find_the_morse

- 분야: forensics
- 키워드: morse code, HxD, file signature

배경

해당 문제는 주어진 PNG 파일을 분석하여 숨겨진 파일을 찾고 모스 부호를 해석하여 플래그를 획득하는 것이 목표입니다. 해당 문제를 통해 파일 시그니처를 분석해보고 모스 부호에 대해 학습할 수 있습니다.

분석

문제 파일을 열면 MORES 와 MORSE 가 섞여있는 문자가 가득 적힌 png 파일을 확인할 수 있습니다. 문제의 제목을 확인해보면, MORSE를 찾아라로 해석되지만, 단순히 화면에서 MORSE 문자열을 찾는 것이 문제 풀이는 아닙니다.

HxD를 이용하여 파일의 헥스 값을 분석해보겠습니다.

關 파일(F) 편집(E) 찾기(S) 보기(V) 분석(A) 도구(T) 창 설정(W) 도움말(H)

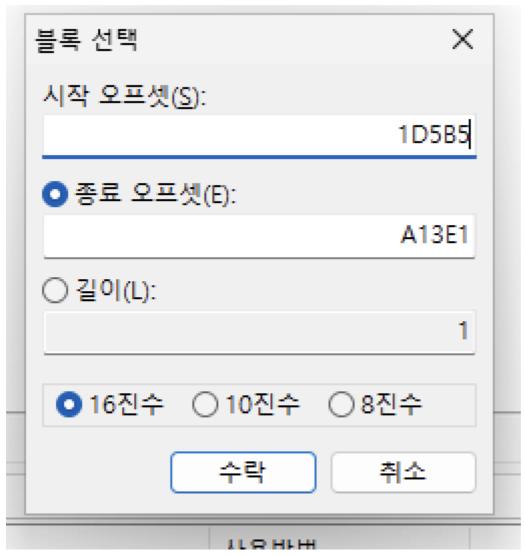
```
find_the_moorse.png
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Decoded text
00000000 B9 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52
                                                           %PNG.....IHDR
00000010
          00 00 04 C8 00 00 02 AA 08 06 00 00 00 CF 22 62
                                                           ...È...ª.....Ï"b
00000020 64 00 00 00 09 70 48 59 73 00 00 16 25 00 00 16
                                                           d....%....
00000030 25 01 49 52 24 F0 00 00 00 01 73 52 47 42 00 AE
                                                           %.IR$8....sRGB.®
00000040 CE 1C E9 00 00 00 04 67 41 4D 41 00 00 B1 8F 0B
                                                           Î.é....gAMA..±..
00000050 FC 61 05 00 01 D5 4A 49 44 41 54 78 01 EC 9D ED
                                                           üa...ÕJIDATx.ì.í
00000060 95 1D 35 B3 85 0F EF E2 3F 10 81 87 08 80 08 18
                                                           •.5³....ïâ?..‡.€..
00000070 22 00 22 00 22 00 47 00 44 60 88 00 88 00 13 01
                                                           ".".".G.D`^.^..
00000080 26 02 20 02 EC 08 CO 11 CC 3D 7B 2E 82 46 AE 92 &. .ì.À.Ì={.,F®'
00000090 AA 54 25 75 9F 39 FB 59 AB EF 7B F1 9C FE 92 4A
                                                           <sup>2</sup>T%uŸ9ûY≪ï{ñœþ′J
000000A0 BB A5 52 A9 F4 DA DD 99 13 21 84 10 42 08 21 84 ȴR©ôÚÝ™.!".B.!"
000000B0 10 42 08 21 57 CA FF 4E 84 10 42 08 21 84 10 42 .B.!WÊÿN".B.!".B
0000000C0 08 21 84 5C 31 74 90 11 42 08 21 84 10 42 08 21 .!"\lt..B.!".B.!
 00000000 04 00 30 00 00 00 40 00 01 04 10 40 00 01 04 10
  체크섬 검색 (0개의 검색 결과)
```

파일의 헥스값은 각 파일의 시작을 알려주는 헤더 시그니처가 존재합니다. png 파일은 푸터 시그니처 또한 존재합니다. png 파일의 헤더 시그니처인 89 50 4e 47 0d 0a 1a 0a를 확인할 수 있습니다.

```
LIRR RI OU OC IO IS OU SI OI IO IS OU SI OI OC
                                                          a pare.........
0001D590 35 74 90 11 42 08 21 84 10 42 08 21 84 90 AB E6
                                                          5t..B.!".B.!".«æ
0001D5A0
         7F DF 9A 60 05 B9 BD 65 F2 00 00 00 00 49 45 4E
                                                          .ßš`.¹⅓eò....IEN
         44 AE 42 60 82 52 49 46 46 20 3E 08 00 57 41 56
                                                          D®B`,RIFF >..WAV
0001D5B0
0001D5C0
         45 66 6D 74 20 10 00 00 00 01 00 01 00 2A 2B 00
                                                         Efmt ....*+.
0001D5D0 00 2A 2B 00 00 01 00 08 00 64 61 74 61 00 3E 08
                                                         .*+.....data.>.
0001D5E0 00 80 80 80 81 80 7F 7E 7C 7C 7D 7F 82 84 85 84
                                                          .€€€.€.~||}.,,....
0001D5F0 82 7E 7A 78 78 7A 7F 84 89 8A 88 84 7D 77 73 73
                                                          ,~zxxz.,%Š^,,}wss
```

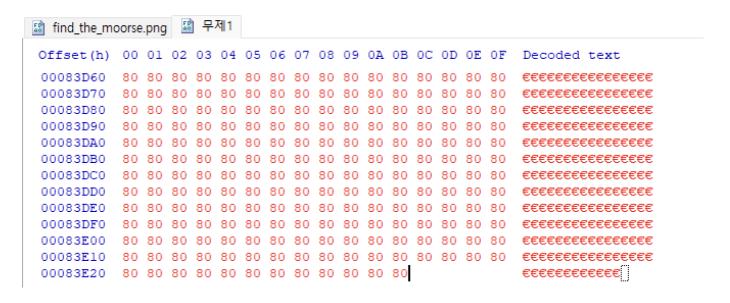
png 파일의 푸터 시그니처인 49 45 4e 44 ae 42 60 82를 검색해 보면, 위와 같은 결과를 확인할 수 있습니다. 파일의 푸터 시그니처로 파일이 끝나는 것이 아닌, 뒤에 다른 헥스 값이 존재합니다. 다른 파일을 숨겨 놓은 것을 확인하고, 파일의 확장자를 알기 위해 파일의 헤더 시그니처를 분석합니다. 다음 파일의 파일 시그니처는 52 46 49 49 로 WAV 파일의 파일시그니처입니다. 따라서 확장자를 wav 으로 가지는 파일이 숨겨져 있습니다.

풀이

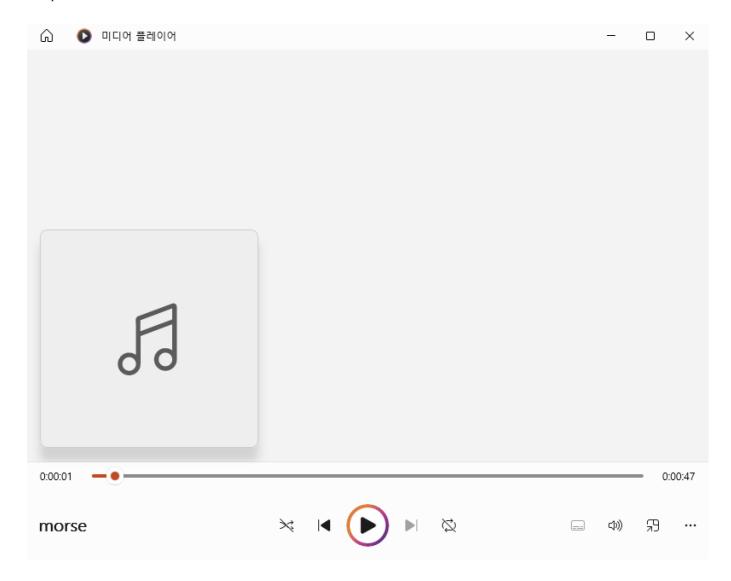


HxD의 블록선택 기능을 이용

하여 png파일의 푸터 시그니처 다음 오프셋부터 마지막 오프셋까지 선택 후 복사합니다.



새로운 파일을 하나 만들어 붙여넣기 해주고, 파일의 확장자를 ₃wav으로 하여 저장합니다.



저장 후 오디오 파일을 확인할 수 있습니다. 재생해보면 반복적인 기계음 소리를 들을 수 있습니다. 문제의 제목에서 morse code라는 힌트를 주었으므로, audio morse code decode 웹 사이트를 이용하여 해석해주겠습니다.

https://morsecode.world/international/decoder/audio-decoder-expert.html

The message is: WA5ITE4SYTOFINDMORSECOD3

파일을 업로드 후 디코드한 결과, 다음과 같은 문자열이 나왔습니다.

문제의 description을 확인해보면 플래그 형식은 ewha $\{[a-z0-9]*\}$ 이므로, 소문자로 바꾸어주고 ewha로 감싸주면 문제의 플레그를 얻을 수 있습니다.

플래그: ewha{wa5ite4syt0findmorsecod3}

레퍼런스

- http://forensic-proof.com/archives/300
- https://morsecode.world/international/decoder/audio-decoder-expert.html