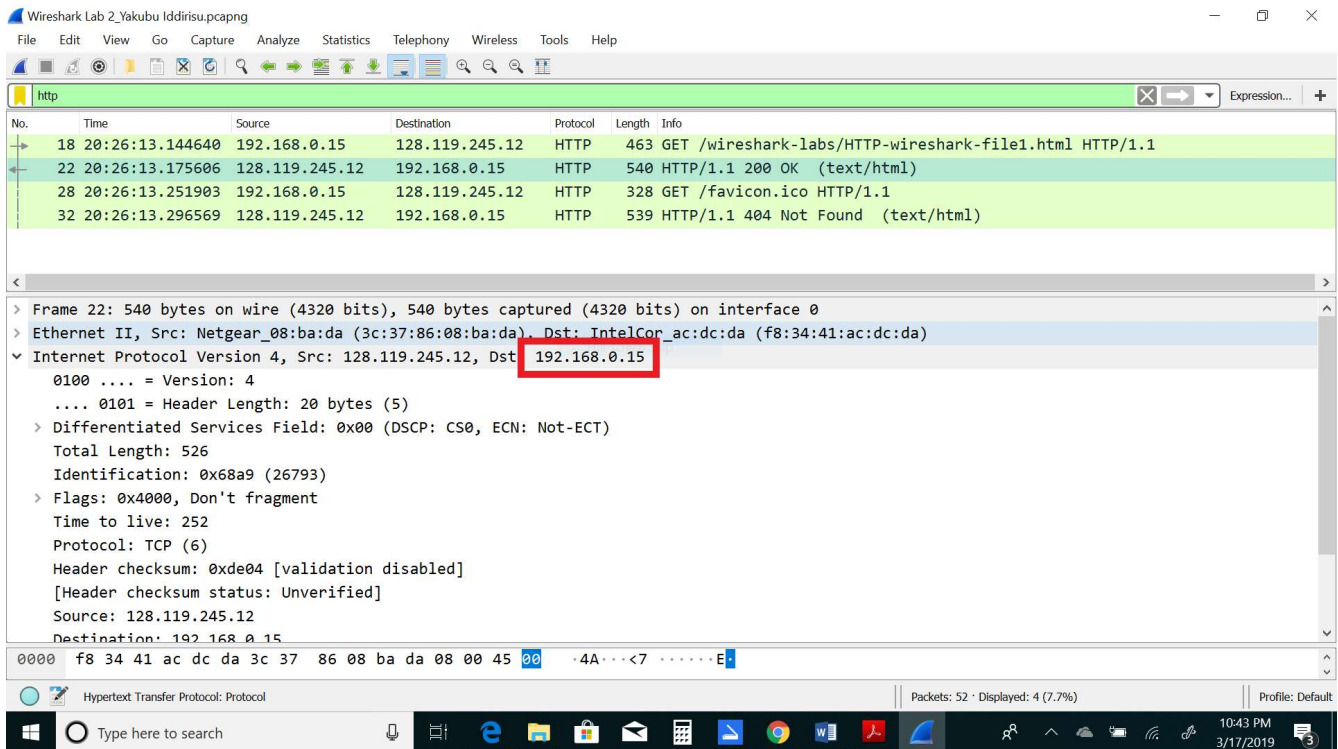


Questions:

1. What is the IP address of your computer? – **Wireshark screenshot not, Terminal**
192.168.0.15



2. What is the total length of the datagram?

526 bytes

Wireshark Lab 2_Yakubu Iddirisu.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
18	20:26:13.144640	192.168.0.15	128.119.245.12	HTTP	463	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
22	20:26:13.175606	128.119.245.12	192.168.0.15	HTTP	540	HTTP/1.1 200 OK (text/html)
28	20:26:13.251903	192.168.0.15	128.119.245.12	HTTP	328	GET /favicon.ico HTTP/1.1
32	20:26:13.296569	128.119.245.12	192.168.0.15	HTTP	539	HTTP/1.1 404 Not Found (text/html)

Ethernet II, Src: Netgear_08:ba:da (3c:37:86:08:ba:da), Dst: IntelCor_ac:dc:da (f8:34:41:ac:dc:da)

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.15

- 0100 = Version: 4
- 0101 = Header Length: 20 bytes (5)
- > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 526**
- Identification: 0x68a9 (26793)
- > Flags: 0x4000, Don't fragment
- Time to live: 252
- Protocol: TCP (6)
- Header checksum: 0xde04 [validation disabled]
- [Header checksum status: Unverified]
- Source: 128.119.245.12
- Destination: 192.168.0.15

Transmission Control Protocol, Src Port: 80, Dst Port: 60324, Seq: 1, Ack: 410, Len: 486

0000 f8 34 41 ac dc da 3c 37 86 08 ba da 08 00 45 00 4A ..<7.....E

Hypertext Transfer Protocol: Protocol

Packets: 52 · Displayed: 4 (7.7%)

Profile: Default

Type here to search

11:35 PM 3/17/2019

3. Has this IP datagram been fragmented?

No, the IP datagram has not been fragmented. Flag is 0 and Offset is also 0.

The image shows a Wireshark packet capture window. The top pane displays a list of captured packets. The second pane shows the details of the selected packet (No. 22), which is an HTTP 200 OK response. The third pane shows the raw packet data in hexadecimal and ASCII.

Packet list:

No.	Time	Source	Destination	Protocol	Length	Info
18	20:26:13.144640	192.168.0.15	128.119.245.12	HTTP	463	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
22	20:26:13.175606	128.119.245.12	192.168.0.15	HTTP	540	HTTP/1.1 200 OK (text/html)
28	20:26:13.251903	192.168.0.15	128.119.245.12	HTTP	328	GET /favicon.ico HTTP/1.1
32	20:26:13.296569	128.119.245.12	192.168.0.15	HTTP	539	HTTP/1.1 404 Not Found (text/html)

Packet details (No. 22):

- Ethernet II, Src: Netgear_08:ba:da (3c:37:86:08:ba:da), Dst: IntelCor_ac:dc:da (f8:34:41:ac:dc:da)
- Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.15
 - 0100 = Version: 4
 - 0101 = Header Length: 20 bytes (5)
 - Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 - Total Length: 526
 - Identification: 0x68a9 (26793)
 - Flags: 0x4000, Don't fragment
 - 0... .. = Reserved bit: Not set
 - .1.. .. = Don't fragment: Set
 - ..0. = More fragments: Not set
 - ...0 0000 0000 0000 = Fragment offset: 0
 - Time to live: 252
 - Protocol: TCP (6)
 - Header checksum: 0xde04 [validation disabled]

Raw packet data (hex): f8 34 41 ac dc da 3c 37 86 08 ba da 08 00 45 00

4. How many bytes are in the IP header?

20 bytes in the IP Header

The image shows a Wireshark packet capture analysis. The top pane displays a list of captured packets. The second pane shows the details of the selected packet (No. 18), which is an HTTP GET request. The third pane shows the packet bytes, with the IP header (0000 f8 34 41 ac dc da 3c 37 86 08 ba da 08 00 45 00) highlighted. The details pane for the Internet Protocol Version 4 (IP) shows the following fields:

- Version: 4
- Header Length: 20 bytes (5)
- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 526
- Identification: 0x68a9 (26793)
- Flags: 0x4000, Don't fragment
- Time to live: 252
- Protocol: TCP (6)
- Header checksum: 0xde04 [validation disabled]
- [Header checksum status: Unverified]
- Source: 128.119.245.12
- Destination: 192.168.0.15

The packet bytes pane shows the raw data of the packet, with the IP header (0000 f8 34 41 ac dc da 3c 37 86 08 ba da 08 00 45 00) highlighted. The details pane for the Transmission Control Protocol (TCP) shows the following fields:

- Source Port: 80
- Destination Port: 60324
- Sequence: 1
- Acknowledgment: 410
- Length: 486

The packet bytes pane shows the raw data of the packet, with the IP header (0000 f8 34 41 ac dc da 3c 37 86 08 ba da 08 00 45 00) highlighted.

5. How many bytes are in the payload *of the IP datagram*? Explain how you determined the number of payload bytes.

526 – 20 = 506 bytes.

There are 20 bytes in the IP header and 526 bytes total length. This gives 506 bytes in the payload of the IP datagram, by subtracting the header size from the total datagram.

The image shows a Wireshark packet capture window titled "Wireshark Lab 2_Yakubu Iddirisu.pcapng". The packet list pane shows four packets, with packet 22 selected. The packet details pane shows the structure of the selected packet, which is an Ethernet II frame containing an Internet Protocol Version 4 (IP) datagram. The IP header fields are expanded, showing the following values:

- Version: 4
- Header Length: 20 bytes (5)
- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 526
- Identification: 0x68a9 (26793)
- Flags: 0x4000, Don't fragment
- Time to live: 252
- Protocol: TCP (6)
- Header checksum: 0xde04 [validation disabled]

The packet bytes pane shows the raw data of the packet, starting with the Ethernet II header (f8 34 41 ac dc da 3c 37 86 08 ba da 08 00 45 00) and the IP header (4a 00 00 00 00 00 00 00).