Introductory Wireshark 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: The following protocols are shown as appearing

1. Without filtering: `TCP`, `TLSv1.2`, `HTTP`, `DNS` and `UDP`
2. With filtering using `http`: `HTTP` only.

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

Answer: The time it takes from when the HTTP GET message was sent until the HTTP OK reply was received is `18:51:18.327286070 - 18:51:18.289307233 = 0.037978837`

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:

- Internet Address of `gaia.cs.umass.edu` is `128.119.245.12`
- Internet Address of of my computer is `10.0.2.15`

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?

Answer: Firefox

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 to which this HTTP request is being sent?

Answer: 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
     59 18:51:18.289307233 10.0.2.15             128.119.245.12        HTTP     478    GET /wireshark-
labs/INTRO-wireshark-file1.html HTTP/1.1
Frame 59: 478 bytes on wire (3824 bits), 478 bytes captured (3824 bits) on interface eth0, id 0
Ethernet II, Src: PCSSystemtec_ad:25:87 (08:00:27:ad:25:87), Dst: 52:54:00:12:35:00 (52:54:00:12:35:00)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 51880, Dst Port: 80, Seq: 1, Ack: 1, Len: 424
    Source Port: 51880
    Destination Port: 80
    [Stream index: 9]
    [Stream Packet Number: 4]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 424]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 674373965
    [Next Sequence Number: 425    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 7356
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
    Window: 64240
    [Calculated window size: 64240]
    [Window size scaling factor: -2 (no window scaling used)]
    Checksum: 0x8355 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    [Timestamps]
    [SEQ/ACK analysis]
    TCP payload (424 bytes)
Hypertext Transfer Protocol
    GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
        Request Method: GET
        Request URI: /wireshark-labs/INTRO-wireshark-file1.html
        Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/
svg+xml,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    Priority: u=0, i\r\n
    \r\n
    [Response in frame: 62]
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
```

```
No.     Time                  Source                Destination           Protocol Length Info
     62 18:51:18.327286070 128.119.245.12        10.0.2.15             HTTP     492    HTTP/1.1 200
OK  (text/html)
Frame 62: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface eth0, id 0
Ethernet II, Src: 52:54:00:12:35:00 (52:54:00:12:35:00), Dst: PCSSystemtec_ad:25:87 (08:00:27:ad:25:87)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.2.15
Transmission Control Protocol, Src Port: 80, Dst Port: 51880, Seq: 1, Ack: 425, Len: 438
    Source Port: 80
    Destination Port: 51880
    [Stream index: 9]
    [Stream Packet Number: 5]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 438]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 7356
    [Next Sequence Number: 439    (relative sequence number)]
    Acknowledgment Number: 425    (relative ack number)
    Acknowledgment number (raw): 674374389
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
    Window: 32344
    [Calculated window size: 32344]
    [Window size scaling factor: -2 (no window scaling used)]
    Checksum: 0x0ff0 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    [Timestamps]
    [SEQ/ACK analysis]
    TCP payload (438 bytes)
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
        Response Version: HTTP/1.1
        Status Code: 200
        [Status Code Description: OK]
        Response Phrase: OK
    Date: Wed, 01 Jan 2025 23:51:19 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Wed, 01 Jan 2025 06:59:02 GMT\r\n
    ETag: "51-62a9f94a29fac"\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
    [Request in frame: 59]
    [Time since request: 0.037978837 seconds]
    [Request URI: /wireshark-labs/INTRO-wireshark-file1.html]
    [Full 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)
```