Dreamhack-structure-based carving(level2)

👉 **[함께실습] structure-based carving에서 실습하는 문제입니다.**

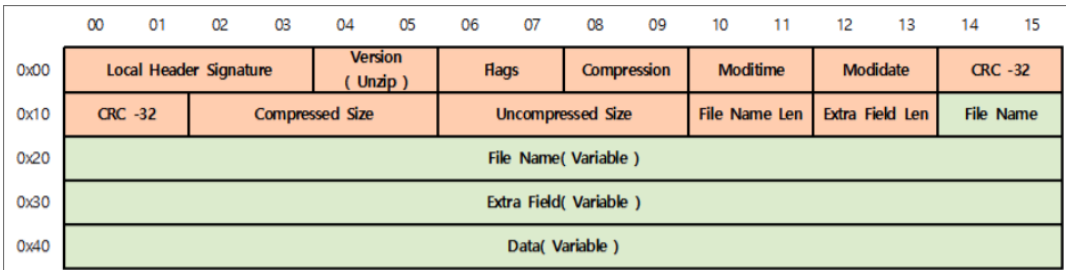
주어진 바이너리 파일에서 플래그를 찾아보세요!

힌트는 `압축 패스워드는 ZIP 구조 어딘가에...` **입니다.**

사용 툴 - HxD

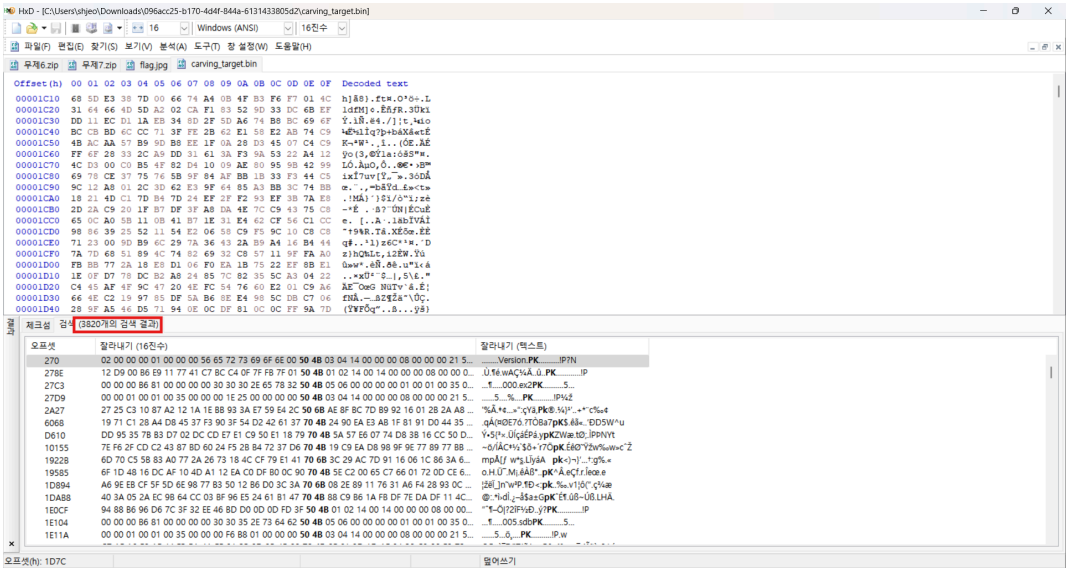
1. Carving
   - 파일 시스템 메타데이터 없이 파일의 구조적 특징을 기반으로 데이터를 추출하는 기술
   - 파일 내부의 시그니처를 활용하여 파일 복원

2. ZIP 파일 구조

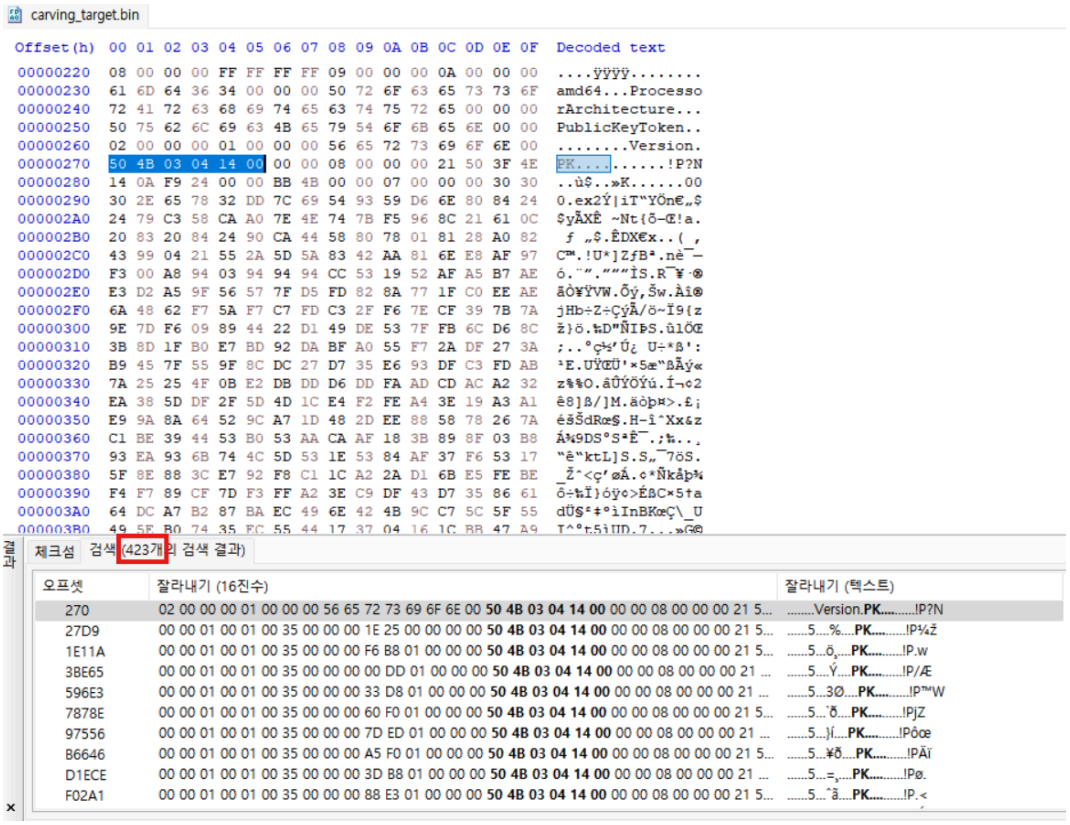


Size	Information
4	Central Directory Header Signature (0x50 4B 01 02)
2	Flags **0x00: Encrypted File** 0x01, 02: Compression Option 0x03: Data Descriptor 0x04: Enhanced Deflation 0x05: Compressed Patched Data **0x06: Strong Encryption** 0x07 ~ 0A: Unused 0x0B: Language Encoding 0x0C: Reserved 0x0D: Mask Header Values 0x0E ~ 0F: Reserved
2	Compression
2	Modified Time
2	Modified Date
4	Compressed Size
4	Uncompressed Size
2	File Name Length
4	Local Header Offset
??	File Name

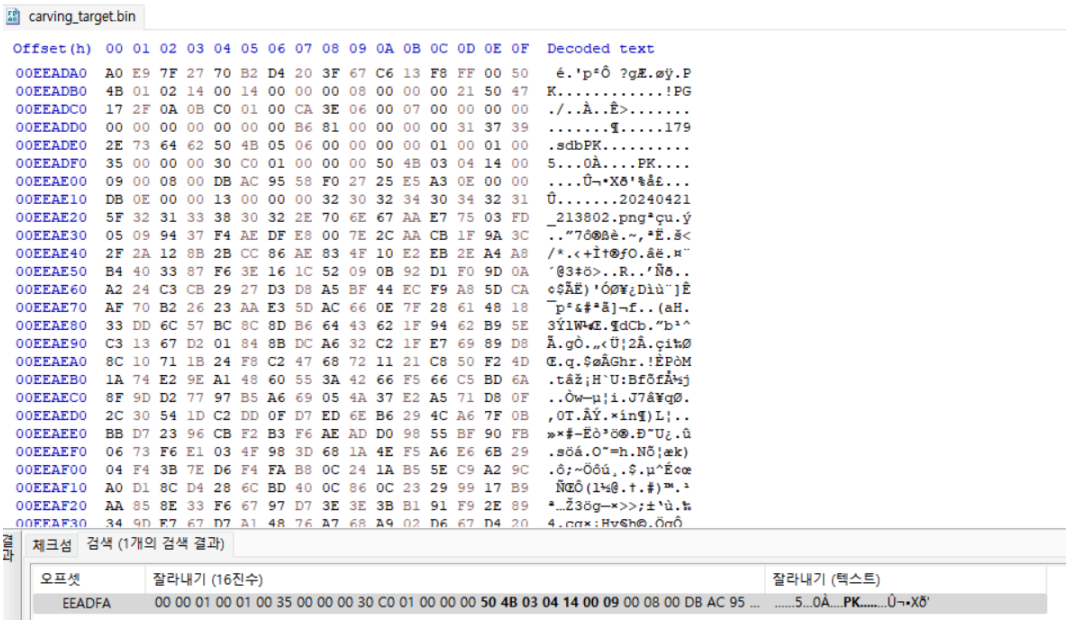
3. HxD 를 통해, PK 파일 확장자를 검색한 결과 3820개의 결과가 나왔음 → 압축 패스워드가 존재하는 것으로 보아 암호화된 ZIP 파일 형태를 찾기로 함



4. 암호화된 ZIP 파일 형태 → 50 4B 03 04 14 00 로 진행하였으나, 검색 결과가 423개로 바이너리 검색의 범위를 좁히기로 함



5. 암호화된 ZIP 파일 형태 → 50 4B 03 04 14 00 08 / 50 4B 03 04 14 00 09 로 진행한 결과, 09 일 때 검색 결과 하나 나옴

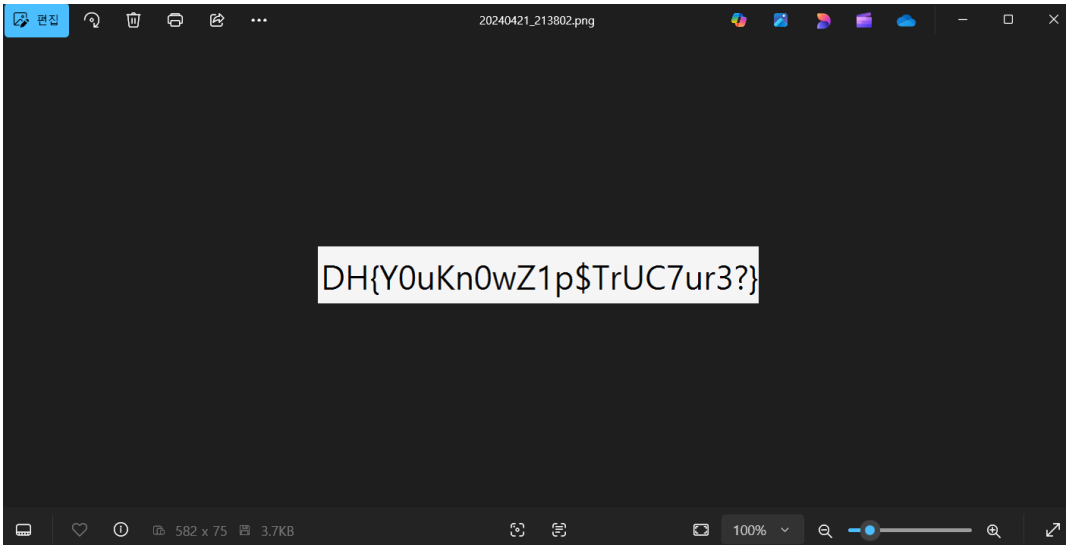


6. 해당 ZIP 파일 추출 및 해당 ZIP 파일 Footer를 확인할 때 암호화된 zip 파일 복호화를 위한 암호 확인

```
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.....
```

⇒ a1b2c3d4e5f6

7. ZIP 파일 추출하면 암호화된 이미지 → 복호화



👉🏻 DH{Y0uKn0wZ1p$TrUC7ur3?}