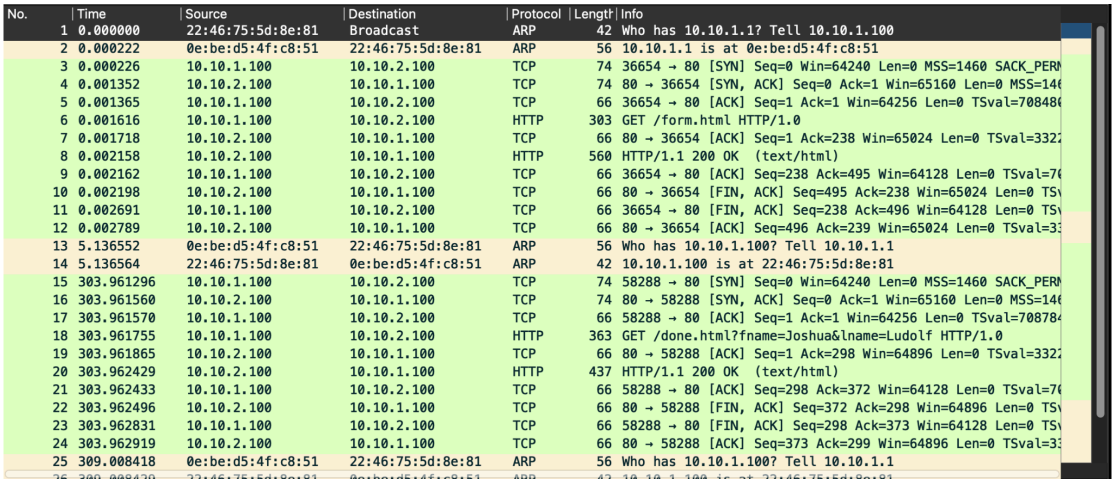
Samantha Jackson
CSCI4406
11-20-2024

CLab 10 - Secure Networked Applications Pt.2

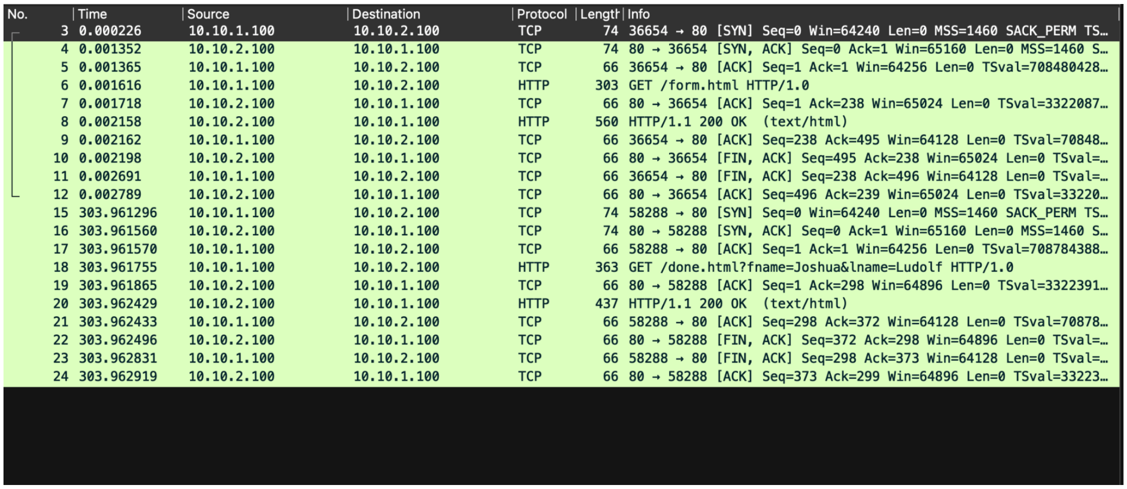
HTTP Traffic

Observations/Issues: Continuing from CLab9. No issues opening these working files so we should be good to start the analysis.



```
No.   Time        Source             Destination        Protocol Length Info
    1 0.000000    22:46:75:5d:8e:81  Broadcast          ARP        42 Who has 10.10.1.1? Tell 10.10.1.100
    2 0.000222    0e:be:d5:4f:c8:51  22:46:75:5d:8e:81  ARP        56 10.10.1.1 is at 0e:be:d5:4f:c8:51
    3 0.000226    10.10.1.100        10.10.2.100        TCP        74 36654 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
    4 0.001352    10.10.2.100        10.10.1.100        TCP        74 80 → 36654 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=146
    5 0.001365    10.10.1.100        10.10.2.100        TCP        66 36654 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=70848
    6 0.001616    10.10.1.100        10.10.2.100        HTTP      303 GET /form.html HTTP/1.0
    7 0.001718    10.10.2.100        10.10.1.100        TCP        66 80 → 36654 [ACK] Seq=1 Ack=238 Win=65024 Len=0 TSval=332
    8 0.002158    10.10.2.100        10.10.1.100        HTTP      560 HTTP/1.1 200 OK  (text/html)
    9 0.002162    10.10.1.100        10.10.2.100        TCP        66 36654 → 80 [ACK] Seq=238 Ack=495 Win=64128 Len=0 TSval=7
   10 0.002198    10.10.2.100        10.10.1.100        TCP        66 80 → 36654 [FIN, ACK] Seq=495 Ack=238 Win=65024 Len=0 TS
   11 0.002691    10.10.1.100        10.10.2.100        TCP        66 36654 → 80 [FIN, ACK] Seq=238 Ack=496 Win=64128 Len=0 TS
   12 0.002789    10.10.2.100        10.10.1.100        TCP        66 80 → 36654 [ACK] Seq=496 Ack=239 Win=65024 Len=0 TSval=33
   13 5.136552    0e:be:d5:4f:c8:51  22:46:75:5d:8e:81  ARP        56 Who has 10.10.1.100? Tell 10.10.1.1
   14 5.136564    22:46:75:5d:8e:81  0e:be:d5:4f:c8:51  ARP        42 10.10.1.100 is at 22:46:75:5d:8e:81
   15 303.961296  10.10.1.100        10.10.2.100        TCP        74 58288 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
   16 303.961560  10.10.2.100        10.10.1.100        TCP        74 80 → 58288 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=146
   17 303.961570  10.10.1.100        10.10.2.100        TCP        66 58288 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=70878
   18 303.961755  10.10.1.100        10.10.2.100        HTTP      363 GET /done.html?fname=Joshua&lname=Ludolf HTTP/1.0
   19 303.961865  10.10.2.100        10.10.1.100        TCP        66 80 → 58288 [ACK] Seq=1 Ack=298 Win=64896 Len=0 TSval=332
   20 303.962429  10.10.2.100        10.10.1.100        HTTP      437 HTTP/1.1 200 OK  (text/html)
   21 303.962433  10.10.1.100        10.10.2.100        TCP        66 58288 → 80 [ACK] Seq=298 Ack=372 Win=64128 Len=0 TSval=7
   22 303.962496  10.10.2.100        10.10.1.100        TCP        66 80 → 58288 [FIN, ACK] Seq=372 Ack=298 Win=64896 Len=0 TS
   23 303.962831  10.10.1.100        10.10.2.100        TCP        66 58288 → 80 [FIN, ACK] Seq=298 Ack=373 Win=64128 Len=0 TS
   24 303.962919  10.10.2.100        10.10.1.100        TCP        66 80 → 58288 [ACK] Seq=373 Ack=299 Win=64896 Len=0 TSval=33
   25 309.008418  0e:be:d5:4f:c8:51  22:46:75:5d:8e:81  ARP        56 Who has 10.10.1.100? Tell 10.10.1.1
   26 309.008429  22:46:75:5d:8e:81  0e:be:d5:4f:c8:51  ARP        42 10.10.1.100 is at 22:46:75:5d:8e:81
```

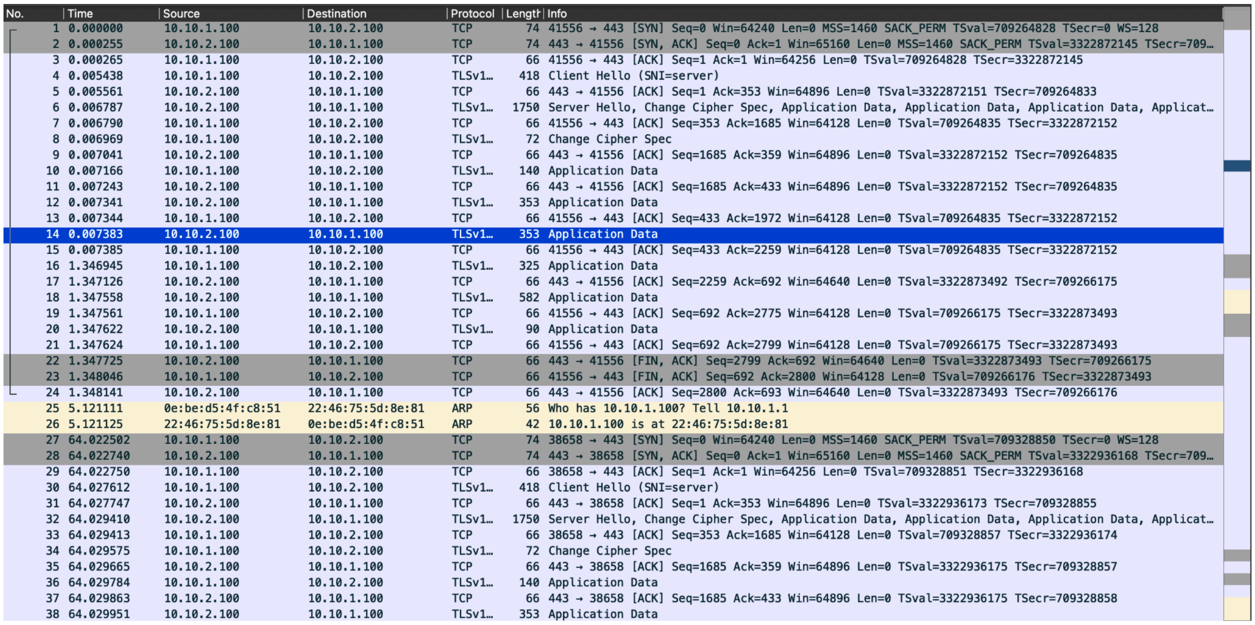
You can see that this HTTP/1.1 file contains three different protocols and 28 frames. ARP, TCP, and HTTP. HTTP is the unencrypted variant of HTTPS and is an older protocol by comparison. HTTP uses TCP as its transport protocol typically through port 80. You can see the filter 'tcp.port == 80' on this PCAP file. Much like the Telnet file you can see the open communication with the server with little to no obfuscation. This makes HTTP/1.1 text-based request-response client-server protocol particularly easy to intercept.



```
No.   Time        Source        Destination   Protocol Length Info
    3 0.000226    10.10.1.100   10.10.2.100   TCP        74 36654 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TS…
    4 0.001352    10.10.2.100   10.10.1.100   TCP        74 80 → 36654 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 S…
    5 0.001365    10.10.1.100   10.10.2.100   TCP        66 36654 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=708480428…
    6 0.001616    10.10.1.100   10.10.2.100   HTTP      303 GET /form.html HTTP/1.0
    7 0.001718    10.10.2.100   10.10.1.100   TCP        66 80 → 36654 [ACK] Seq=1 Ack=238 Win=65024 Len=0 TSval=3322087…
    8 0.002158    10.10.2.100   10.10.1.100   HTTP      560 HTTP/1.1 200 OK  (text/html)
    9 0.002162    10.10.1.100   10.10.2.100   TCP        66 36654 → 80 [ACK] Seq=238 Ack=495 Win=64128 Len=0 TSval=70848…
   10 0.002198    10.10.2.100   10.10.1.100   TCP        66 80 → 36654 [FIN, ACK] Seq=495 Ack=238 Win=65024 Len=0 TSval=…
   11 0.002691    10.10.1.100   10.10.2.100   TCP        66 36654 → 80 [FIN, ACK] Seq=238 Ack=496 Win=64128 Len=0 TSval=…
   12 0.002789    10.10.2.100   10.10.1.100   TCP        66 80 → 36654 [ACK] Seq=496 Ack=239 Win=65024 Len=0 TSval=33220…
   15 303.961296  10.10.1.100   10.10.2.100   TCP        74 58288 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TS…
   16 303.961560  10.10.2.100   10.10.1.100   TCP        74 80 → 58288 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 S…
   17 303.961570  10.10.1.100   10.10.2.100   TCP        66 58288 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=708784388…
   18 303.961755  10.10.1.100   10.10.2.100   HTTP      363 GET /done.html?fname=Joshua&lname=Ludolf HTTP/1.0
   19 303.961865  10.10.2.100   10.10.1.100   TCP        66 80 → 58288 [ACK] Seq=1 Ack=298 Win=64896 Len=0 TSval=3322391…
   20 303.962429  10.10.2.100   10.10.1.100   HTTP      437 HTTP/1.1 200 OK  (text/html)
   21 303.962433  10.10.1.100   10.10.2.100   TCP        66 58288 → 80 [ACK] Seq=298 Ack=372 Win=64128 Len=0 TSval=70878…
   22 303.962496  10.10.2.100   10.10.1.100   TCP        66 80 → 58288 [FIN, ACK] Seq=372 Ack=298 Win=64896 Len=0 TSval=…
   23 303.962831  10.10.1.100   10.10.2.100   TCP        66 58288 → 80 [FIN, ACK] Seq=298 Ack=373 Win=64128 Len=0 TSval=…
   24 303.962919  10.10.2.100   10.10.1.100   TCP        66 80 → 58288 [ACK] Seq=373 Ack=299 Win=64896 Len=0 TSval=33223…
```

HTTPS Traffic

Observations/Issues: No issues opening these working files so we should be good to start the analysis.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.10.1.100	10.10.2.100	TCP	74	41556 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=709264828 TSecr=0 WS=128
2	0.000255	10.10.2.100	10.10.1.100	TCP	74	443 → 41556 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=3322872145 TSecr=709…
3	0.000265	10.10.1.100	10.10.2.100	TCP	66	41556 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=709264828 TSecr=3322872145
4	0.005438	10.10.1.100	10.10.2.100	TLSv1…	418	Client Hello (SNI=server)
5	0.005561	10.10.2.100	10.10.1.100	TCP	66	443 → 41556 [ACK] Seq=1 Ack=353 Win=64896 Len=0 TSval=3322872151 TSecr=709264833
6	0.006787	10.10.2.100	10.10.1.100	TLSv1…	1750	Server Hello, Change Cipher Spec, Application Data, Application Data, Application Data, Applicat…
7	0.006790	10.10.1.100	10.10.2.100	TCP	66	41556 → 443 [ACK] Seq=353 Ack=1685 Win=64128 Len=0 TSval=709264835 TSecr=3322872152
8	0.006969	10.10.1.100	10.10.2.100	TLSv1…	72	Change Cipher Spec
9	0.007041	10.10.2.100	10.10.1.100	TCP	66	443 → 41556 [ACK] Seq=1685 Ack=359 Win=64896 Len=0 TSval=3322872152 TSecr=709264835
10	0.007166	10.10.1.100	10.10.2.100	TLSv1…	140	Application Data
11	0.007243	10.10.2.100	10.10.1.100	TCP	66	443 → 41556 [ACK] Seq=1685 Ack=433 Win=64896 Len=0 TSval=3322872152 TSecr=709264835
12	0.007341	10.10.2.100	10.10.1.100	TLSv1…	353	Application Data
13	0.007344	10.10.1.100	10.10.2.100	TCP	66	41556 → 443 [ACK] Seq=433 Ack=1972 Win=64128 Len=0 TSval=709264835 TSecr=3322872152
14	0.007383	10.10.2.100	10.10.1.100	TLSv1…	353	Application Data
15	0.007385	10.10.1.100	10.10.2.100	TCP	66	41556 → 443 [ACK] Seq=433 Ack=2259 Win=64128 Len=0 TSval=709264835 TSecr=3322872152
16	1.346945	10.10.1.100	10.10.2.100	TLSv1…	325	Application Data
17	1.347126	10.10.2.100	10.10.1.100	TCP	66	443 → 41556 [ACK] Seq=2259 Ack=692 Win=64640 Len=0 TSval=3322873492 TSecr=709266175
18	1.347558	10.10.2.100	10.10.1.100	TLSv1…	582	Application Data
19	1.347561	10.10.1.100	10.10.2.100	TCP	66	41556 → 443 [ACK] Seq=692 Ack=2775 Win=64128 Len=0 TSval=709266175 TSecr=3322873493
20	1.347622	10.10.2.100	10.10.1.100	TLSv1…	90	Application Data
21	1.347624	10.10.1.100	10.10.2.100	TCP	66	41556 → 443 [ACK] Seq=692 Ack=2799 Win=64128 Len=0 TSval=709266175 TSecr=3322873493
22	1.347725	10.10.2.100	10.10.1.100	TCP	66	443 → 41556 [FIN, ACK] Seq=2799 Ack=692 Win=64640 Len=0 TSval=3322873493 TSecr=709266175
23	1.348046	10.10.1.100	10.10.2.100	TCP	66	41556 → 443 [FIN, ACK] Seq=692 Ack=2800 Win=64128 Len=0 TSval=709266176 TSecr=3322873493
24	1.348141	10.10.2.100	10.10.1.100	TCP	66	443 → 41556 [ACK] Seq=2800 Ack=693 Win=64640 Len=0 TSval=3322873493 TSecr=709266176
25	5.121111	0e:be:d5:4f:c8:51	22:46:75:5d:8e:81	ARP	56	Who has 10.10.1.100? Tell 10.10.1.1
26	5.121125	22:46:75:5d:8e:81	0e:be:d5:4f:c8:51	ARP	42	10.10.1.100 is at 22:46:75:5d:8e:81
27	64.022502	10.10.1.100	10.10.2.100	TCP	74	38658 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=709328850 TSecr=0 WS=128
28	64.022740	10.10.2.100	10.10.1.100	TCP	74	443 → 38658 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=3322936168 TSecr=709…
29	64.022750	10.10.1.100	10.10.2.100	TCP	66	38658 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=709328851 TSecr=3322936168
30	64.027612	10.10.1.100	10.10.2.100	TLSv1…	418	Client Hello (SNI=server)
31	64.027747	10.10.2.100	10.10.1.100	TCP	66	443 → 38658 [ACK] Seq=1 Ack=353 Win=64896 Len=0 TSval=3322936173 TSecr=709328855
32	64.029410	10.10.2.100	10.10.1.100	TLSv1…	1750	Server Hello, Change Cipher Spec, Application Data, Application Data, Application Data, Applicat…
33	64.029413	10.10.1.100	10.10.2.100	TCP	66	38658 → 443 [ACK] Seq=353 Ack=1685 Win=64128 Len=0 TSval=709328857 TSecr=3322936174
34	64.029575	10.10.1.100	10.10.2.100	TLSv1…	72	Change Cipher Spec
35	64.029665	10.10.2.100	10.10.1.100	TCP	66	443 → 38658 [ACK] Seq=1685 Ack=359 Win=64896 Len=0 TSval=3322936175 TSecr=709328857
36	64.029784	10.10.1.100	10.10.2.100	TLSv1…	140	Application Data
37	64.029863	10.10.2.100	10.10.1.100	TCP	66	443 → 38658 [ACK] Seq=1685 Ack=433 Win=64896 Len=0 TSval=3322936175 TSecr=709328858
38	64.029951	10.10.2.100	10.10.1.100	TLSv1…	353	Application Data

You can see that this HTTPS file contains 52 frames and three protocols. TLSv1, TCP, and ARP. HTTPS is the encrypted variant of HTTP and is a newer protocol. The encryption in HTTPS is thanks to TLSv1 (Transport Layer Security) which encrypts the data between servers, applications, users and systems. This makes it particularly valuable over public networks protecting it from man in the middle attacks.

HTTPS is significantly more secure than HTTP. HTTP messages are in plaintext compared to HTTPS encrypted text. Over insecure networks HTTPS is incredibly valuable in ensuring user and server security. The large majority of websites run HTTPS making them significantly more resistant to threat actors compared to HTTP.