



작성자	심주완
분석 일자	2024.05.15
작성 일자	2024.05.15
분석 대상	File_deleted.7z
문서 버전	1.0
작성자 E-mail	<a href="mailto:rd002@naver.com">rd002@naver.com</a>

0. 목차

1. 문제 ..... 3

2. 분석 도구 ..... 3

3. 환경 ..... 3


4. Write-Up..... 4

5. Flag ..... 9

6. 별도 첨부 .....10

7. Reference .....11

### 1. 문제

URL	<a href="http://xcz.kr/START/prob/prob36.php">http://xcz.kr/START/prob/prob36.php</a>
문제 내용	<p>피시방에서 아동 청소년 보호법에 위배되는 파일을 소지한 기록을 발견했다.</p> <p>아래의 형식에 맞춰 증거를 수집해라.</p> <p>시간은 GMT+9 입니다. lowercase(md5(원본_경로_만들어진_시간_마지막_실행_된_시간_쓰인_시간_볼륨_시리얼))</p> <p>ex)lowercase(md5(C:\₩CZ₩key.txt_20121021160000_20131022000000_20131022000000_AAAA-BBBB))</p>
문제 파일	 file_deleted.7z
문제 유형	Dics Forensics
난이도	2 / 5

### 2. 분석 도구

도구명	다운로드 링크	Version
010 Editor	<a href="https://www.sweetscape.com/download/010editor/">https://www.sweetscape.com/download/010editor/</a>	14.0.1
알집	<a href="https://altools.co.kr/product/ALZIP">https://altools.co.kr/product/ALZIP</a>	12.24

### 3. 환경

OS
Window 11 Home

## 4. Write-Up

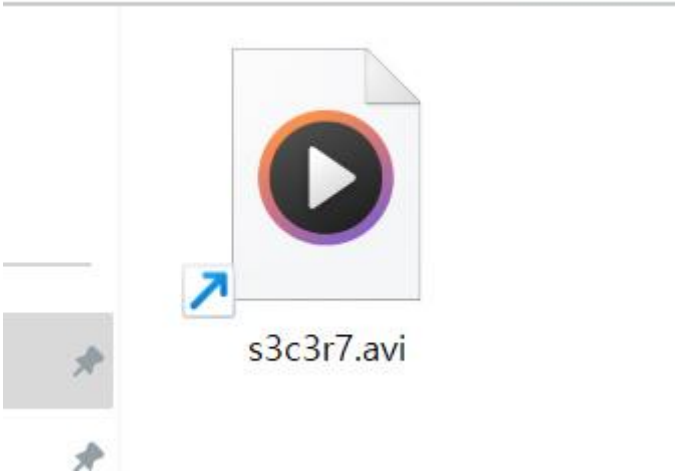
파일명	File_deleted.7z
용량	1,019,370 byte
SHA256	224B94EBFA2D1D6D7560BCCB17998C4498D92F409F3B8A760DE2DBC94625CE3D
Timestamp	2013/10/16 13:52:10

이번 문제 파일은 알집으로 열리는 파일이었다. 그렇기 때문에 ftk imager 를 쓰기 전에 직접 압축을 풀고 파일을 돌려보았다.

이름	수정한 날짜	유형	크기
AppData	2024-05-15 오후 4:57	파일 폴더	
Application Data	2024-05-15 오후 4:57	파일 폴더	
Contacts	2024-05-15 오후 4:57	파일 폴더	
Cookies	2024-05-15 오후 4:57	파일 폴더	
Desktop	2024-05-15 오후 4:57	파일 폴더	
Documents	2024-05-15 오후 4:57	파일 폴더	
Downloads	2024-05-15 오후 4:57	파일 폴더	
Favorites	2024-05-15 오후 4:57	파일 폴더	
Links	2024-05-15 오후 4:57	파일 폴더	
Local Settings	2024-05-15 오후 4:57	파일 폴더	
Music	2024-05-15 오후 4:57	파일 폴더	
My Documents	2024-05-15 오후 4:57	파일 폴더	
NetHood	2024-05-15 오후 4:57	파일 폴더	
Pictures	2024-05-15 오후 4:57	파일 폴더	
PrintHood	2024-05-15 오후 4:57	파일 폴더	
Recent	2024-05-15 오후 4:57	파일 폴더	
Saved Games	2024-05-15 오후 4:57	파일 폴더	
Searches	2024-05-15 오후 4:57	파일 폴더	
SendTo	2024-05-15 오후 4:57	파일 폴더	
Templates	2024-05-15 오후 4:57	파일 폴더	
Videos	2024-05-15 오후 4:57	파일 폴더	
시작 메뉴	2024-05-15 오후 4:57	파일 폴더	

[Figure 1] 문제 파일 내부

하나하나 파일을 다 찾아보았다. 대부분의 파일 안에 삽질을 할만한 파일이 거의 없었기 때문에 Recent 파일 안에서 문제에서 필요한 파일을 찾아볼 수 있었다.



[Figure 2] 의심되는 파일

다음과 같은 파일을 확인할 수 있었는데, 열리지는 않았다. 속성을 통해 조금 더 알아보기로 했다.

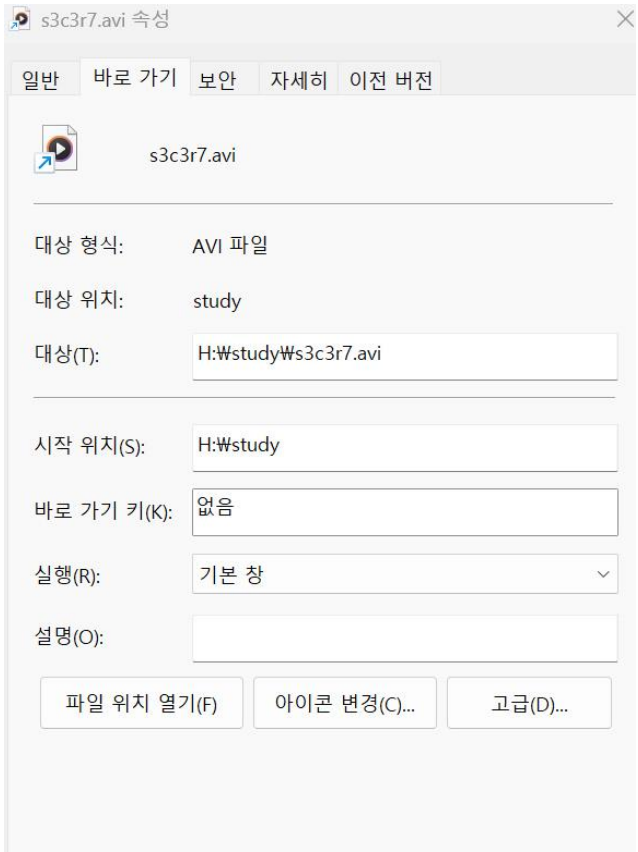
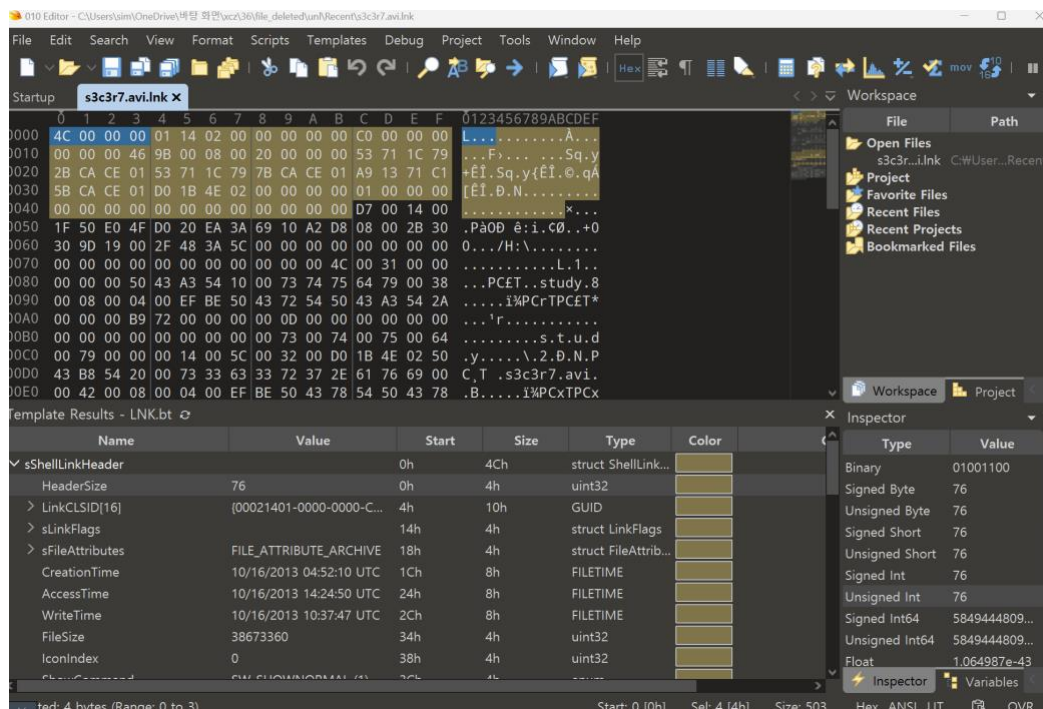


Figure 3 s3c3r7.avi 파일 속성

경로가 study 폴더 안에 있는 파일이라... 이게 문제의 파일이라는 것을 바로 알았다. 하지만 파일이 망가져서 속성으로는 문제에서 요구하는 플래그 포맷을 뽑아낼 수 없었다. 헤더로 플래그를 뽑아야 한다고 생각해서 HxD를 사용해야하나 싶었는데 어느 값이 어디에 저장되어있는지 아는 것이 너무 어려워서 막막했다. 헤더를 분석해주는 프로그램이 있을까 싶어 검색해봤는데 010

## [WHS-2] .iso

Editor이라는 프로그램이 존재하여 이 프로그램을 통하여 분석하였다.



[Figure 4] 010Editor로 연 avi 파일

분석기에서 파일을 열면 다음과 같이 나왔다. 헤더를 분석한 값들을 다음과 같이 어느 칸에 어느 값이 해당되는지 너무 잘 나와있다. 다음에도 애용할 것 같다. 그렇다면 플래그에서 요구하는 값들을 뽑아오자.

CreationTime	10/16/2013 04:52:10 UTC	1Ch	8h	FILETIME	
AccessTime	10/16/2013 14:24:50 UTC	24h	8h	FILETIME	
WriteTime	10/16/2013 10:37:47 UTC	2Ch	8h	FILETIME	

[Figure 5] 위에서 아래로 각각 만들어진 시간, 마지막 실행 된 시간, 쓰인 시간

만들어진 시간, 마지막 실행 된 시간, 쓰인 시간은 다음과 같다. **하지만 문제에서 요구하는건 GMT+9 이기 때문에 각 시간에 +9 를 한다.**

만들어진 시간 : 2013/10/16 04:52:10 +9 -> 2013/10/16 13:52:10

마지막 실행 시간 : 2013/10/16 14:24:50 +9 -> 2013/10/16 23:24:50

쓰인 시간 : 2013/10/16 10:37:47 +9 -> 2013/10/16 19:37:47

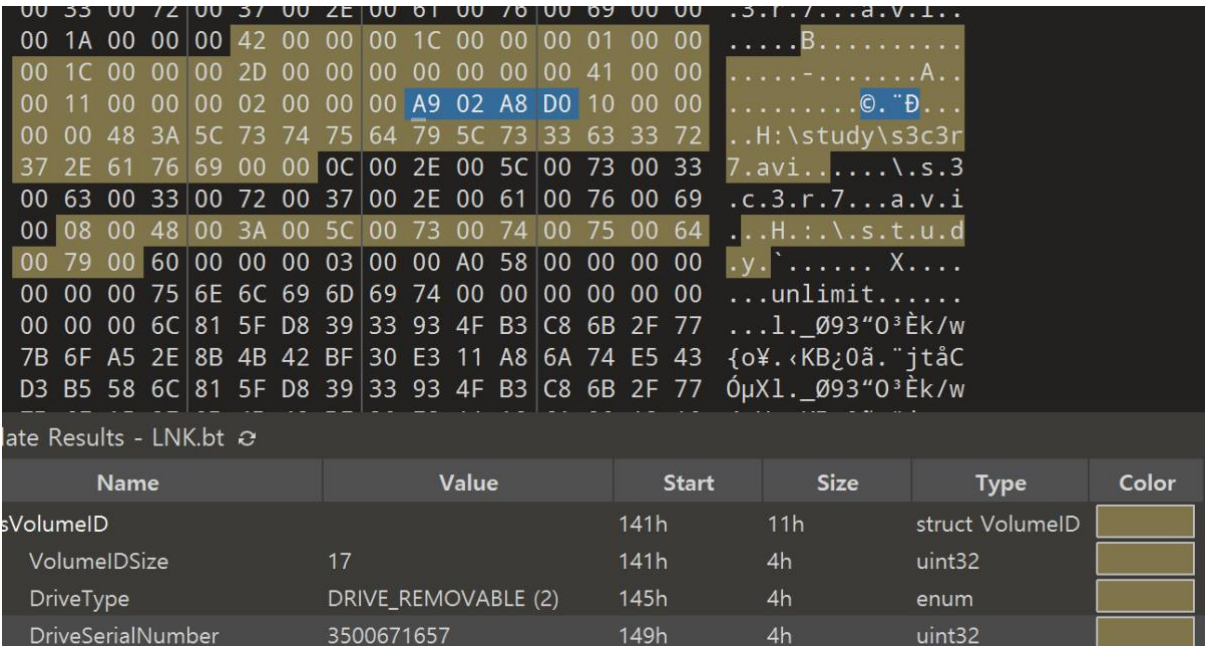
원본 경로는 이미 속성을 통하여 구했지만 헤더값에서도 발견할 수 있었다.

> Data[1]		151h	1h	string	
> LocalBasePath[20]	H:\study\ws3c3r7.avi	152h	14h	string	
✓ CommonPathSuffix[1]		166h	1h	string	

[Figure 6] 010 Editor를 통하여 확인한 경로

[WHS-2] .iso

마지막으로 시리얼 넘버만 남았다. 분석기에서 확인할 수 있었지만 이 부분이 시간을 잡아먹었다.



[Figure 7] 데이터 시리얼 넘버

처음에는 아래에서 확인할 수 있는 3500671657인줄 알고 이를 대입했는데 오답으로 나왔다. 위에 16진수 값인 A902-A8D0으로도 대입을 해봤는데 역시나 오답. 구글링을 통하여 시리얼 넘버는 리틀 엔디언 방식으로 읽는다는 것을 알게 되었다. 그렇기 때문에 시리얼 넘버는 D0A8-02A9가 된다.

이를 모두 적용시키면

lowercase(md5(H:\study\ws3c3r7.avi\_20131016135210\_20131016232450\_20131016193747\_D0A8-02A9))

가 된다. Md5 변환기로 변환을 시키면 플래그 값은

[WHS-2] .iso

Use this generator to create an MD5 hash of a string:

H:\study\ls3c3r7.avi\_20131016135210\_20131016232450\_20131016193747\_D0A8-02A9

Generate →

Your String	H:\study\ls3c3r7.avi_20131016135210_20131016232450_20131016193747_D0A8-02A9	
MD5 Hash	66f67cd42c58763fd8d58eed6b5bfdba	Copy
SHA1 Hash	0a2208f43e00ae475b96a8fbebdd2aac73493f51	Copy

[Figure 8] flag

이다. 사용한 MD5변환 툴은 레퍼런스로 남겨두겠다.



# 5. Flag

66f67cd42c58763fd8d58eed6b5bfdba

## 6. 별도 첨부

## 7. Reference

- <https://www.md5hashgenerator.com/>