LAB 1

1. TLSv1.2, TCP, MDNS, UDP, DNS, QUIC, HTTP
2. Time
    a. GET: Sep 19, 2024 12:57:48.866237000 SE Asia Standard Time
    b. OK: Sep 19, 2024 12:57:49.137501000 SE Asia Standard Time
3. Address
    a. gaia.cs.umass.edu: 128.119.245.12
    b. My computer: 10.226.161.204
4. HTTP:
    a. GET:

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
Connection: keep-alive\r\n
Cache-Control: max-age=0\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.0.0 Safari/537.36\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9\r\n
If-None-Match: "51-622727e630b2a"\r\n
If-Modified-Since: Thu, 19 Sep 2024 05:50:02 GMT\r\n
\r\n
[Response in frame: 59]
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]

    b. OK:

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: Thu, 19 Sep 2024 05:57:51 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: Thu, 19 Sep 2024 05:57:02 GMT\r\n

ETag: "51-6227297703763"\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: 52]
[Time since request: 0.271264000 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

5.

Transmission Control Protocol, Src Port: 60839, Dst Port: 80, Seq: 1, Ack: 1, Len: 584
Source Port: 60839
Destination Port: 80
[Stream index: 2]
[Stream Packet Number: 4]
[Conversation completeness: Incomplete, DATA (15)]
..0. .... = RST: Absent
...0 .... = FIN: Absent
.... 1... = Data: Present
.... .1.. = ACK: Present
.... ..1. = SYN-ACK: Present
....1 = SYN: Present
[Completeness Flags: ··DASS]
[TCP Segment Len: 584]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 719270643
[Next Sequence Number: 585 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 453156074
0101 .... = Header Length: 20 bytes (5)
Flags: 0x018 (PSH, ACK)
000. .... = Reserved: Not set
...0 .... = Accurate ECN: Not set
.... 0... .... = Congestion Window Reduced: Not set
.... .0.. .... = ECN-Echo: Not set
.... ..0. .... = Urgent: Not set
....1 .... = Acknowledgment: Set
.... 1... = Push: Set
.... .0.. = Reset: Not set
....0. = Syn: Not set

```
    .... .... ...0 = Fin: Not set
    [TCP Flags: ·····AP···]
Window: 514
[Calculated window size: 131584]
[Window size scaling factor: 256]
Checksum: 0x2495 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
[Timestamps]
    [Time since first frame in this TCP stream: 0.273068000 seconds]
    [Time since previous frame in this TCP stream: 0.000129000 seconds]
[SEQ/ACK analysis]
    [iRTT: 0.272939000 seconds]
    [Bytes in flight: 584]
    [Bytes sent since last PSH flag: 584]
TCP payload (584 bytes)
```

6. print:

```
No.     Time               Source                Destination           Protocol Length Info
     59 12:57:49.137501    128.119.245.12        10.226.161.204        HTTP     492    HTTP/1.1 200 OK  (text/html)
Frame 59: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface \Device\NPF_{1033507C-5E50-4885-
AD07-33B7FA967B5A}, id 0
Ethernet II, Src: JuniperNetwo_c3:52:01 (40:b4:f0:c3:52:01), Dst: Intel_fb:bf:e4 (84:7b:57:fb:bf:e4)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.226.161.204
Transmission Control Protocol, Src Port: 80, Dst Port: 60839, Seq: 1, Ack: 585, Len: 438
    Source Port: 80
    Destination Port: 60839
    [Stream index: 2]
    [Stream Packet Number: 6]
    [Conversation completeness: Incomplete, DATA (15)]
        ..0. .... = RST: Absent
        ...0 .... = FIN: Absent
        .... 1... = Data: Present
        .... .1.. = ACK: Present
        .... ..1. = SYN-ACK: Present
        .... ...1 = SYN: Present
        [Completeness Flags: ··DASS]
    [TCP Segment Len: 438]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 453156074
    [Next Sequence Number: 439    (relative sequence number)]
    Acknowledgment Number: 585    (relative ack number)
    Acknowledgment number (raw): 719271227
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
    Window: 238
    [Calculated window size: 30464]
    [Window size scaling factor: 128]
    Checksum: 0x4839 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    [Timestamps]
        [Time since first frame in this TCP stream: 0.544332000 seconds]
        [Time since previous frame in this TCP stream: 0.002088000 seconds]
    [SEQ/ACK analysis]
        [iRTT: 0.272939000 seconds]
        [Bytes in flight: 438]
        [Bytes sent since last PSH flag: 438]
    TCP payload (438 bytes)
Hypertext Transfer Protocol
Line-based text data: text/html (3 lines)
```

```
No.     Time               Source                Destination           Protocol Length Info
     52 12:57:48.866237    10.226.161.204        128.119.245.12        HTTP     638    GET /wireshark-labs/INTRO-wireshark-
file1.html HTTP/1.1
Frame 52: 638 bytes on wire (5104 bits), 638 bytes captured (5104 bits) on interface \Device\NPF_{1033507C-5E50-4885-
AD07-33B7FA967B5A}, id 0
Ethernet II, Src: Intel_fb:bf:e4 (84:7b:57:fb:bf:e4), Dst: JuniperNetwo_c3:52:01 (40:b4:f0:c3:52:01)
Internet Protocol Version 4, Src: 10.226.161.204, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 60839, Dst Port: 80, Seq: 1, Ack: 1, Len: 584
    Source Port: 60839
    Destination Port: 80
    [Stream index: 2]
    [Stream Packet Number: 4]
    [Conversation completeness: Incomplete, DATA (15)]
        ..0. .... = RST: Absent
        ...0 .... = FIN: Absent
        .... 1... = Data: Present
        .... .1.. = ACK: Present
        .... ..1. = SYN-ACK: Present
        .... ...1 = SYN: Present
        [Completeness Flags: ··DASS]
    [TCP Segment Len: 584]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 719270643
    [Next Sequence Number: 585    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 453156074
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
    Window: 514
    [Calculated window size: 131584]
    [Window size scaling factor: 256]
    Checksum: 0x2495 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    [Timestamps]
        [Time since first frame in this TCP stream: 0.273068000 seconds]
        [Time since previous frame in this TCP stream: 0.000129000 seconds]
    [SEQ/ACK analysis]
        [iRTT: 0.272939000 seconds]
        [Bytes in flight: 584]
        [Bytes sent since last PSH flag: 584]
    TCP payload (584 bytes)
Hypertext Transfer Protocol
```