



작성자	류나연
분석 일자	2024.05.17
작성 일자	2024.05.17
분석 대상	easy.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.....6

6. 별도 첨부7

7. Reference8

1. 문제

URL	https://h4ckingga.me/challenges#Easy-11
문제 내용	easy.png 파일에서 flag를 획득하여 입력하자.
문제 파일	 easy.png
문제 유형	멀티미디어 포렌식
난이도	1 / 5

2. 분석 도구

도구명	다운로드 링크	Version

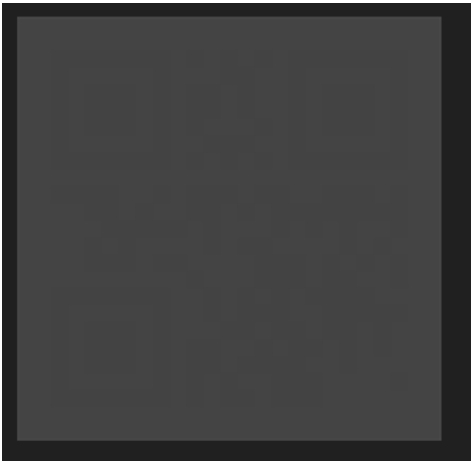
3. 환경

OS
Windows 11 HOME

4. Write-Up

파일명	easy.png	
용량	6.48KB	
SHA256	72d2a233960ff8be657b237faeb2ac36dff1f95983feb408fa81e18826687a0f	
Timestamp	2024-05-16	04:52:00

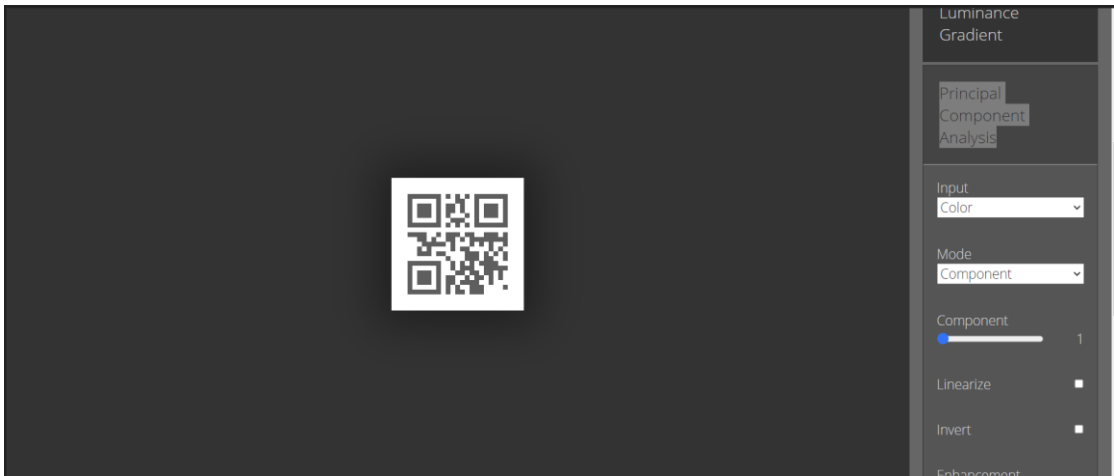
1) 사진 파일 확인



[사진 1] easy.png을 열면 나타나는 사진

해당 사진 파일을 열어보면 어두운 사진 뒤로 바코드 모양이 보임을 알 수 있다. 이에 따라 특정 색깔만 추출하게 하면 되지 않을까 생각할 수 있다.

2) 사진 포렌식 툴 사이트를 이용해 추출

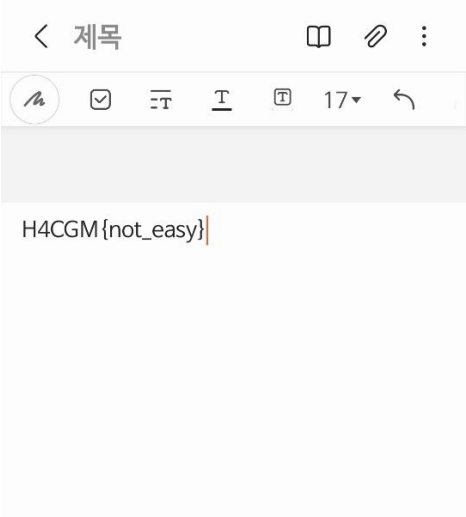


[사진 2] forensically 사이트를 이용하여 추출한 모습

[WHS-2] .iso

해당 사진을 사진 포렌식 사이트인 forensically <https://29a.ch/photo-forensics/#pca> 에서 PCA 기법으로 추출해보았다. 이에 따라 바코드를 발견할 수 있었다. (*PCA 기법은 고차원의 데이터를 저차원의 데이터로 환원시키는 기법을 말한다.)

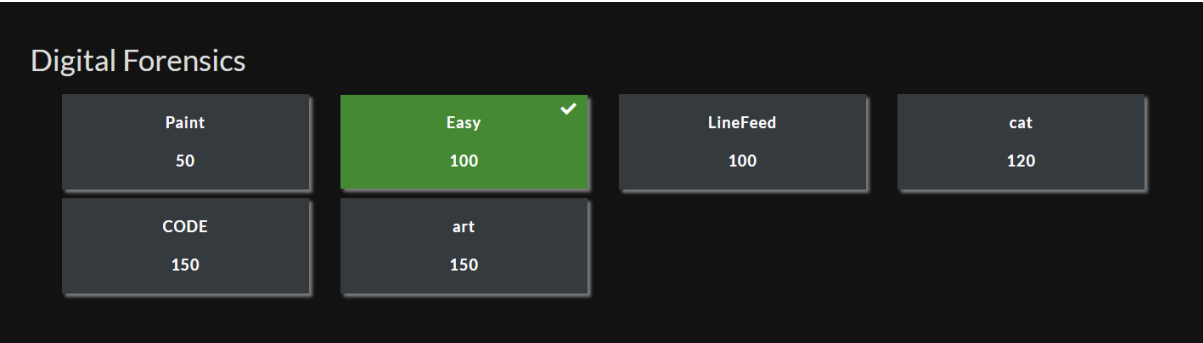
3) 바코드 접속을 통한 flag 발견



[사진 3] 발견된 flag의 모습

위의 바코드를 휴대폰을 통해 접속하였더니 새로운 텍스트 파일이 열렸다.
해당 파일 내에는 flag값이 적혀 있었다.

4) flag 입력으로 문제 해결 완료



[사진 4] 답인 flag 값을 입력하여 변경된 Hacking Game 사이트의 모습

이를 그대로 입력하니 정답으로 인정되었다.

5. Flag

H4CGM {not_easy}

6. 별도 첨부

7. Reference

- [URL]