[포렌식툴 분석 보고서]

[WinPrefetchView]

작성일	2025.05.26
작성자	안서진
검토자	김예은

목차

I. 툴 기본 정보

항목	내용
툴 이름	WinPrefetchView
분석 카테고리	시스템 설치/실행, 파일 사용/조작(일부)
사용 버전	v1.37
다운로드 경로	https://www.nirsoft.net/utils/win_prefetch_view.html
지원 포맷	.pf(prefetch 파일)

[표 1. 툴 기본 정보표]

II. 툴 소개 및 목적

1. WinPrefetchView는 시스템에 저장된 프리패치 파일을 읽고 그 안에 저장된 정보를 표시하는 간단한 유틸리티이다.
2. 이 도구를 통해 각 애플리케이션이 어떤 파일을 사용하고 있는지, Windows 부팅 시 어떤 파일이 로드되는지 등을 알 수 있다.

III. 설치 매뉴얼

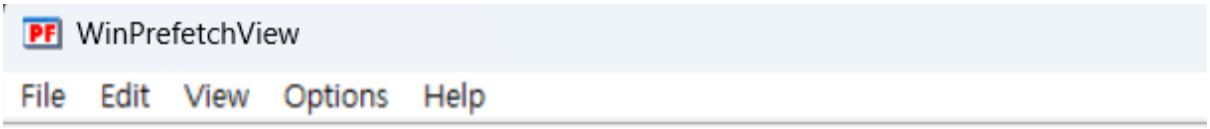
1. 지원 운영체제: Windows XP부터 Windows 10까지 모든 버전의 Windows에서 작동
2. 설치 방식: WinprefetchView 다운로드 링크 에서 다운로드
3. 별도의 설치 없이 사용 가능하며, 압축을 푼 후 "**WinprefetchView.exe**"를 실행하여 사용

IV. 주요 기능 및 사용법

1. 메뉴 바

항목	기능
File	Prefetch 파일 저장, 종료
Edit	항목 복사, 선택/해제 가능
View	컬럼 선택, 새로고침 등 보기 옵션
Options	시간, 경로 변경 옵션
Help	프로그램 정보, 버전 확인

[표 2. 메뉴 바 기능 설명표]

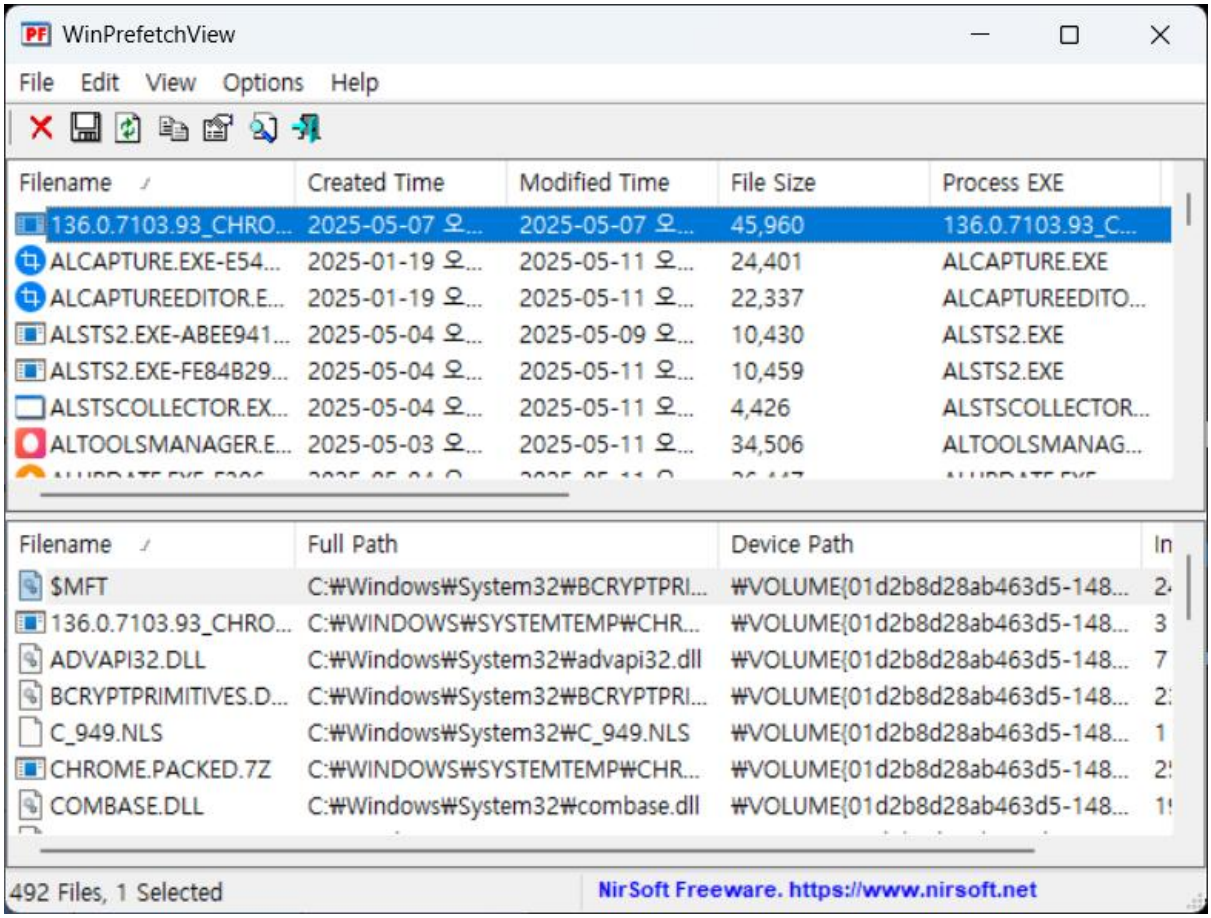


[그림 1. WinPrefetchView 도구 메뉴 바]

2. 기능 1: 기본 실행

1) exe 파일을 실행시키면 pf 파일이 생성되고 pf 파일이 만들어진 시각은 exe 프로그램 최초 실행시각을, pf 파일이 수정된 시각은 exe 프로그램의 마지막 실행 시각을 뜻한다.
2) 기본 경로는 **C:₩Windows₩Prefetch**이며, 프로그램의 대기시간을 줄이기 위해 사용된다.

   (예) 사용자가 **ALCAPTURE.EXE**를 처음 실행한 시각과 마지막으로 실행한 시각을 파악할 수 있다.



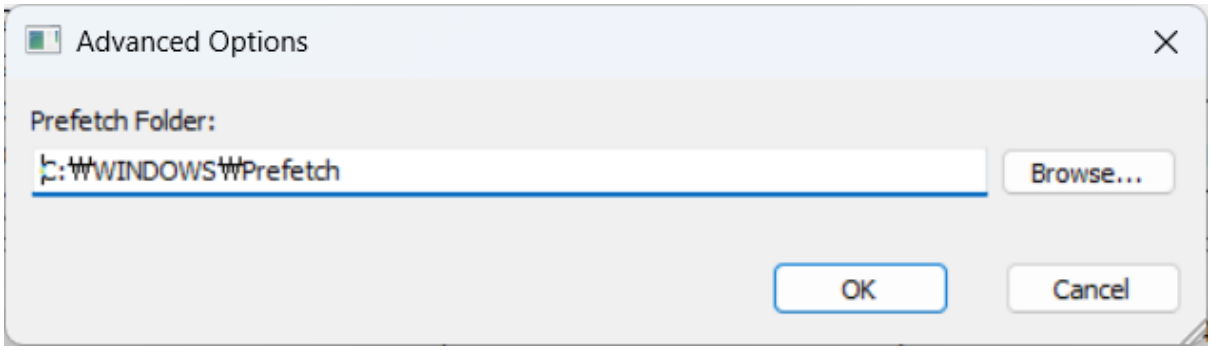
[그림 2. 기본 경로의 프리패치 화면]

3. 기능 2: 경로 변경

1) prefetch 파일을 추출해서 사용하는 경우에는 파일 경로를 수동으로 설정할 수 있다.

2) 다른 PC에서 복사해온 Prefetch 파일을 분석할 때, 경로를 새로 지정해 분석할 수 있다.

(예) Options 메뉴 → **Advanced Options** 혹은 **F9**

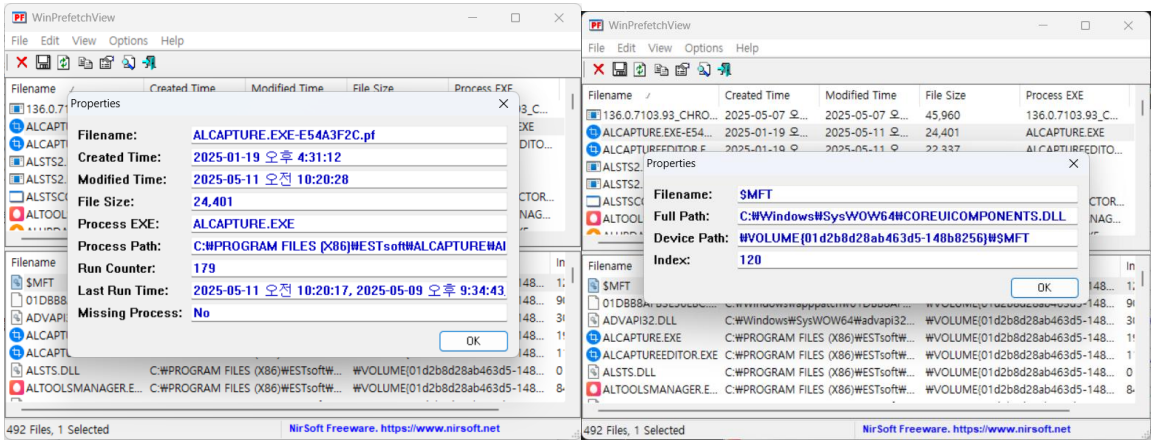


[그림 3. 경로 변경 옵션 화면]

4. 기능 3: 프로그램 상세 정보 확인

1) 파일 항목을 더블 클릭하면, 파일 이름과 카운터(실행횟수), 생성 시간과 변경 시간, 경로, 마지막 실행시간 등의 상세 정보를 확인할 수 있다.

2) 해당 프로그램을 삭제하거나 경로를 변경하더라도 프리패치는 삭제되지 않는다.



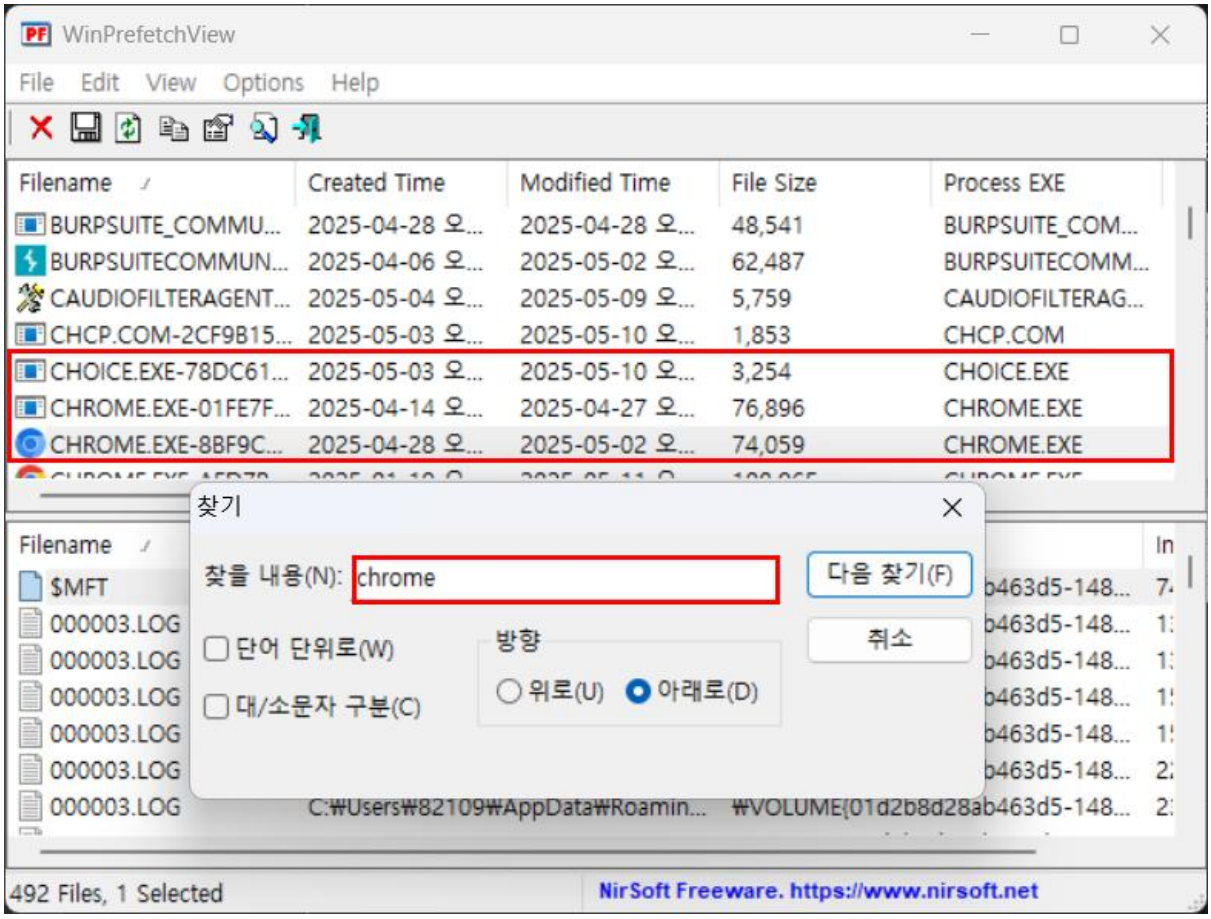
[그림 4, 5. 프로그램 속성 화면]

5. 기능 4: 특정 단어 검색(필터링)

1) 파일 목록에서 특정 파일명을 검색할 수 있으며, 검색 결과로 관련 Prefetch 항목만 필터링하여 보여준다.

2) **chrome** 키워드를 검색해 **CHROME** 실행 기록만 추출이 가능하다.

(예) Edit 메뉴 → **Find**



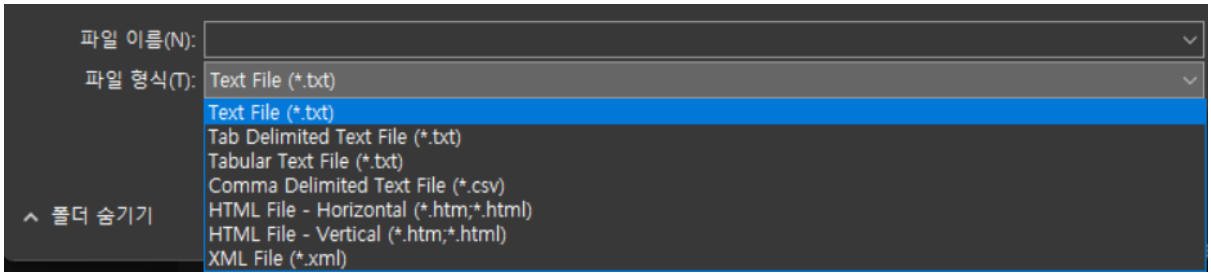
[그림 6. chrome 단어 검색 화면]

6. 기능 5: 내보내기(Export)

1) File 메뉴 → **Save Selected Items** 혹은 **Ctrl +S** 를 통해 Prefetch 분석 데이터를 다양한 포맷(**.csv**, **.txt**, **.html**, **.xml**)으로 저장할 수 있다.

2) 모든 데이터를 내보내고 싶다면 Edit 메뉴 → **Select All** 혹은 **Ctrl + A**를 통해 전체 선택이 가능하다.

(예) Prefetch 분석 결과를 CSV 형태로 저장해 엑셀로 리스트업할 수 있다.



[그림 7. 다양한 포맷을 지원하는 내보내기 기능]

V. 참고 자료

[1] Nir Sofer,「WinPrefetchView - View the contents of Windows Prefetch (.pf) files」, NirSoft, N/A, 2023.

[2] MajorGeeks,「WinPrefetchView 1.37」, MajorGeeks.com, N/A, 2023.