




[Find the cat] Write-Up

작성자	심주완
분석 일자	2024.05.23
작성 일자	2024.05.23
분석 대상	chall9
문서 버전	2.0
작성자 E-mail	rd002@naver.com

0. 목차

- 1. 문제 3
- 2. 분석 도구 3
- 3. 환경 3
- 4. Write-Up..... 4
- 5. Flag 8
- 6. 별도 첨부 9
- 7. Reference10

1. 문제

URL	https://www.root-me.org/en/Challenges/Forensic/Find-the-cat
문제 내용	<p>The president’s cat was kidnapped by separatists. A suspect carrying a USB key has been arrested. Berthier, once again you have to save the Republic! Analyze this key and find out in which city the cat is retained!</p> <p>The md5sum of the archive is edf2f1aaef605c308561888079e7f7f7. Input the city name in lowercase.</p>
문제 파일	 chall9
문제 유형	System Forensics
난이도	3 / 3

2. 분석 도구

도구명	다운로드 링크	Version
FTK Imager	https://accessdata-ftp-imager.software.informer.com/download/#google_vignette	3.1.2.0
		-

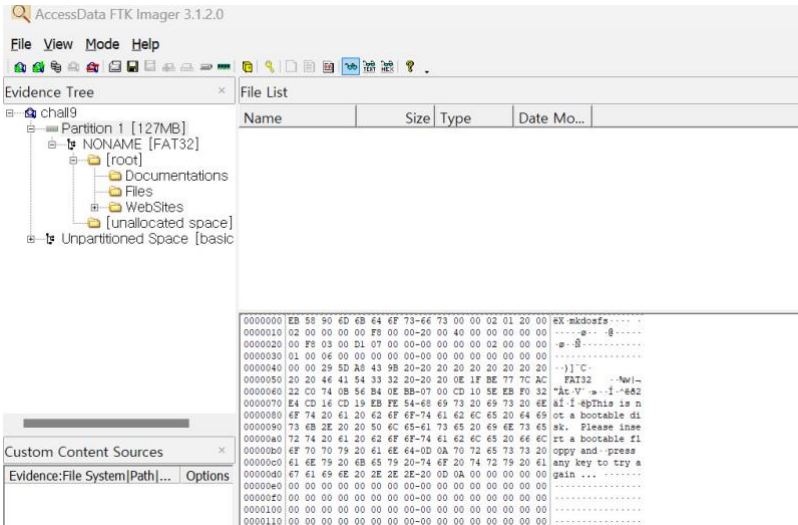
3. 환경

OS
Windows 11 Home

4. Write-Up

파일명	chall9
용량	128MB
SHA256	15877ea3b59d94dbff584048ac885ee484beae2ccc9f1f62826482f152d8091d
Timestamp	2013-07-23 10:22:45

대통령의 납치된 고양이 정보를 얻기 위하여 먼저 구한 USB 를 FTK Imager 를 사용하여 열어보자.



[그림 1] chall9 내부

폴더 내부를 조사하면서 삭제된 파일들을 많이 발견하였고, 이가 수상하여 삭제된 파일 위주로 추출을 진행하며 살펴보았다.

그러던 중, revendtications.odt 파일의 내부에서 단서를 얻은 것 같았다.



RENDEZ L'AUTONOMIE À
L'ALSACE.
SINON NOUS TUERONS.
LE CHAT!!!

[그림 2] revendtications.odt 파일 내부

[WHS-2] .iso

화나게 생긴 고양이 사진이 나온다. 저 말의 뜻이 궁금해서 번역기를 사용했더니

알자스에 자율권을 주다

그렇지 않으면 우리는 죽인다

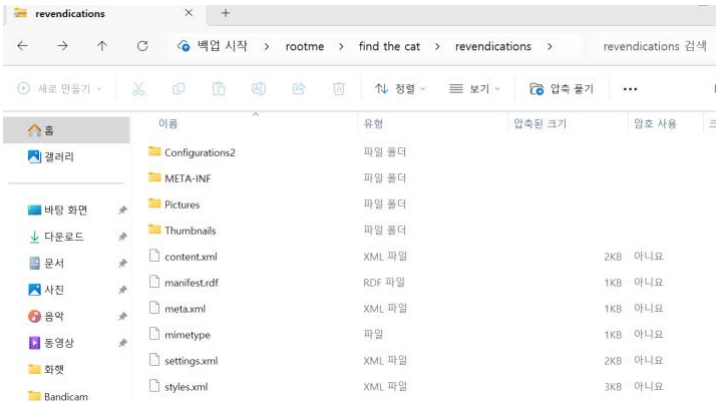
고양이!

라고 나왔다. 이 파일을 분석하면 정답을 얻을 수 있을 것 같다. 플래그 값은 고양이가 납치되어 있는 장소이기 때문에 워드 파일에 있는 고양이 사진을 찍은 장소를 분석하면 플래그를 얻을 수 있을 것이다. 그렇다면 워드 파일에서 이미지를 추출하여 jpg 파일에서 위치를 분석해주는 툴에 넣어보자. 사용한 툴의 주소는 <https://xn--yq5bk9r.com/blog/image-geo-extractor>이다.



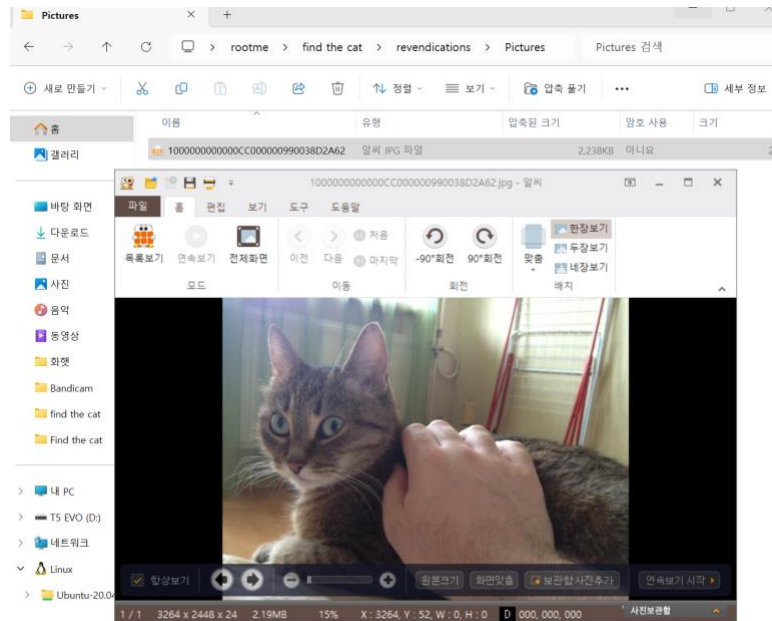
[그림 3] 분석 결과 1

위치 정보를 얻는 데에 실패했다. 이유를 찾아보니 엑셀에서 이미지 데이터를 추출하면 파일의 메타 데이터가 전부 초기화되어 이 사진을 찍은 위치도 날아가버리는 것이었다. 그렇다면 이 이미지의 원본을 찾을 방법을 알아야 했다. **생각한 답안으로는 워드 파일의 확장자를 .zip으로 바꾸면 워드 파일에서 사용된 이미지를 원본으로 확인할 수 있다는 것이었다.** .zip으로 바꿔서 한번 파일 내부를 확인해보자.



[그림 4] .zip으로 연 revendications 내부

다행히 파일 내부를 확인할 수 있었다. 여기서 이미지 파일을 찾아보자.



[그림 5] Pictures 폴더 내부

아까 워드 파일에서 확인한 사진과 같은 내용의 고양이를 찾았다. 이제 이를 사용했던 틀에 넣어 보자.



위도

47.604485000000004

경도

7.4145790000000001

위도, 경도 복사

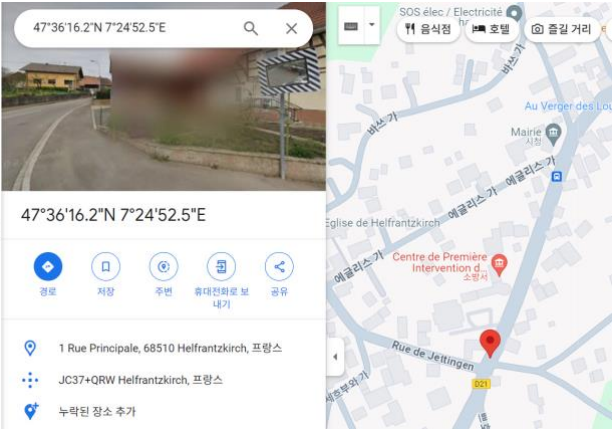
위치 정보 수정 및 다운로드

[구글 지도 바로가기](#)

주소 검색

[그림 6] 분석 결과 2

다음과 같이 위도와 경도를 구할 수 있다. 이제 구한 위도와 경도를 구글 맵을 통하여 검색하면 플래그 값이 나올 것이다.



[그림 7] flag

5. Flag

helfrantzkirch

6. 별도 첨부

7. Reference

- [URL]