

## CSC3064 Practical 1 Network Analysis

This practical covers a series of exercises for you to familiarize yourself with network discovery and analysis tools. Following each exercise, there are some short questions for you to answer. Make a note of your answers and we will discuss them in class next week.

### CODE OF CONDUCT

**You will be undertaking these network security exercises in a virtual environment. The purpose of this is to enable us to scan one machine from another and to sniff the virtual network without touching the University network. It is strictly forbidden to scan or sniff a network that you do not own without permission.**

### DO NOT PEN-TEST THE QUB NETWORK OR ANY OTHER PUBLIC NETWORK

The University has policies relating to information security and acceptable use of computer systems. Breaches of the security policies will be investigated in accordance with the University's disciplinary procedures. You should make yourself aware of these policies: <http://www.qub.ac.uk/directorates/InformationServices/Services/Security/#Policies>

### Exercise 1: Finding the IP address of a website and identifying route to the destination.

This exercise shows you how to obtain information about a website by using ping and traceroute. As the VMs do not have Internet access, run these two commands from the host machine.

Note: In Linux, you can use traceroute, in Windows, you use tracert.

Step 1: Open the command prompt and enter the following command:

```
ping <website name>
```

This request will time out as ping is blocked by the University network. However, the first line should reveal the IP address of the website name that you entered.

Once you see the "Request timed out." Notification, press Ctrl+C to cancel the command.

**Note:** A successful 'ping' command will also identify packet loss statistics on the route to the server hosting the website, approximate round-trip time etc. This information gives you an idea of the connection's performance and quality. The command "man ping" displays the manual for ping.

Step 2: At the command prompt, enter the following command,

```
tracert <ip address>
```

Where <ip address> is the one you recorded in Step 1.

Step 3: The results reveal information about the path that traffic is taking from the local host to the remote host. Note the response times and the locations that may have dropped packets. Again, this request will time out and press Ctrl+C to cancel the command.

**Now answer questions 1 and 2.**

Lab1 Q1: Run the tracert command for IP address 8.8.8.8

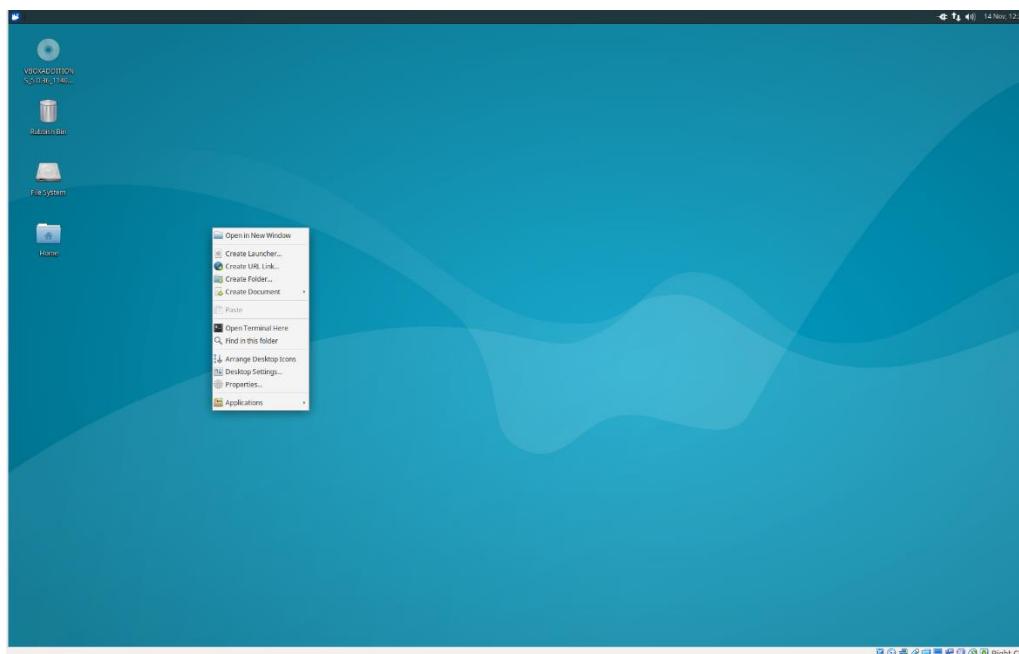
From the results displayed, who owns this IP address and what service is predominantly hosted there?

Lab1 Q2: How does traceroute/tracert work?

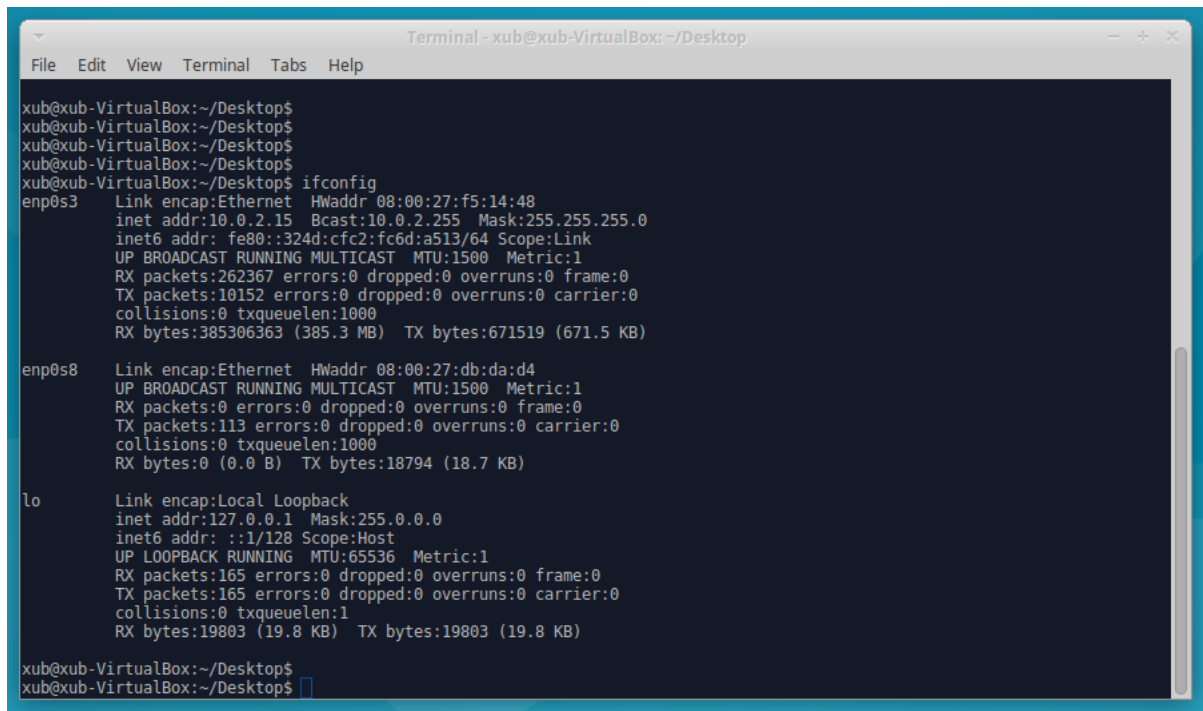
### Test Network Configuration

The next exercises in this practical use 2 Linux virtual machines (VMs) as a simple test network. You will be exploring network analysis tools for vulnerability assessment.

1. From the Windows Desktop, open the folder C:/Vbox/CSC3064/
2. Double-click on the xubuntu1 VM to launch it in virtualbox. Select Import.
3. Double-click on the xubuntu3 VM to launch it in virtualbox. Select Import.
4. Start the 2 xubuntu VMs. Username: xub, Password: CSC3064\_2018
5. Check “ifconfig” on each machine to see the networking information. Note: Right-click anywhere on the screen to open a terminal, as shown in Figure 1.



**Figure 1:** Right-click on the VM window and select “Open Terminal Here”



```

Terminal - xub@xub-VirtualBox: ~/Desktop
File Edit View Terminal Tabs Help

xub@xub-VirtualBox:~/Desktop$
xub@xub-VirtualBox:~/Desktop$
xub@xub-VirtualBox:~/Desktop$
xub@xub-VirtualBox:~/Desktop$ ifconfig
enp0s3  Link encap:Ethernet  HWaddr 08:00:27:f5:14:48
        inet addr:10.0.2.15  Bcast:10.0.2.255  Mask:255.255.255.0
        inet6 addr: fe80::324d:cfc2:fc6d:a513/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:262367 errors:0 dropped:0 overruns:0 frame:0
        TX packets:10152 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:385306363 (385.3 MB)  TX bytes:671519 (671.5 KB)

enp0s8  Link encap:Ethernet  HWaddr 08:00:27:db:da:d4
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:0 errors:0 dropped:0 overruns:0 frame:0
        TX packets:113 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:0 (0.0 B)  TX bytes:18794 (18.7 KB)

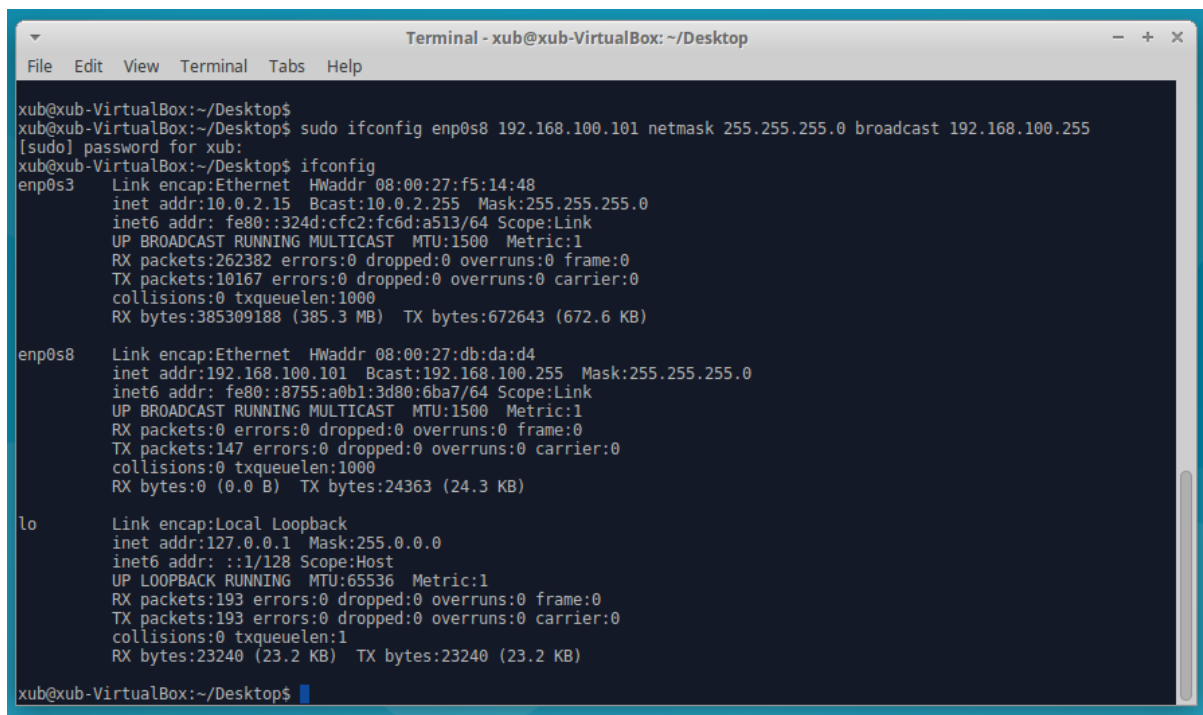
lo      Link encap:Local Loopback
        inet addr:127.0.0.1  Mask:255.0.0.0
        inet6 addr: ::1/128 Scope:Host
        UP LOOPBACK RUNNING  MTU:65536  Metric:1
        RX packets:165 errors:0 dropped:0 overruns:0 frame:0
        TX packets:165 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1
        RX bytes:19803 (19.8 KB)  TX bytes:19803 (19.8 KB)

xub@xub-VirtualBox:~/Desktop$
xub@xub-VirtualBox:~/Desktop$

```

**Figure 2:** Check the networking configuration with “ifconfig”

6. To enable the two VMs to communicate on an internal network, allocate private IP addresses to each VM.
  - a. On VM1, allocate an IP e.g. 192.168.100.101 and check the new IP address settings using “ifconfig”
  - b. On VM2, allocate a different IP e.g. 192.168.100.102 and check the new IP address settings using “ifconfig”



```

Terminal - xub@xub-VirtualBox: ~/Desktop
File Edit View Terminal Tabs Help

xub@xub-VirtualBox:~/Desktop$
xub@xub-VirtualBox:~/Desktop$ sudo ifconfig enp0s8 192.168.100.101 netmask 255.255.255.0 broadcast 192.168.100.255
[sudo] password for xub:
xub@xub-VirtualBox:~/Desktop$ ifconfig
enp0s3  Link encap:Ethernet  HWaddr 08:00:27:f5:14:48
        inet addr:10.0.2.15  Bcast:10.0.2.255  Mask:255.255.255.0
        inet6 addr: fe80::324d:cfc2:fc6d:a513/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:262382 errors:0 dropped:0 overruns:0 frame:0
        TX packets:10167 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:385309188 (385.3 MB)  TX bytes:672643 (672.6 KB)

enp0s8  Link encap:Ethernet  HWaddr 08:00:27:db:da:d4
        inet addr:192.168.100.101 Bcast:192.168.100.255 Mask:255.255.255.0
        inet6 addr: fe80::8755:a0b1:3d80:6ba7/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:0 errors:0 dropped:0 overruns:0 frame:0
        TX packets:147 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:0 (0.0 B)  TX bytes:24363 (24.3 KB)

lo      Link encap:Local Loopback
        inet addr:127.0.0.1  Mask:255.0.0.0
        inet6 addr: ::1/128 Scope:Host
        UP LOOPBACK RUNNING  MTU:65536  Metric:1
        RX packets:193 errors:0 dropped:0 overruns:0 frame:0
        TX packets:193 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1
        RX bytes:23240 (23.2 KB)  TX bytes:23240 (23.2 KB)

xub@xub-VirtualBox:~/Desktop$

```

**Figure 3:** Allocate a private IP address to each VM

**Note:** You may need to run the Step 4 commands twice before the IP addresses are correctly set.

7. Check that you can communicate between the two machines using *ping*

```

Terminal - xub@xub-VirtualBox: ~/Desktop
File Edit View Terminal Tabs Help
collisions:0 txqueuelen:1000
RX bytes:385323831 (385.3 MB) TX bytes:693223 (693.2 KB)

enp0s8  Link encap:Ethernet HWaddr 08:00:27:db:da:d4
        inet addr:192.168.100.101 Bcast:192.168.100.255 Mask:255.255.255.0
        inet6 addr: fe80::a00:27ff:fedb:dad4/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
        RX packets:95 errors:0 dropped:0 overruns:0 frame:0
        TX packets:334 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:14856 (14.8 KB) TX bytes:50705 (50.7 KB)

lo      Link encap:Local Loopback
        inet addr:127.0.0.1 Mask:255.0.0.0
        inet6 addr: ::1/128 Scope:Host
        UP LOOPBACK RUNNING MTU:65536 Metric:1
        RX packets:333 errors:0 dropped:0 overruns:0 frame:0
        TX packets:333 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1
        RX bytes:40332 (40.3 KB) TX bytes:40332 (40.3 KB)

xub@xub-VirtualBox:~/Desktop$ ping 192.168.100.102
PING 192.168.100.102 (192.168.100.102) 56(84) bytes of data:
64 bytes from 192.168.100.102: icmp_seq=1 ttl=64 time=0.199 ms
64 bytes from 192.168.100.102: icmp_seq=2 ttl=64 time=0.249 ms
64 bytes from 192.168.100.102: icmp_seq=3 ttl=64 time=0.242 ms
64 bytes from 192.168.100.102: icmp_seq=4 ttl=64 time=0.242 ms
64 bytes from 192.168.100.102: icmp_seq=5 ttl=64 time=0.243 ms
^C
--- 192.168.100.102 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4000ms
rtt min/avg/max/mdev = 0.199/0.235/0.249/0.018 ms
xub@xub-VirtualBox:~/Desktop$

```

**Figure 4:** Check the internal network communication using “ping”.

8. Note the internal network interface e.g. enp0s8. You will need this in the next exercises.

## Exercise 2: Exploring and auditing a network using nmap

Network addresses are scanned to determine:

- What services (application names and versions) those hosts offer?
- What operating systems (and OS versions) they run?
- The type of packet filters/firewalls that are in use and dozens of other characteristics.

Step 1: Scan an IP range to determine what hosts are up.

On VM1, open the command prompt and enter the following command:

```
nmap -sn -v 192.168.0.0/16
```

If the command successfully finds live hosts, it returns a message stating that the IP address is up. Note the other details provided.

Familiarise yourself with the options (for example “-sn”) that can be used with nmap:

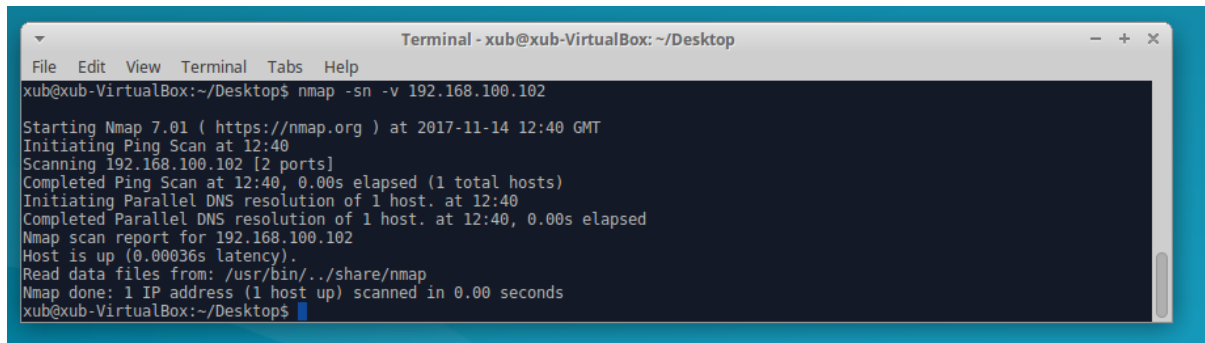
<https://svn.nmap.org/nmap/docs/nmap.usage.txt> or `nmap --help`

Step 2: Perform a ping using nmap

On VM1, open the command prompt and enter the following command:

`nmap -sn -v <VM2 ip address>`

Compare the result of your command with the results shown in Figure 5.



```
Terminal - xub@xub-VirtualBox: ~/Desktop
File Edit View Terminal Tabs Help
xub@xub-VirtualBox:~/Desktop$ nmap -sn -v 192.168.100.102
Starting Nmap 7.01 ( https://nmap.org ) at 2017-11-14 12:40 GMT
Initiating Ping Scan at 12:40
Scanning 192.168.100.102 [2 ports]
Completed Ping Scan at 12:40, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 12:40
Completed Parallel DNS resolution of 1 host. at 12:40, 0.00s elapsed
Nmap scan report for 192.168.100.102
Host is up (0.00036s latency).
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.00 seconds
xub@xub-VirtualBox:~/Desktop$
```

**Figure 5:** Perform a ping using nmap

**Now answer questions 3-6.**

Lab1 Q3: How many live hosts are detected when you run the Step 1 command?

`nmap -sn -v 192.168.0.0/16`

Lab1 Q4: How many addresses are scanned with the IP address range 192.168.32.0/24?

Lab1 Q5: What warning is displayed when you run the Step 2 command?

`nmap -sn -v <VM2 ip address>`

Lab1 Q6: Why do you think the warning is displayed in the Step 2 command?

### Exercise 3: Packet crafting using HPING3 and observation using tcpdump

Using **hping3**, you can create different types of packets and send them to a target. **Tcpdump** prints out a description of the contents of packets on a network interface.

Step 1: On VM2, enter the following command:

`sudo tcpdump -i enp0s8`

Familiarise yourself with tcpdump: [http://www.tcpdump.org/tcpdump\\_man.html](http://www.tcpdump.org/tcpdump_man.html)

Send 10 “pings” from VM1 to VM2.

Check the tcpdump output on VM2. Note the ICMP echo request followed by the ARP request and reply and then the ICMP echo reply.

Step 2: Create an ACK packet and send it to port 80 on VM2

On VM1, enter the following command:

`sudo hping3 -A -c 5 <VM2 ip address> -p 80`

Familiarise yourself with hping3: <https://tools.kali.org/information-gathering/hping3> or man hping3

Check the tcpdump output on VM2 and look for the protocol/service linked to the TCP number.

**Note:** Stop the hping using ctrl+C.

**Note:** In this exercise, the VM is receiving packets and displaying packet contents on the same interface. If you don't limit the number of hping packets as we've done in Step 2, the interface can block. If this happens, you can use wireshark to capture the network traffic instead.

Step 3: Create a SYN scan against different ports on VM2

On VM1, enter the following command:

```
sudo hping3 -8 50-56 -s -i <VM2 ip address> -V
```

Check the tcpdump output on VM2

**Note:** Stop tcpdump using ctrl+C.

**Now answer questions 7 and 8.**

Lab1 Q7: What service/protocol was used in the Step 2 command?

```
sudo hping3 -A -c 5 <VM2 ip address> -p 80
```

Lab1 Q8: What service/protocol runs on port 53?

### Exercise 4: Packet Analysis with Wireshark

Wireshark is a widely deployed network protocol analyser used to dissect and analyse network traffic (<https://www.wireshark.org/>). Wireshark can be used to capture network traffic in real-time. However, in this exercise we will analyse a previously captured packet trace. This is called a pcap file.

Step 1: On VM1, launch wireshark from the terminal with the command:

```
sudo wireshark &
```

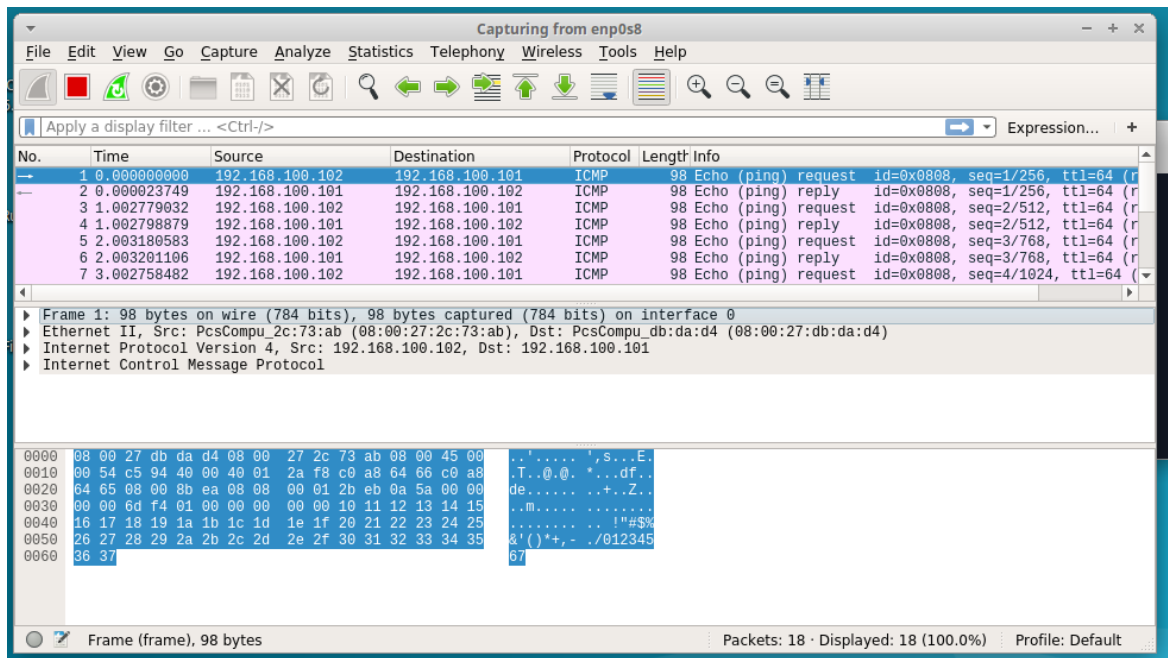
Note: You can ignore the "lua script" error on launching wireshark. Just hit OK.

Step 2: From the wireshark launch page, select to capture on interface enp0s8.

Step 3: Ping VM2 from VM1.

You should see an output similar to that shown in Figure 6.

There are three main panes in wireshark; packet list, packet details, and packet bytes.

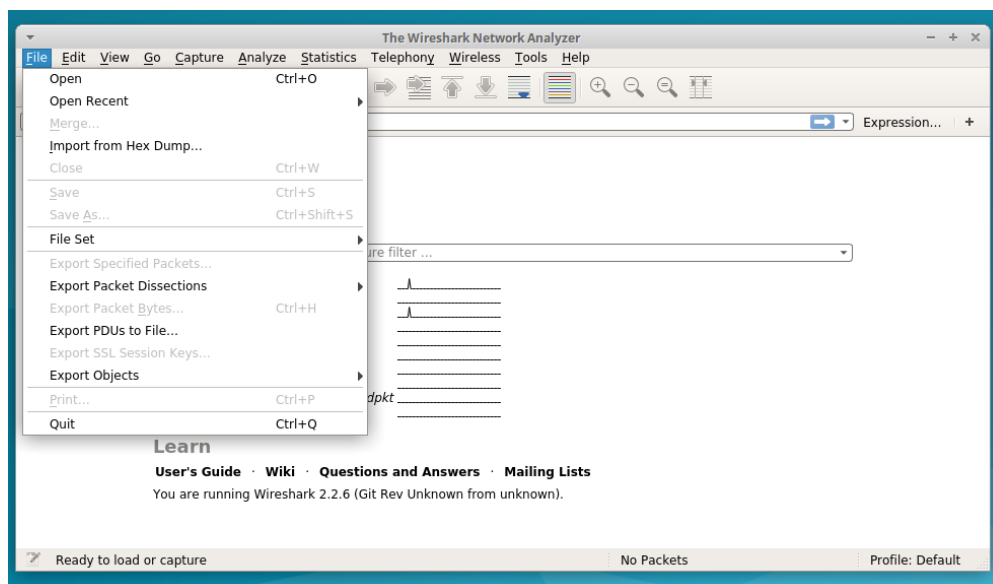


**Figure 6:** The top pane in Wireshark is the packet list, the middle pane provides the packet details, and the bottom pane displays the packet bytes.

Step 4: From the Wireshark file menu, open the file called Practical1.pcapng (this is in the folder – CSC3064\_Practicals/Practical1).

Practical1.pcapng contains a recording of a web browsing session.

**Note:** You will have to stop the existing capture before opening the pcap.



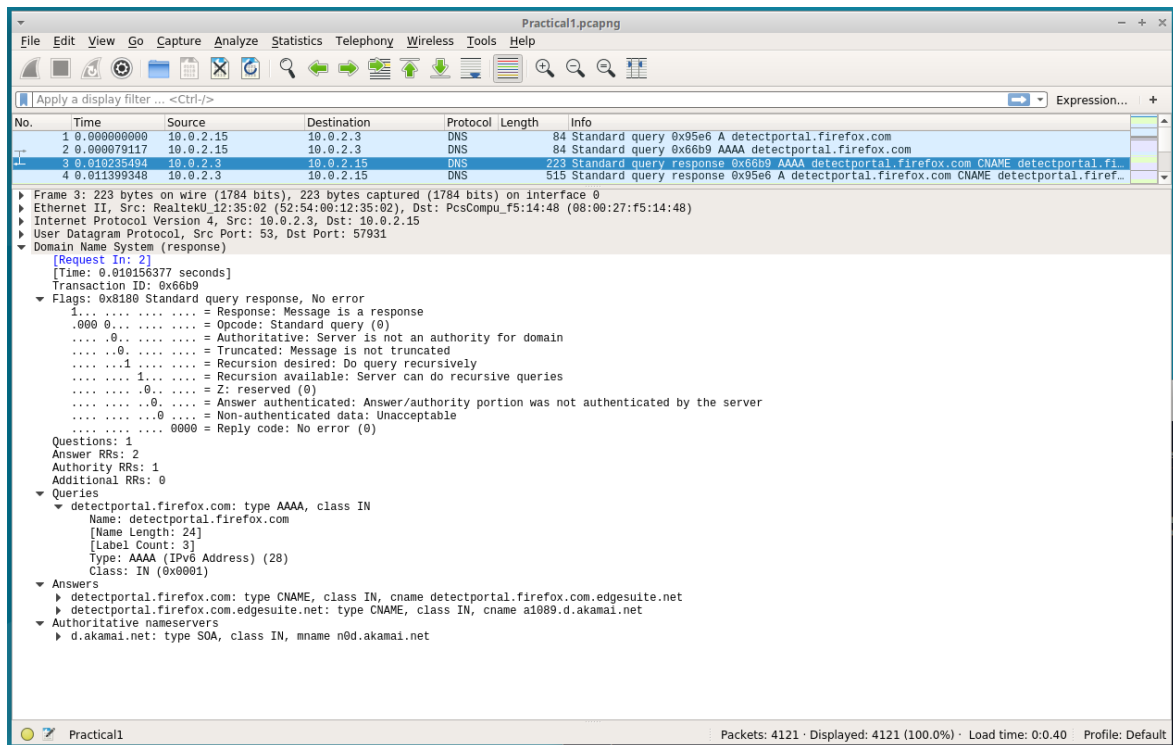
**Figure 7:** Open file Practical1.pcapng

Step 5: Identify protocol types in Wireshark

Select a packet from the packet list.

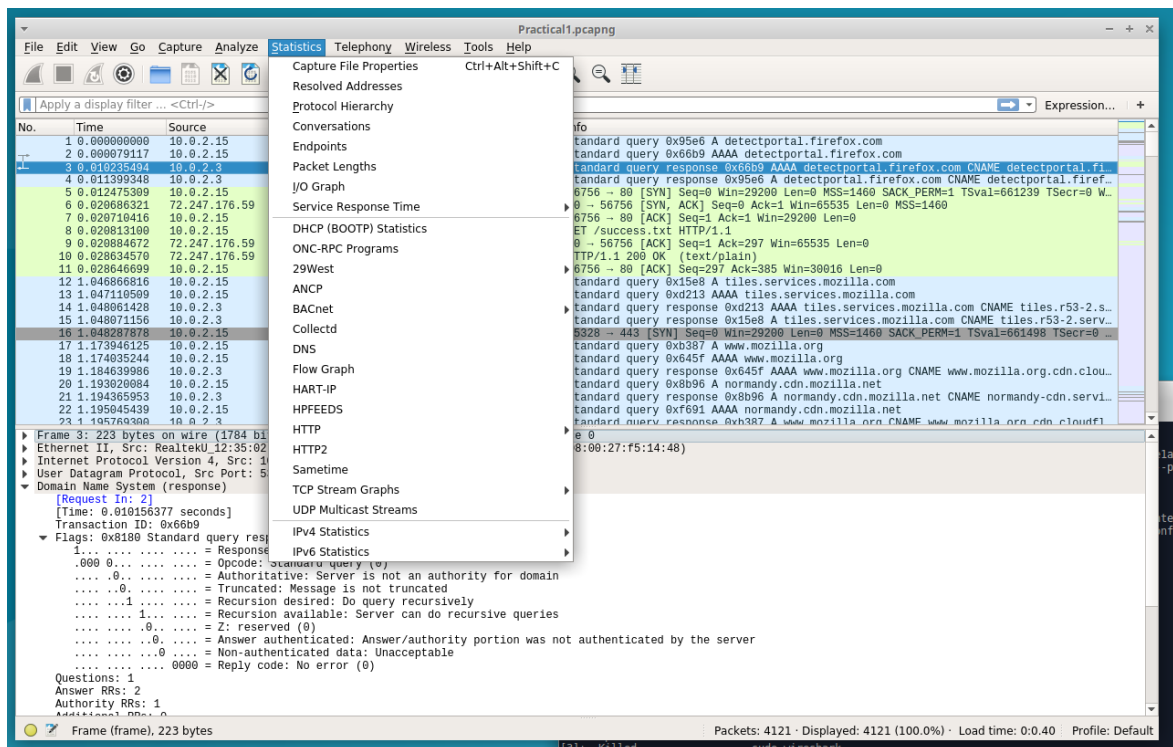
Explore the contents of the packet using the packet details and packet bytes panes. For example, a DNS packet detail is shown in Figure 8.





### Figure 8: DNS Packet Detail

### Step 6: Analyse the packet lengths within the pcap using Statistics -> Packet Lengths



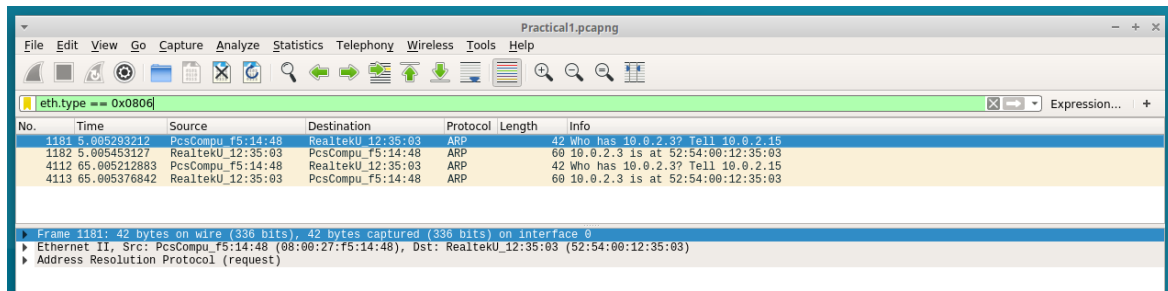
### Figure 9: Using statistics within Wireshark

Step 7: Apply a filter to the traffic e.g. by Ethertype.

EtherType is a two-byte field in an Ethernet frame used to indicate which protocol is encapsulated in the payload of the frame. This field is used by the data link layer to

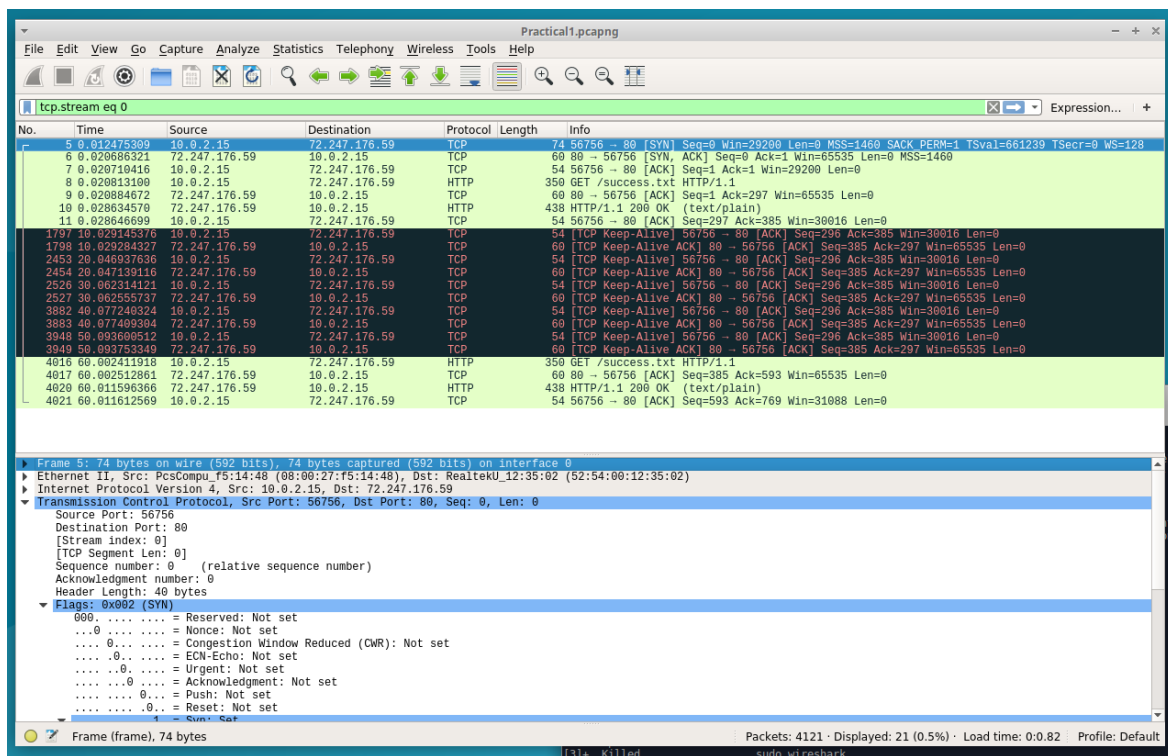


determine which protocol to pass the payload to at the receiver. The field can be used to filter certain types of traffic at a firewall.



**Figure 10:** Using filters within Wireshark

Step 8: Track a flow within the pcap (Hint: follow tcp stream)



**Figure 11:** Using filters by conversation

Now answer questions 9 and 10.

Lab1 Q9: Which flags are set in a DNS standard query?

Lab1 Q10: What percentage of packets in Practical1.pcapng are between 40 and 79 bytes in length?

## SHUTDOWN

When you've completed the practical, close all terminals and applications in the VM and close each VM by powering off the machine.