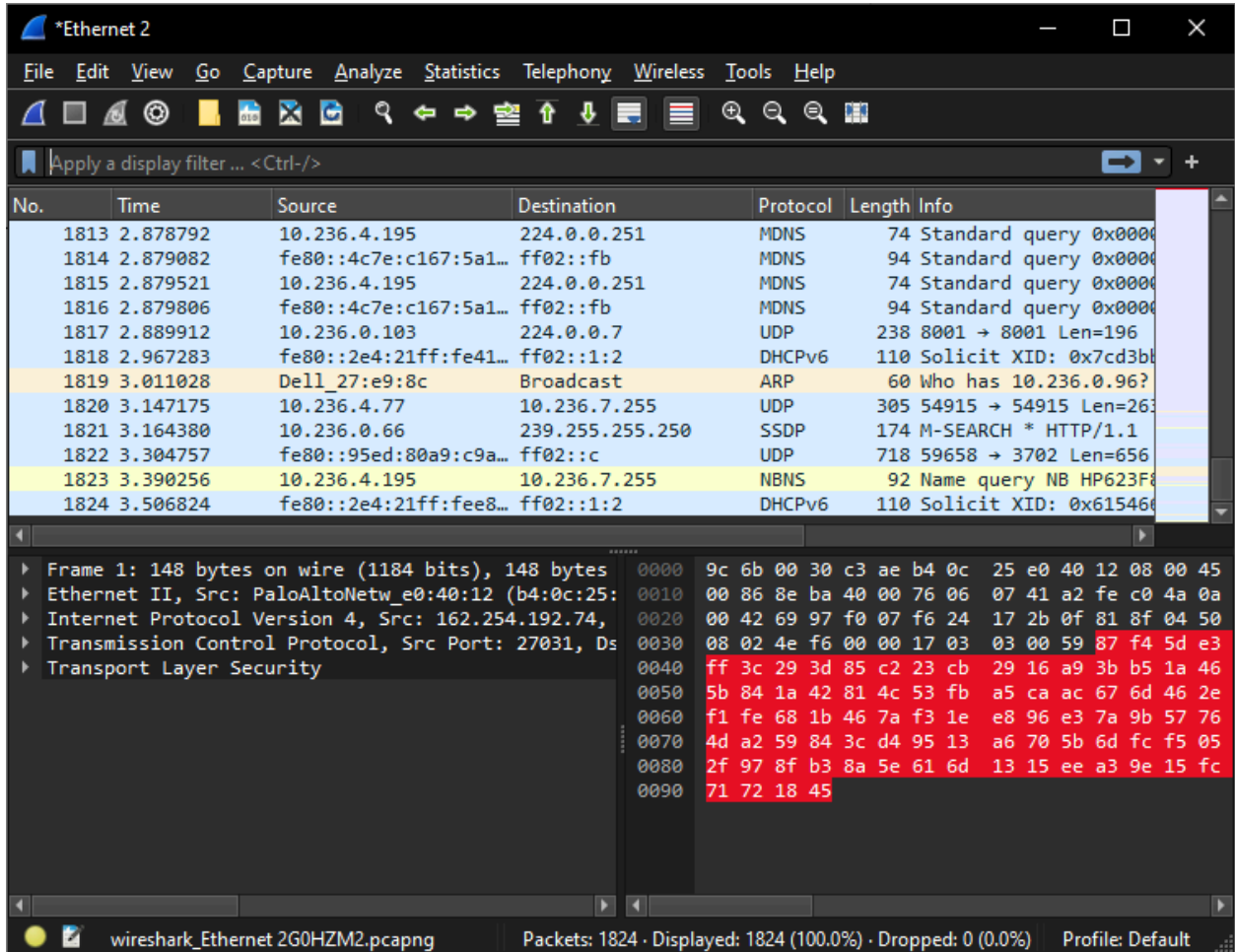


Lab 8 Wireshark

Joshua Richardson

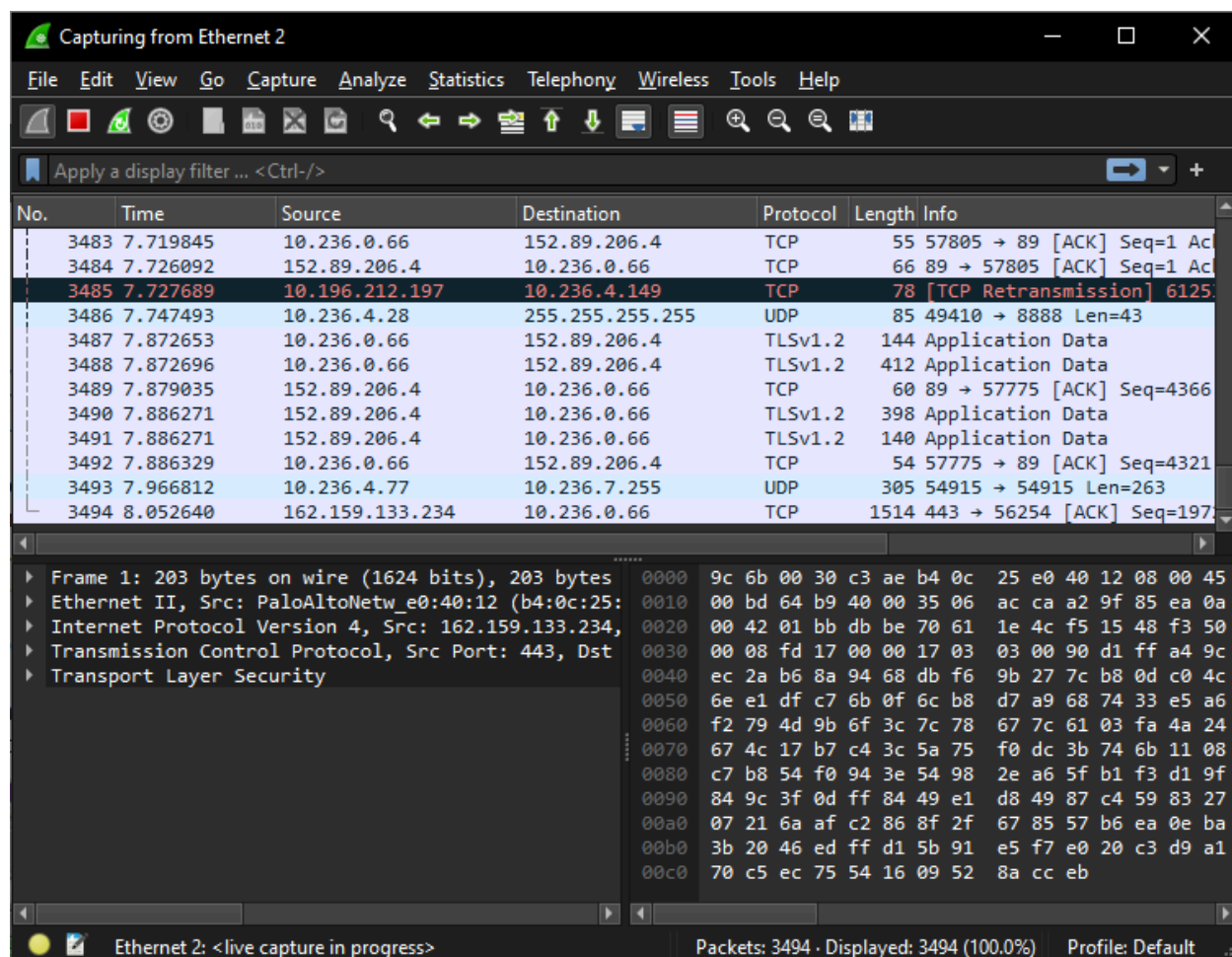
Part 2: Running Wireshark

Opening wireshark prompts me to select a network adapter, and then it shows the current traffic.



Part 3: Live Capture

Pressing the start capture button starts live capture of traffic.



Part 4/5: Testing Wireshark

I started capturing and went to Youtube on Firefox. The highlighted packet is traffic from that.

*Ethernet 2

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
10462	3.643394	10.236.0.66	172.253.63.94	OCSP	482	Request
10497	3.683882	172.253.63.94	10.236.0.66	OCSP	755	Response
10564	3.820412	10.236.0.66	172.253.63.94	OCSP	482	Request
10572	3.859512	172.253.63.94	10.236.0.66	OCSP	755	Response
10602	3.941936	10.236.0.66	172.253.63.94	OCSP	483	Request
10617	3.980417	172.253.63.94	10.236.0.66	OCSP	756	Response
13159	4.807812	10.236.0.66	172.253.63.94	OCSP	482	Request
13168	4.835883	172.253.63.94	10.236.0.66	OCSP	755	Response
13537	6.273972	10.236.0.66	172.253.63.94	OCSP	483	Request
13542	6.302721	172.253.63.94	10.236.0.66	OCSP	756	Response
13628	6.611487	10.236.0.66	10.236.0.28	HTTP	370	GET /apps/49187042-3d
13629	6.628040	10.236.0.28	10.236.0.66	HTTP/X...	452	HTTP/1.1 200 OK

Frame 13628: 370 bytes on wire (2960 bits), 370 by
 Ethernet II, Src: ASRockIncorp_30:c3:ae (9c:6b:00:
 Internet Protocol Version 4, Src: 10.236.0.66, Dst:
 Transmission Control Protocol, Src Port: 58761, Ds
 Hypertext Transfer Protocol

wireshark_Ethernet 2JK9FM2.pcapng Packets: 13726 · Displayed: 16 (0.1%) · Dropped: 0 (0.0%) Profile: Default

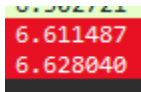
17-127F1F1075E5/YouTube HTTP/1.

1. List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above. Support your answer with an appropriate screenshot from your computer.

OCSP
 HTTP
 HTTP/
 TCP
 TCP
 TCP
 TLSv1
 UDP
 TCP

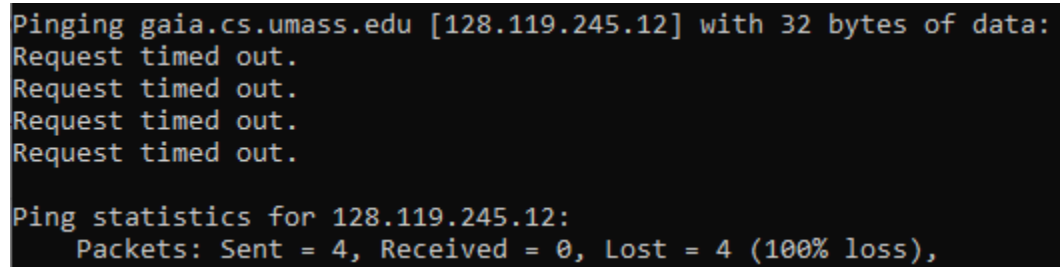
2. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packet-listing window is the amount of time, in seconds, since Wireshark tracing began. To display the Time field in time-of-day format, select the Wireshark View pull down menu, then select Time Display Format, then select Time-of-day.)

These are the two packets from going to Youtube. They are about 1 hundredth of a second apart.



6.611487
6.628040

3. What is the Internet address of the gaia.cs.umass.edu? What is the Internet address of your computer? Support your answer with an appropriate screenshot from your computer.



```
Pinging gaia.cs.umass.edu [128.119.245.12] with 32 bytes of data:  
Request timed out.  
Request timed out.  
Request timed out.  
Request timed out.  
  
Ping statistics for 128.119.245.12:  
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```



My IP Address is:

IPv4: ? 155.133.4.33