NAME : SATHYAPRAKASH SAHOO **CLASS** : BSC. TY. CS

ROLL NO : CS- 4124 **DIV** : 2 **BATCH** : C

SUBJECT : CYBER FORENSICS - PRACTICAL

PRACTICAL NO. 4

AIM : Capturing and analyzing network packets using Wireshark (Fundamentals)

1. Identification of live network.
2. Capture Packets.
3. Analyze the captured packets

STEPS : follow the below steps -

1. Download “Wireshark” (Windows 64 bit) and install it.

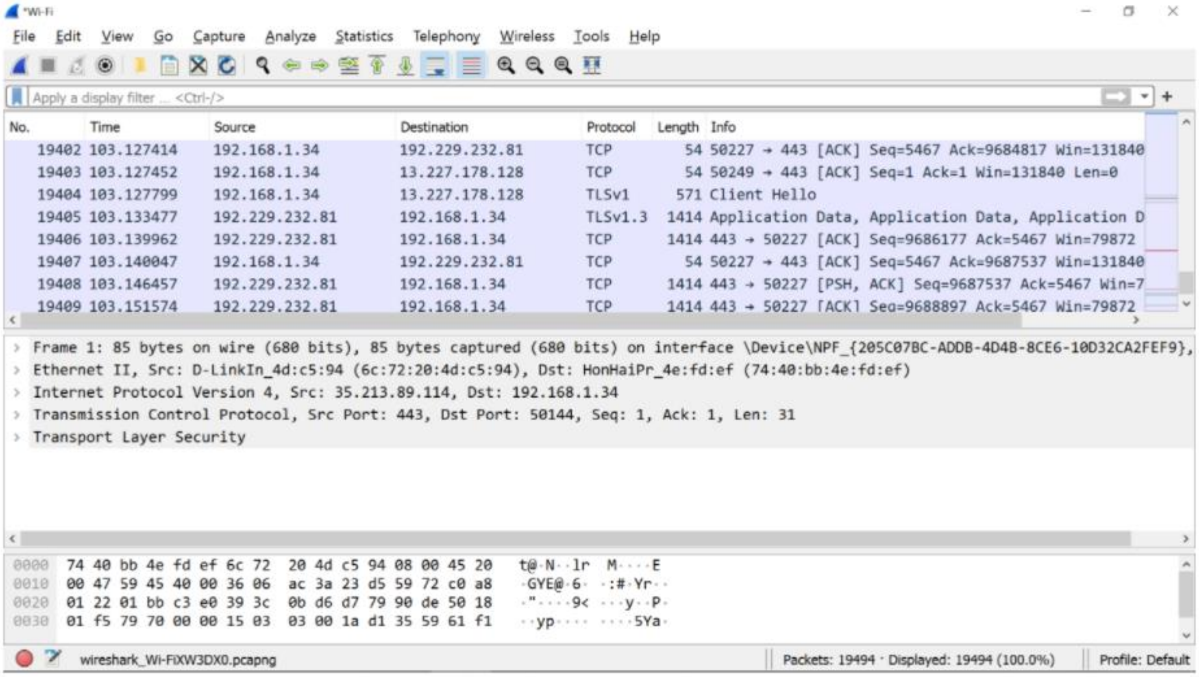
2. Open Wireshark. Select active connection for capturing.

3. Now open chrome and clear previous browsing history.

4. Now open a new tab and search for website (for e.g. cars).

5. Now open Wireshark and start capturing by clicking shark-fin iconon top left.

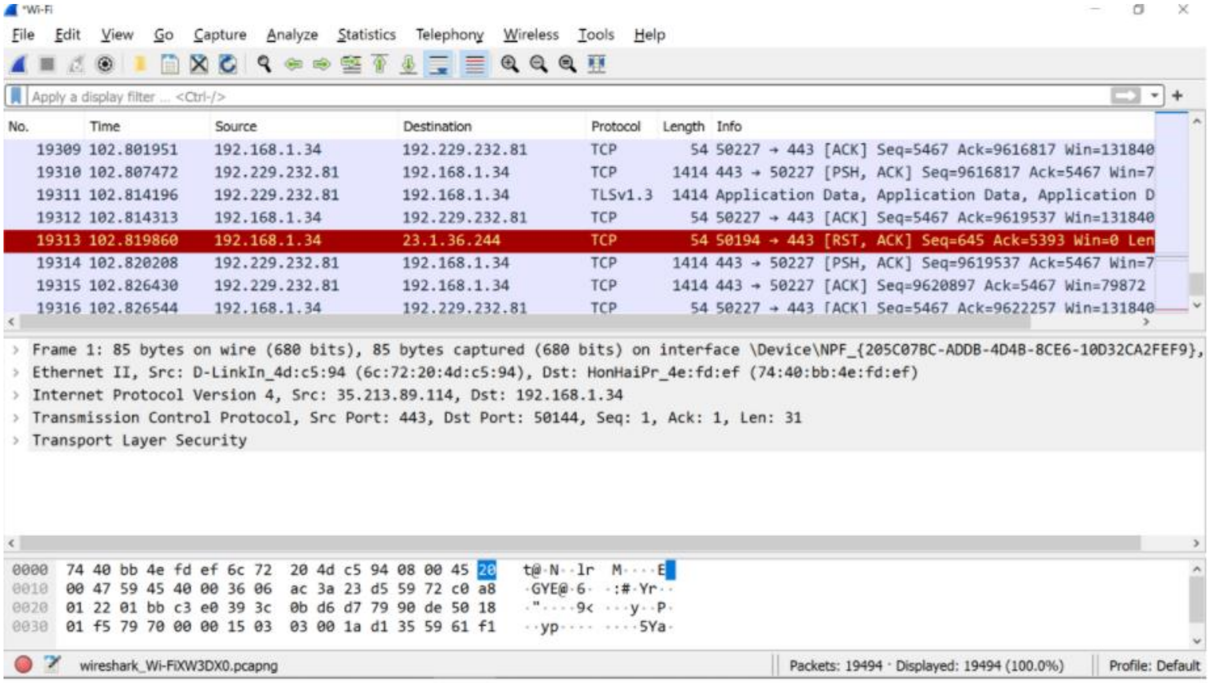
6. Now open website and browse website for sometime. Now stopcapturing. (To stop capturing click on the red square box next to shark-fin on top left).


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
wireshark_Wi-FiXW3DX0.pcapng
Packets: 19494 · Displayed: 19494 (100.0%)
Profile: Default

```
No.   Time       Source          Destination      Protocol Length Info
19402 103.127414 192.168.1.34    192.229.232.81   TCP        54 50227 → 443 [ACK] Seq=5467 Ack=9684817 Win=131840
19403 103.127452 192.168.1.34    13.227.178.128   TCP        54 50249 → 443 [ACK] Seq=1 Ack=1 Win=131840 Len=0
19404 103.127799 192.168.1.34    13.227.178.128   TLSv1     571 Client Hello
19405 103.133477 192.229.232.81  192.168.1.34     TLSv1.3  1414 Application Data, Application Data, Application D
19406 103.139962 192.229.232.81  192.168.1.34     TCP      1414 443 → 50227 [ACK] Seq=9686177 Ack=5467 Win=79872
19407 103.140047 192.168.1.34    192.229.232.81   TCP        54 50227 → 443 [ACK] Seq=5467 Ack=9687537 Win=131840
19408 103.146457 192.229.232.81  192.168.1.34     TCP      1414 443 → 50227 [PSH, ACK] Seq=9687537 Ack=5467 Win=7
19409 103.151574 192.229.232.81  192.168.1.34     TCP      1414 443 → 50227 [ACK] Seq=9688897 Ack=5467 Win=79872
```

```
> Frame 1: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface \Device\NPF_{205C07BC-ADDB-4D4B-8CE6-10D32CA2FEF9},
> Ethernet II, Src: D-LinkIn_4d:c5:94 (6c:72:20:4d:c5:94), Dst: HonHaiPr_4e:fd:ef (74:40:bb:4e:fd:ef)
> Internet Protocol Version 4, Src: 35.213.89.114, Dst: 192.168.1.34
> Transmission Control Protocol, Src Port: 443, Dst Port: 50144, Seq: 1, Ack: 1, Len: 31
> Transport Layer Security
```

```
0000  74 40 bb 4e fd ef 6c 72  20 4d c5 94 08 00 45 20   t@·N··lr M····E
0010  00 47 59 45 40 00 36 06  ac 3a 23 d5 59 72 c0 a8   ·GYE@·6· ·:#·Yr··
0020  01 22 01 bb c3 e0 39 3c  0b d6 d7 79 90 de 50 18   ·"····9< ···y··P·
0030  01 f5 79 70 00 00 15 03  03 00 1a d1 35 59 61 f1   ··yp···· ····5Ya·
```



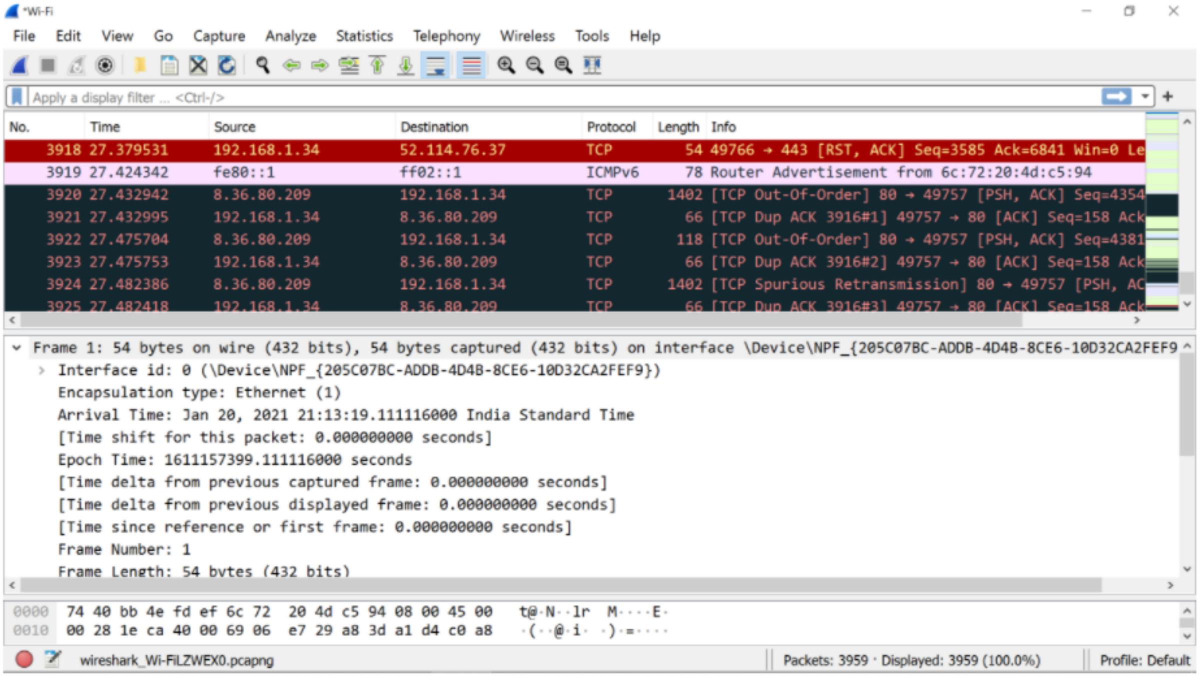
*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.    Time         Source            Destination       Protocol  Length Info
 19309 102.801951   192.168.1.34      192.229.232.81    TCP         54 50227 → 443 [ACK] Seq=5467 Ack=9616817 Win=131840
 19310 102.807472   192.229.232.81    192.168.1.34      TCP       1414 443 → 50227 [PSH, ACK] Seq=9616817 Ack=5467 Win=7
 19311 102.814196   192.229.232.81    192.168.1.34      TLSv1.3   1414 Application Data, Application Data, Application D
 19312 102.814313   192.168.1.34      192.229.232.81    TCP         54 50227 → 443 [ACK] Seq=5467 Ack=9619537 Win=131840
 19313 102.819860   192.168.1.34      23.1.36.244       TCP         54 50194 → 443 [RST, ACK] Seq=645 Ack=5393 Win=0 Len
 19314 102.820208   192.229.232.81    192.168.1.34      TCP       1414 443 → 50227 [PSH, ACK] Seq=9619537 Ack=5467 Win=7
 19315 102.826430   192.229.232.81    192.168.1.34      TCP       1414 443 → 50227 [ACK] Seq=9620897 Ack=5467 Win=79872
 19316 102.826544   192.168.1.34      192.229.232.81    TCP         54 50227 → 443 [ACK] Seq=5467 Ack=9622257 Win=131840
```

```
> Frame 1: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface \Device\NPF_{205C07BC-ADDB-4D4B-8CE6-10D32CA2FEF9},
> Ethernet II, Src: D-LinkIn_4d:c5:94 (6c:72:20:4d:c5:94), Dst: HonHaiPr_4e:fd:ef (74:40:bb:4e:fd:ef)
> Internet Protocol Version 4, Src: 35.213.89.114, Dst: 192.168.1.34
> Transmission Control Protocol, Src Port: 443, Dst Port: 50144, Seq: 1, Ack: 1, Len: 31
> Transport Layer Security
```

```
0000  74 40 bb 4e fd ef 6c 72  20 4d c5 94 08 00 45 20   t@·N··lr  M····E
0010  00 47 59 45 40 00 36 06  ac 3a 23 d5 59 72 c0 a8   ·GYE@·6· ·:#·Yr··
0020  01 22 01 bb c3 e0 39 3c  0b d6 d7 79 90 de 50 18   ·"····9< ···y··P·
0030  01 f5 79 70 00 00 15 03  03 00 1a d1 35 59 61 f1   ··yp···· ····5Ya·
```

wireshark_Wi-FiXW3DX0.pcapng | Packets: 19494 · Displayed: 19494 (100.0%) | Profile: Default



*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
 3918 27.379531   192.168.1.34    52.114.76.37    TCP         54 49766 → 443 [RST, ACK] Seq=3585 Ack=6841 Win=0 Le
 3919 27.424342   fe80::1         ff02::1         ICMPv6      78 Router Advertisement from 6c:72:20:4d:c5:94
 3920 27.432942   8.36.80.209     192.168.1.34    TCP       1402 [TCP Out-Of-Order] 80 → 49757 [PSH, ACK] Seq=4354
 3921 27.432995   192.168.1.34    8.36.80.209     TCP         66 [TCP Dup ACK 3916#1] 49757 → 80 [ACK] Seq=158 Ack
 3922 27.475704   8.36.80.209     192.168.1.34    TCP        118 [TCP Out-Of-Order] 80 → 49757 [PSH, ACK] Seq=4381
 3923 27.475753   192.168.1.34    8.36.80.209     TCP         66 [TCP Dup ACK 3916#2] 49757 → 80 [ACK] Seq=158 Ack
 3924 27.482386   8.36.80.209     192.168.1.34    TCP       1402 [TCP Spurious Retransmission] 80 → 49757 [PSH, AC
 3925 27.482418   192.168.1.34    8.36.80.209     TCP         66 [TCP Dup ACK 3916#3] 49757 → 80 [ACK] Seq=158 Ack
```

```
v Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{205C07BC-ADDB-4D4B-8CE6-10D32CA2FEF9
  > Interface id: 0 (\Device\NPF_{205C07BC-ADDB-4D4B-8CE6-10D32CA2FEF9})
    Encapsulation type: Ethernet (1)
    Arrival Time: Jan 20, 2021 21:13:19.111116000 India Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1611157399.111116000 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: 54 bytes (432 bits)
```

```
0000  74 40 bb 4e fd ef 6c 72  20 4d c5 94 08 00 45 00   t@·N··lr  M····E·
0010  00 28 1e ca 40 00 69 06  e7 29 a8 3d a1 d4 c0 a8   ·(··@·i· ·)·=····
```

wireshark_Wi-FiLZWEX0.pcapng | Packets: 3959 · Displayed: 3959 (100.0%) | Profile: Default