EX:05

VIEW LAST ACTIVITY OF YOUR PC

Madhesh M A
231901029

Aim

To view and document the recent user and system activities on a Windows PC (program executions, file opens, USB insertions, logon/logoff, startup/shutdown, etc.) using **NirSoft – LastActivityView**.

Introduction

LastActivityView is a portable Windows artifact viewer that correlates traces from multiple sources (UserAssist, Prefetch, Jump Lists, RecentDocs, MUICache, event logs, shell history, and more) into a single timeline. It helps quickly answer "what happened, when, and by which process" without installing heavy forensic suites. Typical uses include basic triage, user activity verification, and incident response on a live system or an ofline Windows drive.

Procedure

1. **Acquire the tool**
    - Download **LastActivityView (ZIP)** from the page shown.
    - Extract the ZIP to a working folder (e.g., C:\Tools\LastActivityView\).
2. **Run with elevated rights**
    - Right-click LastActivityView.exe → **Run as administrator** for fuller artifact access.
3. **Initial timeline**
    - The tool auto-loads artifacts and displays a table.
    - Click the **Time** column to sort **Newest → Oldest**.
4. **Filter and focus**
    - Press **Ctrl+Q (Quick Filter)** and type keywords to narrow results:
        - Examples: USB, chrome.exe, .docx, shutdown, setup.exe.
    - (Optional) **Options → Advanced Options…**
        - Set **From/To** time range.
        - Choose **Load activity from external hard-drive** to analyze another Windows installation.
5. **Inspect key columns**
    - **Time** – exact timestamp of the event.

VIEW LAST ACTIVITY OF YOUR PC

- **Description / Action Type** – e.g., *Run .EXE*, *Open file*, *USB plug*, *System Started/Shutdown*.
- **Process / Filename / Full Path** – what ran or opened.
- **More Info** – extra context (parameters, device name, etc.).

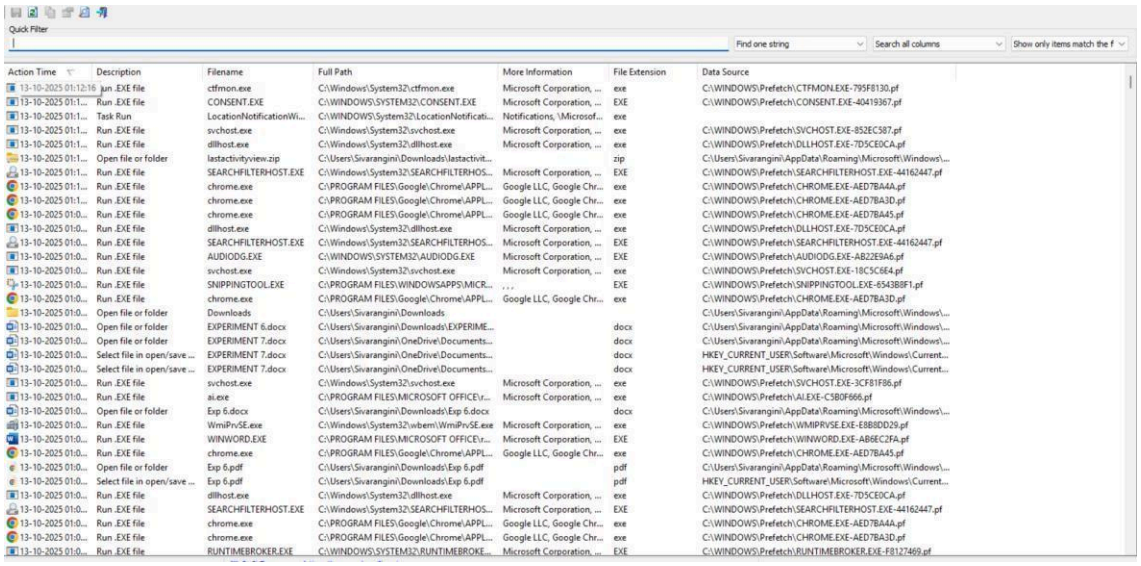
6. **Document findings**
   - Select relevant rows → **Ctrl+S** to export **CSV/HTML/XML**.
   - Or **View** → **HTML Report – All Items** to generate a printable report.
   - Note any gaps, anomalies, or corroborating artifacts (e.g., Prefetch presence for a run event).
7. **(Optional) Corroboration**
   - **Event Viewer** (eventvwr.msc) → Windows Logs for startup/shutdown and device logs.
   - Check C:\Windows\Prefetch\ for corresponding .pf files of executed programs.

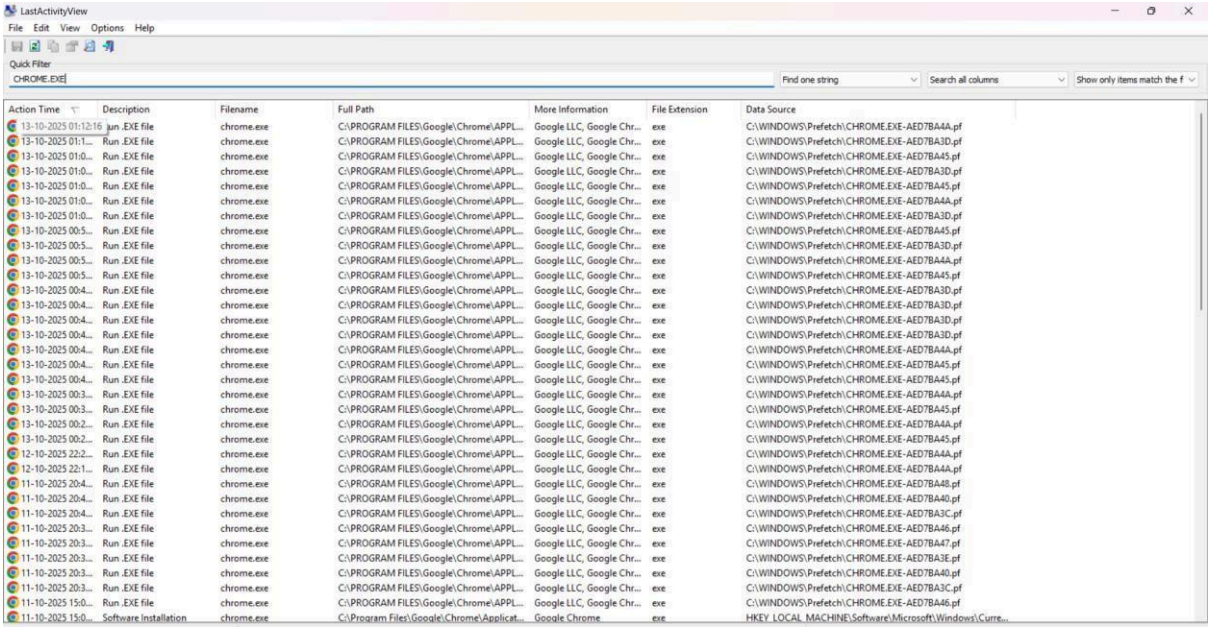
Output

- **On-screen:** A chronological table of activities showing:
  - *Time* (e.g., 2025-10-12 20:14:03)
  - *Action Type* (e.g., **Run .EXE**, **Open File**, **USB Device Connected**, **System Started**, **Shutdown**)
  - *Process/Filename/Path* (e.g., C:\Program Files\Google\Chrome\Application\chrome.exe)
  - *More Info* (e.g., device label SanDisk Ultra, file parameters, user profile path)

EX:05

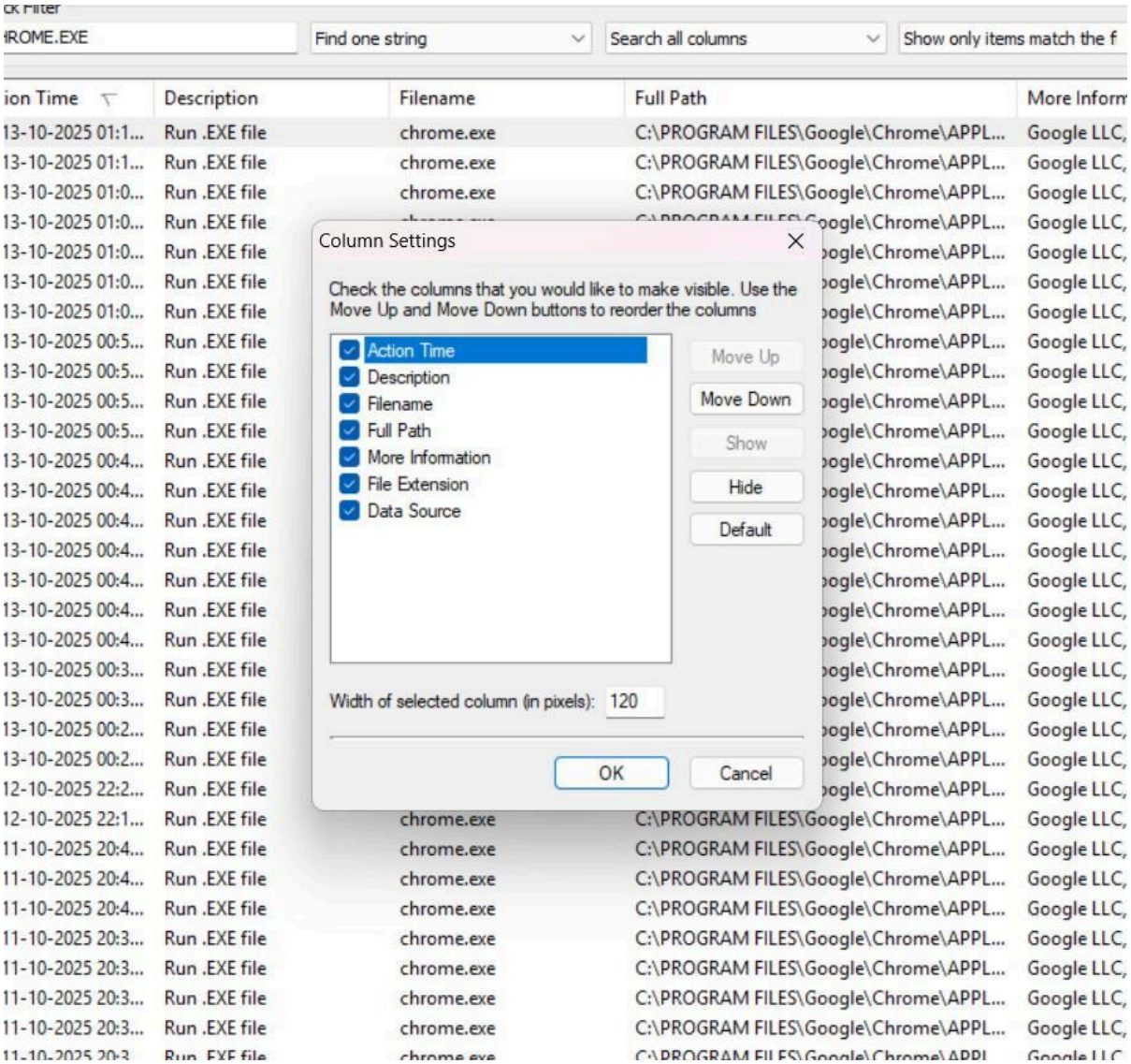
VIEW LAST ACTIVITY OF YOUR PC

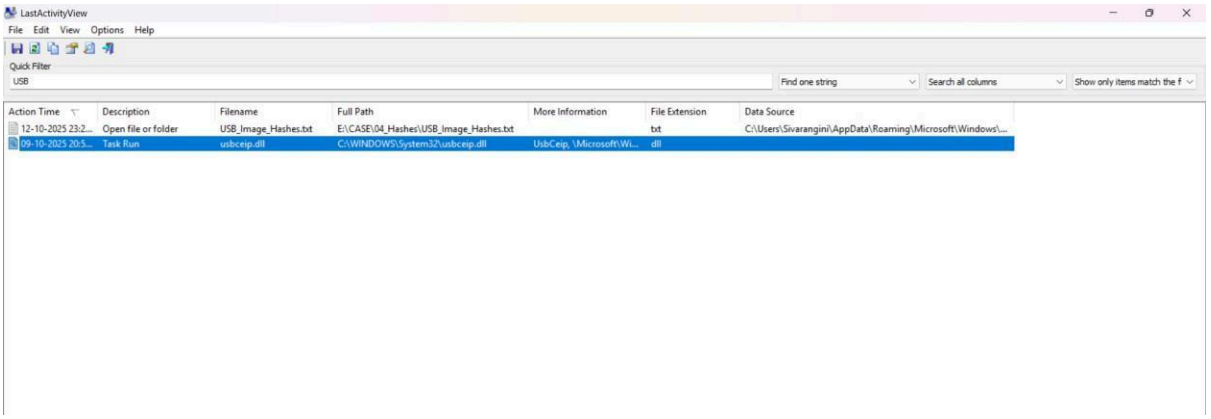




EX:05

VIEW LAST ACTIVITY OF YOUR PC





Conclusion:

The exercise was successfully completed using LastActivityView to generate a chronological

EX:05

VIEW LAST ACTIVITY OF YOUR PC

timeline of user and system activity. Key events—program executions, file/document access, USB connections, and startup/shutdown—were identified and exported as a report. Cross-checks with Prefetch and Event Logs confirmed the timeline's accuracy, making the findings suitable for inclusion as forensic evidence.