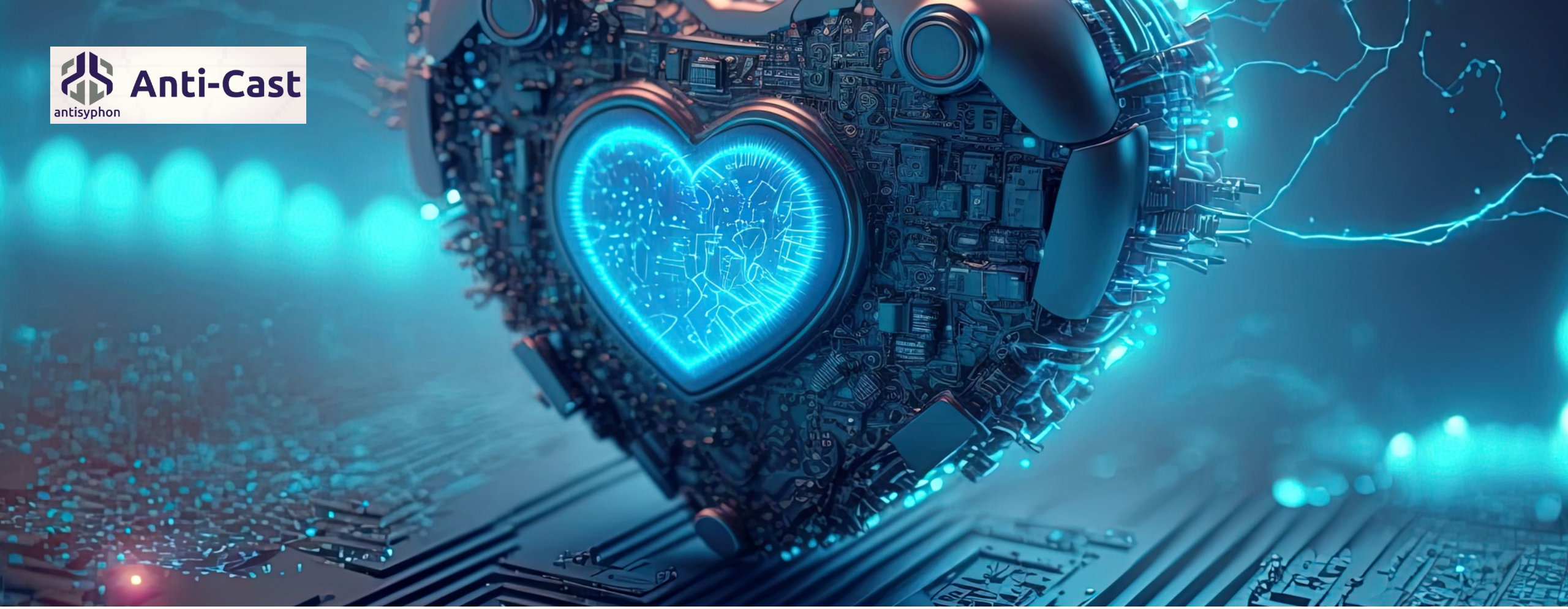


For the Love of the Windows Search Index

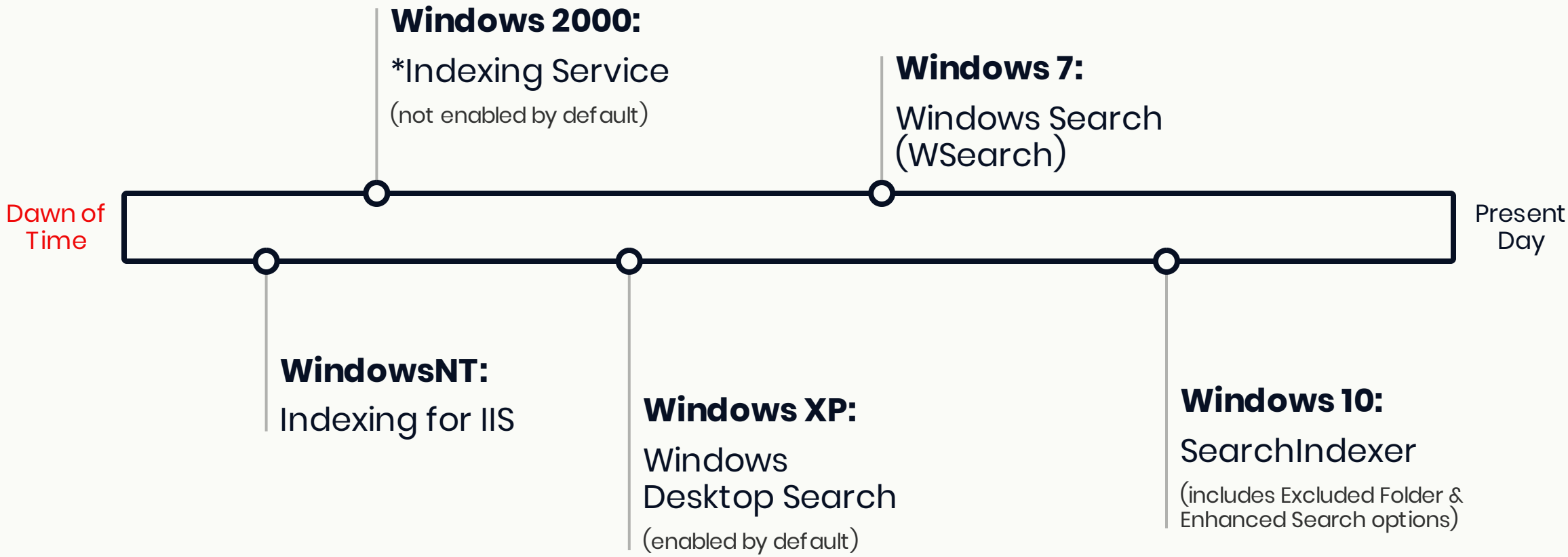
14 FEB 2024

Alissa Torres | @sibertor

What is Windows Search?

- **User Experience Enhancement:** Provides a fast method for users to locate and access files on local device or remote locations.
- Creates a locally stored index of files and **non-file** items stored on a computer.
  - Windows.edb <Win11
  - Windows.db & Windows-gather.db - Win11
- The indexing service references USN Journal changes to trigger index updates.
- The Windows Search Indexer runs as a system service.

Evolution of Windows Search



Windows Search Index

What's in the Windows Search Index Database?

- File, Folder Information
  - *Time stamps, Size, Status*
- Outlook Mail Data (Time, Contents)
- OneNote Title
- Internet History (URLs, Last visit time)
- .lnk list
- Network Drive (When adding offline)
- Favorites
- Activity History (Windows 10 Timeline)

Windows Search Index

Windows.EDB (<Win11) or Windows.DB (Win11)

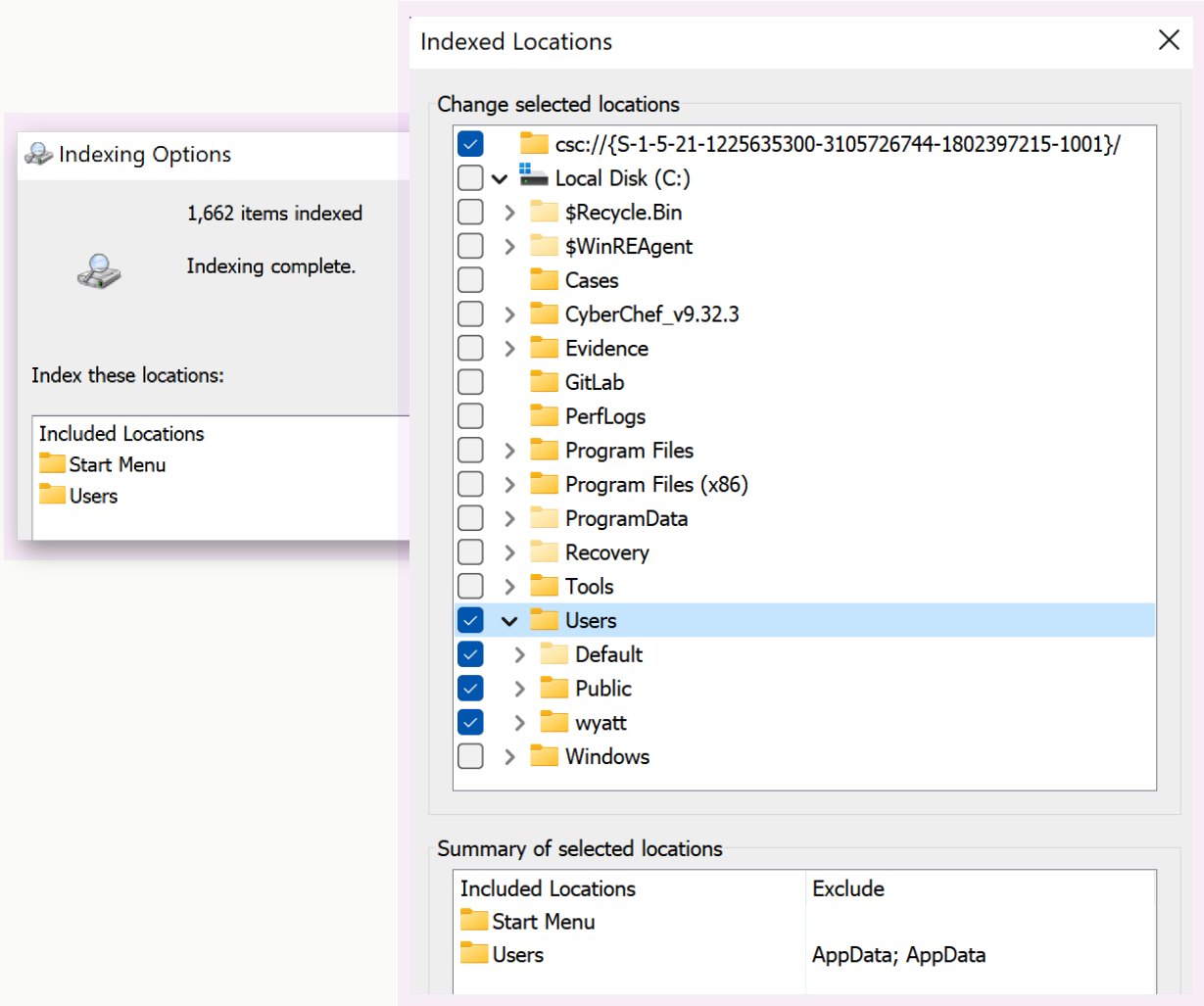
Indexed Default Locations:

- **Start Menu**
  - ProgramData\Microsoft\Windows\Start Menu\Programs*
- **Users directories and contents**
  - AppData directories, but not content

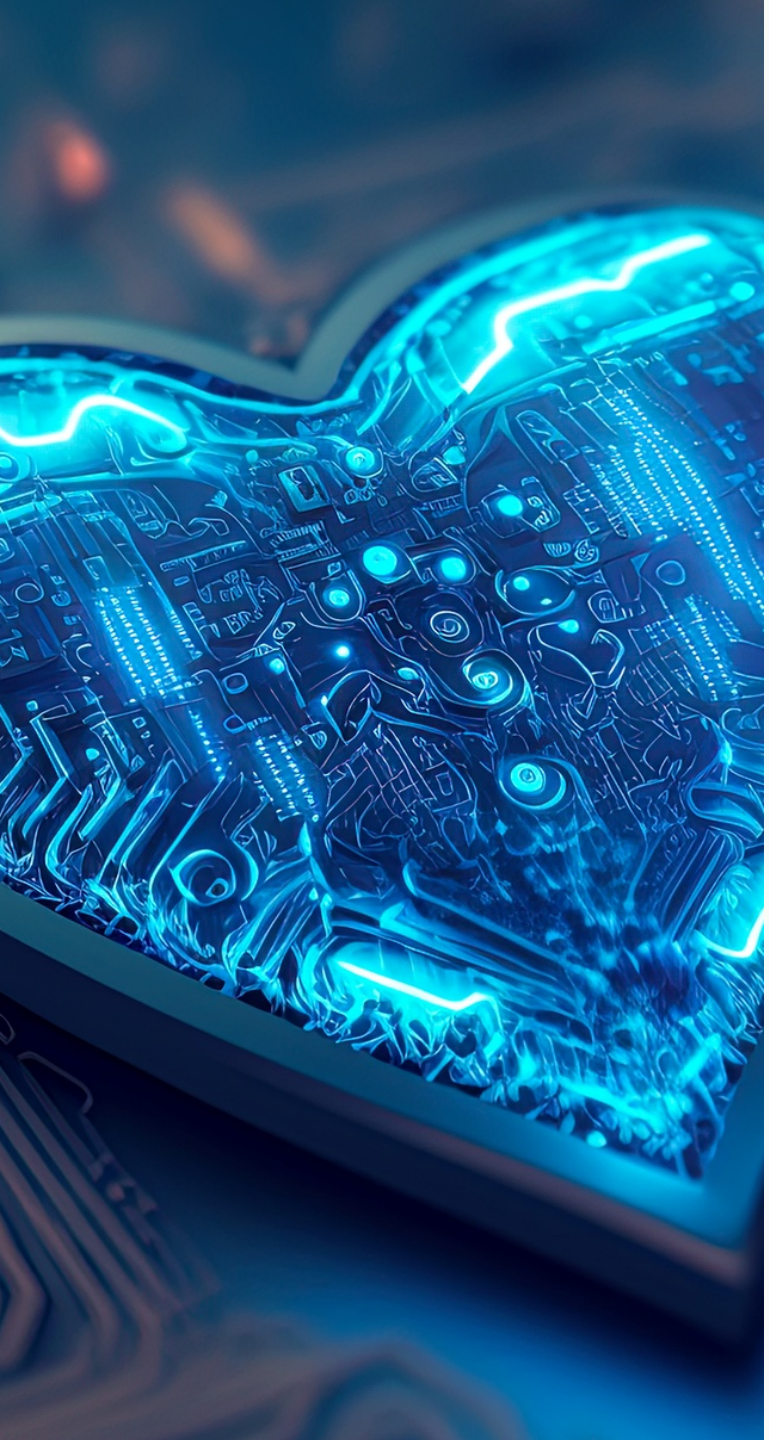
Additional directories can be specified

Indexing service contains a master list of "scope", locations to crawl

Be default, indexing does not include encrypted files, but can be enabled.



*csc:// Client Side Cache - offline files (local copies of network files)



Windows Search Handlers

Protocol Handlers

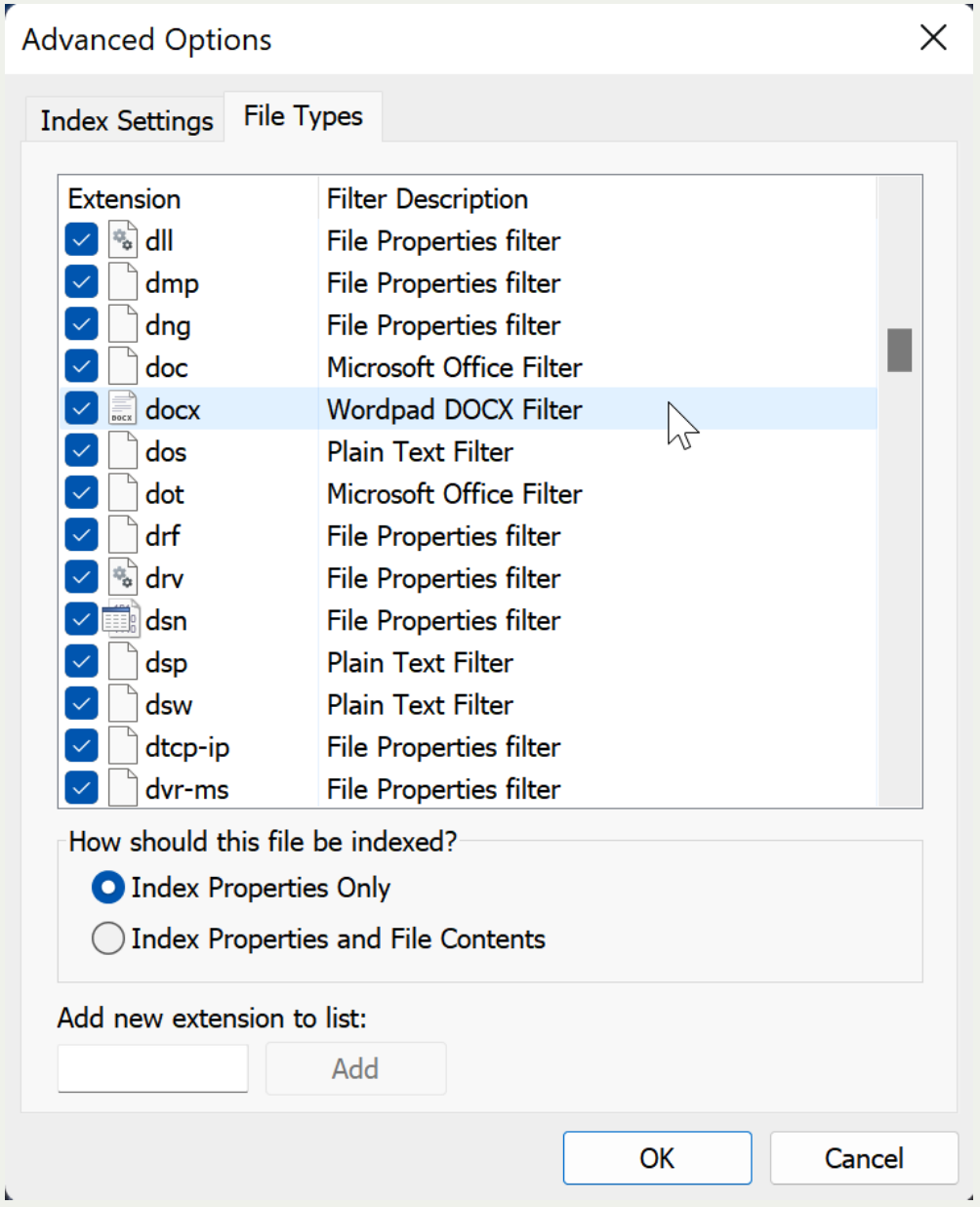
Provides Windows Search Indexer access to data stores.

example #1: **search-ms** URI protocol handler

example #2: **Outlook**

Property Handlers

Allows the Search Indexer to extract file type specific metadata.



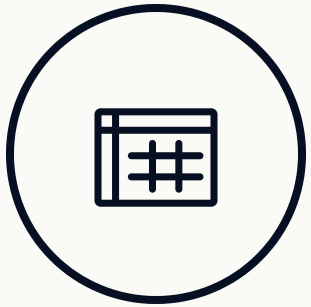
Property Handlers

- Invoked in-process by the indexer to read and index property values.
- Custom property handlers can be registered by third-party developers for specific file types.
- Optimizations include placement of property values where enumeration does not require reading the whole file.
- Schemas that provide insight into a file format to identify meaningful data about the file.
- Defined per file type.

IFilters: Used to extract the property values from specific file types.

Windows Search Service

Indexer Processes



SearchIndexer.exe

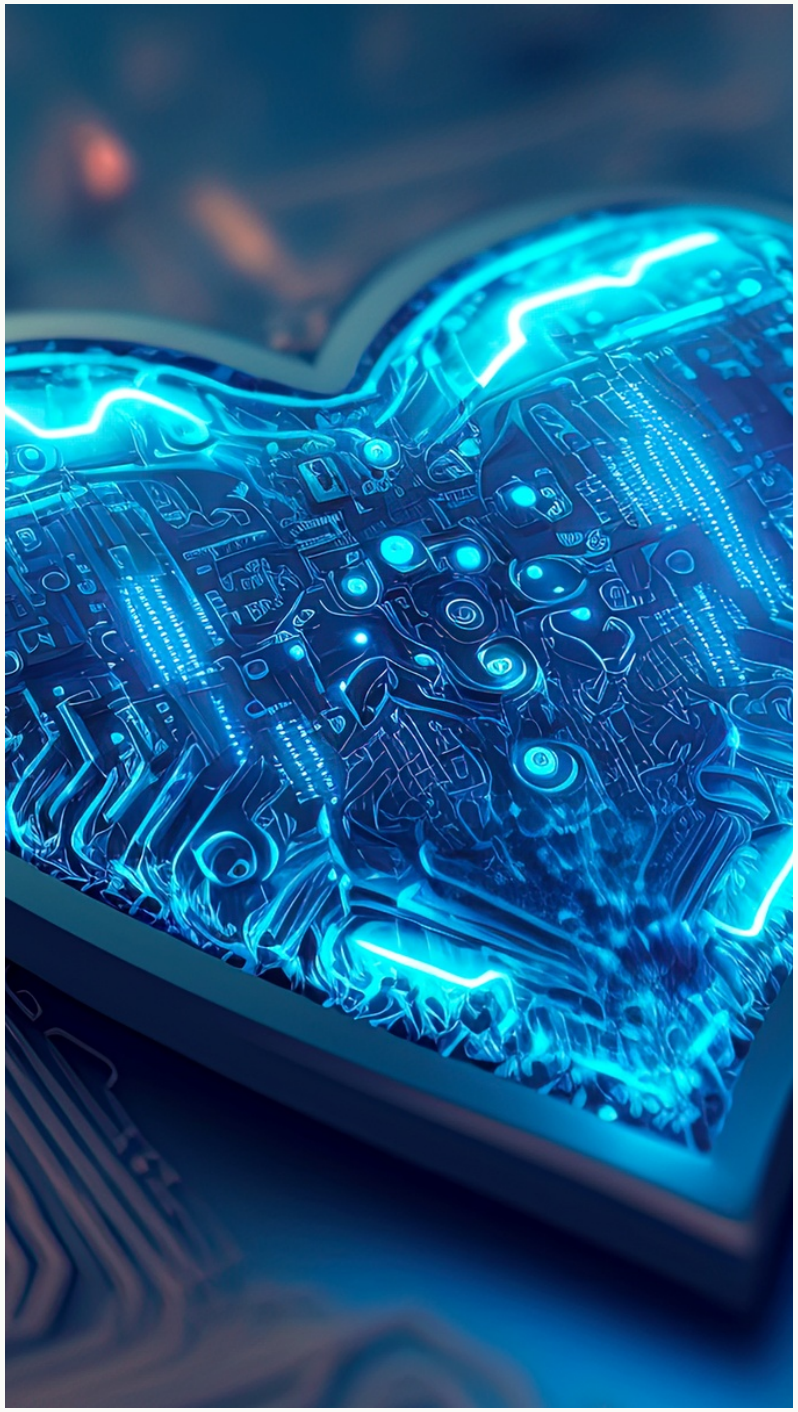
Hosts indexes and the list of URIs that require indexing. Contains the query APIs that other applications use to leverage the Windows Search features.

SearchProtocolHost.exe

Hosts the protocol handlers. Runs with the least privileges required to index.

SearchFilterHost.exe

Hosts the IFilters and property handlers to extract metadata and textual content.Low Integrity Process.



Windows.edb

Windows 10 Search Index ESE Database

Location:

C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Windows.edb

One Database, Three Valuable Tables

- SystemIndex_Gthr: 20 columns
- SystemIndex_GthrPath: 3 columns
- SystemIndex_PropertyStore: 598+ columns

ESEDatabaseView by NirSoft

Extensible Storage Engine Viewer

winrt: Windows Runtime

33-System_ItemUrl
file:C:/ProgramData/Microsoft/Windows/Start Menu
file:C:/Users
winrt://{S-1-5-21-522249870-1839504115-1396688109-1000}
file:C:/ProgramData/Microsoft/Windows/Start Menu/desktop.ini
file:C:/ProgramData/Microsoft/Windows/Start Menu/Programs
file:C:/ProgramData/Microsoft/Windows/Start Menu/Programs/Accessibility
file:C:/ProgramData/Microsoft/Windows/Start Menu/Programs/Accessories
file:C:/ProgramData/Microsoft/Windows/Start Menu/Programs/Administrative Tools
file:C:/ProgramData/Microsoft/Windows/Start Menu/Programs/desktop.ini
file:C:/ProgramData/Microsoft/Windows/Start Menu/Programs/Immersive Control Panel.lnk`
file:C:/ProgramData/Microsoft/Windows/Start Menu/Programs/Maintenance
file:C:/ProgramData/Microsoft/Windows/Start Menu/Programs/StartUp
file:C:/ProgramData/Microsoft/Windows/Start Menu/Programs/System Tools
file:C:/ProgramData/Microsoft/Windows/Start Menu/Programs/Windows 10 Update Assistant.lnk□
file:C:/ProgramData/Microsoft/Windows/Start Menu/Programs/System Tools/desktop.ini
file:C:/ProgramData/Microsoft/Windows/Start Menu/Programs/System Tools/Task Manager.lnk
file:C:/ProgramData/Microsoft/Windows/Start Menu/Programs/StartUp/desktop.ini
file:C:/ProgramData/Microsoft/Windows/Start Menu/Programs/Maintenance/Desktop.ini
file:C:/ProgramData/Microsoft/Windows/Start Menu/Programs/Administrative Tools/Component Services.lnk`
file:C:/ProgramData/Microsoft/Windows/Start Menu/Programs/Administrative Tools/Computer Management.lnk@□
file:C:/ProgramData/Microsoft/Windows/Start Menu/Programs/Administrative Tools/desktop.ini
file:C:/ProgramData/Microsoft/Windows/Start Menu/Programs/Administrative Tools/dfrgui.lnk□
file:C:/ProgramData/Microsoft/Windows/Start Menu/Programs/Administrative Tools/Disk Cleanup.lnk
file:C:/ProgramData/Microsoft/Windows/Start Menu/Programs/Administrative Tools/Event Viewer.lnk
file:C:/ProgramData/Microsoft/Windows/Start Menu/Programs/Administrative Tools/iSCSI Initiator.lnk
nistrative Tools/Memory Diagnostics Tool.lnk
nistrative Tools/ODBC Data Sources (32-bit).lnk`
nistrative Tools/ODBC Data Sources (64-bit).lnk`
file:C:/ProgramData/Microsoft/Windows/Start Menu/Programs/Administrative Tools/Performance Monitor.lnk@□

Download here: https://www.nirsoft.net/utils/ese_database_view.html

SIDR by Stroz Friedberg

- Command-line Search Index database parsing tool written in Rust
- Supports Windows 10 & Windows 11 Database Formats
- Output options: csv or json

```
Usage: sidr [OPTIONS] <INPUT>

Arguments:
  <INPUT>
          Path to input directory (which will be recursively scanned for Windows.edb and Windows.db)

Options:
  -f, --format <FORMAT>
          Output format: json (default) or csv

          [default: json]
          [possible values: json, csv]

  -o, --outdir <OUTPUT DIRECTORY>
          Path to the directory where reports will be created (will be created if not present). Default
is the current directory

  -h, --help
          Print help (see a summary with '-h')

  -V, --version
          Print version
```

Download here: https://github.com/strozfriedberg/sidr

Windows.edb Parsing

SIDR – Parsing tool by Stroz Friedberg

- Parses Win10 ESE and Win11 SQLite databases
- Produces Three Reports (csv or json)
  - File Report
  - Internet History
  - Activity History

```
c:\Tools>sidr.exe c:\users\wyatt\desktop -f csv -o c:\cases
Processing ESE db: c:\users\wyatt\desktop\Windows.edb
c:\cases\DESKTOP-BR131UQ_File_Report_20240214_130859.csv
c:\cases\DESKTOP-BR131UQ_Internet_History_Report_20240214_130859.csv
c:\cases\DESKTOP-BR131UQ_Activity_History_Report_20240214_130859.csv

Found 1 Windows Search database(s)
```

Windows.edb Parsing

Internet History Report

Work Id	System_Computer Name	System_Item Url
1120	DESKTOP-BR131UQ	iehistory://{S-1-5-21-522249870-1839504115-1396688109-1001}
1180	DESKTOP-BR131UQ	iehistory://{S-1-5-21-522249870-1839504115-1396688109-1000}/file:///C:/Users/SANSDIFR/AppData/Local/Temp/Temp1_sysmon-config-r
1182	DESKTOP-BR131UQ	iehistory://{S-1-5-21-522249870-1839504115-1396688109-1000}
1183	DESKTOP-BR131UQ	iehistory://{S-1-5-21-522249870-1839504115-1396688109-1000}/http://www.msftconnecttest.com/redirect
1184	DESKTOP-BR131UQ	iehistory://{S-1-5-21-522249870-1839504115-1396688109-1000}/https://login.live.com/oauth20_desktop.srf?lc=1033
1185	DESKTOP-BR131UQ	iehistory://{S-1-5-21-522249870-1839504115-1396688109-1000}/https://login.live.com/oauth20_authorize.srf?client_id=0000000048
1254	DESKTOP-BR131UQ	iehistory://{S-1-5-21-522249870-1839504115-1396688109-1000}/file:///C:/Users/SANSDIFR/Documents/DebugDiag/Reports/DC-Skeleton-
1256	DESKTOP-BR131UQ	iehistory://{S-1-5-21-522249870-1839504115-1396688109-1000}/file:///C:/Users/SANSDIFR/Documents/DebugDiag/Reports/DC-Skeleton-
1274	DESKTOP-BR131UQ	iehistory://{S-1-5-21-522249870-1839504115-1396688109-1000}/file:///C:/Users/SANSDIFR/Documents/DebugDiag/Reports/DC-Skeleton-

Windows.edb Parsing

File Report

Work Id	System_Computer Name	System_Item Path Display
1	DESKTOP-BR131UQ	C:\ProgramData\Microsoft\Windows\Start Menu
2	DESKTOP-BR131UQ	C:\Users
4	DESKTOP-BR131UQ	\\{S-1-5-21-522249870-1839504115-1396688109-1000}
5	DESKTOP-BR131UQ	C:\ProgramData\Microsoft\Windows\Start Menu\desktop.ini
6	DESKTOP-BR131UQ	C:\ProgramData\Microsoft\Windows\Start Menu\Programs
7	DESKTOP-BR131UQ	C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Windows Ease of Access
8	DESKTOP-BR131UQ	C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Windows Accessories
9	DESKTOP-BR131UQ	C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Windows Administrative Tools
10	DESKTOP-BR131UQ	C:\ProgramData\Microsoft\Windows\Start Menu\Programs\desktop.ini
11	DESKTOP-BR131UQ	C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Settings.lnk
12	DESKTOP-BR131UQ	C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Maintenance
13	DESKTOP-BR131UQ	C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup
14	DESKTOP-BR131UQ	C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Windows System
15	DESKTOP-BR131UQ	C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Windows 10 Update Assistant.lnk
17	DESKTOP-BR131UQ	C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Windows System\desktop.ini
18	DESKTOP-BR131UQ	C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Windows System\Task Manager.lnk
19	DESKTOP-BR131UQ	C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\desktop.ini
20	DESKTOP-BR131UQ	C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Maintenance\Desktop.ini
21	DESKTOP-BR131UQ	C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Windows Administrative Tools\Component Services.lnk
22	DESKTOP-BR131UQ	C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Windows Administrative Tools\Computer Management.lnk

Windows.edb Parsing

File Report

Windows.edb Parsing

File Report

System Search

Auto-Summary

Cell contents

```
// Technique 1: CreateRemoteThread
DWORD demoCreateRemoteThreadW(PCWSTR pszLibFile, DWORD dwProcessId);

// Technique 2: NtCreateThreadEx
DWORD demoNtCreateThreadEx(PCWSTR pszLibFile, DWORD dwProcessId);

struct NtCreateThreadExBuffer {
        ULONG Size;
        ULONG Unknown1;
        ULONG Unknown2;
        PULONG Unknown3;
        ULONG Unknown4;
        ULONG Unknown5;
        ULONG Unknown6;
        PULONG Unknown7;
        ULONG Unknown8;
};
```

Windows.edb Parsing

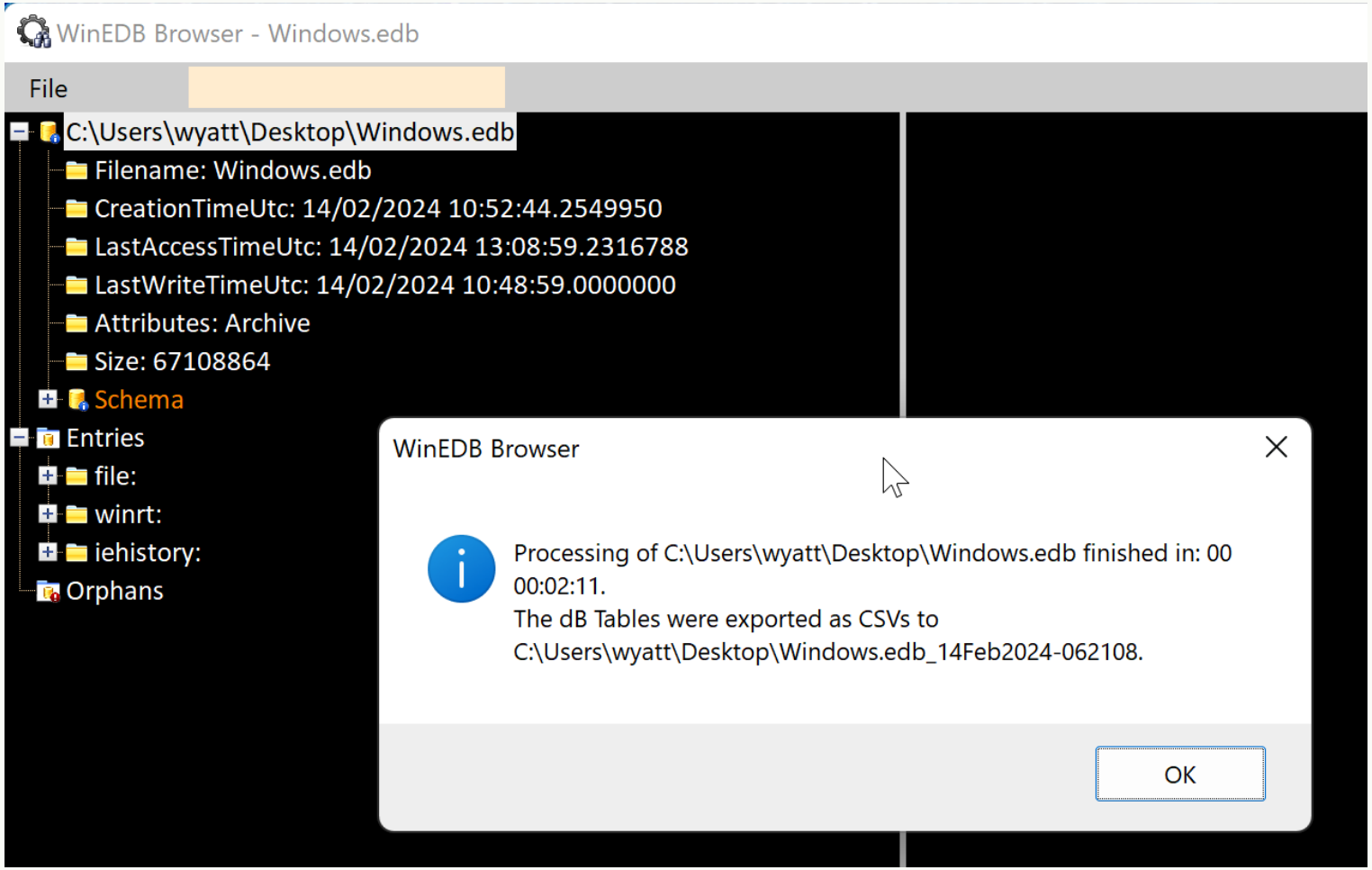
File Report

Indexed AppData directories

C:\Users\SANS_FOR526\AppData\Local\Packages\Microsoft.LockApp_cw5n1h2txyewy
C:\Users\SANS_FOR526\AppData\Local\Packages\Microsoft.LockApp_cw5n1h2txyewy\LocalState
C:\Users\SANS_FOR526\AppData\Local\Packages\Microsoft.LockApp_cw5n1h2txyewy\RoamingState
C:\Users\SANS_FOR526\AppData\Local\Packages\Microsoft.LockApp_cw5n1h2txyewy\LocalCache
C:\Users\SANS_FOR526\AppData\Local\Packages\Microsoft.LockApp_cw5n1h2txyewy\AppData
C:\Users\SANS_FOR526\AppData\Local\Packages\Windows.PrintDialog_cw5n1h2txyewy
C:\Users\SANS_FOR526\AppData\Local\Packages\Windows.PrintDialog_cw5n1h2txyewy\LocalState
C:\Users\SANS_FOR526\AppData\Local\Packages\Windows.PrintDialog_cw5n1h2txyewy\RoamingState
C:\Users\SANS_FOR526\AppData\Local\Packages\Windows.PrintDialog_cw5n1h2txyewy\LocalCache
C:\Users\SANS_FOR526\AppData\Local\Packages\Windows.PrintDialog_cw5n1h2txyewy\AppData
C:\Users\SANS_FOR526\AppData\Local\Packages\Microsoft.XboxGameCallableUI_cw5n1h2txyewy
C:\Users\SANS_FOR526\AppData\Local\Packages\Microsoft.XboxGameCallableUI_cw5n1h2txyewy\LocalState
C:\Users\SANS_FOR526\AppData\Local\Packages\Microsoft.XboxGameCallableUI_cw5n1h2txyewy\RoamingState
C:\Users\SANS_FOR526\AppData\Local\Packages\Microsoft.XboxGameCallableUI_cw5n1h2txyewy\LocalCache
C:\Users\SANS_FOR526\AppData\Local\Packages\Microsoft.XboxGameCallableUI_cw5n1h2txyewy\AppData

WinEDB Browser

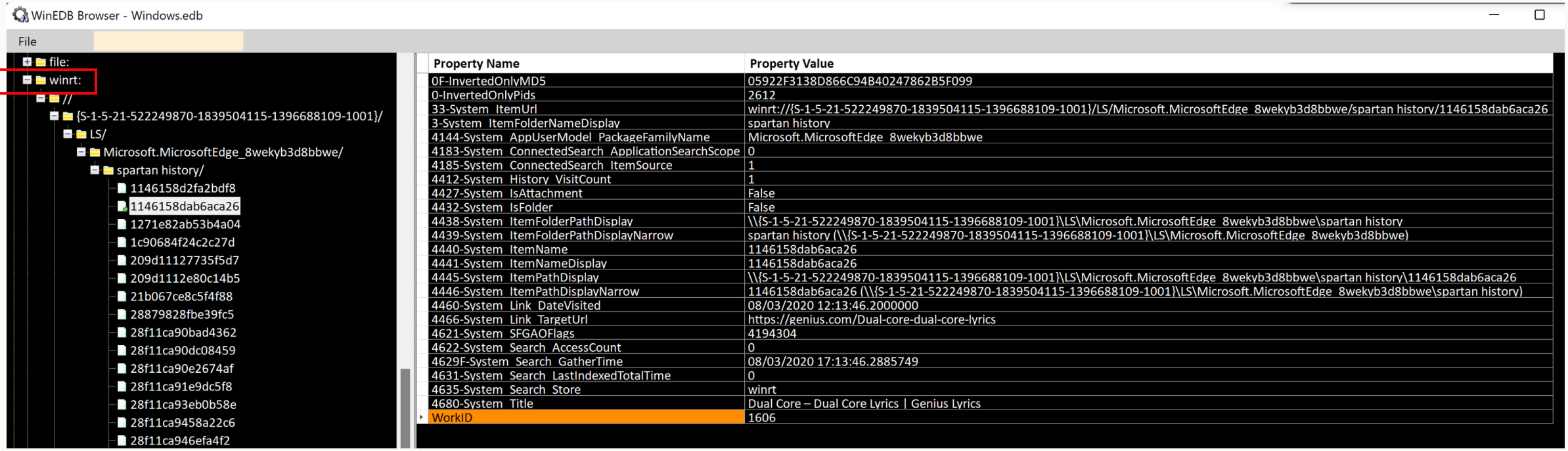
by Costas Katsavounidis



Download here: https://github.com/kacos2000/WinEDB

WinEDB Browser

by Costas Katsavounidis



Property Name	Property Value
0F-InvertedOnlyMD5	05922F3138D866C94B40247862B5F099
0-InvertedOnlyPids	2612
33-System_ItemUrl	winrt://{S-1-5-21-522249870-1839504115-1396688109-1001}/LS/Microsoft.MicrosoftEdge_8wekyb3d8bbwe/spartan history/1146158dab6aca26
3-System_ItemFolderNameDisplay	spartan history
4144-System_AppUserModel_PackageFamilyName	Microsoft.MicrosoftEdge_8wekyb3d8bbwe
4183-System_ConnectedSearch_ApplicationSearchScope	0
4185-System_ConnectedSearch_ItemSource	1
4412-System_History_VisitCount	1
4427-System_IsAttachment	False
4432-System_IsFolder	False
4438-System_ItemFolderPathDisplay	\\{S-1-5-21-522249870-1839504115-1396688109-1001}\LS\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\spartan history
4439-System_ItemFolderPathDisplayNarrow	spartan history (\\{S-1-5-21-522249870-1839504115-1396688109-1001}\LS\Microsoft.MicrosoftEdge_8wekyb3d8bbwe)
4440-System_ItemName	1146158dab6aca26
4441-System_ItemNameDisplay	1146158dab6aca26
4445-System_ItemPathDisplay	\\{S-1-5-21-522249870-1839504115-1396688109-1001}\LS\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\spartan history\1146158dab6aca26
4446-System_ItemPathDisplayNarrow	1146158dab6aca26 (\\{S-1-5-21-522249870-1839504115-1396688109-1001}\LS\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\spartan history)
4460-System_Link_DateVisited	08/03/2020 12:13:46.2000000
4466-System_Link_TargetUrl	https://genius.com/Dual-core-dual-core-lyrics
4621-System_SFGAOFlags	4194304
4622-System_Search_AccessCount	0
4629F-System_Search_GatherTime	08/03/2020 17:13:46.2885749
4631-System_Search_LastIndexedTotalTime	0
4635-System_Search_Store	winrt
4680-System_Title	Dual Core – Dual Core Lyrics | Genius Lyrics
WorkID	1606

WinRT: Windows Runtime Search Connector

Windows 11 Search

Windows.db & Windows-gather.db

Windows 11 Search Index SQLite Databases

Windows-gather.db

- SystemIndex_Gthr:
  - DocumentIDs link to SystemIndex_1_PropertyStore in Windows.db
- SystemIndex_GthrPth:
  - Contains main paths and Parent IDs linked to SystemIndex_Gthr table

Windows.db

- SystemIndex_1_PropertyStore
- SystemIndex_1_PropertyStore_Metadata

Windows-USN.db

Windows.db Parsing

SIDR - Parsing tool by Stroz Friedberg

```
sidr.exe c:\evidence\REvil\Search -f csv -o c:\cases\search
```

ay	System_Date Accessed
\Downloads\faho7-readme.txt	2021-03-16T00:02:01.9251365Z
\Favorites\faho7-readme.txt	2021-03-16T00:02:01.9271445Z
\Links\faho7-readme.txt	2021-03-16T00:02:01.9291424Z
\Music\faho7-readme.txt	2021-03-16T00:02:01.9301858Z
\OneDrive\faho7-readme.txt	2021-03-16T00:02:01.9311532Z
\Pictures\faho7-readme.txt	2021-03-16T00:02:01.9331446Z
\Saved Games\faho7-readme.txt	2021-03-16T00:02:01.9341538Z
\Searches\faho7-readme.txt	2021-03-16T00:02:01.9351889Z
\Videos\faho7-readme.txt	2021-03-16T00:02:01.9361446Z
\Downloads\ed7415b25b53b2f45b339345a7323f5d457e2102911b00952759056997bb6d42\faho7-readme.txt	2021-03-16T00:02:02.0151458Z
\Downloads\ed7415b25b53b2f45b339345a7323f5d457e2102911b00952759056997bb6d42.zip.faho7	2021-03-16T00:02:02.0201325Z
\Downloads\ed7415b25b53b2f45b339345a7323f5d457e2102911b00952759056997bb6d42_2.7z.faho7	2021-03-16T00:02:02.0221396Z
\Favorites\Bing.url.faho7	2021-03-16T00:02:02.0251472Z
\Favorites\Favorites Bar\faho7-readme.txt	2021-03-16T00:02:02.0261357Z
\Pictures\Camera Roll\faho7-readme.txt	2021-03-16T00:02:02.0271387Z
\Pictures\Saved Pictures\faho7-readme.txt	2021-03-16T00:02:02.0281461Z
\Searches\Everywhere.search-ms.faho7	2021-03-16T00:02:02.0321564Z

Use Case #1

The Real Maverick

Mountains

Target

Gif by Rodrigo de Azevedo

Auto-summary of .msg file recovered from Pete's Windows.edb:

"Iceman,

Not sure why I feel compelled to test the limits of the old F/A-18, but I do. I plan to force my team to dive dangerously low to "evade air defense radar" then swoop over the mountain's edge, swoop down into the valley, drop bombs, then swoop up again, "evading surface-to-missiles..."

Windows Search

As an Attack Surface

Windows Search Index

As an Attack Surface

Phantom DLLS

%SYSTEM%\SearchIndexer.exe

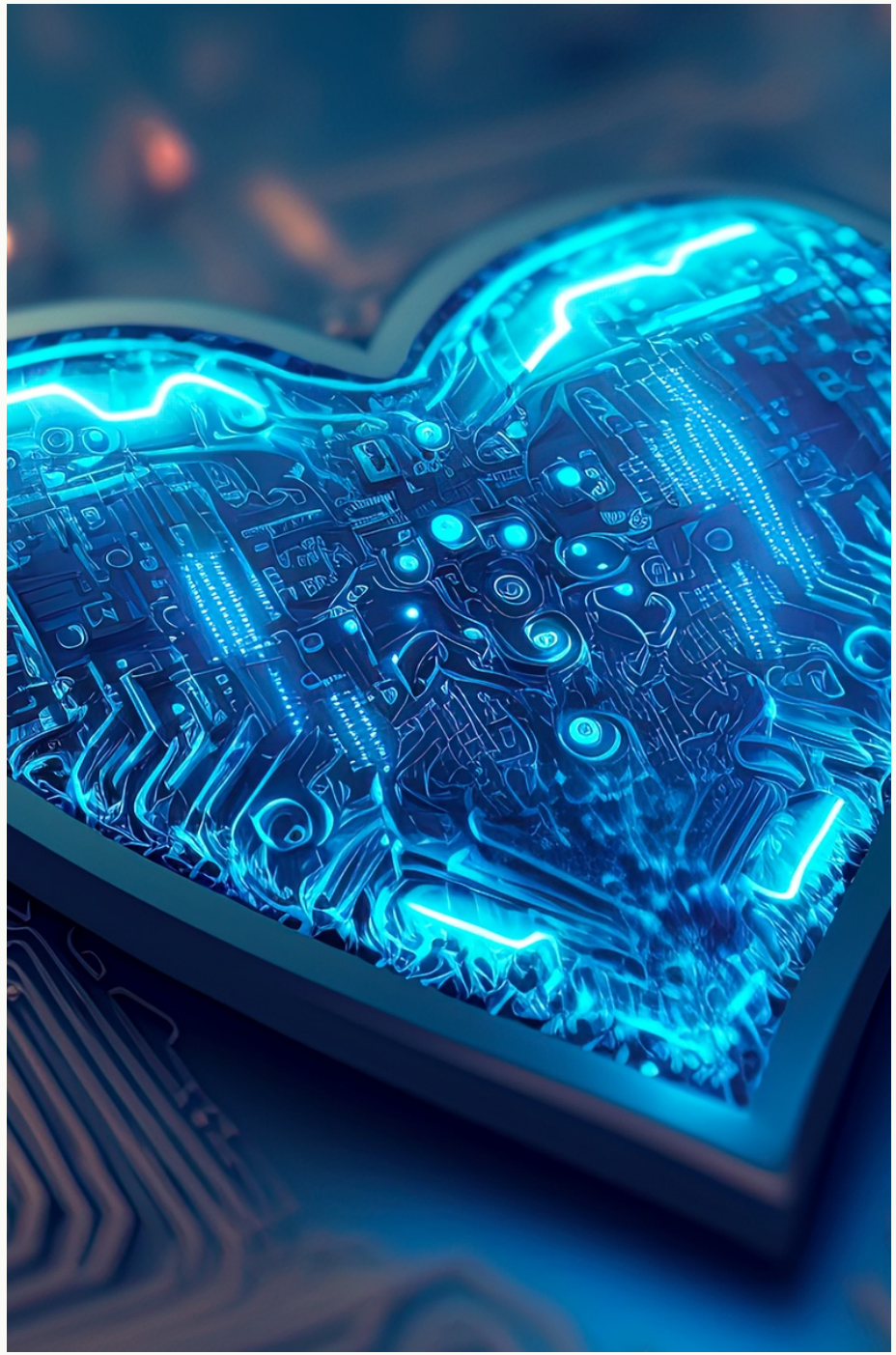
- %SYSTEM%\msfte.dll
- %SYSTEM%\msTracer.dll

%SYSTEM%\SearchProtocolHost.exe

- %SYSTEM%\msfte.dll
- %SYSTEM%\msTracer.dll

SearchNightmare Windows Search Protocol Handler: ms-search

- Opens a search window where remote malware can be executed by launching a Word Doc
- Reported by Matthew Hickey - researcher
- Chains the MS Office OLEObject vuln to the Windows search-ms protocol handler



CVE-2023-36884 Windows Search RCE

Using a specially crafted file, an attacker could exploit an RCE vulnerability existing in

Requires user action to exploit

"An attacker can plant a malicious file evading Mark of the Web (MOTW) defenses which can result in code execution on the victim system."

Summary

Highlights of the Windows Search Index

Point #1

By default, the Search Index tracks the contents of Users directories, Start Menu

Point #2

File types are defined by IFilters so specific metadata, contents can be indexed

Point #3

Location:

ProgramData\Windows\Search\Data\Applications\Windows*

Point #4

Windows 10 - Windows.edb

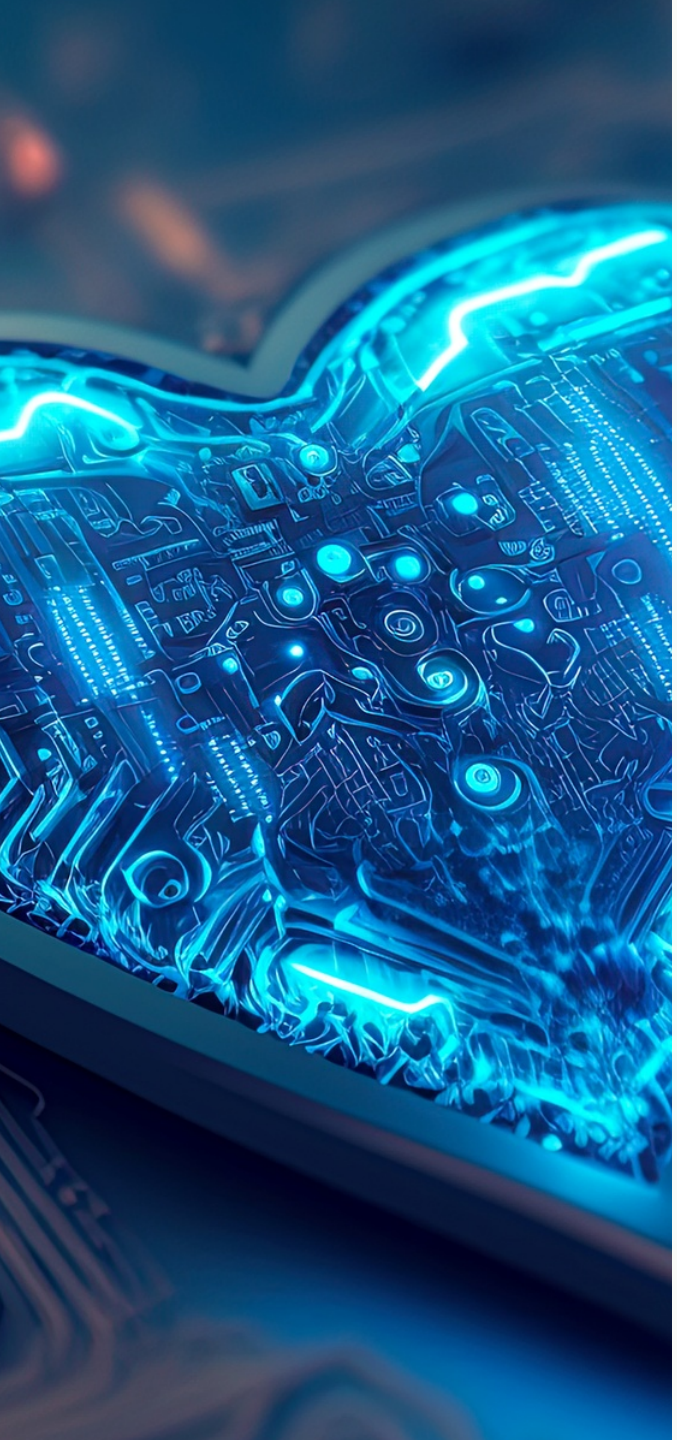
Windows 11 - Windows-gather.db, Windows.db & Windows-USN.db

Point #5

Stroz Friedberg's SIDR parses both db formats; outputs 3 files

Point #6

Consider the contents of the Search Index as highly changeable, volatile



References

- Windows Search Index: The Forensic Artifact You've Been Searching For

  https://www.aon.com/cyber-solutions/aon_cyber_labs/windows-search-index-the-forensic-artifact-youve-been-searching-for/

  Aon YouTube Video: https://youtu.be/X4WTcRdlDAM?si=BxUAMRujzhxTQf9d

- Windows App Development: Windows Search

  https://learn.microsoft.com/en-us/windows/win32/search/windows-search

- Windows Search Platform

  https://devblogs.microsoft.com/windows-search-platform/