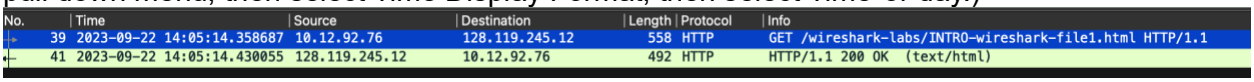
Q1. Which of the following protocols are shown as appearing (i.e., are listed in the Wireshark “protocol” column) in your trace file: TCP, QUIC, HTTP, DNS, UDP, TLSv1.2?

HTTP

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. (If you want 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.)



No.	Time	Source	Destination	Length	Protocol	Info
39	2023-09-22 14:05:14.358687	10.12.92.76	128.119.245.12	558	HTTP	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
41	2023-09-22 14:05:14.430055	128.119.245.12	10.12.92.76	492	HTTP	HTTP/1.1 200 OK (text/html)

Get was at 14.3586 and ok was at 14.4300 so it took about 0.714 seconds

Q3. What is the Internet address of the gaia.cs.umass.edu? What is the Internet address of your computer that sent the HTTP GET message?

Address of the source is 10.12.92.76

The address of my computer IS 128.119.245.12

Q4. Expand the information on the HTTP message in the Wireshark “Details of selected packet” window 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.]
• Example: Firefox, Safari, Microsoft Internet Edge, Other

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.0.0 Safari/537.36\r\n

It was safari.

Q5. Expand the information on the Transmission Control Protocol for this packet in the Wireshark “Details of selected packet” window 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?

Destination Port: 80

Q6. If you enter the URL: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html multiple times during Wireshark packet capture, are there any difference in the sent HTTP message and the received HTTP reply?

There is no difference if you run it in the same same browser (safari) but when I paste the link in chrome would say Not modified 304 instead OK 200.

/var/folders/v7/w7smch4d1y9dkg9rv6fcz6qc0000gn/T/wireshark_Wi-Fi36YIB2.pcapng 42 total packets, 2 shown

```
No.     Time                           Source                Destination           Length Protocol
Info
     39 2023-09-22 14:05:14.358687     10.12.92.76           128.119.245.12        558    HTTP
GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
Frame 39: 558 bytes on wire (4464 bits), 558 bytes captured (4464 bits) on interface en0, id 0
    Section number: 1
    Interface id: 0 (en0)
        Interface name: en0
        Interface description: Wi-Fi
    Encapsulation type: Ethernet (1)
    Arrival Time: Sep 22, 2023 14:05:14.358687000 MDT
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1695413114.358687000 seconds
    [Time delta from previous captured frame: 0.000113000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 5.823968000 seconds]
    Frame Number: 39
    Frame Length: 558 bytes (4464 bits)
    Capture Length: 558 bytes (4464 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
Ethernet II, Src: Apple_8d:db:36 (f4:d4:88:8d:db:36), Dst: Cisco_80:9b:df (6c:8b:d3:80:9b:df)
    Destination: Cisco_80:9b:df (6c:8b:d3:80:9b:df)
        Address: Cisco_80:9b:df (6c:8b:d3:80:9b:df)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source: Apple_8d:db:36 (f4:d4:88:8d:db:36)
        Address: Apple_8d:db:36 (f4:d4:88:8d:db:36)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 10.12.92.76, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        0000 00.. = Differentiated Services Codepoint: Default (0)
        .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 544
    Identification: 0x0000 (0)
    010. .... = Flags: 0x2, Don't fragment
        0... .... = Reserved bit: Not set
        .1.. .... = Don't fragment: Set
        ..0. .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0x5cfc [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.12.92.76
    Destination Address: 128.119.245.12
Transmission Control Protocol, Src Port: 57672, Dst Port: 80, Seq: 1, Ack: 1, Len: 504
    Source Port: 57672
    Destination Port: 80
    [Stream index: 9]
    [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 504]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 364782832
    [Next Sequence Number: 505    (relative sequence number)]
```

```
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 3714818623
    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: 4096
    [Calculated window size: 262144]
    [Window size scaling factor: 64]
    Checksum: 0x9eaa [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    [Timestamps]
        [Time since first frame in this TCP stream: 0.067714000 seconds]
        [Time since previous frame in this TCP stream: 0.000113000 seconds]
    [SEQ/ACK analysis]
        [iRTT: 0.067601000 seconds]
        [Bytes in flight: 504]
        [Bytes sent since last PSH flag: 504]
    TCP payload (504 bytes)
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
    If-None-Match: "51-605d8305477ae"\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: Thu, 21 Sep 2023 05:59:02 GMT\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like
Gecko) Version/16.6 Safari/605.1.15\r\n
    Accept-Language: en-CA,en-US;q=0.9,en;q=0.8\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: 41]
No.     Time                           Source                Destination           Length Protocol
Info
     41 2023-09-22 14:05:14.430055    128.119.245.12        10.12.92.76           492    HTTP
HTTP/1.1 200 OK  (text/html)
Frame 41: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface en0, id 0
    Section number: 1
    Interface id: 0 (en0)
        Interface name: en0
        Interface description: Wi-Fi
    Encapsulation type: Ethernet (1)
```

```
    Arrival Time: Sep 22, 2023 14:05:14.430055000 MDT
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1695413114.430055000 seconds
    [Time delta from previous captured frame: 0.000774000 seconds]
    [Time delta from previous displayed frame: 0.071368000 seconds]
    [Time since reference or first frame: 5.895336000 seconds]
    Frame Number: 41
    Frame Length: 492 bytes (3936 bits)
    Capture Length: 492 bytes (3936 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http:data-text-lines]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
Ethernet II, Src: Cisco_80:9b:df (6c:8b:d3:80:9b:df), Dst: Apple_8d:db:36 (f4:d4:88:8d:db:36)
    Destination: Apple_8d:db:36 (f4:d4:88:8d:db:36)
        Address: Apple_8d:db:36 (f4:d4:88:8d:db:36)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source: Cisco_80:9b:df (6c:8b:d3:80:9b:df)
        Address: Cisco_80:9b:df (6c:8b:d3:80:9b:df)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.12.92.76
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        0000 00.. = Differentiated Services Codepoint: Default (0)
        .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 478
    Identification: 0x072a (1834)
    010. .... = Flags: 0x2, Don't fragment
        0... .... = Reserved bit: Not set
        .1.. .... = Don't fragment: Set
        ..0. .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 32
    Protocol: TCP (6)
    Header Checksum: 0x7614 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 128.119.245.12
    Destination Address: 10.12.92.76
Transmission Control Protocol, Src Port: 80, Dst Port: 57672, Seq: 1, Ack: 505, Len: 438
    Source Port: 80
    Destination Port: 57672
    [Stream index: 9]
    [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 438]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 3714818623
    [Next Sequence Number: 439    (relative sequence number)]
    Acknowledgment Number: 505    (relative ack number)
    Acknowledgment number (raw): 364783336
    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: 237
    [Calculated window size: 30336]
    [Window size scaling factor: 128]
    Checksum: 0xbcfd [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    [Timestamps]
        [Time since first frame in this TCP stream: 0.139082000 seconds]
        [Time since previous frame in this TCP stream: 0.000774000 seconds]
    [SEQ/ACK analysis]
        [iRTT: 0.067601000 seconds]
        [Bytes in flight: 438]
        [Bytes sent since last PSH flag: 438]
    TCP payload (438 bytes)
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]
        Response Version: HTTP/1.1
        Status Code: 200
        [Status Code Description: OK]
        Response Phrase: OK
    Date: Fri, 22 Sep 2023 20:05:14 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: Fri, 22 Sep 2023 05:59:01 GMT\r\n
    ETag: "51-605ec4e276cfa"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 81\r\n
        [Content length: 81]
    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: 0.071368000 seconds]
    [Request in frame: 39]
    [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)
    <html>\n
    Congratulations!  You've downloaded the first Wireshark lab file!\n
    </html>\n
```