



[linefeed] Write-Up

작성자	류나연
분석 일자	2024.05.17
작성 일자	2024.05.17
분석 대상	Linefeed.png
문서 버전	1
작성자 E-mail	01star01ek@gmail.com

0. 목차

1. 문제3

2. 분석 도구3

3. 환경3


4. Write-Up.....4

5. Flag.....7

6. 별도 첨부8

7. Reference9

1. 문제

URL	https://h4ckingga.me/challenges#LineFeed-17
문제 내용	Something is broken. 해당 사진에서 flag 값을 찾아서 입력하라.
문제 파일	<div>  </div> <div>linefeed.png</div>
문제 유형	멀티미디어 포렌식
난이도	1 / 5

2. 분석 도구

도구명	다운로드 링크	Version
HxD	https://mh-nexus.de/en/downloads.php?product=HxD20	2.5.0.0

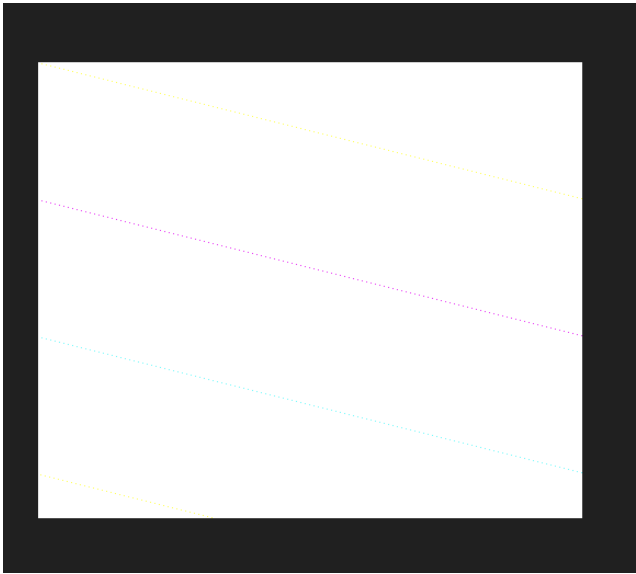
3. 환경

OS
Windows 11 Home

4. Write-Up

파일명	linefeed.png
용량	4.93KB
SHA256	4f6ce8af5debf85d842c8a6e917c804306bd010d15c7fc843bb415e061b7bf97
Timestamp	2024-05-17 05:27:29

1. 파일 확인



[사진 1] linefeed 파일을 열면 보이는 모습

해당 파일을 열어 확인해보니 해당 사진에는 여러가지 색깔의 점선이 있었다.

이를 통해 해당 선에 무언가 해답이 있지 않을까 하고 유추했다.

그러나 확신할 수 없는 생각이므로 일단 파일크기 확인을 통해 해당 파일 내 다른 유형의 파일이 숨겨져 있지는 않을까 확인했다. 그러나 파일 용량이 작기에 이가 불가능하다고 결론이 났다.

정밀한 확인을 위하여 hxd를 사용해보기로 했다.

2. Hxd를 통한 정밀 정보 확인

[WHS-2] .iso

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	01	F0	00	00	01	A0	08	02	00	00	00	44	B4	48	...8... ..D'H
00000020	DD	00	00	00	01	73	52	47	42	00	AE	CE	1C	E9	00	00	Y....sRGB.0i.e..
00000030	00	04	67	41	4D	41	00	00	B1	8F	0B	FC	61	05	00	00	..gAMA...t...ua...
00000040	00	09	70	48	59	73	00	00	0E	C3	00	00	0E	C3	01	C7	..pHYs...A...A.C
00000050	6F	A8	64	00	00	13	50	49	44	41	54	78	5E	ED	DD	51	o'd...PIDATx^iYQ
00000060	42	1B	B9	12	05	D0	B7	2E	16	C4	7A	58	4D	36	93	C5	B...D...AzXM6"A
00000070	CC	B3	8D	09	58	2A	A9	5B	36	9D	19	AE	CF	F9	0B	56	i...X*[6...0iù.V
00000080	57	4B	25	F5	25	01	4C	FE	F7	0F	00	71	84	3B	40	20	WK%0%.Lp÷...q;;@
00000090	E1	0E	10	48	B8	03	04	12	EE	00	81	84	3B	40	20	E1	á..H,...i...;@ á
000000A0	0E	10	48	B8	03	04	12	EE	00	81	84	3B	40	20	E1	0E	..H,...i...;@ á.
000000B0	10	48	B8	03	04	12	EE	00	81	84	3B	40	20	E1	0E	10	.H,...i...;@ á..
000000C0	48	B8	03	04	12	EE	00	81	84	3B	40	20	E1	0E	10	48	H,...i...;@ á..H
000000D0	B8	03	04	12	EE	00	81	84	3B	40	20	E1	0E	10	48	B8	,...i...;@ á..H,
000000E0	03	04	12	EE	00	81	84	3B	40	20	E1	0E	10	48	B8	03	...i...;@ á..H,

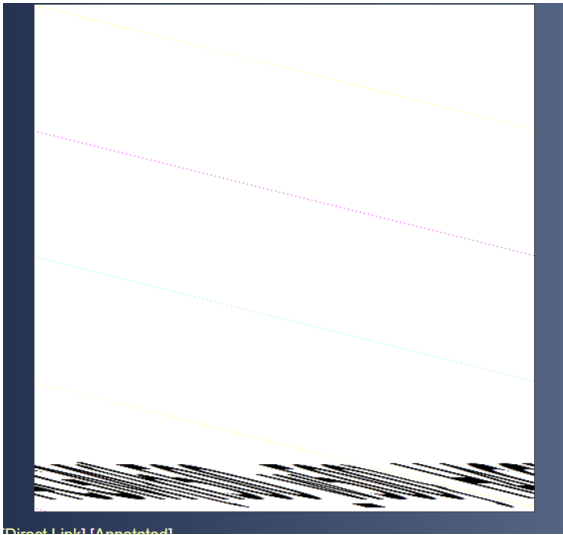
[사진 2] HxD를 통해 정밀 정보를 확인해본 모습

파일 시그니처의 경우 문제가 없었다.

특징으로는 특정 패턴의 문자열이 일정한 범위에 지속하여 기록되어 있다는 것이었다.

해당 부분이 다른 부분을 덮어쓴 것인가 싶어 이 점을 유의한 채로 더 얻을 수 있는 정보가 있을 까 싶어 찾아봤지만 특정한 증거가 없었다,

3. 사진 포렌식 툴 사이트로 추출



[사진 3] FotoForensics을 이용한 사진 내 특이값 추출

일단 포렌식 툴 사이트에 한번 둘러보고자 사진을 업로드하여 확인해보았다. Fonresically 사이트에 해당 사진을 올려봤으나 올라가지 않아 가능한 사이트들을 찾아 해맸다. 타 사이트의 2곳에도 사진을 올려봤으나 처리되지 않아 걱정하던 와중 fotoforensics 사이트에는 처리 가능하여 해당 사이트를 통해 처리했다. 이 과정에서 해당 사진내 hidden pixels가 있음을 알게 되었다.

위 사이트의 정확한 링크는 위와 같다. <https://fotoforensics.com/>

[WHS-2] .iso

이를 통해 숨겨진 메시지가 하단 부에 숨겨져 있음을 알게 되었고 이를 잘 보기 위해 사진 사이즈 조절 방안을 고려하게 되었다,

3. 사진 사이즈 조정

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	01	F0	00	00	01	A0	08	02	00	00	00	44	B4	48	...8... ..D'H

[사진 4] 원본 사진 청크

해당 메시지를 확인하기 위하여 IHDR 청크에서 width와 height 사이즈를 조절해보았다.

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00000000	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	
00000010	00	00	01	F4	00	00	01	FF	08	02	00	00	00	44	B4	48	

[사진 5] 최종적으로 조작한 사진 청크

원본 값 대비 width 와 height를 조금씩 값을 증가시켜 보면서 fotoforensics 사이트에서 flag 값이 잘 보일때까지 크기를 증가시켰다. 이때 width는 00000010부터 시작한 4바이트이며 그 다음 4바이트가 height의 크기이다.

4. flag 발견



[사진 6] 발견한 flag

여러 번의 시도 끝에 flag 값을 발견하였다.

5. Flag

H4CGM{h500_w500}

6. 별도 첨부

7. Reference

- [URL]