Batch: SY-IT (B2) **Experiment Number: 3**

Roll Number: 16010423076 **Name: Ritesh Jha**

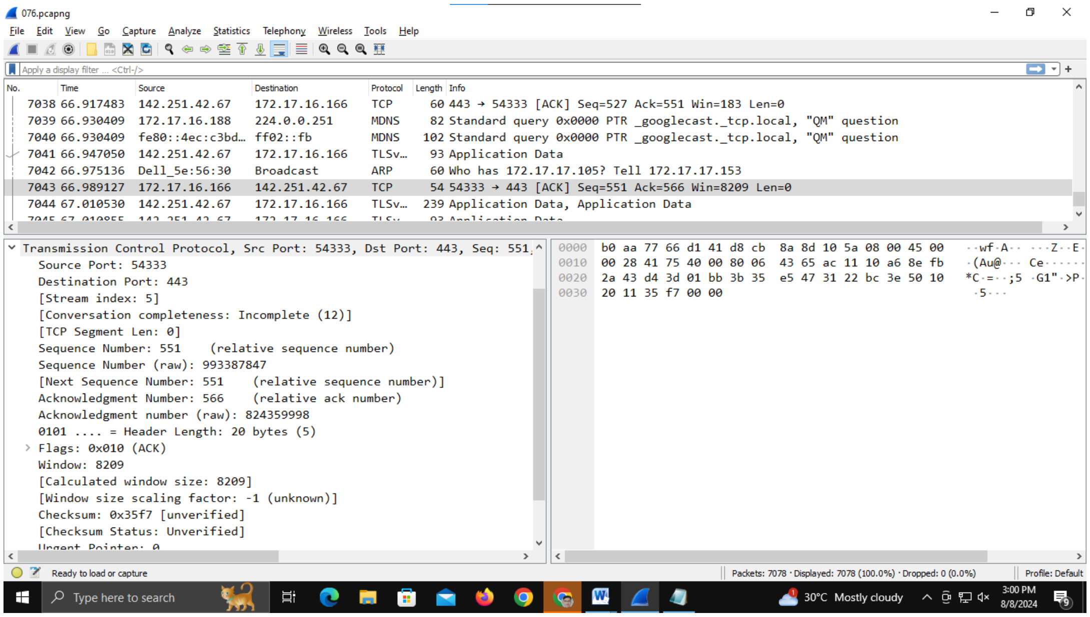
Aim of the Experiment: To explore application layer protocols with packet analysis using Wireshark.

Program/ Steps:

1. Start the machine as an administrator.
2. Start internet.
3. Go to the official website of Wireshark. (www.wireshark.org) and download the old stable version of Wireshark for 32 bit windows operating system.
4. After successful installation you will get the blue icon of Wireshark on the desktop.
5. Click on the icon and start the software.
6. Choose an interface and start capturing the packets.
7. Study the packet details of any one application layer protocols.
8. Understand color code in details.
9. Perform the statistics for captured application layer protocol packet. (Every student should perform for different protocol.)
10. Show the output to the teacher and get it approved.

Output/Result:

1) Wireshark interface


076.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Type here to search
30°C Mostly cloudy
3:00 PM
8/8/2024

```
No.  Time      Source           Destination    Protocol Length Info
7038 66.917483 142.251.42.67    172.17.16.166  TCP       60 443 → 54333 [ACK] Seq=527 Ack=551 Win=183 Len=0
7039 66.930409 172.17.16.188    224.0.0.251    MDNS      82 Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
7040 66.930409 fe80::4ec:c3bd…  ff02::fb       MDNS     102 Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
7041 66.947050 142.251.42.67    172.17.16.166  TLSv…     93 Application Data
7042 66.975136 Dell_5e:56:30    Broadcast      ARP       60 Who has 172.17.17.105? Tell 172.17.17.153
7043 66.989127 172.17.16.166    142.251.42.67  TCP       54 54333 → 443 [ACK] Seq=551 Ack=566 Win=8209 Len=0
7044 67.010530 142.251.42.67    172.17.16.166  TLSv…    239 Application Data, Application Data
```

```
Transmission Control Protocol, Src Port: 54333, Dst Port: 443, Seq: 551,
   Source Port: 54333
   Destination Port: 443
   [Stream index: 5]
   [Conversation completeness: Incomplete (12)]
   [TCP Segment Len: 0]
   Sequence Number: 551    (relative sequence number)
   Sequence Number (raw): 993387847
   [Next Sequence Number: 551    (relative sequence number)]
   Acknowledgment Number: 566    (relative ack number)
   Acknowledgment number (raw): 824359998
   0101 .... = Header Length: 20 bytes (5)
 > Flags: 0x010 (ACK)
   Window: 8209
   [Calculated window size: 8209]
   [Window size scaling factor: -1 (unknown)]
   Checksum: 0x35f7 [unverified]
   [Checksum Status: Unverified]
```

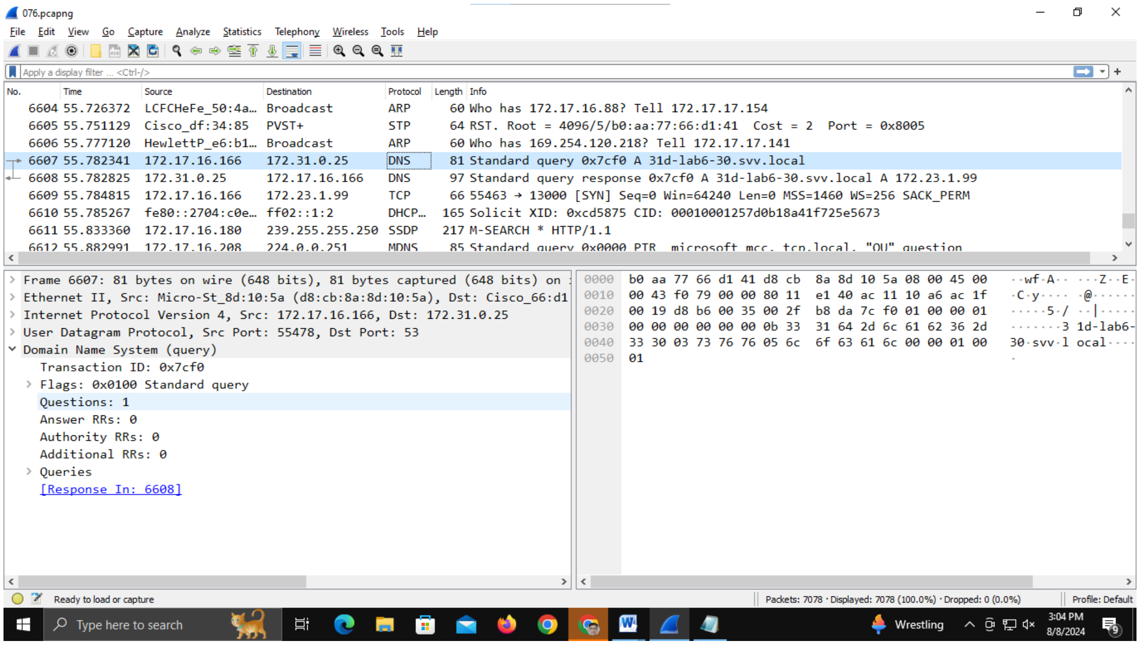
```
0000  b0 aa 77 66 d1 41 d8 cb  8a 8d 10 5a 08 00 45 00   ··wf·A·· ···Z··E·
0010  00 28 41 75 40 00 80 06  43 65 ac 11 10 a6 8e fb   ·(Au@··· Ce······
0020  2a 43 d4 3d 01 bb 3b 35  e5 47 31 22 bc 3e 50 10   *C·=··;5 ·G1"·>P·
0030  20 11 35 f7 00 00                                   ·5···
```

Ready to load or capture

Packets: 7078 · Displayed: 7078 (100.0%) · Dropped: 0 (0.0%)

Profile: Default

2) DNS Query


076.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Type here to search
Wrestling
3:04 PM
8/8/2024

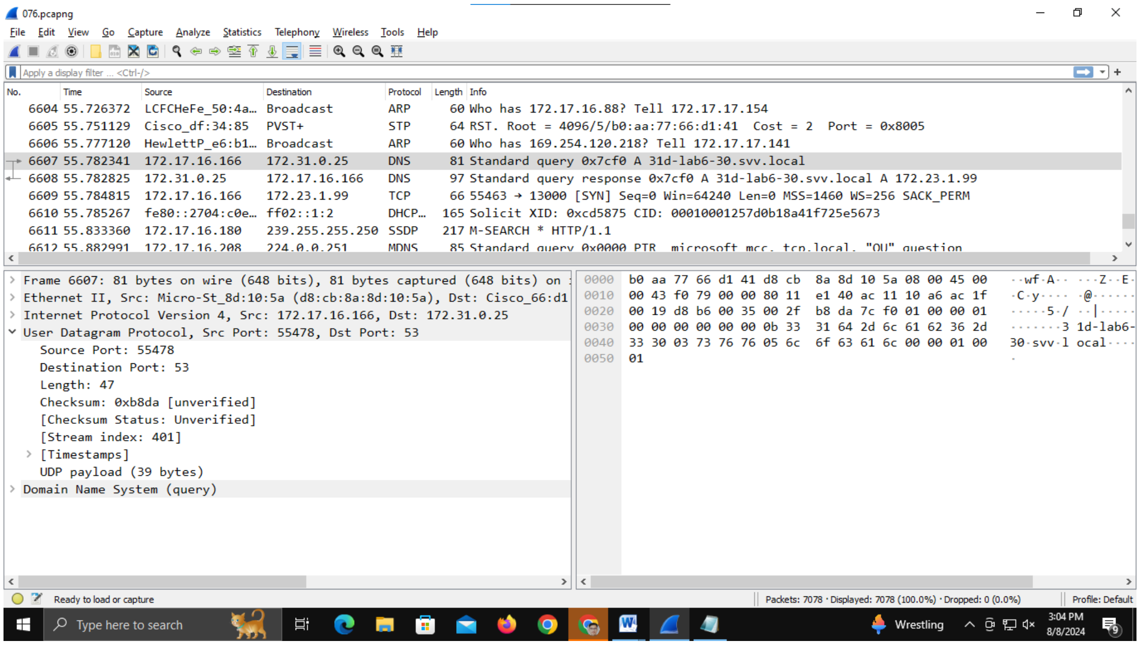
```
No.  Time      Source            Destination      Protocol Length Info
6604 55.726372 LCFCHeFe_50:4a…   Broadcast        ARP      60 Who has 172.17.16.88? Tell 172.17.17.154
6605 55.751129 Cisco_df:34:85    PVST+            STP      64 RST. Root = 4096/5/b0:aa:77:66:d1:41  Cost = 2  Port = 0x8005
6606 55.777120 HewlettP_e6:b1…   Broadcast        ARP      60 Who has 169.254.120.218? Tell 172.17.17.141
6607 55.782341 172.17.16.166     172.31.0.25      DNS      81 Standard query 0x7cf0 A 31d-lab6-30.svv.local
6608 55.782825 172.31.0.25       172.17.16.166    DNS      97 Standard query response 0x7cf0 A 31d-lab6-30.svv.local A 172.23.1.99
6609 55.784815 172.17.16.166     172.23.1.99      TCP      66 55463 → 13000 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
6610 55.785267 fe80::2704:c0e…   ff02::1:2        DHCP…   165 Solicit XID: 0xcd5875 CID: 00010001257d0b18a41f725e5673
6611 55.833360 172.17.16.180     239.255.255.250  SSDP    217 M-SEARCH * HTTP/1.1
6612 55.882991 172.17.16.208     224.0.0.251      MDNS     85 Standard query 0x0000 PTR _microsoft_mcc._tcp.local, "QU" question
```

```
> Frame 6607: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on
> Ethernet II, Src: Micro-St_8d:10:5a (d8:cb:8a:8d:10:5a), Dst: Cisco_66:d1
> Internet Protocol Version 4, Src: 172.17.16.166, Dst: 172.31.0.25
> User Datagram Protocol, Src Port: 55478, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x7cf0
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  > Queries
    [Response In: 6608]
```

```
0000  b0 aa 77 66 d1 41 d8 cb  8a 8d 10 5a 08 00 45 00   ··wf·A·· ···Z··E·
0010  00 43 f0 79 00 00 80 11  e1 40 ac 11 10 a6 ac 1f   ·C·y···· ·@······
0020  00 19 d8 b6 00 35 00 2f  b8 da 7c f0 01 00 00 01   ·····5·/ ··|·····
0030  00 00 00 00 00 00 0b 33  31 64 2d 6c 61 62 36 2d   ·······3 1d-lab6-
0040  33 30 03 73 76 76 05 6c  6f 63 61 6c 00 00 01 00   30·svv·l ocal····
0050  01                                                 ·
```

Ready to load or capture | Packets: 7078 · Displayed: 7078 (100.0%) · Dropped: 0 (0.0%) | Profile: Default

3) User datagram protocol


076.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Type here to search
Wrestling
3:04 PM
8/8/2024

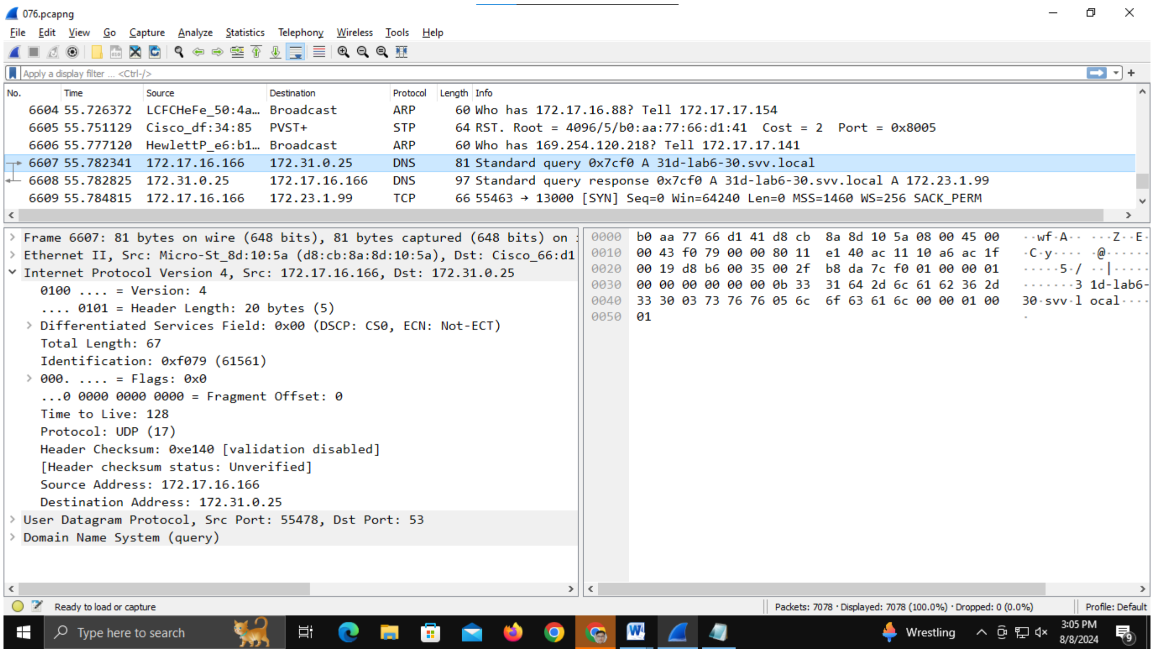
```
No.  Time      Source            Destination      Protocol Length Info
6604 55.726372 LCFCHeFe_50:4a…   Broadcast        ARP      60 Who has 172.17.16.88? Tell 172.17.17.154
6605 55.751129 Cisco_df:34:85    PVST+            STP      64 RST. Root = 4096/5/b0:aa:77:66:d1:41  Cost = 2  Port = 0x8005
6606 55.777120 HewlettP_e6:b1…   Broadcast        ARP      60 Who has 169.254.120.218? Tell 172.17.17.141
6607 55.782341 172.17.16.166     172.31.0.25      DNS      81 Standard query 0x7cf0 A 31d-lab6-30.svv.local
6608 55.782825 172.31.0.25       172.17.16.166    DNS      97 Standard query response 0x7cf0 A 31d-lab6-30.svv.local A 172.23.1.99
6609 55.784815 172.17.16.166     172.23.1.99      TCP      66 55463 → 13000 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
6610 55.785267 fe80::2704:c0e…   ff02::1:2        DHCP…   165 Solicit XID: 0xcd5875 CID: 00010001257d0b18a41f725e5673
6611 55.833360 172.17.16.180     239.255.255.250  SSDP    217 M-SEARCH * HTTP/1.1
6612 55.882991 172.17.16.208     224.0.0.251      MDNS     85 Standard query 0x0000 PTR _microsoft_mcc._tcp.local, "QU" question
```

```
> Frame 6607: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on
> Ethernet II, Src: Micro-St_8d:10:5a (d8:cb:8a:8d:10:5a), Dst: Cisco_66:d1
> Internet Protocol Version 4, Src: 172.17.16.166, Dst: 172.31.0.25
v User Datagram Protocol, Src Port: 55478, Dst Port: 53
    Source Port: 55478
    Destination Port: 53
    Length: 47
    Checksum: 0xb8da [unverified]
    [Checksum Status: Unverified]
    [Stream index: 401]
  > [Timestamps]
    UDP payload (39 bytes)
> Domain Name System (query)
```

```
0000  b0 aa 77 66 d1 41 d8 cb  8a 8d 10 5a 08 00 45 00   ··wf·A·· ···Z··E·
0010  00 43 f0 79 00 00 80 11  e1 40 ac 11 10 a6 ac 1f   ·C·y···· ·@······
0020  00 19 d8 b6 00 35 00 2f  b8 da 7c f0 01 00 00 01   ·····5·/ ··|·····
0030  00 00 00 00 00 00 0b 33  31 64 2d 6c 61 62 36 2d   ·······3 1d-lab6-
0040  33 30 03 73 76 76 05 6c  6f 63 61 6c 00 00 01 00   30·svv·l ocal····
0050  01                                                 ·
```

Ready to load or capture | Packets: 7078 · Displayed: 7078 (100.0%) · Dropped: 0 (0.0%) | Profile: Default

4) Internet Protocol


076.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Type here to search
Wrestling
3:05 PM
8/8/2024

```
No.  Time      Source            Destination   Protocol Length Info
6604 55.726372 LCFCHeFe_50:4a…   Broadcast     ARP      60 Who has 172.17.16.88? Tell 172.17.17.154
6605 55.751129 Cisco_df:34:85    PVST+         STP      64 RST. Root = 4096/5/b0:aa:77:66:d1:41  Cost = 2  Port = 0x8005
6606 55.777120 HewlettP_e6:b1…   Broadcast     ARP      60 Who has 169.254.120.218? Tell 172.17.17.141
6607 55.782341 172.17.16.166     172.31.0.25   DNS      81 Standard query 0x7cf0 A 31d-lab6-30.svv.local
6608 55.782825 172.31.0.25       172.17.16.166 DNS      97 Standard query response 0x7cf0 A 31d-lab6-30.svv.local A 172.23.1.99
6609 55.784815 172.17.16.166     172.23.1.99   TCP      66 55463 → 13000 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
```

```
> Frame 6607: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on 
> Ethernet II, Src: Micro-St_8d:10:5a (d8:cb:8a:8d:10:5a), Dst: Cisco_66:d1
v Internet Protocol Version 4, Src: 172.17.16.166, Dst: 172.31.0.25
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 67
    Identification: 0xf079 (61561)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0xe140 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 172.17.16.166
    Destination Address: 172.31.0.25
> User Datagram Protocol, Src Port: 55478, Dst Port: 53
> Domain Name System (query)
```

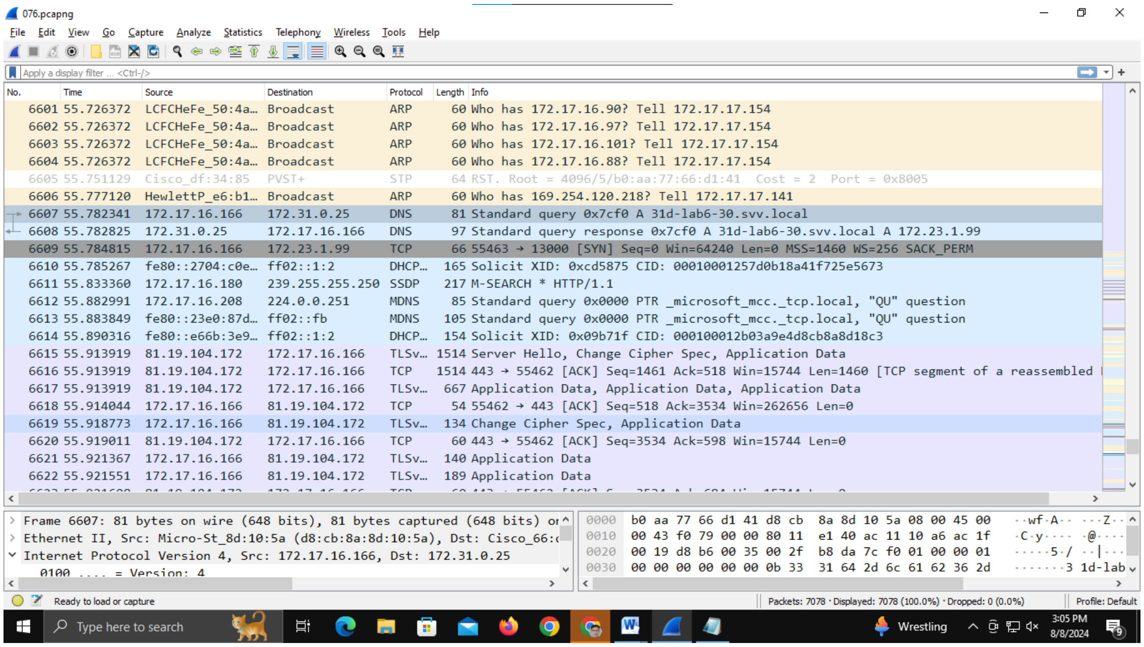
```
0000  b0 aa 77 66 d1 41 d8 cb  8a 8d 10 5a 08 00 45 00   ··wf·A·· ···Z··E·
0010  00 43 f0 79 00 00 80 11  e1 40 ac 11 10 a6 ac 1f   ·C·y···· ·@······
0020  00 19 d8 b6 00 35 00 2f  b8 da 7c f0 01 00 00 01   ·····5·/ ··|·····
0030  00 00 00 00 00 00 0b 33  31 64 2d 6c 61 62 36 2d   ·······3 1d-lab6-
0040  33 30 03 73 76 76 05 6c  6f 63 61 6c 00 00 01 00   30·svv·l ocal····
0050  01                                                 ·
```

Ready to load or capture

Packets: 7078 · Displayed: 7078 (100.0%) · Dropped: 0 (0.0%)

Profile: Default

5) Colored packet list


076.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Type here to search
Wrestling
3:05 PM
8/8/2024

```
No.  Time      Source            Destination     Protocol Length Info
6601 55.726372 LCFCHeFe_50:4a…   Broadcast       ARP      60 Who has 172.17.16.90? Tell 172.17.17.154
6602 55.726372 LCFCHeFe_50:4a…   Broadcast       ARP      60 Who has 172.17.16.97? Tell 172.17.17.154
6603 55.726372 LCFCHeFe_50:4a…   Broadcast       ARP      60 Who has 172.17.16.101? Tell 172.17.17.154
6604 55.726372 LCFCHeFe_50:4a…   Broadcast       ARP      60 Who has 172.17.16.88? Tell 172.17.17.154
6605 55.751129 Cisco_df:34:85    PVST+           STP      64 RST. Root = 4096/5/b0:aa:77:66:d1:41  Cost = 2  Port = 0x8005
6606 55.777120 HewlettP_e6:b1…   Broadcast       ARP      60 Who has 169.254.120.218? Tell 172.17.17.141
6607 55.782341 172.17.16.166     172.31.0.25     DNS      81 Standard query 0x7cf0 A 31d-lab6-30.svv.local
6608 55.782825 172.31.0.25       172.17.16.166   DNS      97 Standard query response 0x7cf0 A 31d-lab6-30.svv.local A 172.23.1.99
6609 55.784815 172.17.16.166     172.23.1.99     TCP      66 55463 → 13000 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
6610 55.785267 fe80::2704:c0e…   ff02::1:2       DHCP…   165 Solicit XID: 0xcd5875 CID: 00010001257d0b18a41f725e5673
6611 55.833360 172.17.16.180     239.255.255.250 SSDP    217 M-SEARCH * HTTP/1.1
6612 55.882991 172.17.16.208     224.0.0.251     MDNS     85 Standard query 0x0000 PTR _microsoft_mcc._tcp.local, "QU" question
6613 55.883849 fe80::23e0:87d…   ff02::fb        MDNS    105 Standard query 0x0000 PTR _microsoft_mcc._tcp.local, "QU" question
6614 55.890316 fe80::e66b:3e9…   ff02::1:2       DHCP…   154 Solicit XID: 0x09b71f CID: 000100012b03a9e4d8cb8a8d18c3
6615 55.913919 81.19.104.172     172.17.16.166   TLSv…  1514 Server Hello, Change Cipher Spec, Application Data
6616 55.913919 81.19.104.172     172.17.16.166   TCP    1514 443 → 55462 [ACK] Seq=1461 Ack=518 Win=15744 Len=1460 [TCP segment of a reassembled 
6617 55.913919 81.19.104.172     172.17.16.166   TLSv…   667 Application Data, Application Data, Application Data
6618 55.914044 172.17.16.166     81.19.104.172   TCP      54 55462 → 443 [ACK] Seq=518 Ack=3534 Win=262656 Len=0
6619 55.918773 172.17.16.166     81.19.104.172   TLSv…   134 Change Cipher Spec, Application Data
6620 55.919011 81.19.104.172     172.17.16.166   TCP      60 443 → 55462 [ACK] Seq=3534 Ack=598 Win=15744 Len=0
6621 55.921367 172.17.16.166     81.19.104.172   TLSv…   140 Application Data
6622 55.921551 172.17.16.166     81.19.104.172   TLSv…   189 Application Data
```

```
> Frame 6607: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) or
> Ethernet II, Src: Micro-St_8d:10:5a (d8:cb:8a:8d:10:5a), Dst: Cisco_66:c
v Internet Protocol Version 4, Src: 172.17.16.166, Dst: 172.31.0.25
    0100 .... = Version: 4
```

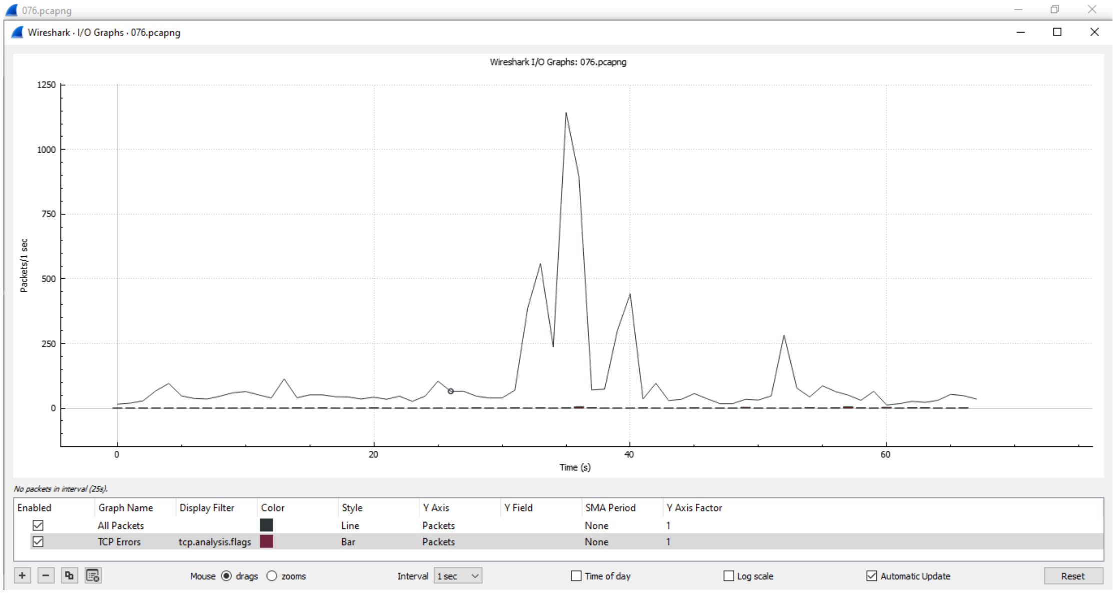
```
0000  b0 aa 77 66 d1 41 d8 cb  8a 8d 10 5a 08 00 45 00   ··wf·A·· ···Z··
0010  00 43 f0 79 00 00 80 11  e1 40 ac 11 10 a6 ac 1f   ·C·y···· ·@····
0020  00 19 d8 b6 00 35 00 2f  b8 da 7c f0 01 00 00 01   ·····5·/ ··|···
0030  00 00 00 00 00 00 0b 33  31 64 2d 6c 61 62 36 2d   ·······3 1d-lab
```

Ready to load or capture

Packets: 7078 · Displayed: 7078 (100.0%) · Dropped: 0 (0.0%)

Profile: Default

6) I/O Graph


076.pcapng
Wireshark · I/O Graphs · 076.pcapng
Wireshark I/O Graphs: 076.pcapng
1250
1000
750
500
250
0
Packets/1 sec
0
20
40
60
Time (s)
+
−
Reset

No packets in interval (25s).

Enabled	Graph Name	Display Filter	Color	Style	Y Axis	Y Field	SMA Period	Y Axis Factor
☑	All Packets		■	Line	Packets		None	1
☑	TCP Errors	tcp.analysis.flags	■	Bar	Packets		None	1

Mouse ● drags ○ zooms Interval 1 sec □ Time of day □ Log scale ☑ Automatic Update

---

Post Lab Question-Answers:

1) NMAP and Wireshark, both tools are used for network analysis. They are also used to troubleshooting the various issues on networks by detecting and fixing them.

NMAP :

1. NMAP is basically an open source tool used for network scanning and auditing.
2. Its main function is to scan the networks and collect data such as the OS, open ports, services and vulnerabilities.
3. It is a command-line tool focused on mapping out network topologies and enumerating network resources.

Wireshark :

1. Wireshark is a network protocol analyzer.
2. Its primary purpose is to capture, analyze and troubleshoot network traffic.
3. It is a graphical user interface (GUI) tool that is more focused on in-depth analysis of network traffic.

2) Wireshark runs at the data link layer of OSI model.

3) Below are the names of 10 WireShark alternatives :
   - TCPdump
   - MicroSoft message analyzer
   - Tshark
   - Colasoft Capsa
   - Network Miner
   - Netwitness
   - Snort
   - Ntopng
   - Ettercap
   - EtherApe

Outcomes:

CO2. Enumerate the layers of the OSI model and TCP/IP model, their functions and Protocols

Conclusion (based on the Results and outcomes achieved):

In experiment 3, I learnt the importance of network data analysis for detecting and troubleshooting issues on the networks. I explored application layer protocols with packet analysis. I used Wireshark analyzer for doing all network operations.

References:

Books/ Journals/ Websites:

- Behrouz A Forouzan, "Data Communication and networking", Tata McGraw hill, India, 4th Edition
- http://www.wireshark.org
- Wireshark user manual.