

# Wireshark

## Aadhitya Swarnesh :

I)

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.

No.	Time	Source	Destination	Protocol	Length	Info
4254	712.014592	192.168.43.114	74.125.24.189	TCP	66	49616 → 443 [ACK] Seq=3447 Ack=5951 Win=2046 Len=0 TSval=333269328 TSecr=2275161083
4255	712.015914	192.168.43.114	74.125.24.189	TLSv1	185	Application Data
4256	712.079809	74.125.24.189	192.168.43.114	TLSv1	105	[TCP Spurious Retransmission] , Application Data
4257	712.079906	192.168.43.114	74.125.24.189	TCP	78	[TCP Dup ACK 4254#1] 49616 → 443 [ACK] Seq=3486 Ack=5951 Win=2048 Len=0 TSval=333269392
4258	712.136058	74.125.24.189	192.168.43.114	TCP	66	443 → 49616 [ACK] Seq=5951 Ack=3486 Win=566 Len=0 TSval=2275161640 TSecr=333269329
4259	712.299998	192.168.43.114	74.125.24.189	TLSv1	367	Application Data
4260	712.367995	74.125.24.189	192.168.43.114	TCP	66	443 → 49616 [ACK] Seq=5951 Ack=3787 Win=576 Len=0 TSval=2275161900 TSecr=333269611
4261	712.377477	74.125.24.189	192.168.43.114	TLSv1	272	Application Data
4262	712.377484	74.125.24.189	192.168.43.114	TLSv1	118	Application Data
4263	712.377591	192.168.43.114	74.125.24.189	TCP	66	49616 → 443 [ACK] Seq=3787 Ack=6157 Win=2044 Len=0 TSval=333269687 TSecr=2275161910
4264	712.377592	192.168.43.114	74.125.24.189	TCP	66	49616 → 443 [ACK] Seq=3787 Ack=6209 Win=2043 Len=0 TSval=333269687 TSecr=2275161910

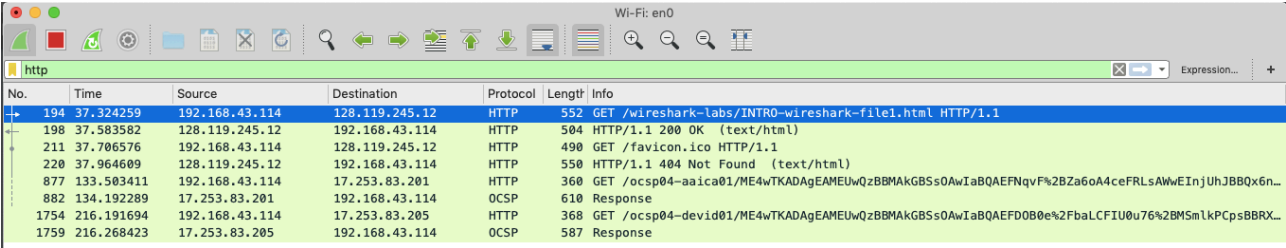
2. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packet-listing window is the amount of time, in seconds, since Wireshark tracing began. To display the Time field in time-of-day format, select the Wireshark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

No.	Time	Source	Destination	Protocol	Length	Info
194	37.324259	192.168.43.114	128.119.245.12	HTTP	552	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
198	37.583582	128.119.245.12	192.168.43.114	HTTP	504	HTTP/1.1 200 OK (text/html)
211	37.706576	192.168.43.114	128.119.245.12	HTTP	490	GET /favicon.ico HTTP/1.1
220	37.964609	128.119.245.12	192.168.43.114	HTTP	550	HTTP/1.1 404 Not Found (text/html)
877	133.503411	192.168.43.114	17.253.83.201	HTTP	360	GET /ocsp04-aaica01/ME4wTKADAgEAMEUwQzBBMAkGBS0AwIaBQAEPNqvF%2BZa6oA4ceFRLsAwEInjUhJBBQx6n...
882	134.192289	17.253.83.201	192.168.43.114	OCSP	610	Response
1754	216.191694	192.168.43.114	17.253.83.205	HTTP	368	GET /ocsp04-devid01/ME4wTKADAgEAMEUwQzBBMAkGBS0AwIaBQAEPD0B0e%2FbaLCFIU0u76%2BM5m1kPCps8BRX...
1759	216.268423	17.253.83.205	192.168.43.114	OCSP	587	Response

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.

Hypertext Transfer Protocol						
▶ GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n						
Host: gaia.cs.umass.edu\r\n						
Connection: keep-alive\r\n						
DNT: 1\r\n						
Upgrade-Insecure-Requests: 1\r\n						
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.120 Safari...						
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b...						
Accept-Encoding: gzip, deflate\r\n						
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8\r\n						
\r\n						
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]						
[HTTP request 1/2]						
[Response in frame: 198]						
[Next request in frame: 211]						

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.



The screenshot shows the Wireshark interface with a packet capture on the 'http' filter. The packet list pane shows several packets, with packet 198 selected. The packet details pane shows the selected packet is an HTTP 200 OK response.

No.	Time	Source	Destination	Protocol	Length	Info
194	37.324259	192.168.43.114	128.119.245.12	HTTP	552	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
198	37.583582	128.119.245.12	192.168.43.114	HTTP	504	HTTP/1.1 200 OK (text/html)
211	37.706576	192.168.43.114	128.119.245.12	HTTP	490	GET /favicon.ico HTTP/1.1
220	37.964609	128.119.245.12	192.168.43.114	HTTP	550	HTTP/1.1 404 Not Found (text/html)
877	133.503411	192.168.43.114	17.253.83.201	HTTP	360	GET /ocsp04-aaica01/ME4wTKADAgEAMEUwQzBBMAKGBSs0AwIaBQAEFNqvF%2BZa6oA4ceFRLsAWwEInjUhJBBQx6n...
882	134.192289	17.253.83.201	192.168.43.114	OCSP	610	Response
1754	216.191694	192.168.43.114	17.253.83.205	HTTP	368	GET /ocsp04-devid01/ME4wTKADAgEAMEUwQzBBMAKGBSs0AwIaBQAEFD0B0e%2FbaLCFIU0u76%2BMSmIkPCpsBBRX...
1759	216.268423	17.253.83.205	192.168.43.114	OCSP	587	Response

## II)

1)

### Capture

...using this filter:

5 interfaces shown, 10 hidden

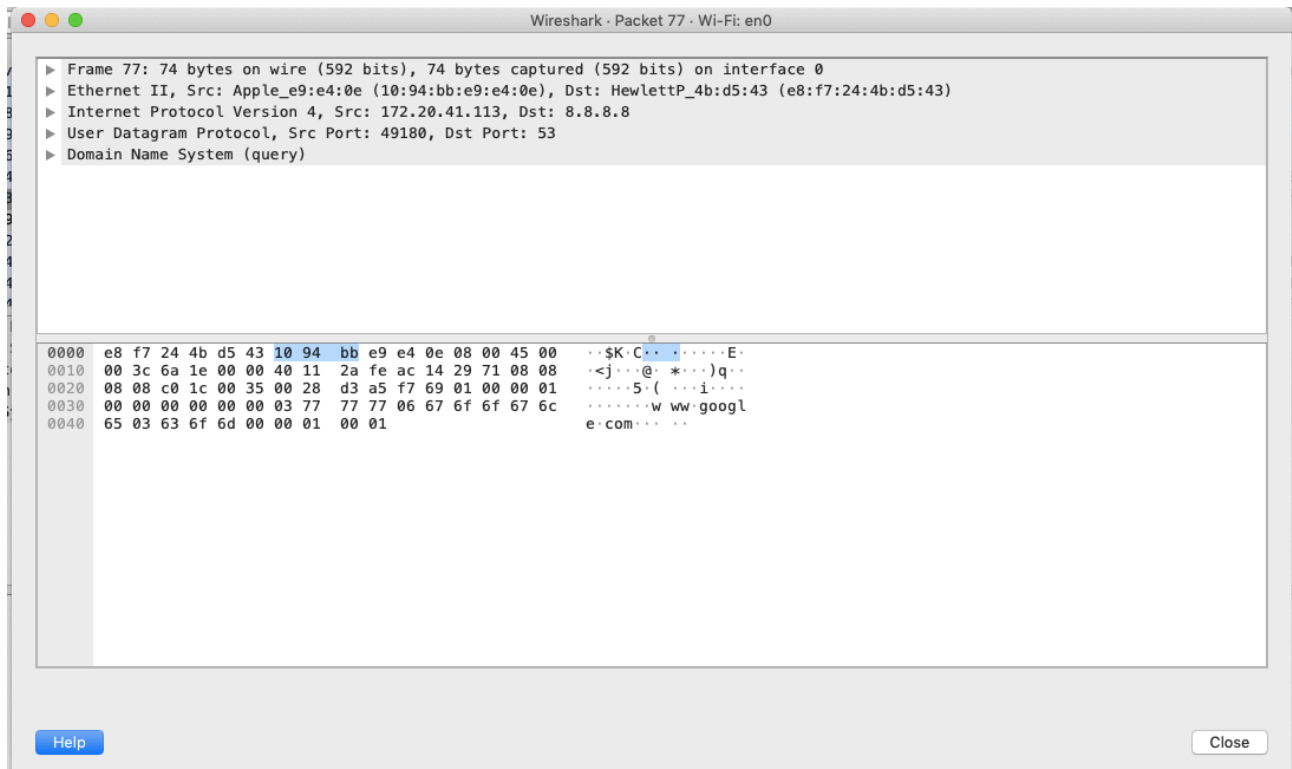
Interface	Wired	USB	External Capture	Virtual
enp3s0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
any	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Loopback-Lo	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
nfiog	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
nfiog	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
nfiog	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

### Learn

[User's Guide](#) · [Wiki](#) · [Questions and Answers](#) · [Mailing Lists](#)

You are running Wireshark 2.4.5 (Git v2.4.5 packaged as 2.4.5-1).

2)



3)

# Resolved addresses found in /var/folders/17/s\_gfyxx51j9\_nzf2rf0xtdxw0000gn/T//wireshark\_Wi-Fi\_20191016211155\_Q4jQmF.pcapng

# Comments

#

# No entries.

# Hosts

#

# 1 entries.

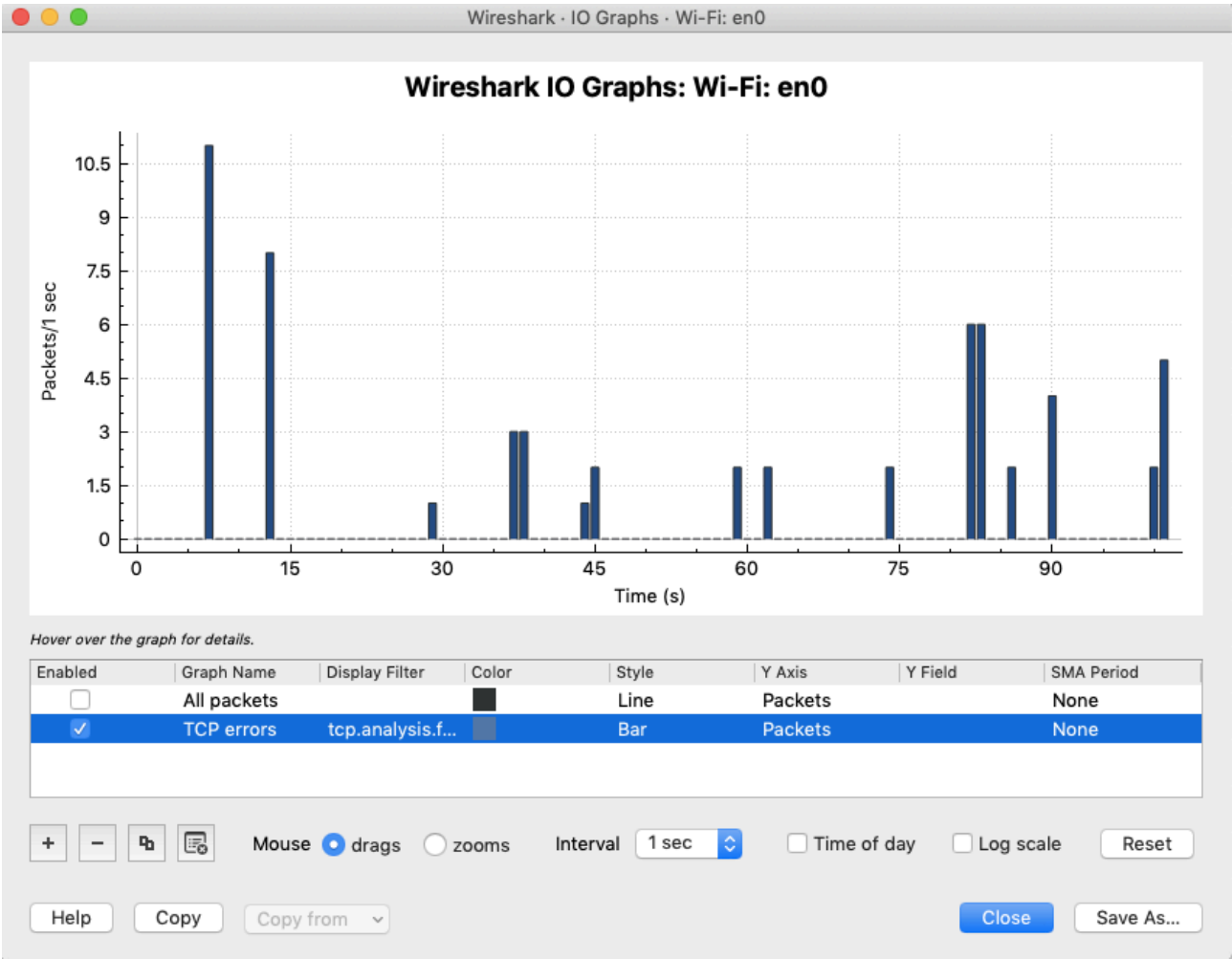
172.217.163.196      www.google.com

# Services

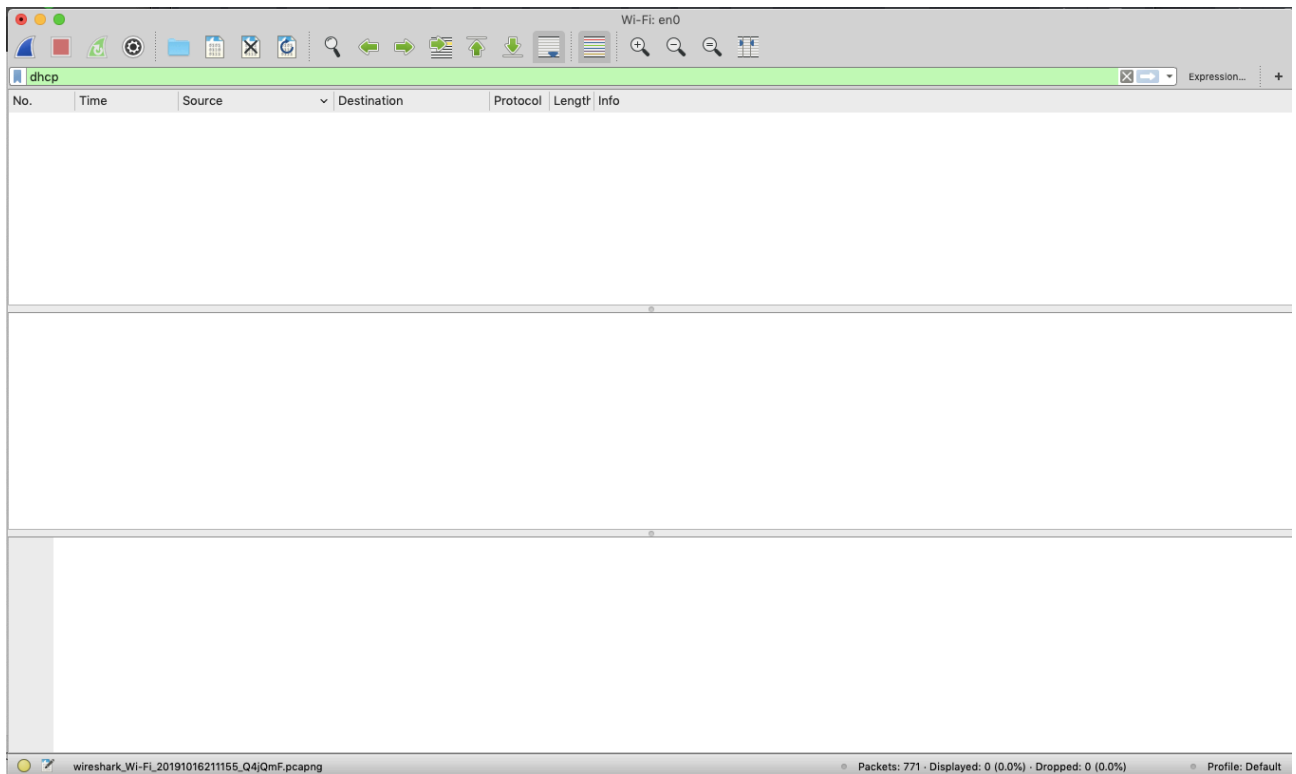
#

# 6076 entries.

4)



5)



6)

