




## [video\_in\_video] Write-Up

작성자	김경민
분석 일자	2024.05.09
작성 일자	2024.05.11
분석 대상	jpg 파일, mp4 파일
문서 버전	2.0
작성자 E-mail	<a href="mailto:rlarudals877@gmail.com">rlarudals877@gmail.com</a>

# 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	<a href="https://dreamhack.io/wargame/challenges/647">https://dreamhack.io/wargame/challenges/647</a>
문제 내용	한가위 비디오를 찾아주세요.....
문제 파일	 video_in_video.jpg
문제 유형	멀티미디어 포렌식
난이도	3 / 5

### 2. 분석 도구

도구명	다운로드 링크	Versi on
DAE_MMF_Parser	<a href="http://cbuilder.borlandforum.com/impboard/impboard.dll?action=read&amp;db=bcb_res&amp;no=681">http://cbuilder.borlandforum.com/impboard/impboard.dll?action=read&amp;db=bcb_res&amp;no=681</a>	0.7.0

### 3. 환경

OS
Window 11 64-bit

## 4. Write-Up

파일명	video_in_video
용량	2766KB
SHA256	7F503457E3D10D5D7D3B2207E544288EAC35B1B08CD5A62EBEE36373C8B4CABE
Timestamp	2024-05-09 10:02:11

1. 일단 파일을 받아보니. jpg 파일이 있었다. 이를 분석하기 위해 hex를 지원하는 웹사이트에서 분석을 진행했다. 위의 이미지 파일의 헤더랑 푸터를 살펴본 결과, 헤더는 FF D8 FF E0 로 잘 있었지만 푸터에서 문제가 있었다. 바로 푸터 시그니처 FF D9 뒤에 무엇인가 더 있었던 것이다.

DD 9D C0 73 9C 78 03 90	8D 38 2E E1 69
75 36 DC 3F 32 A7 A8 1F	FF D9 00 00 00
79 70 69 73 6F 6D 00 00	02 00 69 73 6F
6F 32 61 76 63 31 6D 70	34 31 00 00 19
6F 76 00 00 00 6C 6D 76	68 64 00 00 00

[사진 1] 푸터 뒤에 뭔가 더 있는 상황

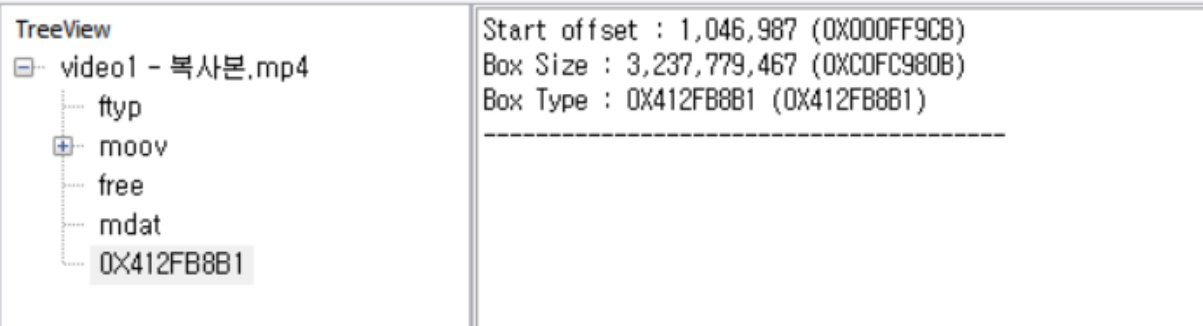
2. 자세히 보니 mp4 의 파일 시그니처가 보였다. -> 66 74 79 70 69 73 6F 6D 따라서 이 부분부터 따로 추출해 확장자를. mp4 로 하고 파일을 열어보았다.



[사진 2] 추출한 mp4

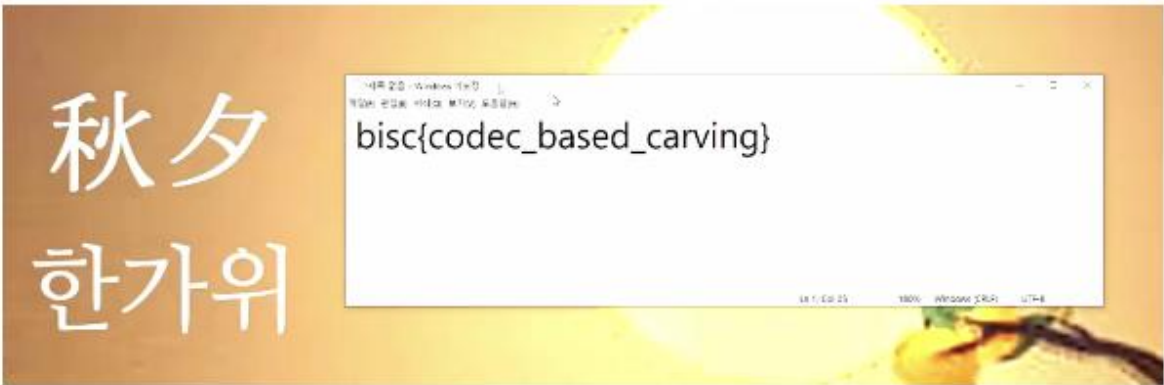
[WHS-2] .iso

3. 그러나 flag 가 나타나지 않아 DAE\_MMV\_Parser 을 통해 영상을 좀 더 분석해 보았다. 분석한 결과, mdat 뒤에 알 수 없는 타입의 박스가 존재한다는 것을 깨달았다. mdat 는 실제 미디어를 저장하는 박스이다.



[사진 3] mp4 분석 결과

4. 따라서 mdat 뒤에 있는 것들을 추출하여 다시 mp4 로 만들어 주고 동영상 재생을 하면 플래그가 나온다.



[사진 4] 재추출한 mp4

5. Flag

BISC{codec\_based\_carving}

## 6. 별도 첨부

## 7. Reference

- [URL]