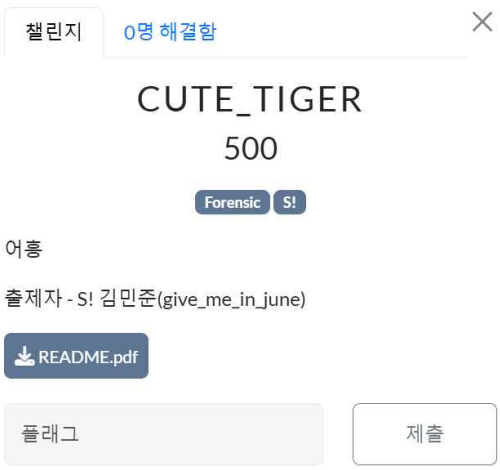
# CUTE_TIGER

32기 안현진

포렌식 문제 CUTE_TIGER을 풀어보기로 했다.




문제 파일을 다운받으면, jpg형식의 이미지 파일이 나온다. 이외에 다른 힌트는 없어보이니, 이제 이미지 파일을 분석하자.

1. 헤더/푸터 시그니처 확인하기

문제가 쉽다고 하셔서, 시그니처를 살펴봤다. jpg파일의 헤더 시그니처는 FF D8이고, 푸터 시그니처는 FF D9이다. 확인해보니 시그니처에는 문제가 없다. 시그니처 뒤에 숨겨진 데이터도 없고.

```
00000000  FF D8
00006260  00 14 51 45 00 7F FF D9
```

2. File Carving - with foremost

파일 카빙을 진행했지만, 유의미한 정보는 얻지 못했다. 파일 카빙도 아니고 스테가노그래피도 아닌것 같은데..대체 뭘까

3. jpg파일 구조 확인하기

혹시 텍스트 문자열에 flag관련 힌트가 있을까싶어, flag를 검색해봤지만 없었다. 그리고 플래

그 형식이 3S라서 이것도 검색했는데, 이건 검색이 되긴한다. 근데 유의미한 정보같지는 않다. 이 외에는 텍스트 문자열에서 걸리는것이 없다. 파일 구조에도 이상한점은 없는 것 같다.

4. Steghide , binwalk ,exiftool 사용

```
┌──(kali㉿kali)-[~/Downloads]
└─$ steghide extract -sf image.jpg
Enter passphrase:
steghide: could not extract any data with that passphrase!
```

이미지에 있는 데이터를 추출해내는 툴인 Steghide를 사용했지만 소득은 없었다. Steghide와 비슷한 zsteg도 사용해보았지만, 이 툴은 jpg 파일은 지원하지 않았다(png, bmp 지원)

```
┌──(kali㉿kali)-[~]
└─$ cd Downloads

┌──(kali㉿kali)-[~/Downloads]
└─$ sudo binwalk image.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, JFIF standard 1.01
```

```
┌──(kali㉿kali)-[~/Downloads]
└─$ exiftool image.jpg
ExifTool Version Number         : 12.76
File Name                       : image.jpg
Directory                       : .
File Size                       : 25 kB
File Modification Date/Time     : 2024:07:27 05:01:48-04:00
File Access Date/Time           : 2024:08:04 22:40:25-04:00
File Inode Change Date/Time     : 2024:07:27 05:01:48-04:00
File Permissions                : -rw-r--r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Resolution Unit                 : None
X Resolution                    : 1
Y Resolution                    : 1
Image Width                     : 507
Image Height                    : 589
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Image Size                      : 507×589
Megapixels                      : 0.299
```

파일 시그니처를 사용해 어떤 데이터가 들어있는지 확인하는 binwalk 툴을 이용했다. 명령어 **#sudo binwalk image.jpg** 사용해 이미지를 분석한 결과 image.jpg 파일이 JPEG 이미지 데이터 형식이라는 것을 다시 한번 확인했고 이외의 소득은 없었다.

더 정보가 있을까 싶어 메타데이터를 확인하는 명령어 **#exiftool image.jpg** 을 사용해 데이터를 추출했지만 flag와 관련된 정보는 없는 것 같았다. 음.. 해볼건 다 해본 것 같은데 진짜 어

떻게 풀어야하는지 모르겠다.

-steghide: 다양한 이미지 파일과 오디오 파일에 데이터를 숨길 수 있게 해주는 스테가노그래피 프로그램
-binwalk: 숨겨진 파일 또는 실행 가능한 파일을 탐색하기 위해 이진수 이미지를 탐색하는 도구
-exiftool: PC에 저장된 모든 사진의 메타데이터를 확인하고 편집할 수 있는 도구

감이 잡히지 않아 출제자분께 연락드렸는데 steghide를 사용한 스테가노그래피 문제라고 한다. 위에서 steghide를 사용했었는데 이 과정에서 뭔가 놓친게 있나보다. 그래서 다시 한번 steghide를 사용해보기로 했다.

5. steghide tool 사용


위에서 steghide를 사용했을 때 출력된 문장이다. ‘could not extract any data with that passphrase!’라는 문장을 ‘출력된 데이터가 없다’라고 대충 해석한게 문제였다. 진짜 의미는 ‘입력한 암호로 데이터를 추출할 수 없다’이다...

이제 문제점을 알게 되었으니 다시 문제를 풀이해보자. passphrase를 찾는게 이번 문제의 핵심인 것 같다.

flag, 보호, protection, 정보호 등등 이미지와 관련된 문자열을 넣어봤지만 맞는 것이 없었다. 그래서 HxD에 힌트가 더 있을지 찾아보고, binwalk로 데이터도 추출했지만 소득은 없었다.

<참고자료>
[Forensics] 포렌식 관점에서 JPEG.. : 네이버블로그 (naver.com)
Giardino Segreto (tistory.com)
암알못의 암호핥기 – 스테가노그래피 – Hackerz on the Ship (wordpress.com)