

Questions:

1. What is the Internet address of your computer?

192.168.0.15

The image shows a Wireshark network traffic capture window. The top pane displays a list of captured packets. The second packet, at time 60.699537, is an HTTP GET request from source IP 192.168.0.15 to destination IP 128.119.245.12. The packet details pane shows the following information:

- Frame 1485: 464 bytes on wire (3712 bits), 464 bytes captured (3712 bits) on interface 0
- Ethernet II, Src: IntelCor_ac:dc:da (f8:34:41:ac:dc:da), Dst: Netgear_08:ba:da (3c:37:86:08:ba:da)
- Internet Protocol Version 4, Src: 192.168.0.15, Dst: 128.119.245.12
- Transmission Control Protocol, Src Port: 51089, Dst Port: 80, Seq: 1, Ack: 1, Len: 410
- Hypertext Transfer Protocol
 - GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
 - User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134\r\n
 - Accept-Language: en-US\r\n
 - Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
 - Upgrade-Insecure-Requests: 1\r\n

The bottom pane shows the raw packet data in hexadecimal and ASCII format.

- List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.

SSDP
ARP
ICMP

Wireshark Lab 1.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Protocol	Length	Info
41	20:11:21.980834	192.168.0.1	239.255.255.250	SSDP	326	NOTIFY * HTTP/1.1
42	20:11:21.980837	192.168.0.1	239.255.255.250	SSDP	317	NOTIFY * HTTP/1.1
43	20:11:21.981428	192.168.0.1	239.255.255.250	SSDP	391	NOTIFY * HTTP/1.1
44	20:11:22.894020	Netgear_08:ba:d9	Broadcast	ARP	60	Who has 192.168.0.17? Tell 98.169.53.74
45	20:11:25.079340	Netgear_08:ba:d9	Broadcast	ARP	60	Who has 192.168.0.17? Tell 98.169.53.74
46	20:11:28.717168	fe80::3e37:86ff...	ff02::1	ICMP	174	Router Advertisement from 3c:37:86:08:ba:da
47	20:11:29.852071	Netgear_08:ba:d9	Broadcast	ARP	60	Who has 192.168.0.17? Tell 98.169.53.74
48	20:11:48.707326	13.91.60.30	192.168.0.15	TLSv...	149	Application Data
49	20:11:48.747952	192.168.0.15	13.91.60.30	TCP	54	49935 → 443 [ACK] Seq=1 Ack=96 Win=254 Len=0
50	20:11:50.936232	192.168.0.1	239.255.255.250	SSDP	381	NOTIFY * HTTP/1.1
51	20:11:50.937694	192.168.0.1	239.255.255.250	SSDP	326	NOTIFY * HTTP/1.1
52	20:11:50.939359	192.168.0.1	239.255.255.250	SSDP	317	NOTIFY * HTTP/1.1
53	20:11:50.940670	192.168.0.1	239.255.255.250	SSDP	391	NOTIFY * HTTP/1.1

> Frame 1496: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface 0

> 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)

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

0010 01 de d5 3e 40 00 fc 06 71 9f 80 77 f5 0c c0 a8 ...>@... q..w....

0020 00 0f 00 50 c7 91 05 ec c8 f9 b3 46 ad c3 50 18 ...P.....F..P..

0030 00 ed 12 72 00 00 48 54 54 50 2f 31 2e 31 20 32 ...r..HT TP/1.1 2

0040 30 30 20 4f 4b 0d 0a 44 61 74 65 3a 20 57 65 64 00 OK...D ate: Wed

Type here to search

10:05 PM 1/29/2019

3. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received?

0.001252000 seconds

Wireshark Lab 1_Yakubu Iddirisu.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
14...	20:12:05.657103	192.168.0.15	128.119.245.12	HTTP	464	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
14...	20:12:05.685668	128.119.245.12	192.168.0.15	HTTP	492	HTTP/1.1 200 OK (text/html)

▼ Frame 1485: 464 bytes on wire (3712 bits), 464 bytes captured (3712 bits) on interface 0

- > Interface id: 0 (\Device\NPF_{1A61960A-18FA-4580-890D-0D99CAC1A800})
- Encapsulation type: Ethernet (1)
- Arrival Time: Jan 29, 2019 20:12:05.657103000 Eastern Standard Time
- [Time shift for this packet: 0.000000000 seconds]
- Epoch Time: 1548810725.657103000 seconds
- [Time delta from previous captured frame: 0.001252000 seconds]**
- [Time delta from previous displayed frame: 0.000000000 seconds]
- [Time since reference or first frame: 60.699537000 seconds]
- Frame Number: 1485
- Frame Length: 464 bytes (3712 bits)
- Capture Length: 464 bytes (3712 bits)

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

0010 01 c2 77 33 40 00 80 06 4b c7 c0 a8 00 0f 80 77 ..w3@... K.....w

0020 f5 0c c7 91 00 50 b3 46 ac 29 05 ec c8 f9 50 18P.F.)....P.

0030 04 00 16 68 00 00 47 45 54 20 2f 77 69 72 65 73 ...h..GE T /wires

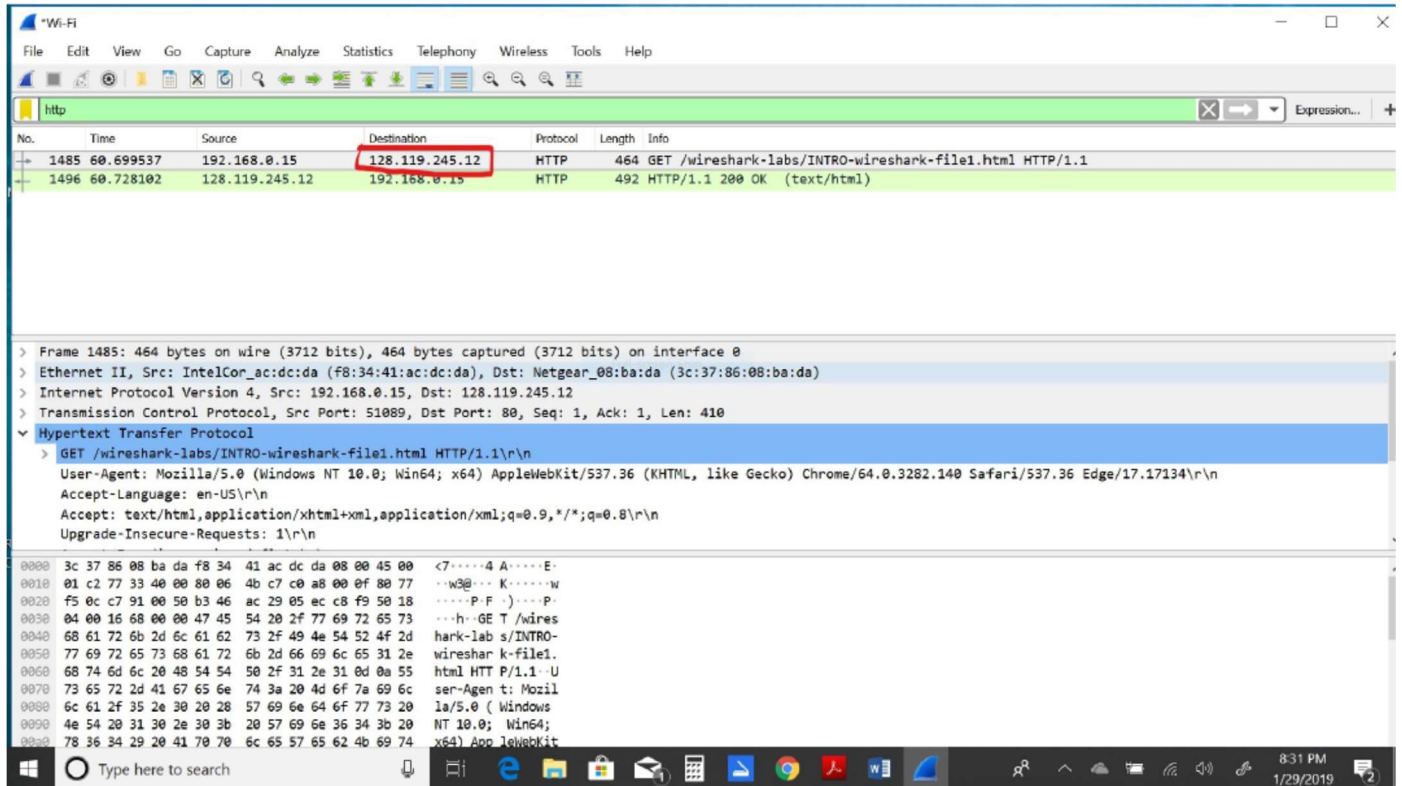
0040 68 61 72 6b 2d 6c 61 62 73 2f 49 4e 54 52 4f 2d hark-lab s/INTRO-

Type here to search

10:47 PM 1/29/2019

4. What is the Internet address of the `gaia.cs.umass.edu` (also known as `www-net.cs.umass.edu`)?

128.119.245.12



5. Print the two HTTP messages (GET and OK) referred to in question 2 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.

