

# Windows Artifact Experiment Report.

Objective: To perform common user activities on a windows 11 machine and identify the digital artifacts created by these user actions.

## 1. Experiment Setup.

Operating System: Windows 11

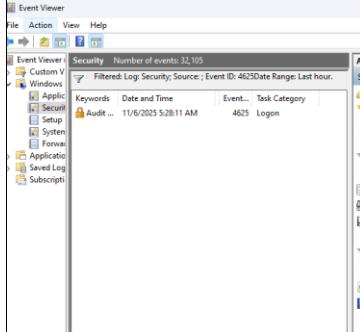
User Account: Local user with administrative privileges.

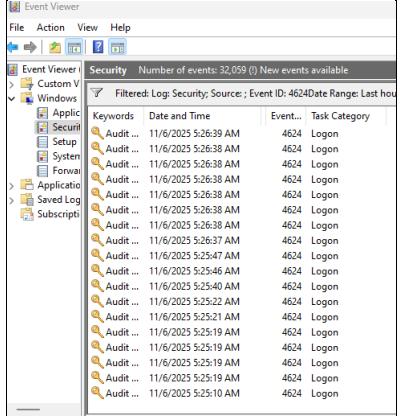
Tools used: Event Viewer, File explore, Registry Editor and DB Browser (SQLite)

## 2. Performed User activities.

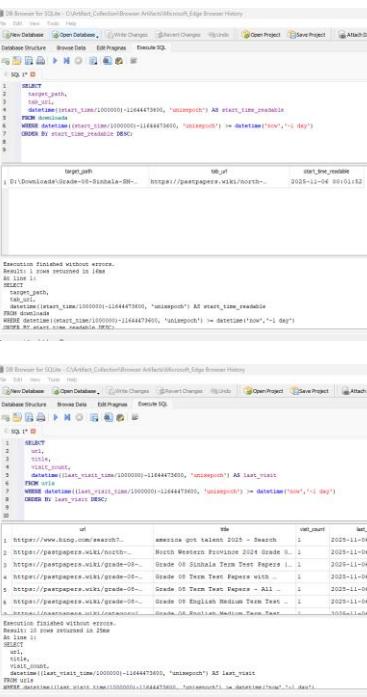
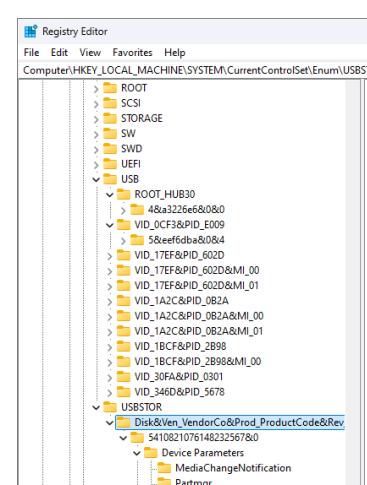
1. Attempted a failed logon with an incorrect password.
2. Performed a successful logon using the correct password.
3. Created a new text file in the Document Folder, added some text, and saved it.
4. Opened Microsoft Edge, searched multiple websites and downloaded a file.
5. Connected a USB drive, created a text file inside it and copied another file into the USB.

## 3. Collected Artifacts and Evidence.

Activity	Artifact Location.	Evidence	Description.
Failed logon	Win +R → eventvwr.msc → Windows Logs → Security Log. Or Event Viewer → Windows logs → Security Log.		I filtered log using Event ID :4625

Successful logon	<p>Win +R → eventvwr.msc → Windows Logs → Security Log.</p> <p>Or</p> <p>Event Viewer → Windows logs → Security Log.</p>	 <p>The screenshot shows the Windows Event Viewer interface. The left pane displays a tree view of logs: Custom V, Windows, Application, Security, System, Forwarder, Application, Saved Log, and Subscriptions. The Security log is selected. The right pane shows a list of events under the heading "Security". A filter bar at the top indicates "Filtered: Log: Security; Source: ; Event ID: 4624 Date Range: Last hour". The list contains 32,059 events. The first few events are listed as follows:</p> <table border="1"> <thead> <tr> <th>Keywords</th><th>Date and Time</th><th>Event...</th><th>Task Category</th></tr> </thead> <tbody> <tr><td>Audit ...</td><td>11/6/2023 5:26:39 AM</td><td>4624</td><td>Logon</td></tr> <tr><td>Audit ...</td><td>11/6/2023 5:26:38 AM</td><td>4624</td><td>Logon</td></tr> <tr><td>Audit ...</td><td>11/6/2023 5:26:37 AM</td><td>4624</td><td>Logon</td></tr> <tr><td>Audit ...</td><td>11/6/2023 5:25:47 AM</td><td>4624</td><td>Logon</td></tr> <tr><td>Audit ...</td><td>11/6/2023 5:25:46 AM</td><td>4624</td><td>Logon</td></tr> <tr><td>Audit ...</td><td>11/6/2023 5:25:40 AM</td><td>4624</td><td>Logon</td></tr> <tr><td>Audit ...</td><td>11/6/2023 5:25:22 AM</td><td>4624</td><td>Logon</td></tr> <tr><td>Audit ...</td><td>11/6/2023 5:25:21 AM</td><td>4624</td><td>Logon</td></tr> <tr><td>Audit ...</td><td>11/6/2023 5:25:19 AM</td><td>4624</td><td>Logon</td></tr> <tr><td>Audit ...</td><td>11/6/2023 5:25:19 AM</td><td>4624</td><td>Logon</td></tr> <tr><td>Audit ...</td><td>11/6/2023 5:25:19 AM</td><td>4624</td><td>Logon</td></tr> <tr><td>Audit ...</td><td>11/6/2023 5:25:19 AM</td><td>4624</td><td>Logon</td></tr> <tr><td>Audit ...</td><td>11/6/2023 5:25:10 AM</td><td>4624</td><td>Logon</td></tr> </tbody> </table>	Keywords	Date and Time	Event...	Task Category	Audit ...	11/6/2023 5:26:39 AM	4624	Logon	Audit ...	11/6/2023 5:26:38 AM	4624	Logon	Audit ...	11/6/2023 5:26:38 AM	4624	Logon	Audit ...	11/6/2023 5:26:38 AM	4624	Logon	Audit ...	11/6/2023 5:26:38 AM	4624	Logon	Audit ...	11/6/2023 5:26:38 AM	4624	Logon	Audit ...	11/6/2023 5:26:37 AM	4624	Logon	Audit ...	11/6/2023 5:25:47 AM	4624	Logon	Audit ...	11/6/2023 5:25:46 AM	4624	Logon	Audit ...	11/6/2023 5:25:40 AM	4624	Logon	Audit ...	11/6/2023 5:25:22 AM	4624	Logon	Audit ...	11/6/2023 5:25:21 AM	4624	Logon	Audit ...	11/6/2023 5:25:19 AM	4624	Logon	Audit ...	11/6/2023 5:25:19 AM	4624	Logon	Audit ...	11/6/2023 5:25:19 AM	4624	Logon	Audit ...	11/6/2023 5:25:19 AM	4624	Logon	Audit ...	11/6/2023 5:25:10 AM	4624	Logon	I filtered log using Event ID :4624
Keywords	Date and Time	Event...	Task Category																																																																								
Audit ...	11/6/2023 5:26:39 AM	4624	Logon																																																																								
Audit ...	11/6/2023 5:26:38 AM	4624	Logon																																																																								
Audit ...	11/6/2023 5:26:38 AM	4624	Logon																																																																								
Audit ...	11/6/2023 5:26:38 AM	4624	Logon																																																																								
Audit ...	11/6/2023 5:26:38 AM	4624	Logon																																																																								
Audit ...	11/6/2023 5:26:38 AM	4624	Logon																																																																								
Audit ...	11/6/2023 5:26:37 AM	4624	Logon																																																																								
Audit ...	11/6/2023 5:25:47 AM	4624	Logon																																																																								
Audit ...	11/6/2023 5:25:46 AM	4624	Logon																																																																								
Audit ...	11/6/2023 5:25:40 AM	4624	Logon																																																																								
Audit ...	11/6/2023 5:25:22 AM	4624	Logon																																																																								
Audit ...	11/6/2023 5:25:21 AM	4624	Logon																																																																								
Audit ...	11/6/2023 5:25:19 AM	4624	Logon																																																																								
Audit ...	11/6/2023 5:25:19 AM	4624	Logon																																																																								
Audit ...	11/6/2023 5:25:19 AM	4624	Logon																																																																								
Audit ...	11/6/2023 5:25:19 AM	4624	Logon																																																																								
Audit ...	11/6/2023 5:25:10 AM	4624	Logon																																																																								
TXT file created	Documents Or Home																																																																										

File opened	C:\Windows\Prefetch\	<table border="1"> <thead> <tr> <th>Name</th><th>Date modified</th><th>Type</th></tr> </thead> <tbody> <tr> <td>CALCULATORAPP.EXE-979F2C0E.pf</td><td>11/6/2025 5:36 AM</td><td>PF Fil</td></tr> <tr> <td>CMD.EXE-8E75B58B.pf</td><td>11/6/2025 9:55 AM</td><td>PF Fil</td></tr> <tr> <td>NOTEPAD.EXE-0B257A77.pf</td><td>11/6/2025 6:13 AM</td><td>PF Fil</td></tr> </tbody> </table>	Name	Date modified	Type	CALCULATORAPP.EXE-979F2C0E.pf	11/6/2025 5:36 AM	PF Fil	CMD.EXE-8E75B58B.pf	11/6/2025 9:55 AM	PF Fil	NOTEPAD.EXE-0B257A77.pf	11/6/2025 6:13 AM	PF Fil	
Name	Date modified	Type													
CALCULATORAPP.EXE-979F2C0E.pf	11/6/2025 5:36 AM	PF Fil													
CMD.EXE-8E75B58B.pf	11/6/2025 9:55 AM	PF Fil													
NOTEPAD.EXE-0B257A77.pf	11/6/2025 6:13 AM	PF Fil													

Browsing History	C:\Users\thira\AppData\Local\Microsoft\Edge\User Data\Default\History		History is basically a database. So I couldn't open it on notepad. So I used DB browser (SQLite) to view the tables. So I filtered this tables as downloads and URLs.
USB connection.	Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR\		

#### 4. Analysis Summary.

- Each action that have done by the user, left identifiable traces within Windows system logs, registry entries and user profile data.
- These traces also known as Artifacts.
- These artifacts can be used in forensic analysis to reconstruct user behavior and verify evidence timelines.

#### 5. Conclusion.

The activity demonstrates that Windows maintains detailed logs and traces of most user actions. During this experiment, I performed several common user activities such as logon attempts, file creation, browsing, and USB usage. Each action generated artifacts that were recorded in different system components.

I used tools such as **Event Viewer**, **Registry Editor**, and **DB Browser for SQLite** to locate and analyze these artifacts.

Event Viewer helped to identify login events, the Registry revealed system-level traces, and DB Browser allowed me to read and interpret browser history records stored in the SQLite database.

This experiment confirmed that even routine activities leave behind digital evidence, highlighting the importance of artifacts in digital forensics and incident analysis.