Factium — Digital Forensics Workbench

> **Every byte tells a story — DigitalHound listens.**



DigitalHound is an all-in-one **computer forensic analysis platform** for law enforcement, forensic laboratories, corporate investigations, incident response, and authorized research. Built on a deeply customized **SleuthKit (libtsk)** core, it carries investigators from **disk image ingestion** through **filesystem exploration**, **artifact parsing**, **timeline review**, **AI-assisted triage**, and **court-ready reporting**—on a single workstation, with **no mandatory cloud dependency**.

Companion utility: disk imaging workflow in the spirit of FTK Imager (free imaging tool in the same product family).

Why Factium

Challenge	How DigitalHound helps
Too many tools, too many exports	One case folder, one SQLite case database, one UI for browse → scan → review → report
Re-scanning wastes time	Scan sessions and artifacts persist in `case.db`; reopen cases and filter by session
Analysts drown in noise	Modular scan catalog (480+ modules), keyword hits, bookmarks, timeline correlation
Sensitive data must stay local	Offline-first design; local AI (GGUF) keeps evidence on the machine
Cross-platform images	Windows, Linux, and macOS artifact modules in a unified catalog
Disclosure and testimony	HTML/PDF/CSV exports, audit log, bookmarks with severity, image hashing

---

Who it is for

Audience	Typical use
Law enforcement & cybercrime units	Electronic evidence examination, case building, disclosure
Forensic laboratories	Repeatable analysis, expert reports, peer review
Corporate security, legal, HR	Insider threat, IP theft, policy violations (with proper authorization)
Incident response	Ransomware and intrusion scoping on acquired images
Education & research	Transparent, auditable forensic toolchain

DigitalHound is intended for lawful, authorized investigations only. Operators are responsible for compliance with applicable laws and organizational policy.

Investigation workflow

```
Create case  →  Add evidence (E01/DD/VHD/…)  →  Browse & preview
      ↓
Automated / modular forensic scan  →  Results tree + timeline + search hits
      ↓
Bookmarks, maps, viewers (registry, SQLite, mail, IM)  →  Export report
      ↓
Archive case folder (.dhcase + case.db) for retention
```

1. **Open or create a case** — structured metadata, evidence list, audit trail
2. **Load disk images** — E01, DD, RAW, VHD/VHDX, VMDK, QCOW, AFF4 (via integrated libraries)
3. **Browse evidence** — partitions, directories, deleted content, hex/text/image preview

4. **Run forensic analysis** — comprehensive scan with 480+ selectable modules, or targeted jobs
5. **Review findings** — AXIOM-style forensic module tree, artifact analysis, unified timeline
6. **Persist automatically** — SQLite `case.db` for reopen, session filter, lazy timeline load
7. **Report** — HTML, PDF, CSV, KML (GPS), bookmarks

Core capabilities

Forensic engine

- **Source-level integration** of libtsk, libewf, libvhdi, libvmdk, libqcow, libpff—not a thin wrapper
- **NTFS, FAT, exFAT, HFS+, APFS, ext2/3/4**, and other filesystems supported through TSK
- **Deleted and unallocated** content accessible where the filesystem exposes it

Modular artifact catalog

- **480+** selectable scan modules grouped by **platform** (Windows, Linux, macOS) and **category**
- Categories include persistence, execution, browsers, network, security, filesystem, credentials, cloud/remote, documents/media, and user activity
- **Unified case database** modeled after industry practice (Autopsy / Magnet AXIOM style): artifacts, attributes, timeline events, keywords, scan sessions

Timeline & search

- Events aggregated into `dh_timeline_events` with a dedicated **Timeline View** (large-case friendly loading)
- **Keyword and content search** with a dedicated hits panel
- Optional **timeline correlation** to surface dense or anomalous activity windows

Communication & credentials

- **Email:** PST/OST-oriented workflows, Foxmail, and related stores
- **IM & chat:** WeChat, QQ, DingTalk, Feishu, Telegram Desktop, Discord, Signal, Skype, Teams, Zoom, and more (module-dependent)
- **Credentials:** browser stores, Wi-Fi profiles, SSH, DPAPI-related material, KeePass, wallets (breadth varies by module)

Threat hunting & anti-forensics

- Defender and security logs, persistence (tasks, WMI, COM, services), log-clearing indicators
- Signature mismatch, high-entropy and encrypted-container detection, duplicate hashing, carving support where enabled

Viewers & specialists tools

- Registry, SQLite, Plist, ESE, hex, strings, prefetch, USN journal, boot sector, write-protect utilities, live response collection (environment-dependent)
- **GPS track map** (Leaflet) with **KML export** from EXIF and related artifacts

Multilingual product UI

- **English, Simplified Chinese, Japanese, Korean** — language preference via **View** → **Language** (restart to apply)
- Light and dark appearance themes

Artifact coverage (representative)

System & execution

Prefetch, BAM/DAM, AppCompat, Jump Lists, RecentDocs, ShellBags, LNK, UserAssist, UWP/AppX inventory, MRU keys, ShimCache, Amcache, SRUM, and related traces.

Browsers & network

Chrome, Edge, Firefox (history, downloads, cookies, credentials, extensions), Zone.Identifier ADS, hosts/DNS/firewall artifacts.

Cloud & remote access

OneDrive, Dropbox, Google Drive metadata, RDP history and bitmap cache, TeamViewer, AnyDesk, VPN profiles.

Logs & scheduling

EVTX parsing and aggregation, Task Scheduler, BITS, Windows Update, PowerShell transcripts.

Deleted & hidden data

Recycle Bin, USN journal, ADS, slack space viewers, extension/signature mismatches, entropy-based detection.

Case database & scan sessions

DigitalHound stores investigative output in a **portable case folder**:

Artifact	Role
`.dhcase`	Case metadata, evidence paths, bookmarks, audit log, UI state
`case.db`	SQLite (WAL) with `dh_*` tables for artifacts, timeline, keywords, forensic modules per **scan session**

Reopen a case to **restore the forensic module tree**, filter by **scan session**, reload **timeline** and **search hits**, without re-scanning the image—while keeping data under your control on local storage.

AI forensic assistant (offline-first)

- Run **local** large language models (**.gguf** via llama.cpp)—no mandatory cloud API
- Investigate in **natural language**; the engine can invoke registered forensic tools
- Turn raw hits into **structured summaries** with timelines and highlighted risk items
- Extend behavior by registering tools on `ForensicAiEngine`

Image intelligence: AI-assisted image categorization for triage (documents, plates, weapons-related classes, CSAM-related classes, and other configured categories—use only in lawful, policy-compliant workflows).

Example analyst intents: find encrypted archives, summarize browser secrets, list suspicious domains, triage images, export a consolidated timeline narrative.

Reporting & chain of custody

- **CSV** — module or category exports, timeline export
- **HTML** — interactive review in any browser
- **PDF** — case overview, sources, artifact summaries
- **Bookmarks** — severity tiers for review prioritization
- **Audit log** — actions recorded in the case
- **Image hashing** — MD5 / SHA-256 (and related) for integrity documentation

---

Technical specifications

Item	Support
Image formats	RAW, DD, E01/EWF-style, VHD/VHDX, VMDK, QCOW, AFF4 (build-dependent)
File systems	NTFS, FAT, exFAT, HFS+, APFS, ext2/3/4, others via TSK
Case store	SQLite; optional SQLCipher path where enabled in build
AI runtime	llama.cpp, GGUF; optional OpenAI-compatible API
Primary platform	Windows 10/11 x64

Product family & roadmap

Product	Focus
DigitalHound	Computer & server media forensics *(this product)*
DigitalHound Mobile	Mobile device forensics *(roadmap / separate SKU)*
DigitalHound Cloud	Cloud acquisition & analysis *(roadmap / separate SKU)*

Active investment areas include **DPAPI decryption chains**, **Telegram Desktop offline decryption**, **WeChat/QQ key acquisition workflows**, and deeper mobile/cloud companions.

Get started (analyst checklist)

1. Acquire a forensic image using your organization's approved imaging process.
2. **File** → **New Case**, then **Add Evidence Source** and load the image.
3. Run **Automated Forensic Scan** or open **Comprehensive Forensic Scan** to pick modules.
4. Review **Forensic Results**, **Timeline View**, **Search Hits**, and specialist viewers.
5. Bookmark critical items, export reports, and **Save Case**; archive the entire case folder for retention.

Taglines (marketing)

- *DigitalHound — leave no byte unexplored.*
- *From image to insight on one forensic workbench.*
- *Local AI. Session-aware case DB. Built for the lab.*
- *480+ parsers. One case database. Your evidence stays on your machine.*

DigitalHound

Custom SleuthKit core · Modular forensic catalog · Offline-capable AI · Court-ready exports