<u>Lab 1</u>

(All your answers should be validated with the screen shots that you take during this exercise)

- 1. For this lab you'll need the Wireshark program installed, which can be obtained from http://www.wireshark.org. It is a free software and supports many platforms.
- 2. When you first start Wireshark you will be brought to the default startup screen, similar to one given below. In order to begin a network capture you will need to choose a network device to use.



If you want to capture packets sent directly to your device only, that you have to uncheck the "Capture packets in promiscuous mode" checkbox.

🚺 Wireshark · Pref	nces	?	\times
 Appearance Layout Columns Font and C Capture Filter Expression Name Resoluti Protocols Statistics Advanced 	Default interface Image: Capture packets in promiscuous mode Image: Capture packets in pcap-ng format Image: Capture packets in pcap-ng format		>
	OK Cancel	Hel	p

Then click Capture->Start from the menu and if your network card is working you should very quickly start to see lines appearing in your packet capture window (see example below).

The Main window

Wireshark's main window consists of parts that are commonly known from many other GUI programs.

File Edit View Go Canture Analyst	e Statistics Telepho	ny Wireless	ss Tools Help	
		= <u>a</u> a	8 H	
				-
Abby a gaplety tale <cdhc></cdhc>				Colossial
ia, Tine Source	Destination	Protocol	Length Info	
343 05.142615 192.168.0.21	174,129,249,228	TCP	00 40955 + 00 [ACK] Seq=1 ACK+1 Win+5000 Lem=0 T5va1+491519340 T5ecr=551	11827
344 05.142715 192.168.0.21	174,129,249,228	HITP .	253 OET /clients/netflix/flash/application.swf/flash_version=flash_lite_2	18071.560
345 45 249242 124 126 249 298	196-100-0-61	HTTP	838 MLLD(1 1 983 Noved Internation Prime Date (2001a227071030 (Sector) 00 06 - 46222 [W/V] 26647 WC64700 Prime Date (2001a227071030 (Sector)	1223394
347 65 341503 103 168 8 31	174 120 340 228	TCP	66 40555 a 88 FAFWT Same188 ArkeJ63 pineJ434 Laned T6uale401510446 TGerm	451811852
· 348 65 242532 192 168 8 21	192.168.0.1	DIS	77 Standard puery 9x2188 & cdn-0.nflxing.com	77X022074
349 65,276870 192,168,0,1	192,168,0.21	DNS	499 Standard query response 0x2188 A cdn-0.nflylee.com CNAVE issues.netfl.	w.con.pder
358 65.277992 192.168.0.21	63.88.242.48	TCP	74 37063 + 80 [SYN] Seg=0 Win=5840 Len=0 MSS=1460 SACK PERM=1 TSval=4015	19482 TSec
351 65.297757 63.80.242.48	192.168.0.21	TCP	74 88 + 37863 [SYN, ACK] Seg-8 Ack-1 Win-5792 Len-8 MSS-1468 SACK PERM-1	TSva1-3295
352 65.298396 192.168.0.21	63.80.242.48	TCP	66 37063 = 80 [ACK] Seg=1 Ack=1 Win=5888 Len=0 TSval=491519582 TSecr=329	5534138
353 65.298687 192.168.0.21	63.88.242.48	HTTP	153 GET /us/nrd/clients/flash/814540.bun HTTP/1.1	
354 65.318730 63.80.242.48	192,168.0.21	TCP	66 80 + 37863 (ACK) Seq=1 Ack=88 Win=5792 Len=0 T5val=3295534151 T5ecr=48	91519503
355 65.321733 63.80.242.48	192.168.0.21	TCP	1514 [TCP segment of a reassembled PDU]	
				13
Frame 349: 489 bytes on wire (3 Ethernet II, Src: Globalsc 00:3 Internet Protocol Version 4, Sr User Datagram Protocol, Src Por 'Domain Name System (response)	912 bits), 489 byt biða (fðiadi4e:80: c: 192.168.0.1, Ds t: 53 (53), Dst Po	es capture 3b:0a), De ti 192.168 rti 34036	ed (3912 bits) st: Viric_14:Sarel (00:10:9d:14:Sarel) 5.0.21 (34036)	
Frame 349: 489 bytes on wire (3 Ethernet II, Src: Globalsc 00:3 Internet Protocol Version 4, Sr User Datagram Protocol, Src Por Domain Name System (response) [Recuest In: 348] [Time: 0.034338000 seconds] Transaction ID: 0x2188 Flags: 0x8180 Standard query Questions: 1 Answer RBs: 4 Authority RBs: 9 Additional RBs: 9	912 bita), 489 byt biBa (f0iadi4e:80) c: 192.168.0.1, Ds t: 53 (53), Dst Po response, No erro	es capture 3b:0a), De ti 192.168 rti 34036	ed (3912 bits) st: Virio_14:8a:e1 (00:19:9d:14:8a:e1) 8.0.21 (14036)	
Frame 349: 489 bytes on wire (3 Ethernet II, Src: Globaler 00:3 Internet Protocol Version 4, Sr User Datagram Protocol, Src Poor Domain Name System (response) [Request In: 345] [Time: 0.034330000 seconds] Transaction ID: 0x128 > flags: 0x0100 Standard query Questions: 1 Answer RRs: 4 Authority RRs: 0 Additional RRs: 0 Y Queries	912 bita), 489 byt b:Ba (f0:adi.4e:R0: c: 192.168.0.1, Ds t: 53 (53), Dst Pa response, No erro	es capture 3b:0a), De ti 192_168 rt: 34036	ed (3912 bits) st: Virio_14:Sa:e1 (00:19:9d:14:Sa:e1) S.0.21 (34036)	
Frame 349: 489 bytes on wire (3 Ethernet II, Src: Globalce 00:3 Internet Protocol Version 4, Sr User Datagram Protocol, Src Por Domain Name System (response) [Sequest Inn 345] [Time: 0.034338000 seconds] Transaction 10: 0x2108 > flags: 0x8100 Standerd query Questions: 1 Answer RRs: 4 Authority RRs: 9 Additional RRs: 9 Y Queries > cdn-0.nflxing.com: type A,	912 bita), 489 byt bida (f0iadi4e:00) c: 192.168.0.1, Ds t: 53 (53), Dst Po response, No erro , class IN	es capture 3b:0a), De ti 192.168 rti 34036	ed (3912 bits) st: vizio_14:Sa:e1 (00:19:9d:14:Sa:e1) S.0.21 (34036)	
Frame 349: 489 bytes on wire (3 Ethernet II, Src: Globales 00:3 Internet Protocol Version 4, Sr User Datagram Protocol, Src Por Domain Name System (response) [hequest In: 345] [Time: 0.034330000 seconds] Transaction ID: 0x2188 > flags: 0x8100 Standard query Questions: 1 Answer RRs: 4 Authority RRs: 9 Additional RRs: 9 Y Queries > cdn-0.nflxing.com: type A, > Answers	912 bits), 489 byt b:8a (f0:adi4e:00) c: 192.168.0.1, Ds t: 53 (53), Dst Pp response, No erro , class TN	es Capture 3b:00), De ti 192.168 rti 34056	ed (3912 bits) st: virio_14:Barel (00:19:9d:14:Barel) 6.0.21 (34036)	
Frame 349: 489 bytes on wire (3 Ethernet II, Src: Globaler 00:3 Internet Protocol Version 4, Sr User Datagram Protocol, Src Por Domain Name System (response) [frames trin 348] [Time: 0.034338000 seconds] Transaction 10: 0x2188 > flags: 0x8100 Standard query Questions: 1 Answer RRs: 4 Authority RRs: 9 Additional RRs: 9 > cdn-0.nflxleg.com: type A, > Answers > Authoritative nameservers	012 bits), 480 byt bida (f0:adi4e:00: c: 102.160.0.1, Ds t: 53 (53), Dst Po response, No error , class IN	es capture 3b:0a), De ti 192.166 rti 34036	ed (3912 bits) st: Virio_14:Ea:e1 (00:19:9d:14:Ea:e1) 6.0.21 (14036)	
<pre>> Frame 349: 489 bytes on wire (3 > Frame 349: 489 bytes on wire (3 > Ethernet II, Src: Glabaler 00:3 > Internet Protocol Version 4, Sr User Datagram Protocol, Src Peer > Domain Name System (response) [Sequent In: 346] (Time: 0.034330000 seconds] Transaction 10: 0x2188 > Flags: 0x8100 Standard query Questions: 1 Answer RRs: 4 Authority RRs: 9 Additional RRs: 9 > Additional RRs: 9 > Additional RRs: 9 > Authoritative nameservers 0020 00 15 00 35 84 f4 01 c7 83 0020 00 15 00 35 84 f4 01 c7 83 0020 00 15 00 35 84 f4 01 c7 83 0020 00 5 00 05 00 35 84 f4 01 c7 83 0020 00 5 00 05 00 05 39 06 22 07 6e 65 74 66 6c 69 78 83</pre>	912 bita), 489 byt b:8a (f0:ad:4e:80; c: 192.168.0.1, Ds t: 53 (53), Dst Po response, No erro , class IN 2f 61 df 81 80 00 6e 2d 30 87 5e 65 09 01 00 01 c0 00 65 69 6d 61 67 65 36 6f 6d 89 55 54	es capture 3b:0a), De t: 192.168 rt: 34856 r 7 00 xing 73 00 xing 73	ed (3912 bits) st: virio_14:8a:e1 (00:19:9d:14:8a:e1) 8.0.21 (34036) 5fm_sc: c dn=0.mfl g.com c dn=0.mfl g.com c images tflix .com.edg	
Frame 349: 489 bytes on wire (3) Fthernet II, Src: Globalcc 00:3 Internet Protocol Version 4, Sr User Datagram Protocol, Src Por Domain Name System (response) <u>[Sequent in: 345]</u> (Time: 0.034338000 seconds] Transaction ID: 0x2188 > Flag:: 0x8100 Standard query Questions: 1 Answer RRs: 4 Authority RRs: 9 * Queries > cdn-0.nflxing.com: type A, > Answers > Authoritative nameservers 0020 00 15 00 35 84 f4 01 c7 83 00 04 00 05 00 99 05 63 64 05 00 81 06 00 05 90 89 20 05 08 20 69 78 83 000 05 00 81 06 00 55 98 62 07 65 74 66 52 98 83 070 53 73 75 69 74 65 03 66 65	912 bita), 489 byt b:8a (f0:ad:4e:80: c: 192.168.0.1, Ds t: 53 (53), Dst Po response, No erro , class IN 3f 14 15 81 80 00 66 20 30 07 56 65 00 01 00 01 c0 00 65 69 66 61 67 65 63 67 66 69 65 64 74 00 c0 27 00 05	es capture 3b:0a), De t: 192.168 rt: 34856 rt: 34856 r 90 xing 73 80 esuit	ed (3912 bits) st: virio_14:8a:e1 (00:19:9d:14:8a:e1) 8.0.21 (34036) 5	

You can see, that the main window consists of three different panes: Packet list pane, Packet details pane, and Packet bytes pane.

Each line in the packet list corresponds to one packet in the capture file. If you select a line in this pane, more details will be displayed in the "Packet Details" and "Packet Bytes" panes.

There are different columns in the list pane, but the default columns will show:

- No. The number of the packet in the capture file. This number won't change, even if a display filter is used.
- **Time** The timestamp of the packet.
- **Source** The address where this packet is coming from.

- **Destination** The address where this packet is going to.
- **Protocol** The protocol name in a short (perhaps abbreviated) version.
- Length The length of each packet.
- Info Additional information about the packet content.

If you double click on the packet line you can obtain more details about that specific packet.

While your capture is running, you can stop it by hitting the Capture->Stop, or pressing the "stop capture" button (red square). You can save the capture by clicking on the "save capture button" in your selected folder. By now, you should have enough data to start to analyze.

Filtering packets

Wireshark can filter packets while capturing or displaying. Display filters allow you to concentrate on the packets you are interested in while hiding the currently uninteresting ones. They allow you to select packets by:

- Protocol
- The presence of a field
- The values of fields
- A comparison between fields etc.

Examining the Packet Capture

- Start a new Capture
- Open the Browser
- Type a web page address (ex. <u>www.mercy.edu</u>)
- Apply a filter for "TCP" protocol.
- Stop the Capture.
- Now you can isolate a TCP stream.
- Right click on a packet in the Packet List and select Follow TCP Stream. This creates an automatic Display Filter which displays packets from that TCP session only.
- It also displays a session window, which is by default, an ASCII representation of the TCP session, where the client packets are in red and the server packets in blue. Change to Hex Dump Mode and view the payloads in raw Hex.
- Wireshark automatically creates a display filter to filter out this TCP conversation.

- 1. From your Wireshark Capture, write the **IP Addresses** and **Port Numbers** for the Client and the Server.
- 2. What **HTTP** version is your browser running? What version of **HTTP** is the server running?
- 3. Identify the **TCP** segments that are used to initiate the **TCP** connection between the client computer and <u>www.mercy.edu</u>.
- 4. For each packet in the **TCP 3-way** handshake, write the Sequence and Acknowledgement numbers.
- You can see the flow traffic with **Statistics->Flow Graph** menu option, too.
 - 5. What are the sequence numbers of the first four **data-carrying segments** in the TCP connection?
 - 6. What is the length of each of these four **TCP segments**? The length of the TCP segment is only the number of data bytes carried inside the segment (excluding the headers).
- Run *nslookup* to determine the authoritative **DNS** servers for your university.
- Enter "dns && ip.addr == host_IP_address" into the display filter, where you obtain host_IP_address with ipconfig.
- Locate the **DNS query** and **response** messages.
 - 7. Are they transported using **UDP** or **TCP**? Explain why or why not.
 - 8. What is the destination port for the **DNS query** message?
 - 9. What is the source port of **DNS response** message?
 - 10. With statistics -> conversations, find which hosts sent and received the most packets?