Report 8

For this week's lab, we covered the last section of Windows Forensics. The first part of the lab involved Web Browser Artifacts using NIRSOFT Tools. Part two was about Viewing, Monitoring, and Analyzing Windows Events. Part 3 then covered Extracting Forensic Data from Computers using OSForensics. Part four involved Handling Windows Registry using Python. Part Five contained Handling Windows Recycle Bin using Python. The last part deals with Reading Browser History, Cookies, and Cache using Python.

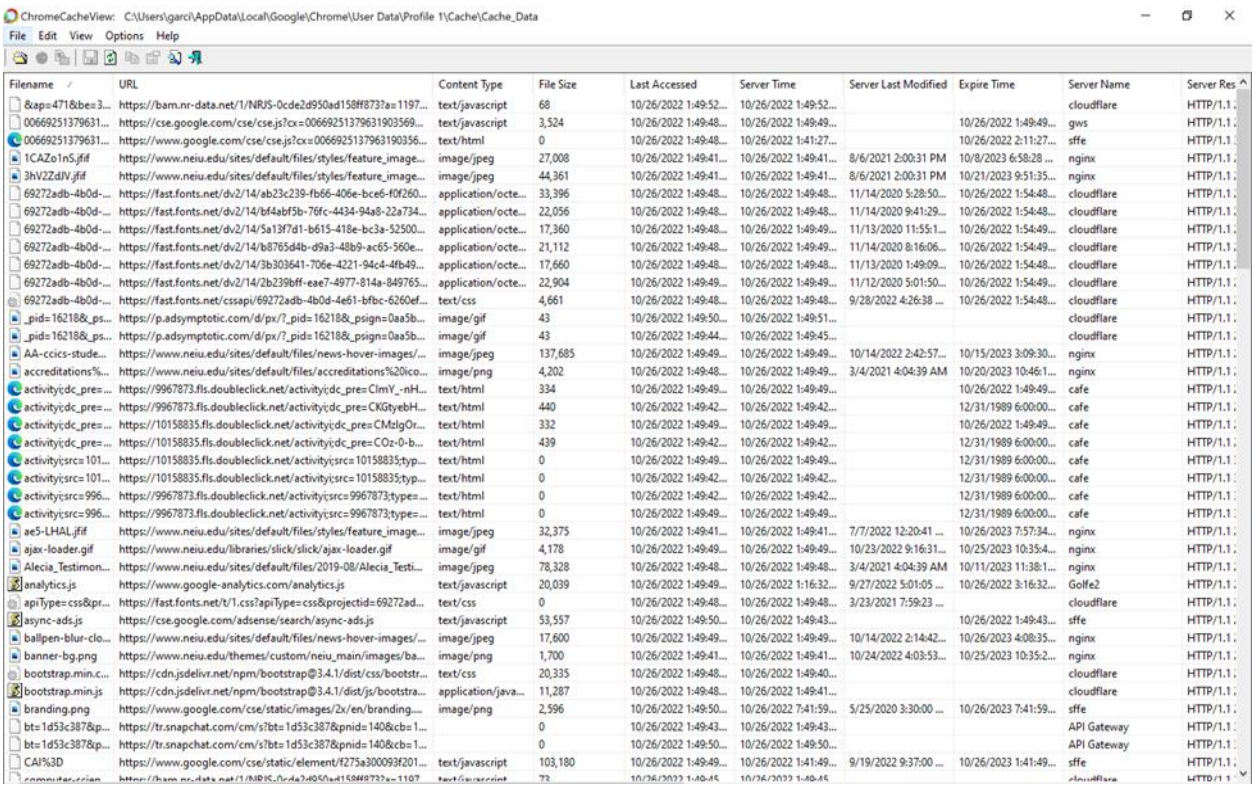
In part 1, In order to extract the Browsing History, Cache, and Cookies, we first needed to download the software required to do this. Here are the links below that I used to download the software.

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

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

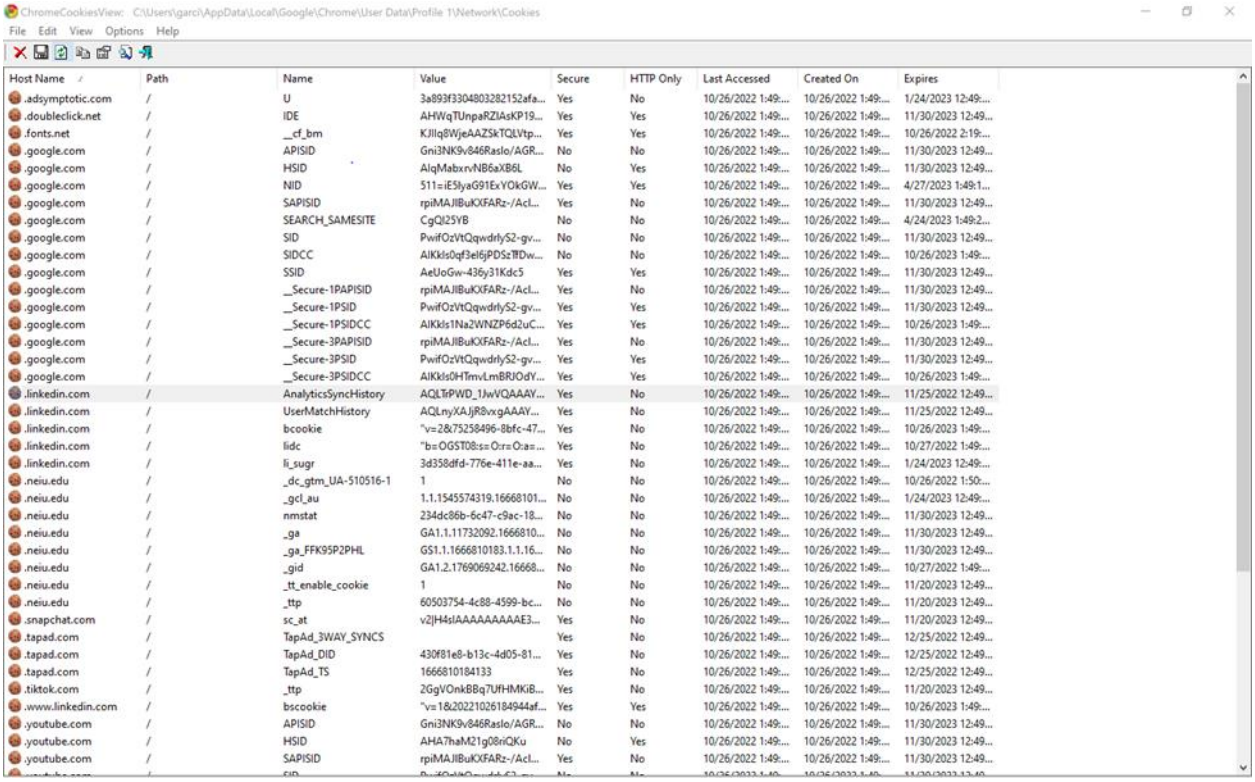
Chrome Cookies: https://www.nirsoft.net/utils/chrome_cookies_view.html

The program that I ran first was the ChromeCacheView. You can see below the caches that were in my system. I only navigated to neiu.edu.



Filename	URL	Content Type	File Size	Last Accessed	Server Time	Server Last Modified	Expire Time	Server Name	Server Res
&ap=471&be=3...	https://bam.nr-data.net/1/NRJS-0cde2d950ad158ff873?a=1197...	text/javascript	68	10/26/2022 1:49:52...	10/26/2022 1:49:52...			cloudflare	HTTP/1.1
006692513796 31...	https://cse.google.com/cse/cse.js?cx=006692513796 3190356 9...	text/javascript	3,524	10/26/2022 1:49:48...	10/26/2022 1:49:49...		10/26/2022 1:49:49...	gws	HTTP/1.1
006692513796 31...	https://www.google.com/cse/cse.js?cx=006692513796 3190356...	text/html	0	10/26/2022 1:49:48...	10/26/2022 1:41:27...		10/26/2022 2:11:27...	sffe	HTTP/1.1
1CAZo1nS.jfif	https://www.neiu.edu/sites/default/files/styles/feature_image...	image/jpeg	27,008	10/26/2022 1:49:41...	10/26/2022 1:49:41...	8/6/2021 2:00:31 PM	10/8/2023 6:58:28 ...	nginx	HTTP/1.1
3hV2ZdJV.jfif	https://www.neiu.edu/sites/default/files/styles/feature_image...	image/jpeg	44,361	10/26/2022 1:49:41...	10/26/2022 1:49:41...	8/6/2021 2:00:31 PM	10/21/2023 9:51:35...	nginx	HTTP/1.1
69272adb-4b0d-...	https://fast.fonts.net/dv2/14/ab23c239-fb66-406e-bce6-f0f260...	application/octe...	33,396	10/26/2022 1:49:48...	10/26/2022 1:49:48...	11/14/2020 5:28:50...	10/26/2022 1:54:48...	cloudflare	HTTP/1.1
69272adb-4b0d-...	https://fast.fonts.net/dv2/14/bf4abf5b-76fc-4434-94a8-22a734...	application/octe...	22,056	10/26/2022 1:49:48...	10/26/2022 1:49:48...	11/14/2020 9:41:29...	10/26/2022 1:54:48...	cloudflare	HTTP/1.1
69272adb-4b0d-...	https://fast.fonts.net/dv2/14/5a13f7d1-b615-418e-bc3a-52500...	application/octe...	17,360	10/26/2022 1:49:48...	10/26/2022 1:49:49...	11/13/2020 11:55:1...	10/26/2022 1:54:49...	cloudflare	HTTP/1.1
69272adb-4b0d-...	https://fast.fonts.net/dv2/14/b8765d4b-d9a3-48b9-ac65-560e...	application/octe...	21,112	10/26/2022 1:49:48...	10/26/2022 1:49:49...	11/14/2020 8:16:06...	10/26/2022 1:54:49...	cloudflare	HTTP/1.1
69272adb-4b0d-...	https://fast.fonts.net/dv2/14/3b303641-706e-4221-94c4-4fb49...	application/octe...	17,660	10/26/2022 1:49:48...	10/26/2022 1:49:48...	11/13/2020 1:49:09...	10/26/2022 1:54:48...	cloudflare	HTTP/1.1
69272adb-4b0d-...	https://fast.fonts.net/dv2/14/2b239bff-eae7-4977-814a-849765...	application/octe...	22,904	10/26/2022 1:49:49...	10/26/2022 1:49:49...	11/12/2020 5:01:50...	10/26/2022 1:54:49...	cloudflare	HTTP/1.1
69272adb-4b0d-...	https://fast.fonts.net/cssapi/69272adb-4b0d-4e61-bfbc-6260ef...	text/css	4,661	10/26/2022 1:49:48...	10/26/2022 1:49:48...	9/28/2022 4:26:38 ...	10/26/2022 1:54:48...	cloudflare	HTTP/1.1
_pid=16218&_ps...	https://p.adsymptotic.com/d/px/?_pid=16218&_psign=0aa5b...	image/gif	43	10/26/2022 1:49:50...	10/26/2022 1:49:51...			cloudflare	HTTP/1.1
_pid=16218&_ps...	https://p.adsymptotic.com/d/px/?_pid=16218&_psign=0aa5b...	image/gif	43	10/26/2022 1:49:44...	10/26/2022 1:49:45...			cloudflare	HTTP/1.1
AA-ccics-stude...	https://www.neiu.edu/sites/default/files/news-hover-images/...	image/jpeg	137,685	10/26/2022 1:49:49...	10/26/2022 1:49:49...	10/14/2022 2:42:57...	10/15/2023 3:09:30...	nginx	HTTP/1.1
accreditations%...	https://www.neiu.edu/sites/default/files/accreditations%20ico...	image/png	4,202	10/26/2022 1:49:48...	10/26/2022 1:49:49...	3/4/2021 4:04:39 AM	10/20/2023 10:46:1...	nginx	HTTP/1.1
activity;dc_pre=...	https://9967873.fls.doubleclick.net/activity;dc_pre=ClmY_-nH...	text/html	334	10/26/2022 1:49:49...	10/26/2022 1:49:49...		10/26/2022 1:49:49...	cafe	HTTP/1.1
activity;dc_pre=...	https://9967873.fls.doubleclick.net/activity;dc_pre=CKGtyebH...	text/html	440	10/26/2022 1:49:42...	10/26/2022 1:49:42...		12/31/1989 6:00:00...	cafe	HTTP/1.1
activity;dc_pre=...	https://10158835.fls.doubleclick.net/activity;dc_pre=CMzIgOr...	text/html	332	10/26/2022 1:49:49...	10/26/2022 1:49:49...		10/26/2022 1:49:49...	cafe	HTTP/1.1
activity;dc_pre=...	https://10158835.fls.doubleclick.net/activity;dc_pre=COz-0-b...	text/html	439	10/26/2022 1:49:42...	10/26/2022 1:49:42...		12/31/1989 6:00:00...	cafe	HTTP/1.1
activity;src=101...	https://10158835.fls.doubleclick.net/activity;src=10158835;typ...	text/html	0	10/26/2022 1:49:49...	10/26/2022 1:49:49...		12/31/1989 6:00:00...	cafe	HTTP/1.1
activity;src=101...	https://10158835.fls.doubleclick.net/activity;src=10158835;typ...	text/html	0	10/26/2022 1:49:42...	10/26/2022 1:49:42...		12/31/1989 6:00:00...	cafe	HTTP/1.1
activity;src=996...	https://9967873.fls.doubleclick.net/activity;src=9967873;type=...	text/html	0	10/26/2022 1:49:42...	10/26/2022 1:49:42...		12/31/1989 6:00:00...	cafe	HTTP/1.1
activity;src=996...	https://9967873.fls.doubleclick.net/activity;src=9967873;type=...	text/html	0	10/26/2022 1:49:49...	10/26/2022 1:49:49...		12/31/1989 6:00:00...	cafe	HTTP/1.1
ae5-LHAL.jfif	https://www.neiu.edu/sites/default/files/styles/feature_image...	image/jpeg	32,375	10/26/2022 1:49:41...	10/26/2022 1:49:41...	7/7/2022 12:20:41 ...	10/26/2023 7:57:34...	nginx	HTTP/1.1
ajax-loader.gif	https://www.neiu.edu/libraries/slick/slick/ajax-loader.gif	image/gif	4,178	10/26/2022 1:49:49...	10/26/2022 1:49:49...	10/23/2022 9:16:31...	10/25/2023 10:35:4...	nginx	HTTP/1.1
Alecia_Testimon...	https://www.neiu.edu/sites/default/files/2019-08/Alecia_Testi...	image/jpeg	78,328	10/26/2022 1:49:48...	10/26/2022 1:49:48...	3/4/2021 4:04:39 AM	10/11/2023 11:38:1...	nginx	HTTP/1.1
analytics.js	https://www.google-analytics.com/analytics.js	text/javascript	20,039	10/26/2022 1:49:49...	10/26/2022 1:16:32...	9/27/2022 5:01:05 ...	10/26/2022 3:16:32...	Golfe2	HTTP/1.1
apiType=css&pr...	https://fast.fonts.net/t/1.css?apiType=css&projectid=69272ad...	text/css	0	10/26/2022 1:49:48...	10/26/2022 1:49:48...	3/23/2021 7:59:23 ...		cloudflare	HTTP/1.1
async-ads.js	https://cse.google.com/adsense/search/async-ads.js	text/javascript	53,557	10/26/2022 1:49:50...	10/26/2022 1:49:43...		10/26/2022 1:49:43...	sffe	HTTP/1.1
ballpen-blur-clo...	https://www.neiu.edu/sites/default/files/news-hover-images/...	image/jpeg	17,600	10/26/2022 1:49:49...	10/26/2022 1:49:49...	10/14/2022 2:14:42...	10/26/2023 4:08:35...	nginx	HTTP/1.1
banner-bg.png	https://www.neiu.edu/themes/custom/neiu_main/images/ba...	image/png	1,700	10/26/2022 1:49:41...	10/26/2022 1:49:41...	10/24/2022 4:03:53...	10/25/2023 10:35:2...	nginx	HTTP/1.1
bootstrap.min.c...	https://cdn.jsdelivr.net/npm/bootstrap@3.4.1/dist/css/bootstr...	text/css	20,335	10/26/2022 1:49:48...	10/26/2022 1:49:40...			cloudflare	HTTP/1.1
bootstrap.min.js	https://cdn.jsdelivr.net/npm/bootstrap@3.4.1/dist/js/bootstra...	application/java...	11,287	10/26/2022 1:49:48...	10/26/2022 1:49:41...			cloudflare	HTTP/1.1
branding.png	https://www.google.com/cse/static/images/2x/en/branding....	image/png	2,596	10/26/2022 1:49:50...	10/26/2022 7:41:59...	5/25/2020 3:30:00 ...	10/26/2023 7:41:59...	sffe	HTTP/1.1
bt=1d53c387&p...	https://tr.snapchat.com/cm/s?bt=1d53c387&pnid=140&cb=1...		0	10/26/2022 1:49:43...	10/26/2022 1:49:43...			API Gateway	HTTP/1.1
bt=1d53c387&p...	https://tr.snapchat.com/cm/s?bt=1d53c387&pnid=140&cb=1...		0	10/26/2022 1:49:50...	10/26/2022 1:49:50...			API Gateway	HTTP/1.1
CAI%3D	https://www.google.com/cse/static/element/f275a300093f201...	text/javascript	103,180	10/26/2022 1:49:49...	10/26/2022 1:41:49...	9/19/2022 9:37:00 ...	10/26/2023 1:41:49...	sffe	HTTP/1.1
computer-scien...	https://bam.nr-data.net/1/NRJS-0cde2d950ad158ff873?a=1197...	text/javascript	73	10/26/2022 1:49:45...	10/26/2022 1:49:45...			cloudflare	HTTP/1.1

The second program was the ChromeCookiesView. You can see below the cookies such as Facebook and LinkedIn even though I did not go to those sites. Also, some aspects of the cookies that are used for the NEIU website are not secure. You can see the in the secure tab.

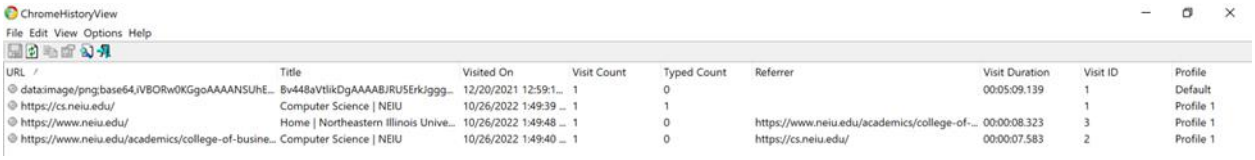


ChromeCookiesView: C:\Users\garci\AppData\Local\Google\Chrome\User Data\Profile 1\Network\Cookies

File Edit View Options Help

Host Name	Path	Name	Value	Secure	HTTP Only	Last Accessed	Created On	Expires
.adsymptotic.com	/	U	3a893f3304803282152afa...	Yes	No	10/26/2022 1:49:...	10/26/2022 1:49:...	1/24/2023 12:49:...
.doubleclick.net	/	IDE	AHWqTUnpaRZlAsKP19...	Yes	Yes	10/26/2022 1:49:...	10/26/2022 1:49:...	11/30/2023 12:49...
.fonts.net	/	__cf_bm	KJIlq8WjeAAZSkTQLVtp...	Yes	Yes	10/26/2022 1:49:...	10/26/2022 1:49:...	10/26/2022 2:19:...
.google.com	/	APISID	Gni3NK9v846RasIo/AGR...	No	No	10/26/2022 1:49:...	10/26/2022 1:49:...	11/30/2023 12:49...
.google.com	/	HSID	AIqMabxrvNB6aXB6L	No	Yes	10/26/2022 1:49:...	10/26/2022 1:49:...	11/30/2023 12:49...
.google.com	/	NID	511=iE5IyaG91ExYOkGW...	Yes	Yes	10/26/2022 1:49:...	10/26/2022 1:49:...	4/27/2023 1:49:1...
.google.com	/	SAPISID	rpiMAJlBuKXFARz-/Acl...	Yes	No	10/26/2022 1:49:...	10/26/2022 1:49:...	11/30/2023 12:49...
.google.com	/	SEARCH_SAMESITE	CgQI25YB	No	No	10/26/2022 1:49:...	10/26/2022 1:49:...	4/24/2023 1:49:2...
.google.com	/	SID	PwifOzVtQqwdrlyS2-gv...	No	No	10/26/2022 1:49:...	10/26/2022 1:49:...	11/30/2023 12:49...
.google.com	/	SIDCC	AIKkIs0qf3eI6jPDSzTBDw...	No	No	10/26/2022 1:49:...	10/26/2022 1:49:...	10/26/2023 1:49:...
.google.com	/	SSID	AeUoGw-436y31Kdc5	Yes	Yes	10/26/2022 1:49:...	10/26/2022 1:49:...	11/30/2023 12:49...
.google.com	/	__Secure-1PAPISID	rpiMAJlBuKXFARz-/Acl...	Yes	No	10/26/2022 1:49:...	10/26/2022 1:49:...	11/30/2023 12:49...
.google.com	/	__Secure-1PSID	PwifOzVtQqwdrlyS2-gv...	Yes	Yes	10/26/2022 1:49:...	10/26/2022 1:49:...	11/30/2023 12:49...
.google.com	/	__Secure-1PSIDCC	AIKkIs1Na2WNZP6d2uC...	Yes	Yes	10/26/2022 1:49:...	10/26/2022 1:49:...	10/26/2023 1:49:...
.google.com	/	__Secure-3PAPISID	rpiMAJlBuKXFARz-/Acl...	Yes	No	10/26/2022 1:49:...	10/26/2022 1:49:...	11/30/2023 12:49...
.google.com	/	__Secure-3PSID	PwifOzVtQqwdrlyS2-gv...	Yes	Yes	10/26/2022 1:49:...	10/26/2022 1:49:...	11/30/2023 12:49...
.google.com	/	__Secure-3PSIDCC	AIKkIs0HTmvLmBRJOdY...	Yes	Yes	10/26/2022 1:49:...	10/26/2022 1:49:...	10/26/2023 1:49:...
.linkedin.com	/	AnalyticsSyncHistory	AQLTrPWD_1JwVQAAAY...	Yes	No	10/26/2022 1:49:...	10/26/2022 1:49:...	11/25/2022 12:49...
.linkedin.com	/	UserMatchHistory	AQLnyXAJjR8vxgAAAY...	Yes	No	10/26/2022 1:49:...	10/26/2022 1:49:...	11/25/2022 12:49...
.linkedin.com	/	bcookie	"v=2&75258496-8bfc-47...	Yes	No	10/26/2022 1:49:...	10/26/2022 1:49:...	10/26/2023 1:49:...
.linkedin.com	/	lidc	"b=OGST08:s=O:r=O:a=...	Yes	No	10/26/2022 1:49:...	10/26/2022 1:49:...	10/27/2022 1:49:...
.linkedin.com	/	li_sugr	3d358dfd-776e-411e-aa...	Yes	No	10/26/2022 1:49:...	10/26/2022 1:49:...	1/24/2023 12:49:...
.neiu.edu	/	_dc_gtm_UA-510516-1	1	No	No	10/26/2022 1:49:...	10/26/2022 1:49:...	10/26/2022 1:50:...
.neiu.edu	/	_gcl_au	1.1.1545574319.16668101...	No	No	10/26/2022 1:49:...	10/26/2022 1:49:...	1/24/2023 12:49:...
.neiu.edu	/	nmstat	234dc86b-6c47-c9ac-18...	No	No	10/26/2022 1:49:...	10/26/2022 1:49:...	11/30/2023 12:49...
.neiu.edu	/	_ga	GA1.1.11732092.1666810...	No	No	10/26/2022 1:49:...	10/26/2022 1:49:...	11/30/2023 12:49...
.neiu.edu	/	_ga_FFK95P2PHL	GS1.1.1666810183.1.1.16...	No	No	10/26/2022 1:49:...	10/26/2022 1:49:...	11/30/2023 12:49...
.neiu.edu	/	_gid	GA1.2.1769069242.16668...	No	No	10/26/2022 1:49:...	10/26/2022 1:49:...	10/27/2022 1:49:...
.neiu.edu	/	_tt_enable_cookie	1	No	No	10/26/2022 1:49:...	10/26/2022 1:49:...	11/20/2023 12:49...
.neiu.edu	/	_ttp	60503754-4c88-4599-bc...	No	No	10/26/2022 1:49:...	10/26/2022 1:49:...	11/20/2023 12:49...
.snapchat.com	/	sc_at	v2|H4sIAAAAAAAAAE3...	Yes	No	10/26/2022 1:49:...	10/26/2022 1:49:...	11/20/2023 12:49...
.tapad.com	/	TapAd_3WAY_SYNCS		Yes	No	10/26/2022 1:49:...	10/26/2022 1:49:...	12/25/2022 12:49...
.tapad.com	/	TapAd_DID	430f81e8-b13c-4d05-81...	Yes	No	10/26/2022 1:49:...	10/26/2022 1:49:...	12/25/2022 12:49...
.tapad.com	/	TapAd_TS	1666810184133	Yes	No	10/26/2022 1:49:...	10/26/2022 1:49:...	12/25/2022 12:49...
.tiktok.com	/	_ttp	2GgVOnkBBq7UfHMKiB...	Yes	No	10/26/2022 1:49:...	10/26/2022 1:49:...	11/20/2023 12:49...
.www.linkedin.com	/	bscookie	"v=1&20221026184944af...	Yes	Yes	10/26/2022 1:49:...	10/26/2022 1:49:...	10/26/2023 1:49:...
.youtube.com	/	APISID	Gni3NK9v846RasIo/AGR...	No	No	10/26/2022 1:49:...	10/26/2022 1:49:...	11/30/2023 12:49...
.youtube.com	/	HSID	AHA7haM21g08riQKu	No	Yes	10/26/2022 1:49:...	10/26/2022 1:49:...	11/30/2023 12:49...
.youtube.com	/	SAPISID	rpiMAJlBuKXFARz-/Acl...	Yes	No	10/26/2022 1:49:...	10/26/2022 1:49:...	11/30/2023 12:49...

The third program was the ChromeHistoryView. This basically shows all the websites that I visited. You can see below the sites I visited foforhis part of the lab



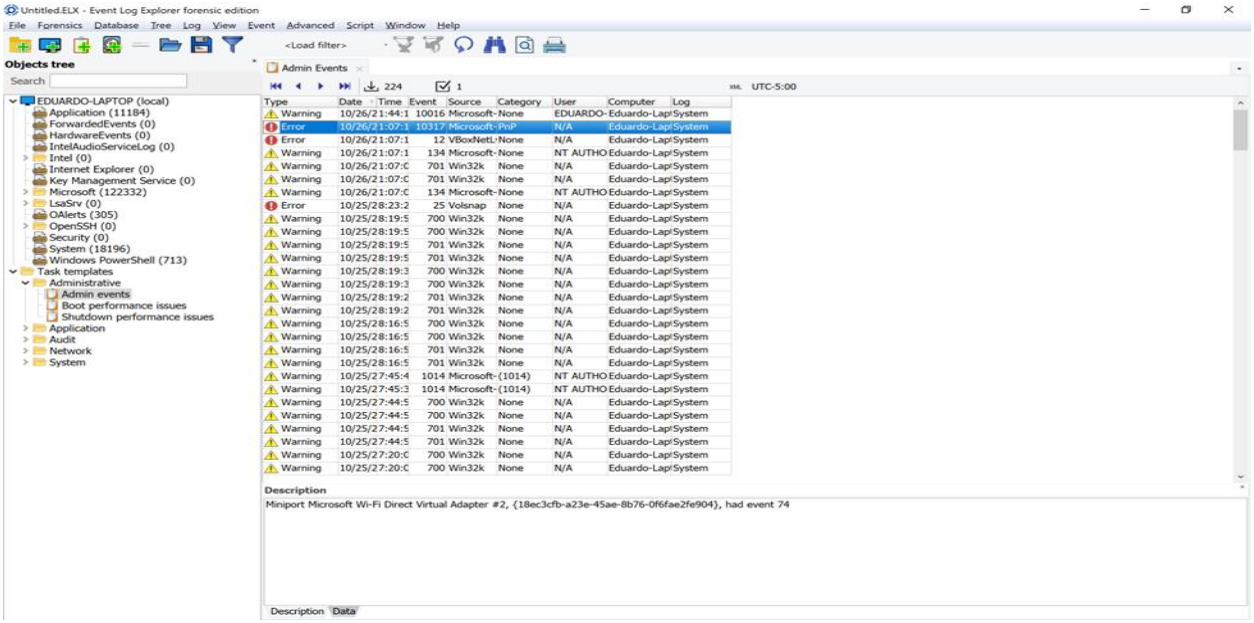
ChromeHistoryView

File Edit View Options Help

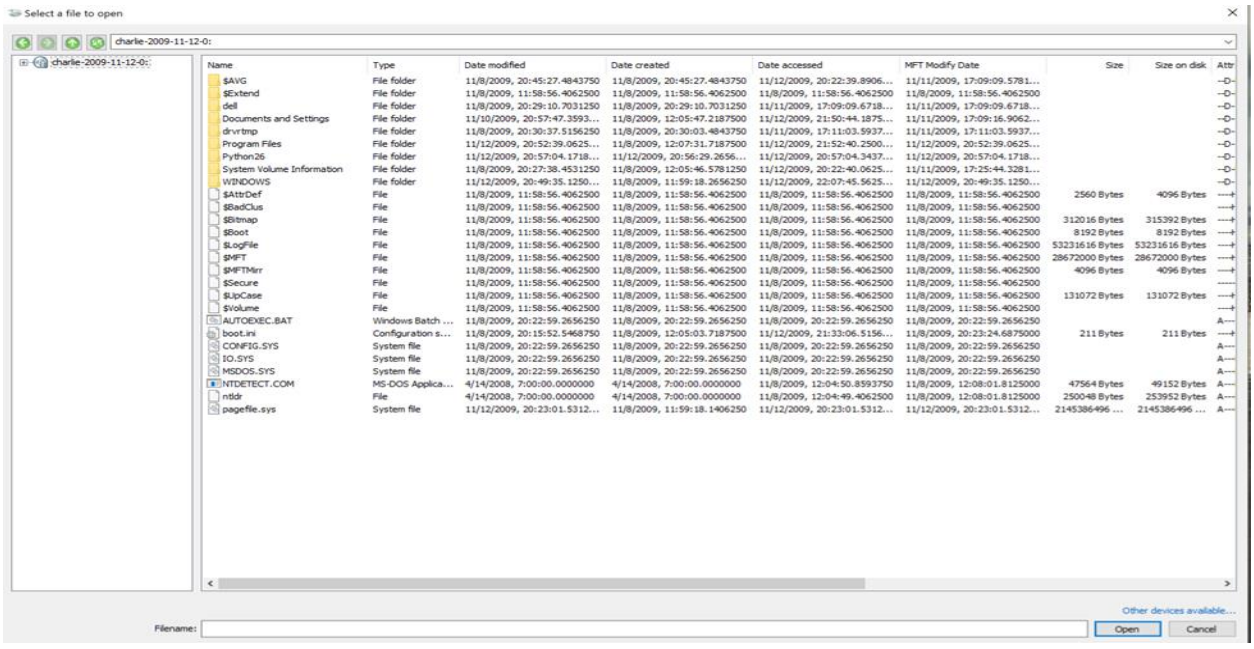
URL	Title	Visited On	Visit Count	Typed Count	Referrer	Visit Duration	Visit ID	Profile
...	Bv448aVtlikDgAAAABJRU5ErkJggg...	12/20/2021 12:59:1...	1	0		00:05:09.139	1	Default
https://cs.neiu.edu/	Computer Science | NEIU	10/26/2022 1:49:39 ...	1	1			1	Profile 1
https://www.neiu.edu/	Home | Northeastern Illinois Unive...	10/26/2022 1:49:48 ...	1	0	https://www.neiu.edu/academics/college-of-...	00:00:08.323	3	Profile 1
https://www.neiu.edu/academics/college-of-busine...	Computer Science | NEIU	10/26/2022 1:49:40 ...	1	0	https://cs.neiu.edu/	00:00:07.583	2	Profile 1

The second part of the lab involved using Event Log Explore to analyze the security logs, system logs, and application logs. With this information, you can create a sequence of events that lead to cybercrimes. The software is located using this link: https://eventlogxp.com/. Remember to

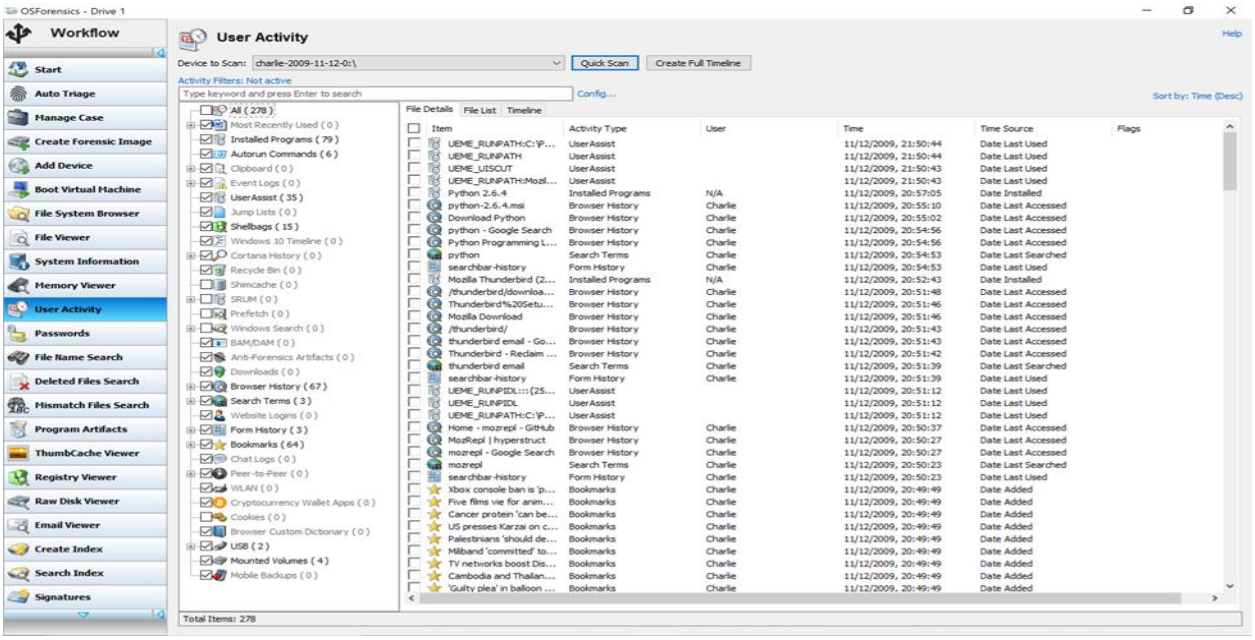
select the 30-day Pro trial to use all the features. Here below I navigated to My Laptop > Task Application > Admin Events > To access the logs below.



The next part of the lab, I used OS Forensics to investigate the contents of a drive. I downloaded the software by sign this link https://www.osforensics.com/. I also downloaded the drive I analyzed from the website https://downloads.digitalcorpora.org/corpora/scenarios/2009-m57-patents/drives-redacted/. The drive that I download was called Charlie-2009-11-12-0. I created a case and I opened to the drive to view what files it contained. Here it is below.



Here was another view of the user activity that occurred in this drive. Note that the last time the contents of this drive were used was in 11/12/2009 at 21:50:44. You are also able to do investigate different aspects of the drive such as Memory Viewer and System Information.



The next part of that lab is about Handling Windows Registry using Python. To do this you need to use the import **winreg** package in python then connect to the hive key of the users. The output will print the first 10 values that are available.

```
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
```

Here is the output for hive key users for my laptop.

```
In [1]: runfile('C:/Users/garci/Documents/Access Registry
0: .DEFAULT
1: S-1-5-19
2: S-1-5-20
3: S-1-5-21-3075618434-26661763-2445377827-1001
4: S-1-5-21-3075618434-26661763-2445377827-1001_Classes
5: S-1-5-18
```

We can also access the registry key and the values. You must use the **pytz** package and import the **datetime** and the **timedelta** as well. This will print the first 500 keys values. It will convert the time filed to an where it is readable.

```
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)
```

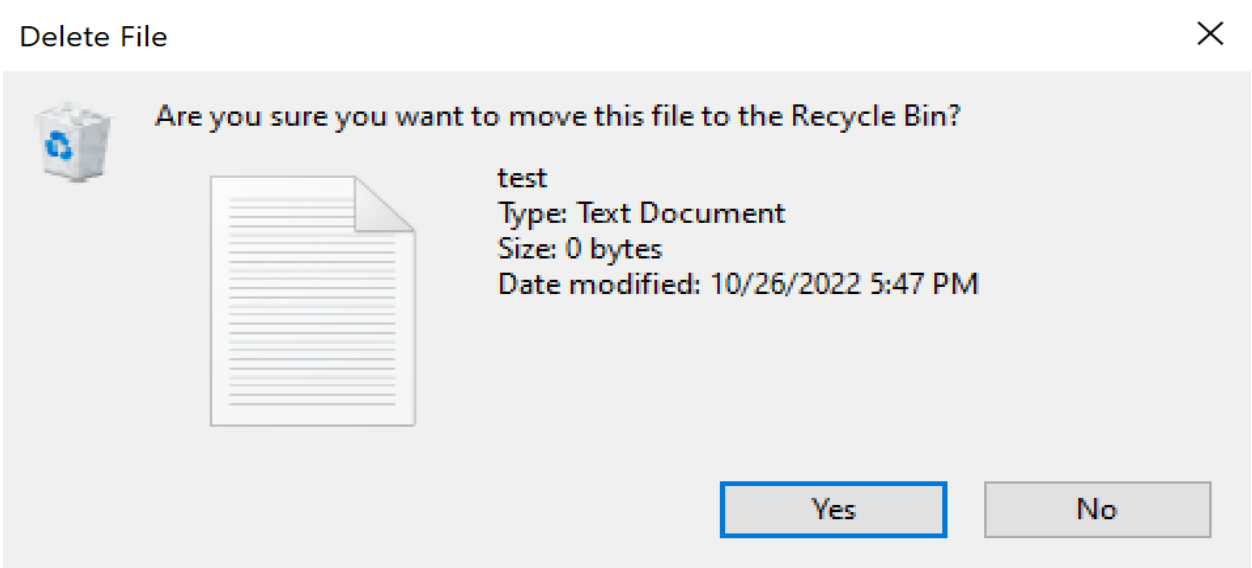
Here below is the output. Note the time of date these keys from the Microsoft software where updated.

```
15.0 : 2022-08-30 16:23:19.378267-05:00
16.0 : 2022-08-30 16:23:19.588561-05:00
ClickToRun : 2022-08-30 16:23:19.588561-05:00
Common : 2022-09-08 18:22:06.416656-05:00
DmsClient : 2022-08-30 16:23:19.596724-05:00
Excel : 2022-08-30 16:23:19.597268-05:00
Outlook : 2022-08-30 16:23:19.597802-05:00
PowerPoint : 2022-08-30 16:23:19.598343-05:00
Teams : 2022-08-30 16:23:19.598846-05:00
Word : 2022-08-30 16:23:19.600272-05:00
```

The next part the lab involved Handling Windows Recycle Bin using Python. To this this, you need to import the **winshell** and the **re** package. First it will read the list items in the recycle bin. Then I will delete and display the files names with the date. This will also retrieve the SID of the user who deleted the file. This so that you can investigate the user who deleted the file.

```python
import winshell
import re

r = list(winshell.recycle_bin())

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\garci\Desktop\test.txt'
with open(path, 'w') as file:
    file.write('This is a test file')


    winshell.delete_file(path)

    winshell.undelete(path)

```

Here is the file below where the python code opens the test file and delete it.



Here below are the file for the contents of my Recycle folder.

```
In [2]: runfile('C:/Users/garci/Documents/Handling Windows Recycle
Bin.py', wdir='C:/Users/garci/Documents')
C:\Users\garci\Desktop\Chrome\ChromeHistoryView.cfg 2022-10-20
21:41:41+00:00
C:\Users\garci\Desktop\step7(2) 2022-09-29 21:21:07+00:00
C:\Users\garci\AppData\Local\Temp\MicrosoftEdgeDownloads
\3c27b06d-8c6a-44db-8996-7bfbdaf12b3b\RamCapturer   2022-10-07
01:14:29+00:00
C:\Users\garci\Desktop\Done - Assignment 3 (Vision and Scope Statement)
2022-10-06 20:57:01+00:00
S-1-5-21-3075618434-26661763-2445377827-1001
```

The last Part of the lab was about Reading Browser History, Cookies, and Cache using Python. You need to import the **os** and the **sqlite3** packages to do this. You also need to set path the desired folder where you can read the contents of the browser. Also look for the profile file name so that you can read the contents of that file. Also, for every element that I printed in results, I displayed the number of times it had occurred.

```python
import os
import sqlite3

path = r'C:\Users\garci\AppData\Roaming\Mozilla\Firefox\Profiles\w6umvydy.default-release'

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()
print(results)

for element in results:
    print(element )

statement = 'SELECT url, visit_count FROM moz_places;'
history_cursor.execute(statement)
results = history_cursor.fetchall()
print(results)

for element in results:
    print(element)
```

Here below are the contents of that file that in the Profiles folder of Mozilla. You can see the cookies, permissions and keys3, etc.

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

Here below is also the websites that I visited using Mozilla Firefox. Note that is also displays the number time that I visited a website. So, there are some sites that I accessed yet I did not when to that website directly.

```
(15, 'origin_id', 'INTEGER', 0, None, 0)
[('https://www.mozilla.org/privacy/firefox/', 1),
('https://support.mozilla.org/products/firefox', 0),
('https://support.mozilla.org/kb/customize-firefox-
controls-buttons-and-toolbars?utm_source=firefox-
browser&utm_medium=default-
bookmarks&utm_campaign=customize', 0), ('https://
www.mozilla.org/contribute/', 0), ('https://
www.mozilla.org/about/', 0), ('https://
www.mozilla.org/en-US/privacy/firefox/', 1),
('https://www.mozilla.org/firefox/central/', 0),
('https://www.google.com/search?client=firefox-b-1-
d&q=g', 1), ('http://google.com/', 1), ('https://
google.com/', 1), ('https://www.google.com/', 1),
```