

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:

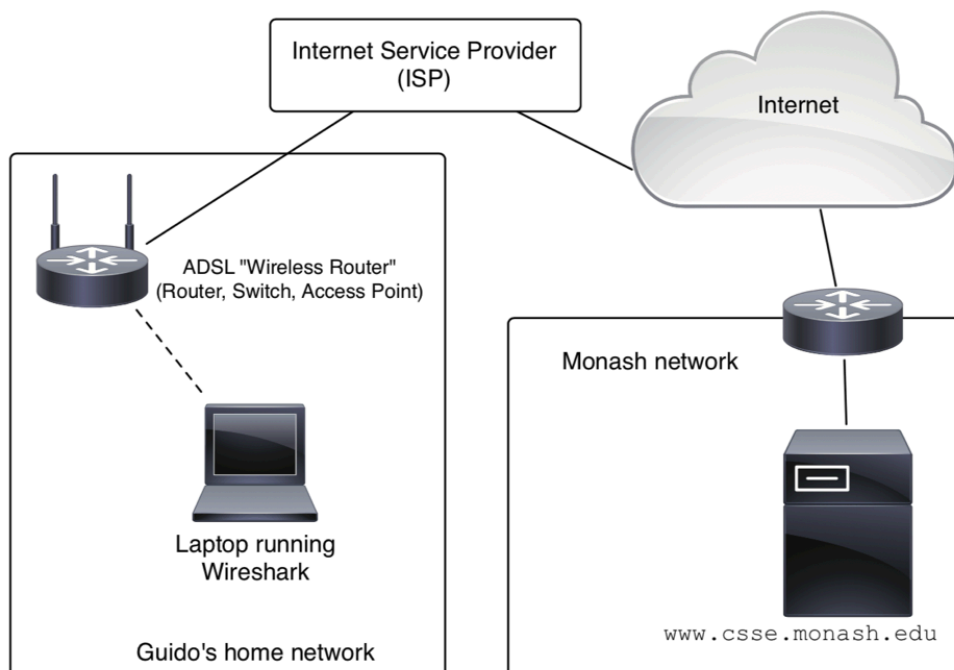


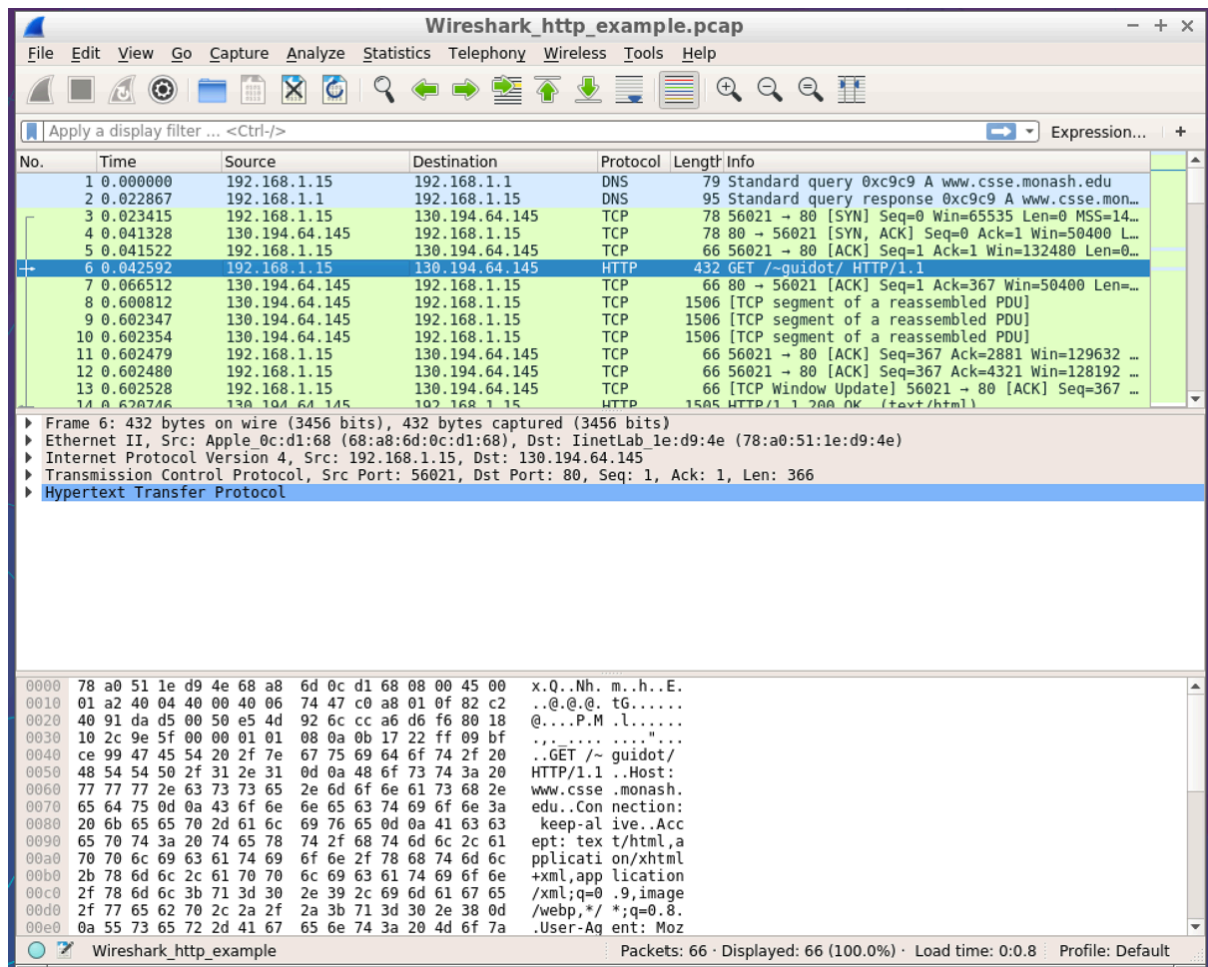
Figure 1: Guido's setup for packet capture

Guido's setup for packet capture

Download the file FIT9137_w6_wireshark.pcap from Moodle week 6 page and save it. Open the CORE emulator and open this "imn" file using the File tab. 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-.



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:

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

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