Exp:05 **Name: Hemanth kumar**

Roll no:231901010

VIEW LAST ACTIVITY OF YOUR PC

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.

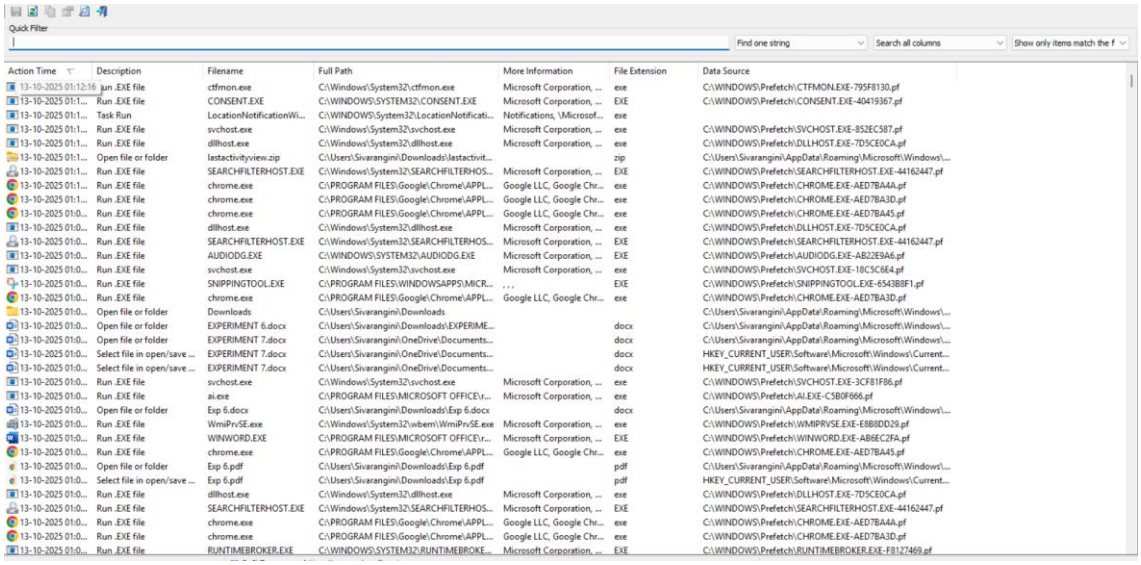
Procedure

1. **Acquire the tool**
    - 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.
    - **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

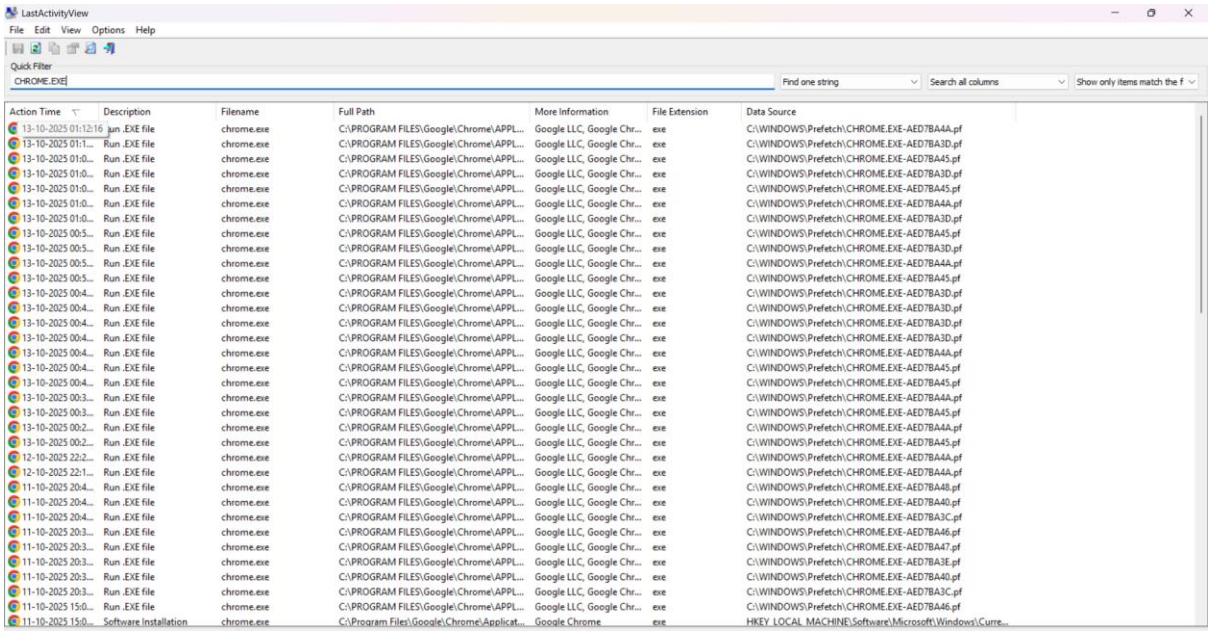
- **On-screen:** A chronological table of activities showing:
    - *Time* (e.g., 2025-10-12 20:14:03)
    - *Action Type* (e.g., **Run .EXE**, **Open File**, **USB Device Connected**, **System Started**, **Shutdown**)
    - *Process/Filename/Path* (e.g., C:\Program Files\Google\Chrome\Application\chrome.exe)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



Quick Filter

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	un .EXE file	ctfmon.exe	C:\Windows\System32\ctfmon.exe	Microsoft Corporation, ...	exe	C:\WINDOWS\Prefetch\CTFMON.EXE-795F8130.pf
13-10-2025 01:1...	Run .EXE file	CONSENT.EXE	C:\WINDOWS\SYSTEM32\CONSENT.EXE	Microsoft Corporation, ...	EXE	C:\WINDOWS\Prefetch\CONSENT.EXE-40419367.pf
13-10-2025 01:1...	Task Run	LocationNotificationWi...	C:\WINDOWS\System32\LocationNotificati...	Notifications, \Microsof...	exe	
13-10-2025 01:1...	Run .EXE file	svchost.exe	C:\Windows\System32\svchost.exe	Microsoft Corporation, ...	exe	C:\WINDOWS\Prefetch\SVCHOST.EXE-852EC587.pf
13-10-2025 01:1...	Run .EXE file	dllhost.exe	C:\Windows\System32\dllhost.exe	Microsoft Corporation, ...	exe	C:\WINDOWS\Prefetch\DLLHOST.EXE-7D5CE0CA.pf
13-10-2025 01:1...	Open file or folder	lastactivityview.zip	C:\Users\Sivarangini\Downloads\lastactivit...		zip	C:\Users\Sivarangini\AppData\Roaming\Microsoft\Windows\...
13-10-2025 01:1...	Run .EXE file	SEARCHFILTERHOST.EXE	C:\Windows\System32\SEARCHFILTERHOS...	Microsoft Corporation, ...	EXE	C:\WINDOWS\Prefetch\SEARCHFILTERHOST.EXE-44162447.pf
13-10-2025 01:1...	Run .EXE file	chrome.exe	C:\PROGRAM FILES\Google\Chrome\APPL...	Google LLC, Google Chr...	exe	C:\WINDOWS\Prefetch\CHROME.EXE-AED7BA4A.pf
13-10-2025 01:1...	Run .EXE file	chrome.exe	C:\PROGRAM FILES\Google\Chrome\APPL...	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\APPL...	Google LLC, Google Chr...	exe	C:\WINDOWS\Prefetch\CHROME.EXE-AED7BA45.pf
13-10-2025 01:0...	Run .EXE file	dllhost.exe	C:\Windows\System32\dllhost.exe	Microsoft Corporation, ...	exe	C:\WINDOWS\Prefetch\DLLHOST.EXE-7D5CE0CA.pf
13-10-2025 01:0...	Run .EXE file	SEARCHFILTERHOST.EXE	C:\Windows\System32\SEARCHFILTERHOS...	Microsoft Corporation, ...	EXE	C:\WINDOWS\Prefetch\SEARCHFILTERHOST.EXE-44162447.pf
13-10-2025 01:0...	Run .EXE file	AUDIODG.EXE	C:\WINDOWS\SYSTEM32\AUDIODG.EXE	Microsoft Corporation, ...	EXE	C:\WINDOWS\Prefetch\AUDIODG.EXE-AB22E9A6.pf
13-10-2025 01:0...	Run .EXE file	svchost.exe	C:\Windows\System32\svchost.exe	Microsoft Corporation, ...	exe	C:\WINDOWS\Prefetch\SVCHOST.EXE-18C5C6E4.pf
13-10-2025 01:0...	Run .EXE file	SNIPPINGTOOL.EXE	C:\PROGRAM FILES\WINDOWSAPPS\MICR...	, , ,	EXE	C:\WINDOWS\Prefetch\SNIPPINGTOOL.EXE-6543B8F1.pf
13-10-2025 01:0...	Run .EXE file	chrome.exe	C:\PROGRAM FILES\Google\Chrome\APPL...	Google LLC, Google Chr...	exe	C:\WINDOWS\Prefetch\CHROME.EXE-AED7BA3D.pf
13-10-2025 01:0...	Open file or folder	Downloads	C:\Users\Sivarangini\Downloads			C:\Users\Sivarangini\AppData\Roaming\Microsoft\Windows\...
13-10-2025 01:0...	Open file or folder	EXPERIMENT 6.docx	C:\Users\Sivarangini\Downloads\EXPERIME...		docx	C:\Users\Sivarangini\AppData\Roaming\Microsoft\Windows\...
13-10-2025 01:0...	Open file or folder	EXPERIMENT 7.docx	C:\Users\Sivarangini\OneDrive\Documents...		docx	C:\Users\Sivarangini\AppData\Roaming\Microsoft\Windows\...
13-10-2025 01:0...	Select file in open/save ...	EXPERIMENT 7.docx	C:\Users\Sivarangini\OneDrive\Documents...		docx	HKEY_CURRENT_USER\Software\Microsoft\Windows\Current...
13-10-2025 01:0...	Select file in open/save ...	EXPERIMENT 7.docx	C:\Users\Sivarangini\OneDrive\Documents...		docx	HKEY_CURRENT_USER\Software\Microsoft\Windows\Current...
13-10-2025 01:0...	Run .EXE file	svchost.exe	C:\Windows\System32\svchost.exe	Microsoft Corporation, ...	exe	C:\WINDOWS\Prefetch\SVCHOST.EXE-3CF81F86.pf
13-10-2025 01:0...	Run .EXE file	ai.exe	C:\PROGRAM FILES\MICROSOFT OFFICE\r...	Microsoft Corporation, ...	exe	C:\WINDOWS\Prefetch\AI.EXE-C5B0F666.pf
13-10-2025 01:0...	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 01:0...	Run .EXE file	WmiPrvSE.exe	C:\Windows\System32\wbem\WmiPrvSE.exe	Microsoft Corporation, ...	exe	C:\WINDOWS\Prefetch\WMIPRVSE.EXE-E8B8DD29.pf
13-10-2025 01:0...	Run .EXE file	WINWORD.EXE	C:\PROGRAM FILES\MICROSOFT OFFICE\r...	Microsoft Corporation, ...	EXE	C:\WINDOWS\Prefetch\WINWORD.EXE-AB6EC2FA.pf
13-10-2025 01:0...	Run .EXE file	chrome.exe	C:\PROGRAM FILES\Google\Chrome\APPL...	Google LLC, Google Chr...	exe	C:\WINDOWS\Prefetch\CHROME.EXE-AED7BA45.pf
13-10-2025 01:0...	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 01:0...	Select file in open/save ...	Exp 6.pdf	C:\Users\Sivarangini\Downloads\Exp 6.pdf		pdf	HKEY_CURRENT_USER\Software\Microsoft\Windows\Current...
13-10-2025 01:0...	Run .EXE file	dllhost.exe	C:\Windows\System32\dllhost.exe	Microsoft Corporation, ...	exe	C:\WINDOWS\Prefetch\DLLHOST.EXE-7D5CE0CA.pf
13-10-2025 01:0...	Run .EXE file	SEARCHFILTERHOST.EXE	C:\Windows\System32\SEARCHFILTERHOS...	Microsoft Corporation, ...	EXE	C:\WINDOWS\Prefetch\SEARCHFILTERHOST.EXE-44162447.pf
13-10-2025 01:0...	Run .EXE file	chrome.exe	C:\PROGRAM FILES\Google\Chrome\APPL...	Google LLC, Google Chr...	exe	C:\WINDOWS\Prefetch\CHROME.EXE-AED7BA4A.pf
13-10-2025 01:0...	Run .EXE file	chrome.exe	C:\PROGRAM FILES\Google\Chrome\APPL...	Google LLC, Google Chr...	exe	C:\WINDOWS\Prefetch\CHROME.EXE-AED7BA3D.pf
13-10-2025 01:0...	Run .EXE file	RUNTIMEBROKER.EXE	C:\WINDOWS\SYSTEM32\RUNTIMEBROKE...	Microsoft Corporation, ...	EXE	C:\WINDOWS\Prefetch\RUNTIMEBROKER.EXE-F8127469.pf

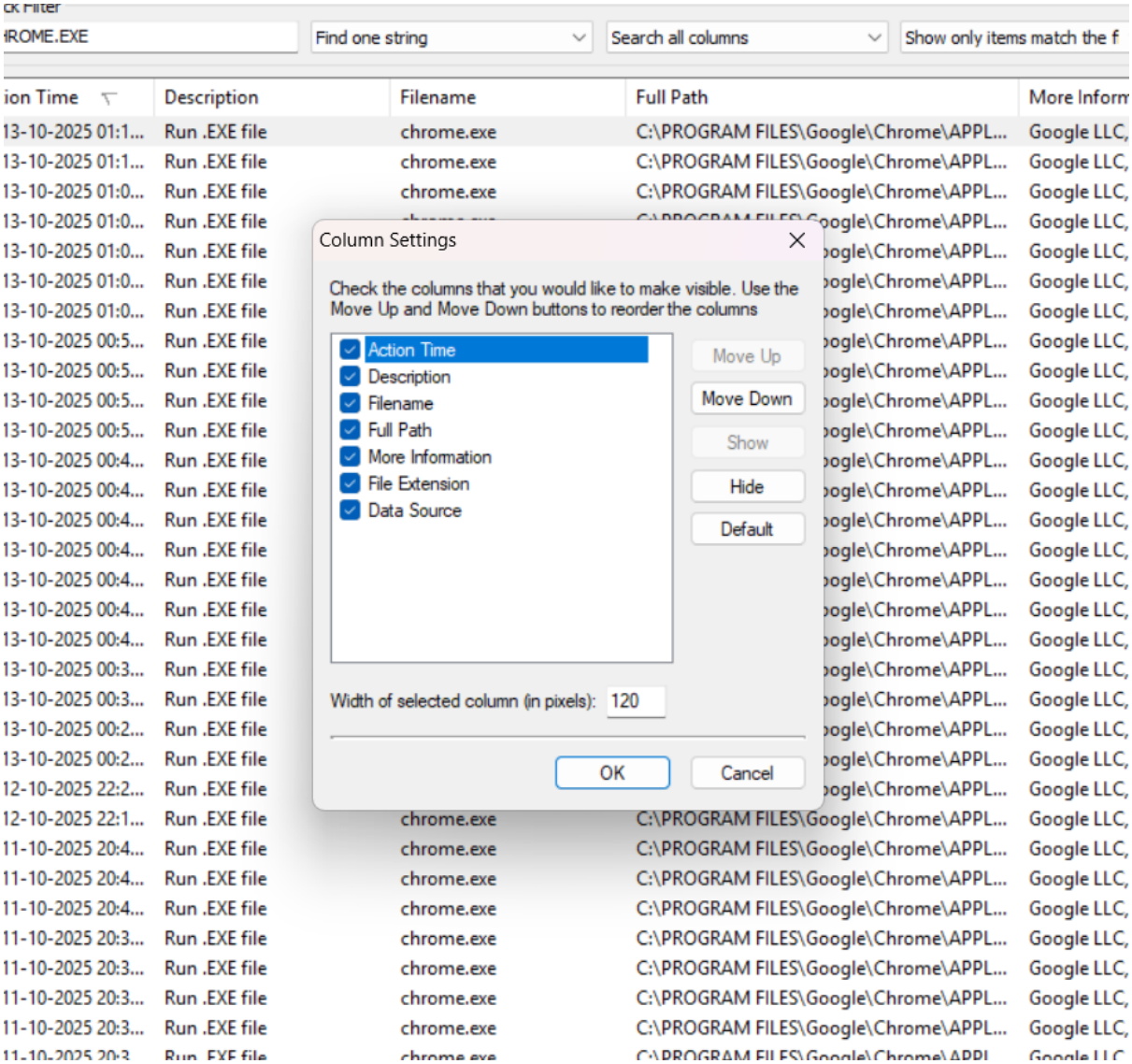


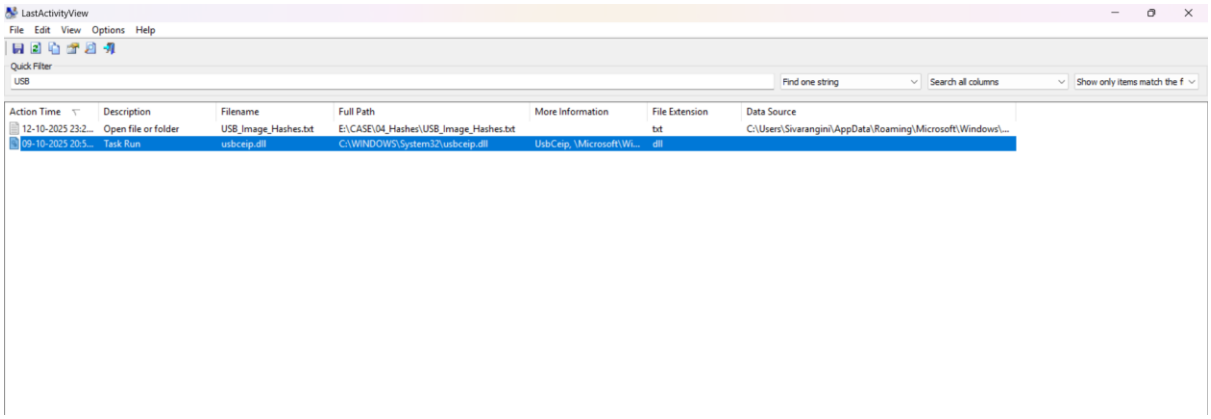
Quick Filter

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	un .EXE file	chrome.exe	C:\PROGRAM FILES\Google\Chrome\APPL...	Google LLC, Google Chr...	exe	C:\WINDOWS\Prefetch\CHROME.EXE-AED7BA4A.pf
13-10-2025 01:1...	Run .EXE file	chrome.exe	C:\PROGRAM FILES\Google\Chrome\APPL...	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\APPL...	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\APPL...	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\APPL...	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\APPL...	Google LLC, Google Chr...	exe	C:\WINDOWS\Prefetch\CHROME.EXE-AED7BA4A.pf
13-10-2025 01:0...	Run .EXE file	chrome.exe	C:\PROGRAM FILES\Google\Chrome\APPL...	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\APPL...	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\APPL...	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\APPL...	Google LLC, Google Chr...	exe	C:\WINDOWS\Prefetch\CHROME.EXE-AED7BA4A.pf
13-10-2025 00:5...	Run .EXE file	chrome.exe	C:\PROGRAM FILES\Google\Chrome\APPL...	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\APPL...	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\APPL...	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\APPL...	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\APPL...	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\APPL...	Google LLC, Google Chr...	exe	C:\WINDOWS\Prefetch\CHROME.EXE-AED7BA4A.pf
13-10-2025 00:4...	Run .EXE file	chrome.exe	C:\PROGRAM FILES\Google\Chrome\APPL...	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\APPL...	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\APPL...	Google LLC, Google Chr...	exe	C:\WINDOWS\Prefetch\CHROME.EXE-AED7BA4A.pf
13-10-2025 00:3...	Run .EXE file	chrome.exe	C:\PROGRAM FILES\Google\Chrome\APPL...	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\APPL...	Google LLC, Google Chr...	exe	C:\WINDOWS\Prefetch\CHROME.EXE-AED7BA4A.pf
13-10-2025 00:2...	Run .EXE file	chrome.exe	C:\PROGRAM FILES\Google\Chrome\APPL...	Google LLC, Google Chr...	exe	C:\WINDOWS\Prefetch\CHROME.EXE-AED7BA45.pf
12-10-2025 22:2...	Run .EXE file	chrome.exe	C:\PROGRAM FILES\Google\Chrome\APPL...	Google LLC, Google Chr...	exe	C:\WINDOWS\Prefetch\CHROME.EXE-AED7BA4A.pf
12-10-2025 22:1...	Run .EXE file	chrome.exe	C:\PROGRAM FILES\Google\Chrome\APPL...	Google LLC, Google Chr...	exe	C:\WINDOWS\Prefetch\CHROME.EXE-AED7BA4A.pf
11-10-2025 20:4...	Run .EXE file	chrome.exe	C:\PROGRAM FILES\Google\Chrome\APPL...	Google LLC, Google Chr...	exe	C:\WINDOWS\Prefetch\CHROME.EXE-AED7BA48.pf
11-10-2025 20:4...	Run .EXE file	chrome.exe	C:\PROGRAM FILES\Google\Chrome\APPL...	Google LLC, Google Chr...	exe	C:\WINDOWS\Prefetch\CHROME.EXE-AED7BA40.pf
11-10-2025 20:4...	Run .EXE file	chrome.exe	C:\PROGRAM FILES\Google\Chrome\APPL...	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\APPL...	Google LLC, Google Chr...	exe	C:\WINDOWS\Prefetch\CHROME.EXE-AED7BA46.pf
11-10-2025 20:3...	Run .EXE file	chrome.exe	C:\PROGRAM FILES\Google\Chrome\APPL...	Google LLC, Google Chr...	exe	C:\WINDOWS\Prefetch\CHROME.EXE-AED7BA47.pf
11-10-2025 20:3...	Run .EXE file	chrome.exe	C:\PROGRAM FILES\Google\Chrome\APPL...	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\APPL...	Google LLC, Google Chr...	exe	C:\WINDOWS\Prefetch\CHROME.EXE-AED7BA40.pf
11-10-2025 20:3...	Run .EXE file	chrome.exe	C:\PROGRAM FILES\Google\Chrome\APPL...	Google LLC, Google Chr...	exe	C:\WINDOWS\Prefetch\CHROME.EXE-AED7BA3C.pf
11-10-2025 15:0...	Run .EXE file	chrome.exe	C:\PROGRAM FILES\Google\Chrome\APPL...	Google LLC, Google Chr...	exe	C:\WINDOWS\Prefetch\CHROME.EXE-AED7BA46.pf
11-10-2025 15:0...	Software Installation	chrome.exe	C:\Program Files\Google\Chrome\Applicat...	Google Chrome	exe	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Curre...


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
13-10-2025 01:0... Run .EXE file
13-10-2025 01:0... Run .EXE file
13-10-2025 01:0... Run .EXE file
13-10-2025 00:5... Run .EXE file
13-10-2025 00:5... Run .EXE file
13-10-2025 00:5... Run .EXE file
13-10-2025 00:5... Run .EXE file
13-10-2025 00:4... Run .EXE file
13-10-2025 00:4... Run .EXE file
13-10-2025 00:4... Run .EXE file
13-10-2025 00:4... Run .EXE file
13-10-2025 00:4... Run .EXE file
13-10-2025 00:4... Run .EXE file
13-10-2025 00:4... Run .EXE file
13-10-2025 00:3... Run .EXE file
13-10-2025 00:3... Run .EXE file
13-10-2025 00:2... Run .EXE file
13-10-2025 00:2... Run .EXE file
12-10-2025 22:2... Run .EXE file
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,
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 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.