Lecture 1 tutorial: Overview of protocols

During tutorials prepare a short report of your activities and show it to your tutor.

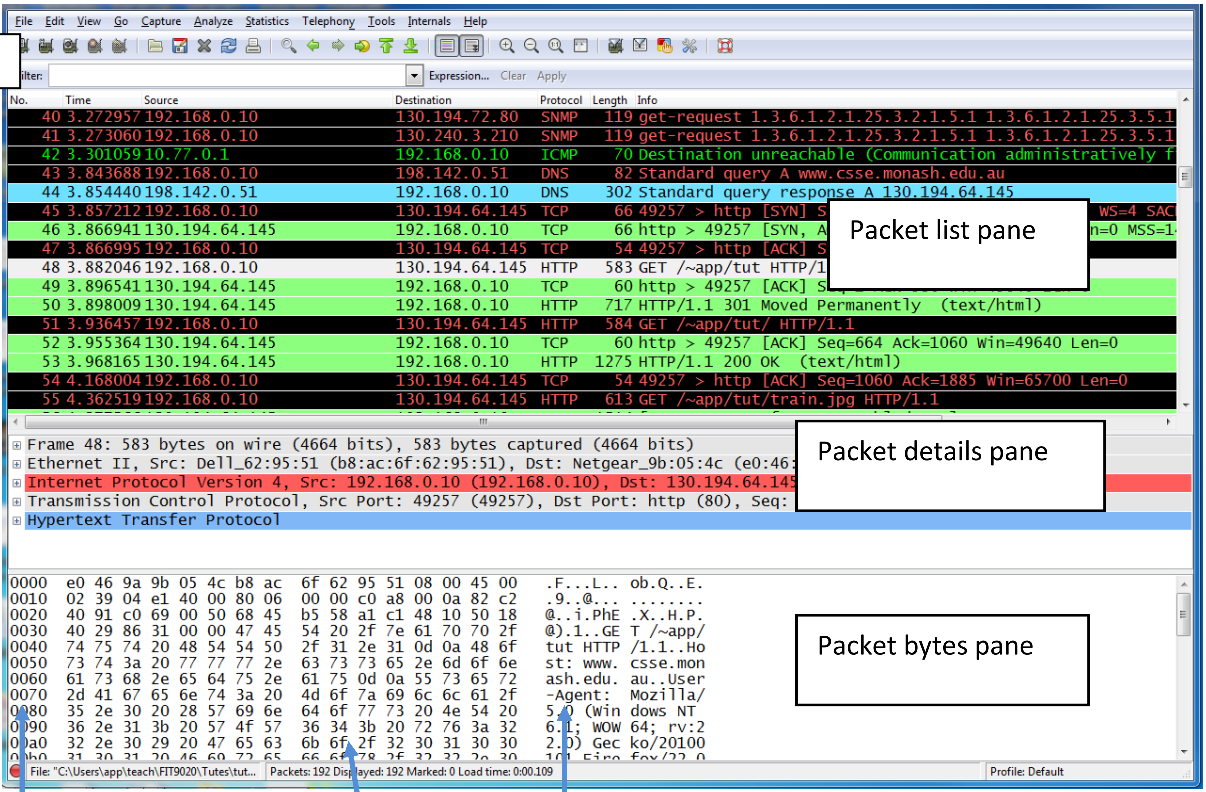
Be aware that the exam question might be directly related to the tutorial questions.

Part 1: Wireshark re-visited

In order to re-familiarize yourselves with the Wireshark, open the file **tutWebPage1.pcap** that was recorded some time ago in my home network

- Open the file tutWebPage1 , Select the frame No. **48** and you should see the screen as in Figure 1:

Figure 1


File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply
Packet list pane
Packet details pane
Packet bytes pane

```
No.  Time     Source          Destination     Protocol Length Info
 40 3.272957 192.168.0.10    130.194.72.80   SNMP     119 get-request 1.3.6.1.2.1.25.3.2.1.5.1 1.3.6.1.2.1.25.3.5.1
 41 3.273060 192.168.0.10    130.240.3.210   SNMP     119 get-request 1.3.6.1.2.1.25.3.2.1.5.1 1.3.6.1.2.1.25.3.5.1
 42 3.301059 10.77.0.1       192.168.0.10    ICMP      70 Destination unreachable (Communication administratively f
 43 3.843688 192.168.0.10    198.142.0.51    DNS       82 Standard query A www.csse.monash.edu.au
 44 3.854440 198.142.0.51    192.168.0.10    DNS      302 Standard query response A 130.194.64.145
 45 3.857212 192.168.0.10    130.194.64.145  TCP       66 49257 > http [SYN] S                        WS=4 SAC
 46 3.866941 130.194.64.145  192.168.0.10    TCP       66 http > 49257 [SYN, A                       n=0 MSS=1
 47 3.866995 192.168.0.10    130.194.64.145  TCP       54 49257 > http [ACK] S
 48 3.882046 192.168.0.10    130.194.64.145  HTTP     583 GET /~app/tut HTTP/1
 49 3.896541 130.194.64.145  192.168.0.10    TCP       60 http > 49257 [ACK] S
 50 3.898009 130.194.64.145  192.168.0.10    HTTP     717 HTTP/1.1 301 Moved Permanently  (text/html)
 51 3.936457 192.168.0.10    130.194.64.145  HTTP     584 GET /~app/tut/ HTTP/1.1
 52 3.955364 130.194.64.145  192.168.0.10    TCP       60 http > 49257 [ACK] Seq=664 Ack=1060 Win=49640 Len=0
 53 3.968165 130.194.64.145  192.168.0.10    HTTP    1275 HTTP/1.1 200 OK  (text/html)
 54 4.168004 192.168.0.10    130.194.64.145  TCP       54 49257 > http [ACK] Seq=1060 Ack=1885 Win=65700 Len=0
 55 4.362519 192.168.0.10    130.194.64.145  HTTP     613 GET /~app/tut/train.jpg HTTP/1.1
```

```
⊞ Frame 48: 583 bytes on wire (4664 bits), 583 bytes captured (4664 bits)
⊞ Ethernet II, Src: Dell_62:95:51 (b8:ac:6f:62:95:51), Dst: Netgear_9b:05:4c (e0:46:
⊞ Internet Protocol Version 4, Src: 192.168.0.10 (192.168.0.10), Dst: 130.194.64.145
⊞ Transmission Control Protocol, Src Port: 49257 (49257), Dst Port: http (80), Seq:
⊞ Hypertext Transfer Protocol
```

```
0000  e0 46 9a 9b 05 4c b8 ac  6f 62 95 51 08 00 45 00   .F...L.. ob.Q..E.
0010  02 39 04 e1 40 00 80 06  00 00 c0 a8 00 0a 82 c2   .9..@... ........
0020  40 91 c0 69 00 50 68 45  b5 58 a1 c1 48 10 50 18   @..i.PhE .X..H.P.
0030  40 29 86 31 00 00 47 45  54 20 2f 7e 61 70 70 2f   @).1..GE T /~app/
0040  74 75 74 20 48 54 54 50  2f 31 2e 31 0d 0a 48 6f   tut HTTP /1.1..Ho
0050  73 74 3a 20 77 77 77 2e  63 73 73 65 2e 6d 6f 6e   st: www. csse.mon
0060  61 73 68 2e 65 64 75 2e  61 75 0d 0a 55 73 65 72   ash.edu. au..User
0070  2d 41 67 65 6e 74 3a 20  4d 6f 7a 69 6c 6c 61 2f   -Agent:  Mozilla/
0080  35 2e 30 20 28 57 69 6e  64 6f 77 73 20 4e 54 20   5.0 (Win dows NT 
0090  36 2e 31 3b 20 57 4f 57  36 34 3b 20 72 76 3a 32   6.1; WOW 64; rv:2
00a0  32 2e 30 29 20 47 65 63  6b 6f 2f 32 30 31 30 30   2.0) Gec ko/20100
00b0  31 30 31 20 46 69 72 65  66 6f 78 2f 32 32 2e 30   101 Fire fox/22.0
```

File: "C:\Users\app\teach\FIT9020\Tutes\tut... | Packets: 192 Displayed: 192 Marked: 0 Load time: 0:00.109 | Profile: Default

Offset (byte numbers) **ASCII** representation of bytes of the frame

Hexadecimal representation of bytes of the frame

You current version of the Wireshark can be a bit different. Refresh you Wireshark skill moving between all three pans.

Q1: Investigating protocols invoked at the start-up of the network connection

- Disconnect your PC from the network (both the Ethernet/cable and the wireless connections) or disable both adapters.

- Clear the IP configuration with typing in the command window: **ipconfig /renew** Most likely you will need to run the command window as an **administrator**.
- Clear the **arp** table typing in: **arp /d**
- Invoke the **Wireshark** (possibly as an administrator) on the Ethernet Network Connections. No frames should be coming at this stage.
- Plug in the Ethernet cable, or enable the adapter, and record, say, 250 frames. For reference, you can find **my Wireshark startup** file on Moodle (**t01:Wrshrk_startup**)

- ➢ **Create a list of all protocols** in the recorded frames and check it against the slides 14–28. Have I missed any protocol in my slides?
- ➢ Memorize at least 10 protocols from your list (different than HTTP and TCP)

Q2: Investigating the SSDP protocol

- In the previously recorded Wireshark file find the frame with the **SSDP protocol**
- Download the standard for this protocol (slide 28) and **explain** the **format, contents and function** of the **M-SEARCH * HTTP/1.1** command.
  If you have problems with your Wireshark recording, you can use the **frame 2** from my Wireshark file. Think about Q2 as a potential **exam question**.

Q3: With reference to a network as in slides 9-13 explain:

- Why the routing computers (aka routers) do not have the transport and application layers implemented?
- What addresses are used to send packets between the two routers?

Q4: With reference to the slide 15 and RFC 2516 describe the structure of the **PPPoE** frame(s)

Q5: With reference to the slide 16 and RFC 3931 describe the structure of the L2TP frame(s)