DNS& WIRESHARK EXPERIMENT

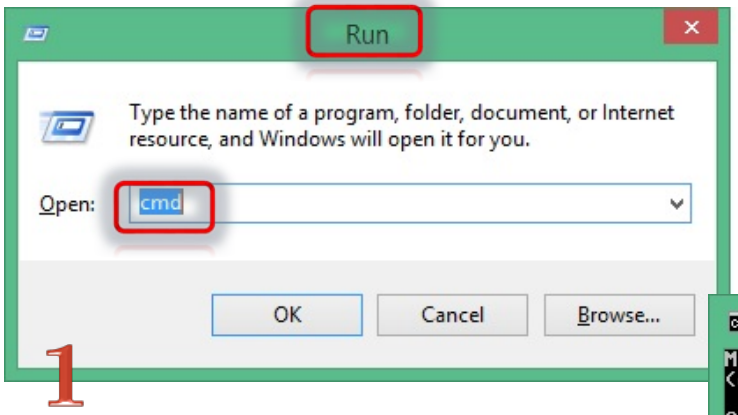
Acknowledgement: Derived for the course by Ibrahim Aljubayri from exercises in Kurose and Ross text (See references provided in the first lecture)

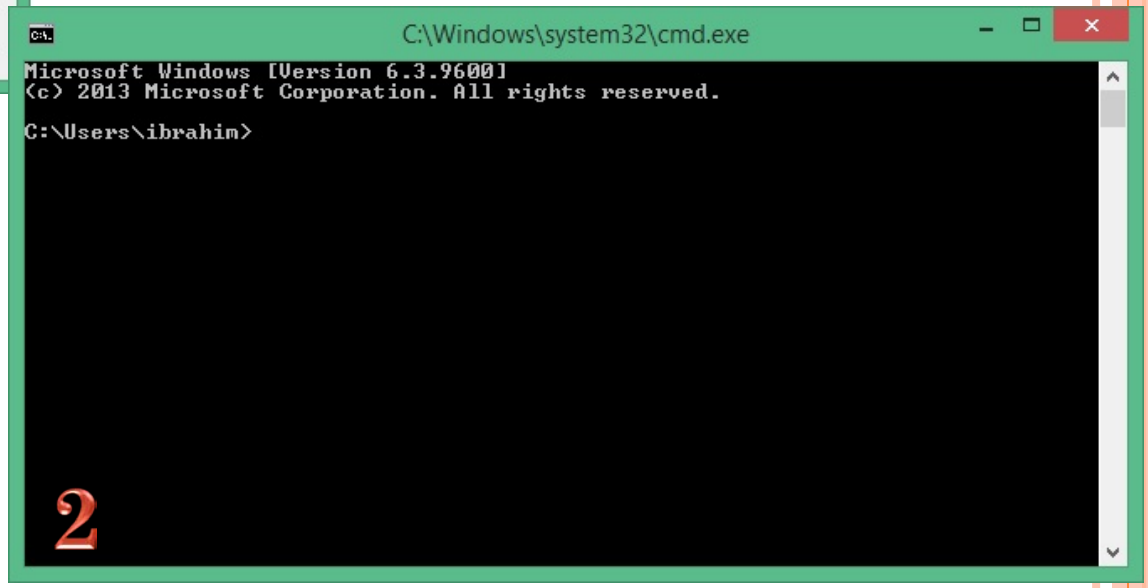
DNS Experiment

- In this lab, we'll take a closer look at the client side of DNS

- We will start by use of the nslookup tool, which is available in most Linux/Unix and Microsoft platforms. To run "nslookup" in Windows, open the Command Prompt and run nslookup on the command line

- We start by opening the Windows Command Prompt application.
- Go to Run → cmd

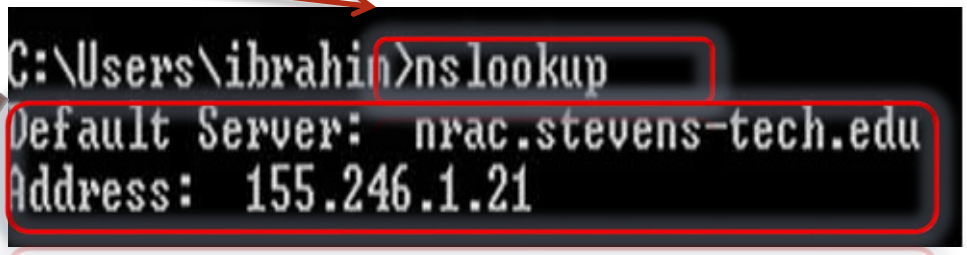


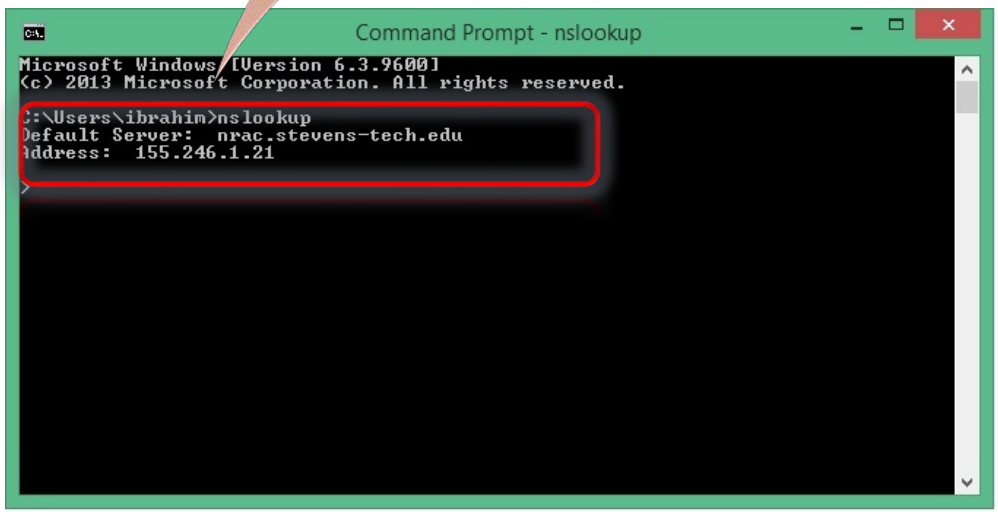


NSLOOKUP

- “nslookup” tool allows the host running the tool to query any specified DNS server for a DNS record. The queried DNS server can be a root DNS server, a top-level-domain DNS server, an authoritative DNS server, or an intermediate DNS server. To accomplish this task, nslookup sends a DNS query to the specified DNS server, receives a DNS reply from that same DNS server, and displays the result.

- After we open the cmd window, we type in “nslookup”





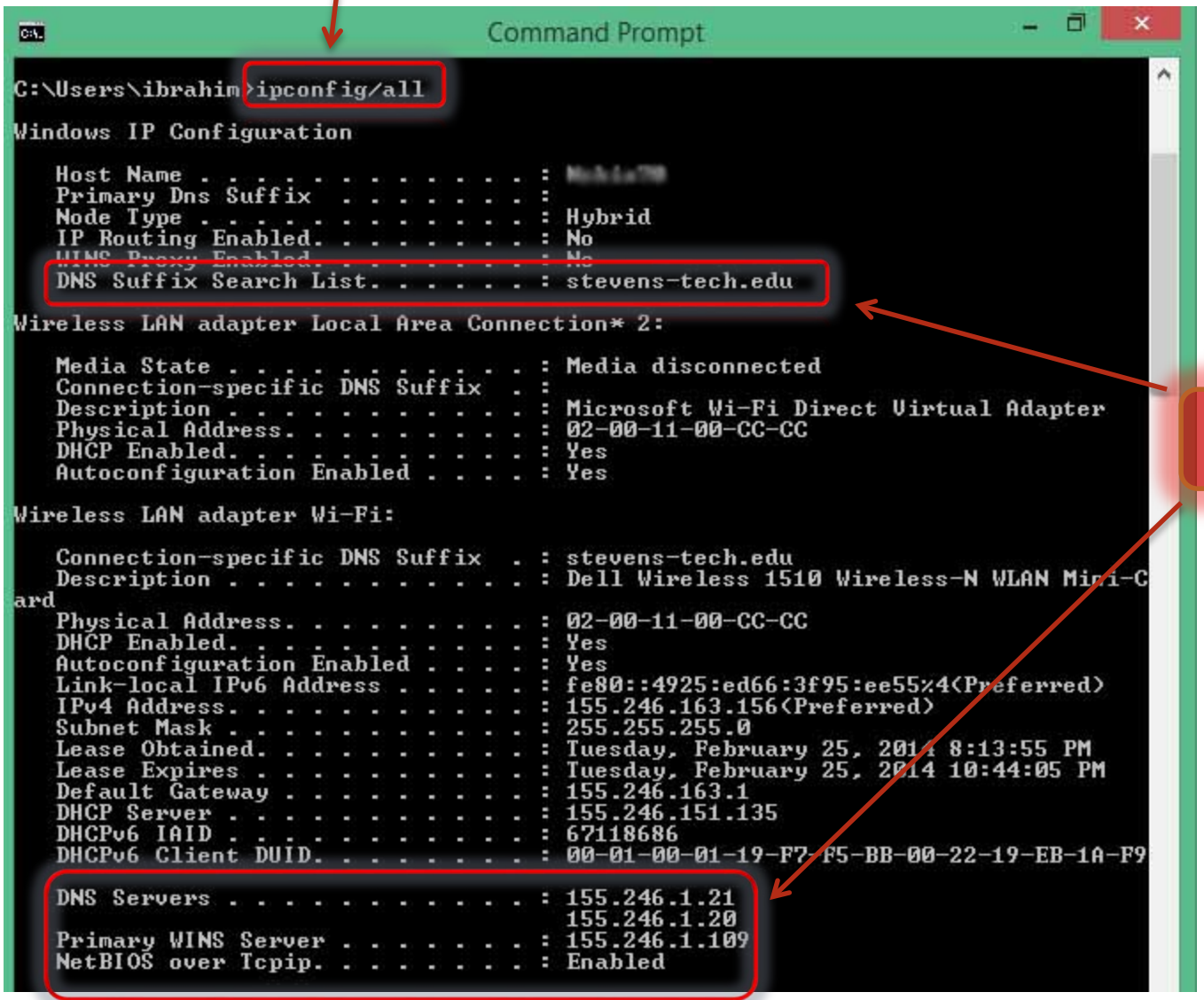
DNS server details

- Also we can check actual ip address for a specific website. For example Google. “nslookup www.google.com”

IPCONFIG

- ipconfig is among the most useful little utilities in your host. ipconfig can be used to show your current TCP/IP information, including your DNS server

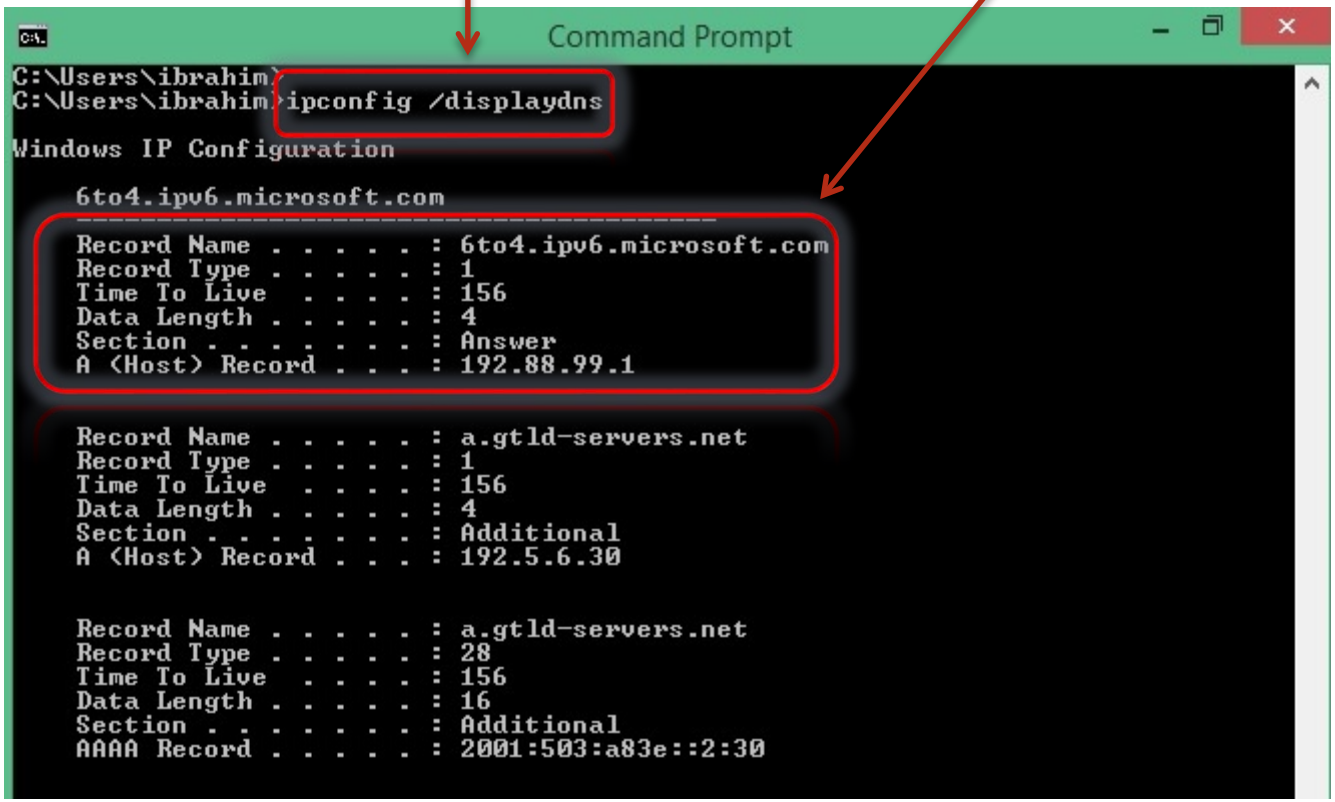
- Type in “ipconfig /all”



DNS details

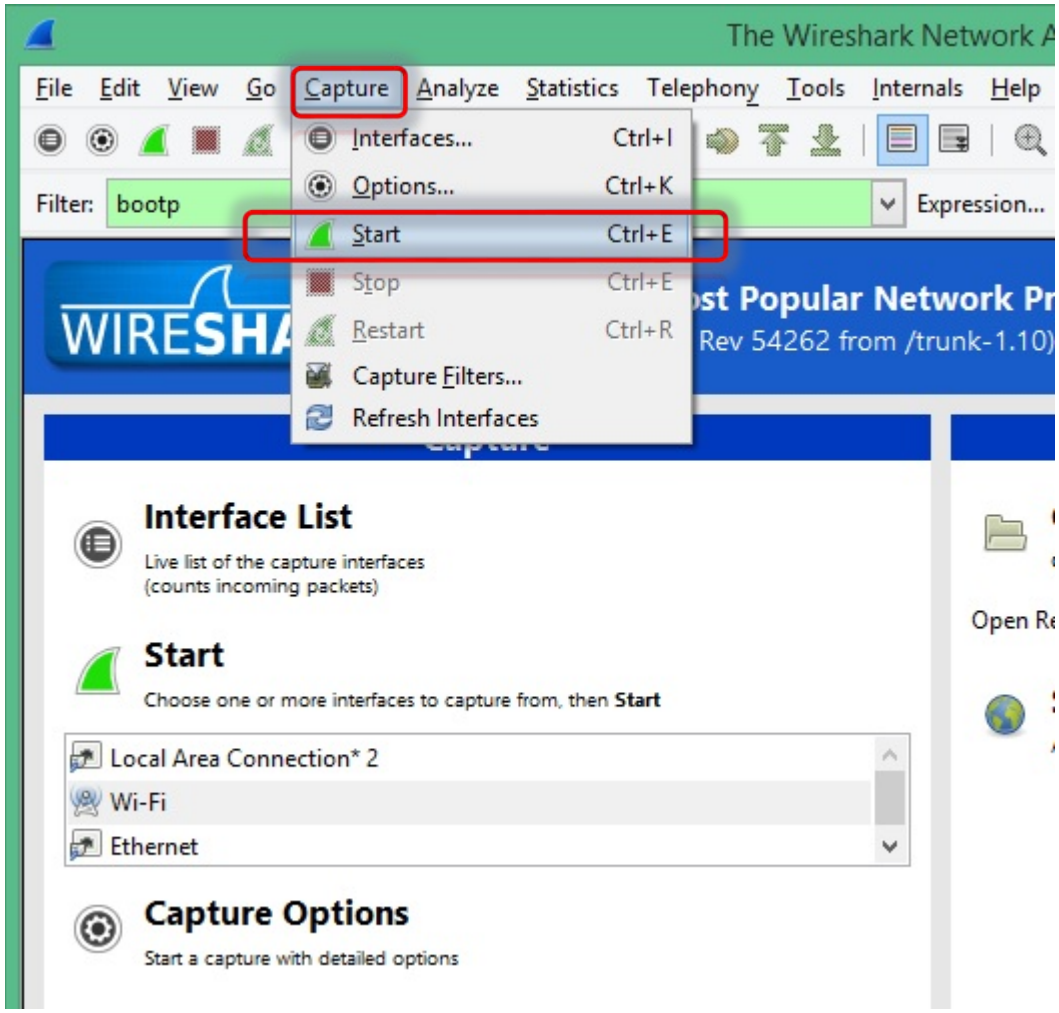
- Type in “ipconfig /displaydns”

DNS responds about web pages addresses inquiries

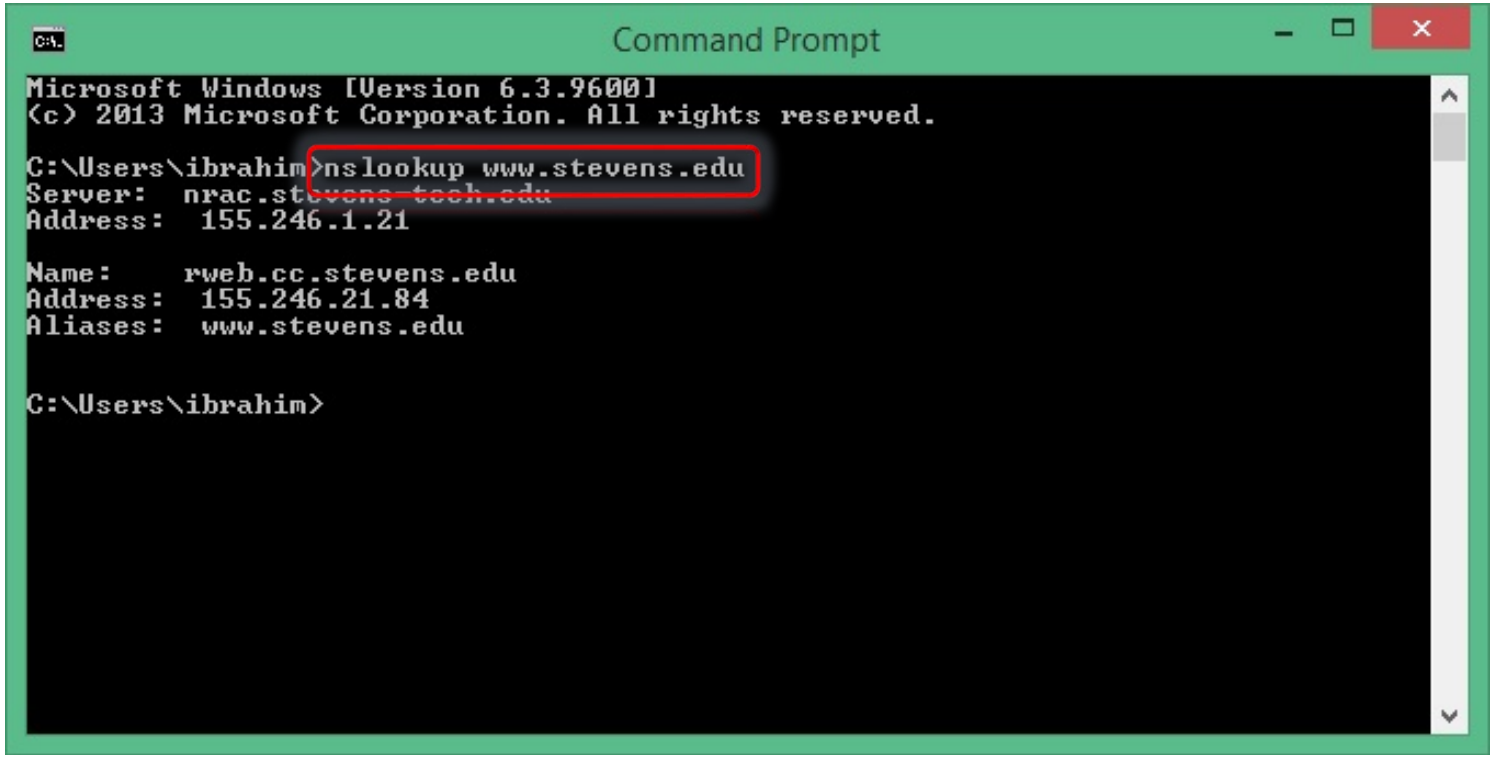


- Now, it's WIRESHARK time

- Now start up the Wireshark packet sniffer, and begin Wireshark packet capture.



- Now go back to the Windows Command Prompt and type “nslookup www.stevens.edu ”.



- After that, go back to Wireshark and stop the packet capturing.

- Now let's take a look at the resulting WireShark window.
- Hint: We entered "DNS" into the filter field so we only see the DNS packets,