



작성자	허은정
분석 일자	2024-05-10
작성 일자	2024-05-10
분석 대상	USB_Image(SuNiNaTaS).파일
문서 버전	2.0
작성자 E-mail	dmswjd4315@yonsei.ac.kr

0. 목차

1. 문제3

2. 분석 도구3

3. 환경3


4. Write-Up.....4

5. Flag.....8

6. 별도 첨부8

7. Reference8

1. 문제

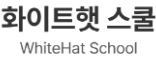
URL	http://suninatas.com/challenge/web32/web32.asp
문제 내용	<p>경찰청으로부터 연쇄 테러 용의자로부터 압수한 USB 이미지 분석을 의뢰 받았다. 최초 분석을 신입 직원에게 맡겼으나 Hex Editor로 여기 저기 둘러 보다 실수로 특정 부분이 손상되고 이미지가 인식되지 않는다. 당신은 포렌식 전문가의 자존심을 걸고 이미지를 살려 내고 다음 테러를 예방하는데 기여를 해야 한다.</p> <p>1. 다음 테러 계획이 들어있는 문서의 수정 일시는? (UTC+9)</p> <p>2. 다음 테러 장소는?</p> <p>인증키 형식 : lowercase(MD5(YYYY-MM-DD_HH:MM:SS_장소)</p> <p>예) lowercase(MD5(2016-03-28_13:00:00_Pink Lake)</p>
문제 파일	 USB_Image(SuNiNaTaS)
문제 유형	Disk Forensics
난이도	2/5

2. 분석 도구

도구명	다운로드 링크	Version
HxD	https://mh-nexus.de/en/downloads.php?product=HxD20	2.5.0
FTK Imager	https://www.exterro.com/	4.7.1.2

3. 환경

OS
Window 11 64-bit

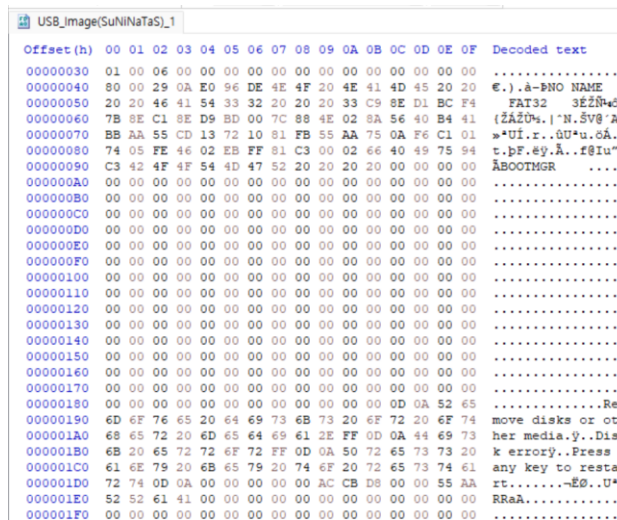


4. Write-Up

문제에 Download 파일이 있어 다운받았다.

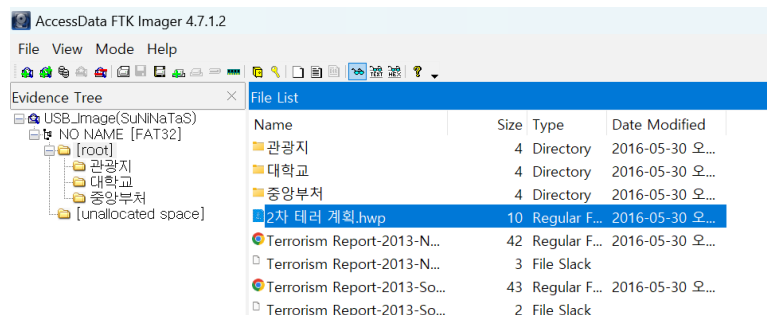


문제에서 보면 특정 부분이 손상되어 있다고 하여 [사진1]처럼 HxD로 열어보았다. HxD로 본 결과, FAT32(EB 58 90)이라는 것을 알 수 있었다. FTA32의 경우 0x1fe ~ 0x01ff에는 부트레코드의 시그니처 55AA가 있어야 하는데, [사진1]을 보면 시그니처의 위치가 이상하다는 것을 알 수 있다.



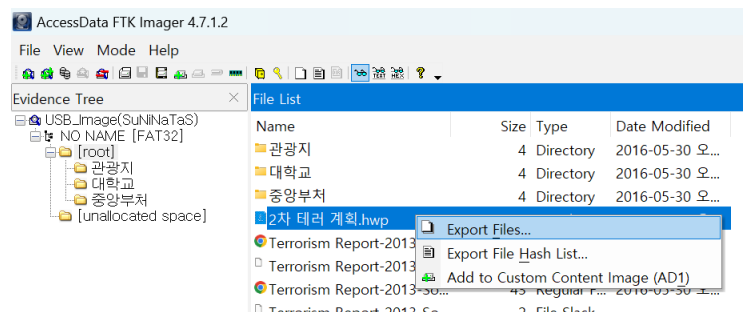
[사진 2] 부트레코드의 시그니처를 옮긴 사진

이를 해결하기 위해 00을 추가하여 0x1fe ~ 0x01ff에 부트레코드의 시그니처를 옮겨 놓았다.



[사진 3] FTK Imager로 열어본 USB_Image

[사진3]을 보면 root 안에 2차 테러 계획.hwp가 있다는 것을 알 수 있습니다.



[사진 4] 해당 hwp 파일 Export

[사진 4]와 같이 해당 hwp파일을 Export 한 후 해당 파일을 열어 보았다.

2차 테러 계획

일 자	2016 - 07 - 15
시 간	09 : 00 : 00
장 소	Rose Park

[사진 5] 해당 hwp파일 내용



[사진 6] 해당 hwp파일의 속성

[사진 5]를 통해 장소는 Rose Park라는 것을 알 수 있었다. [사진 6]을 통해서는 수정된 날짜가 2016-05-30_11:44:02라는 것을 알 수 있었다

MD5 해시 생성기 온라인

2016-05-30_11:44:02_Rose Park

생성하다

입력 문자열	2016-05-30_11:44:02_Rose Park
MD5 해시(32비트)	8ce84f2f0568e3c70665167d44e53c2a
MD5 해시(16비트)	0568e3c70665167d
SHA1 해시	5cbf6a2fdd938534fc33904d87bd034cf43fb4d3
Base64	MjAxNi0wNS0zMjF8xMT0NDowMI9Sb3NIIFBhcms=

[사진 7] MD5 해시 생성한 결과(<http://md5.ko.nrtool.com/>)

해당 정보를 통해 인증키를 도출해보면 lowercase(MD5(2016-05-30_11:44:02_Rose Park))이다. 이를 통해 Auth Key = 8ce84f2f0568e3c70665167d44e53c2a 라는 것을 알 수 있다.

5. Flag

8ce84f2f0568e3c70665167d44e53c2a

6. 별도 첨부

7. Reference

- <https://blog.forensicresearch.kr/13>