




|            |                     |
|------------|---------------------|
| 작성자        | 박혜미                 |
| 분석 일자      | 2024.05.10          |
| 작성 일자      | 2024.05.10          |
| 분석 대상      | Image.E01           |
| 문서 버전      | 2                   |
| 작성자 E-mail | parkm0708@naver.com |

# 0. 목차

- 1. 문제 .....3
- 2. 분석 도구 .....3
- 3. 환경 .....3
- 4. Write-Up.....4
- 5. Flag.....6
- 6. 별도 첨부 .....7
- 7. Reference .....8

1. 문제

|          |   |
|----------|---|
| URL      | <a href="https://dreamhack.io/wargame/challenges/727">https://dreamhack.io/wargame/challenges/727</a>                     |
| 문제<br>내용 | Someone deleted the PDF file which has flag!<br><br>How can I recover it?   |
| 문제<br>파일 | <br>41ce9cc5-62c6-46<br>07-997a-cb02c2c6 |
| 문제<br>유형 | 디스크 포렌식   |
| 난이도      | 1 / 5   |

2. 분석 도구

| 도구명        | 다운로드 링크   | Version |
|------------|---|---------|
| FTK Imager | <a href="https://www.exterro.com/digital-forensics-software/ftk-imager">https://www.exterro.com/digital-forensics-software/ftk-imager</a> | 4.7.1.2 |
| HxD        | <a href="https://mh-nexus.de/en/hxd/">https://mh-nexus.de/en/hxd/</a>   | 2.5     |

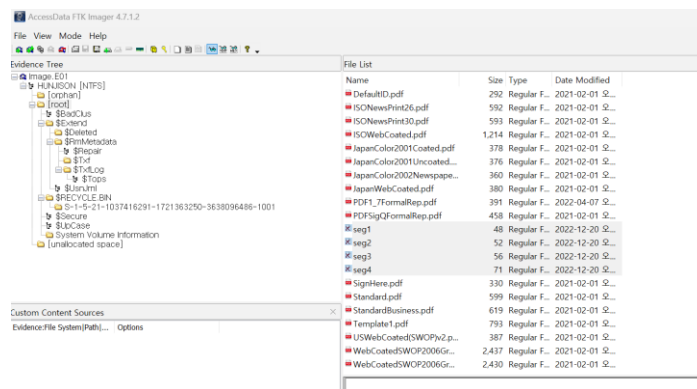
3. 환경

| OS              |
|-----------------|
| Windows 11 Home |

## 4. Write-Up

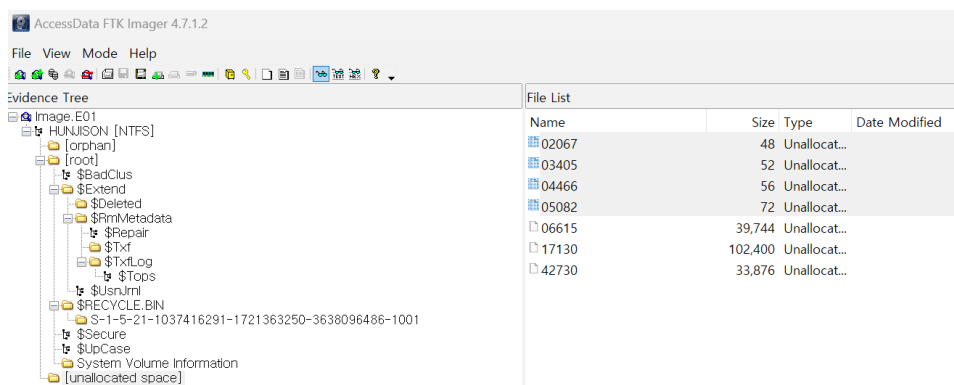
|           |   |
|-----------|---|
| 파일명       | Image.E01   |
| 용량        | 18.7MB  |
| SHA256    | 36c6d523ed44e2be02dbfbb2369154125ebc6775952c947dff9e89efbc105ca |
| Timestamp | 2022.12.21 06:45:32   |

문제 설명을 보니 PDF 파일을 복구하는 문제인 것 같다.



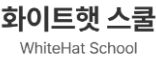
### [그림 1] FTK Imager로 문제 파일 확인

PDF 파일 복구를 위해 FTK Imager 를 사용하여 확인해 보니 삭제된 PDF 파일이 존재하지 않았다. 삭제된 [seg1~4] 파일을 추출해 보았으나 해당 파일은 완전히 비어 있었다.



**[그림 2] unallocated space**

문제 파일에 [unallocated space] 디렉토리를 확인할 수 있다. 해당 디렉토리를 확인해 보니 [seg1~4]와 똑같은 용량의 파일을 확인할 수 있다.



**화이트햇 스쿨**  
WhiteHat School

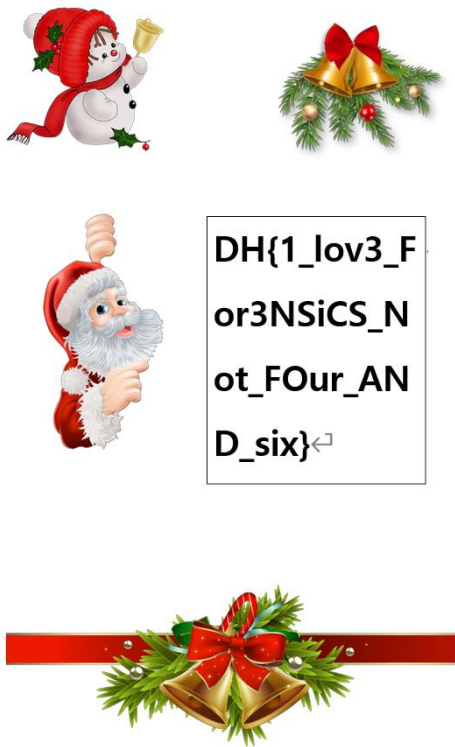
| Name  | Size    | Type         | Date Modified |
|-------|---------|--------------|---------------|
| 02067 | 48      | Unallocat... |               |
| 03405 | 52      | Unallocat... |               |
| 04466 | 56      | Unallocat... |               |
| 05082 | 72      | Unallocat... |               |
| 06615 | 39,744  | Unallocat... |               |
| 17130 | 102,400 | Unallocat... |               |
| 42730 | 33,876  | Unallocat... |               |

### [그림 3] PDF의 헤더 시그니처

[seg1]으로 추정되는 [02067] 파일의 HeX 값을 확인해보니 PDF의 헤더 시그니처를 확인할 수 있다. 보아하니 [seg1~4] 파일의 HeX 값을 서로 연결하면 PDF 파일이 나올 것 같다.

[seg1~4]를 연결하기 위하여 우선 [그림 3]의 파일 4 개를 Export 한다. HxD 를 사용하여 4 개의 Hex 값을 순서대로 붙여 넣어 [seg.pdf]이라는 파일명으로 저장한다.

# 5. Flag



[그림 4] flag 획득

[seg.pdf] 파일을 열어보니 **DH{1\_lov3\_For3NSiCS\_Not\_FOur\_AND\_six}**라는 flag 값을 얻을 수 있다.

## 6. 별도 첨부

## 7. Reference

- [URL]