

[Snowing!] Write-Up

작성자	김경민
분석 일자	2024.05.02
작성 일자	2024.05.11
분석 대상	snow.JPEG, flag.txt
문서 버전	3.0
작성자 E-mail	rlarudals877@gmail.com

0. 목차

1. 문제3

2. 분석 도구3

3. 환경3


4. Write-Up.....4

5. Flag.....6

6. 별도 첨부7

7. Reference8

1. 문제

URL	https://dreamhack.io/wargame/challenges/241
문제 내용	<div> <div>드림이: 우와! 밖에 눈이 많이와요!</div> <div>드림맘: 그렇네~~</div> <div>드림이: 거의 모두 하얀공간뿐이네요.</div> </div>
문제 파일	<div>  <div>9603a472-1bde-401f-a6fb-7d5acd71e93f.zip</div> </div>
문제 유형	멀티미디어 포렌식
난이도	1 / 3

2. 분석 도구

도구명	다운로드 링크	Version
SNOW.EXE	https://darkside.com.au/snow/index.html	1.6

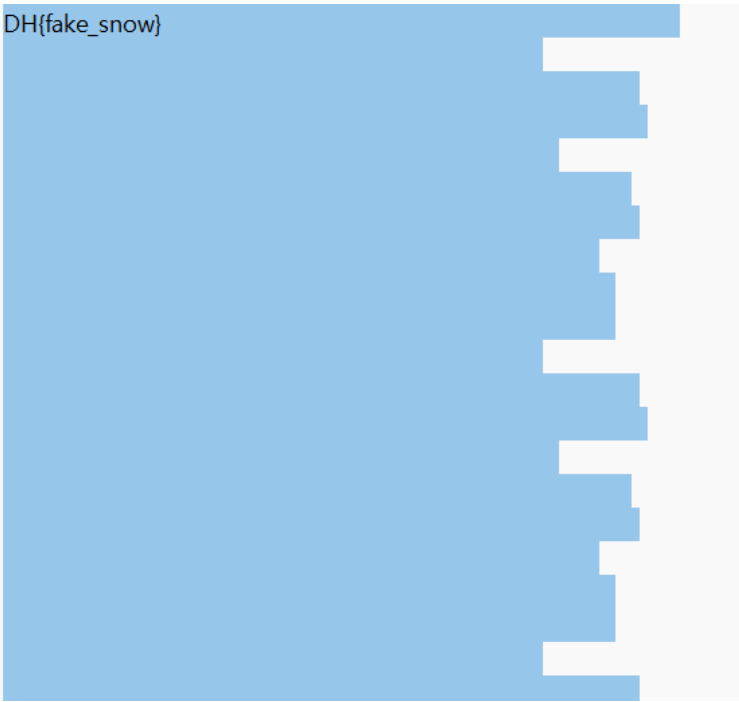
3. 환경

OS
Window 11 64-bit

4. Write-Up

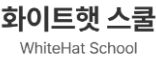
파일명	DH
용량	274KB
SHA256	9E72C0F4B4AF3743137ED74803B1BFC18321E879CBEB912FD9BC02DE613F8875
Timestamp	2024-05-02 13:01:20

1. 문제 파일을 다운로드 하면 눈사람이 있는 사진과 flag 라는 이름의 txt 파일이 주어진다. 먼저 이미지 파일을 보고 스테가노그래피 관련 문제라는 것을 깨닫고 HxD.it 사이트를 이용해 분석을 했지만 이미지에서 Flag 를 얻을 수 없었다.
2. 그 다음에는 메모장을 열어봐서 분석을 해보았는데 DH(fake_snow)란 문자가 보이고 주어진 문자열 끝에서부터 공백이 엄청 많이 있는 것을 알 수 있었다.



[사진 1] 빈공간이 많은 txt 파일

3. 따라서 이 txt 파일을 자세히 분석하고 싶어서 HxD.it을 열어서 다운로드 한 이미지를 분석했고 실제로 공백 부분이 많이 보였다.



화이트햇 스쿨
WhiteHat School

[사진 2] 공백이 많은 이미지 파일

5. 공백 문자 스테가노그래피란 것을 알았으니 Snow.exe 툴을 사용해 숨긴 문자를 확인해 보았다. 그리고 터미널을 이용해서 실행해 주었더니 flag가 나왔다.

[사진 3] SNOW.EXE을 통한 flag 찾기

5. Flag

DH{w0w_1t_Sn0w5}



6. 별도 첨부

7. Reference

- [URL]