

#### 4. 시나리오 문제

1. 내부자료를 외부로 유출한 파일(시나리오 원본)과 관련 파일을 찾고 증거의 속성을 기재하라.

- 해당 시나리오 원본 파일은 '/vol\_vol2/Users/forensic/Desktop/영화 시나리오/Phantom.pdf'로, 시그니처 확인 결과 .zip 파일로 확인되어 확장자 변조되었음을 확인하여 추출 후 확장자 .zip으로 변경 후 압축 해제 실행.

Phantom.pdf
 0
application/zip
pdf

Hex
Text
Application
File Metadata
OS Account
Data Artifacts
Analysis Results
Context
Annota

Page: 1 of 38
Page
Go to Page: 1
Jump to Offset

0x00000000: 50 4B 03 04 14 00 09 00 08 00 04 A7 CE 4E F1 8F PK.....N...

#### Metadata

Name: /img\_PBR복원\_dd사본\_vmdk.001/vol\_vol2/Users/forensic/Desktop/영화 시나리오/Phantom.pdf  
 Type: File System  
 MIME Type: application/zip  
 Size: 614480  
 File Name Allocation: Allocated  
 Metadata Allocation: Allocated  
 Modified: 2019-06-15 10:18:49 KST  
 Accessed: 2019-06-15 10:19:10 KST  
 Created: 2019-06-15 10:19:10 KST  
 Changed: 2019-06-15 11:05:13 KST  
 MD5: b8a049dafd260f7c6594f522a46438ab  
 SHA-256: f99d25b678e13403935f84cc67c2df8996d5b226de9e18ba567d9596348d0f18  
 Hash Lookup Results: UNKNOWN  
 Internal ID: 10706

파일명	Phantom.pdf
경로명	/vol_vol2/Users/forensic/Desktop/영화 시나리오/Phantom.pdf
접근 시간	Modified : 2019-06-15 10:18:49 KST Accessed :2019-06-15 10:19:10 KST Created : 2019-06-15 10:19:10 KST
파일 용량	614480 Bytes
SHA-256 해시값	f99d25b678e13403935f84cc67c2df8996d5b226de9e18ba567d9596348d0f18

- 해당 파일 압축해제 실행 결과 암호화 되어있음을 발견 후 이메일 송수신 내역 확인하여 해당 암호정보 '369369' 획득

'/vol\_vol2/Users/forensic/AppData/Local/Microsoft/Outlook/forensic2level@gmail.com.ost'에서 다음과 같은 암호정보 369369 발견

From: forensic <forensic2level@gmail.com>

To: throw@dreamwiz.com

CC:

Subject: RE: 마이 베스트 렌드~~

Headers Text HTML RTF Attachments (1) Accounts

Download Images

전화해서도 말했지만 이거 개봉전에 유출되면 큰일 나는거 알지??  
절대 유출하지 말고 압축 해제 비밀번호는 369369 로 해놔머  
몰래 과장님 컴퓨터 가서 슬쩍 가져 온거니까 조심해 !!  
참 메일도 가능하면 지우고 알았지?!?!?

From: throw@dreamwiz.com [mailto:throw@dreamwiz.com]

Sent: Saturday, June 15, 2019 9:49 AM

To: forensic2level@gmail.com

Subject: 마이 베스트 렌드~~

하이 마이 베스트 프렌드~~!!

이번 민병천 감독이랑 시나리오 쓴사람이 봉준호 감독인 영화 있잔아? 유령(PHANTOM)!!

시나리오 먼저 좀 받아 볼 수 있을까~!!

너도 알다 싶이 내가 영화 관련 유튜브 채널 운영하잔아~

무조건 개봉 하고나서 올릴건데 그전에 미리 영상 좀 만들어두려고 하거든

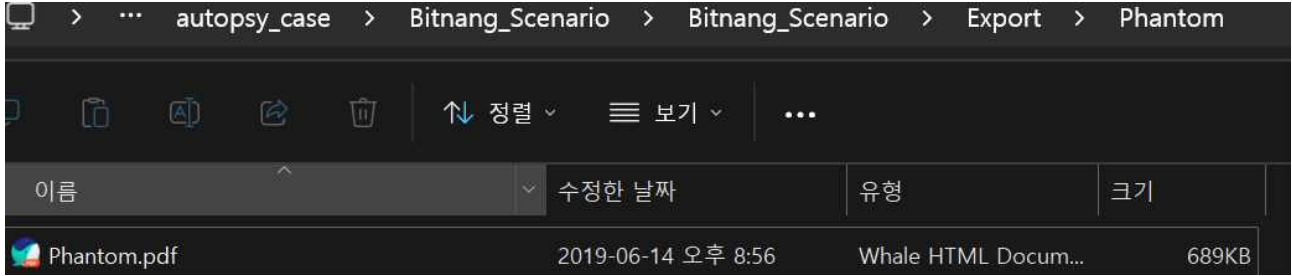
어차피 3일 뒤면 개봉이니 절대 문제 될일 없을거야 ㅎㅎ

딱 한번만 내 부탁 좀 들어주라~ 조회수 잘 나오고 구독자수 많이 늘면 무조건 너한테 크게 한턱 쏜다!!

#### Metadata

Name: /img\_PBR복원\_dd사본\_vmdk.001/vol\_vol2/Users/forensic/AppData/Local/Microsoft/Outlook/forensic2level@gmail.com.ost  
Type: File System  
MIME Type: application/octet-stream  
Size: 16818176  
File Name Allocation: Allocated  
Metadata Allocation: Allocated  
Modified: 2019-06-15 10:41:02 KST  
Accessed: 2019-06-15 10:12:25 KST  
Created: 2019-06-15 10:12:25 KST  
Changed: 2019-06-15 11:04:31 KST  
MD5: c1b599ca5bcb3552dd832f12449a0af7  
SHA-256: 896fbddbce257e80f6cec31d82f61f638971990dd27e76345adaeaaaa56e41a9  
Hash Lookup Results: UNKNOWN  
Internal ID: 3360

- 암호 획득 후 압축 해제 실행한 결과 다음과 같은 'Phantom.pdf' 파일 발견.



- 해당내용 확인하니 영화 [유령(Phantom)]의 시나리오임을 다음과 같이 확인.



2. 유출된 캡처 파일을 찾고, 인터넷 커뮤니티 사이트에 접근한 흔적을 찾아라.

- 이메일 송수신 기록인 ‘/vol\_vol2/Users/forensic/AppData/Local/Microsoft/Outlook/forensic2level@gmail.com.ost’에서 다음과 같은 인터넷 커뮤니티 사이트 링크 확인

forensic2level@gmail.com.ost

throw@dreamwiz.com <throw@dreamwiz.com> 2level@gmail.com RE: RE: 마이 베스트

forensic2level@gmail.com.ost throw@dreamwiz.com <throw@dreamwiz.com> 2level@gmail.com 마이 베스트 렌드~

Hex Text Application Source File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Result: 42 of 43 Result

E-Mail Message

From: throw@dreamwiz.com <throw@dreamwiz.com> 2019-06-15 10:32:32 K

To: 2level@gmail.com

CC:

Subject: RE: RE: 마이 베스트 렌드~~

Headers Text HTML RTF Attachments (0) Accounts

Download Images

역시 내 친구~!! 고마워!! 무조건 잘되서 너한테 크게 쏜다!! 걱정말어!!

참 혹시나 관심이 있을까 해서 하는 말인데 전화에서도 말했지만 시나리오 전부 말고 일부만 찍어서

영화 관련 사이트에 올리면 나같은 사람 말고도 너한테 문의 엄청 줄꺼야. 물론 뭐 네 자유이지만.

어차피 일부만 올라가는거고 뒷처리만 잘하면 아무도 모를꺼야 그리고 일부만 올리는건데 뭐 문제 되겠어? ㅎㅎ

<https://www.filmmakers.co.kr/koreanScreenplays>

이런데 올리면 추가적으로 수입이 생길수도 있을꺼야 후후후.

무튼 고마워!!

- 이후 해당 커뮤니티 사이트 접속 기록 확인을 위해 웹 히스토리 정보를 다음 경로에서 분석 (‘/vol\_vol2/Users/forensic/AppData/Local/Google/Chrome/User Data/Default/History’)

하였고, 그 결과 다음과 같은 접속 기록 확인.

History

History	0	<a href="https://www.filmmakers.co.kr/koreanScreenplays">https://www.filmmakers.co.kr/koreanScreenplays</a>	2019-06-15 10:41:35 KST	한국영화 시나리오 - 필름메이커스 커뮤니티	<a href="https://www.filmmakers.co.kr/koreanScreenplays">https://www.filmmakers.co.kr/koreanScreenplays</a>	Google Chrome	film-makers.co.kr
History	0	<a href="https://www.filmmakers.co.kr/filmmakersWanted">https://www.filmmakers.co.kr/filmmakersWanted</a>	2019-06-15 10:41:35 KST	한국영화 시나리오 - 필름메이커스 커뮤니티	<a href="https://www.filmmakers.co.kr/filmmakersWanted">https://www.filmmakers.co.kr/filmmakersWanted</a>	Google Chrome	film-makers.co.kr
History	0	<a href="https://www.filmmakers.co.kr/filmmakersWanted/72...">https://www.filmmakers.co.kr/filmmakersWanted/72...</a>	2019-06-15 10:41:42 KST	스텝모집 - [올레미리스트] 신규 웰드라마 <인-서울> 음악감독 모집 : 필름메이커스 커뮤니티	<a href="https://www.filmmakers.co.kr/filmmakersWanted/72...">https://www.filmmakers.co.kr/filmmakersWanted/72...</a>	Google Chrome	film-makers.co.kr

Hex Text Application Source File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Result: 6 of 18 Result

Visit Details

Title: 한국영화 시나리오 - 필름메이커스 커뮤니티

Username: Default

Date Accessed: 2019-06-15 10:41:35 KST

Domain: film-makers.co.kr

URL: <https://www.filmmakers.co.kr/koreanScreenplays>

Referrer URL: <https://www.filmmakers.co.kr/koreanScreenplays>

Program Name: Google Chrome

Source

Host: PBR복원\_d4사본\_vmdk.001\_1 Host

Data Source: PBR복원\_d4사본\_vmdk.001

File: /img\_PBR복원\_d4사본\_vmdk.001/vol\_vol2/Users/forensic/AppData/Local/Google/Chrome/User Data/Default/History

- 이메일 송수신 기록을 확인하던 중 [bitnang@naver.com](mailto:bitnang@naver.com)의 이메일 주소를 가진 이와 ftp서버로 의심되는 ip주소를 확인하였음.

History	0	https://www.google.com/search?hl=1C2C AFC_enKRL...	2019-06-15 10:45:22 KST	filezilla - Google 검색	https://www.google.com/search?hl=1C2C...
History	0	https://filezilla-project.org/	2019-06-15 10:45:25 KST	FileZilla - The free FTP solution	https://filezilla-project.org/
History	0	https://filezilla-project.org/download.php?type=server	2019-06-15 10:45:29 KST	Download FileZilla Server for Windows	https://filezilla-project.org/download.php?

Hex
Text
Application
Source File Metadata
OS Account
Data Artifacts
Analysis Results
Context
Annotations
Other Occurrences

Result: 13 of 18
Result

### Visit Details

Title:

filezilla - Google 검색

Username:

Default

Date Accessed:

2019-06-15 10:45:22 KST

Domain:

google.com

URL:

https://www.google.com/search?hl=1C2C AFC\_enKRL853K8R53&source=hp&ei=2E0EXf\_-G83sBAWgvaGABA&q=filezilla&oxq=file&gs\_l=psy-ab.3.1.0i2j0i131j1j0i2j0i131j0i2.1326.2090.18793..0.0.167.541.1j3.....1\_gws-wiz...0.vxSKUKG\_ang

Referrer URL:

https://www.google.com/search?hl=1C2C AFC\_enKRL853K8R53&source=hp&ei=2E0EXf\_-G83sBAWgvaGABA&q=filezilla&oxq=file&gs\_l=psy-ab.3.1.0i2j0i131j1j0i2j0i131j0i2.1326.2090.18793..0.0.167.541.1j3.....1\_gws-wiz...0.vxSKUKG\_ang

Program Name:

Google Chrome

### Source

Host:

PBR복원\_dd사본\_vmdk.001\_1 Host

Data Source:

PBR복원\_dd사본\_vmdk.001

File:

/img PBR복원\_dd사본\_vmdk.001/vol vol2/Users/forensic/AppData/Local/Google/Chrome/User Data/Default/History



- 이후 filezilla를 사용하였음을 의심하고, filezilla의 로그파일을 다음과 같은 경로에서 발견함.

FileZilla Server.log

076c33e0eb9ba6206f251b4bafef44e2f30d12461478a30fc31db4

Hex

Text

Application

File Metadata

OS Account

Data Artifacts

Analysis Results

Context

Annotations

Other Occurrences

**Metadata**

Name:

/img\_PBR복원\_dd사본\_vmdk.001/vol\_vol2/Program Files (x86)/FileZilla Server/FileZilla Server.log

Type:

File System

MIME Type:

text/x-log

Size:

4634

File Name Allocation:

Allocated

Metadata Allocation:

Allocated

Modified:

2019-06-15 10:47:09 KST

Accessed:

2019-06-15 10:46:07 KST

Created:

2019-06-15 10:46:07 KST

Changed:

2019-06-15 11:30:49 KST

MD5:

76c33e0eb9ba6206f251b4bafef44e2f

SHA-256:

30d12461478a30fc31db43b3184ec97e1b4e7cbc6a2e85b960eae7d41a96970

Hash Lookup Results:

UNKNOWN

Internal ID:

11905

- 해당 'FileZilla Server.log' 파일 확인 시 다음과 같음을 확인하여 '명량.pdf' 파일을 FTP서버에 송신한 것으로 보여짐.

```

(000001) 2019-06-15 오전 10:47:02 - (not logged in) (192.168.2.26)> Connected on port 21,
sending welcome message...
(000001) 2019-06-15 오전 10:47:02 - (not logged in) (192.168.2.26)> 220-FileZilla Server
0.9.60 beta
(000001) 2019-06-15 오전 10:47:02 - (not logged in) (192.168.2.26)> 220-written by Tim
Kosse (tim.kosse@filezilla-project.org)
(000001) 2019-06-15 오전 10:47:02 - (not logged in) (192.168.2.26)> 220 Please visit
https://filezilla-project.org/
(000001) 2019-06-15 오전 10:47:02 - (not logged in) (192.168.2.26)> USER anonymous
(000001) 2019-06-15 오전 10:47:02 - (not logged in) (192.168.2.26)> 331 Password required
for anonymous
(000001) 2019-06-15 오전 10:47:02 - (not logged in) (192.168.2.26)> PASS
*****
(000001) 2019-06-15 오전 10:47:02 - anonymous (192.168.2.26)> 230 Logged on
(000001) 2019-06-15 오전 10:47:02 - anonymous (192.168.2.26)> SYST
(000001) 2019-06-15 오전 10:47:02 - anonymous (192.168.2.26)> 215 UNIX emulated by
FileZilla
(000001) 2019-06-15 오전 10:47:02 - anonymous (192.168.2.26)> PWD
(000001) 2019-06-15 오전 10:47:02 - anonymous (192.168.2.26)> 257 "/" is current directory.

```




```
(000001) 2019-06-15 오전 10:47:02 - anonymous (192.168.2.26)> TYPE I
(000001) 2019-06-15 오전 10:47:02 - anonymous (192.168.2.26)> 200 Type set to I
(000001) 2019-06-15 오전 10:47:02 - anonymous (192.168.2.26)> SIZE /
(000001) 2019-06-15 오전 10:47:02 - anonymous (192.168.2.26)> 550 File not found
(000001) 2019-06-15 오전 10:47:02 - anonymous (192.168.2.26)> CWD /
(000001) 2019-06-15 오전 10:47:02 - anonymous (192.168.2.26)> 250 CWD successful. "/" is
current directory.
(000001) 2019-06-15 오전 10:47:02 - anonymous (192.168.2.26)> PASV
(000001) 2019-06-15 오전 10:47:02 - anonymous (192.168.2.26)> 227 Entering Passive Mode
(192,168,2,44,215,140)
(000001) 2019-06-15 오전 10:47:02 - anonymous (192.168.2.26)> LIST -l
(000001) 2019-06-15 오전 10:47:02 - anonymous (192.168.2.26)> 150 Opening data channel
for directory listing of "/"
(000001) 2019-06-15 오전 10:47:02 - anonymous (192.168.2.26)> 226 Successfully transferred
"/"
(000001) 2019-06-15 오전 10:47:02 - anonymous (192.168.2.26)> QUIT
(000001) 2019-06-15 오전 10:47:02 - anonymous (192.168.2.26)> 221 Goodbye
(000001) 2019-06-15 오전 10:47:02 - anonymous (192.168.2.26)> disconnected.
(000002) 2019-06-15 오전 10:47:05 - (not logged in) (192.168.2.26)> Connected on port 21,
sending welcome message...
(000002) 2019-06-15 오전 10:47:05 - (not logged in) (192.168.2.26)> 220-FileZilla Server
0.9.60 beta
(000002) 2019-06-15 오전 10:47:05 - (not logged in) (192.168.2.26)> 220-written by Tim
Kosse (tim.kosse@filezilla-project.org)
(000002) 2019-06-15 오전 10:47:05 - (not logged in) (192.168.2.26)> 220 Please visit
https://filezilla-project.org/
(000002) 2019-06-15 오전 10:47:05 - (not logged in) (192.168.2.26)> USER anonymous
(000002) 2019-06-15 오전 10:47:05 - (not logged in) (192.168.2.26)> 331 Password required
for anonymous
(000002) 2019-06-15 오전 10:47:05 - (not logged in) (192.168.2.26)> PASS
*****
(000002) 2019-06-15 오전 10:47:05 - anonymous (192.168.2.26)> 230 Logged on
(000002) 2019-06-15 오전 10:47:05 - anonymous (192.168.2.26)> SYST
(000002) 2019-06-15 오전 10:47:05 - anonymous (192.168.2.26)> 215 UNIX emulated by
FileZilla
(000002) 2019-06-15 오전 10:47:05 - anonymous (192.168.2.26)> PWD
(000002) 2019-06-15 오전 10:47:05 - anonymous (192.168.2.26)> 257 "/" is current directory.
(000002) 2019-06-15 오전 10:47:05 - anonymous (192.168.2.26)> TYPE I
(000002) 2019-06-15 오전 10:47:05 - anonymous (192.168.2.26)> 200 Type set to I
(000002) 2019-06-15 오전 10:47:05 - anonymous (192.168.2.26)> SIZE /명량.pdf
```

```



(000002) 2019-06-15 오전 10:47:05 - anonymous (192.168.2.26)> 213 1926536
(000002) 2019-06-15 오전 10:47:05 - anonymous (192.168.2.26)> CWD /명량.pdf
(000002) 2019-06-15 오전 10:47:05 - anonymous (192.168.2.26)> 550 CWD failed. "/명량.pdf":
directory not found.
(000002) 2019-06-15 오전 10:47:05 - anonymous (192.168.2.26)> PASV
(000002) 2019-06-15 오전 10:47:05 - anonymous (192.168.2.26)> 227 Entering Passive Mode
(192,168,2,44,202,98)
(000002) 2019-06-15 오전 10:47:05 - anonymous (192.168.2.26)> RETR /명량.pdf
(000002) 2019-06-15 오전 10:47:05 - anonymous (192.168.2.26)> 150 Opening data channel
for file download from server of "/명량.pdf"
(000002) 2019-06-15 오전 10:47:05 - anonymous (192.168.2.26)> 226 Successfully transferred
"/명량.pdf"
(000002) 2019-06-15 오전 10:47:05 - anonymous (192.168.2.26)> disconnected.

```

- 해당 '명량.pdf' 파일을 다음과 같이 찾아내었으며, 해당 파일의 시그니처 확인 시 .png 파일을 포함한 .zip파일로 의심되어 확장자 변환 후 압축 풀기 실행함.

 명량.pdf		0	89d9ef6bedac8b82ac23b8e98ecceda8	6250ad3
 명량.pdf-slack				

Hex	Text	Application	File Metadata	OS Account	Data Artifacts	Analysis Results	Con
Page: 1 of 118      Page   Go to Page: 1      Jump to Off							
0x00000000:	50 4B 03 04 14 00 00 00	08 00 31 A9 CE 4E 9A 38	PK.....1..N.8				
0x00000010:	56 42 ED 6C 05 00 36 EE	05 00 0E 00 00 00 32 30	VB.1..6.....20				
0x00000020:	31 39 30 36 31 34 5F 31	2E 70 6E 67 EC BC 67 54	190614_1.png..gT				



## Metadata

Name:	/img_PBR복원_dd사본_vmdk.001/vol_vol2/Users/forensic/Desktop/영화 시나리오/명량.pdf
Type:	File System
MIME Type:	application/zip
Size:	1926536
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2019-06-14 21:28:30 KST
Accessed:	2019-06-15 10:16:26 KST
Created:	2019-06-15 10:16:26 KST
Changed:	2019-06-15 11:05:13 KST
MD5:	89d9ef6bedac8b82ac23b8e98ecceda8
SHA-256:	6250ad3f69e1ec10971c093c743a63e63a46bb82bbdc2689772709d7527a8afd
Hash Lookup Results:	UNKNOWN
Internal ID:	10718

- 압축 해제 결과, 다음과 같은 영화 [유령(Phantom)]의 시나리오의 일부가 담겨있는 이미지 파일 4개를 확인하였음.

[illegible]

