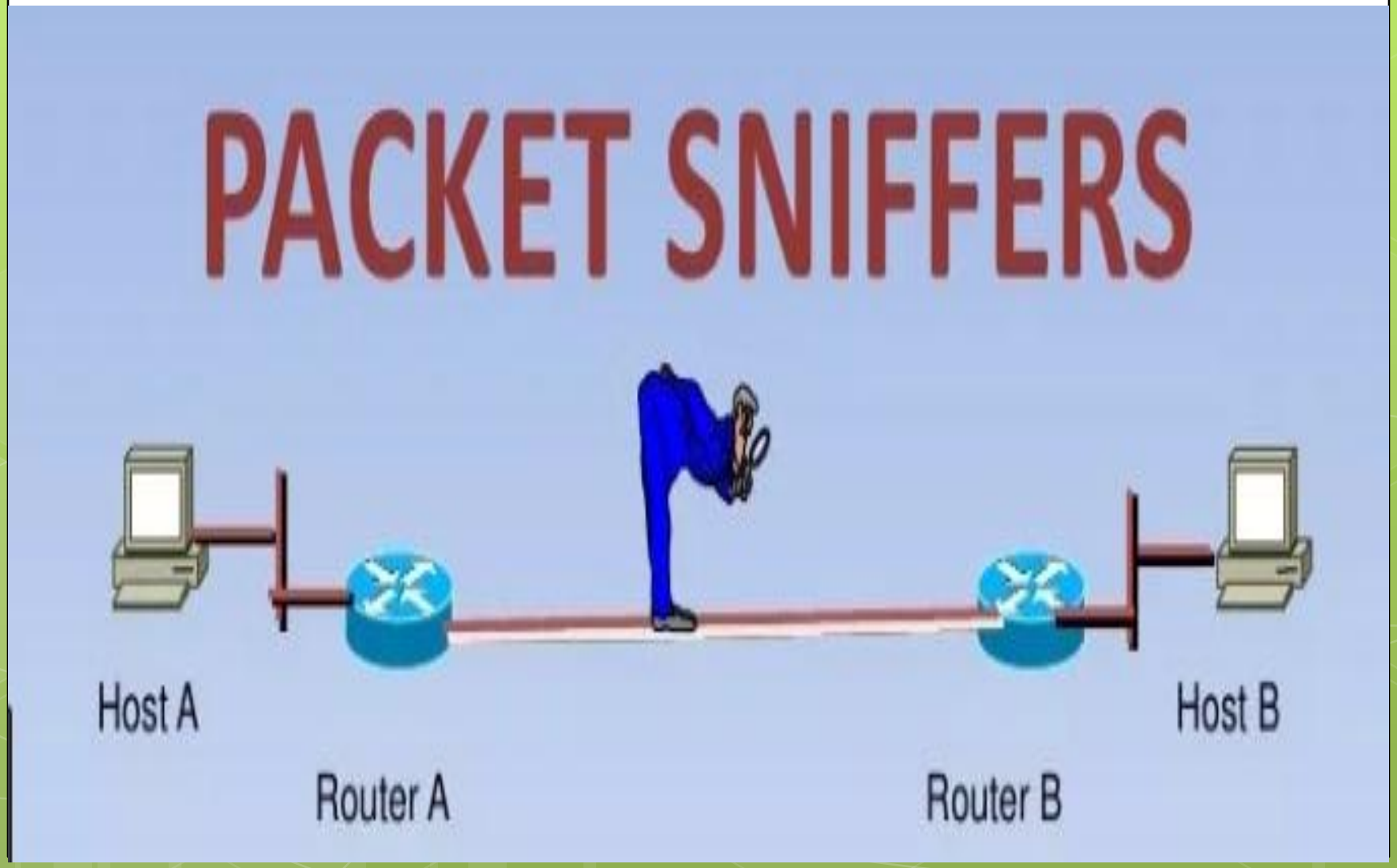
Introduction to Wireshark and Packet Sniffing

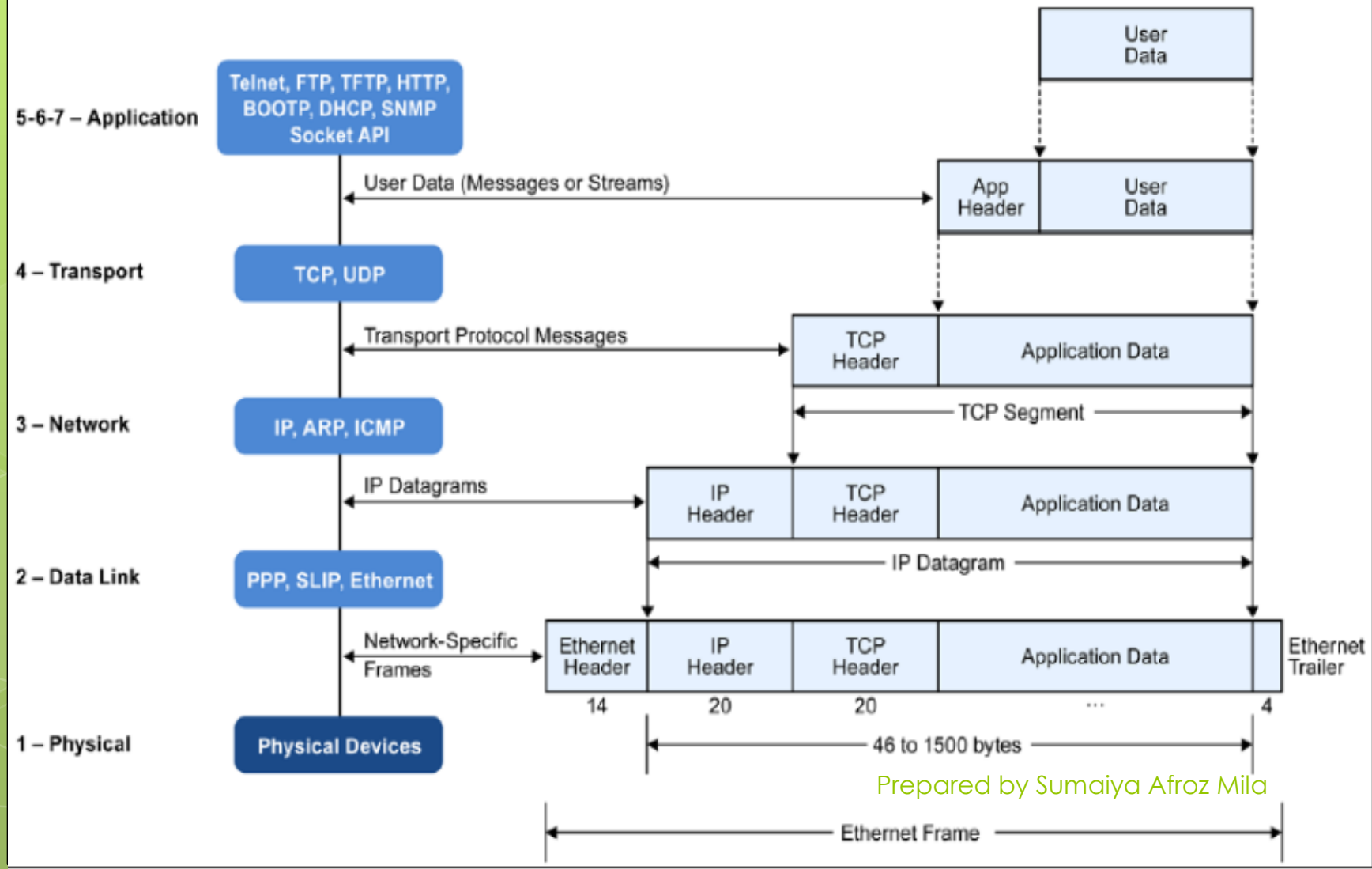
Packet Sniffer

- Captures packet being transferred within the network
- Stores and displays the contents of the fields in the captured packets
- Acts as passive device
- Observes the message being transmitted within the devices, but does not send message itself
- Consists of two parts-
  - Packet capture library – receives a copy of every link-layer frame sent/received by the device. Message sent by the upper layer protocol are encapsulated in link-layer frames.
  - Packet analyzer – displays the contents of the fields in the packet

Packet Sniffer



Encapsulation of data in TCP/IP Network



What is WireShark?

- A network protocol analyzer
- Captures network packets in real time and display them
- Similar to the software TCPdump
- Contains a few additional features of live capturing, coloring rules etc.
- Captures packets generally in the data link layer of OSI model

- WireShark download link - **https://www.wireshark.org/download.html**

https://www.wireshark.org/download.html

WIRESHARK

Download Wireshark

The current stable release of Wireshark is 2.0.1. It supersedes all previous releases.

Stable Release (2.0.1)

- Windows Installer (64-bit)
- Windows Installer (32-bit)
- Windows PortableApps® (32-bit)
- OS X 10.6 and later Intel 64-bit .dmg
- OS X 10.6 and later Intel 32-bit .dmg
- Source Code

Old Stable Release (1.12.9)

Documentation

Having Problems?

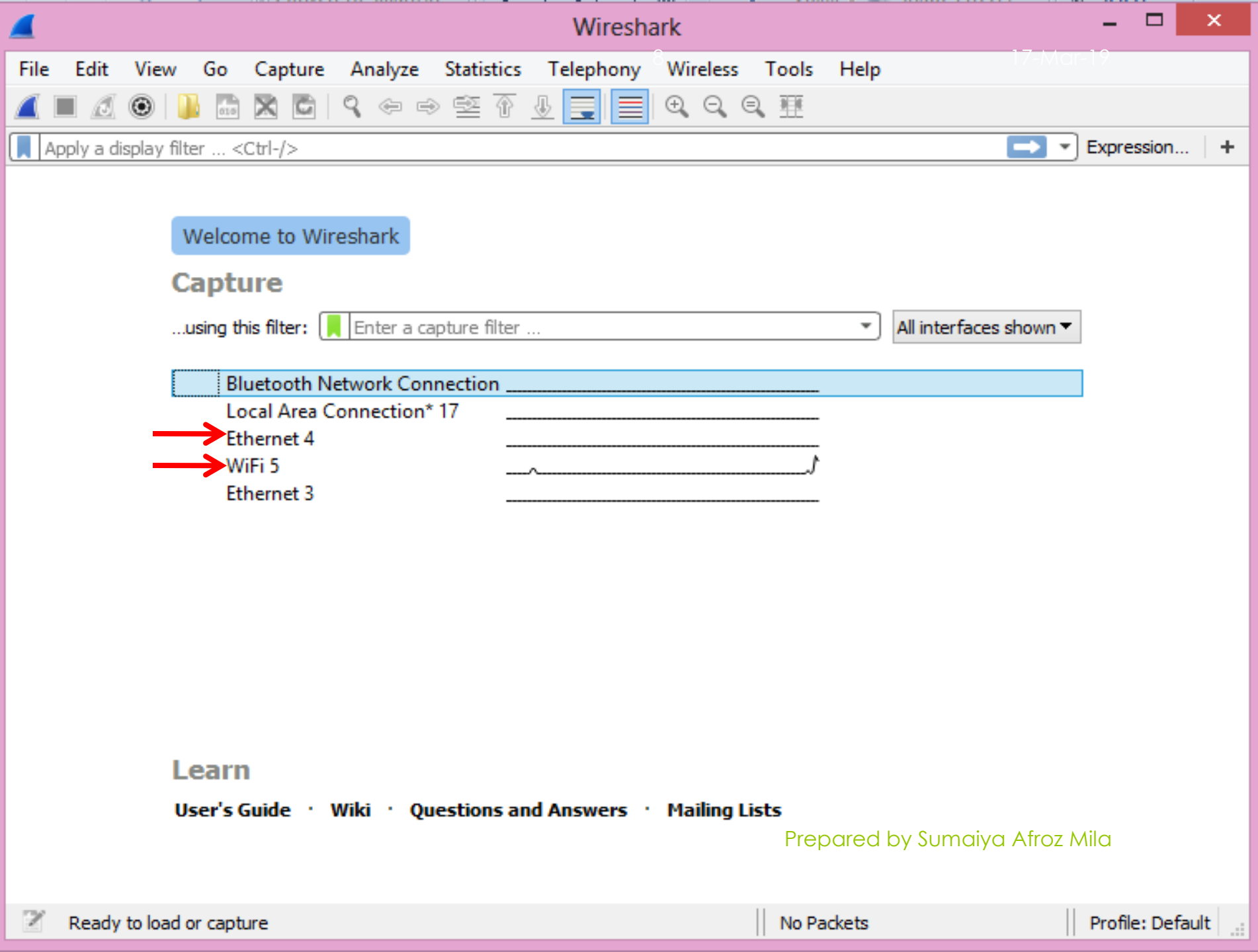
Packet Capture library tools -

- For Windows (wincap)
- For Linux (libcap)
- For wireless network (aircap)

- Wireshark has to be run as administrator to find the “aircap” library

Select interface –

- For laptop – select wifi interface
- For desktop – select ethernet interface



Prepared by Sumaiya Afroz Mila

Capturing from WiFi 5

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression... +

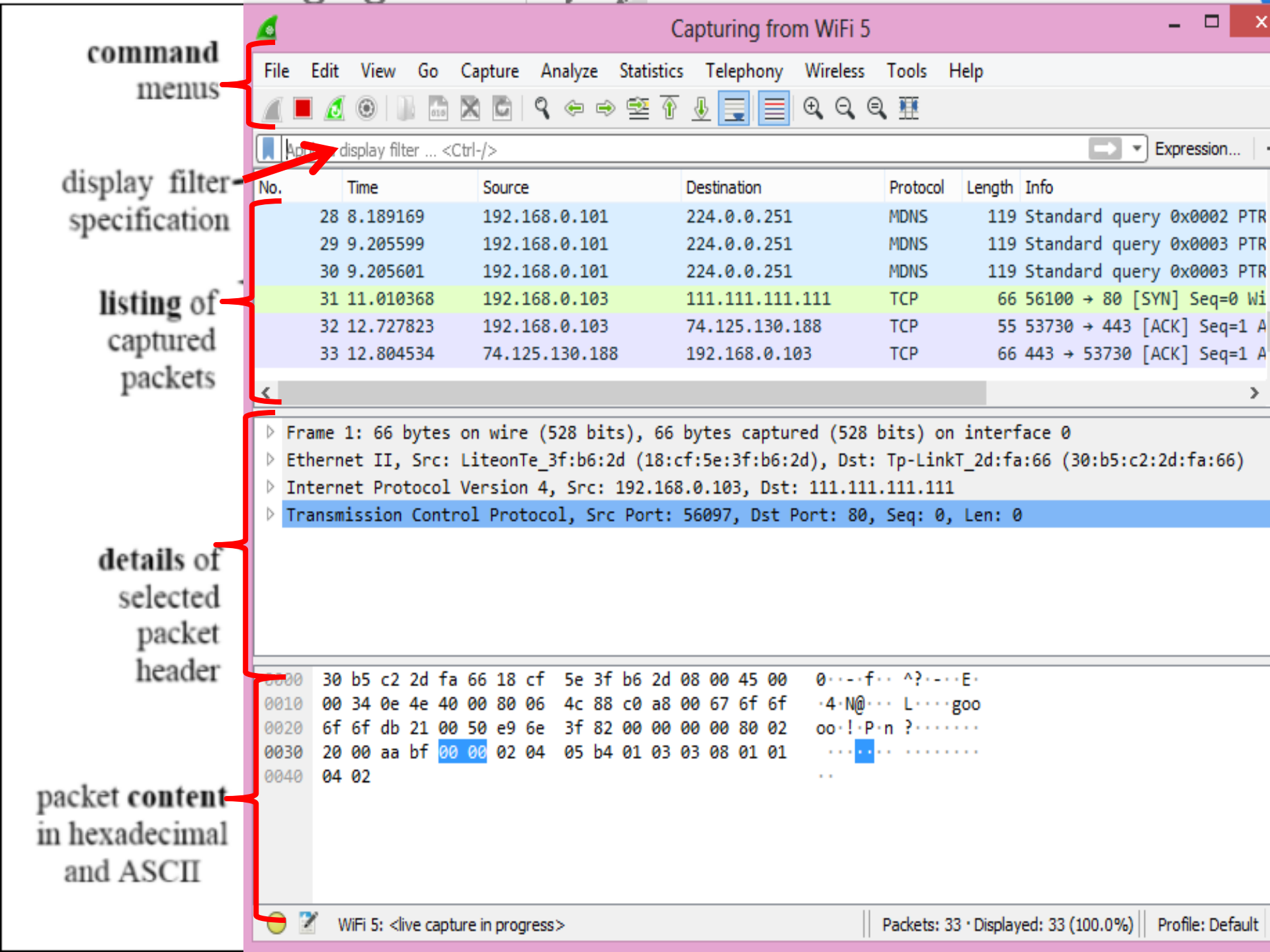
No.	Time	Source	Destination	Protocol	Length	Info
28	8.189169	192.168.0.101	224.0.0.251	MDNS	119	Standard query 0x0002 PTR
29	9.205599	192.168.0.101	224.0.0.251	MDNS	119	Standard query 0x0003 PTR
30	9.205601	192.168.0.101	224.0.0.251	MDNS	119	Standard query 0x0003 PTR
31	11.010368	192.168.0.103	111.111.111.111	TCP	66	56100 → 80 [SYN] Seq=0 Wi
32	12.727823	192.168.0.103	74.125.130.188	TCP	55	53730 → 443 [ACK] Seq=1 A
33	12.804534	74.125.130.188	192.168.0.103	TCP	66	443 → 53730 [ACK] Seq=1 A

```
▷ Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
▷ Ethernet II, Src: LiteonTe_3f:b6:2d (18:cf:5e:3f:b6:2d), Dst: Tp-LinkT_2d:fa:66 (30:b5:c2:2d:fa:66)
▷ Internet Protocol Version 4, Src: 192.168.0.103, Dst: 111.111.111.111
▷ Transmission Control Protocol, Src Port: 56097, Dst Port: 80, Seq: 0, Len: 0
```

```
0000  30 b5 c2 2d fa 66 18 cf  5e 3f b6 2d 08 00 45 00   0···-f·· ^?·-··E·
0010  00 34 0e 4e 40 00 80 06  4c 88 c0 a8 00 67 6f 6f   ·4·N@··· L····goo
0020  6f 6f db 21 00 50 e9 6e  3f 82 00 00 00 00 80 02   oo·!·P·n ?·····
0030  20 00 aa bf 00 00 02 04  05 b4 01 03 03 08 01 01    ····· ·····
0040  04 02                                              ··
```

Prepared by Sumaiya Afroz Mila

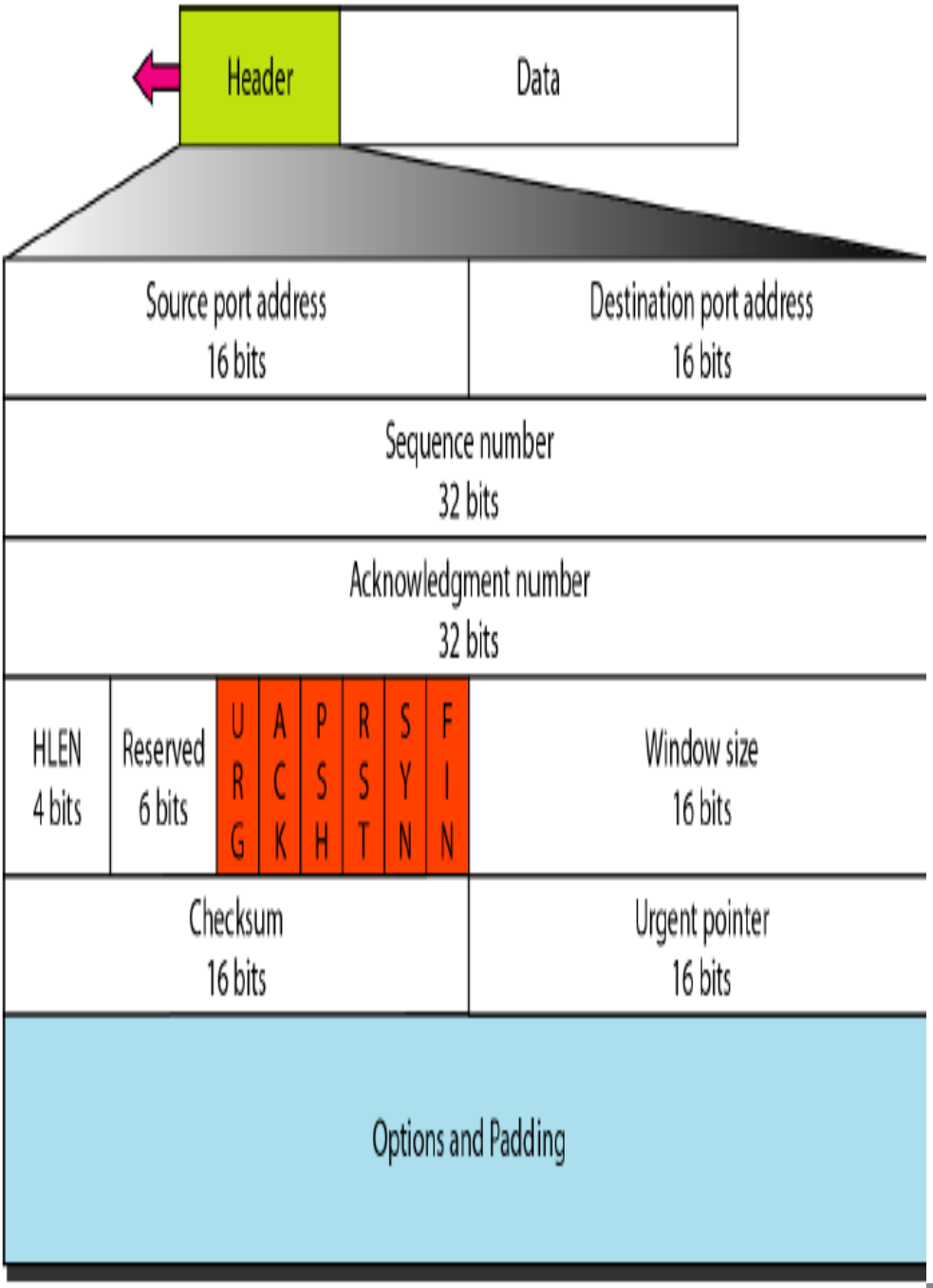
WiFi 5: <live capture in progress> | Packets: 33 · Displayed: 33 (100.0%) | Profile: Default


command menus
display filter specification
listing of captured packets
details of selected packet header
packet content in hexadecimal and ASCII
Capturing from WiFi 5
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
28 8.189169 192.168.0.101 224.0.0.251 MDNS 119 Standard query 0x0002 PTR
29 9.205599 192.168.0.101 224.0.0.251 MDNS 119 Standard query 0x0003 PTR
30 9.205601 192.168.0.101 224.0.0.251 MDNS 119 Standard query 0x0003 PTR
31 11.010368 192.168.0.103 111.111.111.111 TCP 66 56100 → 80 [SYN] Seq=0 Wi
32 12.727823 192.168.0.103 74.125.130.188 TCP 55 53730 → 443 [ACK] Seq=1 A
33 12.804534 74.125.130.188 192.168.0.103 TCP 66 443 → 53730 [ACK] Seq=1 A
Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
Ethernet II, Src: LiteonTe_3f:b6:2d (18:cf:5e:3f:b6:2d), Dst: Tp-LinkT_2d:fa:66 (30:b5:c2:2d:fa:66)
Internet Protocol Version 4, Src: 192.168.0.103, Dst: 111.111.111.111
Transmission Control Protocol, Src Port: 56097, Dst Port: 80, Seq: 0, Len: 0
0000 30 b5 c2 2d fa 66 18 cf 5e 3f b6 2d 08 00 45 00
0010 00 34 0e 4e 40 00 80 06 4c 88 c0 a8 00 67 6f 6f
0020 6f 6f db 21 00 50 e9 6e 3f 82 00 00 00 00 80 02
0030 20 00 aa bf 00 00 02 04 05 b4 01 03 03 08 01 01
0040 04 02
WiFi 5: <live capture in progress>
Packets: 33 · Displayed: 33 (100.0%)
Profile: Default

5 major components of wireshark interfacce-

- Command menue
- Display filter specification
- Packet listing window – displays one-line summary of the captured packets
- Packet-header detail window – provides detailed header info about the packet selected in the packet listing window
- Packet-content window – displays the entire content of the captured packet

Inspecting TCP packet header




```
▲ Transmission Control Protocol, Src Port: 57927, Dst Port: 80, Seq: 529,
    Source Port: 57927
    Destination Port: 80
    [Stream index: 40]
    [TCP Segment Len: 608]
    Sequence number: 529    (relative sequence number)
    [Next sequence number: 1137    (relative sequence number)]
    Acknowledgment number: 3492    (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
  ▷ Flags: 0x018 (PSH, ACK)
    Window size value: 258
    [Calculated window size: 66048]
    [Window size scaling factor: 256]
    Checksum: 0xa4b9 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  ▷ [SEQ/ACK analysis]
  ▷ [Timestamps]
```

Filtering IP address

- For filtering IP address , you have to know the IP of your device
- Go to - https://www.whatismyip.com/
- Select the local IP address

Filtering IP address

*WiFi 5

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr==192.168.0.102 Expression... +

No.	Time	Source	Destination	Protocol	Length	Info
9	3.820439	35.201.85.114	192.168.0.102	TLSv1.2	117	Application Data
10	3.820441	35.201.85.114	192.168.0.102	TCP	54	443 → 58205 [FIN, ACK] Se
11	3.821330	192.168.0.102	35.201.85.114	TCP	54	58205 → 443 [ACK] Seq=1 A
12	3.821837	192.168.0.102	35.201.85.114	TCP	54	58205 → 443 [FIN, ACK] Se
13	3.879382	35.201.85.114	192.168.0.102	TCP	54	443 → 58205 [ACK] Seq=65
14	3.998156	192.168.0.102	111.111.111.111	TCP	66	58341 → 80 [SYN] Seq=0 Wi
15	4.889320	192.168.0.102	172.217.163.162	TCP	55	58077 → 443 [ACK] Seq=1 A
16	4.928691	172.217.163.162	192.168.0.102	TCP	66	443 → 58077 [ACK] Seq=1 A
17	6.234719	172.217.166.110	192.168.0.102	TLSv1.2	117	Application Data
18	6.234721	172.217.166.110	192.168.0.102	TCP	54	443 → 58213 [FIN, ACK] Se
19	6.235645	192.168.0.102	172.217.166.110	TCP	54	58213 → 443 [ACK] Seq=1 A
20	6.236250	192.168.0.102	172.217.166.110	TCP	54	58213 → 443 [FIN, ACK] Se
21	6.281683	172.217.166.110	192.168.0.102	TCP	54	443 → 58213 [ACK] Seq=65
22	6.595457	192.168.0.102	185.86.139.29	TCP	55	58271 → 443 [ACK] Seq=1 A
23	6.858593	185.86.139.29	192.168.0.102	TCP	54	443 → 58271 [RST] Seq=1 W
24	7.005731	192.168.0.102	111.111.111.111	TCP	66	[TCP Retransmission] 5834

```
Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
Ethernet II, Src: LiteonTe_3f:b6:2d (18:cf:5e:3f:b6:2d), Dst: Tp-LinkT_2d:fa:66 (30:b5:c2:2d:fa:66)
Internet Protocol Version 4, Src: 192.168.0.102, Dst: 111.111.111.111
Transmission Control Protocol, Src Port: 58340, Dst Port: 80, Seq: 0, Len: 0
    Source Port: 58340
    Destination Port: 80
```

```
0000  30 b5 c2 2d fa 66 18 cf  5e 3f b6 2d 08 00 45 00   0···-f·· ^?·-··E·
```

wireshark_9816BE4F-2970-445D-9D6F-...A6F84_20190317123620_a17232.pcapng | Packets: 24 · Displayed: 24 (100.0%) | Profile: Default

Color Coding

*WiFi 5

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr==192.168.0.102 Expression...

No.	Time	Source	Destination	Protocol	Length	Info
9	3.820439	35.201.85.114	192.168.0.102	TLSv1.2	117	Application Data
10	3.820441	35.201.85.114	192.168.0.102	TCP	54	443 → 58205 [FIN, ACK] Se
11	3.821330	192.168.0.102	35.201.85.114	TCP	54	58205 → 443 [ACK] Seq=1 A
12	3.821837	192.168.0.102	35.201.85.114	TCP	54	58205 → 443 [FIN, ACK] Se
13	3.879382	35.201.85.114	192.168.0.102	TCP	54	443 → 58205 [ACK] Seq=65
14	3.998156	192.168.0.102	111.111.111.111	TCP	66	58341 → 80 [SYN] Seq=0 Wi
15	4.889320	192.168.0.102	172.217.163.162	TCP	55	58077 → 443 [ACK] Seq=1 A
16	4.928691	172.217.163.162	192.168.0.102	TCP	66	443 → 58077 [ACK] Seq=1 A
17	6.234719	172.217.166.110	192.168.0.102	TLSv1.2	117	Application Data
18	6.234721	172.217.166.110	192.168.0.102	TCP	54	443 → 58213 [FIN, ACK] Se
19	6.235645	192.168.0.102	172.217.166.110	TCP	54	58213 → 443 [ACK] Seq=1 A
20	6.236250	192.168.0.102	172.217.166.110	TCP	54	58213 → 443 [FIN, ACK] Se
21	6.281683	172.217.166.110	192.168.0.102	TCP	54	443 → 58213 [ACK] Seq=65
22	6.595457	192.168.0.102	185.86.139.29	TCP	55	58271 → 443 [ACK] Seq=1 A
23	6.858593	185.86.139.29	192.168.0.102	TCP	54	443 → 58271 [RST] Seq=1 W
24	7.005731	192.168.0.102	111.111.111.111	TCP	66	[TCP Retransmission] 5834

```
Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
Ethernet II, Src: LiteonTe_3f:b6:2d (18:cf:5e:3f:b6:2d), Dst: Tp-LinkT_2d:fa:66 (30:b5:c2:2d:fa:66)
Internet Protocol Version 4, Src: 192.168.0.102, Dst: 111.111.111.111
Transmission Control Protocol, Src Port: 58340, Dst Port: 80, Seq: 0, Len: 0
    Source Port: 58340
    Destination Port: 80
```

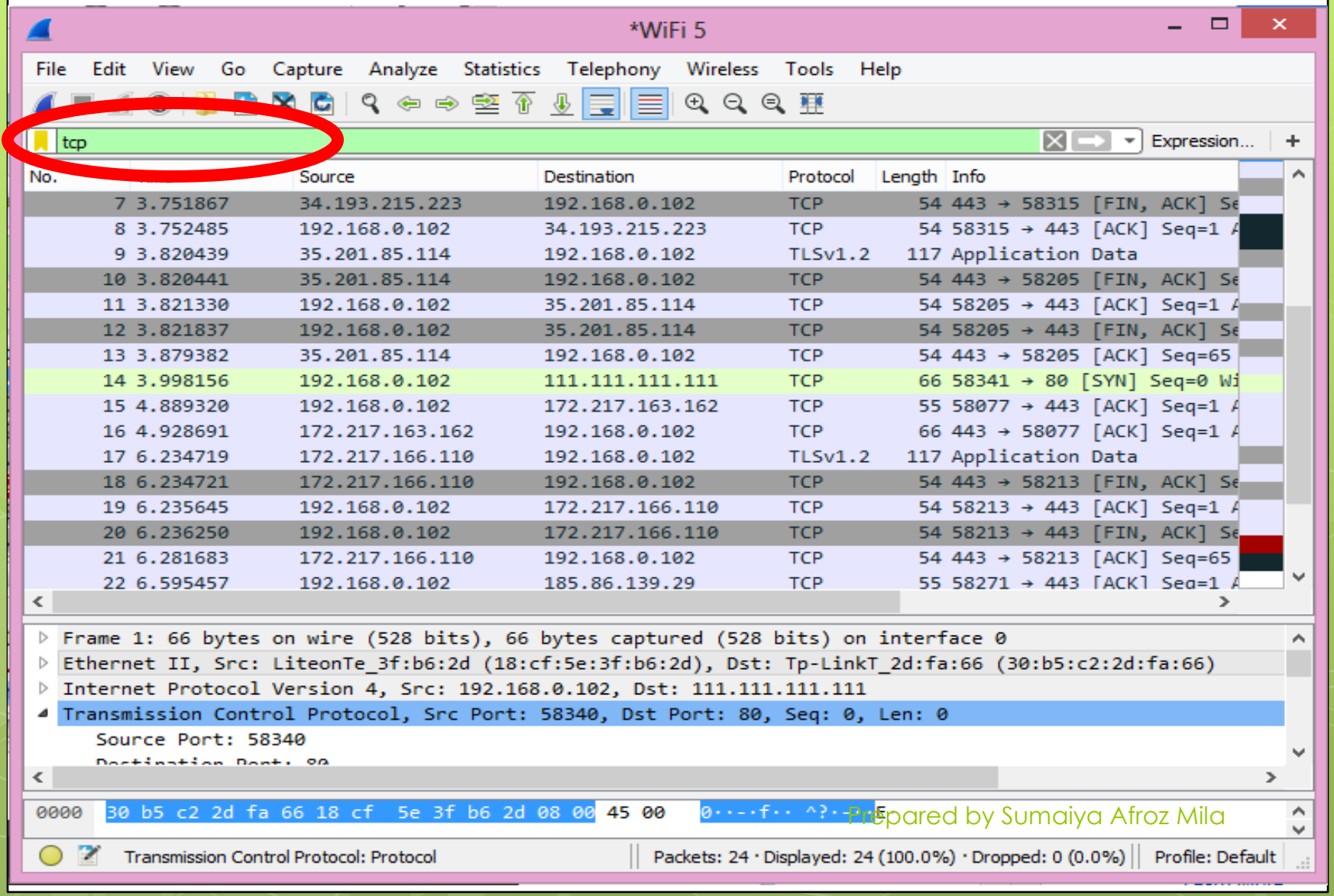
```
0000  30 b5 c2 2d fa 66 18 cf  5e 3f b6 2d 08 00 45 00   0···-f·· ^?·-··E·
```

wireshark_9816BE4F-2970-445D-9D6F-...A6F84_20190317123620_a17232.pcapng | Packets: 24 · Displayed: 24 (100.0%) | Profile: Default

Color Coding

- Uses color to help the users identify the types of traffic at a glance
- View > Coloring rules
- By default –
  - **Green** or **light purple** for TCP
  - **Red** for TCP RST
  - **Dark Blue** for DNS
  - **Light Blue** for UDP
  - **Black** indicates packets with problems or errors

Filtering TCP protocol



Filtering TCP port

Capturing from WiFi 5

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.port == 80 Expression... +

No.	Time	Source	Destination	Protocol	Length	Info
381	14.631649	103.120.39.46	192.168.0.102	TCP	1434	80 → 58444 [ACK] Seq=33121 Ac
382	14.635444	103.120.39.46	192.168.0.102	TCP	1434	80 → 58444 [ACK] Seq=34501 Ac
383	14.635445	103.120.39.46	192.168.0.102	TCP	1434	80 → 58444 [ACK] Seq=35881 Ac
384	14.635447	103.120.39.46	192.168.0.102	TCP	1434	80 → 58444 [ACK] Seq=37261 Ac
385	14.635447	103.120.39.46	192.168.0.102	TCP	1434	80 → 58444 [ACK] Seq=38641 Ac
386	14.635447	103.120.39.46	192.168.0.102	TCP	1434	80 → 58444 [ACK] Seq=40021 Ac
387	14.635448	103.120.39.46	192.168.0.102	TCP	1434	80 → 58444 [ACK] Seq=41401 Ac
388	14.635448	103.120.39.46	192.168.0.102	TCP	1434	80 → 58444 [ACK] Seq=42781 Ac
389	14.635449	103.120.39.46	192.168.0.102	TCP	1434	80 → 58444 [ACK] Seq=44161 Ac
390	14.635449	103.120.39.46	192.168.0.102	TCP	1434	80 → 58444 [ACK] Seq=45541 Ac
391	14.635449	103.120.39.46	192.168.0.102	TCP	1434	80 → 58444 [ACK] Seq=46921 Ac
392	14.635450	103.120.39.46	192.168.0.102	TCP	1434	80 → 58444 [ACK] Seq=48301 Ac
393	14.635451	103.120.39.46	192.168.0.102	TCP	1434	80 → 58444 [ACK] Seq=49681 Ac

```
▷ Frame 383: 1434 bytes on wire (11472 bits), 1434 bytes captured (11472 bits) on interface 0
▷ Ethernet II, Src: Tp-LinkT_2d:fa:66 (30:b5:c2:2d:fa:66), Dst: LiteonTe_3f:b6:2d (18:cf:5e:3f:b6:2d)
▷ Internet Protocol Version 4, Src: 103.120.39.46, Dst: 192.168.0.102
◢ Transmission Control Protocol, Src Port: 80, Dst Port: 58444, Seq: 35881, Ack: 650, Len: 1380
    Source Port: 80
    Destination Port: 58444
    [Stream index: 21]
    [TCP Segment Len: 1380]
    Sequence number: 35881    (relative sequence number)
```

Prepared by Sumaiya Afroz Mila

```
0000  18 cf 5e 3f b6 2d 30 b5  c2 2d fa 66 08 00 45 00   ··^?·-0· ·-·f··E·
```

Ethernet (eth), 14 bytes | Packets: 989 · Displayed: 362 (36.6%) | Profile: Default

Capturing ICMP packets

- Open the command prompt
- Ping to any ip address
- We will ping to google.com
- Filter by “icmp” in wireshark and see the packet-listing window
- Try using “ http://172.217.31.206 ” in the browser and see what happens

Capturing ICMP packets

Command Prompt

```
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Users\User>ping google.com

Pinging google.com [172.217.31.206] with 32 bytes of data:
Reply from 172.217.31.206: bytes=32 time=45ms TTL=53
Reply from 172.217.31.206: bytes=32 time=49ms TTL=53
Reply from 172.217.31.206: bytes=32 time=44ms TTL=53
Reply from 172.217.31.206: bytes=32 time=46ms TTL=53

Ping statistics for 172.217.31.206:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 44ms, Maximum = 49ms, Average = 46ms

C:\Users\User>
```

Capturing ICMP packets

*WiFi 5

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp Expression... +

No.	Time	Source	Destination	Protocol	Length	Info
11338	1496.214749	192.168.0.102	172.217.166.110	ICMP	74	Echo (ping) request id=0x000
11339	1496.252424	172.217.166.110	192.168.0.102	ICMP	74	Echo (ping) reply id=0x000
11345	1497.222872	192.168.0.102	172.217.166.110	ICMP	74	Echo (ping) request id=0x000
11346	1497.258596	172.217.166.110	192.168.0.102	ICMP	74	Echo (ping) reply id=0x000
11370	1498.230784	192.168.0.102	172.217.166.110	ICMP	74	Echo (ping) request id=0x000
11371	1498.264769	172.217.166.110	192.168.0.102	ICMP	74	Echo (ping) reply id=0x000
11391	1499.238254	192.168.0.102	172.217.166.110	ICMP	74	Echo (ping) request id=0x000
11392	1499.272069	172.217.166.110	192.168.0.102	ICMP	74	Echo (ping) reply id=0x000
15991	1595.309474	192.168.0.102	172.217.166.110	ICMP	74	Echo (ping) request id=0x000
15992	1595.344208	172.217.166.110	192.168.0.102	ICMP	74	Echo (ping) reply id=0x000
15993	1596.314061	192.168.0.102	172.217.166.110	ICMP	74	Echo (ping) request id=0x000
15994	1596.348436	172.217.166.110	192.168.0.102	ICMP	74	Echo (ping) reply id=0x000
15995	1597.320787	192.168.0.102	172.217.166.110	ICMP	74	Echo (ping) request id=0x000

Password Sniffing

Password sniffing

- Open **http://mcam.mist.ac.bd/Security/Login.aspx** in a browser
- Login with userID and Password
- Filter by “tcp contains mist” in wireshark and see the packet-listing window
- Right click on a packet > Follow > TCP Stream

*WiFi 5

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp contains mist

Expression...

No.	Time	Source	Destination	Protocol	Length	Info
131	9.887429	103.120.39.46	192.168.0.102	TCP	1434	80 → 59584 [ACK] Seq=9203
132	9.887431	103.120.39.46	192.168.0.102	TCP	1434	80 → 59584 [ACK] Seq=9341
133	9.887432	103.120.39.46	192.168.0.102	TCP	1434	80 → 59584 [ACK] Seq=9479
134	9.887436	103.120.39.46	192.168.0.102	TCP	1434	80 → 59584 [ACK] Seq=9617
135	9.887437	103.120.39.46	192.168.0.102	HTTP	383	HTTP/1.1 200 OK (text/ht
136	9.887831	192.168.0.102	103.120.39.46	TCP	54	59584 → 80 [ACK] Seq=2369
137	9.960370	192.168.0.102	103.120.39.46	HTTP	667	GET /WebResource.axd?d=aj
138	9.960666	192.168.0.102	103.120.39.46	HTTP	703	GET /ScriptResource.axd?d
139	9.961478	192.168.0.102	103.120.39.46	HTTP	703	GET /ScriptResource.axd?d
140	9.961492	192.168.0.102	103.120.39.46	HTTP	558	GET /Security/~/Assets/Sc
141	9.961666	192.168.0.102	103.120.39.46	HTTP	703	GET /ScriptResource.axd?d
142	9.971830	192.168.0.102	103.120.39.46	HTTP	703	GET /WebResource.axd?d=Uc

```
Destination Port: 80
[Stream index: 4]
[TCP Segment Len: 613]
Sequence number: 2369    (relative sequence number)
```

```
0020  27 2e e8 c0 00 50 9a 3c  b3 c0 27 2b 5f 0b 50 18   '.···P·< ··'+_·P·
0030  07 2e 05 dd 00 00 47 45  54 20 2f 57 65 62 52 65   ·.····GE T /WebRe
0040  73 6f 75 72 63 65 2e 61  78 64 3f 64 3d 61 6a 50   source.a xd?d=ajP
0050  45 4b 32 6a 5f 50 4f 50  77 6b 73 78 52 51 6a 32   EK2j_POP wksxRQj2
0060  6d 50 56 41 6b 4b 66 67  37 6d 63 63 6f 63 67 6b   mPVAkKfg 7mccocgk
0070  51 49 51 54 68 46 75 64  69 32 63 67 61 74 39 44   QIQThFud i2cgat9D
0080  54 42 48 4f 64 55 38 6e  66 49 45 6a 51 4c 50 77   TBHOdU8n fIEjQLPw
0090  6f 59 33 7a 67 41 30 39  50 5a 34 6b 57 61 6d 42   oY3zgA09 PZ4kWamB
```

Sequence number (tcp.seq), 4 bytes | Packets: 283 · Displayed: 275 (97.2%) · Dropped: 0 (0.0%) | Profile: Default

Wireshark · Follow TCP Stream (tcp.stream eq 4) · WiFi 5

```
Content-Length: 446
Origin: http://mcam.mist.ac.bd
X-Requested-With: XMLHttpRequest
Cache-Control: no-cache
X-MicrosoftAjax: Delta=true
User-Agent: Mozilla/5.0 (Windows NT 6.2; Win64; x64) AppleWebKit/
537.36 (KHTML, like Gecko) Chrome/73.0.3683.75 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept: */*
Referer: http://mcam.mist.ac.bd/Security/Login.aspx
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: _ga=GA1.3.1149737562.1494482277;
_gid=GA1.3.1094598181.1552749964;
ASP.NET_SessionId=zbjbmqhabmoqplnzyp5jtu05

scMgtMas=upMain%7ClogMain
%24Button1&__EVENTTARGET=&__EVENTARGUMENT=&__VIEWSTATE=
%2FwEPDwUJOTQ2NDg1OTI1ZGTGwjfKPb71bk0lFTNDmimoj1XqIsbOtv8Ya6jBEmIOXg
%3D%3D&__VIEWSTATEGENERATOR=A0A15FC2&__EVENTVALIDATION=
%2FwEdAARLE3w5a5vqRiWgDdpia7MeipYqga6QAg6YjmwFJTffRWnYJAscem4cjcZwrPhG
%2Bu6M%3D&logMain%24UserName=201514021&logMain
%24Password=1234&__ASYNCPOST=true&logMain%24Button1=Log%20InHTTP/1.1
Cache-Control: no-cache
Pragma: no-cache
Content-Type: text/plain; charset=utf-8
```

4 client pkts, 78 server pkts, 7 turns.

Entire conversation (107 kB) | Show and save data as ASCII | Stream 4

Find: | Find Next

Filter Out This Stream | Print | Save as... | Back | Close | Help