

Name: Muhammad Fahad
ID: FA19-BSSE-0014
Section: BM

Lab Task 3

- Filter 1
 - (ip.addr == 192.168.10.3)

The screenshot shows the Wireshark interface with the filter `ip.addr == 192.168.10.3` applied. The packet list displays several packets, with packet 126 selected. The packet details pane shows the following information:

- Frame 126: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface \Device\NPF_{A01953B1-EFD5-4186-BBC2-73B189E20617}, id 0
- Ethernet II, Src: ba:b5:f3:5d:03:5e (ba:b5:f3:5d:03:5e), Dst: TendaTec_Bc:30:f0 (c8:3a:35:8c:30:f0)
- Internet Protocol Version 4, Src: 192.168.10.3, Dst: 192.168.10.1
- User Datagram Protocol, Src Port: 59699, Dst Port: 53
- Domain Name System (query)

The packet bytes pane shows the raw data in hexadecimal and ASCII:

```
0000 c8 3a 35 8c 30 f0 ba b5 f3 5d 03 5e 00 00 45 00 :5 0 ... } ^ ^ E
0010 00 3d 58 03 00 00 80 11 4d 58 c0 a8 0a 03 c0 a8 =X ... M .....
0020 0a 01 e9 33 00 35 00 29 2f a1 b2 3f 01 00 00 01 ...3 5 ) / - ? ....
0030 00 00 00 00 00 04 6a 6f 74 65 06 79 6f 75 64 .....n ote youd
0040 61 6f 03 63 6f 6d 00 00 01 00 01                ao com .....
```

Name: Muhammad Fahad
ID: FA19-BSSE-0014
Section: BM

- Filter 2
 - (ip.src == 192.168.10.3)

The image shows a Wireshark network traffic capture. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains various icons for packet capture and analysis. The filter bar at the top shows the active filter: `ip.src == 192.168.10.3`. The packet list pane displays a table of captured packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. The selected packet is No. 70, a TCP segment from 192.168.10.3 to 192.168.10.1, with a sequence number of 62577 and a length of 443 bytes. The packet details pane shows the structure of the selected packet: Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Domain Name System (query). The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
38	3.166231	192.168.10.3	142.250.181.42	UDP	75	63914 → 443 Len=33
40	4.981900	192.168.10.3	142.250.181.42	UDP	75	63914 → 443 Len=33
43	6.257349	192.168.10.3	168.119.150.210	TCP	54	[TCP ACKed unseen segment] 58627 → 443 [ACK] Seq=1 Ack=2 Win=513 Len=0
44	6.785355	192.168.10.3	40.77.226.250	TCP	66	57363 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
46	7.063321	192.168.10.3	40.77.226.250	TCP	54	57363 → 443 [ACK] Seq=1 Ack=1 Win=131840 Len=0
47	7.063640	192.168.10.3	40.77.226.250	TLSv1.2	571	Client Hello
48	7.241668	192.168.10.3	13.67.9.5	TCP	54	58288 → 443 [FIN, ACK] Seq=1 Ack=1 Win=517 Len=0
52	7.271935	192.168.10.3	40.77.226.250	TCP	54	57363 → 443 [ACK] Seq=518 Ack=3896 Win=131840 Len=0
53	7.273106	192.168.10.3	40.77.226.250	TLSv1.2	147	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
55	7.586726	192.168.10.3	40.77.226.250	TCP	1474	57363 → 443 [ACK] Seq=611 Ack=3947 Win=131840 Len=1420 [TCP segment of a reassembled PDU]
56	7.586726	192.168.10.3	40.77.226.250	TLSv1.2	598	Application Data
60	7.883819	192.168.10.3	40.77.226.250	TCP	54	57363 → 443 [ACK] Seq=2575 Ack=4262 Win=131584 Len=0
62	7.883663	192.168.10.3	40.77.226.250	TLSv1.2	85	Encrypted Alert
63	7.883764	192.168.10.3	40.77.226.250	TCP	54	57363 → 443 [FIN, ACK] Seq=2606 Ack=4262 Win=131584 Len=0
65	8.434638	192.168.10.3	142.250.181.42	UDP	75	63914 → 443 Len=33
68	12.083455	192.168.10.3	178.62.253.213	TCP	54	62577 → 443 [FIN, ACK] Seq=1 Ack=40 Win=16607 Len=0
70	12.084787	192.168.10.3	178.62.253.213	TCP	54	62577 → 443 [RST, ACK] Seq=2 Ack=64 Win=0 Len=0

Frame 70: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface \Device\NPF... (08:00:00:00:00:00), id 0

Ethernet II, Src: ba:b5:f3:5d:03:5e (ba:b5:f3:5d:03:5e), Dst: TendaTec_Bc:30:f0 (c8:3a:35:8c:30:f0)

Internet Protocol Version 4, Src: 192.168.10.3, Dst: 192.168.10.1

User Datagram Protocol, Src Port: 59699, Dst Port: 53

Domain Name System (query)

0000 c8 3a 35 8c 30 f0 ba b5 f3 5d 03 5e 00 00 45 00 :5 0 ...] ^ . E

0010 00 3d 58 03 00 00 00 11 4d 58 c9 a8 0a 03 c0 a8 :X ... MX ...

0020 0a 01 e9 33 00 35 00 29 2f a1 b2 3f 01 00 00 01 :3 5 ... / - ? ...

0030 00 00 00 00 00 00 04 6e 6f 74 65 06 79 6f 75 64 : ... n ote youd

0040 61 6f 03 63 6f 6d 00 00 01 00 01 ao com ...

Name: Muhammad Fahad
ID: FA19-BSSE-0014
Section: BM

- Filter 3
 - (ip.dst==192.168.10.3)

The screenshot shows the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains various icons for file operations, packet selection, and analysis. The packet list pane on the left shows a list of captured packets, with the filter 'ip.dst==192.168.10.3' applied. The packet details pane on the right shows the structure of the selected packet (No. 127), including Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Data. The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
92	20.369344	142.250.181.42	192.168.10.3	UDP	67	443 → 63914 Len=25
93	20.583545	142.250.181.42	192.168.10.3	UDP	68	443 → 63914 Len=26
96	20.991392	40.77.226.250	192.168.10.3	TCP	66	443 → 57372 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1420 WS=256 SACK_PERM=1
99	20.992024	142.250.181.42	192.168.10.3	UDP	68	443 → 63914 Len=26
101	21.209649	40.77.226.250	192.168.10.3	TCP	1506	443 → 57372 [ACK] Seq=1 Ack=518 Win=525056 Len=1452 [TCP segment of a reassembled PDU]
102	21.210654	40.77.226.250	192.168.10.3	TCP	1506	443 → 57372 [ACK] Seq=1453 Ack=518 Win=525056 Len=1452 [TCP segment of a reassembled PDU]
103	21.210654	40.77.226.250	192.168.10.3	TLSv1.2	1045	Server Hello, Certificate, Server Key Exchange, Server Hello Done
106	21.399029	142.250.181.42	192.168.10.3	UDP	68	443 → 63914 Len=26
107	21.399672	40.77.226.250	192.168.10.3	TLSv1.2	185	Change Cipher Spec, Encrypted Handshake Message
111	21.624728	40.77.226.250	192.168.10.3	TCP	54	443 → 57372 [ACK] Seq=3947 Ack=2965 Win=525568 Len=0
112	21.717289	40.77.226.250	192.168.10.3	TLSv1.2	369	Application Data
116	21.747471	142.250.181.42	192.168.10.3	UDP	68	443 → 63914 Len=26
118	21.928952	40.77.226.250	192.168.10.3	TCP	54	443 → 57372 [ACK] Seq=4263 Ack=2997 Win=525568 Len=0
120	22.218494	142.250.181.42	192.168.10.3	UDP	69	443 → 63914 Len=27
122	22.835235	142.250.181.42	192.168.10.3	UDP	69	443 → 63914 Len=27
127	24.888957	142.250.13.188	192.168.10.3	TCP	66	5228 → 57582 [ACK] Seq=1 Ack=2 Win=265 Len=0 SLEN=58F=2

Frame 124: 69 bytes on wire (552 bits), 69 bytes captured (552 bits) on interface \Device\NPF_{A01953B1-EFD5-4186-B0C2-738189E20617}, id 0
Ethernet II, Src: TendaTec, Bc:30:f0:c8:3a:35:8c:30:f0, Dst: ba:b5:f3:5d:03:5e (ba:b5:f3:5d:03:5e)
Internet Protocol Version 4, Src: 142.250.181.42, Dst: 192.168.10.3
User Datagram Protocol, Src Port: 443, Dst Port: 63914
Data (27 bytes)

```
0000  ba b5 f3 5d 03 5e c8 3a 35 8c 30 f0 08 00 45 00  ... ] ^ : 5 0 . . E
0010  00 37 00 00 40 00 3b 11 30 e6 8e fa b5 2a c0 a8  7 @ ; 0 . . .
0020  0a 03 01 b0 f9 aa 00 23 46 3c 41 99 cf 53 0b 10  ... # F A . Sk
0030  bc 85 f5 c4 28 f1 1f 47 cf 4b dc 44 20 c6 c2 78  ... ( . G K D . x
0040  10 51 cb 93 ce                                     Q . . .
```

Name: Muhammad Fahad
ID: FA19-BSSE-0014
Section: BM

- Filter 4
 - (ip.addr == 192.168.10.3/24)

The screenshot shows the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The status bar at the top right indicates a capture rate of 2.2KB/s and 1.1Kbps. The filter bar at the top of the packet list contains the filter expression `ip.addr == 192.168.10.3/24`. The packet list pane displays 13 packets, with packet 117 selected. The packet details pane shows the structure of the selected packet, including Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Data (27 bytes). The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
109	21.400652	192.168.10.3	40.77.226.250	TLSv1.2	988	Application Data
110	21.600508	192.168.10.3	142.250.181.42	UDP	75	63914 → 443 Len=33
111	21.624728	40.77.226.250	192.168.10.3	TCP	54	443 → 57372 [ACK] Seq=3947 Ack=2965 Win=525568 Len=0
112	21.717289	40.77.226.250	192.168.10.3	TLSv1.2	369	Application Data
113	21.717352	192.168.10.3	40.77.226.250	TCP	54	57372 → 443 [ACK] Seq=2965 Ack=4263 Win=131584 Len=0
114	21.718094	192.168.10.3	40.77.226.250	TLSv1.2	85	Encrypted Alert
115	21.718266	192.168.10.3	40.77.226.250	TCP	54	57372 → 443 [FIN, ACK] Seq=2996 Ack=4263 Win=131584 Len=0
116	21.747471	142.250.181.42	192.168.10.3	UDP	68	443 → 63914 Len=26
117	21.928482	192.168.10.3	15.67.9.5	TCP	55	[TCP Retransmission] 58288 → 443 [ACK] Seq=0 Ack=1 Win=517 Len=1
118	21.929952	40.77.226.250	192.168.10.3	TCP	54	443 → 57372 [ACK] Seq=4263 Ack=2997 Win=525568 Len=0
119	21.959025	192.168.10.3	142.250.181.42	UDP	75	63914 → 443 Len=33
120	22.218494	142.250.181.42	192.168.10.3	UDP	69	443 → 63914 Len=27
121	22.631611	192.168.10.3	142.250.181.42	UDP	75	63914 → 443 Len=33
122	22.835235	142.250.181.42	192.168.10.3	UDP	69	443 → 63914 Len=27
123	23.641620	192.168.10.3	142.250.181.42	UDP	75	63914 → 443 Len=33

125 24.688385 192.168.10.3 142.250.13.188 TCP 55 57582 → 5728 [ACK] Seq=1 Ack=1 Win=513 Len=1

Frame 124: 69 bytes on wire (552 bits), 69 bytes captured (552 bits) on interface \Device\NPF... id 0
Ethernet II, Src: TendaTec, Dst: ba:b5:f3:5d:03:5e (ba:b5:f3:5d:03:5e)
Internet Protocol Version 4, Src: 142.250.181.42, Dst: 192.168.10.3
User Datagram Protocol, Src Port: 443, Dst Port: 63914
Data (27 bytes)

0000 ba b5 f3 5d 03 5e c8 3a 35 8c 30 f0 08 00 45 00 ...] ^ : 5 0 ... E
0010 00 37 00 00 40 00 3b 11 30 e6 8e fa b5 2a c0 a8 7 : @ ; 0 ... P ...
0020 0a 03 01 b0 f9 aa 00 23 46 3c 41 99 cf 53 0b 10 ... : # F < A - \$ k
0030 bc 85 f5 c4 28 f1 1f 47 cf 4b dc 44 20 c6 c2 78 ... (: G K D - x
0040 10 51 cb 93 ce Q ...

Name: Muhammad Fahad

ID: FA19-BSSE-0014

Section: BM

- Filter 5
 - (dns)

The screenshot displays the Wireshark network traffic capture interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The top status bar shows the interface as 'Wi-Fi 4' with a speed of 5.3Kbps and 13.2Kbps, and a battery level of 28%. The main display area is filtered for 'dns' traffic. The packet list pane shows a series of DNS queries and responses from 192.168.10.1 to 192.168.10.3. The packet details pane for the selected packet (No. 126) shows the following layers: Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Domain Name System (query). The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
126	25.289649	192.168.10.1	192.168.10.3	DNS	141	Standard query response 0xb23f A note.youdao.com CNAME note.ntes53.netease.com A 59.111.183.194 A 59.111.18...
173	28.211721	192.168.10.3	192.168.10.1	DNS	71	Standard query 0x7996 A i.ytimg.com
179	28.251650	192.168.10.1	192.168.10.3	DNS	247	Standard query response 0x7996 A i.ytimg.com A 142.250.181.150 A 216.58.208.246 A 172.217.21.54 A 216.58.20...
185	28.367815	192.168.10.3	192.168.10.1	DNS	95	Standard query 0x565f A suggestqueries-clients6.youtube.com
195	28.413217	192.168.10.1	192.168.10.3	DNS	111	Standard query response 0x565f A suggestqueries-clients6.youtube.com A 216.58.207.14
300	28.842470	192.168.10.3	192.168.10.1	DNS	73	Standard query 0xc75e A yt3.ggpht.com
320	29.024768	192.168.10.1	192.168.10.3	DNS	125	Standard query response 0xc75e A yt3.ggpht.com CNAME wide-youtube.l.google.com A 108.177.119.198
1298	37.617015	192.168.10.3	192.168.10.1	DNS	75	Standard query 0x9420 A www.youtube.com
1299	37.659501	192.168.10.1	192.168.10.3	DNS	152	Standard query response 0x9420 A www.youtube.com CNAME youtube-ui.l.google.com CNAME wide-youtube.l.google...
1473	38.978878	192.168.10.3	192.168.10.1	DNS	79	Standard query 0x8520 A clients2.google.com
1474	39.025534	192.168.10.1	192.168.10.3	DNS	119	Standard query response 0x8520 A clients2.google.com CNAME clients.l.google.com A 172.217.21.46
1492	39.425584	192.168.10.3	192.168.10.1	DNS	70	Standard query 0xd847 A google.com
1497	39.493715	192.168.10.1	192.168.10.3	DNS	86	Standard query response 0xd847 A google.com A 216.58.207.110
1500	39.513685	192.168.10.3	192.168.10.1	DNS	74	Standard query 0x452c A api.github.com
1501	39.516961	192.168.10.3	192.168.10.1	DNS	69	Standard query 0x2a94 A wpad.Home
1515	39.604567	192.168.10.1	192.168.10.3	DNS	90	Standard query response 0x452c A api.github.com A 13.233.76.15

Frame 126: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface \Device\NPF_{A01953B1-EFD5-4186-BBC2-738189E20617}, id 0
Ethernet II, Src: ba:b5:f3:5d:03:5e (ba:b5:f3:5d:03:5e), Dst: TendaTec_Bc:30:f0 (c8:3a:35:8c:30:f0)
Internet Protocol Version 4, Src: 192.168.10.3, Dst: 192.168.10.1
User Datagram Protocol, Src Port: 59699, Dst Port: 53
Domain Name System (query)

0000 c8 3a 35 8c 30 f0 ba b5 f3 5d 03 5e 00 00 45 00 :5 0 ...] ^ E
0010 00 3d 58 03 00 00 80 11 4d 58 c0 a8 0a 03 c0 a8 :X ... MX ...
0020 0a 01 e9 33 00 35 00 29 2f a1 b2 3f 01 00 00 01 :3 5) / - ? ...
0030 00 00 00 00 00 04 6e 6f 74 65 06 79 6f 75 64 :.....n ote-youd
0040 61 6f 03 63 6f 6d 00 00 01 00 01 :ao.com ...

Name: Muhammad Fahad
ID: FA19-BSSE-0014
Section: BM

- Filter 6
 - (!ip.addr==192.168.10.3)

The image shows a Wireshark network traffic capture on a Windows system. The filter bar at the top is set to `!ip.addr==192.168.10.3`. The packet list on the left shows several ARP requests from TendaTec_8c:30:f0 to ba:b5:f3:5d:03:5e. The packet details pane on the right shows the structure of a frame, including Ethernet II, Internet Protocol Version 6, and Internet Control Message Protocol v6. The packet bytes pane at the bottom shows the raw hex and ASCII data of the selected packet.

No.	Time	Source	Destination	Protocol	Length	Info
59	7.882965	TendaTec_8c:30:f0	ba:b5:f3:5d:03:5e	ARP	42	Who has 192.168.10.3? Tell 192.168.10.1
61	7.883126	ba:b5:f3:5d:03:5e	TendaTec_8c:30:f0	ARP	42	192.168.10.3 is at ba:b5:f3:5d:03:5e
956	34.095773	TendaTec_8c:30:f0	ba:b5:f3:5d:03:5e	ARP	42	Who has 192.168.10.3? Tell 192.168.10.1
957	34.095793	ba:b5:f3:5d:03:5e	TendaTec_8c:30:f0	ARP	42	192.168.10.3 is at ba:b5:f3:5d:03:5e
1520	39.606822	fe80::29f2:fe8c:7...	ff02::fb	MDNS	90	Standard query 0x0000 A wpad.local, "QM" question
1521	39.607212	fe80::29f2:fe8c:7...	ff02::1:3	LLMNR	84	Standard query 0x60b1 A wpad
1617	40.022371	fe80::29f2:fe8c:7...	ff02::1:3	LLMNR	84	Standard query 0x60b1 A wpad
3531	64.468421	TendaTec_8c:30:f0	ba:b5:f3:5d:03:5e	ARP	42	Who has 192.168.10.3? Tell 192.168.10.1
3532	64.468434	ba:b5:f3:5d:03:5e	TendaTec_8c:30:f0	ARP	42	192.168.10.3 is at ba:b5:f3:5d:03:5e
5049	90.651942	TendaTec_8c:30:f0	ba:b5:f3:5d:03:5e	ARP	42	Who has 192.168.10.3? Tell 192.168.10.1
5050	90.651966	ba:b5:f3:5d:03:5e	TendaTec_8c:30:f0	ARP	42	192.168.10.3 is at ba:b5:f3:5d:03:5e
9695	107.155557	192.168.10.1	224.0.0.1	IGMPv3	50	Membership Query, general
11719	116.837974	TendaTec_8c:30:f0	ba:b5:f3:5d:03:5e	ARP	42	Who has 192.168.10.3? Tell 192.168.10.1
11720	116.838006	ba:b5:f3:5d:03:5e	TendaTec_8c:30:f0	ARP	42	192.168.10.3 is at ba:b5:f3:5d:03:5e
17251	143.904546	TendaTec_8c:30:f0	ba:b5:f3:5d:03:5e	ARP	42	Who has 192.168.10.3? Tell 192.168.10.1
17252	143.904574	ba:b5:f3:5d:03:5e	TendaTec_8c:30:f0	ARP	42	192.168.10.3 is at ba:b5:f3:5d:03:5e

Frame 72: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface \Device\NPF_{A0195301-EF05-4186-BBC2-738189E20617}, id 0
Ethernet II, Src: TendaTec_8c:30:f0 (c8:3a:35:8c:30:f0), Dst: IPv6mcast_01 (33:33:00:00:00:01)
Internet Protocol Version 6, Src: fe80::ca3a:35ff:fe8c:30f0, Dst: ff02::1
Internet Control Message Protocol v6

0000 33 33 00 00 00 01 c8 3a 35 8c 30 f0 86 dd 60 00 335 0...
0010 00 00 00 18 3a ff fe 80 00 00 00 00 00 ca 3a
0020 35 ff fe 8c 30 f0 ff 02 00 00 00 00 00 00 00 5...0...
0030 00 00 00 00 00 01 86 00 dc 60 40 58 ff ff 00 00X...
0040 00 00 00 00 00 00 01 01 c8 3a 35 8c 30 f05 0...

Name: Muhammad Fahad
ID: FA19-BSSE-0014
Section: BM

- Filter 7

o (ip.addr==192.168.10.3/24 and ip.addr==192.168.10.1/24)

The screenshot shows a Wireshark packet capture on the 'Wi-Fi 4' interface. The filter bar is set to 'ip.addr==192.168.10.3/24 and ip.addr==192.168.10.1/24'. The packet list shows a TLS handshake sequence:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.10.3	192.168.10.1	UDP	75	63914 → 443 Len=33
2	0.113578	192.168.10.3	40.77.226.250	TCP	66	57360 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
3	0.119156	192.168.10.3	192.168.10.3	TLSPv1.2	110	Application Data
4	0.119940	192.168.10.3	192.168.10.3	TCP	54	443 → 57625 [FIN, ACK] Seq=57 Ack=1 Win=261 Len=0
5	0.119972	192.168.10.3	192.168.10.3	TCP	54	57625 → 443 [ACK] Seq=1 Ack=58 Win=513 Len=0
6	0.165490	192.168.10.3	192.168.10.3	UDP	67	443 → 63914 Len=25
7	0.306202	40.77.226.250	192.168.10.3	TCP	66	443 → 57360 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1420 WS=256 SACK_PERM=1
8	0.306277	192.168.10.3	40.77.226.250	TCP	54	57360 → 443 [ACK] Seq=1 Ack=1 Win=131840 Len=0
9	0.306562	192.168.10.3	40.77.226.250	TLSPv1.2	571	Client Hello
10	0.373262	192.168.10.3	192.168.10.3	UDP	75	63914 → 443 Len=33
11	0.615201	40.77.226.250	192.168.10.3	TCP	1506	443 → 57360 [ACK] Seq=1 Ack=518 Win=262144 Len=1452 [TCP segment of a reassembled PDU]
12	0.616513	40.77.226.250	192.168.10.3	TCP	1506	443 → 57360 [ACK] Seq=1453 Ack=518 Win=262144 Len=1452 [TCP segment of a reassembled PDU]
13	0.616513	40.77.226.250	192.168.10.3	TLSPv1.2	1045	Server Hello, Certificate, Server Key Exchange, Server Hello Done
14	0.616513	192.168.10.3	192.168.10.3	UDP	67	443 → 63914 Len=25
15	0.616592	192.168.10.3	40.77.226.250	TCP	54	57360 → 443 [ACK] Seq=518 Ack=3896 Win=131840 Len=0
16	0.618659	192.168.10.3	40.77.226.250	TLSPv1.2	147	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
17	0.626713	192.168.10.3	192.168.10.1	UDP	75	63914 → 443 Len=33

The packet details pane shows the structure of the Client Hello packet (packet 9):

- Frame 71: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{A01953B1-EF05-4186-BBC2-7381B9E28617}, id 0
- Ethernet II, Src: TendaTec_Bc:30:f0 (c8:3a:35:8c:30:f0), Dst: ba:b5:f3:5d:03:5e (ba:b5:f3:5d:03:5e)
- Internet Protocol Version 4, Src: 178.62.253.213, Dst: 192.168.10.3
- Transmission Control Protocol, Src Port: 443, Dst Port: 62577, Seq: 65, Ack: 2, Len: 0

The packet bytes pane shows the raw data of the Client Hello packet:

```
0000 ba b5 f3 5d 03 5e c8 3a 35 8c 30 f0 00 00 45 00 ... ^: 5 0 ... E
0010 00 28 91 58 40 00 33 06 3b b8 b2 3e fd d5 c0 a8 ... X@ 3 ; -> ...
0020 0a 03 01 bb f4 71 e b9 ab 62 d8 8b 54 b1 50 10 ... q - b - T P
0030 01 f5 45 9a 00 00 ... E ...
```

o (ip.addr==192.168.10.3 and ip.addr==192.168.10.1)

The screenshot shows a Wireshark packet capture on the 'Wi-Fi 4' interface. The filter bar is set to 'ip.addr==192.168.10.3 and ip.addr==192.168.10.1'. The packet list shows a series of DNS queries:

No.	Time	Source	Destination	Protocol	Length	Info
128	25.289649	192.168.10.1	192.168.10.3	DNS	141	Standard query response 0xb23f A note.youdao.com CNAME note.nte53.netease.com A 59.111.183.194 A 59.111.18...
173	28.211721	192.168.10.3	192.168.10.1	DNS	71	Standard query 0x7996 A i.ytimg.com
179	28.251650	192.168.10.1	192.168.10.3	DNS	247	Standard query response 0x7996 A i.ytimg.com A 142.250.181.150 A 216.58.208.246 A 172.217.21.54 A 216.58.20...
185	28.367815	192.168.10.3	192.168.10.1	DNS	95	Standard query 0x565f A suggestqueries-clients6.youtube.com
195	28.413217	192.168.10.1	192.168.10.3	DNS	111	Standard query response 0x565f A suggestqueries-clients6.youtube.com A 216.58.207.14
300	28.842470	192.168.10.3	192.168.10.1	DNS	73	Standard query 0xc75e A yt3.ggpht.com
320	29.024768	192.168.10.1	192.168.10.3	DNS	125	Standard query response 0xc75e A yt3.ggpht.com CNAME wide-youtube.l.google.com A 108.177.119.198
1298	37.617015	192.168.10.3	192.168.10.1	DNS	75	Standard query 0x9420 A www.youtube.com
1299	37.659501	192.168.10.1	192.168.10.3	DNS	152	Standard query response 0x9420 A www.youtube.com CNAME youtube-ui.l.google.com CNAME wide-youtube.l.google...
1473	38.978878	192.168.10.3	192.168.10.1	DNS	79	Standard query 0x8520 A clients2.google.com
1474	39.025534	192.168.10.1	192.168.10.3	DNS	119	Standard query response 0x8520 A clients2.google.com CNAME clients.l.google.com A 172.217.21.46
1492	39.425584	192.168.10.3	192.168.10.1	DNS	70	Standard query 0xd847 A google.com
1497	39.493715	192.168.10.1	192.168.10.3	DNS	86	Standard query response 0xd847 A google.com A 216.58.207.110
1500	39.513685	192.168.10.3	192.168.10.1	DNS	74	Standard query 0x452c A api.github.com
1501	39.516961	192.168.10.3	192.168.10.1	DNS	69	Standard query 0x2a94 A wpad.Home
1515	39.604567	192.168.10.1	192.168.10.3	DNS	80	Standard query response 0x452c A api.github.com A 13.233.76.15

The packet details pane shows the structure of the first DNS query (packet 128):

- Frame 126: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface \Device\NPF_{A01953B1-EF05-4186-BBC2-7381B9E28617}, id 0
- Ethernet II, Src: ba:b5:f3:5d:03:5e (ba:b5:f3:5d:03:5e), Dst: TendaTec_Bc:30:f0 (c8:3a:35:8c:30:f0)
- Internet Protocol Version 4, Src: 192.168.10.3, Dst: 192.168.10.1
- User Datagram Protocol, Src Port: 59699, Dst Port: 53
- Domain Name System (query)

The packet bytes pane shows the raw data of the DNS query:

```
0000 c8 3a 35 8c 30 f0 ba b5 f3 5d 03 5e 00 00 45 00 ... ^: 5 0 ... E
0010 00 3d 58 03 00 00 80 11 4d 58 c0 a8 0a 03 c0 a8 ... X ... MX ...
0020 0a 01 e9 33 00 35 00 29 2f a1 b2 3f 01 00 00 01 ... 3 5 ) / - ? ...
0030 00 00 00 00 00 04 6e 6f 74 65 06 79 6f 75 64 ... n ote-youd
0040 61 6f 03 63 6f 6d 00 00 01 00 01 ... ao.com ...
```

Name: Muhammad Fahad

ID: FA19-BSSE-0014

Section: BM

- Filter 8
 - (eth.addr == BA-B5-F3-5D-03-5E)

The image shows a Wireshark packet capture interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The status bar at the top right shows 0.5KB/s, 1.0KB/s, 14%, and the date/time Wed Nov 3 PM 6:40:50.

The packet list pane shows a filtered list of packets with the filter (eth.addr == BA-B5-F3-5D-03-5E). The list includes:

No.	Time	Source	Destination	Protocol	Length	Info
111	21.624728	40.77.226.250	192.168.10.3	TCP	54	443 → 57372 [ACK] Seq=3947 Ack=2965 Win=525568 Len=0
112	21.717289	40.77.226.250	192.168.10.3	TLSv1.2	369	Application Data
113	21.717352	192.168.10.3	40.77.226.250	TCP	54	57372 → 443 [ACK] Seq=2965 Ack=4263 Win=131584 Len=0
114	21.718094	192.168.10.3	40.77.226.250	TLSv1.2	85	Encrypted Alert
115	21.718266	192.168.10.3	40.77.226.250	TCP	54	57372 → 443 [FIN, ACK] Seq=2996 Ack=4263 Win=131584 Len=0
116	21.747471	142.250.181.42	192.168.10.3	UDP	68	443 → 63914 Len=26
117	21.928482	192.168.10.3	13.67.9.5	TCP	55	[TCP Retransmission] 58288 → 443 [ACK] Seq=0 Ack=1 Win=517 Len=1
118	21.929952	40.77.226.250	192.168.10.3	TCP	54	443 → 57372 [ACK] Seq=4263 Ack=2997 Win=525568 Len=0
119	21.959825	192.168.10.3	142.250.181.42	UDP	75	63914 → 443 Len=33
120	22.219494	142.250.181.42	192.168.10.3	UDP	69	443 → 63914 Len=27
121	22.631611	192.168.10.3	142.250.181.42	UDP	75	63914 → 443 Len=33
122	22.835235	142.250.181.42	192.168.10.3	UDP	69	443 → 63914 Len=27
123	23.641620	192.168.10.3	142.250.181.42	UDP	75	63914 → 443 Len=33
124	23.856369	142.250.181.42	192.168.10.3	UDP	69	443 → 63914 Len=27
125	24.688385	192.168.10.3	142.250.13.188	TCP	55	57582 → 5228 [ACK] Seq=1 Ack=1 Win=513 Len=1

The packet details pane shows the selected packet (No. 127) with the following details:

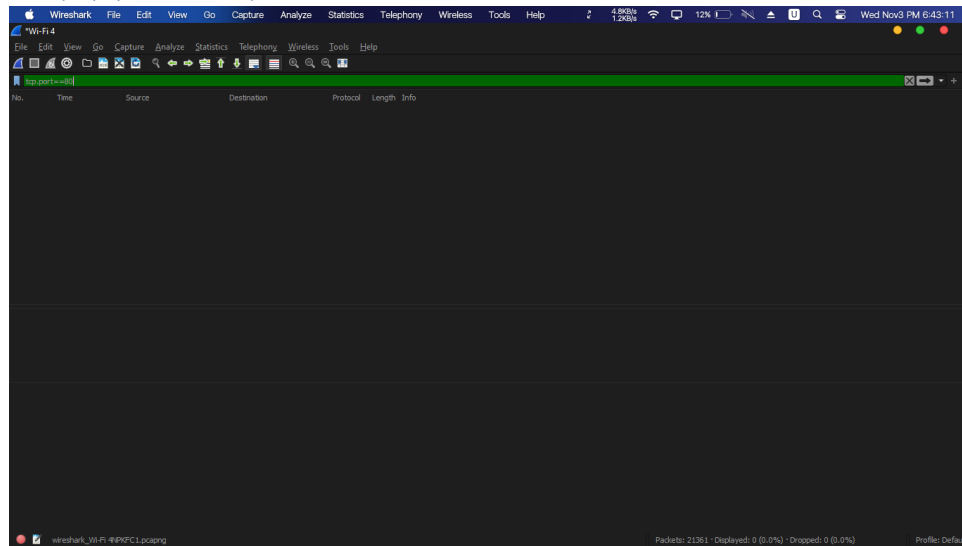
- Frame 126: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface \Device\NPF_{A01953B1-EFD5-4186-B8C2-738189E20617}, id 0
- Ethernet II, Src: ba:b5:f3:5d:03:5e (ba:b5:f3:5d:03:5e), Dst: TendaTec_8c:30:f0 (c8:3a:35:8c:30:f0)
- Internet Protocol Version 4, Src: 192.168.10.3, Dst: 192.168.10.1
- User Datagram Protocol, Src Port: 59699, Dst Port: 53
- Domain Name System (query)

The packet bytes pane shows the raw data in hexadecimal and ASCII:

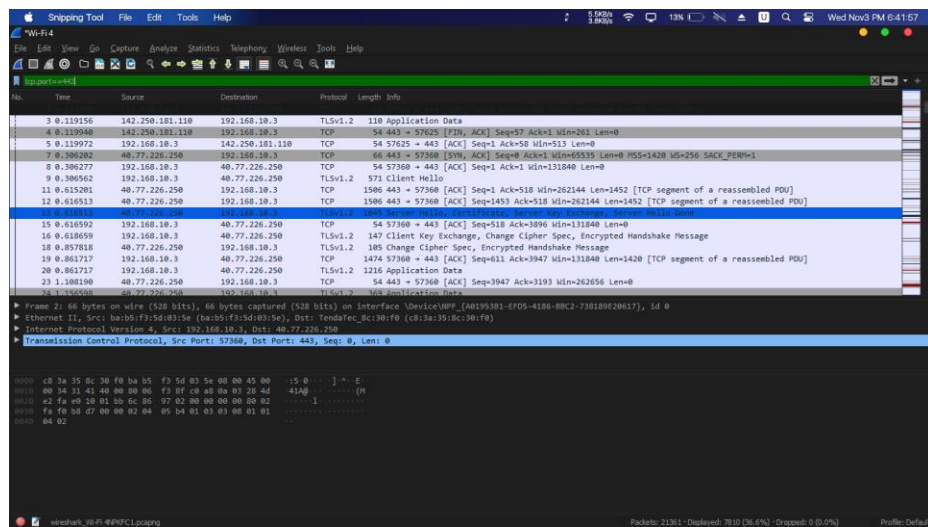
```
0000 c8 3a 35 8c 30 f0 ba b5 f3 5d 03 5e 00 00 45 00 :5 0 ... ] ^ ^ E
0010 00 3d 58 03 00 00 00 11 4d 58 c0 a8 0a 03 c0 a8 =X .... MX ....
0020 0a 01 e9 33 00 35 00 29 2f a1 b2 3f 01 00 00 01 ...3 5 ) / - ? ....
0030 00 00 00 00 00 04 6e 6f 74 65 06 79 6f 75 64 .....n ote youd
0040 61 6f 03 63 6f 6d 00 00 01 00 01 ao com .....
```


Name: Muhammad Fahad
ID: FA19-BSSE-0014
Section: BM

- Filter 9
 - (tcp.port == 80)



- (tcp.port == 443)

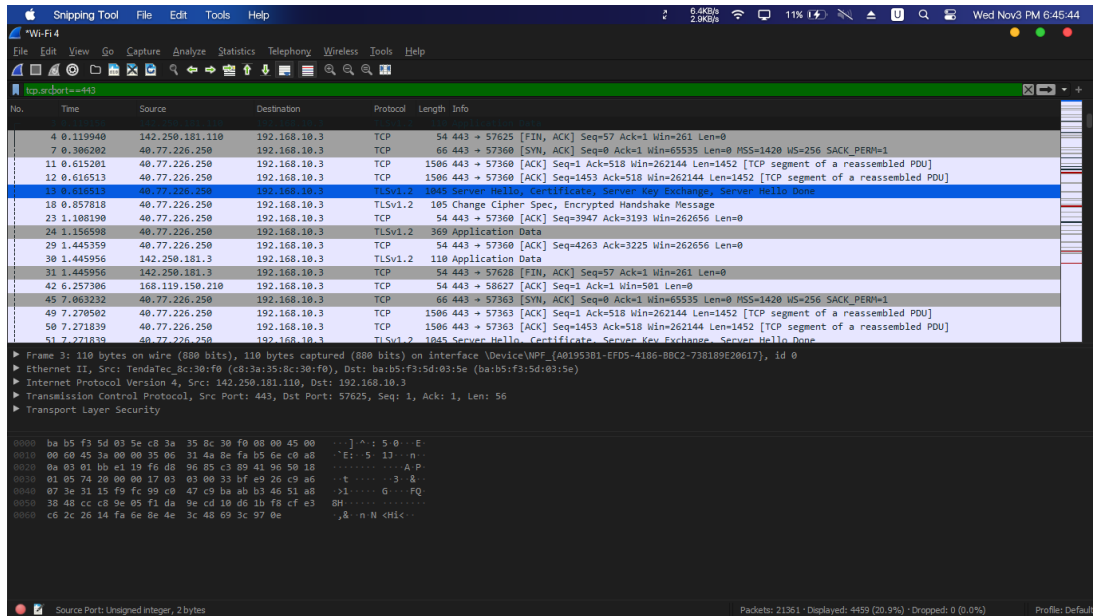


Name: Muhammad Fahad

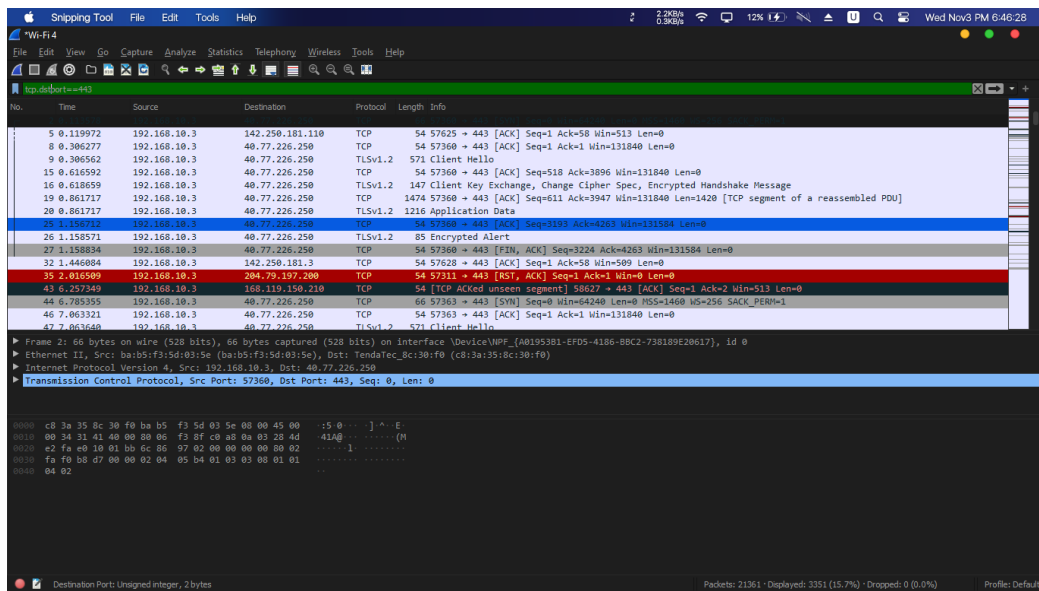
ID: FA19-BSSE-0014

Section: BM

o (tcp.srcport == 80)

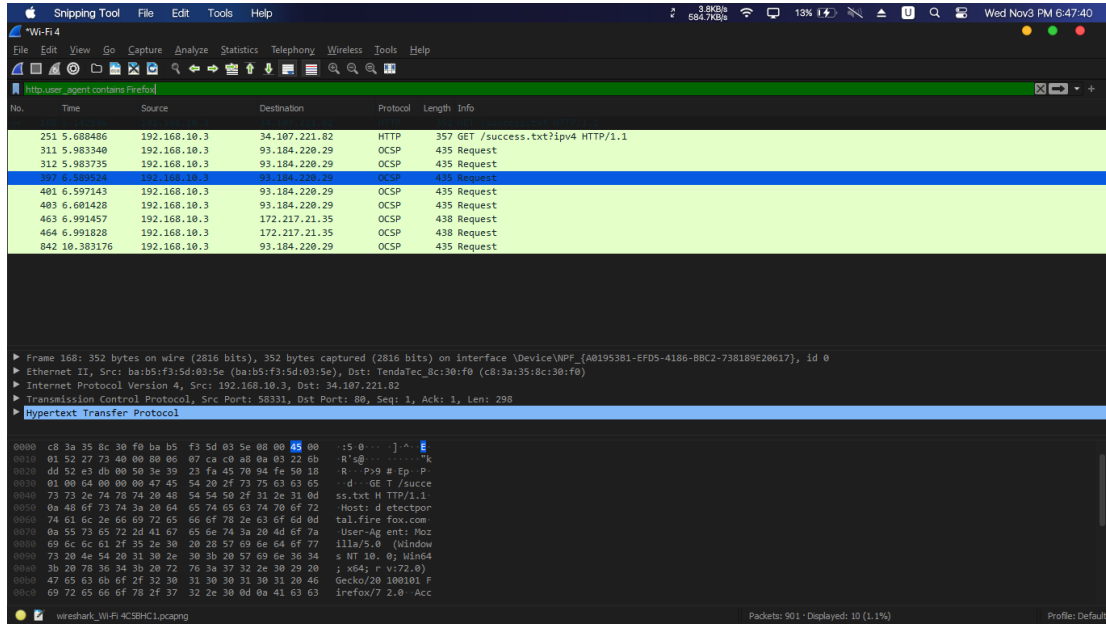


o (tcp.dstport == 80)

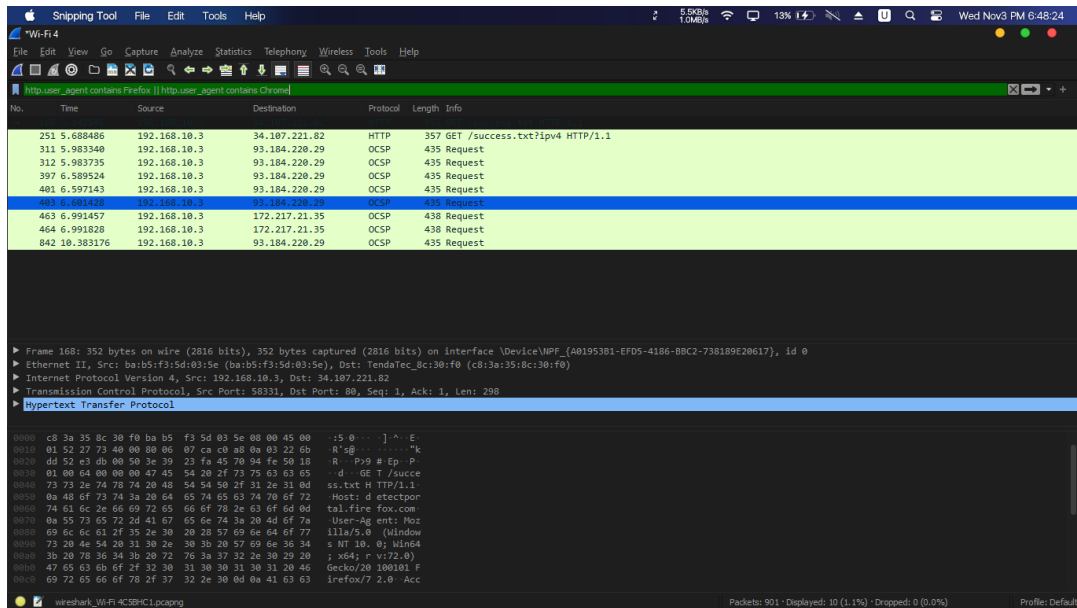


Name: Muhammad Fahad
ID: FA19-BSSE-0014
Section: BM

- Filter 10
 - (http.user_agent contains Firefox)



- (http.user_agent contains Firefox || http.user_agent contains Chrome)



Name: Muhammad Fahad
ID: FA19-BSSE-0014
Section: BM

- Filter 11
 - (tcp.port == 80 && ip.addr == 192.168.10.3)

The image shows a Wireshark packet capture window. The top toolbar includes buttons for File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The filter bar at the top displays the active filter: `tcp.port == 80 && ip.addr == 192.168.10.3`. The packet list on the left shows several packets, with packet 142 selected. The packet details pane on the right shows the structure of the selected packet, which is a TCP segment. The packet bytes pane at the bottom shows the raw data of the selected packet, which is an HTTP GET request for `/ss.txt` from `192.168.10.3` to `34.107.221.82`. The status bar at the bottom indicates that 901 packets were captured, 99 were displayed (11.0%), and 0 were dropped (0.0%).

No.	Time	Source	Destination	Protocol	Length	Info
120	4.004756	192.168.10.3	34.107.221.82	TCP	66	58331 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
129	4.257172	192.168.10.3	34.107.221.82	TCP	66	58333 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
142	5.014534	192.168.10.3	34.107.221.82	TCP	66	[TCP Retransmission] 58331 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
149	5.140725	34.107.221.82	192.168.10.3	TCP	66	80 → 58331 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1430 SACK_PERM=1 WS=256
154	5.140725	34.107.221.82	192.168.10.3	TCP	66	80 → 58333 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1430 SACK_PERM=1 WS=256
164	5.140994	192.168.10.3	34.107.221.82	TCP	54	58331 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
166	5.141258	192.168.10.3	34.107.221.82	TCP	54	58333 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
181	5.307803	34.107.221.82	192.168.10.3	HTTP	274	HTTP/1.1 200 OK (text/plain)
183	5.314373	192.168.10.3	34.107.221.82	TCP	66	58340 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
184	5.353079	192.168.10.3	34.107.221.82	TCP	54	58331 → 80 [ACK] Seq=299 Ack=221 Win=65280 Len=0
191	5.573512	192.168.10.3	34.107.221.82	TCP	66	58346 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
199	5.662335	34.107.221.82	192.168.10.3	TCP	66	[TCP Retransmission] 80 → 58331 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1430 SACK_PERM=1 WS=256
206	5.662335	34.107.221.82	192.168.10.3	TCP	54	80 → 58331 [ACK] Seq=1 Ack=299 Win=66816 Len=0
211	5.662335	34.107.221.82	192.168.10.3	TCP	66	80 → 58340 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1430 SACK_PERM=1 WS=256
226	5.662492	192.168.10.3	34.107.221.82	TCP	66	[TCP Dup ACK 184#1] 58331 → 80 [ACK] Seq=299 Ack=221 Win=65280 Len=0 SLE=0 SRE=1
229	5.662808	192.168.10.3	34.107.221.82	TCP	54	[TCP Dup ACK 184#1] 58331 → 80 [ACK] Seq=299 Ack=221 Win=65280 Len=0

Frame 168: 352 bytes on wire (2816 bits), 352 bytes captured (2816 bits) on interface \Device\NPF{A0195301-EF05-4106-BBC2-730109E20617}, id 0
▶ Ethernet II, Src: ba:b5:f3:5d:03:5e (ba:b5:f3:5d:03:5e), Dst: TendaTec_8c:30:f0 (c8:3a:35:8c:30:f0)
▶ Internet Protocol Version 4, Src: 192.168.10.3, Dst: 34.107.221.82
▶ Transmission Control Protocol, Src Port: 58331, Dst Port: 80, Seq: 1, Ack: 1, Len: 298
▶ Hypertext Transfer Protocol

0000 c8 3a 35 8c 30 f0 ba b5 f3 5d 03 5e 08 00 45 00 :5 0 ...] ^ ^ E
0010 01 52 27 73 40 00 00 06 07 ca c8 a8 0a 03 22 0b R's@ "k
0020 dd 52 c3 d0 00 50 3e 39 23 fa 45 70 94 fe 50 1b R...P9 # Ep..P
0030 01 00 64 00 00 00 47 45 54 20 2f 73 75 63 63 65 ..d..GE T/succe
0040 73 73 2e 74 78 74 20 48 54 54 50 2f 31 2e 31 0d ss.txt H TTP/1.1
0050 0a 48 6f 73 74 3a 20 64 65 74 65 63 74 70 6f 72 Host: d etectpor
0060 74 61 6c 2e 66 69 72 65 66 6f 78 2e 63 6f 6d 0d tal.fire fox.com
0070 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a User-Ag ent: Moz
0080 69 6c 6e 61 2f 35 2e 30 20 28 5f 69 6e 64 6f 77 illa/5.0 (Window
0090 73 20 4e 54 20 31 30 2e 30 3b 20 5f 69 6e 64 34 s NT 10. 0; Win64
00a0 3b 20 78 36 34 3b 20 72 76 3a 37 32 2e 30 29 20 ; x64; r v:72.0)
00b0 47 65 63 6b 6f 2f 32 30 31 30 30 31 30 31 20 46 Gecko/20 100101 F
00c0 69 72 65 66 6f 78 2f 3f 32 2e 30 0d 0a 41 63 63 irefox/7 2.0 Acc

Name: Muhammad Fahad
ID: FA19-BSSE-0014
Section: BM

- Filter 12
 - (http.request)

Sniffing Tool

Wi-Fi 4

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.request

No.	Time	Source	Destination	Protocol	Length	Info
168	5.142546	192.168.10.3	34.107.221.82	HTTP	352	GET /success.txt HTTP/1.1
251	5.688486	192.168.10.3	34.107.221.82	HTTP	357	GET /success.txt?ipv4 HTTP/1.1
311	5.983340	192.168.10.3	93.184.220.29	OCSP	435	Request
312	5.983735	192.168.10.3	93.184.220.29	OCSP	435	Request
397	6.589524	192.168.10.3	93.184.220.29	OCSP	435	Request
401	6.597143	192.168.10.3	93.184.220.29	OCSP	435	Request
403	6.601428	192.168.10.3	93.184.220.29	OCSP	435	Request
463	6.991457	192.168.10.3	172.217.21.35	OCSP	438	Request
464	6.991828	192.168.10.3	172.217.21.35	OCSP	438	Request
842	10.383176	192.168.10.3	93.184.220.29	OCSP	435	Request

Request: Boolean

Packets: 901 · Displayed: 10 (1.1%) · Dropped: 0 (0.0%)

Profile: Default

Name: Muhammad Fahad
ID: FA19-BSSE-0014
Section: BM

- Filter 13
 - (http.request or http.response)

The image shows a Wireshark network traffic capture. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The status bar at the top right shows 4.1KB/s, 2.402/s, and the date/time Wed Nov 3 PM 6:51:43. The main display area is titled "Wi-Fi 4" and shows a list of captured packets. The filter bar at the top of the packet list is set to "http.request or http.response". The packet list shows several HTTP and OCSP packets. The selected packet (No. 463) is an OCSP request. The packet details pane on the right shows the structure of the selected packet, including Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol. The packet bytes pane at the bottom shows the raw data of the selected packet in hexadecimal and ASCII.

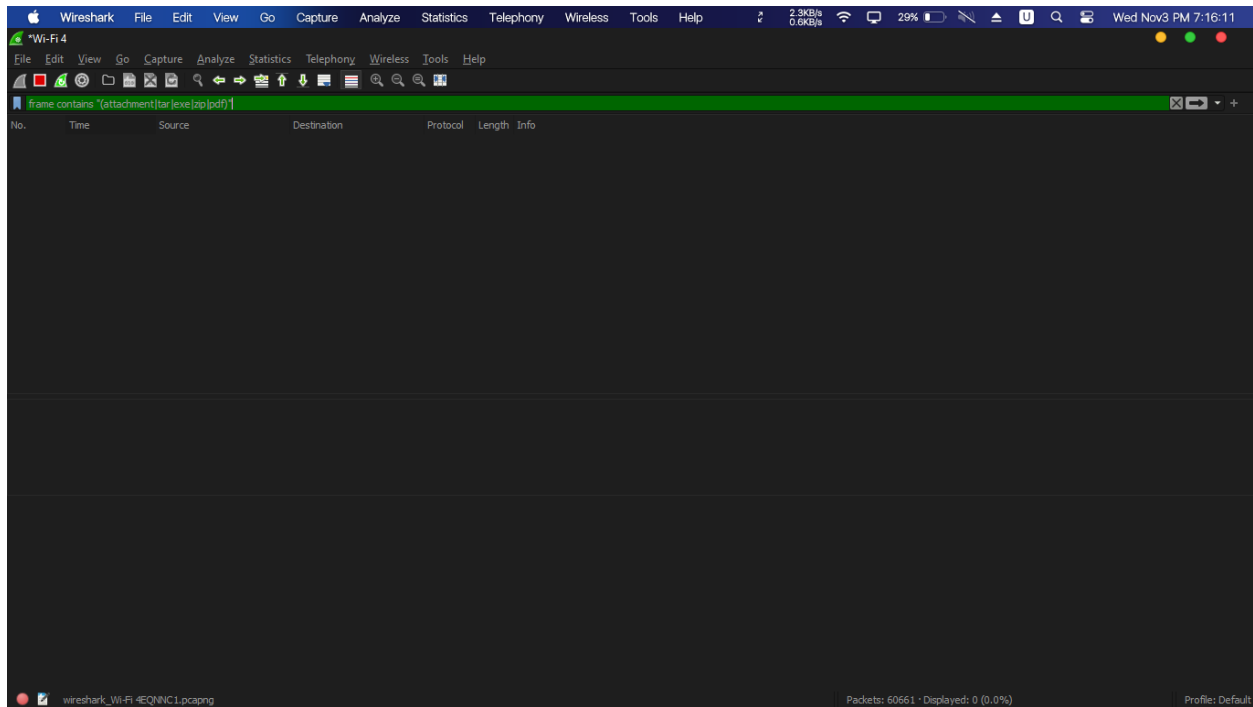
No.	Time	Source	Destination	Protocol	Length	Info
181	5.307803	34.107.221.82	192.168.10.3	HTTP	274	HTTP/1.1 200 OK (text/plain)
251	5.688486	192.168.10.3	34.107.221.82	HTTP	357	GET /success.txt?ip=4 HTTP/1.1
277	5.844886	34.107.221.82	192.168.10.3	HTTP	274	HTTP/1.1 200 OK (text/plain)
311	5.983340	192.168.10.3	93.184.220.29	OCSP	435	Request
312	5.983735	192.168.10.3	93.184.220.29	OCSP	435	Request
381	6.589034	93.184.220.29	192.168.10.3	OCSP	853	Response
387	6.589034	93.184.220.29	192.168.10.3	OCSP	852	Response
397	6.589524	192.168.10.3	93.184.220.29	OCSP	435	Request
401	6.597143	192.168.10.3	93.184.220.29	OCSP	435	Request
403	6.601420	192.168.10.3	93.184.220.29	OCSP	435	Request
420	6.601557	93.184.220.29	192.168.10.3	OCSP	853	[TCP Spurious Retransmission] Response
436	6.989297	93.184.220.29	192.168.10.3	OCSP	852	[TCP Spurious Retransmission] Response
442	6.989297	93.184.220.29	192.168.10.3	OCSP	850	Response
444	6.989297	93.184.220.29	192.168.10.3	OCSP	852	Response
451	6.989297	93.184.220.29	192.168.10.3	OCSP	853	Response
463	6.991457	192.168.10.3	172.217.21.35	OCSP	438	Request

Frame 168: 352 bytes on wire (2816 bits), 352 bytes captured (2816 bits) on interface \Device\NPF_{A0195301-EF05-4106-BBC2-730189E20617}, id 0
Ethernet II, Src: ba:b5:f3:5d:03:5e (ba:b5:f3:5d:03:5e), Dst: TendaTec_8c:30:f0 (c8:3a:35:8c:30:f0)
Internet Protocol Version 4, Src: 192.168.10.3, Dst: 34.107.221.82
Transmission Control Protocol, Src Port: 58331, Dst Port: 80, Seq: 1, Ack: 1, Len: 298
Hypertext Transfer Protocol

0000 c8 3a 35 8c 30 f0 ba b5 f3 5d 03 5e 08 00 45 00 :5 0 ...] ^ E
0010 01 52 27 73 40 00 00 06 07 ca c8 a8 0a 03 22 0b R's@k
0020 dd 52 e3 d0 00 50 3e 39 23 fa 45 70 94 fe 50 10 R P9 # Ep p
0030 01 00 64 00 00 00 47 45 54 20 2f 73 75 63 63 65 d GE T /succe
0040 73 73 2e 74 78 74 20 48 54 54 50 2f 31 2e 31 0d ss.txt H TTP/1.1
0050 0a 48 6f 73 74 3a 20 64 65 74 65 63 74 70 6f 72 Host: d etectpor
0060 74 61 6c 2e 66 69 72 65 66 6f 78 2e 63 6f 6d 0d tal.fire fox.com
0070 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a User-Ag ent: Moz
0080 69 6c 6c 61 2f 35 2e 30 20 28 5f 69 6e 64 6f 77 illa/5.0 (Window
0090 73 20 4e 54 20 31 30 2e 30 30 20 5f 69 6e 36 34 s NT 10. 0; Win64
00a0 3b 20 78 36 34 3b 20 72 76 3a 37 32 2e 30 29 20 ; x64; r v:72.0
00b0 47 65 63 6b 6f 2f 32 30 31 30 30 31 30 31 20 46 Gecko/20 100101 F
00c0 69 72 65 66 6f 78 2f 37 32 2e 30 0d 0a 41 63 63 irefox/7 2.0 Acc

Name: Muhammad Fahad
ID: FA19-BSSE-0014
Section: BM

- Filter 14
 - (frame contains "(attachment|tar|exe|zip|pdf)")



Name: Muhammad Fahad

ID: FA19-BSSE-0014

Section: BM

- Filter 15
 - (tcp contains facebook)

