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

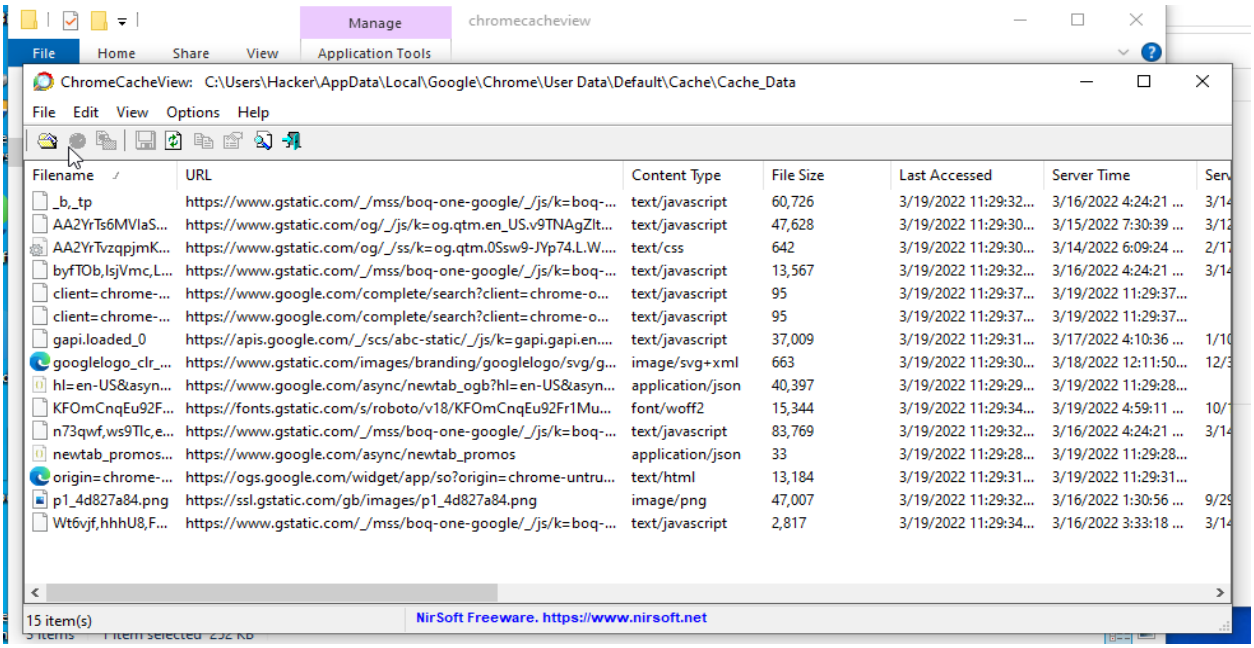
Browsing History: History of webpages that user views

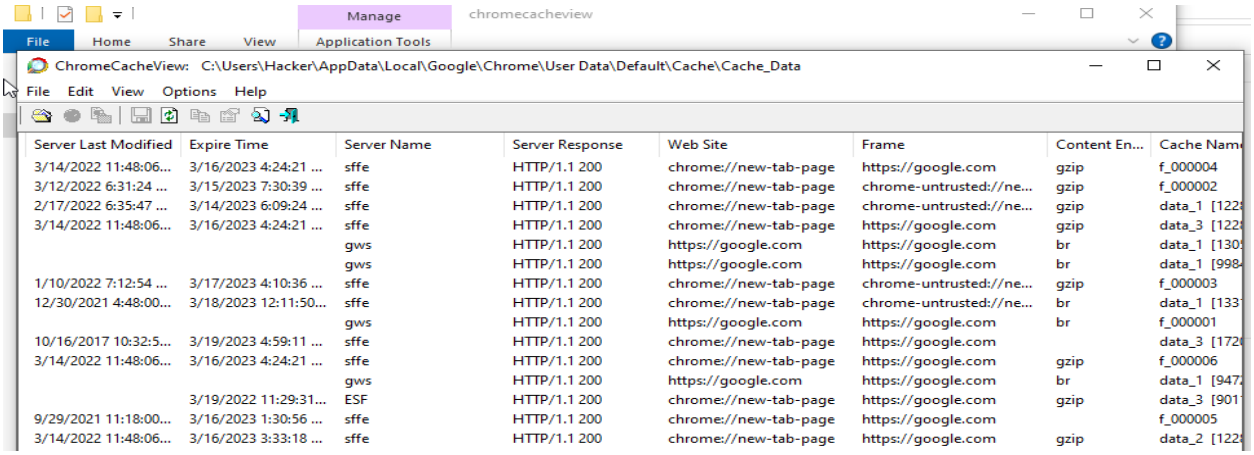
Caches: Information like webpages that are stored so that if webpage is loaded again, it does not take as much time as it took at the first place

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

GOOGLE CHROME

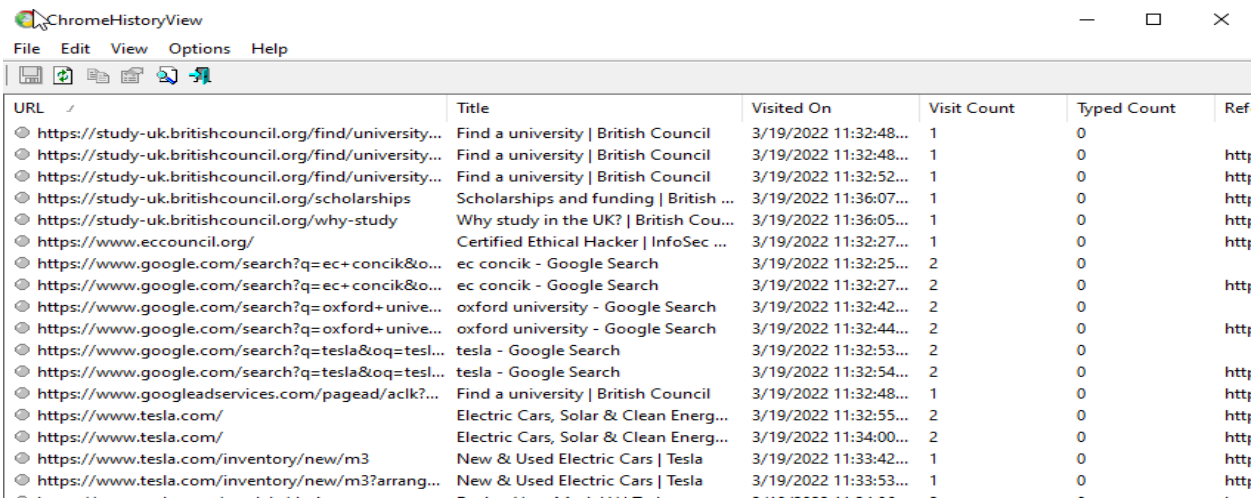
Here we are using tool called **cacheview** from nirsoft that is used to fetch all the details related to caches that has been stored in the chrome





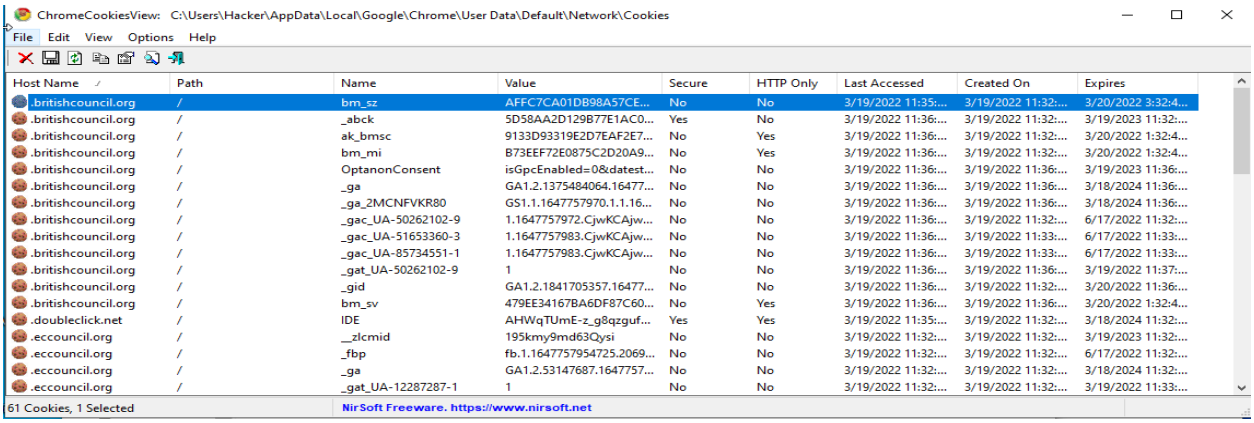
Server Last Modified	Expire Time	Server Name	Server Response	Web Site	Frame	Content En...	Cache Nam
3/14/2022 11:48:06...	3/16/2023 4:24:21 ...	sffe	HTTP/1.1 200	chrome://new-tab-page	https://google.com	gzip	f_000004
3/12/2022 6:31:24 ...	3/15/2023 7:30:39 ...	sffe	HTTP/1.1 200	chrome://new-tab-page	chrome-untrusted://ne...	gzip	f_000002
2/17/2022 6:35:47 ...	3/14/2023 6:09:24 ...	sffe	HTTP/1.1 200	chrome://new-tab-page	chrome-untrusted://ne...	gzip	data_1 [122
3/14/2022 11:48:06...	3/16/2023 4:24:21 ...	sffe	HTTP/1.1 200	chrome://new-tab-page	https://google.com	gzip	data_3 [122
		gws	HTTP/1.1 200	https://google.com	https://google.com	br	data_1 [130
		gws	HTTP/1.1 200	https://google.com	https://google.com	br	data_1 [998
1/10/2022 7:12:54 ...	3/17/2023 4:10:36 ...	sffe	HTTP/1.1 200	chrome://new-tab-page	chrome-untrusted://ne...	gzip	f_000003
12/30/2021 4:48:00...	3/18/2023 12:11:50...	sffe	HTTP/1.1 200	chrome://new-tab-page	chrome-untrusted://ne...	br	data_1 [133
		gws	HTTP/1.1 200	https://google.com	https://google.com	br	f_000001
10/16/2017 10:32:5...	3/19/2023 4:59:11 ...	sffe	HTTP/1.1 200	chrome://new-tab-page	https://google.com		data_3 [172
3/14/2022 11:48:06...	3/16/2023 4:24:21 ...	sffe	HTTP/1.1 200	chrome://new-tab-page	https://google.com	gzip	f_000006
		gws	HTTP/1.1 200	https://google.com	https://google.com	br	data_1 [947
	3/19/2022 11:29:31...	ESF	HTTP/1.1 200	chrome://new-tab-page	https://google.com	gzip	data_3 [901
9/29/2021 11:18:00...	3/16/2023 1:30:56 ...	sffe	HTTP/1.1 200	chrome://new-tab-page	https://google.com		f_000005
3/14/2022 11:48:06...	3/16/2023 3:33:18 ...	sffe	HTTP/1.1 200	chrome://new-tab-page	https://google.com	gzip	data_2 [122

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



URL	Title	Visited On	Visit Count	Typed Count	Ref
https://study-uk.britishcouncil.org/find/university...	Find a university | British Council	3/19/2022 11:32:48...	1	0	
https://study-uk.britishcouncil.org/find/university...	Find a university | British Council	3/19/2022 11:32:48...	1	0	htt
https://study-uk.britishcouncil.org/find/university...	Find a university | British Council	3/19/2022 11:32:52...	1	0	htt
https://study-uk.britishcouncil.org/scholarships	Scholarships and funding | British ...	3/19/2022 11:36:07...	1	0	htt
https://study-uk.britishcouncil.org/why-study	Why study in the UK? | British Cou...	3/19/2022 11:36:05...	1	0	htt
https://www.eccouncil.org/	Certified Ethical Hacker | InfoSec ...	3/19/2022 11:32:27...	1	0	htt
https://www.google.com/search?q=ec+concik&o...	ec concik - Google Search	3/19/2022 11:32:25...	2	0	
https://www.google.com/search?q=ec+concik&o...	ec concik - Google Search	3/19/2022 11:32:27...	2	0	htt
https://www.google.com/search?q=oxford+unive...	oxford university - Google Search	3/19/2022 11:32:42...	2	0	
https://www.google.com/search?q=oxford+unive...	oxford university - Google Search	3/19/2022 11:32:44...	2	0	htt
https://www.google.com/search?q=tesla&oq=tesl...	tesla - Google Search	3/19/2022 11:32:53...	2	0	
https://www.google.com/search?q=tesla&oq=tesl...	tesla - Google Search	3/19/2022 11:32:54...	2	0	htt
https://www.googleadservices.com/pagead/aclk?...	Find a university | British Council	3/19/2022 11:32:48...	1	0	htt
https://www.tesla.com/	Electric Cars, Solar & Clean Energ...	3/19/2022 11:32:55...	2	0	htt
https://www.tesla.com/	Electric Cars, Solar & Clean Energ...	3/19/2022 11:34:00...	2	0	htt
https://www.tesla.com/inventory/new/m3	New & Used Electric Cars | Tesla	3/19/2022 11:33:42...	1	0	htt
https://www.tesla.com/inventory/new/m3?arrang...	New & Used Electric Cars | Tesla	3/19/2022 11:33:53...	1	0	htt

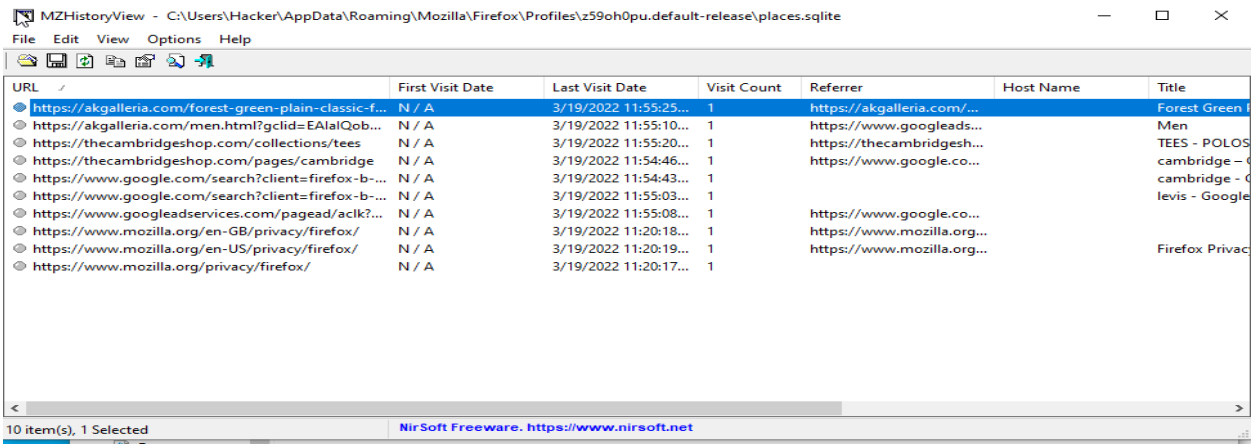
Here we are using tool called **cookieview** from nirsoft that is used to fetch all the details related to cookies and sessions that has been stored in the chrome



Host Name	Path	Name	Value	Secure	HTTP Only	Last Accessed	Created On	Expires
.britishcouncil.org	/	bm_sz	AFFC7CA01DB98A57CE...	No	No	3/19/2022 11:35:...	3/19/2022 11:32:...	3/20/2022 3:32:4...
.britishcouncil.org	/	_abck	5D58AA2D129B77E1AC0...	Yes	No	3/19/2022 11:36:...	3/19/2022 11:32:...	3/19/2023 11:32:...
.britishcouncil.org	/	ak_bmsc	9133D93319E2D7EAF2E7...	No	Yes	3/19/2022 11:36:...	3/19/2022 11:32:...	3/20/2022 1:32:4...
.britishcouncil.org	/	bm_mi	B73EEF72E0875C2D20A9...	No	Yes	3/19/2022 11:36:...	3/19/2022 11:32:...	3/20/2022 1:32:4...
.britishcouncil.org	/	OptanonConsent	isGpcEnabled=0&datest...	No	No	3/19/2022 11:36:...	3/19/2022 11:36:...	3/19/2023 11:36:...
.britishcouncil.org	/	_ga	GA1.2.1375484064.16477...	No	No	3/19/2022 11:36:...	3/19/2022 11:36:...	3/18/2024 11:36:...
.britishcouncil.org	/	_ga_2MCNFVKR80	GS1.1.1647757970.1.1.16...	No	No	3/19/2022 11:36:...	3/19/2022 11:36:...	3/18/2024 11:36:...
.britishcouncil.org	/	_gac_UA-50262102-9	1.1647757972.CjwKCAjw...	No	No	3/19/2022 11:36:...	3/19/2022 11:32:...	6/17/2022 11:32:...
.britishcouncil.org	/	_gac_UA-51653360-3	1.1647757983.CjwKCAjw...	No	No	3/19/2022 11:36:...	3/19/2022 11:33:...	6/17/2022 11:33:...
.britishcouncil.org	/	_gac_UA-85734551-1	1.1647757983.CjwKCAjw...	No	No	3/19/2022 11:36:...	3/19/2022 11:33:...	6/17/2022 11:33:...
.britishcouncil.org	/	_gat_UA-50262102-9	1	No	No	3/19/2022 11:36:...	3/19/2022 11:36:...	3/19/2022 11:37:...
.britishcouncil.org	/	_gid	GA1.2.1841705357.16477...	No	No	3/19/2022 11:36:...	3/19/2022 11:32:...	3/20/2022 11:36:...
.britishcouncil.org	/	bm_sv	479EE34167BA6DF87C60...	No	Yes	3/19/2022 11:36:...	3/19/2022 11:36:...	3/20/2022 1:32:4...
.doubleclick.net	/	IDE	AHWqTUmE-z_g8qzguf...	Yes	Yes	3/19/2022 11:35:...	3/19/2022 11:32:...	3/18/2024 11:32:...
.eccouncil.org	/	__zlcmid	195kmy9md63Qysi	No	No	3/19/2022 11:32:...	3/19/2022 11:32:...	3/19/2023 11:32:...
.eccouncil.org	/	_fbp	fb.1.1647757954725.2069...	No	No	3/19/2022 11:32:...	3/19/2022 11:32:...	6/17/2022 11:32:...
.eccouncil.org	/	_ga	GA1.2.53147687.1647757...	No	No	3/19/2022 11:32:...	3/19/2022 11:32:...	3/18/2024 11:32:...
.eccouncil.org	/	_gat_UA-12287287-1	1	No	No	3/19/2022 11:32:...	3/19/2022 11:32:...	3/19/2022 11:33:...

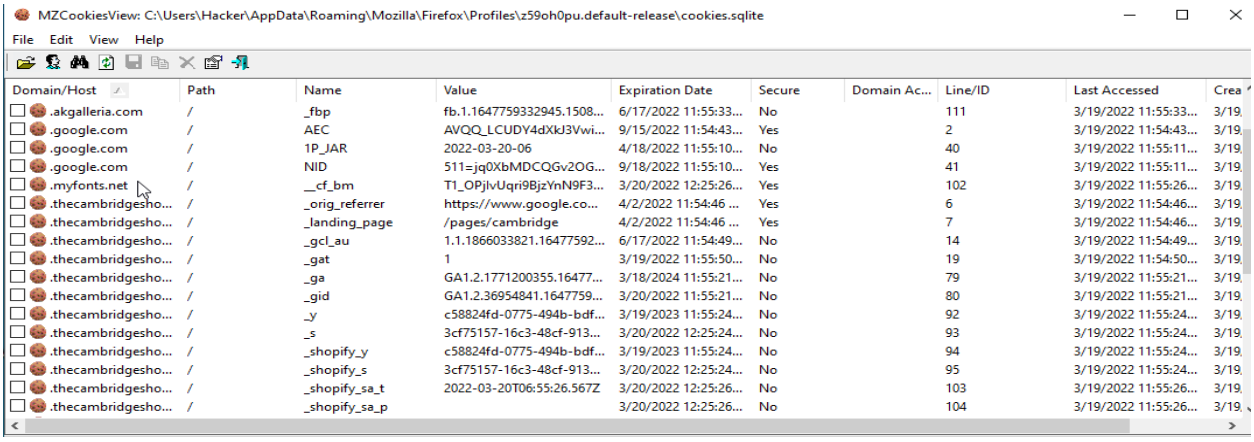
MOZILLA FIREFOX

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



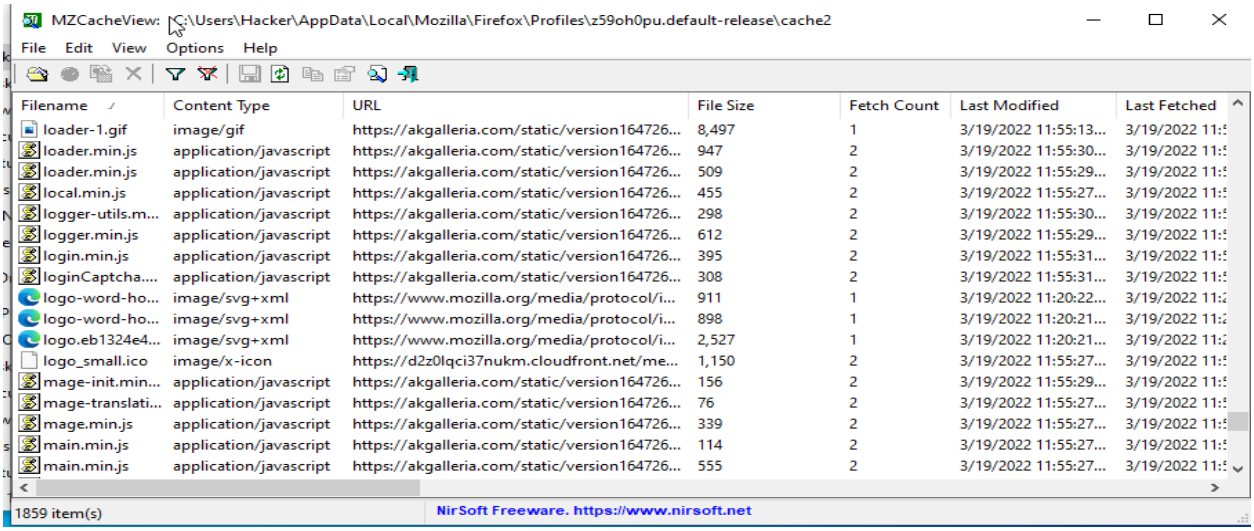
URL	First Visit Date	Last Visit Date	Visit Count	Referrer	Host Name	Title
https://akgalleria.com/forest-green-plain-classic-f...	N / A	3/19/2022 11:55:25...	1	https://akgalleria.com/...		Forest Green
https://akgalleria.com/men.html?gclid=EAIaIQob...	N / A	3/19/2022 11:55:10...	1	https://www.googleads...		Men
https://thecambridgeshop.com/collections/tees	N / A	3/19/2022 11:55:20...	1	https://thecambridgesh...		TEES - POLOS
https://thecambridgeshop.com/pages/cambridge	N / A	3/19/2022 11:54:46...	1	https://www.google.co...		cambridge –
https://www.google.com/search?client=firefox-b-...	N / A	3/19/2022 11:54:43...	1			cambridge -
https://www.google.com/search?client=firefox-b-...	N / A	3/19/2022 11:55:03...	1			levis - Google
https://www.googleadservices.com/pagead/aclk?...	N / A	3/19/2022 11:55:08...	1	https://www.google.co...		
https://www.mozilla.org/en-GB/privacy/firefox/	N / A	3/19/2022 11:20:18...	1	https://www.mozilla.org...		
https://www.mozilla.org/en-US/privacy/firefox/	N / A	3/19/2022 11:20:19...	1	https://www.mozilla.org...		Firefox Privac
https://www.mozilla.org/privacy/firefox/	N / A	3/19/2022 11:20:17...	1			

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



Domain/Host	Path	Name	Value	Expiration Date	Secure	Domain Ac...	Line/ID	Last Accessed	Crea
.akgalleria.com	/	_fbp	fb.1.1647759332945.1508...	6/17/2022 11:55:33...	No		111	3/19/2022 11:55:33...	3/19
.google.com	/	AEC	AVQQ_LCUDY4dXkJ3Vwi...	9/15/2022 11:54:43...	Yes		2	3/19/2022 11:54:43...	3/19
.google.com	/	1P_JAR	2022-03-20-06	4/18/2022 11:55:10...	No		40	3/19/2022 11:55:11...	3/19
.google.com	/	NID	511=jq0XbMDCQGv2OG...	9/18/2022 11:55:10...	Yes		41	3/19/2022 11:55:11...	3/19
.myfonts.net	/	__cf_bm	T1_OPjlvUqri9BjzYnN9F3...	3/20/2022 12:25:26...	Yes		102	3/19/2022 11:55:26...	3/19
.thecambridgesho...	/	_orig_referrer	https://www.google.co...	4/2/2022 11:54:46 ...	Yes		6	3/19/2022 11:54:46...	3/19
.thecambridgesho...	/	_landing_page	/pages/cambridge	4/2/2022 11:54:46 ...	Yes		7	3/19/2022 11:54:46...	3/19
.thecambridgesho...	/	_gcl_au	1.1.1866033821.16477592...	6/17/2022 11:54:49...	No		14	3/19/2022 11:54:49...	3/19
.thecambridgesho...	/	_gat	1	3/19/2022 11:55:50...	No		19	3/19/2022 11:54:50...	3/19
.thecambridgesho...	/	_ga	GA1.2.1771200355.16477...	3/18/2024 11:55:21...	No		79	3/19/2022 11:55:21...	3/19
.thecambridgesho...	/	_gid	GA1.2.36954841.1647759...	3/20/2022 11:55:21...	No		80	3/19/2022 11:55:21...	3/19
.thecambridgesho...	/	_y	c58824fd-0775-494b-bdf...	3/19/2023 11:55:24...	No		92	3/19/2022 11:55:24...	3/19
.thecambridgesho...	/	_s	3cf75157-16c3-48cf-913...	3/20/2022 12:25:24...	No		93	3/19/2022 11:55:24...	3/19
.thecambridgesho...	/	_shopify_y	c58824fd-0775-494b-bdf...	3/19/2023 11:55:24...	No		94	3/19/2022 11:55:24...	3/19
.thecambridgesho...	/	_shopify_s	3cf75157-16c3-48cf-913...	3/20/2022 12:25:24...	No		95	3/19/2022 11:55:24...	3/19
.thecambridgesho...	/	_shopify_sa_t	2022-03-20T06:55:26.567Z	3/20/2022 12:25:26...	No		103	3/19/2022 11:55:26...	3/19
.thecambridgesho...	/	_shopify_sa_p		3/20/2022 12:25:26...	No		104	3/19/2022 11:55:26...	3/19

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



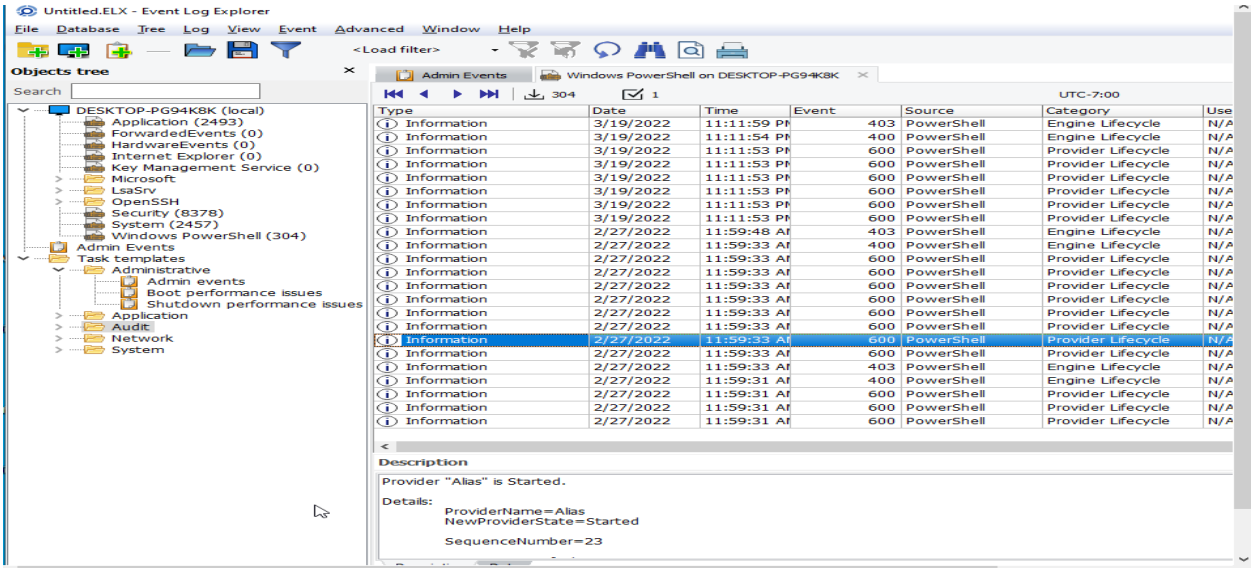
Filename	Content Type	URL	File Size	Fetch Count	Last Modified	Last Fetched
loader-1.gif	image/gif	https://akgalleria.com/static/version164726...	8,497	1	3/19/2022 11:55:13...	3/19/2022 11:
loader.min.js	application/javascript	https://akgalleria.com/static/version164726...	947	2	3/19/2022 11:55:30...	3/19/2022 11:
loader.min.js	application/javascript	https://akgalleria.com/static/version164726...	509	2	3/19/2022 11:55:29...	3/19/2022 11:
local.min.js	application/javascript	https://akgalleria.com/static/version164726...	455	2	3/19/2022 11:55:27...	3/19/2022 11:
logger-utils.m...	application/javascript	https://akgalleria.com/static/version164726...	298	2	3/19/2022 11:55:30...	3/19/2022 11:
logger.min.js	application/javascript	https://akgalleria.com/static/version164726...	612	2	3/19/2022 11:55:29...	3/19/2022 11:
login.min.js	application/javascript	https://akgalleria.com/static/version164726...	395	2	3/19/2022 11:55:31...	3/19/2022 11:
loginCaptcha....	application/javascript	https://akgalleria.com/static/version164726...	308	2	3/19/2022 11:55:31...	3/19/2022 11:
logo-word-ho...	image/svg+xml	https://www.mozilla.org/media/protocol/i...	911	1	3/19/2022 11:20:22...	3/19/2022 11:
logo-word-ho...	image/svg+xml	https://www.mozilla.org/media/protocol/i...	898	1	3/19/2022 11:20:21...	3/19/2022 11:
logo.eb1324e4...	image/svg+xml	https://www.mozilla.org/media/protocol/i...	2,527	1	3/19/2022 11:20:21...	3/19/2022 11:
logo_small.ico	image/x-icon	https://d2z0lqci37nukm.cloudfront.net/me...	1,150	2	3/19/2022 11:55:27...	3/19/2022 11:
mage-init.min...	application/javascript	https://akgalleria.com/static/version164726...	156	2	3/19/2022 11:55:29...	3/19/2022 11:
mage-translati...	application/javascript	https://akgalleria.com/static/version164726...	76	2	3/19/2022 11:55:27...	3/19/2022 11:
mage.min.js	application/javascript	https://akgalleria.com/static/version164726...	339	2	3/19/2022 11:55:27...	3/19/2022 11:
main.min.js	application/javascript	https://akgalleria.com/static/version164726...	114	2	3/19/2022 11:55:27...	3/19/2022 11:
main.min.js	application/javascript	https://akgalleria.com/static/version164726...	555	2	3/19/2022 11:55:27...	3/19/2022 11:

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.



Untitled.ELX - Event Log Explorer

File Database Tree Log View Event Advanced Window Help

<Load filter>

Objects tree

Search

- DESKTOP-PG94K8K (local)
  - Application (2493)
  - ForwardedEvents (0)
  - HardwareEvents (0)
  - Internet Explorer (0)
  - Key Management Service (0)
  - Microsoft
  - LsaSrv
  - OpenSSH
  - Security (8378)
  - System (2457)
  - Windows PowerShell (304)
- Admin Events
- Task templates
  - Administrative
    - Admin events
    - Boot performance issues
    - Shutdown performance issues
  - Application
  - Audit
  - Network
  - System

Admin Events | Windows PowerShell on DESKTOP-PG94K8K

14 1 XML UTC-7:00

Type	Date	Time	Event	Source	Category	User
Warning	3/20/2022	12:11:59 AM	642	ESENT	General	N/A
Error	3/20/2022	12:00:58 AM	8198	Microsoft-Windows-	None	N/A
Error	3/20/2022	12:00:58 AM	8198	Microsoft-Windows-	None	N/A
Error	3/20/2022	12:00:56 AM	8198	Microsoft-Windows-	None	N/A
Warning	3/20/2022	12:00:26 AM	642	ESENT	General	N/A
Warning	3/20/2022	12:00:26 AM	642	ESENT	General	N/A
Warning	3/20/2022	12:00:26 AM	642	ESENT	General	N/A
Warning	3/20/2022	12:00:25 AM	642	ESENT	General	N/A
Warning	3/20/2022	12:00:19 AM	642	ESENT	General	N/A
Warning	3/20/2022	12:00:19 AM	642	ESENT	General	N/A
Error	3/19/2022	11:59:48 PM	6008	EventLog	None	N/A
Critical	3/19/2022	11:59:17 PM	41	Microsoft-Windows-	(63)	\SYST
Warning	3/19/2022	11:16:05 PM	10016	Microsoft-Windows-	None	DESKT
Warning	3/19/2022	11:07:50 PM	10016	Microsoft-Windows-	None	DESKT

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.

```
C:\Users\Hacker\Desktop\Lab-8-tools>python registry_hives.py
0:.DEFAULT
1:S-1-5-19
2:S-1-5-20
3:S-1-5-21-2843756275-1552048814-2127499628-1002
4:S-1-5-21-2843756275-1552048814-2127499628-1002_Classes
5:S-1-5-18
```

- **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.

```
Select C:\Windows\System32\cmd.exe

C:\Users\Hacker\Desktop\Lab-8-tools>python registry_hives_and_values.py
0:.DEFAULT
1:S-1-5-19
2:S-1-5-20
3:S-1-5-21-2843756275-1552048814-2127499628-1002
4:S-1-5-21-2843756275-1552048814-2127499628-1002_Classes
5:S-1-5-18

<--Displaying Values of registry WinRAR-->

ArcHistory : 2022-03-19 23:40:44.947890-07:00
DialogEditHistory : 2021-09-18 12:25:58.024593-07:00
FileList : 2021-09-19 02:47:58.063204-07:00
General : 2022-02-27 08:08:33.200357-08:00
Interface : 2021-09-19 02:47:58.010354-07:00
Profiles : 2021-09-18 12:19:04.095070-07:00
Setup : 2021-09-18 12:18:47.376019-07:00
```

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.

recycle_bin.py - C:\Users\Hacker\Desktop\Lab-8-tools\recycle_bin.py (3.10.3)

File Edit Format Run Options Window Help

```python
import winshell
import win32
import re

r = list(winshell.recycle_bin())

for x in r:
    print(x.original_filename(), x.recycle_date(), sep='\t')
    fl = r[0].filename()
    y = re.search(r"S.*\d{4}", fl)
    print(y.group(0))

    path = r'C:\Users\Hacker\Desktop\Lab-8-tools\Mytest.txt'
    with open(path,'w') as file:
        file.write("This is MY TESTING FILE")
    winshell.delete_file(path)

    winshell.undelete(path)

```

IDLE Shell 3.10.3

File Edit Shell Debug Options Window Help

```
Python 3.10.3 (tags/v3.10.3:a342a49, Mar 16 2022, 13:07:40) [MSC v.1929 64 bit (
AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
========== RESTART: C:\Users\Hacker\Desktop\Lab-8-tools\recycle_bin.py =========
C:\Users\Hacker\Desktop\Lab-8-tools\Mytest.txt  2022-03-20 10:34:55+00:00
S-1-5-21-2843756275-1552048814-2127499628-1002
C:\Users\Hacker\Desktop\Lab-8-tools\Mytest.txt - Shortcut       2022-03-20 10:33
:11+00:00
S-1-5-21-2843756275-1552048814-2127499628-1002
C:\Users\Hacker\Desktop\Lab-8-tools\Mytest.txt  2022-03-20 10:33:04+00:00
S-1-5-21-2843756275-1552048814-2127499628-1002
C:\Users\Hacker\Desktop\abc.pdf 2022-03-20 10:32:06+00:00
S-1-5-21-2843756275-1552048814-2127499628-1002
C:\Users\Hacker\Desktop\Lab-8-tools\Mytest.txt  2022-03-20 10:34:27+00:00
S-1-5-21-2843756275-1552048814-2127499628-1002
C:\Users\Hacker\Desktop\Lab-8-tools\Mytest.txt  2022-03-20 10:34:11+00:00
S-1-5-21-2843756275-1552048814-2127499628-1002
>>>
```

Mytest.txt - Notepad

File Edit Format View Help

```
This is MY TESTING FILE
```

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.

reading_browser.py - C:\Users\Hacker\Desktop\Lab-8-tools\reading_browser.py (3.10.3)

File Edit Format Run Options Window Help

```
import os
path = r'C:\Users\Hacker\AppData\Roaming\Mozilla\Firefox\Profiles\z59oh0pu.defau
files = os.listdir(path)
for file in files:
    if file.endswith(".sqlite") or file.endswith(".db"):
        print(file)
```

IDLE Shell 3.10.3

Edit Shell Debug Options Window Help

```
Python 3.10.3 (tags/v3.10.3:a342a49, Mar 16 2022, 13:07:40) [MSC v.1929 64 bit (
AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>
======== RESTART: C:\Users\Hacker\Desktop\Lab-8-tools\reading_browser.py =======
cert9.db
content-prefs.sqlite
cookies.sqlite
favicons.sqlite
formhistory.sqlite
key4.db
permissions.sqlite
places.sqlite
protections.sqlite
storage.sqlite
webappsstore.sqlite
>
```

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

reading_browser.py - C:\Users\Hacker\Desktop\Lab-8-tools\reading_browser.py (3.10.3)

File Edit Format Run Options Window Help

```python
import os
import sqlite3
path = r'C:\Users\Hacker\AppData\Roaming\Mozilla\Firefox\Profiles\z59oh0pu.defau
files = os.listdir(path)
for file in files:
    if file.endswith(".sqlite") or file.endswith(".db"):
        print(file)

history = os.path.join(path, 'places.sqlite')
history_connect = sqlite3.connect(history)
history_cursor = history_connect.cursor()

history_cursor.execute("PRAGMA table_info(moz_places)")
results = history_cursor.fetchall()
statement = 'SELECT url, visit_count FROM moz_places;'
history_cursor.execute(statement)
results = history_cursor.fetchall()
print("\nSHOWING HISTORY\n")
print(results)
```

IDLE Shell 3.10.3

File Edit Shell Debug Options Window Help

```
Python 3.10.3 (tags/v3.10.3:a342a49, Mar 16 2022, 13:07:40) [MSC v.1929 64 bit (
AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
======== RESTART: C:\Users\Hacker\Desktop\Lab-8-tools\reading_browser.py =======
cert9.db
content-prefs.sqlite
cookies.sqlite
favicons.sqlite
formhistory.sqlite
key4.db
permissions.sqlite
places.sqlite
protections.sqlite
storage.sqlite
webappsstore.sqlite

SHOWING HISTORY

[('https://support.mozilla.org/products/firefox', 0), ('https://support.mozilla.
org/kb/customize-firefox-controls-buttons-and-toolbars?utm_source=firefox-browse
r&utm_medium=default-bookmarks&utm_campaign=customize', 0), ('https://www.mozill
a.org/contribute/', 0), ('https://www.mozilla.org/about/', 0), ('https://www.moz
illa.org/firefox/central/', 0), ('https://www.mozilla.org/privacy/firefox/', 1),
 ('https://www.mozilla.org/en-GB/privacy/firefox/', 1), ('https://www.mozilla.or
g/en-US/privacy/firefox/', 1), ('https://www.google.com/search?client=firefox-b-
d&q=cambridge', 1), ('https://thecambridgeshop.com/pages/cambridge', 1), ('https
://www.google.com/search?client=firefox-b-d&q=levis', 1), ('https://www.googlead
services.com/pagead/aclk?sa=L&ai=DChcSEwiwrrPfjdT2AhVY-VEKHbtfBUwYABABGgJ3cw&oho
st=www.google.com&cid=CAASJORotwpWX_3JY9qzIaTTbx_bFy4MDJDdhd-6OR0JcanSJiUZrQ&sig
=AOD64_0EBRftcjqQ6-Ej9GklzERTUONj5Q&ved=2ahUKEwiMoKvfjdT2AhUIuRoKHUeOCK0QqyQoAHo
ECAIQBQ&adurl=', 1), ('https://akgalleria.com/men.html?gclid=EAIaIQobChMIsK6z343
U9gIVWPlRCh27XwVMEAAYASABEgIvj_D_BwE', 1), ('https://thecambridgeshop.com/collec
tions/tees', 1), ('https://akgalleria.com/forest-green-plain-classic-fit-button-
down-washed-oxford-shirt-ct-csr0903frg-forestgreen.html', 1)]
>>>
```

Ln: 20 Col: 0

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.