AUTOSPY

- Autopsy is a Graphical User Interface (GUI) for the Sleuth Kit (TSK), an open-source digital forensics platform. It is widely used in cybercrime investigations, forensic analysis, and incident response.
- Provides an easy-to-use interface for examining disk images, recovering deleted files, analyzing file systems, and reporting findings.

Key Features

1. Case Management- Allows creation of new cases with metadata (case name, number, examiner details). It keeps all evidence, analysis results, and reports organized.
2. Evidence Handling -Supports adding multiple evidence sources:
    - Disk images (E01, RAW, VHD, AFF, etc.)
    - Local drives
    - Individual files or directories

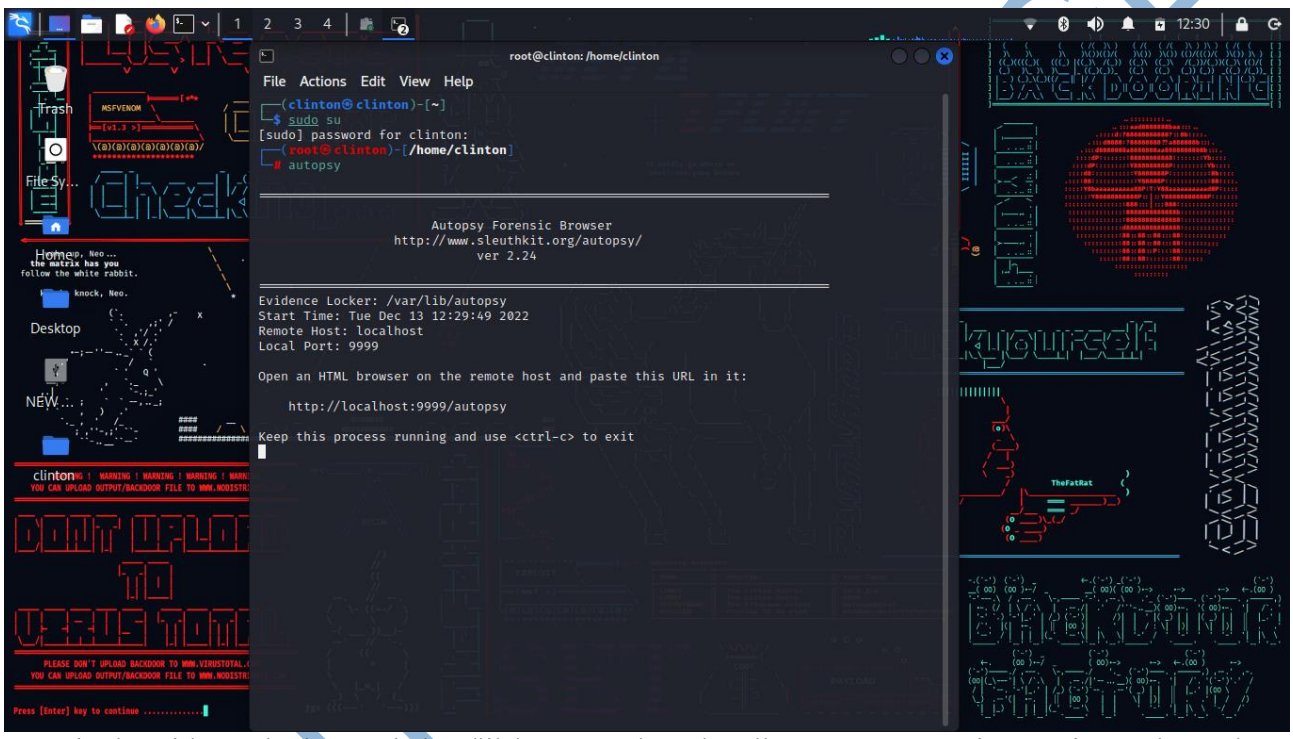
    Maintains evidence integrity using hash verification (MD5, SHA1, SHA256).

3. File System Analysis
    - Supports popular file systems (FAT, NTFS, EXT, HFS+, etc.).
    - Displays directories, hidden files, and deleted data.
    - Provides metadata such as timestamps (created, modified, accessed, entry modified).
4. Data Recovery
    - Recovers deleted files and folders if they haven't been overwritten.
    - Supports keyword searches to locate relevant evidence.
5. Artifact Analysis
    - Extracts and analyzes user activities such as:
        - Web browser history (URLs, cookies, downloads).
        - Email archives.
        - Chat logs.
        - Installed applications.
        - Registry keys.
6. Timeline Analysis
    - Presents a chronological view of system events (logins, file accesses, deletions).
    - Helps investigators reconstruct user actions.
7. Hashing and File Identification
    - Generates hash values for each file to verify authenticity.
    - Compares files against known hash sets (e.g., NSRL database) to identify known good or bad files.
8. Keyword Search
    - Allows simple text searches or regular expressions.
    - Helps locate specific terms (e.g., emails, passwords, suspicious strings).

9. Reporting
    - Generates detailed forensic reports in HTML, CSV, Excel, and PDF.
    - Reports include evidence summary, file listings, hash values, and examiner notes.
    - Supports bookmarking evidence for court presentation.

Workflow in Autopsy

Start the tool by typing autopsy in the CLI root. Autopsy Forensic Browser **v2.24** started from



terminal; evidence locker path /var/lib/autopsy; host localhost, port **9999**; instruction to keep the process running.

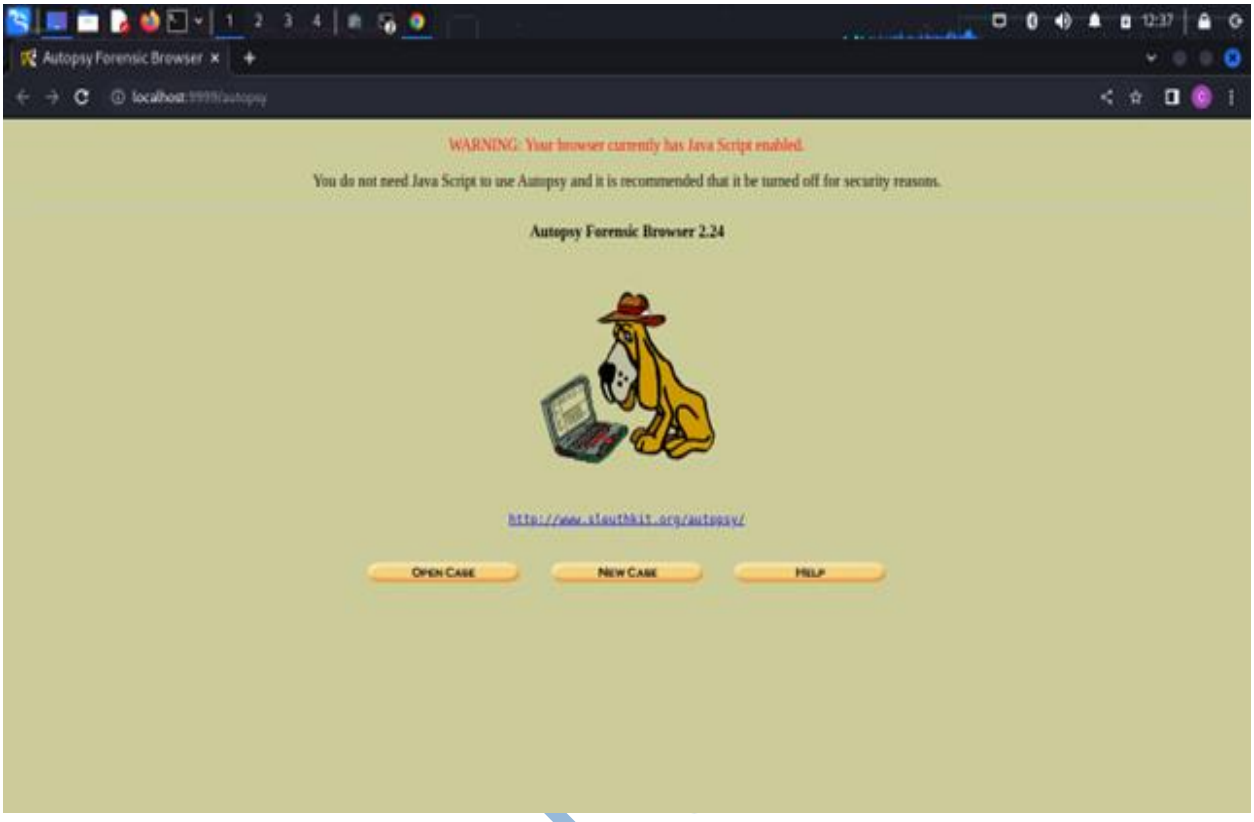
You can either open a former case or start a new case, by clicking the web-based GUI.

Investigators must create a new case or open an existing one.

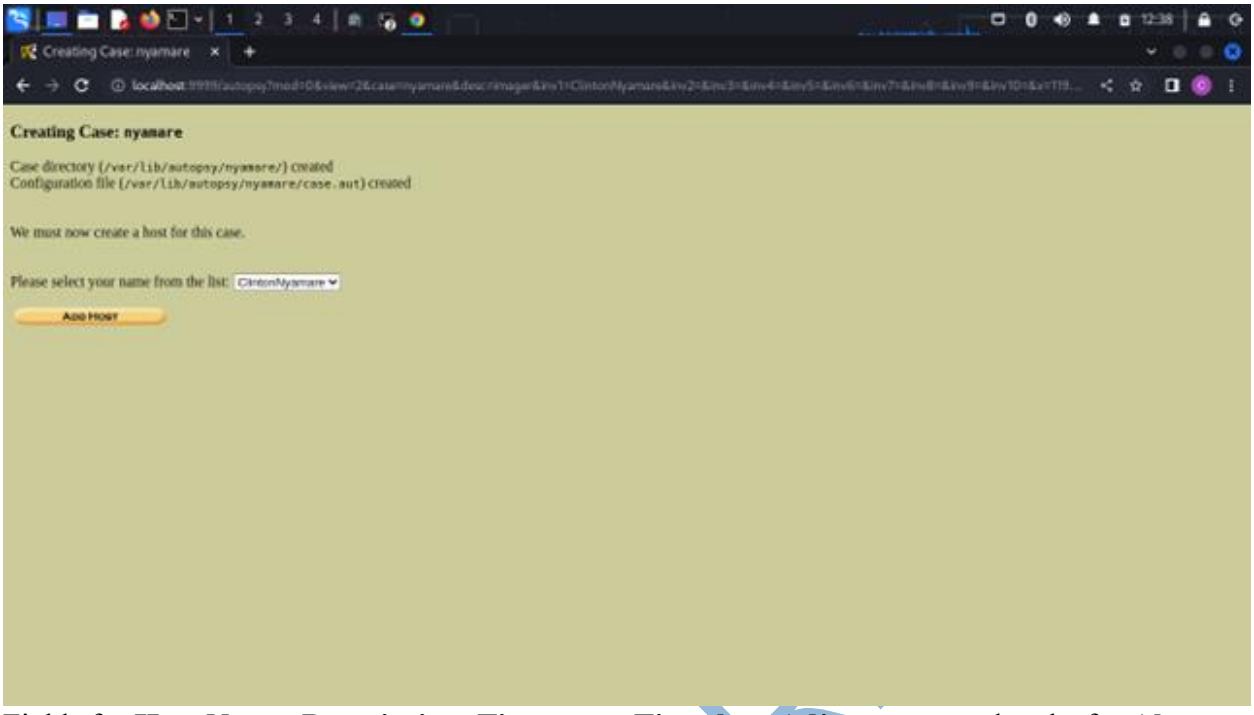
Autopsy's classic web UI runs as a local web service. The evidence locker is where Autopsy stores case data and copies of imported images.

Autopsy welcome page

Use “New Case” for every investigation to keep artifacts isolated and chain-of-custody clean.



Confirmation that the **case directory** and **config file** were created; a dropdown to select the examiner name, then **Add Host**.
examiner must match worksheet/assignment sheet for traceability.

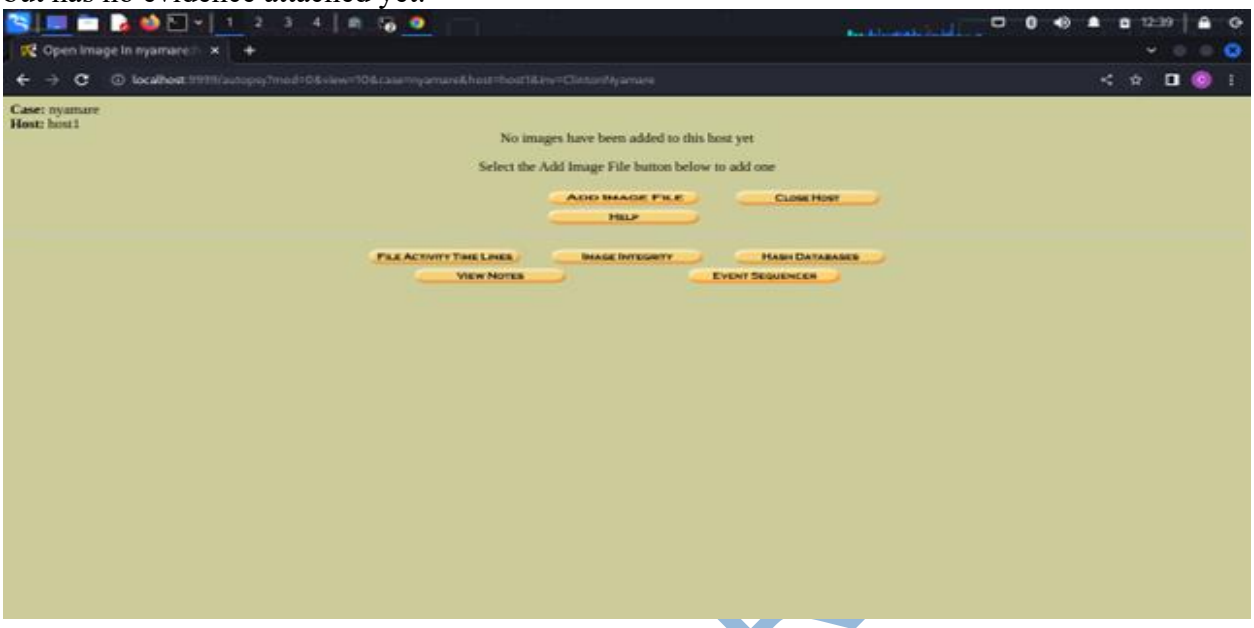


Fields for **Host Name**, **Description**, **Time zone**, **Timeskew Adjustment**, and paths for **Alert Hash DB** (known bad) and **Ignore Hash DB** (known good). These fields define the logical machine being investigated and set analysis context (e.g., timezone, clock drift).

Forensic note:

- **Time zone** should match the source system (or the jurisdiction) to keep timelines correct.
- **Timeskew** lets you offset systems with wrong clocks.
- Point **Alert/Ignore** to NSRL or custom hash sets when available to quickly triage known good/bad files.

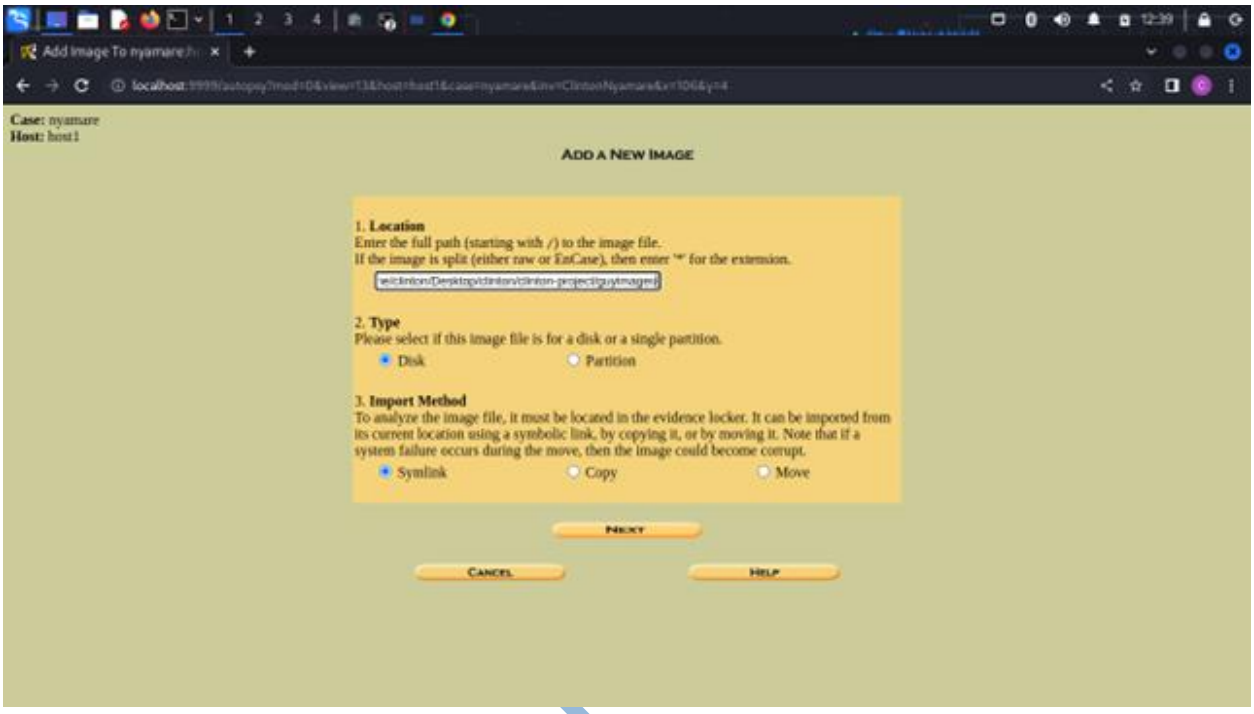
Host view with buttons: **Add Image File**, **Analyze**, **File Activity Timelines**, **Image Integrity**, **Hash Databases**, **Event Sequencer**, etc. Status line says *No images have been added*. Hot exists but has no evidence attached yet.



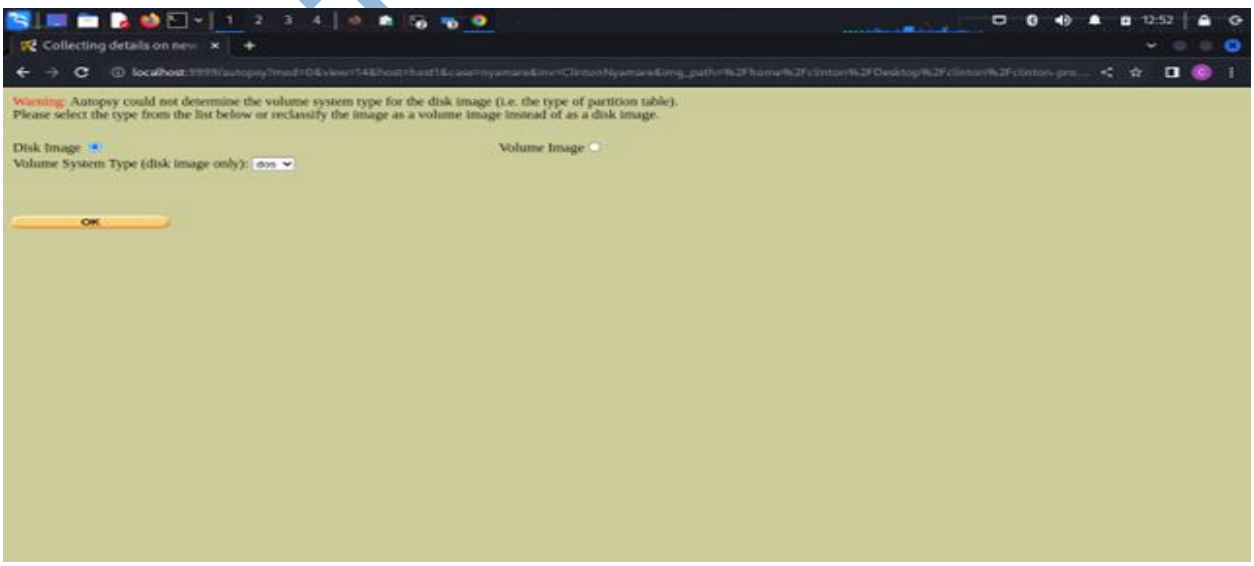
Location (absolute path to image), **Type** (**Disk** vs **Partition**), **Import Method** (**Symlink**, **Copy**, **Move**).
Here You define where the evidence image lives and how Autopsy should bring it into the evidence locker.
Forensic note:

- Prefer **Copy** to maintain immutability of the original source path.
- Use **Disk** if the file contains a whole-disk image; **Partition** for single-volume captures.

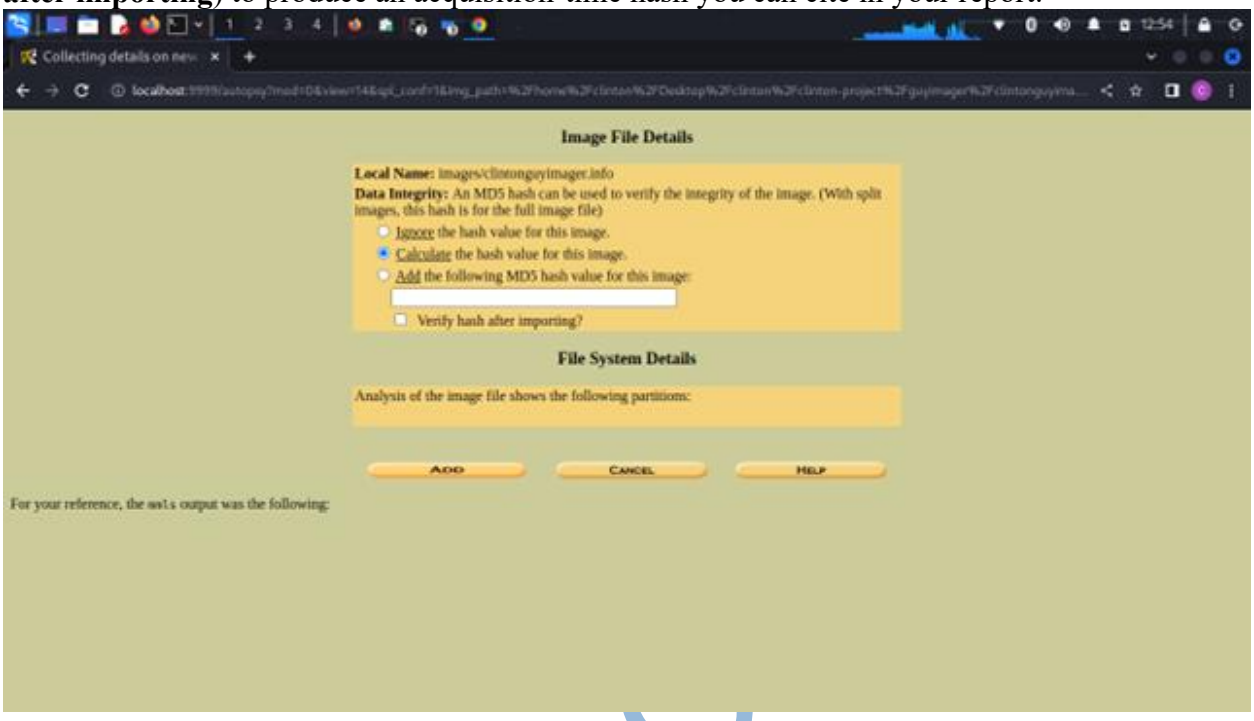
Here you're importing the image *via the Guymager ".info" descriptor*. Autopsy will reference the actual data segments from that descriptor.
Keep the Guymager image set (EWF/RAW segments + .info) together and read-only. Consider **Copy** if the evidence locker must contain a full, independent copy.



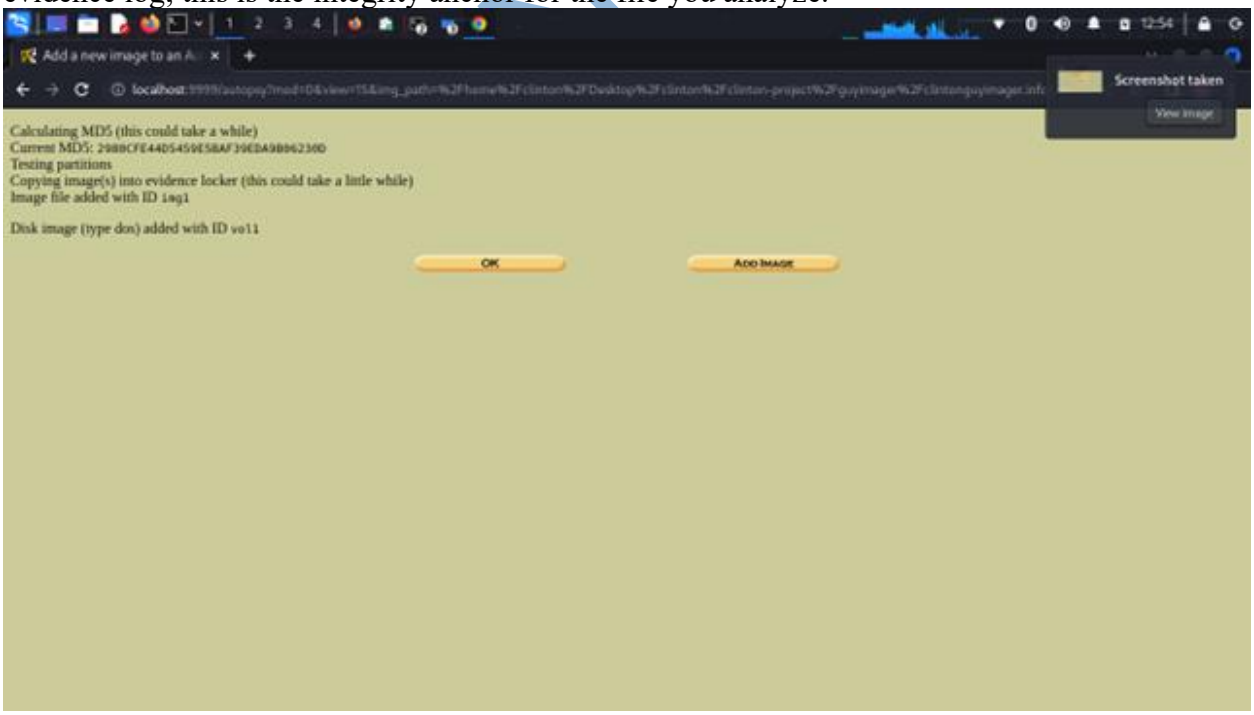
Manual classification is required (likely an MBR/"DOS" partition table).
Forensic note: Choosing the correct volume system is crucial for partition discovery and downstream artifact parsing.



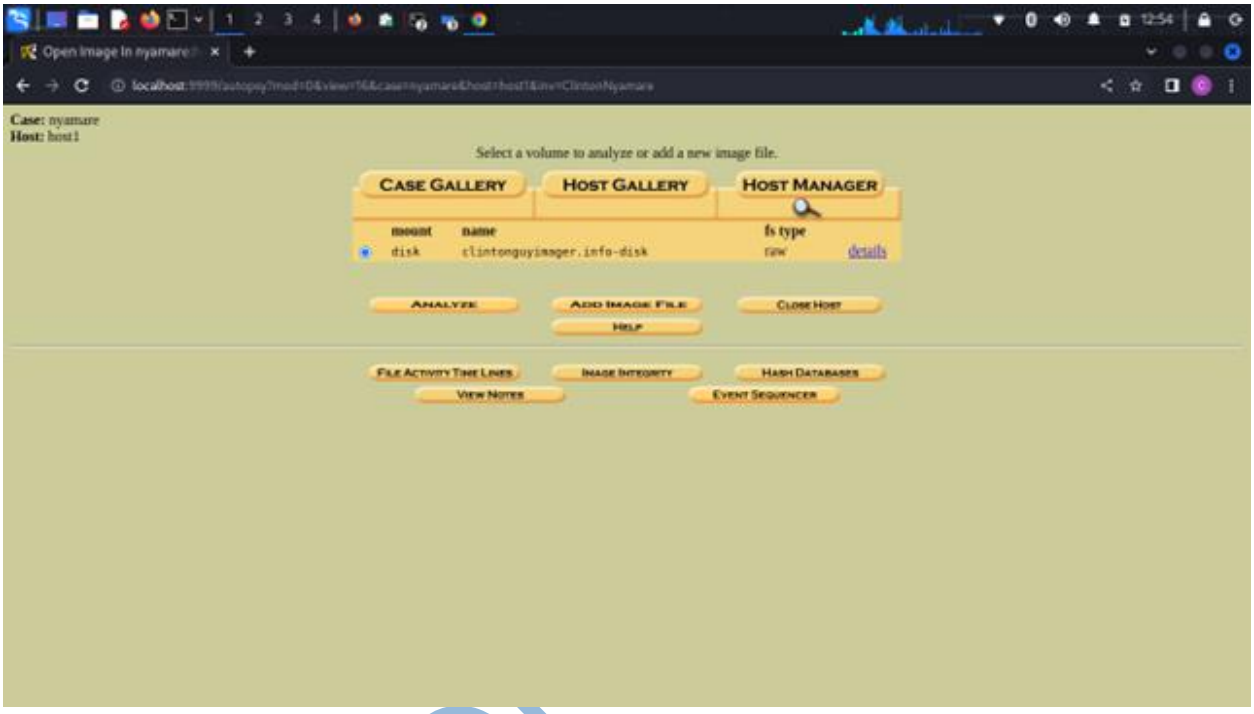
Options to **Ignore**, **Calculate**, or **Add** a known **MD5**; checkbox to **Verify hash after importing**. **This means** Integrity controls before Autopsy finalizes the import. Select **Calculate** (and **Verify after importing**) to produce an acquisition-time hash you can cite in your report.



The image is registered and tracked by internal IDs for auditing and record the **MD5** in your evidence log; this is the integrity anchor for the file you analyze.



Case Gallery / Host Gallery / Host Manager; table entry for the imported image: mount **disk**, name **clintonguymager.info-disk**, **fs type: raw**, with **details** link; action buttons including **Analyze**.This means that the image is ready for analysis; “raw” indicates Autopsy will parse the filesystem directly.
Proceed with **Analyze** (or jump into modules like timelines/keyword search). Capture a screenshot of the **details** page if your submission requires exact sizes and geometry.



Analysis workspace with tabs (**File Analysis, Keyword Search, File Type, Image Details, Meta Data, Data Unit**). The **Data Unit** tab is active; left pane has **Unit Number**, **Number of Units**, **Unit Size 512**, **Lazarus Addr** option; **View** button.
This means Low-level sector access mode to read arbitrary units/blocks of the filesystem. It is useful for *carving* and verifying byte-level content (e.g., checking partition boot sectors, MFT records, or slack space). Keep track of unit size (512) when documenting offsets.