Kenneth Aidoo

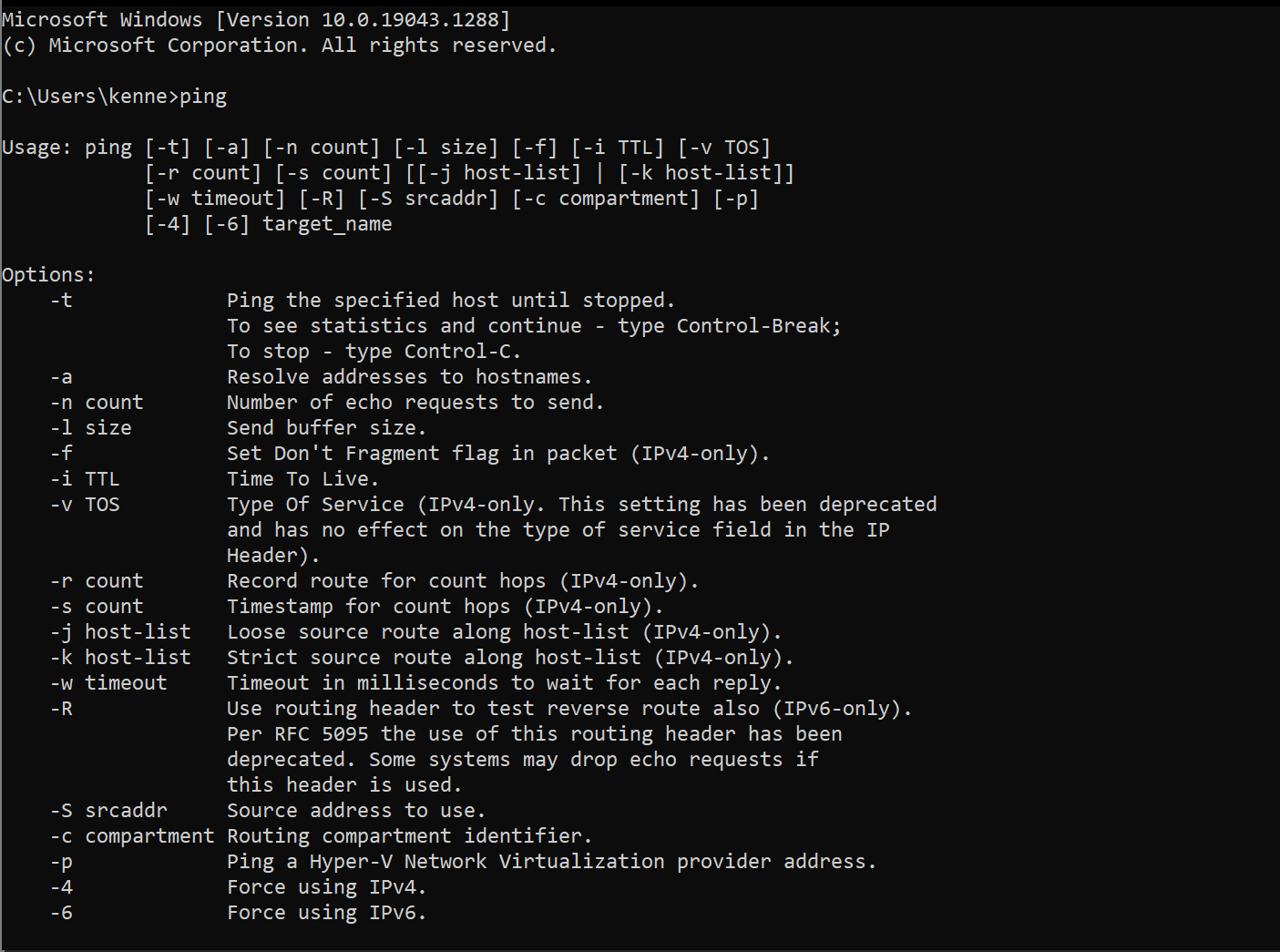
251129019

2021-11-08

**Lab # 2: DNS and Mininet Lab**

**Task 1**

**Q1. List a few flags that are used with the ping command.**



Some useful flags for the ping command are:

-t: pings the specified host until stopped

-n count: specifies the number of echo requests to send

-l size: send buffer size for ping

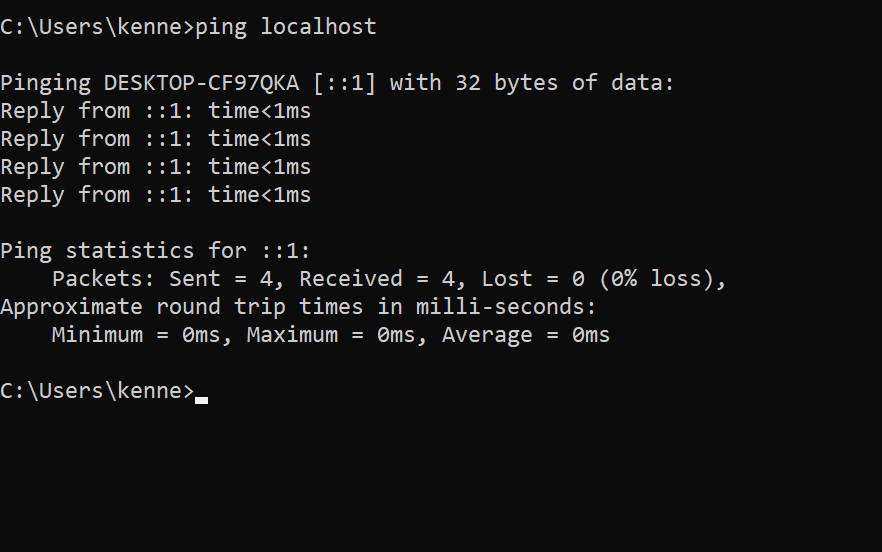
-S srcaddr: specifies the sources addressed to be used in the ping

-W: Set time and wait

-4: Force using IPv4

-6: Force using IPv6

**Q2. Ping your workstation’s loopback interface (localhost). What command did you use? Was the ping successful? If the ping is successful, then TCP/IP is properly installed and functioning on this workstation**

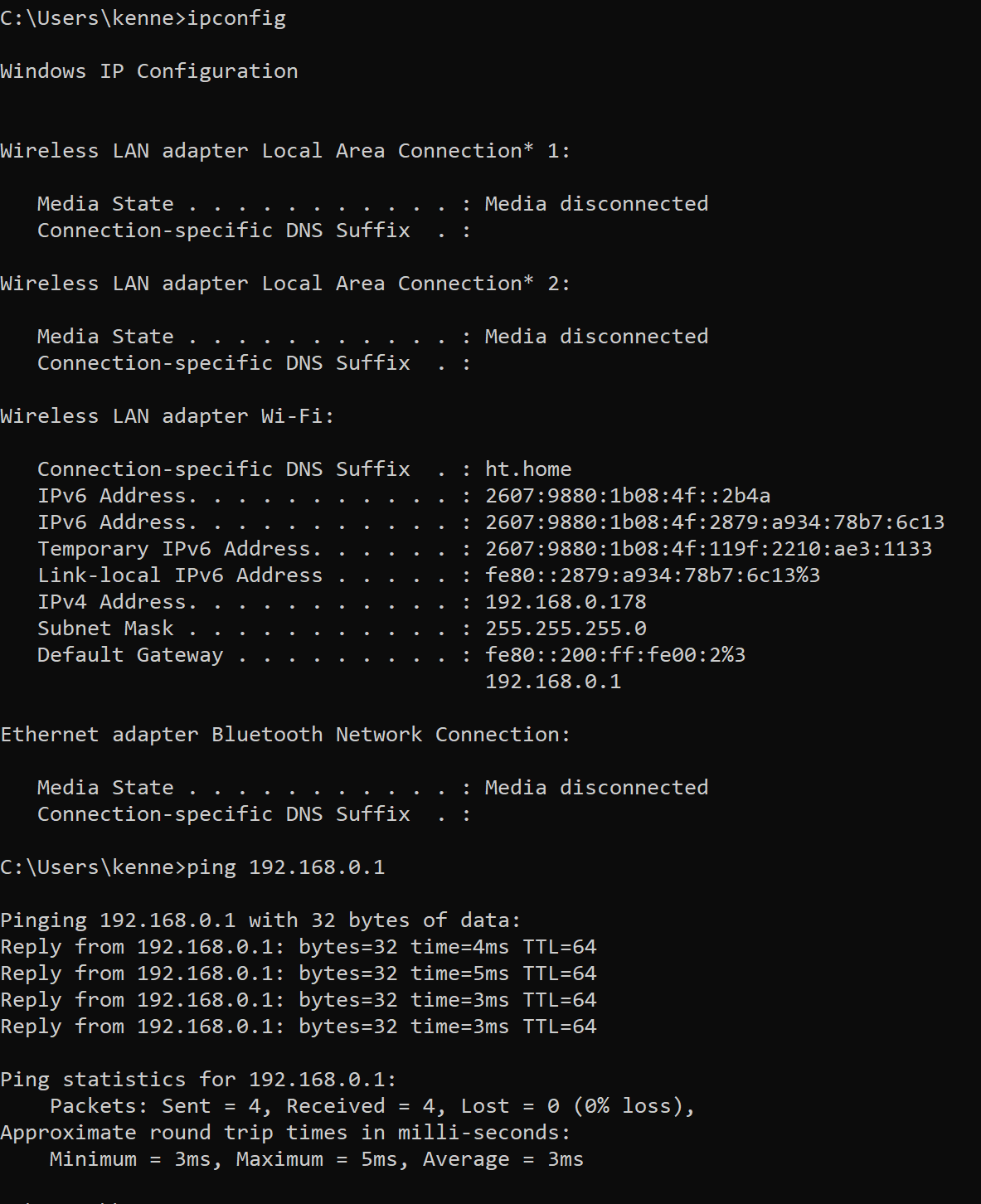


I used the following command: ping localhost

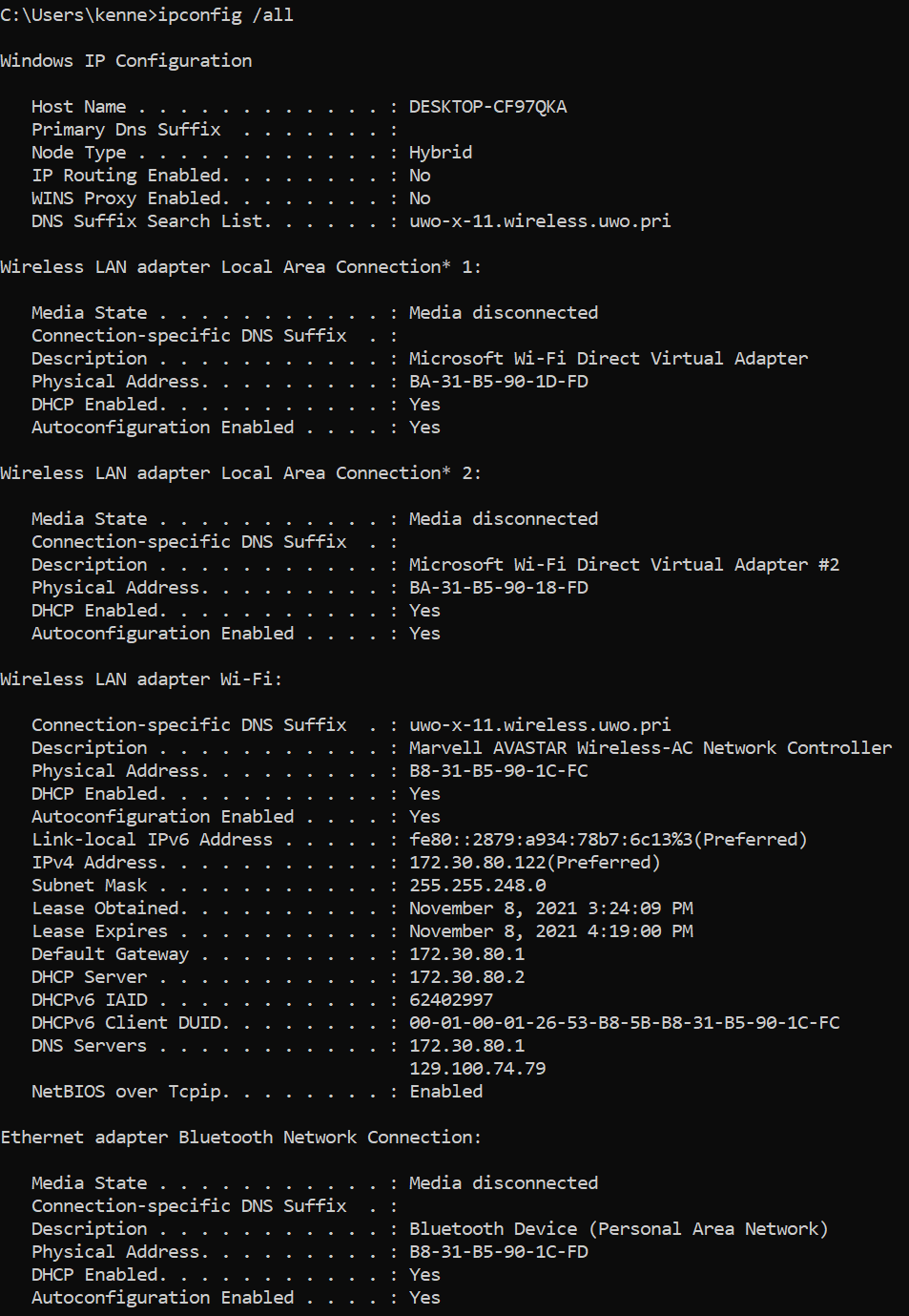
The ping was successful as all 4 packets were sent and received.

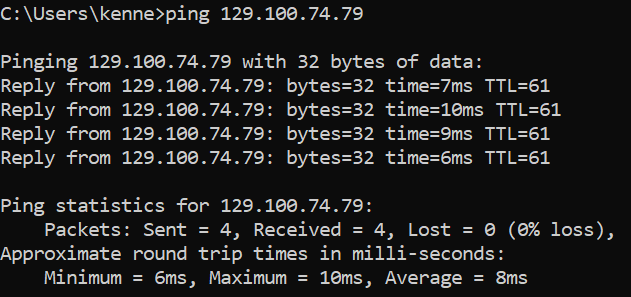
**Q3. Use the ipconfig command to determine the address of your DNS server and the IP address of the default gateway and ping them. [6 Marks]**

*Pinging Default Gateway (192.168.0.1)*

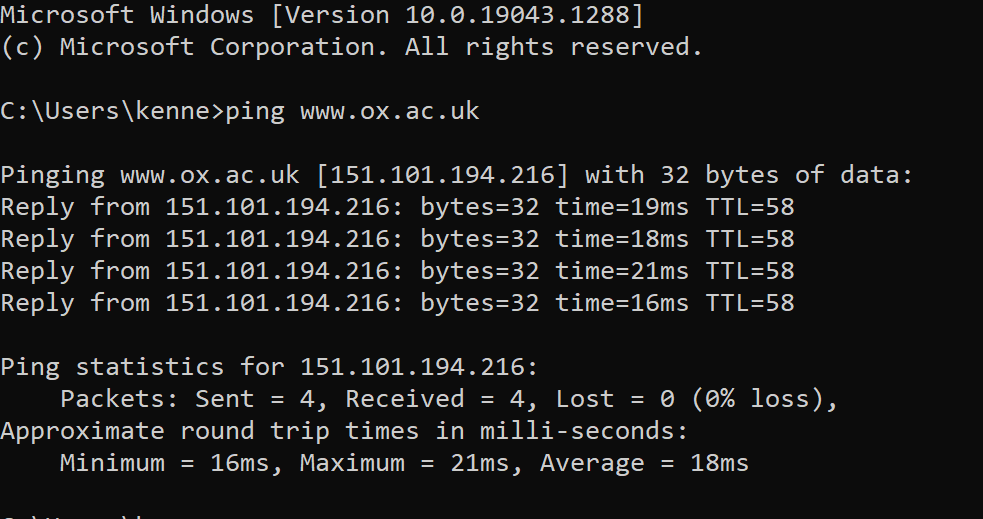


*Pinging DNS Server (129.100.74.79)*





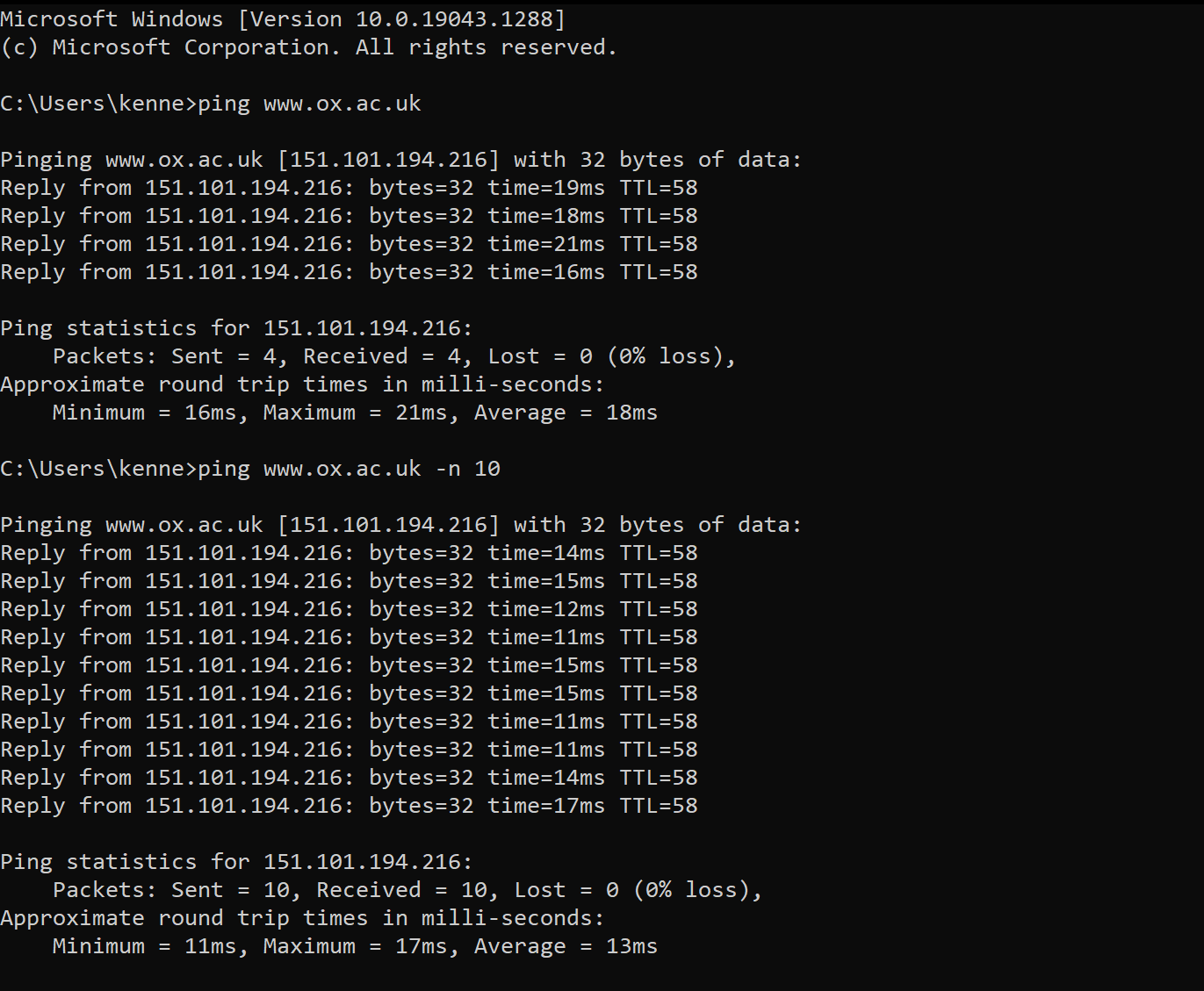
**Q4. Ping www.ox.ac.uk (Oxford University). What is the IP address you pinged? Was the ping successful? Please list the maximum, minimum, and average roundtrip times.**



Maximum: 21ms, Minimum: 16ms, Average = 18ms

The IP address that was pinged is 151.101.194.216

**Q5. Repeat the steps from Q4 but this time ping www.ox.ac.uk 10 times (hint: use the -n flag). Please list the maximum, minimum and average roundtrip times from this exercise. Do the results differ than those in Q4?**

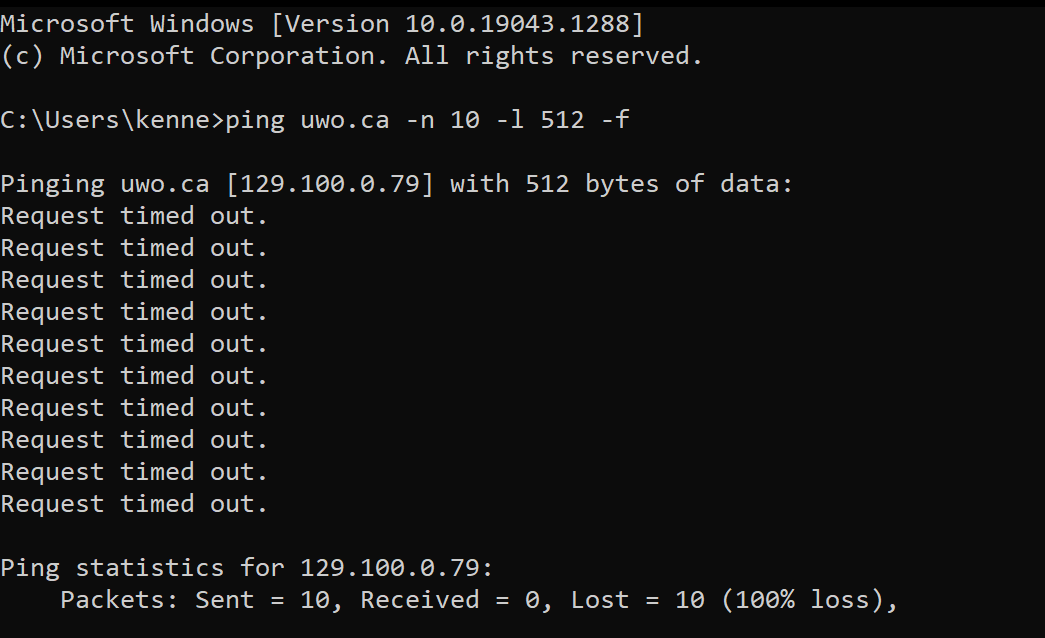


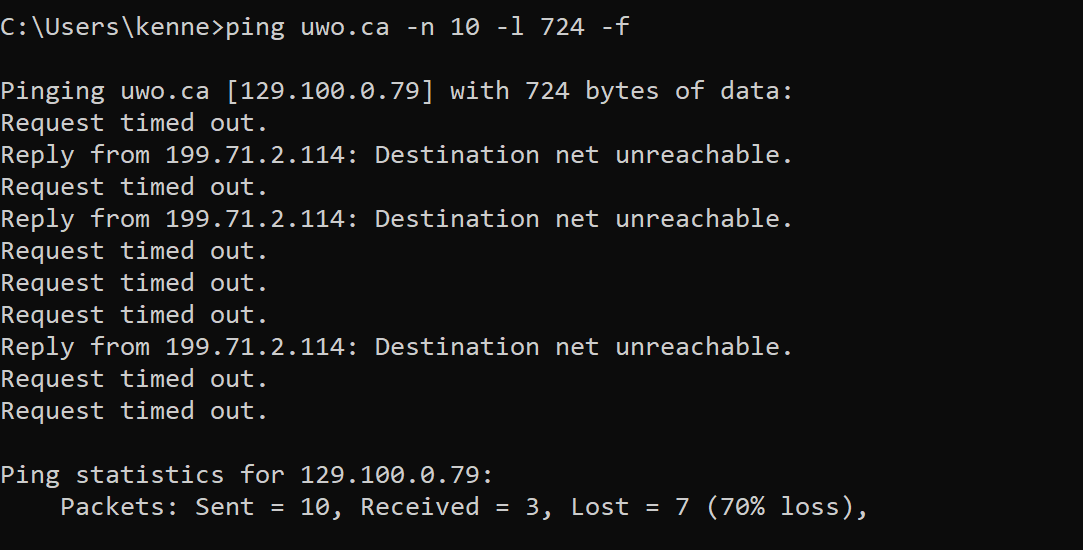
Maximum = 17ms; Minimum = 11ms; Average = 13ms;

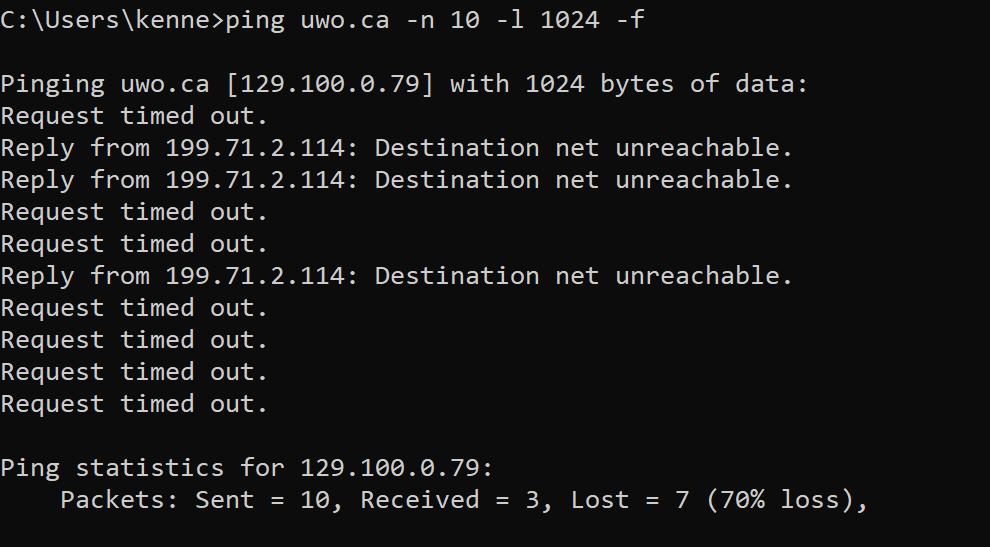
The results from Q5 are very similar to those from Q4, although the maximum, minimum and the average time are slightly lower.

**Q6. Use ping to measure Round Trip Time (RTT) for 10 messages of size 512, 724, 1024, and 4072 bytes for the following. Use the "-f" configuration switch to make sure that the message is not fragmented. Analyze your results. Calculate the average and standard deviation for every destination. State any observations or trends you see.**

1. **pinging uwo.ca**

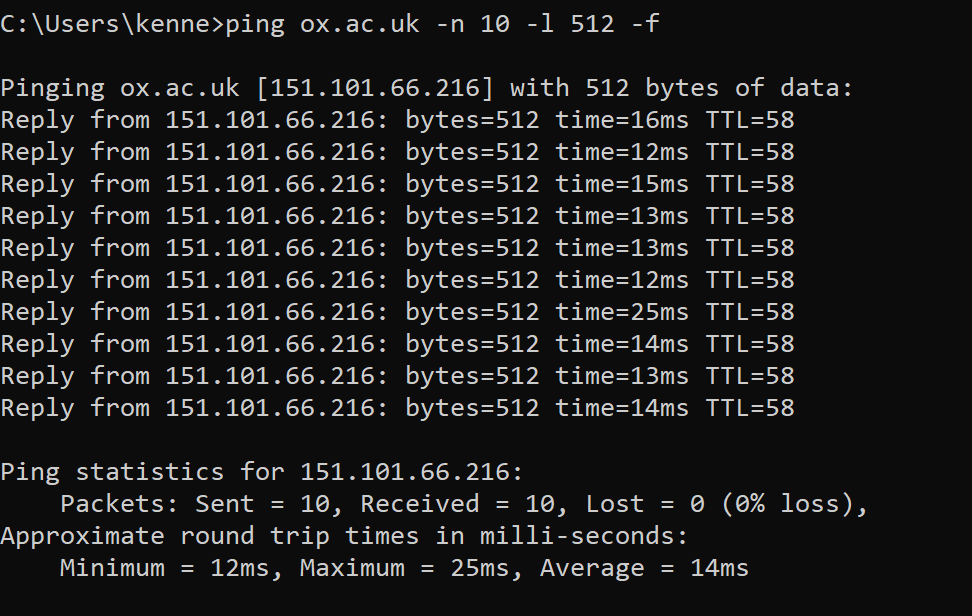


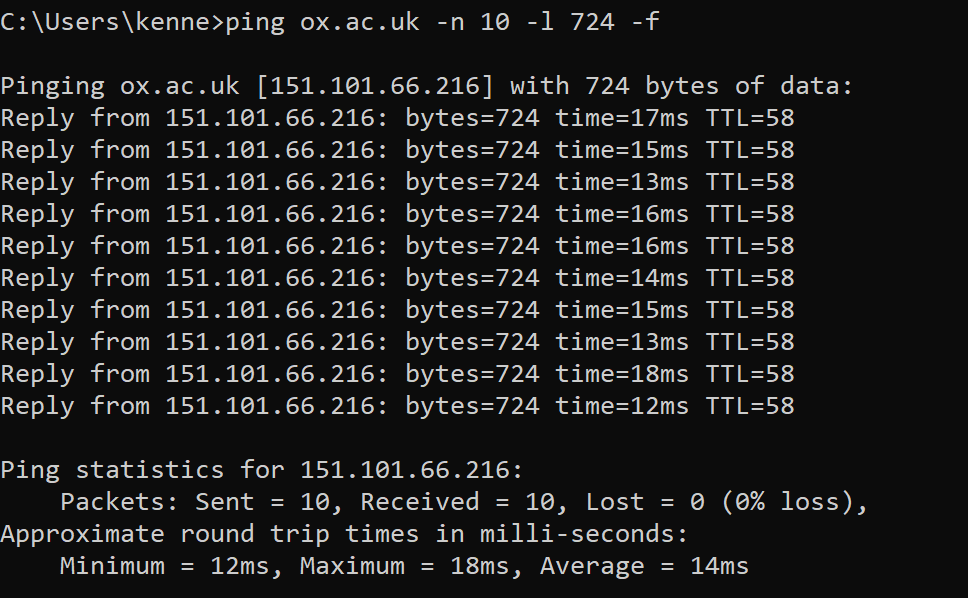


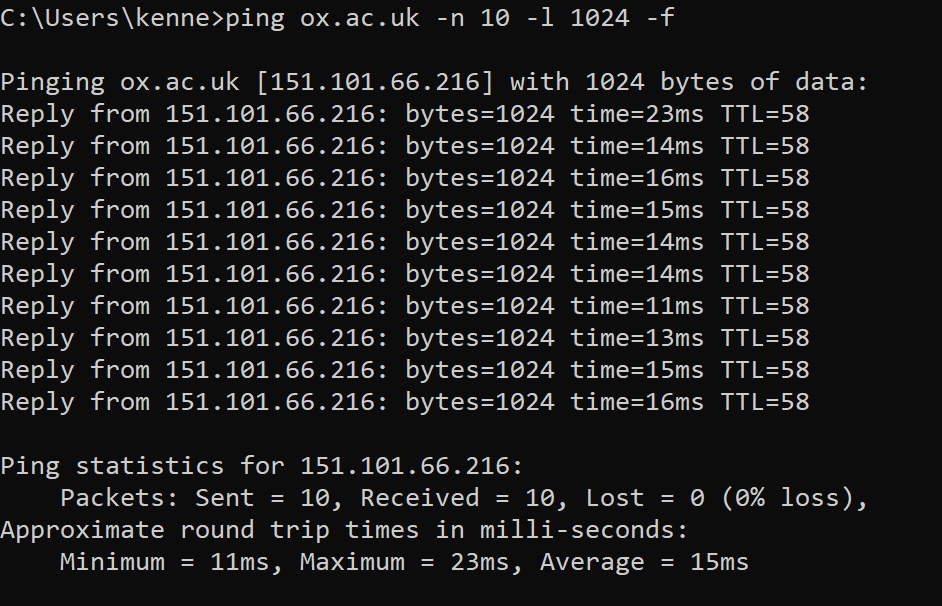


Timeouts for uwo.ca when > 512 bytes

1. **pinging ox.ac.uk**







No timeouts in any of the retrievals, successful every time.

*Results of calculations*

Xv

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | uwo.ca | | | | ox.ac.uk | | | |
| **Packet #** | **512** | **724** | **1024** | **4072** | **512** | **724** | **1024** | **4072** |
| 1 | T/O | T/O | T/O | T/O | 16 | 17 | 23 | T/O |
| 2 | T/O | T/O | T/O | T/O | 12 | 15 | 14 | T/O |
| 3 | T/O | T/O | T/O | T/O | 15 | 13 | 16 | T/O |
| 4 | T/O | T/O | T/O | T/O | 13 | 16 | 15 | T/O |
| 5 | T/O | T/O | T/O | T/O | 13 | 16 | 14 | T/O |
| 6 | T/O | T/O | T/O | T/O | 12 | 14 | 14 | T/O |
| 7 | T/O | T/O | T/O | T/O | 25 | 15 | 11 | T/O |
| 8 | T/O | T/O | T/O | T/O | 14 | 13 | 13 | T/O |
| 9 | T/O | T/O | T/O | T/O | 13 | 18 | 15 | T/O |
| 10 | T/O | T/O | T/O | T/O | 14 | 12 | 16 | T/O |
| **Avg** | **0** | **0** | **0** | **0** | **14.7** | **14.9** | **15.1** | **0** |
| **StdDev** | **0** | **0** | **0** | **0** | **3.83** | **1.91** | **3.14** | **0** |

As the packet size increases, the average time for the round trip and standard deviation also increase. Also, as the distance of the pinged host increased, so do the average and standard deviation time increase for the round trip. Request to send 4072 bytes timed out for ox.ac.uk destination and completely timed out for uwo.ca.

**Q7. Use the tracert utility on your lab workstation to find the route to a host. For each, state the number of hops and estimate the number of ISPs traversed.**

1. **in North America (uwo.ca)**

**Text

Description automatically generated**Number of hops: 11

Estimate ISP: 1, I pinged very close to campus so I should be in the ISP range

1. **in Europe (cam.ac.uk)**

Graphical user interface

Description automatically generated with medium confidence

Number of hops: 20

Estimated ISP travelled: 2

1. **in Australia (sydney.edu.au)**

Text

Description automatically generated

Number of hops: 30

Estimated ISP travelled: 2

**Q8. The results obtained in Q7 are formatted in a six-column output; what do these columns mean? Do you see any \* (if so, what do they mean)?**

On my machine there are only 5 columns. The first column is the hop #. The 2nd to 4th columns displays the RTT for the packet to reach that point and receive a response. Traceroute sends 3 different packet signals. The last column is the IP address of where the message was routed.

The “\*” indicates that the message timed out/packet was lost.

**Q9. Use the trace route utilities at the site www.traceroute.org to find the routes between a host in Europe and a host in South America.**

Host chosen: snlink.net

*From Europe to Host in South America (uchile.cl):*

A screenshot of a social media post

Description automatically generated

**Q10. Wait for 30 minutes and perform the same trace route as in Q9. Do the routes differ? If so, why? [4 Marks]**

The route chosen is a tad different. Perhaps closer web servers managed to cache the website between that time, as I chose a very popular website (a university).

A screenshot of a cell phone

Description automatically generated

**Task 2**

**Q11. Run nslookup to obtain the IP address of any Web server in Australia. What is the IP address of that server? [6 Marks]**

Text

Description automatically generated

Text

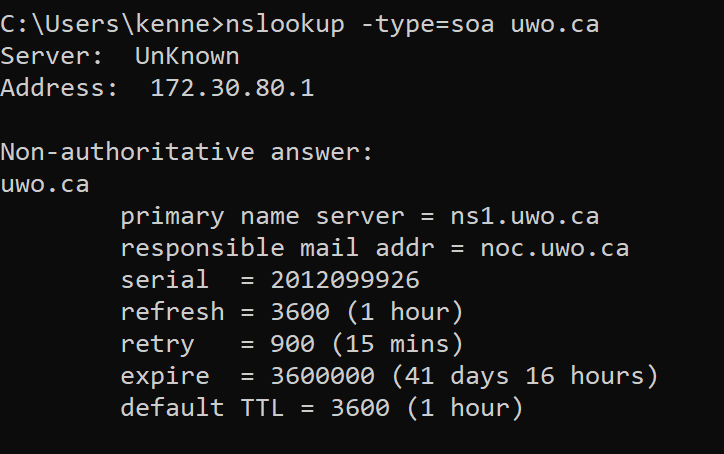
Description automatically generated

The IP address of the university of Sydney is 129.78.5.8

**Q12. Run nslookup to determine the authoritative DNS servers for our university and another of your choosing that Is not in north America. [6 Marks]**

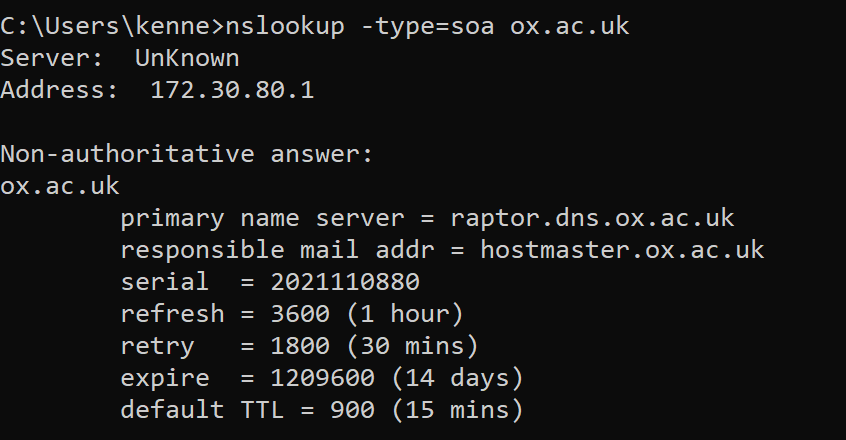
*uwo.ca*

Primary Name Server: ns1.uwo.ca

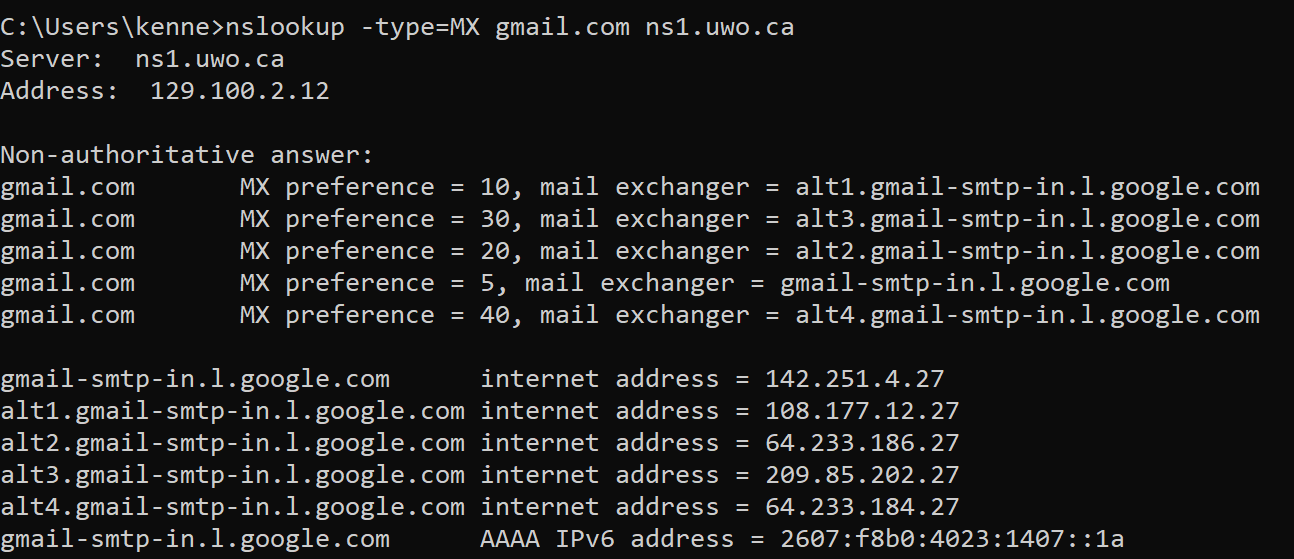


*ox.ac.uk*

Primary name server: nighthawk.dsn.ox.ac.uk



**Q13. Run nslookup so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Gmail. What is its IP address?**



The ns1.uwo.ca IP address is 129.100.2.12.

The mail server address is 213.239.32.10

The mail exchanger is gmail-smtp-in.1.google.com

**Task 3**

**Q14. Are then sent over UDP or TCP?**

They are being sent over UDP.

**Q15. What are the destination and source ports for the DNS query message?**

A screenshot of a computer

Description automatically generated

The source port is 57093 and the destination port is 53

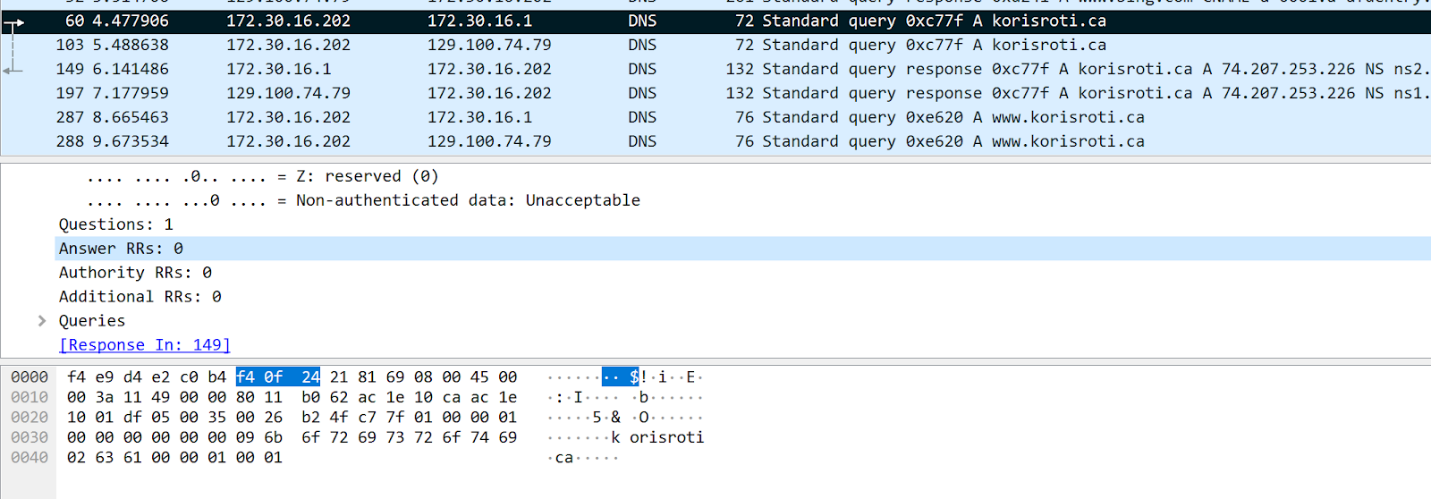
**Q16. To what IP address is the DNS query message sent?**

It is being sent to 172.30.16.1

**Q17. Examine the DNS query message. What “Type” of DNS query is it?**

It is a standard DNS query.

**Q18. Does the query message contain any “answers”, how many?**



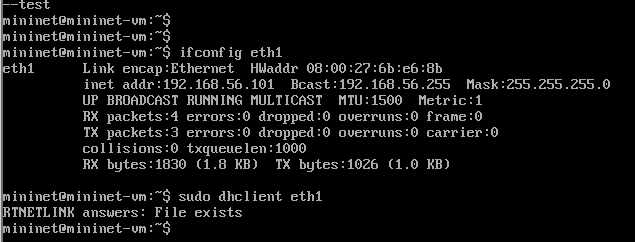
The query message does not contain any answers.

**Lab module 2**

**Task 1**

**Q19. Are the IP address of the virtual network adapter of your host OS (step 7) and the IP address of the VM’s eth1 interface in the same subnet? Why?**

Both IP address’s are in the same subnet, since both OS are hosted on the same machine.



**A screenshot of a cell phone screen with text

Description automatically generated**

*Pinging virtual machine from host OS*

**A picture containing text

Description automatically generated**

*Pinging host OS from VM*

**A screenshot of a computer

Description automatically generated**

**Task 2 [5 marks]**

**Q20. Are the IP address of h1 and the IP address of h2 interface in the same subnet? Why?**

Both the IP address of h1 and h2 interface are in the same subnet (see screenshots below). Since they are both being hosted on the same machine, the subnet is the same for both interfaces.

*Setting up nodes using Mobaxterm*

A screenshot of a cell phone

Description automatically generated

*H1 and H2 interface IP address’s*

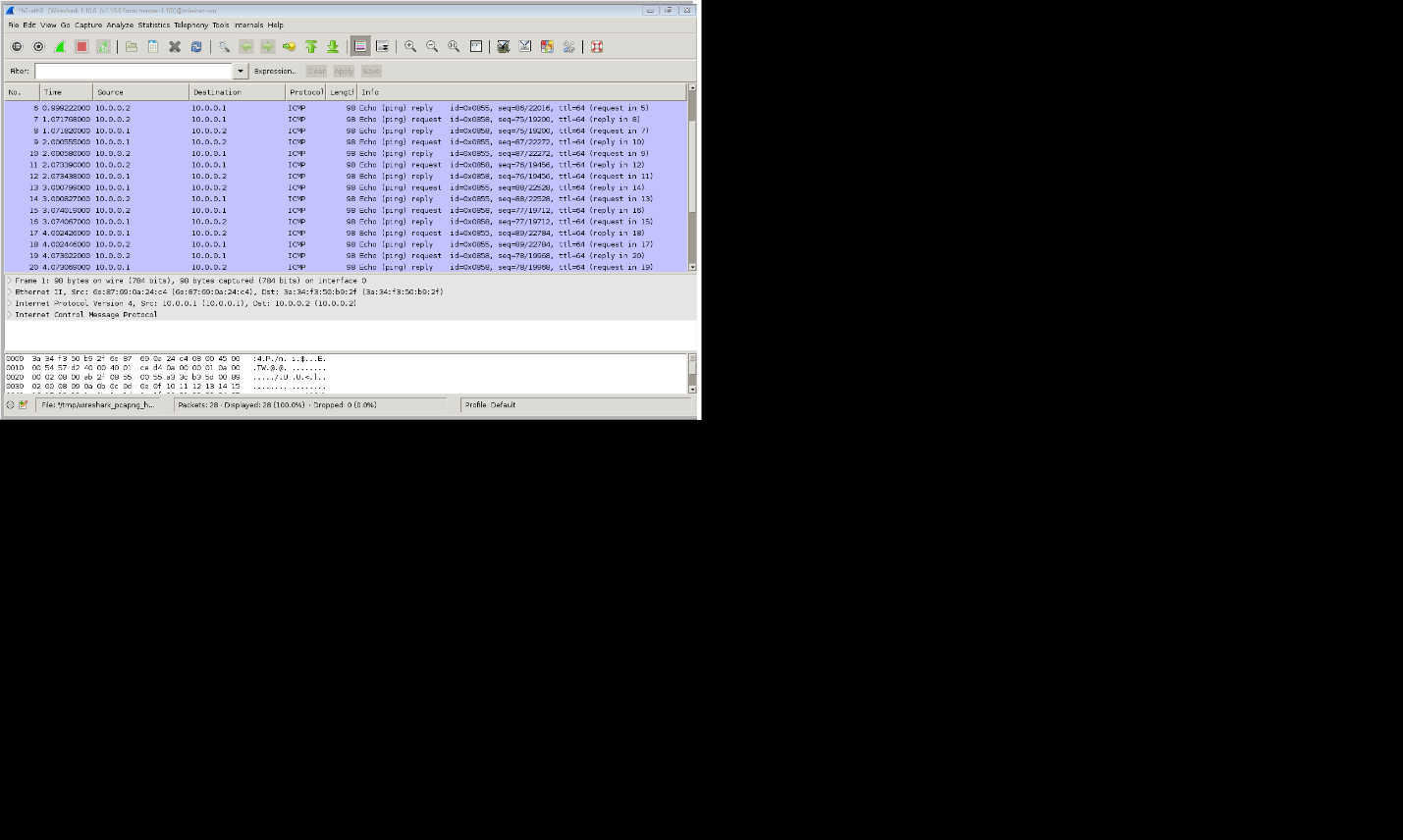
A screenshot of a cell phone

Description automatically generated

*Pinging H1 and H2 hosts*A screenshot of a cell phone

Description automatically generated

*H2 to H1 Wireshark Capture*



*H1 to H2 Wireshark Capture*

