FIT1047 Tutorial 8

Topics and goals

- Network layers and protocols, learn about addresses at various layers

- Application layer – HTTP

- Familiarise yourself with some of the networking tools

Instructions

The tasks are supposed to be done in groups of two or three students.

Task 1: Basic knowledge

Briefly explain the following terms:

1. Bit rate, bandwidth

2. Latency

3. Networks layers, PDU, encapsulation

Task 2: Packet sniffing

A packet analyser (sometimes also called "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. You can download it on your own computer from `www.wireshark.org`, or use the version installed on the Monash lab computers.

This week, we will analyse a sequence of packets captured on Guido's network at home. You can download the log file that Wireshark produced from the FIT1047 Moodle site (week 7). The file is called `Wireshark_http_example.pcap`. The diagram in Figure 1 explains how Guido's computer is connected to the Monash web server.

1. Start Wireshark and load the capture file (see Fig. 2). After opening the file, the main window should look like the one in Fig. 3.

2. Select "frame" number 6 (as in Fig. 3). This frame shows a request sent from Guido's home computer to the web server at `www.csse.monash.edu`, requesting his homepage

3. Familiarise yourself with the three main sections (panes) of the Wireshark window:
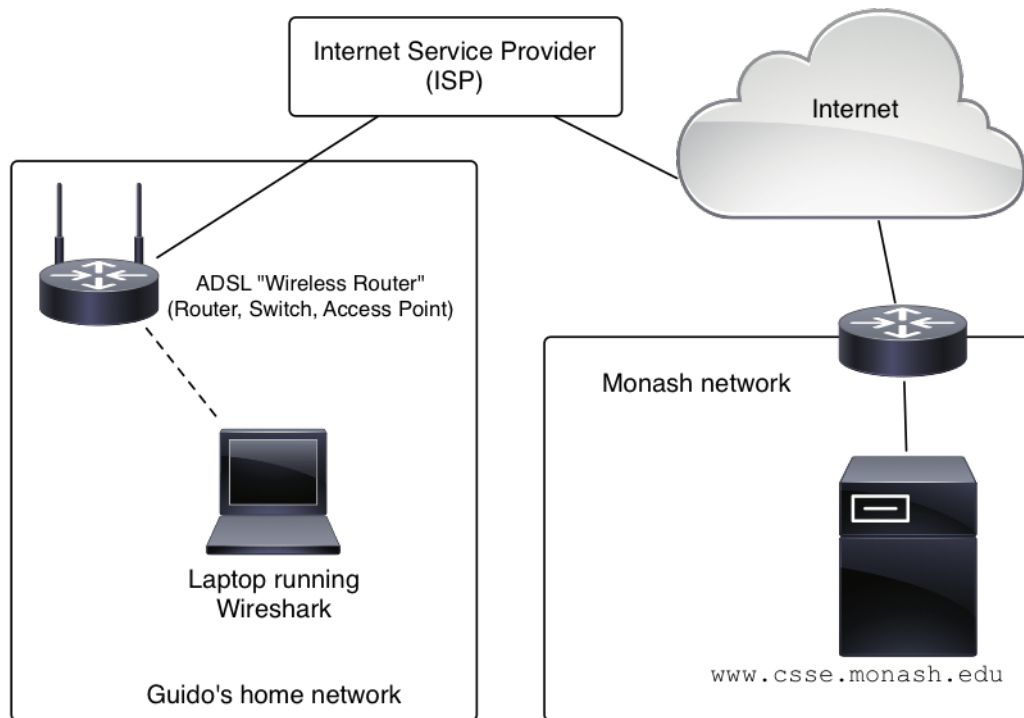
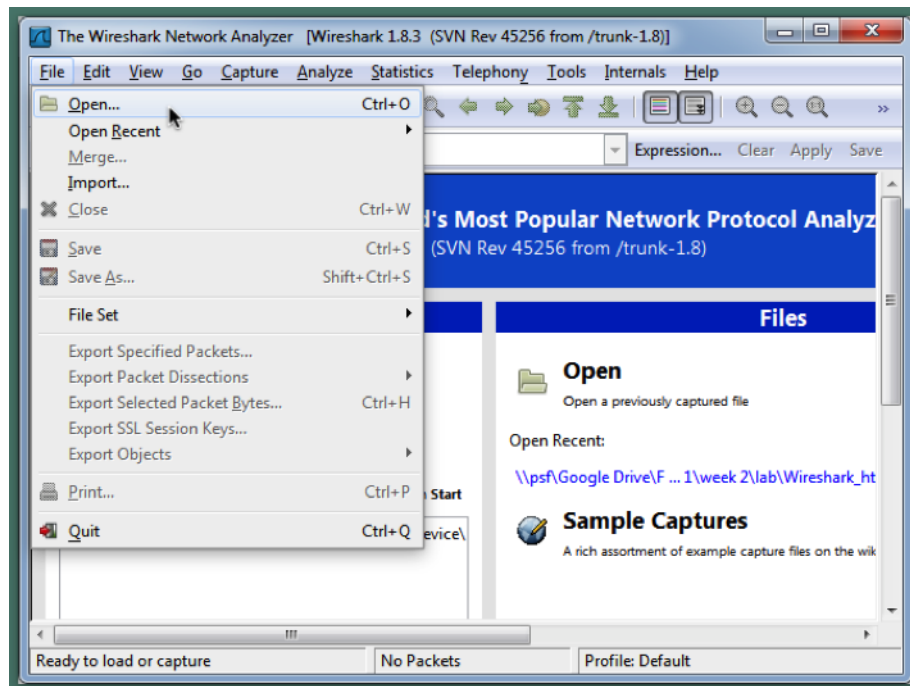Figure 1: The network where the traffic was captured
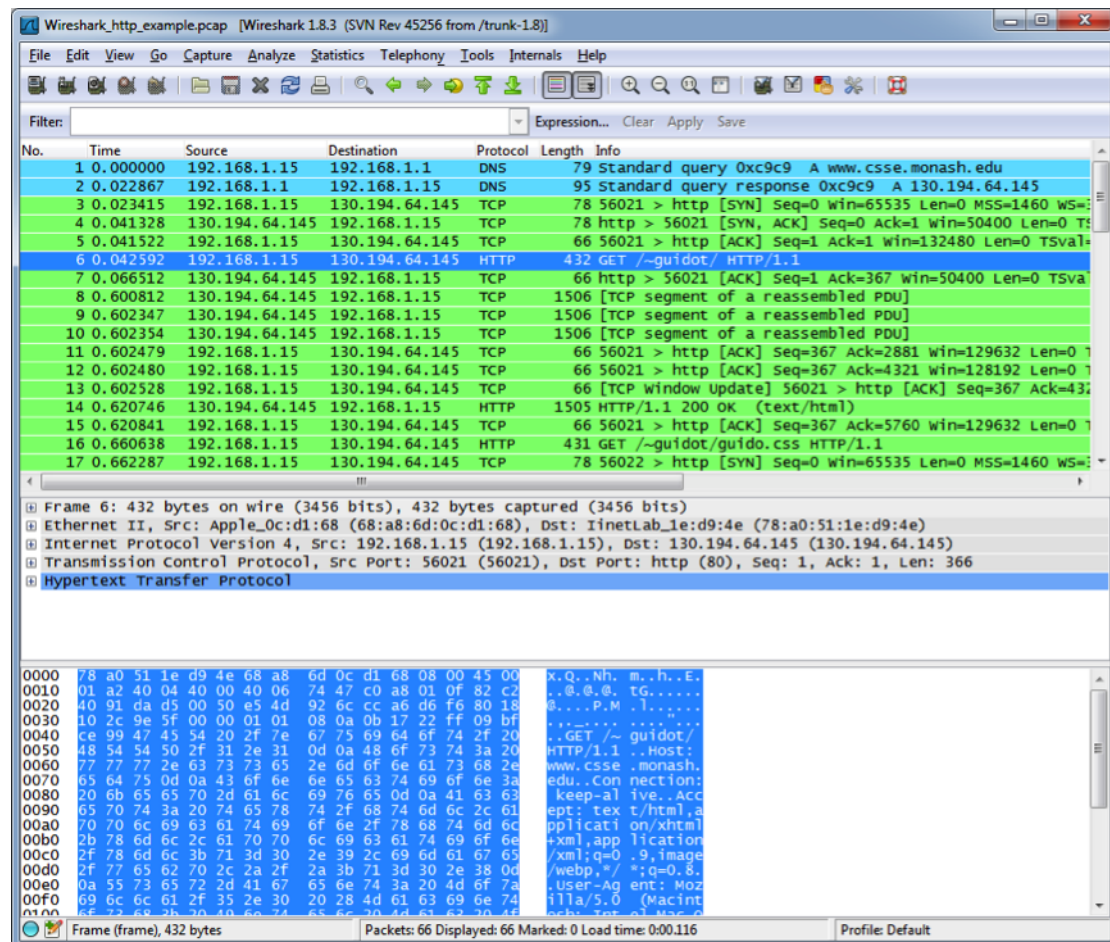

Figure 2: Wireshark File menu

Figure 3: Wireshark main 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 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.

Navigate between the panes and explore the relationships between the displayed pieces of information.

4. Click on frame 6.

   a) How long is it in bytes?

   b) Which application layer protocol does it use?

5. There are five lines in the packet details pane for frame 6, each of which can be expanded by clicking on the "+" symbol.

   a) Can you identify what they stand for?

   b) Which protocols are being used?

   c) What are the names of the PDUs for each protocol?

   d) Recall that each protocol layer encapsulates the message from the layer above and adds a header. What are the sizes of the headers for each PDU used in frame 6?