Wireshark Lab 1 -- Getting Started

Jiaying Li

jl10919

Lab environment:

*Answer:* My PC uses macOS Catalina 10.15.6, shows the following setting with *ifconfig*:

A screenshot of text

Description automatically generated

Q1. List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.

*Answer:* As shown in the screenshot below, there are some protocols: TCP, TLSv1.3, DNS, HTTP and DNS

A screenshot of a computer

Description automatically generated

Q2. 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*.)

*Answer:* As shown in the screenshot below, the Get was sent at 20:25:43.799302 and the reply was received at 20:25:43.813936. The delay was thus 0.014634 secs.

A screenshot of a computer

Description automatically generated

3. 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?

*Answer:* As shown in the screenshot below, the IP address of source(my laptop) and destination(gaia.cs.umass.edu) are circled in blue. The IP address of the gaia.cs.umass.edu is 128.119.245.12; the IP address of my laptop is 192.168.1.155

A screenshot of a computer

Description automatically generated

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.

*Answer:*

HTTP GET message:

No. Time Source Destination Protocol Length Info

66 20:25:43.799302 192.168.1.155 128.119.245.12 HTTP 551 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1

Frame 66: 551 bytes on wire (4408 bits), 551 bytes captured (4408 bits) on interface en0, id 0

Ethernet II, Src: Apple\_7b:7f:83 (ac:bc:32:7b:7f:83), Dst: Arcadyan\_5e:ea:89 (b8:f8:53:5e:ea:89)

Internet Protocol Version 4, Src: 192.168.1.155, Dst: 128.119.245.12

Transmission Control Protocol, Src Port: 58626, Dst Port: 80, Seq: 1, Ack: 1, Len: 485

Hypertext Transfer Protocol

GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n

Host: gaia.cs.umass.edu\r\n

If-None-Match: "51-5af675d320fc9"\r\n

Upgrade-Insecure-Requests: 1\r\n

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8\r\n

If-Modified-Since: Wed, 16 Sep 2020 05:16:03 GMT\r\n

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_15\_6) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/13.1.2 Safari/605.1.15\r\n

Accept-Language: en-us\r\n

Accept-Encoding: gzip, deflate\r\n

Connection: keep-alive\r\n

\r\n

[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]

[HTTP request 1/1]

[Response in frame: 68]

HTTP REPLY message:

No. Time Source Destination Protocol Length Info

68 20:25:43.813936 128.119.245.12 192.168.1.155 HTTP 504 HTTP/1.1 200 OK (text/html)

Frame 68: 504 bytes on wire (4032 bits), 504 bytes captured (4032 bits) on interface en0, id 0

Ethernet II, Src: Arcadyan\_5e:ea:89 (b8:f8:53:5e:ea:89), Dst: Apple\_7b:7f:83 (ac:bc:32:7b:7f:83)

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.155

Transmission Control Protocol, Src Port: 80, Dst Port: 58626, Seq: 1, Ack: 486, Len: 438

Hypertext Transfer Protocol

HTTP/1.1 200 OK\r\n

Date: Thu, 17 Sep 2020 00:25:43 GMT\r\n

Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.10 mod\_perl/2.0.11 Perl/v5.16.3\r\n

Last-Modified: Wed, 16 Sep 2020 05:59:01 GMT\r\n

ETag: "51-5af67f6dbf90d"\r\n

Accept-Ranges: bytes\r\n

Content-Length: 81\r\n

Keep-Alive: timeout=5, max=100\r\n

Connection: Keep-Alive\r\n

Content-Type: text/html; charset=UTF-8\r\n

\r\n

[HTTP response 1/1]

[Time since request: 0.014634000 seconds]

[Request in frame: 66]

[Request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]

File Data: 81 bytes

Line-based text data: text/html (3 lines)