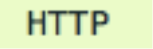
Lab 5

Wireshark Introduction

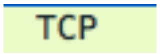
Nicole Merritt

Questions

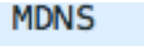
1) List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window



HTTP stands of Hyper Text Transport Protocol. HTTP allows communication between HTTP client and HTTP server. HTTP is text based with headers written in text lines. Furthermore, for webpages that require security HTTPS is used. HTTPS is the combination of security protocol (SSL for example) and HTTP working together to create an encrypted connection.

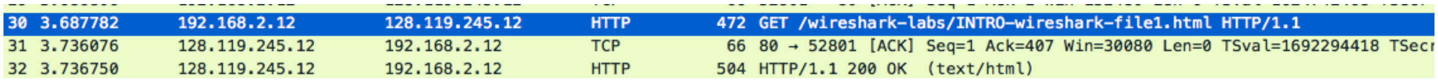


TCP stands for Transmission Control Protocol. TCP initiates a three-way handshake in order to control the connection and minimize problems such as packet loss. The transfer of data is sent as a stream, meaning it is a continuous flow of information until the connection is ended. TCP is reliable and ordered



MDNS stands for Multicast Domain Name System. MDNS is used to link host name to IP address when there is no local name server. To find a host name, a query is sent out that asks the host to identify itself. What is received back is a message including its IP address. From here other machines in the subnet can update using this information.

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



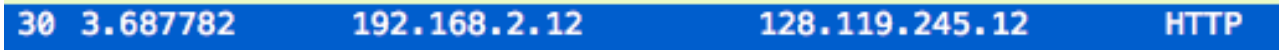
```
30 3.687782   192.168.2.12     128.119.245.12   HTTP   472 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
31 3.736076   128.119.245.12   192.168.2.12     TCP     66 80 → 52801 [ACK] Seq=1 Ack=407 Win=30080 Len=0 TSval=1692294418 TSecr
32 3.736750   128.119.245.12   192.168.2.12     HTTP   504 HTTP/1.1 200 OK  (text/html)
```

HTTP GET occurs at 3.687782

HTTP OK occurs at 3.736076

Therefore, it took 0.04829 seconds between GET and OK

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



```
30  3.687782       192.168.2.12         128.119.245.12        HTTP
```

Gaia.cs.umass.edu IP is 128.119.245.12 **My IP** is 193.168.2.12

Question 4)

```
No.     Time           Source                Destination           Protocol Length Info

     30 3.687782       192.168.2.12          128.119.245.12        HTTP     472    GET /wireshark-
labs/INTRO-wireshark-file1.html HTTP/1.1


Frame 30: 472 bytes on wire (3776 bits), 472 bytes captured (3776 bits) on interface 0

Ethernet II, Src: Apple_a4:89:fe (5c:f9:38:a4:89:fe), Dst: Sagemcom_f5:2d:64 (54:64:d9:f5:2d:64)

Internet Protocol Version 4, Src: 192.168.2.12, Dst: 128.119.245.12

Transmission Control Protocol, Src Port: 52801, Dst Port: 80, Seq: 1, Ack: 1, Len: 406

Hypertext Transfer Protocol


No.     Time           Source                Destination           Protocol Length Info

     32 3.736750       128.119.245.12        192.168.2.12          HTTP     504    HTTP/1.1 200 OK
(text/html)


Frame 32: 504 bytes on wire (4032 bits), 504 bytes captured (4032 bits) on interface 0

Ethernet II, Src: Sagemcom_f5:2d:6a (54:64:d9:f5:2d:6a), Dst: Apple_a4:89:fe (5c:f9:38:a4:89:fe)

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.2.12

Transmission Control Protocol, Src Port: 80, Dst Port: 52801, Seq: 1, Ack: 407, Len: 438

Hypertext Transfer Protocol

Line-based text data: text/html
```