



[Deleted file] Write-Up

작성자	김경민
분석 일자	2024.05.17
작성 일자	2024.05.18
분석 대상	usb.image
문서 버전	2.0
작성자 E-mail	rlarudals877@gmail.com

0. 목차

1. 문제3

2. 분석 도구3

3. 환경3


4. Write-Up.....4

5. Flag.....6

6. 별도 첨부7

7. Reference8

1. 문제

URL	https://www.root-me.org/en/Challenges/Forensic/Deleted-file
문제 내용	<p>Your cousin found a USB drive in the library this morning. He's not very good with computers, so he's hoping you can find the owner of this stick!</p> <p>The flag is the owner's identity in the form <code>firstname_lastname</code></p>
문제 파일	<div>  </div> <p>ch39.gz</p>
문제 유형	파일 포렌식
난이도	1 / 5

2. 분석 도구

도구명	다운로드 링크	Version
FTK Imager	https://www.exterro.com/digital-forensics-software/ftk-imager	4.7

3. 환경

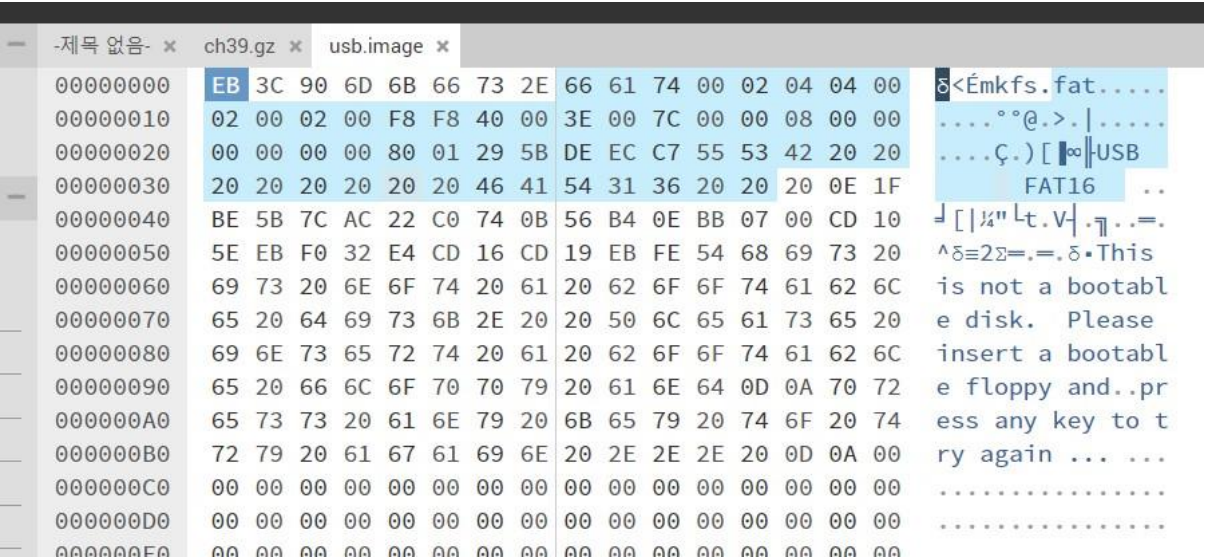
OS
Window11 64-bit

4. Write-Up

파일명	usb.image
용량	31,744KB
SHA256	cd9f4ada5e2a97ec6def6555476524712760e3d8ee99c26ec2f11682a1194778
Timestamp	2021-09-12 22:16:20

1. 파일을 다운로드 받아서 압출을 풀고 풀어서 나온 usb.image 파일을 hexs 웹사이트에서 분석해주었다.

2. hexs(<https://hexed.it/>) 코드를 보면 앞부분에 파일 시스템의 종류가 나와있다. -> fat16 부분



Offset	Hex	ASCII
00000000	EB 3C 90 6D 6B 66 73 2E	<Émkfs.fat.....
00000010	02 00 02 00 F8 F8 40 00°@.>.
00000020	00 00 00 00 80 01 29 5BÇ.)[USB
00000030	20 20 20 20 20 20 46 41	FAT16 ..
00000040	BE 5B 7C AC 22 C0 74 0B	↓[¼"Ł.V .̣..=.
00000050	5E EB F0 32 E4 CD 16 CD	^δ≡2Σ=.=.δ.This
00000060	69 73 20 6E 6F 74 20 61	is not a bootabl
00000070	65 20 64 69 73 6B 2E 20	e disk. Please
00000080	69 6E 73 65 72 74 20 61	insert a bootabl
00000090	65 20 66 6C 6F 70 70 79	e floppy and..pr
000000A0	65 73 73 20 61 6E 79 20	ess any key to t
000000B0	72 79 20 61 67 61 69 6E	ry again
000000C0	00 00 00 00 00 00 00 00
000000D0	00 00 00 00 00 00 00 00

[사진 1] hexs로 분석한 결과

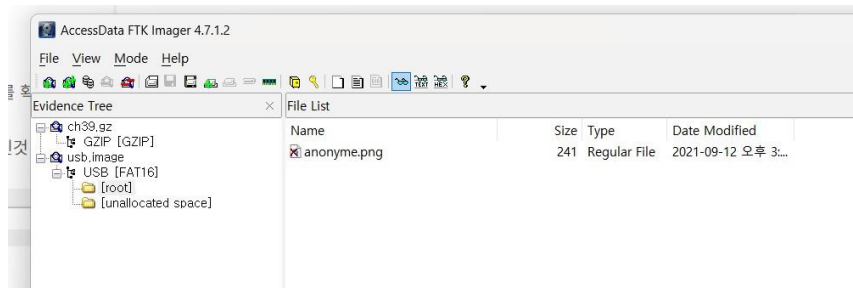
3. VBR에는 파일 시스템에 대한 메타데이터, 즉 파일 시스템의 종류(FAT12, FAT16, FAT32 등), 클러스터 크기, 파일 시스템의 시작 위치 및 크기 등의 정보가 포함되어 있다.

VBR은 특정 파티션의 부팅 절차를 관리하며, 파일 시스템의 중요한 정보를 포함하고 있어, 파일 시스템 분석 및 데이터 복구 시 중요한 역할을 한다.

FTK Imager는 디스크 이미징 및 데이터 수집 도구로, 디스크 이미지를 생성하고 VBR을 포함한 모든 데이터를 캡처할 수 있다. FTK Imager를 사용하여 디스크 이미지를 캡처하면 VBR에 저장된 파일 시스템 정보를 분석하여 파일 시스템을 이해하고 데이터를 복구할 수 있다.

[WHS-2] .iso

4. 따라서 해당 파일이 VBR과 관련 있다는 것을 깨닫고 FTK Imager 로 파일을 분석해보았다.



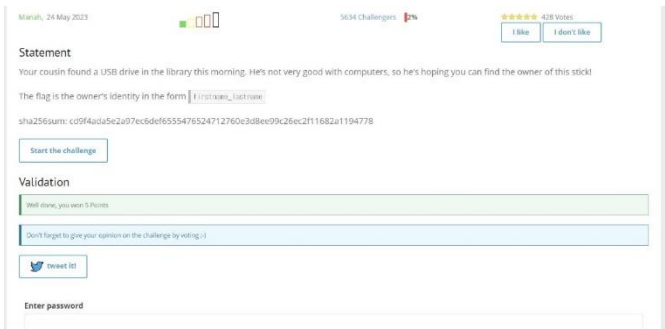
[사진 2] usb.image 파일 분석 결과

5. 분석 결과 root 파일에 뭔가 이상한 x자로 되어 있는 표시가 보였다. 삭제된 파일인가 보다. 그리고 이 파일을 View files with plain text 로 보면 문제에서 요구한 이름과 성을 확인할 수 있다.



[사진 3] 키 값 요소 확인

6. 키형식은 firstname_lastname 이니 이에 맞게 구성하면 키 값은 javier_turcot 이다.



[사진 4] 플래그 성공

5. Flag

javier_turcot

6. 별도 첨부

7. Reference

- [URL]