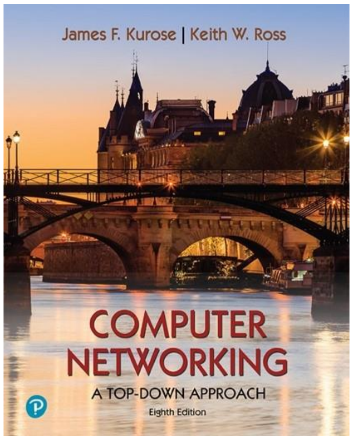
Wireshark Lab: Getting Started v8.0

Supplement to *Computer Networking: A Top-Down Approach, 8th ed.*, J.F. Kurose and K.W. Ross

"Tell me and I forget. Show me and I remember. Involve me and I understand." Chinese proverb

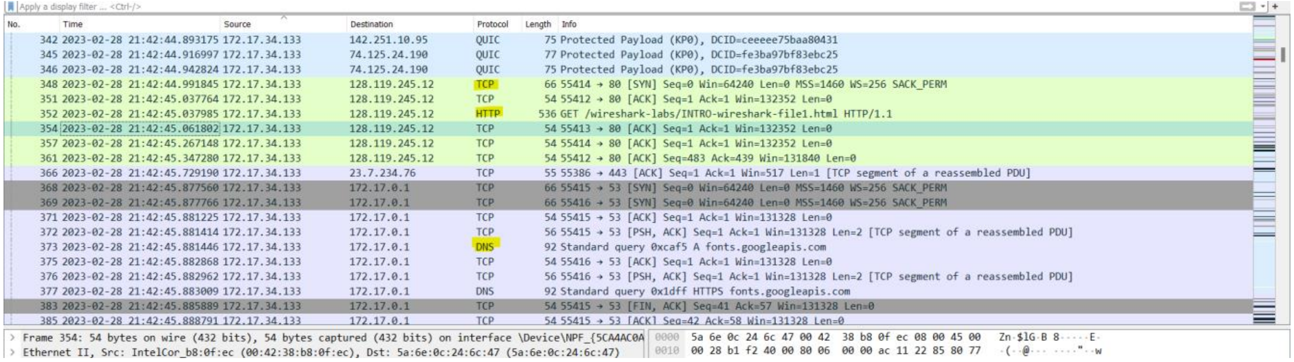


Student Name : Nguyễn Hữu Hiếu
Student ID : 2013149

What to hand in

The goal of this first lab was primarily to introduce you to Wireshark. The following questions will demonstrate that you've been able to get Wireshark up and running, and have explored some of its capabilities. Answer the following questions, based on your Wireshark experimentation:

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

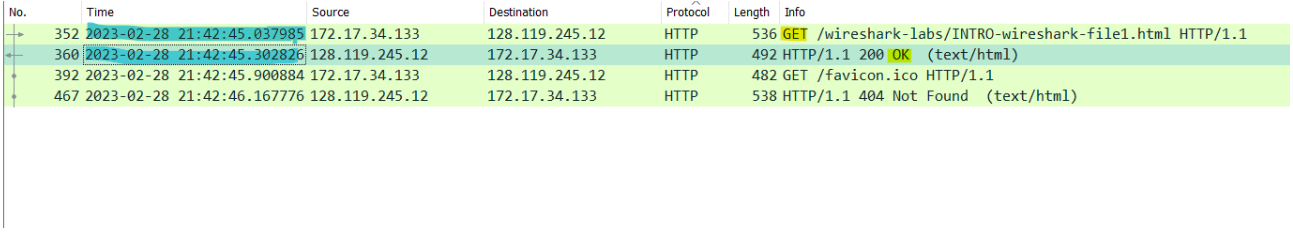


```
No.   Time                        Source          Destination      Protocol Length Info
  342 2023-02-28 21:42:44.893175 172.17.34.133   142.251.10.95    QUIC       75 Protected Payload (KP0), DCID=ceeeee75baa80431
  345 2023-02-28 21:42:44.916997 172.17.34.133   74.125.24.190    QUIC       77 Protected Payload (KP0), DCID=fe3ba97bf83ebc25
  346 2023-02-28 21:42:44.942824 172.17.34.133   74.125.24.190    QUIC       75 Protected Payload (KP0), DCID=fe3ba97bf83ebc25
  348 2023-02-28 21:42:44.991845 172.17.34.133   128.119.245.12   TCP        66 55414 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
  351 2023-02-28 21:42:45.037764 172.17.34.133   128.119.245.12   TCP        54 55412 → 80 [ACK] Seq=1 Ack=1 Win=132352 Len=0
  352 2023-02-28 21:42:45.037985 172.17.34.133   128.119.245.12   HTTP      536 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
  354 2023-02-28 21:42:45.061802 172.17.34.133   128.119.245.12   TCP        54 55413 → 80 [ACK] Seq=1 Ack=1 Win=132352 Len=0
  357 2023-02-28 21:42:45.267148 172.17.34.133   128.119.245.12   TCP        54 55414 → 80 [ACK] Seq=1 Ack=1 Win=132352 Len=0
  361 2023-02-28 21:42:45.347280 172.17.34.133   128.119.245.12   TCP        54 55412 → 80 [ACK] Seq=483 Ack=439 Win=131840 Len=0
  366 2023-02-28 21:42:45.729190 172.17.34.133   23.7.234.76      TCP        55 55386 → 443 [ACK] Seq=1 Ack=1 Win=517 Len=1 [TCP segment of a reassembled PDU]
  368 2023-02-28 21:42:45.877560 172.17.34.133   172.17.0.1       TCP        66 55415 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
  369 2023-02-28 21:42:45.877766 172.17.34.133   172.17.0.1       TCP        66 55416 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
  371 2023-02-28 21:42:45.881225 172.17.34.133   172.17.0.1       TCP        54 55415 → 53 [ACK] Seq=1 Ack=1 Win=131328 Len=0
  372 2023-02-28 21:42:45.881414 172.17.34.133   172.17.0.1       TCP        56 55415 → 53 [PSH, ACK] Seq=1 Ack=1 Win=131328 Len=2 [TCP segment of a reassembled PDU]
  373 2023-02-28 21:42:45.881446 172.17.34.133   172.17.0.1       DNS        92 Standard query 0xcaf5 A fonts.googleapis.com
  375 2023-02-28 21:42:45.882868 172.17.34.133   172.17.0.1       TCP        54 55416 → 53 [ACK] Seq=1 Ack=1 Win=131328 Len=0
  376 2023-02-28 21:42:45.882962 172.17.34.133   172.17.0.1       TCP        56 55416 → 53 [PSH, ACK] Seq=1 Ack=1 Win=131328 Len=2 [TCP segment of a reassembled PDU]
  377 2023-02-28 21:42:45.883009 172.17.34.133   172.17.0.1       DNS        92 Standard query 0x1dff HTTPS fonts.googleapis.com
  383 2023-02-28 21:42:45.885889 172.17.34.133   172.17.0.1       TCP        54 55415 → 53 [FIN, ACK] Seq=41 Ack=57 Win=131328 Len=0
  385 2023-02-28 21:42:45.888791 172.17.34.133   172.17.0.1       TCP        54 55415 → 53 [ACK] Seq=42 Ack=58 Win=131328 Len=0

> Frame 354: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{5CA4AC0A
> Ethernet II, Src: IntelCor_b8:0f:ec (00:42:38:b8:0f:ec), Dst: 5a:6e:0c:24:6c:47 (5a:6e:0c:24:6c:47)

0000  5a 6e 0c 24 6c 47 00 42  38 b8 0f ec 08 00 45 00   Zn·$lG·B 8·····E·
0010  00 28 b1 f2 40 00 80 06  00 00 ac 11 22 85 80 77   ·(··@··· ····"··w
```

3 different protocols:

1) DNS
2) TCP
3) HTTP

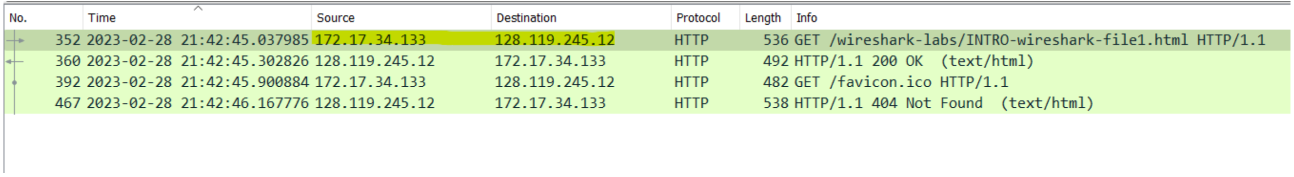
2. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received



No.	Time	Source	Destination	Protocol	Length	Info
352	2023-02-28 21:42:45.037985	172.17.34.133	128.119.245.12	HTTP	536	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
360	2023-02-28 21:42:45.302826	128.119.245.12	172.17.34.133	HTTP	492	HTTP/1.1 200 OK (text/html)
392	2023-02-28 21:42:45.900884	172.17.34.133	128.119.245.12	HTTP	482	GET /favicon.ico HTTP/1.1
467	2023-02-28 21:42:46.167776	128.119.245.12	172.17.34.133	HTTP	538	HTTP/1.1 404 Not Found (text/html)

The arrival time of HTTP GET message is : Feb 28, 2023 21:42:45.037985000 SE Asia Standard Time
The arrival time of HTTP OK message is : Feb 28, 2023 21:42:45.302826000 SE Asia Standard Time
So it's take close to 0.3s

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?

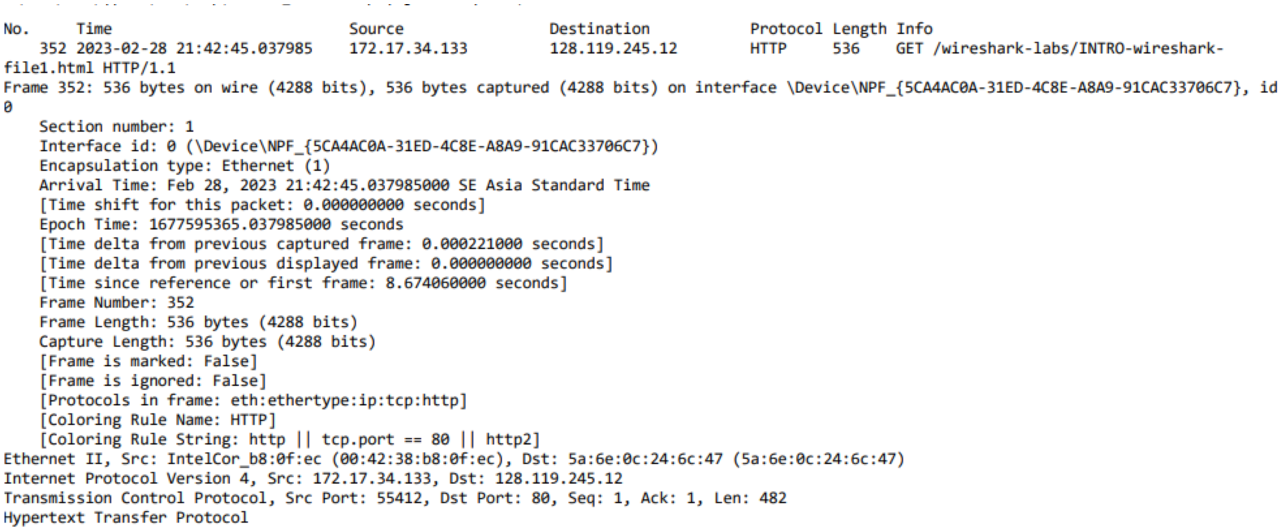


No.	Time	Source	Destination	Protocol	Length	Info
352	2023-02-28 21:42:45.037985	172.17.34.133	128.119.245.12	HTTP	536	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
360	2023-02-28 21:42:45.302826	128.119.245.12	172.17.34.133	HTTP	492	HTTP/1.1 200 OK (text/html)
392	2023-02-28 21:42:45.900884	172.17.34.133	128.119.245.12	HTTP	482	GET /favicon.ico HTTP/1.1
467	2023-02-28 21:42:46.167776	128.119.245.12	172.17.34.133	HTTP	538	HTTP/1.1 404 Not Found (text/html)

The internet address of the gaia.cs.umass.edu (Source Address) is 172.17.34.133
My internet address of my computer (Destination Address) is 128.119.245.12

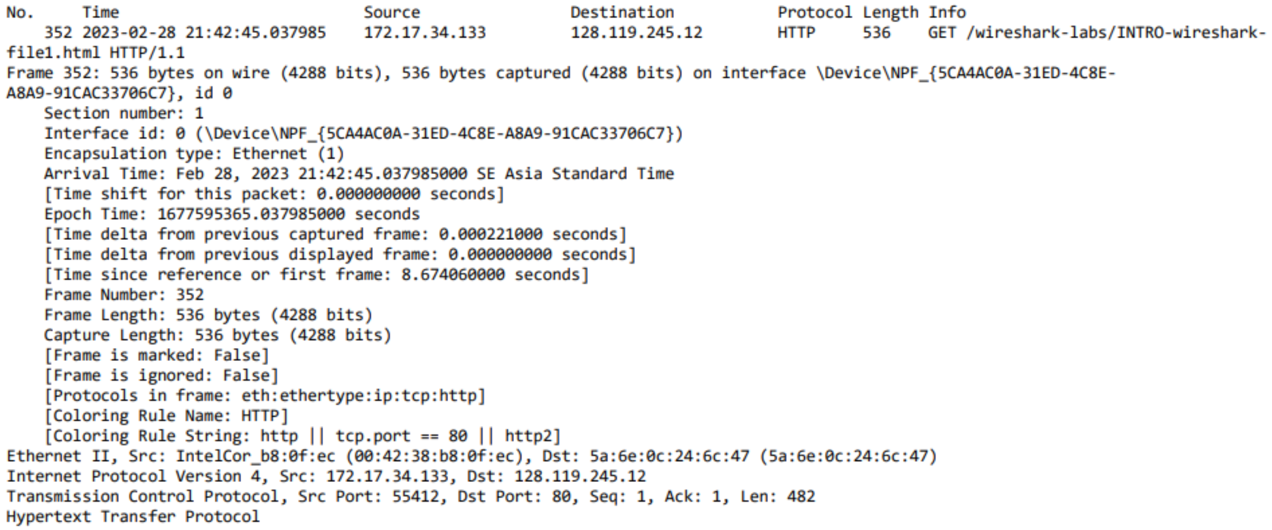
4. Print the two HTTP messages (GET and OK) referred to in question 2 above. To do so, select *Print* from the Wireshark *File* command menu, and select the "*Selected Packet Only"* and *"Print as displayed"* radial buttons, and then click OK.

HTTP GET:



```
No.     Time                          Source                Destination           Protocol Length Info
    352 2023-02-28 21:42:45.037985    172.17.34.133         128.119.245.12        HTTP     536    GET /wireshark-labs/INTRO-wireshark-
file1.html HTTP/1.1
Frame 352: 536 bytes on wire (4288 bits), 536 bytes captured (4288 bits) on interface \Device\NPF_{5CA4AC0A-31ED-4C8E-A8A9-91CAC33706C7}, id
0
    Section number: 1
    Interface id: 0 (\Device\NPF_{5CA4AC0A-31ED-4C8E-A8A9-91CAC33706C7})
    Encapsulation type: Ethernet (1)
    Arrival Time: Feb 28, 2023 21:42:45.037985000 SE Asia Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1677595365.037985000 seconds
    [Time delta from previous captured frame: 0.000221000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 8.674060000 seconds]
    Frame Number: 352
    Frame Length: 536 bytes (4288 bits)
    Capture Length: 536 bytes (4288 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: IntelCor_b8:0f:ec (00:42:38:b8:0f:ec), Dst: 5a:6e:0c:24:6c:47 (5a:6e:0c:24:6c:47)
Internet Protocol Version 4, Src: 172.17.34.133, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 55412, Dst Port: 80, Seq: 1, Ack: 1, Len: 482
Hypertext Transfer Protocol
```

HTTP OK:



```
No.     Time                          Source                Destination           Protocol Length Info
    352 2023-02-28 21:42:45.037985    172.17.34.133         128.119.245.12        HTTP     536    GET /wireshark-labs/INTRO-wireshark-
file1.html HTTP/1.1
Frame 352: 536 bytes on wire (4288 bits), 536 bytes captured (4288 bits) on interface \Device\NPF_{5CA4AC0A-31ED-4C8E-
A8A9-91CAC33706C7}, id 0
    Section number: 1
    Interface id: 0 (\Device\NPF_{5CA4AC0A-31ED-4C8E-A8A9-91CAC33706C7})
    Encapsulation type: Ethernet (1)
    Arrival Time: Feb 28, 2023 21:42:45.037985000 SE Asia Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1677595365.037985000 seconds
    [Time delta from previous captured frame: 0.000221000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 8.674060000 seconds]
    Frame Number: 352
    Frame Length: 536 bytes (4288 bits)
    Capture Length: 536 bytes (4288 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: IntelCor_b8:0f:ec (00:42:38:b8:0f:ec), Dst: 5a:6e:0c:24:6c:47 (5a:6e:0c:24:6c:47)
Internet Protocol Version 4, Src: 172.17.34.133, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 55412, Dst Port: 80, Seq: 1, Ack: 1, Len: 482
Hypertext Transfer Protocol
```