



작성자	김경민
분석 일자	2024.05.17
작성 일자	2024.05.18
분석 대상	flag.rar, format_it
문서 버전	3.0
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
난이도	1 / 3

2. 분석 도구

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

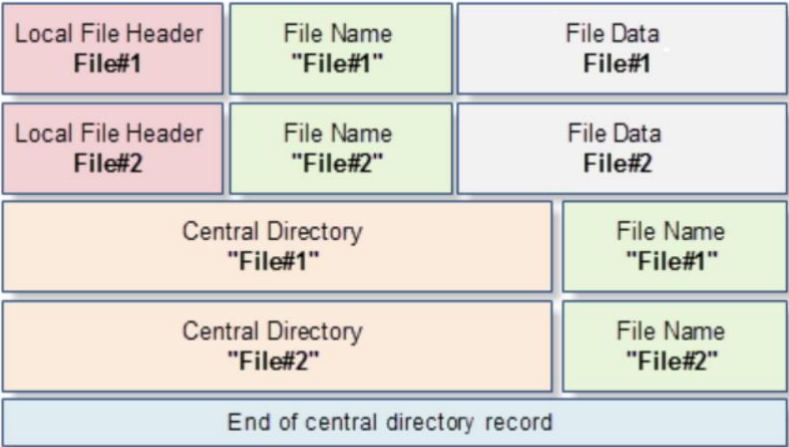
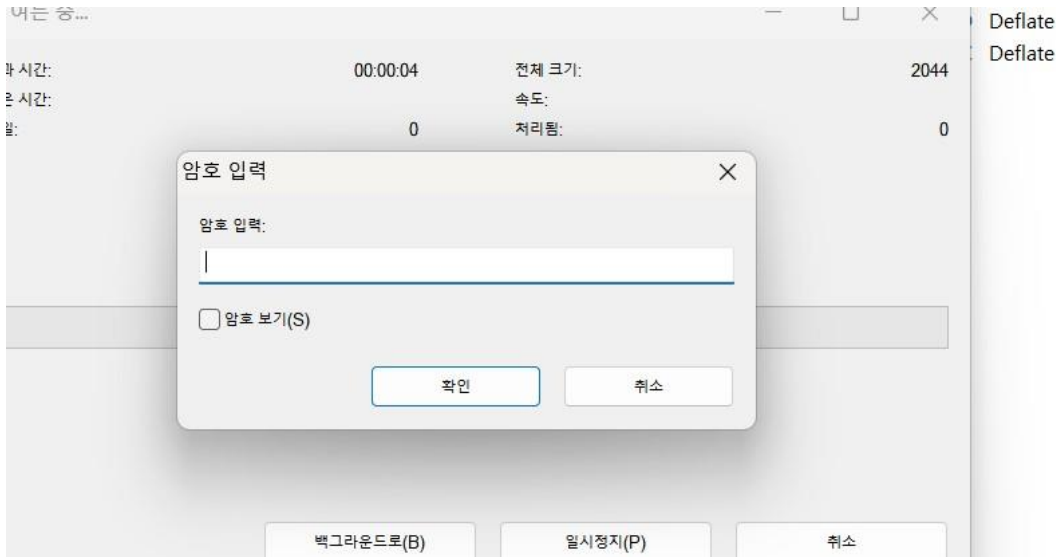
3. 환경

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)

[WHS-2] .iso

2. 다운로드 받은 파일을 헥스(<https://hexed.it/>) 웹사이트를 통해 분석해보았다. 압축 파일에는 총 두 개의 파일이 존재하니 위의 사진을 참고해 보면 local header 2개 central header 2개 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.

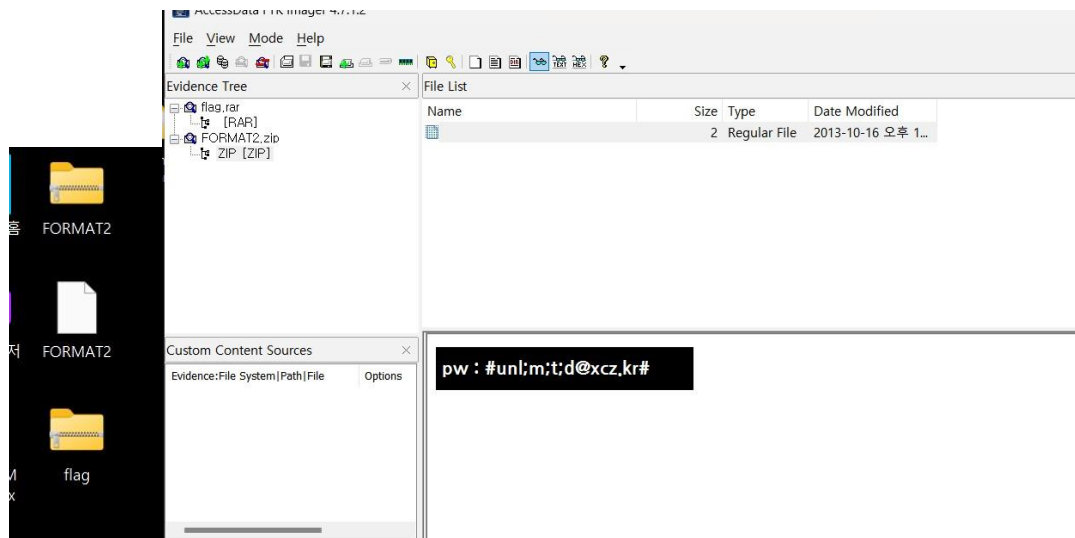
00000000	50 4B 03 04 14 00 00 00	08 00 D2 BE 50
00000010	08 97 71 05 00 00 76 05	00 00 09 00 08
00000020	00 00 00 00 00 00 00 7A	E5 04 00 B5 03
00000030	04 50 00 10 0A 00 C7 47	00 40 05 10 05
00000040	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000050	5C 74 DC 01 5B DD 80 DD	0F 37
00000060	41 A4 7F FA 59 3F 00 6F	19 1C
00000070	06 44 E8 EF 7E 25 00 63	75 0E
00000080	50 4B 03 04 14 00 00 00	08 00
00000090	85 A1 01 08 00 00 FC 07	00 00
000000A0	61 67 2E 72 61 72 01 FC	07 03
000000B0	07 00 B4 39 73 84 00 0D	00 00
000000C0	16 D9 D4 A1 7F 3F 63 53	12 B9 C5 68 1B
000000D0	D1 41 AB 59 14 84 2D 3B	43 DF E0 C5 30
000000E0	5F 49 AF D5 56 A7 16 F5	FE 69 32 5E C9
000000F0	A7 37 15 8E 14 10 EF 50	4B 01 02 14 00
00000100	00 08 00 00 BF 50 43 BD	A8 85 A1 01 08
00000110	07 00 00 08 00 00 00 00	00 00 00 01 00
00000120	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000130	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000140	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000150	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000160	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000170	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000180	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000190	00 00 00 00 00 00 00 00	00 00 00 00 00 00
000001A0	00 00 00 00 00 00 00 00	00 00 00 00 00 00
000001B0	00 00 00 00 00 00 00 00	00 00 00 00 00 00
000001C0	00 00 00 00 00 00 00 00	00 00 00 00 00 00
000001D0	00 00 00 00 00 00 00 00	00 00 00 00 00 00
000001E0	00 00 00 00 00 00 00 00	00 00 00 00 00 00
000001F0	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000200	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000210	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000220	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000230	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000240	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000250	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000260	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000270	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000280	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000290	00 00 00 00 00 00 00 00	00 00 00 00 00 00
000002A0	00 00 00 00 00 00 00 00	00 00 00 00 00 00
000002B0	00 00 00 00 00 00 00 00	00 00 00 00 00 00
000002C0	00 00 00 00 00 00 00 00	00 00 00 00 00 00
000002D0	00 00 00 00 00 00 00 00	00 00 00 00 00 00
000002E0	00 00 00 00 00 00 00 00	00 00 00 00 00 00
000002F0	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000300	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000310	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000320	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000330	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000340	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000350	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000360	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000370	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000380	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000390	00 00 00 00 00 00 00 00	00 00 00 00 00 00
000003A0	00 00 00 00 00 00 00 00	00 00 00 00 00 00
000003B0	00 00 00 00 00 00 00 00	00 00 00 00 00 00
000003C0	00 00 00 00 00 00 00 00	00 00 00 00 00 00
000003D0	00 00 00 00 00 00 00 00	00 00 00 00 00 00
000003E0	00 00 00 00 00 00 00 00	00 00 00 00 00 00
000003F0	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000400	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000410	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000420	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000430	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000440	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000450	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000460	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000470	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000480	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000490	00 00 00 00 00 00 00 00	00 00 00 00 00 00
000004A0	00 00 00 00 00 00 00 00	00 00 00 00 00 00
000004B0	00 00 00 00 00 00 00 00	00 00 00 00 00 00
000004C0	00 00 00 00 00 00 00 00	00 00 00 00 00 00
000004D0	00 00 00 00 00 00 00 00	00 00 00 00 00 00
000004E0	00 00 00 00 00 00 00 00	00 00 00 00 00 00
000004F0	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000500	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000510	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000520	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000530	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000540	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000550	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000560	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000570	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000580	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000590	00 00 00 00 00 00 00 00	00 00 00 00 00 00
000005A0	00 00 00 00 00 00 00 00	00 00 00 00 00 00
000005B0	00 00 00 00 00 00 00 00	00 00 00 00 00 00
000005C0	00 00 00 00 00 00 00 00	00 00 00 00 00 00
000005D0	00 00 00 00 00 00 00 00	00 00 00 00 00 00
000005E0	00 00 00 00 00 00 00 00	00 00 00 00 00 00
000005F0	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000600	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000610	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000620	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000630	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000640	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000650	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000660	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000670	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000680	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000690	00 00 00 00 00 00 00 00	00 00 00 00 00 00
000006A0	00 00 00 00 00 00 00 00	00 00 00 00 00 00
000006B0	00 00 00 00 00 00 00 00	00 00 00 00 00 00
000006C0	00 00 00 00 00 00 00 00	00 00 00 00 00 00
000006D0	00 00 00 00 00 00 00 00	00 00 00 00 00 00
000006E0	00 00 00 00 00 00 00 00	00 00 00 00 00 00
000006F0	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000700	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000710	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000720	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000730	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000740	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000750	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000760	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000770	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000780	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000790	00 00 00 00 00 00 00 00	00 00 00 00 00 00
000007A0	00 00 00 00 00 00 00 00	00 00 00 00 00 00
000007B0	00 00 00 00 00 00 00 00	00 00 00 00 00 00
000007C0	00 00 00 00 00 00 00 00	00 00 00 00 00 00
000007D0	00 00 00 00 00 00 00 00	00 00 00 00 00 00
000007E0	00 00 00 00 00 00 00 00	00 00 00 00 00 00
000007F0	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000800	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000810	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000820	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000830	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000840	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000850	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000860	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000870	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000880	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000890	00 00 00 00 00 00 00 00	00 00 00 00 00 00
000008A0	00 00 00 00 00 00 00 00	00 00 00 00 00 00
000008B0	00 00 00 00 00 00 00 00	00 00 00 00 00 00
000008C0	00 00 00 00 00 00 00 00	00 00 00 00 00 00
000008D0	00 00 00 00 00 00 00 00	00 00 00 00 00 00
000008E0	00 00 00 00 00 00 00 00	00 00 00 00 00 00
000008F0	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000900	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000910	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000920	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000930	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000940	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000950	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000960	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000970	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000980	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000990	00 00 00 00 00 00 00 00	00 00 00 00 00 00
000009A0	00 00 00 00 00 00 00 00	00 00 00 00 00 00
000009B0	00 00 00 00 00 00 00 00	00 00 00 00 00 00
000009C0	00 00 00 00 00 00 00 00	00 00 00 00 00 00
000009D0	00 00 00 00 00 00 00 00	00 00 00 00 00 00
000009E0	00 00 00 00 00 00 00 00	00 00 00 00 00 00
000009F0	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000A00	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000A10	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000A20	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000A30	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000A40	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000A50	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000A60	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000A70	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000A80	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000A90	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000AA0	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000AB0	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000AC0	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000AD0	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000AE0	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000AF0	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000B00	00 00 00 00 00 00 00 00	00 00 00 00 00 00
00000B10	00 00 00 00 00 00 00 00	00 00

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 00 00 00 00 00 00 00 00 00 00 00 00 00 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

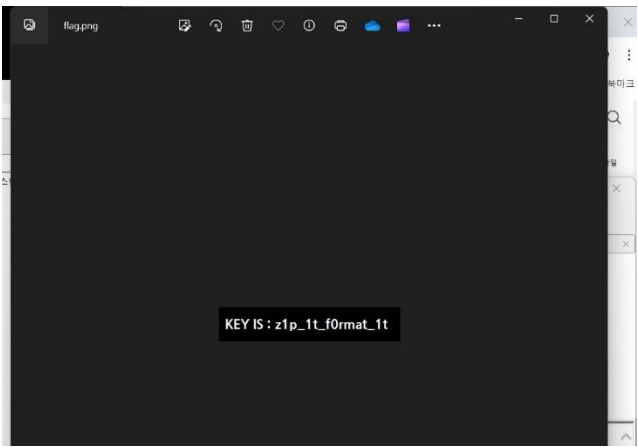
4. hexs에서 위의 코드를 넣어주고 확장자 zip 으로 해서 바탕화면에 다시 저장해 주었다. 그러나 파일이 열리지 않아 ftk imager 로 살펴보았다. 그런 다음 파일을 열어주었더니 pw 가 나왔다. -
- ```
> pw: #unl;m;t;d@xcz.kr#
```



[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