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

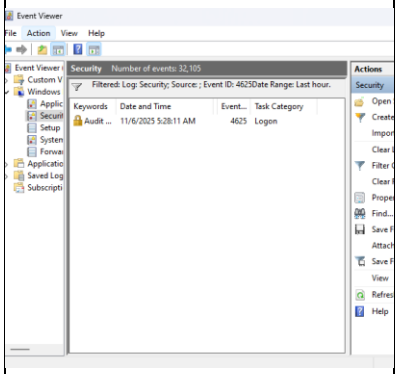
User Account: Local user with administrative privileges.

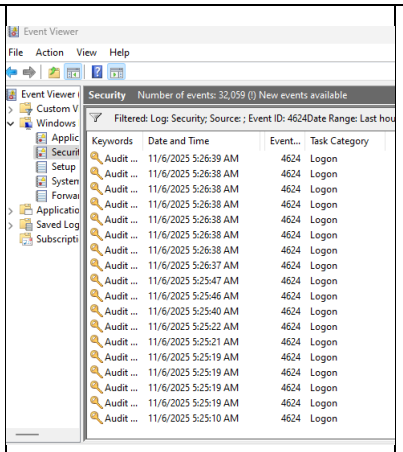
Tools used: Event Viewer, File explore, Registry Editor and DB Browser (SQLite)

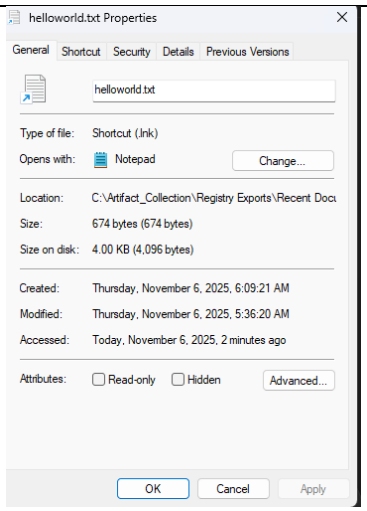
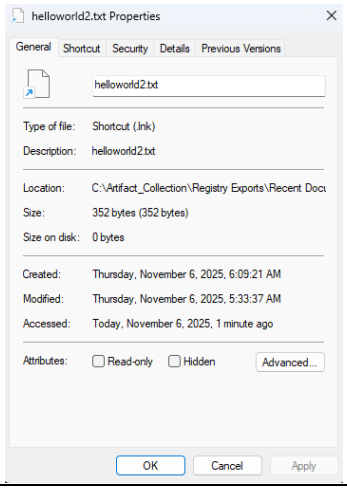
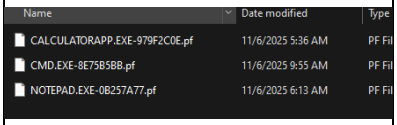
2. Performed User activities.

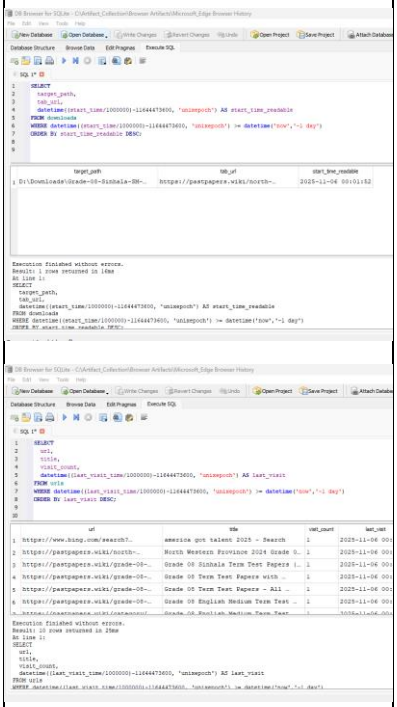
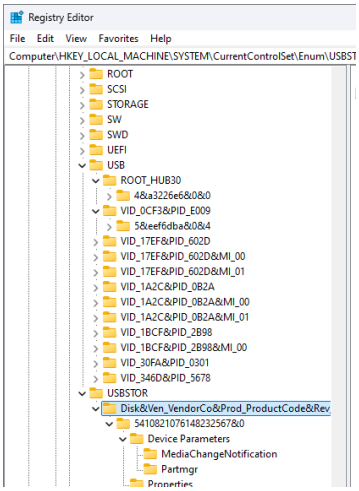
1. Attempted a failed logon with an incorrect password.
2. Performed a successful logon using the correct password.
3. Created a new text file in the Document Folder, added some text, and saved it.
4. Opened Microsoft Edge, searched multiple websites and downloaded a file.
5. Connected a USB drive, created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

Succes sful logon	Win +R → eventvwr.msc →Windows Logs →Security Log. Or Event Viewer →Windows logs →Security Log.		I filtered log using Event ID :4624
TXT file create d	Documents Or Home		

		 	
File opened	C:\Windows\Prefetch\		

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 Summery.

- 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.