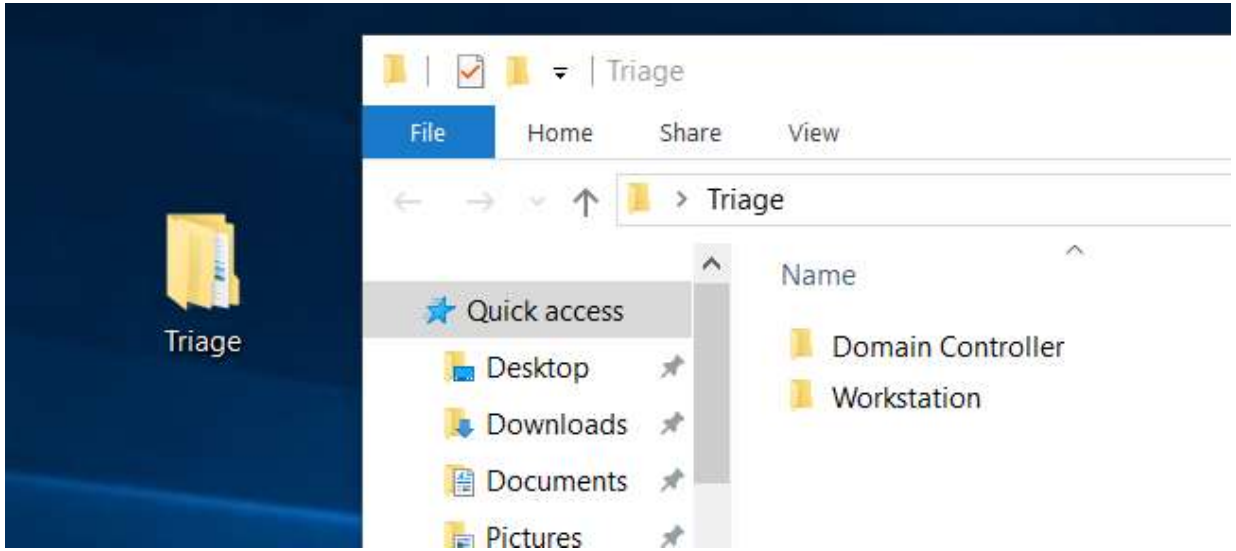
# HTB sherlocks: Campfire-1

Write up by: Chanan shenker

## Start:

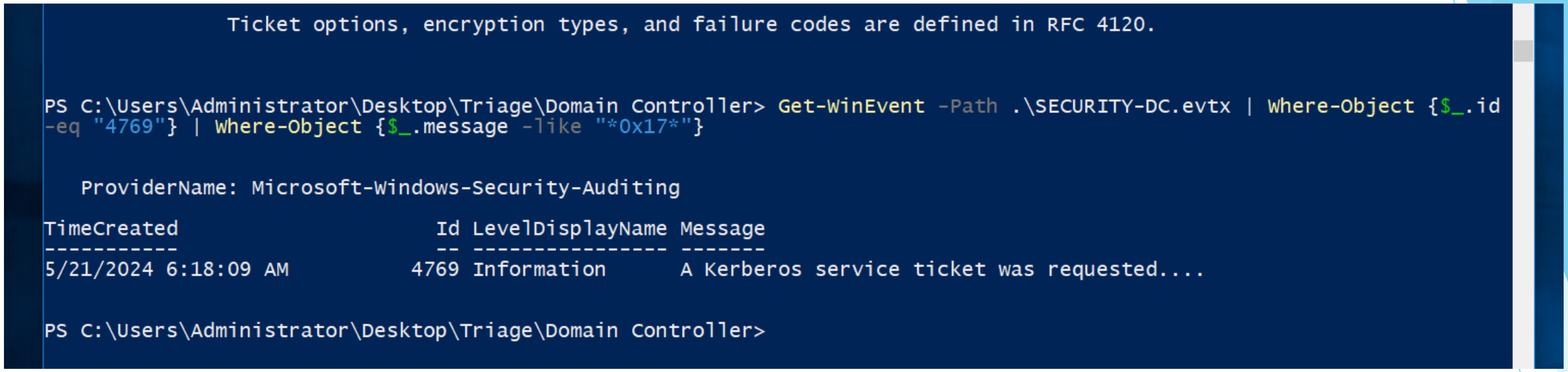
I started the challenge and recieved two directories.



Domain Controller
Workstation

The “Domain Controler” had only a .evtx file and the “Workstation” had a .evtx file and a bunch of Parfetch files.

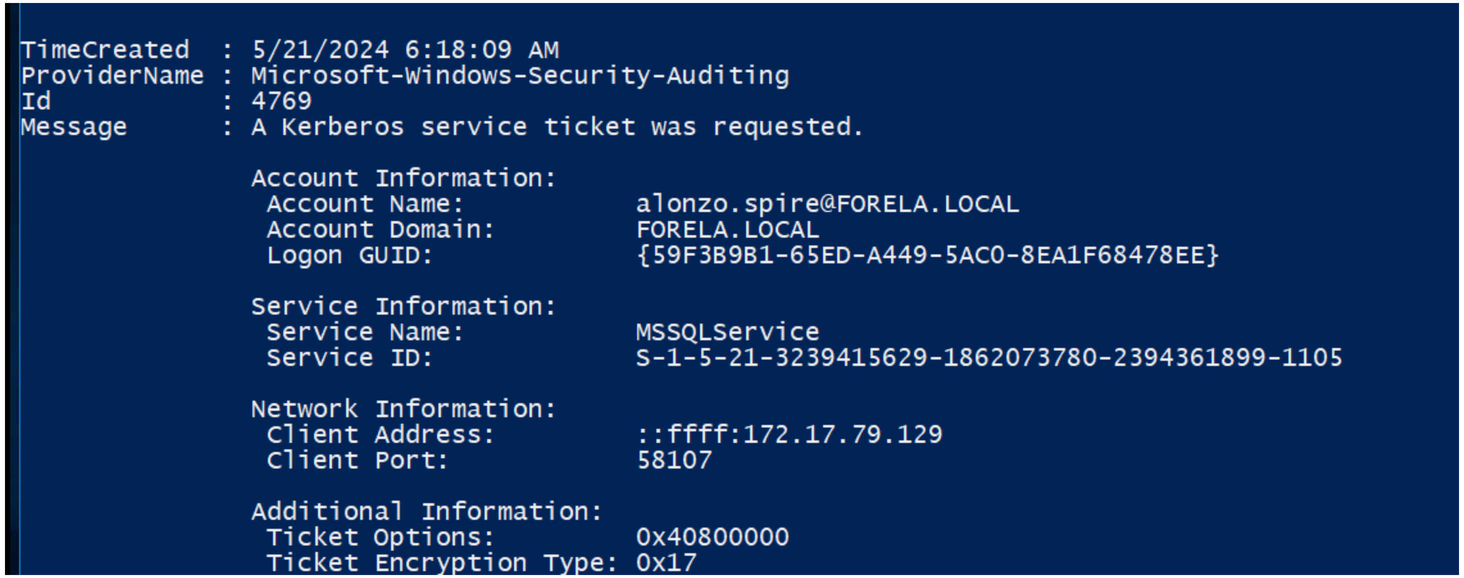
- Question 1: Analyzing Domain Controller Security Logs, can you confirm the date & time when the kerberoasting activity occurred?
- I started by looking up the term ‘kerberoasting’ and found a page by HackTricks explaining it.
- Kerberoasting is an act of requesting TGS tickets for Active Directory users that will be encrypted with the users password therefore opening the possibility for offline cracking of the users password.
- I knew I had to look for an event with the id 4769, which is an even t that is created when a TGS ticket is requested ,and I looked at the hint given and saw they recommended to search for those event with the encryption type of ‘0x17’, which indicates to us that ‘AES256-CTS-HMAC-SHA1-96’ encryption algorithm was used.



```
               Ticket options, encryption types, and failure codes are defined in RFC 4120.


PS C:\Users\Administrator\Desktop\Triage\Domain Controller> Get-WinEvent -Path .\SECURITY-DC.evtx | Where-Object {$_.id
-eq "4769"} | Where-Object {$_.message -like "*0x17*"}


   ProviderName: Microsoft-Windows-Security-Auditing

TimeCreated                     Id LevelDisplayName Message
-----------                     -- ---------------- -------
5/21/2024 6:18:09 AM          4769 Information      A Kerberos service ticket was requested....


PS C:\Users\Administrator\Desktop\Triage\Domain Controller>
```

All I found was a single event, so I found the time. I had some issues but a bit of research led me to understand that I had to convert the time to UTC.  And I get ‘2024-05-21 03:18:09’ as a correct answer.

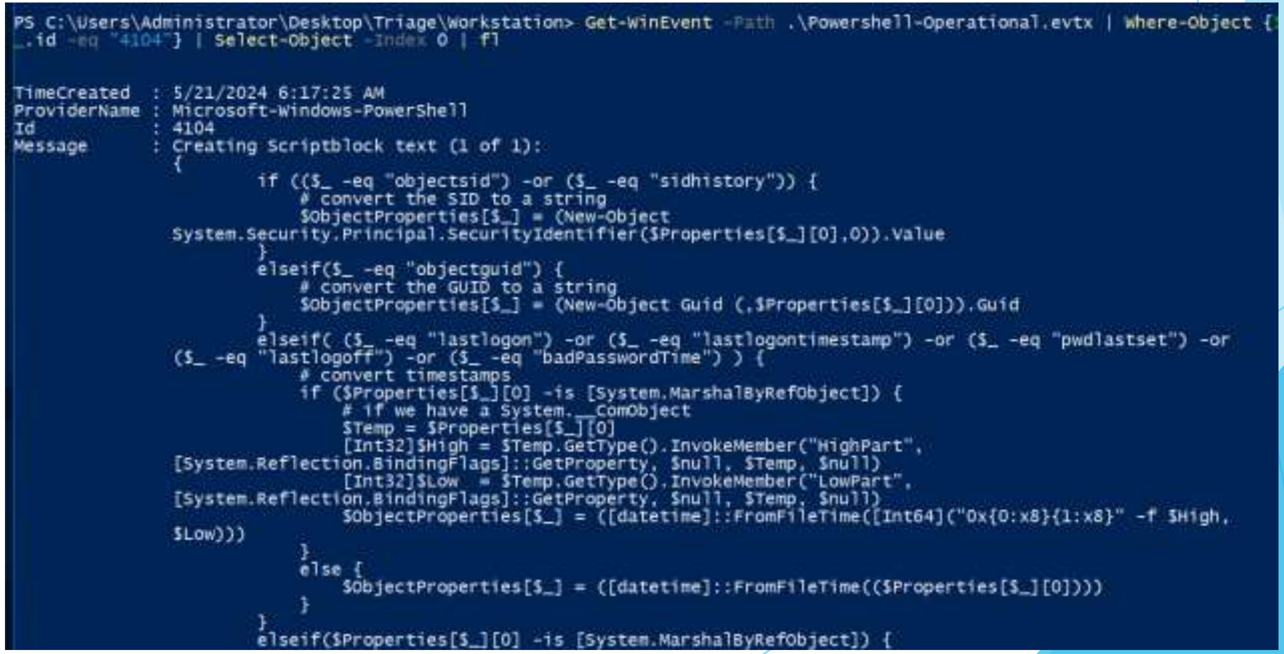
- Question 2&3: What is the Service Name that was targeted? & It is really important to identify the Workstation from which this activity occurred. What is the IP Address of the workstation?
- For this part all I did was open the event with the ‘fl’ powershell command, which opens up and parses the xml fomat of the event, and answered the next 2 questions.



```
TimeCreated  : 5/21/2024 6:18:09 AM
ProviderName : Microsoft-Windows-Security-Auditing
Id           : 4769
Message      : A Kerberos service ticket was requested.

               Account Information:
                Account Name:           alonzo.spire@FORELA.LOCAL
                Account Domain:         FORELA.LOCAL
                Logon GUID:             {59F3B9B1-65ED-A449-5AC0-8EA1F68478EE}

               Service Information:
                Service Name:           MSSQLService
                Service ID:             S-1-5-21-3239415629-1862073780-2394361899-1105

               Network Information:
                Client Address:         ::ffff:172.17.79.129
                Client Port:            58107

               Additional Information:
                Ticket Options:         0x40800000
                Ticket Encryption Type: 0x17
```

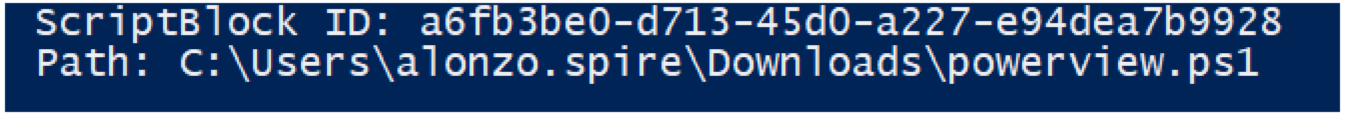
2nd answer: MSSQLService. 3rd answer: 172.17.79.129.

- Question 4: Now that we have identified the workstation, a triage including PowerShell logs and Prefetch files are provided to you for some deeper insights so we can understand how this activity occurred on the endpoint. What is the name of the file used to Enumerate Active directory objects and possibly find Kerberoastable accounts in the network?
- I started by looking at the hint and saw the event id “4104”, which shows a stream of a powershell script being executed ,and I found a few. I decided to open the first one and saw a powershell script which had a few command to enumerate object within AD.



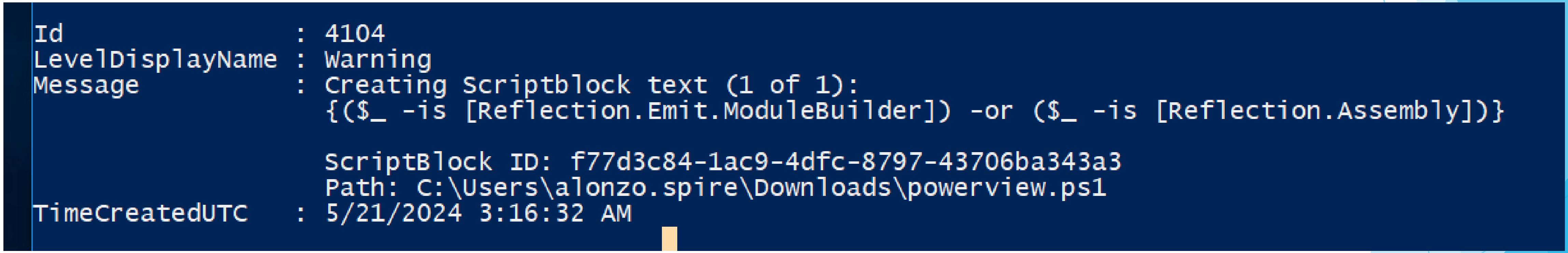
```
PS C:\Users\Administrator\Desktop\Triage\Workstation> Get-WinEvent -Path .\Powershell-Operational.evtx | Where-Object {$
_.id -eq "4104"} | Select-Object -Index 0 | fl


TimeCreated  : 5/21/2024 6:17:25 AM
ProviderName : Microsoft-Windows-PowerShell
Id           : 4104
Message      : Creating Scriptblock text (1 of 1):
               {
                       if (($_ -eq "objectsid") -or ($_ -eq "sidhistory")) {
                           # convert the SID to a string
                           $ObjectProperties[$_] = (New-Object
               System.Security.Principal.SecurityIdentifier($Properties[$_][0],0)).Value
                       }
                       elseif($_ -eq "objectguid") {
                           # convert the GUID to a string
                           $ObjectProperties[$_] = (New-Object Guid (,$Properties[$_][0])).Guid
                       }
                       elseif( ($_ -eq "lastlogon") -or ($_ -eq "lastlogontimestamp") -or ($_ -eq "pwdlastset") -or
               ($_ -eq "lastlogoff") -or ($_ -eq "badPasswordTime") ) {
                           # convert timestamps
                           if ($Properties[$_][0] -is [System.MarshalByRefObject]) {
                               # if we have a System.__ComObject
                               $Temp = $Properties[$_][0]
                               [Int32]$High = $Temp.GetType().InvokeMember("HighPart",
               [System.Reflection.BindingFlags]::GetProperty, $null, $Temp, $null)
                               [Int32]$Low  = $Temp.GetType().InvokeMember("LowPart",
               [System.Reflection.BindingFlags]::GetProperty, $null, $Temp, $null)
                               $ObjectProperties[$_] = ([datetime]::FromFileTime([Int64]("0x{0:x8}{1:x8}" -f $High,
               $Low)))
                           }
                           else {
                               $ObjectProperties[$_] = ([datetime]::FromFileTime(($Properties[$_][0])))
                           }
                       }
                       elseif($Properties[$_][0] -is [System.MarshalByRefObject]) {
```

- At the bottom I saw the name of the file.



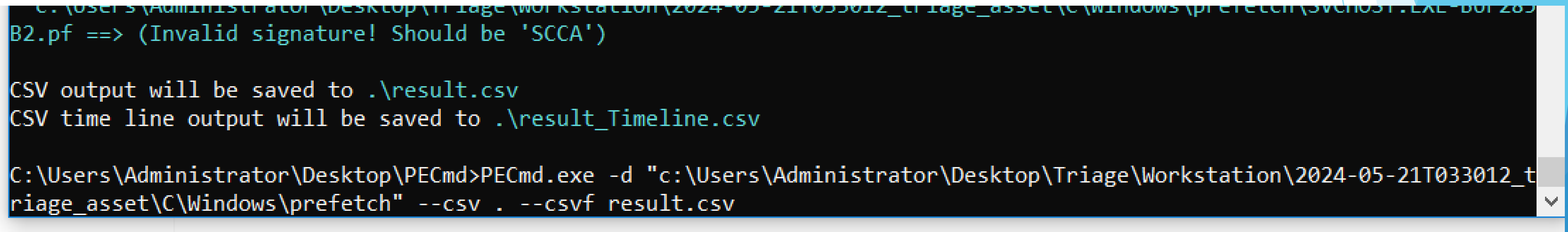
```
ScriptBlock ID: a6fb3be0-d713-45d0-a227-e94dea7b9928
Path: C:\Users\alonzo.spire\Downloads\powerview.ps1
```

- So I submitted the answer and continued.
- <u>Question 5: When was this script executed?</u>
- I converted the time from that event stream and success.

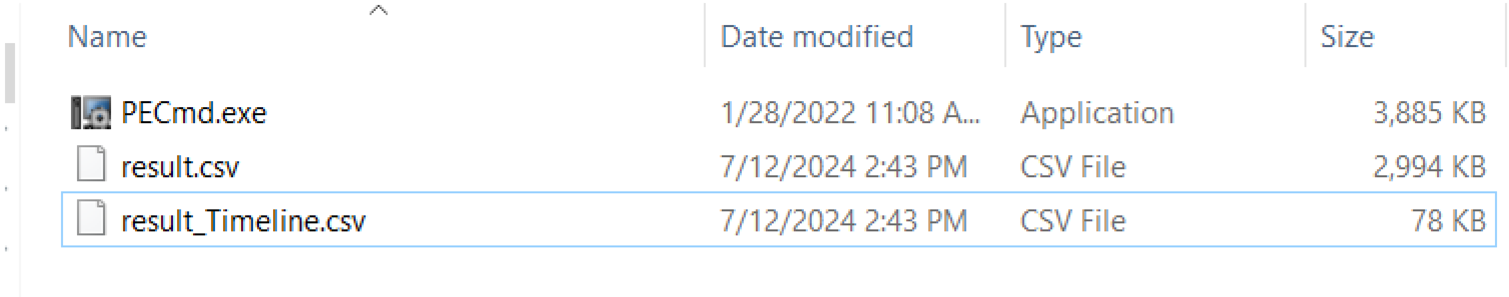


```
Id               : 4104
LevelDisplayName : Warning
Message          : Creating Scriptblock text (1 of 1):
                   {($_ -is [Reflection.Emit.ModuleBuilder]) -or ($_ -is [Reflection.Assembly])}

                   ScriptBlock ID: f77d3c84-1ac9-4dfc-8797-43706ba343a3
                   Path: C:\Users\alonzo.spire\Downloads\powerview.ps1
TimeCreatedUTC   : 5/21/2024 3:16:32 AM
```

- Qustion 6: What is the full path of the tool used to perform the actual kerberoasting attack?
- for this part I looked at the hint and they recommended to use a tool by Eric Zimmerman called “PECmd.exe” a quick look and I learned that it is a parsing tool for prefetch files, these are file used by window to speed up the loading process. I downloaded the tool and gave it the directory with all the prefetch files.

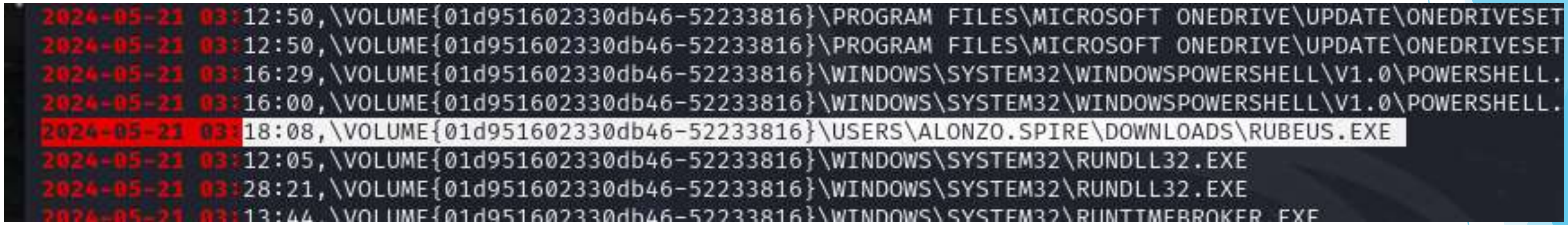


```
 c:\Users\Administrator\Desktop\Triage\Workstation\2024-05-21T033012_triage_asset\C\Windows\prefetch\SVCHOST.EXE-B0F285
B2.pf ==> (Invalid signature! Should be 'SCCA')

CSV output will be saved to .\result.csv
CSV time line output will be saved to .\result_Timeline.csv

C:\Users\Administrator\Desktop\PECmd>PECmd.exe -d "c:\Users\Administrator\Desktop\Triage\Workstation\2024-05-21T033012_t
riage_asset\C\Windows\prefetch" --csv . --csvf result.csv
```



| Name | Date modified | Type | Size |
|---|---|---|---|
| PECmd.exe | 1/28/2022 11:08 A... | Application | 3,885 KB |
| result.csv | 7/12/2024 2:43 PM | CSV File | 2,994 KB |
| result_Timeline.csv | 7/12/2024 2:43 PM | CSV File | 78 KB |

- I took the csv file over to my linux machine and started using text manipulation to find relavent stuff. I went file by file checking online if the file was a known tool and found a tool called Rubeus.exe



```
2024-05-21 03:12:50,\VOLUME{01d951602330db46-52233816}\PROGRAM FILES\MICROSOFT ONEDRIVE\UPDATE\ONEDRIVESET
2024-05-21 03:12:50,\VOLUME{01d951602330db46-52233816}\PROGRAM FILES\MICROSOFT ONEDRIVE\UPDATE\ONEDRIVESET
2024-05-21 03:16:29,\VOLUME{01d951602330db46-52233816}\WINDOWS\SYSTEM32\WINDOWSPOWERSHELL\V1.0\POWERSHELL.
2024-05-21 03:16:00,\VOLUME{01d951602330db46-52233816}\WINDOWS\SYSTEM32\WINDOWSPOWERSHELL\V1.0\POWERSHELL.
2024-05-21 03:18:08,\VOLUME{01d951602330db46-52233816}\USERS\ALONZO.SPIRE\DOWNLOADS\RUBEUS.EXE
2024-05-21 03:12:05,\VOLUME{01d951602330db46-52233816}\WINDOWS\SYSTEM32\RUNDLL32.EXE
2024-05-21 03:28:21,\VOLUME{01d951602330db46-52233816}\WINDOWS\SYSTEM32\RUNDLL32.EXE
2024-05-21 03:13:44,\VOLUME{01d951602330db46-52233816}\WINDOWS\SYSTEM32\RUNTIMEBROKER.EXE
```

- Success.

<u>Last question: When was the tool executed to dump credentials?</u>

Lastly I looked at the date next to this file (2024-05-21 03:18:08) and I was done!