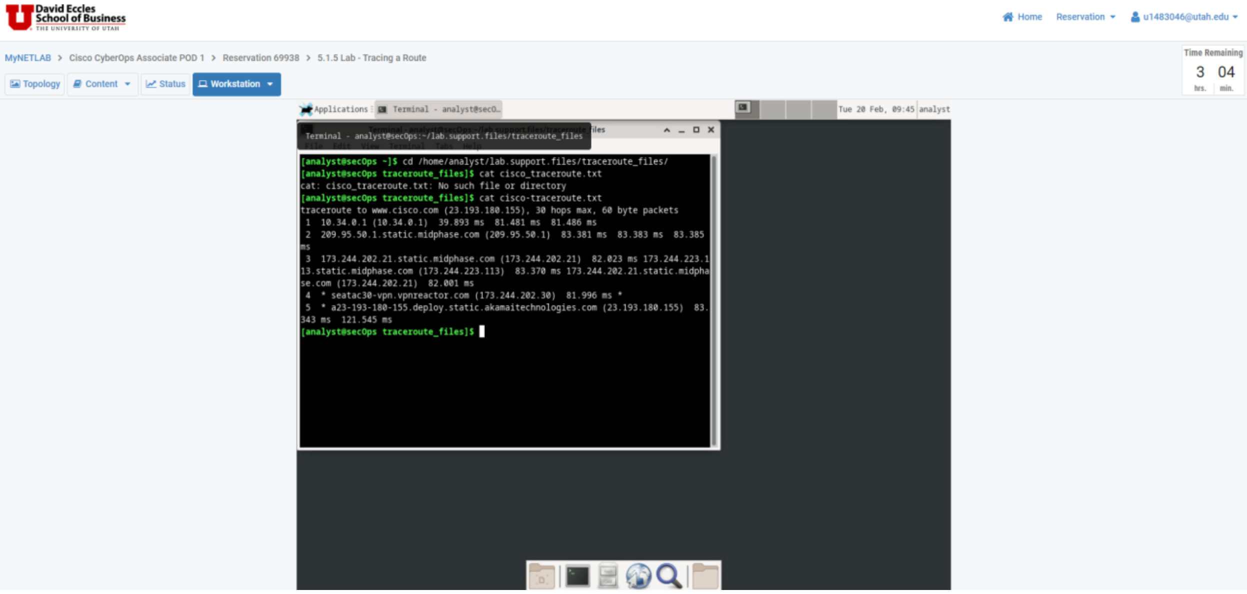
Vu Nguyen

UID: u1483046

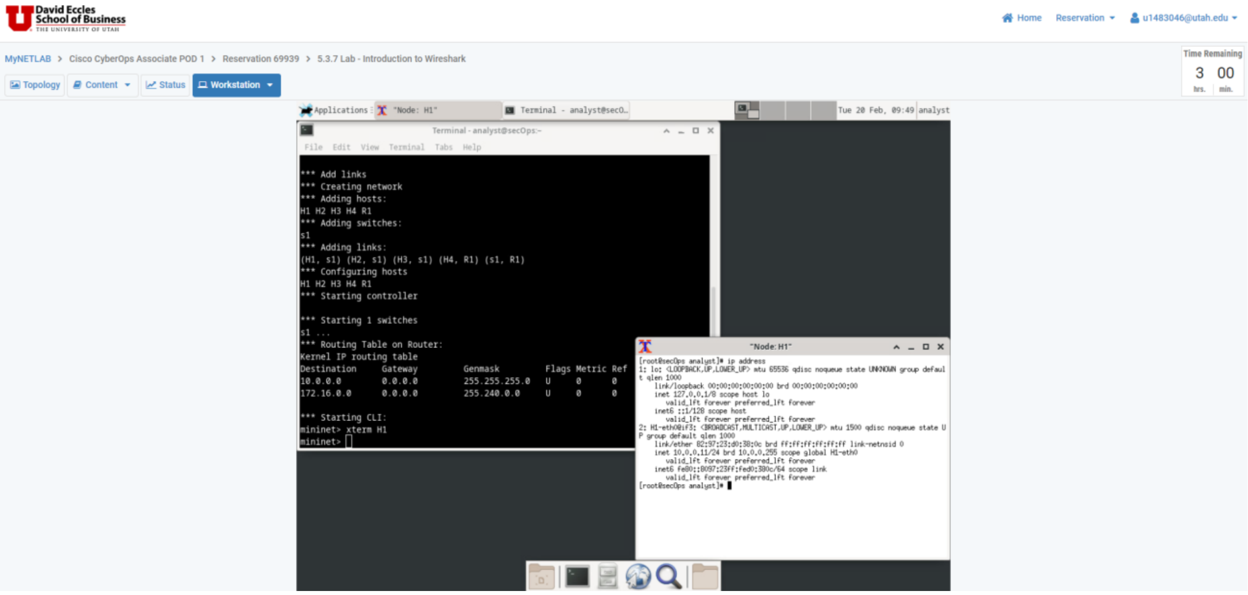
Assignment 20 - Traceroute and Wireshark (Lab and Quiz)

1. Lab 5.1.5, Part 1, Step 1c:


David Eccles School of Business
THE UNIVERSITY OF UTAH
Home
Reservation
u1483046@utah.edu
MyNETLAB > Cisco CyberOps Associate POD 1 > Reservation 69938 > 5.1.5 Lab - Tracing a Route
Topology
Content
Status
Workstation
Time Remaining
3 04
hrs. min.
Applications
Terminal - analyst@secO…
Tue 20 Feb, 09:45
analyst
Terminal - analyst@secOps:~/lab.support.files/traceroute_files

```
[analyst@secOps ~]$ cd /home/analyst/lab.support.files/traceroute_files/
[analyst@secOps traceroute_files]$ cat cisco_traceroute.txt
cat: cisco_traceroute.txt: No such file or directory
[analyst@secOps traceroute_files]$ cat cisco-traceroute.txt
traceroute to www.cisco.com (23.193.180.155), 30 hops max, 60 byte packets
 1  10.34.0.1 (10.34.0.1)  39.893 ms  81.481 ms  81.486 ms
 2  209.95.50.1.static.midphase.com (209.95.50.1)  83.381 ms  83.383 ms  83.385
ms
 3  173.244.202.21.static.midphase.com (173.244.202.21)  82.023 ms 173.244.223.1
13.static.midphase.com (173.244.223.113)  83.370 ms 173.244.202.21.static.midpha
se.com (173.244.202.21)  82.001 ms
 4  * seatac30-vpn.vpnreactor.com (173.244.202.30)  81.996 ms *
 5  * a23-193-180-155.deploy.static.akamaitechnologies.com (23.193.180.155)  83.
343 ms  121.545 ms
[analyst@secOps traceroute_files]$ 
```

2. Lab 5.3.7, Part 1, Step 3b (Node: H1):

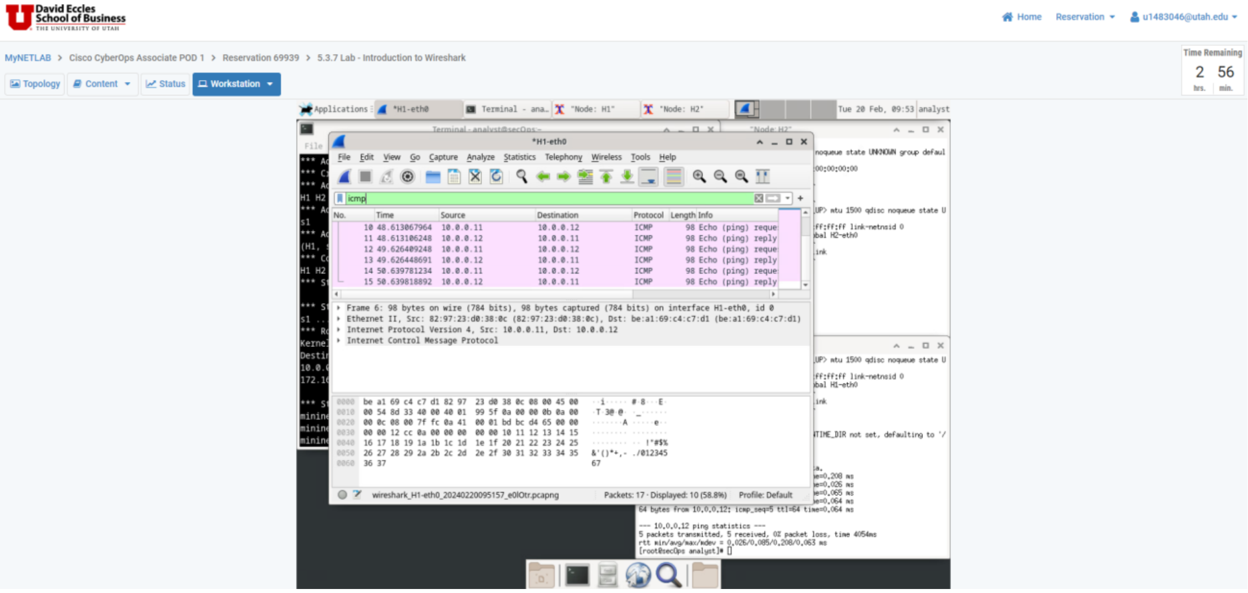

MyNETLAB > Cisco CyberOps Associate POD 1 > Reservation 69939 > 5.3.7 Lab - Introduction to Wireshark
Home
Reservation
u1483046@utah.edu
Topology
Content
Status
Workstation
Time Remaining 3 hrs. 00 min.
Applications
"Node: H1"
Terminal - analyst@secO…
Tue 20 Feb, 09:49
analyst
Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help

```
*** Add links
*** Creating network
*** Adding hosts:
H1 H2 H3 H4 R1
*** Adding switches:
s1
*** Adding links:
(H1, s1) (H2, s1) (H3, s1) (H4, R1) (s1, R1)
*** Configuring hosts
H1 H2 H3 H4 R1
*** Starting controller

*** Starting 1 switches
s1 ...
*** Routing Table on Router:
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref
10.0.0.0        0.0.0.0         255.255.255.0   U     0      0
172.16.0.0      0.0.0.0         255.240.0.0     U     0      0

*** Starting CLI:
mininet> xterm H1
mininet> 
```

"Node: H1"

```
[root@secOps analyst]# ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: H1-eth0@if3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state U
P group default qlen 1000
    link/ether 82:97:23:d0:38:0c brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.0.0.11/24 brd 10.0.0.255 scope global H1-eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::8097:23ff:fed0:380c/64 scope link
       valid_lft forever preferred_lft forever
[root@secOps analyst]# 
```

3. Lab 5.3.7, Part 2, Step 1f:


MyNETLAB > Cisco CyberOps Associate POD 1 > Reservation 69939 > 5.3.7 Lab - Introduction to Wireshark
Home
Reservation
u1483046@utah.edu
Topology
Content
Status
Workstation
Time Remaining 2 hrs. 56 min.
Applications
*H1-eth0
Terminal - ana…
"Node: H1"
"Node: H2"
Tue 20 Feb, 09:53
analyst
*H1-eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

```
No.  Time          Source      Destination  Protocol Length Info
  10 48.613067964  10.0.0.11   10.0.0.12    ICMP       98 Echo (ping) reque
  11 48.613106248  10.0.0.12   10.0.0.11    ICMP       98 Echo (ping) reply
  12 49.626409248  10.0.0.11   10.0.0.12    ICMP       98 Echo (ping) reque
  13 49.626448691  10.0.0.12   10.0.0.11    ICMP       98 Echo (ping) reply
  14 50.639781234  10.0.0.11   10.0.0.12    ICMP       98 Echo (ping) reque
  15 50.639818892  10.0.0.12   10.0.0.11    ICMP       98 Echo (ping) reply
```

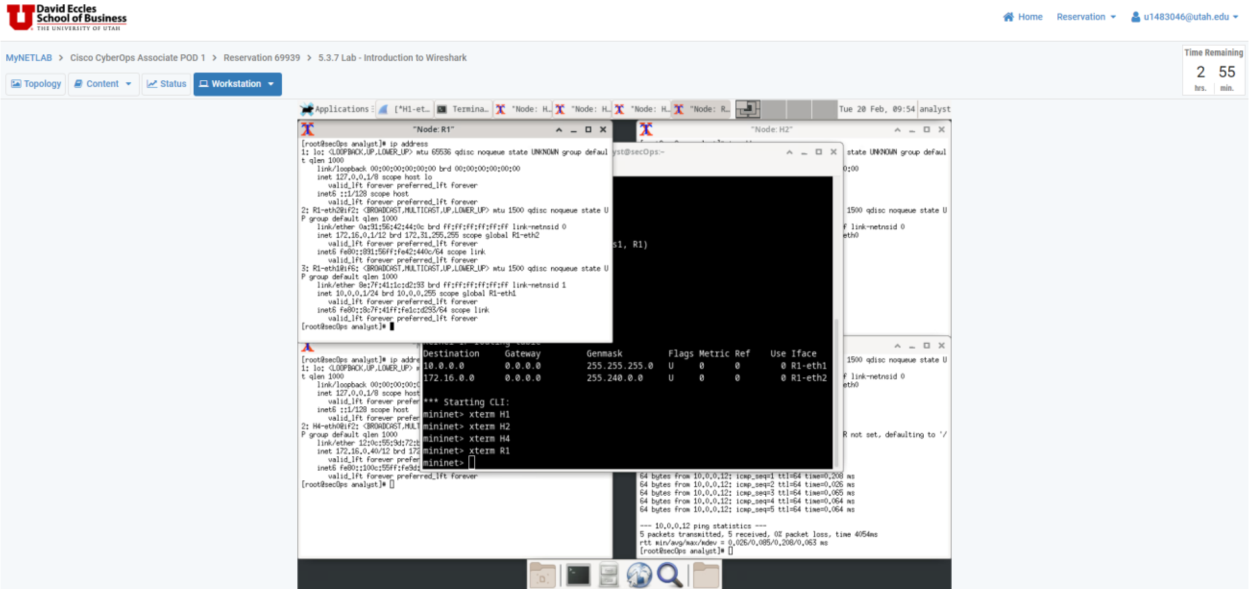
```
▸ Frame 6: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface H1-eth0, id 0
▸ Ethernet II, Src: 82:97:23:d0:38:0c (82:97:23:d0:38:0c), Dst: be:a1:69:c4:c7:d1 (be:a1:69:c4:c7:d1)
▸ Internet Protocol Version 4, Src: 10.0.0.11, Dst: 10.0.0.12
▸ Internet Control Message Protocol
```

```
0000  be a1 69 c4 c7 d1 82 97  23 d0 38 0c 08 00 45 00   ··i····· #·8···E·
0010  00 54 8d 33 40 00 40 01  99 5f 0a 00 00 0b 0a 00   ·T·3@·@· ·_······
0020  00 0c 08 00 7f fc 0a 41  00 01 bd bc d4 65 00 00   ·······A ·····e··
0030  00 00 12 cc 0a 00 00 00  00 00 10 11 12 13 14 15   ········ ········
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ········ ·· !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345
0060  36 37                                              67
```

wireshark_H1-eth0_20240220095157_e0lOtr.pcapng   Packets: 17 · Displayed: 10 (58.8%)   Profile: Default

```
64 bytes from 10.0.0.12: icmp_seq=5 ttl=64 time=0.064 ms

--- 10.0.0.12 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4054ms
rtt min/avg/max/mdev = 0.026/0.085/0.208/0.063 ms
[root@secOps analyst]# 
```

4. Lab 5.3.7, Part 2, Step 2b (Node: R1):



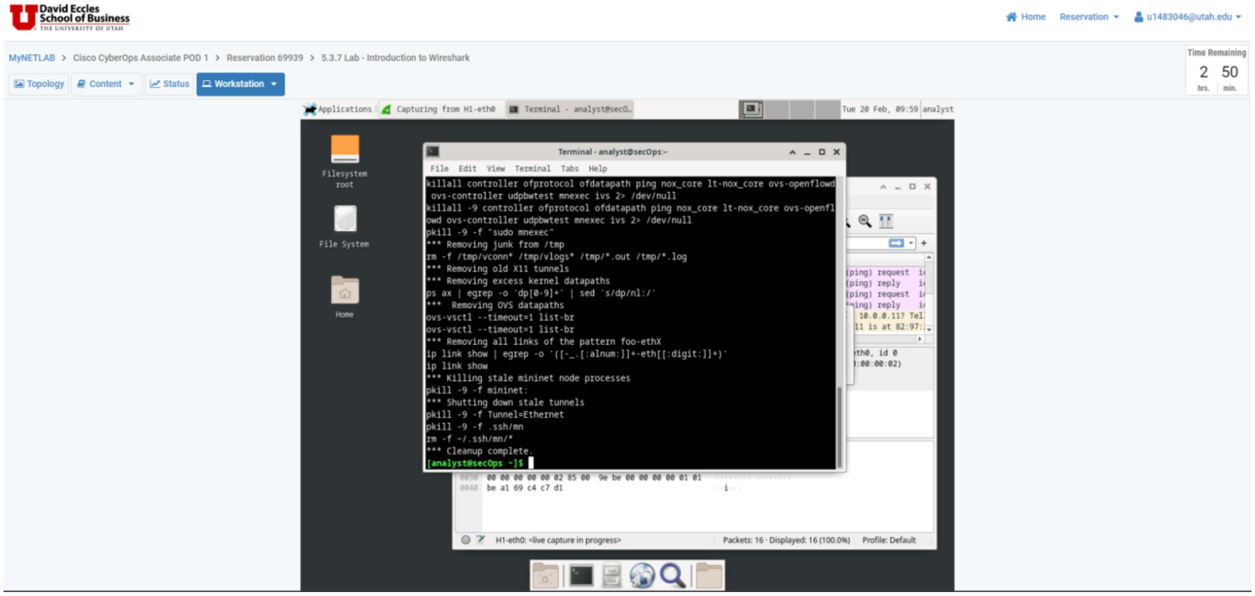
MyNETLAB > Cisco CyberOps Associate POD 1 > Reservation 69939 > 5.3.7 Lab - Introduction to Wireshark
Home
Reservation
u1483046@utah.edu
Time Remaining 2 hrs. 55 min.
Topology
Content
Status
Workstation
Tue 20 Feb, 09:54 analyst
"Node: R1"
"Node: H2"

```
[root@secOps analyst]# ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: R1-eth2@if2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state U
P group default qlen 1000
    link/ether 0a:91:56:42:44:0c brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 172.16.0.1/12 brd 172.31.255.255 scope global R1-eth2
       valid_lft forever preferred_lft forever
    inet6 fe80::891:56ff:fe42:440c/64 scope link
       valid_lft forever preferred_lft forever
3: R1-eth1@if6: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state U
P group default qlen 1000
    link/ether 8e:7f:41:1c:d2:93 brd ff:ff:ff:ff:ff:ff link-netnsid 1
    inet 10.0.0.1/24 brd 10.0.0.255 scope global R1-eth1
       valid_lft forever preferred_lft forever
    inet6 fe80::8c7f:41ff:fe1c:d293/64 scope link
       valid_lft forever preferred_lft forever
[root@secOps analyst]#
```

```
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
10.0.0.0        0.0.0.0         255.255.255.0   U     0      0        0 R1-eth1
172.16.0.0      0.0.0.0         255.240.0.0     U     0      0        0 R1-eth2

*** Starting CLI:
mininet> xterm H1
mininet> xterm H2
mininet> xterm H4
mininet> xterm R1
mininet>
```

```
64 bytes from 10.0.0.12: icmp_seq=1 ttl=64 time=0.208 ms
64 bytes from 10.0.0.12: icmp_seq=2 ttl=64 time=0.026 ms
64 bytes from 10.0.0.12: icmp_seq=3 ttl=64 time=0.065 ms
64 bytes from 10.0.0.12: icmp_seq=4 ttl=64 time=0.064 ms
64 bytes from 10.0.0.12: icmp_seq=5 ttl=64 time=0.064 ms

--- 10.0.0.12 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4054ms
rtt min/avg/max/mdev = 0.026/0.085/0.208/0.063 ms
[root@secOps analyst]#
```

5. Lab 5.3.7, Part 2, Step 2g:



MyNETLAB > Cisco CyberOps Associate POD 1 > Reservation 69939 > 5.3.7 Lab - Introduction to Wireshark
Home
Reservation
u1483046@utah.edu
Time Remaining 2 hrs. 50 min.
Topology
Content
Status
Workstation
Applications
Capturing from H1-eth0
Terminal - analyst@secO...
Tue 20 Feb, 09:59 analyst
Filesystem root
File System
Home
Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help
H1-eth0: <live capture in progress>
Packets: 16 · Displayed: 16 (100.0%)
Profile: Default

```
killall controller ofprotocol ofdatapath ping nox_core lt-nox_core ovs-openflowd
 ovs-controller udpbwtest mnexec ivs 2> /dev/null
killall -9 controller ofprotocol ofdatapath ping nox_core lt-nox_core ovs-openfl
owd ovs-controller udpbwtest mnexec ivs 2> /dev/null
pkill -9 -f "sudo mnexec"
*** Removing junk from /tmp
rm -f /tmp/vconn* /tmp/vlogs* /tmp/*.out /tmp/*.log
*** Removing old X11 tunnels
*** Removing excess kernel datapaths
ps ax | egrep -o 'dp[0-9]+' | sed 's/dp/nl:/'
***  Removing OVS datapaths
ovs-vsctl --timeout=1 list-br
ovs-vsctl --timeout=1 list-br
*** Removing all links of the pattern foo-ethX
ip link show | egrep -o '([-_.[:alnum:]]+-eth[[:digit:]]+)'
ip link show
*** Killing stale mininet node processes
pkill -9 -f mininet:
*** Shutting down stale tunnels
pkill -9 -f Tunnel=Ethernet
pkill -9 -f .ssh/mn
rm -f ~/.ssh/mn/*
*** Cleanup complete.
[analyst@secOps ~]$
```

```
0030  00 00 00 00 00 02 85 00  9e be 00 00 00 00 01 01
0040  be a1 69 c4 c7 d1                                   ··i···
```