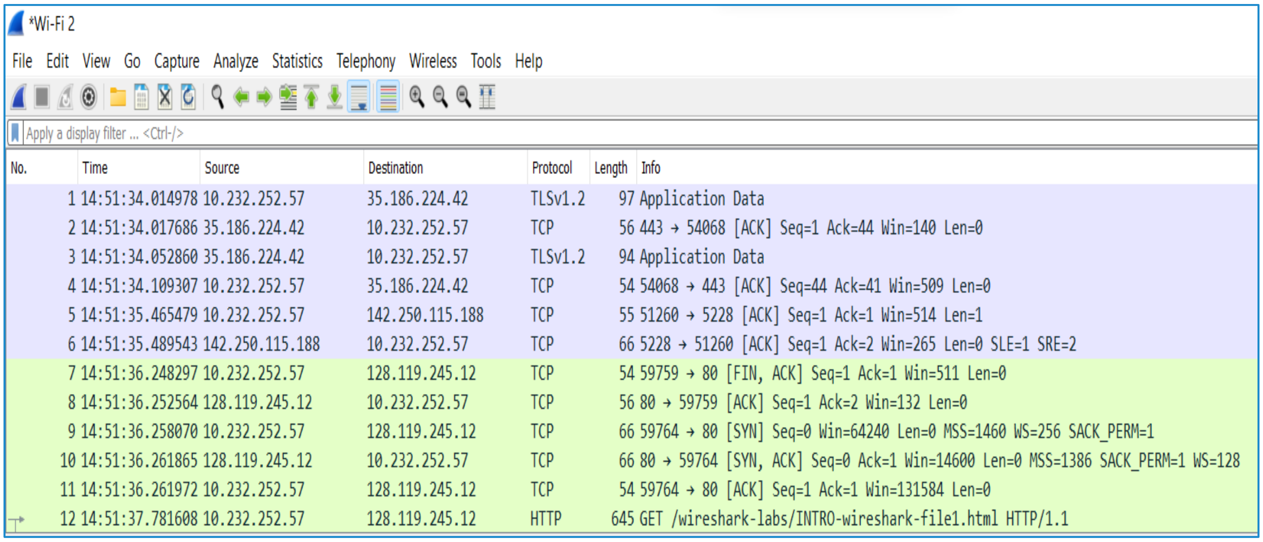
WIRESHARK LAB: GETTING STARTED

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

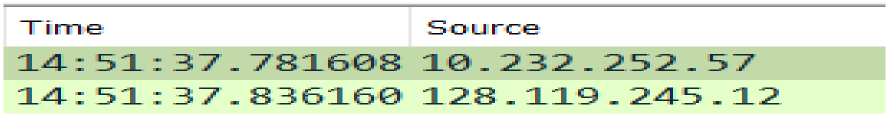

*Wi-Fi 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	14:51:34.014978	10.232.252.57	35.186.224.42	TLSv1.2	97	Application Data
2	14:51:34.017686	35.186.224.42	10.232.252.57	TCP	56	443 → 54068 [ACK] Seq=1 Ack=44 Win=140 Len=0
3	14:51:34.052860	35.186.224.42	10.232.252.57	TLSv1.2	94	Application Data
4	14:51:34.109307	10.232.252.57	35.186.224.42	TCP	54	54068 → 443 [ACK] Seq=44 Ack=41 Win=509 Len=0
5	14:51:35.465479	10.232.252.57	142.250.115.188	TCP	55	51260 → 5228 [ACK] Seq=1 Ack=1 Win=514 Len=1
6	14:51:35.489543	142.250.115.188	10.232.252.57	TCP	66	5228 → 51260 [ACK] Seq=1 Ack=2 Win=265 Len=0 SLE=1 SRE=2
7	14:51:36.248297	10.232.252.57	128.119.245.12	TCP	54	59759 → 80 [FIN, ACK] Seq=1 Ack=1 Win=511 Len=0
8	14:51:36.252564	128.119.245.12	10.232.252.57	TCP	56	80 → 59759 [ACK] Seq=1 Ack=2 Win=132 Len=0
9	14:51:36.258070	10.232.252.57	128.119.245.12	TCP	66	59764 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
10	14:51:36.261865	128.119.245.12	10.232.252.57	TCP	66	80 → 59764 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1386 SACK_PERM=1 WS=128
11	14:51:36.261972	10.232.252.57	128.119.245.12	TCP	54	59764 → 80 [ACK] Seq=1 Ack=1 Win=131584 Len=0
12	14:51:37.781608	10.232.252.57	128.119.245.12	HTTP	645	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1

Figure 1: Packet-listing window

We can receive all the protocols in the packet-listing window. In this lab TLS, TCP, and HTTP some of the protocols that appear in the protocol column.

2. 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.)

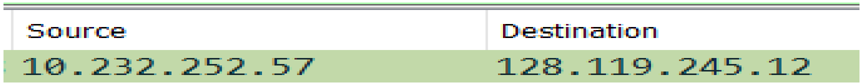


Time	Source
14:51:37.781608	10.232.252.57
14:51:37.836160	128.119.245.12

Figure 2: Time and Source column in packet-listing window

In the packet-listing window, there is a time column where we can receive the time that spends between source and destination. In this lab, the time column is set up in time-of-day format. HTTP GET message is sent at 14:51:37.781608 and HTTP OK reply was received at 14:51:37.836160. The time difference between these hours is 0.054552 second.

3. What is the Internet address of the gaia.cs.umass.edu (also known as www.net.cs.umass.edu)? What is the Internet address of your computer?



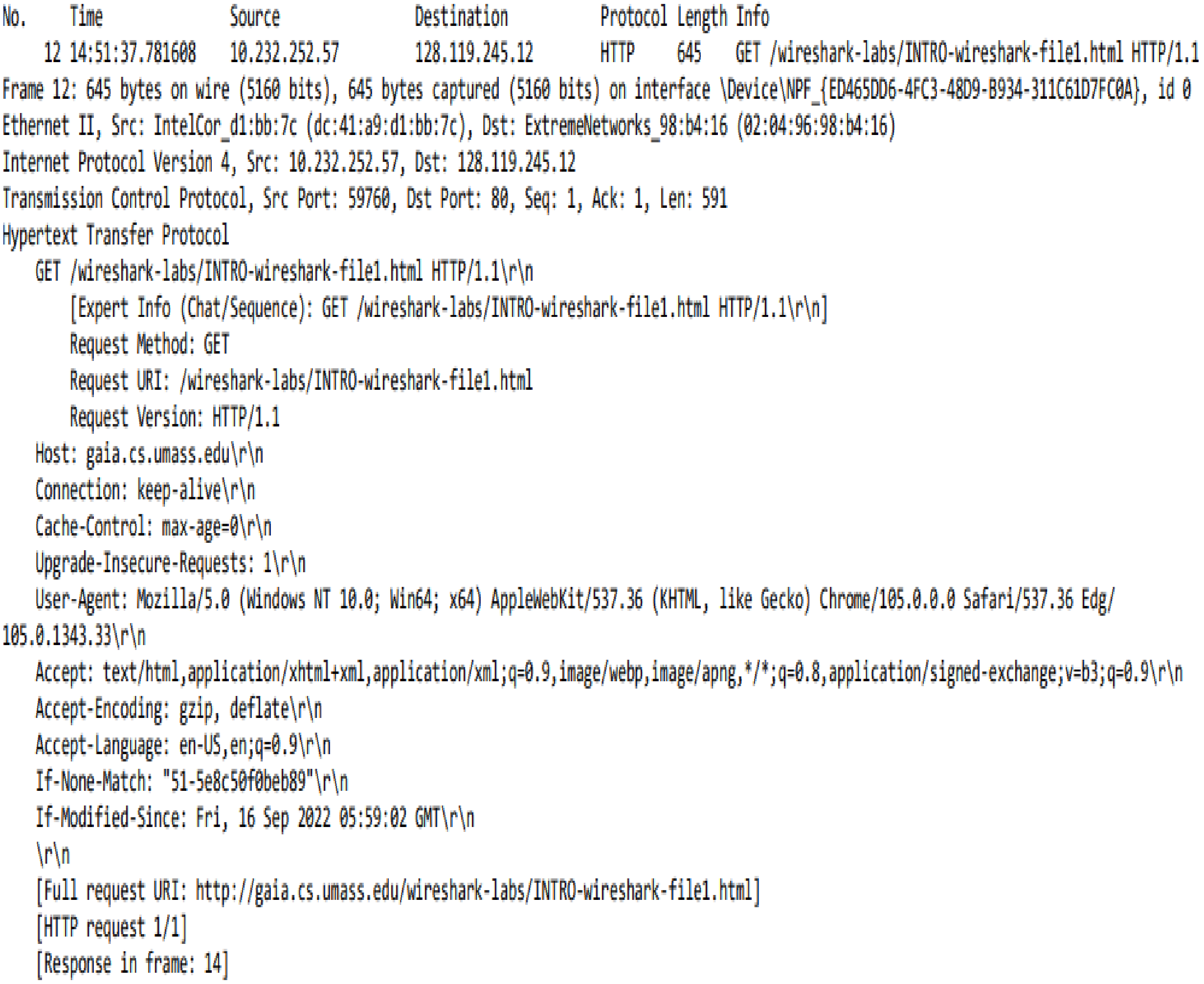
Source	Destination
10.232.252.57	128.119.245.12

Figure 3: Destination and Source column in the packet-listing window

In the packet-listing window, there is a destination and source column that shows the IP addresses of the source and destination. In this lab on the HTTP GET message row, the destination is the web server that we want to download its web page and the source is the web server that our laptop is connected to. As a result, the IP address of gaia.cs.umass.edu is 128.119.245.12, and the IP address of my laptop is 10.232.252.57.

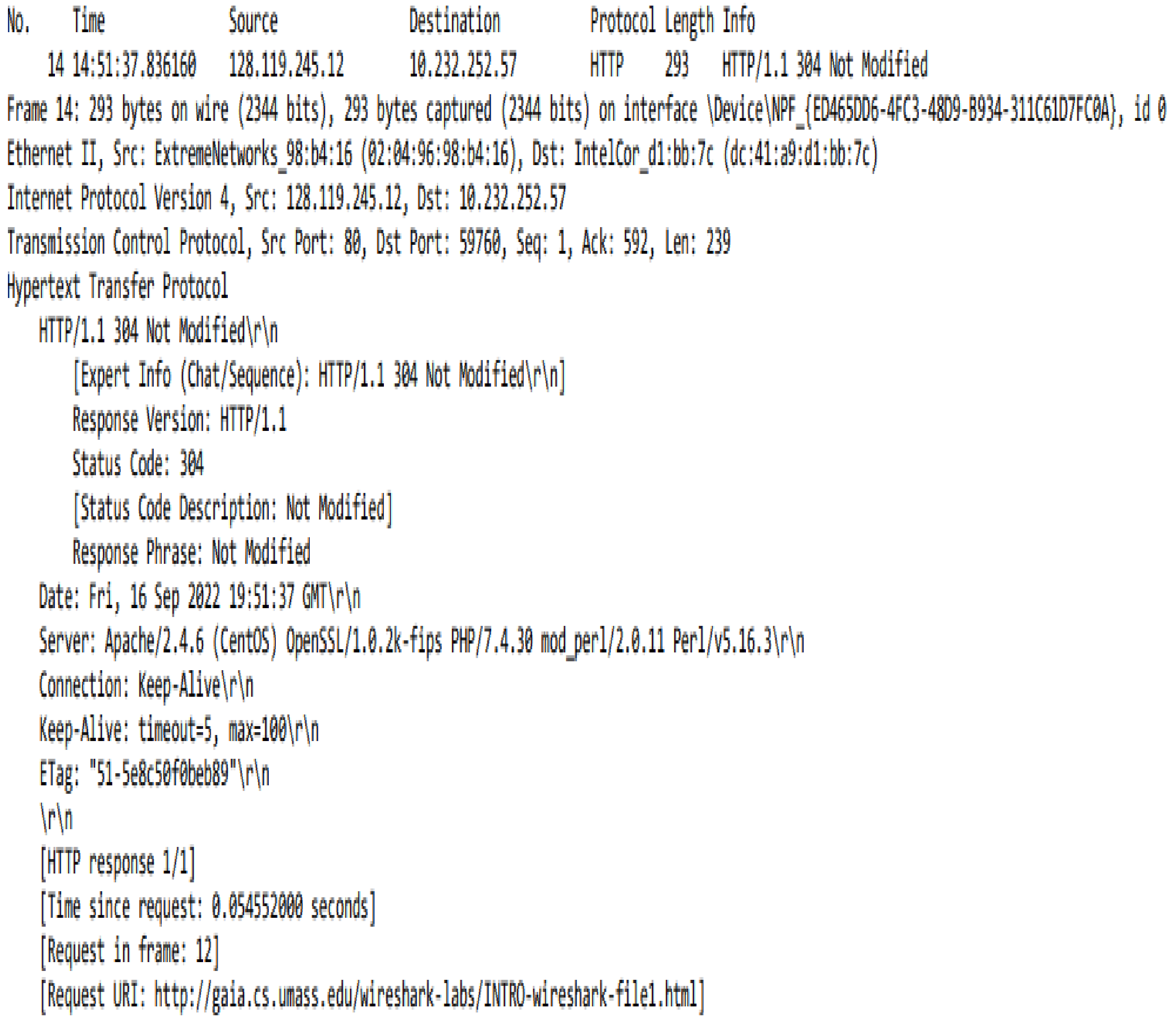
4. Print the two HTTP messages (GET and OK) referred to in question 2 above. To do so, select Print from the Wireshark File command menu, and select the “Selected Packet Only” and “Print as displayed” radial buttons, and then click OK.

HTTP GET message print:



```
No.     Time               Source                Destination           Protocol Length Info
     12 14:51:37.781608    10.232.252.57         128.119.245.12        HTTP     645    GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
Frame 12: 645 bytes on wire (5160 bits), 645 bytes captured (5160 bits) on interface \Device\NPF_{ED465DD6-4FC3-48D9-B934-311C61D7FC0A}, id 0
Ethernet II, Src: IntelCor_d1:bb:7c (dc:41:a9:d1:bb:7c), Dst: ExtremeNetworks_98:b4:16 (02:04:96:98:b4:16)
Internet Protocol Version 4, Src: 10.232.252.57, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 59760, Dst Port: 80, Seq: 1, Ack: 1, Len: 591
Hypertext Transfer Protocol
    GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
        [Expert Info (Chat/Sequence): GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n]
        Request Method: GET
        Request URI: /wireshark-labs/INTRO-wireshark-file1.html
        Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Cache-Control: max-age=0\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Safari/537.36 Edg/
105.0.1343.33\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    If-None-Match: "51-5e8c50f0beb89"\r\n
    If-Modified-Since: Fri, 16 Sep 2022 05:59:02 GMT\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
    [HTTP request 1/1]
    [Response in frame: 14]
```

HTTP OK message print:



```
No.     Time               Source                Destination           Protocol Length Info
     14 14:51:37.836160    128.119.245.12        10.232.252.57         HTTP     293    HTTP/1.1 304 Not Modified
Frame 14: 293 bytes on wire (2344 bits), 293 bytes captured (2344 bits) on interface \Device\NPF_{ED465DD6-4FC3-48D9-B934-311C61D7FC0A}, id 0
Ethernet II, Src: ExtremeNetworks_98:b4:16 (02:04:96:98:b4:16), Dst: IntelCor_d1:bb:7c (dc:41:a9:d1:bb:7c)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.232.252.57
Transmission Control Protocol, Src Port: 80, Dst Port: 59760, Seq: 1, Ack: 592, Len: 239
Hypertext Transfer Protocol
    HTTP/1.1 304 Not Modified\r\n
        [Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]
        Response Version: HTTP/1.1
        Status Code: 304
        [Status Code Description: Not Modified]
        Response Phrase: Not Modified
    Date: Fri, 16 Sep 2022 19:51:37 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Connection: Keep-Alive\r\n
    Keep-Alive: timeout=5, max=100\r\n
    ETag: "51-5e8c50f0beb89"\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.054552000 seconds]
    [Request in frame: 12]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
```