

Dreamhack-Steg-Pack(level1)

[forensics]

Description

가짜 flag를 피해서 진짜 flag를 찾아라!@ (2025.01.01)

Write up

- 사용 도구: HxD
- `flag.png`
 - DH{fkae_flag}는 가짜 flag이므로 진짜 flag를 찾아야함

DH {fake_flag}

- HxD를 통해 `flag.png` 내부 분석
- PNG 파일 시그니처: `89 50 4E 47 0D 0A 1A 0A` (%PNG....)

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	PNG....IHDR
00000010	00	00	04	A3	00	00	01	EA	08	06	00	00	00	D8	95	8D	...........
00000020	12	00	00	00	01	73	52	47	42	00	AE	CE	1C	E9	00	00sRGB....
00000030	00	04	67	41	4D	41	00	00	B1	8F	0B	FC	61	05	00	00	..gAMA......a...
00000040	00	09	70	48	59	73	00	00	0E	C3	00	00	0E	C3	01	C7	..pHYs.......Ç
00000050	6F	A8	64	00	00	46	0B	49	44	41	54	78	5E	ED	DD	6B	o`d...F.IDATx^iYk
00000060	8C	55	D7	79	3F	E0	D8	0A	FE	83	65	2E	56	A0	6E	64	Uxy?à.fe.V nd

- PNG 파일에서 IEND 체크(이미지 트레일러)는 파일의 종료를 의미함

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00004630	A5	11	46	01	00	00	00	50	1A	61	14	00	00	00	00	A5	.F....P.a....
00004640	11	46	01	00	00	00	50	1A	61	14	00	00	00	00	A5	11	.F....P.a.....
00004650	46	01	00	00	00	50	1A	61	14	00	00	00	00	25	29	8A	F....P.a....)
00004660	FF	0F	BC	C9	B7	29	E0	B7	66	C5	00	00	00	00	49	45	y.)à-f....IE
00004670	4E	44	AE	42	60	82	70	61	73	73	3A	39	39	39	39	39	NDB`,pass:99999

- flag.png 내부에서 ZIP 파일 시그니처 발견
 - PK(50 4B 03 04)

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00004660	FF	0F	BC	C9	B7	29	E0	B7	66	C5	00	00	00	00	49	45	y.)à-f....IE
00004670	4E	44	AE	42	60	82	70	61	73	73	3A	39	39	39	39	39	NDB`,pass:99999
00004680	50	4B	03	04	14	00	00	00	00	00	CF	BE	21	5A	00	00	PK.....!Z..
00004690	00	00	00	00	00	00	00	00	00	00	09	00	00	00	41	70Ap
000046A0	70	20	44	61	74	61	2F	50	4B	03	04	14	00	00	00	00	p Data/PK.....
000046B0	00	27	B7	21	5A	00	00	00	00	00	00	00	00	00	00	00	..!Z.....
000046C0	00	11	00	00	00	41	70	70	6C	69	63	61	74	69	6F	6EApplication
000046D0	20	44	61	74	61	2F	50	4B	03	04	14	00	00	00	00	00	Data/PK.....
000046E0	C5	BA	21	5A	00	00	00	00	00	00	00	00	00	00	00	00	!Z.....

- flag.png에서 EOCD 를 제외한 나머지 부분 삭제 후 파일 시그니처를 기준으로 flag.zip 으로 저장
 - ZIP 파일 구조상 EOCD (End of Central Directory) 이후로는 불필요하므로, 나머지는 삭제하여 정상적인 ZIP 구조 유지

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00007180	2A	B7	1E	55	5C	DB	01	50	4B	01	02	14	00	14	00	00	*..U\Û.PK.....
00007190	00	00	00	C4	BE	21	5A	00	00	00	00	00	00	00	00	00	...Ä%!Z.....
000071A0	00	00	00	0B	00	24	00	00	00	00	00	00	00	10	00	00\$......
000071B0	00	FE	27	00	00	56	69	64	65	6F	2F	47	4E	53	33	2F	.p'..Video/GNS3/
000071C0	0A	00	20	00	00	00	00	00	01	00	18	00	76	5B	28	02v[(.
000071D0	5D	5C	DB	01	76	5B	28	02	5D	5C	DB	01	1A	F9	86	DE] \Û.v[(.) \Û..ù+P
000071E0	55	5C	DB	01	50	4B	05	06	00	00	00	00	09	00	09	00	U\Û.PK.....
000071F0	3D	03	00	00	27	28	00	00	00	00	50	2E	2E	2E	2E	40	=...'(.....P....@
00007200	2E	2E	2E	2E	24	24	2E	2E	2E	2E	39	39	2E	39	39	2E\$\$....99.99.
00007210	39	29															9)

- **flag.zip** 파일을 압축 해제한 결과, 여러 파일이 존재

App Data	2025-07-24 오후 3:13	파일 폴더
Application Data	2025-07-24 오후 3:13	파일 폴더
Download	2025-07-24 오후 3:13	파일 폴더
E-mail	2025-07-24 오후 3:13	파일 폴더
Music	2025-07-24 오후 3:13	파일 폴더
Pictures	2025-07-24 오후 3:13	파일 폴더
Video	2025-07-24 오후 3:13	파일 폴더

flag.zip 파일 내부

- Pictures 폴더 내부의 **flag.PNG** 파일 확인
 - 해당 flag가 진짜 flag임을 확인

Picture_in_flag?

- FLAG는, DH{Picture_iN_fl@g?}
-

FLAG

DH{Picture_iN_fl@g?}