

## 303 – Audit My Corporation

### Team Information

Team Name : ForensicGPT

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

Email Address : forensicgpt@googlegroups.com

### Instructions

**Description** We have discovered that the report of a highly confidential forensic analysis project has been leaked to a competing company. To identify the suspect among the employees involved in the project, we have obtained audit logs and Google Drive files from the Google Workspace, which is our internal groupware system. Please analyze these logs and files to determine the leaked documents, identify the suspect, and investigate the circumstances surrounding the leak.

Target	Hash (MD5)
dfc_corp_audit.ad1	58190A85B3ACDA88F46C5650B312DEDF

### Questions

- 1) Who is the person responsible for leaking the highly confidential report? (50 points)
- 2) Describe in a timeline the entirety of the suspect's actions and describe the leak process. (100 points)
- 3) Find the original leaked confidential report. (MD5 Hash) (150 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® FTK® Imager
Version:	4.7.1.2		
URL:	<a href="https://go.exterro.com/l/43312/2023-05-03/fc4b78">https://go.exterro.com/l/43312/2023-05-03/fc4b78</a>		

Name:	Visual Studio Code	Publisher:	Microsoft
Version:	1.79.2		
URL:	<a href="https://code.visualstudio.com/download">https://code.visualstudio.com/download</a>		

Name:	CoolUtils Outlook Viewer	Publisher:	CoolUtils
Version:	4.2.0.11		
URL:	<a href="https://www.coolutils.com/">https://www.coolutils.com/</a>		

Name:	ida64	Publisher:	Hex-Rays SA
Version:	7.6.210427		
URL:	<a href="https://hex-rays.com/">https://hex-rays.com/</a>		

Name:	Hashtab	Publisher:	Implbits Software
Version:	6.0.0		
URL:	<a href="https://implbits.com">https://implbits.com</a>		

Name:	HxD	Publisher:	Maël Hörz
Version:	2.5.0.0		
URL:	<a href="https://www.mh-nexus.de">https://www.mh-nexus.de</a>		

Name:	7-zip	Publisher:	Igor Pavlov
Version:	22.01		
URL:	<a href="https://www.7-zip.org">https://www.7-zip.org</a>		

Name:	반디집	Publisher:	Bandisoft Inc.
Version:	7.25		
URL:	<a href="https://www.bandisoft.com/bandizip/">https://www.bandisoft.com/bandizip/</a>		

Name:	pestudio	Publisher:	Marc Ochsenmeier
Version:	9.53		
URL:	<a href="https://www.winitor.com/">https://www.winitor.com/</a>		

#### VM(Test) PC used:

OS:	Windows 10 pro	Version:	19044.1288
System Name:	DESKTOP-M3J1EH3		

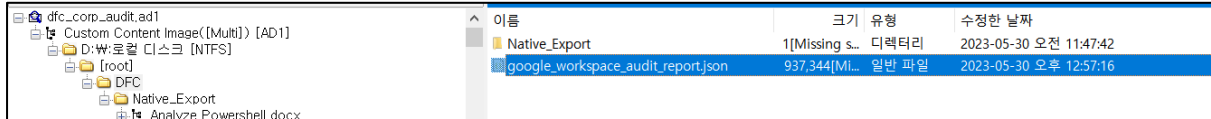
## Step-by-step methodology:



[그림 1] 증거 파일의 해시 값 확인

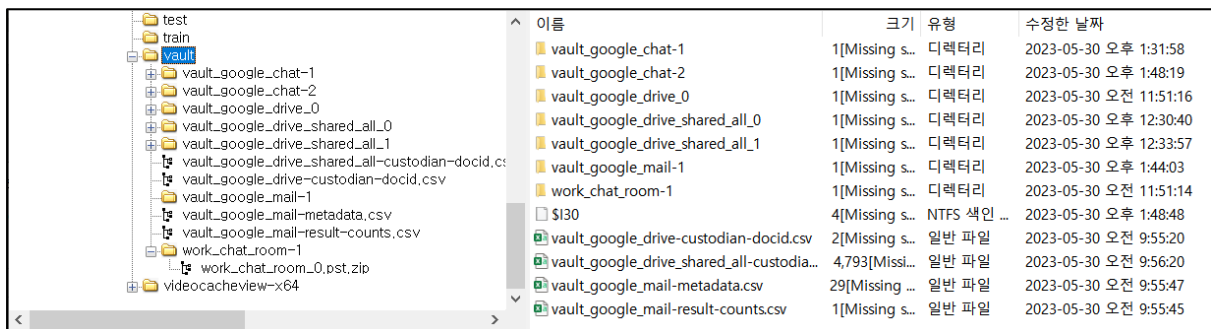
분석에 앞서, 증거 파일의 해시 값 산출을 통해 MD5 해시 값이 일치함을 확인하였습니다.

1) Who is the person responsible for leaking the highly confidential report? (50 points)



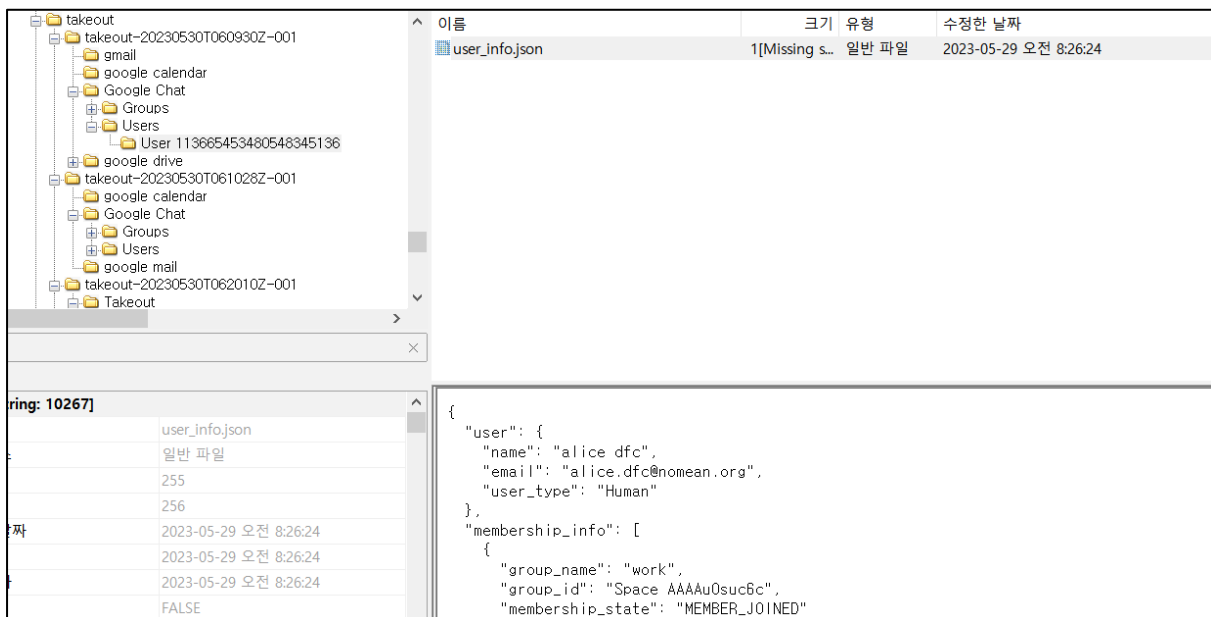
이름	크기	유형	수정한 날짜
Native_Export	1[Missing s...	디렉터리	2023-05-30 오전 11:47:42
google_workspace_audit_report.json	937,344[MI...	일반 파일	2023-05-30 오후 12:57:16

[그림 2] 증거 파일 내 audit log 파일 수집



이름	크기	유형	수정한 날짜
vault_google_chat-1	1[Missing s...	디렉터리	2023-05-30 오후 1:31:58
vault_google_chat-2	1[Missing s...	디렉터리	2023-05-30 오후 1:48:19
vault_google_drive_0	1[Missing s...	디렉터리	2023-05-30 오전 11:51:16
vault_google_drive_shared_all_0	1[Missing s...	디렉터리	2023-05-30 오후 12:30:40
vault_google_drive_shared_all_1	1[Missing s...	디렉터리	2023-05-30 오후 12:33:57
vault_google_drive_shared_all-custodian-docid.csv	1[Missing s...	디렉터리	2023-05-30 오후 1:44:03
vault_google_mail-1	1[Missing s...	디렉터리	2023-05-30 오전 11:51:14
work_chat_room-1	1[Missing s...	디렉터리	2023-05-30 오전 11:51:14
\$I30	4[Missing s...	NTFS 색인 ...	2023-05-30 오후 1:48:48
vault_google_drive-custodian-docid.csv	2[Missing s...	일반 파일	2023-05-30 오전 9:55:20
vault_google_drive_shared_all-custodia...	4,793[Missi...	일반 파일	2023-05-30 오전 9:56:20
vault_google_mail-metadata.csv	29[Missing ...	일반 파일	2023-05-30 오전 9:55:47
vault_google_mail-result-counts.csv	1[Missing s...	일반 파일	2023-05-30 오전 9:55:45

[그림 3] 증거 파일 내 google drive, chat, mail 관련 파일 수집



이름	크기	유형	수정한 날짜
user_info.json	1[Missing s...	일반 파일	2023-05-29 오전 8:26:24

이름	크기	유형	수정한 날짜
user_info.json	255	일반 파일	2023-05-29 오전 8:26:24
	256		2023-05-29 오전 8:26:24
			2023-05-29 오전 8:26:24
			FALSE

```

{
  "user": {
    "name": "alice dfc",
    "email": "alice.dfc@nonean.org",
    "user_type": "Human"
  },
  "membership_info": [
    {
      "group_name": "work",
      "group_id": "Space AAAAu0suc6c",
      "membership_state": "MEMBER_JOINED"
    }
  ]
}

```

[그림 4] takeout 폴더 수집

FTK Imager를 통해 증거 파일 내 Google drive, chat, mail과 관련 있는 파일들과 DFC 폴더 내에 존재하는 google\_workspace\_audit\_resport.json 파일을 export 를 통해 수집하였습니다. 또한, 그림 4와 같이 workspace와 관련된 파일이 포함된 takeout 폴더를 export를 통해 수집하였습니다.

Email	AccountStatus	SuccessCount	MessageErrorCount	ChatErrorCount
Totals		94	0	0
delta.dfc@nomean.org	Success	40	0	0
echo.dfc@nomean.org	Success	17	0	0
bravo.dfc@nomean.org	Success	14	0	0
charlie.dfc@nomean.org	Success	12	0	0
alice.dfc@nomean.org	Success	11	0	0

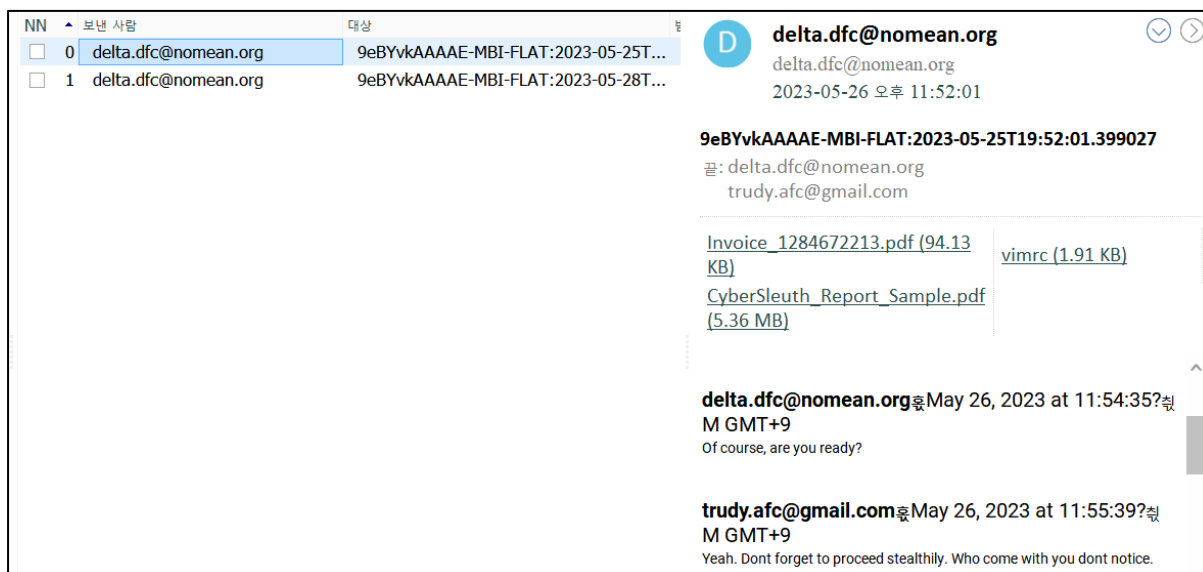
[그림 5] vault\_google\_mail-result-counts.csv 내 존재하는 계정 식별

수집한 Vault 폴더 내 vault\_google\_mail-result-counts.csv 파일에서는 프로젝트 관련 직원들의 메일을 확인할 수 있습니다.

delta.dfc@nomean.org	^DELETED,^DRAFT,^OLD VER delta.dfc@nomean.org	[business mail]_The newest episode.	trudy.afc@gmail.com
delta.dfc@nomean.org	^DELETED,^DRAFT,^OLD VER delta.dfc@nomean.org	[business mail]_The newest episode.	trudy.afc@gmail.com
delta.dfc@nomean.org	^DELETED,^DRAFT,^OLD VER delta.dfc@nomean.org	[business mail]_The newest episode.	trudy.afc@gmail.com
delta.dfc@nomean.org	^DELETED,^DRAFT,^OLD VER delta.dfc@nomean.org	[business mail]_The newest episode.	trudy.afc@gmail.com
delta.dfc@nomean.org	^DELETED,^DRAFT,^OLD VER delta.dfc@nomean.org	[business mail]_The newest episode.	trudy.afc@gmail.com
delta.dfc@nomean.org	^DELETED,^DRAFT,^OLD VER delta.dfc@nomean.org	[business mail]_The newest episode.	trudy.afc@gmail.com
delta.dfc@nomean.org	^DELETED,^DRAFT,^OLD VER delta.dfc@nomean.org	[business mail]_The newest episode of The Bit is out n	trudy.afc@gmail.com
delta.dfc@nomean.org	^DELETED,^DRAFT,^OLD VER delta.dfc@nomean.org	[business mail]_	trudy.afc@gmail.com
delta.dfc@nomean.org	^DELETED,^DRAFT,^OLD VER delta.dfc@nomean.org	[business mail]_	trudy.afc@gmail.com
delta.dfc@nomean.org	^DELETED,^DRAFT,^OLD VER delta.dfc@nomean.org	[business mail]_	trudy.afc@gmail.com
delta.dfc@nomean.org	^DELETED,^DRAFT,^OLD VER delta.dfc@nomean.org	[business mail]_	trudy.afc@gmail.com
delta.dfc@nomean.org	^DELETED,^DRAFT,^OLD VER delta.dfc@nomean.org	[business mail]_	trudy.afc@gmail.com
delta.dfc@nomean.org	^DELETED,^DRAFT,^OLD VER delta.dfc@nomean.org	[business mail]_	trudy.afc@gmail.com
delta.dfc@nomean.org	^DELETED,^DRAFT,^OLD VER delta.dfc@nomean.org	[business mail]_	trudy.afc@gmail.com
delta.dfc@nomean.org	^DELETED,^DRAFT,^OLD VER delta.dfc@nomean.org	[business mail]_	trudy.afc@gmail.com
delta.dfc@nomean.org	^DELETED,^DRAFT,^OLD VER delta.dfc@nomean.org	[]	trudy.afc@gmail.com
delta.dfc@nomean.org	^DELETED,^DRAFT,^OLD VER delta.dfc@nomean.org		trudy.afc@gmail.com

[그림 6] 삭제된 라벨을 가지고 있는 row 행 확인

또한, vault 폴더 내 valut\_google\_mail-metadata.csv 파일에서는 메일 관련 메타데이터를 확인할 수 있는데, 위 그림에서 확인했던 직원 계정 외의 **trudy.afc@gmail.com** 라는 nomean.org 도메인을 사용하지 않는 계정이 발견되었습니다.



[그림 7] pst 파일 내 확인된 두 계정 식별

Vault 폴더 내 vault\_google\_chat\_delta\_0.pst 파일을 coolutils outlook viewer로 확인해보았고, 앞선 메일 메타데이터와 관련 있는 두 계정 delta.dfc@nomean.org 과 trudy.afc@gamil.com 간에 주고받은 내용을 살펴볼 수 있었습니다.

[표 1] delta.dfc@nomean.org와 trudy.afc@gmail.com 간의 대화 발체 내용

**delta.dfc@nomean.org** ㄹ May 26, 2023 at 11:52:01? ㄹ M GMT+9  
Hi, Trudy are you there?

**trudy.afc@gmail.com** ㄹ May 26, 2023 at 11:53:57? ㄹ M GMT+9  
Yep, im here. Did You arrive in our city??

**delta.dfc@nomean.org** ㄹ May 26, 2023 at 11:54:35? ㄹ M GMT+9  
Of course, are you ready?

**trudy.afc@gmail.com** ㄹ May 26, 2023 at 11:55:39? ㄹ M GMT+9  
Yeah. Dont forget to proceed stealthily. Who come with you dont notice.

**delta.dfc@nomean.org** ㄹ May 26, 2023 at 11:55:55? ㄹ M GMT+9  
got it see you soon.

**trudy.afc@gmail.com** ㄹ May 26, 2023 at 11:56:07? ㄹ M GMT+9  
Okay. Good luck

**delta.dfc@nomean.org** ㄹ May 27, 2023 at 12:18:00? ㄹ M GMT+9  
Did you receive the invitation well?

**trudy.afc@gmail.com** ㄹ May 27, 2023 at 12:18:28? ㄹ M GMT+9  
Sure i alreay join meeting.

**delta.dfc@nomean.org** ㄹ May 27, 2023 at 1:07:16? ㄹ M GMT+9  
Invoice\_1284672213.pdf

**delta.dfc@nomean.org** ㄹ May 27, 2023 at 1:07:57? ㄹ M GMT+9  
vimrc

**delta.dfc@nomean.org** ㄹ May 27, 2023 at 1:08:26? ㄹ M GMT+9

**delta.dfc@nomean.org** ㄹ May 27, 2023 at 1:10:45? ㄹ M GMT+9

here is sample report

CyberSleuth\_Report\_Sample.pdf

-----  
**delta.dfc@nomean.org** ㄹ May 30, 2023 at 2:42:30? ㄹ M GMT+9

Hey trudy, are you downloaded??

**trudy.afc@gmail.com** ㄹ May 30, 2023 at 2:43:14? ㄹ M GMT+9

Yep. I downloaded it. But i can't check it????

**delta.dfc@nomean.org** ㄹ May 30, 2023 at 2:44:11? ㄹ M GMT+9

Encryption is applied for security. I'll pass it over a more encrypted channel. let's wait and see

**delta.dfc@nomean.org** ㄹ May 30, 2023 at 2:48:49? ㄹ M GMT+9

First of all, take this well and keep it. i'll be in touch soon. This might lead you to data.

**delta.dfc@nomean.org** ㄹ May 30, 2023 at 2:49:08? ㄹ M GMT+9

tell me if you downloaded

**trudy.afc@gmail.com** ㄹ May 30, 2023 at 2:49:55? ㄹ M GMT+9

I can't access it. Would you share about link??

**delta.dfc@nomean.org** ㄹ May 30, 2023 at 2:50:37? ㄹ M GMT+9

Okay, here you are,

[https://docs.google.com/presentation/d/1\\_pJAoOwqMu2nWveJi6pmUNw5IPbiqXv/edit?usp=share\\_link&oid=115830431782957231483&rtpof=true&sd=true](https://docs.google.com/presentation/d/1_pJAoOwqMu2nWveJi6pmUNw5IPbiqXv/edit?usp=share_link&oid=115830431782957231483&rtpof=true&sd=true)

[https://drive.google.com/open?id=1\\_pJAoOwqMu2nWveJi6pmUNw5IPbiqXv](https://drive.google.com/open?id=1_pJAoOwqMu2nWveJi6pmUNw5IPbiqXv)

[https://docs.google.com/presentation/d/1\\_pJAoOwqMu2nWveJi6pmUNw5IPbiqXv/edit?usp=share\\_link&oid=115830431782957231483&rtpof=true&sd=true](https://docs.google.com/presentation/d/1_pJAoOwqMu2nWveJi6pmUNw5IPbiqXv/edit?usp=share_link&oid=115830431782957231483&rtpof=true&sd=true)

**trudy.afc@gmail.com** ㄹ May 30, 2023 at 2:59:51? ㄹ M GMT+9

I can't download it. Any other way????

**delta.dfc@nomean.org** ㄹ May 30, 2023 at 3:00:04? ㄹ M GMT+9

okay, wait..

**delta.dfc@nomean.org** ㄹ May 30, 2023 at 3:04:03? ㄹ M GMT+9

Here!!

presentation.zip

**trudy.afc@gmail.com** ㄹ May 30, 2023 at 3:04:54? ㄹ M GMT+9

Nice got it. I downloaded it!

**delta.dfc@nomean.org** ㄹ May 30, 2023 at 3:05:28? ㄹ M GMT+9

okay. I'll leave this chat room



위 내용에서 보이는 은밀성과 암호화, 그리고 파일을 주고 받는 부분과 본 유출 사건을 토대로 미루어 보았을 때, 극비 보고서 유출 직원은 delta.dfc@nomean.org 계정을 가진 사람으로 판단하였습니다.

```
{
  "user": {
    "name": "delta dfc",
    "email": "delta.dfc@nomean.org",
    "user_type": "Human"
  },
  "membership_info": [
    {
      "group_id": "DM 9eBYvkAAAAE",
      "membership_state": "MEMBER_JOINED"
    }
  ],
}
```

[그림 8] user\_info.json 내 이름 식별

```
1  {
2    "members": [
3      {
4        "name": "delta dfc",
5        "email": "delta.dfc@nomean.org",
6        "user_type": "Human"
7      },
8      {
9        "name": "trudy AFC",
10       "email": "trudy.afc@gmail.com",
11       "user_type": "Human"
12     }
13   ]
14 }
```

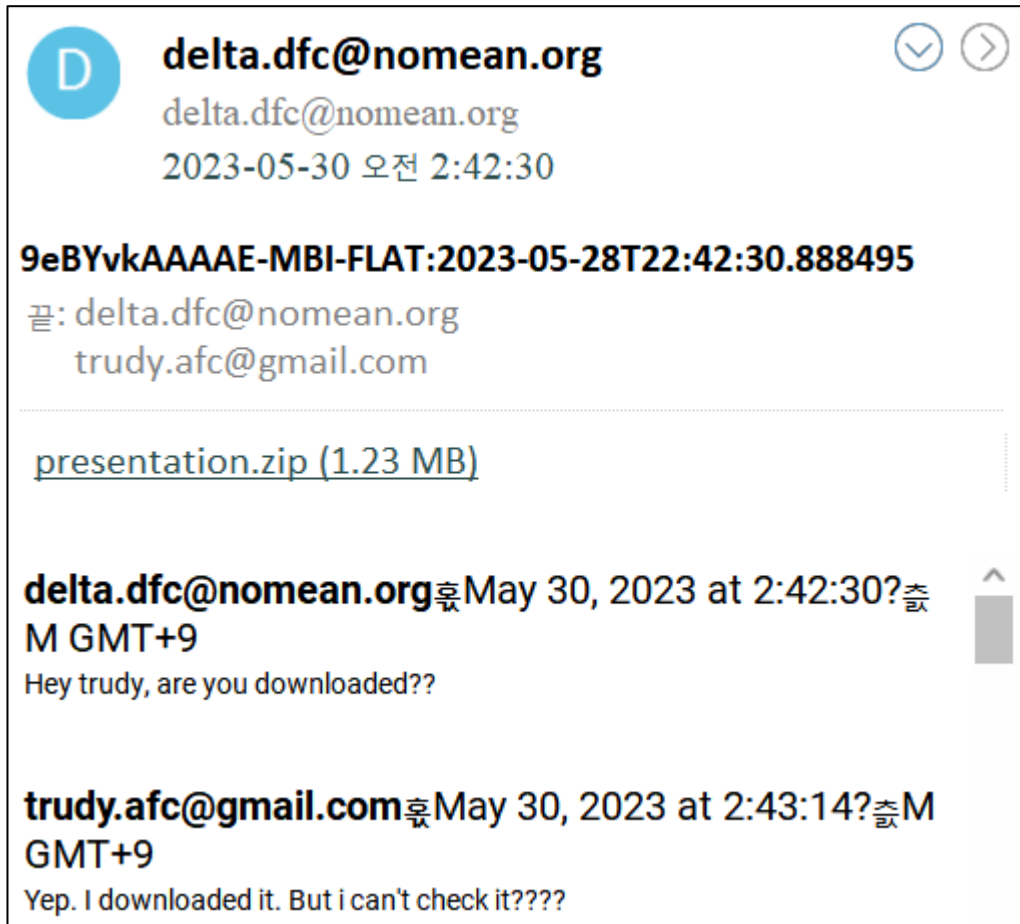
[그림 9] delta의 DM 9eBYvkAAAAE chat room group info

takeout 폴더 내 delta의 그룹 중 DM 9eBYvkAAAAE라는 폴더가 존재합니다. 해당 폴더는 space로 시작하지 않기 때문에 DM chat이며, 그룹 정보에 trudy가 있는 것을 확인하였습니다.

따라서, 종합해보았을 때 극비 보고서 유출 직원의 이름은 **delta dfc**, 계정은 **delta.dfc@nomean.org**로 판단하였습니다.

2) Describe in a timeline the entirety of the suspect's actions and describe the leak process. (100 points)

용의자의 행동과 유출 과정을 개략적으로 설명하기 위해 먼저 분석 기준 시각을 설정하였습니다.



[그림 10] delta와 trudy 간의 주고받은 메일 두번째 대화 내용


vault\_google\_chat\_delta\_0.pst 파일 내 첫번째 대화와 두번째 대화 내용을 살펴보면 위 [표 1]에서도 알 수 있듯이, 2023-05-27 오전 01:10:45(GMT+9)에 delta가 sample report를 전송하고, 약 3일 뒤 2023-05-30 오전 02:42:30(GMT+9)에 delta가 다운로드를 받았는지 물어보는 부분이 존재합니다.

그러나 sample report 파일은 실제로 해당 뷰어에서 다운받은 후 정상적으로 열리기 때문에, 해당 두 시간 간격 사이에 의심스러운 다른 report 유출 흔적을 찾기 위해 2023-05-30 오전 02:42:30(GMT+9) 시각을 분석 기준 시각으로 잡고 시간 관련 정보가 포함된 google\_workspace\_audit\_report 파일과 delta의 mail 파일에서 전후를 살펴보았습니다.

28	Gmail 팀	Gmail 앱을 다운로드하세요!	delta dfc	6	Gmail 팀	Gmail 앱을 다운로드하세요!	alice dfc
29	Gmail 팀	새 받은편지함 사용 관련 도움말	delta dfc	5	Gmail 팀	새 받은편지함 사용 관련 도움말	alice dfc
27	Admin Jin	Welcome to our team at DFC Corp!!	alice dfc,bravo dfc,	4	Admin Jin	Welcome to our team at DFC Corp!!	alice dfc,bravo d...
26	Admin Jin(Google Dri...	공유 드라이브 DFC_Shared에 추가됨	delta dfc@nomean.	3	Admin Jin(Google Drive에서 전...	공유 드라이브 DFC_Shared에 추가됨	alice dfc@nome...
25	delta dfc	Re: Welcome to our team at DFC Corp!!	Admin Jin	2	alice dfc	Re: Welcome to our team at DFC Corp!!	Admin Jin
39	echo.dfc@nomean.org	Invitation: weekly meeting @ Mon 29 May 2023...	delta.dfc@nomean.	10	delta.dfc@nomean.org	Invitation: Weekly @ Tue May 23, 2023...	alice.dfc@nome...
38	echo.dfc@nomean.org	Invitation: forensic study @ Thu 1 Jun 2023 10a...	delta.dfc@nomean.	9	echo.dfc@nomean.org	Invitation: weekly meeting @ Mon May...	alice.dfc@nome...
37	delta.dfc@nomean.org	Accepted: Training Sessions @ Weekly from 3p...	delta.dfc@nomean.	8	alice.dfc@nomean.org	Accepted: Training Sessions @ Weekly...	alice.dfc@nome...
36	admin@nomean.org	Invitation: digital forensic workshop @ Fri 26 M...	delta.dfc@nomean.	7	admin@nomean.org	Invitation: digital forensic workshop @ ...	alice.dfc@nome...
35	delta.dfc@nomean.org	Accepted: collaboration meeting with APC. @ S...	delta.dfc@nomean.	1	Admin Jin	[work] It is our project report	alice dfc,bravo d...
24	Admin Jin	Re: 초대장: collaboration meeting with APC. - 20...	delta dfc bravo	0	Admin Jin	[Notice] Regret Regarding Information...	alice dfc,bravo d...
34	delta.dfc@nomean.org	Accepted: collaboration meeting with APC. @ S...	delta.dfc@nomean.				
33	delta.dfc@nomean.org	Accepted: collaboration meeting with APC. @ S...	delta.dfc@nomean.				
32	delta.dfc@nomean.org	Accepted: collaboration meeting with APC. @ S...	delta.dfc@nomean.				
23	delta dfc						
22	Admin Jin	[work] It is our project report	alice dfc,bravo dfc,				
31	delta.dfc@nomean.org	Accepted: work meeting @ Tue 30 May 2023 2a...	delta.dfc@nomean.				
30	delta.dfc@nomean.org	Accepted: work meeting @ Tue 30 May 2023 8a...	delta.dfc@nomean.				
21	delta dfc	Re: Accepted: work meeting @ Tue 30 May 202...	trudy AFC				

[그림 11] delta 계정 메일함(좌), alice 계정 메일함(우)

vault\_google\_mail—delta.dfc 파일에는 다른 직원보다 훨씬 많은 메일을 확인할 수 있습니다.



**Admin Jin**  
 admin@nomean.org  
 2023-05-30 오전 12:52:17

**[work] It is our project report**

끝: alice dfc <alice.dfc@nomean.org>  
 bravo dfc <bravo.dfc@nomean.org>  
 charlie dfc <charlie.dfc@nomean.org>  
 delta dfc <delta.dfc@nomean.org>  
 echo dfc <echo.dfc@nomean.org>

**Dear Alice, Bravo, Charlie, Delta, and Echo,**

I hope this email finds you well. I would like to share with you the project report that we have been working on. You can access the document using the Google Drive link provided below:

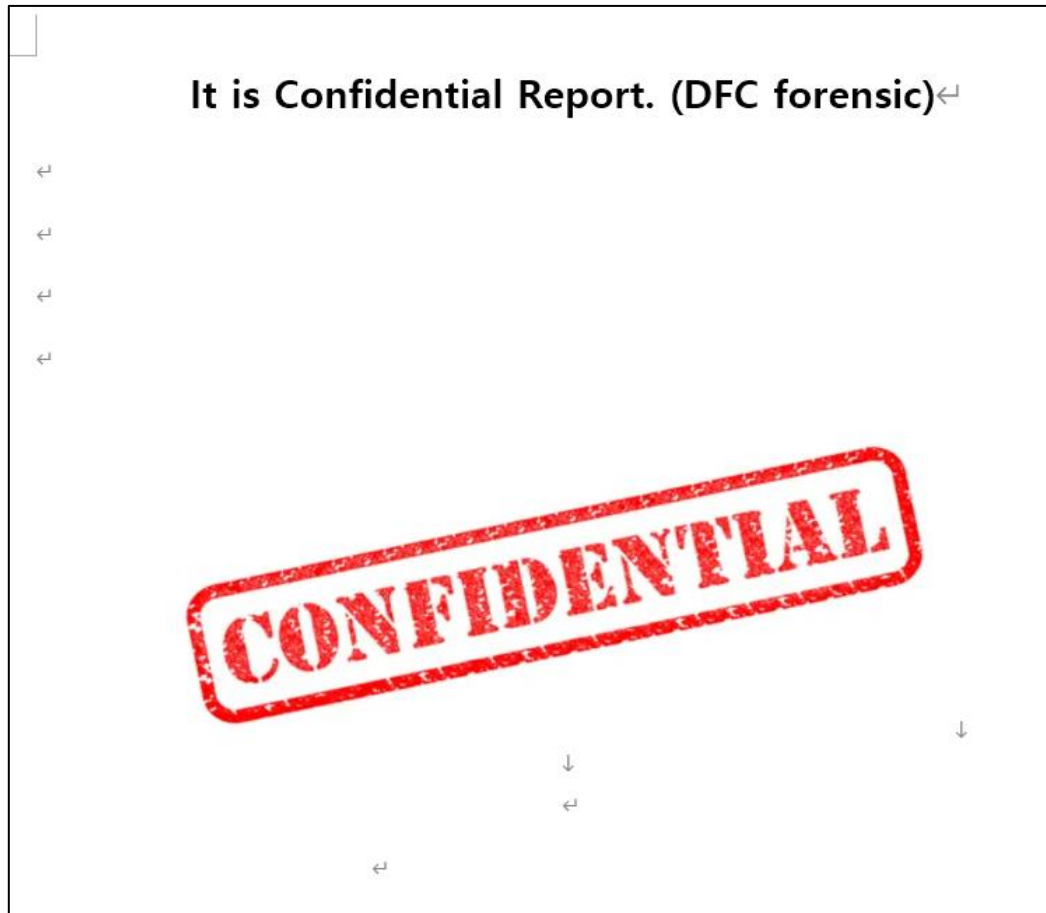
[Google Drive Link: Project Report](https://docs.google.com/document/d/1C9sDRd2DgqC8MhOfn3v81Hh82hGk_Avq/edit?usp=sharing)

We have put considerable effort into this report, and I believe it provides a comprehensive overview of our project's progress and outcomes. However, before finalizing it, I would appreciate your valuable input and feedback to ensure its accuracy and completeness.

[그림 12] Project Report 관련 메일

모든 직원에게 발송된 위 그림 속 메일은 본 사건과 관련이 있는 프로젝트 Report로 정황상 판단됩니다. 해당 구글 드라이브 링크는 다음과 같았습니다.

**[https://docs.google.com/document/d/1C9sDRd2DgqC8MhOfn3v81Hh82hGk\\_Avq/edit?usp=sharing](https://docs.google.com/document/d/1C9sDRd2DgqC8MhOfn3v81Hh82hGk_Avq/edit?usp=sharing)**



[그림 13] 1C9sDRd2DgqC8MhOfn3v81Hh82hGk\_Avq 파일 내용 확인

해당 구글 드라이브 링크는 현재 접속되지 않지만, Vault 폴더 내 google\_drive\_0 폴더에서 URL 속에서 본 doc id와 동일한 id를 가진 파일을 확인할 수 있었습니다. 해당 파일을 열어보면 confidential report 임을 확인할 수 있었습니다.

다만, 실제로 delta가 trudy에게 보낸 유출 report가 해당 doc id를 가진 report인지는 모르기 때문에 추가 분석을 수행하기 위해 google\_workspace\_audit\_report.json 파일 분석을 진행하였습니다.

```
import json

def split_json_file(input_filepath, num_files):
    with open(input_filepath, "r") as input_file:
        json_data = json.load(input_file)

    lines_per_file = len(json_data) // num_files
    remaining_lines = len(json_data) % num_files
    splits = []
    start = 0
    for i in range(num_files):
        lines = lines_per_file + (1 if remaining_lines > 0 else 0)
        splits.append(json_data[start:start + lines])
        start += lines
        remaining_lines -= 1

    for index, split in enumerate(splits):
        with open(f"output_{index}.json", "w") as output_file:
            json.dump(split, output_file, indent=4)

input_filepath = "google_workspace_audit_report.json"
num_files = 20

split_json_file(input_filepath, num_files)
```

[그림 14] 파일 분할 코드

google\_workspace\_audit\_report.json 파일의 크기가 커서 해당 파일을 20개의 파일로 분할하여 살펴보았고, 분석 기준 시각 2023-05-30 오전 02:42:30(GMT+9) 이전에 delta가 trudy에게 보낸 흔적을 다음과 같은 표로 정리하였습니다.

- **2023-05-30 오전 02:42:30 (GMT +9) 이전 주요 타임라인**

[표 2] audit report log를 통해 delta가 수행한 행위 기반 타임라인 구성

타임라인	설명	event
2023-05-29T16:51:33.039Z (2023-05-30 01:51:33.039, UTC+9)	delta가 doc id 1C9sDRd2DgqC8MhOfn3v81Hh82hGk_Avq에 해당하는 [DFC]_Forensic_Report.docx를 다운로드	download
2023-05-29T17:22:32.045Z (2023-05-30 02:22:32.045, UTC+9)	delta가 team project에서 작업하던 [DFC]_Forensic_Report.docx를 삭제. Doc id는 1C9sDRd2DgqC8MhOfn3v81Hh82hGk_Avq	trash
2023-05-29T17:23:15.620Z (2023-05-30 02:23:15.620, UTC+9)	delta가 doc id 1C1Viz_EbP50SDSmZ5G2AVFYWkduDuSZE인데	upload, edit, add_to_folder

	제목은 [DFC]_Forensic_Report.docx인 파일을 드라이브에 업로드. 업로드 후에 report폴더에 추가.	
2023-05-29T17:23:29.734Z (2023-05-30 02:23:29.734, UTC+9)	delta가 [DFC]_Forensic_Report.docx를 사본 만들기(source_copy)를 통해 "[DFC]_Forensic_Report.docx의 사본"을 생성. 기존의 [DFC]_Forensic_Report.docx의 doc id는 1C1Viz_EbP50SDSmZ5G2AVFYWkduDuSZE. delta가 생성한 [DFC]_Forensic_Report.docx의 사본의 doc_id는 12sVRnsytVypNPu93xmkSkrkFyH9tHw3x 수정 후, report라는 폴더에 추가.	source_copy, edit, add_to_folder
2023-05-29T17:23:47.770Z (2023-05-30 02:23:47.770, UTC+9)	delta가 '[DFC]_Forensic_Report.docx의 사본'이라는 이름을 가진 파일을 Sample_Template.docx로 이름 변경.(doc_id는 동일)	rename, edit
2023-05-29T17:25:24.433Z (2023-05-30 02:25:24.433, UTC+9)	delta가 doc_id가 12sVRnsytVypNPu93xmkSkrkFyH9tHw3x인 Sample_Template.docx를 people_with_link 권한으로 바꾸고, acl_change를 통해 접근 권한을 링크를 가진 사람이 볼 수 있도록 변경하고 visibility를 external로 변경.	edit, acl_change (change_document_visibility, change_document_access_scope)

이를 통해, delta는 google drive에서 팀 프로젝트로 작업하던 '[DFC]\_Forensic\_Report.docx' 파일을 다운로드 한 후, 기존의 파일을 삭제하고 동일한 파일 이름으로 다시 업로드하여 파일이름을 바꾸고 접근권한을 수정하였음을 알 수 있습니다.

- 2023-05-30 오전 02:42:30 (GMT +9) 전후 trudy로 추정되는 흔적

[표 3] trudy로 추정되는 용의자가 수행한 행위 기반 타임라인

타임라인	설명	event
2023-05-29T17:26:25.856Z (2023-05-30 02:26:25.856, UTC+9) ~ 2023-05-29T17:51:16.000Z (2023-05-30 02:51:16.000, UTC+9)	trudy로 추정되는 용의자가 doc id가 12sVRnsytVypNPu93xmkSkrkFyH9tHw3x인 Sample_Template.docx를 다수 확인.	view
2023-05-29T17:29:51.558Z (2023-05-30 02:29:51.558, UTC+9) 2023-05-29T17:32:03.514Z (2023-05-30 02:32:03.514, UTC+9)	trudy로 추정되는 용의자가 Sample_Template.docx를 다운로드	download

google\_workspace\_audit\_report.json 파일에서는 profile Id가 105250506097979753968 인 로그를 살펴볼 수 있었습니다. 팀 프로젝트 직원들의 id에 포함되지 않는 id이며, email 정보도 기록되어 있지 않았습니다.

또한, delta가 doc id 12sVRnsytVypNPu93xmkSkrkFyH9tHw3x 에 해당하는 파일을 업로드하고 접근권한을 변경한 이후 시각부터 trudy로 추정되는 용의자가 동일한 doc\_id에 해당하는 파일을 보고, 다운로드하였음을 확인할 수 있었습니다.

이름	크기	유형	수정한 날짜
Sample_Template.docx	5,269[Missi...	일반 파일	2023-05-29 오전 8:26:24
[DFC]_Forensic_Report.docx	5,269[Missi...	일반 파일	2023-05-29 오전 8:26:24

[그림 15] project – report 폴더 내 delta가 업로드한 파일 존재 확인

또한, FTK Imager상에서도 audit report log에 기반하여 delta가 업로드한 파일을 확인할 수 있었습니다.

- 2023-05-30 오전 02:42:30 (GMT +9) 이후 delta의 주요 행위

[표 4] 분석 기준 시각 이후 delta 주요 행위 – google workspace audit log

타임라인	설명
2023-05-29T17:48:49.429Z 2023-05-30 02:48:49.429(GMT+9)	delta가 room_id가 9eBYvkAAAAE이고 room_name이 빈 chat room에서 0ebdca4abc6ea14bc3f01139c9e027cc84f2ad88852ee34918bf98a981372f33라는 sha256 해시 값을 가진 presentation.pptx를 첨부파일로 업로드. 해당 파일은 DLP_SCANNED 상태
2023-05-29T18:04:03.303Z 2023-05-30 03:04:03.303(GMT+9)	delta가 room_id가 9eBYvkAAAAE이고 room_name이 빈 chat room에서 fb1afa8815f71effd097aed0b82d9a9b397c5286b42122b041cb59646f0d6a91라는 sha256 해시 값을 가진 presentation.zip 파일을 첨부파일로 업로드. 해당 파일은 DLP_SCAN_FAILED 상태

- 2023-05-30 오전 02:42:30 (GMT +9) 이후 delta의 주요 행위

[표 5] 분석 기준 시각 이후 delta의 주요 행위 – 메일

타임라인	설명
2023-05-30 오전 02:50:37(GMT+9)	[표 1]에서와 같이 trudy에게 다음의 링크를 보냄. <a href="https://docs.google.com/presentation/d/1_pJAoOwqMu2nWveJi6pmUNw5IPibiqXv/edit?usp=share_link&amp;oid=115830431782957231483&amp;rtpof=true&amp;sd=true">https://docs.google.com/presentation/d/1_pJAoOwqMu2nWveJi6pmUNw5IPibiqXv/edit?usp=share_link&amp;oid=115830431782957231483&amp;rtpof=true&amp;sd=true</a>
2023-05-30 오전 03:04:03(GMT+9)	trudy가 다운로드 되지 않는다고 하자 presentation.pptx를 암호화해서 압축한 presentation.zip 파일을 전송.
2023-05-30 오전 03:15:25(GMT+9)	trudy에게 Google Meet 초대 메일과 함께 수상한 값을 보냄. <ul style="list-style-type: none"> <li>● 내용</li> </ul> Hey, take a look at this. it is first. 6c4575c9ec1709de06f48546004a7d0f



2023-05-30 오전 03:17:04(GMT+9)	trudy에게 한 번 더 수상한 값을 보냄. <ul style="list-style-type: none"> <li>● 내용</li> </ul> You will need more of this. Please note.  b3ad8aa05409cbec4578117f12b2f835
-------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------

delta는 trudy에게 유출한 report에 대해 암호화가 걸려있으니 더 암호화된 채널로 보내겠다고 말하면서 data를 얻을 수 있도록 해주는 presentation.pptx를 먼저 전송해주었습니다. 그 후, trudy가 파일이 열리지 않는다고 하자 delta는 google drive link로 전송해주었습니다. trudy가 다운로드에 실패하자 마지막으로 delta는 zip파일로 암호화해서 presentation.pptx파일을 전송해주었습니다. 그 후, delta는 trudy에게 암호화된 채널로 추측되는 google meet를 통해서 수상한 16byte의 값 두 개를 전송하였습니다.

결론적으로, 분석 기준 시각 전후로 살펴본 delta와 trudy의 행위 기반 타임라인을 통해 분석이 필요한 파일들을 다음과 같이 정리하였습니다.

파일
<p><b>[DFC]_Forensic_Report.docx, Sample_Template.docx, presentation.pptx, presentation.zip</b></p>

### 3) Find the original leaked confidential report. (MD5 Hash) (150 points)

Vault폴더 내 vault\_google\_drive\_0 폴더에는 앞서 살펴본 doc id에 해당하는 파일들이 모두 존재했습니다.

- -DFC-\_Forensic\_Report\_1C9sDRd2DgqC8MhOfn3v81Hh82hGk\_Avq.docx
- -DFC-\_Forensic\_Report\_1C1Viz\_EbP50SDSmZ5G2AVFYWkduDuSZE.docx
- Sample\_Template.docx\_12sVRnsytVypNPu93xmkSkrkFyH9tHw3x.docx의 사본
- presentation\_1\_pJAoOwqMu2nWveJi6pmUNw5lPlbiqXv.pptx

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	40	97	46	1E	15	35	8D	60	47	C5	6F	9A	33	EB	18	BF	[-F..5.`GÅoš3ë.¿
00000010	66	08	B9	40	06	D4	2C	E6	EE	27	21	FB	DB	4E	F2	D1	f.²@.Ô,æi'!ûÛNòÑ
00000020	8A	C2	B8	E2	26	21	8B	CD	31	B4	67	43	F8	88	A4	D6	ŠÂ,â&!<Íl'gCø`»Ö
00000030	3E	D8	E5	7E	27	22	33	0D	5F	A1	3B	E1	49	04	1A	6D	>Øâ~'"3._;áI..m
00000040	AB	87	D2	FD	D0	6D	D9	85	21	D2	F6	A6	4D	96	54	7E	«+ÖýDmÜ...!Öö;M-T~
00000050	44	81	CE	DA	20	1A	01	EF	A0	E2	B9	47	A9	7B	6F	DA	D.ÎÚ ..i â²G@{oÚ
00000060	0F	E3	22	80	30	92	5F	90	F7	E8	94	60	90	8E	72	D5	.ã"€0'_.÷è"`.ŽrÖ
00000070	CB	50	F8	2D	66	A9	6C	86	10	C6	54	17	4C	1C	CC	2D	ËPø-f@l+.ÆT.L.Ï-

[그림 16] Sample\_Template.docx의 파일 헤더 시그니처

project-report 폴더 내 위치하던 파일 헤더 시그니처는 위 그림과 같이 정상적인 docx파일 헤더 시그니처가 아니었고, 앞서 살펴본 정황 상 암호화된 것으로 판단하였습니다. 또한, 두 파일의 해시 값은 다음과 같이 동일하였습니다.

- **md5 : E6C30FEC686AD2ACEBCCE44D4D1E514A**
- **sha1 : 0C12B341A49A51F50ADBCC16A830D1D08411381E**

따라서, audit report 로그에서 확인한 결과를 바탕으로 원본 유출 기밀 보고서는 팀 프로젝트에서 작업하던 1C9sDRd2DgqC8MhOfn3v81Hh82hGk\_Avq라는 doc id를 가진 파일이라고 가정하고 동일성 검증을 위해 추가 분석을 진행하였습니다.

pptx 파일을 살펴보면,

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	4D	5A	90	00	03	00	04	00	00	00	00	00	FF	FF	00	00	MZ.....yy..
00000010	8B	00	00	00	00	00	00	00	40	00	00	00	00	00	00	00	<.....@.....
00000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000030	00	00	00	00	00	00	00	00	00	00	00	00	80	00	00	00	.....€...
00000040	0E	1F	BA	0E	00	B4	09	CD	21	B8	01	4C	CD	21	54	68	..°..'.í!.Lí!Th
00000050	69	73	20	70	72	6F	67	72	61	6D	20	63	61	6E	6E	6F	is program canno
00000060	74	20	62	65	20	72	75	6E	20	69	6E	20	44	4F	53	20	t be run in DOS
00000070	6D	6F	64	65	2E	0D	0D	0A	24	00	00	00	00	00	00	00	mode....\$......

[그림 17] presentation.pptx의 파일 헤더 시그니처 확인

delta가 trudy에게 보냈던 presentation.pptx 관련 link에서 확인할 수 있는 doc id와 일치하는 파일의 헤더 시그니처를 살펴보았을 때, 해당 파일은 MZ로 시작하여 exe 파일임을 확인하였습니다. 해당 파일은 또한, project 폴더 경로에 위치한 presentation.pptx와 sha1 hash값이 210EBB913849BCB2A0B206AE2A57D9D86075F6F6로 동일함을 확인하였습니다.

c:\users\wehfeh\Desktop#2023dfc#303 - audit	engine (71/71)	score (8/71)	date (dd.mm.yyyy)	age (days)
indicators (wait...)	Elastic	malicious (moderate confidence)	31.05.2023	52
footprints (wait...)	Cynet	Malicious (score: 100)	06.06.2023	46
virustotal (8/71)	APEX	Malicious	04.06.2023	48
> dos-header (64 bytes)	McAfee-GW-Edition	BehavesLike.Win64.BackdoorCobaltStr.vh	06.06.2023	46
> dos-stub (wait...)	Ikarus	Trojan.WinGo.Shellcoderunner	06.06.2023	46
> rich-header (n/a)	Google	Detected	06.06.2023	46
> file-header (Amd64)	Acronis	suspicious	19.02.2023	153
> optional-header (console)	DeepInstinct	MALICIOUS	28.05.2023	55
> directories (3)				

[그림 18] presentation\_1\_pJAoOwqMu2nWveJi6pmUNw5IPlbiqXv.pptx 파일 정보

또한, virus total 상에서 악성 파일로 탐지되었기 때문에 앞서 delta가 link를 보냈을 때 다운로드에 실패했음을 판단할 수 있었습니다.

따라서, 지금껏 살펴본 정황상 delta가 trudy에게 건네준 16 bytes value 2개의 단서와 현재 docx파일을 암호화하는 암호화 파일로 추정되는 exe파일을 통해 ida 분석을 진행해야 하는 것으로 판단하였습니다.

분석에 앞서, delta가 trudy에게 건네준 presentation.zip 내 presentation.pptx로 분석을 하는 것이 정확한 분석이지만, 비밀번호를 찾지 못했기 때문에 기존에 분석하려는 pptx와의 동일성 검증을 진행하였습니다.

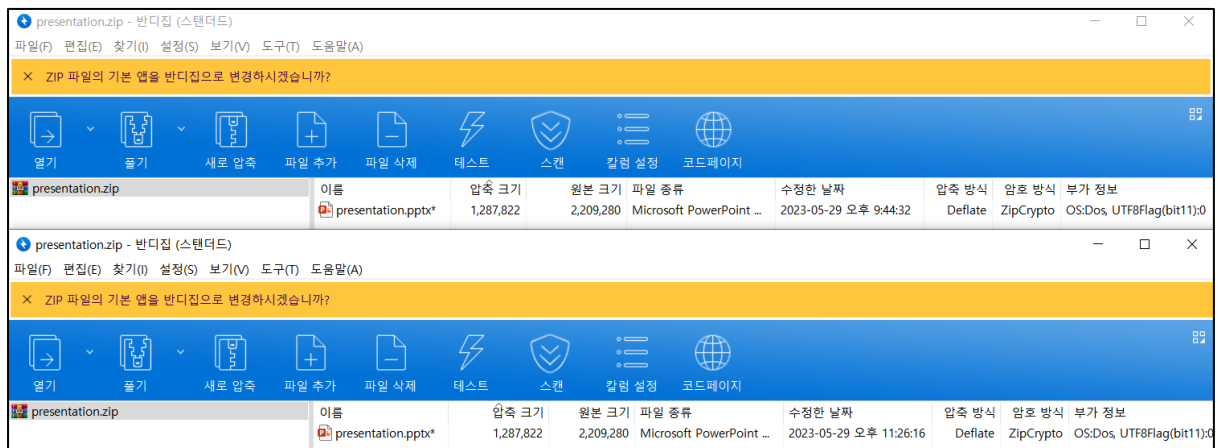
이름	크기	압축된 크기	수정된 날짜	만든 날짜	액세스한 날짜	속...	암호화	설.	CRC
presentation.pptx	2 209 280	1 287 822	2023-05-29 21:44	2023-05-29 21:44	2023-05-29 21:44	A	+		16C0EEFD

체크섬 정보	
이름	presentation_1_pJAoOwqMu2nWveJi6pmUNw5IPibiqXv.pptx
크기	2209280 바이트 (2157 KiB)
CRC32	16C0EEFD

[그림 19] presentation.zip 내 pptx 파일과의 동일성 입증 - CRC32

먼저, CRC32 값이 분석하려던 pptx와 zip 파일 내 pptx가 일치함을 확인하였습니다.



[그림 20] presentation.zip 내 pptx 파일(상), 분석 수행 pptx 파일(하) 과의 동일성 입증

반디집 도구를 통해 다음의 옵션 값으로 암호화 압축을 수행하여 압축 크기가 동일함을 확인하였습니다.

- 압축 방식 : Deflate
- 암호 방식 : ZipCrypto
- 압축 방법 : 압축률 최대
- 암호화 o (16자 이상)

presentation\_1\_pJAoOwqMu2nWveJi6pmUNw5IPlbqXv.pptx 파일 확장자를 exe로 변경 후, ida에서 분석을 수행하였습니다. 분석 대상 exe 파일은 golang으로 작성되었으며, 별 다른 난독화 없이 main\_main() 함수가 존재하였습니다.

```
if ( (unsigned __int64)qword_56E288 <= 2 )
    runtime_panicIndex();
v2 = *(_QWORD *)(os_Args + 16);
v3 = *(_QWORD *)(os_Args + 24);
if ( (unsigned __int64)qword_56E288 <= 3 )
    runtime_panicIndex();
v27 = *(_QWORD *)(os_Args + 40);
v33 = *(_QWORD *)(os_Args + 32);
v30 = v2;
v29 = v3;
main_decodeHexKey();
if ( (unsigned __int64)qword_56E288 <= 4 )
LABEL_22:
    runtime_panicIndex();
```

[그림 21] main\_main() 함수 분석 - 1

main 함수에서는 인자 개수가 5개 이상이 아니면 runtime\_panicIndex() 함수를 실행하는 것을 알 수 있습니다.

```
if ( (unsigned __int64)qword_56E288 <= 4 )
LABEL_22:
    runtime_panicIndex();
v32 = v4;
v5 = *(_QWORD *)(os_Args + 72);
v12 = ((__int64 (__golang *)())main_decodeHexKey());
v31 = v6;
v26 = v7;
((void (__golang *))(__int64, __int64, __int64))main_getOutputFileName)(v12, v16, v20);
v34 = v8;
v28 = v27;
OutputFileName = ((__int64 (__golang *))(__int64, __int64, __int64))main_getOutputFileName)(v13, v17, v21);
```

[그림 22] main\_main() 함수 분석 - 2

5개 이상이 온다면, decodeHexKey를 통해 hex key를 decoding하고 outputfilename을 설정합니다.

```

if ( *(_WORD *)v30 != 'ne' )
{
    v9 = v29 == 3;
    goto LABEL_14;
}
if ( *(_BYTE *)(v30 + 2) != 'c' )
{
    v9 = v29 == 3;
LABEL_14:
    if ( v9 && *(_WORD *)v30 == 'ed' && *(_BYTE *)(v30 + 2) == 'c' )
    {
        main_decryptFile(v31, v5);
        if ( v11 )
        {
            v41 = v1;
            v39 = &unk_4ACB80;
            v40 = &off_4E63E8;
            *(_QWORD *)&v41 = *(_QWORD *)(v11 + 8);
            *((_QWORD *)&v41 + 1) = v27;
        }
        else
        {
            v35 = &unk_4ACB80;
            v36 = &off_4E63F8;
        }
        fmt_Fprintln(v15, v19, v26, OutputFileName);
    }
}

```

[그림 23] main\_main() 함수 분석 - 3

그리고 인자에 dec를 포함하면 main\_decryptFile을 실행하고, enc를 포함하면 main\_encryptFile(그림에선 생략)을 실행하는 것을 알 수 있습니다.

```

v14 = crypto_cipher_NewCBCDecrypter();
v21 = v24 + (((__int64)(16 - v20) >> 63) & 0x10);
((void (*)(void))v14[4])();
v15 = crypto_cipher_NewCBCDecrypter();
((void (*)(void))v15[4])();
if ( v2 - 17 >= v2 - 16 )
    runtime_panicIndex();
if ( v2 - *(unsigned __int8 *)(v2 + v21 - 17) - 16 > v20 - 16 )
    runtime_panicSliceAcap();
os_WriteFile(File, v17, v18, v19);
}
else
{
    runtime_newobject(File);
    v13[1] = 58LL;
    *v13 = "Invalid key size. Keys should be 16, 24, or 32 bytes long";
}

```

[그림 24] main\_decryptFile 함수

main\_decryptFile함수에서는 CBC 모드로 복호화를 두 번 진행하고 key size가 16, 24, 32 bytes 를 요구하는 것을 토대로 해당 exe에서는 aes cbc 암호화를 수행하는 것을 확인하였습니다.

```

C:\Users\juhoheo\Desktop>presentation.exe 1
panic: runtime error: index out of range [2] with length 2

goroutine 1 [running]:
main.main()
    D:/Challenge/2023_DFC/src/presentation.go:18 +0x40f

C:\Users\juhoheo\Desktop>presentation.exe 1 2
panic: runtime error: index out of range [3] with length 3

goroutine 1 [running]:
main.main()
    D:/Challenge/2023_DFC/src/presentation.go:20 +0x405

C:\Users\juhoheo\Desktop>presentation.exe 1 2 3
panic: Invalid hex key: 3

```

[그림 25] exe 파일 동작 방식 확인

또한, 실제 exe파일을 실행 시 발생하는 error를 기반으로 대입을 수행해보았습니다.

```
C:\Users\juhoheo\Desktop>presentation.exe dec -DFC- Forensic_Report_1C1Viz_EbP50SDSmZ5G2AVFYWkduDuSZE.docx
6c4575c9ec1709de06f48546004a7d0f b3ad8aa05409cbec4578117f12b2f835
File decrypted successfully.
```

#### [그림 26] -DFC- Forensic\_Report\_1C1Viz\_EbP50SDSmZ5G2AVFYWkduDuSZE.docx 복호화 성공

```
C:\Users\juhoheo\Desktop>presentation.exe dec Sample_Template.docx_12sVRnsytVypNPu93xmkSkrkFyH9tHw3x.docx
6c4575c9ec1709de06f48546004a7d0f b3ad8aa05409cbec4578117f12b2f835
File decrypted successfully.
```

#### [그림 27] Sample\_Template.docx\_12sVRnsytVypNPu93xmkSkrkFyH9tHw3x.docx 복호화 성공

이를 토대로 앞서 가지고 있던 16 bytes key 2개를 각각 입력하고 알아낸 복호화 payload를 가지고 암호화되어 있던 report 폴더 내 암호화 되어있던 두 파일을 복호화 할 수 있었습니다.

복호화 한 파일들은 원본 파일이라고 가정했던 doc id 1C9sDRd2DgqC8MhOfn3v81Hh82hGk\_Avq와 해시 값이 다음과 같이 모두 동일했습니다.

- MD5 : 986C8FC0D4A91C26388AF65633898CFE
- SHA1 : E8AB401E3ED5D8F2D20DEE7CF90A9A3E813CB823

따라서, 유출된 기밀 보고서의 원본으로 가정하였던 docx파일과 delta가 trudy에게 유출했던 기밀 보고서의 사본(Sample\_Template.docx)과 동일성을 해시 값을 통해 일치함을 증명하였습니다.

[표 6] 복호화 된 극비 보고서 유출 사본과 원본의 동일성 증명

파일명	doc id 및 해시값
[DFC]_Forensic_Report.docx(원본)	doc id: 1C9sDRd2DgqC8MhOfn3v81Hh82hGk_Avq MD5: 986C8FC0D4A91C26388AF65633898CFE SHA1: E8AB401E3ED5D8F2D20DEE7CF90A9A3E813CB823
[DFC]_Forensic_Report.docx(사본)	doc id: 1C1Viz_EbP50SDSmZ5G2AVFYWkduDuSZE MD5: 986C8FC0D4A91C26388AF65633898CFE SHA1: E8AB401E3ED5D8F2D20DEE7CF90A9A3E813CB823
Sample_Template.docx(사본)	doc id: 12sVRnsytVypNPu93xmkSkrkFyH9tHw3x MD5: 986C8FC0D4A91C26388AF65633898CFE SHA1: E8AB401E3ED5D8F2D20DEE7CF90A9A3E813CB823

따라서, 모든 delta의 행위를 종합해보았을 때, 극비 보고서 원본은 vault\_google\_drive\_0 폴더에 존재하는 -DFC- Forensic\_Report\_1C9sDRd2DgqC8MhOfn3v81Hh82hGk\_Avq입니다. 또한, audit report log를 통해 파악한 원본의 이름은 [DFC]\_Forensic\_Report.docx이며, md5는 986C8FC0D4A91C26388AF65633898CFE입니다.