Anthony Chavez

Professor Sun

Wireshark Lab

Question 1

No.	Time	Source	Destination	Protocol	Length	Info
1	16:23:57.069661	10.114.2.168	3.235.96.206	TLSv1.2	271	Application Data
2	16:23:57.164084	3.235.96.206	10.114.2.168	TCP	60	443 → 61816 [ACK] Seq=1 Ack=218 Win=1110 Len=0
3	16:23:57.164173	3.235.96.206	10.114.2.168	TLSv1.2	249	Application Data
4	16:23:57.204057	10.114.2.168	3.235.96.206	TCP	54	61816 → 443 [ACK] Seq=218 Ack=196 Win=514 Len=0
5	16:24:04.395308	10.114.2.168	3.235.72.249	TLSv1.2	89	Application Data
6	16:24:04.492860	3.235.72.249	10.114.2.168	TLSv1.2	85	Application Data

In the beginning of the capture, the TLSv1.2 and the TCP protocol can be seen in the screenshot above. According to keycdn.com, “TLS stands for Transport Layer Security, which is a cryptographic protocol used to increase security over computer networks. Transmission Control Protocol is a standard that defines how to establish and maintain a network conversation through which application programs can exchange data (https://searchnetworking.techtarget.com/definition/TCP).

No.	Time	Source	Destination	Protocol	Length	Info
42	16:24:09.331662	02:50:41:00:00:01	02:50:41:00:00:02	ARP	42	Who has 3.235.72.249? Tell 10.114.2.168
43	16:24:09.331750	02:50:41:00:00:02	02:50:41:00:00:01	ARP	60	3.235.72.249 is at 02:50:41:00:00:02
44	16:24:10.332057	02:50:41:00:00:01	02:50:41:00:00:02	ARP	42	Who has 130.86.251.251? Tell 10.114.2.168
45	16:24:10.332386	02:50:41:00:00:02	02:50:41:00:00:01	ARP	60	130.86.251.251 is at 02:50:41:00:00:02

ARP can be seen in the above screenshot. “Address Resolution Protocol (ARP) is a procedure for mapping a dynamic Internet Protocol address (IP address) to a permanent physical machine address in a local area network (LAN).” (https://searchnetworking.techtarget.com/definition/Address-Resolution-Protocol-ARP)

Question 2

No.	Time	Source	Destination	Protocol	Length	Info
59	16:24:20.424334	10.114.2.168	128.119.245.12	HTTP	433	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
61	16:24:20.530459	128.119.245.12	10.114.2.168	HTTP	492	HTTP/1.1 200 OK (text/html)

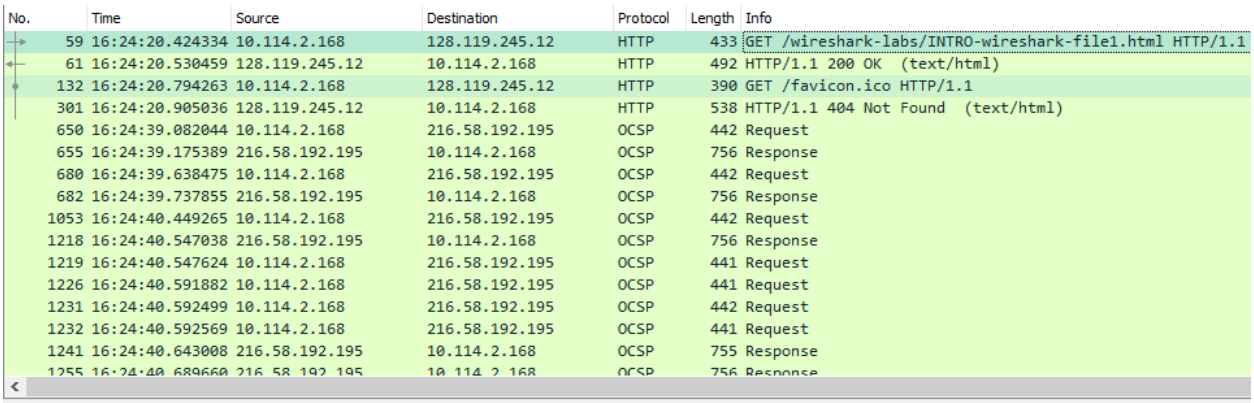
The HTTP GET message was sent at 16:24:20.424334 and the HTTP OK reply was received at 16:24:20.530459. Therefore 20.530459s – 20.424334s = 0.106125 seconds.

Question 3

There are two options of determining the Internet address of the gaia.cs.umass.edu and my computer.

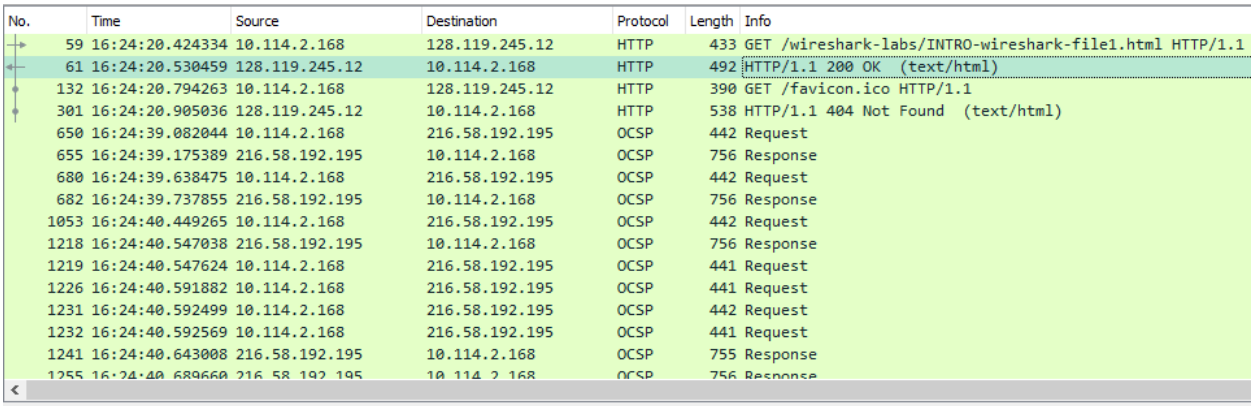
No.	Time	Source	Destination	Protocol	Length	Info
59	16:24:20.424334	10.114.2.168	128.119.245.12	HTTP	433	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
61	16:24:20.530459	128.119.245.12	10.114.2.168	HTTP	492	HTTP/1.1 200 OK (text/html)

For the HTTP GET message, you can see under the Destination column that the Internet address of gaia.cs.umass.edu is “128.119.245.12” and under the Source column my Internet address is “10.114.2.168”. This is because my computer is sending the HTTP GET message to gaia.cs.umass.edu. On the other hand, the HTTP OK reply is sent by gaia.cs.umass.edu, so gaia.cs.umass.edu has its Internet address as the source and my computer is the destination.



No.	Time	Source	Destination	Protocol	Length	Info
59	16:24:20.424334	10.114.2.168	128.119.245.12	HTTP	433	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
61	16:24:20.530459	128.119.245.12	10.114.2.168	HTTP	492	HTTP/1.1 200 OK (text/html)
132	16:24:20.794263	10.114.2.168	128.119.245.12	HTTP	390	GET /favicon.ico HTTP/1.1
301	16:24:20.905036	128.119.245.12	10.114.2.168	HTTP	538	HTTP/1.1 404 Not Found (text/html)
650	16:24:39.082044	10.114.2.168	216.58.192.195	OCSP	442	Request
655	16:24:39.175389	216.58.192.195	10.114.2.168	OCSP	756	Response
680	16:24:39.638475	10.114.2.168	216.58.192.195	OCSP	442	Request
682	16:24:39.737855	216.58.192.195	10.114.2.168	OCSP	756	Response
1053	16:24:40.449265	10.114.2.168	216.58.192.195	OCSP	442	Request
1218	16:24:40.547038	216.58.192.195	10.114.2.168	OCSP	756	Response
1219	16:24:40.547624	10.114.2.168	216.58.192.195	OCSP	441	Request
1226	16:24:40.591882	10.114.2.168	216.58.192.195	OCSP	441	Request
1231	16:24:40.592499	10.114.2.168	216.58.192.195	OCSP	442	Request
1232	16:24:40.592569	10.114.2.168	216.58.192.195	OCSP	441	Request
1241	16:24:40.643008	216.58.192.195	10.114.2.168	OCSP	755	Response
1255	16:24:40.689660	216.58.192.195	10.114.2.168	OCSP	756	Response

```
> Ethernet II, Src: 02:50:41:00:00:01 (02:50:41:00:00:01), Dst: 02:50:41:00:00:02 (02:50:41:00:00:02)
v Internet Protocol Version 4, Src: 10.114.2.168, 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: 419
    Identification: 0x5531 (21809)
  > Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 128
    Protocol: TCP (6)
    Header checksum: 0x2186 [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.114.2.168
    Destination: 128.119.245.12
> Transmission Control Protocol, Src Port: 62242, Dst Port: 80, Seq: 1, Ack: 1, Len: 379
> Hypertext Transfer Protocol
```



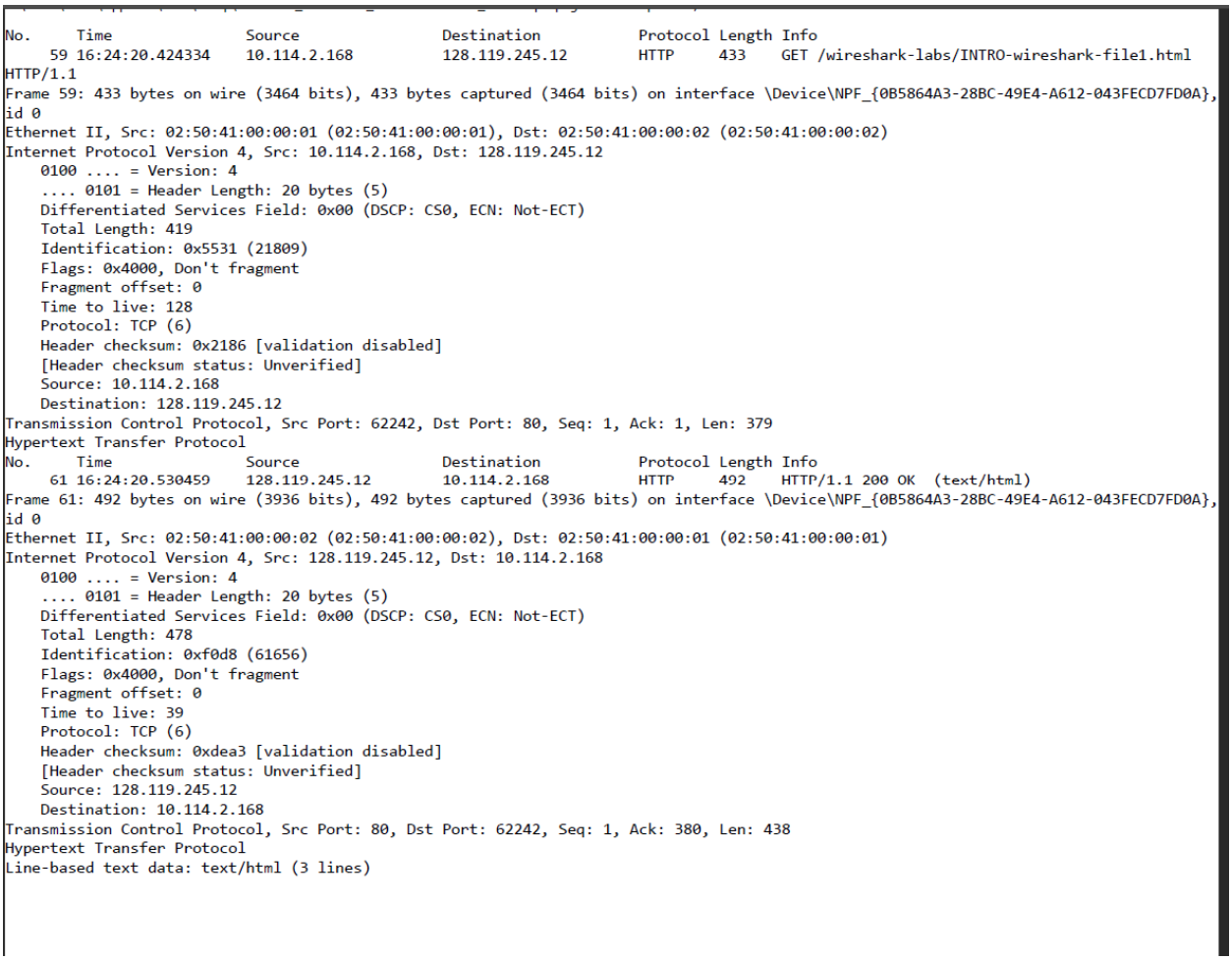
No.	Time	Source	Destination	Protocol	Length	Info
59	16:24:20.424334	10.114.2.168	128.119.245.12	HTTP	433	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
61	16:24:20.530459	128.119.245.12	10.114.2.168	HTTP	492	HTTP/1.1 200 OK (text/html)
132	16:24:20.794263	10.114.2.168	128.119.245.12	HTTP	390	GET /favicon.ico HTTP/1.1
301	16:24:20.905036	128.119.245.12	10.114.2.168	HTTP	538	HTTP/1.1 404 Not Found (text/html)
650	16:24:39.082044	10.114.2.168	216.58.192.195	OCSP	442	Request
655	16:24:39.175389	216.58.192.195	10.114.2.168	OCSP	756	Response
680	16:24:39.638475	10.114.2.168	216.58.192.195	OCSP	442	Request
682	16:24:39.737855	216.58.192.195	10.114.2.168	OCSP	756	Response
1053	16:24:40.449265	10.114.2.168	216.58.192.195	OCSP	442	Request
1218	16:24:40.547038	216.58.192.195	10.114.2.168	OCSP	756	Response
1219	16:24:40.547624	10.114.2.168	216.58.192.195	OCSP	441	Request
1226	16:24:40.591882	10.114.2.168	216.58.192.195	OCSP	441	Request
1231	16:24:40.592499	10.114.2.168	216.58.192.195	OCSP	442	Request
1232	16:24:40.592569	10.114.2.168	216.58.192.195	OCSP	441	Request
1241	16:24:40.643008	216.58.192.195	10.114.2.168	OCSP	755	Response
1255	16:24:40.689660	216.58.192.195	10.114.2.168	OCSP	756	Response

```
> Ethernet II, Src: 02:50:41:00:00:02 (02:50:41:00:00:02), Dst: 02:50:41:00:00:01 (02:50:41:00:00:01)
v Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.114.2.168
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 478
    Identification: 0xf0d8 (61656)
  > Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 39
    Protocol: TCP (6)
    Header checksum: 0xdea3 [validation disabled]
    [Header checksum status: Unverified]
    Source: 128.119.245.12
    Destination: 10.114.2.168
```

Alternatively, you can select one packet capture at a time and open the “Internet Protocol Version 4” segment. The HTTP GET message is sent by my computer, so the source is my computer’s Internet address. This message is being received by gaia, so the destination is gaia’s Internet address. (See first screenshot) When the HTTP OK reply is sent, the source becomes

gaia's Internet address and the destination becomes my computer's Internet address. (See second screenshot)

Question 4



```
No.     Time              Source                Destination           Protocol Length Info
     59 16:24:20.424334    10.114.2.168          128.119.245.12        HTTP     433    GET /wireshark-labs/INTRO-wireshark-file1.html
HTTP/1.1
Frame 59: 433 bytes on wire (3464 bits), 433 bytes captured (3464 bits) on interface \Device\NPF_{0B5864A3-28BC-49E4-A612-043FECD7FD0A},
id 0
Ethernet II, Src: 02:50:41:00:00:01 (02:50:41:00:00:01), Dst: 02:50:41:00:00:02 (02:50:41:00:00:02)
Internet Protocol Version 4, Src: 10.114.2.168, 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: 419
    Identification: 0x5531 (21809)
    Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 128
    Protocol: TCP (6)
    Header checksum: 0x2186 [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.114.2.168
    Destination: 128.119.245.12
Transmission Control Protocol, Src Port: 62242, Dst Port: 80, Seq: 1, Ack: 1, Len: 379
Hypertext Transfer Protocol
No.     Time              Source                Destination           Protocol Length Info
     61 16:24:20.530459    128.119.245.12        10.114.2.168          HTTP     492    HTTP/1.1 200 OK  (text/html)
Frame 61: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface \Device\NPF_{0B5864A3-28BC-49E4-A612-043FECD7FD0A},
id 0
Ethernet II, Src: 02:50:41:00:00:02 (02:50:41:00:00:02), Dst: 02:50:41:00:00:01 (02:50:41:00:00:01)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.114.2.168
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 478
    Identification: 0xf0d8 (61656)
    Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 39
    Protocol: TCP (6)
    Header checksum: 0xdea3 [validation disabled]
    [Header checksum status: Unverified]
    Source: 128.119.245.12
    Destination: 10.114.2.168
Transmission Control Protocol, Src Port: 80, Dst Port: 62242, Seq: 1, Ack: 380, Len: 438
Hypertext Transfer Protocol
Line-based text data: text/html (3 lines)
```

This is a printout of the HTTP GET and HTTP OK packet from my Wireshark capture.