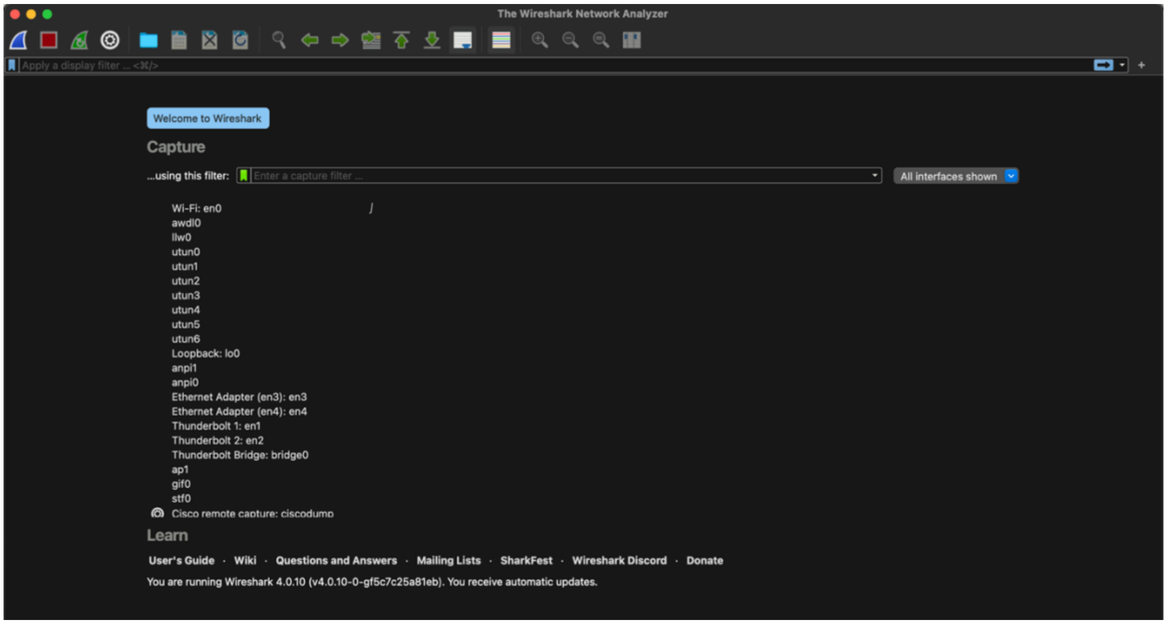
Suyog Joshi
Assignment 2
21/10/2023
Computer Networks

Question 1)



The Wireshark Network Analyzer

Apply a display filter ... <⌘/>

Welcome to Wireshark

Capture

...using this filter: Enter a capture filter ... All interfaces shown

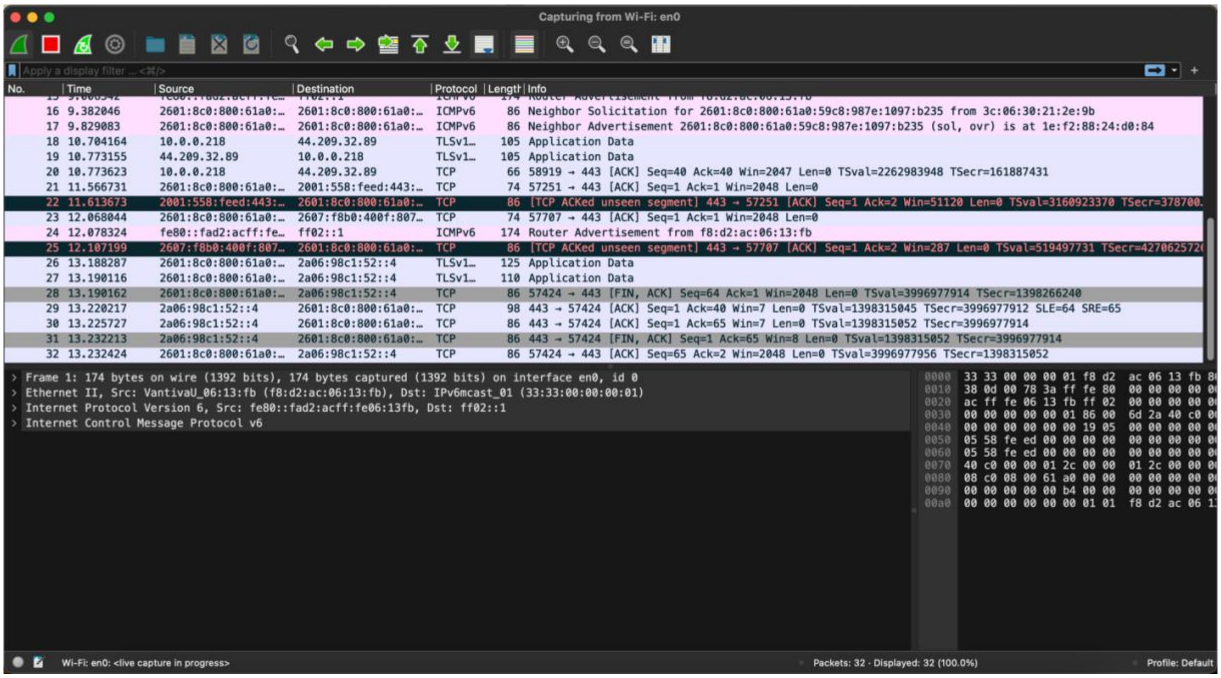
Wi-Fi: en0
awdl0
llw0
utun0
utun1
utun2
utun3
utun4
utun5
utun6
Loopback: lo0
anpi1
anpi0
Ethernet Adapter (en3): en3
Ethernet Adapter (en4): en4
Thunderbolt 1: en1
Thunderbolt 2: en2
Thunderbolt Bridge: bridge0
ap1
gif0
stf0
Cisco remote capture: ciscodump

Learn

User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate

You are running Wireshark 4.0.10 (v4.0.10-0-gf5c7c25a81eb). You receive automatic updates.

Question 2)



Capturing from Wi-Fi: en0

Apply a display filter ... <⌘/>

```
No.  Time       Source                Destination           Protocol Length Info
  16 9.382046   2601:8c0:800:61a0:…   2601:8c0:800:61a0:…   ICMPv6    86 Neighbor Solicitation for 2601:8c0:800:61a0:59c8:987e:1097:b235 from 3c:06:30:21:2e:9b
  17 9.829083   2601:8c0:800:61a0:…   2601:8c0:800:61a0:…   ICMPv6    86 Neighbor Advertisement 2601:8c0:800:61a0:59c8:987e:1097:b235 (sol, ovr) is at 1e:f2:88:24:d0:84
  18 10.704164  10.0.0.218            44.209.32.89          TLSv1…   105 Application Data
  19 10.773155  44.209.32.89          10.0.0.218            TLSv1…   105 Application Data
  20 10.773623  10.0.0.218            44.209.32.89          TCP       66 58919 → 443 [ACK] Seq=40 Ack=40 Win=2047 Len=0 TSval=2262983948 TSecr=161887431
  21 11.566731  2601:8c0:800:61a0:…   2001:558:feed:443:…   TCP       74 57251 → 443 [ACK] Seq=1 Ack=1 Win=2048 Len=0
  22 11.613673  2001:558:feed:443:…   2601:8c0:800:61a0:…   TCP       86 [TCP ACKed unseen segment] 443 → 57251 [ACK] Seq=1 Ack=2 Win=51120 Len=0 TSval=3160923370 TSecr=378700…
  23 12.068044  2601:8c0:800:61a0:…   2607:f8b0:400f:807…   TCP       74 57707 → 443 [ACK] Seq=1 Ack=1 Win=2048 Len=0
  24 12.078324  fe80::fad2:acff:fe…   ff02::1               ICMPv6   174 Router Advertisement from f8:d2:ac:06:13:fb
  25 12.107199  2607:f8b0:400f:807…   2601:8c0:800:61a0:…   TCP       86 [TCP ACKed unseen segment] 443 → 57707 [ACK] Seq=1 Ack=2 Win=287 Len=0 TSval=519497731 TSecr=427062572
  26 13.188287  2601:8c0:800:61a0:…   2a06:98c1:52::4       TLSv1…   125 Application Data
  27 13.190116  2601:8c0:800:61a0:…   2a06:98c1:52::4       TLSv1…   110 Application Data
  28 13.190162  2601:8c0:800:61a0:…   2a06:98c1:52::4       TCP       86 57424 → 443 [FIN, ACK] Seq=64 Ack=1 Win=2048 Len=0 TSval=3996977914 TSecr=1398266240
  29 13.220217  2a06:98c1:52::4       2601:8c0:800:61a0:…   TCP       98 443 → 57424 [ACK] Seq=1 Ack=40 Win=7 Len=0 TSval=1398315045 TSecr=3996977912 SLE=64 SRE=65
  30 13.225727  2a06:98c1:52::4       2601:8c0:800:61a0:…   TCP       86 443 → 57424 [ACK] Seq=1 Ack=65 Win=7 Len=0 TSval=1398315052 TSecr=3996977914
  31 13.232213  2a06:98c1:52::4       2601:8c0:800:61a0:…   TCP       86 443 → 57424 [FIN, ACK] Seq=1 Ack=65 Win=8 Len=0 TSval=1398315052 TSecr=3996977914
  32 13.232424  2601:8c0:800:61a0:…   2a06:98c1:52::4       TCP       86 57424 → 443 [ACK] Seq=65 Ack=2 Win=2048 Len=0 TSval=3996977956 TSecr=1398315052
```

```
> Frame 1: 174 bytes on wire (1392 bits), 174 bytes captured (1392 bits) on interface en0, id 0
> Ethernet II, Src: VantivaU_06:13:fb (f8:d2:ac:06:13:fb), Dst: IPv6mcast_01 (33:33:00:00:00:01)
> Internet Protocol Version 6, Src: fe80::fad2:acff:fe06:13fb, Dst: ff02::1
> Internet Control Message Protocol v6
```

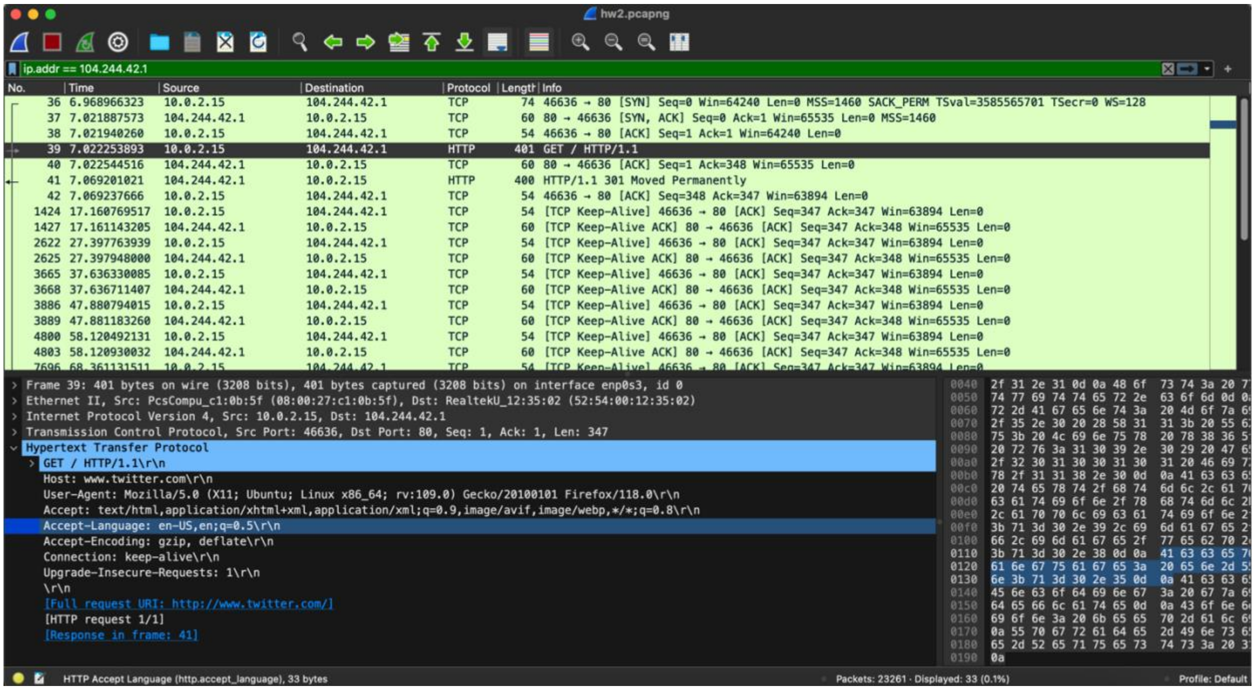
```
0000  33 33 00 00 00 01 f8 d2  ac 06 13 fb 8
0010  38 0d 00 78 3a ff fe 80  00 00 00 00 0
0020  ac ff fe 06 13 fb ff 02  00 00 00 00 0
0030  00 00 00 00 00 01 86 00  6d 2a 40 c0 0
0040  00 00 00 00 00 00 19 05  00 00 00 00 0
0050  05 58 fe ed 00 00 00 00  00 00 00 00 0
0060  05 58 fe ed 00 00 00 00  00 00 00 00 0
0070  40 c0 00 00 01 2c 00 00  01 2c 00 00 0
0080  08 c0 08 00 61 a0 00 00  00 00 00 00 0
0090  00 00 00 00 00 b4 00 00  00 00 00 00 0
00a0  00 00 00 00 00 00 01 01  f8 d2 ac 06 1
```

Wi-Fi: en0: <live capture in progress>   Packets: 32 · Displayed: 32 (100.0%)   Profile: Default

Question 3)

Twitter.com

1) Accept-Language: en-US,en;q=0.5\r\n



```
No.   Time          Source         Destination    Protocol Length Info
   36 6.968966323   10.0.2.15      104.244.42.1   TCP      74 46636 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3585565701 TSecr=0 WS=128
   37 7.021887573   104.244.42.1   10.0.2.15      TCP      60 80 → 46636 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
   38 7.021940260   10.0.2.15      104.244.42.1   TCP      54 46636 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
   39 7.022253893   10.0.2.15      104.244.42.1   HTTP    401 GET / HTTP/1.1
   40 7.022544516   104.244.42.1   10.0.2.15      TCP      60 80 → 46636 [ACK] Seq=1 Ack=348 Win=65535 Len=0
   41 7.069201021   104.244.42.1   10.0.2.15      HTTP    400 HTTP/1.1 301 Moved Permanently
   42 7.069237666   10.0.2.15      104.244.42.1   TCP      54 46636 → 80 [ACK] Seq=348 Ack=347 Win=63894 Len=0
 1424 17.160769517  10.0.2.15      104.244.42.1   TCP      54 [TCP Keep-Alive] 46636 → 80 [ACK] Seq=347 Ack=347 Win=63894 Len=0
 1427 17.161143205  104.244.42.1   10.0.2.15      TCP      60 [TCP Keep-Alive ACK] 80 → 46636 [ACK] Seq=347 Ack=348 Win=65535 Len=0
 2622 27.397763939  10.0.2.15      104.244.42.1   TCP      54 [TCP Keep-Alive] 46636 → 80 [ACK] Seq=347 Ack=347 Win=63894 Len=0
 2625 27.397948000  104.244.42.1   10.0.2.15      TCP      60 [TCP Keep-Alive ACK] 80 → 46636 [ACK] Seq=347 Ack=348 Win=65535 Len=0
 3665 37.636330085  10.0.2.15      104.244.42.1   TCP      54 [TCP Keep-Alive] 46636 → 80 [ACK] Seq=347 Ack=347 Win=63894 Len=0
 3668 37.636711407  104.244.42.1   10.0.2.15      TCP      60 [TCP Keep-Alive ACK] 80 → 46636 [ACK] Seq=347 Ack=348 Win=65535 Len=0
 3886 47.880794015  10.0.2.15      104.244.42.1   TCP      54 [TCP Keep-Alive] 46636 → 80 [ACK] Seq=347 Ack=347 Win=63894 Len=0
 3889 47.881183260  104.244.42.1   10.0.2.15      TCP      60 [TCP Keep-Alive ACK] 80 → 46636 [ACK] Seq=347 Ack=348 Win=65535 Len=0
 4800 58.120492131  10.0.2.15      104.244.42.1   TCP      54 [TCP Keep-Alive] 46636 → 80 [ACK] Seq=347 Ack=347 Win=63894 Len=0
 4803 58.120930032  104.244.42.1   10.0.2.15      TCP      60 [TCP Keep-Alive ACK] 80 → 46636 [ACK] Seq=347 Ack=348 Win=65535 Len=0
 7696 68.361131511  10.0.2.15      104.244.42.1   TCP      54 [TCP Keep-Alive] 46636 → 80 [ACK] Seq=347 Ack=347 Win=63894 Len=0
```

```
> Frame 39: 401 bytes on wire (3208 bits), 401 bytes captured (3208 bits) on interface enp0s3, id 0
> Ethernet II, Src: PcsCompu_c1:0b:5f (08:00:27:c1:0b:5f), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
> Internet Protocol Version 4, Src: 10.0.2.15, Dst: 104.244.42.1
> Transmission Control Protocol, Src Port: 46636, Dst Port: 80, Seq: 1, Ack: 1, Len: 347
v Hypertext Transfer Protocol
  > GET / HTTP/1.1\r\n
    Host: www.twitter.com\r\n
    User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/118.0\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://www.twitter.com/]
    [HTTP request 1/1]
    [Response in frame: 41]
```

```
0040  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20
0050  74 77 69 74 74 65 72 2e  63 6f 6d 0d
0060  72 2d 41 67 65 6e 74 3a  20 4d 6f 7a
0070  2f 35 2e 30 20 28 58 31  31 3b 20 55
0080  75 3b 20 4c 69 6e 75 78  20 78 38 36
0090  20 72 76 3a 31 30 39 2e  30 29 20 47
00a0  2f 32 30 31 30 30 31 30  31 20 46 69
00b0  78 2f 31 31 38 2e 30 0d  0a 41 63 63
00c0  20 74 65 78 74 2f 68 74  6d 6c 2c 61
00d0  63 61 74 69 6f 6e 2f 78  68 74 6d 6c
00e0  2c 61 70 70 6c 69 63 61  74 69 6f 6e
00f0  3b 71 3d 30 2e 39 2c 69  6d 61 67 65
0100  66 2c 69 6d 61 67 65 2f  77 65 62 70
0110  3b 71 3d 30 2e 38 0d 0a  41 63 63 65
0120  61 6e 67 75 61 67 65 3a  20 65 6e 2d
0130  6e 3b 71 3d 30 2e 35 0d  0a 41 63 63
0140  45 6e 63 6f 64 69 6e 67  3a 20 67 7a
0150  64 65 66 6c 61 74 65 0d  0a 43 6f 6e
0160  69 6f 6e 3a 20 6b 65 65  70 2d 61 6c
0170  0a 55 70 67 72 61 64 65  2d 49 6e 73
0180  65 2d 52 65 71 75 65 73  74 73 3a 20
0190  0a
```

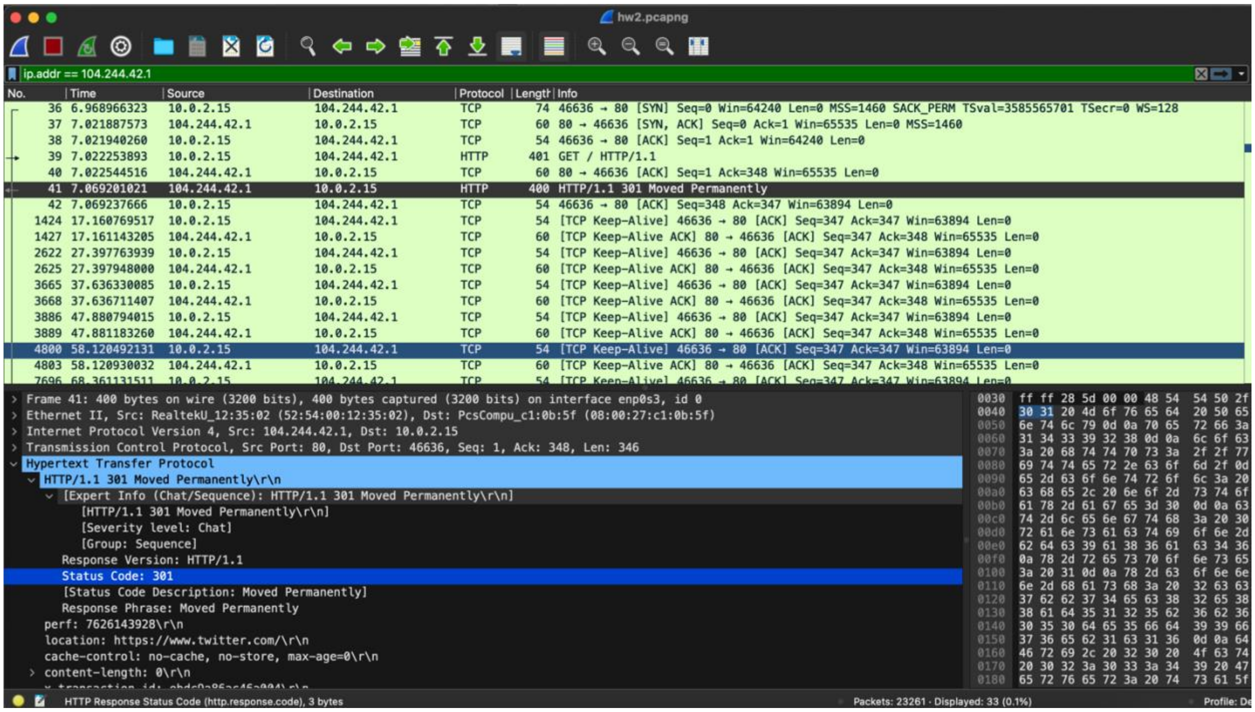
HTTP Accept Language (http.accept_language), 33 bytes

Packets: 23261 · Displayed: 33 (0.1%)

Profile: Default

2) IP address of computer = 10.0.2.15
IP address of the URL = 104.244.42.1

3) Status code : 301 Moved Permanently



```
ip.addr == 104.244.42.1
No.    Time          Source         Destination    Protocol Length Info
   36  6.968966323   10.0.2.15      104.244.42.1   TCP       74 46636 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3585565701 TSecr=0 WS=128
   37  7.021887573   104.244.42.1   10.0.2.15      TCP       60 80 → 46636 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
   38  7.021940260   10.0.2.15      104.244.42.1   TCP       54 46636 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
   39  7.022253893   10.0.2.15      104.244.42.1   HTTP     401 GET / HTTP/1.1
   40  7.022544516   104.244.42.1   10.0.2.15      TCP       60 80 → 46636 [ACK] Seq=1 Ack=348 Win=65535 Len=0
   41  7.069201021   104.244.42.1   10.0.2.15      HTTP     400 HTTP/1.1 301 Moved Permanently
   42  7.069237666   10.0.2.15      104.244.42.1   TCP       54 46636 → 80 [ACK] Seq=348 Ack=347 Win=63894 Len=0
 1424 17.160769517   10.0.2.15      104.244.42.1   TCP       54 [TCP Keep-Alive] 46636 → 80 [ACK] Seq=347 Ack=347 Win=63894 Len=0
 1427 17.161143205   104.244.42.1   10.0.2.15      TCP       60 [TCP Keep-Alive ACK] 80 → 46636 [ACK] Seq=347 Ack=348 Win=65535 Len=0
 2622 27.397763939   10.0.2.15      104.244.42.1   TCP       54 [TCP Keep-Alive] 46636 → 80 [ACK] Seq=347 Ack=347 Win=63894 Len=0
 2625 27.397948000   104.244.42.1   10.0.2.15      TCP       60 [TCP Keep-Alive ACK] 80 → 46636 [ACK] Seq=347 Ack=348 Win=65535 Len=0
 3665 37.636330085   10.0.2.15      104.244.42.1   TCP       54 [TCP Keep-Alive] 46636 → 80 [ACK] Seq=347 Ack=347 Win=63894 Len=0
 3668 37.636711407   104.244.42.1   10.0.2.15      TCP       60 [TCP Keep-Alive ACK] 80 → 46636 [ACK] Seq=347 Ack=348 Win=65535 Len=0
 3886 47.880794015   10.0.2.15      104.244.42.1   TCP       54 [TCP Keep-Alive] 46636 → 80 [ACK] Seq=347 Ack=347 Win=63894 Len=0
 3889 47.881183260   104.244.42.1   10.0.2.15      TCP       60 [TCP Keep-Alive ACK] 80 → 46636 [ACK] Seq=347 Ack=348 Win=65535 Len=0
 4800 58.120492131   10.0.2.15      104.244.42.1   TCP       54 [TCP Keep-Alive] 46636 → 80 [ACK] Seq=347 Ack=347 Win=63894 Len=0
 4803 58.120930032   104.244.42.1   10.0.2.15      TCP       60 [TCP Keep-Alive ACK] 80 → 46636 [ACK] Seq=347 Ack=348 Win=65535 Len=0
 7696 68.361131511   10.0.2.15      104.244.42.1   TCP       54 [TCP Keep-Alive] 46636 → 80 [ACK] Seq=347 Ack=347 Win=63894 Len=0
```

```
> Frame 41: 400 bytes on wire (3200 bits), 400 bytes captured (3200 bits) on interface enp0s3, id 0
> Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_c1:0b:5f (08:00:27:c1:0b:5f)
> Internet Protocol Version 4, Src: 104.244.42.1, Dst: 10.0.2.15
> Transmission Control Protocol, Src Port: 80, Dst Port: 46636, Seq: 1, Ack: 348, Len: 346
v Hypertext Transfer Protocol
  v HTTP/1.1 301 Moved Permanently\r\n
    v [Expert Info (Chat/Sequence): HTTP/1.1 301 Moved Permanently\r\n]
        [HTTP/1.1 301 Moved Permanently\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Response Version: HTTP/1.1
      Status Code: 301
      [Status Code Description: Moved Permanently]
      Response Phrase: Moved Permanently
    perf: 7626143928\r\n
    location: https://www.twitter.com/\r\n
    cache-control: no-cache, no-store, max-age=0\r\n
  > content-length: 0\r\n
```

```
0030  ff ff 28 5d 00 00 48 54  54 50 2f
0040  30 31 20 4d 6f 76 65 64  20 50 65
0050  6e 74 6c 79 0d 0a 70 65  72 66 3a
0060  31 34 33 39 32 38 0d 0a  6c 6f 63
0070  3a 20 68 74 74 70 73 3a  2f 2f 77
0080  69 74 74 65 72 2e 63 6f  6d 2f 0d
0090  65 2d 63 6f 6e 74 72 6f  6c 3a 20
00a0  63 68 65 2c 20 6e 6f 2d  73 74 6f
00b0  61 78 2d 61 67 65 3d 30  0d 0a 63
00c0  74 2d 6c 65 6e 67 74 68  3a 20 30
00d0  72 61 6e 73 61 63 74 69  6f 6e 2d
00e0  62 64 63 39 61 38 36 61  63 34 36
00f0  0a 78 2d 72 65 73 70 6f  6e 73 65
0100  3a 20 31 0d 0a 78 2d 63  6f 6e 6e
0110  6e 2d 68 61 73 68 3a 20  32 63 63
0120  37 62 62 37 34 65 63 38  32 65 38
0130  38 61 64 35 31 32 35 62  36 62 36
0140  30 35 30 64 65 35 66 64  39 39 66
0150  37 36 65 62 31 63 31 36  0d 0a 64
0160  46 72 69 2c 20 32 30 20  4f 63 74
0170  20 30 32 3a 30 33 3a 34  39 20 47
0180  65 72 76 65 72 3a 20 74  73 61 5f
```

HTTP Response Status Code (http.response.code), 3 bytes

Packets: 23261 · Displayed: 33 (0.1%)

Profile: De

4) There is a 3-way handshake in establishing a TCP connection between the client and the server. Here is a brief overview of the TCP three-way handshake:

1) SYN from client: The client initiates the connection by sending a TCP segment with the SYN flag set to the server. This segment contains the initial sequence number.

2) SYN-ACK from server: After receiving the SYN segment, the server responds with a TCP segment that has both the SYN and ACK flags set. The acknowledgement number is set to one more than the received sequence number from the client.

3)ACK from client: The client acknowledges the server's response by sending a TCP segment with the ACK flag set. The acknowledge number is set to one more than the received sequence number from the server.

After this 3-way handshake, the TCP connection is established, and data can be exchanged between the client and the server.

5) The port numbers used are 46636 and 80 with respect to client and server respectively. The various protocols used are TCP and HTTP.

6) Transport Layer Protocol used are TCP (Transmission Control Protocol) and TLS (Transport Layer Security)

7) Cookies play an important role in data exchange between browser and the server. Cookies are transmitted through HTTP headers, with "Set-Cookie" header in server response indicating the creation or modification of cookies. Cookies are involved in the interaction with the URIs, enabling functions like user authentication, session management and more. They store the information on user's side for future reference.

8) The difference in accessing the website for the first time vs second time is that when accessing a website for the first time, the browser needs to download resources, perform DNS resolution and establish connection, resulting in a potentially longer load time but the accessing the website second time benefits from caching, where locally stored copies of resources are used, speeding up the page load. First time cookie is set and second time it might recognize the cookies set.

UNM.edu

1) Accept-Language: en-US,en;q=0.5\r\n

2) IP address of computer = 10.0.2.15
   IP address of the URL = 129.24.172.124

3) Status code: 302

4) There is a 3-way handshake in establishing a TCP connection between the client and the server. Here is a brief overview of the TCP three-way handshake:

   1) SYN from client: The client initiates the connection by sending a TCP segment with the SYN flag set to the server. This segment contains the initial sequence number.

      2) SYN-ACK from server: After receiving the SYN segment, the server responds with a TCP segment that has both the SYN and ACK flags set. The acknowledgement number is set to one more than the received sequence number from the client.

3)ACK from client: The client acknowledges the server's response by sending a TCP segment with the ACK flag set. The acknowledge number is set to one more than the received sequence number from the server.

After this 3-way handshake, the TCP connection is established, and data can be exchanged between the client and the server.

5) The protocols used are TCP, HTTP, TLSv1.2 Record Layer: HandShake Protocol. And, the port numbers used are 50546, 80, 46102, 443.

6) Transport Layer Protocol used are TCP (Transmission Control Protocol) and TLS (Transport Layer Security)

7) Cookies play an important role in data exchange between browser and the server. Cookies are transmitted through HTTP headers, with "Set-Cookie" header in server response indicating the creation or modification of cookies. Cookies are involved in the interaction with the URIs, enabling functions like user authentication, session management and more. They store the information on user's side for future reference.

8) The difference in accessing the website for the first time vs second time is that when accessing a website for the first time, the browser needs to download resources, perform DNS resolution and establish connection, resulting in a potentially longer load time but the accessing the website second time benefits from caching, where locally stored copies of resources are used, speeding up the page load. First time cookie is set and second time it might recognize the cookies set.

CS.UNM.edu

1) Accept-Language: en-US,en;q=0.5\r\n

2) IP address of computer = 10.0.2.15
IP address of the URL = 64.106.20.76

3) Status Code: 301

4) There is a 3-way handshake in establishing a TCP connection between the client and the server. Here is a brief overview of the TCP three-way handshake:

1) SYN from client: The client initiates the connection by sending a TCP segment with the

SYN flag set to the server. This segment contains the initial sequence number.

2) SYN-ACK from server: After receiving the SYN segment, the server responds with a TCP segment that has both the SYN and ACK flags set. The acknowledgement number is set to one more than the received sequence number from the client.

3)ACK from client: The client acknowledges the server's response by sending a TCP segment with the ACK flag set. The acknowledge number is set to one more than the received sequence number from the server.

After this 3-way handshake, the TCP connection is established, and data can be exchanged between the client and the server.

5) The protocols used are TCP, HTTP, TLSv1.2 Record Layer: HandShake Protocol. And, the port numbers used are 36818, 80, 58902, 443.

6) Transport Layer Protocol used are TCP (Transmission Control Protocol) and TLS (Transport Layer Security)

7) Cookies play an important role in data exchange between browser and the server. Cookies are transmitted through HTTP headers, with "Set-Cookie" header in server response indicating the creation or modification of cookies. Cookies are involved in the interaction with the URIs, enabling functions like user authentication, session management and more. They store the information on user's side for future reference.

8) The difference in accessing the website for the first time vs second time is that when accessing a website for the first time, the browser needs to download resources, perform DNS resolution and establish connection, resulting in a potentially longer load time but the accessing the website second time benefits from caching, where locally stored copies of resources are used, speeding up the page load. First time cookie is set and second time it might recognize the cookies set.

Canvas.unm.edu

1) Accept-Language: en-US,en;q=0.5\r\n

2) IP address of computer = 10.0.2.15
   IP address of the URL = 52.24.4.139

3) Status code: 301

4) There is a 3-way handshake in establishing a TCP connection between the client and the server. Here is a brief overview of the TCP three-way handshake:

   1) SYN from client: The client initiates the connection by sending a TCP segment with the SYN flag set to the server. This segment contains the initial sequence number. Packet 7948 is the client's initial SYN packet.

   2) SYN-ACK from server: After receiving the SYN segment, the server responds with a TCP segment that has both the SYN and ACK flags set. The acknowledgement number is set to one more than the received sequence number from the client. Packet 7950 is the server's SYN-ACK response.

   3)ACK from client: The client acknowledges the server's response by sending a TCP segment with the ACK flag set. The acknowledge number is set to one more than the received sequence number from the server. Packet 7951 is the client's ACK of SYN-ACK.

   After this 3-way handshake, the TCP connection is established, and data can be exchanged between the client and the server.

5) The protocols used are TCP, HTTP. And, the port numbers used are 46356, 80, 46358.

6) Transport Layer Protocol used are TCP (Transmission Control Protocol) and TLS (Transport Layer Security)

7) Cookies play an important role in data exchange between browser and the server. Cookies are transmitted through HTTP headers, with "Set-Cookie" header in server response indicating the creation or modification of cookies. Cookies are involved in the interaction with the URIs, enabling functions like user authentication, session management and more. They store the information on user's side for future reference.

8) The difference in accessing the website for the first time vs second time is that when accessing a website for the first time, the browser needs to download resources, perform DNS resolution and establish connection, resulting in a potentially longer load time but the accessing the website second time benefits from caching, where locally stored copies of resources are used, speeding up the page load. First time cookie is set and second time it might recognize the cookies set.

Facebook.com

1) Accept-Language: en-US,en;q=0.5\r\n

2) IP address of computer = 10.0.2.15
   IP address of the URL = 31.13.71.36

3) .

4) The initial step involves the client obtaining the IP address of the URL by querying the local DNS cache. As this was the first access to the website, a DNS resolver was consulted due to the absence of information in the local cache. Following the acquisition of the IP address, the client initiates a TCP connection with the server, and a TCP 3-way handshake ensues. In the context of using HTTPS, an extended 4-way handshake occurs. This process facilitates the establishment of encryption keys and a session ID through TLS, ensuring the secure encryption of data transmitted between the client and the server. Subsequently, with the encryption parameters established, the client and server engage in a data exchange, leading to successful access to the desired website.

5) The protocols used are TCP, TLS, and QUIC and the port numbers used are 41084, 41098 and 433.

6) The transport layer protocol used are TCP, TLS and QUIC.

7) Cookies play an important role in data exchange between browser and the server. Cookies are transmitted through HTTP headers, with “Set-Cookie” header in server response indicating the creation or modification of cookies. Cookies are involved in the interaction with the URIs, enabling functions like user authentication, session management and more. They store the information on user’s side for future reference.

8) The difference in accessing the website for the first time vs second time is that when accessing a website for the first time, the browser needs to download resources, perform DNS resolution and establish connection, resulting in a potentially longer load time but the accessing the website second time benefits from caching, where locally stored copies of resources are used, speeding up the page load. First time cookie is set and second time it might recognize the cookies set.

Usenix.org

1) Accept-Language: en-US,en;q=0.5\r\n

2) IP address of computer = 10.0.2.15
   IP address of the URL = 23.185.0.4

3) Status code: 301

4) The process begins with the client obtaining the IP of the URL by checking the local DNS cache. Since this is the initial access to the website, the client queries a DNS resolver due to the empty local cache. After acquiring the IP, the client establishes a TCP connection with the server, followed by a TCP 3-way handshake. Upon successful connection, the client issues an HTTP request to the obtained IP. The server responds with an HTTP status code of 301, indicating a permanent move and providing the new URL. Subsequently, given the use of HTTPS, which combines HTTP with TLS for security, an additional 4-way handshake occurs. This handshake results in the generation of encryption keys and a session ID, ensuring the secure encryption of data exchanged between the client and the server. Following the establishment of secure communication parameters, the client and server engage in a data exchange, ultimately leading to the successful access of the website.

5) The protocols used are TCP, TLS, and HTTP. And, the port numbers used are 34242, 443, 49548 and 80.

6) Transport Layer Protocol used are TCP (Transmission Control Protocol) and TLS (Transport Layer Security)

7) Cookies play an important role in data exchange between browser and the server. Cookies are transmitted through HTTP headers, with “Set-Cookie” header in server response indicating the creation or modification of cookies. Cookies are involved in the interaction with the URIs, enabling functions like user authentication, session management and more. They store the information on user’s side for future reference.

8) The difference in accessing the website for the first time vs second time is that when accessing a website for the first time, the browser needs to download resources, perform DNS resolution and establish connection, resulting in a potentially longer load time but the accessing the website second time benefits from caching, where locally

stored copies of resources are used, speeding up the page load. First time cookie is set and second time it might recognize the cookies set.
Iijlab.net

1) Accept-Language: en-US,en;q=0.5\r\n

2) IP address of computer = 10.0.2.15
   IP address of the URL = 202.238.220.76

3) .

4) The process begins with the client obtaining the IP of the URL by checking the local DNS cache. Since this is the initial access to the website, the client queries a DNS resolver due to the empty local cache. After acquiring the IP, the client establishes a TCP connection with the server, followed by a TCP 3-way handshake. Upon successful connection, the client issues an HTTP request to the obtained IP. The server responds with an HTTP status code of 301, indicating a permanent move and providing the new URL. Subsequently, given the use of HTTPS, which combines HTTP with TLS for security, an additional 4-way handshake occurs. This handshake results in the generation of encryption keys and a session ID, ensuring the secure encryption of data exchanged between the client and the server. Following the establishment of secure communication parameters, the client and server engage in a data exchange, ultimately leading to the successful access of the website.

5) The protocols used are TCP and TLS. And, the port numbers used are 53196, 443, 53168 and 53180.

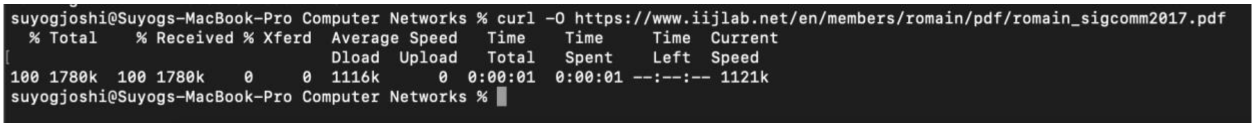
6) Transport Layer Protocol used are TCP (Transmission Control Protocol) and TLS (Transport Layer Security)

7) Cookies play an important role in data exchange between browser and the server. Cookies are transmitted through HTTP headers, with "Set-Cookie" header in server response indicating the creation or modification of cookies. Cookies are involved in the interaction with the URIs, enabling functions like user authentication, session management and more. They store the information on user's side for future reference.

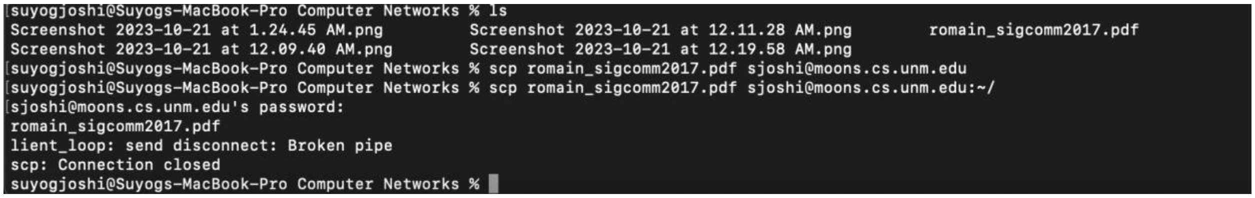
8) The difference in accessing the website for the first time vs second time is that when accessing a website for the first time, the browser needs to download resources, perform DNS resolution and establish connection, resulting in a potentially longer

load time but the accessing the website second time benefits from caching, where locally stored copies of resources are used, speeding up the page load. First time cookie is set and second time it might recognize the cookies set.

Question 4)



```
suyogjoshi@Suyogs-MacBook-Pro Computer Networks % curl -O https://www.iijlab.net/en/members/romain/pdf/romain_sigcomm2017.pdf
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
[                                 Dload  Upload   Total   Spent    Left  Speed
100 1780k  100 1780k    0     0  1116k      0  0:00:01  0:00:01 --:--:-- 1121k
suyogjoshi@Suyogs-MacBook-Pro Computer Networks %
```



```
[suyogjoshi@Suyogs-MacBook-Pro Computer Networks % ls
Screenshot 2023-10-21 at 1.24.45 AM.png         Screenshot 2023-10-21 at 12.11.28 AM.png        romain_sigcomm2017.pdf
Screenshot 2023-10-21 at 12.09.40 AM.png        Screenshot 2023-10-21 at 12.19.58 AM.png
[suyogjoshi@Suyogs-MacBook-Pro Computer Networks % scp romain_sigcomm2017.pdf sjoshi@moons.cs.unm.edu
[suyogjoshi@Suyogs-MacBook-Pro Computer Networks % scp romain_sigcomm2017.pdf sjoshi@moons.cs.unm.edu:~/
[sjoshi@moons.cs.unm.edu's password:
romain_sigcomm2017.pdf
lient_loop: send disconnect: Broken pipe
scp: Connection closed
suyogjoshi@Suyogs-MacBook-Pro Computer Networks %
```

1) DNS and HTTP Requests: DNS (Domain Name System): Before downloading the file, there will likely be a DNS resolution to translate the domain name "www.iijlab.net" to an IP address. HTTP Requests: When you use wget or curl to download a file, it typically sends an HTTP GET request to the server to retrieve the specified resource (in this case, the PDF file).

2) The number of packets transported during download and upload is not explicitly mentioned. The packet count depends on factors like the file size, the underlying protocol (e.g., TCP), and the network conditions.

3) The attributes of the datagram depend on the underlying protocol. If the file is downloaded using HTTP, it will likely be over TCP. TCP datagrams include source and destination port numbers, sequence numbers, acknowledgment numbers, and control flags.

4) TCP, being a reliable transport protocol, incorporates error checking.

5) The TCP checksum provides a strong level of error detection. It helps ensure that the data received at the destination is the same as the data sent by the source. If the checksum indicates an error, TCP mechanisms trigger retransmission to correct any issues.

Question 5)

RFC 2616

Redirection:

It is the process of instructing a web client such as browser to take additional actions in response to a request. These instructions are conveyed through specific HTTP status code in the 300 range. This group of status codes indicates that the user agent needs to take additional steps to fulfill the request. If the subsequent. Request uses the GET or HEAD method, the user agent can execute the required action without user involvement. It is recommended for the client to recognize and manage infinite redirection loops since they lead to repeated network traffic during each redirection. Redirection is needed to facilitate a dynamic and responsive web environment, allowing for changes in resource locations, improving load distribution, maintaining SEO, and enhancing overall user experiencing. It's fundamental mechanism in the HTTP protocol that contributes to the flexibility and adaptability of the web.

There are various 300 level status code and some of them are:
1) 300 Multiple Choices
2) 301 Moved Permanently
3) 302 Found
4) 303 See Other
5) Not Modified
6) Use Proxy
7) 306 (Unused)
8) 307 Temporary Redirect

Client Error:

The 400 HTTP status codes are designed for conditions wherein the customer is deemed to have made an error. The server, in responding to requests (apart from HEAD requests), is counseled to encompass an explanatory message, indicating whether the error is transient or permanent. These codes are applicable to any request method, and it's recommended that person dealers display the provided explanation to customers. Regarding records transmission from the purchaser, specifically while using TCP, it's crucial for the server to make certain that the patron recognizes acquired response packets earlier than ultimate the input connection. This precaution is important to prevent problems if the purchaser continues sending statistics after closure, as the server's TCP stack might also send a reset packet to the consumer, probably erasing unacknowledged input buffers before processing via the HTTP utility.

There are various 400 level status code and some of them are:
1) 400 Bad Request
2) 401 Unauthorized
3) 402 Payment Required
4) 403 Forbidden
5) 404 Not Found
6) 405 Method Not Allowed
7) 406 Not Acceptable
8) 407 Proxy Authentication Required
9) 408 Request Timeout
10) 409 Conflict
11) 410 Gone
12) 411 Length Required
13) 412 Precondition Failed
14) 413 Payload Too Large
15) 414 URI Too Long
16) 415 Unsupported Media Type

Server Error:

HTTP response status codes starting with "5" signify instances where the server acknowledges an error or its inability to fulfill a request. Unless processing a HEAD request, it is recommended for the server to include an explanatory entity that describes the error and indicates whether it is a temporary or permanent condition. User agents are advised to present any included entity to the user. These response codes are relevant to requests of any method type.
It is important because they communicate server issues to the client. It also specifies whether the error is temporary or permanent. It helps user understand the information and improve their understanding. So, they help diagnose errors, guide users and maintain consistency in handling errors across different types of requests.

There are various 500 level status code and some of them are:
1) 500 Internal Server Error
2) 501 Not Implemented
3) 502 Bad Gateway
4) 503 Service Unavailable
5) 504 Gateway Timeout
6) 505 HTTP Version Not Supported

Caching:

HTTP, the technology used for websites and online systems, uses something called response caches to make things faster. Imagine it like a quick memory for frequently used information. In the HTTP/1.1 protocol, there are tools to make this caching work really well. It's like having a system to avoid asking for the same things over and over or sending a lot of unnecessary data. The goal is to make everything clear and understandable, but sometimes, to meet other needs like speed or availability, it's okay to be a bit flexible. The protocol lets the main servers, memory caches, and your device talk to each other and decide when to be super clear and when it's okay to be a bit more flexible. It's kind of like a balance between making things really simple and fast for users, but still making sure everything works smoothly. There are rules to make sure everyone knows when things are being a bit flexible, and it's encouraged that the people building these systems try to keep things clear unless they have a really good reason not to.

Expiration:

Expiration mechanisms, often defined through headers like “Expires” and “Cache-Control” helps in managing the freshness of cached resources. They are necessary to ensure that clients do not use outdated content and receive the latest version of a resource when needed. It explains the expiration model in HTTP caching, highlighting how servers and caches maintain the accuracy of cached responses:

1) Server-Specified Expiration:
   Optimal caching happens when servers tell browsers how long they can keep certain information using instructions like “Expires” or “max-age”. This influences how long the stored information remains useful, but it doesn’t force the browser to refresh or show it to the user unless necessary. It’s well organized where information is stored for quick access, and rules determine when to keep or update that information.

2) Heuristic Expiration:
   When the main servers don’t specifically say how long information can be kept, browsers use their best guess. It’s estimating the life when there’s no expiration date.

3) Age Calculations:
   When your browser saves information, it keeps track of how long it’s been around using something called the “Age” header. It’s like putting a timestamp on the information to

know how old it is. Now, to make sure the time is accurate, the browser doesn't rely on just one method. It uses two different ways to figure out how much time has passes. It's like using both a clock on the wall and timer on your phone to be really sure about the time. By doping, this your browser makes sure it has a reliable and accurate measure of how old the stored information is.

4) Expiration Calculations:
   Cache decides if a response is fresh or stale by comparing its freshness lifetime to its age. The browser stores information and decides if it's still good by checking how long it was supposed to stay fresh set by max-age and how old the stored information is now using a timestamp. If the information is older than it was supposed to be fresh, it might consider it as stale. The browser uses heuristics and warning if it doesn't have clear instructions about how long the information should stay fresh. The browser is being smart and deciding if the stored information is still okay to use.

5) Disambiguating Expiration Values:
   When your browser has saved information and gets a new version from the internet, it decides what to do. If it already has a recent version, it might ignore the new one. If there are multiple new versions, it chooses the one with the most recent timestamp.

6) Disambiguating Multiple Responses:
   When the browser gets information from different places, it decides which one to use. It picks the one that was made most recently. And also forces a check meaning the browser wants to make sure the stored information is still good, it might ask all the places it got information from to double-check.

Security Considerations:

It is meant to inform application developers, information providers, and users of the security limitations. It doesn't include definitive solutions to the problems revealed, but it does make some suggestions for reducing security risks.

1) Personal Information Handling:

The web browser has the personal information like name, locations and passwords. To keep this safe, it's suggested that the browser should have settings where you can decide whom to share the information to. This way, the browser is careful not to accidently share your private info with others on the internet.

2) Abuse of Server Log Information:

Server can save personal data about the user requests. Sometimes, it can save details about what users do on a website. But, the people who run the website need to make sure that any personal information is kept private. They're responsible for not sharing your private stuff with others without asking you first. It's like a rule to make sure your personal details stay safe.

3) Transfer of Sensitive Information:

Internet is like a highway, and HTTP is like the traffic rules for information travelling on that highway. But, these rules can't control what the information says. So, when making websites or apps, the people building them should have ways for users to control what information is shared. They need to be careful about showing details like what kind of server they're using and handling certain pieces of information. It's like making sure there are safety measures to control what details are visible on the information highway.

4) Encoding Sensitive Information in URIs:

When you visit a website, your browser might tell the new site where you came from (like the previous webpage). This is done using something called the "Referer" field. However, it's suggested that you should have control over whether your browser shares this information. Also, it's a good idea not to share this "Referer" information if the website you are visiting is not using a secure connection (HTTP instead of HTTPS). It's like having a choice to keep your previous steps private and not sharing them when it's not safe.

5) Privacy Issues Connected to Accept Headers:

When you visit a website, your browser tells the site what kind of content it prefers using something called "Accept headers." However, this information can reveal things about you. So, it's suggested that your browser should let you know about this and give you some control. It's like a friendly reminder that your preferences might be seen by the website, and you should be cautious about making them too detailed for privacy reasons.

Reference:

RFC 2616: Hypertext Transfer Protocol -- HTTP/1.1. (1999, June 1). IETF Datatracker.

https://datatracker.ietf.org/doc/html/rfc2616#section-10.3