

# Assignment 1

## Computer Networks

Vikas Gola

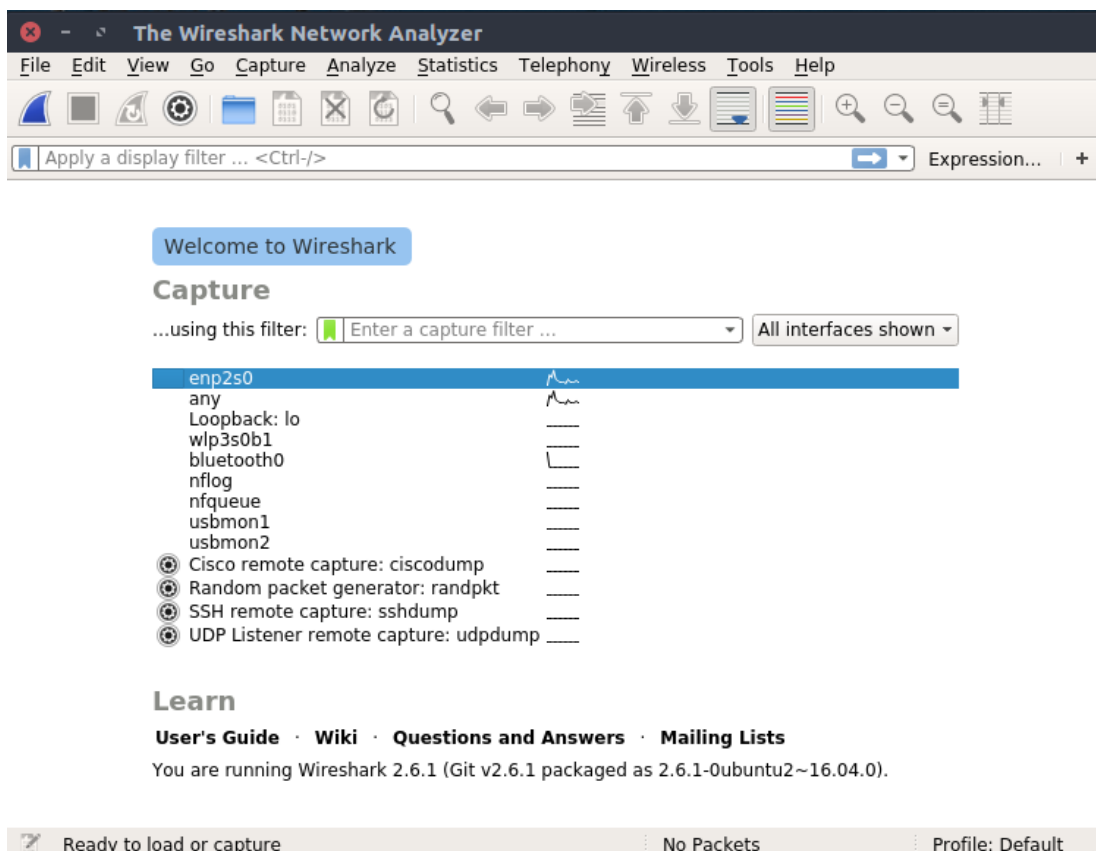
September 10, 2018

**Question 1** What are the network interfaces available on your computer?  
Which network did you eventually select in your experiments.

**Answer** The following network interfaces are available

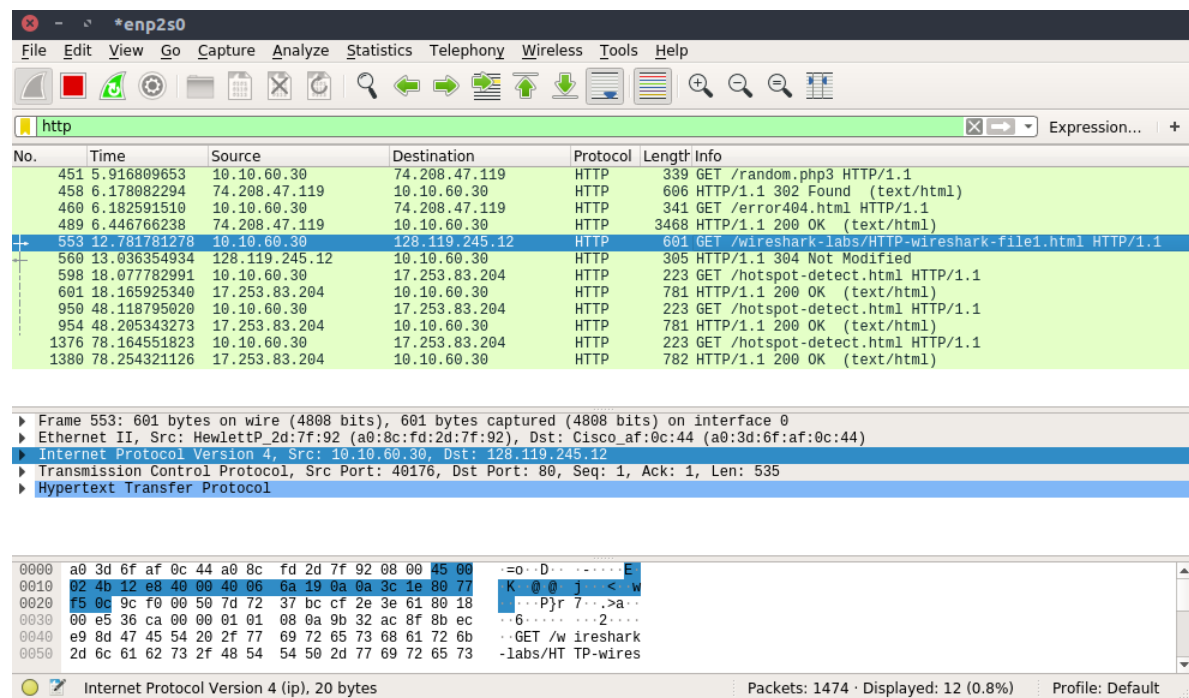
- enp2s0
- any
- Loopback:lo
- wlp3s0b1
- bluetooth0
- nflog
- nfqueue
- usbmon1
- usbmon2

enp2s0 network interface is selected



**Question 2** Which application layer protocol is used in this case?

**Answer** HyperText Transfer Protocol(HTTP).



**Question 3** What are the other protocols used and displayed in the unfiltered packet listing window of wireshark, besides the one that you answered in Q2?

**Answer** The other protocols in unfiltered packet listing windows are

- UDP
- TLS
- CDP
- TCP
- ARP
- STP
- SSDP
- DNS

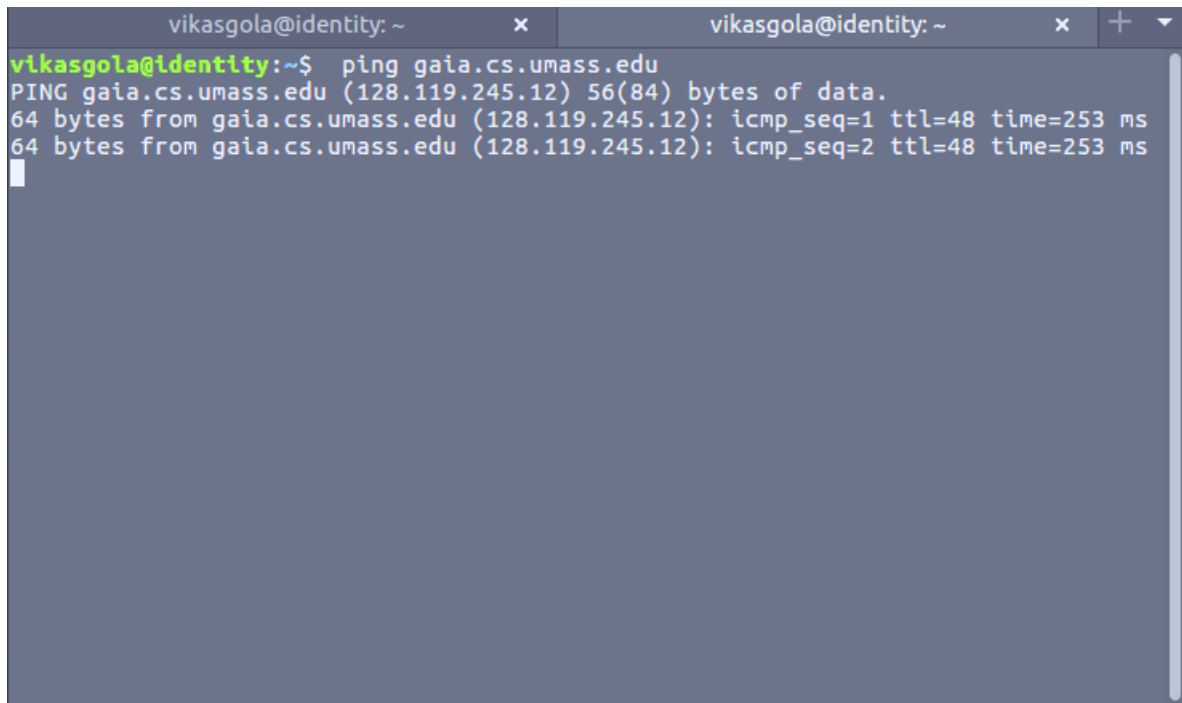
- MDNS
- NBNS
- LLMNR
- DHCP

No.	Time	Source	Destination	Protocol	Length	Info
59...	414.6244...	117.18.232.200	10.10.60.30	TCP	60	[TCP Keep-Alive ACK] 443 → 56892 [A...
59...	415.2294...	10.10.60.103	10.10.60.255	UDP	305	54915 → 54915 Len=263
59...	415.2846...	Cisco_53:ee:27	Spanning-tree-...	STP	60	Conf. Root = 4096/60/a0:3d:6f:af:0c...
59...	415.3291...	10.10.41.186	10.10.60.184	TCP	66	[TCP Retransmission] 19814 → 7680 [A...
59...	415.3721...	HewlettP_e3:90...	Broadcast	ARP	60	Who has 10.10.60.10? Tell 10.10.60...
59...	415.4110...	fe80::16b3:1ff...	ff02::fb	MDNS	121	Standard query 0x0000 TXT VIVASVAN...
59...	416.2330...	10.10.60.103	10.10.60.255	UDP	305	54915 → 54915 Len=263
59...	416.2453...	HewlettP_e3:90...	Broadcast	ARP	60	Who has 10.10.60.10? Tell 10.10.60...
59...	416.4864...	10.10.60.245	10.10.60.255	NBNS	92	Name query NB WPAD<00>
59...	416.4869...	10.10.60.245	224.0.0.251	MDNS	70	Standard query 0x0000 A wpad.local,...
59...	416.4869...	fe80::3468:b48...	ff02::fb	MDNS	90	Standard query 0x0000 A wpad.local,...
59...	416.4872...	fe80::3468:b48...	ff02::1:3	LLMNR	84	Standard query 0x145f A wpad
59...	416.4873...	10.10.60.245	224.0.0.252	LLMNR	64	Standard query 0x145f A wpad
59...	416.6384...	fe80::3b5b:1b6...	ff02::fb	MDNS	180	Standard query 0x0000 PTR _ftp._tcp...
59...	416.6385...	10.10.60.30	224.0.0.251	MDNS	160	Standard query 0x0000 PTR _ftp._tcp...
59...	416.8966...	fe80::c112:900...	ff02::1:2	LLMNR	84	Standard query 0x145f A wpad
59...	416.8966...	10.10.60.245	224.0.0.252	LLMNR	64	Standard query 0x145f A wpad
59...	417.2339...	10.10.60.103	10.10.60.255	UDP	305	54915 → 54915 Len=263
59...	417.2356...	10.10.60.245	10.10.60.255	NBNS	92	Name query NB WPAD<00>
59...	417.2453...	HewlettP_e3:90...	Broadcast	ARP	60	Who has 10.10.60.10? Tell 10.10.60...
59...	417.2851...	Cisco_53:ee:27	Spanning-tree-...	STP	60	Conf. Root = 4096/60/a0:3d:6f:af:0c...
59...	417.6655...	fe80::c112:900...	ff02::1:2	DHCPv6	145	Solicit XID: 0xee8581 CID: 00010001...
59...	417.9433...	Cisco_af:0c:44	Broadcast	ARP	60	Who has 10.10.60.21? Tell 10.10.60.1...

Internet Protocol Version 4 (ip), 20 bytes      Packets: 10360 · Displayed: 10360 (100.0%)      Profile: Default

**Question 4** What is the IPA of your machine? What is the IPA of the destination machine? Is there any way by which you can ascertain that the IPA of the destination indeed is the same as that you observed in wireshark? If so, how ?

**Answer** IPA of my machine is 10.10.60.30. IP address of destination is 128.119.245.12. IPA of destination can be verified by using the ping on the host of website which is [gaia.cs.umass.edu](http://gaia.cs.umass.edu).

A terminal window with two tabs, both labeled 'vikasgola@identity: ~'. The active tab shows a command prompt where the user has entered 'ping gaia.cs.umass.edu'. The output shows two successful ping responses from 128.119.245.12, each with 64 bytes of data, an icmp sequence number of 1 and 2 respectively, a TTL of 48, and a response time of 253 ms.

```
vikasgola@identity:~$ ping gaia.cs.umass.edu
PING gaia.cs.umass.edu (128.119.245.12) 56(84) bytes of data.
64 bytes from gaia.cs.umass.edu (128.119.245.12): icmp_seq=1 ttl=48 time=253 ms
64 bytes from gaia.cs.umass.edu (128.119.245.12): icmp_seq=2 ttl=48 time=253 ms
```

**Question 5** What is the class of the IPA of the source machine ? That of destination machine?

**Answer** class A, class B

**Question 6** How many bits were captured in this packet? At what time was this packet captured?

**Answer** 490 bytes were captured in this packet on date Aug 20,2018 at time 02:39:42.595559043 IST.

http						
Vo.	Time	Source	Destination	Protocol	Length	Info
49	3.418995...	10.10.60.30	104.119.49.32	HTTP	223	GET /hotspot-detect.html HTTP/1.1
51	3.452361...	104.119.49.32	10.10.60.30	HTTP	359	HTTP/1.1 200 OK (text/html)
186	7.834254...	10.10.60.30	128.119.245.12	HTTP	490	GET /wireshark-labs/HTTP-wireshark-
195	8.089195...	128.119.245.12	10.10.60.30	HTTP	552	HTTP/1.1 200 OK (text/html)

Frame 186: 490 bytes on wire (3920 bits), 490 bytes captured (3920 bits) on interface 0  
 Interface id: 0 (enp2s0)  
 Encapsulation type: Ethernet (1)  
 Arrival Time: Aug 20, 2018 02:39:42.595559043 IST  
 [Time shift for this packet: 0.000000000 seconds]  
 Epoch Time: 1534712982.595559043 seconds  
 [Time delta from previous captured frame: 0.000295889 seconds]  
 [Time delta from previous displayed frame: 4.381893251 seconds]  
 [Time since reference or first frame: 7.834254635 seconds]  
 Frame Number: 186  
 Frame Length: 490 bytes (3920 bits)  
 Capture Length: 490 bytes (3920 bits)  
 [Frame is marked: False]  
 [Frame is ignored: False]  
 [Protocols in frame: eth:ethertype:ip:tcp:http]  
 [Coloring Rule Name: HTTP]  
 [Coloring Rule String: http || tcp.port == 80 || http2]  
 Ethernet II, Src: HewlettP\_2d:7f:92 (a0:8c:fd:2d:7f:92), Dst: Cisco\_af:0c:44 (a0:3d:6f:af:0c:44)  
 Internet Protocol Version 4, Src: 10.10.60.30, Dst: 128.119.245.12

**Question 7** What is the interface id used? What is the address of the interface?

**Answer** Interface id is 0 (enp2s0) and address of this interface is a0:8c:fd:2d:7f:92.

Frame Number: 186
Frame Length: 490 bytes (3920 bits)
Capture Length: 490 bytes (3920 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:tcp:http]
[Coloring Rule Name: HTTP]
[Coloring Rule String: http    tcp.port == 80    http2]
▼ Ethernet II, Src: HewlettP_2d:7f:92 (a0:8c:fd:2d:7f:92), Dst: Cisco_af:0c:44 (a0:3d:6f:af:0c:44)
Destination: Cisco_af:0c:44 (a0:3d:6f:af:0c:44)
Source: HewlettP_2d:7f:92 (a0:8c:fd:2d:7f:92)
Address: HewlettP_2d:7f:92 (a0:8c:fd:2d:7f:92)
... ..0. .... = LG bit: Globally unique address (factory default)
... ..0. .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 10.10.60.30, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 40762, Dst Port: 80, Seq: 1, Ack: 1, Len: 424
Hypertext Transfer Protocol

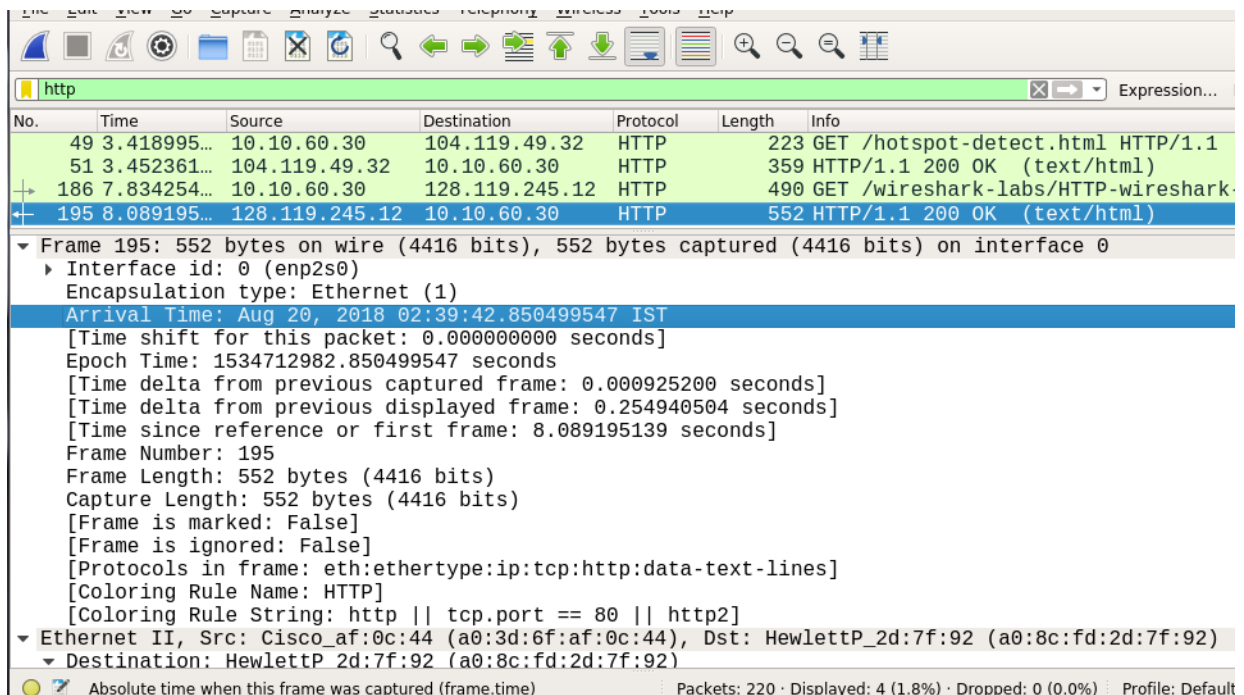
Source or Destination Hardware Address (eth.addr), 6 bytes      Packets: 220 · Displayed: 4 (1.8%) · Dropped: 0 (0.0%)      Profile: Default

**Question 8** How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packet-listing window is the amount of time, in seconds,

since Wireshark tracing began. To display the Time field in time- of-day format, select the Wireshark View pull down menu, then select Time Display Format, then select Time-of-day.)

**Answer** HTTP GET message was sent at 02:39:42.595559043 IST and HTTP OK was received at 02:39:42.850499547 IST.

Time taken = received time - sent time  
 = 42.850499547 - 42.595559043  
 = 0.254940504 seconds.

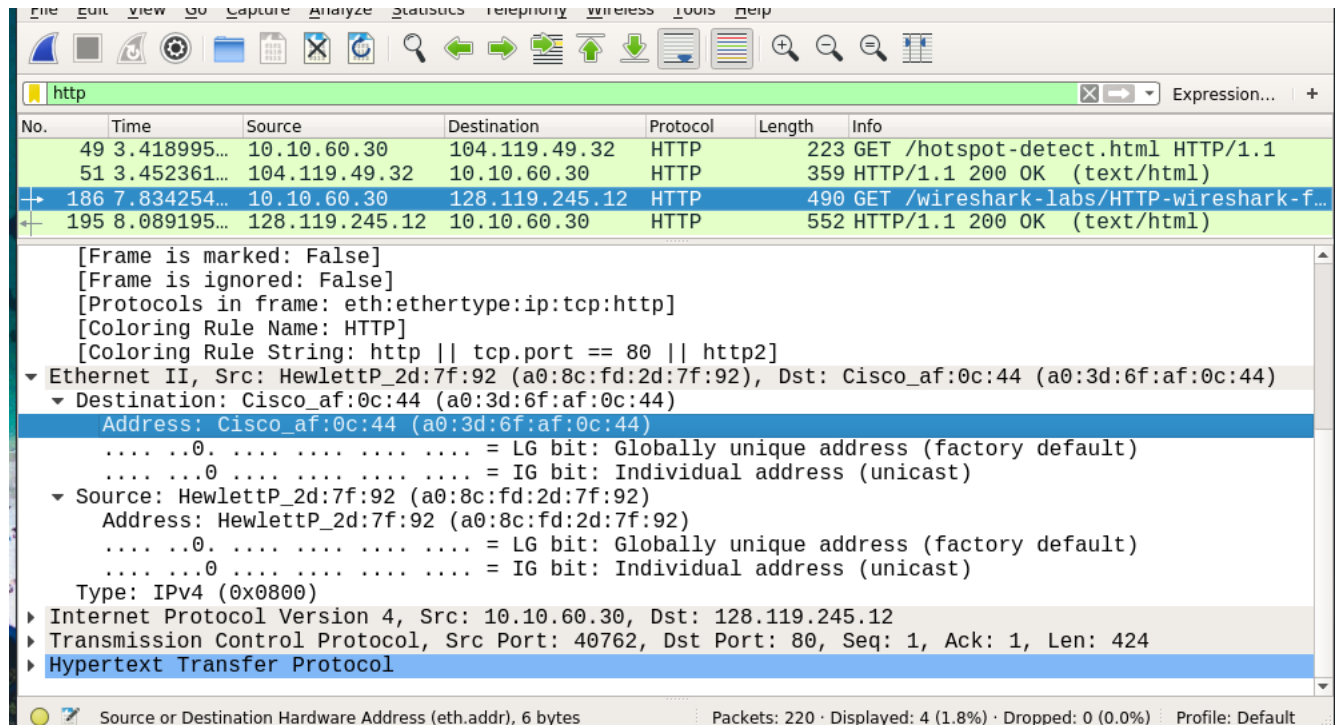


**Question 10** Print the two HTTP messages (GET and OK) referred to in question above. To do so, select Print from the Wireshark File command menu, and select the "Selected Packet Only" and "Print as displayed" radial buttons, and then click OK.

**Answer** HTTP GET message and OK message can be checked at last of the pdf file respectively.

**Question 11** What is the destination physical address of the first packet captured? What device does it belong to? Show where in the capture would you find this information.

**Answer** Physical address of the destination in the first packet is a0:3d:6f:af:0c:44 which is find in the destination tab of Ethernet Block.



**Question 12** How many bytes of header does the first frame sent have? Show where in the capture would you find this information.

**Answer** 20 bytes of header have been sent and this information is find in Internet Protocol Version 4 block.



No.	Time	Source	Destination	Protocol	Length	Info
49	3.418995...	10.10.60.30	104.119.49.32	HTTP	223	GET /hotspot-detect.html HTTP/1.1
51	3.452361...	104.119.49.32	10.10.60.30	HTTP	359	HTTP/1.1 200 OK (text/html)
186	7.834254...	10.10.60.30	128.119.245.12	HTTP	490	GET /wireshark-labs/HTTP-wireshark
195	8.089195...	128.119.245.12	10.10.60.30	HTTP	552	HTTP/1.1 200 OK (text/html)

Frame 186: 490 bytes on wire (3920 bits), 490 bytes captured (3920 bits) on interface 0

Ethernet II, Src: HewlettP\_2d:7f:92 (a0:8c:fd:2d:7f:92), Dst: Cisco\_af:0c:44 (a0:3d:6f:af:0c:44)

Internet Protocol Version 4, Src: 10.10.60.30, Dst: 128.119.245.12

- 0100 .... = Version: 4
- .... 0101 = Header Length: 20 bytes (5)
- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 476
- Identification: 0x5ea6 (24230)
- Flags: 0x4000, Don't fragment
- Time to live: 64
- Protocol: TCP (6)
- Header checksum: 0x1eca [validation disabled]
- [Header checksum status: Unverified]
- Source: 10.10.60.30
- Destination: 128.119.245.12

Transmission Control Protocol, Src Port: 40762, Dst Port: 80, Seq: 1, Ack: 1, Len: 424

Hypertext Transfer Protocol

Flags (3 bits) (io.flags), 2 bytes

Packets: 220 · Disposed: 4 (1.8%) · Dropped: 0 (0.0%) · Profile: Default

**Question 13** By looking at the Ethernet header of a frame, can we determine if it contains an IP packet? Show where in the capture would you find this information.

**Answer** Yes, we can easily determine it by looking at the "type" in Ethernet header of a frame.

**Question 14** Is it possible to know if the first packet captured has TCP or UDP as transport protocol by looking at the IP header? Explain and show where in the capture would you find this information.

**Answer** Yes, it is possible to find the transport protocol type of first captured packet which is visible in IP header written as "Protocol: TCP" indicates the TCP transport protocol.

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.10.60.30

0100 .... = Version: 4

.... 0101 = Header Length: 20 bytes (5)

- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 538
- Identification: 0x70d9 (28889)
- Flags: 0x4000, Don't fragment
- Time to live: 48
- Protocol: TCP (6)
- Header checksum: 0x1c59 [validation disabled]
- [Header checksum status: Unverified]
- Source: 128.119.245.12
- Destination: 10.10.60.30

Transmission Control Protocol, Src Port: 80, Dst Port: 40762, Seq: 1, Ack: 425, Len: 496

**Question 15** In the SYN, ACK. What are the source and destination ports? Are these the same for the client and the server? Explain why.

**Answer** Source Port: 40762 and Destination Port:80

No, these are not same for client and server as same port indicates same process and also there are some fix ports for handling specific type requests.

**Question 16** Why does the Server Hello message sent by the server have 1 as a relative sequence number and 185 as a relative acknowledgement number.

**Answer** Wireshark always displayed a SYN(Sequence) and ACK(Acknowledgement) number relative to the first seen segment for that conversation. That's why all SYN and ACK numbers always start at 0 for the first packet seen in each conversation. After setting up the connection between client and server, when server starts transmitting data, relative ACK number is equal to (Bytes sent +1). That's why in this example, relative SEQ number is 1 and relative ACK is (184+1=185), because packets sent till Server Hello message are 184.

```
+ Ethernet II, Src: HewlettP_2d:7f:92 (a0:8c:fd:2d:7f:92), Dst: Cisco_af:0c:44 (a0:3d:6f:af:0c:44)
+ Internet Protocol Version 4, Src: 10.10.60.30, Dst: 128.119.245.12
- Transmission Control Protocol, Src Port: 40762, Dst Port: 80, Seq: 1, Ack: 1, Len: 424
  Source Port: 40762
  Destination Port: 80
  [Stream index: 9]
  [TCP Segment Len: 424]
  Sequence number: 1 (relative sequence number)
  [Next sequence number: 425 (relative sequence number)]
  Acknowledgment number: 1 (relative ack number)
  Header Length: 32 bytes
+ Flags: 0x018 (PSH, ACK)
  Window size value: 229
  [Calculated window size: 29312]
  [Window size scaling factor: 128]
  Checksum: 0xdb83 [unverified]
  [Checksum Status: Unverified]
  Urgent pointer: 0
+ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
- [SEQ/ACK analysis]
  [iRTT: 0.253269255 seconds]
  [Bytes in flight: 424]
  [Bytes sent since last PSH flag: 424]
+ Hypertext Transfer Protocol
```

**Question 17** What is the first sequence number sent by the server to the client. Why is it not the 0 displayed by Wireshark?

**Answer** As explained in answer of last question, Wireshark always displayed a SYN(Sequence) and ACK(Acknowledgement) number relative to the first seen segment for that conversation. Because, client has already sent some packets to server and hence packets sent by server is not the first in communication and it's not 0.

```
+ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.10.60.30
- Transmission Control Protocol, Src Port: 80, Dst Port: 40762, Seq: 1, Ack: 425, Len: 486
  Source Port: 80
  Destination Port: 40762
  [Stream index: 9]
  [TCP Segment Len: 486]
  Sequence number: 1      (relative sequence number)
  [Next sequence number: 487      (relative sequence number)]
  Acknowledgment number: 425      (relative ack number)
  Header Length: 32 bytes
  + Flags: 0x018 (PSH, ACK)
  Window size value: 235
  [Calculated window size: 30080]
  [Window size scaling factor: 128]
  Checksum: 0xfb0a [unverified]
  [Checksum Status: Unverified]
  Urgent pointer: 0
  + Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  - [SEQ/ACK analysis]
    [iRTT: 0.253269255 seconds]
    [Bytes in flight: 486]
    [Bytes sent since last PSH flag: 486]
+ Hypertext Transfer Protocol
+ Line-based text data: text/html
```

```
Frame 186: 490 bytes on wire (3920 bits), 490 bytes captured (3920 bits) on interface 0
Interface id: 0 (enp2s0)
Encapsulation type: Ethernet (1)
Arrival Time: Aug 20, 2018 02:39:42.595559043 IST
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1534712982.595559043 seconds
[Time delta from previous captured frame: 0.000295889 seconds]
[Time delta from previous displayed frame: 4.381893251 seconds]
[Time since reference or first frame: 7.834254635 seconds]
Frame Number: 186
Frame Length: 490 bytes (3920 bits)
Capture Length: 490 bytes (3920 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:tcp:http]
[Coloring Rule Name: HTTP]
[Coloring Rule String: http || tcp.port == 80 || http2]
Ethernet II, Src: HewlettP_2d:7f:92 (a0:8c:fd:2d:7f:92), Dst: Cisco_af:0c:44 (a0:3d:6f:af:0c:44)
Destination: Cisco_af:0c:44 (a0:3d:6f:af:0c:44)
Address: Cisco_af:0c:44 (a0:3d:6f:af:0c:44)
.... ..0. .... = LG bit: Globally unique address (factory default)
.... ..0. .... = IG bit: Individual address (unicast)
Source: HewlettP_2d:7f:92 (a0:8c:fd:2d:7f:92)
Address: HewlettP_2d:7f:92 (a0:8c:fd:2d:7f:92)
.... ..0. .... = LG bit: Globally unique address (factory default)
.... ..0. .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 10.10.60.30, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 40762, Dst Port: 80, Seq: 1, Ack: 1, Len: 424
Hypertext Transfer Protocol
```

```
195 8.089195139 128.119.245.12 10.10.60.30 HTTP 552 HTTP/1.1 200 OK (text/html)
Frame 195: 552 bytes on wire (4416 bits), 552 bytes captured (4416 bits) on interface 0
Interface id: 0 (enp2s0)
Encapsulation type: Ethernet (1)
Arrival Time: Aug 20, 2018 02:39:42.850499547 IST
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1534712982.850499547 seconds
[Time delta from previous captured frame: 0.000925200 seconds]
[Time delta from previous displayed frame: 0.254940504 seconds]
[Time since reference or first frame: 8.089195139 seconds]
Frame Number: 195
Frame Length: 552 bytes (4416 bits)
Capture Length: 552 bytes (4416 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:tcp:http:data-text-lines]
[Coloring Rule Name: HTTP]
[Coloring Rule String: http || tcp.port == 80 || http2]
Ethernet II, Src: Cisco_af:0c:44 (a0:3d:6f:af:0c:44), Dst: HewlettP_2d:7f:92 (a0:8c:fd:2d:7f:92)
Destination: HewlettP_2d:7f:92 (a0:8c:fd:2d:7f:92)
Address: HewlettP_2d:7f:92 (a0:8c:fd:2d:7f:92)
.... ..0. .... = LG bit: Globally unique address (factory default)
.... ...0 .... = IG bit: Individual address (unicast)
Source: Cisco_af:0c:44 (a0:3d:6f:af:0c:44)
Address: Cisco_af:0c:44 (a0:3d:6f:af:0c:44)
.... ..0. .... = LG bit: Globally unique address (factory default)
.... ...0 .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.10.60.30
Transmission Control Protocol, Src Port: 80, Dst Port: 40762, Seq: 1, Ack: 425, Len: 486
Hypertext Transfer Protocol
Line-based text data: text/html (4 lines)
```