Madhan kumar b
231901028

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 offline Windows drive.

Procedure

1. **Acquire the tool**

   o Download **LastActivityView (ZIP)** from the page shown.

   o Extract the ZIP to a working folder (e.g., C:\Tools\LastActivityView\).

2. **Run with elevated rights**

   o Right-click LastActivityView.exe → **Run as administrator** for fuller artifact access.

3. **Initial timeline**

   o The tool auto-loads artifacts and displays a table.

   o Click the **Time** column to sort **Newest → Oldest**.

4. **Filter and focus**

   o Press **Ctrl+Q (Quick Filter)** and type keywords to narrow results:

   ▪ Examples: USB, chrome.exe, .docx, shutdown, setup.exe.

   o (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**

   o **Time** – exact timestamp of the event.

- o **Description / Action Type** – e.g., *Run .EXE*, *Open file*, *USB plug*, *System Started/Shutdown*.

- o **Process / Filename / Full Path** – what ran or opened.

- o **More Info** – extra context (parameters, device name, etc.).

6. **Document findings**

- o Select relevant rows → **Ctrl+S** to export **CSV/HTML/XML**.

- o Or **View → HTML Report – All Items** to generate a printable report.

- o Note any gaps, anomalies, or corroborating artifacts (e.g., Prefetch presence for a run event).

7. **(Optional) Corroboration**

- o **Event Viewer** (eventvwr.msc) → Windows Logs for startup/shutdown and device logs.

- o Check C:\Windows\Prefetch\ for corresponding .pf files of executed programs.

Output

- • **On-screen:** A chronological table of activities showing:

  - o *Time* (e.g., 2025-10-12 20:14:03)

  - o *Action Type* (e.g., **Run .EXE**, **Open File**, **USB Device Connected**, **System Started**, **Shutdown**)

  - o *Process/Filename/Path* (e.g., C:\Program Files\Google\Chrome\Application\chrome.exe)

  - o *More Info* (e.g., device label SanDisk Ultra, file parameters, user profile path)

Madhan kumar b
231901028

CK FIlter

| ROME.EXE | Find one string ˅ | Search all columns ˅ | Show only items match the f |

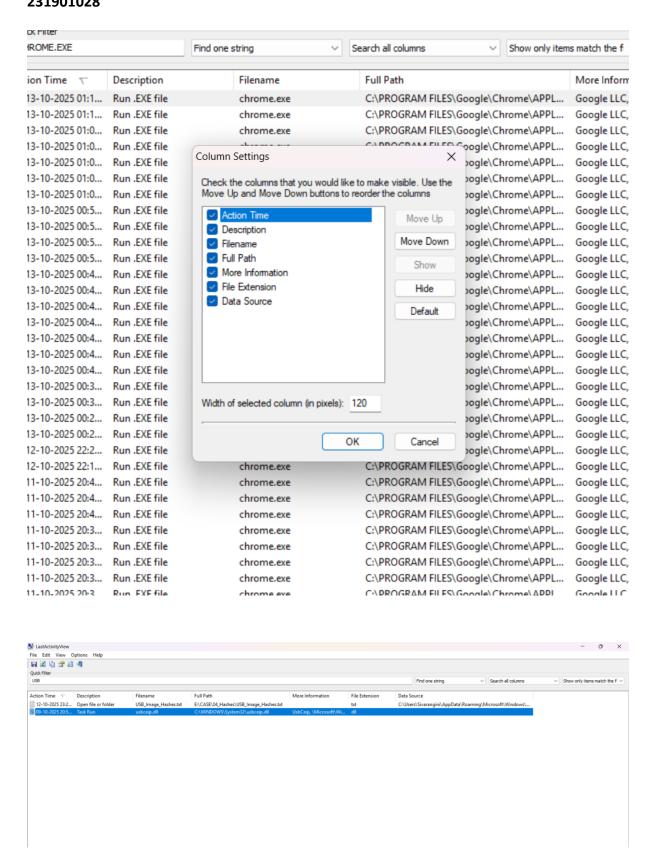| ion Time ▽	Description	Filename	Full Path	More Inform
13-10-2025 01:1...	Run .EXE file	chrome.exe	C:\PROGRAM FILES\Google\Chrome\APPL...	Google LLC,
13-10-2025 01:1...	Run .EXE file	chrome.exe	C:\PROGRAM FILES\Google\Chrome\APPL...	Google LLC,
13-10-2025 01:0...	Run .EXE file	chrome.exe	C:\PROGRAM FILES\Google\Chrome\APPL...	Google LLC,
13-10-2025 01:0...	Run .EXE file	chrome.exe	C:\PROGRAM FILES\Google\Chrome\APPL...	Google LLC,
13-10-2025 01:0...	Run .EXE file			Google LLC,
13-10-2025 01:0...	Run .EXE file			Google LLC,
13-10-2025 01:0...	Run .EXE file			Google LLC,
13-10-2025 00:5...	Run .EXE file			Google LLC,
13-10-2025 00:5...	Run .EXE file			Google LLC,
13-10-2025 00:5...	Run .EXE file			Google LLC,
13-10-2025 00:5...	Run .EXE file			Google LLC,
13-10-2025 00:4...	Run .EXE file			Google LLC,
13-10-2025 00:4...	Run .EXE file			Google LLC,
13-10-2025 00:4...	Run .EXE file			Google LLC,
13-10-2025 00:4...	Run .EXE file			Google LLC,
13-10-2025 00:4...	Run .EXE file			Google LLC,
13-10-2025 00:4...	Run .EXE file			Google LLC,
13-10-2025 00:4...	Run .EXE file			Google LLC,
13-10-2025 00:3...	Run .EXE file			Google LLC,
13-10-2025 00:3...	Run .EXE file			Google LLC,
13-10-2025 00:2...	Run .EXE file			Google LLC,
13-10-2025 00:2...	Run .EXE file			Google LLC,
12-10-2025 22:2...	Run .EXE file			Google LLC,
12-10-2025 22:1...	Run .EXE file	chrome.exe	C:\PROGRAM FILES\Google\Chrome\APPL...	Google LLC,
11-10-2025 20:4...	Run .EXE file	chrome.exe	C:\PROGRAM FILES\Google\Chrome\APPL...	Google LLC,
11-10-2025 20:4...	Run .EXE file	chrome.exe	C:\PROGRAM FILES\Google\Chrome\APPL...	Google LLC,
11-10-2025 20:4...	Run .EXE file	chrome.exe	C:\PROGRAM FILES\Google\Chrome\APPL...	Google LLC,
11-10-2025 20:3...	Run .EXE file	chrome.exe	C:\PROGRAM FILES\Google\Chrome\APPL...	Google LLC,
11-10-2025 20:3...	Run .EXE file	chrome.exe	C:\PROGRAM FILES\Google\Chrome\APPL...	Google LLC,
11-10-2025 20:3...	Run .EXE file	chrome.exe	C:\PROGRAM FILES\Google\Chrome\APPL...	Google LLC,
11-10-2025 20:3...	Run .EXE file	chrome.exe	C:\PROGRAM FILES\Google\Chrome\APPL...	Google LLC,
11-10-2025 20:3	Run .EXE file	chrome.exe	C:\PROGRAM FILES\Google\Chrome\APPL	Google LLC

Column Settings ✕

Check the columns that you would like to make visible. Use the
Move Up and Move Down buttons to reorder the columns

- ☑ Action Time
- ☑ Description
- ☑ Filename
- ☑ Full Path
- ☑ More Information
- ☑ File Extension
- ☑ Data Source

[Move Up] [Move Down] [Show] [Hide] [Default]

Width of selected column (in pixels): 120

[OK] [Cancel]

LastActivityView   — ☐ ✕

File Edit View Options Help

Quick Filter

| USB | | | | | | | Find one string ˅ | Search all columns ˅ | Show only items match the f ˅ |

Action Time ▽	Description	Filename	Full Path	More Information	File Extension	Data Source
12-10-2025 23:2...	Open file or folder	USB_Image_Hashes.txt	E:\CASE\04_Hashes\USB_Image_Hashes.txt		txt	C:\Users\Sivarangini\AppData\Roaming\Microsoft\Windows\...
09-10-2025 20:5...	Task Run	usbceip.dll	C:\WINDOWS\System32\usbceip.dll	UsbCeip, \Microsoft\Wi...	dll	

Conclusion:

The exercise was successfully completed using LastActivityView to generate a chronological

EXP NO: 5   **VIEW LAST ACTIVITY OF YOUR PC**
Madhan kumar b
231901028

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.