**그래픽, 클립아트, 그림, 디자인이(가) 표시된 사진

자동 생성된 설명**

**[Who’s Notebook?] Write-Up**

|  |  |
| --- | --- |
| **작성자** | 심주완 |
| **분석 일자** | 2024.05.15 |
| **작성 일자** | 2024.05.15 |
| **분석 대상** | notebook |
| **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/prob22.php> |
| **문제**  **내용** | 내친구 A는 어느날 출근길에 누군가 잃어버린 것 같은 노트북을 발견한다.  A는 이 노트북을 주인에게 찾아주고 싶지만 찾을 방법을 몰라서 포렌서인 나에게 노트북을 맡기게된다.  이 노트북의 주인을 찾아주자.  인증키 형식 : 출발지\_거쳐가는곳(1곳)\_최종도착지  인증키는 모두 대문자로, 띄어쓰기무시  예) PLACE1\_PLACE2\_PLACE3 |
| **문제**  **파일** |  |
| **문제**  **유형** | Disk Forencics |
| **난이도** | 1 / 3 |

# **분석 도구**

|  |  |  |
| --- | --- | --- |
| **도구명** | **다운로드 링크** | **Version** |
| HxD | <https://mh-nexus.de/en/hxd/> | 2.5 |
| FTKImager | [https://accessdata-ftk-imager.software.informer.com/download/#downloading](https://accessdata-ftk-imager.software.informer.com/download/%23downloading) | 3.1.2.0 |
| GPS Route Editor | <http://www.gpsnote.net/HammerBoard/List.aspx?alias=download> | 4.4.6 |

# **환경**

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

# **Write-Up**

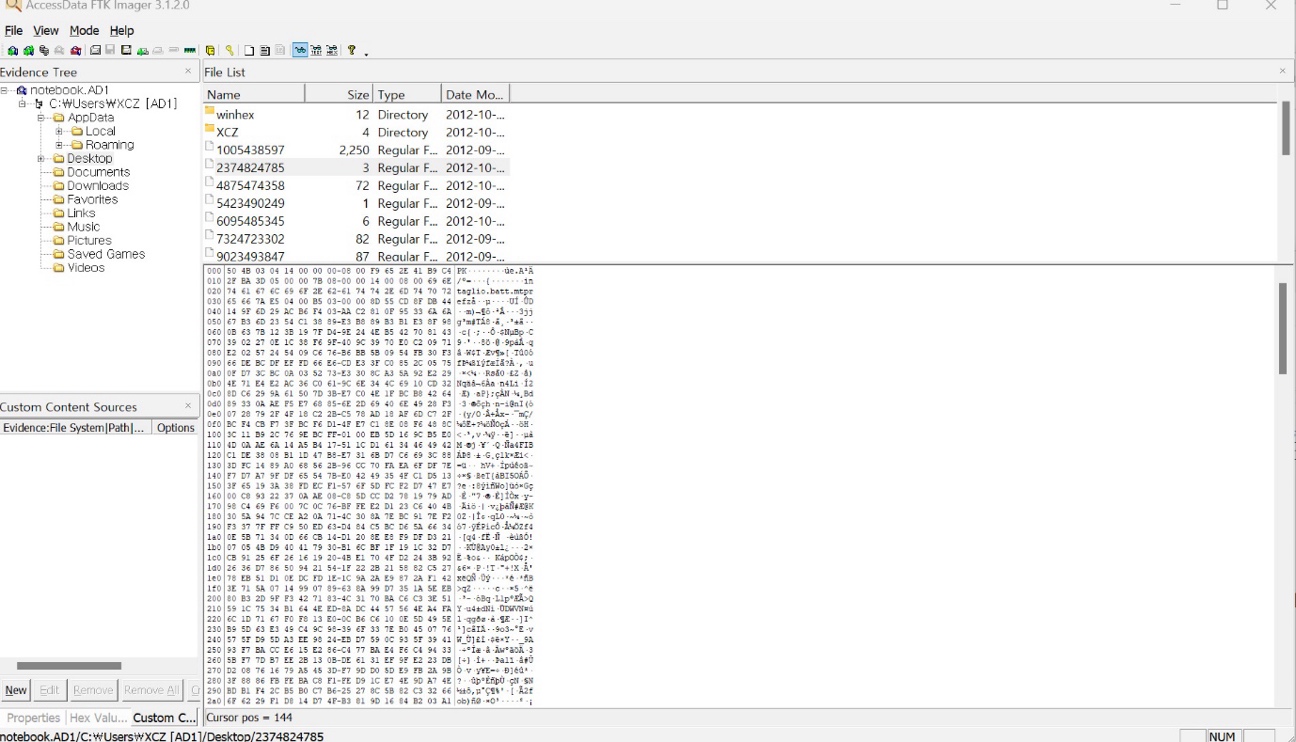
|  |  |
| --- | --- |
| **파일명** | notebook |
| **용량** | 4,949 KB |
| **SHA256** | 4864B3003B0BAA51EEBAF814B2BDDB58BFA9F6BF90CA19701D7E5611A14B9888 |
| **Timestamp** | 2012-10-14 12:35:24 |

먼저 배부받은 파일을 잘펴보자. 확장자도 나와있지 않으니 HxD를 통하여 열어보았다.



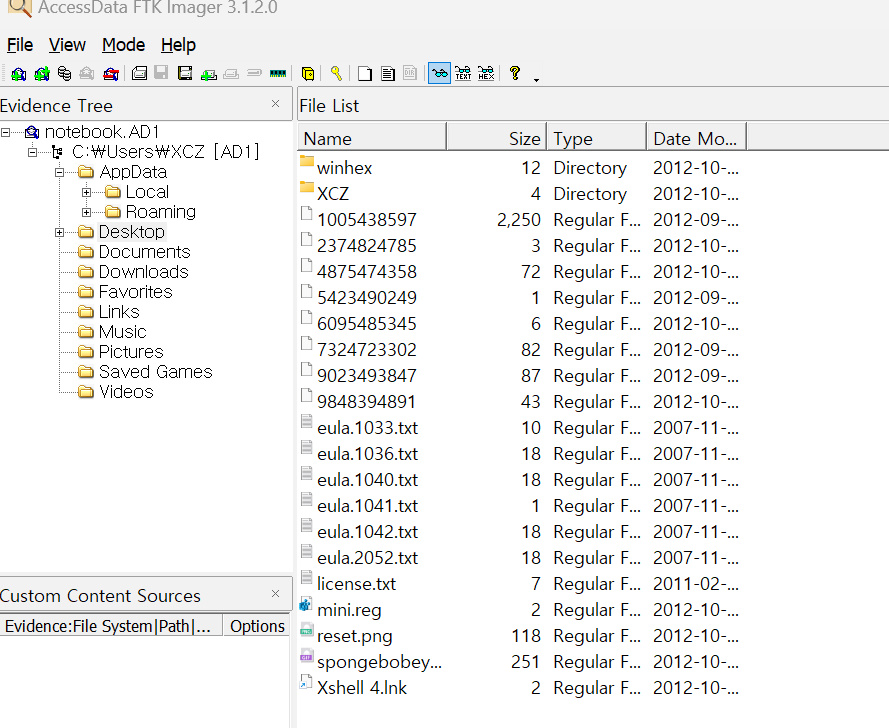
[사진 1] HxD로 열어본 notebook 파일

이 요상한 확장자는 뭘까… 처음보는 확장자이기 때문에 인터넷 서칭을 통하여 알아보았다. 알아보니 dump된 ftk imager파일이었다. ftk imager로 열기 위해서 파일의 확장자를 notebook.AD1으로 바꿔서 ftk imager로 열어보았다.



[사진 2] FTK Imager로 확인한 notebook 파일

역시나 파일이 열렸다. 키의 형식이 들렸던 장소들을 나열하는 것이니 Desktop 디렉토리를 확인해보았다.



[사진 3] Desktop 디렉토리 내부

처음에는 png파일과 gif파일이 수상해서 열어보았다.

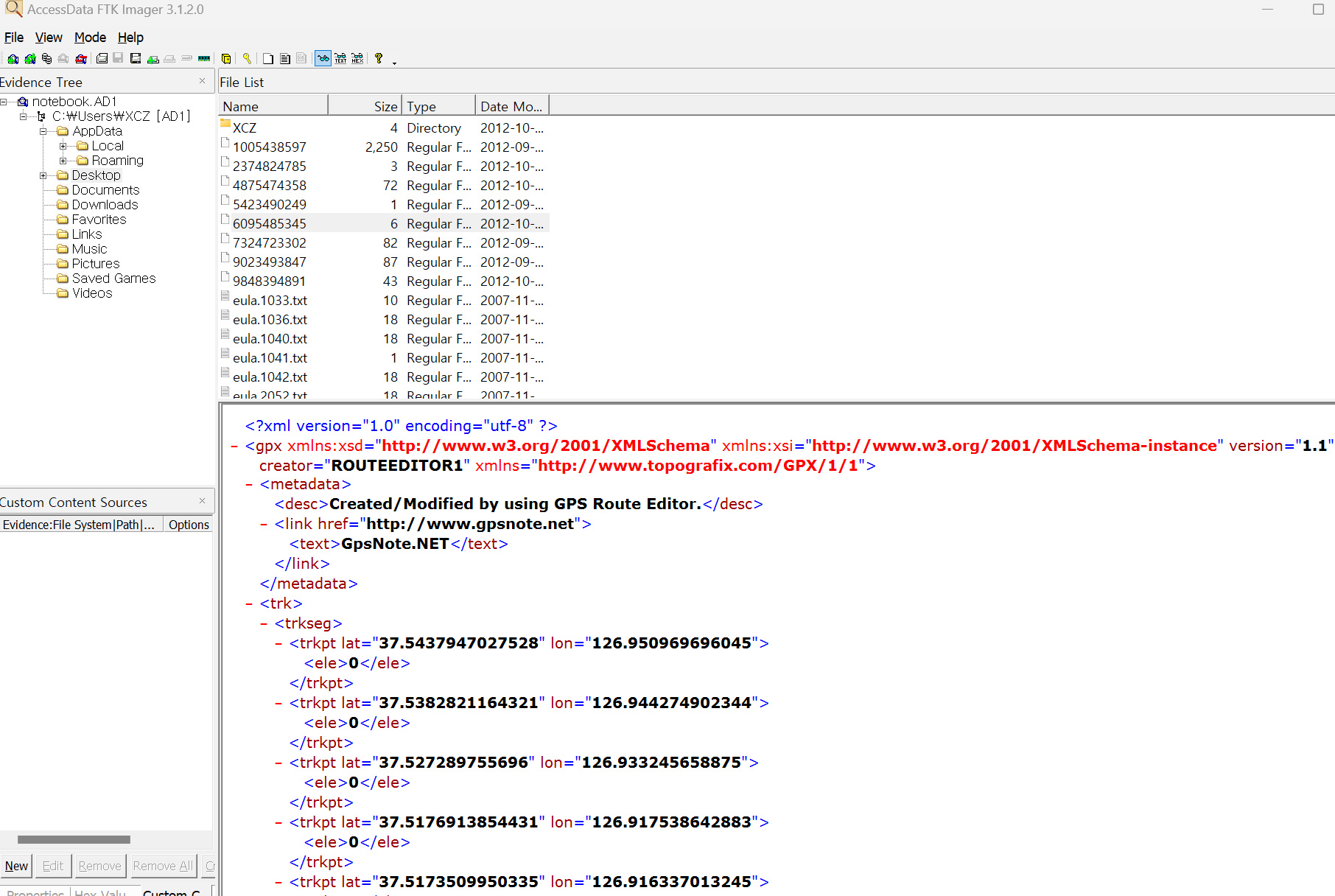


[사진 4] png 파일



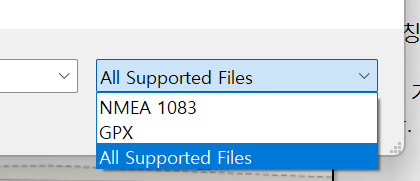
[사진 5] gif 파일

위치와 관련된 정보는 들어있지 않았고, 혹시나해서 사진을 저장한 gps정보를 따보았지만 플래그 형식과는 일치하지 않아 활용하기 어렵다는 결론에 이르렀다. 다른 파일을 살펴보자.



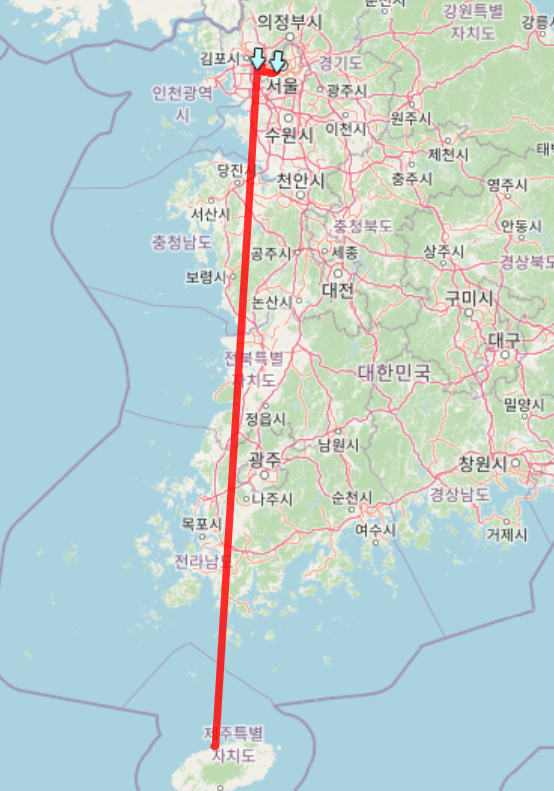
[사진 6] 6095485345 파일 내부

6095485345 파일 내부 형식을 보니 위도, 경도를 의미하는 lat, lon 형식의 코드를 확인할 수 있었다. 파일을 보자마자 정답과 관련되어있다는 것을 확신하고 코드 내부에서 하이퍼링크가 걸려있는 <http://www.gpsnote.net>로 향하였다. 이 사이트에서는 GPS ROUTE EDITOR이라는 파일을 다운받을 수 있었는데, 사용자가 이동한 GPS의 정보를 저장하고 이를 지도에 대입하여 보여주는 프로그램이었다. 6095485345파일을 GPS ROUTE EDITOR로 열어보기로 하였다.



[사진 7] GPS ROUTE EDITOR 지원 파일 형식

확인을 해보니 다음 형식만 지원을 하였고, 해당 파일을 6095485345.GPX로 변경하여 열었다.



[사진 8] 6095485345 파일

드디어 플래그를 얻을 수 있는 정보를 얻었다. 확대하여 확인을 해보니 시작은 공덕역, 중간지점은 김포공항 마지막으로 도착은 제주국제공항의 시프렌트 카 렌트 샵임을 확인할 수 있었다. 키를 포멧과 맞춰서 작성을 해보면

**GONGDEOK\_GIMPOINTERNATIONALAIRPORT\_SEFRIENDRENDACARSHARP**

가 플래그 답일 것이다! 하지만 여기서 큰 문제가 발생한다. 계속해서 플래그를 제출하면 오답으로 표기가 되는 것이다. 너무 답답하여 다른 Write-Up을 확인하니 같은 문제가 나오고 있었다. 이유는 이 파일이 2012년에 만들어져서 그때는 시프렌트 카 렌트 샵이 아니라 세븐일레븐이었다는 것이다… 결국 다음과 같은 플레그로 바뀌어야 할 것이다.

GONGDEOK\_GIMPOINTERNATIONALAIRPORT\_7-ELEVEN

# **Flag**

GONGDEOK\_GIMPOINTERNATIONALAIRPORT\_7-ELEVEN

# **별도 첨부**

# **Reference**

* [URL]