Dreamhack-structure-based carving

문제

Description

[함께실습] structure-based carving에서 실습하는 문제입니다.

주어진 바이너리 파일에서 플래그를 찾아보세요!

힌트는 압축 패스워드는 ZIP 구조 어딘가에... 입니다.

풀이

- 문제 파악
 바이너리 파일 안 ZIP파일에 플래그 존재 → ZIP파일을 찾아야하므로 ZIP파일 시그니처 기반 분석을 진행
- 2. 문제 풀이

arving_target.bin																	
Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	50	63	6D	48	01	00	00	00	00	00	00	00	D2	25	D2	D5	PcmHÒ%ÒÕ
00000010	FC	7 F	20	12	0F	00	00	00	84	00	00	00	0B	00	00	00	ü
00000020	54	00	00	00	00	00	00	00	00	00	00	00	01	00	00	00	T
00000030	80	00	00	00	00	00	00	00	00	00	00	00	03	00	00	00	€
00000040	FF	FF	FF	FF	FF	1B	35	28	25	D5	55	41	AC	B0	6E	7C	ÿÿÿÿÿ.5(%ÕUA¬°n
00000050	64	C7	25	D8	08	00	00	00	08	00	00	00	0E	00	00	00	dÇ%Ø
00000060	0B	00	00	00	05	00	00	00	0C	00	00	00	07	00	00	00	
00000070	0D	00	00	00	09	00	00	00	OA.	00	00	00	06	00	00	00	
00000080	04	00	00	00	1C	00	00	01	E0	01	00	00	10	00	00	06	à
00000090	FC	00	00	00	08	00	00	01	60	02	00	00	14	00	00	09	ü`
000000A0	0C	01	00	00	34	00	00	04	FC	01	00	00	1D	00	00	02	4ü
000000B0	30	01	00	00	05	00	00	02	30	02	00	00	0B	00	00	02	0
000000C0	20	01	00	00	21	00	00	02	50	01	00	00	10	00	00	02	!P
000000D0		01	00	00	15	00	00	02	38	02	00	00	04	00	00		t8
000000E0		01	00	00		00	00	02	68	02	00	00	0E	00			,h
000000F0	50	02	00	00	5C	00	00	02	84	01	00	00	01	01	00	00	₽\"
00000100	7C	9E	08	4E	01	00	00	00	00	00	00	00	00	02	00	00	ž.N
00000110	00	00	00	00	01	00	00	00	01	00	00	00	02	00	00	00	
00000120		2E	30	2E	31	35	39	31	32	2E	30	00	4E	61		65	4.0.15912.0.Name
00000130	53	79	73	74	65		2E			2E		6F	6D	70		65	System.IO.Compre
00000140	73	73	69	6F	6E	2E	5A	69	70	46	69	6C	65	00	00	00	ssion.ZipFile
00000150	53	79	73	74	65	6D	2E	49	4F	2E	43	6F	6D	70	72	65	System.IO.Compre
00000160	73	73	69	6F	6E	2E		69	70	46		6C	65	2E		6C	ssion.ZipFile.dl
00000170	6C	00	00	00	62	37	37	61	35	63	35	36	31	39		34	1b77a5c561934
00000180	65	30	38	39	4D	69	63	72	6F	73		66			4E		e089Microsoft.NE
00000190		5C	41	73	73	65	6D	62	6C	79	5C	47	41	43	5F		T\Assembly\GAC_M
000001A0	53	49	4C	5C	53	79	73	74	65	6D	2E	49	4F	2E	43	6F	SIL\System.IO.Co
000001B0	6D	70	72	65	73	73	69	6F	6E	2E	5A	69	70	46	69		mpression.ZipFil
000001C0	65	5C	76	34	2E	30	5F	34	2E	30	2E	30	2E	30	5F		e\v4.0_4.0.0.0_
000001D0	62	37	37	61	35	63	35	36	31	39	33	34	65	30	38	39	b77a5c561934e089
000001E0		00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000001F0	FF	FF	FF	FF	FF	FF	FF	FF	00	00	00	00	04	00	00	00	ÿÿÿÿÿÿÿ nnnn
00000200	FF	FF	FF	FF	03	00	00	00	04	00	00	00	FF	FF	FF	FF	ÿÿÿÿÿÿÿÿ
00000210	05	00	00	00	06	00	00	00	FF	FF	FF	FF	07	00	00	00	·····ÿÿÿÿ····
00000220	08	00	00	00	FF	FF	FF	FF	09	00	00	00	0A	00	00	00	····ÿÿÿÿ······
00000230		6D	64	36	34	00	00	00	50	72	6F	63	65	73	73	6F	amd64Processo
00000240	72	41	72	63	68	69	74	65	63	74	75	72	65	00	00	00	rArchitecture

바이너리 파일

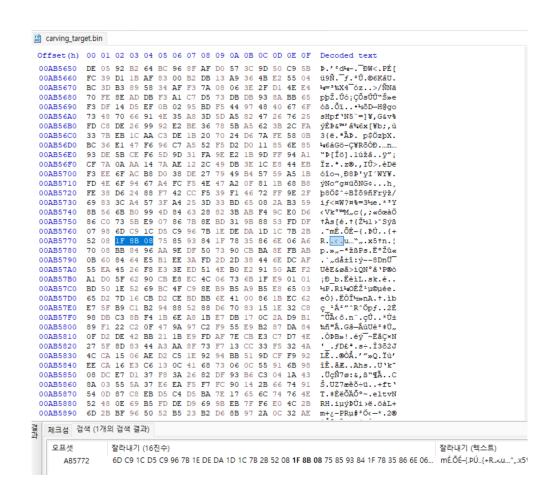
GCK File Signature Table Powered by



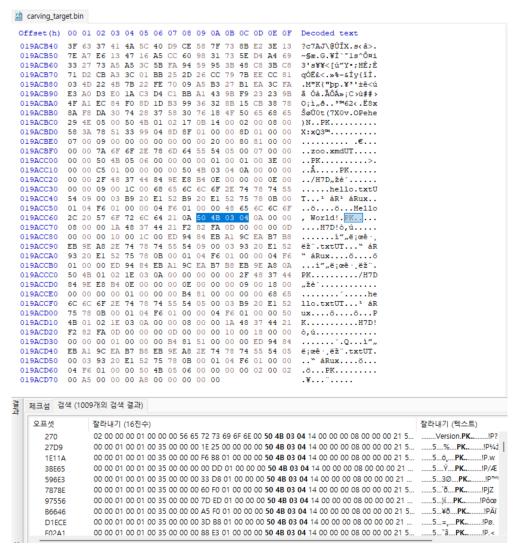
ASCII File Description	zip			Show Pa	aginated
ASCII File Description	Header (HEX)	File Extension	File Class	Header Offset	Trailer (He
GZIP archive file	1F 8B 08	GZ	Compressed archive	0	(null)
7-Zip compressed file	37 7A BC AF 27 1C	7Z	Compressed archive	0	(null)
bzip2 compressed archive	42 5A 68	BZ2 TAR BZ2 TBZ2 TB2	Compressed archive	0	(null)
PKZIP archive_1	50 4B 03 04	ZIP	Compressed archive	0	50 4B ????
ZLock Pro encrypted ZIP	50 4B 03 04 14 00 01 00	ZIP	Compressed archive	0	(null)
PKZIP archive_2	50 4B 05 06	ZIP	Compressed archive	0	(null)
PKZIP archive_3	50 4B 07 08	ZIP	Compressed archive	0	(null)
WinZip compressed archive	57 69 6E 5A 69 70	ZIP	Compressed archive	29152	(null)

© 2025 SEARCH Group, Incorporated

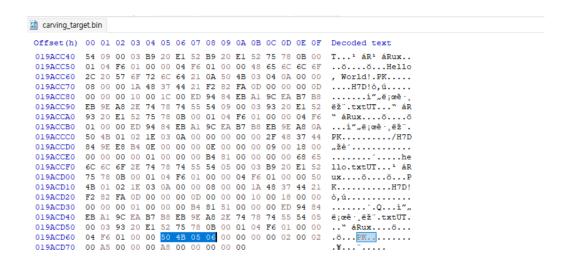
ZIP파일 HxD값을 검색하여 분석하였다.



GZIP archive file: 1F 8B 08

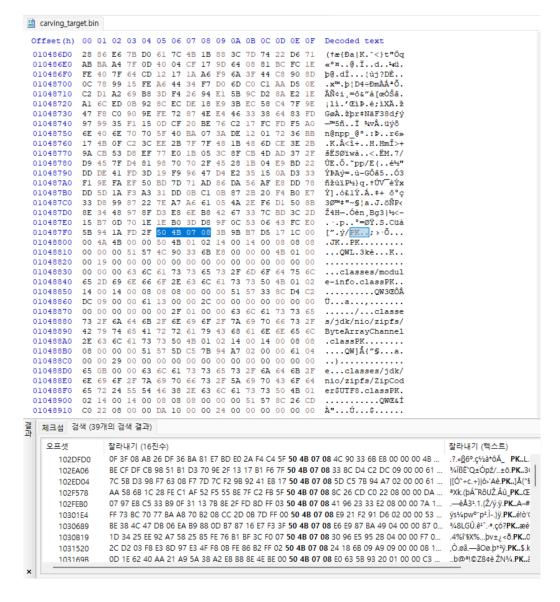


PKZIP archive 1: 50 4B 03 04



오프셋	잘라내기 (16진수)	잘라내기 (텍스트)
27C3	00 00 00 B6 81 00 00 00 00 30 30 30 2E 65 78 32 50 4B 05 06 00 00 00 01 00 01 00 35 0	¶000.ex2 PK 5
1E104	00 00 00 B6 81 00 00 00 00 30 30 35 2E 73 64 62 50 4B 05 06 00 00 00 00 01 00 01 00 35 0	¶005.sdb PK 5
3BE4F	00 00 00 B6 81 00 00 00 00 30 30 38 2E 73 64 62 50 4B 05 06 00 00 00 00 01 00 01 00 35 0	¶008.sdb PK 5
596CD	00 00 00 B6 81 00 00 00 00 30 30 39 2E 73 64 62 50 4B 05 06 00 00 00 00 01 00 01 00 35 0	¶009.sdb PK 5
78778	00 00 00 B6 81 00 00 00 00 30 31 30 2E 73 64 62 50 4B 05 06 00 00 00 00 01 00 01 00 35 0	¶010.sdb PK 5
97540	00 00 00 B6 81 00 00 00 00 30 31 31 2E 73 64 62 50 4B 05 06 00 00 00 00 01 00 01 00 35 0	¶011.sdb PK 5
B6630	00 00 00 B6 81 00 00 00 00 30 31 32 2E 73 64 62 50 4B 05 06 00 00 00 00 01 00 01 00 35 0	¶012.sdb PK 5
D1EB8	00 00 00 B6 81 00 00 00 00 30 31 37 2E 73 64 62 50 4B 05 06 00 00 00 00 01 00 01 00 35 0	¶017.sdb PK 5
F028B	00 00 00 B6 81 00 00 00 00 30 32 31 2E 73 64 62 50 4B 05 06 00 00 00 00 01 00 01 00 35 0	¶021.sdb PK 5
10FDD4	00 00 00 B6 81 00 00 00 00 30 32 32 2E 73 64 62 50 4B 05 06 00 00 00 01 00 01 00 35 0	¶022.sdb PK

PKZIP archive_2: 50 4B 05 06



PKZIP archive_3: 50 4B 07 08