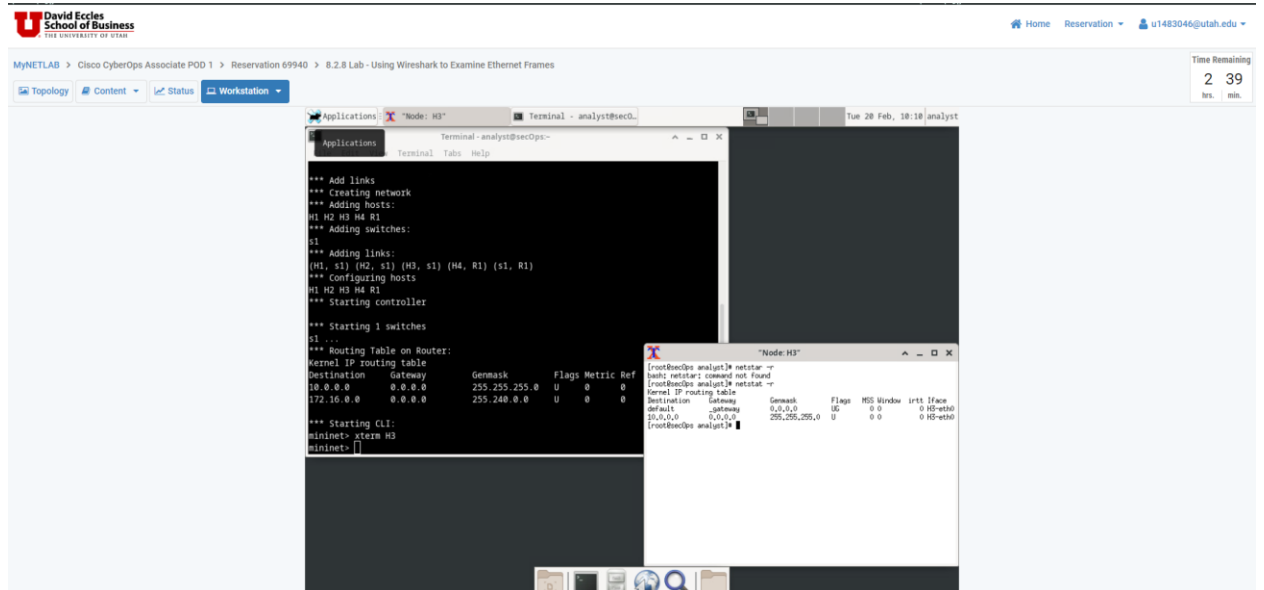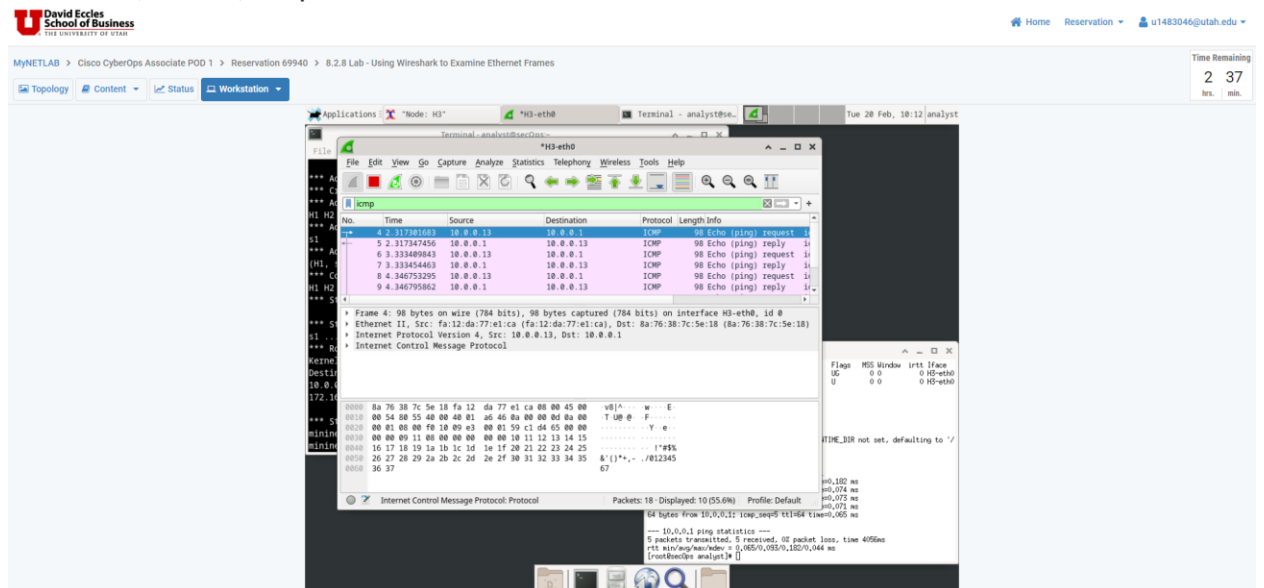Vu Nguyen

UID: u1483046

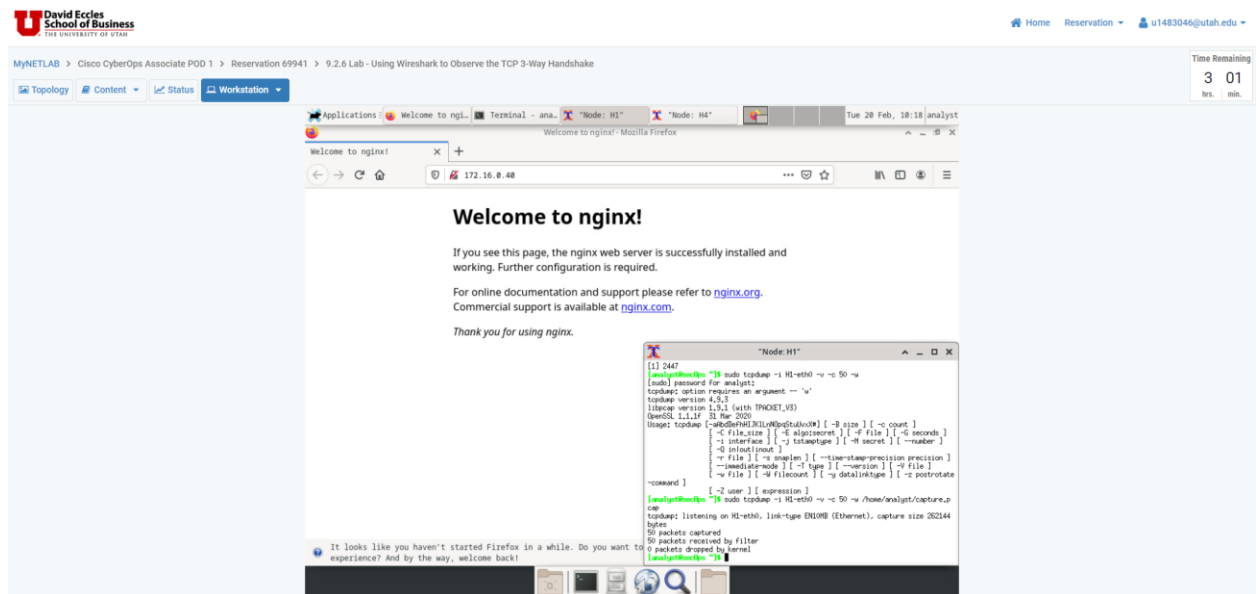# Assignment 21 - Using Wireshark (Lab and Quiz)

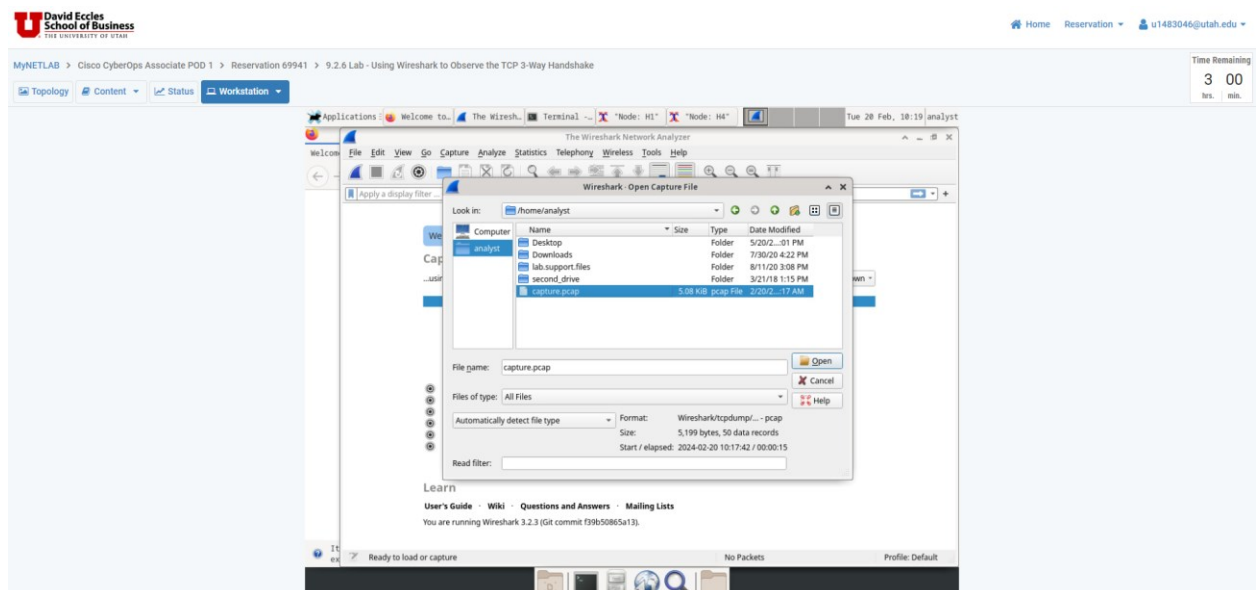1. Lab 8.2.8, Part 2, Step 1e (Node: H3):

2. Lab 8.2.8, Part 2, Step 4:

3. Lab 9.2.6, Part 1, Step 1g (Noe: H1):

4. Lab 9.2.6, Part 2, Step 1a&b:

5. Lab 9.2.6, Part 2, Step 1c (after applying the tcp filter it may be empty and you may have to repeat this step as indicated in Step 1c):

Home   Reservation ▾   u1483046@utah.edu ▾

MyNETLAB > Cisco CyberOps Associate POD 1 > Reservation 69941 > 9.2.6 Lab - Using Wireshark to Observe the TCP 3-Way Handshake

Time Remaini

2   55
hrs.   min.

Topology   Content ▾   Status   Workstation ▾

Applications   Welcome to..   capture.pc..   Terminal -...   "Node: H1"   "Node: H4"   Tue 20 Feb, 10:24 analyst

Welcome to nginx! - Mozilla Firefox

capture.pcap

Welc

Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
35	9.174020	172.16.0.40	10.0.0.11	HTTP	246	HTTP/1.1 304 Not Modified
36	9.174111	10.0.0.11	172.16.0.40	TCP	66	43996 → 80 [ACK] Seq=875 Ack=361 Win=42496 Len
37	9.354235	10.0.0.11	172.16.0.40	HTTP	503	GET / HTTP/1.1
38	9.354265	172.16.0.40	10.0.0.11	TCP	66	80 → 43996 [ACK] Seq=361 Ack=1312 Win=43008 Len
39	9.354326	172.16.0.40	10.0.0.11	HTTP	246	HTTP/1.1 304 Not Modified
40	9.354358	10.0.0.11	172.16.0.40	TCP	66	43996 → 80 [ACK] Seq=1312 Ack=541 Win=42496 Len
41	9.535299	10.0.0.11	172.16.0.40	HTTP	503	GET / HTTP/1.1
42	9.535326	172.16.0.40	10.0.0.11	TCP	66	80 → 43996 [ACK] Seq=541 Ack=1749 Win=43008 Len
43	9.535382	172.16.0.40	10.0.0.11	HTTP	246	HTTP/1.1 304 Not Modified
44	9.535410	10.0.0.11	172.16.0.40	TCP	66	43996 → 80 [ACK] Seq=1749 Ack=721 Win=42496 Len

▸ Frame 39: 246 bytes on wire (1968 bits), 246 bytes captured (1968 bits)
▸ Ethernet II, Src: 2e:74:ac:fc:f0:be (2e:74:ac:fc:f0:be), Dst: 92:95:59:b8:07:0d (92:95:59:b8:07:0d)
▸ Internet Protocol Version 4, Src: 172.16.0.40, Dst: 10.0.0.11
▾ Transmission Control Protocol, Src Port: 80, Dst Port: 43996, Seq: 361, Ack: 1312, Len: 180
    Source Port: 80
    Destination Port: 43996
    [Stream index: 0]
    [TCP Segment Len: 180]
    Sequence number: 361   (relative sequence number)
    Sequence number (raw): 2991904523
    [Next sequence number: 541   (relative sequence number)]
    Acknowledgment number: 1312   (relative ack number)

```
0000  92 95 59 b8 07 0d 2e 74  ac fc f0 be 08 00 45 00   ··Y····t ······E·
0010  00 e8 08 7c 40 00 3f 06  7c 51 ac 10 00 28 0a 00   ···|@·?· |Q···(··
0020  00 0b 00 50 ab dc b2 54  d7 0b a5 89 75 59 80 18   ···P···T ····uY··
0030  00 54 b7 1d 00 00 01 01  08 0a 35 fc 39 0f b7 71   ·T······ ··5·9··q
0040  f1 72 48 54 54 50 2f 31  2e 31 20 33 30 34 20 4e   ·rHTTP/1 .1 304 N
0050  6f 74 20 4d 6f 64 69 66  69 65 64 0d 0a 53 65 72   ot Modif ied··Ser
```

capture.pcap   Packets: 100 · Displayed: 69 (69.0%)   Profile: Default

It
ex