Toan Ngo
date:3/29/24

LAB9 Window forensic
Browser data log retrieval and registry/ sam files

For this lab report, I will be talking about what data the browser stored on your local machine when you used it on a daily basis and I will also talk about what those types of data contain and their function, later in the report we will also cover some methods to extract them. We are also gonna take a look into the window registry of how a file is stored/logged there and later in the report we will then do some demo of how we can get files from the window registry.

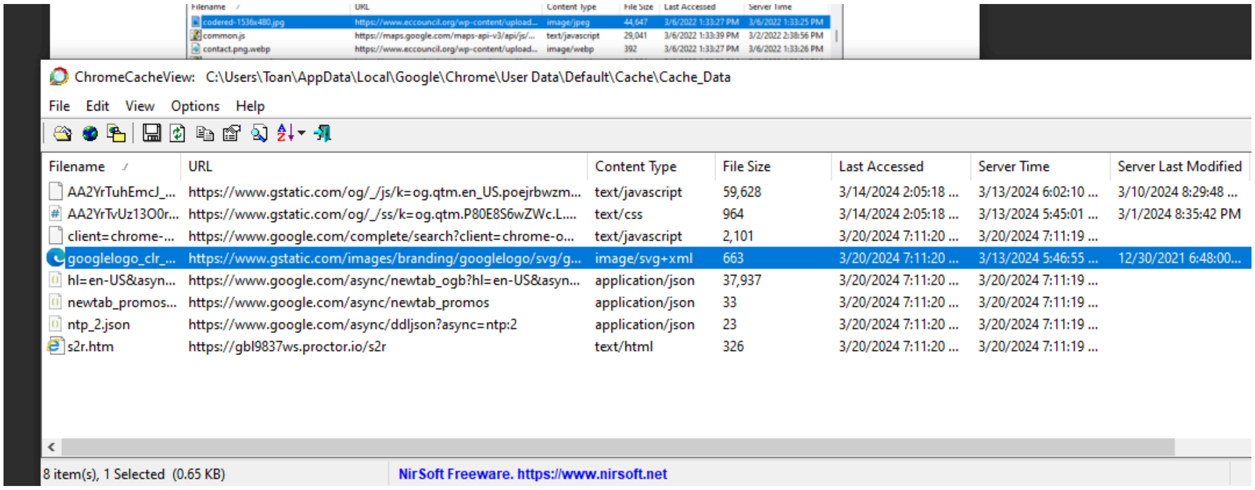
Now lets cover some basic information first,the browser that you are currently has keeping track of all your activity when you go online in a log and it is stored in your system locally and those files are categorized in the following 3 type: cookies files where it keeps your personal preference for the site that you have visited and it's also let the webserver know the time frame your visited the website, cache keeps any resources that the website need to function on your local machine, so that the next time you visit it, the site will load faster because of the cache that stored local on your machine, and finally history log where it task is to keeping track of your browsing history so that you can revisited any website that you have visited in the past in a more convenient manner. You can extract these logs in the browser itself or later in this report we will cover some tools that help us collect these logs.

Next what is window registry and what is the correlation between sam files and window registry ? first window registry is a hierarchical database that stores low-level settings for the Microsoft Windows operating system and for applications that opt to use the registry, you can think of it like the big stored space for all the system function, and it responsibility is to helping/ensuring the OS get the necessary resource to perform the function that was called for and it also responsible for helping configure whatever operation system setting that you wanted to configure. A sam files or System Account Management files, its a particular registry hive that stores credentials and account information for local users, for example if your personal computer have two users account then, it is this files responsibility to keep track of all credentials information and all information about each users that exist in the system, and this files are stored and located in the window registry, that is the main correlation between two system, they work depend on each others. Later in the report we will try to do some activity with the registry just to demonstrate what you could do in it.

Testing part

First we will look at some of these tools that help us extract the log data from the browser.
And also for these demonstrations, i will only be doing the extracting to chrome browser only, however in the extra section you i will provide the link for downloading for both chrome and firefox version so that you could use and test it out if you want.

Toan Ngo
date:3/29/24



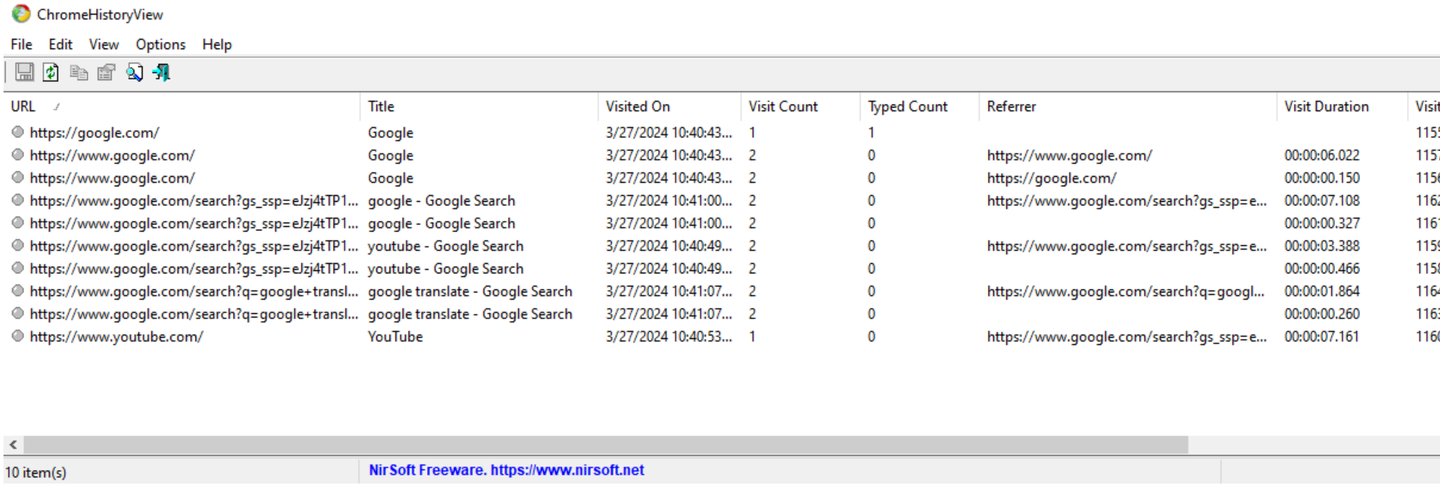
Filename	URL	Content Type	File Size	Last Accessed	Server Time
codered-1536x480.jpg	https://www.eccouncil.org/wp-content/upload...	image/jpeg	44,647	3/6/2022 1:33:27 PM	3/6/2022 1:33:25 PM
common.js	https://maps.google.com/maps-api-v3/api/js/...	text/javascript	29,041	3/6/2022 1:33:39 PM	3/2/2022 2:38:56 PM
contact.png.webp	https://www.eccouncil.org/wp-content/upload...	image/webp	392	3/6/2022 1:33:27 PM	3/6/2022 1:33:26 PM

ChromeCacheView: C:\Users\Toan\AppData\Local\Google\Chrome\User Data\Default\Cache\Cache_Data

Filename	URL	Content Type	File Size	Last Accessed	Server Time	Server Last Modified
AA2YrTuhEmcJ_...	https://www.gstatic.com/og/_/js/k=og.qtm.en_US.poejrbwzm...	text/javascript	59,628	3/14/2024 2:05:18 ...	3/13/2024 6:02:10 ...	3/10/2024 8:29:48 ...
AA2YrTvUz13O0r...	https://www.gstatic.com/og/_/ss/k=og.qtm.P80E8S6wZWc.L....	text/css	964	3/14/2024 2:05:18 ...	3/13/2024 5:45:01 ...	3/1/2024 8:35:42 PM
client=chrome-...	https://www.google.com/complete/search?client=chrome-o...	text/javascript	2,101	3/20/2024 7:11:20 ...	3/20/2024 7:11:19 ...	
googlelogo_clr_...	https://www.gstatic.com/images/branding/googlelogo/svg/g...	image/svg+xml	663	3/20/2024 7:11:20 ...	3/13/2024 5:46:55 ...	12/30/2021 6:48:00...
hl=en-US&asyn...	https://www.google.com/async/newtab_ogb?hl=en-US&asyn...	application/json	37,937	3/20/2024 7:11:20 ...	3/20/2024 7:11:19 ...	
newtab_promos...	https://www.google.com/async/newtab_promos	application/json	33	3/20/2024 7:11:20 ...	3/20/2024 7:11:19 ...	
ntp_2.json	https://www.google.com/async/ddljson?async=ntp:2	application/json	23	3/20/2024 7:11:20 ...	3/20/2024 7:11:19 ...	
s2r.htm	https://gbl9837ws.proctor.io/s2r	text/html	326	3/20/2024 7:11:20 ...	3/20/2024 7:11:19 ...	

8 item(s), 1 Selected (0.65 KB)

First the cache view tools help with the export of the cache of your browser. As you can see all the files there are the caches that are stored in your local machine.



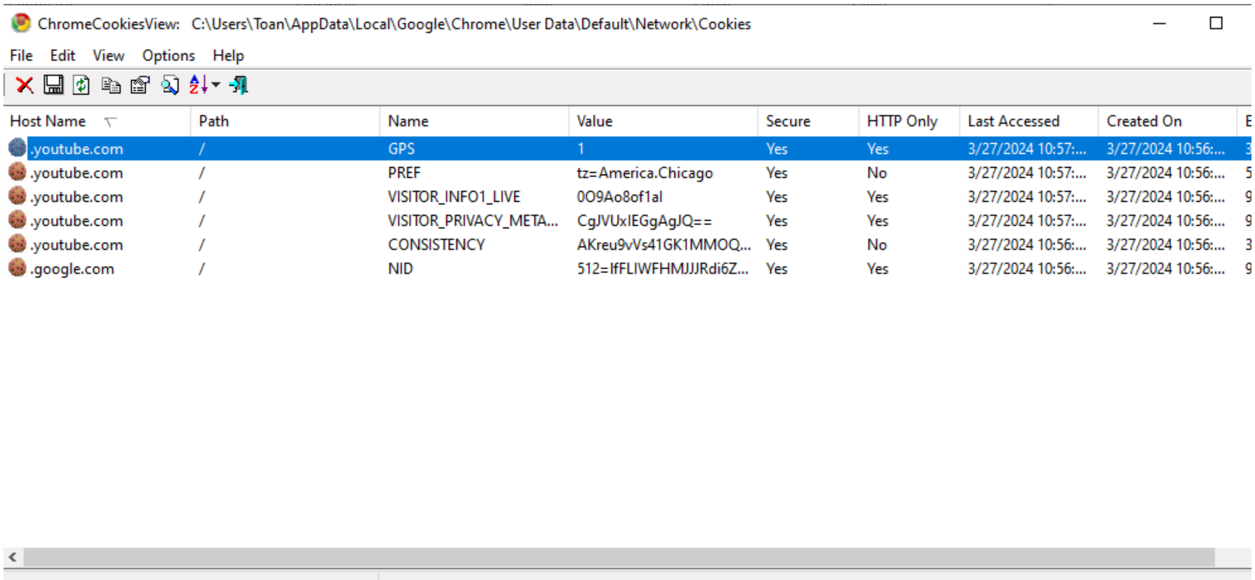
ChromeHistoryView

URL	Title	Visited On	Visit Count	Typed Count	Referrer	Visit Duration	Visi
https://google.com/	Google	3/27/2024 10:40:43...	1	1			1155
https://www.google.com/	Google	3/27/2024 10:40:43...	2	0	https://www.google.com/	00:00:06.022	1157
https://www.google.com/	Google	3/27/2024 10:40:43...	2	0	https://google.com/	00:00:00.150	1156
https://www.google.com/search?gs_ssp=eJzj4tTP1...	google - Google Search	3/27/2024 10:41:00...	2	0	https://www.google.com/search?gs_ssp=e...	00:00:07.108	1162
https://www.google.com/search?gs_ssp=eJzj4tTP1...	google - Google Search	3/27/2024 10:41:00...	2	0		00:00:00.327	1161
https://www.google.com/search?gs_ssp=eJzj4tTP1...	youtube - Google Search	3/27/2024 10:40:49...	2	0	https://www.google.com/search?gs_ssp=e...	00:00:03.388	1159
https://www.google.com/search?gs_ssp=eJzj4tTP1...	youtube - Google Search	3/27/2024 10:40:49...	2	0		00:00:00.466	1158
https://www.google.com/search?q=google+transl...	google translate - Google Search	3/27/2024 10:41:07...	2	0	https://www.google.com/search?q=googl...	00:00:01.864	1164
https://www.google.com/search?q=google+transl...	google translate - Google Search	3/27/2024 10:41:07...	2	0		00:00:00.260	1163
https://www.youtube.com/	YouTube	3/27/2024 10:40:53...	1	0	https://www.google.com/search?gs_ssp=e...	00:00:07.161	1160

10 item(s)

Second tools historyView helps with extracting history from the browser that are stored in your local machine. As you see it not just contains all the history for your browser, it also includes the day of visit or anything related to that visit.

Toan Ngo
date:3/29/24


ChromeCookiesView: C:\Users\Toan\AppData\Local\Google\Chrome\User Data\Default\Network\Cookies
File
Edit
View
Options
Help

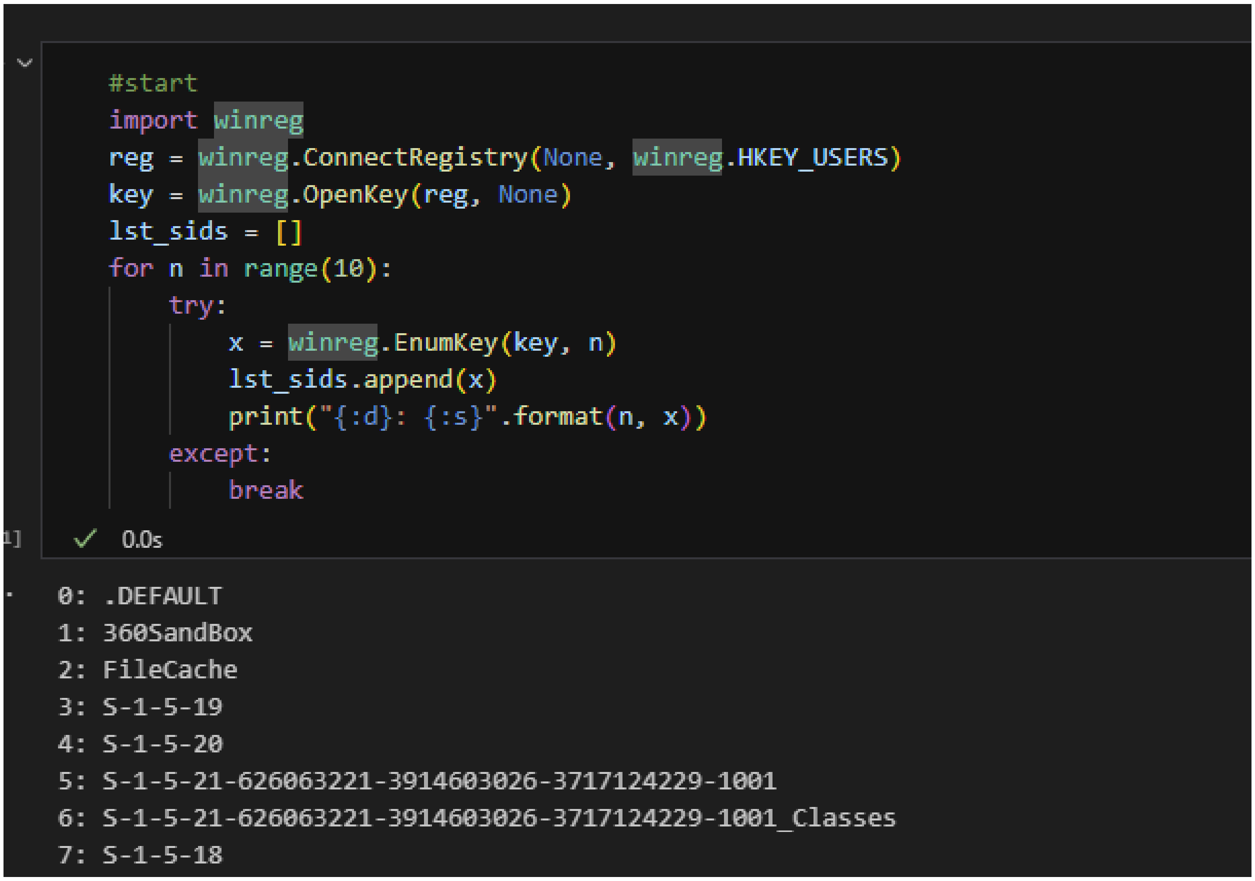
Host Name	Path	Name	Value	Secure	HTTP Only	Last Accessed	Created On	E
.youtube.com	/	GPS	1	Yes	Yes	3/27/2024 10:57:...	3/27/2024 10:56:...	3
.youtube.com	/	PREF	tz=America.Chicago	Yes	No	3/27/2024 10:57:...	3/27/2024 10:56:...	5
.youtube.com	/	VISITOR_INFO1_LIVE	0O9Ao8of1al	Yes	Yes	3/27/2024 10:57:...	3/27/2024 10:56:...	9
.youtube.com	/	VISITOR_PRIVACY_META...	CgJVUxIEGgAgJQ==	Yes	Yes	3/27/2024 10:57:...	3/27/2024 10:56:...	9
.youtube.com	/	CONSISTENCY	AKreu9vVs41GK1MMOQ...	Yes	No	3/27/2024 10:56:...	3/27/2024 10:56:...	3
.google.com	/	NID	512=IfFLIWFHMJJJRdi6Z...	Yes	Yes	3/27/2024 10:56:...	3/27/2024 10:56:...	9

Final tools the cookies view help with the extraction of the cookies that were stored on your local machine by the browser.

Just a note: once you download the files for each of these tools, you really don't need to do anything other than click into the .exe files and it will automatically perform its function for each tool.

Next is window registry demonstrating

Toan Ngo
date:3/29/24

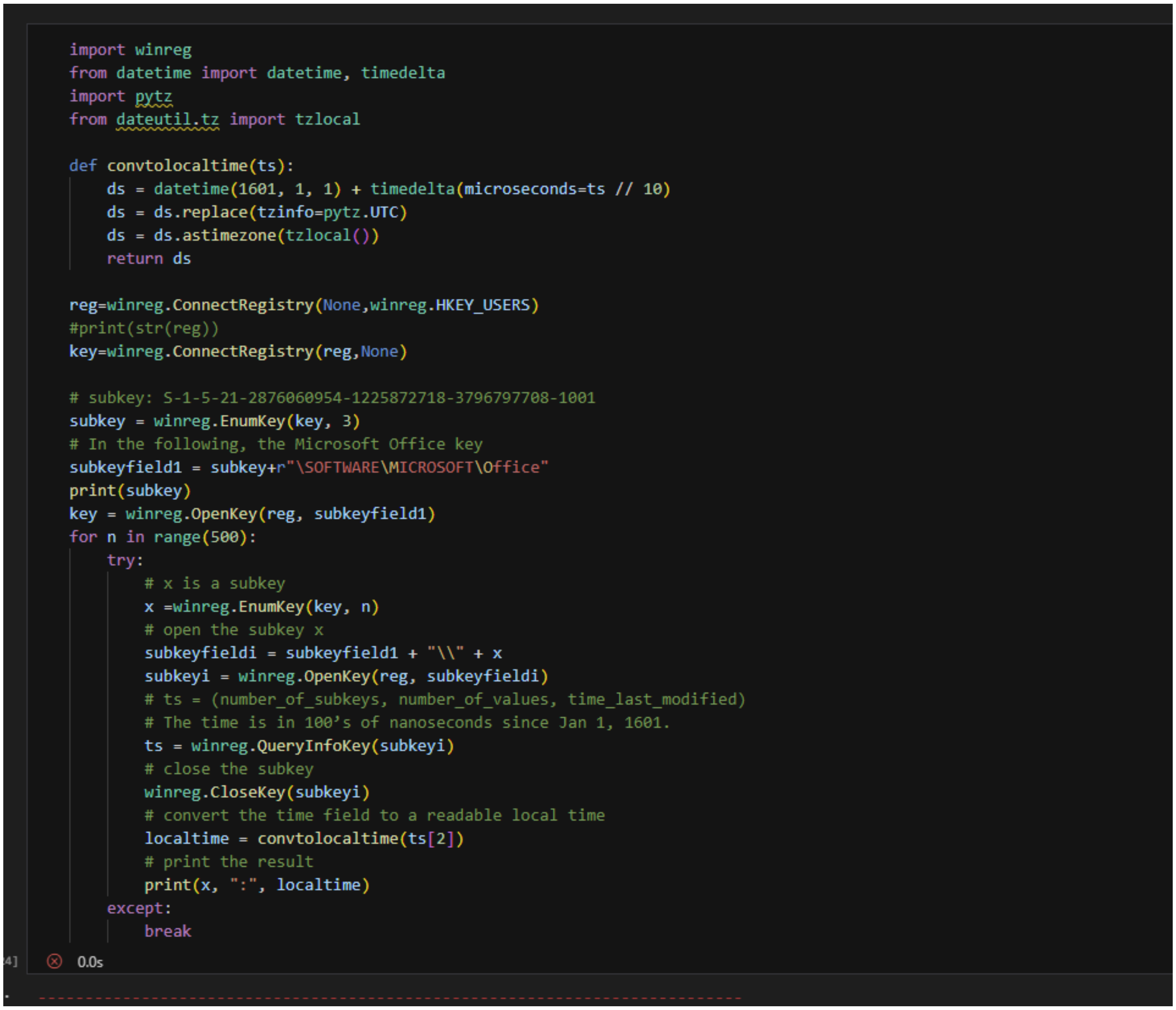


```python
#start
import winreg
reg = winreg.ConnectRegistry(None, winreg.HKEY_USERS)
key = winreg.OpenKey(reg, None)
lst_sids = []
for n in range(10):
    try:
        x = winreg.EnumKey(key, n)
        lst_sids.append(x)
        print("{:d}: {:s}".format(n, x))
    except:
        break
```

```
0: .DEFAULT
1: 360SandBox
2: FileCache
3: S-1-5-19
4: S-1-5-20
5: S-1-5-21-626063221-3914603026-3717124229-1001
6: S-1-5-21-626063221-3914603026-3717124229-1001_Classes
7: S-1-5-18
```

What we are trying to do here is to look into the window registry, and try to see what are the key variables that exist in the registry.

Toan Ngo
date:3/29/24



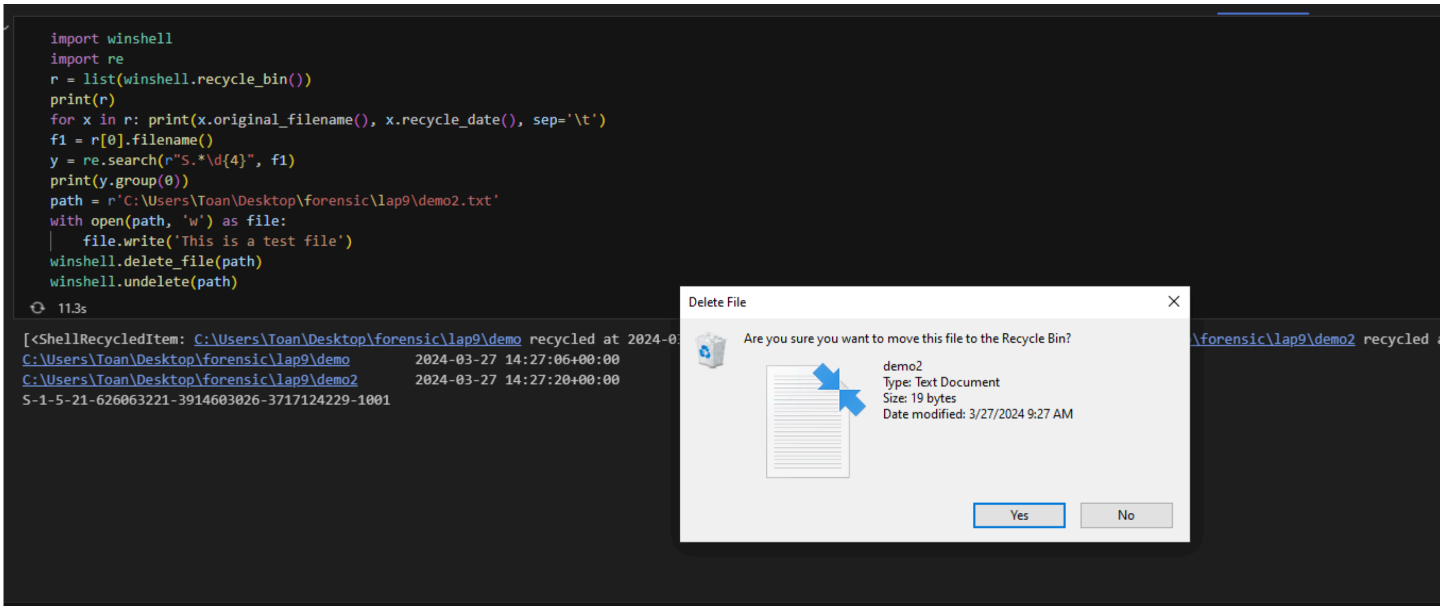
```
import winreg
from datetime import datetime, timedelta
import pytz
from dateutil.tz import tzlocal

def convtolocaltime(ts):
    ds = datetime(1601, 1, 1) + timedelta(microseconds=ts // 10)
    ds = ds.replace(tzinfo=pytz.UTC)
    ds = ds.astimezone(tzlocal())
    return ds

reg=winreg.ConnectRegistry(None,winreg.HKEY_USERS)
#print(str(reg))
key=winreg.ConnectRegistry(reg,None)

# subkey: S-1-5-21-2876060954-1225872718-3796797708-1001
subkey = winreg.EnumKey(key, 3)
# In the following, the Microsoft Office key
subkeyfield1 = subkey+r"\SOFTWARE\MICROSOFT\Office"
print(subkey)
key = winreg.OpenKey(reg, subkeyfield1)
for n in range(500):
    try:
        # x is a subkey
        x =winreg.EnumKey(key, n)
        # open the subkey x
        subkeyfieldi = subkeyfield1 + "\\" + x
        subkeyi = winreg.OpenKey(reg, subkeyfieldi)
        # ts = (number_of_subkeys, number_of_values, time_last_modified)
        # The time is in 100's of nanoseconds since Jan 1, 1601.
        ts = winreg.QueryInfoKey(subkeyi)
        # close the subkey
        winreg.CloseKey(subkeyi)
        # convert the time field to a readable local time
        localtime = convtolocaltime(ts[2])
        # print the result
        print(x, ":", localtime)
    except:
        break
```

Ok for this one i will explain in parts: first convtolcaltime function basically convert anything that was past into it to human readable time zone.

Second, what we trying to do in the second half of the code is that we trying to look in to the window registry and drag all the key out and stored it in key,after that we create subkey object that loop through key and then select the key at the 3 slots from key, after that we combine the subkey with a relative path to microsoft office, after that we overwrite the prev key with an new function and this time is openkey with is to get the key for the main key for microsoft office, and finally we create a range loop that print out the any information relate to that microsoft office key we get, this could including what document was open, when it open, or day modify/time etc……

>The main goal of this is to demonstrate that you can go into the window registry, get the application key and then combine it with the application path, so that you can view the history of the application.

Toan Ngo
date:3/29/24



```
import winshell
import re
r = list(winshell.recycle_bin())
print(r)
for x in r: print(x.original_filename(), x.recycle_date(), sep='\t')
f1 = r[0].filename()
y = re.search(r"S.*\d{4}", f1)
print(y.group(0))
path = r'C:\Users\Toan\Desktop\forensic\lap9\demo2.txt'
with open(path, 'w') as file:
    file.write('This is a test file')
winshell.delete_file(path)
winshell.undelete(path)
```

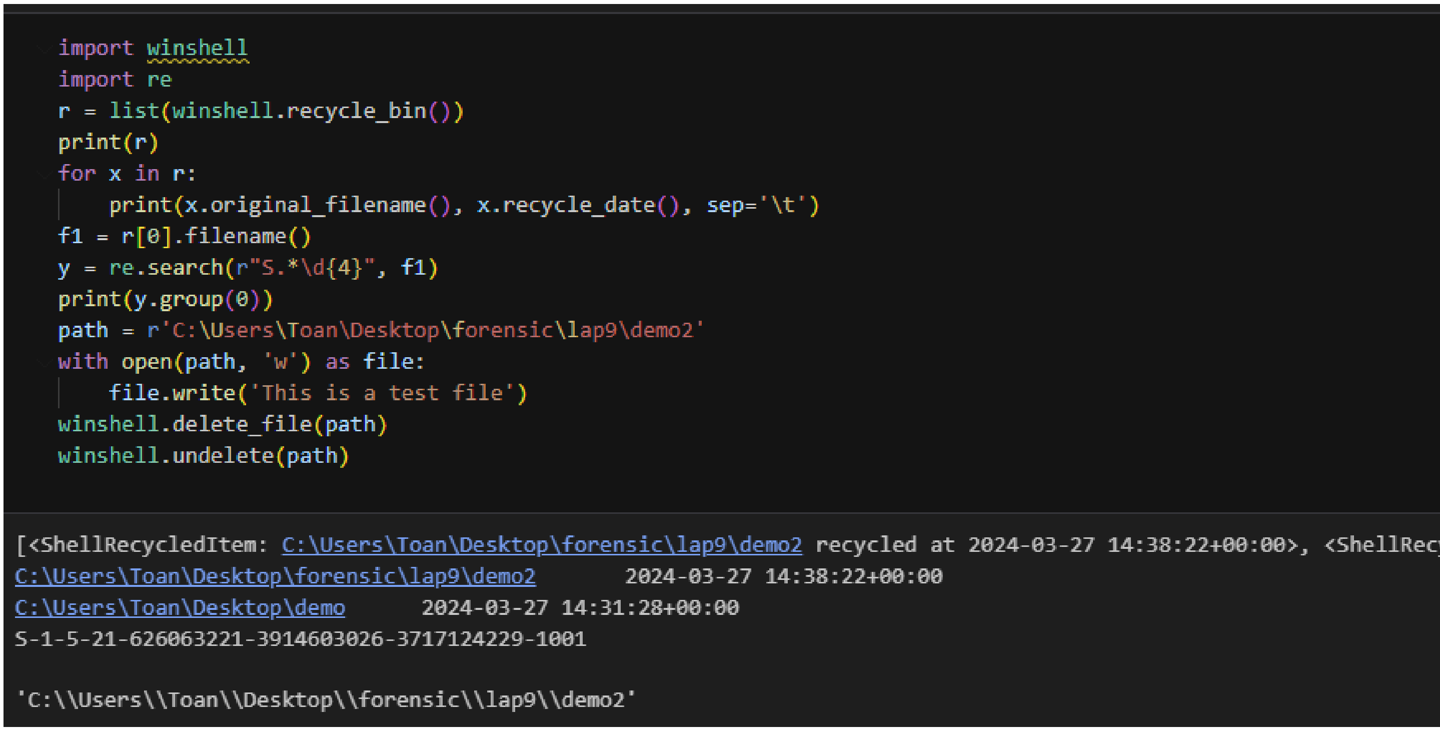
```
[<ShellRecycledItem: C:\Users\Toan\Desktop\forensic\lap9\demo recycled at 2024-0                                              \forensic\lap9\demo2 recycled a
C:\Users\Toan\Desktop\forensic\lap9\demo        2024-03-27 14:27:06+00:00
C:\Users\Toan\Desktop\forensic\lap9\demo2       2024-03-27 14:27:20+00:00
S-1-5-21-626063221-3914603026-3717124229-1001
```

Delete File

Are you sure you want to move this file to the Recycle Bin?

demo2
Type: Text Document
Size: 19 bytes
Date modified: 3/27/2024 9:27 AM

For this part we will demonstrate some of the use for the winshell function, and one of those functions are delete_file(deleted the file) and undelete(undeleted the file), they both take the files path for them to be functions. Also in the first half of the code it shows what file are currently in the recycle bin and what date did it get deleted.

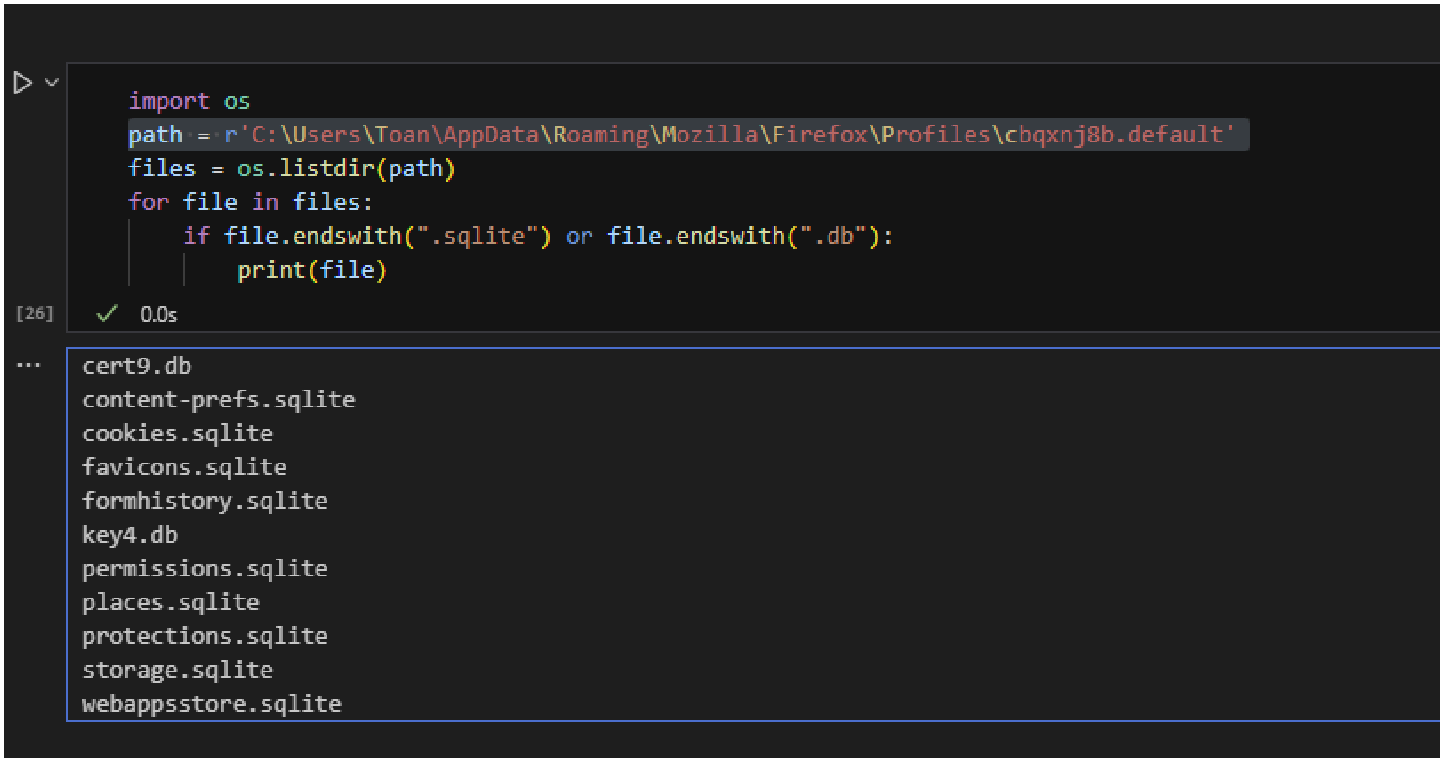


```
import winshell
import re
r = list(winshell.recycle_bin())
print(r)
for x in r:
    print(x.original_filename(), x.recycle_date(), sep='\t')
f1 = r[0].filename()
y = re.search(r"S.*\d{4}", f1)
print(y.group(0))
path = r'C:\Users\Toan\Desktop\forensic\lap9\demo2'
with open(path, 'w') as file:
    file.write('This is a test file')
winshell.delete_file(path)
winshell.undelete(path)
```

```
[<ShellRecycledItem: C:\Users\Toan\Desktop\forensic\lap9\demo2 recycled at 2024-03-27 14:38:22+00:00>, <ShellRec
C:\Users\Toan\Desktop\forensic\lap9\demo2       2024-03-27 14:38:22+00:00
C:\Users\Toan\Desktop\demo      2024-03-27 14:31:28+00:00
S-1-5-21-626063221-3914603026-3717124229-1001

'C:\\Users\\Toan\\Desktop\\forensic\\lap9\\demo2'
```

You could also do this for any file type.

Toan Ngo
date:3/29/24

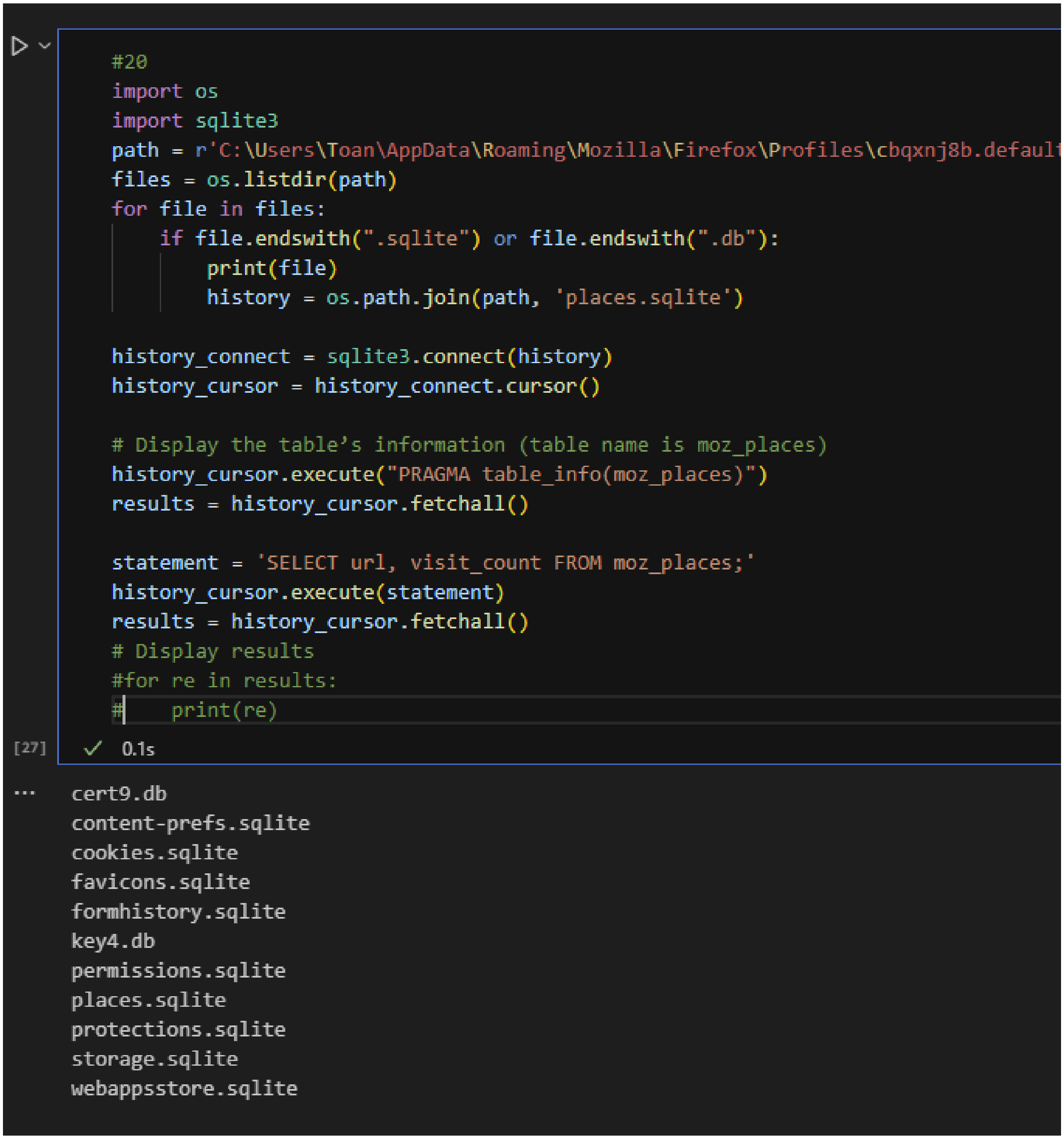


```python
import os
path = r'C:\Users\Toan\AppData\Roaming\Mozilla\Firefox\Profiles\cbqxnj8b.default'
files = os.listdir(path)
for file in files:
    if file.endswith(".sqlite") or file.endswith(".db"):
        print(file)
```

```
cert9.db
content-prefs.sqlite
cookies.sqlite
favicons.sqlite
formhistory.sqlite
key4.db
permissions.sqlite
places.sqlite
protections.sqlite
storage.sqlite
webappsstore.sqlite
```

This code is responsible for extracting all the files that end with .sqlite and .db extension which are responsible for keeping track of your browser activity.

Toan Ngo
date:3/29/24



```python
#20
import os
import sqlite3
path = r'C:\Users\Toan\AppData\Roaming\Mozilla\Firefox\Profiles\cbqxnj8b.default
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()

# Display the table’s information (table name is moz_places)
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()
# Display results
#for re in results:
#    print(re)
```

```
cert9.db
content-prefs.sqlite
cookies.sqlite
favicons.sqlite
formhistory.sqlite
key4.db
permissions.sqlite
places.sqlite
protections.sqlite
storage.sqlite
webappsstore.sqlite
```

Finally this we did the same thing as the prev step extract the .db and .sqlite files and then we feed it to sqlite3 function which is responsible for extracting all the history data from the .db and sqlite files, and at the and we prepare a statement object of what we want get from the file, and call fetchall function with it turn get all the the relative data you want in the statement.

Toan Ngo
date:3/29/24

In conclusion, there are many tools out there that are used for the extraction of cookies,history,and cache of a browser. Any of them should be just fine to use, however just making sure that you are downloading the correct version of the tools and you should be all set. System registry are extremely important to keep safe because all your sensitive system information are stored in there, and if compromised it will lead to suspicious malware injection and leaking sensitive private information, if you need more prove then just look at this report with demonstration part,i just use a ide to access the file that is exist on my computer by using the window registry what say the bad actor can't do too that if your window registry is compromised, so in order to be safe in today standard, practice good online safety is a must.

Toan Ngo
date:3/29/24

Resource

Tools to extract: cookies,history,cache

Chrome Cache: https://www.nirsoft.net/utils/chrome_cache_view.html
Chrome History: https://www.nirsoft.net/utils/chrome_history_view.html
Chrome Cookies: https://www.nirsoft.net/utils/chrome_cookies_view.html
Mozilla Cache: https://www.nirsoft.net/utils/mozilla_cache_viewer.html
Mozilla History: https://www.nirsoft.net/utils/mozilla_history_view.html
Mozilla Cookies: https://www.nirsoft.net/utils/mzcv.html

Lab9 resource

Window registry:
https://learn.microsoft.com/en-us/troubleshoot/windows-server/performance/windows-registry-advanced-users

Sam files:
https://www.lsoft.net/posts/what-is-a-sam-file/

Extra information for chrome about cookies,history,cache
https://support.google.com/accounts/answer/32050?hl=en&co=GENIE.Platform%3DDesktop

Extra information for firefox about cookies,history,cache

https://support.mozilla.org/en-US/kb/clear-cookies-and-site-data-firefox