

Forensics: Unzip it

Description

A zip file came for investigation and inside it the flag is hidden to extract it.

Approach

Step 1:

Check the file type and try to extract it directly.

```
(ritikrajput@kali)-[~/Documents/HackAWay2.0_Writups/forensics/Unzip it]
$ file evidence.zip
evidence.zip: Zip archive data, made by v3.0 UNIX, extract using at least v1.0, last modified Sep 11 2025 00:21:28, uncompressed size 27, method=stor

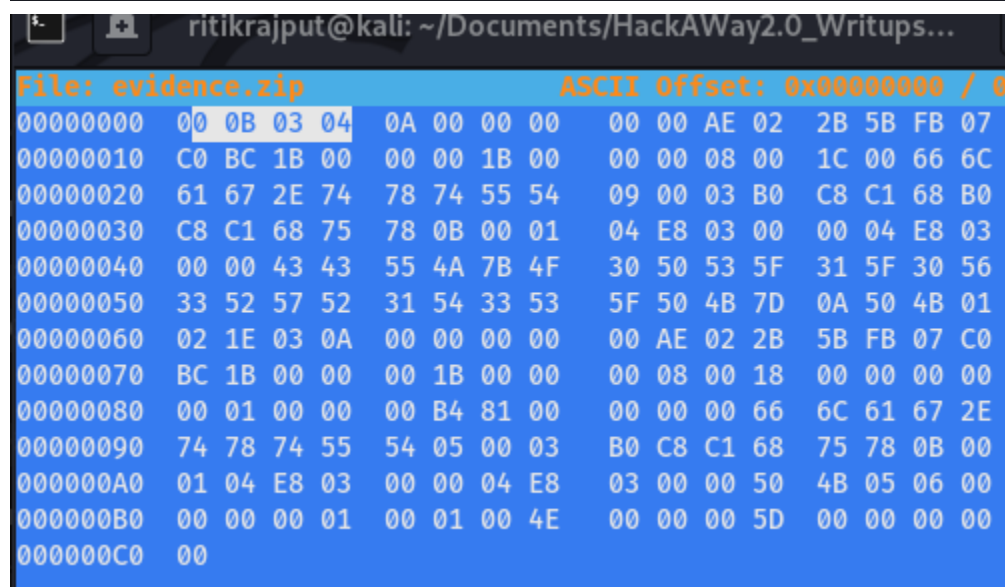
(ritikrajput@kali)-[~/Documents/HackAWay2.0_Writups/forensics/Unzip it]
$ unzip evidence.zip

Archive:  evidence.zip
file #1:  bad zipfile offset (local header sig):  0
```

Step 2:

Check the header of the zip file using hexeditor tool and we found the it was overwrite to corrupt the zip file

```
(ritikrajput@kali)-[~/Documents/HackAWay2.0_Writups/forensics/Unzip it]
$ hexeditor evidence.zip
```



File: evidence.zip	ASCII	Offset: 0x00000000 / 0
00000000 00 0B 03 04 0A 00 00 00	00 00 AE 02 2B 5B FB 07	
00000010 C0 BC 1B 00 00 00 1B 00	00 00 08 00 1C 00 66 6C	
00000020 61 67 2E 74 78 74 55 54	09 00 03 B0 C8 C1 68 B0	
00000030 C8 C1 68 75 78 0B 00 01	04 E8 03 00 00 04 E8 03	
00000040 00 00 43 43 55 4A 7B 4F	30 50 53 5F 31 5F 30 56	
00000050 33 52 57 52 31 54 33 53	5F 50 4B 7D 0A 50 4B 01	
00000060 02 1E 03 0A 00 00 00 00	00 AE 02 2B 5B FB 07 C0	
00000070 BC 1B 00 00 00 1B 00 00	00 08 00 18 00 00 00 00	
00000080 00 01 00 00 00 B4 81 00	00 00 00 66 6C 61 67 2E	
00000090 74 78 74 55 54 05 00 03	B0 C8 C1 68 75 78 0B 00	
000000A0 01 04 E8 03 00 00 04 E8	03 00 00 50 4B 05 06 00	
000000B0 00 00 00 01 00 01 00 4E	00 00 00 5D 00 00 00 00	
000000C0 00		

Step 3:

Change the header to zip file header and save it

ritikrajput@kali: ~/Documents/HackAWay2.0_Writups...

File: evidence.zip	ASCII	Offset: 0x00000001 / 0
00000000	50 4B 03 04 0A 00 00 00	00 00 AE 02 2B 5B FB 07
00000010	C0 BC 1B 00 00 00 1B 00	00 00 08 00 1C 00 66 6C
00000020	61 67 2E 74 78 74 55 54	09 00 03 B0 C8 C1 68 B0
00000030	C8 C1 68 75 78 0B 00 01	04 E8 03 00 00 04 E8 03
00000040	00 00 43 43 55 4A 7B 4F	30 50 53 5F 31 5F 30 56
00000050	33 52 57 52 31 54 33 53	5F 50 4B 7D 0A 50 4B 01
00000060	02 1E 03 0A 00 00 00 00	00 AE 02 2B 5B FB 07 C0
00000070	BC 1B 00 00 00 1B 00 00	00 08 00 18 00 00 00 00
00000080	00 01 00 00 00 B4 81 00	00 00 00 66 6C 61 67 2E
00000090	74 78 74 55 54 05 00 03	B0 C8 C1 68 75 78 0B 00
000000A0	01 04 E8 03 00 00 04 E8	03 00 00 50 4B 05 06 00
000000B0	00 00 00 01 00 01 00 4E	00 00 00 5D 00 00 00 00
000000C0	00	

Step 4:

Unzip the file and get the flag

```
(ritikrajput@kali)-[~/Documents/HackAWay2.0_Writups/forensics/Unzip it]
└─$ unzip evidence.zip

Archive: evidence.zip
replace flag.txt? [y]es, [n]o, [A]ll, [N]one, [r]ename:
error: invalid response [{ENTER}]
replace flag.txt? [y]es, [n]o, [A]ll, [N]one, [r]ename: y
  extracting: flag.txt

(ritikrajput@kali)-[~/Documents/HackAWay2.0_Writups/forensics/Unzip it]
└─$ ls
evidence.zip  flag.txt

(ritikrajput@kali)-[~/Documents/HackAWay2.0_Writups/forensics/Unzip it]
└─$ cat flag.txt

CCUJ{00PS_1_0V3RWR1T3S_PK}
```

Flag: CCUJ{00PS_1_0V3RWR1T3S_PK}