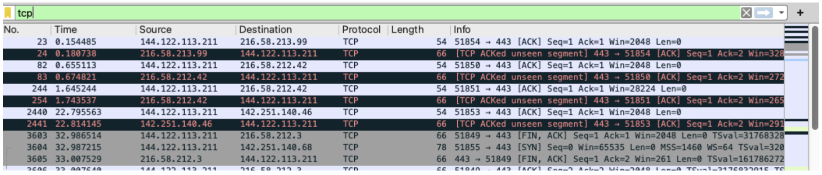
Derya Tınmaz - 2380947

Wireshark Lab: Getting Started v8.1

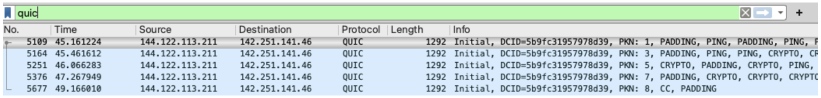
1.

TCP:



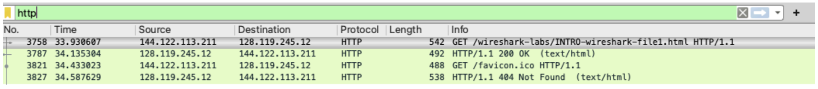
```
tcp
No.   Time        Source           Destination      Protocol Length Info
  23  0.154485    144.122.113.211  216.58.213.99    TCP        54  51854 → 443 [ACK] Seq=1 Ack=1 Win=2048 Len=0
  24  0.180738    216.58.213.99    144.122.113.211  TCP        66  [TCP ACKed unseen segment] 443 → 51854 [ACK] Seq=1 Ack=2 Win=328
  82  0.655113    144.122.113.211  216.58.212.42    TCP        54  51850 → 443 [ACK] Seq=1 Ack=1 Win=2048 Len=0
  83  0.674821    216.58.212.42    144.122.113.211  TCP        66  [TCP ACKed unseen segment] 443 → 51850 [ACK] Seq=1 Ack=2 Win=272
 244  1.645244    144.122.113.211  216.58.212.42    TCP        54  51851 → 443 [ACK] Seq=1 Ack=1 Win=28224 Len=0
 254  1.743537    216.58.212.42    144.122.113.211  TCP        66  [TCP ACKed unseen segment] 443 → 51851 [ACK] Seq=1 Ack=2 Win=265
2440  22.795563   144.122.113.211  142.251.140.46   TCP        54  51853 → 443 [ACK] Seq=1 Ack=1 Win=2048 Len=0
2441  22.814145   142.251.140.46   144.122.113.211  TCP        66  [TCP ACKed unseen segment] 443 → 51853 [ACK] Seq=1 Ack=2 Win=291
3603  32.986514   144.122.113.211  216.58.212.3     TCP        66  51849 → 443 [FIN, ACK] Seq=1 Ack=1 Win=2048 Len=0 TSval=31768328
3604  32.987215   144.122.113.211  142.251.140.68   TCP        78  51855 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=320
3605  33.007529   216.58.212.3     144.122.113.211  TCP        66  443 → 51849 [FIN, ACK] Seq=1 Ack=2 Win=261 Len=0 TSval=161786272
```

QUIC:



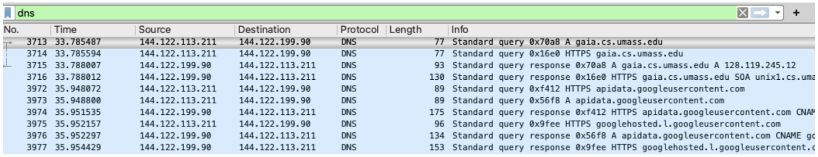
```
quic
No.   Time        Source           Destination      Protocol Length Info
5109  45.161224   144.122.113.211  142.251.141.46   QUIC     1292  Initial, DCID=5b9fc31957978d39, PKN: 1, PADDING, PING, PADDING, PING, P
5164  45.461612   144.122.113.211  142.251.141.46   QUIC     1292  Initial, DCID=5b9fc31957978d39, PKN: 3, PADDING, PING, PING, CRYPTO, CR
5251  46.066283   144.122.113.211  142.251.141.46   QUIC     1292  Initial, DCID=5b9fc31957978d39, PKN: 5, CRYPTO, PADDING, CRYPTO, PING,
5376  47.267949   144.122.113.211  142.251.141.46   QUIC     1292  Initial, DCID=5b9fc31957978d39, PKN: 7, PADDING, CRYPTO, CRYPTO, CRYPTC
5677  49.166010   144.122.113.211  142.251.141.46   QUIC     1292  Initial, DCID=5b9fc31957978d39, PKN: 8, CC, PADDING
```

HTTP:



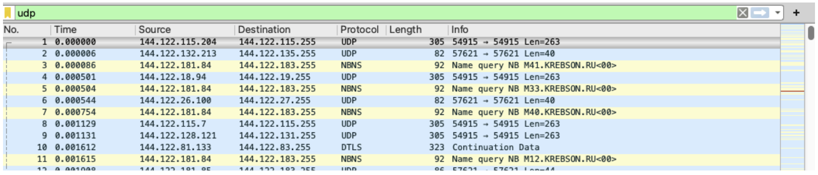
```
http
No.   Time        Source           Destination      Protocol Length Info
3758  33.930607   144.122.113.211  128.119.245.12   HTTP      542  GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
3787  34.135304   128.119.245.12   144.122.113.211  HTTP      492  HTTP/1.1 200 OK  (text/html)
3821  34.433023   144.122.113.211  128.119.245.12   HTTP      488  GET /favicon.ico HTTP/1.1
3827  34.587629   128.119.245.12   144.122.113.211  HTTP      538  HTTP/1.1 404 Not Found  (text/html)
```

DNS:



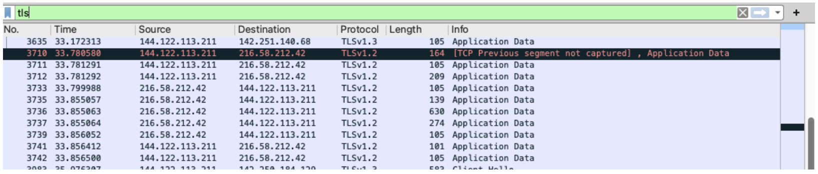
```
dns
No.   Time        Source           Destination      Protocol Length Info
3713  33.785487   144.122.113.211  144.122.199.90   DNS        77  Standard query 0x70a8 A gaia.cs.umass.edu
3714  33.785594   144.122.113.211  144.122.199.90   DNS        77  Standard query 0x16e0 HTTPS gaia.cs.umass.edu
3715  33.788007   144.122.199.90   144.122.113.211  DNS        93  Standard query response 0x70a8 A gaia.cs.umass.edu A 128.119.245.12
3716  33.788012   144.122.199.90   144.122.113.211  DNS       130  Standard query response 0x16e0 HTTPS gaia.cs.umass.edu SOA unix1.cs.uma
3972  35.948072   144.122.113.211  144.122.199.90   DNS        89  Standard query 0xf412 HTTPS apidata.googleusercontent.com
3973  35.948800   144.122.113.211  144.122.199.90   DNS        89  Standard query 0x56f8 A apidata.googleusercontent.com
3974  35.951535   144.122.199.90   144.122.113.211  DNS       175  Standard query response 0xf412 HTTPS apidata.googleusercontent.com CNAM
3975  35.952157   144.122.113.211  144.122.199.90   DNS        96  Standard query 0x9fee HTTPS googlehosted.l.googleusercontent.com
3976  35.952297   144.122.199.90   144.122.113.211  DNS       134  Standard query response 0x56f8 A apidata.googleusercontent.com CNAME gc
3977  35.954429   144.122.199.90   144.122.113.211  DNS       153  Standard query response 0x9fee HTTPS googlehosted.l.googleusercontent.c
```

UDP:



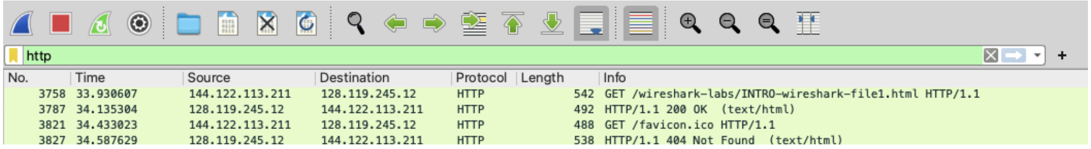
```
udp
No.   Time        Source           Destination      Protocol Length Info
   1  0.000000    144.122.115.204  144.122.115.255  UDP       305  54915 → 54915 Len=263
   2  0.000006    144.122.132.213  144.122.135.255  UDP        82  57621 → 57621 Len=40
   3  0.000086    144.122.181.84   144.122.183.255  NBNS       92  Name query NB M41.KREBSON.RU<00>
   4  0.000501    144.122.18.94    144.122.19.255   UDP       305  54915 → 54915 Len=263
   5  0.000504    144.122.181.84   144.122.183.255  NBNS       92  Name query NB M33.KREBSON.RU<00>
   6  0.000544    144.122.26.100   144.122.27.255   UDP        82  57621 → 57621 Len=40
   7  0.000754    144.122.181.84   144.122.183.255  NBNS       92  Name query NB M40.KREBSON.RU<00>
   8  0.001129    144.122.115.7    144.122.115.255  UDP       305  54915 → 54915 Len=263
   9  0.001131    144.122.128.121  144.122.131.255  UDP       305  54915 → 54915 Len=263
  10  0.001612    144.122.81.133   144.122.83.255   DTLS      323  Continuation Data
  11  0.001615    144.122.181.84   144.122.183.255  NBNS       92  Name query NB M12.KREBSON.RU<00>
```

TLSv1.2 :



```
tls
No.   Time        Source           Destination      Protocol Length Info
3635  33.172313   144.122.113.211  142.251.140.68   TLSv1.3   105  Application Data
3710  33.780580   144.122.113.211  216.58.212.42    TLSv1.2   164  [TCP Previous segment not captured] , Application Data
3711  33.781291   144.122.113.211  216.58.212.42    TLSv1.2   105  Application Data
3712  33.781292   144.122.113.211  216.58.212.42    TLSv1.2   209  Application Data
3733  33.799988   216.58.212.42    144.122.113.211  TLSv1.2   105  Application Data
3735  33.855057   216.58.212.42    144.122.113.211  TLSv1.2   139  Application Data
3736  33.855063   216.58.212.42    144.122.113.211  TLSv1.2   630  Application Data
3737  33.855064   216.58.212.42    144.122.113.211  TLSv1.2   274  Application Data
3739  33.856052   216.58.212.42    144.122.113.211  TLSv1.2   105  Application Data
3741  33.856412   144.122.113.211  216.58.212.42    TLSv1.2   101  Application Data
3742  33.856500   144.122.113.211  216.58.212.42    TLSv1.2   105  Application Data
```

2.

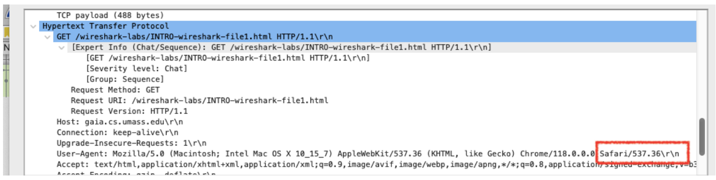


```
http
No.   Time        Source           Destination      Protocol Length Info
3758  33.930607   144.122.113.211  128.119.245.12   HTTP      542  GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
3787  34.135304   128.119.245.12   144.122.113.211  HTTP      492  HTTP/1.1 200 OK  (text/html)
3821  34.433023   144.122.113.211  128.119.245.12   HTTP      488  GET /favicon.ico HTTP/1.1
3827  34.587629   128.119.245.12   144.122.113.211  HTTP      538  HTTP/1.1 404 Not Found  (text/html)
```

34.135304-33.930607 = 0.204697 -> 0.205

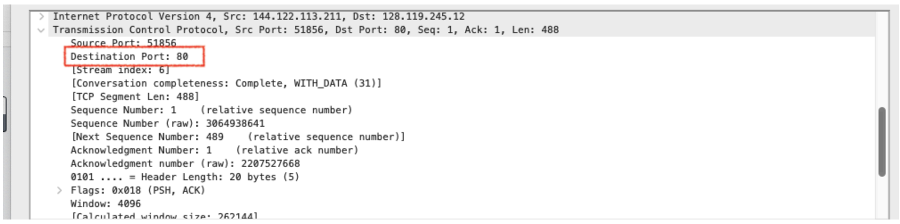
3. gaia.cs.umass.edu 's internet adres is the destination address in previous screen shot's first packet: 128.119.245.12, the internet address of my computer is the source address: 144.122.113.211

4.



```
    TCP payload (488 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
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.0.0 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
```

5.



```
> Internet Protocol Version 4, Src: 144.122.113.211, Dst: 128.119.245.12
v Transmission Control Protocol, Src Port: 51856, Dst Port: 80, Seq: 1, Ack: 1, Len: 488
    Source Port: 51856
    Destination Port: 80
    [Stream index: 6]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 488]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 3064938641
    [Next Sequence Number: 489    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 2207527668
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window: 4096
    [Calculated window size: 262144]
```