FIT9137 Workshop
Week 6

Topics:

- Protocol Layering
- Encapsulation and Decapsulation, Multiplexing and Demultiplexing
- Addresses at various layers (domain names, IP addresses, MAC addresses)
- **Network Tools:** Wireshark GUI, ifconfig, ping, nslookup, traceroute

Covered Learning Outcomes:

- Examine networks using the underlying fundamental theories, models and protocols for data transmission.

Instructions:

- One of the main targets of workshops is to anchor the learner into the session and create many opportunities to reinforce the learning in different ways – individually and in small groups. Sometimes we also teach key practical/theoretical concepts to you during these sessions.
- Form groups of 4-5 students to work through the exercises. If met a problem, try to solve it within your group by discussing it with your group members. If not resolved within the group, ask one of the support tutors to help you.
- You still have a question? Jump into one of many consultation hours run by our experienced tutors and seek help. Please visit the "Teaching Team and Unit Resources" tile in the FIT9137 Moodle site.

ACTIVITY A: Network Tools

Activity A.1: Addressing

In this activity, we will use some network tools to learn more about the concept of addressing in the TCP/IP protocol stack. We will learn more about each layer in the following weeks. In this week, we only intend to become more familiar with the discussed topics of a layered architecture in the context of TCP/IP protocol stack.

1. Open ***Firefox*** in the VM and visit the Monash University website by entering `www.monash.edu` in the address bar.

   a) What kind of address did you use to visit the Monash website?

b) The address is used in which layer in the TCP/IP protocol stack?

2. Enter the following command in the VM terminal:

```
nslookup www.monash.edu
```

a) What does the command do? (`man nslookup`)

b) What layer of the TCP/IP protocol stack the returned address belongs to?

3. Enter the following command in the VM terminal

```
ifconfig
```

a) What is the purpose of this command? (`man ifconfig`)

b) What addresses can you identify in the output of the command, and to which layer these addresses belong?

Activity A.2: Testing Network Connectivity

In this part, we will become familiar with two commands used to test the network connectivity and troubleshoot network problems.

1. Open a terminal in the VM and enter the following command:

```
ping www.monash.edu
```

a) What is the purpose of this command? (`man ping`)

b) What information does the output of the command convey? What else can we learn from the output besides whether the destination host is reachable?

c) Limit the number of messages sent to 5 and the time to wait to 1 second (`ping -h` to see the brief command option help).

2. Enter the following command:

```
traceroute www.monash.edu
```

a) What is the purpose of this command? (`man traceroute`)

b) What do we learn from the output? Can you identify where (city and or country) each reported hop (router) is located?

ACTIVITY B: Packet Sniffing

A packet analyser (sometimes also referred to as “packet sniffer”) is a program that can log all packets that are received and transmitted over a network interface. We will be using Wireshark, a very popular open-source tool for packet analysis. It is already installed in the FIT9137 virtual machine.

This week, we will analyse a sequence of packets captured on Guido's network at home. The following diagram depicts how Guido's computer is connected to the Monash web server:

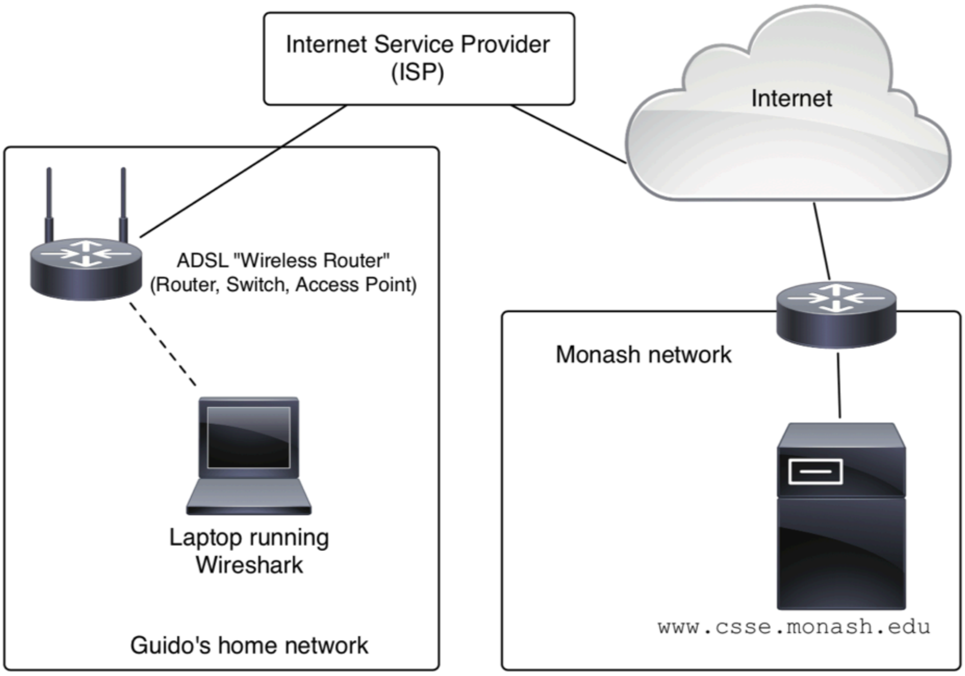


Figure 1: Guido's setup for packet capture

Guido's setup for packet capture

Open a terminal window in VM and change directory to ~/Desktop and execute the following command (**no** new lines and **no** space within the google drive path placed in the single quotes):

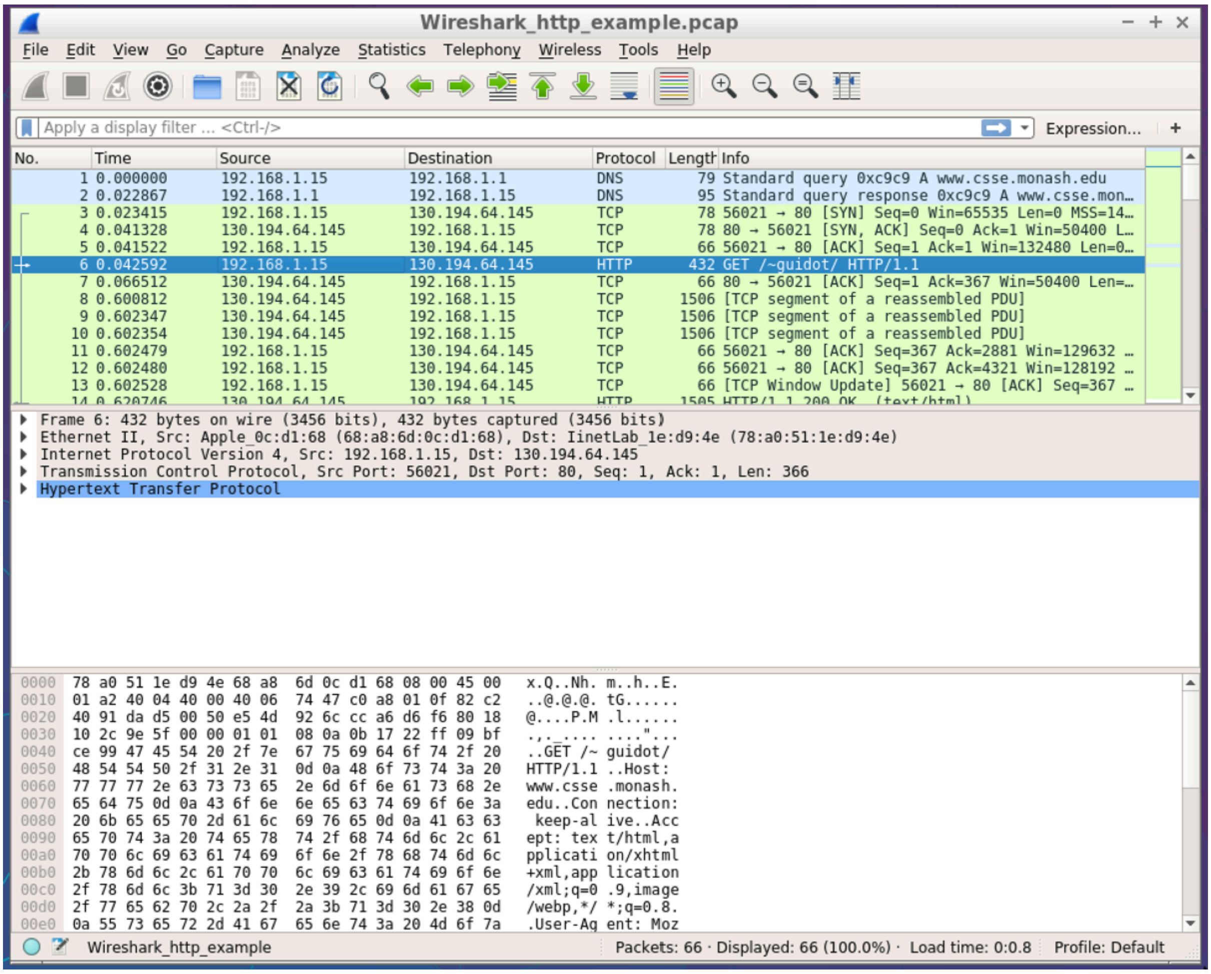
```
wget --no-check-certificate -r
'https://drive.google.com/file/d/1iPOtYBLeWNVgXYm2mdada-TFTp_6ZhVw/view?us
p=drive_link' -O workshop_files.zip
```

Right click the downloaded file "workshop_files.zip" on Desktop, and select **Extract Here**. This will create a folder named **workshop_files** on Desktop. Inside this folder, you will find the Workshop files we will use throughout the semester. This week, we will use **FIT9137_w6_wireshark.pcap**

Perform the following tasks inside the virtual machine.

Open the pcap file either by double clicking on it or first open Wireshark and from menu bar **File** → **Open** and browse to the pcap file.

After opening the file, you should see a window as shown in Figure-.



```
No.  Time       Source           Destination      Protocol Length Info
   1 0.000000   192.168.1.15     192.168.1.1      DNS        79 Standard query 0xc9c9 A www.csse.monash.edu
   2 0.022867   192.168.1.1      192.168.1.15     DNS        95 Standard query response 0xc9c9 A www.csse.mon…
   3 0.023415   192.168.1.15     130.194.64.145   TCP        78 56021 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=14…
   4 0.041328   130.194.64.145   192.168.1.15     TCP        78 80 → 56021 [SYN, ACK] Seq=0 Ack=1 Win=50400 L…
   5 0.041522   192.168.1.15     130.194.64.145   TCP        66 56021 → 80 [ACK] Seq=1 Ack=1 Win=132480 Len=0…
   6 0.042592   192.168.1.15     130.194.64.145   HTTP      432 GET /~guidot/ HTTP/1.1
   7 0.066512   130.194.64.145   192.168.1.15     TCP        66 80 → 56021 [ACK] Seq=1 Ack=367 Win=50400 Len=…
   8 0.600812   130.194.64.145   192.168.1.15     TCP      1506 [TCP segment of a reassembled PDU]
   9 0.602347   130.194.64.145   192.168.1.15     TCP      1506 [TCP segment of a reassembled PDU]
  10 0.602354   130.194.64.145   192.168.1.15     TCP      1506 [TCP segment of a reassembled PDU]
  11 0.602479   192.168.1.15     130.194.64.145   TCP        66 56021 → 80 [ACK] Seq=367 Ack=2881 Win=129632 …
  12 0.602480   192.168.1.15     130.194.64.145   TCP        66 56021 → 80 [ACK] Seq=367 Ack=4321 Win=128192 …
  13 0.602528   192.168.1.15     130.194.64.145   TCP        66 [TCP Window Update] 56021 → 80 [ACK] Seq=367 …
  14 0.620746   130.194.64.145   192.168.1.15     HTTP     1505 HTTP/1.1 200 OK  (text/html)
```

```
▸ Frame 6: 432 bytes on wire (3456 bits), 432 bytes captured (3456 bits)
▸ Ethernet II, Src: Apple_0c:d1:68 (68:a8:6d:0c:d1:68), Dst: IinetLab_1e:d9:4e (78:a0:51:1e:d9:4e)
▸ Internet Protocol Version 4, Src: 192.168.1.15, Dst: 130.194.64.145
▸ Transmission Control Protocol, Src Port: 56021, Dst Port: 80, Seq: 1, Ack: 1, Len: 366
▸ Hypertext Transfer Protocol
```

```
0000  78 a0 51 1e d9 4e 68 a8  6d 0c d1 68 08 00 45 00   x.Q..Nh. m..h..E.
0010  01 a2 40 04 40 00 40 06  74 47 c0 a8 01 0f 82 c2   ..@.@.@. tG......
0020  40 91 da d5 00 50 e5 4d  92 6c cc a6 d6 f6 80 18   @....P.M .l......
0030  10 2c 9e 5f 00 00 01 01  08 0a 0b 17 22 ff 09 bf   .,._.... ...."...
0040  ce 99 47 45 54 20 2f 7e  67 75 69 64 6f 74 2f 20   ..GET /~ guidot/
0050  48 54 54 50 2f 31 2e 31  0d 0a 48 6f 73 74 3a 20   HTTP/1.1 ..Host:
0060  77 77 77 2e 63 73 73 65  2e 6d 6f 6e 61 73 68 2e   www.csse .monash.
0070  65 64 75 0d 0a 43 6f 6e  6e 65 63 74 69 6f 6e 3a   edu..Con nection:
0080  20 6b 65 65 70 2d 61 6c  69 76 65 0d 0a 41 63 63    keep-al ive..Acc
0090  65 70 74 3a 20 74 65 78  74 2f 68 74 6d 6c 2c 61   ept: tex t/html,a
00a0  70 70 6c 69 63 61 74 69  6f 6e 2f 78 68 74 6d 6c   pplicati on/xhtml
00b0  2b 78 6d 6c 2c 61 70 70  6c 69 63 61 74 69 6f 6e   +xml,app lication
00c0  2f 78 6d 6c 3b 71 3d 30  2e 39 2c 69 6d 61 67 65   /xml;q=0 .9,image
00d0  2f 77 65 62 70 2c 2a 2f  2a 3b 71 3d 30 2e 38 0d   /webp,*/ *;q=0.8.
00e0  0a 55 73 65 72 2d 41 67  65 6e 74 3a 20 4d 6f 7a   .User-Ag ent: Moz
```

File `w4_wireshark.pcap` *opened in Wireshark and frame 6 is selected in packet list pane*

Familiarise yourself with the three main sections (panes) of the Wireshark window:

a) The packet list pane displays a summary of each packet captured. When you click on a packet here, the other two panes are updated with the details for that packet.

b) The packet details pane below packet list (middle pane) shows information about the selected packet.

c) The packet bytes pane displays the raw data for the selected packet. It highlights the data for the field that is selected in the packet details pane.

The **frame 6** shows a request sent from Guido's home computer to the Guido's page hosted on Monash web server. Select this frame in the list of packets pane (as shown in Figure-) and answer the following questions.

1. Identify the Monash web server host URL (domain name) and the complete address (what Guido used in the browser to visit the page) by inspecting the details presented in the middle pane. Which layer contains this information?

2. What is the network address (IP) of the Monash web server? Which layer contains this information?

3. What is the frame size in bytes?

4. Identify all the layers (protocols) used in the protocol stack for this frame. In what order Wireshark presents the layers?

5. What are the PDU names for each protocol?

6. Recall that each protocol layer encapsulates the message from the layer above and adds a header. What are the header sizes for each layer?

7. Can multiplexing/demultiplexing be used in this communication between Guido's browser and Monash web server? How the lower layer (TCP) knows that the destination host is a web server (we learn more about this in Transport Layer)?

8. What format is used to represent the raw data in the third windowpane in each column?