# 19-12-2023(Tuesday) Digital Forensics Practical Experiment)

# Title: Examine the Last Activity of Your PC(Practical)

[Experiment procedure in detail step-by-step process]

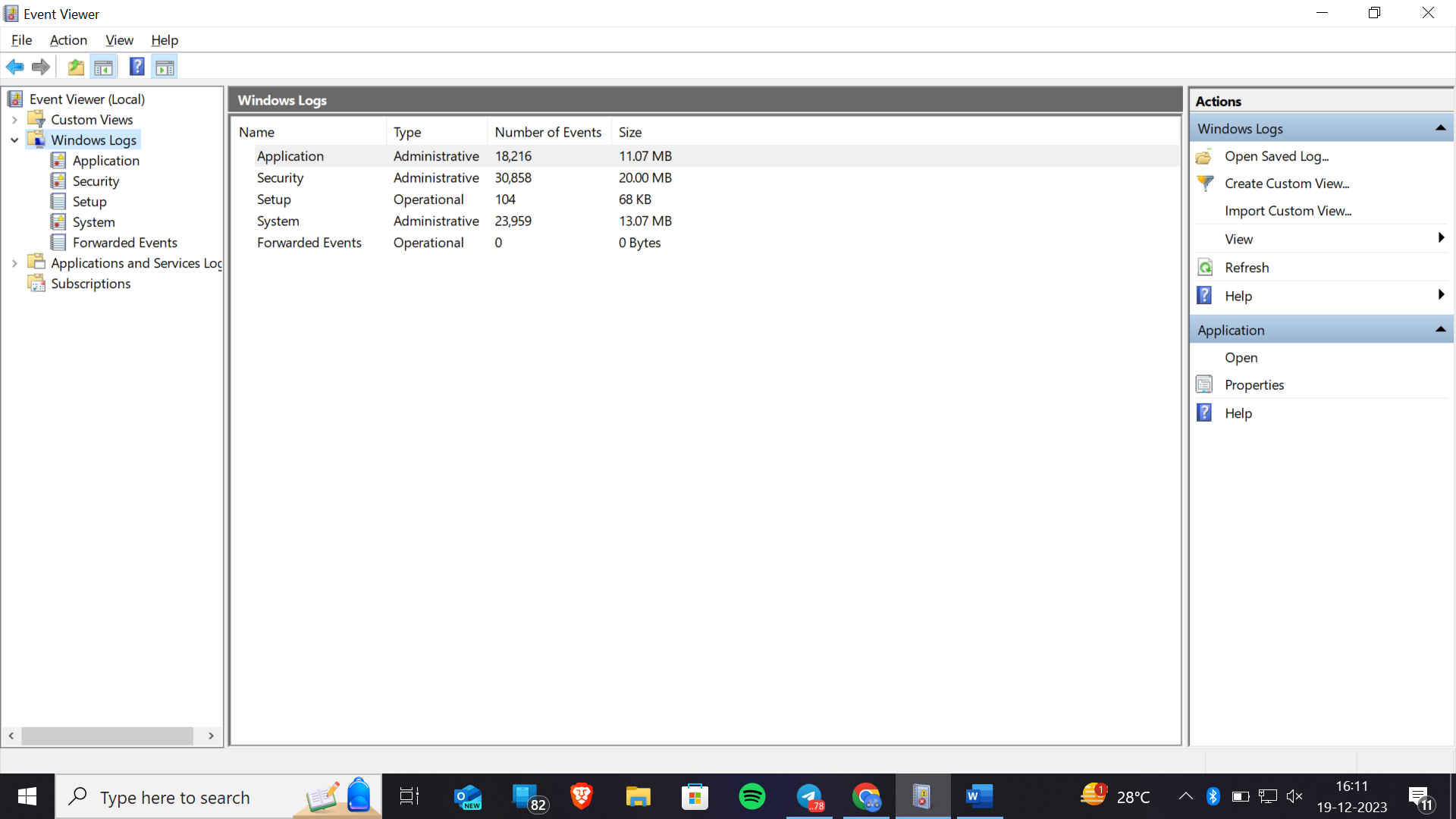
## Windows Event Viewer:

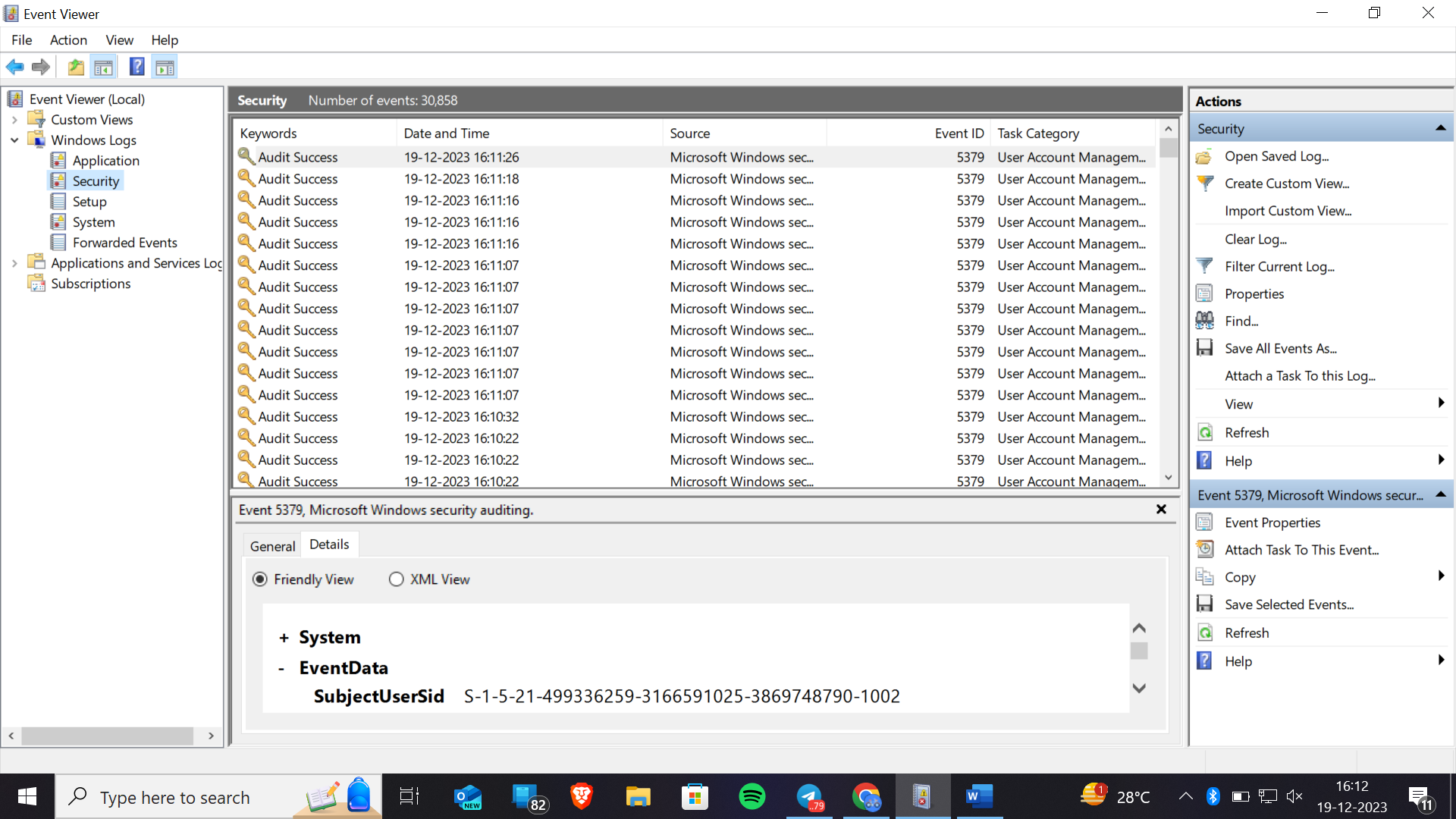
Procedure:

Press Win + X and select "Event Viewer" from the menu.

Navigate to "Windows Logs" and choose "Security" or "System." Look for events around the specific time of interest.





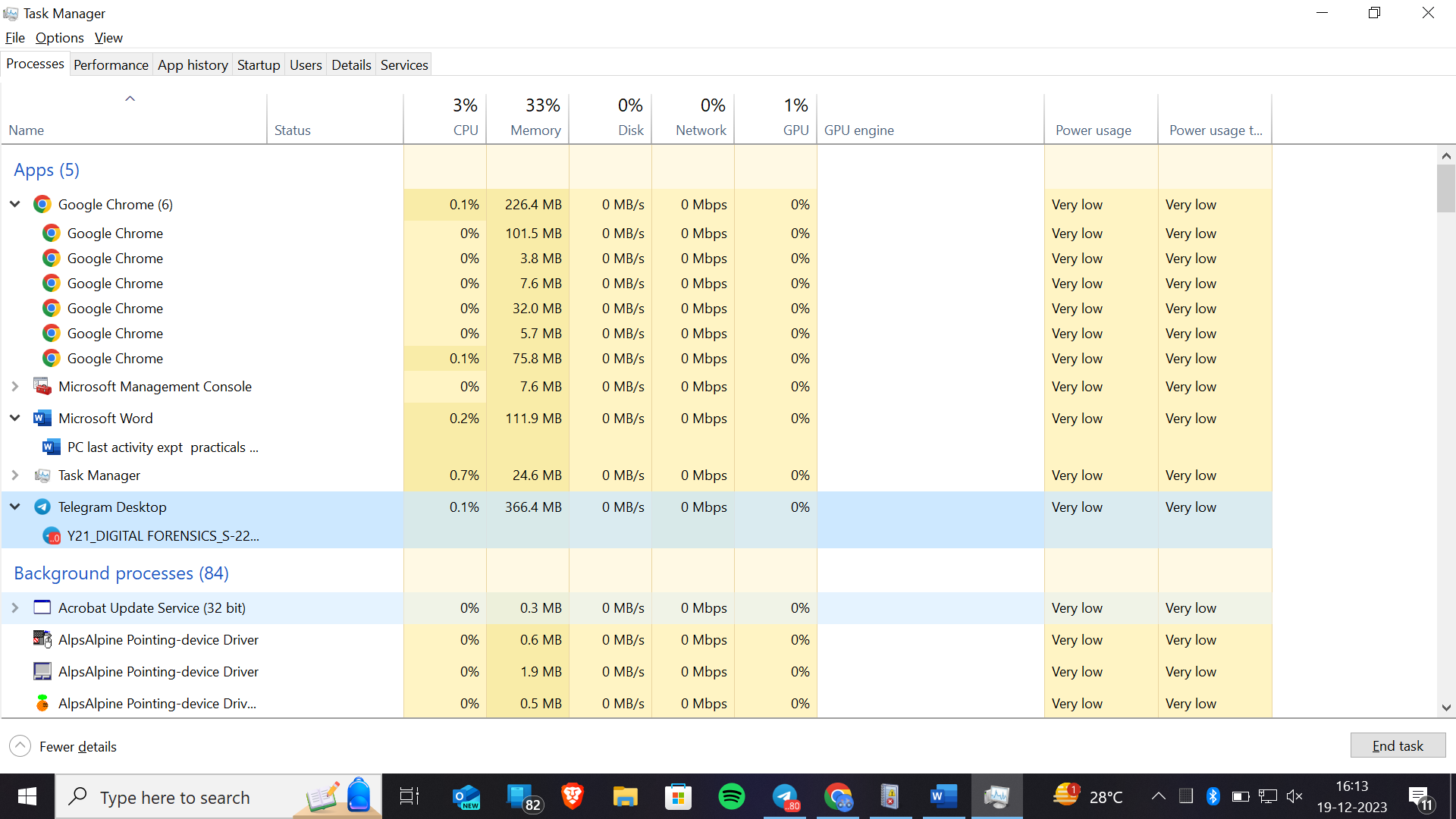


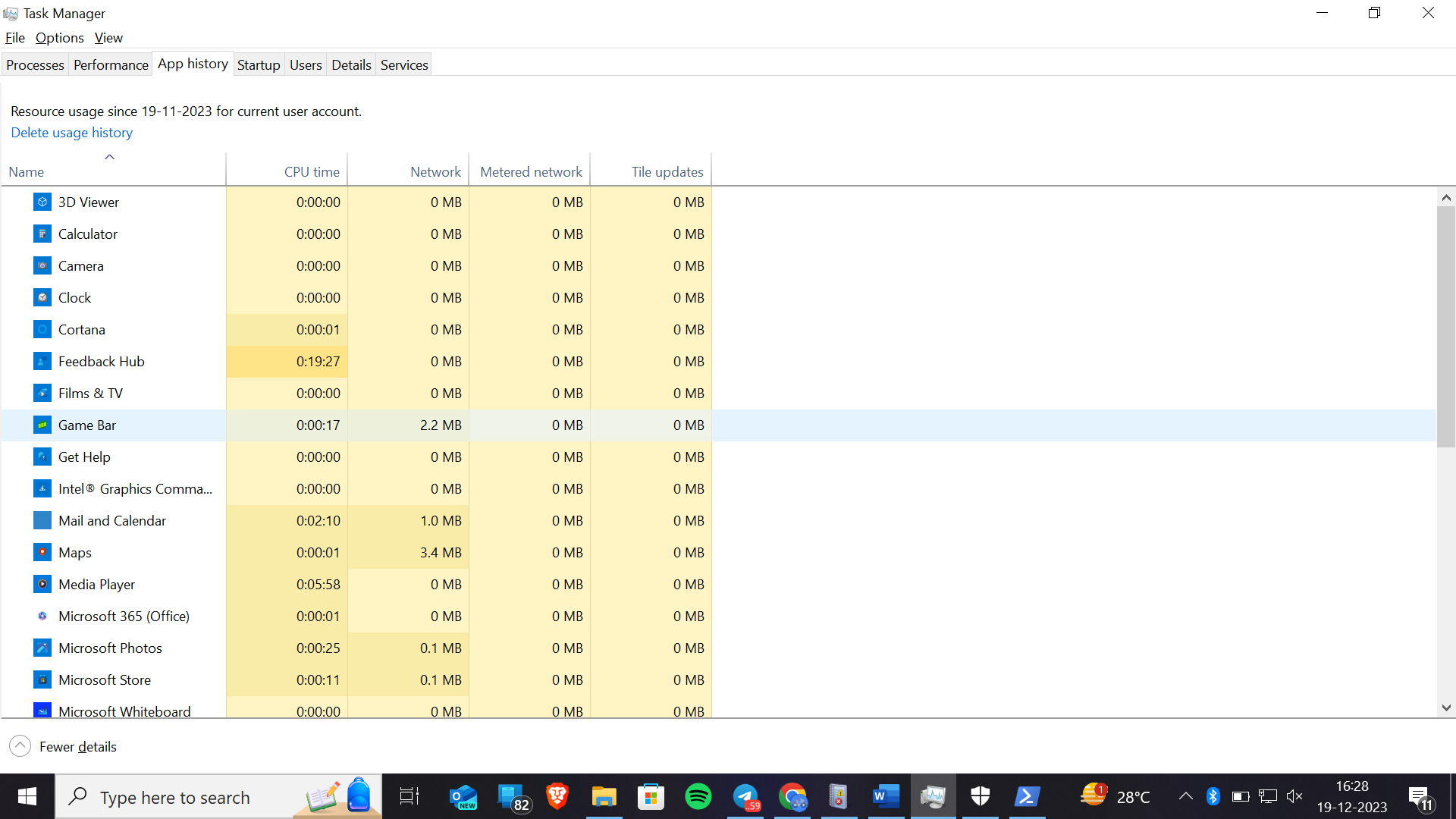
## Task Manager:

Procedure:

Right-click on the taskbar and select "Task Manager" or press Ctrl + Shift + Esc. Check the "Processes" tab for currently running applications.

Examine the "App history" or "Details" tab for recent application activity.

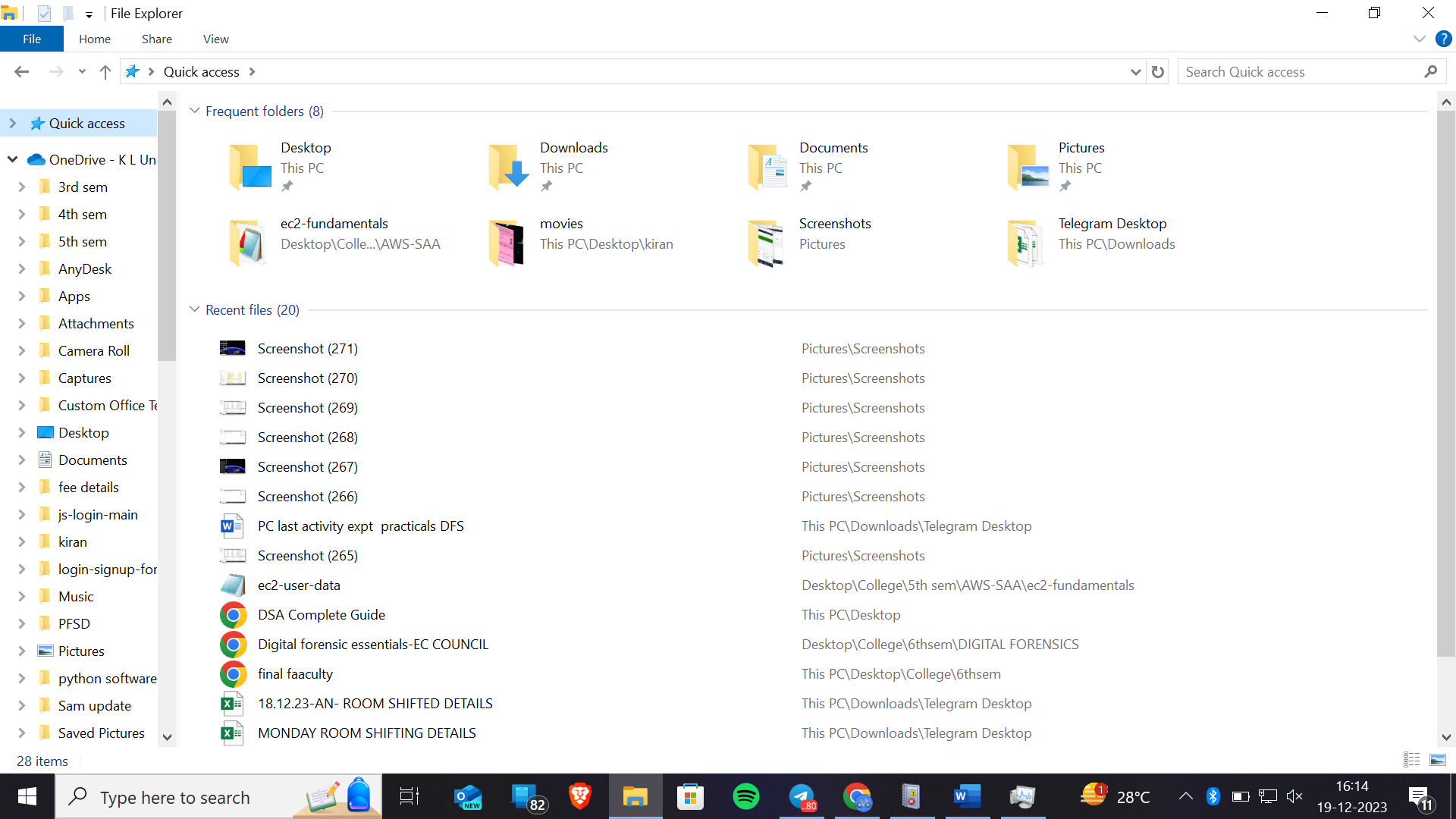




## File Explorer (Recent Files):

Procedure:

Open File Explorer and navigate to "Quick access" or "Recent files." Review the list of recently accessed files.



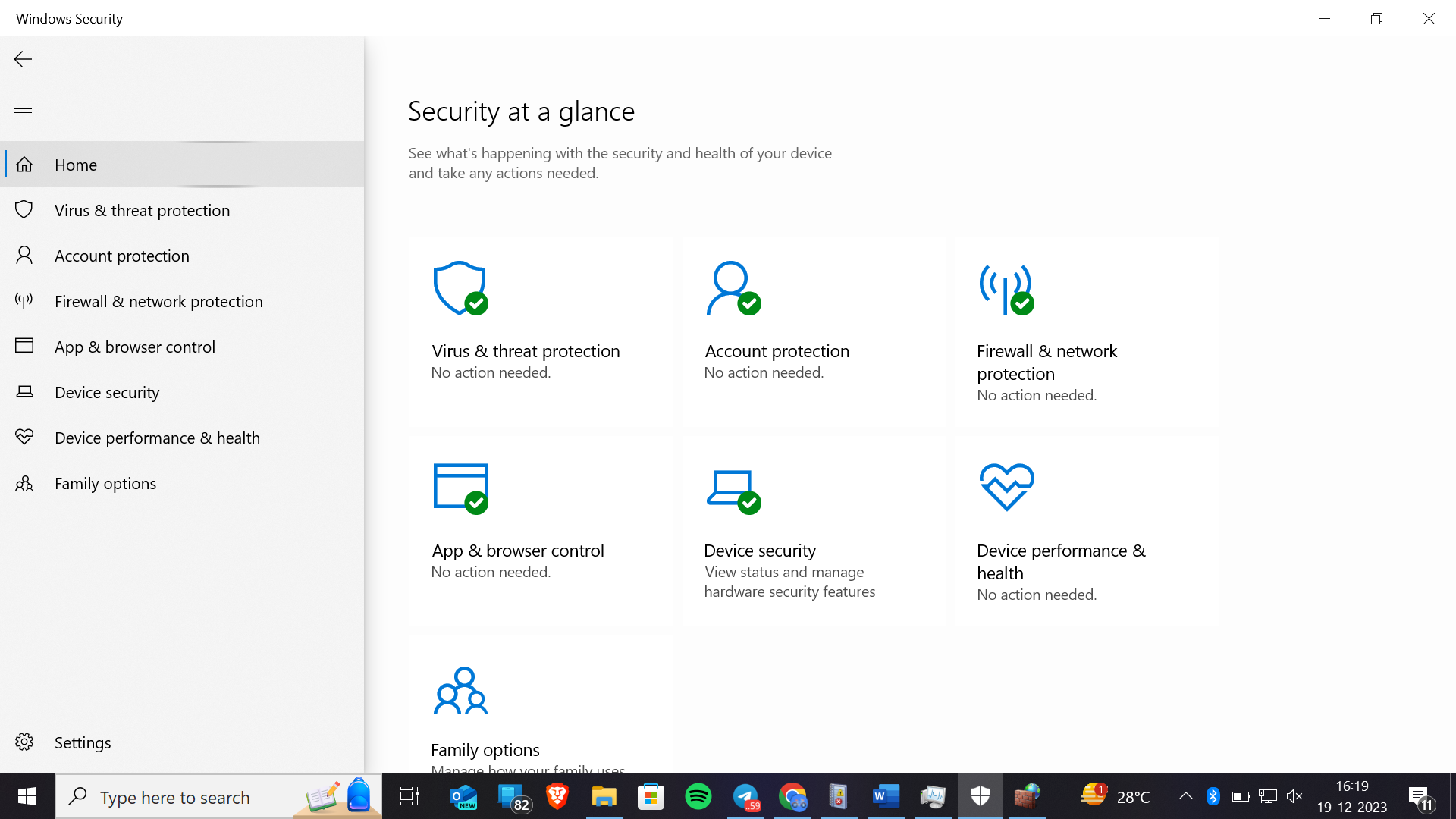
## Security Software Logs:

Procedure:

Access the interface of your installed security software (antivirus, firewall, etc.).

Check logs or history for recent security events. Program:

Depends on the installed security software (e.g., Norton, McAfee).



## System Resource Monitoring Tools:

Procedure:

Use built-in performance monitoring tools like Resource Monitor. Check for recent CPU, memory, and disk activity.

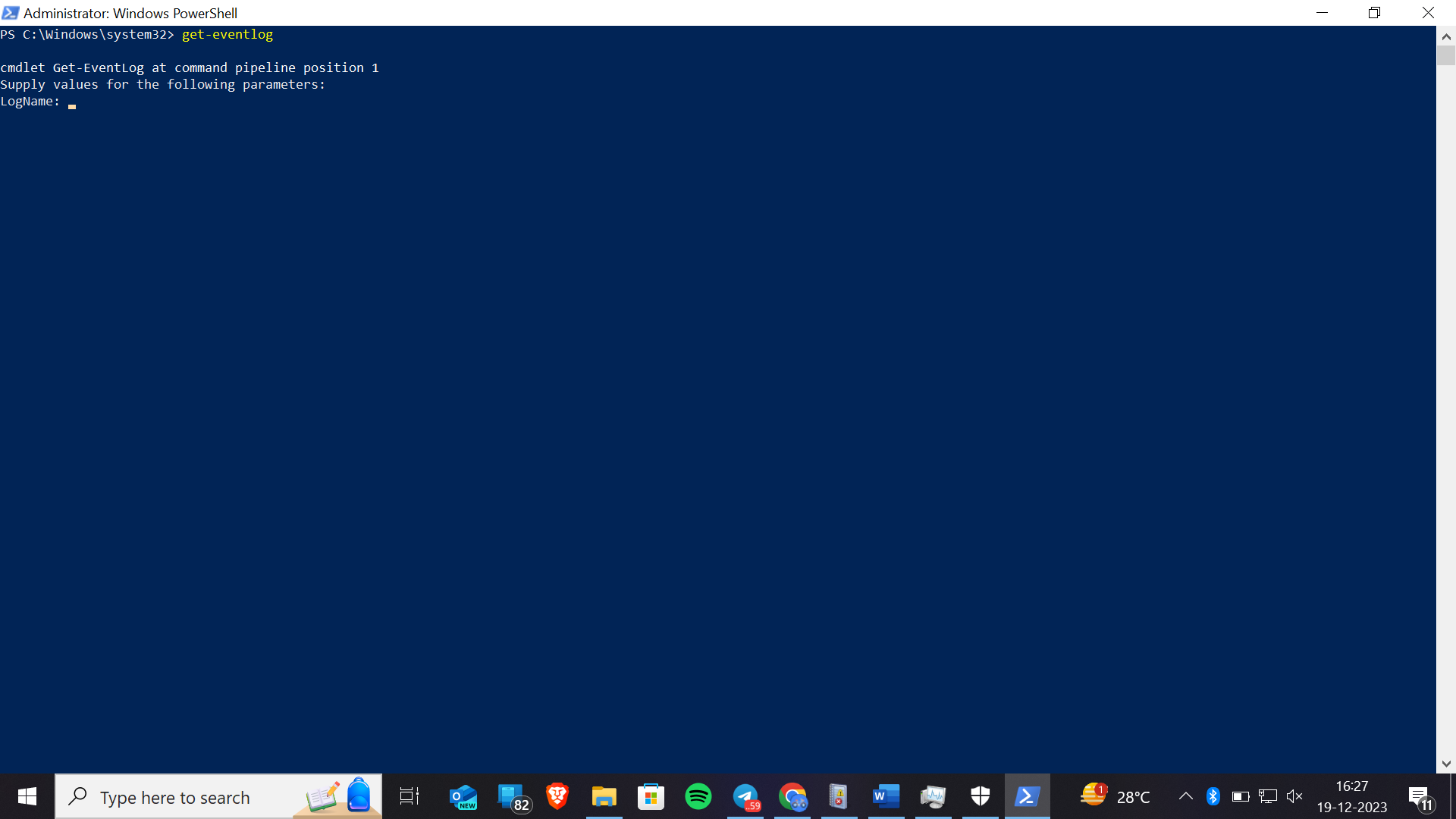
## 

## PowerShell Commands:

Procedure:

Open PowerShell as an administrator.

Use commands like Get-EventLog or Get-WinEvent to fetch system logs.



## Third-Party System Monitoring Tools:

Procedure:

Install a third-party system monitoring tool like Sysinternals Suite.

Utilize tools such as Process Explorer for detailed process information.

Screenshot

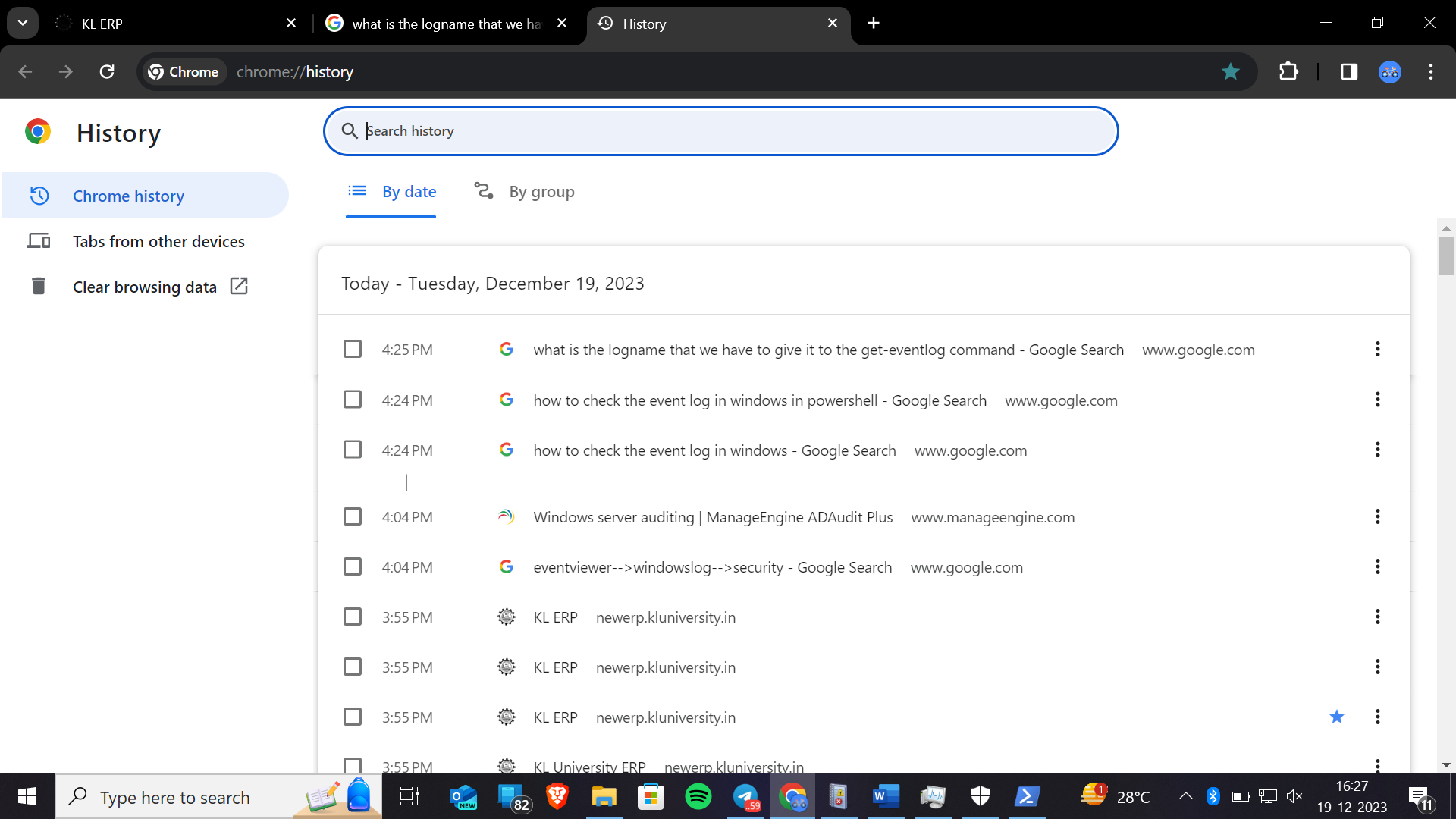
## Browser History:

Procedure:

Open your web browser and check the browsing history. Review visited websites and the time of access.

Program:

Built-in to web browsers (e.g., Chrome, Firefox).



## System Logs:

Procedure:

Open "Event Viewer" and navigate to "Windows Logs" -> "System." Look for system-related events around the desired time.

