**WIRESHARK LABS**

I would like to share my experience and the issues I faced while completing my Wireshark Labs. I started first of all with the main Intro Lab where I downloaded the Wireshark file from the given link I didn’t face any issues while downloading the file. The Installation of the file was very easy and I was able to follow all the steps for Installation. Then I faced difficulty in downloading the labs. I was not able to download the labs on my laptop but that issue got solved in the evening. I downloaded all the files and started with my labs. I majorly focussed on the diagram that is given in the intro lab and while following the steps I kept an Eye that my output should be similar to the diagram in the lab book. So when I started with my first lab I first understood which packet I need to trace and as my connection is on a Wifi interface. I decided to start packet tracing on the Wifi Network interface as there was major traffic only on Wifi Network then I opened my web browser and entered the URL given in the Lab book and it was working well. Then as I wanted to check the HTTP message exchange I wrote HTTP in the display filter of the Wireshark and I was able to see the HTTP message that was exchanged with the gaia.cs.umass.edu web server. This was something new to me as I was using Wireshark after many years. So I was looking forward to learning more and then decided to go with my 2nd lab where I learned more about HTTP GET/Response. I didn’t face any challenges but I forgot to clear the cache and started the packet capture I did not get the exact output so I decided to do the process again and the second time I did get the output. Here an HTTP message was placed inside a TCP and this was then transported in a Wi-fi Frame in my case. Wireshark displayed the frame, Wifi, IP, and TCP packet information as well. As a Fun part, I also tried to solve the question of the second lab. Then I started with the DNS lab here I understood the Domain Name server helps in translating the hostname into IP addresses. I came across the nslookup command whose main task is to write a query to the DNS server to get a DNS record. As we know that if we go across a webserver that record is stored in a server. The DNS can be a root server, an authoritative server, or an intermediate server but here in my case when I cleared the cache and when a nslookup [www.nyu.edu](http://www.nyu.edu) I got only a non-authoritative server. I also got some ns lookup commands such as A record, NS record, SOA record, MX record, and Reverse DNS lookup. In this lab we, made use of -type=NS record which helps in getting the authoritative servers for the given nyu website. Then I cleared the cache on the web browser ran nslookup on the command prompt and started capturing packets on wireshark when the process was completed I stopped packet tracing and wrote dns in the display filter which showed up with display packets. I then proceeded with TCP lab which is called the Transmission control protocol here as a lab procedure firstly I went on the link and copied the entire Alice text into notepad and saved it as Alice.txt and then uploaded it on another link. Before uploading I started the Wireshark for packet tracing and then uploaded the alice.txt file and for the fun part I also answered the question of the lab. The HTTP POST has reassembled TCP segment when we uploaded the alice.txt file as this POST message has the contents of the Alice file in response when the image is uploaded we get OK in response. Then further I wrote tcp in the Display filter to capture tcp packets. When the SYN bit is set it is the first TCP segment in the three-way handshake method and SYNACK is the second step and then to trace TCP congestion we made use of TCP Graphing utilities called Time Sequence Graph(Stevens) and the I zoom in and out and clicked on the direction part to get the same result as given in the figure. After completing this lab I went on doing the UDP lab where I ran the nslookup command on the command prompt for [www.nyu.edu](http://www.nyu.edu) before running nslookup I cleared cache and started packet tracing on wireshark and then ran nslookup and as the process was completed I stopped packet tracing went to the display filter and type dns so that it can show only the DNS packets that have been captured. Then I started with the IP lab i.e internet protocol which focussed on IPv4 and IPv6 datagram. Here I learned for capturing packets using a traceroute. Traceroute firstly sends IP datagram to the TTL field and after this the IP header will be set to 1 and then IP datagram are sent to the same destination but now it will set the TTL value to 2 and 3 and so on. Router in this does the opposite process it will decrement its TTL each time it receives and when it reaches to zero the router will revert host with an ICMP message. Here in my case I made use of tracert command instead of using traceroute as I am using windows computer but tracert command has a disadvantage that it will not generate large ICMP messages so here I made use of a ping plotter to execute this lab though I was asked to execute with tracert. Then I started with NAT LAB and to be honest I was not sure of what to perform in the Lab so I decided to move further with another lab. Here I understood NAT is network address translation and it helps the host to communicate with the server in a LAN connection. I then started with the ICMP lab to capture the ICMP packet where I understood the concept of PING and it is useful for troubleshooting purpose if suppose I send a ping request and the target destination is live it will respond back so here we ping a webserver and captured ICMP packets on the wireshark and in last I came across DHCP( Dynamic Host Configuration Protocol) which helps the hosts to assign IP addresses Automatically and this concept was brought in use to save IP address and whenever needed the host will be assigned with an IP address. Here to perform lab work I followed the commands ipconfig /release and then started Wireshark to capture packet and then ran ipconfig /renew for some time and stopped tracing and then in display filter I wrote dhcp to DHCP packet. Doing this lab took me 3 days as I also focussed on solving the problems but as I was getting near to deadline I just performed the LAB.