[Deleted file] WriteUp

작성자	윤건우
분석 일자	2025.04.20
분석 대상	usb.image
작성자 이메일	liiiiiiiqueur@gmail.com

목차

1.문제

URL	https://www.root-me.org/en/Challenges/Forensic/Deleted-file
문제 설명	오늘 아침 우리 사촌이 도서관에서 USB 드라이브를 발견했어요. 컴퓨터 다루는 데 서툴러서 이 USB 드라이브 주인을 찾아주길 바라고 있어요! 플래그는 이름_성 형식으로 소유자의 신원을 나타냅니다. sha256sum: cd9f4ada5e2a97ec6def6555476524712760e3d8ee99c26ec2f11682a1194778
문제 파일	ch39.gz
문제 유형	Disk Forensic
난이도	1 / 5

2.분석 도구

도구명	다운로드 링크	버전
Exterro FTK Imager	https://www.exterro.com/digital-forensics-software/ftk-imager	4.7.3.81

3.환경

운영체제
Microsoft Windows 11 Home 64-bit 10.0.26100

*확인 명령어(cmd): wmic os get Caption,CSDVersion,OSArchitecture,Version

4.WriteUp

파일명	usb.image
용량	32505856 bytes
MD5	X
SHA256	cd9f4ada5e2a97ec6def6555476524712760e3d8ee99c26ec2f11682a1194778
타임스탬프	2021-09-12 22:16:32.000000000 +0900

다운로드 받은 ch39.gz 파일의 sha256 해시 값이 동일함을 확인한다.

```
C:\Users\Yungeonwoo\Desktop\Forensic-Challenge\Disk_Forensic\Deleted file>sha256sum ch39.gz
cd9f4ada5e2a97ec6def6555476524712760e3d8ee99c26ec2f11682a1194778 *ch39.gz
```

사진 1 - 해시 값 비교

압축을 해제한 파일인 usb.image 의 타임스탬프는 2021-09-12 22:16:32.000000000 +0900 이며, 용량은 32505856 bytes 임을 확인한다.

```
C:\Users\Yungeonwoo\Desktop>stat usb.image
  File: usb.image
  Size: 32505856        Blocks: 31744      IO Block: 65536  regular file
Device: 64656f7bh/1684369275d   Inode: 5629499534551924  Links: 1
Access: (0644/-rw-r--r--)  Uid: (197609/Yungeonwoo)   Gid: (197609/Yungeonwoo)
Access: 2025-04-20 02:19:40.503980900 +0900
Modify: 2021-09-12 22:16:32.000000000 +0900
Change: 2025-04-20 02:14:37.855282800 +0900
 Birth: 2025-04-20 02:14:37.813125000 +0900
```

사진 2 - 용량, 타임스탬프 확인

FTK Imager 로 파일을 열어보면 FAT16 파일 시스템이라는 것과 root 폴더 내부에 삭제된 png 파일이 존재하는 것을 확인할 수 있다.

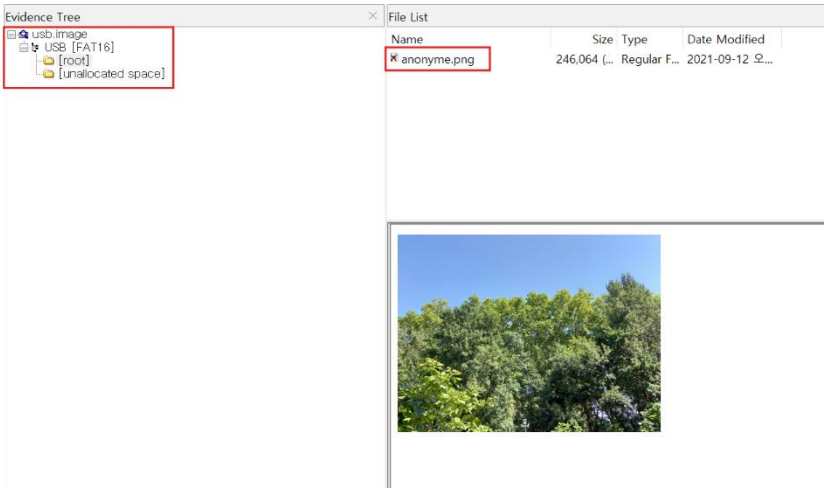

사진 3 - usb.image 파일 분석 결과

이 png 파일을 FTK Imager 기능 중 하나인 "View files in plain text"를 클릭해 다시 보면 문제에서 요구한 소유자의 신원을 확인할 수 있다.

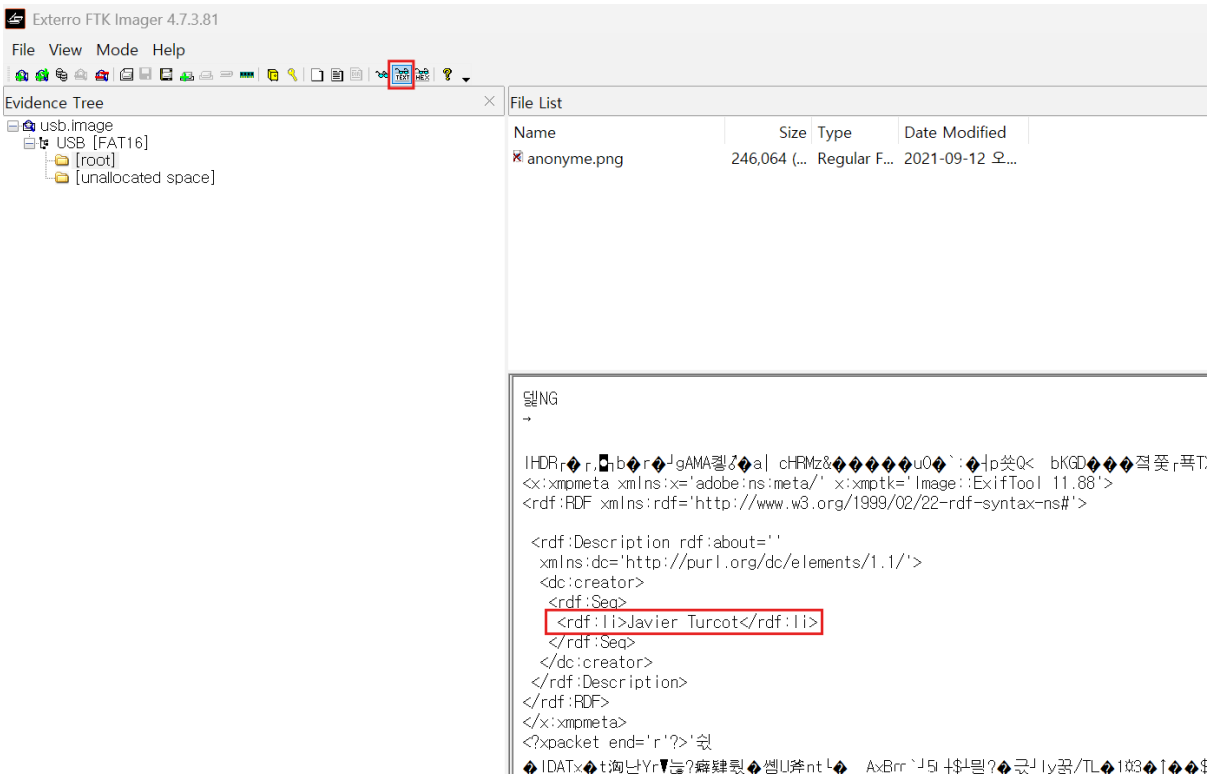

사진 4 - 소유자 신원 확인

소유자는 Javier Turcot 임을 알 수 있다.

5. Reference