




[Basic_Forensics_1] Write-Up

작성자	심주완
분석 일자	2024.5.8
작성 일자	2024.5.8
분석 대상	이미지 파일
문서 버전	4
작성자 E-mail	rd002@naver.com

0. 목차

- 1. 문제 3
- 2. 분석 도구 3
- 3. 환경 3
- 4. Write-Up..... 4
- 5. Flag 5
- 6. 별도 첨부 6
- 7. Reference 7

1. 문제

URL	https://dreamhack.io/wargame/challenges/518	
문제 내용	<p>이미지 파일안에 Hidden 메시지가 숨어있다.</p> <p>keyword : W4!teBear</p> <p>flag : DH{flag}</p>	
문제 파일		
문제 유형	multimedia forensics	
난이도	1 / 3	

2. 분석 도구

도구명	다운로드 링크	Version
Steganography Online	https://stylesuxx.github.io/steganography/	

3. 환경

OS
MAC



[WHS-2] .iso

4. Write-Up

파일명	whitebear.png
용량	136KB
SHA256	509cdc75c2995f4dd234ff03be42523c26b8d464b90ff77a6789b7a24f7b4d76
Timestamp	2022-07-11 17:09:00

Steganography Online

Encode


Decode

Decode image

To decode a hidden message from an image, just choose an image and hit the **Decode** button.

Neither the image nor the message that has been hidden will be at any moment transmitted over the web, all the magic happens within your browser.

파일 선택

 whitebear.png

Decode

[그림 1] Steganography Online에서 Decodeing 진행

문제가 이미지 파일에서 Hidden 메시지를 찾으라고 나와있어서 스테가노그래피라는 생각이 바로 들었고, HxD를 사용하지도 않고 바로 스테가노그래피 분석 사이트로 향하여 디코딩을 진행하였다.

Hidden message

DH(White_Be4r_In_Dream_4ack)W4lteBeardøyyyyyyøyyyyyyøyyyyyyøyyyyyyøyyyyyyøyyyyyyøyyyyyyøyyyyyyøyyyyyyøyyyyyyø
 yyyyyyøyyyyyyøyyyyyyøyyyyyyøyyyyyyøyyyyyyøyyyyyyøyyyyyyøyyyyyyøyyyyyyø

[그림 2] Hidden message

디코딩을 진행하니 다음과 같이 플래그를 구할 수 있었다.

5. Flag

DH{Wh!te_Be4r_In_Dream_4ack}

6. 별도 첨부

7. Reference

- [URL]