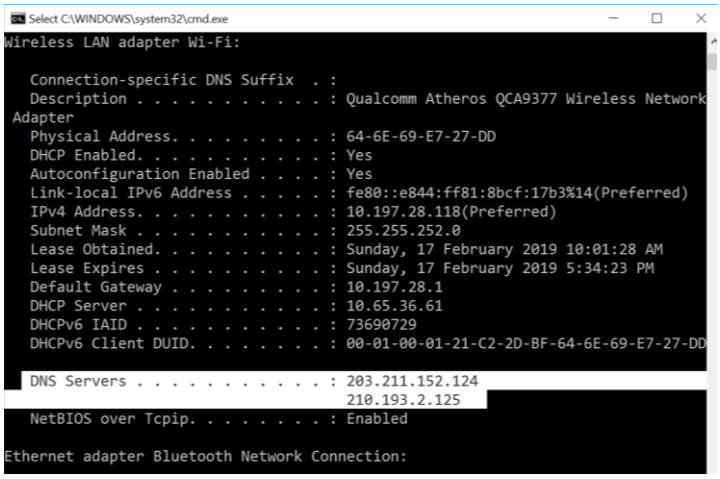
Practical 07
Capture DNS Traffic

A. Capture DNS Traffic
B. Analyze DNS Request Traffic
C. Analyze DNS Response Traffic

A. Capture DNS Traffic

1. Start a Wireshark capture.
2. Open a command prompt.
3. Type ipconfig /all to locate the DNS server(s)



Record down your DNS server(s)

DNS server(s) IP Address:	172.25.25.111	172.25.25.112

4. Type ipconfig /displaydns and press Enter to display the DNS cache.
5. Type ipconfig /flushdns and press Enter to clear the DNS cache.
6. Type ipconfig /displaydns and press Enter to display the DNS cache. Observe the results. Notice the only records currently displayed come from the hosts file.
7. Type nslookup en.wikiversity.org and press Enter.
8. Observe the results.

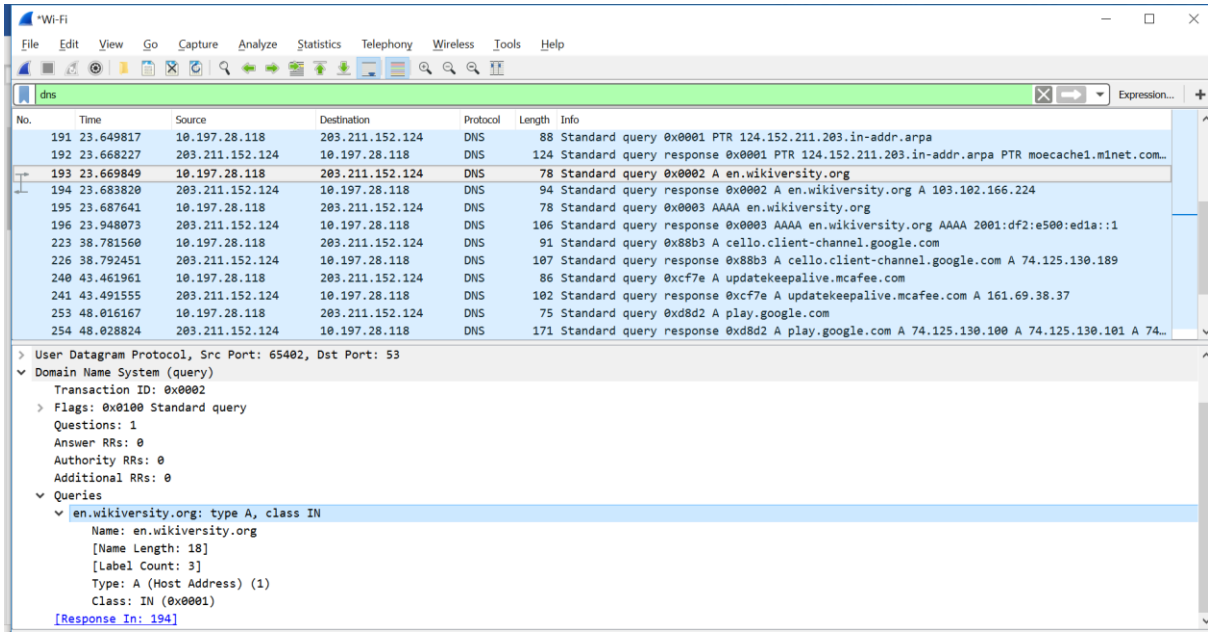
Record down your observation:

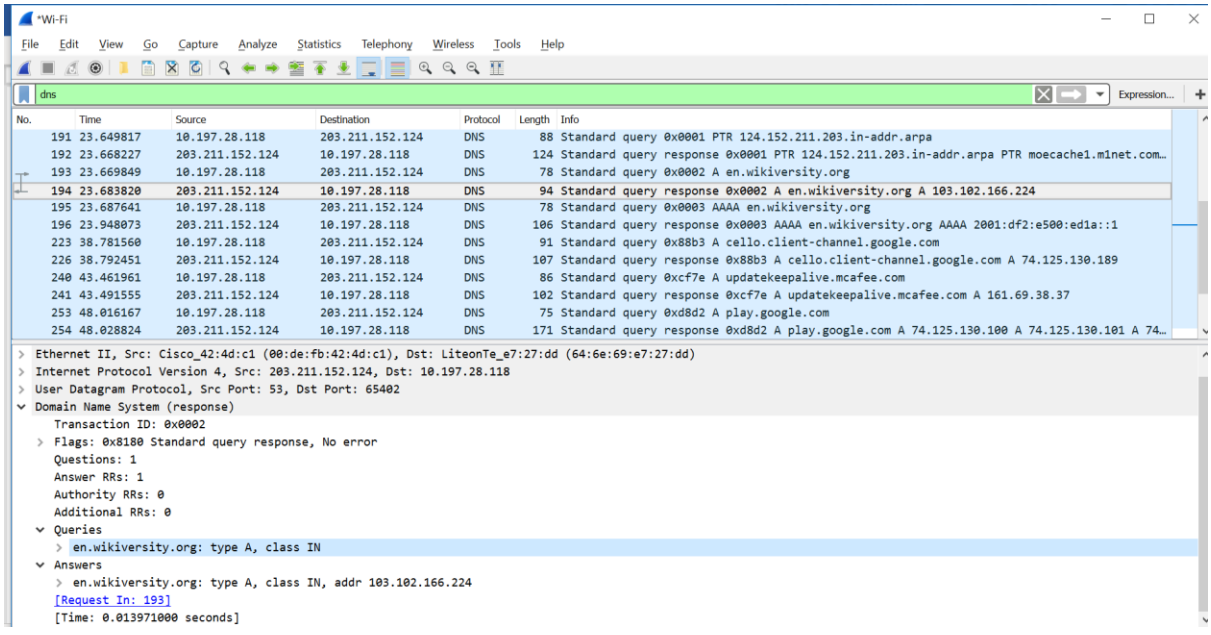
DNS server name	dyna.wikimedia.org
DNS server IP	2001:df2:e500:ed1a::1
IP address for en.wikiversity.org	103.102.166.224 en.wikiversity.org

9. Close the command prompt.
10. Stop the Wireshark capture.

B. Analyze DNS Request Traffic

1. Observe the traffic captured in the top Wireshark packet list pane. To view only DNS traffic, type udp.port == 53 (lower case) in the Filter box and press Enter.
2. Select the DNS packet labeled Standard query A en.wikiversity.org.
3. Observe the packet details in the middle Wireshark packet details pane. Notice that it is an Ethernet II / Internet Protocol Version 4 / User Datagram Protocol / Domain Name System (query) frame.
4. Observe the DNS request and response

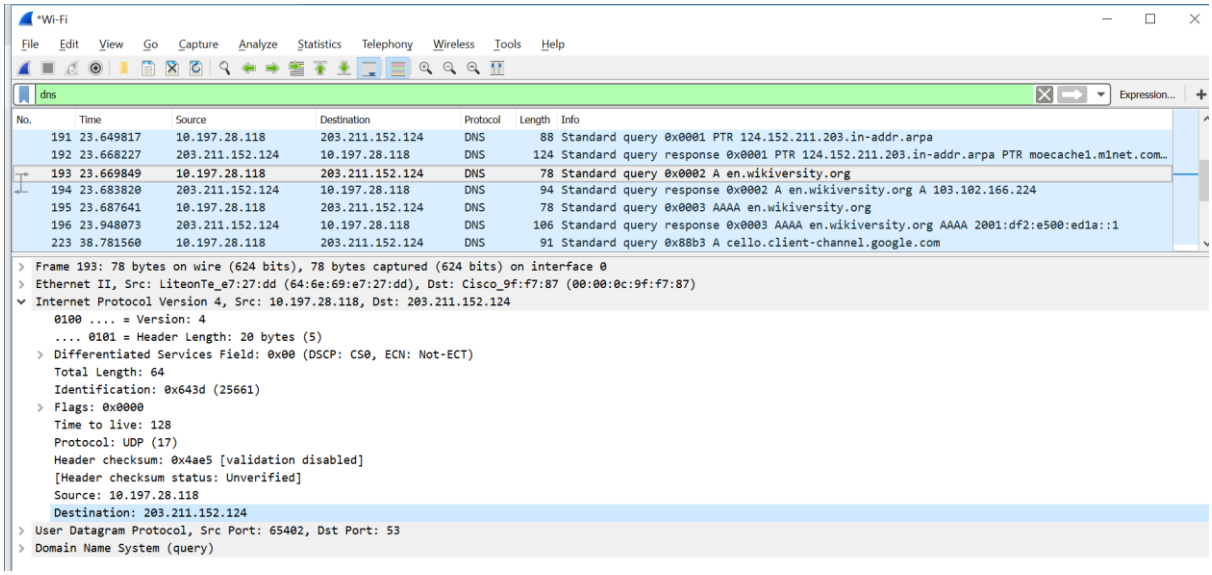




Record down CNAME and A records in response to the DNS query.

CNAME	dyna.wikimedia.org
A Records	103.102.166.224

1. Select the DNS request and Expand Internet Protocol Version 4 to view IP details.



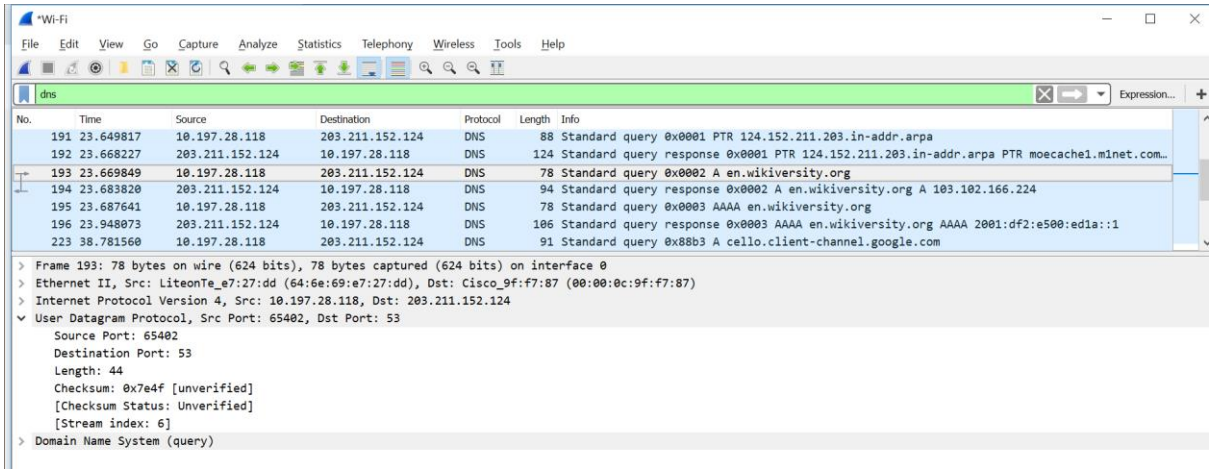
2. Observe the Source address. Notice that the source address is your IP address.

Source IP address	172.25.25.111
Is the source IP address your Own IP address? (true or false)	True

3. Observe the Destination address. Notice that the destination address is the IP address of the DNS server.

Destination IP address	172.22.37.248
Is the destination IP address your DNS Server (true or false)	True

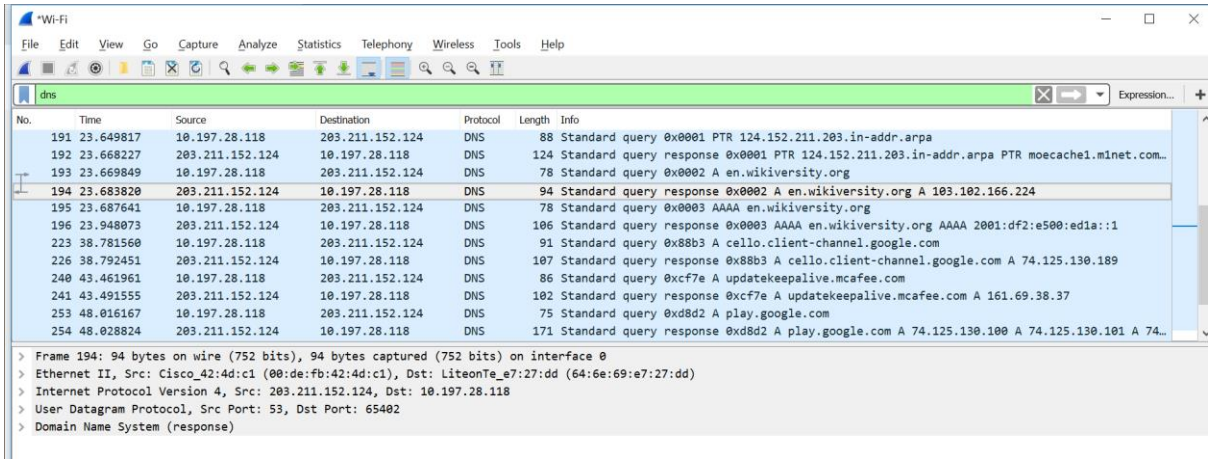
4. Expand User Datagram Protocol to view UDP details.
5. Observe the Source port. Notice that it is a dynamic port selected for this DNS query.



6. Observe the Destination port. Notice that it is domain (53), the DNS server port.

C. Analyze DNS Response Traffic

1. Select DNS Response Traffic.



2. Observe the Destination address.

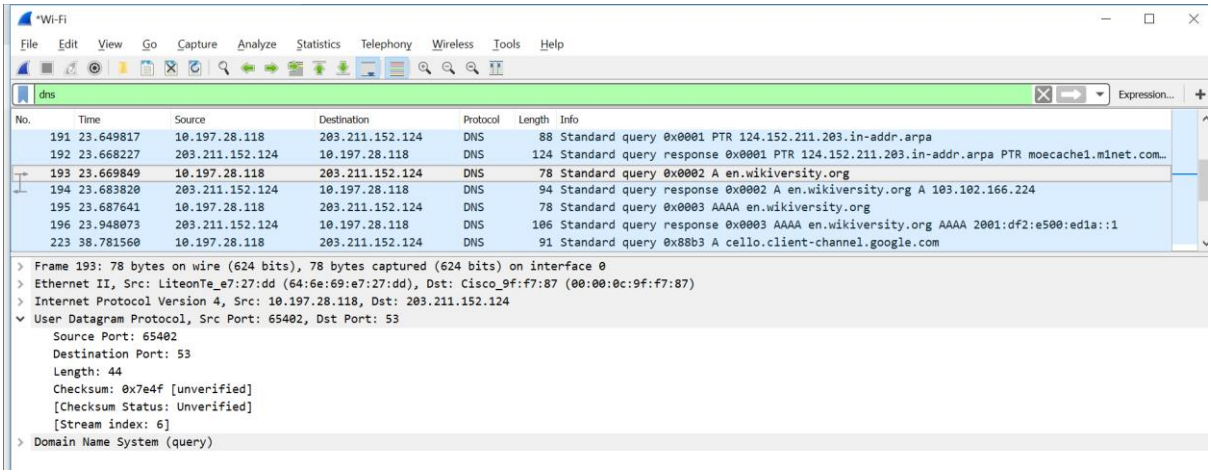
Destination IP address	172.25.25.111
Is the Destination IP address your Own IP address? (true or false)	True

3. Observe the Source address.

Source IP address	172.22.37.248
Is the Source IP address your DNS Server (true or false)	True

4. Expand User Datagram Protocol to view UDP details.

5. Observe the Source port. Notice that it is domain (53), the DNS port.



6. Observe the Destination port. Notice that it is a dynamic port selected for this DNS response.

Practical Reflection

Suggested contents:

1. What have you learnt?
2. Why is it important?
3. Any difficulty encountered in the practical and how do you solve the problem?

1. How to check DNS and check the CNAME type
2. CNAME and A records are important because they are used to resolve domain names to IP addresses. This is how your computer knows where to find the website or server that you are trying to connect to. Being able to see CNAME and A records with Wireshark can be helpful for troubleshooting DNS problems. For example, if you are unable to connect to a website, you can use Wireshark to see if the DNS records are correct. You can also use Wireshark to see if the DNS records are being changed by a malicious actor.
   In addition, being able to see CNAME and A records with Wireshark can be helpful for security auditing. For example, you can use Wireshark to see if any unauthorized CNAME records have been added to your domain. This could be a sign that someone is trying to redirect traffic to a malicious website
3. no

End of Practical