19CSE301 - COMPUTER NETWORKS

LAB PRACTICE - WIRESHARK

- R.Abhinav
- CB.EN.U4CSE19453

1. List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.

   STUN,UDP, TLS,TCP(TLSV1.2, TLSV1.3)

1427…	417.719905	52.113.92.3	192.168.0.3	STUN	114	Binding Success Response XOR-MAPPED-ADDRESS: 103.105.103.13:50027
1427…	417.720140	213.179.210.198	192.168.0.3	UDP	243	50002 → 60058 Len=201
1427…	417.720274	52.113.92.3	192.168.0.3	UDP	182	3479 → 50002 Len=140
1427…	417.720942	192.168.0.3	213.179.210.198	UDP	250	60058 → 50002 Len=208
1427…	417.726231	162.159.130.234	192.168.0.3	TLSv1.3	188	Application Data
1427…	417.726435	192.168.0.3	162.159.130.234	TCP	54	60604 → 443 [ACK] Seq=3146 Ack=332849 Win=131072 Len=0
1427…	417.728517	162.159.130.234	192.168.0.3	TLSv1.3	598	Application Data
1427…	417.739950	52.113.92.3	192.168.0.3	STUN	114	Binding Success Response XOR-MAPPED-ADDRESS: 103.105.103.13:50057
1427…	417.739950	52.113.92.3	192.168.0.3	UDP	178	3479 → 50002 Len=136
1427…	417.740205	213.179.210.198	192.168.0.3	UDP	236	50002 → 60058 Len=194
1427…	417.747632	192.168.0.3	213.179.210.198	UDP	233	60058 → 50002 Len=191
1427…	417.750950	213.179.210.198	192.168.0.3	UDP	233	50002 → 60058 Len=191

2. 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. 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.)

   Difference = 0.029049s
   The time interval in the range of 0.015 ~ 0.040 will be accepted.

684	16.229787	192.168.0.3	104.18.21.226	HTTP	265	GET /root-r2.crl HTTP/1.1
666	16.121229	182.18.179.90	192.168.0.3	HTTP	322	HTTP/1.1 304 Not Modified

3. **What is the Internet address of the vidya.ettimadai.net? What is the Internet address of your computer? Where did you find this information in Wireshark?**

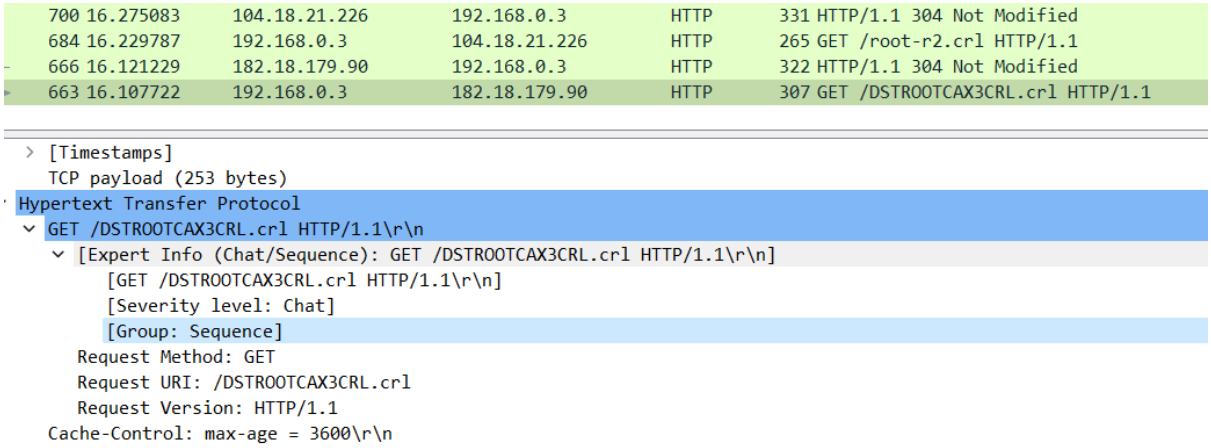
   vidya.ettimadai.net : 182.18.179.90
   My computer : 192.168.0.3

4. **For the HTTP page request from your computer to the vidya server, what was the source port and what was the destination port?**

   Destination port : 182.18.179.90
   source port : 192.168.0.3

5. **Print the two HTTP messages (GET and OK) referred to in question 2 above. To do so, select Print from the Wireshark File command menu, and select the "Selected Packet Only" and "Print as displayed" radial buttons, and then click OK.**

   GET :



OK:

```
    684 16.229787    192.168.0.3      104.18.21.226    HTTP    265 GET /root-r2.crl HTTP/1.1
    666 16.121229    182.18.179.90    192.168.0.3      HTTP    322 HTTP/1.1 304 Not Modified
    663 16.107722    192.168.0.3      182.18.179.90    HTTP    307 GET /DSTROOTCAX3CRL.crl HTTP/1.1
```

```
  > [Timestamps]
    TCP payload (253 bytes)
Hypertext Transfer Protocol
  > GET /DSTROOTCAX3CRL.crl HTTP/1.1\r\n
    Cache-Control: max-age = 3600\r\n
    Connection: Keep-Alive\r\n
    Accept: */*\r\n
    If-Modified-Since: Wed, 21 Jul 2021 19:43:29 GMT\r\n
    If-None-Match: "4a6-5c7a76279951d"\r\n
    User-Agent: Microsoft-CryptoAPI/10.0\r\n
    Host: crl.identrust.com\r\n
    \r\n
```

6. Record the number of packets that has been observed by your interface this far.

```
Packets: 142820 · Displayed: 84 (0.1%) · Dropped: 0 (0.0%)
```

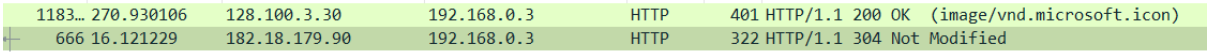
7. What is the version of HTTP that is running on the browser? What HTTP version is running on the server?

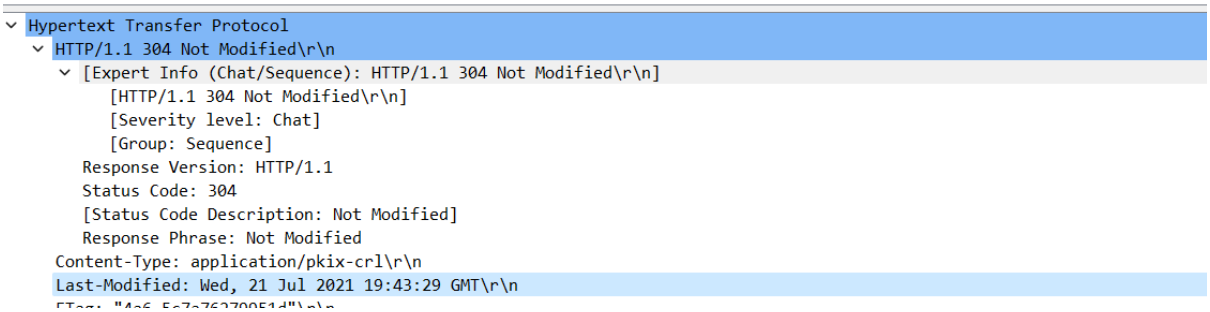
   Version : 1.1

```
    700 16.275083    104.18.21.226    192.168.0.3      HTTP    331 HTTP/1.1 304 Not Modified
    684 16.229787    192.168.0.3      104.18.21.226    HTTP    265 GET /root-r2.crl HTTP/1.1
    666 16.121229    182.18.179.90    192.168.0.3      HTTP    322 HTTP/1.1 304 Not Modified
    663 16.107722    192.168.0.3      182.18.179.90    HTTP    307 GET /DSTROOTCAX3CRL.crl HTTP/1.1
```

```
  > [Timestamps]
    TCP payload (253 bytes)
Hypertext Transfer Protocol
  v GET /DSTROOTCAX3CRL.crl HTTP/1.1\r\n
    v [Expert Info (Chat/Sequence): GET /DSTROOTCAX3CRL.crl HTTP/1.1\r\n]
        [GET /DSTROOTCAX3CRL.crl HTTP/1.1\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Request Method: GET
      Request URI: /DSTROOTCAX3CRL.crl
      Request Version: HTTP/1.1
    Cache-Control: max-age = 3600\r\n
```

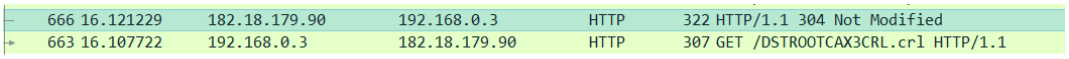
8. When was the HTML file that you were retrieving last modified by the server?

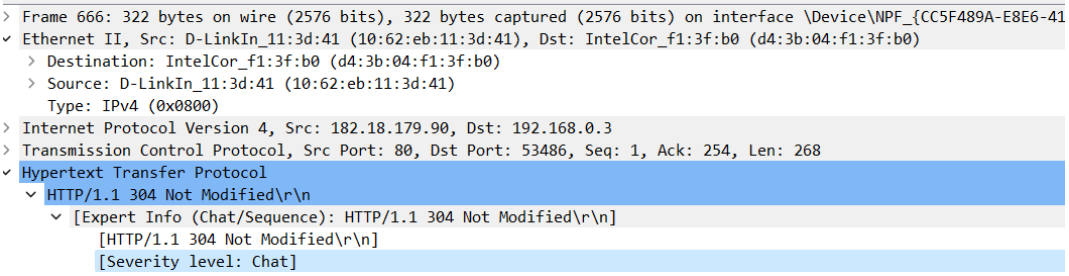




9. Use Wireshark to capture HTTP packets while loading the following URL

   vidya.ettimadai.net:





10. How many GET requests did your browser send?

    Count : 3