



[Windows Search] Write-Up

작성자	심주완
분석 일자	2024.05.09
작성 일자	2024.05.09
분석 대상	WindowSearch 파일
문서 버전	2
작성자 E-mail	rd002@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	https://dreamhack.io/wargame/challenges/729
문제 내용	Do you know "Windows Search" with (windows + s) command? Find the flag.txt!
문제 파일	 Windows.edb
문제 유형	dicsc forencics
난이도	1.5 / 5

2. 분석 도구

도구명	다운로드 링크	Version
WinSearchDBAnalyzer	https://moaistory.blogspot.com/2018/10/winsearchdbanalyzer.html	1.0.0.6

3. 환경

OS
Windows 11 Home



4. Write-Up

먼저, WindowSearch 파일은 .edb 파일로 나타내는데, WindowSearch 파일이 무엇인지 찾아보았다.

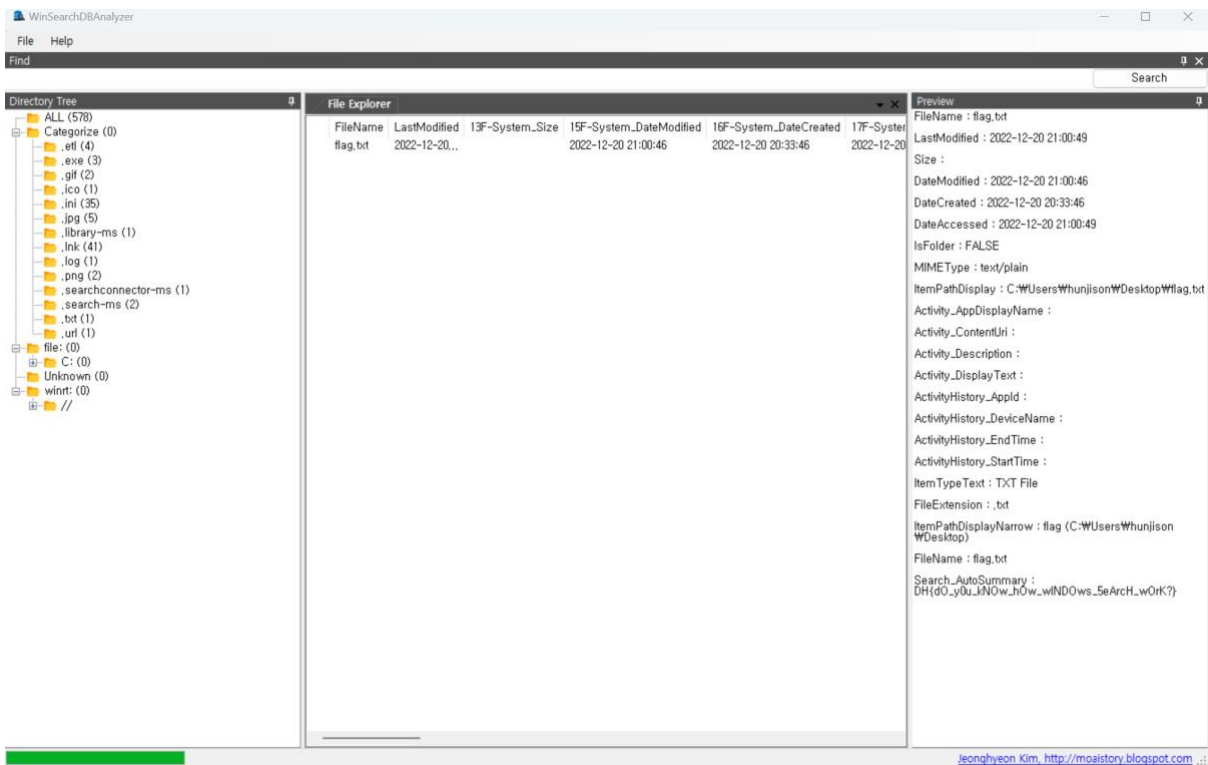
그렇다면 이 정보를 정리하자면, 주어진 윈도우 검색 파일을 하나하나 확인하여 남긴 플래그를 찾는 것이 되겠다.

다음은 설치가 끝난 이후 문제 파일을 WinSearchDBAnalyzer 에 넣은 사진이다.



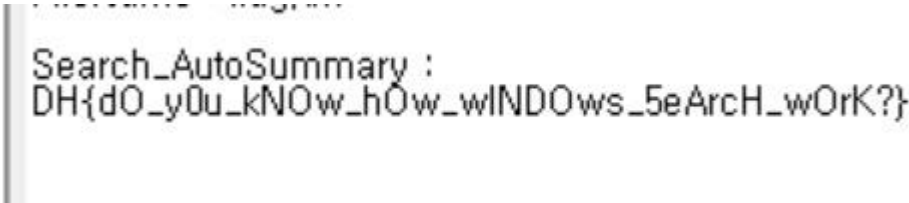
[WHS-2] .iso

Directory Tree를 확인해보면 많은 수의 확장자별로 파일과 폴더를 나누어져 나타나있다. **다른 힌트가 없었기 때문에 폴더 안에 파일을 하나하나 확인해보았다.**



[Figure 2] .txt 파일 내용

.txt폴더를 확인하던 중 flag.txt 파일을 찾을 수 있었다. Preview를 확인하면 간단한 파일 정보를 확인할 수 있다.



[Figure 3] Preview를 확인 도중 플래그를 찾음

Preview 를 활용하여 간단하게 파일내부를 열람했고, 이 안에 플래그를 구했다.

5. Flag

DH{dO_y0u_kNOw_hOw_wINDOWs_5eArcH_wOrK?}

6. 별도 첨부

7. Reference

- [URL]