[Art] Write-Up

작성자	허은정
분석 일자	2024-05-13 ~ 2024-05-16
작성 일자	2024-05-16
분석 대상	data.mp4
문서 버전	1.0
작성자 E-mail	dmswjd4315@yonsei.ac.kr

0. 목차

1. 문제

URL	https://h4ckingga.me/challenges#art-42
문제내용	Can you turn off the lights, look at my ram
문제파일	https://drive.google.com/file/d/1tEwm00JxCGKg4yavw2Covh9s_322SX2l/view?usp=sharing
문제유형	forensics
난이도	2/ 5

2. 분석 도구

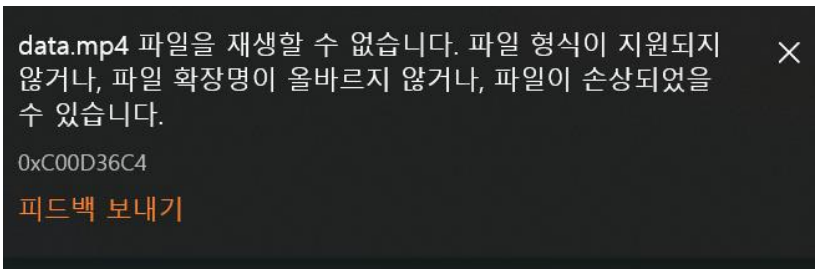
도구명	다운로드 링크	Version
HxD	https://mh-nexus.de/en/downloads.php?product=HxD20	2.5.0
Volatility	https://drive.google.com/file/d/13KhjlrVkPLUlkEytp8jzWD1eaAhl6-q_/view	2.6

3. 환경

OS
Window 11 64-bit

4. Write-Up

파일명	data.mp4
용량	1.99GB
SHA256	d7b16358b54c87f56bc5af3c0cd02128903ea87982ebb37ed227dede63e43e12
Timestamp	2024.05.13 08:53:55



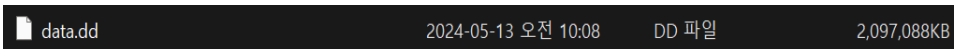
[사진 1] 문제 파일 열어본 내용

문제 파일을 다운 받아 들어가 보면 [사진 1]처럼 파일을 재생할 수 없다고 나온다.

```
7EEC2C20  5C 00 57 00 69 00 6E 00 64 00 6F 00 77 00 73 00  \.W.i.n.d.o.w.s.
7EEC2C30  5C 00 53 00 79 00 73 00 74 00 65 00 6D 00 33 00  \.S.y.s.t.e.m.3.
7EEC2C40  32 00 5C 00 61 00 70 00 69 00 73 00 65 00 74 00  2.\.a.p.i.s.e.t.
7EEC2C50  73 00 63 00 68 00 65 00 6D 00 61 00 2E 00 64 00  s.c.h.e.m.a...d.
7EEC2C60  6C 00 6C 00 00 00 65 6E 20 76 6F 6C 75 6D 65 20  l.l...en volume
```

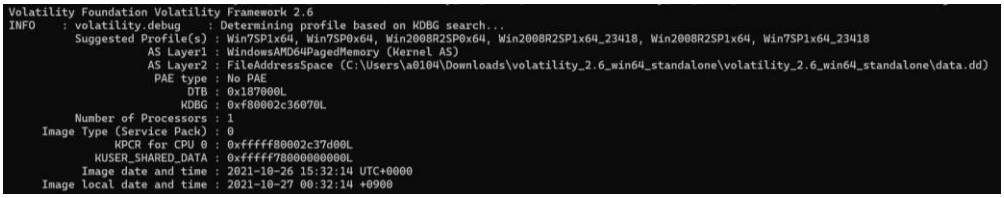
[사진 2] HxD로 열어본 내용

해당 문제 파일을 HxD 로 열어보았더니, 시스템 관련 데이터가 있었다는 것을 볼 수 있었다.



[사진 3] 확장자를 .dd로 바꾼 사진

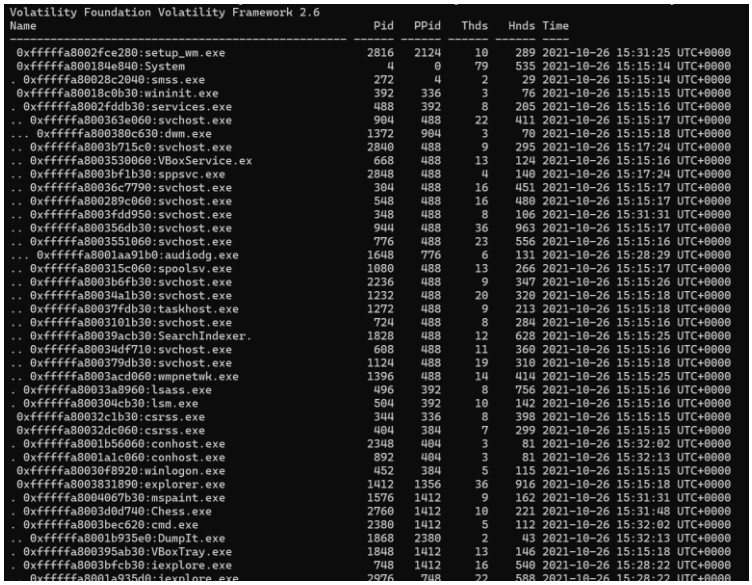
문제 내용에 있는 'look at my ram'을 보고 HXD 를 통해 메모리 덤프 파일이라는 것으로 예상하여 .dd 로 확장자를 바꾸었다.



[사진 4] profile 수집

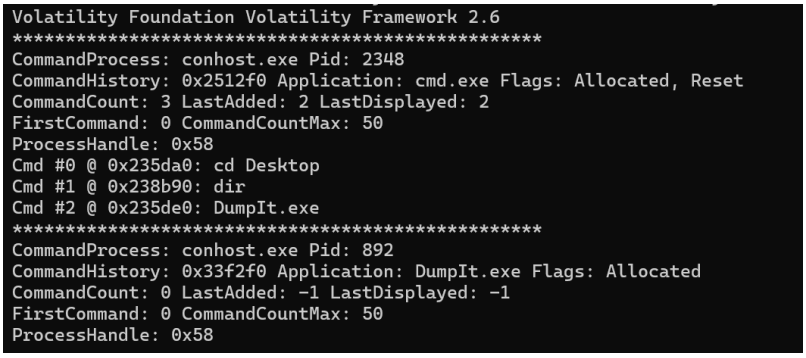
확장자를 바꾼 파일을 volatility 을 이용하여 메모리를 분석해보기로 하였다. 메모리를 분석하기 전에 profile 을 수집하기로 하였다.

.₩volatility_2.6_win64_standalone.exe -f data.dd imageinfo 를 이용하여 해당 메모리 덤프 파일의 프로필 정보가 Win7SP1x64 라는 것을 알 수 있었다.



[사진 5] 현재 실행되고 있는 프로세스 확인

현재 실행되고 있는 프로세스를 확인하기 위해 volatility_2.6_win64_standalone.exe -f "data.dd" --profile=Win7SP1x64 pstree 를 입력해보았다. 분석해보니, cmd 가 실행되어 있다는 것을 볼 수 있다.



[사진 6] cmd 입력한 기록 확인

cmd 명령어가 플래그가 있다는 생각이 들어 .₩volatility_2.6_win64_standalone.exe -f data.dd --profile=Win7SP1x64 cmdscan 를 입력해보았다.
해당 내용을 분석해본 결과, DumpIt.exe 를 실행한 기록이 있었다.

```
0x000000007db81b50      5      0 R--rwd ₩Device₩HarddiskVolume2₩Windows₩System32₩adsldpc.dll
0x000000007db821f0     13      0 R--rwd ₩Device₩HarddiskVolume2₩Windows₩System32₩accessibilitycpl.dll
0x000000007db82b30      6      0 R--r-- ₩Device₩HarddiskVolume2₩Users₩start₩Desktop₩flag.bmp
0x000000007db82c80      9      0 R--r-d ₩Device₩HarddiskVolume2₩Windows₩System32₩NlsData0000.dll
```

[사진 7] 메모리 덤프 파일에 존재하는 파일을 스캔 후, 열어본 내용

.₩volatility_2.6_win64_standalone.exe -f data.dd --profile=Win7SP1x64 filescan > filelist.txt 를 입력하여 텍스트 파일을 만든 후 해당 텍스트 파일에 들어가 메모리 덤프에 존재하는 파일 리스트를 확인해보았다.
이를 통해, flag.bmp 파일이 존재한다는 것을 확인하였다.

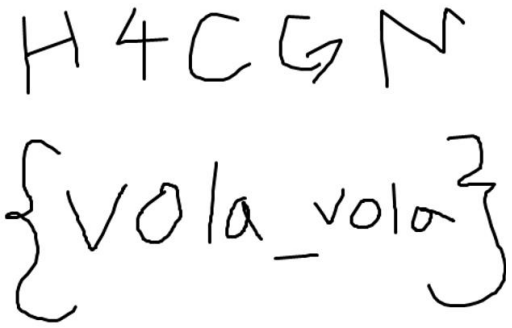
```
Volatility Foundation Volatility Framework 2.6
DataSectionObject 0x7db82b30   None   \Device\HarddiskVolume2\Users\start\Desktop\flag.bmp
```

[사진 8] 실제 메모리 파일로부터 실제 데이터 파일로 추출 할 때 사용하는 명령어

.₩volatility_2.6_win64_standalone.exe -f .₩data.dd --profile=Win7SP1x64 dumpfiles -Q 0x000000007db82b30 -D ./를 입력하여 메모리 덤프 내에 존재하는 파일 데이터를 추출하였다.

```
file.None.0xfffffa80036435a0    2024-05-16 오후 8:49    BMP 파일    508KB
```

[사진 9] dat 확장자를 bmp확장자로 바꾼 사진



[사진 10] 해당 파일을 열어본 내용

해당 파일의 확장자를 .bmp 로 바꾼 후 열어보았더니 H4CGM{vola_vola}라는 플래그 값을 구할 수 있었다.

Flag

H4CGM{vola_vola}

5. 별도 첨부

6. Reference

- https://m.blog.naver.com/meyouhappy/221815800556