***Lab Title:*** Wireshark – DNS

**Name: Mujtaba Shahid Faizi**

**Regn No: 131818**

**Your current IP address: 10.99.0.227**

***Instructions:***

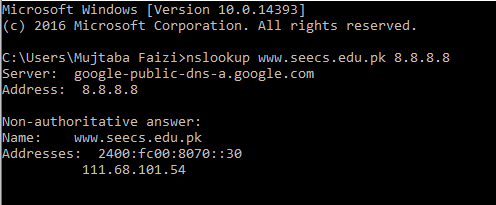
* *Read carefully before starting the lab.*
* *These exercises are to be done individually.*
* *You are supposed to provide the answers to the questions listed at the end of this document and upload the completed report to your course’s LMS site.*
* *Avoid plagiarism by copying from the Internet or from your peers. You may refer to source/ text but you must paraphrase the original work.*

***Steps for performing this lab:***

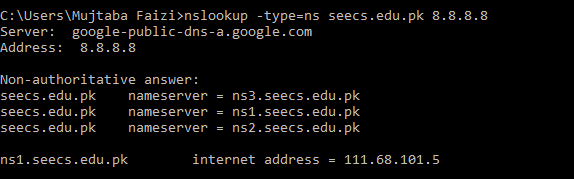
***Exercise 01: nslookup***

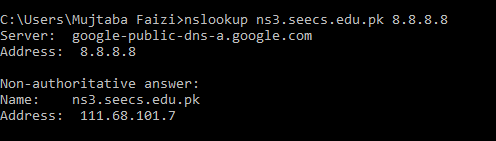
You have to use 8.8.8.8 as your local DNS server for all these exercises. Do the following (and write down the results):

**1.1 Run *nslookup* to obtain the IP address of the Web server hosting www.seecs.edu.pk.**

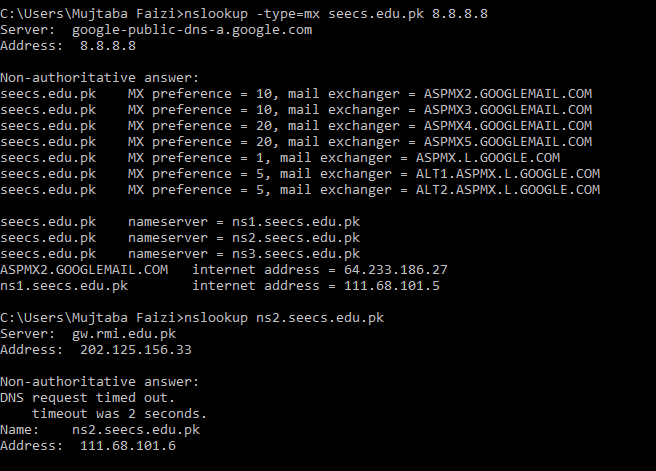


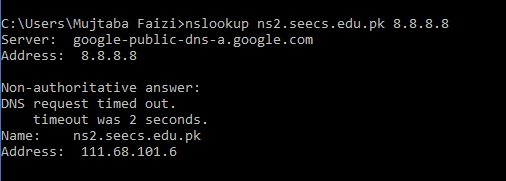
**1.2 Run *nslookup* to determine the authoritative DNS servers for domain seecs.edu.pk. Provide both the names of these DNS servers and also the IP addresses of one of the DNS servers.**



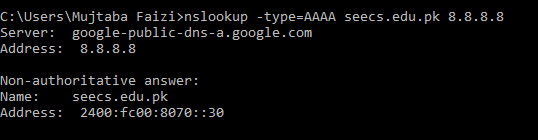


**1.3 Run nslookup to determine the mail servers for** [seecs.edu.pk](http://www.seecs.edu.pk)**. Provide both the names of these Mail servers and also the IP address of one of these Mail servers.**



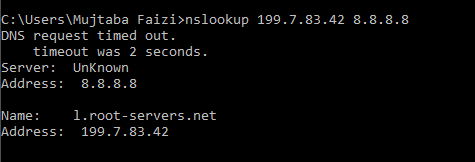


**1.4 Query the public DNS service provided by Google at 8.8.8.8 to query for the IPv6 address of www.seecs.edu.pk. Provide the IPv6 address. Note how this address is different from the IPv4 addresses that you were getting for the previous questions.**

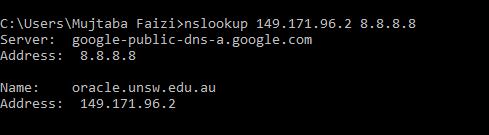


***IPv6 is in hexadecimal with greater bits whereas IPv4 is in number format.***

**1.5 Find out the IP address of at-least one ROOT name server located in Pakistan.**



**1.6 Find out the fully qualified domain name for IP address 149.171.96.2**



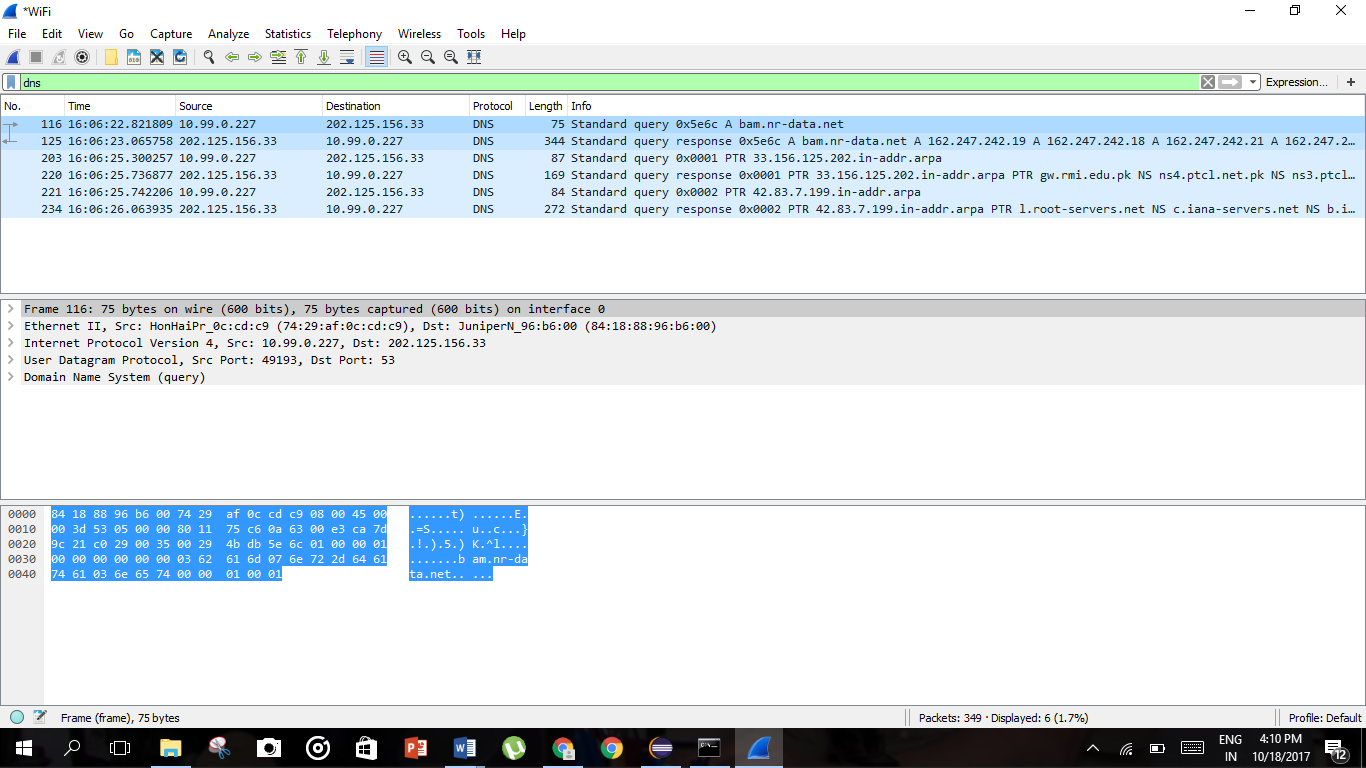
***Exercise 02: Tracing DNS with Wireshark (while using browser)***

Now that we are familiar with *nslookup* and *ipconfig*, we’re ready to get down to some serious business. Let’s first capture the DNS packets that are generated by ordinary Web-surfing activity.

* Use *ipconfig* to empty the DNS cache in your host.
* Open your browser and empty your browser cache. (With Internet Explorer, go to Tools menu and select Internet Options; then in the General tab select Delete Files.)
* Open Wireshark and enter “ip.addr == your\_IP\_address” into the filter, where you obtain your\_IP\_address with ipconfig. This filter removes all packets that neither originate nor are destined to your host.
* Start packet capture in Wireshark.
* With your browser, visit the Web page: http://www.uts.edu.au
* Stop packet capture.

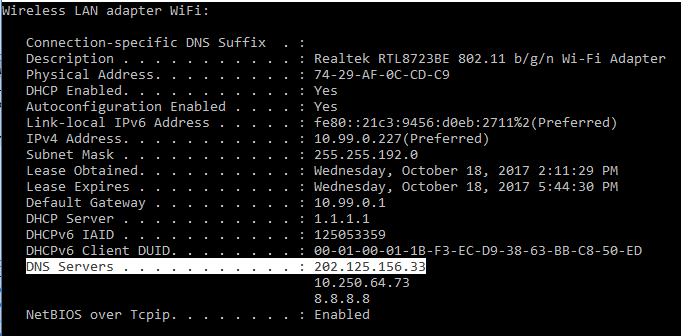
Answer the following questions:

* 1. **Locate the DNS query and response messages. Are these sent over UDP or TCP (i.e., what transport layer protocol is being used)?**

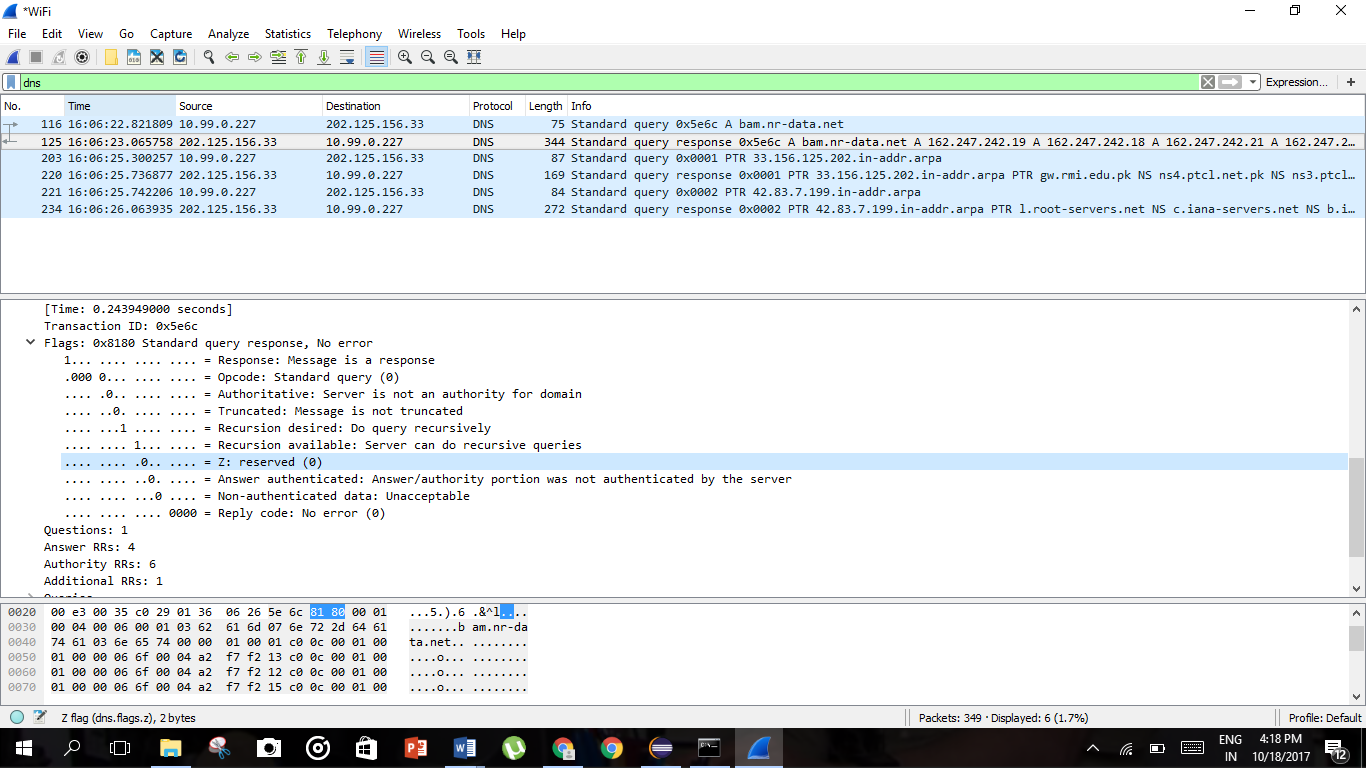


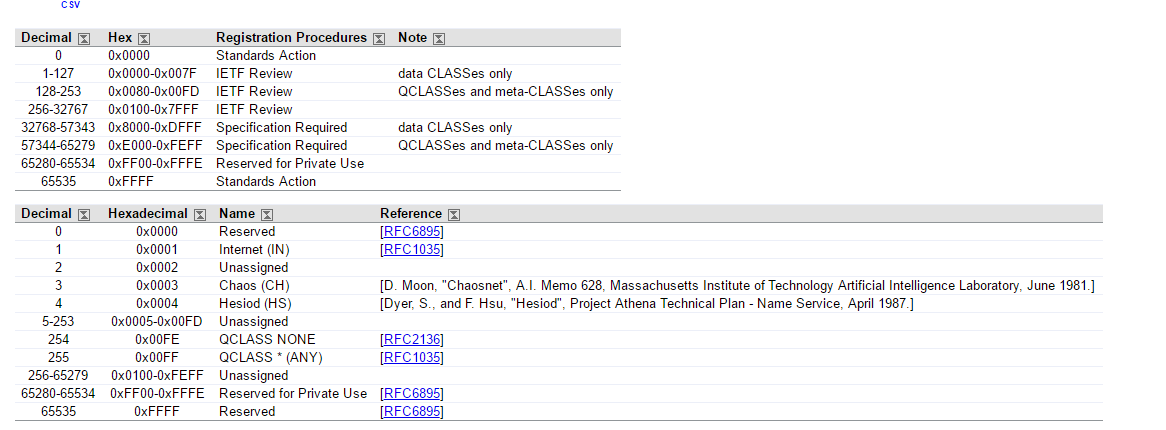
**DNS uses only UDP**

* 1. **To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?**



***2.3* What is contained in the flag field of your DNS request and response? Explain each set bit.**





***2.4* What %age is the delay of DNS resolution as compared with the total page load time?**

***DNS=y=36.710224-36.3538658=0.171566***

Total page load time=x=41.278696-36.538658=4.740038

%delay=(y/x)\*100=3.62%

