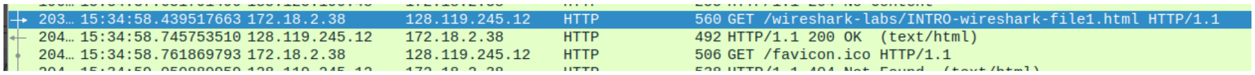
1)

ARP
UDP
MDNS
TCP
NBNS
LLC
ICMPv6
HTTP

2)



```
203… 15:34:58.439517663 172.18.2.38      128.119.245.12    HTTP        560 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
204… 15:34:58.745753510 128.119.245.12   172.18.2.38       HTTP        492 HTTP/1.1 200 OK  (text/html)
204… 15:34:58.761869793 172.18.2.38      128.119.245.12    HTTP        506 GET /favicon.ico HTTP/1.1
```

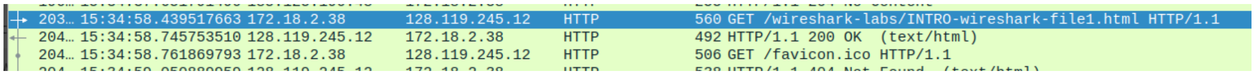
20395 15:34:58.439517663   172.18.2.38   128.119.245.12   HTTP   560   GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1

20413 15:34:58.745753510   128.119.245.12   172.18.2.38   HTTP   492   HTTP/1.1 200 OK (text/html)

OK -   15:34:58 745753510
GET -   15:34:58 439517663
—----------------------------------
SUBSTRACT - 00:00:00 306235847

Means 306 milliseconds 235 microseconds and 847 nanoseconds

3)

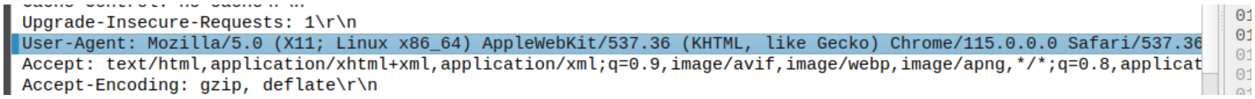


```
203… 15:34:58.439517663 172.18.2.38      128.119.245.12    HTTP        560 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
204… 15:34:58.745753510 128.119.245.12   172.18.2.38       HTTP        492 HTTP/1.1 200 OK  (text/html)
204… 15:34:58.761869793 172.18.2.38      128.119.245.12    HTTP        506 GET /favicon.ico HTTP/1.1
```

20395 15:34:58.439517663   172.18.2.38   128.119.245.12   HTTP 560   GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1

Internet address of the gaia.cs.umass.edu is 128.119.245.12
Internet address of my computer 172.18.2.38

4)

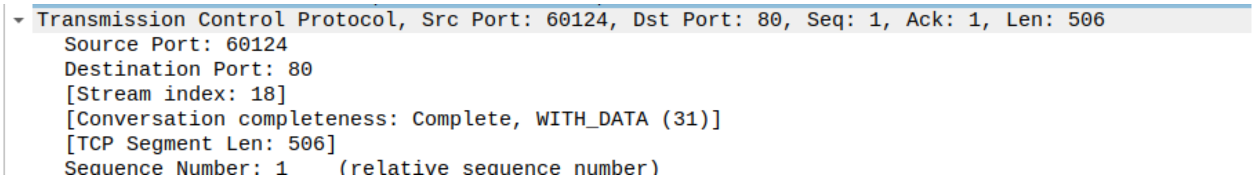


```
Cache-Control: no-cache\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,applicat
Accept-Encoding: gzip, deflate\r\n
```

User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.0.0 Safari/537.36\r\n

5)

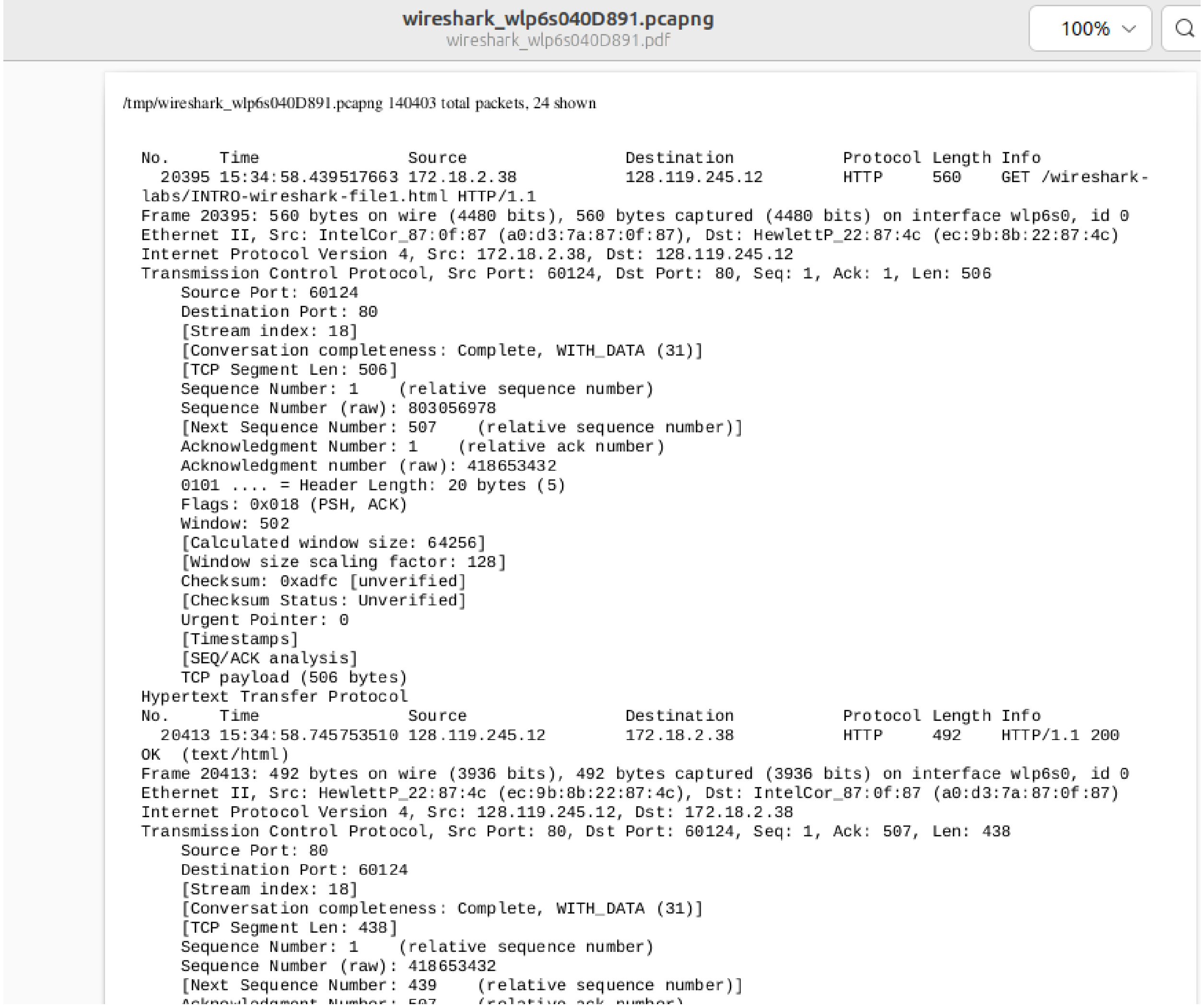
Dest port : 80



```
▾ Transmission Control Protocol, Src Port: 60124, Dst Port: 80, Seq: 1, Ack: 1, Len: 506
    Source Port: 60124
    Destination Port: 80
    [Stream index: 18]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 506]
    Sequence Number: 1    (relative sequence number)
```

6)

Given below is the printed file:



/tmp/wireshark_wlp6s040D891.pcapng 140403 total packets, 24 shown

```
No.     Time               Source                Destination           Protocol Length Info
  20395 15:34:58.439517663 172.18.2.38           128.119.245.12        HTTP     560    GET /wireshark-
labs/INTRO-wireshark-file1.html HTTP/1.1
Frame 20395: 560 bytes on wire (4480 bits), 560 bytes captured (4480 bits) on interface wlp6s0, id 0
Ethernet II, Src: IntelCor_87:0f:87 (a0:d3:7a:87:0f:87), Dst: HewlettP_22:87:4c (ec:9b:8b:22:87:4c)
Internet Protocol Version 4, Src: 172.18.2.38, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 60124, Dst Port: 80, Seq: 1, Ack: 1, Len: 506
    Source Port: 60124
    Destination Port: 80
    [Stream index: 18]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 506]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 803056978
    [Next Sequence Number: 507    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 418653432
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
    Window: 502
    [Calculated window size: 64256]
    [Window size scaling factor: 128]
    Checksum: 0xadfc [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    [Timestamps]
    [SEQ/ACK analysis]
    TCP payload (506 bytes)
Hypertext Transfer Protocol
No.     Time               Source                Destination           Protocol Length Info
  20413 15:34:58.745753510 128.119.245.12        172.18.2.38           HTTP     492    HTTP/1.1 200
OK  (text/html)
Frame 20413: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface wlp6s0, id 0
Ethernet II, Src: HewlettP_22:87:4c (ec:9b:8b:22:87:4c), Dst: IntelCor_87:0f:87 (a0:d3:7a:87:0f:87)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 172.18.2.38
Transmission Control Protocol, Src Port: 80, Dst Port: 60124, Seq: 1, Ack: 507, Len: 438
    Source Port: 80
    Destination Port: 60124
    [Stream index: 18]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 438]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 418653432
    [Next Sequence Number: 439    (relative sequence number)]
    Acknowledgment Number: 507    (relative ack number)
```

7)

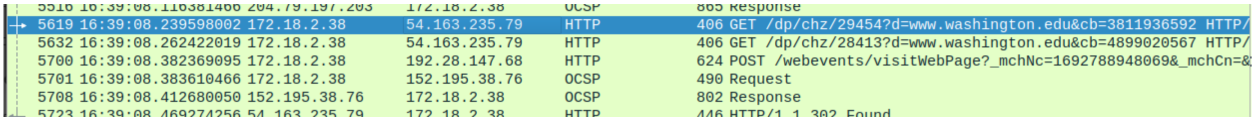
washington.edu/

Visible protocols:

ARP
UDP
MDNS
TCP
ICMPv6
HTTP
TLSv1.3
DNS

OSCP

Time calculation:



```
5516 16:39:08.116381466 204.79.197.203 172.18.2.38    OCSP 865 Response
5619 16:39:08.239598002 172.18.2.38    54.163.235.79  HTTP 406 GET /dp/chz/29454?d=www.washington.edu&cb=3811936592 HTTP/
5632 16:39:08.262422019 172.18.2.38    54.163.235.79  HTTP 406 GET /dp/chz/28413?d=www.washington.edu&cb=4899020567 HTTP/
5700 16:39:08.382369095 172.18.2.38    192.28.147.68  HTTP 624 POST /webevents/visitWebPage?_mchNc=1692788948069&_mchCn=&
5701 16:39:08.383610466 172.18.2.38    152.195.38.76  OCSP 490 Request
5708 16:39:08.412680050 152.195.38.76  172.18.2.38    OCSP 802 Response
5723 16:39:08.469274256 54.163.235.79  172.18.2.38    HTTP 446 HTTP/1.1 302 Found
```

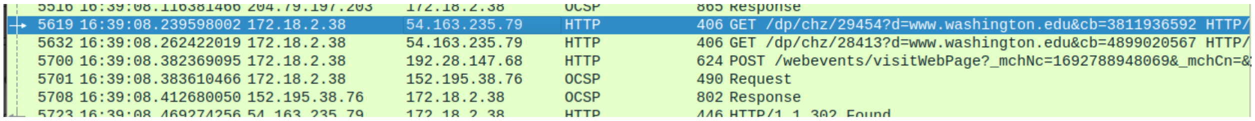
5619 16:39:08.239598002 172.18.2.38 54.163.235.79 HTTP 406 GET /dp/chz/29454?d=www.washington.edu&cb=3811936592 HTTP/1.1

5723 16:39:08.469274256 54.163.235.79 172.18.2.38 HTTP 446 HTTP/1.1 302 Found

OK - 16:39:08.469274256
GET - 16:39:08.239598002
—-----------------------------------
SUBSTRACT - 00:00:00 219676254

Means 219 milliseconds 676 microseconds and 254 nanoseconds

IP address:



```
5516 16:39:08.116381466 204.79.197.203 172.18.2.38    OCSP 865 Response
5619 16:39:08.239598002 172.18.2.38    54.163.235.79  HTTP 406 GET /dp/chz/29454?d=www.washington.edu&cb=3811936592 HTTP/
5632 16:39:08.262422019 172.18.2.38    54.163.235.79  HTTP 406 GET /dp/chz/28413?d=www.washington.edu&cb=4899020567 HTTP/
5700 16:39:08.382369095 172.18.2.38    192.28.147.68  HTTP 624 POST /webevents/visitWebPage?_mchNc=1692788948069&_mchCn=&
5701 16:39:08.383610466 172.18.2.38    152.195.38.76  OCSP 490 Request
5708 16:39:08.412680050 152.195.38.76  172.18.2.38    OCSP 802 Response
5723 16:39:08.469274256 54.163.235.79  172.18.2.38    HTTP 446 HTTP/1.1 302 Found
```

Internet address of the washington.edu is 54.163.235.79
Internet address of my computer 172.18.2.38

example.com

Visible protocols:

ARP
UDP
MDNS
TCP
ICMPv6
HTTP

TLSv1.3
DNS
OSCP

Time calculation:

```
311     17:09:40.694781632          172.18.2.38   93.184.216.34         HTTP  525     GET /
HTTP/1.1

319     17:09:40.912375485          93.184.216.34         172.18.2.38   HTTP  1088
HTTP/1.1 200 OK  (text/html)
```

OK -   17:09:40.912375485
GET -   17:09:40.694781632
—-----------------------------------
SUBSTRACT - 00:00:00 317593853

Means 317 milliseconds 593 microseconds and 853 nanoseconds

IP address:

```
311     17:09:40.694781632          172.18.2.38   93.184.216.34         HTTP  525     GET /
HTTP/1.1

319     17:09:40.912375485          93.184.216.34         172.18.2.38   HTTP  1088
HTTP/1.1 200 OK  (text/html)
```

Internet address of the example.com is 93.184.216.34
Internet address of my computer 172.18.2.38

Iith.ac.in

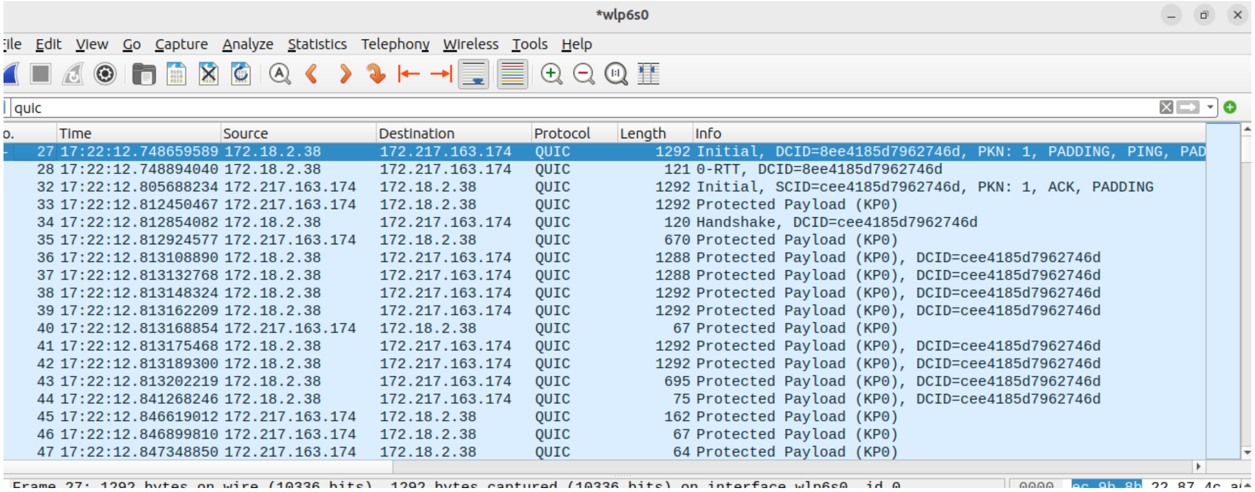
This website by default uses https and due to which it is not able to see packets.
Tried to use http but the browser is not supported.

youtube.com

Visible protocols:

ARP
UDP
MDNS
TCP
ICMPv6
HTTP
QUIC
TLSv1.3
DNS
OSCP

Time calculation:


*wlp6s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
quic
o.   Time               Source          Destination     Protocol Length Info
  27 17:22:12.748659589 172.18.2.38     172.217.163.174 QUIC       1292 Initial, DCID=8ee4185d7962746d, PKN: 1, PADDING, PING, PAD
  28 17:22:12.748894040 172.18.2.38     172.217.163.174 QUIC        121 0-RTT, DCID=8ee4185d7962746d
  32 17:22:12.805688234 172.217.163.174 172.18.2.38     QUIC       1292 Initial, SCID=cee4185d7962746d, PKN: 1, ACK, PADDING
  33 17:22:12.812450467 172.217.163.174 172.18.2.38     QUIC       1292 Protected Payload (KP0)
  34 17:22:12.812854082 172.18.2.38     172.217.163.174 QUIC        120 Handshake, DCID=cee4185d7962746d
  35 17:22:12.812924577 172.217.163.174 172.18.2.38     QUIC        670 Protected Payload (KP0)
  36 17:22:12.813108890 172.18.2.38     172.217.163.174 QUIC       1288 Protected Payload (KP0), DCID=cee4185d7962746d
  37 17:22:12.813132768 172.18.2.38     172.217.163.174 QUIC       1288 Protected Payload (KP0), DCID=cee4185d7962746d
  38 17:22:12.813148324 172.18.2.38     172.217.163.174 QUIC       1292 Protected Payload (KP0), DCID=cee4185d7962746d
  39 17:22:12.813162209 172.18.2.38     172.217.163.174 QUIC       1292 Protected Payload (KP0), DCID=cee4185d7962746d
  40 17:22:12.813168854 172.217.163.174 172.18.2.38     QUIC         67 Protected Payload (KP0)
  41 17:22:12.813175468 172.18.2.38     172.217.163.174 QUIC       1292 Protected Payload (KP0), DCID=cee4185d7962746d
  42 17:22:12.813189300 172.18.2.38     172.217.163.174 QUIC       1292 Protected Payload (KP0), DCID=cee4185d7962746d
  43 17:22:12.813202219 172.18.2.38     172.217.163.174 QUIC        695 Protected Payload (KP0), DCID=cee4185d7962746d
  44 17:22:12.841268246 172.18.2.38     172.217.163.174 QUIC         75 Protected Payload (KP0), DCID=cee4185d7962746d
  45 17:22:12.846619012 172.217.163.174 172.18.2.38     QUIC        162 Protected Payload (KP0)
  46 17:22:12.846899810 172.217.163.174 172.18.2.38     QUIC         67 Protected Payload (KP0)
  47 17:22:12.847348850 172.217.163.174 172.18.2.38     QUIC         64 Protected Payload (KP0)
Frame 27: 1292 bytes on wire (10336 bits), 1292 bytes captured (10336 bits) on interface wlp6s0, id 0    0000  ec 9b 8b 22 87 4c a
```

Not able to calculate time as the details of the QUIC protocol is not known to me at this point of time due to which the response request is not visible.

Internet address of the youtube is 172.217.163.174
Internet address of my computer 172.18.2.38

8)

http://www.washington.edu/ can be tracked over the wireshark, but It is found that two get and ok responses are visible in wireshark for a single request from the browser(the same is verified multiple times). Also, the domain name is easily visible in the wireshark.

Its packet are completely different in terms of number of get and ok response and also in terms of domain name.
http://example.com/ can be tracked from the wireshark using the destination ip (looking from lookup website)
https://www.iith.ac.in/ is uses secure protocol https and also when tried to use http the it uses its default https.

https://www.youtube.com/ is using the QUIC protocol of the internet and also when tried to use http the it uses its default https.