

# 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

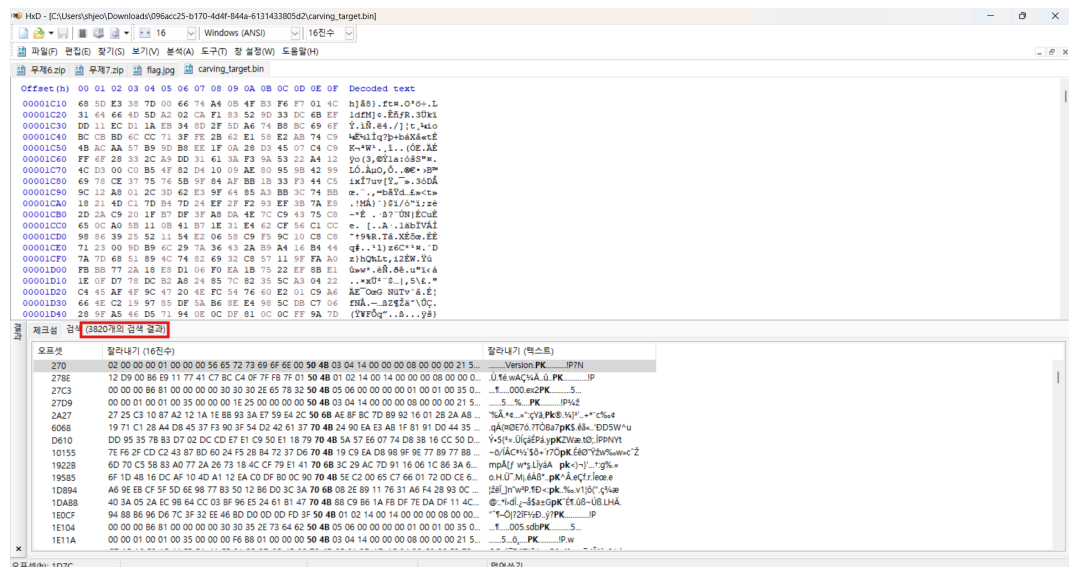
- 파일 시스템 메타데이터 없이 파일의 구조적 특징을 기반으로 데이터를 추출하는 기술
- 파일 내부의 시그니처를 활용하여 파일 복원

### 2. ZIP 파일 구조

	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15
0x00	Local Header Signature				Version ( Unzip )		Flags		Compression		Moditime		Modidate		CRC -32	
0x10	CRC -32		Compressed Size				Uncompressed Size				File Name Len		Extra Field Len		File Name	
0x20	File Name( Variable )															
0x30	Extra Field( Variable )															
0x40	Data( Variable )															

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 패스워드 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

carving\_target.bin

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000220	08	00	00	00	FF	FF	FF	09	00	00	00	0A	00	00	00	00	....YYY.....
00000230	61	6D	64	36	34	00	00	00	50	72	6F	63	65	73	73	6F	amd64...Processo
00000240	72	41	72	63	68	69	74	65	63	74	75	72	65	00	00	00	rArchitecture...
00000250	50	75	62	6C	69	63	4B	65	79	54	6F	6B	65	6E	00	00	PublicKeyToken...
00000260	02	00	00	00	01	00	00	00	56	65	72	73	69	6F	6E	00	.....Version.
00000270	50	4B	03	04	14	00	00	00	08	00	00	00	21	50	3F	4E	PK.....!P?N
00000280	14	0A	F9	24	00	00	00	00	00	00	00	00	00	00	00	30	..u\$...K.....00
00000290	30	2E	65	78	32	DD	7C	69	54	93	59	D6	6E	80	84	24	0.ex2Y iT"YOne,\$
000002A0	24	79	C3	58	CA	A0	7E	4E	74	7B	F5	96	8C	21	61	0C	\$yAXE ~Nt(5-Q!a.
000002B0	20	83	20	84	24	90	CA	44	58	80	78	01	81	28	A0	82	f..\$.EDXex..( ,
000002C0	43	99	04	21	55	2A	5D	5A	83	42	AA	81	6E	E8	AF	97	C".!U"jZfB*.ne-
000002D0	F3	00	A8	94	03	94	94	94	CC	53	19	52	AF	A5	B7	AE	ó..".""iS.R"Y-@
000002E0	E3	D2	A5	9F	56	57	7F	D5	FD	82	8A	77	1F	C0	EE	AE	ãÖYVW.Öy,Sw.Äi@
000002F0	6A	48	62	F7	5A	F7	C7	FD	C3	2F	F6	7E	CF	39	7B	7A	jHb÷Z÷ÇýÄ/ö-i9(z
00000300	9E	7D	F6	09	89	44	22	D1	49	DE	53	7F	FB	6C	D6	8C	ž)ö.kD*NIPs.ÜlÖE
00000310	3B	8D	1F	B0	E7	BD	92	DA	BF	A0	55	F7	2A	DF	27	3A	;..*ç'Uç U÷*B':
00000320	B9	45	7F	55	9F	8C	DC	27	D7	35	E6	93	DF	C3	FD	AB	+E.UYÜU'«5«BÄy«
00000330	7A	25	25	4F	0B	E2	DB	DD	D6	DD	FA	AD	CD	AC	A2	32	z%0.äÜYÖYü.î~c2
00000340	EA	38	5D	DF	2F	5D	4D	1C	E4	F2	FE	A4	3E	19	A3	A1	è8]B/JM.äöþ»>.éj
00000350	E9	9A	8A	64	52	9C	A7	1D	48	2D	EE	88	58	78	26	7A	és5dRøç.H-i"Xxëz
00000360	C1	BE	39	44	53	B0	53	AA	CA	AF	18	3B	89	8F	03	B8	Ä%9DS°S+E";;w...
00000370	93	EA	93	6B	74	4C	5D	53	1E	53	84	AF	37	F6	53	17	"è"ktL]S.S..7öS.
00000380	5F	8E	88	3C	E7	92	F8	C1	1C	A2	2A	D1	6B	E5	FE	BE	Ž~<ç'«Ä.c*Nkâþ%4
00000390	F4	F7	89	CF	7D	F3	FF	A2	3E	C9	DF	43	D7	35	86	61	ö~kI)öyç>ÉAC×5ta
000003A0	64	DC	A7	B2	87	BA	EC	49	6E	42	4B	9C	C7	5C	5F	55	dÜ\$*+*iInBKøÇ_U
000003B0	49	5F	B0	74	35	FC	55	44	17	37	04	16	1C	BB	47	A9	T^+5iID.7...»G@

체크섬 검색 (423개)의 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 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 08 00 00 00 21 5...	5....%.PK.....!P%z
1E11A	00 00 01 00 01 00 35 00 00 00 F6 88 01 00 00 00 50 4B 03 04 14 00 00 08 00 00 00 21 5...	5....ö...PK.....!P.w
38E65	00 00 01 00 01 00 35 00 00 00 DD 01 00 00 00 50 4B 03 04 14 00 00 08 00 00 00 21 ...	5....Y...PK.....!P/E
596E3	00 00 01 00 01 00 35 00 00 00 33 D8 01 00 00 00 50 4B 03 04 14 00 00 08 00 00 00 21 ...	5...3Ö...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 08 00 00 00 21 5...	5....ö...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 08 00 00 00 21 ...	5....j]...PK.....!Pöe
B6646	00 00 01 00 01 00 35 00 00 00 A5 F0 01 00 00 00 50 4B 03 04 14 00 00 08 00 00 00 21 5...	5....#ö...PK.....!PÄi
D1ECE	00 00 01 00 01 00 35 00 00 00 3D B8 01 00 00 00 50 4B 03 04 14 00 00 08 00 00 00 21 ...	5....=...PK.....!Pø.
F02A1	00 00 01 00 01 00 35 00 00 00 88 E3 01 00 00 00 50 4B 03 04 14 00 00 08 00 00 00 21 5...	5....ä...PK.....!P.<

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

carving\_target.bin

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00EEADA0	A0	E9	7F	27	70	B2	D4	20	3F	67	C6	13	F8	FF	00	50	é.'p'ô ?qÆ.øý.P
00EEADB0	4B	01	02	14	00	14	00	00	08	00	00	00	21	50	47		K.....!FG
00EEADC0	17	2F	0A	0B	C0	01	00	CA	3E	06	00	07	00	00	00	00	/..Ä..È>.....
00EADD00	00	00	00	00	00	00	00	B6	81	00	00	00	00	31	37	39	.....¶.....179
00EEADE0	2E	73	64	62	50	4B	05	06	00	00	00	00	01	00	01	00	.sdbPK.....
00EADF00	35	00	00	00	30	C0	01	00	00	00	50	4B	03	04	14	00	5....0Ä.....PK.....
00EEAF00	09	00	08	00	DB	AC	95	58	F0	27	25	E5	A3	0E	00	00	....Ü~Xö'«äé...
00EEAF10	DB	0E	00	00	13	00	00	00	32	30	32	34	30	34	32	31	Ü.....20240421
00EEAF20	5F	32	31	33	38	30	32	2E	70	6E	67	AA	E7	75	03	FD	_213802.png*çu.ý
00EEAF30	05	09	94	37	F4	AE	DF	E8	00	7E	2C	AA	CB	1F	9A	3C	..7Ööøè..~,*È.š<
00EEAF40	2F	2A	12	8B	2B	CC	86	AE	83	4F	10	E2	EB	2E	A4	A8	/*..<+itøfO.äé.h"
00EEAF50	B4	40	33	87	F6	3E	16	1C	52	09	0B	92	D1	F0	9D	0A	'@3+ö>...R..Nö..
00EEAF60	A2	24	C3	CB	29	27	D3	D8	A5	BF	44	EC	F9	A8	5D	CA	ç\$ÄE)'ÖöYçDiù`jÈ
00EEAF70	AF	70	B2	26	23	AA	E3	5D	AC	66	0E	7F	28	61	48	18	p'«#*Ä]~f..(aH.
00EEAF80	33	DD	6C	57	BC	8C	8D	B6	64	43	62	1F	94	62	B9	5E	3Y1W4E.çdCb.."b'^
00EEAF90	C3	13	67	D2	01	84	8B	DC	A6	32	C2	1F	E7	69	89	D8	Ä.gö..«Ü;2Ä.çit«Ø
00EEAFA0	8C	10	71	1B	24	F8	C2	47	68	72	11	21	C8	50	F2	4D	Æ.q.ø«ÄGhr.'ÈPòM
00EEAFB0	1A	74	E2	9E	A1	48	60	55	3A	42	66	F5	66	C5	BD	6A	.täž;H`U:BföfÄyçj
00EEAFC0	8F	9D	D2	77	97	B5	A6	69	05	4A	37	E2	A5	71	D8	0F	..Öw~µ;i.U7ÄYqØ.
00EEAFD0	2C	30	54	1D	C2	DD	0F	D7	ED	6E	B6	29	4C	A6	7F	0B	,OT.ÄY..inç)l]..
00EEAFE0	B6	D7	23	96	CB	F2	B3	F6	AE	AD	D0	98	55	BF	90	FB	»*#-Èö'øØ.D`Üç.ä
00EEAFF0	0B	73	F6	E1	03	4F	98	3D	68	1A	4E	F5	A6	E6	6B	29	.söä.O"=h.Nö;«k)
00EEAF00	04	F4	3B	7E	D6	F4	FA	B8	0C	24	1A	B5	5E	C9	A2	9C	.ö;~Ööü..\$.µ^Éç«
00EEAF10	A0	D1	8C	D4	28	6C	BD	40	0C	86	0C	23	29	99	17	B9	NöÖ(14ü.†.#)™..^
00EEAF20	AA	85	8E	33	F6	67	97	D7	3E	3E	3B	B1	91	F9	2E	89	*...Ž3öç~x>>;±'ü.ü
00EEAF30	34	9D	F7	67	D7	A1	48	76	A7	68	A9	02	D6	67	D4	20	4.gçx:HvSh@.ÖçÖ

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..0Ä...PK.....Ü~Xö'

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

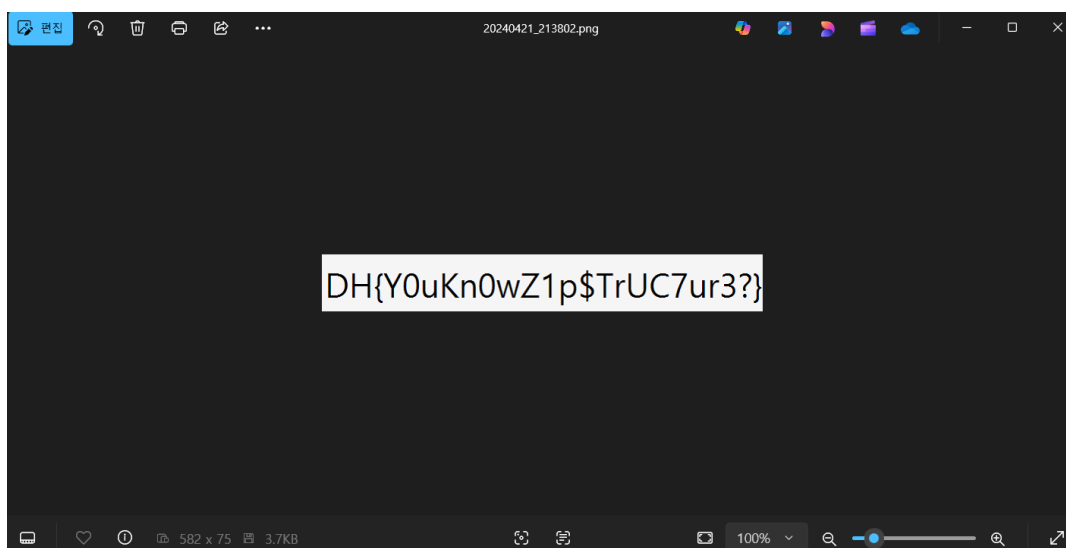
```

00EEBCE0 25 E5 A3 0E 00 00 DB 0E 00 00 13 00 24 00 00 00 %â&...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 lp_p4s5w03d_ls_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?}