**그래픽, 클립아트, 그림, 디자인이(가) 표시된 사진

자동 생성된 설명**

**[File Deleted] Write-Up**

|  |  |
| --- | --- |
| **작성자** | 심주완 |
| **분석 일자** | 2024.05.15 |
| **작성 일자** | 2024.05.15 |
| **분석 대상** | File\_deleted.7z |
| **문서 버전** | 3 |
| **작성자 E-mail** | <rd002@naver.com> |

1. **목차**

[**1.** **문제** 3](#_Toc165902295)

[**2.** **분석 도구** 3](#_Toc165902296)

[**3.** **환경** 3](#_Toc165902297)

[**4.** **Write-Up** 4](#_Toc165902298)

[**5.** **Flag** 5](#_Toc165902299)

[**6.** **별도 첨부** 6](#_Toc165902300)

[**7.** **Reference** 7](#_Toc165902301)

# **문제**

|  |  |
| --- | --- |
| **URL** | <http://xcz.kr/START/prob/prob36.php> |
| **문제**  **내용** | 피시방에서 아동 청소년 보호법에 위배되는 파일을 소지한 기록을 발견했다.  아래의 형식에 맞춰 증거를 수집해라.  시간은 GMT+9 입니다. lowercase(md5(원본 경로\_만들어진 시간\_마지막 실행 된 시간\_쓰인 시간\_볼륨 시리얼))  ex)lowercase(md5(C:\XCZ\key.txt\_20121021160000\_20131022000000\_20131022000000\_AAAA-BBBB)) |
| **문제**  **파일** |  |
| **문제**  **유형** | Disk Forensics |
| **난이도** | 1 / 3 |

# **분석 도구**

|  |  |  |
| --- | --- | --- |
| **도구명** | **다운로드 링크** | **Version** |
| 010 Editor | <https://www.sweetscape.com/download/010editor/> | 14.0.1 |
|  |  |  |
|  |  |  |

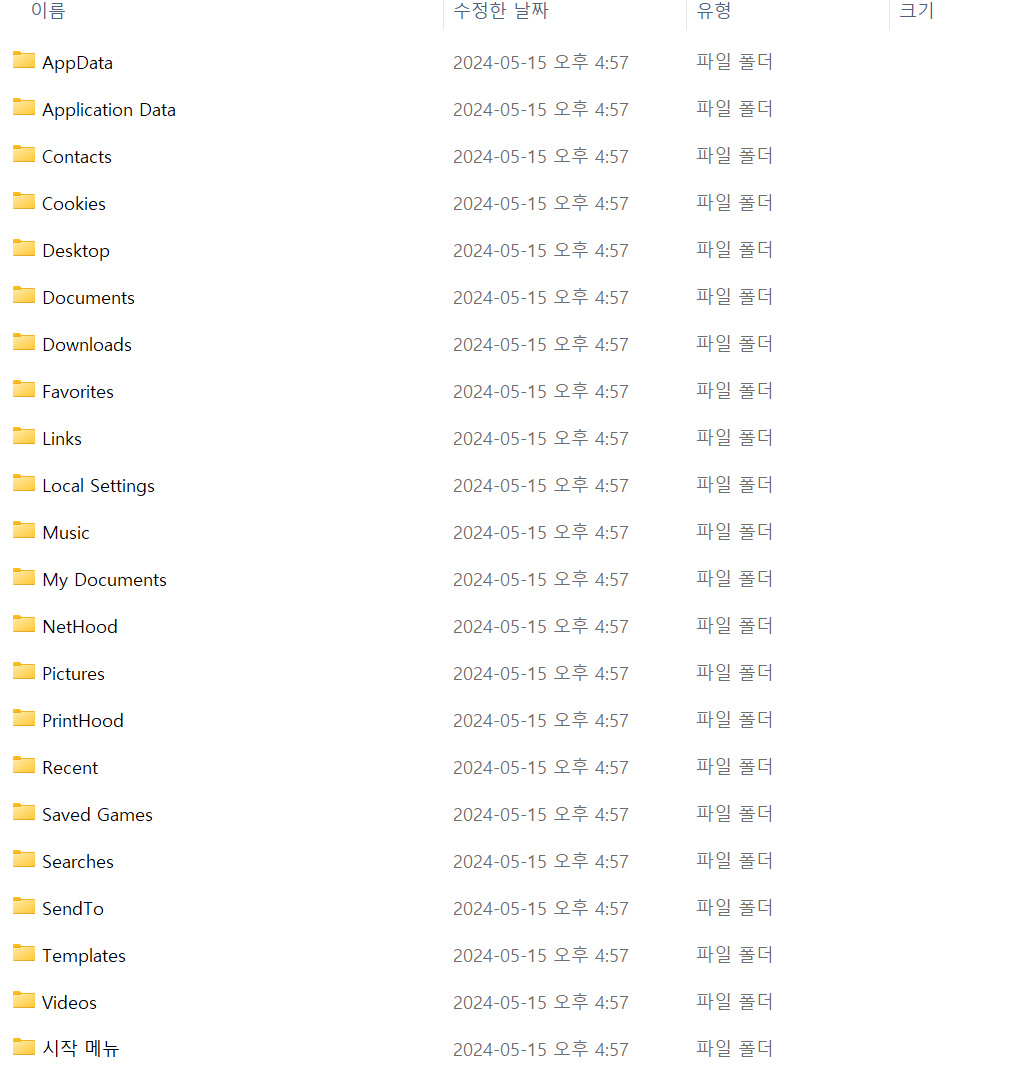
# **환경**

|  |
| --- |
| **OS** |
| Window 11 Home |

# **Write-Up**

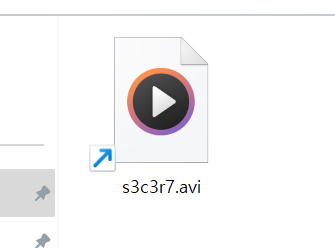
|  |  |
| --- | --- |
| **파일명** | File\_deleted.7z |
| **용량** | 996 KB |
| **SHA256** | 224B94EBFA2D1D6D7560BCCB17998C4498D92F409F3B8A760DE2DBC94625CE3D |
| **Timestamp** | 2013-10-16 13:52:10 |

이번 문제 파일은 알집으로 열리는 파일이었다. 그렇기 때문에 ftk imager를 쓰기 전에 직접 압축을 풀고 파일을 둘러보았다.



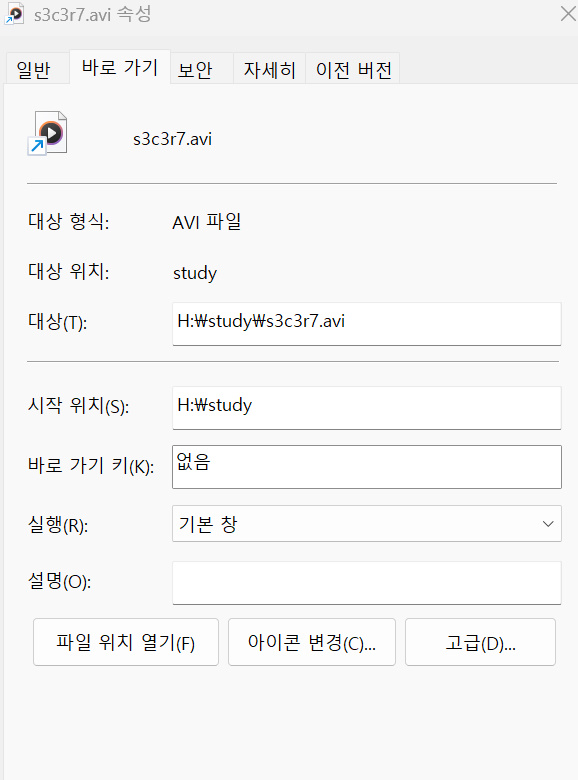
[사진 1] 문제 파일 내부

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



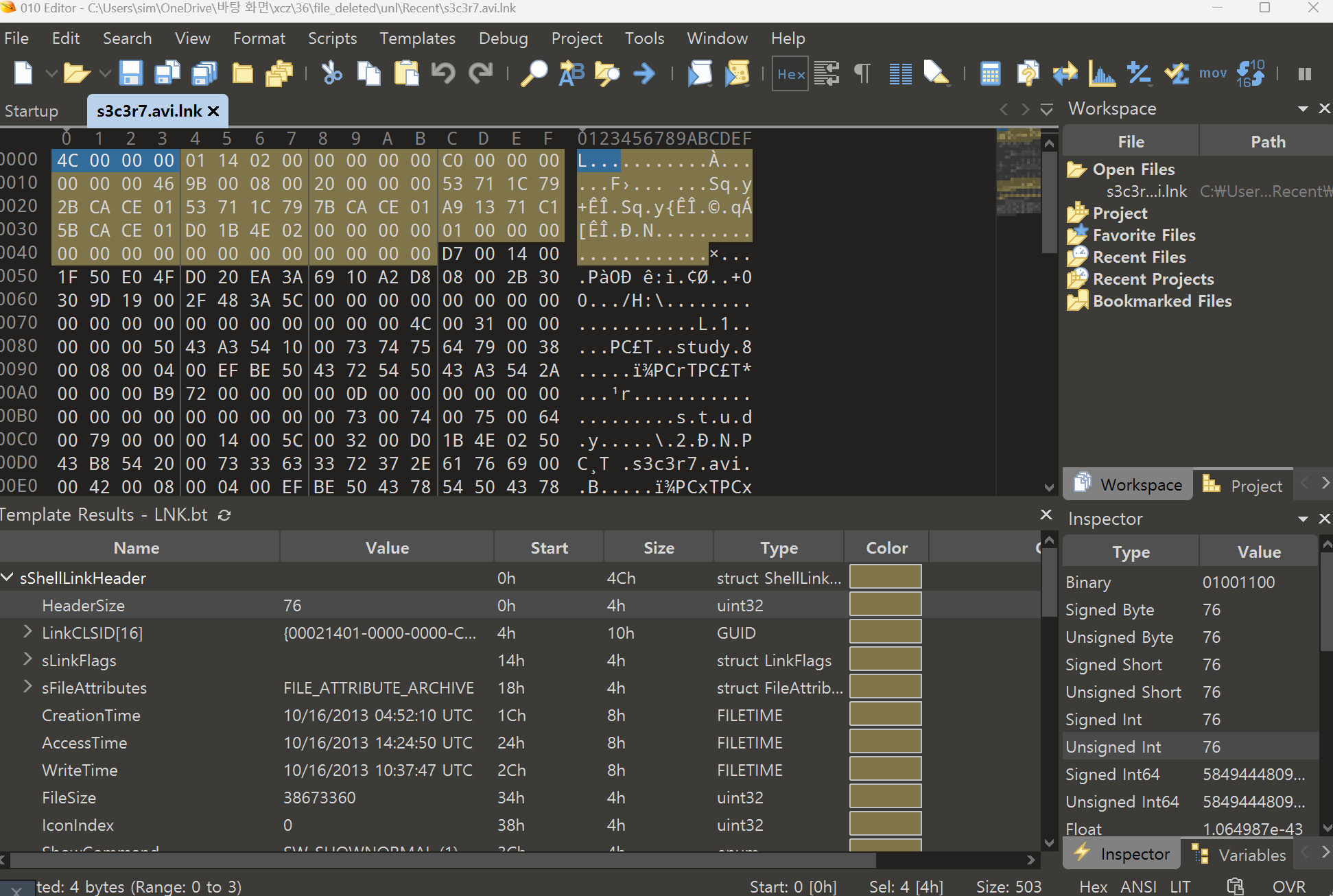
[사진 2] 의심되는 파일

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



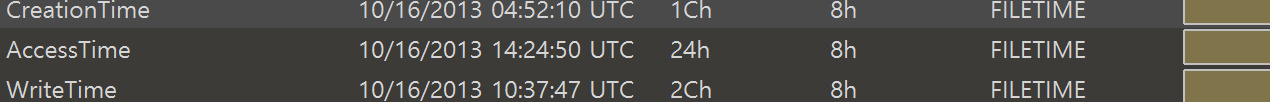
[사진 3] s3c3r7.avi 파일 속성

**경로가 study 폴더 안에 있는 파일이라… 이게 문제의 파일이라는 것을 바로 알았다.** 하지만 파일이 망가져서 속성으로는 문제에서 요구하는 플래그 포멧을 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 Editor이라는 프로그램이 존재하여 이 프래그램을 통하여 분석하였다.**



[사진 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.



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

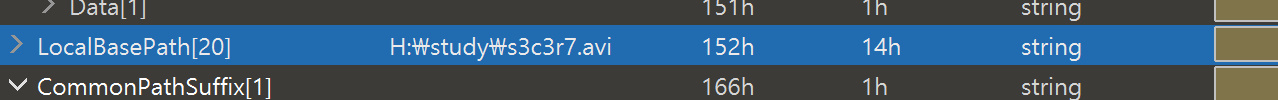
만들어진 시간, 마지막 실행 된 시간, 쓰인 시간은 다음과 같다. **하지만 문제에서 요구하는건 GMT+9이기 때문에 각 시간에 +9를 한다.**

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

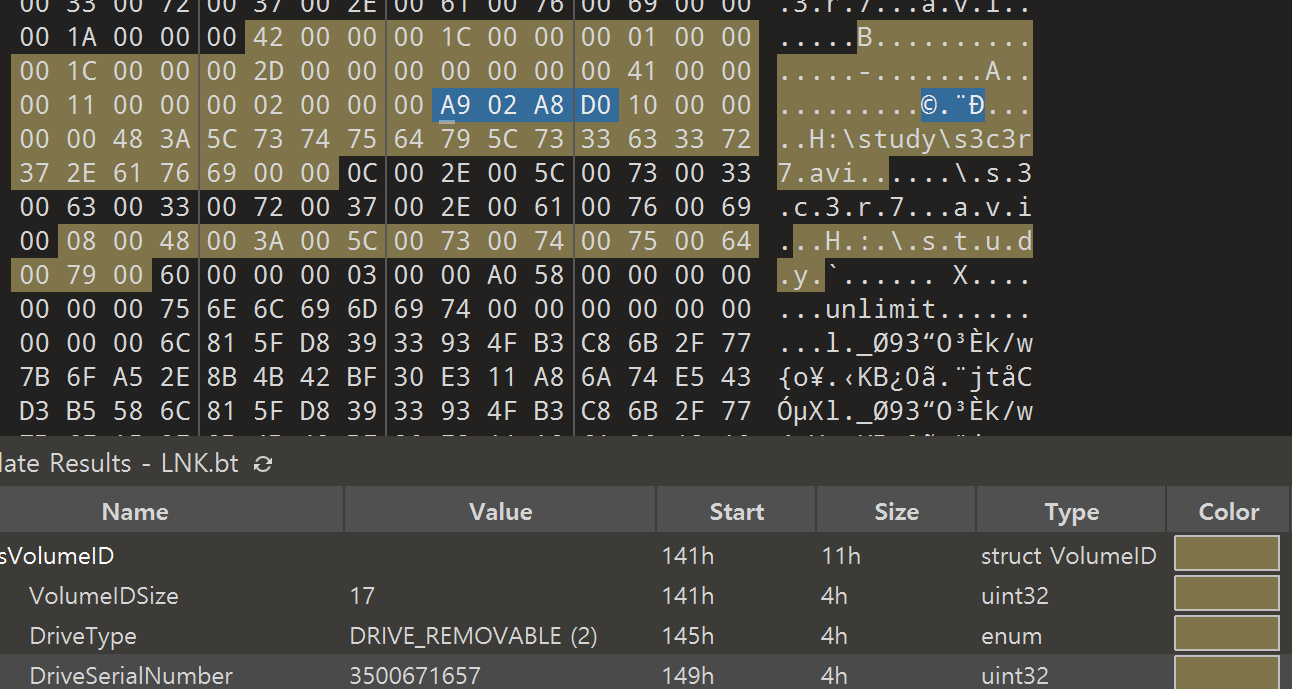
쓰인 시간 : 2013/10/16 10:37:47 +9 -> 2013/10/16 19:37:47

원본 경로는 이미 속성을 통하여 구했지만 헤더값에서도 발견할 수 있었다.



[사진 6] 010 Editor를 통하여 확인한 경로

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



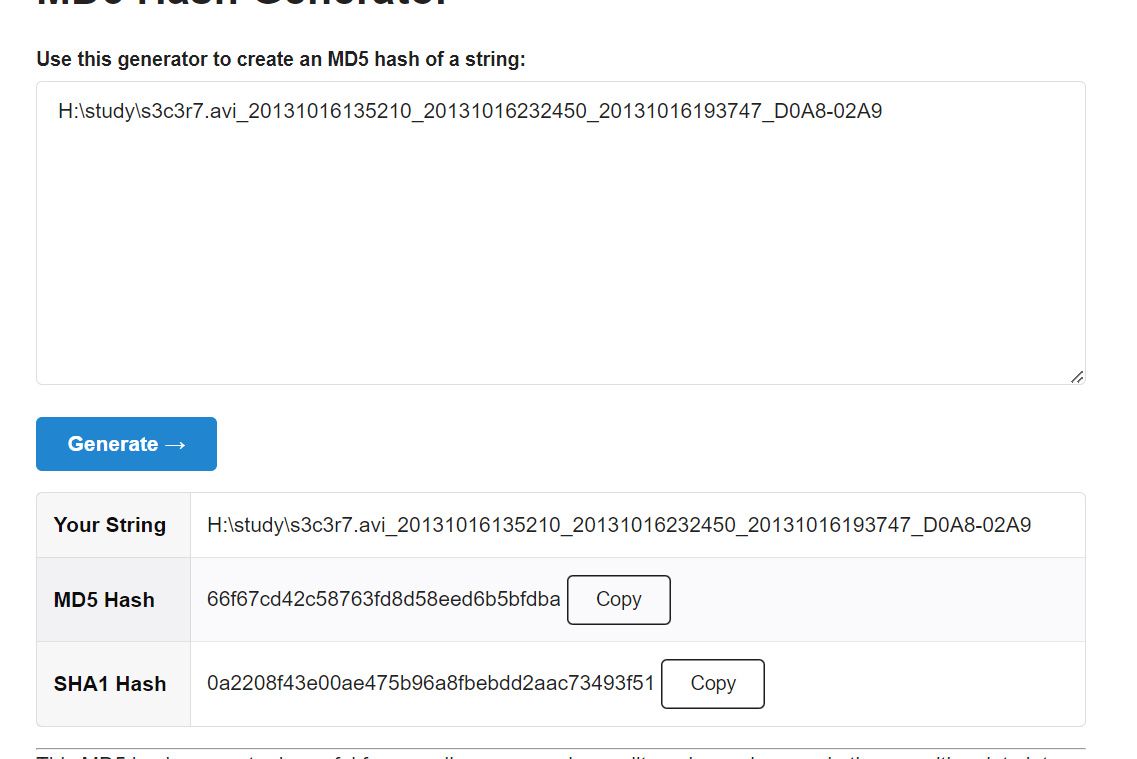
[사진 7] 데이터 시리얼 넘버

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

이를 모두 적용시키면

lowercase(md5(H:\study\s3c3r7.avi\_20131016135210\_20131016232450\_20131016193747\_D0A8-02A9))

가 된다. Md5 변환기로 변환을 시키면 플래그 값은



[사진 8] flag

이다. 사용한 MD5변환 툴은 레퍼런스로 남겨두겠다.

# **Flag**

66f67cd42c58763fd8d58eed6b5bfdba

# **별도 첨부**

# **Reference**

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