Steg-Pack

Description

가짜 flag를 피해서 진짜 flag를 찾아라!@

사용한 도구

HxD

Background

zip 파일 시그니처

1. HxD 사용하여 분석

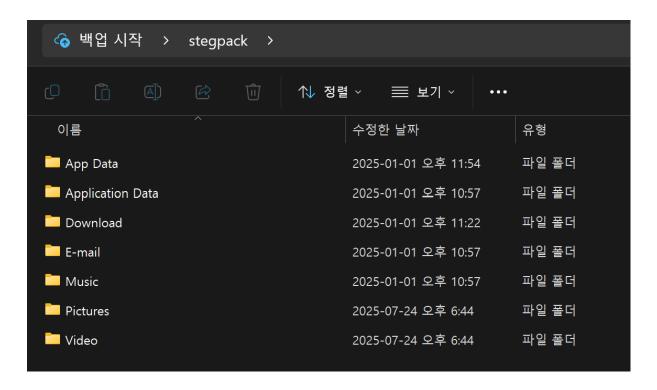
```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Decoded text
00004540 A5 11 46 01 00 00 00 50 1A 61 14 00 00 00 A5 ¥.F....P.a.....¥
                     A5 11 46 01 00 00 00 50 1A 61 14 00 00 00 00 05 11 46 01 00 00 00 50 1A 61 14 00 00 00 00 A5 11 46 01 00 00 00 50 1A 61 14 00 00 00 00 A5 11 46 01 00 00 00 50 1A 61 14 00 00 00 00 A5 11 46 01 00 00 00 50 1A 61 14 00 00 00 00 A5 11 46 01 00 00 00 50 1A 61 14 00 00 00 00 A5 11 46 01 00 00 00 50 1A 61 14 00 00 00 00 A5 11 46 01 00 00 00 50 1A 61 14 00 00 00 00 A5 11 46 01 00 00 50 1A 61 14 00 00 00 A5 11 46 01 00 00 50 1A 61 14 00 00 00 A5 11 46 01 00 00 00 50 1A 61 14 00 00 00 A5 11 46 01 00 00 00 50 1A 61 14 00 00 00 A5 11 46 01 00 00 00 50 1A 61 14 00 00 00 00 A5 11 46 01 00 00 00 50 1A 61 14 00 00 00 00 A5 11 46 01 00 00 00 50
 00004580
 00004590
 000045A0
000045B0
                                                                                                                                     10 61 14 00 00 00 00 A5 11 46 01 00 00 00 50 1A 61 14 00 00 00 00 A5 11 46 01 00 00 00 50 1A 61 14 00 00 00 00 A5 11 46 01 00 00 05 01 A61 14 00 00 00 00 A5 11 46 01 00 00 00 50 1A 61 40 00 00 00 A5 11 46 01 00 00 00 50 1A 61 14 00
 000045C0
 000045D0
000045E0
 000045F0
                                                                                                                                      ...¥.F....P.a...
..¥.F....P.a....
¥.F....P.a....¥
 00004600
                      00 00 00 A5 11 46 01 00 00 00 50 1A 61 14 00 00
                                           AS 11 46 01 00 00 00 50 1A 61 14 00 00 00 14 60 10 00 00 50 1A 61 14 00 00 00 00 14 60 10 00 00 00 50 1A 61 14 00 00 00 00 00 01 00 00 00 50 1A 61 14 00 00 00 00 A5
 00004610
00004620
                    00004630
                      A5 11 46
                                                                                                                                     00004640
 00004650
00004660
 00004670
 00004680
 000046B0
                                                                                                                                    ...Application
Data/PK....
Ű!Z....Download/PK...-!Z....E-mai
1/PK...$:!Z
 000046C0
 000046D0
000046E0
 000046F0
 00004720
                     00004730
                                                                                                                                      Music/PK.....
00004730
00004740
00004750
00004760
                                                                                                                                       04 14 00 00 00 08 00 13 B8 21 5A A8 23 FE 7B BE 26 00 00 03 2E 00 00 11 00 00 00 50 69 63 74 75 72 65 73 2F 66 66 16 72 E 50 4E 47 ED 7A 69 54 D2 5D FB 2E 95 4D 4F A8 95 99 E5 50 D9 E0 6C 45
                                                                                                                                      ....,!Z"#p{%
&....Pictu
res flag.PNGiziT
Ò]û.•MO£•™åPUålE
 00004770
 00004780
 000047A0
000047A0 E6 88 66 83 94 56 8E 38 4F A5 82 E6 94 1A 0E 10
000047C0 52 D9 E8 10 0D 8E 99 52 8F 61 8A 82 9A 22 CE 58
                                                                                                                                       æ^ff"VŽ8O¥,æ".
```

zip 파일 시그니처인 504B0304 검색 → 존재

Steg-Pack 1

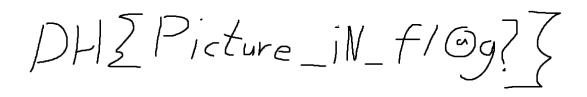
2. zip 파일 추출

zip 에 해당하는 offset 추출 후 stegpack.zip 으로 저장했다.



별다른 암호 없이 압축해제가 가능했다.

C:\Users\user\Desktop\stegpack\Pictures\flag.PNG 경로에서 flag.png 를 찾을 수 있었다



FLAG

DH{Picture_iN_fl@g?}