

Dreamhack find-the-spy

당신은 보안 담당자로서 내부 기밀을 유출한 혐의를 받고 있는 직원 A에 대해 내부 감사를 진행하고 있습니다. A의 PC에서 획득한 메모리 덤프로부터 A의 혐의를 입증하여 플래그를 찾으세요.

A의 회사 동료 B의 증언은 다음과 같습니다.

“그날 따라 행동이 수상하고 무언가 불안해 보였어요. 특히 어떤 압축 파일을 유심히 보는 것처럼 보였는데... 자세한 내용은 잘 모르겠습니다”

Info

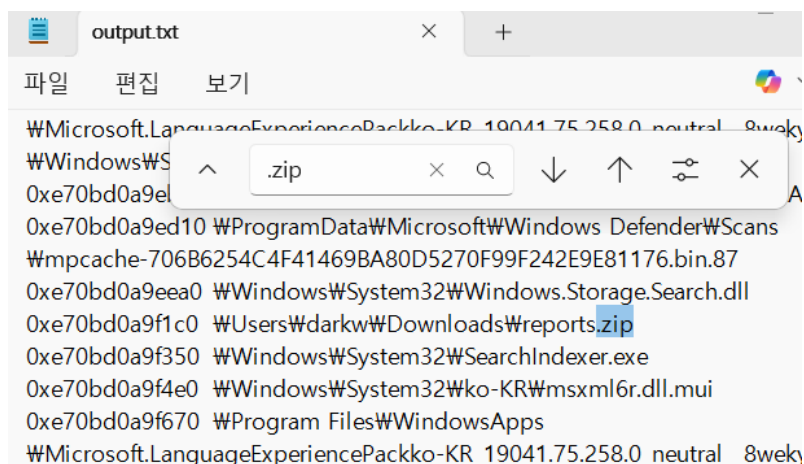
- FLAG = `DH{A_B}`
 - A: 시간 (`yyyyMMddhhmmss` 형식)
 - B: 장소
- 예를 들어 A가 `20240315180312` 이고, B가 `Seoul` 이라면, 플래그는 `DH{20240315180312_Seoul}` 입니다.

문제는 다음과 같다.

먼저 주어진 메모리 덤프에서 압축 파일 형태, 즉 zip을 찾아야 할 것 같다.

```
PS C:\volatility3> $env:PYTHONUTF8=1
PS C:\volatility3> python vol.py -f memory2.vmem windows.filescan.FileScan > output.txt
PS C:\volatility3> PDB scanning finished
```

Volatility의 windows.filescan 플러그인을 이용하여 windows.filescan 플러그인의 결과를 텍스트 파일로 저장한다. 이렇게 하면 더 쉽게 zip 파일을 찾아낼 수 있다.



```

W124.0.2478.67
0xe70bd3530 ^ .zip
WCache_Data
0xe70bd3530810 WWindows\System32\config\systemprofile\W
WMicrosoft\Windows\WebCache\W01.log
0xe70bd3530b30 WUsers\darkw\Downloads\reports.zip
0xe70bd3530b60

```

zip으로 찾아보면 두 개의 주소가 존재한다. 가상 메모리 주소를 얻었으므로 각각 값을 덤프해서 데이터를 살펴보고 했다.

```

PS C:\volatility> python vol.py -f memory2.vmem windows.dumpfiles --virtaddr 0xe70bd0a9f1c0
Volatility 3 Framework 2.25.0
Progress: 100.00 PDB scanning finished
Cache FileObject FileName Result
DataSectionObject 0xe70bd0a9f1c0 reports.zip file.0xe70bd0a9f1c0.0xe70bd471e610.DataSection
.dat

```

API_CHANGES.mru	2025-03
CITATION.cff	2025-03
file.0xe70bd0a9f1c0.0xe70bd471e610.Da...	2025-04
LICENSE.txt	2025-03
MANIFEST.in	2025-03

Dat 파일이 생성되었다.

[ZoneTransfer]↵

ZoneId=3↵

ReferrerUrl=https://mail.google.com/↵

HostUrl=https://mail-

attachment.googleusercontent.com/attachment/u/0/?ui=2&ik=bbacd80191&attid=0.1&permmsgid=msg-

f:1797502558728222925&th=18f2030db7d9f8cd&view=att&disp=safe&realattid=f_lvi9grqm0&sadbat=ANGjdJ9M77mhHQ8MlcUYaxlZM3aEY-

_Q60T7NKhza7osmvi raA0Gb5NiSMavz6-

1TukWpjJgacFbF0QcIfUwlx1btTZ_itwo0rgh00wAYQcS5xrhy1Hj sxl_hhBL9_ZuUubdC0Vd_Ky2iqNft39N3dVvTSxwemJp7Qpfa0q79vShdJvkGXJel-

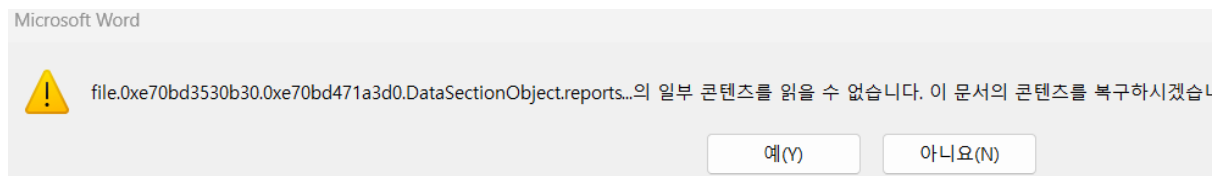
t_DPed6C3lu9oam93YKvs6FRYroLn_SJZyQ7hjWHihSydiDf3wfiQlajyHCwC1suTWmpTgeD1boA9fdDECsJWndt_BbezuXWedyLpNkhMCxGqq53JC9NFT8-

gYdLhpxYn1cRFh_gh6vB1BpbSzvAjYIT2pN0nXVL8xJXyiaDVJ20qD9165bJzFamQUauYxZjUd

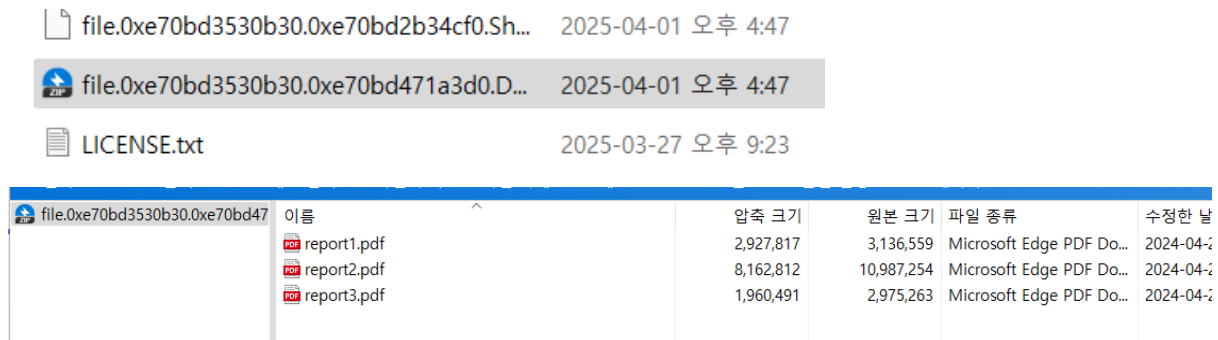
이 파일을 열어보면 다음과 같다. Gmail의 첨부 파일인 것 같은데 딱히 유의미한 결과를 찾기 어려워 일단 두 번째 주소의 값을 먼저 보기로 했다.

```
PS C:\volatility3> python vol.py -f memory2.vmem windows.dumpfiles --virtaddr 0xe70bd3530b30
Volatility 3 Framework 2.25.0
Progress: 100.00 PDB scanning finished
Cache FileObject FileName Result
DataSectionObject 0xe70bd3530b30 reports.zip file.0xe70bd3530b30.0xe70bd471a3d0.DataSectionObject
.dat
SharedCacheMap 0xe70bd3530b30 reports.zip file.0xe70bd3530b30.0xe70bd2b34cf0.SharedCacheMap.reports.z
```

이제 두 번째 주소의 값을 덤프 한다. 첫번째 주소에서 했던 것과 동일한 방법으로 파일을 생성 해준다.



그런데 이렇게 에러가 생긴다. 확장자를 zip으로 바꿔주고 다시 열어보려고 했다.



안에는 이렇게 pdf파일들이 들어있다. 그런데 유의미한 결과는 없는 거 같아서 zip파일을 헥스 에 디터에서 열어보았다.

```
Offset(h) 00 01 02 03 04 05 (
00000000 50 4B 03 04 14 00 (
00000010 44 87 C9 AC 2C 00 :
00000020 70 6F 72 74 31 2E :
00000030 DF C6 65 18 0D 06 :
```

헤더 시그니처는 정상적으로 들어가 있다. 그 뒤에는 푸터 시그니처를 찾아보았다.

```
00C725E0 71 2B EA 1D 00 1F 66 2D 00 0B 00 00 00 00 00
00C72600 00 00 00 20 00 00 00 17 3B A9 00 72 65 70 6F 72
00C72610 74 33 2E 70 64 66 50 4B 05 06 00 00 00 00 03 00
00C72620 03 00 AB 00 00 00 6B 25 C7 00 00 00 89 50 4E 47
00C72630 0D 0A 1A 0A 00 00 00 0D 49 48 44 52 00 00 02 86
```

푸터 시그니처도 확인할 수 있었다. 그런데 그 줄 좀 아래에 png 파일의 헤더 시그니처가 보였다. 즉 이 문제는 zip파일 뒷부분에 png 파일을 숨겨둔 문제라 할 수 있겠다.

Png 파일의 헤더 시그니처부터 파일 끝까지 복사해서 새로운 파일에 붙여넣는다.

```
@6....  
Èf...d  
Í...€1  
àÿ...%ê  
END@B`
```

Deco
%PNG
...%
" ...
Ä. • +
ìÝw\
NÄ=*
Áí . m

Date: 24.01.31 12:00:00

Place: COEX

※ You need to prepare your company's
secret documents on a USB.

Rewards will be sent to your Bitcoin
wallet.

따라서 플래그는 **DH{20240131120000_COEX}** 이다.