



LEARN TO FORENSICATE

LAB3-R01

CONTENTS

Lab #0: Connecting to your Lab System.....	2
Incident Background	3
Lab #1 - Malware Triage	4
Lab #2.1 - File Analysis	8
Lab #2.2 - User Login Analysis.....	11
Lab #2.3 - File/Folder INTERACTION Analysis.....	16
Lab #2.4 - Program Execution Analysis.....	19
Lab #2.5 - Internet History Analysis.....	22
Lab #2.6 - Timeline Generation	25
Lab #3.1 Domain Controller Analysis	27

LAB #0: CONNECTING TO YOUR LAB SYSTEM

- **Step 1:** Go to *portal.azure.com* in your browser.
- **Step 2:** Use the given credentials to login to Microsoft Azure. You may choose to skip MFA set up and the tour.
- **Step 3:** After logging into Microsoft Azure, search for “DevTest Labs” and then click on *Lab3_R01*.
- **Step 4:** Go to “Claimable Virtual Machines”; Then click on the three dots (“...”) at the end of the row of a virtual machine and click on “Claim VM”.
- **Step 5:** Click on your claimed VM and then click on *Connect*. This will download an RDP file to your system.
- **Step 6:** Double click on this file. When the password prompt is issued, please type in “Forensicate@RSA2024!” to connect to your system.
- **Step 7:** Please wait for a minute or two until Windows sets up for the first time.
- **Step 8:** Once you see the Desktop, you should be all set up.

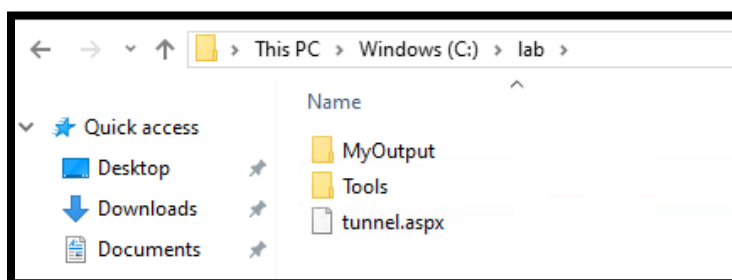
INCIDENT BACKGROUND

- On March 13, 2024, PA CB Industries set up a new network to manage their HR, Payroll and Intellectual Property related data.
- On March 19, their IT administrator detected suspicious activity in this network.
 - Specifically, a desktop wallpaper where a threat actor group is claiming ransom for stolen files.
- The IT administrator attempted to collect digital evidence and has identified a suspicious file on PA CB's File Server ("WEF").
- PA CB Industries has engaged you to perform an investigation into the cyber incident.



LAB #1 - MALWARE TRIAGE

Goal: To determine if the file “tunnel.aspx” provided by the IT administrator is malicious

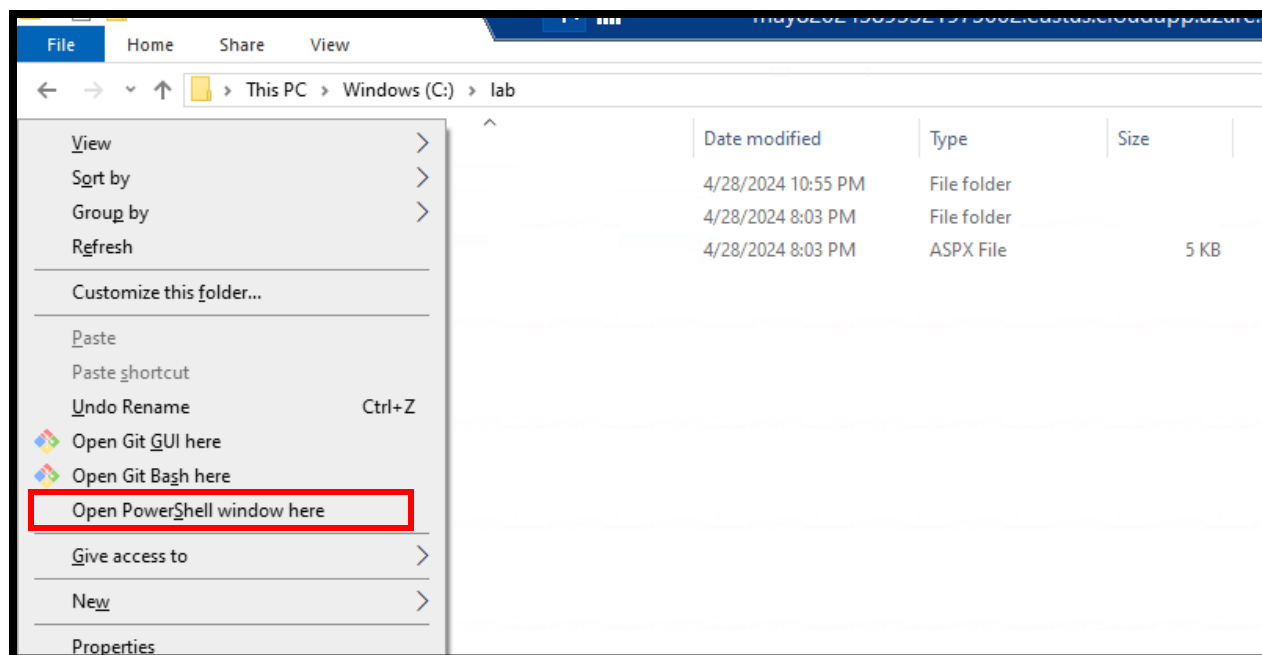


Question 1.1: What is the SHA-256 hash value of this file?

Hash value is a unique identifier generated by running a file through a hash function, akin to a digital fingerprint. There are multiple hashing algorithms such as MD5, SHA-1, SHA-256 etc. Hash values can be used to identify known malware and expedite incident response by quickly identifying suspicious files.

In this case, we want to calculate the hash value of the malware using the SHA-256 algorithm. To do this we can utilize Windows PowerShell.

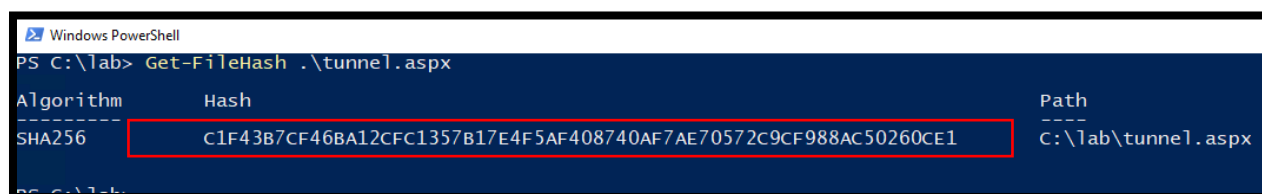
Navigate to C:\Lab using File Explorer, then press **Shift+F10**. This results in the following options. Please click on **Open PowerShell window here**. This opens PowerShell in the folder you are currently in.



Once you have the PowerShell window open, we will utilize a PowerShell cmdlet (pronounced “command-let”) called “Get-FileHash”. To get the SHA-256 hash value of this file, execute the following command in Windows PowerShell.

```
Get-FileHash tunnel.aspx
```

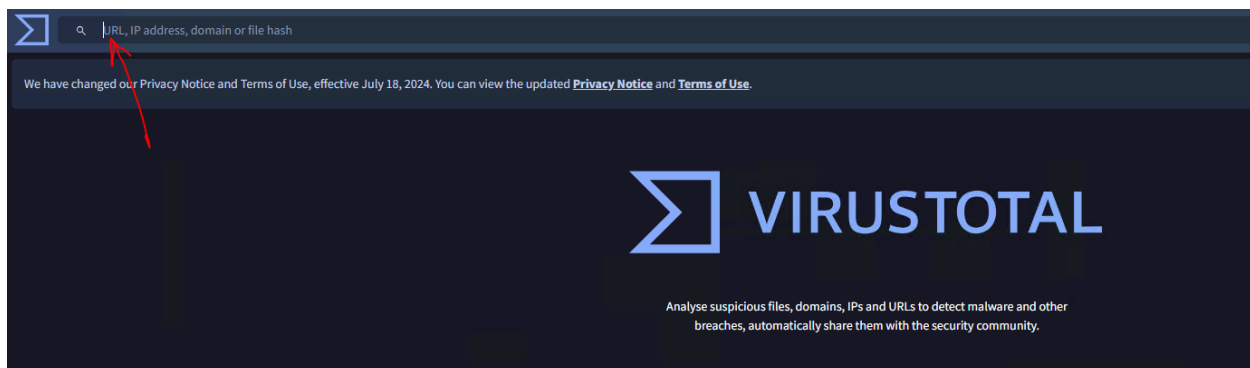
Now, you can highlight the hash value within PowerShell and right click to copy it.



Question 1.2: Is this a malicious file?

To answer this question, we will use open-source intelligence (OSINT) tools like VirusTotal. VirusTotal is a free online service that analyzes files and URLs for potential malware or malicious activities by scanning them with multiple antivirus engines and other security tools.

Go to www.virustotal.com in your browser and paste the hash value you recovered from the previous step.



Upon submitting the hash value, you can immediately see the results for this file. 32 anti-virus engines have flagged this file as malicious. **As a result, this file is likely malicious.**

32 / 61
Community Score

32/61 security vendors and no sandboxes flagged this file as malicious

Reanalyze Similar More

c1f43b7cf46ba12cf1357b17e4f5af408740af7ae70572c9cf988ac50260ce1
tunnel.aspx
Size: 4.84 KB
Last Modification Date: 2 days ago
TXT

DETECTION DETAILS RELATIONS TELEMETRY COMMUNITY 8

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label: hacktool.regeorg/aspix Threat categories: hacktool trojan Family labels: regeorg aspx hktl

Security vendors' analysis

Vendor	Detection	Vendor	Detection
AhnLab-V3	HackTool/ASP.ReGeorg.S1477	ALYac	Misc.HackTool.ASP.ReGeorg
Antiy-AVL	Trojan/APT/ASP.Volatilecedar	Arcabit	Application.Hacktool.ReGeorg.A
Avast	Other:Malware-gen [Trj]	AVG	Other:Malware-gen [Trj]
BitDefender	Application.Hacktool.ReGeorg.A	Bkav Pro	W32.Common.7F702946
DrWeb	PowerShell.Proxifier.3	Emsisoft	Application.Hacktool.ReGeorg.A (B)

Bonus question: What are the capabilities of this file?

To answer this question, we need to understand two main things:

- What malware family does this file belong to?
- What is this malware capable of?

Reviewing the “popular threat label” in Virustotal, it appears that the file has signatures associated with **ReGeorg webshell**.

If you have time, google “WebShell” and “ReGeorg” to understand how this malware is used by threat actors.

LAB #2.1 - FILE ANALYSIS

Goal: To determine when the malware was created on the File server

Question: When was the malware (tunnel.aspx) created on disk?

To determine timestamps of when files were created on a Windows system, forensic examiners typically rely on a forensic artifact called “MFT”. The Master File Table (MFT) is a crucial part of the NTFS file system used by Windows. It serves as a database that stores information about all files and directories on a disk partition, including their attributes, permissions, timestamps and data location. To learn more about the MFT, you can visit Microsoft’s documentation using [this link](#).

Note: our MFT file is in a zip called \$MFT.zip – be sure to unzip this to the current directory by *right-clicking on the file -> 7-Zip -> Extract here*.

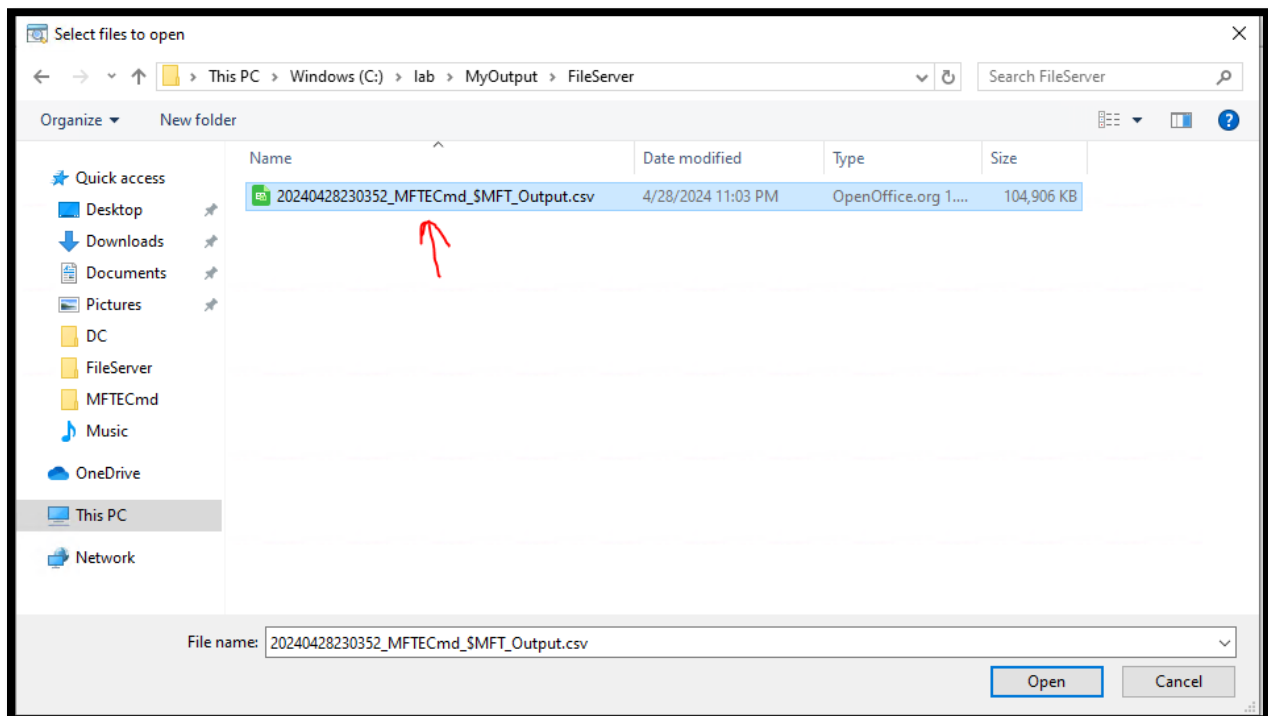
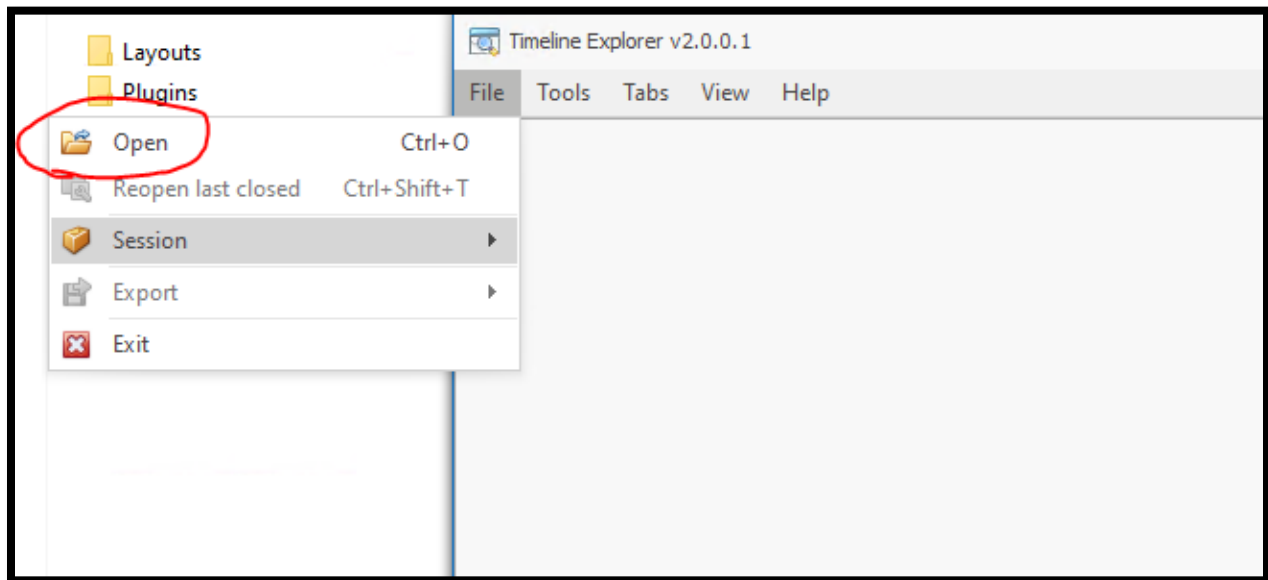
To parse this artifact, we will rely on a tool called MFTECmd.

To execute MFTECmd, execute the following command:

```
&'C:\lab\Tools\MFTECmd\MFTECmd.exe' -f  
'C:\lab\Tools\MFTECmd\FileServer\$MFT' --csv  
C:\Lab\MyOutput\FileServer
```

The output of this tool can be found under C:\Lab\MyOutput\FileServer. We will utilize a tool called TimelineExplorer located in C:\Lab\Tools\TimelineExplorer.

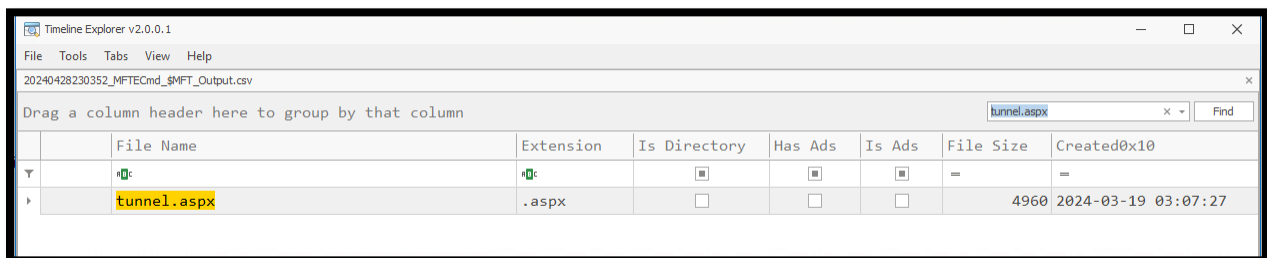
Double-click on TimelineExplorer.exe. Then, go to File>Open>Choose the output file and click on “Open”.



Give it a few seconds to load the file. Once the file is loaded, on the top-right type “**tunnel.aspx**” and click on “Find”.



Give it a few seconds for the program to file the relevant entry. After a few seconds, you should see a match. Scroll to the right to find a column named “Created0x10”. This column contains the creation timestamp of the file in UTC.



It appears that the file was created on **March 19, 2024 at 03:07:27 UTC**.

NOTE: Do not close Timeline Explorer. We will use in upcoming labs.

LAB #2.2 - USER LOGIN ANALYSIS

Goal: To determine the user that created the malware

Question: Who was logged in at the time of file creation of the malware?

Now that we know when the malware was created on the File Server, we want to understand which user created the file. Additionally, we would also want to determine the time of login and the logoff for this user. Evidence of user logins or logoffs can be found in Windows Event Logs.

Windows Event Logs or EVTX files are a built-in feature of the Windows operating system that records important system and application events. They are categorized into different event logs, such as System, Security, and Application, each capturing specific types of events using unique Event IDs. System administrators and security professionals use event logs to troubleshoot issues, monitor system health, and detect security incidents. Windows Event Logs are in the path *C:\Windows\System32\winevt\Logs* on every modern Windows system.

Typically, there are dozens of Windows Event Logs recording many activities on the device. For this lab, we have provided just one – “Microsoft-Windows-TerminalServices-LocalSessionManager%4Operational.evtx”. This log records user logins that utilize the Remote Desktop Protocol (“RDP”). Windows RDP is

used by users to connect to systems remotely - just like you are connecting to your lab system remotely from your laptop.

As described above, every EVTX file records many types of events using a distinct Event ID. For example, in our example, Microsoft-Windows-TerminalServices-LocalSessionManager%4Operational.evtx contains many event IDs such as 21, 23, 24 and 25. The following table may help in better understanding this.

<i>Evtx File Name</i>	Event ID	Description
<i>Microsoft-Windows-TerminalServices-LocalSessionManager%4Operational.evtx</i>	21	Remote Desktop Services: Session logon succeeded
	23	Remote Desktop Services: Session logoff succeeded
	24	Remote Desktop Services: Session has been disconnected
	25	Remote Desktop Services: Session reconnection succeeded

To parse this EVTX file, we will utilize a tool called EvtxECmd. To execute EvtxECmd, execute the following command:

```
&'C:\lab\Tools\EvtxECmd\EvtxECmd.exe' -f
'C:\lab\Tools\EvtxECmd\FileServer\Microsoft-Windows-TerminalServices-
LocalSessionManager%4Operational.evtx' --csv
C:\Lab\MyOutput\Fileserver
```

The output of this tool can be found under C:\Lab\MyOutput\FileServer. We will use TimelineExplorer to open this file. Follow steps mentioned in Lab 2.1 to open the EvtxECmd output file.

Now, let us try and determine which user created the tunnel.aspx malware. From our previous lab the file was created on **March 19, 2024, at 03:07:27 UTC**.

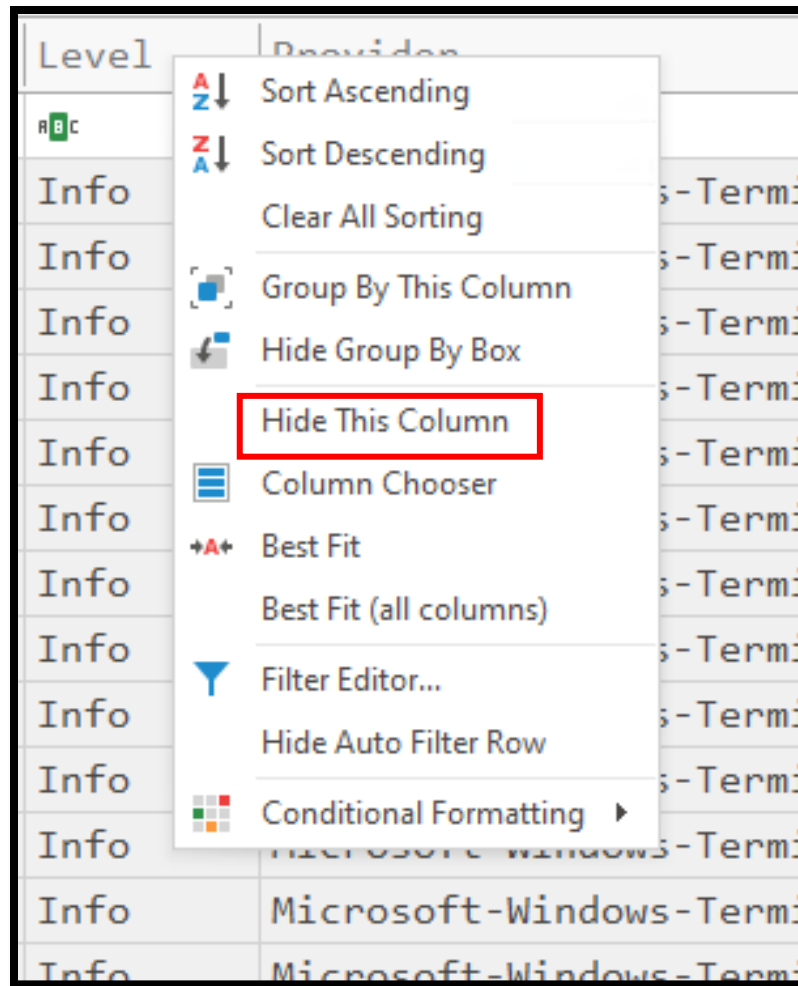
The first step is to filter on events on March 19, 2024. We can do that by entering the date in the “Time Created” column.

Drag a column header here to group by that column

	Line	Tag	Record Number	Event Record Id	Time Created	Event Id	Level
▼	=	<input type="checkbox"/>	=	=	= 2024-03-19 00:00:00	=	<input type="checkbox"/>
	94	<input type="checkbox"/>	174	174	2024-03-19 00:12:01	23	Info
▶	95	<input type="checkbox"/>	175	175	2024-03-19 00:12:02	54	Info
	96	<input type="checkbox"/>	176	176	2024-03-19 00:12:14	32	Info
	97	<input type="checkbox"/>	177	177	2024-03-19 00:12:23	41	Info
	98	<input type="checkbox"/>	178	178	2024-03-19 00:12:23	42	Info
	99	<input type="checkbox"/>	179	179	2024-03-19 00:12:23	21	Info
	100	<input type="checkbox"/>	180	180	2024-03-19 00:12:23	22	Info
	101	<input type="checkbox"/>	181	181	2024-03-19 00:12:53	23	Info
	102	<input type="checkbox"/>	182	182	2024-03-19 00:12:53	39	Info
	103	<input type="checkbox"/>	183	183	2024-03-19 00:12:53	59	Info
	104	<input type="checkbox"/>	184	184	2024-03-19 00:12:53	40	Info
	105	<input type="checkbox"/>	185	185	2024-03-19 00:12:53	24	Info
	106	<input type="checkbox"/>	186	186	2024-03-19 00:13:17	41	Info
	107	<input type="checkbox"/>	187	187	2024-03-19 00:13:17	42	Info
	108	<input type="checkbox"/>	188	188	2024-03-19 00:13:17	21	Info
	109	<input type="checkbox"/>	189	189	2024-03-19 00:13:18	22	Info
	110	<input type="checkbox"/>	190	190	2024-03-19 02:34:54	41	Info
	111	<input type="checkbox"/>	191	191	2024-03-19 02:34:54	42	Info
	112	<input type="checkbox"/>	192	192	2024-03-19 02:34:55	21	Info
	113	<input type="checkbox"/>	193	193	2024-03-19 02:34:55	22	Info
	114	<input type="checkbox"/>	194	194	2024-03-19 03:23:49	39	Info
	115	<input type="checkbox"/>	195	195	2024-03-19 03:23:49	59	Info
	116	<input type="checkbox"/>	196	196	2024-03-19 03:23:49	40	Info

This gets us events from March 19, 2024. Now let us sort the Time Created column in ascending order. You can do this by clicking on the Time Created column.

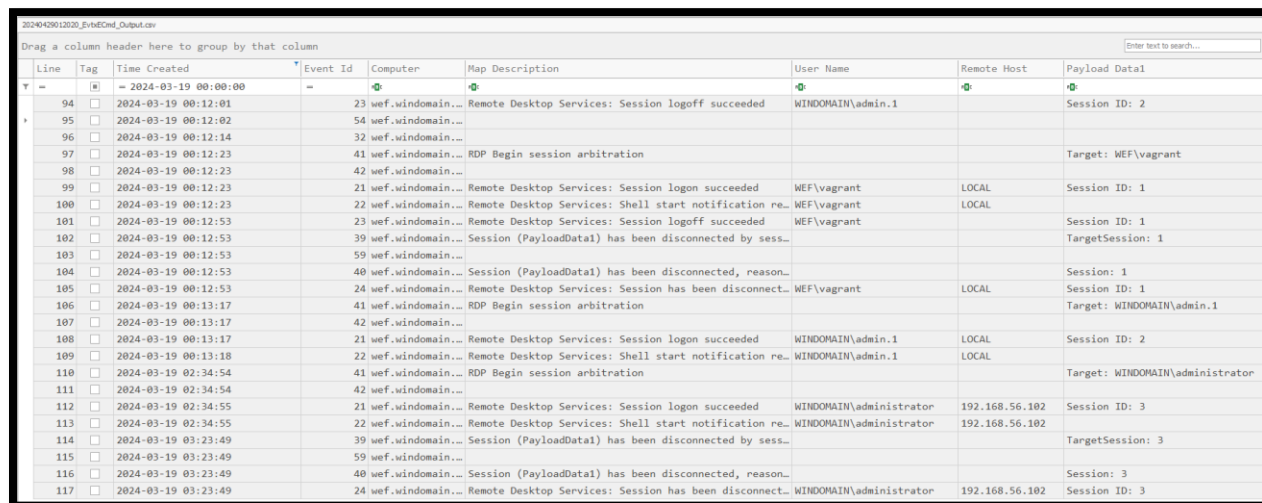
We will now try and hide unnecessary columns. You can right click on a column and choose Hide This Column.



We'll go ahead and hide the following columns:

1. Record Number
2. Event Record Id
3. Level
4. Provider
5. Channel
6. Process Id
7. User Id

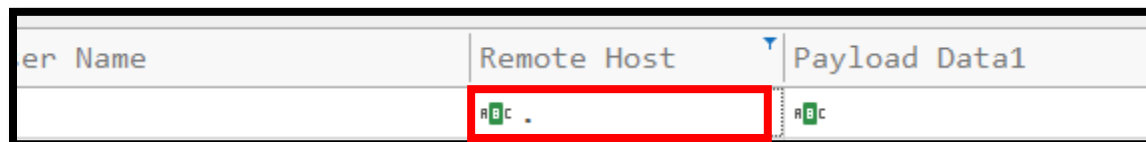
This should result in something like this:



Line	Tag	Time Created	Event Id	Computer	Map Description	User Name	Remote Host	Payload Data1
94		2024-03-19 00:12:01	23	wef.windomain...	Remote Desktop Services: Session logoff succeeded	WINDOMAIN\admin.1		Session ID: 2
95		2024-03-19 00:12:02	54	wef.windomain...				
96		2024-03-19 00:12:14	32	wef.windomain...				
97		2024-03-19 00:12:23	41	wef.windomain...	RDP Begin session arbitration			Target: WEF\vagrant
98		2024-03-19 00:12:23	42	wef.windomain...				
99		2024-03-19 00:12:23	21	wef.windomain...	Remote Desktop Services: Session logon succeeded	WEF\vagrant	LOCAL	Session ID: 1
100		2024-03-19 00:12:23	22	wef.windomain...	Remote Desktop Services: Shell start notification re...	WEF\vagrant	LOCAL	
101		2024-03-19 00:12:53	23	wef.windomain...	Remote Desktop Services: Session logoff succeeded	WEF\vagrant		Session ID: 1
102		2024-03-19 00:12:53	39	wef.windomain...	Session (PayloadData1) has been disconnected by sess...			TargetSession: 1
103		2024-03-19 00:12:53	59	wef.windomain...				
104		2024-03-19 00:12:53	40	wef.windomain...	Session (PayloadData1) has been disconnected, reason...			Session: 1
105		2024-03-19 00:12:53	24	wef.windomain...	Remote Desktop Services: Session has been disconnect...	WEF\vagrant	LOCAL	Session ID: 1
106		2024-03-19 00:13:17	41	wef.windomain...	RDP Begin session arbitration			Target: WINDOMAIN\admin.1
107		2024-03-19 00:13:17	42	wef.windomain...				
108		2024-03-19 00:13:17	21	wef.windomain...	Remote Desktop Services: Session logon succeeded	WINDOMAIN\admin.1	LOCAL	Session ID: 2
109		2024-03-19 00:13:18	22	wef.windomain...	Remote Desktop Services: Shell start notification re...	WINDOMAIN\admin.1	LOCAL	
110		2024-03-19 02:34:54	41	wef.windomain...	RDP Begin session arbitration			Target: WINDOMAIN\administrator
111		2024-03-19 02:34:54	42	wef.windomain...				
112		2024-03-19 02:34:55	21	wef.windomain...	Remote Desktop Services: Session logon succeeded	WINDOMAIN\administrator	192.168.56.102	Session ID: 3
113		2024-03-19 02:34:55	22	wef.windomain...	Remote Desktop Services: Shell start notification re...	WINDOMAIN\administrator	192.168.56.102	
114		2024-03-19 03:23:49	39	wef.windomain...	Session (PayloadData1) has been disconnected by sess...			TargetSession: 3
115		2024-03-19 03:23:49	59	wef.windomain...				
116		2024-03-19 03:23:49	40	wef.windomain...	Session (PayloadData1) has been disconnected, reason...			Session: 3
117		2024-03-19 03:23:49	24	wef.windomain...	Remote Desktop Services: Session has been disconnect...	WINDOMAIN\administrator	192.168.56.102	Session ID: 3

Now, we want to exclude all LOCAL logins and just focus on remote logins.

Remote logins have an IP address filled out in the **Remote Host** column. So, we can apply another filter where Remote Host contains an IP address. We can do this by clicking right below the “Remote Host” column and typing in a period (“.”) like so:



User Name	Remote Host	Payload Data1
	Remote Host contains .	

The remaining results indicate that the only user who remotely logged in during our timeframe is the **administrator** account where the login and log off times are as below:

2024-03-19 02:34:55 - WINDOMAIN\administrator logon succeeded

2024-03-19 03:23:49 - WINDOMAIN\administrator session disconnected

LAB #2.3 - FILE/FOLDER INTERACTION ANALYSIS

Goal: To determine file/folder interaction activity from the administrator account between 02:34 and 03:23 on March 19

Question: What files/folders did the threat actor interact with?

To recap, we know that on March 19:

- 1. At 2:34, the threat actor utilized the administrator account to login to the file server.**
- 2. At 3:07, they drop the “tunnel.aspx” malware on the file server.**
- 3. At 3:23, their login session is disconnected.**

We need to determine if there were additional actions taken by the threat actor between 2:34 and 3:23 on the file server.

Typically, forensic examiners focus on file/folder interaction when trying to determine threat actor actions on a system. While there are many forensic artifacts that provide insight into file/folder interactions, in this lab, we will focus on just one such artifact – Jump Lists.

Jump Lists are a feature in Windows that stores recently accessed files and frequently used tasks for specific applications, accessible via the taskbar or Start menu. In forensics, Jump Lists can provide valuable insights into user activities,

such as frequently accessed files and executed commands, aiding in investigations by reconstructing user actions and identifying relevant evidence.

To simplify analysis, we have provided the Jump Lists only for the administrator user. To parse this artifact, we will utilize a tool called JLECmd.

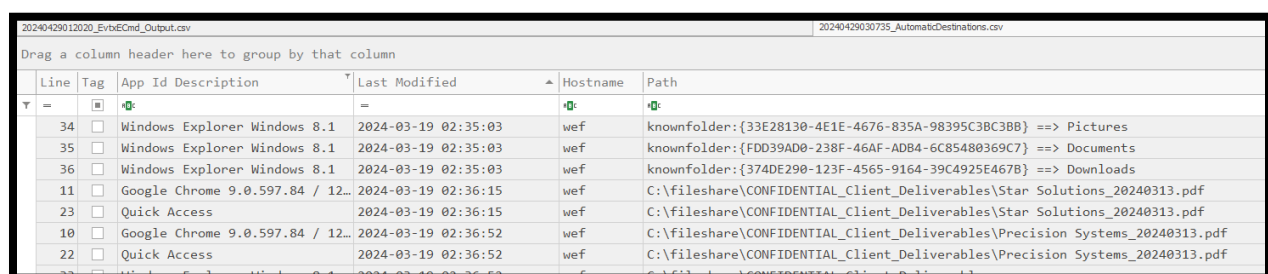
Using Windows PowerShell, please execute the following command:

```
&'C:\lab\Tools\JLECmd\JLECmd.exe' -d 'C:\lab\Tools\JLECmd\FileServer'
--csv C:\Lab\MyOutput\Fileserver
```

Open the output in Timeline Explorer and hide the following columns:

- Source File
- Source Created
- Source Modified
- Source Accessed
- App Id
- Has Sps
- Pin Status
- Dest List Version
- Last Used Entry Number
- Entry Number
- MRU
- Creation Time
- Interaction Count
- Mac Address

The resulting view should look something like this:



Line	Tag	App Id	Description	Last Modified	Hostname	Path
34	<input type="checkbox"/>	Windows Explorer	Windows 8.1	2024-03-19 02:35:03	wef	knownfolder:{33E28130-4E1E-4676-835A-98395C3BC3B8} ==> Pictures
35	<input type="checkbox"/>	Windows Explorer	Windows 8.1	2024-03-19 02:35:03	wef	knownfolder:{FDD39AD0-238F-46AF-ADB4-6C85480369C7} ==> Documents
36	<input type="checkbox"/>	Windows Explorer	Windows 8.1	2024-03-19 02:35:03	wef	knownfolder:{374DE290-123F-4565-9164-39C4925E467B} ==> Downloads
11	<input type="checkbox"/>	Google Chrome 9.0.597.84 / 12...		2024-03-19 02:36:15	wef	C:\fileshare\CONFIDENTIAL_Client_Deliverables\Star Solutions_20240313.pdf
23	<input type="checkbox"/>	Quick Access		2024-03-19 02:36:15	wef	C:\fileshare\CONFIDENTIAL_Client_Deliverables\Star Solutions_20240313.pdf
10	<input type="checkbox"/>	Google Chrome 9.0.597.84 / 12...		2024-03-19 02:36:52	wef	C:\fileshare\CONFIDENTIAL_Client_Deliverables\Precision Systems_20240313.pdf
22	<input type="checkbox"/>	Quick Access		2024-03-19 02:36:52	wef	C:\fileshare\CONFIDENTIAL_Client_Deliverables\Precision Systems_20240313.pdf

We will utilize the “**Last Modified**” timestamp as the timestamp of the file/folder interaction. Reviewing the output, it appears that the threat actors have browsed through several sensitive files and folders using Google Chrome and File Explorer including but not limited to:

- **C:\fileshare\CONFIDENTIAL_Client_Deliverables**
- **C:\fileshare\Taxes**
- **C:\fileshare\Payroll**
- **C:\fileshare\Design_documents**

LAB #2.4 - PROGRAM EXECUTION ANALYSIS

Goal: To determine program execution activity from the administrator account between 02:34 and 03:23 on March 19

Question: What programs did the threat actor execute on the file server?

In addition to determining file/folder interactions, forensic examiners supplement their analysis by reviewing the different programs executed by the threat actor. While there are many forensic artifacts that track program execution, in this lab we will utilize a forensic artifact called User Assist.

User Assist is a Windows feature that keeps track of user activity by recording the execution of programs and the frequency of program usage. It stores this information in the user registry hive ("NTUSER.DAT") under "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist".

In DFIR, User Assist is crucial for reconstructing user behavior, identifying commonly used programs, and understanding user interactions with the system. Analysts can leverage User Assist data to establish timelines of activity, detect suspicious behavior, and uncover potential evidence relevant to an investigation.

To simplify analysis, we have provided the user registry hive (“NTUSER.DAT”) for only the administrator user. To parse this artifact, we will utilize a tool called ReCmd.

In PowerShell, execute the following command:

```
&'C:\lab\Tools\ReCmd\ReCmd.exe' -f  
'C:\lab\Tools\ReCmd\FileServer\NTUSER.DAT' --bn  
'C:\lab\Tools\ReCmd\BatchExamples\BatchExampleUserAssist.reb' --csv  
C:\Lab\MyOutput\Fileserver
```

The output should be located under *C:\Lab\MyOutput\Fileserver*. We will utilize Timeline Explorer to open this file.

We will need to hide the following unnecessary columns to make our analysis easier:

- Hive Path
- Hive Type
- Description
- Category
- Key Path
- Value Name
- Value Type

This should result in a view like below:

Line	Tag	Value Data2	Value Data
1	<input type="checkbox"/>	Last executed:	UEME_CTLCUACount:ctor
2	<input type="checkbox"/>	Last executed: 2024-03-19 02:33:15.3865112	{System32}\SnippingTool.exe
3	<input type="checkbox"/>	Last executed:	UEME_CTLSESSION
4	<input type="checkbox"/>	Last executed: 2024-03-19 03:07:56.8450000	{System32}\mspaint.exe
5	<input type="checkbox"/>	Last executed: 2024-03-19 03:13:51.8660000	{System32}\notepad.exe
6	<input type="checkbox"/>	Last executed: 2024-03-19 03:03:09.6340000	Microsoft.Windows.Explorer
7	<input type="checkbox"/>	Last executed:	{Program Files}\Notepad++\notepad++.exe
8	<input type="checkbox"/>	Last executed: 2024-03-19 02:39:21.8480000	{Program Files x86}\Google\Chrome\Application\chrome.exe
9	<input type="checkbox"/>	Last executed: 2024-03-19 03:00:27.9980000	Chrome

To see only entries of programs recently executed, filter on the “Value Data2” column by entering “2024” like below:

Line	Tag	Value Data2	Value Data
	<input checked="" type="checkbox"/>	2024	
2	<input type="checkbox"/>	Last executed: 2024-03-19 02:33:15.3865112	{System32}\SnippingTool.exe
20	<input type="checkbox"/>	Last executed: 2024-03-19 02:33:15.3865112	{Common Programs}\Accessories\Snipping Tool.lnk
36	<input type="checkbox"/>	Last executed: 2024-03-19 02:33:15.3865112	{System32}\SnippingTool.exe
56	<input type="checkbox"/>	Last executed: 2024-03-19 02:33:15.3865112	{Common Programs}\Accessories\Snipping Tool.lnk
8	<input type="checkbox"/>	Last executed: 2024-03-19 02:39:21.8480000	{Program Files x86}\Google\Chrome\Application\chrome.exe
42	<input type="checkbox"/>	Last executed: 2024-03-19 02:39:21.8480000	{Program Files x86}\Google\Chrome\Application\chrome.exe
12	<input type="checkbox"/>	Last executed: 2024-03-19 02:41:40.4210000	C:\Users\administrator\Downloads\7z2401-x64.exe
46	<input type="checkbox"/>	Last executed: 2024-03-19 02:41:40.4210000	C:\Users\administrator\Downloads\7z2401-x64.exe
14	<input type="checkbox"/>	Last executed: 2024-03-19 02:59:51.2670000	{System32}\win32calc.exe
26	<input type="checkbox"/>	Last executed: 2024-03-19 02:59:51.2670000	{Common Programs}\Accessories\Calculator.lnk
48	<input type="checkbox"/>	Last executed: 2024-03-19 02:59:51.2670000	{System32}\win32calc.exe
62	<input type="checkbox"/>	Last executed: 2024-03-19 02:59:51.2670000	{Common Programs}\Accessories\Calculator.lnk
9	<input type="checkbox"/>	Last executed: 2024-03-19 03:00:27.9980000	Chrome
25	<input type="checkbox"/>	Last executed: 2024-03-19 03:00:27.9980000	{User Pinned}\TaskBar\Google Chrome.lnk
43	<input type="checkbox"/>	Last executed: 2024-03-19 03:00:27.9980000	Chrome
61	<input type="checkbox"/>	Last executed: 2024-03-19 03:00:27.9980000	{User Pinned}\TaskBar\Google Chrome.lnk
6	<input type="checkbox"/>	Last executed: 2024-03-19 03:03:09.6340000	Microsoft.Windows.Explorer
24	<input type="checkbox"/>	Last executed: 2024-03-19 03:03:09.6340000	{User Pinned}\TaskBar\File Explorer.lnk
40	<input type="checkbox"/>	Last executed: 2024-03-19 03:03:09.6340000	Microsoft.Windows.Explorer
60	<input type="checkbox"/>	Last executed: 2024-03-19 03:03:09.6340000	{User Pinned}\TaskBar\File Explorer.lnk
4	<input type="checkbox"/>	Last executed: 2024-03-19 03:07:56.8450000	{System32}\mspaint.exe

You can click on the “Value Data2” column to get the timestamps in ascending order. By reviewing the output, we can determine that the threat actor executed a variety of programs including:

- **Google Chrome Browser**
- **7-zip compression utility**
- **Calculator**
- **Windows File Explorer** Since the threat actor used Google Chrome, we should follow that thread by parsing internet history next.

LAB #2.5 - INTERNET HISTORY ANALYSIS

Goal: To determine internet history activity from the administrator account between 02:34 and 03:23 on March 19

Question: What websites did the threat actor visit on the file server?

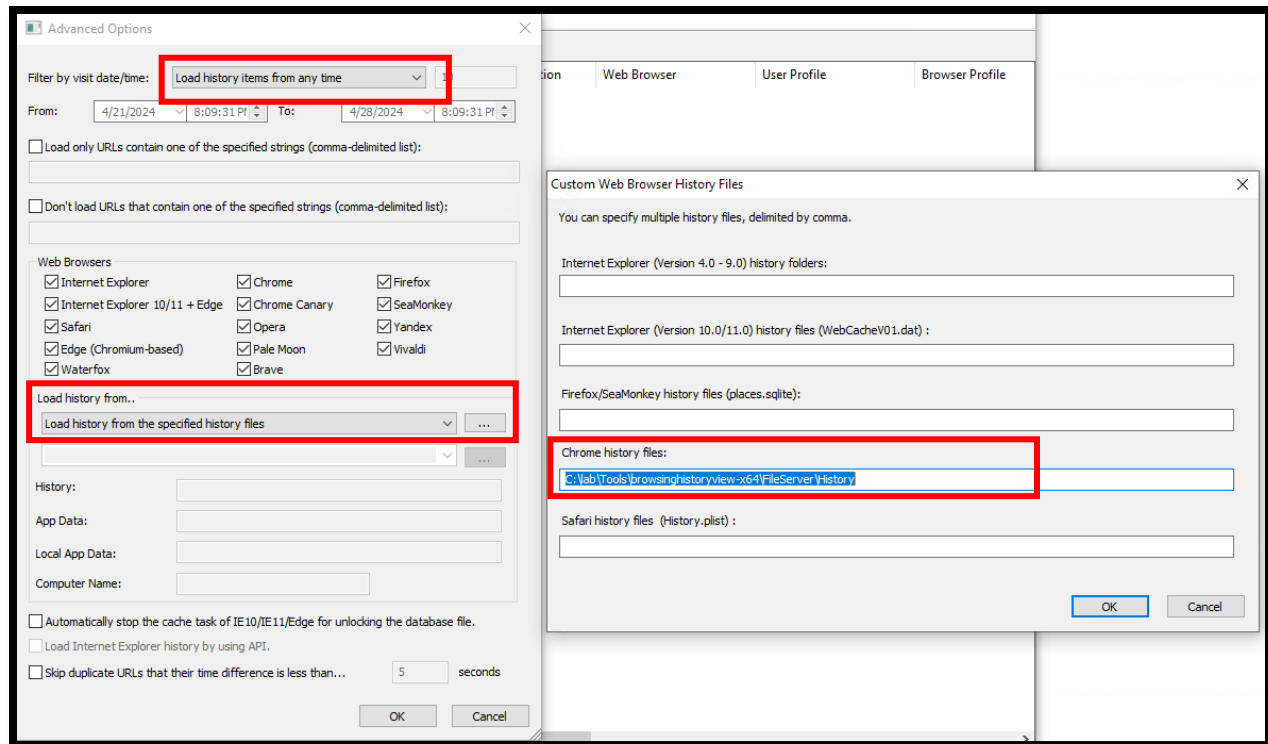
From our previous lab, we have determined that the threat actor utilized the Google Chrome Browser. In this lab, we will try to determine what websites the threat actors browsed to using Google Chrome.

Browsers like Google Chrome record the websites visited by a user. Depending on the browser, it may also store additional information such as how long a user spent on a particular website, autofill or form input information, cookies etc.

In this lab, we will focus only on the sites visited by the threat actor using the administrator account. To do this, we will utilize a freeware tool by NirSoft called BrowsingHistoryView.

Browse to *C:\Lab\Tools\browsinghistoryview-x64* and double click on *BrowsingHistoryView.exe*.

It will pop up with a window with several options. Please change the following fields as seen below:

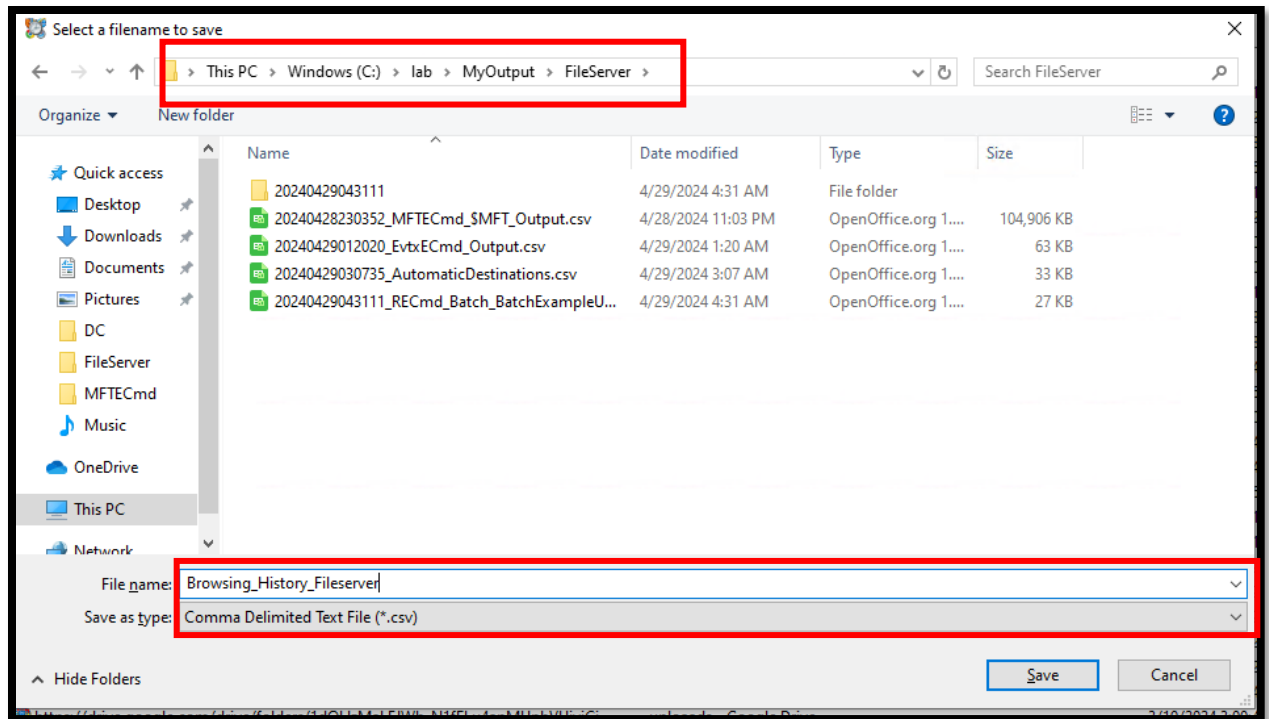


You should now see all the websites browsed to by the threat actor:

URL	Title	Visit Time	Visit Count	Visited From	Visit Type	Visit Duration	Web Browser
file:///C:/fileshare/Payroll/chris_j_2023-11-02.pdf	chris_j_2023-11-02.pdf	3/19/2024 2:38:12 AM	1		Auto TopLevel	00:01:27.039	Chrome
file:///C:/fileshare/Payroll/daniel_t_2023-09-24.pdf	daniel_t_2023-09-24.pdf	3/19/2024 2:38:21 AM	1		Auto TopLevel	00:01:16.709	Chrome
file:///C:/fileshare/Payroll/emily_b_2023-11-30.pdf	emily_b_2023-11-30.pdf	3/19/2024 2:38:33 AM	1		Auto TopLevel	00:01:04.159	Chrome
file:///C:/fileshare/Taxes/daniel_j_2024-03-13.pdf	daniel_j_2024-03-13.pdf	3/19/2024 2:38:54 AM	1		Auto TopLevel	00:00:41.554	Chrome
file:///C:/fileshare/Taxes/jane_j_2024-03-13.pdf	jane_j_2024-03-13.pdf	3/19/2024 2:39:10 AM	1		Auto TopLevel	00:00:23.295	Chrome
file:///C:/fileshare/Taxes/daniel_b_2024-03-13.pdf	daniel_b_2024-03-13.pdf	3/19/2024 2:39:22 AM	1		Auto TopLevel	00:00:10.161	Chrome
https://www.google.com/search?q=file+transfer+sites+temp&rlz=1C1GGER_enUS11...	file transfer sites temp - Google Search	3/19/2024 2:52:02 AM	5		Generated	00:00:00.659	Chrome
https://www.google.com/search?q=file+transfer+sites+temp&rlz=1C1GGER_enUS11...	file transfer sites temp - Google Search	3/19/2024 2:52:03 AM	5	https://www.google.co...	Link	00:00:15.999	Chrome
https://www.file.io/	file.io - Super simple file sharing	3/19/2024 2:52:19 AM	1	https://www.google.co...	Link	00:00:12.189	Chrome
https://www.google.com/search?q=file+transfer+sites+temp&rlz=1C1GGER_enUS11...	file transfer sites temp - Google Search	3/19/2024 2:52:36 AM	5		Generated	00:00:04.726	Chrome
https://temp-file-share.web.app/	TempFileShare - share disappearing files to anyone	3/19/2024 2:52:47 AM	1	https://www.google.co...	Link	00:00:11.184	Chrome
https://www.google.com/search?q=file+transfer+sites+temp&rlz=1C1GGER_enUS11...	file transfer sites temp - Google Search	3/19/2024 2:52:57 AM	5		Generated	00:00:09.757	Chrome
https://tmpfiles.org/	/tmp/files - Temporary File Upload	3/19/2024 2:52:57 AM	1	https://www.google.co...	Link	00:00:11.184	Chrome
https://www.google.com/search?q=file+transfer+sites+temp&rlz=1C1GGER_enUS11...	file transfer sites temp - Google Search	3/19/2024 2:53:01 AM	5		Generated	00:00:46.585	Chrome
https://www.google.com/search?q=design+documents&rlz=1C1GGER_enUS1102US1...	design documents - Google Search	3/19/2024 2:53:48 AM	2		Generated	00:00:00.886	Chrome
https://www.google.com/search?q=design+documents&rlz=1C1GGER_enUS1102US1...	design documents - Google Search	3/19/2024 2:53:48 AM	2	https://www.google.co...	Link	00:00:07.361	Chrome
https://www.google.com/search?q=design+documents&rlz=1C1GGER_enUS1102US1...	design documents - Google Search	3/19/2024 2:53:56 AM	1	https://www.google.co...	Link	00:00:19.498	Chrome

You can export these records into a CSV format by following the steps below:

1. Ctrl+A to select all the entries in the view.
2. Ctrl+S to save the records as a CSV.
3. Choose the output location as *C:\Lab\MyOutput\FileServer*, provide a file name and save as CSV as seen below:



Reviewing the output, you can see some Google searches conducted by the threat actor. However, the most important observation are the visits to the below file sharing sites:

1. **tempfiles.org**
2. **file.io**
3. **temp-file-share.web.app**
4. **drive.google.com** (We can see the folder named “uploadss”)

Threat actors typically visit file sharing sites to exfiltrate data from victims or download malware on to victim systems.

LAB #2.6 – TIMELINE GENERATION

From our previous labs, we have determined a lot of information. Now, we need to timeline everything so that we understand the order of events. For example: Did the threat actors visit file sharing sites towards the end of their login session or at the beginning? Did file/folder browsing activity happen before or after the visits to the file sharing sites? We need to get all the output from all our labs into a single, normalized CSV report that is ready for analysis.

Creating a normalized CSV is quite arduous when done manually. As a result, for this lab, we have developed a custom tool called CSV2Timeline. Its main job is to read CSVs of any format and convert it into a normalized CSV to make it easier for a human to review.

We've simplified this lab by collecting the output of Labs 2.1 through Lab 2.5 into a single folder located in: *C:\Lab\Tools\CSV2Timeline\Fileserver*.

To generate the timeline, open Windows PowerShell and execute the following commands:

<code>cd C:\lab\Tools\CSV2Timeline\</code>
<code>&'C:\lab\Tools\CSV2Timeline\CSV2Timeline.exe' -i 'C:\lab\Tools\CSV2Timeline\Fileserver' -o 'C:\lab\Tools\CSV2Timeline\FileServer' -s WEF</code>

This generates a timeline.csv file in *C:\lab\Tools\CSV2Timeline\FileServer*, containing a normalized timeline of all events from our tools' output files. Let's open this in Timeline Viewer and review the output.

To filter out the noise, let's just focus on activity from March 19, 2024 by applying a filter on the "Timestamp" column as seen below.

Click on the Timestamp column to arrange the records in Ascending order.

Drag a column header here to group by that column

Line	Tag	Timestamp	Source...	Message
26	<input type="checkbox"/>	03/19/2024 00:12:23	WEF	Remote Desktop Services: Session logon succeeded WEF\vagrant from LOCAL - Session ID: 1
27	<input type="checkbox"/>	03/19/2024 00:12:53	WEF	Remote Desktop Services: Session has been disconnected WEF\vagrant from LOCAL - Session ID: 1
28	<input type="checkbox"/>	03/19/2024 00:13:17	WEF	Remote Desktop Services: Session logon succeeded WINDOMAIN\admin.1 from LOCAL - Session ID: 2
29	<input type="checkbox"/>	03/19/2024 02:34:55	WEF	Remote Desktop Services: Session logon succeeded WINDOMAIN\administrator from 192.168.56.102 - Session ID: 3
64	<input type="checkbox"/>	03/19/2024 02:35:03	WEF	Opened knownfolder:{33E28130-4E1E-4676-835A-98395C3BC3BB} ==> Pictures
65	<input type="checkbox"/>	03/19/2024 02:35:03	WEF	Opened knownfolder:{FDD39AD0-238F-46AF-ADB4-6C85480369C7} ==> Documents
66	<input type="checkbox"/>	03/19/2024 02:35:03	WEF	Opened knownfolder:{374DE290-123F-4565-9164-39C4925E467B} ==> Downloads
41	<input type="checkbox"/>	03/19/2024 02:36:15	WEF	Opened C:\fileshare\CONFIDENTIAL_Client_Deliverables\Star Solutions_20240313.pdf
53	<input type="checkbox"/>	03/19/2024 02:36:15	WEF	Opened C:\fileshare\CONFIDENTIAL_Client_Deliverables\Star Solutions_20240313.pdf
75	<input type="checkbox"/>	03/19/2024 02:36:23	WEF	file:///C:/fileshare/CONFIDENTIAL_Client_Deliverables/Star%20Solutions_20240313.pdf visited using Chrome
40	<input type="checkbox"/>	03/19/2024 02:36:52	WEF	Opened C:\fileshare\CONFIDENTIAL_Client_Deliverables\Precision Systems_20240313.pdf
52	<input type="checkbox"/>	03/19/2024 02:36:52	WEF	Opened C:\fileshare\CONFIDENTIAL_Client_Deliverables\Precision Systems_20240313.pdf
63	<input type="checkbox"/>	03/19/2024 02:36:52	WEF	Opened C:\fileshare\CONFIDENTIAL_Client_Deliverables

- **At 2:34:55**, we can see that the login from the threat actors started from 192.168.56.102 (PA CB's domain controller).
- **Between 2:35:03 and 2:39:22**, the threat actors opened files and folders mostly focusing on the C:\fileshare folder. This folder appears to host a lot of PA CB's sensitive information like Payroll, HR, Design Documents and Client Deliverables.
- **At 2:41:40**, a compression utility named 7-zip is executed. Threat actors typically stage their data i.e. prepare the data for data exfiltration, before transferring it out of the network. During data staging, threat actors often compress any important files and folders into a single compressed archive.
- **Between 2:52:19 and 3:04:34**, they visit several file transfer sites including Google Drive.
- **At 3:07:27**, the malware is dropped under *C:\PerfLogs*.
- **At 3:17:31**, the ransom note is created.
- **At 3:23:49**, their session is logged off.

LAB #3.1 DOMAIN CONTROLLER ANALYSIS

Goal: To determine threat actor activity on the domain controller on March 19, 2024

Recap:

From our analysis of the file server, we determined that the threat actor moved laterally from the domain controller (192.168.56.102) to the file server on **March 19, 2024 at 2:34:55** using the administrator account.

In this lab, we will answer several questions about the domain controller. Namely:

- 1. Which user was logged in on the domain controller on March 19, 2024, at 2:34:55?**
- 2. What are the login and logoff times of that user session? What was the originating IP address of that session?**
- 3. Are there other sessions with the same originating IP address?**
- 4. What happened during these sessions in terms of file/folder interaction, program execution, and internet browsing activity?**

To simplify analysis, we have already executed all the tools mentioned in labs 2.1 through 2.6. We have also generated a normalized CSV timeline from the output from all the different tools. For this lab, we will be answering the questions mentioned above using the timeline output for the domain controller.

Let's load the already generated timeline output into Timeline Explorer. To do this, let's navigate to *C:\lab\Tools\CSV2Timeline\DC*. Load the CSV report in this folder into Timeline Explorer.

Once it is loaded, you should see the output like this:

Line	Tag	Timestamp	Source System	Message
1		03/19/2024 03:06:42	DC	File Creation of tunnel.aspx in the path .\PerfLogs
2		03/19/2024 02:34:55	DC	Opened bc3296e3fd9adcb8
3		03/19/2024 02:21:36	DC	Opened C:\Users\administrator\Downloads\x64\out.7z
4		03/19/2024 02:15:30	DC	Opened C:\Users\Public\Documents\Documents.zip
5		03/19/2024 01:14:02	DC	Opened C:\Users\admin.1\Desktop\helpdesk_password\password_policy.txt
6		03/19/2024 01:13:54	DC	Opened C:\Users\admin.1\Desktop\router_configs\Router3_config.txt
7		03/19/2024 01:13:11	DC	Opened C:\Users\admin.1\Desktop\my_network_deets.txt
8		03/19/2024 02:17:41	DC	Opened C:\Users\administrator\Documents\fi.txt
9		03/19/2024 02:08:32	DC	Opened C:\Users\administrator\Downloads\x64\out.log
10		03/19/2024 01:34:17	DC	Opened C:\Users\administrator\Downloads\nm.txt
11		03/19/2024 01:14:02	DC	Opened C:\Users\admin.1\Desktop\helpdesk_password\password_policy.txt
12		03/19/2024 01:13:54	DC	Opened C:\Users\admin.1\Desktop\router_configs\Router3_config.txt
13		03/19/2024 01:13:11	DC	Opened C:\Users\admin.1\Desktop\my_network_deets.txt
14		03/19/2024 03:06:47	DC	Opened C:\PerfLogs
15		03/19/2024 03:06:47	DC	Opened \\tsclient_home_kali_Documents
16		03/19/2024 02:32:28	DC	Opened knownfolder:{374DE290-123F-4565-9164-39C4925E467B} ==> Downloads
17		03/19/2024 02:21:36	DC	Opened C:\Users\administrator\Downloads\x64
18		03/19/2024 02:17:41	DC	Opened knownfolder:{FDD39AD0-238F-46AF-ADB4-6C85480369C7} ==> Documents

Let's first sort the events in ascending order. To do this, we will click on the Timestamp column.

Next, let us apply a Timestamp filter to focus on our date of interest - March 19, 2024. We can do this by clicking on the row right below the Timestamp column and entering our date '03/19/2024'. Like so:

Line	Tag	Timestamp	Source System	Message
82		03/19/2024 01:07:58	DC	Remote Desktop Services: Session logon succeeded WINDOMAIN\administrator from 185.107.56.154 - Session ID: 3
23		03/19/2024 01:08:06	DC	Opened knownfolder:{754AC886-DF64-4CBA-86B5-F7FBF4FBCE5} ==> ThisPCDesktopFolder
22		03/19/2024 01:08:07	DC	Opened knownfolder:{33E28130-4E1E-4676-835A-98395C3BC3BB} ==> Pictures
7		03/19/2024 01:13:11	DC	Opened C:\Users\admin.1\Desktop\my_network_deets.txt
13		03/19/2024 01:13:11	DC	Opened C:\Users\admin.1\Desktop\my_network_deets.txt
21		03/19/2024 01:13:11	DC	Opened C:\Users\admin.1\Desktop
6		03/19/2024 01:13:54	DC	Opened C:\Users\admin.1\Desktop\router_configs\Router3_config.txt
12		03/19/2024 01:13:54	DC	Opened C:\Users\admin.1\Desktop\router_configs\Router3_config.txt
20		03/19/2024 01:13:54	DC	Opened C:\Users\admin.1\Desktop\router_configs
5		03/19/2024 01:14:02	DC	Opened C:\Users\admin.1\Desktop\helpdesk_password\password_policy.txt
11		03/19/2024 01:14:02	DC	Opened C:\Users\admin.1\Desktop\helpdesk_password\password_policy.txt
19		03/19/2024 01:14:02	DC	Opened C:\Users\admin.1\Desktop\helpdesk_password
24		03/19/2024 01:17:00	DC	https://angryip.org/ visited using Chrome
25		03/19/2024 01:17:20	DC	https://angryip.org/google_widgets visited using Chrome

Question: Which user was logged in on the domain controller on March 19, 2024, at 2:34:55?

Let us scroll down to a timestamp around 2:34:55 on March 19, 2024.

03/19/2024 02:32:28	DC	Opened C:\Users\administrator\Downloads
03/19/2024 02:32:30	DC	C:\Users\administrator\Downloads\TeamViewer_Host_Setup_x64.exe was executed
03/19/2024 02:32:30	DC	C:\Users\administrator\Downloads\TeamViewer_Host_Setup_x64.exe was executed
03/19/2024 02:34:55	DC	Opened C:\Windows\System32\mstsc.exe /v:"192.168.56.103"
03/19/2024 02:55:10	DC	Remote Desktop Services: Session has been disconnected WINDOMAIN\administrator from 185.107.56.154 - Session ID: 2
03/19/2024 02:59:08	DC	Remote Desktop Services: Session reconnection succeeded WINDOMAIN\administrator from 185.107.56.154 - Session ID: 2

We see that at 2:34:55, a program named “mstsc.exe” was executed with the arguments “192.168.56.103”.

MSTSC (Microsoft Terminal Services Client) is the program name for Windows RDP. This record confirms that the domain controller was utilized to remotely connect to the file server (192.168.56.103) using Windows RDP.

To find out which user logged in during this time, scroll up to find the most recent login. We see a user session with Session ID #2 originating from an external IP address, 185.107.56.154, that began at 1:57:25 using the **administrator** account.

Question: What are the login and logoff times of that user session? What was the originating IP address of that session?

In the previous section, we determined that the session began at 1:57:25 using the **administrator** account.

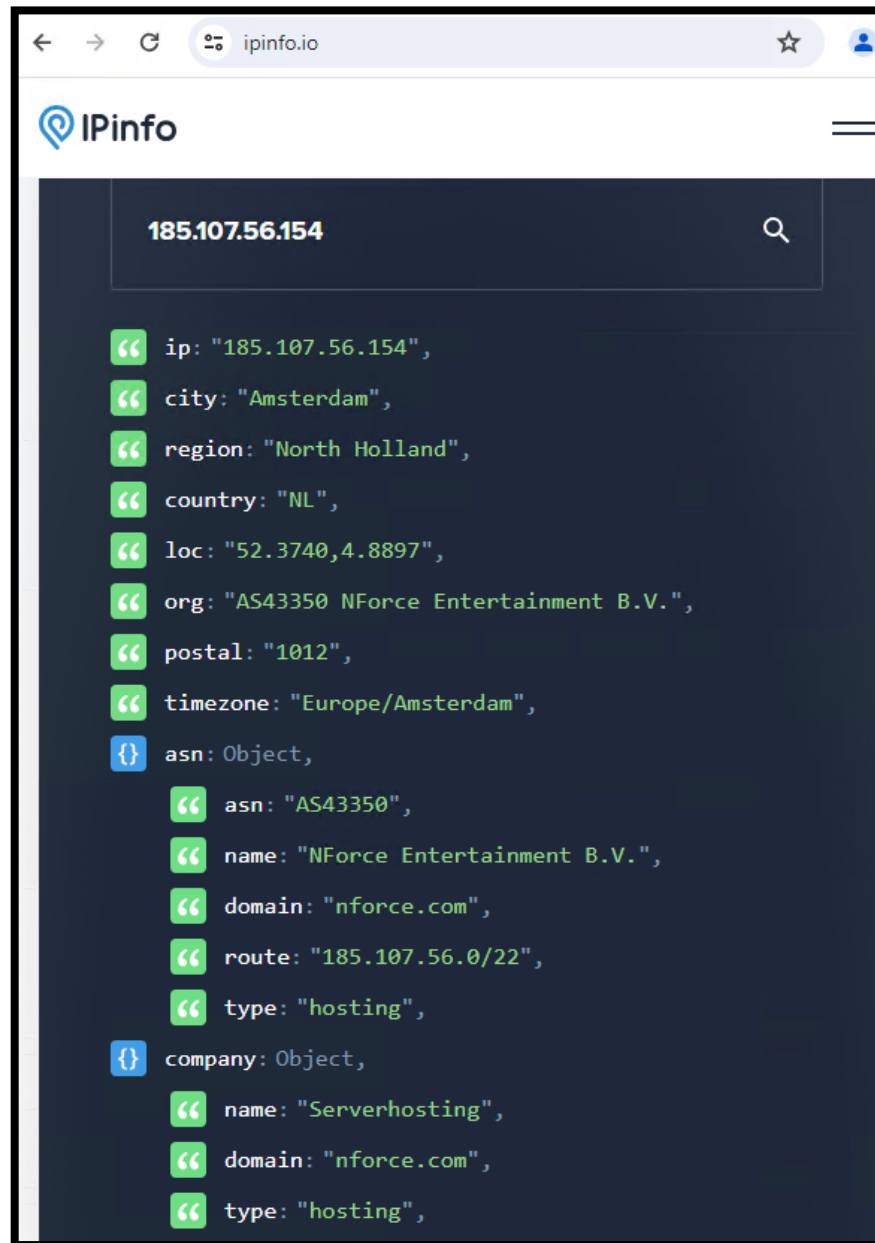
Now, let’s find out when this session ended. Filter for “Session ID: 2” in the Message column as seen in the screenshot below.

Line	Tag	Timestamp	Source System	Message
=		03/19/2024		Session ID: 2
89		03/19/2024 01:57:25	DC	Remote Desktop Services: Session logon succeeded WINDOMAIN\administrator from 185.107.56.154 - Session ID: 2
90		03/19/2024 02:55:10	DC	Remote Desktop Services: Session has been disconnected WINDOMAIN\administrator from 185.107.56.154 - Session ID: 2
91		03/19/2024 02:59:08	DC	Remote Desktop Services: Session reconnection succeeded WINDOMAIN\administrator from 185.107.56.154 - Session ID: 2
92		03/19/2024 03:25:59	DC	Remote Desktop Services: Session has been disconnected WINDOMAIN\administrator from 185.107.56.154 - Session ID: 2

Looks like this session ended at 03:25:59, lasting for 1 hour 28 minutes.

The originating IP address for this session is 185.107.56.154. Let us try to gather some more information about this IP address.

Visit www.ipinfo.io and submit the IP address. This website is useful to determine details about an IP address such as geo-location, ISP and association with anonymizing services like proxies, VPNs, TOR and dedicated hosting providers.





It appears that 185.107.56.154 is an IP address associated with a VPN provider named Proton VPN. It appears that the threat actors were utilizing a VPN service to hide their actual location. You can learn more about Proton VPN here: <https://protonvpn.com/>.

Question: Are there other user sessions with the same originating IP address?

Let's filter on "185.107.56.154" in the "Message" field as seen below:

Timestamp	Source System	Message
03/19/2024	DC	185.107.56.154
03/19/2024 01:07:58	DC	Remote Desktop Services: Session logon succeeded WINDOMAIN\administrator from 185.107.56.154 - Session ID: 3
03/19/2024 01:44:36	DC	Remote Desktop Services: Session has been disconnected WINDOMAIN\administrator from 185.107.56.154 - Session ID: 3
03/19/2024 01:45:14	DC	Remote Desktop Services: Session reconnection succeeded WINDOMAIN\administrator from 185.107.56.154 - Session ID: 3
03/19/2024 01:45:36	DC	Remote Desktop Services: Session has been disconnected WINDOMAIN\administrator from 185.107.56.154 - Session ID: 3
03/19/2024 01:46:43	DC	Remote Desktop Services: Session reconnection succeeded WINDOMAIN\administrator from 185.107.56.154 - Session ID: 3
03/19/2024 01:54:49	DC	Remote Desktop Services: Session has been disconnected WINDOMAIN\administrator from 185.107.56.154 - Session ID: 3
03/19/2024 01:57:25	DC	Remote Desktop Services: Session logon succeeded WINDOMAIN\administrator from 185.107.56.154 - Session ID: 2
03/19/2024 02:55:10	DC	Remote Desktop Services: Session has been disconnected WINDOMAIN\administrator from 185.107.56.154 - Session ID: 2
03/19/2024 02:59:08	DC	Remote Desktop Services: Session reconnection succeeded WINDOMAIN\administrator from 185.107.56.154 - Session ID: 2
03/19/2024 03:25:59	DC	Remote Desktop Services: Session has been disconnected WINDOMAIN\administrator from 185.107.56.154 - Session ID: 2

Reviewing the records here, it appears that there are two sessions associated with this IP address:

Session ID	Session Start	Session End
Session ID # 3	2024-03-19 01:07:58	2024-03-19 01:54:49
Session ID #2	2024-03-19 01:57:25	2024-03-19 03:25:59

Question: What happened during these sessions in terms of file/folder interaction, program execution, and internet browsing activity?

Let us start with Session ID #3: 2024-03-19 01:07:58 – 01:54:49

- **File/Folder Interaction:** The threat actor browsed through multiple files and folders associated with the “admin.1” user profile including files associated with network information and password policies.
- **Program Execution:** The threat actor executed Nmap, which is an IP scanning tool. Typically, threat actors utilize Nmap during the reconnaissance phase to identify systems to exploit in the victim network.
- **Internet Browsing:** We also see the threat actor utilizing Google Chrome to visit websites related to IP scanning products such as Angry IP scanner and Advanced IP Scanner.

Next, let us focus on Session ID #2: 2024-03-19 1:57:25 - 03:25:59

- **File/Folder Interaction:** The threat actor appears to have accessed files in suspiciously named folders. Specifically, files named “out.log” and “out.7z” in C:\Users\administrator\Downloads\x64 and files named “Documents.zip” and “fi.txt” in C:\Users\Public\Documents and

C:\Users\administrator\Documents respectively. We also see the threat actor create the malware file “tunnel.aspx” in C:\Perflogs.

- **Program Execution:** The threat actor executed several tools like 7-Zip, Google Chrome, Windows RDP and TeamViewer. It is important to note that remote administration tools like TeamViewer are often installed by threat actors to maintain backdoor access to victim systems to reenter the network if their initial method of access (in this case external RDP) is later blocked.
- **Internet Browsing:** We also see the threat actor utilizing Google Chrome to visit a website related to a file sharing site named “file.io”, potentially indicating an attempt to exfiltrate data.