FIT9137 Applied
Week 6

Topics:

- Protocol Layering

Covered Learning Outcomes:

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

Instructions:

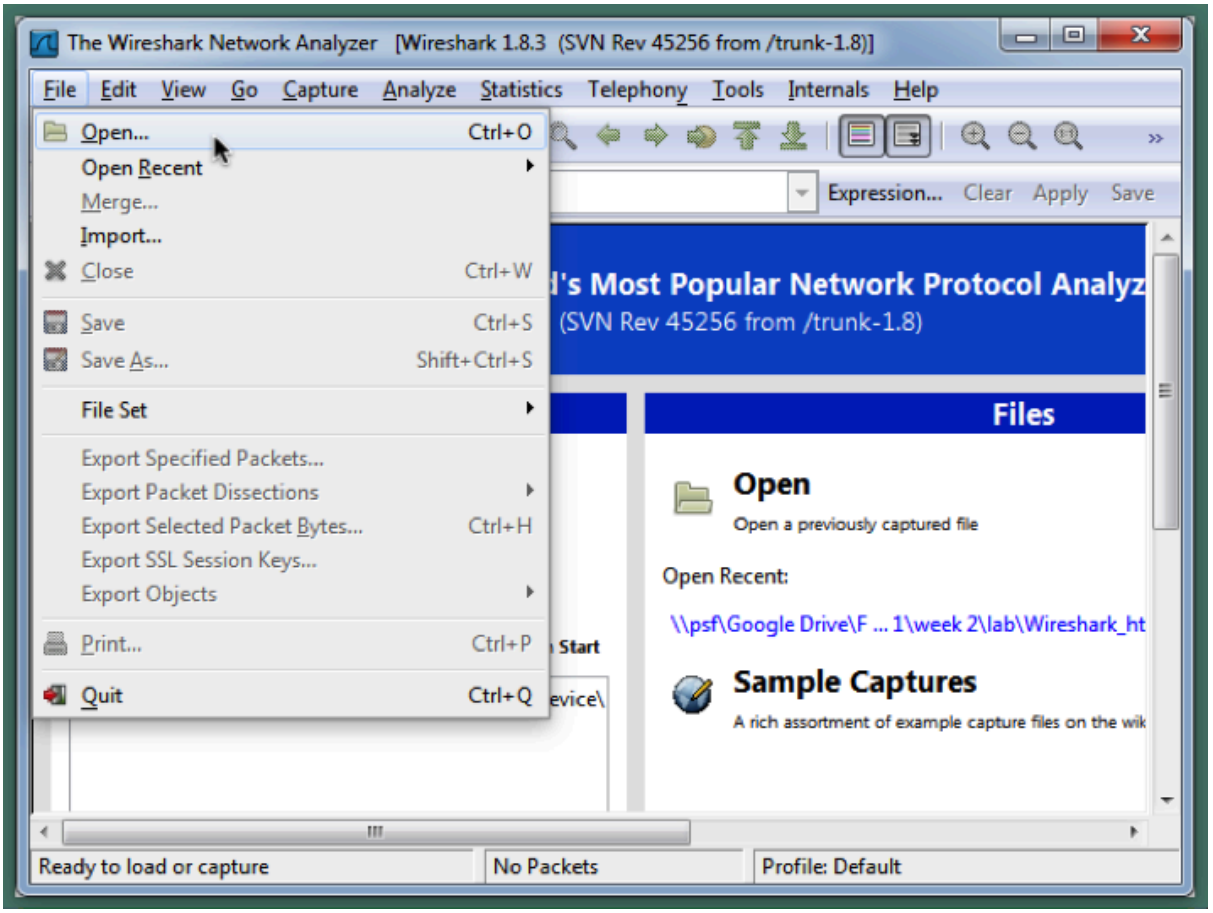
- One of the main purposes of an applied session is to build the learning community, create connections and include the learners. The other goal is to give and receive feedback from your peers and or your tutors.
- Form groups of 2 students (peers) to work through the exercises. If met a problem, try to solve it by asking direct questions to your peer. If the issue was not solved within peers, ask your tutor. If did not get a chance to solve the problem during your applied session with your peer or tutor, jump into one of many consultation hours and ask any of the tutors to help you. Please visit the "Teaching Team and Unit Resources" tile in the FIT9137 Moodle site.

Task A. Understanding Layered Architecture

1. Explain the following concepts in the context of data communication and computer networks:
   - a protocol
   - protocol layering
2. What are the benefits of a layered architecture?
3. Is there any disadvantage to a layered architecture?
4. What is a logical connection?
5. What is "addressing" in a layered architecture?
6. What is Encapsulation and Decapsulation in a layered architecture?
7. What is Multiplexing and Demultiplexing in a layered architecture?

Task B. Using Wireshark

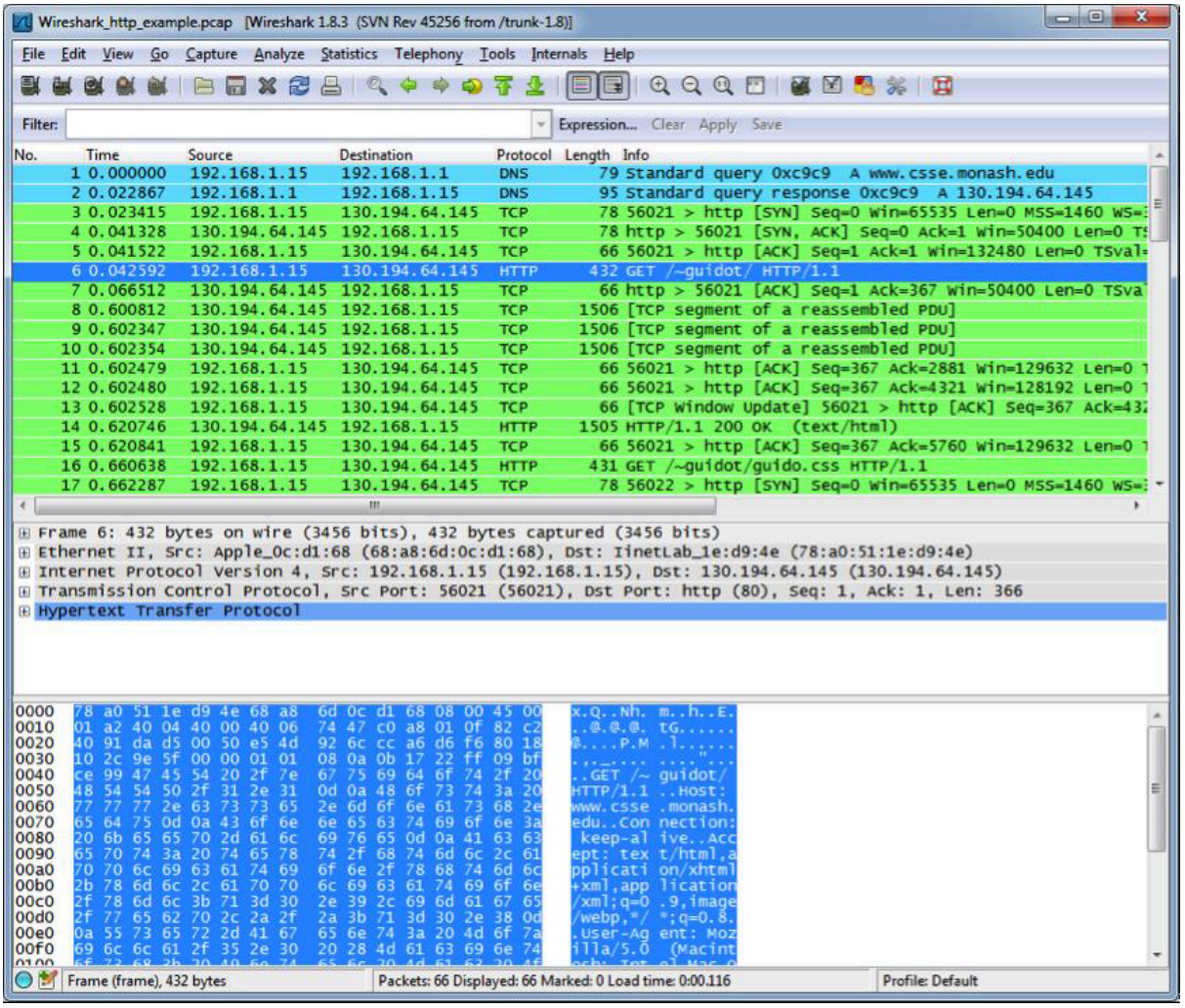
A packet analyser (sometimes also called “packet sniffer”) is a program that can log all packets that are received and transmitted over a network interface. We will be using Wireshark, a very popular open-source tool for packet analysis. You can find this software in your VM. To use it in your host OS, you download it from www.wireshark.org.



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.


Wireshark_http_example.pcap [Wireshark 1.8.3 (SVN Rev 45256 from /trunk-1.8)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: Expression... Clear Apply Save
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 130.194.64.145
3 0.023415 192.168.1.15 130.194.64.145 TCP 78 56021 > http [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=
4 0.041328 130.194.64.145 192.168.1.15 TCP 78 http > 56021 [SYN, ACK] Seq=0 Ack=1 Win=50400 Len=0 TS
5 0.041522 192.168.1.15 130.194.64.145 TCP 66 56021 > http [ACK] Seq=1 Ack=1 Win=132480 Len=0 TSval=
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 http > 56021 [ACK] Seq=1 Ack=367 Win=50400 Len=0 TSva
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 > http [ACK] Seq=367 Ack=2881 Win=129632 Len=0
12 0.602480 192.168.1.15 130.194.64.145 TCP 66 56021 > http [ACK] Seq=367 Ack=4321 Win=128192 Len=0
13 0.602528 192.168.1.15 130.194.64.145 TCP 66 [TCP Window Update] 56021 > http [ACK] Seq=367 Ack=43
14 0.620746 130.194.64.145 192.168.1.15 HTTP 1505 HTTP/1.1 200 OK (text/html)
15 0.620841 192.168.1.15 130.194.64.145 TCP 66 56021 > http [ACK] Seq=367 Ack=5760 Win=129632 Len=0
16 0.660638 192.168.1.15 130.194.64.145 HTTP 431 GET /~guidot/guido.css HTTP/1.1
17 0.662287 192.168.1.15 130.194.64.145 TCP 78 56022 > http [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=
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 (192.168.1.15), Dst: 130.194.64.145 (130.194.64.145)
Transmission Control Protocol, Src Port: 56021 (56021), Dst Port: http (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
00f0 69 6c 6c 61 2f 35 2e 30 20 28 4d 61 63 69 6e 74 illa/5.0 (Macint
Frame (frame), 432 bytes
Packets: 66 Displayed: 66 Marked: 0 Load time: 0:00.116
Profile: Default