

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 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.

VIEW LAST ACTIVITY OF YOUR PC

- 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)

EX:05

VIEW LAST ACTIVITY OF YOUR PC

Action Time	Description	Filename	Full Path	More Information	File Extension	Data Source
13-10-2025 01:16	Run .EXE file	ctfmon.exe	C:\Windows\System32\ctfmon.exe	Microsoft Corporation,exe	C:\WINDOWS\Prefetch\CTFMON.EXE-795F8130.pf
13-10-2025 01:16	Run .EXE file	CONSENT.exe	C:\WINDOWS\SYSYSTEM32\CONSENT.EXE	Microsoft Corporation,EXE	C:\WINDOWS\Prefetch\CONSENT.EXE-40419367.pf
13-10-2025 01:16	Task Run	LocationNotificationW...	C:\Windows\System32\LocationNotificati...	Notifications, \Microsof...	.exe	
13-10-2025 01:16	Run .EXE file	svchost.exe	C:\Windows\System32\svchost.exe	Microsoft Corporation,exe	C:\WINDOWS\Prefetch\SVCHOST.EXE-852EC87.pf
13-10-2025 01:16	Run .EXE file	dlhhost.exe	C:\Windows\System32\dlhhost.exe	Microsoft Corporation,exe	C:\WINDOWS\Prefetch\DLHOST.EXE-7D5CE0CA.pf
13-10-2025 01:16	Open file or folder	lastactivityview.zip	C:\Users\Sivarangini\Downloads\lastactivi...		.zip	C:\Users\Sivarangini\AppData\Roaming\Microsoft\Windows\...
13-10-2025 01:16	Run .EXE file	SEARCHFILTERHOST.EXE	C:\Windows\System32\SEARCHFILTERHOS...	Microsoft Corporation,exe	C:\WINDOWS\Prefetch\SEARCHFILTERHOST.EXE-44162447.pf
13-10-2025 01:16	Run .EXE file	chrome.exe	C:\PROGRAM FILES\Google\Chrome\APPL...	Google LLC, Google Chr...	.exe	C:\WINDOWS\Prefetch\CHROME.EXE-AED7B4A4.pf
13-10-2025 01:16	Run .EXE file	chrome.exe	C:\PROGRAM FILES\Google\Chrome\APPL...	Google LLC, Google Chr...	.exe	C:\WINDOWS\Prefetch\CHROME.EXE-AED7B4A4.pf
13-10-2025 01:16	Run .EXE file	chrome.exe	C:\PROGRAM FILES\Google\Chrome\APPL...	Google LLC, Google Chr...	.exe	C:\WINDOWS\Prefetch\CHROME.EXE-AED7B4A4.pf
13-10-2025 01:16	Run .EXE file	dlhhost.exe	C:\Windows\System32\dlhhost.exe	Microsoft Corporation,exe	C:\WINDOWS\Prefetch\DLHOST.EXE-7D5CE0CA.pf
13-10-2025 01:16	Run .EXE file	SEARCHFILTERHOST.EXE	C:\Windows\System32\SEARCHFILTERHOS...	Microsoft Corporation,EXE	C:\WINDOWS\Prefetch\SEARCHFILTERHOST.EXE-44162447.pf
13-10-2025 01:16	Run .EXE file	AUDIODG.EXE	C:\WINDOWS\SYSYSTEM32\AUDIODG.EXE	Microsoft Corporation,EXE	C:\WINDOWS\Prefetch\AUDIODG.EXE-AB228A6.pf
13-10-2025 01:16	Run .EXE file	svchost.exe	C:\Windows\System32\svchost.exe	Microsoft Corporation,exe	C:\WINDOWS\Prefetch\SVCHOST.EXE-185C6E4.pf
13-10-2025 01:16	Run .EXE file	SNIPPINGTOOL.EXE	C:\PROGRAM FILES\WINDOWSAPPS\MICRO...EXE	C:\WINDOWS\Prefetch\SNIPPINGTOOL.EXE-654B8F1.pf
13-10-2025 01:16	Run .EXE file	chrome.exe	C:\PROGRAM FILES\Google\Chrome\APPL...	Google LLC, Google Chr...	.exe	C:\WINDOWS\Prefetch\CHROME.EXE-AED7B4A4.pf
13-10-2025 01:16	Open file or folder	Downloads	C:\Users\Sivarangini\Downloads			C:\Users\Sivarangini\AppData\Roaming\Microsoft\Windows\...
13-10-2025 01:16	Open file or folder	EXPERIMENT 6.docx	C:\Users\Sivarangini\Downloads\EXPERIME...		.docx	C:\Users\Sivarangini\AppData\Roaming\Microsoft\Windows\...
13-10-2025 01:16	Open file or folder	EXPERIMENT 7.docx	C:\Users\Sivarangini\OneDrive\Documents...		.docx	C:\Users\Sivarangini\AppData\Roaming\Microsoft\Windows\...
13-10-2025 01:16	Select file in open/save...	EXPERIMENT 7.docx	C:\Users\Sivarangini\OneDrive\Documents...		.docx	HKEX_CURRENT_USER\Software\Microsoft\Windows\Current...
13-10-2025 01:16	Select file in open/save...	EXPERIMENT 7.docx	C:\Users\Sivarangini\OneDrive\Documents...		.docx	HKEX_CURRENT_USER\Software\Microsoft\Windows\Current...
13-10-2025 01:16	Run .EXE file	svchost.exe	C:\Windows\System32\svchost.exe	Microsoft Corporation,exe	C:\WINDOWS\Prefetch\SVCHOST.EXE-3C81F86.pf
13-10-2025 01:16	Run .EXE file	al.exe	C:\PROGRAM FILES\MICROSOFT OFFICE\...	Microsoft Corporation,exe	C:\WINDOWS\Prefetch\AL.EXE-C80B666.pf
13-10-2025 01:16	Open file or folder	Exp 6.docx	C:\Users\Sivarangini\Downloads\Exp 6.docx		.docx	C:\Users\Sivarangini\AppData\Roaming\Microsoft\Windows\...
13-10-2025 01:16	Run .EXE file	WmPrvSE.exe	C:\Windows\System32\wbem\WmPrvSE.exe	Microsoft Corporation,exe	C:\WINDOWS\Prefetch\WMPRVSE.EXE-E8B8D029.pf
13-10-2025 01:16	Run .EXE file	WINWORD.exe	C:\PROGRAM FILES\MICROSOFT OFFICE\...	Microsoft Corporation,EXE	C:\WINDOWS\Prefetch\WINWORD.EXE-AB6EC2FA.pf
13-10-2025 01:16	Run .EXE file	chrome.exe	C:\PROGRAM FILES\Google\Chrome\APPL...	Google LLC, Google Chr...	.exe	C:\WINDOWS\Prefetch\CHROME.EXE-AED7B4A4.pf
13-10-2025 01:16	Open file or folder	Exp 6.pdf	C:\Users\Sivarangini\Downloads\Exp 6.pdf		.pdf	C:\Users\Sivarangini\AppData\Roaming\Microsoft\Windows\...
13-10-2025 01:16	Select file in open/save...	Exp 6.pdf	C:\Users\Sivarangini\Downloads\Exp 6.pdf		.pdf	HKEX_CURRENT_USER\Software\Microsoft\Windows\Current...
13-10-2025 01:16	Run .EXE file	dlhhost.exe	C:\Windows\System32\dlhhost.exe	Microsoft Corporation,exe	C:\WINDOWS\Prefetch\DLHOST.EXE-7D5CE0CA.pf
13-10-2025 01:16	Run .EXE file	SEARCHFILTERHOST.EXE	C:\Windows\System32\SEARCHFILTERHOS...	Microsoft Corporation,EXE	C:\WINDOWS\Prefetch\SEARCHFILTERHOST.EXE-44162447.pf
13-10-2025 01:16	Run .EXE file	chrome.exe	C:\PROGRAM FILES\Google\Chrome\APPL...	Google LLC, Google Chr...	.exe	C:\WINDOWS\Prefetch\CHROME.EXE-AED7B4A4.pf
13-10-2025 01:16	Run .EXE file	chrome.exe	C:\PROGRAM FILES\Google\Chrome\APPL...	Google LLC, Google Chr...	.EXE	C:\WINDOWS\Prefetch\CHROME.EXE-AED7B4A4.pf
13-10-2025 01:16	Run .EXE file	RUNTIMEBROKER.EXE	C:\WINDOWS\SYSYSTEM32\RUNTIMEBROKER...	Microsoft Corporation,EXE	C:\WINDOWS\Prefetch\RUNTIMEBROKER.EXE-F8127469.pf

LastActivityView						
File Edit View Options Help						
Quick Filter C:\chrome.exe						
			Find one string		Search all columns	Show only items match the f
Action Time	Description	Filename	Full Path	More Information	File Extension	Data Source
13-10-2025 01:12:16	Run EXE file	chrome.exe	C:\PROGRAM FILES\Google\Chrome\APPLI...	Google LLC, Google Chr...	.exe	C:\WINDOWS\Prefetch\CHROME.EXE-AED7BAAA.pf
13-10-2025 01:1...	Run EXE file	chrome.exe	C:\PROGRAM FILES\Google\Chrome\APPLI...	Google LLC, Google Chr...	.exe	C:\WINDOWS\Prefetch\CHROME.EXE-AED7BA3D.pf
13-10-2025 01:0...	Run EXE file	chrome.exe	C:\PROGRAM FILES\Google\Chrome\APPLI...	Google LLC, Google Chr...	.exe	C:\WINDOWS\Prefetch\CHROME.EXE-AED7BA45.pf
13-10-2025 01:0...	Run EXE file	chrome.exe	C:\PROGRAM FILES\Google\Chrome\APPLI...	Google LLC, Google Chr...	.exe	C:\WINDOWS\Prefetch\CHROME.EXE-AED7BA3D.pf
13-10-2025 01:0...	Run EXE file	chrome.exe	C:\PROGRAM FILES\Google\Chrome\APPLI...	Google LLC, Google Chr...	.exe	C:\WINDOWS\Prefetch\CHROME.EXE-AED7BAAA.pf
13-10-2025 01:0...	Run EXE file	chrome.exe	C:\PROGRAM FILES\Google\Chrome\APPLI...	Google LLC, Google Chr...	.exe	C:\WINDOWS\Prefetch\CHROME.EXE-AED7BA3D.pf
13-10-2025 00:5...	Run EXE file	chrome.exe	C:\PROGRAM FILES\Google\Chrome\APPLI...	Google LLC, Google Chr...	.exe	C:\WINDOWS\Prefetch\CHROME.EXE-AED7BA45.pf
13-10-2025 00:5...	Run EXE file	chrome.exe	C:\PROGRAM FILES\Google\Chrome\APPLI...	Google LLC, Google Chr...	.exe	C:\WINDOWS\Prefetch\CHROME.EXE-AED7BA3D.pf
13-10-2025 00:5...	Run EXE file	chrome.exe	C:\PROGRAM FILES\Google\Chrome\APPLI...	Google LLC, Google Chr...	.exe	C:\WINDOWS\Prefetch\CHROME.EXE-AED7BA45.pf
13-10-2025 00:5...	Run EXE file	chrome.exe	C:\PROGRAM FILES\Google\Chrome\APPLI...	Google LLC, Google Chr...	.exe	C:\WINDOWS\Prefetch\CHROME.EXE-AED7BA3D.pf
13-10-2025 00:4...	Run EXE file	chrome.exe	C:\PROGRAM FILES\Google\Chrome\APPLI...	Google LLC, Google Chr...	.exe	C:\WINDOWS\Prefetch\CHROME.EXE-AED7BA3D.pf
13-10-2025 00:4...	Run EXE file	chrome.exe	C:\PROGRAM FILES\Google\Chrome\APPLI...	Google LLC, Google Chr...	.exe	C:\WINDOWS\Prefetch\CHROME.EXE-AED7BA3D.pf
13-10-2025 00:4...	Run EXE file	chrome.exe	C:\PROGRAM FILES\Google\Chrome\APPLI...	Google LLC, Google Chr...	.exe	C:\WINDOWS\Prefetch\CHROME.EXE-AED7BAAA.pf
13-10-2025 00:4...	Run EXE file	chrome.exe	C:\PROGRAM FILES\Google\Chrome\APPLI...	Google LLC, Google Chr...	.exe	C:\WINDOWS\Prefetch\CHROME.EXE-AED7BA45.pf
13-10-2025 00:4...	Run EXE file	chrome.exe	C:\PROGRAM FILES\Google\Chrome\APPLI...	Google LLC, Google Chr...	.exe	C:\WINDOWS\Prefetch\CHROME.EXE-AED7BA45.pf
13-10-2025 00:3...	Run EXE file	chrome.exe	C:\PROGRAM FILES\Google\Chrome\APPLI...	Google LLC, Google Chr...	.exe	C:\WINDOWS\Prefetch\CHROME.EXE-AED7BAAA.pf
13-10-2025 00:3...	Run EXE file	chrome.exe	C:\PROGRAM FILES\Google\Chrome\APPLI...	Google LLC, Google Chr...	.exe	C:\WINDOWS\Prefetch\CHROME.EXE-AED7BA45.pf
13-10-2025 00:2...	Run EXE file	chrome.exe	C:\PROGRAM FILES\Google\Chrome\APPLI...	Google LLC, Google Chr...	.exe	C:\WINDOWS\Prefetch\CHROME.EXE-AED7BA45.pf
12-10-2025 23:22...	Run EXE file	chrome.exe	C:\PROGRAM FILES\Google\Chrome\APPLI...	Google LLC, Google Chr...	.exe	C:\WINDOWS\Prefetch\CHROME.EXE-AED7BAAA.pf
12-10-2025 22:1...	Run EXE file	chrome.exe	C:\PROGRAM FILES\Google\Chrome\APPLI...	Google LLC, Google Chr...	.exe	C:\WINDOWS\Prefetch\CHROME.EXE-AED7BAAA.pf
11-10-2025 20:4...	Run EXE file	chrome.exe	C:\PROGRAM FILES\Google\Chrome\APPLI...	Google LLC, Google Chr...	.exe	C:\WINDOWS\Prefetch\CHROME.EXE-AED7BA45.pf
11-10-2025 20:4...	Run EXE file	chrome.exe	C:\PROGRAM FILES\Google\Chrome\APPLI...	Google LLC, Google Chr...	.exe	C:\WINDOWS\Prefetch\CHROME.EXE-AED7BA4D.pf
11-10-2025 20:3...	Run EXE file	chrome.exe	C:\PROGRAM FILES\Google\Chrome\APPLI...	Google LLC, Google Chr...	.exe	C:\WINDOWS\Prefetch\CHROME.EXE-AED7BA3C.pf
11-10-2025 20:3...	Run EXE file	chrome.exe	C:\PROGRAM FILES\Google\Chrome\APPLI...	Google LLC, Google Chr...	.exe	C:\WINDOWS\Prefetch\CHROME.EXE-AED7BA4D.pf
11-10-2025 20:3...	Run EXE file	chrome.exe	C:\PROGRAM FILES\Google\Chrome\APPLI...	Google LLC, Google Chr...	.exe	C:\WINDOWS\Prefetch\CHROME.EXE-AED7BA4F.pf
11-10-2025 20:3...	Run EXE file	chrome.exe	C:\PROGRAM FILES\Google\Chrome\APPLI...	Google LLC, Google Chr...	.exe	C:\WINDOWS\Prefetch\CHROME.EXE-AED7BA3E.pf
11-10-2025 20:3...	Run EXE file	chrome.exe	C:\PROGRAM FILES\Google\Chrome\APPLI...	Google LLC, Google Chr...	.exe	C:\WINDOWS\Prefetch\CHROME.EXE-AED7BA4D.pf
11-10-2025 15:0...	Software Installation	chrome.exe	C:\Program Files\Google\Chrome\Appl...	Google Chrome	.exe	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Cur...

EX:05

VIEW LAST ACTIVITY OF YOUR PC

The image shows a 'Column Settings' dialog box in the foreground, partially obscuring a table of file execution logs in the background. The background table has five columns: 'Action Time', 'Description', 'Filename', 'Full Path', and 'More Information'. It contains multiple rows of log entries, each starting with a timestamp (e.g., '13-10-2025 01:1...') followed by a description ('Run .EXE file'), a filename ('chrome.exe'), a full path ('C:\PROGRAM FILES\Google\Chrome\APPL...'), and the name of the application ('Google LLC'). The 'Column Settings' dialog box is a light pink window with a title bar and a close button (X). It contains a list of columns with checkboxes: 'Action Time' (checked), 'Description' (checked), 'Filename' (checked), 'Full Path' (checked), 'More Information' (checked), 'File Extension' (checked), and 'Data Source' (checked). To the right of the list are buttons for 'Move Up', 'Move Down', 'Show', 'Hide', and 'Default'. At the bottom of the dialog, there is a text field labeled 'Width of selected column (in pixels):' with the value '120', and 'OK' and 'Cancel' buttons.

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	usbcep.dll	C:\WINDOWS\System32\usbcep.dll	UsbCep, I\Microsoft\Wl...	.dll	

Conclusion:

The exercise was successfully completed using LastActivityView to generate a chronological

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.