**Step-by-step Quick Start for Autopsy**

**(The digital forensics tool )**

**1) Install Autopsy**

* **Windows:** Download the current Windows installer from the official site and run it. As of now, the site lists **Autopsy 4.x** with a one-click 64-bit installer. [Autopsy+1](https://www.autopsy.com/?utm_source=chatgpt.com)
* **Linux / macOS:** Autopsy 4 runs, but you install via ZIP + extra dependencies (Sleuth Kit, Java, etc.). Follow the platform notes; on macOS/Linux you typically build or install Sleuth Kit separately. [Autopsy](https://www.autopsy.com/download/?utm_source=chatgpt.com)[slo-sleuth.github.io](https://slo-sleuth.github.io/tools/InstallingAutopsyOnMacOS.html?utm_source=chatgpt.com)

**Recommended resources / prerequisites**

* **System memory:** 16 GB RAM recommended; you can raise Autopsy’s JVM memory later via **Tools → Options → Application → Maximum JVM Memory**. [Sleuth Kit](https://sleuthkit.org/autopsy/docs/user-docs/4.16.0/installation_page.html?utm_source=chatgpt.com)

**2) Launch & create a case**

1. Open Autopsy → **Create New Case**.
2. Fill in **Case Name**, choose a **Base Directory**, and (optionally) **Case Number** / **Examiner**.
3. Finish to create the empty case.  
   *A “case” can hold one or many data sources (images, drives, logical folders).* [Sleuth Kit](https://sleuthkit.org/autopsy/docs/user-docs/4.5.0/cases_page.html?utm_source=chatgpt.com)

**3) Add a data source**

Choose **Add Data Source** and pick one of:

* **Disk Image / VM** (E01, RAW/DD, VMDK, VHD, etc.)
* **Local Disk/Device** (attached drive)
* **Logical Files** (folders/files you exported elsewhere) [Sleuth Kit](https://sleuthkit.org/autopsy/docs/user-docs/4.5.0/cases_page.html?utm_source=chatgpt.com)

Point Autopsy at the file/device and proceed.

**4) Select ingest modules (the analysis plug-ins)**

On the **Ingest Modules** screen, tick what you need. Common starters:

* **Recent Activity** (browser history, downloads, logins, etc.)
* **File Type Identification**
* **Hash Lookup** (with NSRL or your own hash sets)
* **Keyword Search** (indexing for fast text search)
* **EXIF/Metadata** (pictures, docs)  
  These modules parse files and generate artifacts while data is added/ingested. You can re-run modules later on selected data if needed. [Sleuth Kit](https://sleuthkit.org/autopsy/docs/user-docs/3.1/ingest_page.html?utm_source=chatgpt.com)[GitHub](https://github.com/sleuthkit/autopsy_addon_modules?utm_source=chatgpt.com)

Tip: Start with Recent Activity + Keyword Search for a quick overview; add heavier modules (full hash lookups, carving) once you see where to dig.

**5) Let ingest run & watch progress**

You’ll see progress in the lower right. As modules finish, results appear in the left **Data Sources** / **Views** tree.

**6) Explore key views (the daily workflow)**

* **Results / Artifacts:** consolidated findings from modules (web history, accounts, installed apps, etc.).
* **File Types / MIME:** pivot by type (docs, images, archives…).
* **Keyword Hits:** terms matched during indexing.
* **Timeline:** sequence events across the case to see activity bursts.  
  These are standard Autopsy UI areas you’ll use in almost every case. [Sleuth Kit](https://sleuthkit.org/autopsy/docs/user-docs/4.5.0/cases_page.html?utm_source=chatgpt.com)

**7) Search, filter, and carve**

* Use **Keyword Search** (indexed) for fast text queries.
* Apply **Filters** (time range, file type, known/unknown files, tags).
* Use **File Search by Attributes** (size/date/hash) when narrowing large sets.  
  (These capabilities are provided by built-in modules and UI tools.) [Sleuth Kit](https://sleuthkit.org/autopsy/docs/user-docs/3.1/ingest_page.html?utm_source=chatgpt.com)

**8) Tag, comment, and bookmark**

Right-click items → **Add Tag** or **Add Comment** to keep your findings organized. Tags drive your reports later.

**9) Generate reports**

Go to **Tools → Generate Report** and pick formats (HTML, CSV, KML, etc.) and which artifacts/tags to include. Report modules are part of Autopsy’s plug-in system. [GitHub](https://github.com/sleuthkit/autopsy_addon_modules?utm_source=chatgpt.com)

**10) Adjust settings as your case grows**

* **Raise memory** (if you hit “Out of memory” or sluggish indexing): **Tools → Options → Application → Maximum JVM Memory**. [Sleuth Kit](https://sleuthkit.org/autopsy/docs/user-docs/4.16.0/installation_page.html?utm_source=chatgpt.com)
* **Add/disable modules** anytime from the **Ingest** panel if you need deeper or faster passes. [Sleuth Kit](https://sleuthkit.org/autopsy/docs/user-docs/3.1/ingest_page.html?utm_source=chatgpt.com)

**(Optional) Multi-user / bigger setups**

Autopsy supports a multi-user configuration (PostgreSQL, ActiveMQ, Solr) so multiple examiners can work the same case; the docs include suggested hardware for those roles. Only set this up if you truly need collaboration at scale. [Sleuth Kit+1](https://sleuthkit.org/autopsy/docs/user-docs/4.0/install_multiuser_page.html?utm_source=chatgpt.com)

**Troubleshooting cheatsheet**

* **“Can’t open image” / dependencies (macOS/Linux):** confirm Sleuth Kit/Java versions per platform notes. [slo-sleuth.github.io](https://slo-sleuth.github.io/tools/InstallingAutopsyOnMacOS.html?utm_source=chatgpt.com)
* **Very slow ingest:** start with fewer modules; add more after initial triage. [Sleuth Kit](https://sleuthkit.org/autopsy/docs/user-docs/3.1/ingest_page.html?utm_source=chatgpt.com)
* **Search returns nothing:** ensure **Keyword Search** ran; if not, (re)run it on the data source. [Sleuth Kit](https://sleuthkit.org/autopsy/docs/user-docs/3.1/ingest_page.html?utm_source=chatgpt.com)
* **Memory errors:** increase JVM memory in **Tools → Options**. [Sleuth Kit](https://sleuthkit.org/autopsy/docs/user-docs/4.16.0/installation_page.html?utm_source=chatgpt.com)

**Download & docs (official)**

* **Autopsy site & downloads:** official homepage and download page. [Autopsy+1](https://www.autopsy.com/?utm_source=chatgpt.com)
* **User docs (cases, installation, modules):** official user documentation.