

Lab 8

Filter = HTTP

No.	Time	Source	Destination	Protocol	Length	Info
346	1.2.28907000 10.102.110.7	213.202.3.240	10.102.110.7	HTTP	484	/filestreamingservice/files/13d0ef9b-70c8-43c9-9a51-13c752dfb7777p1=1761688167&p2=404&p3=2&p4=TkepdvRgBHuycE1516C182JURv%2bGL%2b51v4#VTZLYB1s%2FPxAcZLvnkNfLw
360	1.4.333421000 213.202.3.240	10.102.110.7	10.102.110.7	HTTP	954	HTTP/1.1 206 Partial Content (Application/x-chrome-extension)
528	2.0.446654000 10.102.110.23	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1	
602	2.572789000 10.102.110.7	213.202.3.240	HTTP	484	GET /filestreamingservice/files/13d0ef9b-70c8-43c9-9a51-13c752dfb7777p1=1761688167&p2=404&p3=2&p4=TkepdvRgBHuycE1516C182JURv%2bGL%2b51v4#VTZLYB1s%2FPxAcZLvnkNfLw	
603	2.572789000 10.102.110.23	10.102.110.7	HTTP	724	HTTP/1.1 206 Partial Content (Application/x-chrome-extension)	
949	1.6.480389000 10.102.110.7	213.202.3.240	HTTP	484	GET /filestreamingservice/files/13d0ef9b-70c8-43c9-9a51-13c752dfb7777p1=1761688167&p2=404&p3=2&p4=TkepdvRgBHuycE1516C182JURv%2bGL%2b51v4#VTZLYB1s%2FPxAcZLvnkNfLw	
984	1.788151000 213.202.3.240	10.102.110.7	HTTP	932	HTTP/1.1 206 Partial Content (Application/x-chrome-extension)	
1195	4.1.391720000 10.102.110.7	213.202.3.240	HTTP	484	GET /filestreamingservice/files/13d0ef9b-70c8-43c9-9a51-13c752dfb7777p1=1761688167&p2=404&p3=2&p4=TkepdvRgBHuycE1516C182JURv%2bGL%2b51v4#VTZLYB1s%2FPxAcZLvnkNfLw	
1200	4.1.391720000 10.102.110.23	10.102.110.7	HTTP	394	HTTP/1.1 206 Partial Content (Application/x-chrome-extension)	
1273	5.0.490484000 10.102.110.23	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1	
1475	5.9.002264000 10.102.110.7	213.202.3.240	HTTP	484	GET /filestreamingservice/files/13d0ef9b-70c8-43c9-9a51-13c752dfb7777p1=1761688167&p2=404&p3=2&p4=TkepdvRgBHuycE1516C182JURv%2bGL%2b51v4#VTZLYB1s%2FPxAcZLvnkNfLw	
1519	6.0.611297000 213.202.3.240	10.102.110.7	HTTP	60	HTTP/1.1 206 Partial Content (Application/x-chrome-extension)	
2620	6.0.611297000 10.102.110.13	239.255.255.250	SSDP	211	M-SEARCH * HTTP/1.1	
2629	6.0.6062182000 10.102.110.23	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1	
3618	6.9.938105000 10.102.110.13	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1	
4007	7.9.9526439000 10.102.110.13	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1	
4441	8.0.9526439000 10.102.110.13	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1	
4738	11.0.093778000 10.102.110.23	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1	
6346	12.8.1819100 10.102.110.7	34.104.35.123	HTTP	327	HEAD /edged1/release2/chrome_component/j2hxfel20cc5s1tu1t1wgpx6x1_3/ojhpjlocmboigmpkhl1aaeambhph3_a11_gplutbkdljxxbjol3s1q7kive.crx3 HTTP/1.1	
6356	12.8.1819100 10.102.110.7	34.104.35.123	HTTP	395	GET /edged1/release2/chrome_component/j2hxfel20cc5s1tu1t1wgpx6x1_3/ojhpjlocmboigmpkhl1aaeambhph3_a11_gplutbkdljxxbjol3s1q7kive.crx3 HTTP/1.1	
6784	13.0.093778000 10.102.110.23	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1	
6993	14.8.838348000 10.102.110.7	34.104.35.123	HTTP	402	GET /edged1/release2/chrome_component/j2hxfel20cc5s1tu1t1wgpx6x1_3/ojhpjlocmboigmpkhl1aaeambhph3_a11_gplutbkdljxxbjol3s1q7kive.crx3 HTTP/1.1	
7232	16.0.043183000 10.102.110.7	34.104.35.123	HTTP	402	GET /edged1/release2/chrome_component/j2hxfel20cc5s1tu1t1wgpx6x1_3/ojhpjlocmboigmpkhl1aaeambhph3_a11_gplutbkdljxxbjol3s1q7kive.crx3 HTTP/1.1	
7337	16.0.043183000 10.102.110.7	12.8.1819100	HTTP	442	GET /wlanclient.htm INTR0-wreshark-File1.html HTTP/1.1	
7385	16.5.32293100 128.119.245.12	10.102.110.7	HTTP	492	HTTP/1.1 200 (text/html)	
7465	17.0.07172000 10.102.110.7	34.104.35.123	HTTP	403	GET /edged1/release2/chrome_component/j2hxfel20cc5s1tu1t1wgpx6x1_3/ojhpjlocmboigmpkhl1aaeambhph3_a11_gplutbkdljxxbjol3s1q7kive.crx3 HTTP/1.1	
7467	17.0.01334000 10.102.110.7	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1	
7597	17.0.01334000 10.102.110.7	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1	
7602	18.1.12818000 10.102.110.7	34.104.35.123	HTTP	404	GET /edged1/release2/chrome_component/j2hxfel20cc5s1tu1t1wgpx6x1_3/ojhpjlocmboigmpkhl1aaeambhph3_a11_gplutbkdljxxbjol3s1q7kive.crx3 HTTP/1.1	
7608	19.1.14611300 10.102.110.7	34.104.35.123	HTTP	395	GET /edged1/release2/chrome_component/j2hxfel20cc5s1tu1t1wgpx6x1_3/ojhpjlocmboigmpkhl1aaeambhph3_a11_gplutbkdljxxbjol3s1q7kive.crx3 HTTP/1.1	
7759	20.1.19602700 10.102.110.7	34.104.35.123	HTTP	404	GET /edged1/release2/chrome_component/j2hxfel20cc5s1tu1t1wgpx6x1_3/ojhpjlocmboigmpkhl1aaeambhph3_a11_gplutbkdljxxbjol3s1q7kive.crx3 HTTP/1.1	
8030	21.2.283664000 10.102.110.7	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1	
8091	21.2.273743000 10.102.110.7	34.104.35.123	HTTP	406	GET /edged1/release2/chrome_component/j2hxfel20cc5s1tu1t1wgpx6x1_3/ojhpjlocmboigmpkhl1aaeambhph3_a11_gplutbkdljxxbjol3s1q7kive.crx3 HTTP/1.1	
8312	22.22.283664000 10.102.110.7	34.104.35.123	HTTP	406	GET /edged1/release2/chrome_component/j2hxfel20cc5s1tu1t1wgpx6x1_3/ojhpjlocmboigmpkhl1aaeambhph3_a11_gplutbkdljxxbjol3s1q7kive.crx3 HTTP/1.1	
8689	23.2.327171000 10.102.110.7	34.104.35.123	HTTP	406	GET /edged1/release2/chrome_component/j2hxfel20cc5s1tu1t1wgpx6x1_3/ojhpjlocmboigmpkhl1aaeambhph3_a11_gplutbkdljxxbjol3s1q7kive.crx3 HTTP/1.1	
8800	23.2.327171000 10.102.110.23	10.102.110.7	HTTP	1541	HTTP/1.1 200 (application/octet-stream)	
8908	23.2.92889000 10.102.110.28	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1	
8914	24.0.04000200 10.102.110.22	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1	
9004	25.0.04200000 10.102.110.22	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1	
9005	25.0.04200000 10.102.110.22	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1	
9148	26.9.43287000 10.102.110.28	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1	
9166	27.0.06060000 10.102.110.22	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1	
9170	29.0.07406000 10.102.110.28	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1	
9372	31.3.26272000 10.102.110.28	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1	
9609	32.3.18476600 10.102.110.28	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1	

List up to 10 protocols that appear in the protocol column

following are 10 protocols:

- TCP
- UDP
- MDNS
- HTTP
- SSDP
- LLMNR
- DNS
- NBNS
- TLSv1.3
- DHCP

Cmd ipconfig

Ethernet adapter Ethernet 4:

```
Connection-specific DNS Suffix . : fastlhr.nu.edu.pk
Link-local IPv6 Address . . . . . : fe80::64c3:a16c:fd12:2beb%14
IPv4 Address. . . . . : 10.102.110.7
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.102.110.1
```

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

8019 20. 920479000 10.102.110.28	239.255.255.250	SSDP	179 M-SEARCH * HTTP/1.1
8039 20. 920479000 10.102.110.28	34.104.35.123	HTTP	406 GET /edgeg1/release2/chrome_component/32hxfel2occ5s1tujtwgp6x1_3/ojhp]ocmboodgmfpkhlaeasnlbhrphh_3_a11_gp1utbkd1jxbjolks1q7k1ve.crx3 HTTP/1.1
8312 22. 283664000 10.102.110.7	34.104.35.123	HTTP	406 GET /edgeg1/release2/chrome_component/32hxfel2occ5s1tujtwgp6x1_3/ojhp]ocmboodgmfpkhlaeasnlbhrphh_3_a11_gp1utbkd1jxbjolks1q7k1ve.crx3 HTTP/1.1
8689 23. 323716000 10.102.110.7	34.104.35.123	HTTP	406 GET /edgeg1/release2/chrome_component/32hxfel2occ5s1tujtwgp6x1_3/ojhp]ocmboodgmfpkhlaeasnlbhrphh_3_a11_gp1utbkd1jxbjolks1q7k1ve.crx3 HTTP/1.1
8804 23. 364679000 34.104.35.123	10.102.110.7	HTTP	1514 HTTP/1.1 200 OK (application/octet-stream)
8908 23. 928890000 10.102.110.28	239.255.255.250	SSDP	179 M-SEARCH * HTTP/1.1

$$23.364 - 23.237 = 0.127\text{s}$$

What is the Internet address of the gaia.cs.umass.edu? What is the Internet address of your computer?

Address of gaia.cs.umass.edu: 34.104.35.123

Address of my computer: 10.102.110.1

Write down the sequence number of the first TCP packet.

Seq=1

*Ethernet 4 [Wireshark 1.12.1 (v1.12.1-0-g01b65bf from master-1.12)]						
File	Edit	View	Go	Capture	Analyze	Statistics
Telephony	Tools	Internals	Help			
Filter: tcp				Expression...	Clear	Apply
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.102.110.7	10.102.110.20	TCP	54	7680-50070 [ACK] Seq=1 Ack=1 Win=8194 Len=0
2	0.000694000	10.102.110.20	10.102.110.7	TCP	63	50070-7680 [PSH, ACK] Seq=1 Ack=1 Win=1026 Len=9
3	0.002735000	142.250.202.195	10.102.110.7	TCP	60	443-52278 [ACK] Seq=1 Ack=1 Win=1045 Len=0
4	0.002736000	142.250.202.195	10.102.110.7	TCP	60	443-52278 [ACK] Seq=1 Ack=112 Win=1045 Len=0
5	0.002736000	142.250.202.195	10.102.110.7	TLSv1.2	195	Application Data
6	0.002758000	10.102.110.7	142.250.202.195	TCP	54	52278-443 [ACK] Seq=112 Ack=142 Win=8196 Len=0
7	0.002809000	142.250.202.195	10.102.110.7	TLSv1.2	196	Application Data
8	0.002811000	142.250.202.195	10.102.110.7	TLSv1.2	93	Application Data
9	0.002817000	10.102.110.7	142.250.202.195	TCP	54	52278-443 [ACK] Seq=112 Ack=323 Win=8195 Len=0
10	0.003005000	10.102.110.7	142.250.202.195	TLSv1.2	93	Application Data
11	0.007363000	10.102.110.7	142.250.202.195	TLSv1.2	165	Application Data

POST-LAB

Q: What do you mean by TCP three-way handshaking? Identify SYN, SYN-ACK and ACK packets generated for TCP connection setup.

Three-way handshaking is a procedure followed by the connection-oriented protocol TCP. TCP ensures reliable data delivery across the network. The three-way handshake involves the following three steps:

- synchronize (SYN)
- synchronize-acknowledge (SYN-ACK)
- acknowledge (ACK)

The client sends a synchronization SYN request requesting to initiate the TCP connection. The server responds by sending a SYN-ACK reply which is an acknowledgment to the request sent by the client. Finally, the client again responds with an acknowledgment ACK to complete the TCP connection and this forms the three-way handshaking.

Q: What is the purpose of FIN and ACK flags in TCP header?

In the TCP header, the FIN and ACK are flags in the TCP header which are used to indicate the closing of the TCP connection. The FIN flag is set when the client requests to finish the TCP connection. The ACK flag is then set to acknowledge this request, thus closing the TCP connection.