Computer Network

Name: Rana AbdullaSaeed Dabwan

Student Number: 2021034184

Date: 2022/09/27

First Lab

---

1. Which of the following protocols are shown as appearing (i.e., are listed in the Wireshark “protocol” column) in your trace file: TCP, QUIC, HTTP, DNS, UDP, TLSv1.2?

Answer - HTTP, TCP, DNS, TLSv1.2

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 packetlisting window is the amount of time, in seconds, since Wireshark tracing began.

The HTTP get message sent time = 10:12:48.433912

The HTTP OK message receiving time = 10:12:48.767887

Time between sent and receive HTTP messages = 0.333975

3. What is the Internet address of the gaia.cs.umass.edu (also known as wwwnet.cs.umass.edu)? What is the Internet address of your computer or (if you are using the trace file) the computer that sent the HTTP GET message?

My Computer Address 192.168.0.5

Destination address 128.119.245.12

4. Expand the information on the HTTP message in the Wireshark “Details of selected packet” window (see Figure 3 above) so you can see the fields in the HTTP GET request message. What type of Web browser issued the HTTP request? The answer is shown at the right end of the information following the “User-Agent:” field in the expanded HTTP message display. [This field value in the HTTP message is how a web server learns what type of browser you are Using.]

http.user_agent == "Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.71 Safari/537.36"

5. Expand the information on the Transmission Control Protocol for this packet in the Wireshark "Details of selected packet" window (see Figure 3 in the lab writeup) so you can see the fields in the TCP segment carrying the HTTP message. What is the destination port number (the number following "Dest Port:" for the TCP segment containing the HTTP request) to which this HTTP request is being sent?

tcp.dstport == 80

6. 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.

```
No.     Time                          Source
Destination           Protocol Length Info
   8073 2017-01-28 23:52:12.290000    160.39.134.64
128.119.245.12        HTTP     501    GET
/wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1

Frame 8073: 501 bytes on wire (4008 bits), 501 bytes captured (4008
bits) on interface 0
Ethernet II, Src: Apple_ea:75:8b (d0:a6:37:ea:75:8b), Dst:
Cisco_9f:f0:00 (00:00:0c:9f:f0:00)
Internet Protocol Version 4, Src: 160.39.134.64, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 58522, Dst Port: 80, Seq: 1,
Ack: 1, Len: 435
Hypertext Transfer Protocol
    GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
        [Expert Info (Chat/Sequence): GET
/wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n]
            [GET /wireshark-labs/INTRO-wireshark-file1.html
HTTP/1.1\r\n]
            [Severity level: Chat]
            [Group: Sequence]
        Request Method: GET
        Request URI: /wireshark-labs/INTRO-wireshark-file1.html
        Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_2)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/55.0.2883.95
Safari/537.36\r\n
    Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;
q=0.8\r\n
    DNT: 1\r\n
    Accept-Encoding: gzip, deflate, sdch\r\n
    Accept-Language: en-US,en;q=0.8\r\n
    \r\n
    [Full request URI:
http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
    [HTTP request 1/1]
    [Response in frame: 8075]
```

and

```
No.     Time                          Source
Destination           Protocol Length Info
   8073 2017-01-28 23:52:12.290000    160.39.134.64
128.119.245.12        HTTP     501    GET
/wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1

Frame 8073: 501 bytes on wire (4008 bits), 501 bytes captured (4008
bits) on interface 0
Ethernet II, Src: Apple_ea:75:8b (d0:a6:37:ea:75:8b), Dst:
Cisco_9f:f0:00 (00:00:0c:9f:f0:00)
Internet Protocol Version 4, Src: 160.39.134.64, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 58522, Dst Port: 80, Seq: 1,
Ack: 1, Len: 435
Hypertext Transfer Protocol
    GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
        [Expert Info (Chat/Sequence): GET
/wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n]
            [GET /wireshark-labs/INTRO-wireshark-file1.html
HTTP/1.1\r\n]
            [Severity level: Chat]
            [Group: Sequence]
        Request Method: GET
        Request URI: /wireshark-labs/INTRO-wireshark-file1.html
        Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_2)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/55.0.2883.95
Safari/537.36\r\n
    Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;
q=0.8\r\n
    DNT: 1\r\n
    Accept-Encoding: gzip, deflate, sdch\r\n
    Accept-Language: en-US,en;q=0.8\r\n
    \r\n
    [Full request URI:
http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
    [HTTP request 1/1]
    [Response in frame: 8075]

No.     Time                          Source
Destination           Protocol Length Info
   8075 2017-01-28 23:52:12.302459    128.119.245.12
160.39.134.64         HTTP     504    HTTP/1.1 200 OK  (text/html)

Frame 8075: 504 bytes on wire (4032 bits), 504 bytes captured (4032
bits) on interface 0
Ethernet II, Src: Cisco_72:32:c0 (64:f6:9d:72:32:c0), Dst:
Apple_ea:75:8b (d0:a6:37:ea:75:8b)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 160.39.134.64
Transmission Control Protocol, Src Port: 80, Dst Port: 58522, Seq: 1,
Ack: 436, Len: 438
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
        [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
            [HTTP/1.1 200 OK\r\n]
            [Severity level: Chat]
            [Group: Sequence]
        Request Version: HTTP/1.1
        Status Code: 200
        Response Phrase: OK
    Date: Sun, 29 Jan 2017 04:52:12 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16
mod_perl/2.0.10 Perl/v5.16.3\r\n
    Last-Modified: Sat, 28 Jan 2017 06:59:01 GMT\r\n
    ETag: "51-547221e05df04"\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: 0.012459000 seconds]
        [Request in frame: 8073]
        File Data: 81 bytes
    Line-based text data: text/html
```