

Lab 8

Filter = HTTP

The screenshot shows a Wireshark capture of network traffic. The top toolbar includes icons for File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, Internals, and Help. The main display area is divided into three panes: Packet List, Packet Details, and Packet Bytes.

Packet List: The list shows 100 packets, all of which are HTTP. The columns are No., Time, Source, Destination, Protocol, Length, and Info. The first packet is a GET request to /Filestreamingservice/Files/13d0ef9b-70c8-43c9-9a51-13c752dfb777P1=1761688167&P2=404&P3=2&P4=TKepdvrgBhuyCE1516C18ZJURV6ZbGL2b51v4mVZLYB1sN2FPAZCLVKNFLW. The last packet is a 200 OK response.

Packet Details: The details pane shows the structure of the selected packet (No. 100). It is an HTTP GET request. The fields shown are: Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol. The Hypertext Transfer Protocol section shows the request line: GET /Filestreamingservice/Files/13d0ef9b-70c8-43c9-9a51-13c752dfb777P1=1761688167&P2=404&P3=2&P4=TKepdvrgBhuyCE1516C18ZJURV6ZbGL2b51v4mVZLYB1sN2FPAZCLVKNFLW HTTP/1.1.

Packet Bytes: The bytes pane shows the raw data of the packet. It starts with the Ethernet II header, followed by the IP header, the TCP header, and the HTTP request. The request line is: GET /Filestreamingservice/Files/13d0ef9b-70c8-43c9-9a51-13c752dfb777P1=1761688167&P2=404&P3=2&P4=TKepdvrgBhuyCE1516C18ZJURV6ZbGL2b51v4mVZLYB1sN2FPAZCLVKNFLW HTTP/1.1.

List up to 10 protocols that appear in the protocol column

following are 10 protocols:

- TCP
- UDP
- MDNS
- HTTP
- SSDP
- LLNMR
- 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	20.92040200	10.102.110.28	239.255.255.250	SSDP	179 M-SEARCH * HTTP/1.1
8051	21.23743000	10.102.110.7	34.104.35.123	HTTP	406 GET /edged1/release2/chrome_component/j2hfe120cc5s1ttu3t7wpp6xi_3/ojhpjlocmbogdgnfphlaaeantbhrphh_1_all_gplutbkd1jxxbjolk3stq7kive.crx3 HTTP/1.1
8312	22.28366400	10.102.110.7	34.104.35.123	HTTP	406 GET /edged1/release2/chrome_component/j2hfe120cc5s1ttu3t7wpp6xi_3/ojhpjlocmbogdgnfphlaaeantbhrphh_1_all_gplutbkd1jxxbjolk3stq7kive.crx3 HTTP/1.1
8689	23.32371600	10.102.110.7	34.104.35.123	HTTP	406 GET /edged1/release2/chrome_component/j2hfe120cc5s1ttu3t7wpp6xi_3/ojhpjlocmbogdgnfphlaaeantbhrphh_1_all_gplutbkd1jxxbjolk3stq7kive.crx3 HTTP/1.1
8804	23.36467900	34.104.35.123	10.102.110.7	HTTP	1514 HTTP/1.1 200 OK (application/octet-stream)
8908	23.92889000	10.102.110.28	239.255.255.250	SSDP	179 M-SEARCH * HTTP/1.1

$$23.364 - 23.237 = 0.127s$$

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 Save

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.