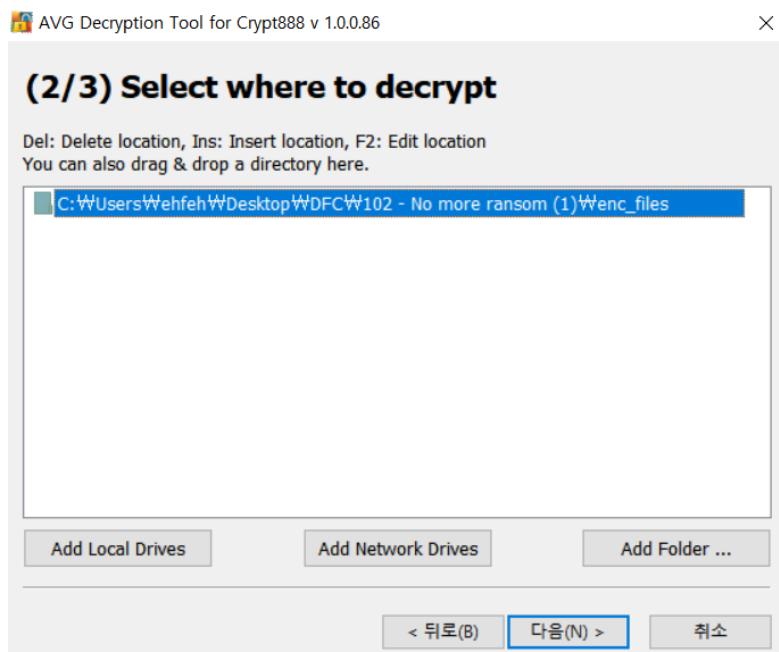
[그림 22]. IMG_1095.JPG에 대한 메타데이터

다음 [그림 21], [그림 22]은 IMG_1095.JPG에 대한 사진과 메타데이터를 나타낸다. 해당 파일 역시 Artist와 Copyright를 식별할 수 있다.

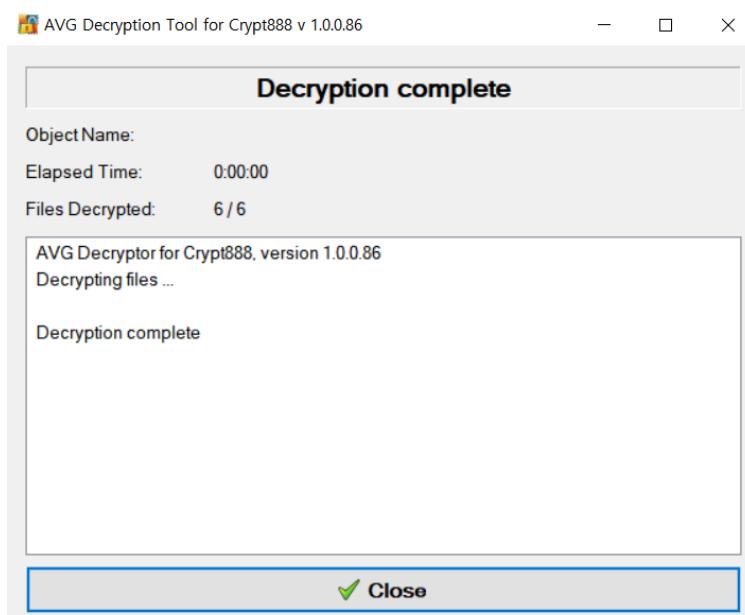
(수정필요?)

2-3) MicroCop(or Crypt888) Ransomware Decrypt Process

세번째로 MicroCop(or Crypt888)에 대한 복호화 진행과정이다.



[그림 23]. 복호화 할 파일 선택



[그림 24] 복호화 성공

AVG Decryption Tool을 통해 Crypt888(or MirCop) ransomware 복호화를 진행했다. 해당 툴은 랜섬노트가 따로 필요하지 않았다.

 plaque.zip	2022-05-25 오후 3:52	압축(ZIP) 파일	1,945KB
 query.txt	2022-05-25 오후 3:52	텍스트 문서	1KB

[그림 25]. AVG decrypt tool로 복호화 된 파일1

 w_8723.jpg	2022-05-25 오후 3:52	JPG 파일	5,264KB
 w_8724.jpg	2022-05-25 오후 3:52	JPG 파일	4,011KB
 w_8725.jpg	2022-05-25 오후 3:52	JPG 파일	3,824KB
 w_8726.jpg	2022-05-25 오후 3:52	JPG 파일	4,156KB

[그림 26]. AVG decrypt tool로 복호화 된 파일2

다음 [그림 25], [그림 26]은 복호화 된 파일 리스트를 나타낸다.



[그림 27]. 복호화 된 w_8723.jpg

```
root@ubuntu:/home/tobecert/ExifTool# ./exiftool check_file/w_8723.jpg
ExifTool Version Number      : 12.43
File Name                   : w_8723.jpg
Directory                   : check_file
File Size                    : 5.4 MB
File Modification Date/Time : 2022:07:12 07:28:00-07:00
File Access Date/Time       : 2022:07:12 07:28:00-07:00
File Inode Change Date/Time: 2022:07:12 07:28:00-07:00
File Permissions            : -rw-rw-r--
File Type                   : JPEG
File Type Extension         : jpg
MIME Type                   : image/jpeg
Exif Byte Order              : Little-endian (Intel, II)
Make                         : Canon
Camera Model Name           : Canon EOS 6D Mark II
X Resolution                 : 240
Y Resolution                 : 240
Resolution Unit              : inches
Software                      : Adobe Photoshop Lightroom Classic 10.0 (Windows)
Modify Date                  : 2021:11:04 15:25:35
Exposure Time                : 1/250
F Number                      : 7.1
Exposure Program             : Manual
ISO                           : 200
Sensitivity Type             : Recommended Exposure Index
Recommended Exposure Index   : 200
Exif Version                 : 0231
Date/Time Original           : 2021:11:04 12:08:40
```

[그림 28]. w_8723.jpg에 대한 메타데이터 정보

다음 [그림 27], [그림 28]은 복호화 된 w_8723.jpg에 대한 사진 정보와 메타데이터 정보를 나타낸다.



[그림 29]. 복호화 된 w_8724.jpg

```
root@ubuntu:/home/tobecert/ExifTool# ./exiftool check_file/w_8724.jpg
ExifTool Version Number      : 12.43
File Name                   : w_8724.jpg
Directory                   : check_file
File Size                    : 4.1 MB
File Modification Date/Time : 2022:07:12 07:28:06-07:00
File Access Date/Time       : 2022:07:12 07:28:06-07:00
File Inode Change Date/Time: 2022:07:12 07:28:06-07:00
File Permissions            : -rw-rw-r--
File Type                   : JPEG
File Type Extension         : jpg
MIME Type                   : image/jpeg
Exif Byte Order              : Little-endian (Intel, II)
Make                         : Canon
Camera Model Name           : Canon EOS 6D Mark II
X Resolution                 : 240
Y Resolution                 : 240
Resolution Unit              : inches
Software                      : Adobe Photoshop Lightroom Classic 10.0 (Windows)
Modify Date                  : 2021:11:04 15:25:41
Exposure Time                : 1/125
F Number                      : 3.2
Exposure Program             : Manual
ISO                           : 2000
Sensitivity Type             : Recommended Exposure Index
Recommended Exposure Index   : 2000
Exif Version                 : 0231
Date/Time Original           : 2021:11:04 12:12:07
```

[그림 30]. w_8724.jpg에 대한 메타데이터 정보

다음 [그림 29], [그림 30]은 복호화 된 w_8724.jpg에 대한 사진 정보와 메타데이터 정보를 나타낸다.



[그림 31]. 복호화 된 w_8725.jpg

```
root@ubuntu:/home/tobecert/ExifTool# ./exiftool check_file/w_8725.jpg
ExifTool Version Number      : 12.43
File Name                   : w_8725.jpg
Directory                   : check_file
File Size                    : 3.9 MB
File Modification Date/Time : 2022:07:12 07:28:15-07:00
File Access Date/Time       : 2022:07:12 07:28:15-07:00
File Inode Change Date/Time: 2022:07:12 07:28:15-07:00
File Permissions            : -rw-rw-r--
File Type                   : JPEG
File Type Extension         : jpg
MIME Type                   : image/jpeg
Exif Byte Order             : Little-endian (Intel, II)
Make                         : Canon
Camera Model Name           : Canon EOS 6D Mark II
X Resolution                : 240
Y Resolution                : 240
Resolution Unit              : inches
Software                     : Adobe Photoshop Lightroom Classic 10.0 (Windows)
Modify Date                 : 2021:11:04 15:25:41
Exposure Time               : 1/125
F Number                     : 3.2
Exposure Program             : Manual
ISO                          : 2000
Sensitivity Type            : Recommended Exposure Index
Recommended Exposure Index   : 2000
Exif Version                : 0231
Date/Time Original          : 2021:11:04 12:12:19
```

[그림 32]. w_8725.jpg 에 대한 메타데이터 정보

다음 [그림 31], [그림 32]은 복호화 된 w_8725.jpg에 대한 사진 정보와 메타데이터 정보를 나타낸다.



[그림 33]. 복호화 된 w_8726.jpg

```
root@ubuntu:/home/tobecert/ExifTool# ./exiftool check_file/w_8726.jpg
ExifTool Version Number      : 12.43
File Name                   : w_8726.jpg
Directory                   : check_file
File Size                    : 4.3 MB
File Modification Date/Time : 2022:07:12 07:28:21-07:00
File Access Date/Time       : 2022:07:12 07:28:21-07:00
File Inode Change Date/Time: 2022:07:12 07:28:21-07:00
File Permissions            : -rw-rw-r--
File Type                   : JPEG
File Type Extension         : jpg
MIME Type                   : image/jpeg
Exif Byte Order             : Little-endian (Intel, II)
Make                         : Canon
Camera Model Name           : Canon EOS 6D Mark II
X Resolution                : 240
Y Resolution                : 240
Resolution Unit             : inches
Software                     : Adobe Photoshop Lightroom Classic 10.0 (Windows)
Modify Date                 : 2021:11:04 15:25:41
Exposure Time               : 1/125
F Number                     : 3.2
Exposure Program             : Manual
ISO                          : 2000
Sensitivity Type            : Recommended Exposure Index
Recommended Exposure Index   : 2000
Exif Version                : 0231
Date/Time Original          : 2021:11:04 12:12:27
```

[그림 34]. w_8726.jpg에 대한 메타데이터 정보

다음 [그림 33], [그림 34]은 복호화 된 w_8726.jpg에 대한 사진 정보와 메타데이터 정보를 나타낸다.

```

query.txt - Windows 메모장
파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)
CREATE TABLE MISC.dbo.PRESS_TB
(
    PRESS_ID_PK INT PRIMARY KEY,
    PRESS_NM NVARCHAR(50),
    RELEASE_SUM INT
)

CREATE TABLE MISC.dbo.ARTICLE_TB
(
    ARTICLE_ID_PK INT PRIMARY KEY,
    PRESS_ID_FK1 INT FOREIGN KEY REFERENCES MISC.dbo.PRESS_TB(PRESS_ID_PK),
    ARTICLE_URL TEXT,
    UPLOAD_DT INT,
    CHG_DT INT
)

CREATE TABLE MISC.dbo.REPLY_TB
(
    REPLY_ID_PK INT PRIMARY KEY,
    ARTICLE_ID_FK1 INT FOREIGN KEY REFERENCES MISC.dbo.ARTICLE_TB(ARTICLE_ID_PK),
    ID NVARCHAR(40),
    REPLY_URL TEXT,
    REPLY_DT INT
)

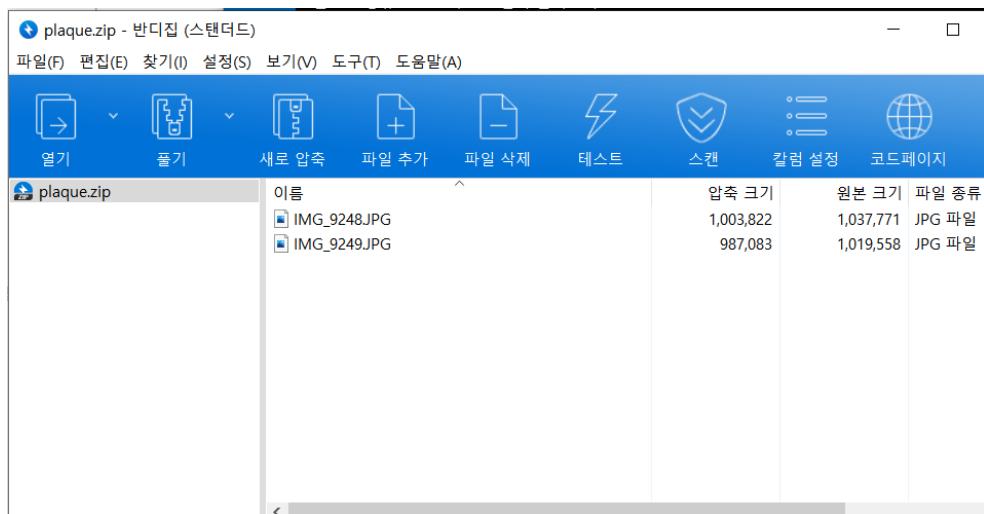
CREATE TABLE MISC.dbo.ACTION_TB
(
    ACTION_ID_PK INT PRIMARY KEY,
    REPLY_ID_FK1 INT FOREIGN KEY REFERENCES MISC.dbo.REPLY_TB(REPLY_ID_PK),
    ID NVARCHAR(40),
    CLK_DT INT,
    REPLY_ACTION NVARCHAR(30)
)

CREATE TABLE PIC_DB.dbo.ARTICLE_PIC_TB
(
    ARTICLE_PIC_ID_PK INT PRIMARY KEY,
    ARTICLE_ID_FK1 INT FOREIGN KEY REFERENCES MISC.dbo.ARTICLE_TB(ARTICLE_ID_PK),
    UPLOAD_DT DATE,
    CHG_DT DATE,
    PIC IMAGE
)

```

[그림 35]. 복호화 된 query.txt 파일

다음 [그림 35]는 복호화 된 query.txt를 나타낸다.



[그림 36]. 복호화 된 plaque.zip 안에 들어있는 IMG 파일

zip파일 안에 두개의 JPG파일을 확인할 수 있었고, 이 두 이미지 파일 역시 확인과정을 거쳤다.



[그림 37]. 복호화 된 plaque.zip 내부에 들어있는 IMG_9248.JPG

```
root@ubuntu:/home/tobecert/ExifTool# ./exiftool check_file/IMG_9248.JPG
ExifTool Version Number          : 12.43
File Name                        : IMG_9248.JPG
Directory                         : check_file
File Size                          : 1038 kB
File Modification Date/Time      : 2022:07:11 21:28:35-07:00
File Access Date/Time             : 2022:07:11 21:29:05-07:00
File Inode Change Date/Time       : 2022:07:11 21:28:35-07:00
File Permissions                  : -rw-r--r--
File Type                         : JPEG
File Type Extension               : jpg
MIME Type                         : image/jpeg
Exif Byte Order                   : Little-endian (Intel, II)
Make                             : Canon
Camera Model Name                 : Canon EOS 6D Mark II
Orientation                        : Horizontal (normal)
X Resolution                      : 72
Y Resolution                      : 72
Resolution Unit                   : inches
Modify Date                       : 2021:11:05 12:45:37
Artist                            :
Y Cb Cr Positioning              : Co-sited
Copyright                          :
Exposure Time                     : 1/125
F Number                           : 2.8
Exposure Program                  : Manual
ISO                               : 2000
Sensitivity Type                  : Recommended Exposure Index
Recommended Exposure Index        : 2000
Exif Version                      : 0230
Date/Time Original                : 2021:11:05 12:45:37
```

[그림 38]. IMG_9248.JPG에 대한 메타데이터 정보

다음 [그림 37], [그림 38]은 복호화 된 IMG_9248.JPG에 대한 사진 정보와 메타데이터 정보를 나타낸다.



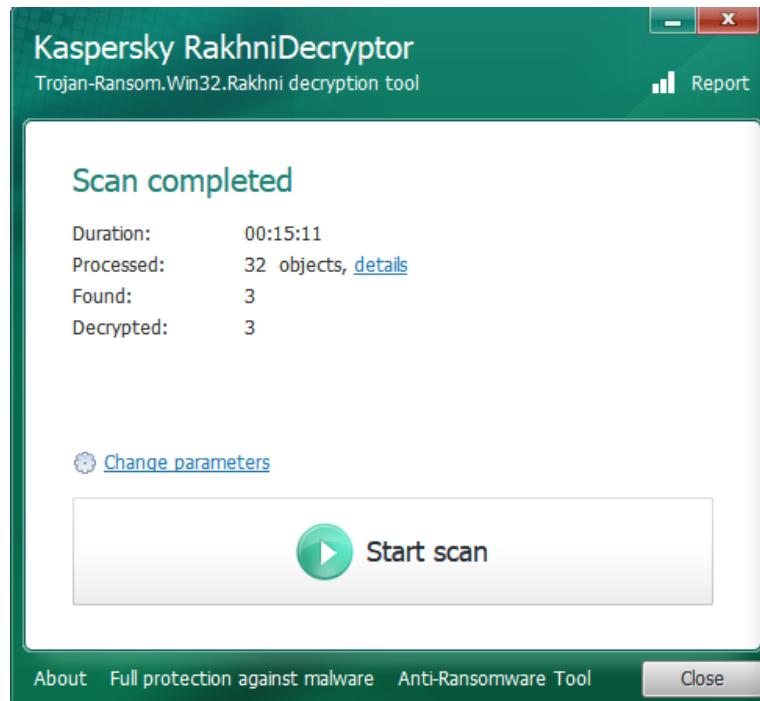
[그림 39]. 복호화 된 plaque.zip 내부에 들어있는 IMG_9249.jpg

```
root@ubuntu:/home/tobecert/ExifTool# ./exiftool check_file/IMG_9249.JPG
ExifTool Version Number      : 12.43
File Name                   : IMG_9249.JPG
Directory                  : check_file
File Size                   : 1020 kB
File Modification Date/Time : 2022:07:11 21:28:35-07:00
File Access Date/Time       : 2022:07:11 21:28:35-07:00
File Inode Change Date/Time: 2022:07:11 21:28:35-07:00
File Permissions            : -rw-r--r--
File Type                   : JPEG
File Type Extension         : jpg
MIME Type                   : image/jpeg
Exif Byte Order              : Little-endian (Intel, II)
Make                         : Canon
Camera Model Name           : Canon EOS 6D Mark II
Orientation                 : Horizontal (normal)
X Resolution                : 72
Y Resolution                : 72
Resolution Unit             : inches
Modify Date                 : 2021:11:05 12:45:45
Artist                       :
Y Cb Cr Positioning        : Co-sited
Copyright                   :
Exposure Time               : 1/125
F Number                     : 2.8
Exposure Program             : Manual
ISO                          : 2000
Sensitivity Type            : Recommended Exposure Index
Recommended Exposure Index   : 2000
Exif Version                 : 0230
Date/Time Original          : 2021:11:05 12:45:45
```

[그림 40]. IMG_9249.JPG에 대한 메타데이터 정보

다음 [그림 39], [그림 40]은 복호화 된 IMG_9249.JPG에 대한 사진 정보와 메타데이터 정보를 나타낸다.

2-4) Yatron Ransomware Decrypt Process



[그림 41]. Yatron 랜섬웨어로 암호화된 파일 Detect

Scan results	
Event	Object
Decrypted	WW?WC:WUsers\Wehfeh\WDesktop\WDFCW102 - No more ransom (1)\Wenc_files\#tree.mp4.Yatron
Decrypted	WW?WC:WUsers\Wehfeh\WDesktop\WDFCW102 - No more ransom (1)\Wenc_files\#w_8732.jpg.Yatron
Decrypted	WW?WC:WUsers\Wehfeh\WDesktop\WDFCW102 - No more ransom (1)\Wenc_files\#w_8733.jpg.Yatron

[그림 42]. Yatron 랜섬웨어로 암호화된 파일 복호화 완료

다음 [그림 41], [그림 42]은 Yatron Decrypt tool로 복호화가 완료된 그림이다.

tree.mp4	2022-07-09 오후 12:22	MP4 파일	3,577KB
tree.mp4.Yatron	2022-07-09 오후 12:22	YATRON 파일	3,577KB
w_8732.jpg	2022-07-09 오후 12:22	JPG 파일	2,898KB
w_8732.jpg.Yatron	2022-07-09 오후 12:22	YATRON 파일	2,898KB
w_8733.jpg	2022-07-09 오후 12:22	JPG 파일	2,274KB
w_8733.jpg.Yatron	2022-07-09 오후 12:22	YATRON 파일	2,274KB

[그림 43]. 복호화 된 파일 확인



[그림 44]. 복호화 된 w_8732.jpg

```
root@ubuntu:/home/tobecert/ExifTool# ./exiftool check_file/w_8732.jpg
ExifTool Version Number      : 12.43
File Name                   : w_8732.jpg
Directory                   : check_file
File Size                    : 3.0 MB
File Modification Date/Time : 2022:07:11 21:28:35-07:00
File Access Date/Time       : 2022:07:11 21:31:28-07:00
File Inode Change Date/Time: 2022:07:11 21:28:35-07:00
File Permissions            : -rw-r--r--
File Type                   : JPEG
File Type Extension         : jpg
MIME Type                   : image/jpeg
Exif Byte Order              : Little-endian (Intel, II)
Make                         : Canon
Camera Model Name           : Canon EOS 6D Mark II
X Resolution                : 240
Y Resolution                : 240
Resolution Unit             : inches
Software                     : Adobe Photoshop Lightroom Classic 10.0 (Windows)
Modify Date                 : 2021:11:04 15:25:54
Exposure Time               : 1/125
F Number                     : 3.2
Exposure Program             : Manual
ISO                          : 2000
Sensitivity Type            : Recommended Exposure Index
Recommended Exposure Index  : 2000
Exif Version                : 0231
Date/Time Original          : 2021:11:04 12:13:52
```

[그림 45]. w_8732.jpg에 대한 메타데이터 정보

다음 [그림 44], [그림 45]은 복호화 된 w_8732.jpg에 대한 사진 정보와 메타데이터 정보를 나타낸다.



[그림 46]. 복호화 된 w_8733.jpg

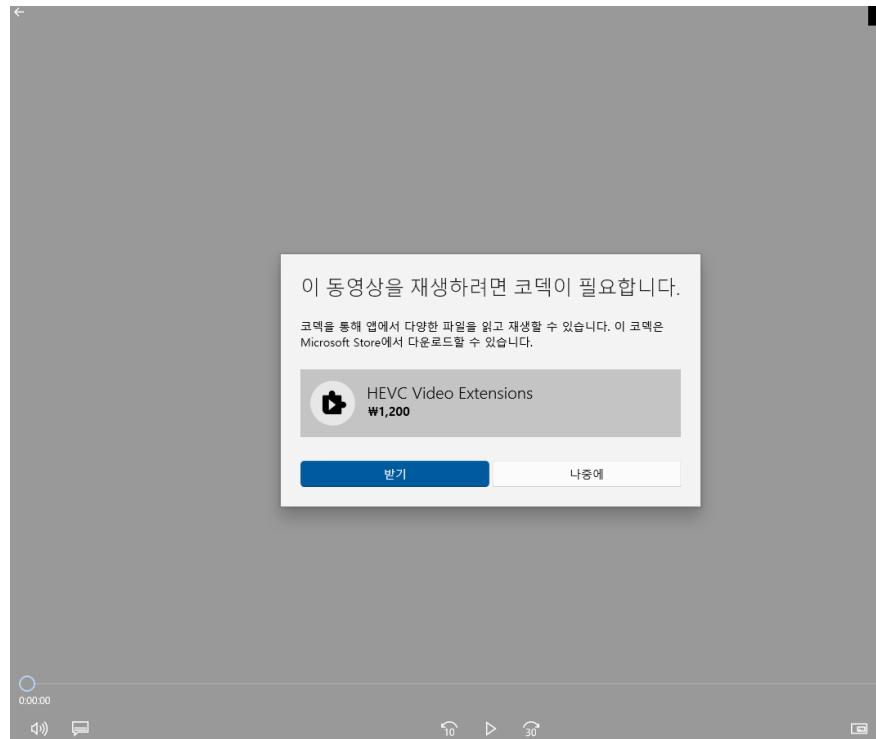
```

root@ubuntu:/home/tobecert/ExifTool# ./exiftool check_file/w_8733.jpg
ExifTool Version Number      : 12.43
File Name                   : w_8733.jpg
Directory                   : check_file
File Size                    : 2.3 MB
File Modification Date/Time : 2022:07:11 21:28:35-07:00
File Access Date/Time       : 2022:07:11 21:28:35-07:00
File Inode Change Date/Time: 2022:07:11 21:28:35-07:00
File Permissions            : -rw-r--r--
File Type                   : JPEG
File Type Extension         : jpg
MIME Type                   : image/jpeg
Exif Byte Order              : Little-endian (Intel, II)
Make                         : Canon
Camera Model Name           : Canon EOS 6D Mark II
X Resolution                 : 240
Y Resolution                 : 240
Resolution Unit              : inches
Software                     : Adobe Photoshop Lightroom Classic 10.0 (Windows)
Modify Date                  : 2021:11:04 15:25:55
Exposure Time                : 1/125
F Number                      : 3.2
Exposure Program             : Manual
ISO                           : 2000
Sensitivity Type             : Recommended Exposure Index
Recommended Exposure Index   : 2000
Exif Version                 : 0231
Date/Time Original           : 2021:11:04 12:14:37

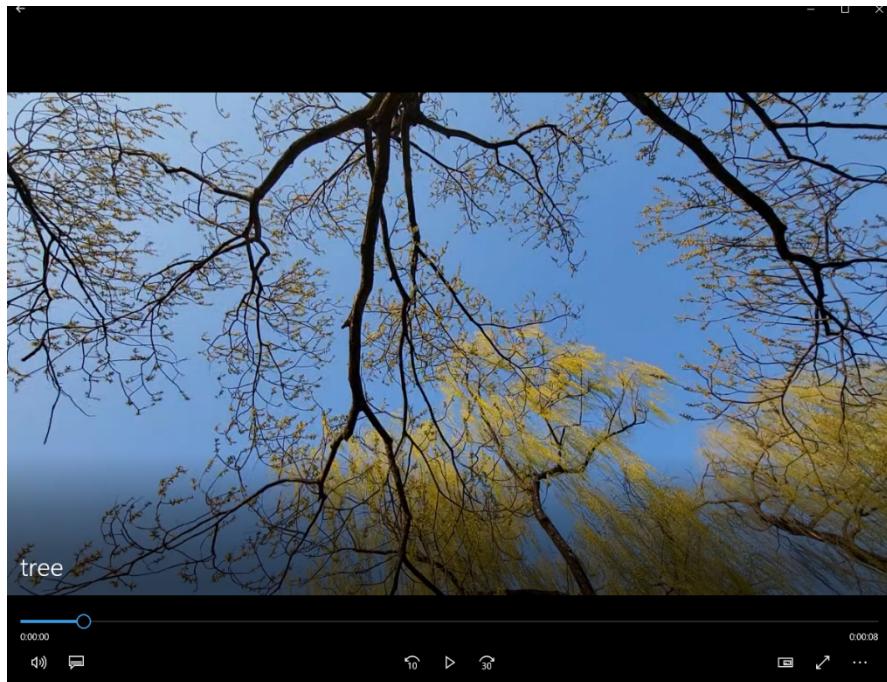
```

[그림 47]. w_8733.jpg에 대한 메타데이터 정보

다음 [그림 46], [그림 47]은 복호화 된 w_8733.jpg에 대한 사진 정보와 메타데이터 정보를 나타낸다.



[그림 48]. tree.mp4 실행을 위한 코덱 설치



[그림 49]. tree.mp4 정상 실행 확인

```
root@ubuntu:/home/tobecert/ExifTool# ./exiftool check_file/tree.mp4
ExifTool Version Number      : 12.43
File Name                   : tree.mp4
Directory                   : check_file
File Size                    : 3.7 MB
File Modification Date/Time : 2022:07:12 07:40:20-07:00
File Access Date/Time       : 2022:07:12 07:40:39-07:00
File Inode Change Date/Time : 2022:07:12 07:40:28-07:00
File Permissions            : -RW-RW-R--
File Type                   : MP4
File Type Extension        : mp4
MIME Type                   : video/mp4
Major Brand                 : MP4 Base Media v1 [ISO 14496-12:2003]
Minor Version               : 0.2.0
Compatible Brands           : isom, iso2, mp41
Movie Header Version        : 0
Create Date                 : 0000:00:00 00:00:00
Modify Date                 : 0000:00:00 00:00:00
Time Scale                  : 1000
Duration                    : 8.63 s
Preferred Rate              : 1
Preferred Volume            : 100.00%
Preview Time                : 0 s
Preview Duration            : 0 s
Poster Time                 : 0 s
Selection Time              : 0 s
Selection Duration          : 0 s
Current Time                : 0 s
Next Track ID               : 3
Track Header Version        : 0
Track Create Date           : 0000:00:00 00:00:00
```

[그림 50]. tree.mp4에 대한 메타데이터 확인

다음 [그림 48], [그림 49], [그림 50]은 tree.mp4에 대한 파일 확인과 메타데이터 확인 정보이다.

3) Calculate the MD5 hash of the decrypted files. (40 points)

Decrypted Files	MD5
211104_121252.jpg	8FEED9F9F03DB67511DE754DB7656E99
211104_121305.jpg	1F7BEAAAB4D9C5424A0CC6D8F565FAD5
211104_121307.jpg	82DAF710E8916029909225BB515296F5
211104_121321.jpg	306F41F0FFC228826AEFE1ABFF0D63FE
IMG_0210.JPG	32DF1F0084A336FC917D01ECE177FEFC
IMG_1095.JPG	974B00B34765D3AF2C5ACA96A5590119
w_8723.jpg	F925FD951B21CC93ECBE3AEC721E870F
w_8724.jpg	36779A360CD1596BAC6DC17D996CC229
w_8725.jpg	3F7D5B32A867D33990E6254788097C3F
w_8726.jpg	8B63A1E67AEDC4C0DA69CB25CE10D63B
query.txt	7D58303F6A437E433FC9CFF7FC36E73F
plaque.zip	BC0E0D6D0937711AAB3E36A8EC95E39C
IMG_9248.JPG	073AE9F8C9E846DD3EE71E946B73AF3B
IMG_9249.JPG	D0541B30ED48AE4106F6693A2A0E5E8B
w_8732.jpg	F48229095E61E8F9187018FC4D1E84C2
w_8733.jpg	828E634B36D4514B97AFA32010EB3543
tree.mp4	D749A158B01AE91B6D5E7B862D94E61E

[표 2]. 복호화 된 파일에 대한 MD5 정보

복호화 된 파일들에 대한 MD5 정보를 테이블 형태로 나타내었다.