

WireShark Lab 4

Jennifer Hurst

Include screen shot before question 1, with IP showing highlighted.

Include screen shot of Print with Selected Packet only and print as displayed marked.

Include a terminal screenshot showing computer IP address on the front page before Question 1, and a full PRINT of the HTTP OK message as the last page.

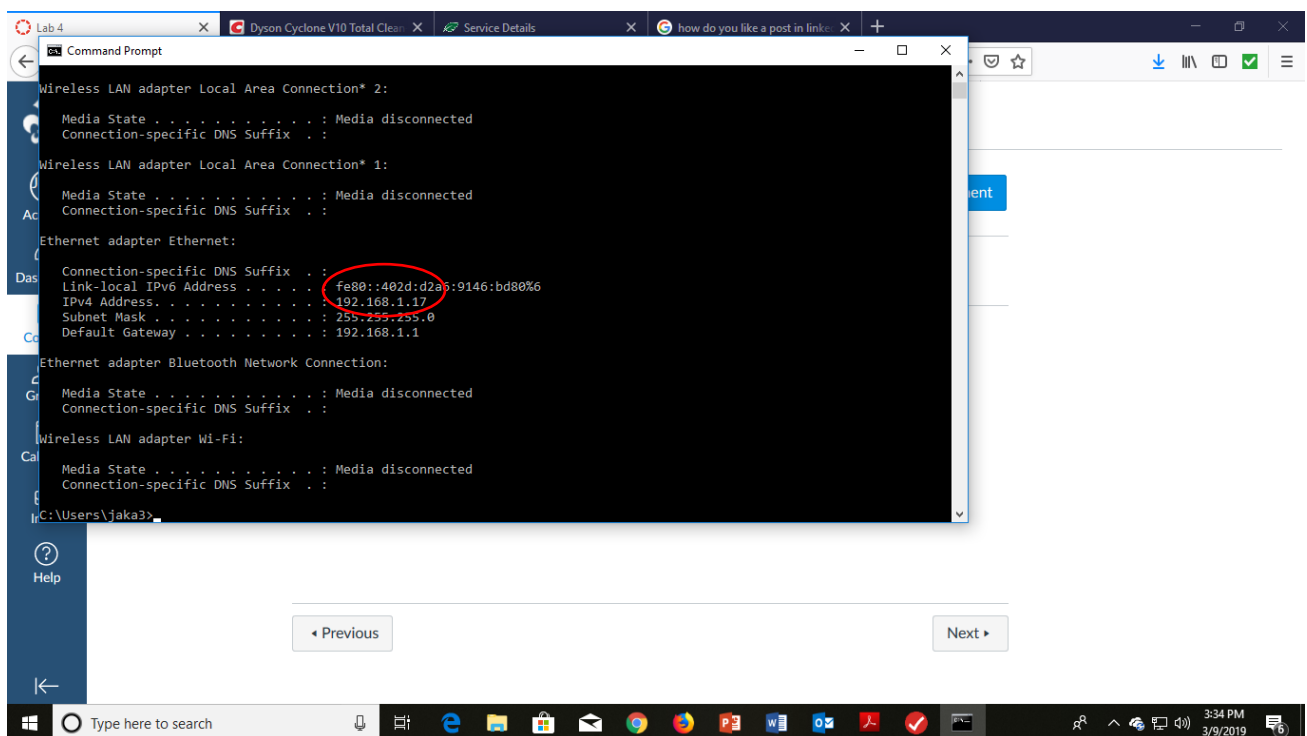
Save all as .pdf before uploading.

Follow the instructions in Lab 2 and expand the IP detail section. • Pay attention to the text in bold. I expect you to explain?

Questions:

1. What is the IP address of your computer? – **Wireshark screenshot not, Terminal**

My IP address is shown below, 192.168.1.17 in this terminal screen shot.



```
Lab 4 X Dyson Cyclone V10 Total Clea X Service Details X how do you like a post in link X +
Command Prompt
Wireless LAN adapter Local Area Connection* 2:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Wireless LAN adapter Local Area Connection* 1:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Ethernet adapter Ethernet:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::402d:d2a6:9146:bd80%6
IPv4 Address. . . . . : 192.168.1.17
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
Ethernet adapter Bluetooth Network Connection:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Wireless LAN adapter Wi-Fi:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
C:\Users\jaka3>
```

2. What is the total length of the datagram?

There are 40 bytes total length.

The image shows a Wireshark packet capture of an Ethernet II frame containing an Internet Protocol Version 4 (IPv4) datagram. The packet list at the top shows packet 100, which is 60 bytes long. The packet details pane shows the following structure:

- Frame 100: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
- Ethernet II, Src: Netgear_bd:73:8c (50:6a:03:bd:73:8c), Dst: WistronI_7e:38:bb (98:ee:cb:7e:38:bb)
- Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.17
 - 0100 = Version: 4
 - 0101 = Header Length: 20 bytes (5)
 - > Differentiated Services Field: 0x20 (DSCP: CS1, ECN: Not-ECT)
 - Total Length: 40
 - Identification: 0xa68f (42639)
 - Flags: 0x4000, Don't fragment
 - Time to live: 49
 - Protocol: TCP (6)
 - Header checksum: 0x1be3 (validation disabled)

The packet bytes pane shows the raw data of the packet, which is 60 bytes long. The data is not fragmented because the fragment offset is set to 0.

3. Has this IP datagram been fragmented? The data is not fragmented because fragment offset is set to 0.

*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-F>

No.	Time	Source	Destination	Protocol	Length	Info
92	15:51:11.877572	192.168.1.17	13.107.42.12	TCP	54	60168 → 443 [ACK] Seq=2098 Ack=9811 Win=65280 Len=0
93	15:51:11.885672	13.107.42.12	192.168.1.17	TCP	60	443 → 60167 [ACK] Seq=9811 Ack=2099 Win=262656 Len=0
94	15:51:11.886376	13.107.42.12	192.168.1.17	TCP	60	443 → 60167 [FIN, ACK] Seq=9811 Ack=2099 Win=262656 Len=0
95	15:51:11.886441	192.168.1.17	13.107.42.12	TCP	54	60167 → 443 [ACK] Seq=2099 Ack=9812 Win=65024 Len=0
96	15:51:11.910896	192.168.1.17	13.107.42.12	TCP	54	60168 → 443 [FIN, ACK] Seq=2098 Ack=9811 Win=65280 Len=0
97	15:51:11.926853	13.107.42.12	192.168.1.17	TCP	60	443 → 60168 [ACK] Seq=9811 Ack=2099 Win=262656 Len=0
98	15:51:11.927644	13.107.42.12	192.168.1.17	TCP	60	443 → 60168 [FIN, ACK] Seq=9811 Ack=2099 Win=262656 Len=0
99	15:51:11.927683	192.168.1.17	13.107.42.12	TCP	54	60168 → 443 [ACK] Seq=2099 Ack=9812 Win=65280 Len=0
100	15:51:12.115495	128.119.245.12	192.168.1.17	TCP	60	80 → 60164 [FIN, ACK] Seq=486 Ack=275 Win=30336 Len=0
101	15:51:12.115579	192.168.1.17	128.119.245.12	TCP	54	60164 → 80 [ACK] Seq=275 Ack=487 Win=261632 Len=0

0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 > Differentiated Services Field: 0x20 (DSCP: CS1, ECN: Not-ECT)
 Total Length: 40
 Identification: 0xa68f (42639)
 > Flags: 0x4000, Don't fragment
 0... .. = Reserved bit: Not set
 .1... .. = Don't fragment: Set
 ..0... .. = More fragments: Not set
 ..0000 0000 0000 = Fragment offset: 0
 Time to live: 49
 Protocol: TCP (6)

0000 98 ee cb 7e 38 bb 50 6a 03 bd 73 8c 08 00 45 20 ...8 Pj ...s...E
 0010 00 28 a6 8f 40 0c 31 06 6b e3 80 77 f5 0c c0 a8 ...k...w...
 0020 01 11 00 50 eb 04 71 93 99 a8 e1 84 4b 8b 50 11 ...P...q...K...P...
 0030 00 ed 54 08 00 00 00 00 48 81 23 d2 ...T...H#

Fragment offset (13 bits) (p frag_offset), 2 bytes

Packets: 101 · Displayed: 101 (100.0%) · Dropped: 0 (0.0%) Profile: Default

Type here to search

4. How many bytes are in the IP header?

There are 20 bytes in the IP header.

*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-F>

No.	Time	Source	Destination	Protocol	Length	Info
92	15:51:11.877572	192.168.1.17	13.107.42.12	TCP	54	60168 → 443 [ACK] Seq=2098 Ack=9811 Win=65280 Len=0
93	15:51:11.885672	13.107.42.12	192.168.1.17	TCP	60	443 → 60167 [ACK] Seq=9811 Ack=2099 Win=262656 Len=0
94	15:51:11.886376	13.107.42.12	192.168.1.17	TCP	60	443 → 60167 [FIN, ACK] Seq=9811 Ack=2099 Win=262656 Len=0
95	15:51:11.886441	192.168.1.17	13.107.42.12	TCP	54	60167 → 443 [ACK] Seq=2099 Ack=9812 Win=65024 Len=0
96	15:51:11.910896	192.168.1.17	13.107.42.12	TCP	54	60168 → 443 [FIN, ACK] Seq=2098 Ack=9811 Win=65280 Len=0
97	15:51:11.926853	13.107.42.12	192.168.1.17	TCP	60	443 → 60168 [ACK] Seq=9811 Ack=2099 Win=262656 Len=0
98	15:51:11.927644	13.107.42.12	192.168.1.17	TCP	60	443 → 60168 [FIN, ACK] Seq=9811 Ack=2099 Win=262656 Len=0
99	15:51:11.927683	192.168.1.17	13.107.42.12	TCP	54	60168 → 443 [ACK] Seq=2099 Ack=9812 Win=65280 Len=0
100	15:51:12.115495	128.119.245.12	192.168.1.17	TCP	60	80 → 60164 [FIN, ACK] Seq=486 Ack=275 Win=30336 Len=0
101	15:51:12.115579	192.168.1.17	128.119.245.12	TCP	54	60164 → 80 [ACK] Seq=275 Ack=487 Win=261632 Len=0

> Frame 100: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
 > Ethernet II, Src: Netgear_bd73:8c (50:6a:03:bd:73:8c), Dst: WistronI_7e:38:bb (98:ee:cb:7e:38:bb)
 > Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.17
 0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 > Differentiated Services Field: 0x20 (DSCP: CS1, ECN: Not-ECT)
 Total Length: 40
 Identification: 0xa68f (42639)
 > Flags: 0x4000, Don't fragment
 0... .. = Reserved bit: Not set
 .1... .. = Don't fragment: Set
 ..0... .. = More fragments: Not set
 ..0000 0000 0000 = Fragment offset: 0
 Time to live: 49
 Protocol: TCP (6)

0000 98 ee cb 7e 38 bb 50 6a 03 bd 73 8c 08 00 45 20 ...8 Pj ...s...E
 0010 00 28 a6 8f 40 0c 31 06 6b e3 80 77 f5 0c c0 a8 ...k...w...
 0020 01 11 00 50 eb 04 71 93 99 a8 e1 84 4b 8b 50 11 ...P...q...K...P...
 0030 00 ed 54 08 00 00 00 00 48 81 23 d2 ...T...H#

Fragment offset (13 bits) (p frag_offset), 2 bytes

Packets: 101 · Displayed: 101 (100.0%) · Dropped: 0 (0.0%) Profile: Default

Type here to search

5. How many bytes are in the payload of the IP datagram? **Explain how you determined the number of payload bytes.** There are 20 bytes in the IP header, and 40 bytes total length, this means there are 20 bytes in the payload of the IP datagram because you subtract out the 20 from the header.

The image shows a Wireshark packet capture window titled "*Ethernet". The packet list pane at the top shows several TCP packets. Packet 100 is selected, showing a frame of 60 bytes on wire (480 bits) and 60 bytes captured (480 bits) on interface 0. The packet details pane shows the following structure:

- Frame 100: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
- Ethernet II, Src: Netgear bd:73:8c (50:6a:03:bd:73:8c), Dst: WistronI_7e:38:bb (98:ee:cb:7e:38:bb)
- Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.17
 - 0100 = Version: 4
 - 0101 = Header Length: 20 bytes (5)
 - > Differentiated Services Field: 0x20 (DSCP: CS1, ECN: Not-ECT)
 - Total Length: 40**
 - Identification: 0xae68f (42639)
 - Flags: 0x4000, Don't fragment
 - Time to live: 49
 - Protocol: TCP (6)
 - Header checksum: 0x5b3e3 (validation disabled)
- Header checksum: 0x5b3e3 (validation disabled)

The packet bytes pane shows the raw data of the packet, with the first 20 bytes (the IP header) highlighted in blue. The data is displayed in hexadecimal and ASCII columns.

At the bottom of the window, the status bar shows "Total Length (p.len), 2 bytes" and "Packets: 101 - Displayed: 101 (100.0%) - Dropped: 0 (0.0%)". The system tray at the bottom right shows the time as 3:57 PM on 3/9/2019.

Print screen, final page.

