Windows Forensics

PART 1: Web Browser Artifacts

Web browser stores valuable forensics information on the user machine. This information is very useful when presented at court. The three important information that can be collected are

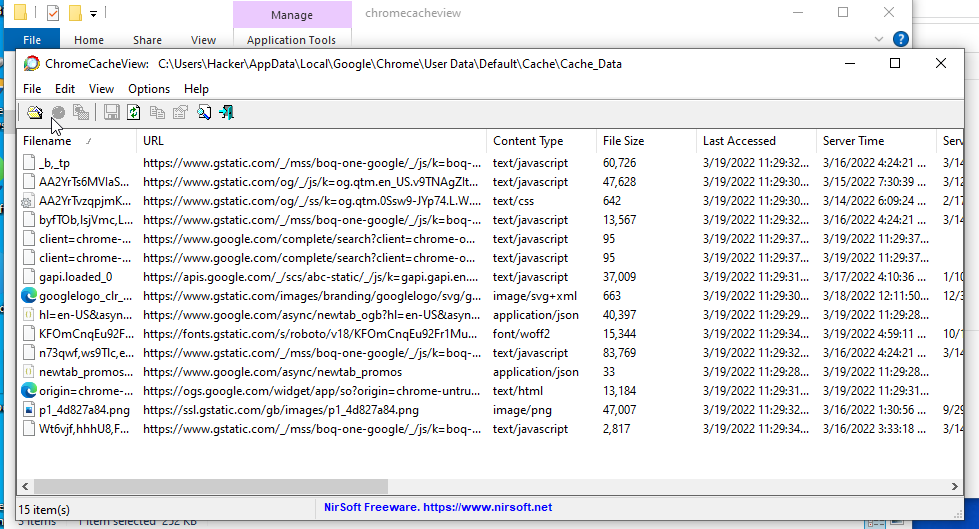
**Browsing** **History**: History of webpages that user views

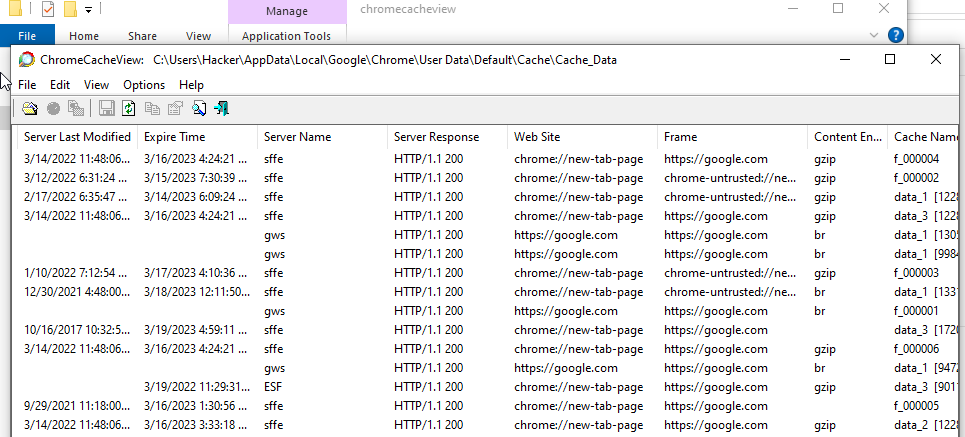
**Caches**: Information like webpages that are stored so that if webpage is loaded again, it does not take as much time as it took at the first place

**Cookies**: Information like tokens and sessions of user that are stored for login purposes

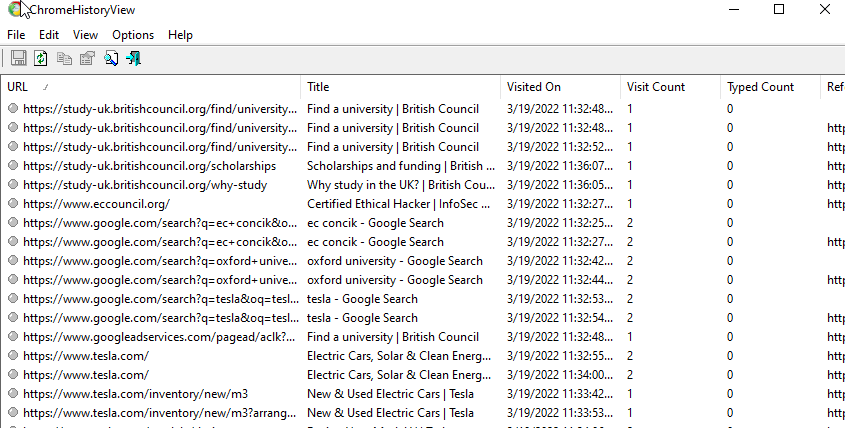
**GOOGLE CHROME**

Here we are using tool called **cacheview** from nirsoft that is used to fetch all the details related to caches that has been stored in the chrome

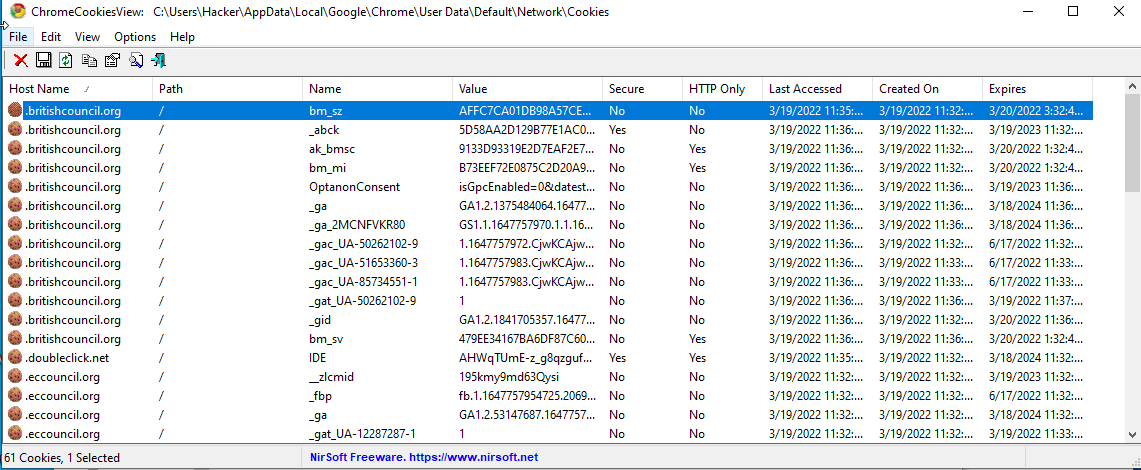




Here we are using tool called **historyview** from nirsoft that is used to fetch all the details related to the websites visited by the user in the chrome

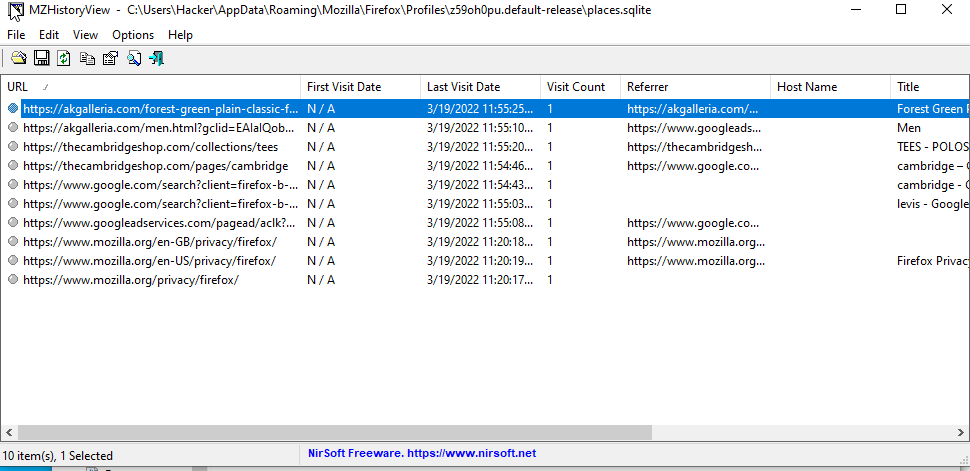


Here we are using tool called **cookieview** from nirsoft that is used to fetch all the details related to cookies and sessions that has been stored in the chrome

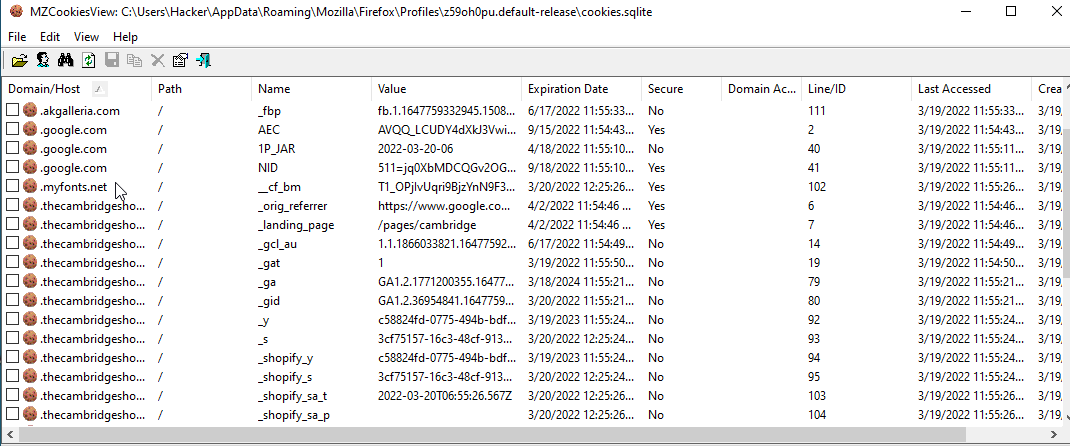


**MOZILLA FIREFOX**

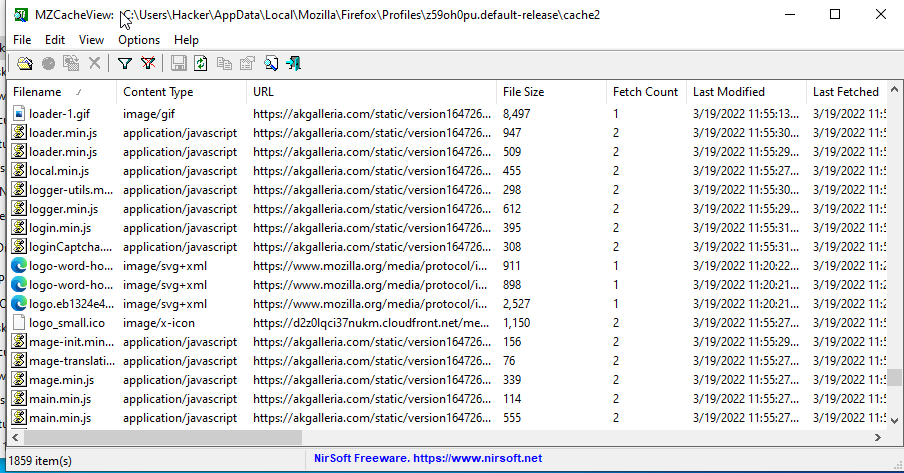
Here we are using tool called **historyview** from nirsoft that is used to fetch all the details related to the websites visited by the user in the Mozilla Firefox



Here we are using tool called **cookieview** from nirsoft that is used to fetch all the details related to cookies and sessions that has been stored in the Mozilla Firefox



Here we are using tool called **cacheview** from nirsoft that is used to fetch all the details related to caches that has been stored in the Mozilla Firefox

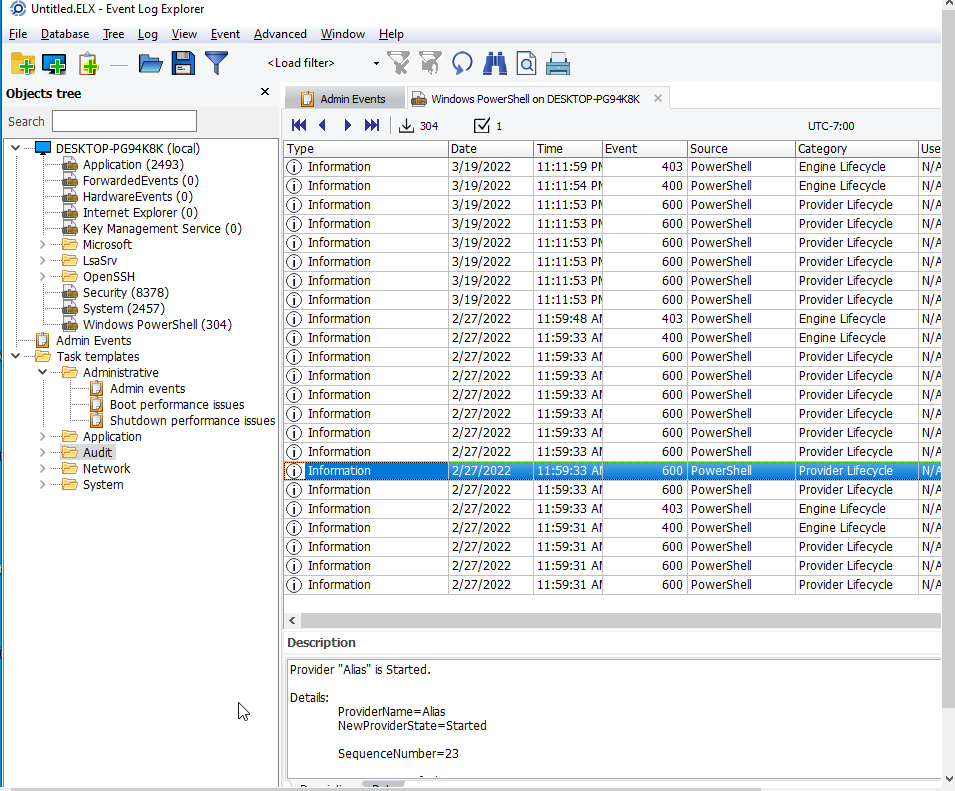


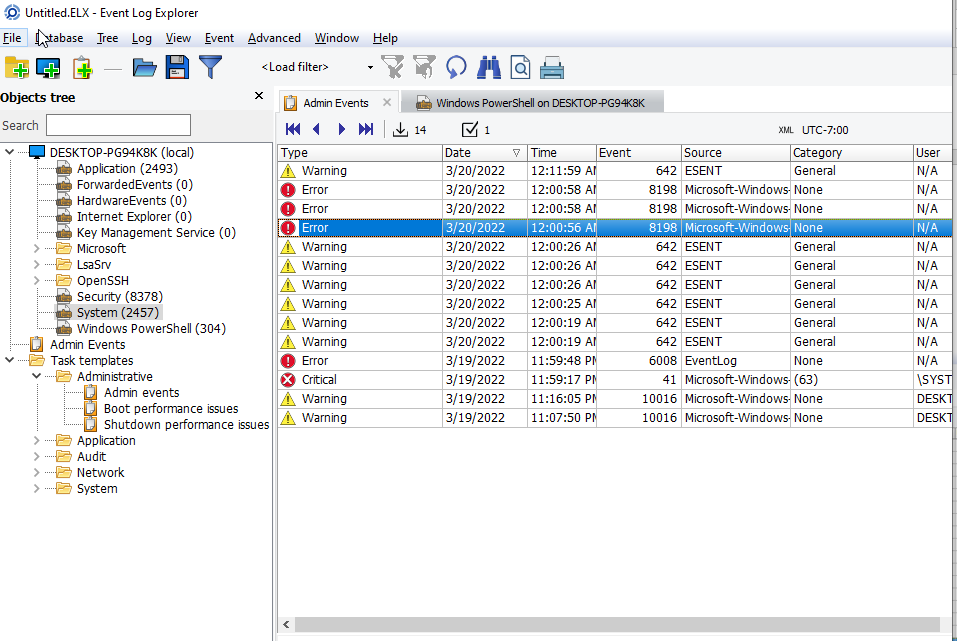
PART 2: Viewing and Analyzing Win Events

In this part, investigators analyze all the security logs, system logs and application logs to get the accurate information about the events leading to cybercrime.

The log file are generally stores in **C:\Windows\System32\config[.]**

We are using a tool called **EventLogXP** that is used to examine all of the logs on our host. We see our Desktop here and on clicking it we further see Application, which contains logs related to the Software that are installed on the machine. We are able to see other modules too such as ForwardEvents, WindowsPowershell, etc.



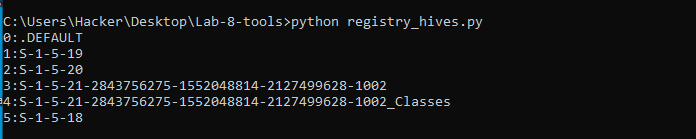


PART 4: Handling Windows Registry Python

Here we will be using python and its library **winreg** to access windows registry files. We can access the keys and its values can be created, read and updated. The content that we can access are HKEY\_USERS, HKEY\_CURRENT\_USER, HKEY\_LOCAL\_MACHINE, HKEY\_CURRENT\_CONFIG, etc.

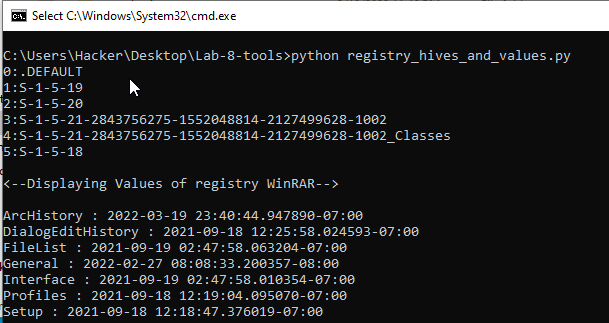
* **Access the registry HKEY\_USERS hives.**

Here we have written a simple python script that access the registry and gets HKEY\_USERS contents out of it.



* **Access the registry HKEY\_USERS keys and its values**

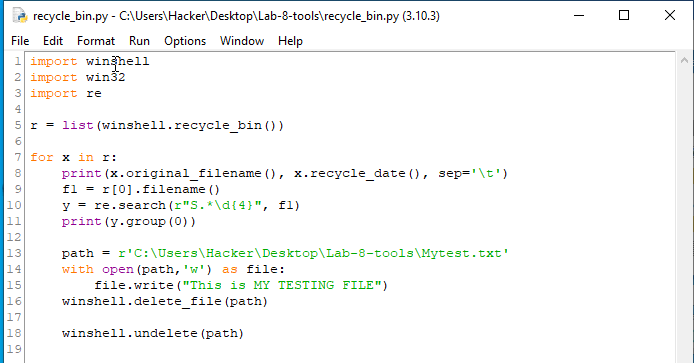
Here we have written another simple python script that access the registry and in the HKEY\_USERS content it goes to the SOFTWARE and get the values of WinRAR.

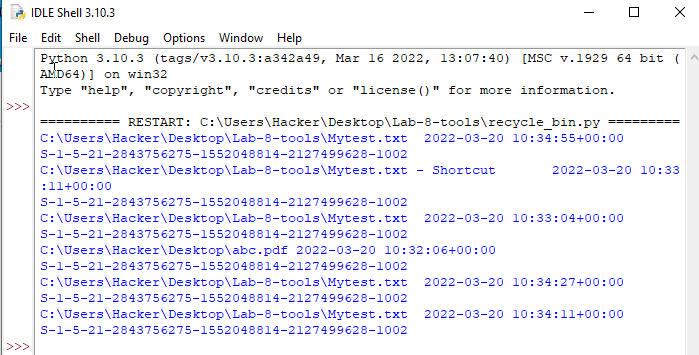


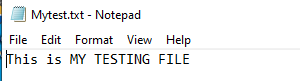
PART 5: Handling Windows Recycle Python

In this part we are using **winshell** library that is used to give us Windows shell functions. One of the function that we are going to using is of recycle bin as we are going to access recycle bin and delete and recover file from it.

Here we have written a script that access the recycle bin , shows us what is inside it . Then it creates a file named “Mytest.txt” and write content in it. Then it deletes the file and then recover it from the recycle bin.







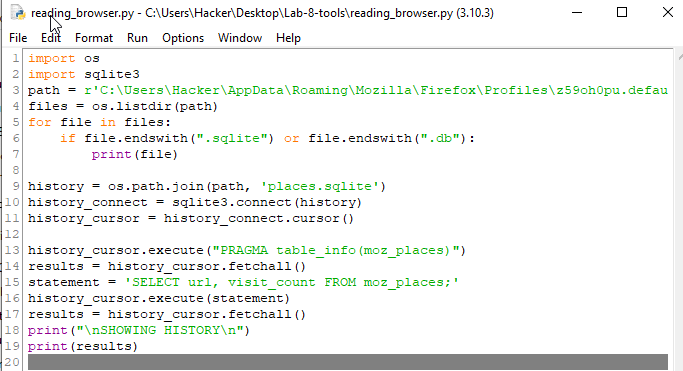
PART 6: Reading Browser History, Cookies and Cache Using Python

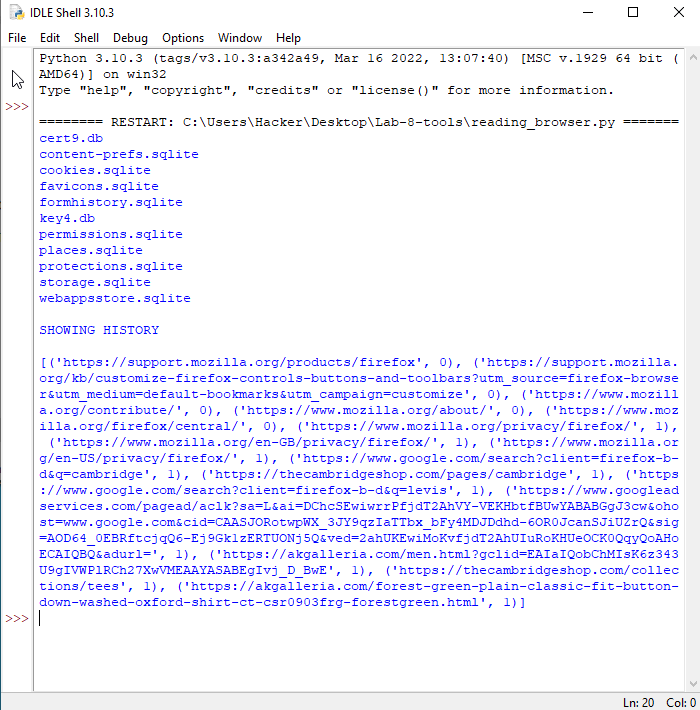
Here we are going to use python to read browsers history

In this script we just gave a path to which our Mozilla Firefox is located and then read the files that have the extension of .sqlite and .db.



Now this script accesses the database files of Mozilla Firefox and then reads the history after that history is shown.





SUMMARY

This lab taught us a lot about windows forensics from getting manual information of web-browser history, cache and cookies to automate python scripts. In the first part we get to know about the util tools of **Nirsoft** that we used to see Google Chrome and Mozilla Firefox history, cache and cookies. Then we used a tool called **EventLogXP** which gave us detailed information about the logs, for example when the system is log-in and which application started at specific time. Then we moved on to python script and learned how to deal with Windows Registry using script as we were able to list the contents of HKEY\_USERS registry. We also learned to delete and recover files from recycle bin using python and to create and write a file. At last, we make use of python script to access the browser and read its history, cache and cookies.