WIRESHARK SNIFFER

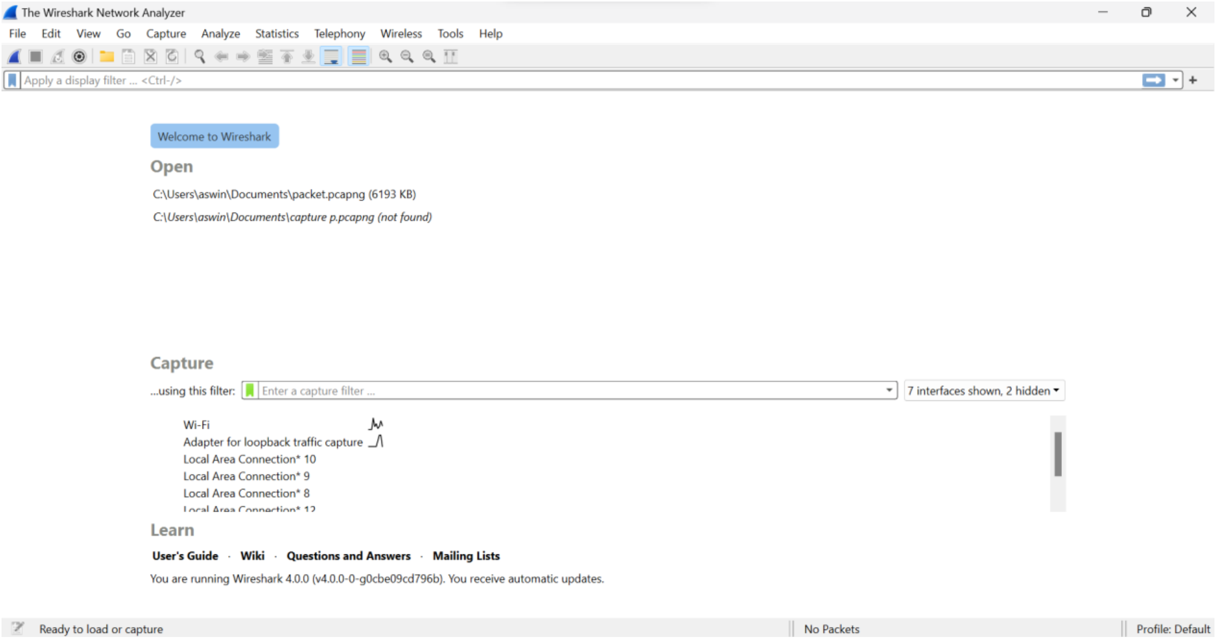
Aim :

- TO use WireShark sniffer tool to capture and analyse network traffic.

Procedure :

1. Install and open wireshark.
2. Connect to a network.
3. Open any website.
4. Now in the tool click on the connection type (Example wifi).
5. Now click on capture and start capturing the data.
6. We can filter the packets too in filter search bar.

Output :


The Wireshark Network Analyzer
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Open

C:\Users\aswin\Documents\packet.pcapng (6193 KB)

C:\Users\aswin\Documents\capture p.pcapng (not found)

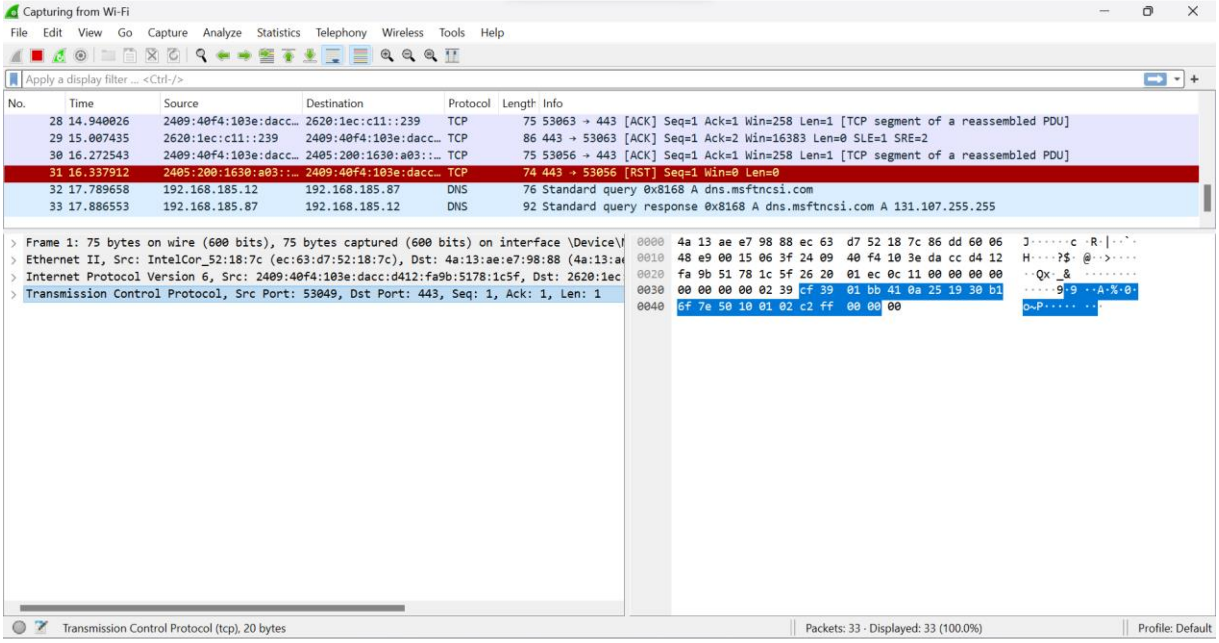
Capture
...using this filter:
Enter a capture filter ...
7 interfaces shown, 2 hidden

Wi-Fi
Adapter for loopback traffic capture
Local Area Connection* 10
Local Area Connection* 9
Local Area Connection* 8
Local Area Connection* 12

Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists

You are running Wireshark 4.0.0 (v4.0.0-0-g0cbe09cd796b). You receive automatic updates.

Ready to load or capture | No Packets | Profile: Default

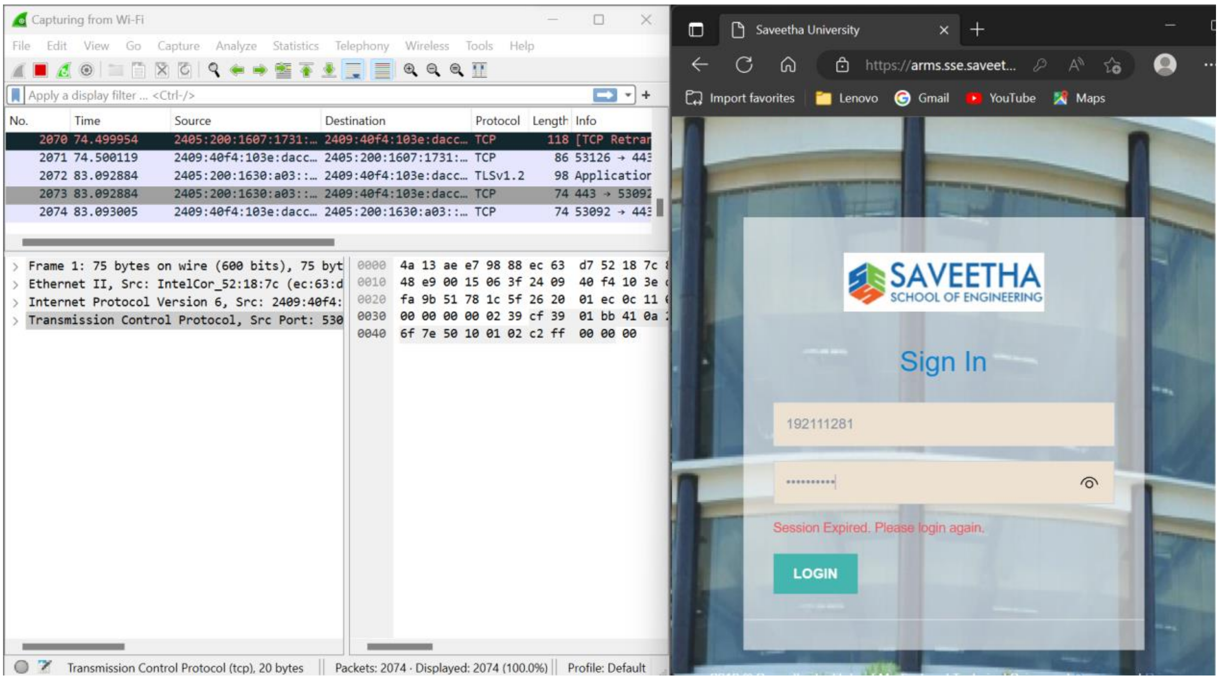

Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  Time       Source                Destination           Protocol Length Info
  28 14.940026  2409:40f4:103e:dacc…  2620:1ec:c11::239     TCP        75 53063 → 443 [ACK] Seq=1 Ack=1 Win=258 Len=1 [TCP segment of a reassembled PDU]
  29 15.007435  2620:1ec:c11::239     2409:40f4:103e:dacc…  TCP        86 443 → 53063 [ACK] Seq=1 Ack=2 Win=16383 Len=0 SLE=1 SRE=2
  30 16.272543  2409:40f4:103e:dacc…  2405:200:1630:a03::…  TCP        75 53056 → 443 [ACK] Seq=1 Ack=1 Win=258 Len=1 [TCP segment of a reassembled PDU]
  31 16.337912  2405:200:1630:a03::…  2409:40f4:103e:dacc…  TCP        74 443 → 53056 [RST] Seq=1 Win=0 Len=0
  32 17.789658  192.168.185.12        192.168.185.87        DNS        76 Standard query 0x8168 A dns.msftncsi.com
  33 17.886553  192.168.185.87        192.168.185.12        DNS        92 Standard query response 0x8168 A dns.msftncsi.com A 131.107.255.255
```

```
> Frame 1: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface \Device\I
> Ethernet II, Src: IntelCor_52:18:7c (ec:63:d7:52:18:7c), Dst: 4a:13:ae:e7:98:88 (4a:13:ae
> Internet Protocol Version 6, Src: 2409:40f4:103e:dacc:d412:fa9b:5178:1c5f, Dst: 2620:1ec
> Transmission Control Protocol, Src Port: 53049, Dst Port: 443, Seq: 1, Ack: 1, Len: 1
```

```
0000  4a 13 ae e7 98 88 ec 63  d7 52 18 7c 86 dd 60 06   J······c ·R·|··`·
0010  48 e9 00 15 06 3f 24 09  40 f4 10 3e da cc d4 12   H····?$· @··>····
0020  fa 9b 51 78 1c 5f 26 20  01 ec 0c 11 00 00 00 00   ··Qx·_&  ········
0030  00 00 00 00 02 39 cf 39  01 bb 41 0a 25 19 30 b1   ·····9·9 ··A·%·0·
0040  6f 7e 50 10 01 02 c2 ff  00 00 00                  o~P····· ···
```

Transmission Control Protocol (tcp), 20 bytes | Packets: 33 · Displayed: 33 (100.0%) | Profile: Default


Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  Time       Source                Destination           Protocol Length Info
2070 74.499954  2405:200:1607:1731:…  2409:40f4:103e:dacc…  TCP       118 [TCP Retrar
2071 74.500119  2409:40f4:103e:dacc…  2405:200:1607:1731:…  TCP        86 53126 → 443
2072 83.092884  2405:200:1630:a03::…  2409:40f4:103e:dacc…  TLSv1.2    98 Applicatior
2073 83.092884  2405:200:1630:a03::…  2409:40f4:103e:dacc…  TCP        74 443 → 53092
2074 83.093005  2409:40f4:103e:dacc…  2405:200:1630:a03::…  TCP        74 53092 → 443
```

```
> Frame 1: 75 bytes on wire (600 bits), 75 byt
> Ethernet II, Src: IntelCor_52:18:7c (ec:63:d
> Internet Protocol Version 6, Src: 2409:40f4:
> Transmission Control Protocol, Src Port: 530
```

```
0000  4a 13 ae e7 98 88 ec 63  d7 52 18 7c
0010  48 e9 00 15 06 3f 24 09  40 f4 10 3e
0020  fa 9b 51 78 1c 5f 26 20  01 ec 0c 11
0030  00 00 00 00 02 39 cf 39  01 bb 41 0a
0040  6f 7e 50 10 01 02 c2 ff  00 00 00
```

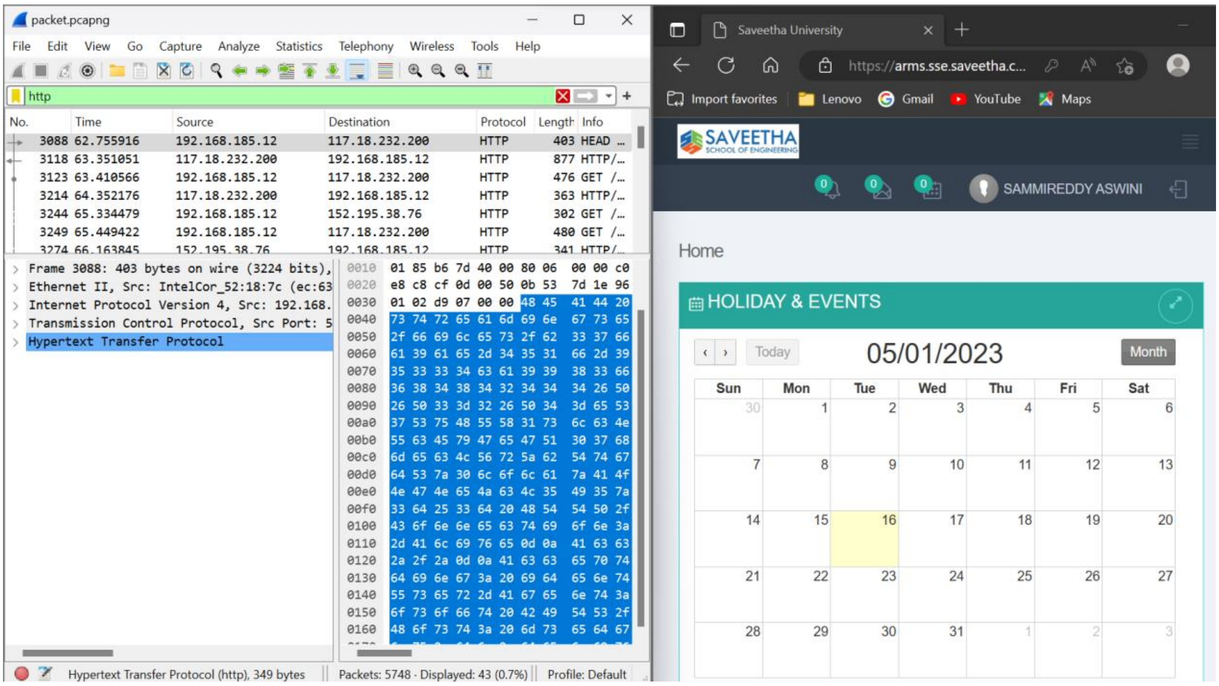
Transmission Control Protocol (tcp), 20 bytes | Packets: 2074 · Displayed: 2074 (100.0%) | Profile: Default

Sign In

192111281

••••••••••

Session Expired. Please login again.


packet.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Saveetha University
https://arms.sse.saveetha.c...
Import favorites
Lenovo
Gmail
YouTube
Maps
SAVEETHA SCHOOL OF ENGINEERING
SAMMIREDDY ASWINI
Home
HOLIDAY & EVENTS
Today
Month

```
No.    Time        Source           Destination      Protocol Length Info
  3088 62.755916   192.168.185.12   117.18.232.200   HTTP      403 HEAD …
  3118 63.351051   117.18.232.200   192.168.185.12   HTTP      877 HTTP/…
  3123 63.410566   192.168.185.12   117.18.232.200   HTTP      476 GET /…
  3214 64.352176   117.18.232.200   192.168.185.12   HTTP      363 HTTP/…
  3244 65.334479   192.168.185.12   152.195.38.76    HTTP      302 GET /…
  3249 65.449422   192.168.185.12   117.18.232.200   HTTP      480 GET /…
  3274 66.163845   152.195.38.76    192.168.185.12   HTTP      341 HTTP/…
```

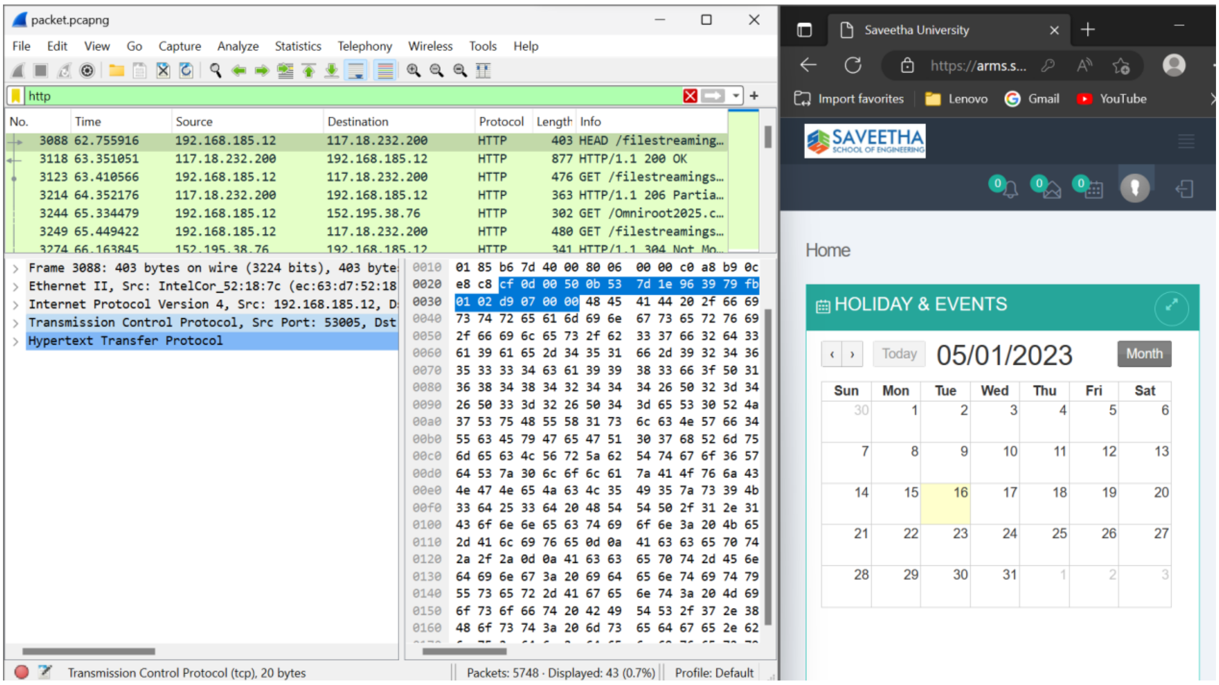
```
> Frame 3088: 403 bytes on wire (3224 bits),
> Ethernet II, Src: IntelCor_52:18:7c (ec:63
> Internet Protocol Version 4, Src: 192.168.
> Transmission Control Protocol, Src Port: 5
> Hypertext Transfer Protocol
```

```
0010  01 85 b6 7d 40 00 80 06  00 00 c0
0020  e8 c8 cf 0d 00 50 0b 53  7d 1e 96
0030  01 02 d9 07 00 00 48 45  41 44 20
0040  73 74 72 65 61 6d 69 6e  67 73 65
0050  2f 66 69 6c 65 73 2f 62  33 37 66
0060  61 39 61 65 2d 34 35 31  66 2d 39
0070  35 33 33 34 63 61 39 39  38 33 66
0080  36 38 34 38 34 32 34 34  34 26 50
0090  26 50 33 3d 32 26 50 34  3d 65 53
00a0  37 53 75 48 55 58 31 73  6c 63 4e
00b0  55 63 45 79 47 65 47 51  30 37 68
00c0  6d 65 63 4c 56 72 5a 62  54 74 67
00d0  64 53 7a 30 6c 6f 6c 61  7a 41 4f
00e0  4e 47 4e 65 4a 63 4c 35  49 35 7a
00f0  33 64 25 33 64 20 48 54  54 50 2f
0100  43 6f 6e 6e 65 63 74 69  6f 6e 3a
0110  2d 41 6c 69 76 65 0d 0a  41 63 63
0120  2a 2f 2a 0d 0a 41 63 63  65 70 74
0130  64 69 6e 67 3a 20 69 64  65 6e 74
0140  55 73 65 72 2d 41 67 65  6e 74 3a
0150  6f 73 6f 66 74 20 42 49  54 53 2f
0160  48 6f 73 74 3a 20 6d 73  65 64 67
```

```
Hypertext Transfer Protocol (http), 349 bytes || Packets: 5748 · Displayed: 43 (0.7%) || Profile: Default
```

05/01/2023

Sun	Mon	Tue	Wed	Thu	Fri	Sat
30	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31	1	2	3



```
No.    Time        Source           Destination      Protocol Length Info
  3088 62.755916   192.168.185.12   117.18.232.200   HTTP      403 HEAD /filestreaming…
  3118 63.351051   117.18.232.200   192.168.185.12   HTTP      877 HTTP/1.1 200 OK
  3123 63.410566   192.168.185.12   117.18.232.200   HTTP      476 GET /filestreamings…
  3214 64.352176   117.18.232.200   192.168.185.12   HTTP      363 HTTP/1.1 206 Partia…
  3244 65.334479   192.168.185.12   152.195.38.76    HTTP      302 GET /Omniroot2025.c…
  3249 65.449422   192.168.185.12   117.18.232.200   HTTP      480 GET /filestreamings…
  3274 66.163845   152.195.38.76    192.168.185.12   HTTP      341 HTTP/1.1 304 Not Mo…
```

```
> Frame 3088: 403 bytes on wire (3224 bits), 403 byte
> Ethernet II, Src: IntelCor_52:18:7c (ec:63:d7:52:18
> Internet Protocol Version 4, Src: 192.168.185.12, D
> Transmission Control Protocol, Src Port: 53005, Dst
> Hypertext Transfer Protocol
```

```
0010  01 85 b6 7d 40 00 80 06  00 00 c0 a8 b9 0c
0020  e8 c8 cf 0d 00 50 0b 53  7d 1e 96 39 79 fb
0030  01 02 d9 07 00 00 48 45  41 44 20 2f 66 69
0040  73 74 72 65 61 6d 69 6e  67 73 65 72 76 69
0050  2f 66 69 6c 65 73 2f 62  33 37 66 32 64 33
0060  61 39 61 65 2d 34 35 31  66 2d 39 32 34 36
0070  35 33 33 34 63 61 39 39  38 33 66 3f 50 31
0080  36 38 34 38 34 32 34 34  34 26 50 32 3d 34
0090  26 50 33 3d 32 26 50 34  3d 65 53 30 52 4a
00a0  37 53 75 48 55 58 31 73  6c 63 4e 57 66 34
00b0  55 63 45 79 47 65 47 51  30 37 68 52 6d 75
00c0  6d 65 63 4c 56 72 5a 62  54 74 67 6f 36 57
00d0  64 53 7a 30 6c 6f 6c 61  7a 41 4f 76 6a 43
00e0  4e 47 4e 65 4a 63 4c 35  49 35 7a 73 39 4b
00f0  33 64 25 33 64 20 48 54  54 50 2f 31 2e 31
0100  43 6f 6e 6e 65 63 74 69  6f 6e 3a 20 4b 65
0110  2d 41 6c 69 76 65 0d 0a  41 63 63 65 70 74
0120  2a 2f 2a 0d 0a 41 63 63  65 70 74 2d 45 6e
0130  64 69 6e 67 3a 20 69 64  65 6e 74 69 74 79
0140  55 73 65 72 2d 41 67 65  6e 74 3a 20 4d 69
0150  6f 73 6f 66 74 20 42 49  54 53 2f 37 2e 38
0160  48 6f 73 74 3a 20 6d 73  65 64 67 65 2e 62
```

```
Transmission Control Protocol (tcp), 20 bytes || Packets: 5748 · Displayed: 43 (0.7%) || Profile: Default
```

05/01/2023

Sun	Mon	Tue	Wed	Thu	Fri	Sat
30	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31	1	2	3

Result :

Hence using WireShark sniffer tool to capture and analyse network traffic is implemented successfully.