LAB 8: WINDOWS FORENSICS – PART III

Lab Requirements

1. Microsoft Windows virtual machine
2. NIRSOFT Browser cache, history, and cookies history software
3. Python 3.x with winreg, os, and winshell libraries installed

Content

Part I: Web Browser Artifacts using NIRSOFT Tools

STEP 1: Web browsers store valuable forensic information on the host computer. This information can be gathered by investigators and presented as evidence of user's actions in the court of law. Among other information, browsers store caches, browsing history, and cookies.

> NOTE 1-1. **Browsing history:** It contains the list of visited webpages, webpages' titles, and time of visit, among other metadata.
>
> NOTE 1-2. **Caches:** When visiting a webpage, the browser stores certain information gathered from the visited website. Such information is referred to as web browsing cache. Cache might information html files, JavaScript files, image files, among others.
>
> NOTE 1-3. **Cookies:** Web servers need to keep track of established sessions with users (the user uses a web browser). The web server created small packets of information stores on the client's machine. This information is retrieved by the server in subsequent interactions between the client (i.e., web browser) and the web server. Such information might include access time,

history of visited pages, autocompletion of names, addresses, etc. and shopping cards, among other essential information for stateful interactions.

STEP 2: Download the following tools and unzip the downloaded files in a folder on your computer.

Chrome Cache: https://www.nirsoft.net/utils/chrome_cache_view.html

Chrome History: https://www.nirsoft.net/utils/chrome_history_view.html

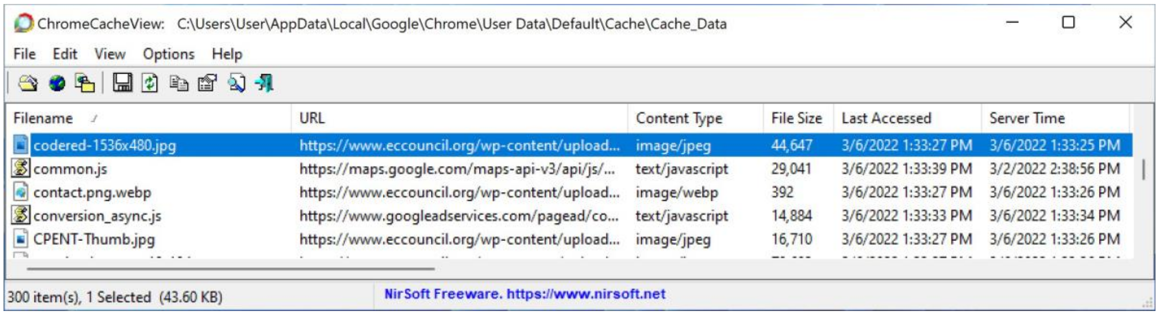
Chrome Cookies: https://www.nirsoft.net/utils/chrome_cookies_view.html

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

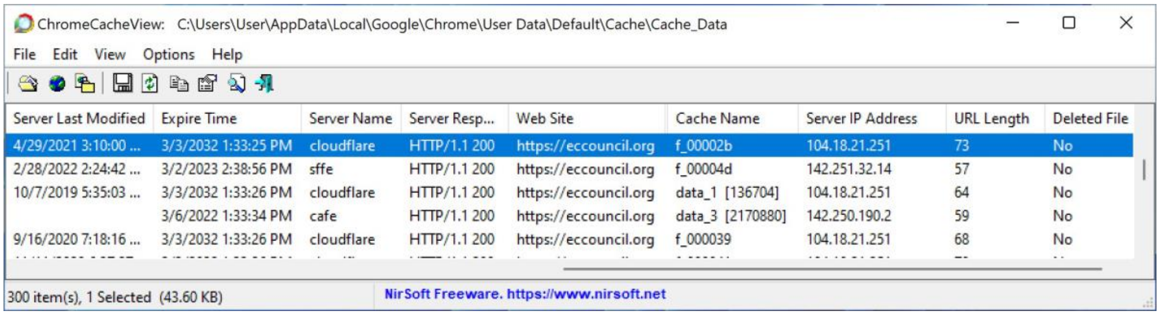
STEP 3: Run ChromeCacheView.exe from downloaded in STEP 2. Note that the Chrome cache data is stored in the folder C:\Users\User\AppData\Local\Google\Chrome\User Data\Default\Cache\Cache_Data


ChromeCacheView: C:\Users\User\AppData\Local\Google\Chrome\User Data\Default\Cache\Cache_Data
File
Edit
View
Options
Help
NirSoft Freeware. https://www.nirsoft.net

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
conversion_async.js	https://www.googleadservices.com/pagead/co...	text/javascript	14,884	3/6/2022 1:33:33 PM	3/6/2022 1:33:34 PM
CPENT-Thumb.jpg	https://www.eccouncil.org/wp-content/upload...	image/jpeg	16,710	3/6/2022 1:33:27 PM	3/6/2022 1:33:26 PM

300 item(s), 1 Selected (43.60 KB)

Part 1

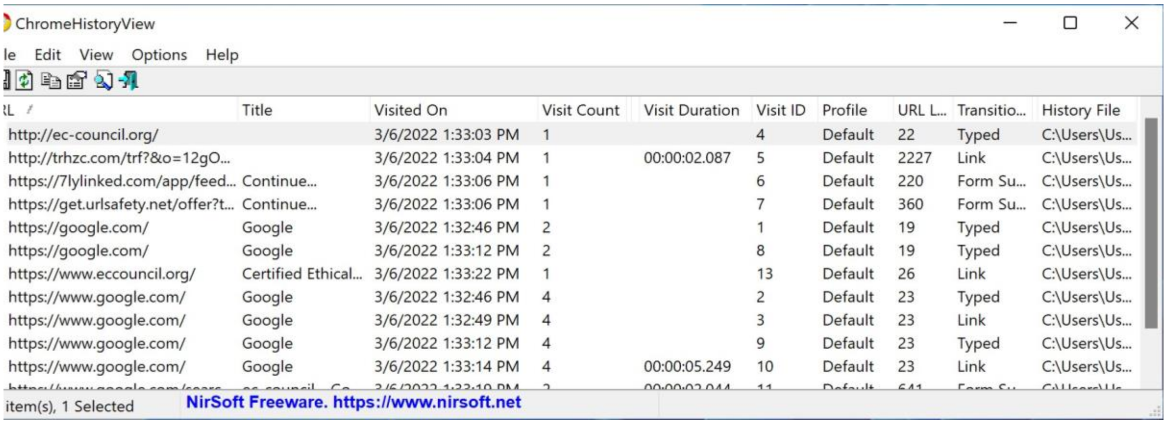

ChromeCacheView: C:\Users\User\AppData\Local\Google\Chrome\User Data\Default\Cache\Cache_Data
File
Edit
View
Options
Help
NirSoft Freeware. https://www.nirsoft.net

Server Last Modified	Expire Time	Server Name	Server Resp...	Web Site	Cache Name	Server IP Address	URL Length	Deleted File
4/29/2021 3:10:00 ...	3/3/2032 1:33:25 PM	cloudflare	HTTP/1.1 200	https://eccouncil.org	f_00002b	104.18.21.251	73	No
2/28/2022 2:24:42 ...	3/2/2023 2:38:56 PM	sffe	HTTP/1.1 200	https://eccouncil.org	f_00004d	142.251.32.14	57	No
10/7/2019 5:35:03 ...	3/3/2032 1:33:26 PM	cloudflare	HTTP/1.1 200	https://eccouncil.org	data_1 [136704]	104.18.21.251	64	No
	3/6/2022 1:33:34 PM	cafe	HTTP/1.1 200	https://eccouncil.org	data_3 [2170880]	142.250.190.2	59	No
9/16/2020 7:18:16 ...	3/3/2032 1:33:26 PM	cloudflare	HTTP/1.1 200	https://eccouncil.org	f_000039	104.18.21.251	68	No

300 item(s), 1 Selected (43.60 KB)

Part 2

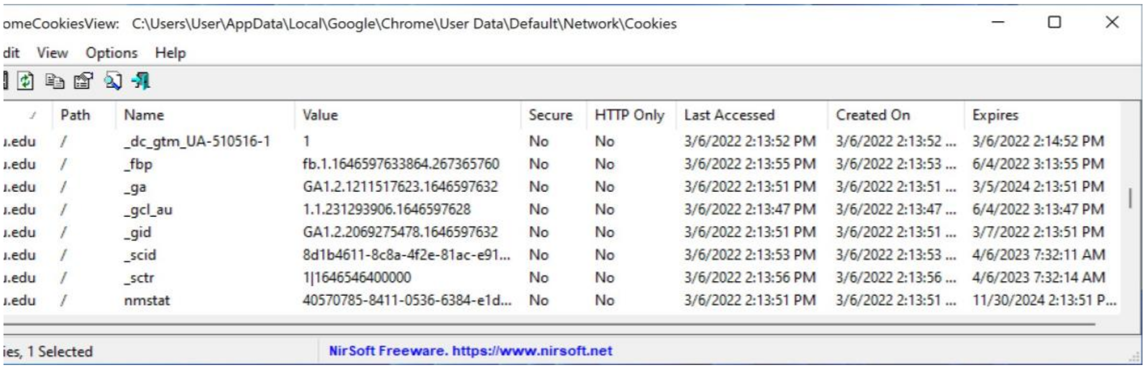
STEP 4: Run ChromeHistoryView.exe[.] The browsing history is stored in the file C:\Users\User\AppData\Local\Google\Chrome\User Data\Default\History



RL	Title	Visited On	Visit Count	Visit Duration	Visit ID	Profile	URL L...	Transitio...	History File
http://ec-council.org/		3/6/2022 1:33:03 PM	1		4	Default	22	Typed	C:\Users\Us...
http://trhzc.com/trf?&o=12gO...		3/6/2022 1:33:04 PM	1	00:00:02.087	5	Default	2227	Link	C:\Users\Us...
https://7lylinked.com/app/feed...	Continue...	3/6/2022 1:33:06 PM	1		6	Default	220	Form Su...	C:\Users\Us...
https://get.urlsafety.net/offer?t...	Continue...	3/6/2022 1:33:06 PM	1		7	Default	360	Form Su...	C:\Users\Us...
https://google.com/	Google	3/6/2022 1:32:46 PM	2		1	Default	19	Typed	C:\Users\Us...
https://google.com/	Google	3/6/2022 1:33:12 PM	2		8	Default	19	Typed	C:\Users\Us...
https://www.eccouncil.org/	Certified Ethical...	3/6/2022 1:33:22 PM	1		13	Default	26	Link	C:\Users\Us...
https://www.google.com/	Google	3/6/2022 1:32:46 PM	4		2	Default	23	Typed	C:\Users\Us...
https://www.google.com/	Google	3/6/2022 1:32:49 PM	4		3	Default	23	Link	C:\Users\Us...
https://www.google.com/	Google	3/6/2022 1:33:12 PM	4		9	Default	23	Typed	C:\Users\Us...
https://www.google.com/	Google	3/6/2022 1:33:14 PM	4	00:00:05.249	10	Default	23	Link	C:\Users\Us...
https://www.google.com/searc...	ec-council - Go...	3/6/2022 1:33:10 PM	2	00:00:02.044	11	Default	641	Form Su...	C:\Users\Us...

item(s), 1 Selected NirSoft Freeware. https://www.nirsoft.net

STEP 5: Run ChromeCookiesView.exe. The following screen will appear containing the cookies stored on your machine by remote servers.



omeCookiesView: C:\Users\User\AppData\Local\Google\Chrome\User Data\Default\Network\Cookies
dit View Options Help

	Path	Name	Value	Secure	HTTP Only	Last Accessed	Created On	Expires
ı.edu	/	_dc_gtm_UA-510516-1	1	No	No	3/6/2022 2:13:52 PM	3/6/2022 2:13:52 ...	3/6/2022 2:14:52 PM
ı.edu	/	_fbp	fb.1.1646597633864.267365760	No	No	3/6/2022 2:13:55 PM	3/6/2022 2:13:53 ...	6/4/2022 3:13:55 PM
ı.edu	/	_ga	GA1.2.1211517623.1646597632	No	No	3/6/2022 2:13:51 PM	3/6/2022 2:13:51 ...	3/5/2024 2:13:51 PM
ı.edu	/	_gcl_au	1.1.231293906.1646597628	No	No	3/6/2022 2:13:47 PM	3/6/2022 2:13:47 ...	6/4/2022 3:13:47 PM
ı.edu	/	_gid	GA1.2.2069275478.1646597632	No	No	3/6/2022 2:13:51 PM	3/6/2022 2:13:51 ...	3/7/2022 2:13:51 PM
ı.edu	/	_scid	8d1b4611-8c8a-4f2e-81ac-e91...	No	No	3/6/2022 2:13:53 PM	3/6/2022 2:13:53 ...	4/6/2023 7:32:11 AM
ı.edu	/	_sctr	1|1646546400000	No	No	3/6/2022 2:13:56 PM	3/6/2022 2:13:56 ...	4/6/2023 7:32:14 AM
ı.edu	/	nmstat	40570785-8411-0536-6384-e1d...	No	No	3/6/2022 2:13:51 PM	3/6/2022 2:13:51 ...	11/30/2024 2:13:51 P...

ies, 1 Selected NirSoft Freeware. https://www.nirsoft.net

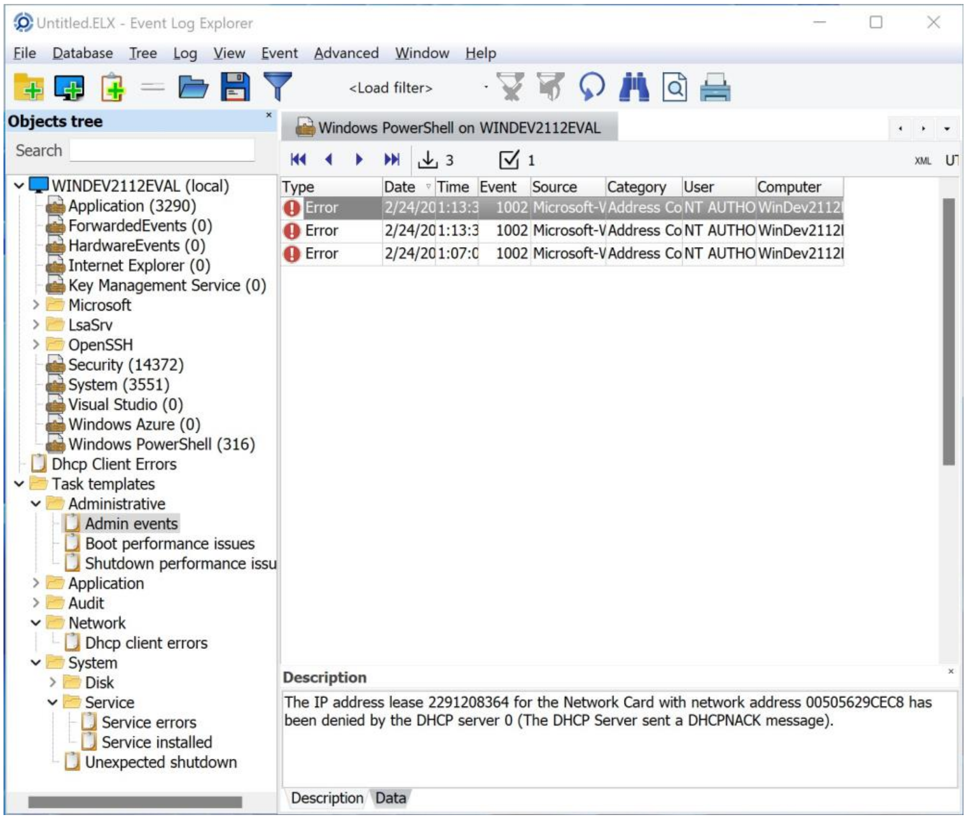
STEP 6: Repeat steps 3-5 for Mozilla Firefox browser.

Part II: Viewing, Monitoring, and Analyzing Windows Events

STEP 7: In the event of a security incident, investigators analyze the security logs, system logs, and application logs, to analyze the sequence of events leading to the cybercrime.

STEP 8: The log files on Windows 11 operating system are located on the folder C:\Windows\System32\config[.]

STEP 9: Download Event Log Explorer through the following website: https://eventlogxp.com/[.] Install the Home edition and use the provided key to activate the installed software. The home edition has limited functionalities. You might choose to download the 30-day Pro trial version. For instance, the feature of opening a given log file is not available in the home edition.



Type	Date	Time	Event	Source	Category	User	Computer
Error	2/24/20	1:13:3	1002	Microsoft-V	Address Co	NT AUTHO	WinDev2112I
Error	2/24/20	1:13:3	1002	Microsoft-V	Address Co	NT AUTHO	WinDev2112I
Error	2/24/20	1:07:0	1002	Microsoft-V	Address Co	NT AUTHO	WinDev2112I

Description

The IP address lease 2291208364 for the Network Card with network address 00505629CEC8 has been denied by the DHCP server 0 (The DHCP Server sent a DHCPNACK message).

STEP 10: Run a selected tasks from the task templates and check log files provided under the name of the Windows' machine (WINDEV2112EVAL (local) in the previous screenshot).

Part III: [Extra] Extracting Forensic Data from Computers using OSForensics

STEP 11: Download the Free version of OSForensics available at https://www.osforensics.com/download.html[.]

STEP 12: Download small drive image from the Digital Corpora website, create a case, and analyze the downloaded image. Choose a small file. Link: https://downloads.digitalcorpora.org/corpora/scenarios/2009-m57-patents/drives-redacted/

Part IV: Handling Windows Registry using Python

STEP 12: The Python library winreg provides access to the Windows registry. Using this library, keys and values can be created, read, and updated. The library is available at https://docs.python.org/3/library/winreg.html[.]

STEP 13: Access the registry hives.

```

# In this example, we examine the content of the HKEY_USERS hive
# Other constants in winreg: HKEY_CLASSES_ROOT, HKEY_CURRENT_USER,
# HKEY_LOCAL_MACHINE, HKEY_CURRENT_CONFIG,  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

```

Output:

```
0: .DEFAULT
1: S-1-5-19
2: S-1-5-20
3: S-1-5-21-2876060954-1225872718-3796797708-1001
4: S-1-5-21-2876060954-1225872718-3796797708-1001_Classes
5: S-1-5-18
```

Step 14: Access the registry keys and values.

```

# This code should go after the code provided in Step 13. 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

# 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" 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
```

```
15.0 : 2021-12-16 00:58:57.735227-06:00
16.0 : 2021-12-16 00:58:58.407564-06:00
ClickToRun : 2021-12-16 00:58:58.516913-06:00
Common : 2021-12-16 00:58:58.532538-06:00
DmsClient : 2021-12-16 00:58:58.532538-06:00
Excel : 2021-12-16 00:58:58.532538-06:00
Lync : 2021-12-16 00:58:58.532538-06:00
Outlook : 2021-12-16 00:58:58.532538-06:00
PowerPoint : 2021-12-16 00:58:58.532538-06:00
Teams : 2021-12-16 00:58:58.532538-06:00
Word : 2021-12-16 00:58:58.532538-06:00
```

Part V: Handling Windows Recycle Bin using Python

Step 15: The winshell module provides access to Windows shell functions. These functionalities include:

- Recycle bin
- Special Folders
- File Operations
- Shortcuts
- Structured Storage

Step 16: Accessing and handling the recycle bin.

```python
# import necessary libraries
import winshell import re

# read the items inside the recycle bin as a list  r
= list(winshell.recycle_bin())

# iterate over the deleted files and display their full names and recycle date
for x in r:
    print(x.original_filename(), x.recycle_date(), sep='\t')
# The filename() method of an element within r contains the SID of the user who
# deleted the file. This is a very important forensic feature for attribution.
# Retrieve the SID of the user who deleted the file
f1 = r[0].filename() y = re.search(r"S.*\d{4}", f1)
print(y.group(0))

# create a file, delete it, and undelete files
path = r'C:\Users\User\Desktop\test.txt' with
open(path, 'w') as file:
    file.write('This is a test file')
# delete the file
winshell.delete_file(path)

# recover the deleted file winshell.undelete(path)
```

Step 17: The winshell module's documentation is available at https://winshell.readthedocs.io/en/latest/contents.html[.]

Part VI: Reading Browser History, Cookies, and Cache using Python

STEP 18: In this part of the lab, we focus on Mozilla Firefox Web Browser. The generalization to other browsers should be straightforward. Firefox web browser stores .sqlite database files.

STEP 19: The path to these database files and a list of the contained database files in this folder are found using the following code:

```
# Import necessary libraries import os

# The path to the database files path =
r'C:\Users\User\AppData\Roaming\Mozilla\Firefox\Profiles\6nljacx9.defaultrelease'

# Get the content of the path folder files =
os.listdir(path)

# Display the .sqlite files 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          #
 browsing, download history protections.sqlite
 storage.sqlite webappsstore.sqlite
```

STEP 20: use the following code to retrieve the browsing history.

```
# Import necessary libraries
import os
```

```
# The path to the database files path =
r'C:\Users\User\AppData\Roaming\Mozilla\Firefox\Profiles\6nljacx9.defaultrelease'

# Get the content of the path folder files =
os.listdir(path)

# Display the .sqlite files 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
```