cs23mtech11026_Lab Assignment_1

1. Protocols in my trace file are
   TLSv1.2, TCP, ARP, DNS, MDNS, TLSv1.3, QUIC, HTTP, OCSP, ICMP

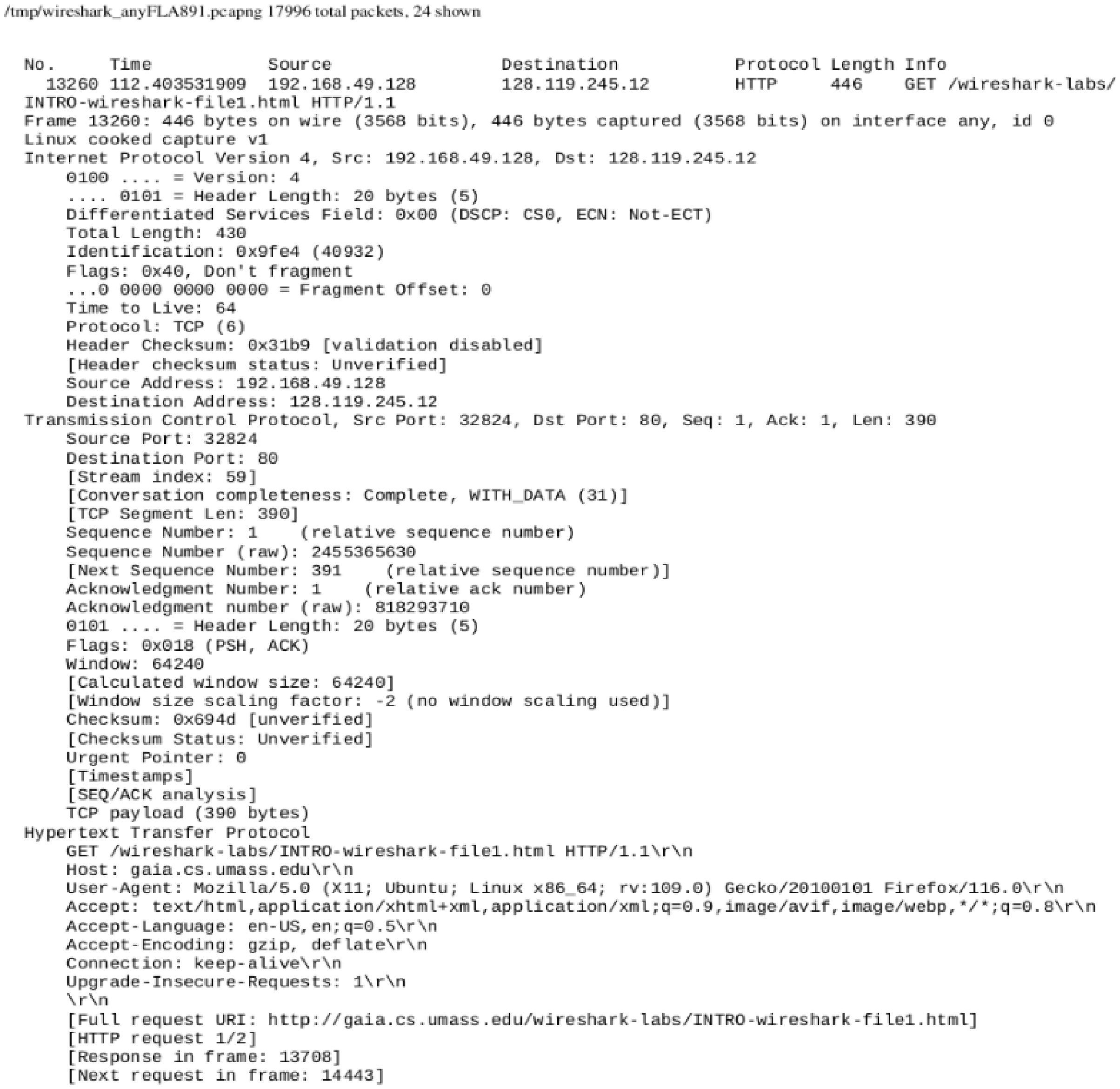
2. 0.337557078

3. Internet address of gaia.cs.umass.edu - 128.119.245.12
   Internet address of computer that sent HTTP GET - 192.168.49.128

4. Web browser issued - Mozilla/5.0

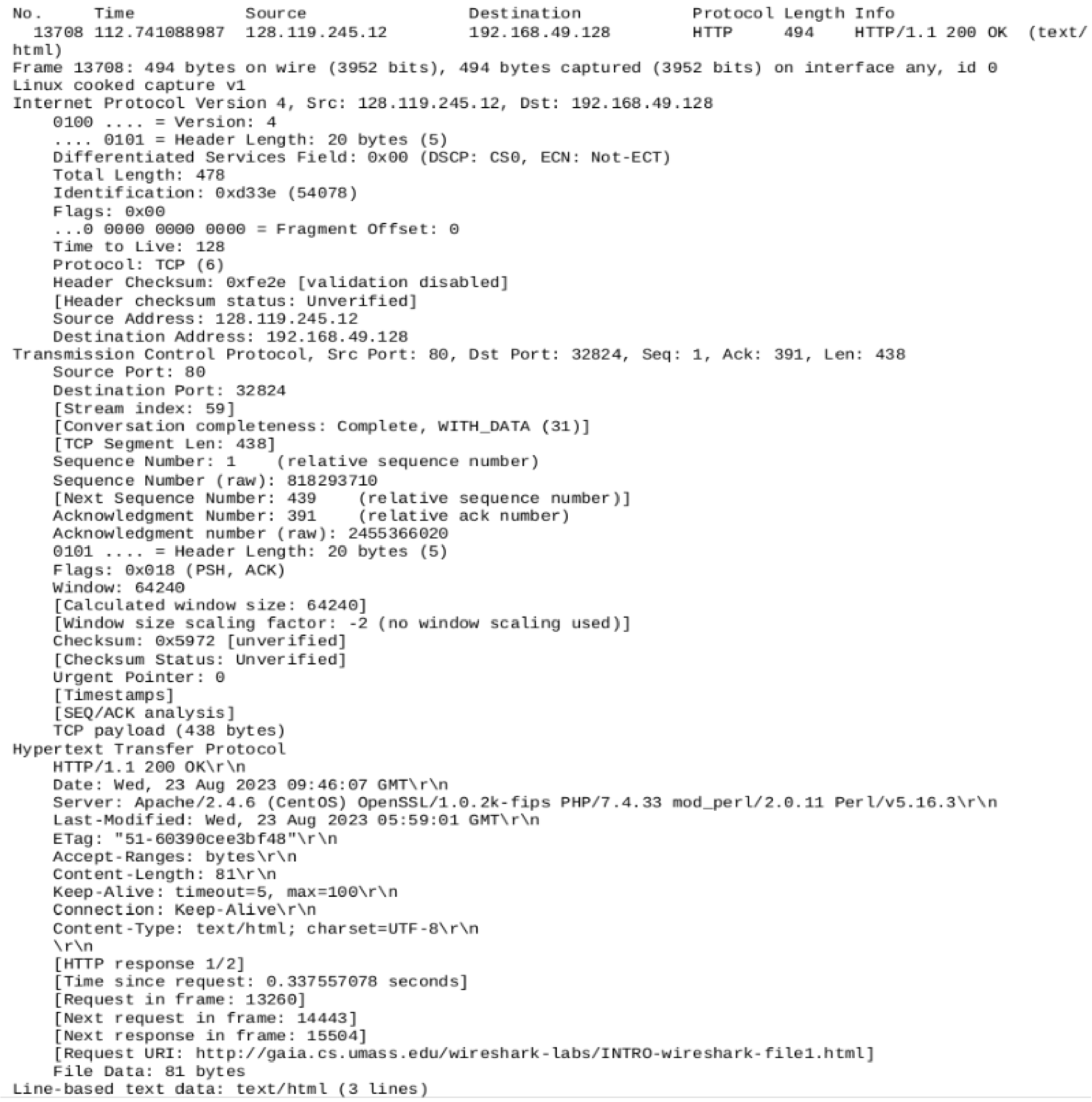
5. Destination port number - 80

6. The below given are the screenshots for GET and OK for gaia.cs.umass.edu



```
/tmp/wireshark_anyFLA891.pcapng 17996 total packets, 24 shown

No.     Time           Source                Destination           Protocol Length Info
  13260 112.403531909  192.168.49.128        128.119.245.12        HTTP     446    GET /wireshark-labs/
INTRO-wireshark-file1.html HTTP/1.1
Frame 13260: 446 bytes on wire (3568 bits), 446 bytes captured (3568 bits) on interface any, id 0
Linux cooked capture v1
Internet Protocol Version 4, Src: 192.168.49.128, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 430
    Identification: 0x9fe4 (40932)
    Flags: 0x40, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0x31b9 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.49.128
    Destination Address: 128.119.245.12
Transmission Control Protocol, Src Port: 32824, Dst Port: 80, Seq: 1, Ack: 1, Len: 390
    Source Port: 32824
    Destination Port: 80
    [Stream index: 59]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 390]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 2455365630
    [Next Sequence Number: 391    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 818293710
    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: 0x694d [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    [Timestamps]
    [SEQ/ACK analysis]
    TCP payload (390 bytes)
Hypertext Transfer Protocol
    GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/116.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;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
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
    [HTTP request 1/2]
    [Response in frame: 13708]
    [Next request in frame: 14443]
```



```
No.     Time           Source                Destination           Protocol Length Info
  13708 112.741088987  128.119.245.12        192.168.49.128        HTTP     494    HTTP/1.1 200 OK  (text/
html)
Frame 13708: 494 bytes on wire (3952 bits), 494 bytes captured (3952 bits) on interface any, id 0
Linux cooked capture v1
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.49.128
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 478
    Identification: 0xd33e (54078)
    Flags: 0x00
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: TCP (6)
    Header Checksum: 0xfe2e [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 128.119.245.12
    Destination Address: 192.168.49.128
Transmission Control Protocol, Src Port: 80, Dst Port: 32824, Seq: 1, Ack: 391, Len: 438
    Source Port: 80
    Destination Port: 32824
    [Stream index: 59]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 438]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 818293710
    [Next Sequence Number: 439    (relative sequence number)]
    Acknowledgment Number: 391    (relative ack number)
    Acknowledgment number (raw): 2455366020
    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: 0x5972 [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
    Date: Wed, 23 Aug 2023 09:46:07 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, 23 Aug 2023 05:59:01 GMT\r\n
    ETag: "51-60390cee3bf48"\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 1/2]
    [Time since request: 0.337557078 seconds]
    [Request in frame: 13260]
    [Next request in frame: 14443]
    [Next response in frame: 15504]
    [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)
```

7. The protocols observed in the below given traces in wireshark were same as observed in the test website which was gaia.cs.umass.edu.

   www.washington.edu/
   Protocols in my trace file are - TLSv1.2, TCP, ARP, DNS, MDNS, TLSv1.3, QUIC, HTTP, OCSP, ICMP
   Time - 0.419842172
   Internet address of www.washington.edu/ - 34.192.204.121
   Internet address of computer that sent HTTP - 192.168.49.128

example.com/
Protocols in my trace file are - TLSv1.2, TCP, ARP, DNS, MDNS, TLSv1.3, QUIC, HTTP, OCSP, ICMP
Time - 0.22316307
Internet address of example.com/ - 93.184.216.34
Internet address of computer that sent HTTP - 192.168.49.128

www.iith.ac.in
Protocols in my trace file are - TLSv1.2, TCP, ARP, DNS, MDNS, TLSv1.3, QUIC, HTTP, OCSP, ICMP
Time - 0.011335754
Internet address of example.com/ - 192.168.36.56
Internet address of computer that sent HTTP - 192.168.49.128

www.youtube.com
Protocols in my trace file are - TLSv1.2, TCP, ARP, DNS, MDNS, TLSv1.3, QUIC, HTTP, OCSP, ICMP
Time - 0.034106637
Internet address of www.youtube.com - 142.250.193.100
Internet address of computer that sent HTTP - 192.168.49.128

8. As I searched the domain name in the browser the GET request is sent to the server which we can see slightly on the search bar, But the actual internal process can be seen in the wireshark. In wireshark we can see all the protocols which are called in order to load the particular website which we have searched.

   We can also observe the time stamps for the GET and OK which is the get request for the website and the ok response of the website which is being loaded to the browser.

   Except for www.youtube.com all the other websites were running on the HTTP protocol whereas the youtube was running on QUIC protocol.