

Meepwn CTF Quals 2018

White Snow , Black Shadow

100pts



evidence.jpg - This is the file found in zip download



At the first time, I tried to strings this file. So I put it in hex editor and I noticed something interesting

```
....."  
/..."/...Oq  
0A~..L0. ...%v..  
A@L..0 .....3  
3.....  
...{..}..0A ..  
...R.X.....A.  
?~..vj YZ.v01C.  
Xh.....8...o|  
..HZ...p .....  
...iF.. ..N..PK  
.....[hL..  
Tt1...L. ...$...  
... ..messa  
ge.pdf. ....  
...#.. \. ....{7.  
..O[.7. ....PK...  
.....]. ...I....
```

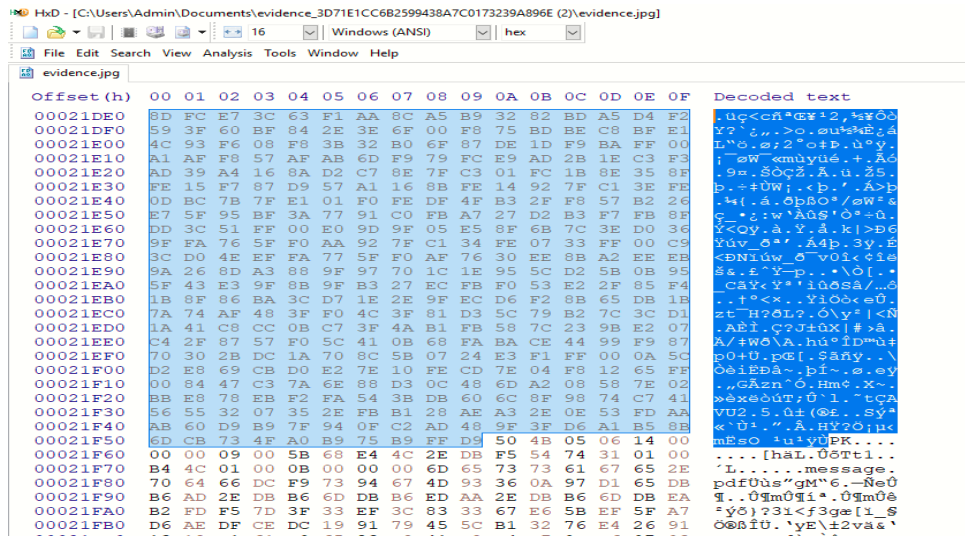
You can see I found PDF File from this image and I have to extract it by anyway. When I checked it again, I found another file after JPEG Image. And as you see there is a interesting thing which is (PK). This's PK Signature!

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00021F20	BB	E8	78	EB	F2	FA	54	3B	DB	60	6C	8F	98	74	C7	41	»èxèdóúT;Û`l.~tÇA
00021F30	56	55	32	07	35	2E	FB	B1	28	AE	A3	2E	0E	53	FD	AA	VU2.5.û± (@£...SÝª
00021F40	AB	60	D9	B9	7F	94	0F	C2	AD	48	9F	3F	D6	A1	B5	8B	«`Û¹."`Â.Hÿ?Ö;µ<
00021F50	6D	CB	73	4F	A0	B9	75	B9	FF	D9	50	4B	05	06	14	00	mËsO `u¹ÿÜPK...].
00021F60	00	00	09	00	5B	68	E4	4C	2E	DB	F5	54	74	31	01	00[häL.ÜöTt1..
00021F70	B4	4C	01	00	0B	00	00	00	6D	65	73	73	61	67	65	2E	`L.....message.
00021F80	70	64	66	DC	F9	73	94	67	4D	93	36	0A	97	D1	65	DB	pdfÜùs"gm`6.-ÑeÛ
00021F90	B6	AD	2E	DB	B6	6D	DB	B6	ED	AA	2E	DB	B6	6D	DB	EA	¶...Ô¶mÔ¶¶iª.Ô¶mÔê

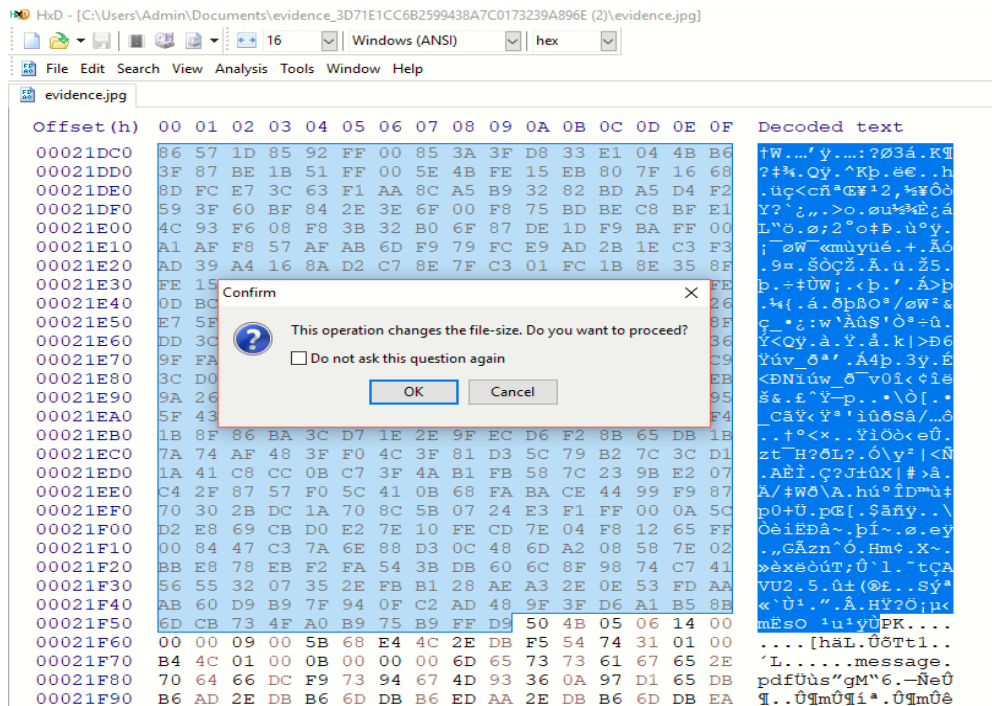
From a [List of File Signatures](#) (I searched it in Google), I got that PK Signature can support ZIP Files which means that signature can be ZIP File Signature which means that:

Image = Image + ZIP File

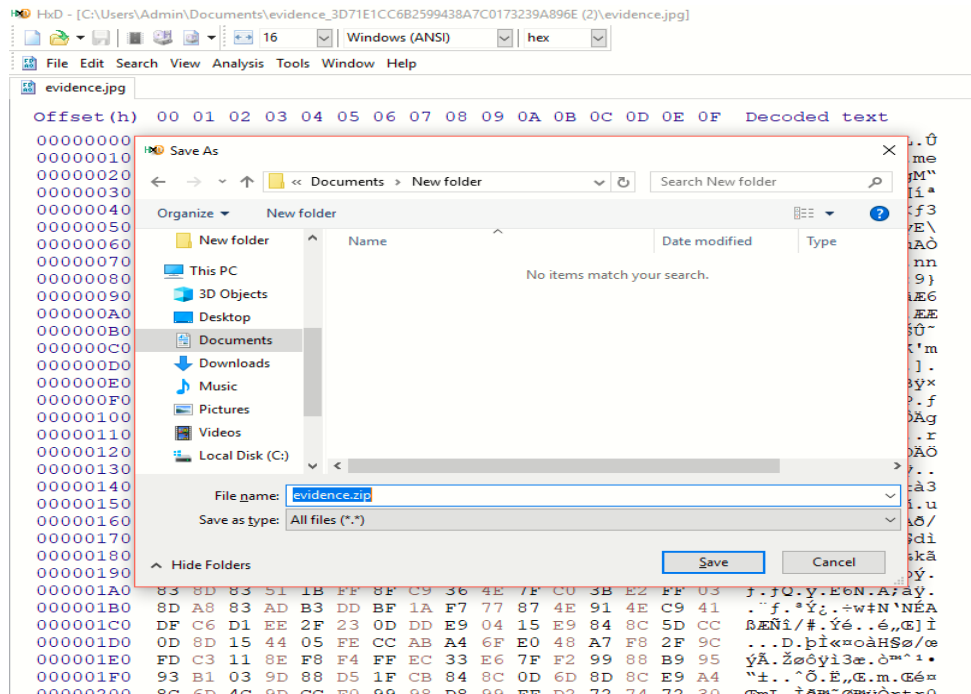
And you know I need check and extract just the ZIP File. So let's start it:



Select the image bytes until End of JPEG Image



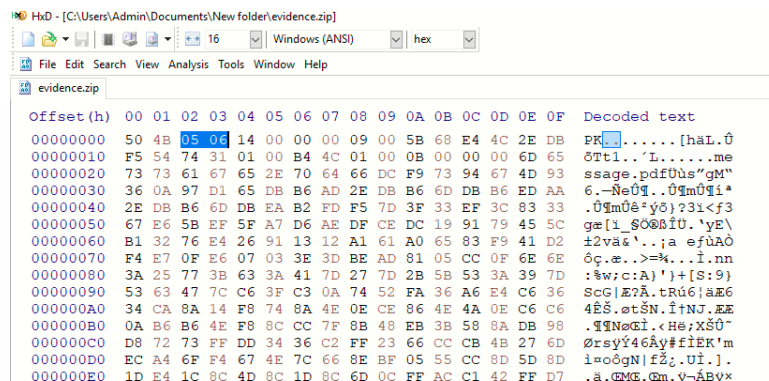
Delete the selected bytes



Save a new file

But I can't open this ZIP File, and this is a big problem. I checked it again 'cause I could lost something. Wait, something wrong with the header of this ZIP File and I checked a [List of File Signatures](#) one again. And the problem was in two bytes (05 06), so to fix it I have to change it into (03 04).

Before



After

```

HxD - [C:\Users\Admin\Documents\New folder\evidence.zip]
File Edit Search View Analysis Tools Window Help
evidence.zip
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Decoded text
00000000 50 4B 03 04 14 00 00 00 09 00 5B 68 E4 4C 2E DB PK...[hãL.Û
00000010 F5 54 74 31 01 00 B4 4C 01 00 0B 00 00 00 6D 65 òTt1..'L.....me
00000020 73 73 61 67 65 2E 70 64 66 DC F9 73 94 67 4D 93 ssage.pdfÙùs"gm"
00000030 36 0A 97 D1 65 DB B6 AD 2E DB B6 6D DB B6 ED AA 6.-ÑeÛq..ÛmÛqíª
00000040 2E DB B6 6D DB EA B2 FD F5 7D 3F 33 EF 3C 83 33 .ÛmÛé:ýð}?3i<f3
00000050 67 E6 5B EF 5F A7 D6 AE DF CE DC 19 91 79 45 5C gæ[i_s000îÛ.'yE\
00000060 B1 32 76 E4 26 91 13 12 A1 61 A0 65 83 F9 41 D2 ±2vã&'..ja efûAò
00000070 F4 E7 0F E6 07 03 3E 3D BE AD 81 05 CC 0F 6E 6E ôç.æ..>=¾...î.nn
00000080 3A 25 77 3B 63 3A 41 7D 27 7D 2B 5B 53 3A 39 7D :%w;c:A)'')+[s:9)
00000090 53 63 47 7C C6 3F C3 0A 74 52 FA 36 A6 E4 C6 36 ScG|Æ?Ä.trú6;aÆ6
000000A0 34 CA 8A 14 F8 74 8A 4E 0E CE 86 4E 4A 0E C6 C6 4ÊŠ.øtŠN.î+NJ.ÆE
000000B0 0A B6 B6 4E F8 8C CC 7F 8B 48 EB 3B 58 8A DB 98 .ÛqNøGî.<Hø;XŠÛ~
000000C0 D8 72 73 FF DD 34 36 C2 FF 23 66 CC CB 4B 27 6D ørsýÝ46Äÿ#fiEK'm

```

Then saved it as message.zip, extracted it with 7-Zip instead of Winrar and i found (message.pdf). But it's corrupted file and I used [Online Repair PDF File Tool](#) to repair before I open it. Then you can saved it as (nameulike.pdf).

ANALYZE AND REPAIR PDF FILE

You can use this online sample to analyse PDF files against corruption, repair or recover content from corrupt files.

Select PDF file to repair

Choisir un fichier Aucun fichier choisi

message.pdf
148518 bytes
(not a correct PDF)

load PDF

☐ Analyze Only

☒ Recover Cross Reference Table

☒ Recover Pages

☒ Rebuild streams

☒ Rebuild fonts

product page

☒ evaluation mode
(creates water mark)

Execute..

The file is corrupt and cannot be repaired, but possibly recovered
1 page recovered.

Save As..

Do you find this application useful? Your feedback is appreciated: [click here](#)

So sad 'cause I couldn't see the flag after I read it many times. And I tried to Google to find the original text and [compared](#) it with my text. Differences between the original text and the text which i found in PDF File (message.pdf), that's maybe a flag. Collect, read the text then sort all off-topic words or characters and finally i collected the Flag .

*FLAG is: **MeePwnCTF{T3xt_Und3r_t3Xt!!!!}***