302 – Find evidence of a conspiracy

Team Information

Team Name : ISEGYE_IDOL

Team Member : Eungchang Lee, Sojeong Kim, Mingyu Seong, Donghyun HA

Email Address : dfc-isegyeidol@googlegroups.com

Instructions

Description Police arrested a broker for leaking blueprints of Space Z's new engine. The broker stated that he passed on information about a document file **(R:Blue Moon(UP).pptx)** that includes the appointment time and place through e-mail. The officer confiscated the researcher's computer for digital forensic analysis.

Target	Hash (MD5)
Windows11.dd.zip	68b05a9c173c9d8d8ea679cbcca3df67

Questions

Please solve all problems based on the time zone of the system.

Data in any language other than English is not relevant to problem-solving.

1) What is the SHA1 hash value of a document file that the researcher received from the broker? (20 points)

2) What is the password of the file that the researcher received from the broker? (150 points)

3) When did the researcher read the e-mail containing the password of the document file? (UTC+9) (80 points)

4) What is the GPS information of the place where the researcher is supposed to meet the broker? (50 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:	FTK Imager	Publisher:	AccessData
Version:	4.5.0.3		
URL:	https://accessdata.com/		

Name:	DB Browser for SQLite	Publisher:	DigitalOcean
Version:	3.12.2		
URL:	http://sqlitebrowser.org		

Name:	Outlook PST Viewer	Publisher:	SysTools
Version:	5.0.0.0		
URL:	https://www.systoolsgroup.com/ko/pst/viewer.html		

Step-by-step methodology:

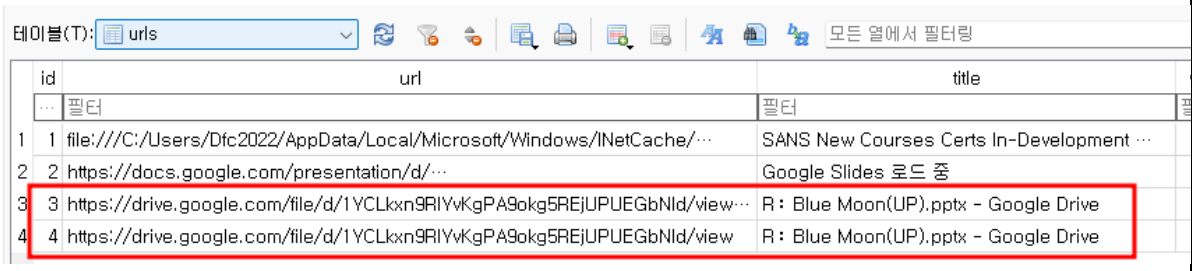
1. What is the SHA1 hash value of a document file that the researcher received from the broker?

FTK Imager를 사용하여 Windows11_3 - V2.dd를 분석하였다.

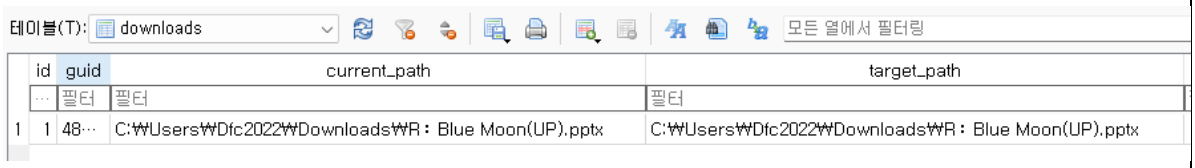
FTK Imager 를 사용하여 아래 아티팩트를 수집 후 분석하였다.

수집한 아티팩트 목록	
Chrome 사용기록	[root]₩Users₩trudy₩Appdata₩Local₩Google₩Chrome₩User Data₩Default₩History

[표 1] 수집한 아티팩트 목록



[그림 1] 방문 기록



[그림 2] 다운로드 기록

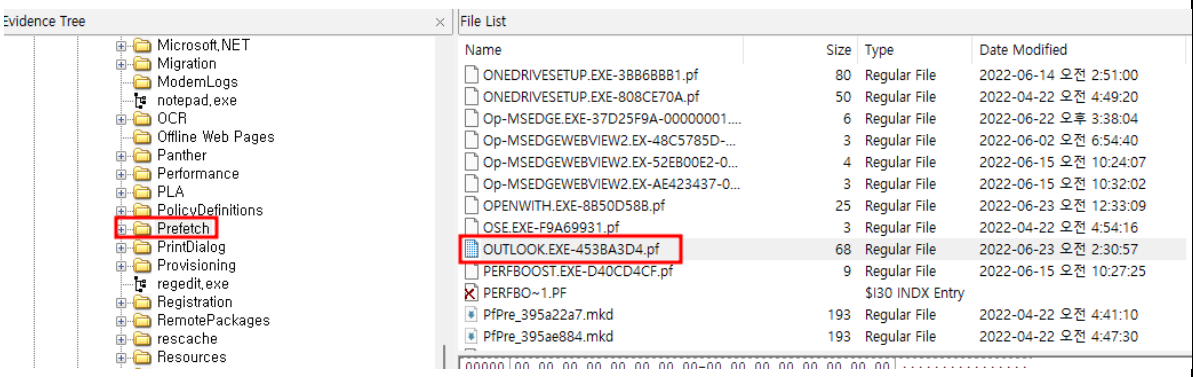
2022년 6월 23일 9:33:34 KST에 다운로드했다.

연구원이 브로커로부터 받은 것으로 추정되는 R:Blue Moon(UP).pptx의 구글 드라이브 링크를 확인할 수 있다. 해당 링크를 통해 다운받은 파일의 sha1값은 다음과 같다.

6e36ba7c6f36712ad13085cab2987d9cf3e175aa

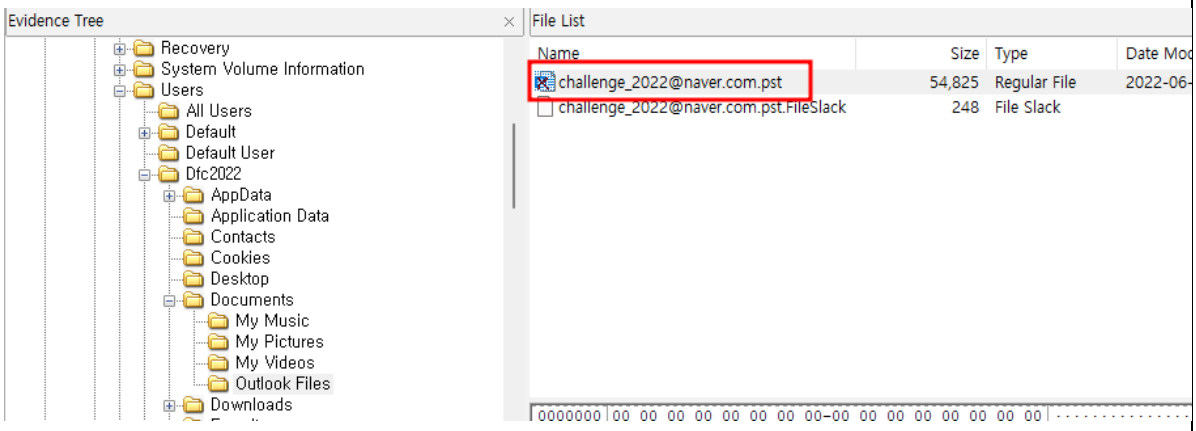
R:Blue Moon(UP).pptx 에는 암호가 걸려있었다.

2. What is the password of the file that the researcher received from the broker?



[그림 3] outlook.exe 프리패치

[root]/Windows/Prefetch/OUTLOOK.EXE-543BA3D4.pf 프리패치 파일을 통해 메일앱인 OUTLOOK.EXE를 사용한 것을 확인할 수 있다.



[그림 4] challenge_2022@naver.com.pst

그리고 [root]/Users/Dfc2022/Documents/Outllook Files 에서 삭제된 challenge_2022@naver.com.pst 파일을 찾을 수 있었다.

해당 파일을 PST Viewer를 사용하여 분석했다.

scowl_bobcats0y@icloud.c... Blue Moon Project challenge_2022@naver.com; 2022-06-22 오후 7:22:44 2022-06-22 오후 7:22:48 14

scowl_bobcats0y@icloud.c... Blue Moon Project challenge_2022@naver.com; 2022-06-22 오후 7:22:44 2022-06-22 오후 7:22:48 14

Normal Mail View | Hex | Properties | Message Header | MIME | HTML | RTF | Attachments

Path : ₩₩challenge_2022@naver.com.pst₩IPMRoot₩Top of Outlook data file₩Inbox₩ **Date Time** : 2022-06-22 오후 7:22:44

From : scowl_bobcats0y@icloud.com

To : challenge_2022@naver.com

Cc :

Bcc :

Subject : Blue Moon Project

Attachment(s) :

Hi, Challenger

I am a member of a secret team in Space Z.
I know you are very interested in the recently developed rocket engine of our company.
I can help you get the blueprints of the new motor.

Let me know if you want to get them.

Good Luck.

BlueMoon

[그림 5] 브로커의 첫 접근 메일

Sent Items

From	Subject	To	Sent	Received	Size(KB)
challenge_2022@naver.com	RE: Way to the treasure isla...	'SANS' <dfc.sans@icloud.c...	2022-06-22 오후 7:27:34	2022-06-22 오후 7:27:00	4998
challenge_2022@naver.com	RE: Blue Moon Project	'scowl_bobcats0y@icloud.c...	2022-06-23 오전 12:46:56	2022-06-23 오전 12:46:00	4
challenge_2022@naver.com	RE: Blue Moon Project	'scowl_bobcats0y@icloud.c...	2022-06-23 오전 9:43:16	2022-06-23 오전 9:43:00	4

Normal Mail View | Hex | Properties | Message Header | MIME | HTML | RTF | Attachments

Path : ₩₩challenge_2022@naver.com.pst₩IPMRoot₩Top of Outlook data file₩Sent Items₩ **Date Time** : 2022-06-23 오전 12:46:56

From : challenge_2022@naver.com

To : 'scowl_bobcats0y@icloud.com'

Cc :

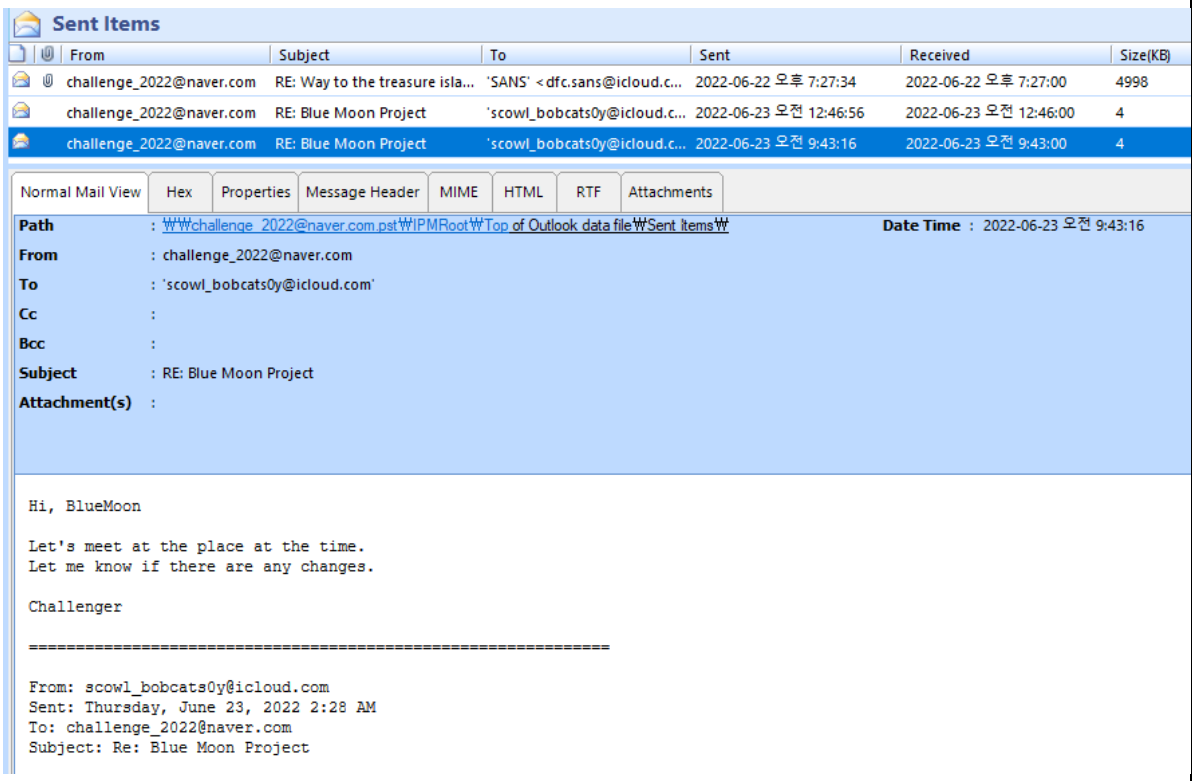
Bcc :

Subject : RE: Blue Moon Project

Attachment(s) :

```
Hi, BlueMoon

I am really interested in the space engine.
Give me any detailed information about it so that I believe that you have that.

I look forward to having your reply.

Thank you for your help in advance.

Challenger

============================================================

From: scowl_bobcats0y@icloud.com
Sent: Wednesday, June 22, 2022 7:23 PM
To: challenge_2022@naver.com
Subject: Blue Moon Project

Hi, Challenger

I am a member of a secret team in Space Z.
I know you are very interested in the recently developed rocket engine of our company.
I can help you get the blueprints of the new motor.

Let me know if you want to get them.

Good Luck.

BlueMoon
```

[그림 6] 연구원의 답장 1



[그림 7] 연구원의 답장 2

연구원과 브로커가 주고 받은 메일 내역을 확인할 수 있었으며 표로 정리하면 아래와 같다.

제목	보낸 이	시각
Blue Moon Project	scowl_bobcats0y@icloud.com	2022-06-22 19:22:48 KST
RE: Blue Moon Project	challenge_2022@naver.com	2022-06-23 00:46:00 KST
RE: Blue Moon Project	challenge_2022@naver.com	2022-06-23 09:43:00 KST

그림 7의 메일 내용을 보면 브로커가 2022-06-23 02:28에 보낸 메일에 연구원이 답장한 내용임을 확인할 수 있다. 연구원이 답장한 내용을 보면, 브로커가 보낸 메일 내용에 연구원과 브로커가 서로 만날 장소와 시간에 대한 정보가 포함되어 있던 것으로 보인다.

브로커로부터 전달받은 것으로 보이는 R:Blue Moon(UP).pptx 역시 2022-06-23 9:33:34 KST에 다운된 것을 보아 앞서 브로커가 보낸 메일을 읽은 뒤 다운받은 것으로 보이며 해당 메일에 파일 링크도 같이 포함되어 있을 것으로 보인다.

그러나 해당 메일을 challenge_2022@naver.com.pst 파일에서 찾을 수 없었다.