NAME: AKSHAT SAHU

Admission Number: U22CS034

Roll Number: A-34

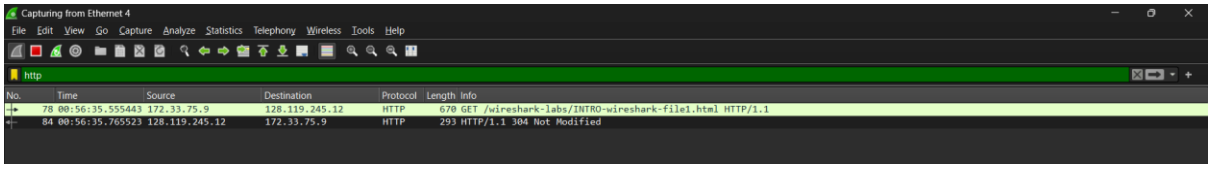
1. Packet sniffer and its structure.

2. Steps involved in installation and running the wireshark with its components.

3. Steps for capturing packets using URL given below:

http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html

4. After your browser has displayed the INTRO-wireshark-file1.html page, stop Wireshark packet capture by selecting stop in the Wireshark capture window. Type in “http” into the display filter specification window at the top of the main Wireshark window. Then select Apply or just hit return. Find the HTTP GET message that was sent from your computer to the gaia.cs.umass.edu HTTP server.

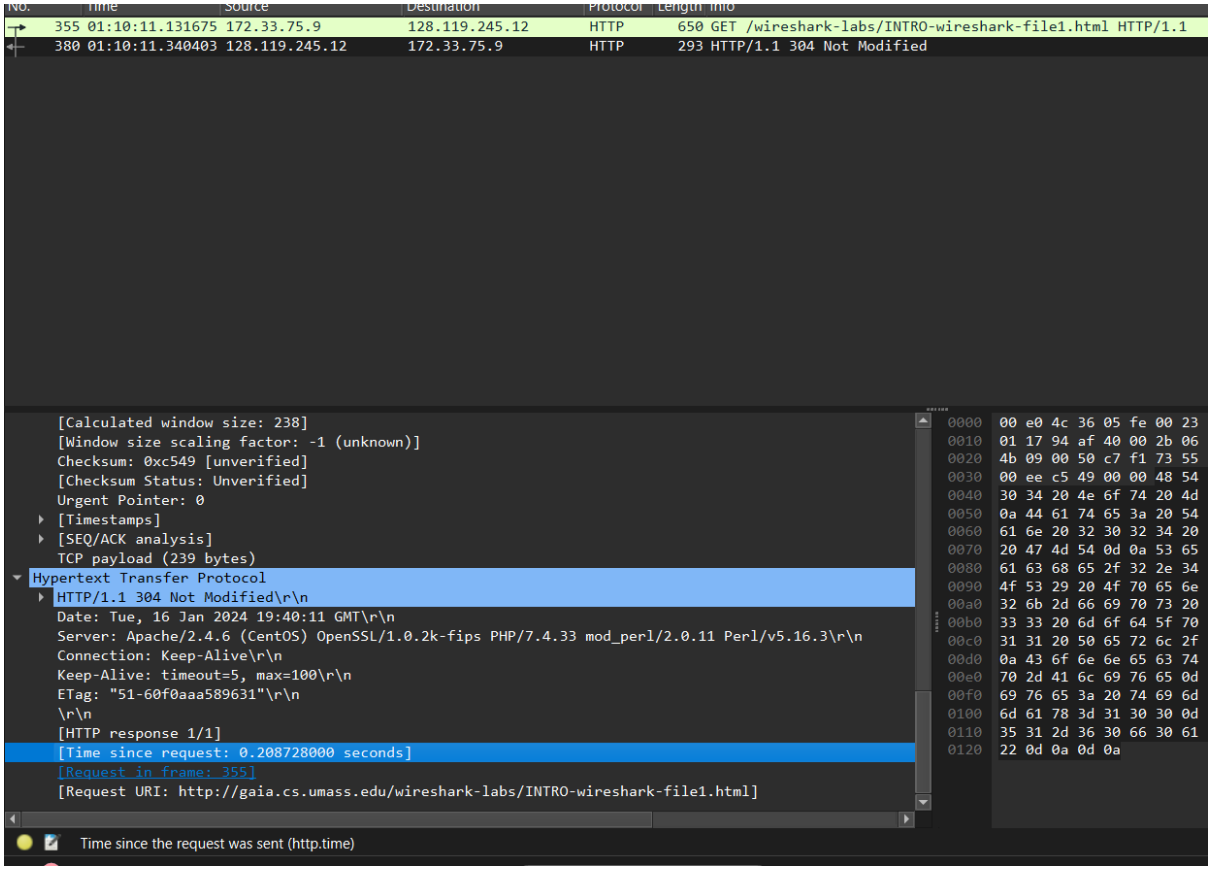


Answer the following questions:

a) In the unfiltered packet-listing window in step above, list the three distinct protocols that are present in the protocol column.

No.	Time	Source	Destination	Protocol	Length	Info
346	01:10:11.038645	142.251.42.65	172.33.75.9	QUIC	654	Protected Payload (KP0)
347	01:10:11.039333	172.33.75.9	142.251.42.65	QUIC	77	Protected Payload (KP0), DCID=fa9b7e4938ca83f7
348	01:10:11.040480	142.251.42.65	172.33.75.9	QUIC	64	Protected Payload (KP0)
349	01:10:11.057459	172.33.75.9	142.250.66.14	QUIC	74	Protected Payload (KP0), DCID=ea98f22061f1fe67
350	01:10:11.073495	172.33.75.9	142.251.42.65	QUIC	74	Protected Payload (KP0), DCID=fa9b7e4938ca83f7
351	01:10:11.074412	142.251.42.65	172.33.75.9	QUIC	66	Protected Payload (KP0)
352	01:10:11.079226	142.251.42.65	172.33.75.9	QUIC	64	Protected Payload (KP0)
353	01:10:11.079488	172.33.75.9	142.251.42.65	QUIC	75	Protected Payload (KP0), DCID=fa9b7e4938ca83f7
354	01:10:11.105762	172.33.75.9	142.250.70.78	UDP	71	60855 → 443 Len=29
355	01:10:11.131675	172.33.75.9	128.119.245.12	HTTP	650	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
356	01:10:11.152499	142.250.70.78	172.33.75.9	UDP	66	443 → 60855 Len=24
357	01:10:11.166586	142.250.66.14	172.33.75.9	QUIC	716	Protected Payload (KP0)
358	01:10:11.166586	142.250.66.14	172.33.75.9	QUIC	101	Protected Payload (KP0)
359	01:10:11.167272	172.33.75.9	142.250.66.14	QUIC	77	Protected Payload (KP0), DCID=ea98f22061f1fe67
360	01:10:11.196220	142.250.70.78	172.33.75.9	UDP	1292	443 → 60855 Len=1250
361	01:10:11.196220	142.250.70.78	172.33.75.9	UDP	73	443 → 60855 Len=31
362	01:10:11.196220	142.250.66.14	172.33.75.9	QUIC	716	Protected Payload (KP0)
363	01:10:11.196645	172.33.75.9	142.250.66.14	QUIC	75	Protected Payload (KP0), DCID=ea98f22061f1fe67
364	01:10:11.197122	172.33.75.9	142.250.70.78	UDP	77	60855 → 443 Len=35
365	01:10:11.209375	142.250.70.78	172.33.75.9	UDP	63	443 → 60855 Len=21

b) How long did it take between sending the HTTP GET message and receiving the HTTP OK response? (By default, the Time column in the packet listing window displays the duration of Wireshark tracing in seconds.Select the Wireshark View pull-down menu, then click Time Show Format, then click Time-of-day to display the Time field in time-of-day format.)



c) 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?