Tracing DNS with Wireshark
LAB # 08

Spring 2025

Submitted by: **Mohsin Sajjad**
Registration No: **22pwsce2149**

Class Section: **A**

"On my honor, as student of University of Engineering and Technology, I have neither given nor received unauthorized assistance on this academic work."

Student Signature: _____

Submitted to:
Dr. Yasir Saleem Afridi
Month Day, Year (21 05, 2025)

Department of Computer Systems Engineering
University of Engineering and Technology, Peshawar

CSE 303L: Data Communication and Computer Networks

Credit Hours: 1

Demonstration of Concepts	**Poor (Does not meet expectation (1))** The student failed to demonstrate a clear understanding of the assignment concepts	**Fair (Meet Expectation (2-3))** The student demonstrated a clear understanding of some of the assignment concepts	**Good (Exceeds Expectation (4-5)** The student demonstrated a clear understanding of the assignment concepts	**Score** **30%**
Accuracy	The student mis-configured enough network settings that the lab computer couldn't function properly on the network	The student configured enough network settings that the lab computer partially functioned on the network	The student configured the network settings that the lab computer fully functioned on the network	**30%**
Following Directions	The student clearly failed to follow the verbal and written instructions to successfully complete the lab	The student failed to follow the some of the verbal and written instructions to successfully complete all requirements of the lab	The student followed the verbal and written instructions to successfully complete requirements of the lab	**20%**
Time Utilization	The student failed to complete even part of the lab in the allotted amount of time	The student failed to complete the entire lab in the allotted amount of time	The student completed the lab in its entirety in the al	**20%**

Tracing DNS with Wireshark

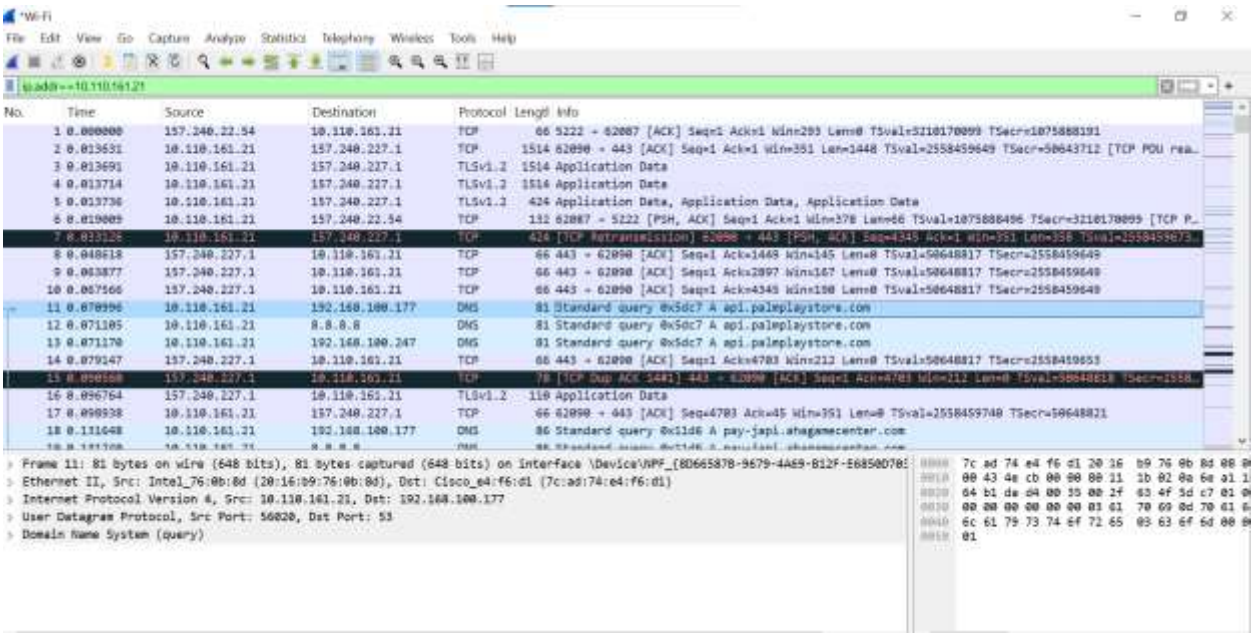
• Open Wireshark and enter “ip.addr == your_IP_address” into the filter, where you obtain your_IP_address with ipconfig. This filter removes all packets that neither originate nor are destined to your host.

• Start packet capture in Wireshark.

• With your browser, visit the Web page: http://www.ietf.org

• Stop packet capture.

To print a packet, use File->Print, choose Selected packet only, choose Packet summary line, and select the minimum amount of packet detail that you need to answer the question.



Question 1:

Locate the DNS query and response messages. Are then sent over UDP or TCP?

Answer:

The DNS message sent over UDP not TCP.

Question 02:

What is the destination port for the DNS query message? What is the source port of DNS response message?

Answer:

Destination port for DNS query: 56020.

Source port of DNS response: 53.

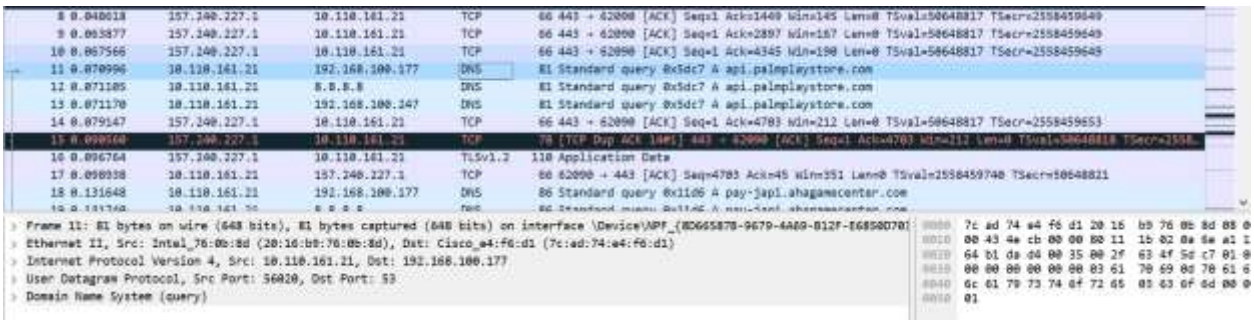
Question 03:

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?

Answer:

```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Dual Band Wireless-AC 8260
   Physical Address. . . . . . . . . : 20-16-B9-76-0B-8D
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::9dc6:b9f4:1da7:872e%10(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.110.161.21(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Lease Obtained. . . . . . . . . . : Wednesday, 21 May 2025 10:03:37 am
   Lease Expires . . . . . . . . . . : Friday, 20 June 2025 10:33:38 am
   Default Gateway . . . . . . . . . : 10.110.160.1
   DHCP Server . . . . . . . . . . . : 192.168.100.153
   DHCPv6 IAID . . . . . . . . . . . : 136320697
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2D-B6-17-6E-8C-16-45-E2-71-14
   DNS Servers . . . . . . . . . . . : 192.168.100.177
                                       8.8.8.8
                                       192.168.100.247
   NetBIOS over Tcpip. . . . . . . . : Enabled
```



Answer:

Yes, the ip address of DNS server is same as in packet.

Question 04:

Examine the DNS query message. What "Type" of DNS query is it? Does the query message contains any "answers"?

Answer:

The query is of Type A (requesting IPv4 address for a domain, e.g., api.palmplaystore.com).

No, the query message does not contain any answers—it's only a request.

Question 05:

Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

```
> Frame 21: 209 bytes on wire (1672 bits), 209 bytes captured (1672 bits) on interface \Device\NPF_{8D66587B-9679-4A69-B12F-E6856
> Ethernet II, Src: Cisco_e4:f6:d1 (7c:ad:74:e4:f6:d1), Dst: Intel_76:0b:8d (20:16:b9:76:0b:8d)
> Internet Protocol Version 4, Src: 8.8.8.8, Dst: 10.110.161.21
> User Datagram Protocol, Src Port: 53, Dst Port: 56020
v Domain Name System (response)
    Transaction ID: 0x5dc7
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 8
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > api.palmplaystore.com: type A, class IN
  v Answers
    > api.palmplaystore.com: type A, class IN, addr 52.31.145.61
    > api.palmplaystore.com: type A, class IN, addr 52.209.170.126
    > api.palmplaystore.com: type A, class IN, addr 54.77.107.132
    > api.palmplaystore.com: type A, class IN, addr 52.50.201.214
    > api.palmplaystore.com: type A, class IN, addr 52.210.216.206
    > api.palmplaystore.com: type A, class IN, addr 99.81.45.27
    > api.palmplaystore.com: type A, class IN, addr 52.212.211.142
    > api.palmplaystore.com: type A, class IN, addr 34.247.199.66
    [Request In: 12]
    [Time: 0.065421000 seconds]
```

Answer:

For api.palmplaystore.com, DNS responses included multiple answers. For example:
Packet 21 contained 8 answers:
A records like 52.31.145.61, 52.209.170.126, etc.
Packet 29 contained more than 8 answers including A records (IP addresses) and NS records (name servers).

Each answer includes:

A Records: IP addresses associated with the queried domain.
NS Records (in some cases): Name server domain names (and sometimes A records for them too).

NSLOOKUP

Question 1:

What is the destination port for the DNS query message? What is the source port of DNS response message?
Destination port of DNS query: 53 (standard for DNS).

Source port of DNS response: 56020

Question 02:

To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

Answer:

The DNS query is likely sent to your local DNS server 192.168.100.177.
Run ipconfig /all and check the “DNS Servers” line. That IP should match the destination IP in your DNS query.

```
> Frame 47: 368 bytes on wire (2944 bits), 368 bytes captured (2944 bits) on interface \Device\NPF_{8D66587B-9679-4A69-B12F-E6
> Ethernet II, Src: Cisco_e4:f6:d1 (7c:ad:74:e4:f6:d1), Dst: Intel_76:0b:8d (20:16:b9:76:0b:8d)
> Internet Protocol Version 4, Src: 192.168.100.177, Dst: 10.110.161.21
> User Datagram Protocol, Src Port: 53, Dst Port: 56020
v Domain Name System (response)
    Transaction ID: 0x10d7
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 2
    Authority RRs: 4
    Additional RRs: 8
  v Queries
    > b-graph.facebook.com: type A, class IN
```

Question 03:

Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

Answer:

```
> Ethernet II, Src: Intel_76:0b:8d (20:16:b9:76:0b:8d), Dst: Cisco_e4:f6:d1 (7c:ad:74:e4:f6:d1)
> Internet Protocol Version 4, Src: 10.110.161.21, Dst: 192.168.100.177
> User Datagram Protocol, Src Port: 49647, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x446e
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > www.ietf.org: type A, class IN
    [Response In: 47]
```

Answer to Question 3:

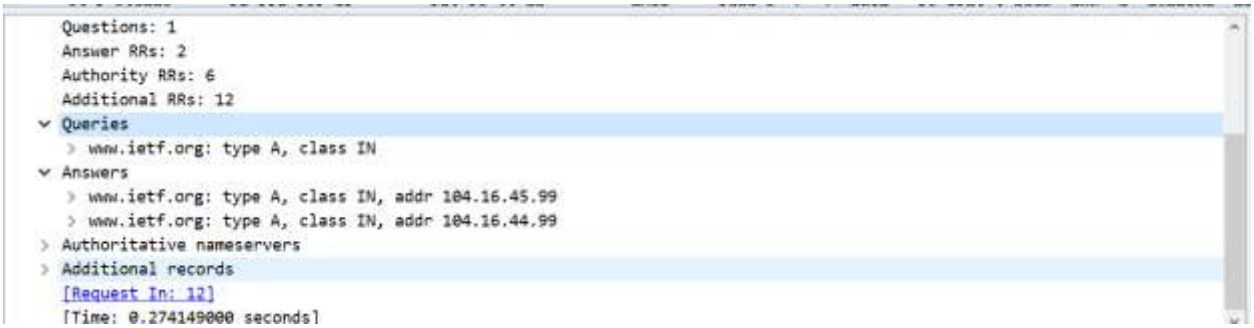
Type of DNS Query:

Type A, which means it is requesting the IPv4 address for the domain www.ietf.org.

Does the Query Message Contain Any Answers?

No, the DNS query message does not contain any answers.
It only includes the question section, asking for the A record of www.mit.edu.
The answers come only in the response message, not in the query.

4. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?



Answer:

2 answers are provided in the DNS response.

Each Answer Contains:

Answer 1:

- **Name: www.ietf.org**
- **Type: A (IPv4 address)**
- **Address: 104.16.45.99**

Answer 2:

- **Name: www.ietf.org**
- **Type: A (IPv4 address)**
- **Address: 104.16.44.99**

These are two A records, meaning www.ietf.org resolves to two different IP addresses, likely for load balancing or redundancy.