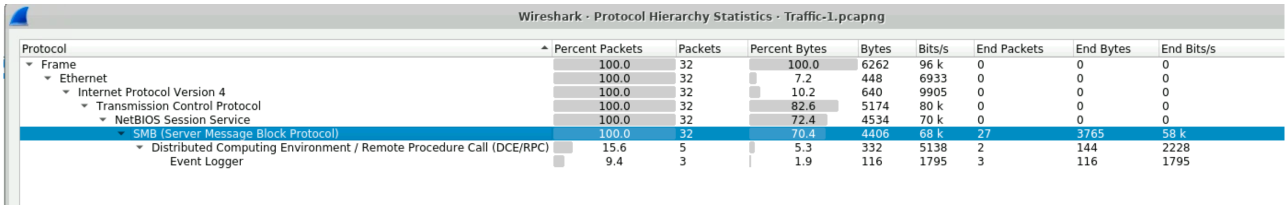
Loren KWOK Packet Detective - Cyberdefenders

File: Traffic-1.pcapng

Q1)

On the taskbar, navigate to Statistics -> Protocol Hierarchy


Wireshark · Protocol Hierarchy Statistics · Traffic-1.pcapng

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	32	100.0	6262	96 k	0	0	0
Ethernet	100.0	32	7.2	448	6933	0	0	0
Internet Protocol Version 4	100.0	32	10.2	640	9905	0	0	0
Transmission Control Protocol	100.0	32	82.6	5174	80 k	0	0	0
NetBIOS Session Service	100.0	32	72.4	4534	70 k	0	0	0
SMB (Server Message Block Protocol)	100.0	32	70.4	4406	68 k	27	3765	58 k
Distributed Computing Environment / Remote Procedure Call (DCE/RPC)	15.6	5	5.3	332	5138	2	144	2228
Event Logger	9.4	3	1.9	116	1795	3	116	1795

You can easily find answer under bytes.

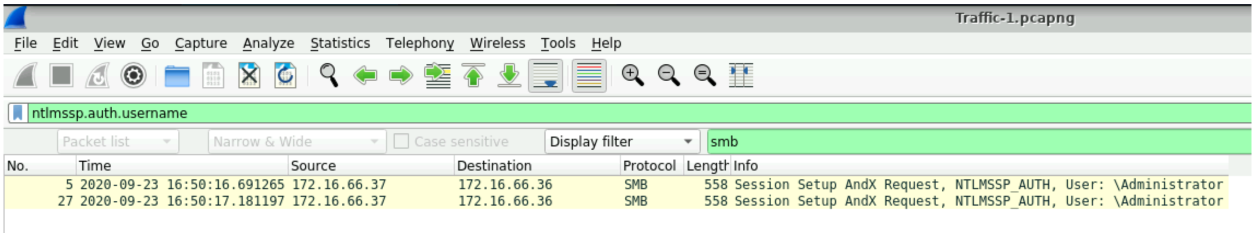
Q2)

There are two types of authentication:

- NTLM (NT LAN Manager)
- Kerberos

In the logs, you can notice a user who is trying to authenticate with NTLM.

Quick way to find out if there is a username associated with NTLM is to use the filter: “ntlmssp.auth.username”


Traffic-1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ntlmssp.auth.username

Packet list
Narrow & Wide
□ Case sensitive

Display filter: smb

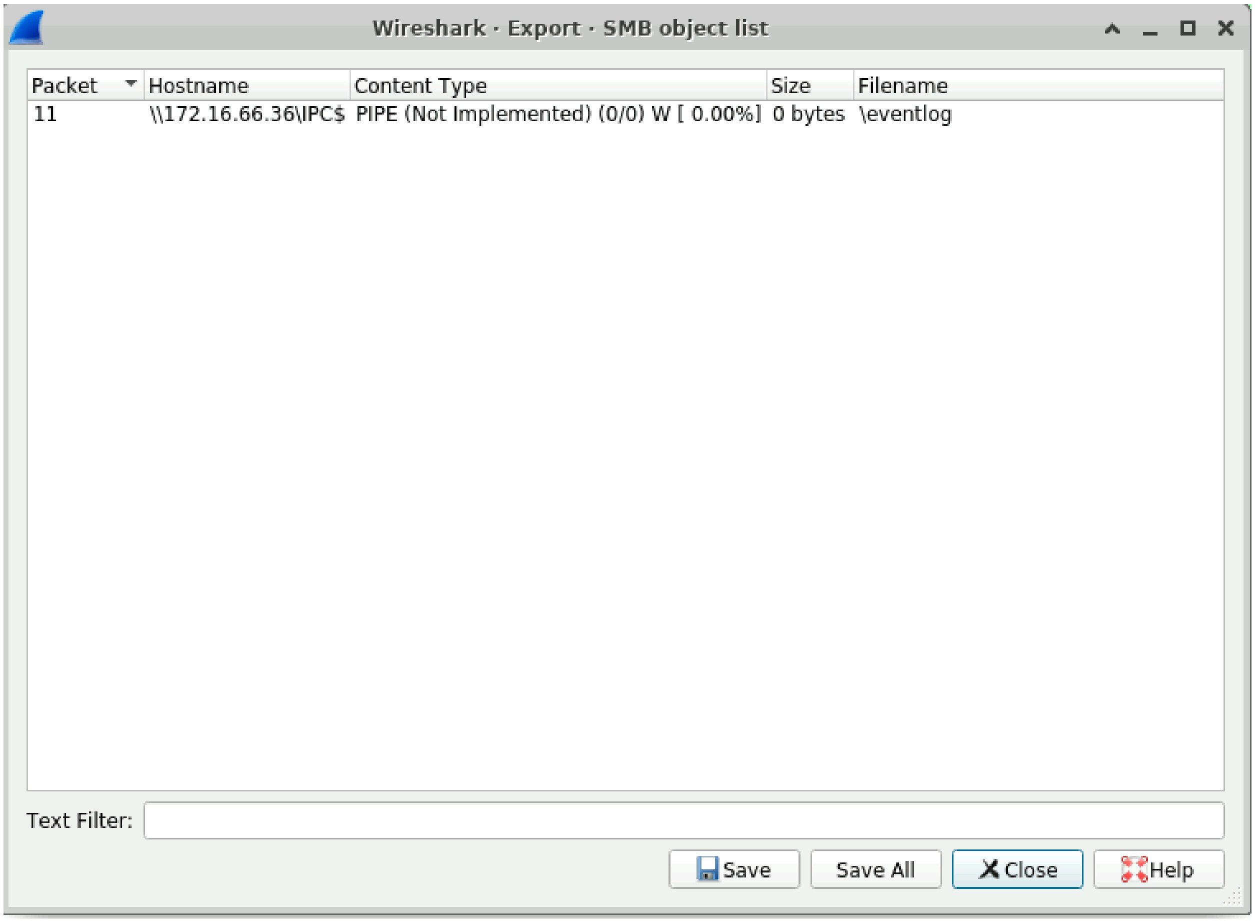
```
No.   Time                       Source         Destination    Protocol Length Info
    5 2020-09-23 16:50:16.691265 172.16.66.37   172.16.66.36   SMB      558 Session Setup AndX Request, NTLMSSP_AUTH, User: \Administrator
   27 2020-09-23 16:50:17.181197 172.16.66.37   172.16.66.36   SMB      558 Session Setup AndX Request, NTLMSSP_AUTH, User: \Administrator
```

Alternatively, you can easily scroll the packet list to find the first authentication attempt associated with a username.

Q3)

Since the files utilize the SMB protocol, use the taskbar and navigate to File -> Export Objects -> SMB

Finds any objects associated with SMB that is being accessed.



Packet	Hostname	Content Type	Size	Filename
11	\\172.16.66.36\IPC$	PIPE (Not Implemented) (0/0) W [0.00%]	0 bytes	\eventlog

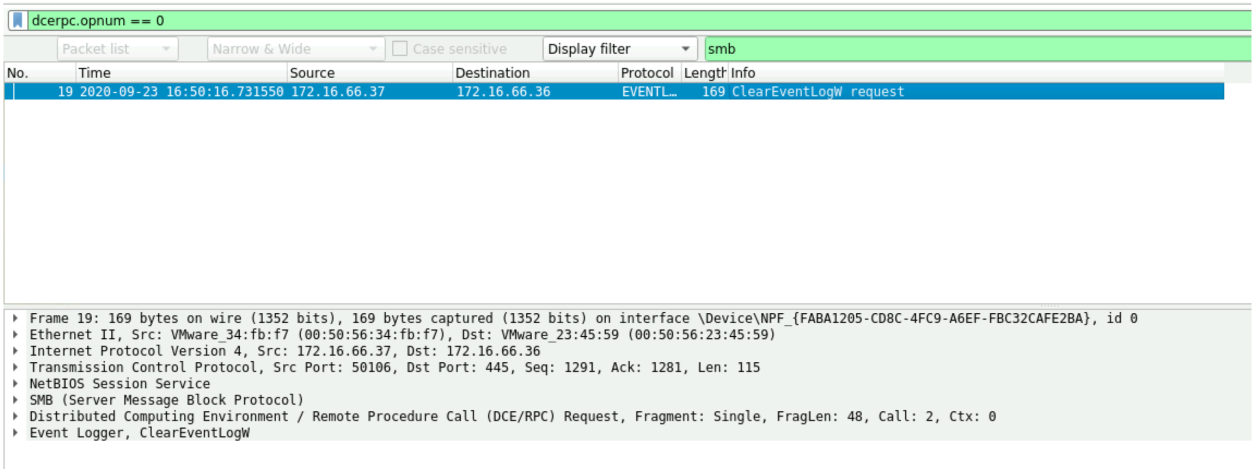
Here, can easily notice the file name.

Q4)

Use "dcerpc.opnum == 0" filter to find the Clear Request. Opnum is an easy way to look for certain events:

- Opnum 0 is for ClearEventLog
- Opnum 7 is for ReadEventLog
- Opnum 1 is for BackupEventLog
- Opnum 4 and 5 are for GetNumberofEventLogRecords and GetOldestEventLogRecord respectively

In the taskbar, go to View -> Time Display Format -> UTC Date and Time of Day



```
dcerpc.opnum == 0
```

```
smb
```

```
No.   Time                        Source         Destination    Protocol  Length Info
   19 2020-09-23 16:50:16.731550 172.16.66.37   172.16.66.36   EVENTL…      169 ClearEventLogW request
```

```
▸ Frame 19: 169 bytes on wire (1352 bits), 169 bytes captured (1352 bits) on interface \Device\NPF_{FABA1205-CD8C-4FC9-A6EF-FBC32CAFE2BA}, id 0
▸ Ethernet II, Src: VMware_34:fb:f7 (00:50:56:34:fb:f7), Dst: VMware_23:45:59 (00:50:56:23:45:59)
▸ Internet Protocol Version 4, Src: 172.16.66.37, Dst: 172.16.66.36
▸ Transmission Control Protocol, Src Port: 50106, Dst Port: 445, Seq: 1291, Ack: 1281, Len: 115
▸ NetBIOS Session Service
▸ SMB (Server Message Block Protocol)
▸ Distributed Computing Environment / Remote Procedure Call (DCE/RPC) Request, Fragment: Single, FragLen: 48, Call: 2, Ctx: 0
▸ Event Logger, ClearEventLogW
```

Doing so can easily allow you to find the Date and Time.

File: Traffic-2.pcapng

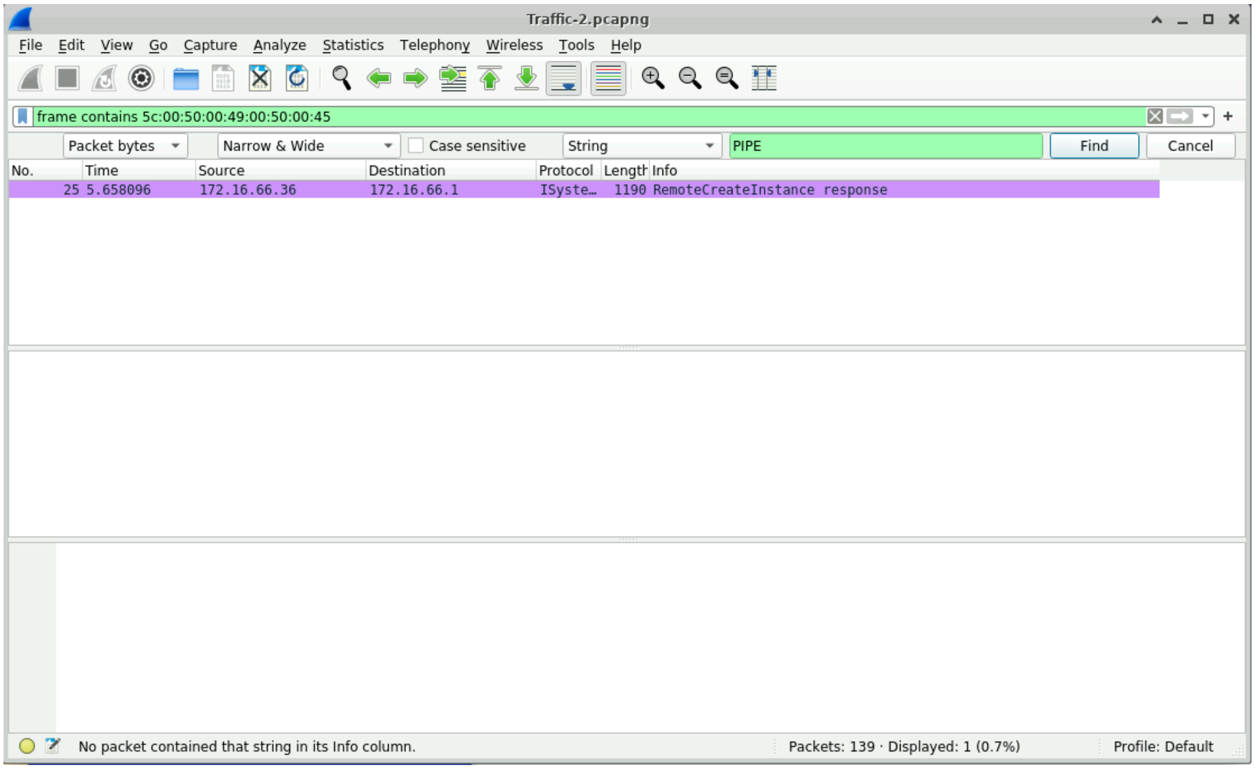
Q5)

Use the following filter: “frame contains 5c:00:50:00:49:00:50:00:45”. These are Unicode for the following:

- 5c:00 is \
- 50:00 is P
- 49:00 is I
- 50:00 is P
- 45:00 is E

Loren KWOK Packet Detective - Cyberdefenders

You will find one packet.


Traffic-2.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Find
Cancel

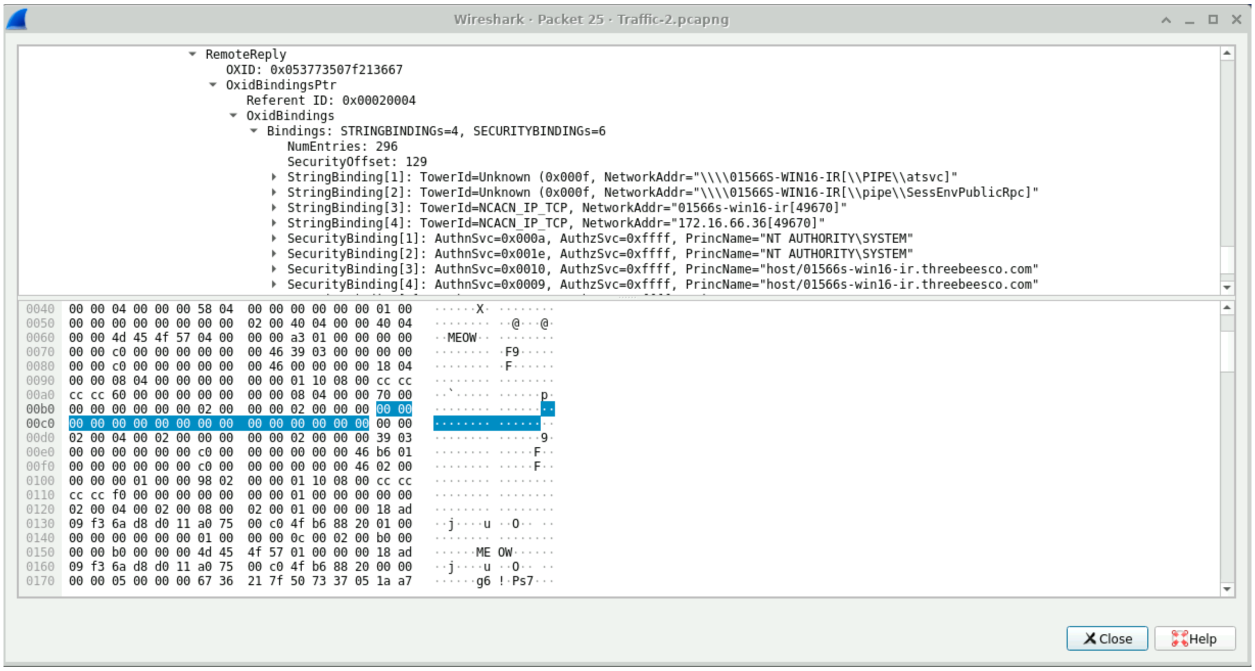
```
frame contains 5c:00:50:00:49:00:50:00:45
```

Packet bytes ▾ | Narrow & Wide ▾ | □ Case sensitive | String ▾ | PIPE

```
No.     Time        Source         Destination    Protocol Length Info
     25 5.658096    172.16.66.36   172.16.66.1    ISyste…    1190 RemoteCreateInstance response
```

No packet contained that string in its Info column. Packets: 139 · Displayed: 1 (0.7%) Profile: Default

Investigate the packet details



```
▾ RemoteReply
    OXID: 0x053773507f213667
  ▾ OxidBindingsPtr
      Referent ID: 0x00020004
    ▾ OxidBindings
      ▾ Bindings: STRINGBINDINGs=4, SECURITYBINDINGs=6
          NumEntries: 296
          SecurityOffset: 129
        ▸ StringBinding[1]: TowerId=Unknown (0x000f, NetworkAddr="\\\\01566S-WIN16-IR[\\PIPE\\atsvc]"
        ▸ StringBinding[2]: TowerId=Unknown (0x000f, NetworkAddr="\\\\01566S-WIN16-IR[\\pipe\\SessEnvPublicRpc]"
        ▸ StringBinding[3]: TowerId=NCACN_IP_TCP, NetworkAddr="01566s-win16-ir[49670]"
        ▸ StringBinding[4]: TowerId=NCACN_IP_TCP, NetworkAddr="172.16.66.36[49670]"
        ▸ SecurityBinding[1]: AuthnSvc=0x000a, AuthzSvc=0xffff, PrincName="NT AUTHORITY\SYSTEM"
        ▸ SecurityBinding[2]: AuthnSvc=0x001e, AuthzSvc=0xffff, PrincName="NT AUTHORITY\SYSTEM"
        ▸ SecurityBinding[3]: AuthnSvc=0x0010, AuthzSvc=0xffff, PrincName="host/01566s-win16-ir.threebeesco.com"
        ▸ SecurityBinding[4]: AuthnSvc=0x0009, AuthzSvc=0xffff, PrincName="host/01566s-win16-ir.threebeesco.com"
```

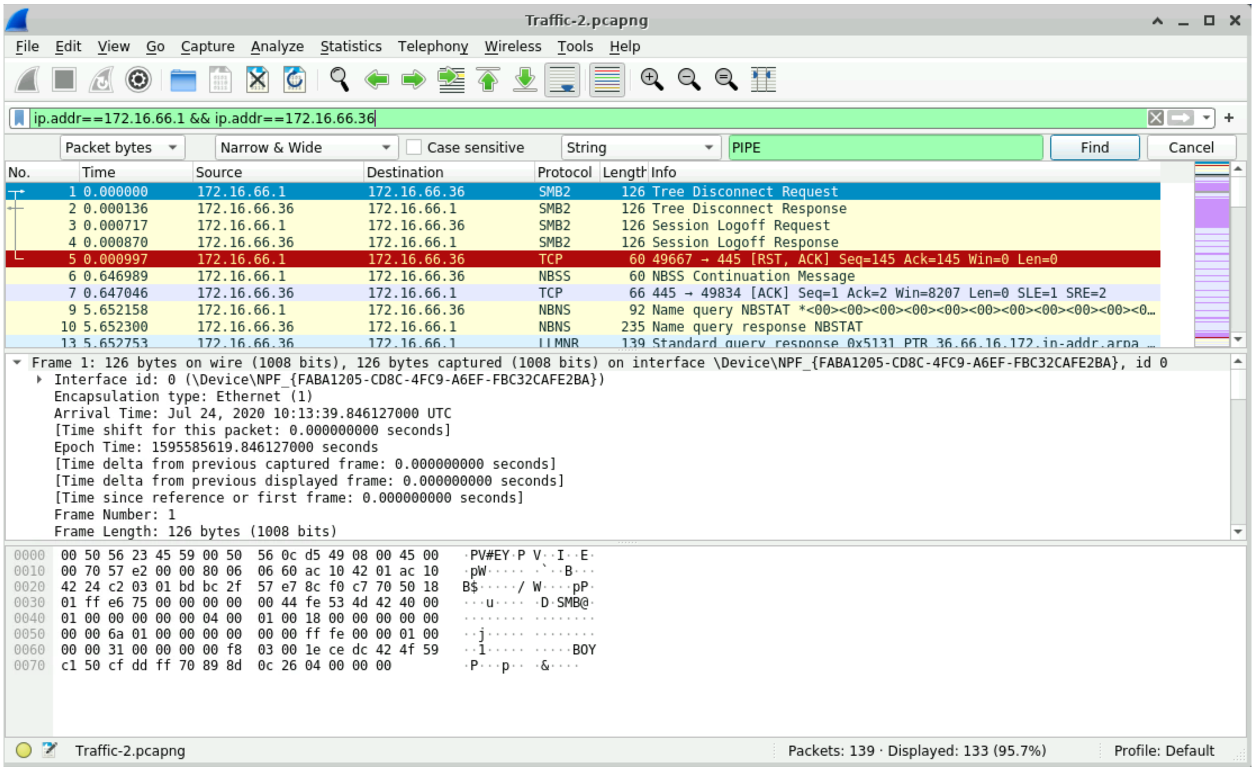
```
0040  00 00 04 00 00 00 58 04  00 00 00 00 00 00 01 00   ······X· ········
0050  00 00 00 00 00 00 00 00  02 00 40 04 00 00 40 04   ········ ··@···@·
0060  00 00 4d 45 4f 57 04 00  00 00 a3 01 00 00 00 00   ··MEOW·· ········
0070  00 00 c0 00 00 00 00 00  00 46 39 03 00 00 00 00   ········ ·F9·····
0080  00 00 c0 00 00 00 00 00  00 46 00 00 00 00 18 04   ········ ·F······
0090  00 00 08 04 00 00 00 00  00 00 01 10 08 00 cc cc   ········ ········
00a0  cc cc 60 00 00 00 00 00  00 00 08 04 00 00 70 00   ··`····· ······p·
00b0  00 00 00 00 00 00 02 00  00 00 02 00 00 00 00 00   ········ ········
00c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00d0  02 00 04 00 02 00 00 00  00 00 02 00 00 00 39 03   ········ ······9·
00e0  00 00 00 00 00 00 c0 00  00 00 00 00 00 46 b6 01   ········ ·····F··
00f0  00 00 00 00 00 00 c0 00  00 00 00 00 00 46 02 00   ········ ·····F··
0100  00 00 00 01 00 00 98 02  00 00 01 10 08 00 cc cc   ········ ········
0110  cc cc f0 00 00 00 00 00  00 00 01 00 00 00 00 00   ········ ········
0120  02 00 04 00 02 00 08 00  02 00 01 00 00 00 18 ad   ········ ········
0130  09 f3 6a d8 d0 11 a0 75  00 c0 4f b6 88 20 01 00   ··j····u ··O·· ··
0140  00 00 00 00 00 00 01 00  00 00 0c 00 02 00 b0 00   ········ ········
0150  00 00 b0 00 00 00 4d 45  4f 57 01 00 00 00 18 ad   ······ME OW······
0160  09 f3 6a d8 d0 11 a0 75  00 c0 4f b6 88 20 00 00   ··j····u ··O·· ··
0170  00 00 05 00 00 00 67 36  21 7f 50 73 37 05 1a a7   ······g6 !·Ps7···
```

If you look hard enough for "PIPE", you will find a file called atsvc which indicates an "AT Service/Task Scheduler."

Alternatively, you may also find the same packet using CTRL+F, changing the search parameter to “Packet bytes” and a “String”, and type in PIPE. It will direct you to the only file with PIPE in its details. Using the same procedure, find the file associated with PIPE.

Q6)

Filter by “ip.addr” for both. Alternatively, you can use “ip.dst” and “ip.src” filters if you wanted to be more specific, but “ip.addr” is faster for this exercise.


Traffic-2.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Find
Cancel

Display filter: ip.addr==172.16.66.1 && ip.addr==172.16.66.36

Packet bytes | Narrow & Wide | □ Case sensitive | String | PIPE

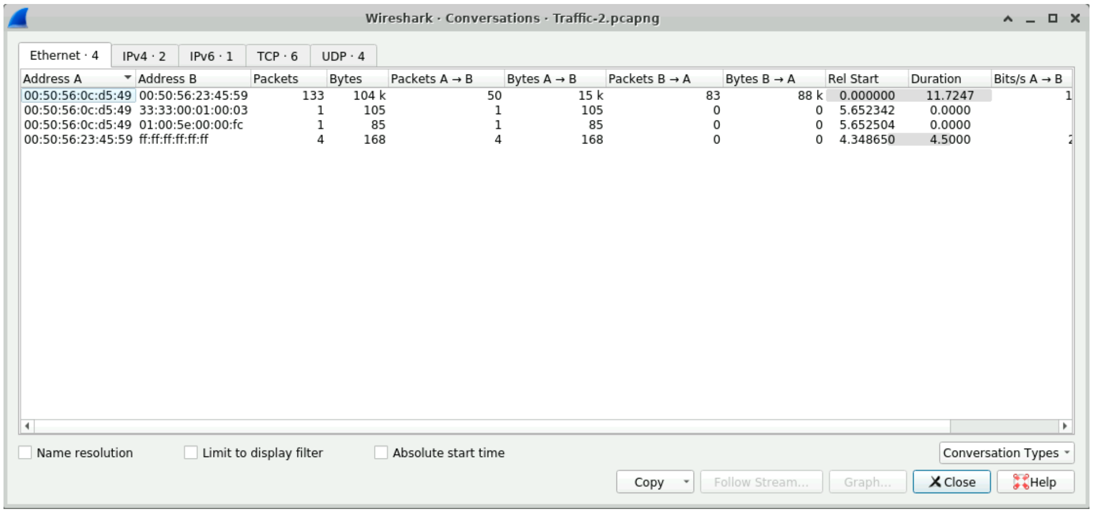
```
No.   Time       Source         Destination    Protocol Length Info
    1 0.000000   172.16.66.1    172.16.66.36   SMB2      126 Tree Disconnect Request
    2 0.000136   172.16.66.36   172.16.66.1    SMB2      126 Tree Disconnect Response
    3 0.000717   172.16.66.1    172.16.66.36   SMB2      126 Session Logoff Request
    4 0.000870   172.16.66.36   172.16.66.1    SMB2      126 Session Logoff Response
    5 0.000997   172.16.66.1    172.16.66.36   TCP        60 49667 → 445 [RST, ACK] Seq=145 Ack=145 Win=0 Len=0
    6 0.646989   172.16.66.1    172.16.66.36   NBSS       60 NBSS Continuation Message
    7 0.647046   172.16.66.36   172.16.66.1    TCP        66 445 → 49834 [ACK] Seq=1 Ack=2 Win=8207 Len=0 SLE=1 SRE=2
    9 5.652158   172.16.66.1    172.16.66.36   NBNS       92 Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><0…
   10 5.652300   172.16.66.36   172.16.66.1    NBNS      235 Name query response NBSTAT
   13 5.652753   172.16.66.36   172.16.66.1    LLMNR     139 Standard query response 0x5131 PTR 36.66.16.172.in-addr.arpa …
```

```
▾ Frame 1: 126 bytes on wire (1008 bits), 126 bytes captured (1008 bits) on interface \Device\NPF_{FABA1205-CD8C-4FC9-A6EF-FBC32CAFE2BA}, id 0
  ▸ Interface id: 0 (\Device\NPF_{FABA1205-CD8C-4FC9-A6EF-FBC32CAFE2BA})
    Encapsulation type: Ethernet (1)
    Arrival Time: Jul 24, 2020 10:13:39.846127000 UTC
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1595585619.846127000 seconds
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.000000000 seconds]
    Frame Number: 1
    Frame Length: 126 bytes (1008 bits)
```

```
0000  00 50 56 23 45 59 00 50  56 0c d5 49 08 00 45 00   ·PV#EY·P V··I··E·
0010  00 70 57 e2 00 00 80 06  06 60 ac 10 42 01 ac 10   ·pW····· ·`··B···
0020  42 24 c2 03 01 bd bc 2f  57 e7 8c f0 c7 70 50 18   B$·····/ W····pP·
0030  01 ff e6 75 00 00 00 00  00 44 fe 53 4d 42 40 00   ···u···· ·D·SMB@·
0040  01 00 00 00 00 00 04 00  01 00 18 00 00 00 00 00   ········ ········
0050  00 00 6a 01 00 00 00 00  00 00 ff fe 00 00 01 00   ··j····· ········
0060  00 00 31 00 00 00 00 f8  03 00 1e ce dc 42 4f 59   ··1····· ·····BOY
0070  c1 50 cf dd ff 70 89 8d  0c 26 04 00 00 00         ·P···p·· ·&····
```

Traffic-2.pcapng | Packets: 139 · Displayed: 133 (95.7%) | Profile: Default

Under the taskbar, navigate to Statistics -> Conversations



Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B
00:50:56:0c:d5:49	00:50:56:23:45:59	133	104 k	50	15 k	83	88 k	0.000000	11.7247	1
00:50:56:0c:d5:49	33:33:00:01:00:03	1	105	1	105	0	0	5.652342	0.0000	
00:50:56:0c:d5:49	01:00:5e:00:00:fc	1	85	1	85	0	0	5.652504	0.0000	
00:50:56:23:45:59	ff:ff:ff:ff:ff:ff	4	168	4	168	0	0	4.348650	4.5000	2

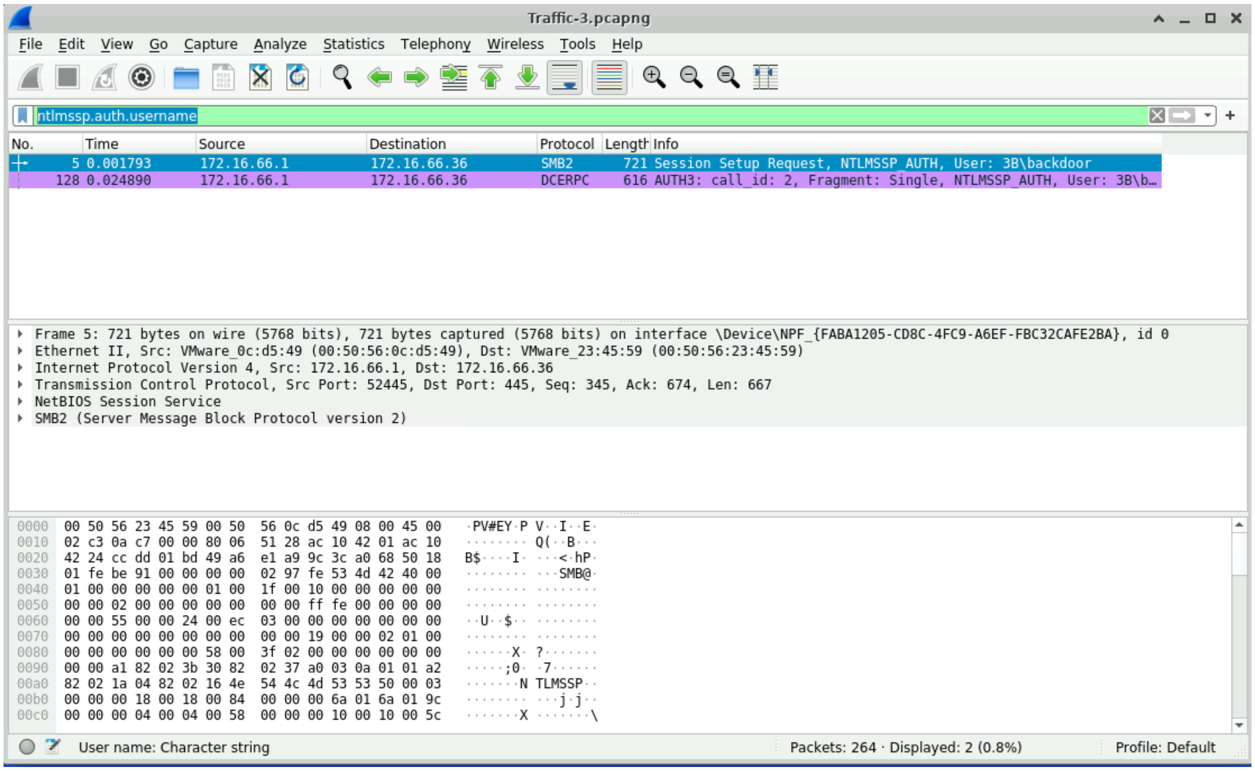
□ Name resolution □ Limit to display filter □ Absolute start time

Under Duration, you will find the duration of the conversation between the two IP addresses.

File: Traffic-3.pcap.ng

Q7)

Once again, you can use “ntlmssp.auth.username” command to look for any usernames that are trying to do a NTLM authentication.


Traffic-3.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ntlmssp.auth.username

```
No.   Time      Source        Destination    Protocol Length Info
    5 0.001793  172.16.66.1   172.16.66.36   SMB2     721 Session Setup Request, NTLMSSP_AUTH, User: 3B\backdoor
  128 0.024890  172.16.66.1   172.16.66.36   DCERPC   616 AUTH3: call_id: 2, Fragment: Single, NTLMSSP_AUTH, User: 3B\b…
```

```
▸ Frame 5: 721 bytes on wire (5768 bits), 721 bytes captured (5768 bits) on interface \Device\NPF_{FABA1205-CD8C-4FC9-A6EF-FBC32CAFE2BA}, id 0
▸ Ethernet II, Src: VMware_0c:d5:49 (00:50:56:0c:d5:49), Dst: VMware_23:45:59 (00:50:56:23:45:59)
▸ Internet Protocol Version 4, Src: 172.16.66.1, Dst: 172.16.66.36
▸ Transmission Control Protocol, Src Port: 52445, Dst Port: 445, Seq: 345, Ack: 674, Len: 667
▸ NetBIOS Session Service
▸ SMB2 (Server Message Block Protocol version 2)
```

```
0000  00 50 56 23 45 59 00 50  56 0c d5 49 08 00 45 00   ·PV#EY·P V··I··E·
0010  02 c3 0a c7 00 00 80 06  51 28 ac 10 42 01 ac 10   ········ Q(··B···
0020  42 24 cc dd 01 bd 49 a6  e1 a9 9c 3c a0 68 50 18   B$····I· ···<·hP·
0030  01 fe be 91 00 00 00 00  02 97 fe 53 4d 42 40 00   ········ ···SMB@·
0040  01 00 00 00 00 00 01 00  1f 00 10 00 00 00 00 00   ········ ········
0050  00 00 02 00 00 00 00 00  00 00 ff fe 00 00 00 00   ········ ········
0060  00 00 55 00 00 24 00 ec  03 00 00 00 00 00 00 00   ··U··$·· ········
0070  00 00 00 00 00 00 00 00  00 00 19 00 00 02 01 00   ········ ········
0080  00 00 00 00 00 00 58 00  3f 02 00 00 00 00 00 00   ······X· ?·······
0090  00 00 a1 82 02 3b 30 82  02 37 a0 03 0a 01 01 a2   ·····;0· ·7······
00a0  82 02 1a 04 82 02 16 4e  54 4c 4d 53 53 50 00 03   ·······N TLMSSP··
00b0  00 00 00 18 00 18 00 84  00 00 00 6a 01 6a 01 9c   ········ ···j·j··
00c0  00 00 00 04 00 04 00 58  00 00 00 10 00 10 00 5c   ·······X ·······\
```

User name: Character string

Packets: 264 · Displayed: 2 (0.8%)

Profile: Default

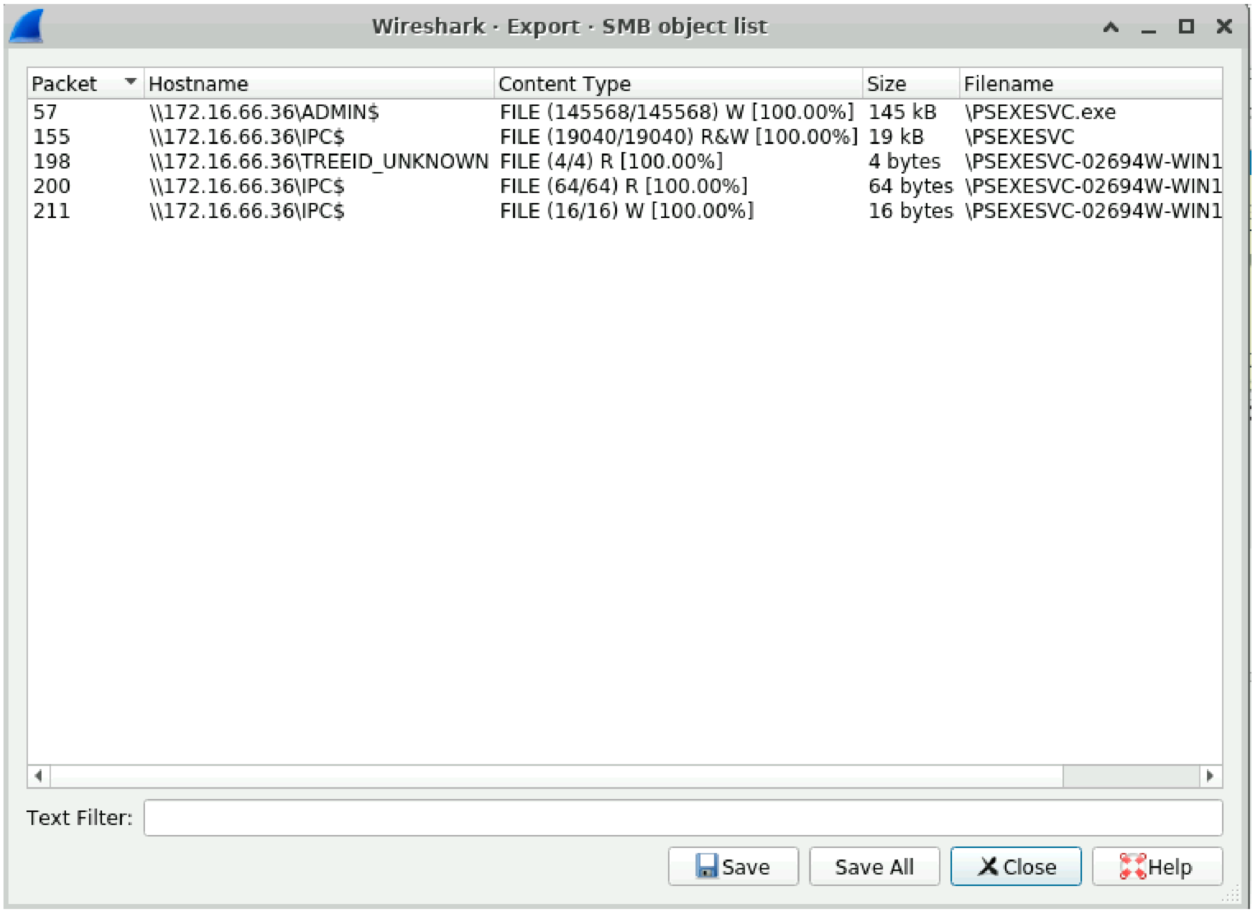
You will find two files, and you’ll be able to see the username of the first request.

Q8)

Once again, use File -> Export Objects to file any files that are involved.

SMB is the only protocol that you need to be concerned with for this exercise if you look at the packets in the log. However, you can try each one to see what you can find. You will notice that there are only executables associated with SMB.

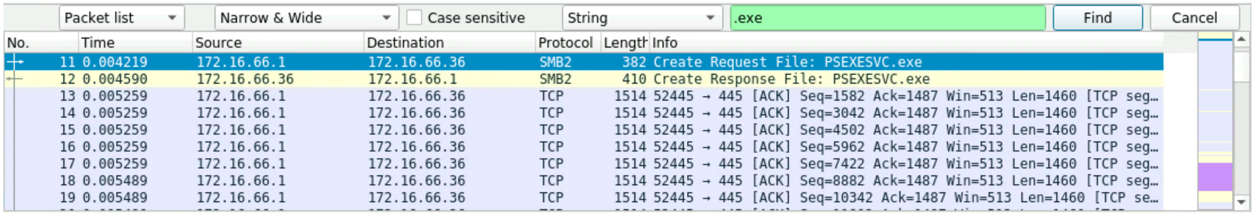
Loren KWOK Packet Detective - Cyberdefenders



Packet	Hostname	Content Type	Size	Filename
57	\\172.16.66.36\ADMIN$	FILE (145568/145568) W [100.00%]	145 kB	\PSEXESVC.exe
155	\\172.16.66.36\IPC$	FILE (19040/19040) R&W [100.00%]	19 kB	\PSEXESVC
198	\\172.16.66.36\TREEID_UNKNOWN	FILE (4/4) R [100.00%]	4 bytes	\PSEXESVC-02694W-WIN1
200	\\172.16.66.36\IPC$	FILE (64/64) R [100.00%]	64 bytes	\PSEXESVC-02694W-WIN1
211	\\172.16.66.36\IPC$	FILE (16/16) W [100.00%]	16 bytes	\PSEXESVC-02694W-WIN1

The only executable can be found here.

You can also use CTRL+F and do a String search for packet list including ".exe"



No.	Time	Source	Destination	Protocol	Length	Info
11	0.004219	172.16.66.1	172.16.66.36	SMB2	382	Create Request File: PSEXESVC.exe
12	0.004590	172.16.66.36	172.16.66.1	SMB2	410	Create Response File: PSEXESVC.exe
13	0.005259	172.16.66.1	172.16.66.36	TCP	1514	52445 → 445 [ACK] Seq=1582 Ack=1487 Win=513 Len=1460 [TCP seg…
14	0.005259	172.16.66.1	172.16.66.36	TCP	1514	52445 → 445 [ACK] Seq=3042 Ack=1487 Win=513 Len=1460 [TCP seg…
15	0.005259	172.16.66.1	172.16.66.36	TCP	1514	52445 → 445 [ACK] Seq=4502 Ack=1487 Win=513 Len=1460 [TCP seg…
16	0.005259	172.16.66.1	172.16.66.36	TCP	1514	52445 → 445 [ACK] Seq=5962 Ack=1487 Win=513 Len=1460 [TCP seg…
17	0.005259	172.16.66.1	172.16.66.36	TCP	1514	52445 → 445 [ACK] Seq=7422 Ack=1487 Win=513 Len=1460 [TCP seg…
18	0.005489	172.16.66.1	172.16.66.36	TCP	1514	52445 → 445 [ACK] Seq=8882 Ack=1487 Win=513 Len=1460 [TCP seg…
19	0.005489	172.16.66.1	172.16.66.36	TCP	1514	52445 → 445 [ACK] Seq=10342 Ack=1487 Win=513 Len=1460 [TCP se…

Congratulations! You have completed all of the exercises in Packet Detective!