

EXP NO: 5

View Last Activity of Your PC

Aim :

How to View Last Activity of Your PC

Procedure :

LastActivityView is a tool for Windows operating system that collects information from various sources on a running system, and displays a log of actions made by the user and events occurred on this computer.

| Actual Time | Description | Process | Full Path | More Information | File Extension | Data Source |
|-------------------|-------------------------|---------------------------------------|--|-------------------------------------|----------------|--|
| 10/9/2023 6:11:00 | Run EXE File | cmd.exe | C:\Windows\WinSxS\X-MSDN-MICROSOFT... | Microsoft Corporation... | .exe | C:\WINDOWS\Fetch\CONTENT\EX-404087.gp |
| 10/9/2023 6:10:51 | Run EXE File | dllhost.exe | C:\Windows\System32\dllhost.exe | Microsoft Corporation... | .exe | C:\WINDOWS\Fetch\EXLHOST\EX-70523CA.gp |
| 10/9/2023 6:10:54 | Run EXE File | dllhost.exe | C:\Windows\System32\dllhost.exe | Microsoft Corporation... | .exe | C:\WINDOWS\Fetch\EXLHOST\EX-387099.gp |
| 10/9/2023 6:10:54 | Run EXE File | dllhost.exe | C:\Windows\System32\dllhost.exe | Microsoft Corporation... | .exe | C:\WINDOWS\Fetch\EXLHOST\EX-5857022.gp |
| 10/9/2023 6:10:54 | Run EXE File | dllhost.exe | C:\Windows\System32\dllhost.exe | Microsoft Corporation... | .exe | C:\WINDOWS\Fetch\EXLHOST\EX-1948310.gp |
| 10/9/2023 6:10:51 | Run EXE File | OpenWith.exe | C:\Windows\System32\OpenWith.exe | Microsoft Corporation... | .exe | C:\WINDOWS\Fetch\OPENWITH\EX-483038.gp |
| 10/9/2023 6:10:51 | Run EXE File | SEARCHHOST.EXE | C:\Windows\System32\SEARCHHOST.EXE | Microsoft Corporation... | .EXE | C:\WINDOWS\Fetch\SEARCHHOST\EX-483038.gp |
| 10/9/2023 6:10:51 | Run EXE File | svchost.exe | C:\Windows\System32\svchost.exe | Microsoft Corporation... | .exe | C:\WINDOWS\Fetch\SVCHOST\EX-1632049.gp |
| 10/9/2023 6:10:51 | Run EXE File | chrome.exe | C:\PROGRAM FILES\Google\Chrome\APPL... | Google LLC, Google Co... | .exe | C:\WINDOWS\Fetch\CHROME\EX-4873444.gp |
| 10/9/2023 6:10:51 | Run EXE File | chrome.exe | C:\PROGRAM FILES\Google\Chrome\APPL... | Google LLC, Google Co... | .exe | C:\WINDOWS\Fetch\CHROME\EX-4873433.gp |
| 10/9/2023 6:10:51 | Run EXE File | svchost.exe | C:\Windows\System32\svchost.exe | Microsoft Corporation... | .exe | C:\WINDOWS\Fetch\SVCHOST\EX-321878.gp |
| 10/9/2023 6:10:51 | Run EXE File | WinPcap.exe | C:\Windows\System32\WinPcap.exe | Microsoft Corporation... | .exe | C:\WINDOWS\Fetch\WINPCAP\EX-5880323.gp |
| 10/9/2023 6:10:51 | Run EXE File | SEARCHHOST.EXE | C:\Windows\WinSxS\X-MSDN-MICROSOFT... | Microsoft Corporation... | .EXE | C:\WINDOWS\Fetch\SEARCHHOST\EXLHOST\EX-483038... |
| 10/9/2023 6:10:51 | Open File in Explorer | C:\WINDOWS\WinSxS\X-MSDN-MICROSOFT... | Open S:\WEB AND DIGITAL FORENSIC... | Open S:\WEB AND DIGITAL FORENSIC... | | C:\Users\Kavya\AppData\Roaming\Microsoft\Windows\Re... |
| 10/9/2023 6:10:51 | Open File in Explorer | NEW FOLDER | Open S:\WEB AND DIGITAL FORENSIC... | Open S:\WEB AND DIGITAL FORENSIC... | | C:\Users\Kavya\AppData\Roaming\Microsoft\Windows\Re... |
| 10/9/2023 6:10:51 | View Folder in Explorer | new1 | Open S:\WEB AND DIGITAL FORENSIC... | Open S:\WEB AND DIGITAL FORENSIC... | | HEXY CURRENT_USER\Software\Classes\Local Settings\Softw... |
| 10/9/2023 6:10:51 | View Folder in Explorer | | Open S:\WEB AND DIGITAL FORENSIC... | Open S:\WEB AND DIGITAL FORENSIC... | | HEXY CURRENT_USER\Software\Classes\Local Settings\Softw... |
| 10/9/2023 6:10:51 | Run EXE File | AUDIODG.EXE | C:\WINDOWS\SYSTEM32\AUDIODG.EXE | Microsoft Corporation... | .EXE | C:\WINDOWS\Fetch\AUDIODG\EX-483038.gp |
| 10/9/2023 6:10:51 | Run EXE File | svchost.exe | C:\Windows\System32\svchost.exe | Microsoft Corporation... | .exe | C:\WINDOWS\Fetch\SVCHOST\EX-1632049.gp |
| 10/9/2023 6:10:51 | Run EXE File | WINPACDLOG.DLL | C:\PROGRAM FILES\WINPACDLOG.DLL | Microsoft Corporation... | .dll | C:\WINDOWS\Fetch\WINPACDLOG\EX-483038.gp |
| 10/9/2023 6:10:51 | Run EXE File | svchost.exe | C:\Windows\System32\svchost.exe | Microsoft Corporation... | .exe | C:\WINDOWS\Fetch\SVCHOST\EX-70523CA.gp |
| 10/9/2023 6:10:51 | Run EXE File | SMARTSCREEN.DLL | C:\WINDOWS\SYSTEM32\SMARTSCREEN.DLL | Microsoft Corporation... | .DLL | C:\WINDOWS\Fetch\SMARTSCREEN\EX-5880323.gp |
| 10/9/2023 6:10:51 | Run EXE File | svchost.exe | C:\Windows\System32\svchost.exe | Microsoft Corporation... | .exe | C:\WINDOWS\Fetch\EXLHOST\EX-70523CA.gp |
| 10/9/2023 6:10:51 | Run EXE File | svchost.exe | C:\Windows\System32\svchost.exe | Microsoft Corporation... | .exe | C:\WINDOWS\Fetch\EXLHOST\EX-387099.gp |
| 10/9/2023 6:10:51 | Run EXE File | svchost.exe | C:\Windows\System32\svchost.exe | Microsoft Corporation... | .exe | C:\WINDOWS\Fetch\EXLHOST\EX-5857022.gp |
| 10/9/2023 6:10:51 | Run EXE File | FILECAUTH.DLL | C:\PROGRAM FILES\MICROSOFT DYNAMIC... | Microsoft Corporation... | .DLL | C:\WINDOWS\Fetch\FILECAUTH\EX-70523CA.gp |
| 10/9/2023 6:10:51 | Run EXE File | audiodg.exe | C:\Windows\System32\audiodg.exe | Microsoft Corporation... | .exe | C:\WINDOWS\Fetch\AUDIODG\EX-70523CA.gp |
| 10/9/2023 6:10:51 | View Folder in Explorer | | Open S:\WEB AND DIGITAL FORENSIC... | Open S:\WEB AND DIGITAL FORENSIC... | | HEXY CURRENT_USER\Software\Classes\Local Settings\Softw... |
| 10/9/2023 6:10:51 | Run EXE File | SEARCHHOST.EXE | C:\Windows\System32\SEARCHHOST.EXE | Microsoft Corporation... | .EXE | C:\WINDOWS\Fetch\SEARCHHOST\EXLHOST\EX-483038.gp |
| 10/9/2023 6:10:51 | Run EXE File | SEARCHHOST.EXE | C:\Windows\WinSxS\X-MSDN-MICROSOFT... | Microsoft Corporation... | .EXE | C:\WINDOWS\Fetch\SEARCHHOST\EXLHOST\EX-483038... |
| 10/9/2023 6:10:51 | Run EXE File | svchost.exe | C:\Windows\System32\svchost.exe | Microsoft Corporation... | .exe | C:\WINDOWS\Fetch\SVCHOST\EX-1632049.gp |
| 10/9/2023 6:10:51 | Run EXE File | chrome.exe | C:\PROGRAM FILES\Google\Chrome\APPL... | Google LLC, Google Co... | .exe | C:\WINDOWS\Fetch\CHROME\EX-4873444.gp |
| 10/9/2023 6:10:51 | Run EXE File | chrome.exe | C:\PROGRAM FILES\Google\Chrome\APPL... | Google LLC, Google Co... | .exe | C:\WINDOWS\Fetch\CHROME\EX-4873433.gp |
| 10/9/2023 6:10:51 | Run EXE File | svchost.exe | C:\Windows\System32\svchost.exe | Microsoft Corporation... | .exe | C:\WINDOWS\Fetch\WINPCAP\EX-5880323.gp |
| 10/9/2023 6:10:51 | Task Fails | Authentication.exe | C:\WINDOWS\system32\Authentication.exe | USO, Windows, Microso... | .exe | |
| 10/9/2023 6:10:51 | Run EXE File | svchost.exe | C:\Windows\System32\svchost.exe | Microsoft Corporation... | .exe | C:\WINDOWS\Fetch\SVCHOST\EX-483038.gp |

Result:

Thus, the forensic tools executed successfully, and the evidence was captured and analyzed accurately.