



User Guide

Digital Forensics & Investigation Platform
Version 1.0.0-beta
Developed by Rodel Plasabas
October 2026

Contents

Introduction

Installing VESTIGEX

- What you need

- Install

- Upgrading

- Uninstalling

Getting started

- Signing in

- Examiner accounts

- Creating or opening a case

- The main window

Adding and processing evidence

- Adding evidence

- Processing evidence

- Jobs

- Re-extracting artifacts

Browsing evidence

- Data Sources

- File System

- The file viewer

- File Types

- Deleted & Carved

- Tables, sorting and filters

Searching

- Keyword Search

- Hash Sets

- YARA Rules

Analysis

- Timeline

- Connections

- Media Analysis

- AI Investigation

Artifacts

- Registry, OS Artifacts and Web History

- Messaging

- Email

- Memory

- Mobile

- SQLite Databases

- Credentials

Threat hunt

Review and reporting

- Bookmarks and review status

Refined Results

Reports

Audit Log and chain of custody

Settings

Setting up the local AI

Troubleshooting

Where things are kept

Introduction

VESTIGEX is a digital forensics and investigation platform for Windows. It opens disk images, triage collections, phone extractions, memory dumps and log files, extracts what the evidence holds (files, deleted files, registry, browser history, chats, e-mail, photos and more) and helps you search, review and report on it. Everything runs on your own computer: no evidence, search or AI question leaves the machine.

Results produced automatically (detections, picture categories, AI answers, translations, scores) are leads for an examiner to review, never conclusions on their own. Always confirm them against the evidence before you rely on them.

Installing VESTIGEX

What you need

- Windows 10 (version 1809 or later) or Windows 11, 64-bit.
- About 12 GB of free disk space for the program, plus room for your cases (a case folder can grow to a sizable fraction of the evidence it holds).
- 16 GB of RAM or more is recommended; 32 GB for large cases.
- An NVIDIA graphics card is optional. With one, photo scanning, OCR and speech-to-text run on the GPU; without one they run on the processor, more slowly.
- Windows 11 includes the Edge WebView2 runtime that VESTIGEX uses for reports. Windows 10 may need it installed from Microsoft.

Install

1. Copy the whole `VESTIGEX-<version>` folder to the computer. Keep `Install VESTIGEX.cmd`, `vestigex.zip` and `OllamaSetup.exe` together.
2. Close VESTIGEX if an earlier version is open.
3. Double-click **Install VESTIGEX.cmd** and answer **Y** to install.
4. VESTIGEX unpacks into `%LOCALAPPDATA%\Programs\VESTIGEX` (about 11 GB, several minutes). No administrator rights are needed.
5. When asked, choose whether to install **Ollama** (needed for the local AI features) and whether to start VESTIGEX.

Setup adds **VESTIGEX** to the Start menu and the desktop, a **VESTIGEX logs** shortcut and an entry in Windows **Settings > Apps**.

This installer works with Windows Smart App Control turned on. The wizard version (`VESTIGEX-Setup-<version>.exe`) only runs on computers where Smart App Control is off, until it is signed with a code-signing certificate.

Upgrading

Run the new version's **Install VESTIGEX.cmd**. It replaces the program files and keeps your user accounts, AI and processing settings, hash sets and organization logo. Cases are stored wherever you created them and are never touched by setup.

Uninstalling

Use **Settings > Apps > VESTIGEX > Uninstall** or the **Uninstall VESTIGEX** Start menu shortcut. You are asked whether to keep or delete the user accounts and settings. Cases are never deleted.

Getting started

Signing in

VESTIGEX opens on a sign-in screen. A new installation has one administrator account:

- User name: **admin**
- Password: **admin**

You must choose a new password the first time you sign in. Sessions end after 12 hours without activity, and five wrong passwords lock an account name for one minute.

Use the **user menu** (your name in the top bar) to change your password or sign out. Signing out closes the open case and asks first if background work is still running.

Examiner accounts

Administrators manage accounts in **Settings > Users** (or the **Users** button on the open-case screen):

- **Create** an account with a temporary password; the examiner sets their own at first sign-in.
- Change the display name or the role (**Examiner** or **Administrator**).
- **Reset** a password (signs that user out everywhere), or **disable** and enable an account. At least one active administrator is always kept.
- **Sign-in activity** lists successful and failed sign-ins and account changes with the source address.

The signed-in examiner's name fills the Examiner field of new cases and is written into every chain-of-custody entry.

Creating or opening a case

After signing in you choose a case:

- **Create New Case:** give the case a name, the examiner, organization, description, the **case type** and a folder. VESTIGEX creates `case.vestigex` and the case database `vestigex.db` in that folder.
- **Open Existing Case:** pick a case folder or its `case.vestigex` file.

The **case type** decides which checks **Refined Results** runs: Compromise assessment / incident response, Insider data theft, Employee misconduct, Fraud & financial crime, Harassment, threats & cyberbullying, Sexual exploitation & voyeurism, Violence & threats to life, Litigation & e-discovery, or General. You can change it later in **Case Management > Edit Case**.

When a case opens, VESTIGEX compares each data source's files, sizes and modified times with what was recorded at intake and warns if evidence changed or is missing.

The main window

- **Sidebar:** every screen, grouped as Overview, Evidence, Search, Analysis, Artifacts, Threat Hunt and Reporting. The ☰ button collapses it.

- **Top bar**: the open case, counters (artifacts, events, findings, critical/high, bookmarked), the **date range**, the **data source filter**, ★ **snapshots**, your user menu and **Close Case**.
- **Status bar** (bottom): backend health, index and hash status, running jobs, the AI model, and the version. Click the version to open **About VESTIGEX**.

The **date range** limits findings, the timeline, artifacts, lateral movement and processes to an inclusive range, in the display time zone. The **data source filter** shows only the evidence of the ticked sources. A **snapshot** saves the current date range and source filter under a name (for example "Initial access window") so anyone on the case can return to it.

Adding and processing evidence

Adding evidence

Go to **Evidence > Data Sources** and press **+ Add evidence**. The wizard asks three things:

1. **Category**: Computer, Mobile, Memory or Logs.
2. **Platform**: Windows, Mac, Linux, Android or iOS.
3. **Evidence type**, for example:

Category	Evidence types
Computer	Disk image (E01, raw/dd, VHD/VHDX, VMDK, DMG ...), files and folders, KAPE / Velociraptor / UAC collection, Mac logical .zip
Mobile	Full file system (zip / tar / folder), iTunes / Finder backup, Cellebrite UFDR
Memory	RAM dump (.mem, .raw, .vmem, .dmp), page file, swap file, hiberfil.sys
Logs	Windows event logs, web server logs, Plaso timelines and other log files

The file picker only shows matching files. Before adding, VESTIGEX opens the evidence and tells you what it found (for example "macOS 15.4 (24E248) · Alexs-MacBook-Pro") and warns if it is not the platform you chose. Give each source a clear label, usually the host or device name.

Encrypted **iTunes / Finder backups** ask for the backup password when added; it is checked and kept in memory only. A disk image with a locked **BitLocker** volume stops with an unlock box on the data source: enter the recovery key (eight groups of six digits) or the password, and VESTIGEX checks it and queues the image again.

A data source can be **renamed** at any time and **removed** only before it is processed (or after processing failed).

Processing evidence

Press **Process Evidence**. A dialog lets you choose what runs, showing only the steps that apply to the waiting sources:

- File hashing and hash set lookup, deleted files, the keyword index
- Event and web logs, threat hunt, YARA
- Registry, OS artifacts, web history, e-mail, photo EXIF, messaging apps, encrypted files, stored credentials
- Volume Shadow Copies, page files, memory analysis
- Media: speech-to-text and OCR
- macOS: mac_apr artifacts and (optionally) Unified Logs

Presets: **Everything**, **Suggested for this case type** and **Quick triage**. Your last choice is remembered and recorded in the audit log. Phone extractions always run in full.

Before reading a source, VESTIGEX hashes it (MD5 and SHA-256) for the chain of custody. Disk images are hashed as one stream over all segments, matching imaging tools.

Processing runs in the background. Several data sources are processed at the same time, and within each source files are hashed and have their text extracted several at a time (8 by default), also inside disk images and other containers: each worker opens the evidence itself. Both numbers are set in **Settings > Processing**.

Jobs

Overview > Jobs (also from the status bar) lists every background job with a progress bar, the current step, elapsed time and a log of its steps. Processing shows one sub-job per data source. **Cancel** stops a job; cancelling one data source sends just that source back to pending.

Re-extracting artifacts

Every artifact screen has a **Re-extract artifacts** button for sources processed by an earlier version, so improved parsers can be applied without processing everything again.

Browsing evidence

Data Sources

Each source shows its type, platform, status, file counts and evidence hashes. **Verify** re-hashes the evidence and compares (verified, HASH MISMATCH or missing). **System information** shows what was read from the source: computer name, operating system and build, time zone, users, network interfaces and known Wi-Fi networks (Windows, macOS and Linux).

File System

A folder tree of every volume in every source, with the files of the selected folder in a table. Volume Shadow Copies (when processed) appear as their own volumes labelled with their creation date.

The file viewer

Selecting a file opens its detail pane. Depending on the file, it has these tabs:

- **Hex** and **Text**: the raw content.
- **Extracted text**: the text indexed for keyword search.
- **Metadata**: names, sizes, MACB times, hashes, signature, hash set and YARA matches, and the review panel.
- **Document**: PDF, Word (with tracked changes and comments), Excel (with hidden sheets flagged), PowerPoint (with speaker notes), CSV, HTML, RTF and property lists. Everything except PDF is rendered by VESTIGEX in a sandbox that blocks scripts and network access.
- **Preview**: pictures, including HEIC/HEIF and AVIF. Photos with GPS show their location; the map loads only when you ask, because loading it contacts OpenStreetMap.
- **Video / Audio**: a player that streams the file read-only from the evidence.
- **Video check**: what the video container records (camera, editing software, creation time, GPS, structural oddities).
- **Registry**: browse a registry hive's keys and values.

Export file saves a copy; the export is recorded in the audit log. ★ **Bookmark** adds the file to the case's bookmarks.

File Types

Files grouped by what they are (pictures, videos, audio, documents, archives, executables ...), identified by their content signature, not their extension. A mismatch between extension and content is flagged. Pictures and videos have a **Gallery** view: thumbnail sizes S / M / L, arrow keys move, **B** bookmarks the selected item.

Deleted & Carved

- **Deleted**: files whose MFT records (NTFS) or directory entries (FAT/exFAT) are marked deleted.

- **Carved:** press Carve to recover JPEG, PNG, GIF, PDF and ZIP / Office files from unallocated space (all unallocated space by default, or free space in file systems only). Carved files become a "(carved)" data source and are hashed, typed and indexed like any other file. Deleted NTFS MFT records found in free space are listed under OS Artifacts > Carved MFT records.

Tables, sorting and filters

All file and artifact tables work the same way:

- Click a column header to sort; click again to reverse, a third time to clear.
- Type in the filter row under the headers to filter that column. Filters run on the whole case, not only the rows on screen.
- Drag a header edge to resize a column; double-click it to reset. Widths are remembered.

Filter	Examples
Text	invoice (contains)
Size	> 1 MB , 1MB-5MB
Date	2024-05 , > 2023 , 2024-01..2024-03
Deleted	Yes / No

Searching

Keyword Search

Search every file's text and every log event. Choose **Words**, **Exact phrase** or **Regex**. **Keyword lists** run a saved list of terms (for example the built-in e-mail address pattern) across the case; **Save and run** stores a list for later. If the index has not been built yet, **Index now** builds it.

Hash Sets

Import known-file and alert hash sets (MD5, SHA-1 or SHA-256 lists, NSRL RDSv3 SQLite databases, and Project VIC / CAID VICS JSON exports with their categories). Matching files are listed per set and marked in their metadata. Hash sets are shared by every case on this installation.

YARA Rules

A rule library shared by all cases: import a `.yar` file or a folder of rules, or write rules in place (each is checked before saving), and switch rule files on or off. Enabled rules run during Process Evidence and on carved files; **Scan case files** rescans the whole case. Matches show the rule, severity, matched strings and offsets.

Analysis

Timeline

Every log event, parsed artifact and file system time in one table, built at the end of processing. Filter by source type, host, text and "detections only", or with the column filters; the histogram shows activity per day (or per hour) and clicking a bar zooms in. Rows open the event, artifact or file in place, and log events can be bookmarked from their pop-up.

Connections

E-mail addresses, phone numbers, accounts, IP addresses and web domains collected from every parsed artifact and linked when they appear in the same records. Pick an entity to centre it in a graph with the data sources it appears in and everything it shares records with. Click a linked entity or a line to see the records behind the link, with the shared values highlighted. Drag nodes to untangle the graph; **Reset layout** puts them back.

Media Analysis

Scan Photos runs offline over every photo and five frames of every video:

- **Skin / nudity** (NudeNet, double-checked by CLIP), **Weapons** (CLIP) and **AI-generated** (labels inside the file such as C2PA content credentials or generator settings, plus a UniversalFakeDetect score).
- **Picture categories**: documents and receipts, ID cards and passports, screenshots, cash and bank cards, drugs, vehicles and plates, maps and locations, children.
- **Near-duplicate pictures**: the same image resized, recompressed or lightly edited.

Each list has a **minimum score** filter and a **List / Gallery** view. With **Blur** on, thumbnails stay blurred until you select one; click the open photo again to blur it again.

Check with local AI shows each hit at or above the minimum score to the local vision model with one narrow question and records its answer: confirmed (AI ✓), rejected (AI X) or unsure (AI ?), with a one-line description. The **AI check** filter hides rejected hits by default. Nothing is deleted and the detector score is kept.

Read text & speech transcribes audio and video (Whisper, in the original language with timestamps) and reads text in pictures and scanned PDFs (OCR). Both are added to Keyword Search and the IOC sweep.

AI Investigation

Ask questions about the case in plain language. The local model answers from the case data and cites what it used: findings, events, files and artifact records. Click a citation to open the exact record; citations the model could not back with evidence are marked unverified. Conversations are kept with the case. Configure the model in **Settings > Local AI**.

Artifacts

Registry, OS Artifacts and Web History

Parsed records, grouped by artifact with counts. Windows examples: run keys, services, UserAssist, ShellBags, USB devices, ShimCache, Amcache, BAM, Prefetch, LNK files, Jump Lists, Recycle Bin, scheduled tasks, PowerShell history and script blocks, SRUM, Windows Timeline, Defender, remote-access tools, encrypted and password-protected files. macOS (through mac_apr and VESTIGEX's own parsers): KnowledgeC, Biome, quarantine events, TCC permissions, FSEvents, Unified Logs, Notes, iMessage, Wi-Fi and more. Linux: users, shell history, authentication logs, logins, cron, services, syslog and the journal. Web History covers browsers (per browser) and cloud storage clients (OneDrive, Google Drive, Box Drive, Dropbox).

Each record's detail pane shows every field, the review panel, ☆ **Bookmark** and ♦ **Ask AI**.

Messaging

Chats from computers (Skype, Viber, Teams, Slack, WhatsApp Desktop, Discord) and from each phone (SMS, iMessage, WhatsApp, Telegram, Signal ...), shown as conversations with message bubbles or as a table. **Read chats with AI** gives each message its language, an English translation and topics (threats, weapons, drugs, money, sexual content, minors, meetings, self-harm, fraud, hiding evidence and your own topics); topic chips filter the conversations.

Email

Messages from .eml , .mbox , Outlook PST / OST and .msg files, with attachments.

Memory

RAM dumps and hiberfil.sys are analysed offline with Volatility 3: processes (including unlinked and exited ones), command lines, DLLs, network connections, services, injected code and registry hives. Every memory file's text goes into Keyword Search, and its URLs, IP and e-mail addresses are listed with counts.

Mobile

One tab per phone with its device details (name, model, OS, number, IMEI, serial), then the artifacts in ALEAPP / iLEAPP's own categories: accounts, apps, locations on a map, Wi-Fi, browser, photos metadata and more. Cellebrite UFDR imports appear the same way.

SQLite Databases

Every SQLite database in the evidence, found by signature, grouped by the app it belongs to. Browse tables with sorting and search. 🔄 **Recovered records** lists deleted rows recovered from free pages, free space inside pages and the write-ahead log.

Credentials

Local account password hashes (SAM), LSA secrets and saved browser passwords. Values stay masked until revealed. Local hashes export in pwdump format for your own offline tools, and the export's SHA-256 is written to the audit log.

Threat hunt

- **Findings:** detection rules run against the log events, grouped by severity with MITRE ATT&CK techniques and the matching events. Open the evidence viewer to page through every event.
- **Lateral Movement:** logons and remote connections between hosts drawn as a graph, notable connections first (failed logons, RDP, explicit credentials, admin shares, service installs). Click a line to see its accounts, logon types and time span.
- **Process Inspector:** process creation events as a tree.
- **Detection Rules:** the rules the threat hunt uses, with an editor to add or change your own.
- **IOC Hunting:** IPs, domains, URLs, e-mail addresses and file hashes typed or imported from text, CSV, STIX 2 or MISP. **Sweep** looks for every IOC across file hashes and names, artifacts, chats, memory, file contents and log events.
- **ATT&CK & IOCs:** findings laid out by ATT&CK tactic and technique, with the IOC sweep results beside them.

Review and reporting

Bookmarks and review status

Bookmark files, artifact records, chat messages, phone records and log events with ☆ **Bookmark**, and add a note to each. **Reporting > Bookmarks** lists them all. Any record or file can also be marked **Relevant**, **Follow up** or **Not relevant** with comments for the team; each change records who and when.

Refined Results

For the case type, a set of checks pulls together the evidence that usually matters in that kind of case (for example USB devices and cloud uploads for insider data theft). Results follow the date range and source filter; **Show all** loads every item and ↺ **Refresh** recomputes.

Reports

- **Case report** as HTML, PDF (printed by Microsoft Edge so it looks the same), Word or Excel. Choose the findings and sections to include; the report follows the date range, source filter and display time zone.
- **Draft with AI** writes an executive summary from the report's data only. You edit it, and the report states that AI assisted unless you mark it as rewritten.
- **Portable case**: a zip for a lawyer, investigator or supervisor without VESTIGEX. It opens in any browser with no internet: case summary, evidence hashes, findings, bookmarked and reviewed items with copies of the files. The reviewer marks items and comments, then sends back a small review file that you import with **Import review**.

Every report is saved in the case's reports folder and its SHA-256 is written to the audit log.

Audit Log and chain of custody

Reporting > Audit Log is the case's hash-chained activity log: every examiner action with time (UTC), examiner and details (case opened and closed, sources added, jobs and their results, bookmarks, exports, reports). Each entry stores the hash of the previous one, so editing or deleting an entry is detected. Filter by text, action, examiner and date, and export as CSV.

Settings

- **Backend:** the address of the VESTIGEX backend (normally left as it is).
- **Appearance:** themes (Graphite, Dim, Light, Blue, Green, Dark Coffee, Coffee, Pink or Match Windows).
- **Users:** examiner accounts (administrators only).
- **Organization logo:** replace the VESTIGEX mark with your organization's PNG, JPEG, WebP or GIF logo (up to 2 MB).
- **Processing:** how many data sources are processed at the same time, and how many files within a source are hashed and have their text extracted at the same time (default 8).
- **Time:** the display time zone for every timestamp (UTC by default).
- **Local AI:** the model server (**Ollama**, or an OpenAI-compatible server such as LM Studio), the model, the context window and reasoning. **Test connection** checks it. Picture checks need a model that can see images (for example Gemma 3 or 4, Qwen-VL or LLaVA).

Setting up the local AI

1. Install Ollama (offered by setup, or from ollama.com).
2. Download a model, for example in a Command Prompt: `ollama pull gemma3:12b`. Choose a size that fits your graphics card's memory.
3. In **Settings > Local AI**, choose Ollama, pick the model and press **Test connection**.

Troubleshooting

Problem	What to do
Starting VESTIGEX again does nothing new	Only one VESTIGEX can run; starting it again brings the open window to the front. Setup refuses to run while VESTIGEX is open.
Windows blocks the setup wizard	Smart App Control is on. Use Install VESTIGEX.cmd instead.
VESTIGEX does not start	Open the VESTIGEX logs shortcut and check <code>backend.log</code> .
Photo scanning or OCR is slow	Without an NVIDIA GPU these run on the processor. Close games or other GPU-heavy programs.
AI features say the model is not reachable	Start Ollama, then Settings > Local AI > Test connection .
"This image has an encrypted volume that is still locked"	Enter the BitLocker recovery key or password on the data source.
Processing on a slow external or hard disk	Copying the evidence to an SSD first makes processing much faster.

Where things are kept

What	Where
Program	%LOCALAPPDATA%\Programs\VESTIGEX
Accounts, settings, hash sets, YARA rules	%LOCALAPPDATA%\Programs\VESTIGEX\backend\data
Logs	%LOCALAPPDATA%\Programs\VESTIGEX\logs
A case	the folder you chose: case.vestigex , vestigex.db , reports and caches