ENCRYPT CTF

Write up (D.F)

Y. M. Jeon

Get Schwifty

10

Forensics

Evil Morty, the first democratically-elected President of the Citadel of Ricks, has killed off twenty-seven known Ricks from various dimensions, as well as capturing, torturing, and enslaving hundreds of Mortys. As a fellow Rick-less Morty, Investigator Rick gives you a file revealing Evil Morty's past and true nature. However he cannot seem to access it. Can you help recover it to stop Evil Morty ?

meme

Download file here: link

Author: maskofmydisguise

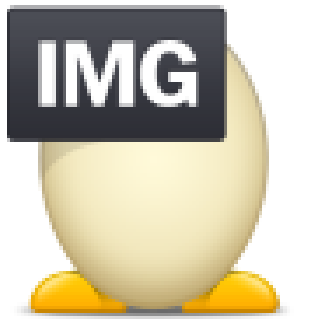
Unlock Hint for 75 points

Flag

Submit

GetSchwifty.7z 항목 1개

GetSchwifty.img



GetSchwifty.img


```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00000000   EB 3C 90 6D 6B 66 73 2E 66 61 74 00 02 04 04 00   ë<.mkfs.fat.....
00000010   02 00 02 00 00 F8 80 00 3E 00 FC 00 00 08 00 00   .....ø€.>.ü.....
00000020   00 00 02 00 80 01 29 44 A1 22 C7 48 50 20 20 20   ....€.)D¡"ÇHP
00000030   20 20 20 20 20 20 46 41 54 31 36 20 20 20 0E 1F         FAT16   ..
00000040   BE 5B 7C AC 22 C0 74 0B 56 B4 0E BB 07 00 CD 10   ¾[|¬"Àt.V´.»..Í.
00000050   5E EB F0 32 E4 CD 16 CD 19 EB FE 54 68 69 73 20   ^ëð2äÍ.Í.ëþThis
00000060   69 73 20 6E 6F 74 20 61 20 62 6F 6F 74 61 62 6C
00000070   65 20 64 69 73 6B 2E 20 20 50 6C 65 61 73 65 20
00000080   69 6E 73 65 72 74 20 61 20 62 6F 6F 74 61 62 6C
00000090   65 20 66 6C 6F 70 70 79 20 61 6E 64 0D 0A 70 72
000000A0   65 73 73 20 61 6E 79 20 6B 65 79 20 74 6F 20 74
000000B0   72 79 20 61 67 61 69 6E 20 2E 2E 2E 20 0D 0A 00
```

Extension	Signature	Description
IMG	EB 3C 90 2A	GEM Raster file
	ASCII <*	Sizet: 4 Bytes Offset: 0 Bytes

?!?

```
0007A000   89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52   ‰PNG........IHDR
0007A010   00 00 07 55 00 00 01 06 08 06 00 00 00 3D A3 CC   ...U.........=£Ì
0007A020   34 00 00 00 06 62 4B 47 44 00 00 00 00 00 00 F9   4....bKGD......ù
0007A030   43 BB 7F 00 00 00 09 70 48 59 73 00 00 2E 23 00   C».....pHYs...#.

0007FF50   15 00 00 00 00 00 00 20 41 A8 0A 00 00 00 00 00   ....... A¨......
0007FF60   00 90 20 54 05 00 00 00 00 00 00 48 10 AA 02 00   .. T.......H.ª..
0007FF70   00 00 00 00 00 24 FC 1B D9 8E E9 05 1B 91 C7 59   .....$ü.ÙŽé..'ÇY
0007FF80   00 00 00 00 49 45 4E 44 AE 42 60 82 00 00 00 00   ....IEND®B`,....
```

```
00098C00   89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52   ‰PNG........IHDR
00098C10   00 00 07 55 00 00 01 06 08 06 00 00 00 3D A3 CC   ...U.........=£Ì
00098C20   34 00 00 00 06 62 4B 47 44 00 00 00 00 00 00 F9   4....bKGD......ù
00098C30   43 BB 7F 00 00 00 09 70 48 59 73 00 00 2E 23 00   C».....pHYs...#.

0009EB50   15 00 00 00 00 00 00 20 41 A8 0A 00 00 00 00 00   ....... A¨......
0009EB60   00 90 20 54 05 00 00 00 00 00 00 48 10 AA 02 00   .. T.......H.ª..
0009EB70   00 00 00 00 00 24 FC 1B D9 8E E9 05 1B 91 C7 59   .....$ü.ÙŽé..'ÇY
0009EB80   00 00 00 00 49 45 4E 44 AE 42 60 82 00 00 00 00   ....IEND®B`,....
```

FLAG !!!

encryptCTF{ }

Journey to the centre of the file 1

75

forensics

"Nearly everything is really interesting if you go into it deeply enough ..." - Richard Feynman

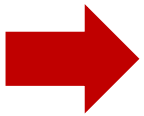
Author: maskofmydisguise

ziptunnel1.gz

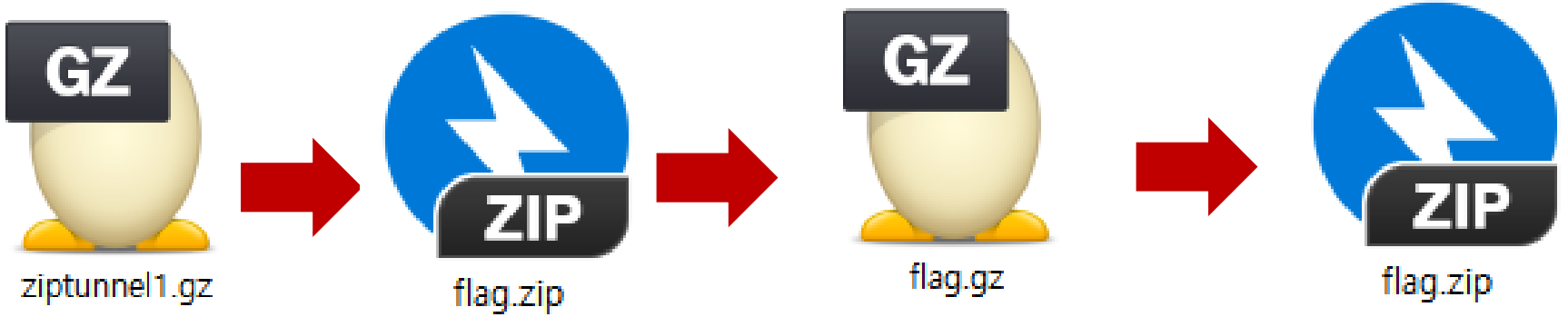
Flag

Submit

ziptunnel1.gz



flag.zip




```
00000000  1F 8B 08 08 57 0E 75 5C 00 03 66 6C 61 67 2E 7A  ‹‹..W.u\..flag.z
00000010  69 70 00 75 98 E5 57 14 00 94 C5 07 90 18 BA 5B  ip.u˜åW..”Å...°[
00000020  06 49 91 92 EE EE CE A1 4B 40 60 86 86 19 C2 A1  .I'îîÎ¡K@`††.Â¡
```

```
00000000  50 4B 03 04 0A 00 00 00 00 00 3C 7D 5A 4E F4 FD  PK........<}ZNôý
00000010  C2 06 0E 24 00 00 0E 24 00 00 04 00 1C 00 66 6C  Â..$...$......fl
00000020  61 67 55 54 09 00 03 EC 10 75 5C EC 10 75 5C 75  agUT...ì.u\ì.u\u
```

Extension	Signature	Description
GZ	1F 8B 08	GZIP archive file
	ASCII ••	Sizet: 3 Bytes Offset: 0 Bytes

Extension	Signature	Description
ZIP	50 4B 03 04	PKZIP archive_1
	ASCII PK••	Sizet: 4 Bytes Offset: 0 Bytes

binwalk

```
yumin3404@ubuntu:~/Desktop$ binwalk ziptunnel1.gz

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
-
0             0x0             gzip compressed data, has original file name: "fl
ag.zip", from Unix, last modified: 2019-02-26 10:00:55
```

```
yumin3404@ubuntu:~/Desktop$ binwalk flag

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
-
0             0x0             Zip archive data, at least v1.0 to extract, compr
essed size: 5483, uncompressed size: 5483, name: flag.gz
5625          0x15F9          End of Zip archive
```

Journey to the centre of the file 1

75

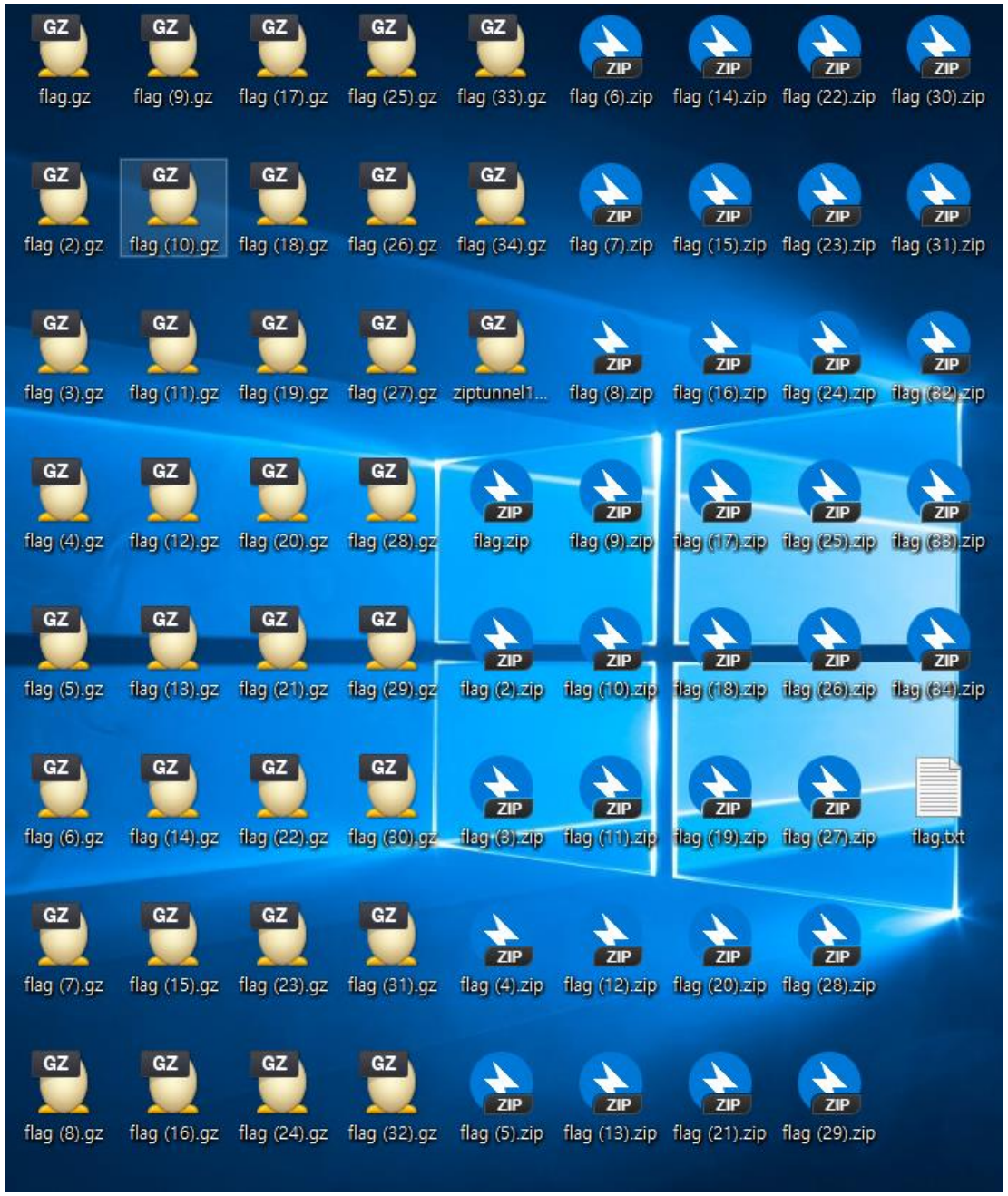
"Nearly everything is really interesting if you go into it deeply enough ..." - Richard Feynman

Author: maskofmydisguise

ziptunnel1.gz

Flag

Submit



X 70

FLAG !!!

flag.txt - 메모장

파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

encryptCTF{[redacted]}

Journey to the centre of the file 2

150

forensics

Improvise. Adapt. Overcome

Author: maskofmydisguise

Unlock Hint for 125 points

ziptunnel2

Flag

Submit

ziptunnel2

Evidence Tree

- ziptunnel2
  - bzip2 [bzip2]

File List

Name	Size	Type	Date Modified
ziptunnel2.out	10	Regular File	

Properties

Name	ziptunnel2.out
File Class	Regular File
File Size	9,561
Compressed Size	10,025

```
0000 50 4B 03 04 0A 00 00 00-00 00 3C 7D 5A 4E 1D F3 PK·····<}ZN·ó
0010 88 40 BB 24 00 00 BB 24-00 00 04 00 1C 00 66 6C ·@»$··»$·····fl
0020 61 67 55 54 09 00 03 EC-10 75 5C EC 10 75 5C 75 agUT···ì·u\ì·u\u
0030 78 0B 00 01 04 E8 03 00-00 04 E8 03 00 00 1F 8B x····è····è·····
0040 08 08 EC 10 75 5C 00 03-66 6C 61 67 2E 7A 69 70 ··ì·u\··flag.zip
0050 00 75 BA 53 70 25 0C 13-2D 1A DB B6 6D 4C 3C B1 ·u°Sp%··-·Û¶mL<±
0060 6D DB 99 68 62 DB B6 6D-EF D8 C9 64 C7 B6 6D DB mÛ·hbÛ¶mïØÉdÇ¶mÛ
0070 C6 FD BF 3A 75 5F 4E D5-59 5D BD BA AA 7B 75 55 Æý¿:u_NÕY]½°ª{uU
0080 BF F5 CB 52 92 05 87 80-03 F9 0F BF 7D 75 14 1E ¿õËR·····ù·¿}u··
0090 BF FA A1 90 28 40 40 FE-4B 08 10 02 10 0B 5B 63 ¿ú¡·(@@þK·····[c
00a0 4B 75 35 58 10 F0 4B 14-57 BD FF D2 D5 03 1E 04 Ku5X·ðK·W½ÿÒÕ···
00b0 14 E2 14 FC 7F E3 FF 88-38 1A 06 E6 BF 36 08 F8 ·â·ü·ãÿ·8··æ¿6·ø
00c0 7F 4A 26 AF 3F 0E 20 A1-9D EA 4A 04 08 E8 2D 91 ·J&¯?·· ¡·êJ··è-·
00d0 D0 EE FF C1 D2 01 6D 53-3F B8 AB 0B 3A 3C 70 F7 ÐîÿÁÒ·mS?¸«·:<p÷
00e0 9A 68 73 CB CE C1 3D BD-77 17 E2 FB 06 00 7C B6 ·hsËÎÁ=½w·âû··|¶
00f0 A8 6E 7D 76 79 3A 8B BE-EE E1 D7 8C CF 42 FB 85 ¨n}vy:·¾îá×·ÏBû·
0100 40 36 E8 8F 86 34 AB 7A-67 1F 60 73 57 14 14 F0 @6è··4«zg·`sW··ð
0110 5A 67 4C 12 41 5A 43 20-07 00 DA 90 0A 09 19 16 ZgL·AZC ··Ú·····
0120 7A E3 7C AE 10 6D 4B A1-24 B0 58 CE FE E8 FE 58 zã|®·mK¡$°XÎþèþX
0130 26 79 71 82 11 A0 75 36-67 75 86 77 E1 51 A1 D4 &yq·· u6gu·wáQ¡Ô
0140 0B 18 FE 00 D7 07 CE D0-7D DE 8F 5A 3A BE 1C 9A ··þ·×·ÎÐ}Þ·Z:¾··
0150 1E EC 3D 09 6E 7B D7 3F-9E 0F FD E7 8B D7 1B FC ·ì=·n{×?··ýç·×·ü
0160 F0 EB 17 5A 2E CA D7 8F-E9 67 B7 BC 5F 50 66 97 ðë·Z.Ê×·ég·¾_Pf·
0170 5B 8F 84 BD 75 B7 16 BA-B7 0E 56 5C 1F 72 48 5F [··½u··°··V\·rH_
0180 1D 36 2E 9A CE D6 96 5D-B3 3B 26 96 5D AF BC 45 ·6.·ÎÖ·]³;&·]¯¼E
0190 8B 9E 12 F5 7B 24 65 23-10 A1 00 C2 6F 64 C7 F2 ···õ{$e#·¡·ÂodÇò
1a0 14 BD 0C C2 28 60 9E A2-84 FD 96 F5 7D C1 21 54 ·½·Â(`·¢·ý·õ}Á!T
1b0 42 60 D7 7B 77 B1 E3 33-A7 F7 CE AC A1 FD 0E B3 B`×{w±ã3§÷Î¬¡ý·³
1c0 3B 55 9F EC 21 6C 91 56-E8 19 AE EA 90 4B A0 D7 ;U·ì!l·Vè·®ê·K ×
```

Cursor pos = 0

FTK Imager

Extension	Signature	Description
ZIP	50 4B 03 04	PKZIP archive_1
	ASCII PK••	Sizet: 4 Bytes Offset: 0 Bytes

ziptunnel2.zip

flag

```
00000000  1F 8B 08 08 EC 10 75 5C 00 03 66 6C 61 67 2E 7A  .‹..ì.u\..flag.z
00000010  69 70 00 75 BA 53 70 25 0C 13 2D 1A DB B6 6D 4C  ip.u°Sp%..-.Û¶mL
00000020  3C B1 6D DB 99 68 62 DB B6 6D EF D8 C9 64 C7 B6  <±mÛ™hbÛ¶mïØÉdÇ¶
```

Extension	Signature	Description
GZ	1F 8B 08	GZIP archive file
	ASCII ••	Sizet: 3 Bytes Offset: 0 Bytes

flag.gz

flag

X 70

.ZIP

.GZ

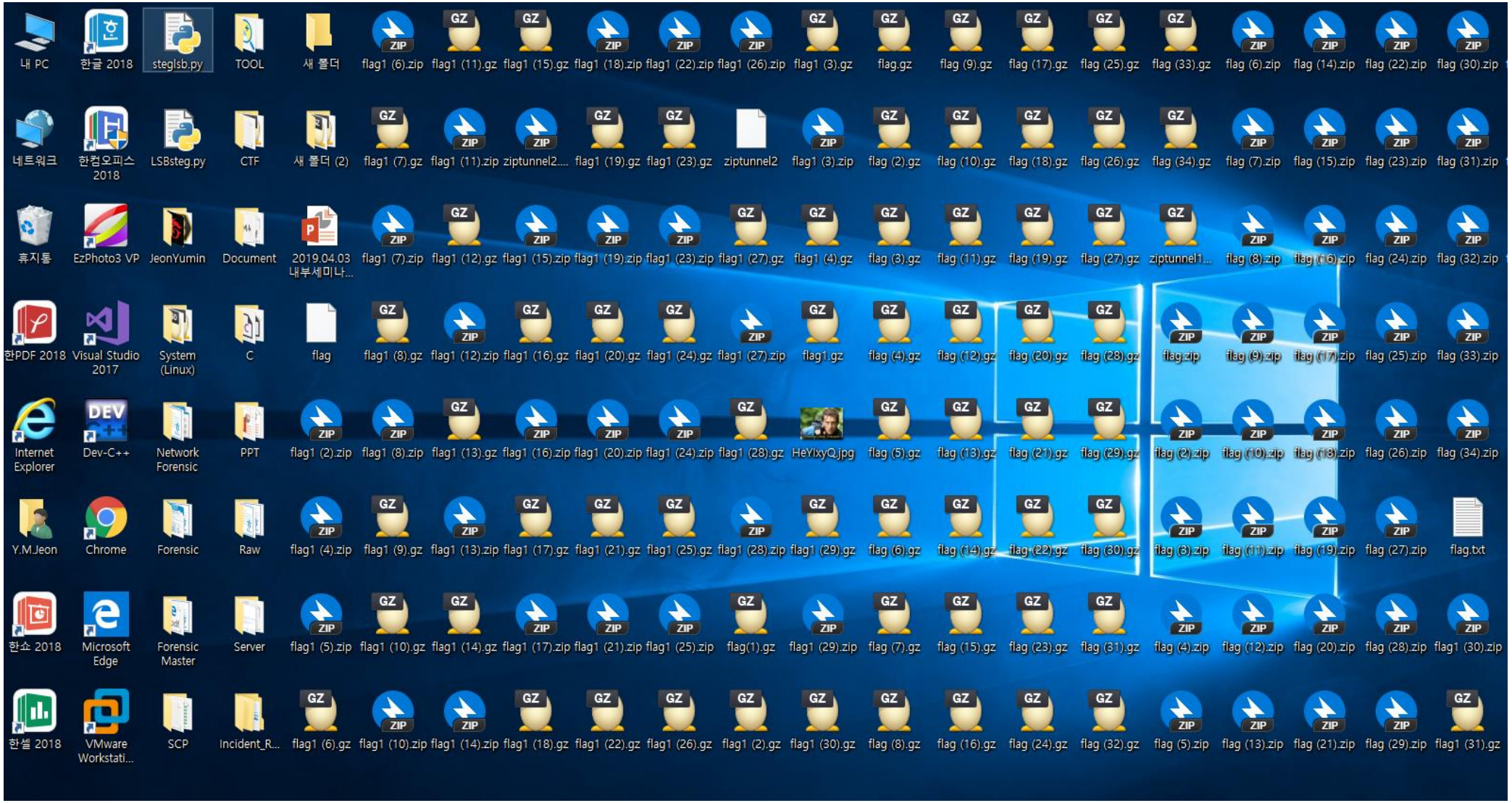
FLAG !!!

flag.txt - 메모장

파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

encryptCTF{[redacted]}

QnA


내 PC
한글 2018
steglsb.py
TOOL
새 폴더
네트워크
한컴오피스 2018
LSBsteg.py
CTF
새 폴더 (2)
휴지통
EzPhoto3 VP
JeonYumin
Document
2019.04.03 내부세미나...
한PDF 2018
Visual Studio 2017
System (Linux)
C
flag
Internet Explorer
Dev-C++
Network Forensic
PPT
Y.M.Jeon
Chrome
Forensic
Raw
한쇼 2018
Microsoft Edge
Forensic Master
Server
한셀 2018
VMware Workstati...
SCP
Incident_R...
flag1 (6).zip
flag1 (11).gz
flag1 (15).gz
flag1 (18).zip
flag1 (22).zip
flag1 (26).zip
flag1 (3).gz
flag.gz
flag (9).gz
flag (17).gz
flag (25).gz
flag (33).gz
flag (6).zip
flag (14).zip
flag (22).zip
flag (30).zip
flag1 (7).gz
flag1 (11).zip
ziptunnel2....
flag1 (19).gz
flag1 (23).gz
ziptunnel2
flag1 (3).zip
flag (2).gz
flag (10).gz
flag (18).gz
flag (26).gz
flag (34).gz
flag (7).zip
flag (15).zip
flag (23).zip
flag (31).zip
flag1 (7).zip
flag1 (12).gz
flag1 (15).zip
flag1 (19).zip
flag1 (23).zip
flag1 (27).gz
flag1 (4).gz
flag (3).gz
flag (11).gz
flag (19).gz
flag (27).gz
ziptunnel1...
flag (8).zip
flag (16).zip
flag (24).zip
flag (32).zip
flag1 (8).gz
flag1 (12).zip
flag1 (16).gz
flag1 (20).gz
flag1 (24).gz
flag1 (27).zip
flag1.gz
flag (4).gz
flag (12).gz
flag (20).gz
flag (28).gz
flag.zip
flag (9).zip
flag (17).zip
flag (25).zip
flag (33).zip
flag1 (2).zip
flag1 (8).zip
flag1 (13).gz
flag1 (16).zip
flag1 (20).zip
flag1 (24).zip
flag1 (28).gz
HeYlxyQ.jpg
flag (5).gz
flag (13).gz
flag (21).gz
flag (29).gz
flag (2).zip
flag (10).zip
flag (18).zip
flag (26).zip
flag (34).zip
flag1 (4).zip
flag1 (9).gz
flag1 (13).zip
flag1 (17).gz
flag1 (21).gz
flag1 (25).gz
flag1 (28).zip
flag1 (29).gz
flag (6).gz
flag (14).gz
flag (22).gz
flag (30).gz
flag (3).zip
flag (11).zip
flag (19).zip
flag (27).zip
flag.txt
flag1 (5).zip
flag1 (10).gz
flag1 (14).gz
flag1 (17).zip
flag1 (21).zip
flag1 (25).zip
flag(1).gz
flag1 (29).zip
flag (7).gz
flag (15).gz
flag (23).gz
flag (31).gz
flag (4).zip
flag (12).zip
flag (20).zip
flag (28).zip
flag1 (30).zip
flag1 (6).gz
flag1 (10).zip
flag1 (14).zip
flag1 (18).gz
flag1 (22).gz
flag1 (26).gz
flag1 (2).gz
flag1 (30).gz
flag (8).gz
flag (16).gz
flag (24).gz
flag (32).gz
flag (5).zip
flag (13).zip
flag (21).zip
flag (29).zip
flag1 (31).gz