



SearchTrace

EXPLORER

USER MANUAL



1. Introduction

SearchTrace Explorer is a digital forensic analysis application designed to parse and visualize Windows Search Index databases (windows.db and windows-gather.db).

It enables forensic practitioners and investigators to explore metadata relating to indexed files, system activity, and search gatherer events.

The tool provides:

- Indexed item browsing for both windows.db and windows-gather.db
- Accurate parent-path reconstruction
- Raw property store extraction (PS_All)
- Evidence bookmarking with notes and selected raw properties
- CSV/JSON export capabilities for reporting or offline review
- Timeline activity graphing
- Dashboard summaries of database contents

2. System Requirements

Operating System

- Windows 10 / 11
- .NET 8 Runtime Installed

Important Handling Notice

The program should always be run on a *copy* of the search database files and *not* the original system files.

This is because:

- The program does **not modify any original Windows tables**,
- **But it does create additional helper tables** inside the SQLite file (required for export, decoding, and indexing functions).

Running on a forensic clone or disk image copy is recommended.

3. Location of Database Files

"C:\ProgramData\Microsoft\Search\Data\Applications\Windows"

Note – Sometimes when extracting the db file from a mounted forensic image in read only mode it may result in the db file being unable to be loaded into the program. Mounting the forensic image in write mode can resolve the issue.

4. User Interface Overview

Dashboard

Provides at-a-glance statistics:

- Total indexed records
- Database type
- Evidence count
- Last loaded state

Windows.db Explorer

Primary indexed-file viewer with:

- Search filters (top-level + deep property search)
- Reconstructed file names and paths
- Multiple timestamp columns
- Reordering and resizing of columns

Gather Explorer (windows-gather.db)

Displays gatherer pipeline entries:

- Fully reconstructed paths via Scope chain
- Decoded TransactionFlags
- File names extracted from gatherer metadata
- Lightweight filter (top-level search)

Timeline View

Shows visual activity distribution across timestamps.

Item Details View

Allows:

- Bookmarking items
- Adding investigator notes

- Selecting raw PS_All properties
- Persisting items in a .evidence.json file
- Exporting bookmarked-only output

Export View

Exports:

- Current page only
- All filtered results
- Bookmarked-only evidence

Options include:

- CSV / JSON
- Timestamp formats (UTC | Local)
- Workld-only export
- Include/exclude paths and timestamps

Settings/About View

Option:

- Set Default timestamp column for sorting

5. Loading a Database

Windows.db

1. Navigate to Windows Explorer view.
2. Enter the path to your database copy.
3. Click **Open Database**.

windows-gather.db

1. Navigate to Gather Explorer.
2. Enter the file path.
3. Click **Open Database**.

Evidence state is stored separately for each DB file:

windows.db.evidence.json

windows-gather.db.evidence.json

These load automatically on re-open.

6. Searching & Filtering

Windows.db

Supports:

- **Top-level search** (ItemName, PathOrUrl, ItemPathDisplay)
- **Deep FTS search** across PS_All values

Gather.db

Current version supports:

- **Top-level search** only
-

7. Evidence Features

Double Click a Row

To view all raw properties associated with an entry in the Windows.db double click the row to go directly to Item Details View

Bookmarking

Click the  icon to add/remove bookmarks.

Notes

Each evidence item supports investigator notes.

Raw Properties

Users may include selected PS_All properties for export.

Evidence Persistence

Evidence is automatically saved per database file.

Export

Bookmarked-only export supports:

- Notes
- All timestamps
- All selected raw properties

8. Exporting Data

Generic Export (Windows.db / Gather.db)

Export:

- Current page
- All filtered results

Gather-specific Export

Includes additional metadata fields:

- ScopeID
- SDID
- AppOwnerID
- RequiredSIDs
- DeletedCount
- **Decoded TransactionFlags**
- FileName
- EffectivePath

Evidence Export

Exports only user-marked forensic items.

Contains:

- WorkId / DocumentID
- Paths
- File names
- Timestamps
- Notes
- All selected PS_All properties

9. Data Integrity Notes

The program **DOES NOT** modify the original Windows-created tables.

However:

✓ The program **WILL** create additional tables inside the copied DB file.

These internal tables are used for:

- Export consolidation
- Path reconstruction
- Property normalization
- Transaction flag decoding

Because of this, the application **must not be run on original system DB files**, only forensic copies.

Export Behavior

- All exported metadata is based on data present in the index
- No alteration to original record values
- No timestamps or field content are modified during export

10. Error Handling

Common issues:

Error	Explanation
"No DB loaded"	Attempted export without an open DB
SQLite Error: no such table	Wrong file type or incorrect DB provided
404 Not Found	Incorrect dbKind switching (windows vs gather)
Access denied	Opening DB copy from protected directories

11. Licensing Terms

SearchTrace Explorer – Freeware License Agreement (Closed Source)

Version 1.0.0

Developed by Andrew Smith

1. Grant of Use

SearchTrace Explorer is provided free of charge as closed-source software.

You are granted a non-exclusive, non-transferable, revocable license to use the software subject to the terms of this agreement.

Permitted Uses

You may use this software for:

- Internal organisational use
- Personal or academic forensic research
- Training and education
- Internal investigations, casework, and reporting
- Internal operational or analytical workflows
- Professional and commercial services, including but not limited to:
 - Digital forensic investigations
 - Incident response and breach analysis
 - Expert witness work
 - Investigative reporting
 - Consulting or advisory services

You may charge clients or third parties for professional services performed using the software, provided that:

- The software itself is not sold, licensed, rented, or otherwise provided to clients
- Clients are charged for services and professional expertise, not for software access
- Clients do not receive copies of the software
- Clients do not gain interactive access to, or operational control of, the software

Prohibited Uses

This license expressly does not permit:

- Selling, licensing, or monetising the software itself
- Redistributing, sublicensing, or transferring the software to third parties
- Providing the software as a hosted service or Software-as-a-Service (SaaS)
- Allowing third parties to directly operate, access, or control the software
- Bundling the software with paid products, platforms, or toolkits
- White-labeling, rebranding, or presenting the software as your own
- Reverse engineering, decompiling, disassembling, or attempting to derive source code

Commercial Software Distribution

Any use involving:

- Sale or licensing of the software
- Distribution to third parties
- Integration into commercial products
- Offering the software as a forensic platform or service

requires explicit prior written permission from the author.

2. “As-Is” Disclaimer

THIS SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO:

- MERCHANTABILITY
- FITNESS FOR A PARTICULAR PURPOSE
- NON-INFRINGEMENT
- ACCURACY, COMPLETENESS, OR RELIABILITY OF OUTPUT
- SUITABILITY FOR LEGAL, EVIDENTIARY, OR COURT USE

Users are solely responsible for independently validating all results, findings, and conclusions generated by the software.

3. Limitation of Liability

IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, CONSEQUENTIAL, OR SPECIAL DAMAGES ARISING FROM:

- Use or misuse of the software
- Inability to use the software

SearchTrace Explorer – User Manual - Version 1.0.1

- Errors, omissions, or inaccuracies in forensic interpretation
- Loss, corruption, or exposure of data
- Incorrect analysis, reporting, or conclusions
- Reliance on outputs for legal, evidentiary, or operational decisions

Use of the software is entirely at the user's own risk.

4. Evidence Handling and Legal Responsibilities

The user is solely responsible for:

- Maintaining proper forensic chain-of-custody
- Ensuring compliance with applicable laws, regulations, and professional standards
- Verifying timestamps, metadata, and artefact interpretations
- Determining the admissibility and appropriateness of evidence in legal or regulatory contexts

The software does not replace professional judgment or legal expertise.

5. Redistribution

Redistribution of this software, whether in original or modified form, is strictly prohibited without explicit written permission from the author.

This includes, but is not limited to:

- Public or private redistribution
 - Sharing within third-party organisations
 - Inclusion in tool collections or forensic distributions
-

6. Acceptance of License

By installing, copying, or using SearchTrace Explorer, you acknowledge that you have read, understood, and agree to be bound by the terms of this license agreement.

If you do not agree to these terms, you must not use the software.

SearchTrace Explorer is freeware. This license governs all use of the software.

12. About This Manual

This manual describes **SearchTrace Explorer v1.0.0**.

Features, UI layout, and capabilities are accurate as of this release.