



작성자	김경민
분석 일자	2024.05.17
작성 일자	2024.05.18
분석 대상	flag.rar 파일, format_it 파일
문서 버전	1
작성자 E-mail	rlarudals877@gmail.com

0. 목차

1. 문제3

2. 분석 도구3

3. 환경3


4. Write-Up.....4

5. Flag.....8

6. 별도 첨부9

7. Reference 10

1. 문제

URL	http://xcz.kr/START/challenge.php
문제 내용	<p>해커그룹 'XCZ'에서는 데이터를 전송할 때 파일이 외부로 유출되더라도 볼 수 없게 숨겨냈다고 한다.</p> <p>아래의 파일에서 숨겨져 있는 파일을 찾아라.</p> <p>HINT 1: RAR 패스워드 브루트포싱 문제가 아닙니다.</p>
문제 파일	 format_it.zip
문제 유형	파일 포렌식 분석
난이도	2 / 5

2. 분석 도구

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

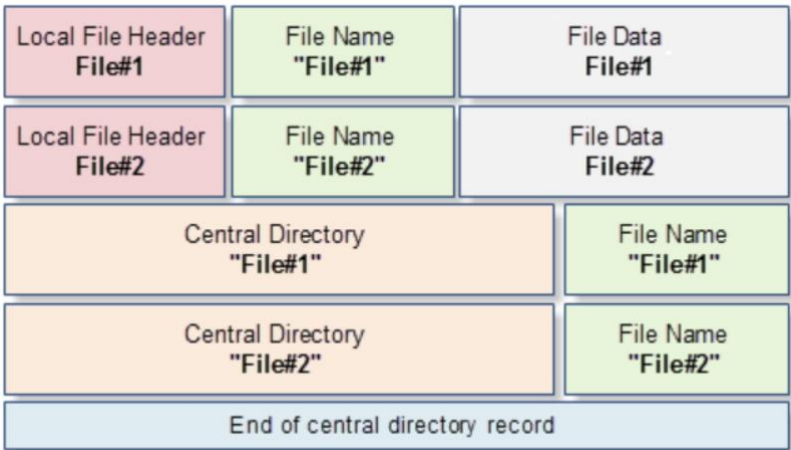
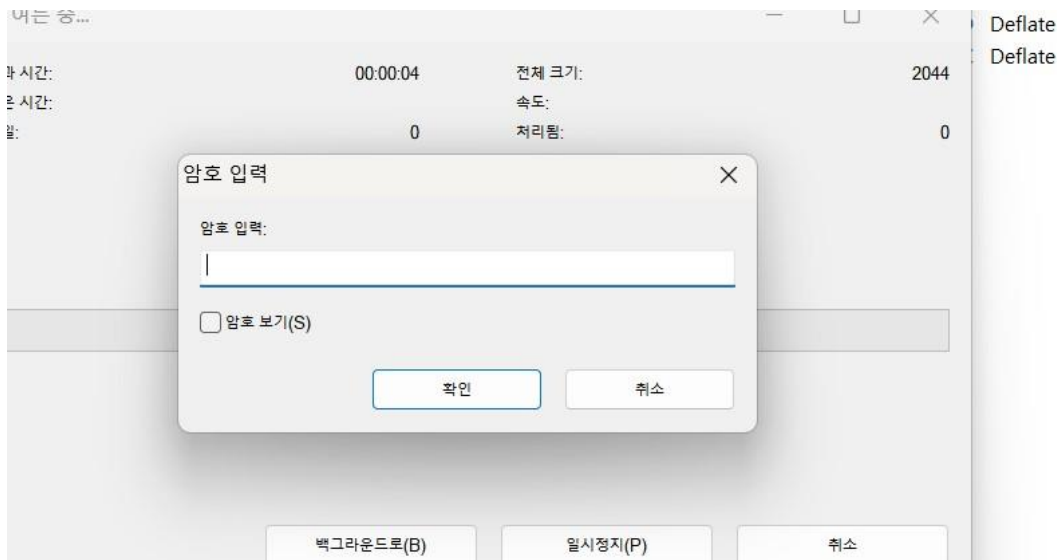
3. 환경

OS
Window 11 64-bit

4. Write-Up

파일명	format_it.zip
용량	4KB
SHA256	DDC0CA895DDA15558A1FA8DF2111641E6AD0C135E056E5EE812C3CD16F3D9338
Timestamp	2013-10-16 02:20:27

1. 파일을 열어보니 .rar 형식의 압축파일이 있었고 비번이 걸려 있었다. -> 비번을 찾거나 or 비번을 없애거나 하는 문제인 것을 파악했다. zip 파일의 구조를 살펴보면 밑에와 같다. 따라서 현재 다운로드 받은 파일의 밑의 형식을 따르고 있는지 살펴보았다.



[사진 1] .rar 파일에 비번 걸려 있는 모습, zip 파일 형식(압축 파일이 2개일 때)



2. 다운로드 받은 파일을 **헥스(<https://hexed.it/>)** 웹사이트를 통해 분석해보았다. 압축 파일에는 총 두 개의 파일이 존재하니 위의 사진을 참고해 보면 local header 2 개 central header 2 개 가 있어야 한다. 그러나 검사한 내용을 보면 flag.rar 외의 format_it 파일의 Central Directory 가 없는 것을 알 수 있다. 그러한 이유로 압축을 해제하면 구조상 오류 때문에 파일이 보이지 않는다. 또한 파일 이름도 존재하지 않는다.

[illegible]

[사진 2] flag.rar의 로컬 헤더 -> format it의 로컬 헤더 -> flag.rar 의 센트럴 디렉토리 -> 푸터

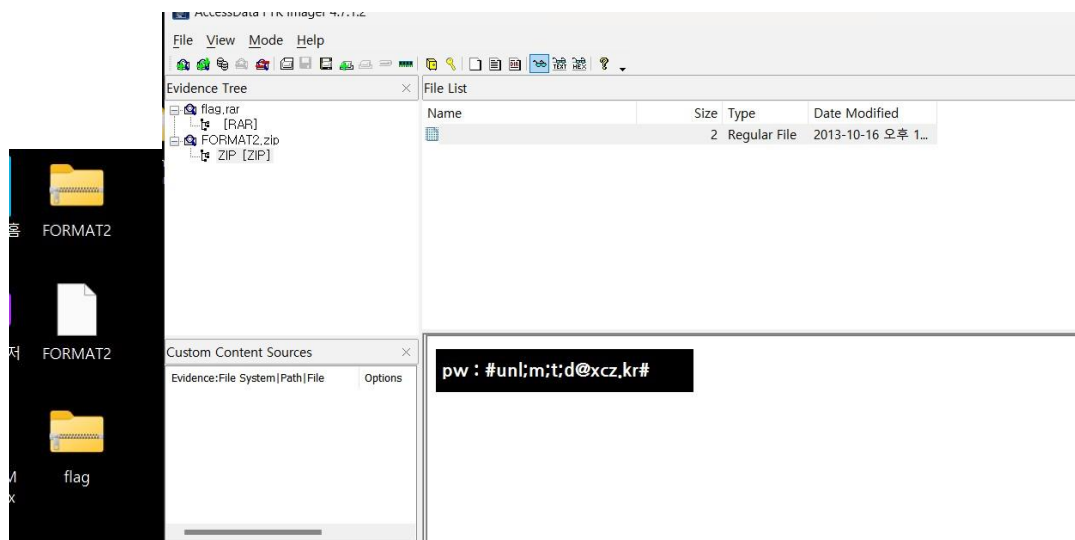
3. 따라서 central header을 만들어주고 넣어주어서 압축 파일을 완성시켜 보았다. 넣어주는 위치는 flag.rar의 central header 바로 앞이다. -> 50 4B 01 02 14 00 14 00 00 00 08 00 D2 BE 50 43 EC BD 08 97 71 05 00 00 76 05 00 00 09 00 08 00 00 00 00 00 01 00 20 00 삽입

00000DA0	D1	41	AB	59	14	84	2D	3B	43	DF	E0	C5	30	0A	AC	55
00000DB0	5F	49	AF	D5	56	A7	16	F5	FE	69	32	5E	C9	E2	BD	8F
00000DC0	A7	37	15	8E	14	10	EF	50	4B	01	02	14	00	14	00	00
00000DD0	00	08	00	D2	BE	50	43	EC	BD	08	97	71	05	00	00	76
00000DE0	05	00	00	09	00	08	00	00	00	00	00	01	00	20	00	00
00000DF0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	50	4B
00000E00	01	02	14	00	14	00	00	00	08	00	00	BF	50	43	BD	A8
00000E10	85	A1	01	08	00	00	FC	07	00	00	08	00	00	00	00	00
00000E20	00	00	01	00	20	00	00	00	A0	05	00	00	66	6C	61	67

[사진 3] central header 삽입

4. hex에서 위의 코드를 넣어주고 확장자 zip 으로 해서 바탕화면에 다시 저장해 주었다. 그러나 파일이 열리지 않아 ftk imager 로 살펴보았다. 그런 다음 파일을 열어주었더니 pw 가 나왔다. -

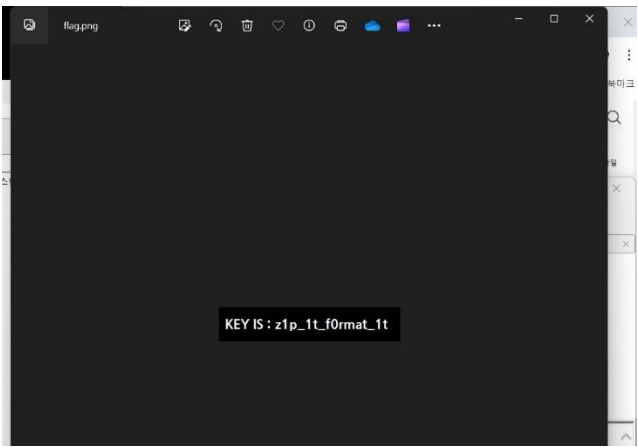
```
> pw: #unl;m;t;d@xcz.kr#
```



[사진 4] zip 파일로 저장한 결과, FTK Imager로 파일 열어본 결과

[WHS-2] .iso

5. 나온 pw 를 가지고 rar 파일을 풀어주었더니 png 파일이 나오면서 key 값이 나왔다. ->KEY IS:
z1p_1t_f0rmat_1t



[그림 5] .rar 파일을 열어본 모습 -> 키 값 발견 -> 플래그 성공

5. Flag

z1p_1t_f0rmat_1t

6. 별도 첨부

7. Reference