Dreamhack-structure-based carving(level2)

[forensics]

Description

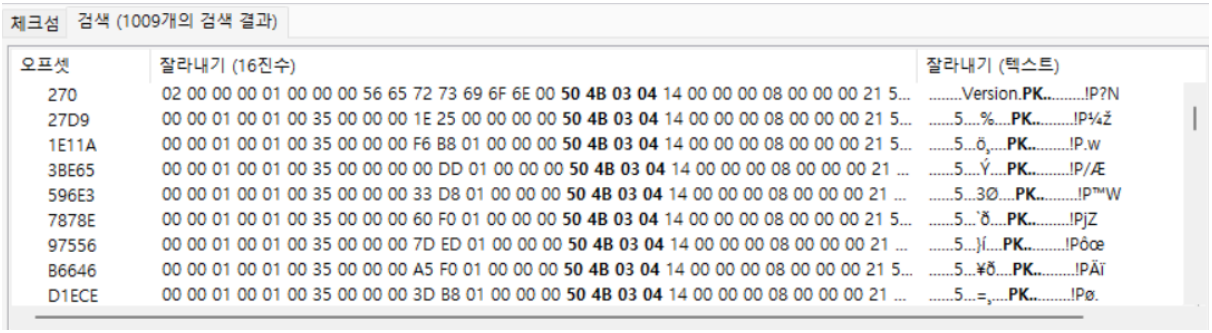
주어진 바이너리 파일에서 플래그를 찾아보세요!

힌트는 `압축 패스워드는 ZIP 구조 어딘가에...` **입니다.** (2024.10.02)

Write up

- 사용 도구: HxD

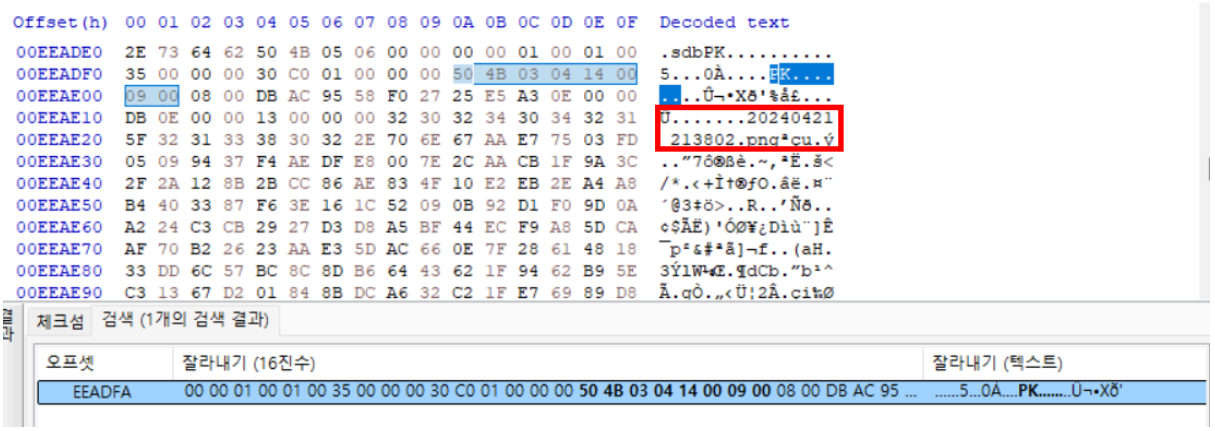
- Zip 파일 헤더(`50 4B 03 04`) 검색 → 1009개의 검색 결과 확인



체크섬 검색 (1009개의 검색 결과)

오프셋	잘라내기 (16진수)	잘라내기 (텍스트)
270	02 00 00 00 01 00 00 00 56 65 72 73 69 6F 6E 00 **50 4B 03 04** 14 00 00 00 08 00 00 00 21 5...	.....Version.**PK**.....!P?N
27D9	00 00 01 00 01 00 35 00 00 00 1E 25 00 00 00 00 **50 4B 03 04** 14 00 00 00 08 00 00 00 21 5...	.....5.....%....**PK**.....!P¼ž
1E11A	00 00 01 00 01 00 35 00 00 00 F6 B8 01 00 00 00 **50 4B 03 04** 14 00 00 00 08 00 00 00 21 5...	.....5...ö¸....**PK**.....!P.w
3BE65	00 00 01 00 01 00 35 00 00 00 00 DD 01 00 00 00 **50 4B 03 04** 14 00 00 00 08 00 00 00 21 ...	.....5....Ý....**PK**.....!P/Æ
596E3	00 00 01 00 01 00 35 00 00 00 33 D8 01 00 00 00 **50 4B 03 04** 14 00 00 00 08 00 00 00 21 ...	.....5...3Ø....**PK**.....!P™W
7878E	00 00 01 00 01 00 35 00 00 00 60 F0 01 00 00 00 **50 4B 03 04** 14 00 00 00 08 00 00 00 21 5...	.....5...`ð....**PK**.....!PjZ
97556	00 00 01 00 01 00 35 00 00 00 7D ED 01 00 00 00 **50 4B 03 04** 14 00 00 00 08 00 00 00 21 ...	.....5...}í....**PK**.....!Póœ
B6646	00 00 01 00 01 00 35 00 00 00 A5 F0 01 00 00 00 **50 4B 03 04** 14 00 00 00 08 00 00 00 21 5...	.....5...¥ð....**PK**.....!PÄï
D1ECE	00 00 01 00 01 00 35 00 00 00 3D B8 01 00 00 00 **50 4B 03 04** 14 00 00 00 08 00 00 00 21 ...	.....5...=¸....**PK**.....!Pø.

- `50 4B 03 04 14 00 09 00` 검색 → 1개의 검색 결과 확인
  - `50 4B 03 04` → zip 파일 시그니처
  - `14 00` → zip을 추출하는 데 필요한 최소 버전(2.0)
  - `09 00` → 암호화된 UTF-8 파일
  - 내부의 `20240421_213802.png` 파일 확인



Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Decoded text

00EEADE0 2E 73 64 62 50 4B 05 06 00 00 00 00 01 00 01 00 .sdbPK.....
00EEADF0 35 00 00 00 30 C0 01 00 00 00 50 4B 03 04 14 00 5...0À....PK....
00EEAE00 09 00 08 00 DB AC 95 58 F0 27 25 E5 A3 0E 00 00 ....Û¬•Xð'%å£...
00EEAE10 DB 0E 00 00 13 00 00 00 32 30 32 34 30 34 32 31 Û.......20240421
00EEAE20 5F 32 31 33 38 30 32 2E 70 6E 67 AA E7 75 03 FD _213802.png ªçu.ý
00EEAE30 05 09 94 37 F4 AE DF E8 00 7E 2C AA CB 1F 9A 3C ..”7ô®ßè.~,ªË.š<
00EEAE40 2F 2A 12 8B 2B CC 86 AE 83 4F 10 E2 EB 2E A4 A8 /*.‹+Ì†®ƒO.âë.¤¨
00EEAE50 B4 40 33 87 F6 3E 16 1C 52 09 0B 92 D1 F0 9D 0A ´@3‡ö>..R..'Ñð..
00EEAE60 A2 24 C3 CB 29 27 D3 D8 A5 BF 44 EC F9 A8 5D CA ¢$ÃË)'ÓØ¥¿DìùÊ
00EEAE70 AF 70 B2 26 23 AA E3 5D AC 66 0E 7F 28 61 48 18 ¯p²&#ªã]¬f..(aH.
00EEAE80 33 DD 6C 57 BC 8C 8D B6 64 43 62 1F 94 62 B9 5E 3ÝlW¼Œ.¶dCb.”b¹^
00EEAE90 C3 13 67 D2 01 84 8B DC A6 32 C2 1F E7 69 89 D8 Ã.gÒ.„‹Ü¦2Â.çi‰Ø

체크섬 검색 (1개의 검색 결과)

오프셋	잘라내기 (16진수)	잘라내기 (텍스트)
EEADFA	00 00 01 00 01 00 35 00 00 00 30 C0 01 00 00 00 **50 4B 03 04 14 00 09 00** 08 00 DB AC 95 ...	.....5...0À....**PK.....**Û¬•X

- zip 파일 구조 내부에서 평문 형태의 비밀번호 확인
  - 비밀번호: `a1b2c3d4e5f6`

Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Decoded text

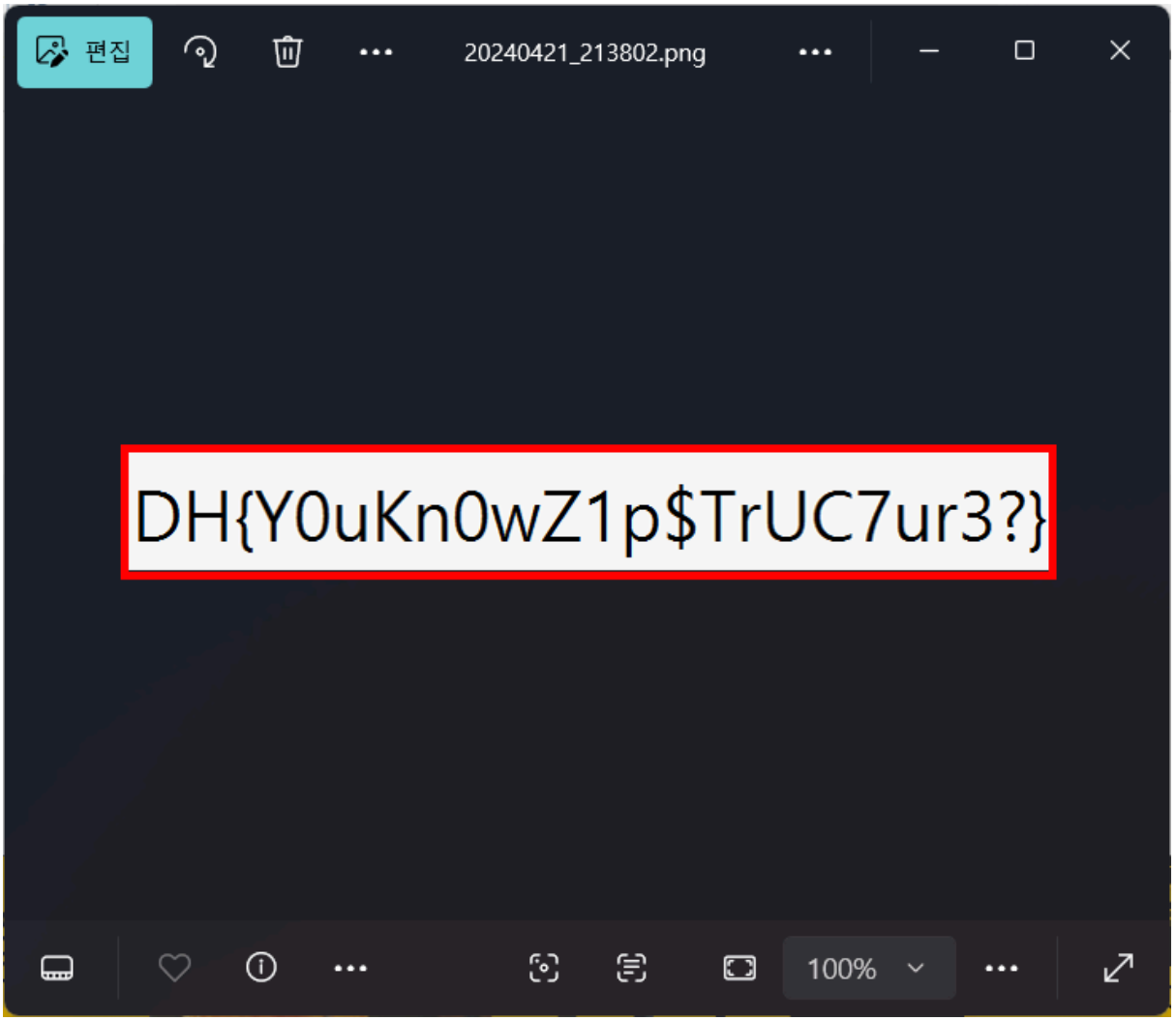
00EEBCB0 18 CF ED 70 60 E8 64 D3 B9 91 A6 75 D9 2F 2C F8 .Ïíp`èdÓ¹'¦uÙ/,ø
00EEBCC0 29 BC A8 CD 49 00 78 69 E9 B0 13 63 FA 25 50 4B)¼¨ÍI.xié°.cú%PK
00EEBCD0 01 02 14 00 14 00 09 00 08 00 DB AC 95 58 F0 27 ....Û¬•Xð'
00EEBCE0 25 E5 A3 0E 00 00 DB 0E 00 00 13 00 24 00 00 00 %å£...Û.....$...
00EEBCF0 00 00 00 00 20 00 00 00 00 00 00 00 32 30 32 34 2024
00EEBD00 30 34 32 31 5F 32 31 33 38 30 32 2E 70 6E 67 7A 0421_213802.pngz
00EEBD10 31 70 5F 70 34 73 35 77 30 33 64 5F 31 73 5F 61 1p_p4s5w03d_1s_a
00EEBD20 31 62 32 63 33 64 34 65 35 66 36 00 00 00 00 00 1b2c3d4e5f6.....
00EEBD30 00 00 00 50 4B 05 06 00 00 00 00 01 00 01 00 65 ...PK..........e
00EEBD40 00 00 00 D4 0E 00 00 00 00 50 4B 03 04 14 00 00 ...Ô.....PK.....
00EEBD50 00 08 00 00 00 21 50 CA 12 DF 97 AA B6 01 00 77 .....!PÊ.ß—ª¶..w
00EEBD60 28 06 00 07 00 00 00 32 32 30 2E 73 64 62 BC 9D (.......220.sdb¼.

- `50 4B 03 04 14 00 09 00` 부터 추출 후 `flag.zip`으로 저장

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 09 00 08 00 DB AC 95 58 F0 27 PK.....Û¬•Xð'
00000010 25 E5 A3 0E 00 00 DB 0E 00 00 13 00 00 00 32 30 %å£...Û.....20
00000020 32 34 30 34 32 31 5F 32 31 33 38 30 32 2E 70 6E 240421_213802.pn
00000030 67 AA E7 75 03 FD 05 09 94 37 F4 AE DF E8 00 7E gªçu.ý..”7ô®ßè.~
00000040 2C AA CB 1F 9A 3C 2F 2A 12 8B 2B CC 86 AE 83 4F ,ªË.š</*.‹+Ì†®ƒO
00000050 10 E2 EB 2E A4 A8 B4 40 33 87 F6 3E 16 1C 52 09 .âë.¤¨´@3‡ö>..R.
00000060 0B 92 D1 F0 9D 0A A2 24 C3 CB 29 27 D3 D8 A5 BF .'Ñð..¢$ÃË)'Ó Ø¥¿
00000070 44 EC F9 A8 5D CA AF 70 B2 26 23 AA E3 5D AC 66 DìùÊ¯p²&#ªã]¬f
00000080 0E 7F 28 61 48 18 33 DD 6C 57 BC 8C 8D B6 64 43 ..(aH.3ÝlW¼Œ.¶dC
00000090 62 1F 94 62 B9 5E C3 13 67 D2 01 84 8B DC A6 32 b.”b¹^Ã.gÒ.„‹Ü¦2
000000A0 C2 1F E7 69 89 D8 8C 10 71 1B 24 F8 C2 47 68 72 Â.çi‰ØŒ.q.$øÂGhr
000000B0 11 21 C8 50 F2 4D 1A 74 E2 9E A1 48 60 55 3A 42 .!ÈPòM.tâž¡H`U:B

- 압축 해제 후 `20240421_213802.png` 파일 확인
  - DH{Y0uKn0wZ1p$TrUC7ur3?}



- FLAG는, DH{Y0uKn0wZ1p$TrUC7ur3?}

FLAG

DH{Y0uKn0wZ1p$TrUC7ur3?}