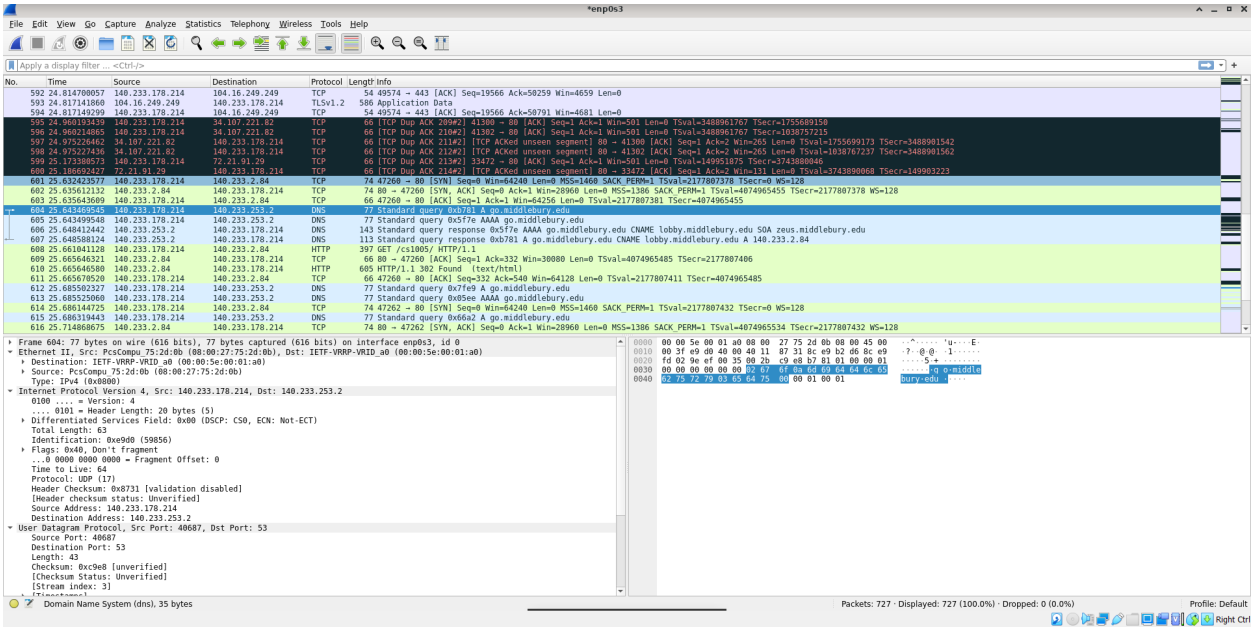
Manual HTTP

1 See go/ in action

- Use the tools we have discussed to observe the various steps (DNS and HTTP) involved in visiting a go link.

We opened wireshark, then Firefox. On firefox, we typed go/cs1005/. On wireshark, we saw the following: There are two DNS request for the IP of "go.middlebury.edu"one of type A



and the other of type AAAA. I am guessing these A's refer to IP v4 (A) and IP v6 (AAAA). The details of the A request is:

```
Frame 604: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on
    interface enp0s3, id 0
Ethernet II, Src: PcsCompu_75:2d:0b (08:00:27:75:2d:0b), Dst: IETF-VRRP-
    VRID_a0 (00:00:5e:00:01:a0)
     Destination: IETF-VRRP-VRID_a0 (00:00:5e:00:01:a0)
     Source: PcsCompu_75:2d:0b (08:00:27:75:2d:0b)
     Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 140.233.178.214, Dst: 140.233.253.2
     0100 .... = Version: 4
     .... 0101 = Header Length: 20 bytes (5)
     Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
     Total Length: 63
     Identification: 0xe9d0 (59856)
     Flags: 0x40, Dont fragment
     ...0 0000 0000 0000 = Fragment Offset: 0
     Time to Live: 64
     Protocol: UDP (17)
     Header Checksum: 0x8731 [validation disabled]
```

```
    [Header checksum status: Unverified]
    Source Address: 140.233.178.214
    Destination Address: 140.233.253.2
User Datagram Protocol, Src Port: 40687, Dst Port: 53
    Source Port: 40687
    Destination Port: 53
    Length: 43
    Checksum: 0xc9e8 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 3]
    [Timestamps]
    UDP payload (35 bytes)
Domain Name System (query)
    Transaction ID: 0xb781
    Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
    Queries
    [Response In: 607]
```

We see two responses to these requests, only A's response contain an IP address:

```
Frame 607: 113 bytes on wire (904 bits), 113 bytes captured (904 bits) on
   interface enp0s3, id 0
Ethernet II, Src: JuniperN_c1:73:b6 (c0:bf:a7:c1:73:b6), Dst: PcsCompu_75
   :2d:0b (08:00:27:75:2d:0b)
    Destination: PcsCompu_75:2d:0b (08:00:27:75:2d:0b)
    Source: JuniperN_c1:73:b6 (c0:bf:a7:c1:73:b6)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 140.233.253.2, Dst: 140.233.178.214
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0xb8 (DSCP: EF PHB, ECN: Not-ECT)
    Total Length: 99
    Identification: 0xbf9c (49052)
    Flags: 0x00
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 62
    Protocol: UDP (17)
    Header Checksum: 0xf289 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 140.233.253.2
    Destination Address: 140.233.178.214
User Datagram Protocol, Src Port: 53, Dst Port: 40687
    Source Port: 53
    Destination Port: 40687
    Length: 79
    Checksum: 0x6549 [unverified]
    [Checksum Status: Unverified]
```

```
    [Stream index: 3]
    [Timestamps]
    UDP payload (71 bytes)
Domain Name System (response)
    Transaction ID: 0xb781
    Flags: 0x8580 Standard query response, No error
    Questions: 1
    Answer RRs: 2
    Authority RRs: 0
    Additional RRs: 0
    Queries
    Answers
        go.middlebury.edu: type CNAME, class IN, cname lobby.middlebury.edu
        lobby.middlebury.edu: type A, class IN, addr 140.233.2.84
    [Request In: 604]
    [Time: 0.005118579 seconds]
```

We see that this response idicate that "go.middlebury.edy" is at 140.233.2.84. Directly following this response, we see an HTTP GET request to 140.233.2.84:

```
Frame 608: 397 bytes on wire (3176 bits), 397 bytes captured (3176 bits) on interface enp0s3, id 0
Ethernet II, Src: PcsCompu_75:2d:0b (08:00:27:75:2d:0b), Dst: IETF-VRRP-VRID_a0 (00:00:5e:00:01:a0)
    Destination: IETF-VRRP-VRID_a0 (00:00:5e:00:01:a0)
    Source: PcsCompu_75:2d:0b (08:00:27:75:2d:0b)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 140.233.178.214, Dst: 140.233.2.84
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 383
    Identification: 0xb573 (46451)
    Flags: 0x40, Dont fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0xb508 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 140.233.178.214
    Destination Address: 140.233.2.84
Transmission Control Protocol, Src Port: 47260, Dst Port: 80, Seq: 1, Ack: 1, Len: 331
    Source Port: 47260
    Destination Port: 80
    [Stream index: 25]
    [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 331]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 410667962
```

```
    [Next Sequence Number: 332    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 513856551
    1000 .... = Header Length: 32 bytes (8)
    Flags: 0x018 (PSH, ACK)
    Window: 502
    [Calculated window size: 64256]
    [Window size scaling factor: 128]
    Checksum: 0xd06e [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    Options: (12 bytes), No-Operation (NOP), No-Operation (NOP),
   Timestamps
    [Timestamps]
    [SEQ/ACK analysis]
    TCP payload (331 bytes)
Hypertext Transfer Protocol
    GET /cs1005/ HTTP/1.1\r\n
    Host: go\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:96.0) Gecko/20100101
   Firefox/96.0\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://go/cs1005/]
    [HTTP request 1/1]
    [Response in frame: 610]
```

We see that the Hypertext Transfer Protocol (HTTP) contains the expected key:value pairs. The first line starts with the type of the request (GET), then the name of the resource (/cs1005/), and finally the protocol used and its version (HTTP/1.1) ending it with the Microsoft choice of a new line (/r/n).

It is interesting that Firefox automatically recognized "go" as "go.middlebury.edu". I didn't see any request in wireshark before the image above that ask for the meaning of "go". Even though Firefox recognized "go" as "go.middlebury.edu", in the HOST key in the HTTP Get request, it only placed "go/r/n" rather than "go.middlebury.edu/r/n". My virtual machine recognise that "go" = "go.middlebury.edu" when it first connects to the Middlebury access point. It receives this info as a DHCP response. We can see this in the "/etc/resolv.conf" file.

After the GET request, we see a GET response (found 302). The content of the response is that /cs1005/ has been redirected to http://go.middlebury.edu/redirect.php?code=cs1005:

```
Frame 610: 605 bytes on wire (4840 bits), 605 bytes captured (4840 bits)
   on interface enp0s3, id 0
```

```
Ethernet II, Src: JuniperN_33:aa:64 (c0:bf:a7:33:aa:64), Dst: PcsCompu_75:2d:0b (08:00:27:75:2d:0b)
    Destination: PcsCompu_75:2d:0b (08:00:27:75:2d:0b)
    Source: JuniperN_33:aa:64 (c0:bf:a7:33:aa:64)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 140.233.2.84, Dst: 140.233.178.214
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 591
    Identification: 0xddcb (56779)
    Flags: 0x40, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 63
    Protocol: TCP (6)
    Header Checksum: 0x8ce0 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 140.233.2.84
    Destination Address: 140.233.178.214
Transmission Control Protocol, Src Port: 80, Dst Port: 47260, Seq: 1, Ack: 332, Len: 539
    Source Port: 80
    Destination Port: 47260
    [Stream index: 25]
    [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 539]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 513856551
    [Next Sequence Number: 540    (relative sequence number)]
    Acknowledgment Number: 332    (relative ack number)
    Acknowledgment number (raw): 410668293
    1000 .... = Header Length: 32 bytes (8)
    Flags: 0x018 (PSH, ACK)
    Window: 235
    [Calculated window size: 30080]
    [Window size scaling factor: 128]
    Checksum: 0x1ee4 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    [Timestamps]
    [SEQ/ACK analysis]
    TCP payload (539 bytes)
Hypertext Transfer Protocol
    HTTP/1.1 302 Found\r\n
    Date: Mon, 31 Jan 2022 18:31:23 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.27\r\n
    Location: http://go.middlebury.edu/redirect.php?code=cs1005/\r\n
    Content-Length: 234\r\n
```

```
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=iso-8859-1\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.004605452 seconds]
    [Request in frame: 608]
    [Request URI: http://go/cs1005/]
    File Data: 234 bytes
Line-based text data: text/html (7 lines)
    <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">\n
    <html><head>\n
    <title>302 Found</title>\n
    </head><body>\n
    <h1>Found</h1>\n
    <p>The document has moved <a href="http://go.middlebury.edu/redirect.
   php?code=cs1005/">here</a>.</p>\n
    </body></html>\n
```

Another GET request follows to the redirection link (perceeded by DNS request to find the IP of go.middlebury.edu):

```
Frame 618: 430 bytes on wire (3440 bits), 430 bytes captured (3440 bits)
   on interface enp0s3, id 0
Ethernet II, Src: PcsCompu_75:2d:0b (08:00:27:75:2d:0b), Dst: IETF-VRRP-
   VRID_a0 (00:00:5e:00:01:a0)
    Destination: IETF-VRRP-VRID_a0 (00:00:5e:00:01:a0)
    Source: PcsCompu_75:2d:0b (08:00:27:75:2d:0b)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 140.233.178.214, Dst: 140.233.2.84
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 416
    Identification: 0x7625 (30245)
    Flags: 0x40, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0xf435 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 140.233.178.214
    Destination Address: 140.233.2.84
Transmission Control Protocol, Src Port: 47262, Dst Port: 80, Seq: 1, Ack:
    1, Len: 364
    Source Port: 47262
    Destination Port: 80
    [Stream index: 26]
    [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 364]
    Sequence Number: 1    (relative sequence number)
```

```
    Sequence Number (raw): 2964543821
    [Next Sequence Number: 365    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 2981316705
    1000 .... = Header Length: 32 bytes (8)
    Flags: 0x018 (PSH, ACK)
    Window: 502
    [Calculated window size: 64256]
    [Window size scaling factor: 128]
    Checksum: 0xd08f [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    [Timestamps]
    [SEQ/ACK analysis]
    TCP payload (364 bytes)
Hypertext Transfer Protocol
    GET /redirect.php?code=cs1005/ HTTP/1.1\r\n
    Host: go.middlebury.edu\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:96.0) Gecko/20100101 Firefox/96.0\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://go.middlebury.edu/redirect.php?code=cs1005/]
    [HTTP request 1/1]
    [Response in frame: 623]
```

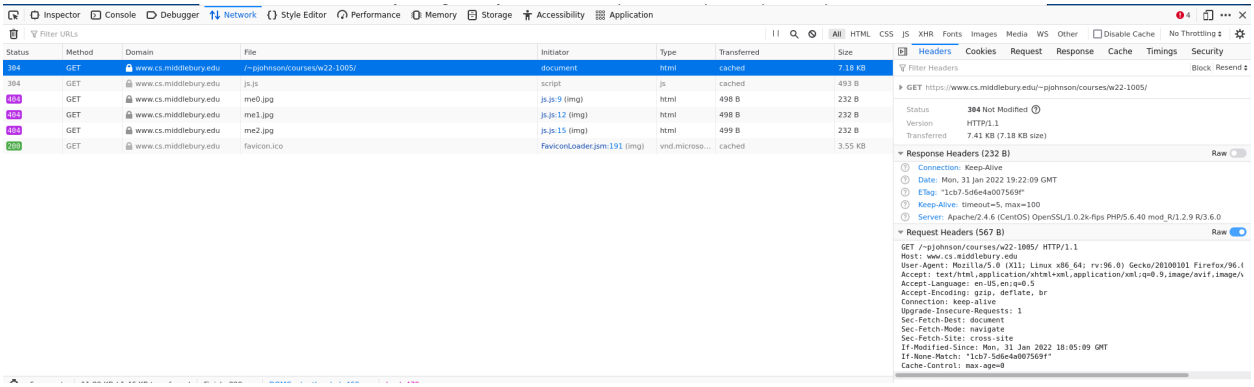
Here we see that the Host value is "go.middlebury.edu/r/n". The response to this request is:

```
Frame 623: 395 bytes on wire (3160 bits), 395 bytes captured (3160 bits) on interface enp0s3, id 0
Ethernet II, Src: JuniperN_33:aa:64 (c0:bf:a7:33:aa:64), Dst: PcsCompu_75:2d:0b (08:00:27:75:2d:0b)
    Destination: PcsCompu_75:2d:0b (08:00:27:75:2d:0b)
    Source: JuniperN_33:aa:64 (c0:bf:a7:33:aa:64)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 140.233.2.84, Dst: 140.233.178.214
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 381
    Identification: 0x4247 (16967)
    Flags: 0x40, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 63
```

```
    Protocol: TCP (6)
    Header Checksum: 0x2937 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 140.233.2.84
    Destination Address: 140.233.178.214
Transmission Control Protocol, Src Port: 80, Dst Port: 47262, Seq: 1, Ack:
    365, Len: 329
    Source Port: 80
    Destination Port: 47262
    [Stream index: 26]
    [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 329]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 2981316705
    [Next Sequence Number: 330    (relative sequence number)]
    Acknowledgment Number: 365    (relative ack number)
    Acknowledgment number (raw): 2964544185
    1000 .... = Header Length: 32 bytes (8)
    Flags: 0x018 (PSH, ACK)
    Window: 235
    [Calculated window size: 30080]
    [Window size scaling factor: 128]
    Checksum: 0xb21f [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    Options: (12 bytes), No-Operation (NOP), No-Operation (NOP),
   Timestamps
    [Timestamps]
    [SEQ/ACK analysis]
    TCP payload (329 bytes)
Hypertext Transfer Protocol
    HTTP/1.1 302 Found\r\n
    Date: Mon, 31 Jan 2022 18:31:23 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.27\r\n
    X-Powered-By: PHP/7.4.27\r\n
    Location: http://www.cs.middlebury.edu/~pjohnson/courses/w22-1005\r\n
    Content-Length: 0\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 1/1]
    [Time since request: 0.020209804 seconds]
    [Request in frame: 618]
    [Request URI: http://go.middlebury.edu/redirect.php?code=cs1005/]
```

This response redirect us to "http://www.cs.middlebury.edu/ pjohnson/courses/w22-1005" which is the actual location. I didn't find any HTTP request or responses after. This is because it switched to HTTPs (secured) and wireshark can't decipher these messages but at least we can see them under TLSc protocol messages. To see the encrypted messages we go

to Firefox > developer tool > Network.



2 Verify HTTP

- Fetch my webpage using a graphical browser. Observe the operation using Wireshark. Verify that you understand the meaning and importance of each packet. Understand why the packets are sent (ie, what computation the browser is performing that causes each packet to be sent).

When we go to the page without the go link (just refresh the page), we see only the TLSv messages on wireshark and the deciphered messages on Firefox (Fig. 1)

```
5 0.012735794 140.233.20.9  140.233.178.214 TCP 66  443     46130 [ACK]
   Seq=1 Ack=593 Win=30208 Len=0 TSval=2246148080 TSecr=2471071273
11  0.396605790 140.233.20.9  140.233.178.214 TCP 66  443     46130 [ACK]
   Seq=138 Ack=1133 Win=31360 Len=0 TSval=2246148462 TSecr=2471071655
9 0.056704302 140.233.20.9  140.233.178.214 TCP 66  443     46130 [ACK]
   Seq=138 Ack=644 Win=30208 Len=0 TSval=2246148124 TSecr=2471071277
27  5.439241048 140.233.20.9  140.233.178.214 TCP 66  443     46130 [ACK]
   Seq=1875 Ack=2143 Win=33792 Len=0 TSval=2246153505 TSecr=2471076698
23  5.434415063 140.233.20.9  140.233.178.214 TCP 66  443     46130 [FIN,
   ACK] Seq=1874 Ack=2111 Win=33792 Len=0 TSval=2246153501 TSecr
   =2471071735
2 0.002094244 140.233.20.9  140.233.178.214 TCP 74  443     46130 [SYN,
   ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1386 SACK_PERM=1 TSval=2246148070
   TSecr=2471071263 WS=128
3 0.002112594 140.233.178.214 140.233.20.9  TCP 66  46130     443 [ACK]
   Seq=1 Ack=1 Win=64256 Len=0 TSval=2471071265 TSecr=2246148070
13  0.399422149 140.233.178.214 140.233.20.9  TCP 66  46130     443 [ACK]
   Seq=1133 Ack=707 Win=64128 Len=0 TSval=2471071663 TSecr=2246148466
16  0.414152971 140.233.178.214 140.233.20.9  TCP 66  46130     443 [ACK]
   Seq=1622 Ack=1275 Win=64128 Len=0 TSval=2471071677 TSecr=2246148481
```

```
19  0.471981825 140.233.178.214 140.233.20.9  TCP 66  46130     443 [ACK] Seq=2111 Ack=1843 Win=64128 Len=0 TSval=2471071735 TSecr=2246148496
24  5.434454789 140.233.178.214 140.233.20.9  TCP 66  46130     443 [ACK] Seq=2111 Ack=1874 Win=64128 Len=0 TSval=2471076698 TSecr=2246153501
7 0.012824280 140.233.178.214 140.233.20.9  TCP 66  46130     443 [ACK] Seq=593 Ack=138 Win=64128 Len=0 TSval=2471071276 TSecr=2246148080
26  5.434757656 140.233.178.214 140.233.20.9  TCP 66  46130     443 [FIN, ACK] Seq=2142 Ack=1875 Win=64128 Len=0 TSval=2471076698 TSecr=2246153501
1 0.000000000 140.233.178.214 140.233.20.9  TCP 74  46130     443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2471071263 TSecr=0 WS=128
20  0.502227792 140.233.178.214 52.85.61.69 TCP 66  60752     443 [ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=469967789 TSecr=3413959200
10  0.392070085 140.233.178.214 140.233.20.9  TLSv1.2 555 Application Data
14  0.409728184 140.233.178.214 140.233.20.9  TLSv1.2 555 Application Data
17  0.423513307 140.233.178.214 140.233.20.9  TLSv1.2 555 Application Data
12  0.399409232 140.233.20.9  140.233.178.214 TLSv1.2 635 Application Data, Application Data
15  0.414129999 140.233.20.9  140.233.178.214 TLSv1.2 634 Application Data, Application Data
18  0.430213625 140.233.20.9  140.233.178.214 TLSv1.2 634 Application Data, Application Data
8 0.013878129 140.233.178.214 140.233.20.9  TLSv1.2 117 Change Cipher Spec, Encrypted Handshake Message
4 0.009402882 140.233.178.214 140.233.20.9  TLSv1.2 658 Client Hello
22  5.434414636 140.233.20.9  140.233.178.214 TLSv1.2 97  Encrypted Alert
25  5.434724197 140.233.178.214 140.233.20.9  TLSv1.2 97  Encrypted Alert
6 0.012737109 140.233.20.9  140.233.178.214 TLSv1.2 203 Server Hello, Change Cipher Spec, Encrypted Handshake Message
21  0.516222911 52.85.61.69 140.233.178.214 TCP 66  [TCP ACKed unseen segment] 443     60752 [ACK] Seq=1 Ack=2 Win=133 Len=0 TSval=3413969227 TSecr=469877455
```

It switches automatically to secure messaging because the link we refreshed on firefox starts with https (https://www.cs.middlebury.edu/ pjohnson/courses/w22-1005/lectures/15/).

3 Manual HTTP (client

- To continue our theme of avoiding fancy programs that do all the work for us, use netcat (likely along with the sed trick above) to manually construct and send an HTTP request. Observe the traffic in Wireshark.

4 Manual HTTP (server)

- On the flip-side, set up netcat to behave as an HTTP server and point your browser at it (you can use an IP address instead of the hostname in the URL). Type random-ish responses to the browser, see how it responds.

5 Messing with TCP: sequence numbers

- Extend your Scapy-based TCP connection program from last week to mess with sequence numbers; see how the remote host responds. Try higher or lower than expected values; try much higher or lower than expected values. Record your results. Draw conclusions about how the TCP protocol is supposed to work.

6 Messing with TCP: timing

- Extend your Scapy-based TCP connection program from last week to delay expected responses such as ACKs; see how the remote host responds. Measure the behavior you see. Draw conclusions about how the TCP protocol is supposed to work.