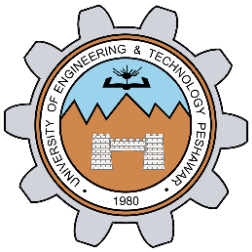
TRACING DNS WITH WIRESHARK

Lab #07



Spring 2021

CSE303L Data Communication and Networks Lab

Submitted by: **Shah Raza**

Registration No. : **18PWCSE1658**

Class Section: **B**

"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:

Engr. Faiz Ullah

Saturday, July 10, 2021

Department of Computer Systems Engineering

University of Engineering and Technology, Peshawar

CSE 303L: Data Communication and Computer Networks

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 allotted amount of time	**20%**

Credit Hours: 1

Lab 07

i) **The Domain Name System (DNS)** translates hostnames to IP addresses, fulfilling a critical role in the Internet infrastructure. In this lab, we'll take a closer look at the client side of DNS. Recall that the client's role in the

DNS is relatively simple – a client sends a query to its local DNS server, and receives a response back.
The hierarchical DNS servers communicate with each other to either recursively or iteratively resolve the client's DNS query. From the DNS client's standpoint, however, the protocol is quite simple – a query is formulated to the local DNS server and a response is received from that server.

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.

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

   Ans: They are sent over UDP.

```
User Datagram Protocol, Src Port: 57300, Dst Port: 53
    Source Port: 57300
    Destination Port: 53
    Length: 38
    Checksum: 0xbc41 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 19]
  > [Timestamps]
    UDP payload (30 bytes)
```

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

   Ans: Destination port of query: 53
   Source port of response: 53

```
User Datagram Protocol, Src Port: 53, Dst Port: 57300
    Source Port: 53
    Destination Port: 57300
    Length: 115
    Checksum: 0x9e21 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 19]
  > [Timestamps]
    UDP payload (107 bytes)
Domain Name System (response)
```

3. **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?**
   Ans: The DNS query message is sent to 192.168.1.1. It is the same IP address as my local DNS server.

4. **Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?**
   Ans: The type of DNS query is 'A' and DNS query message contains no answers.

```
Domain Name System (query)
    Transaction ID: 0xbdba
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
```

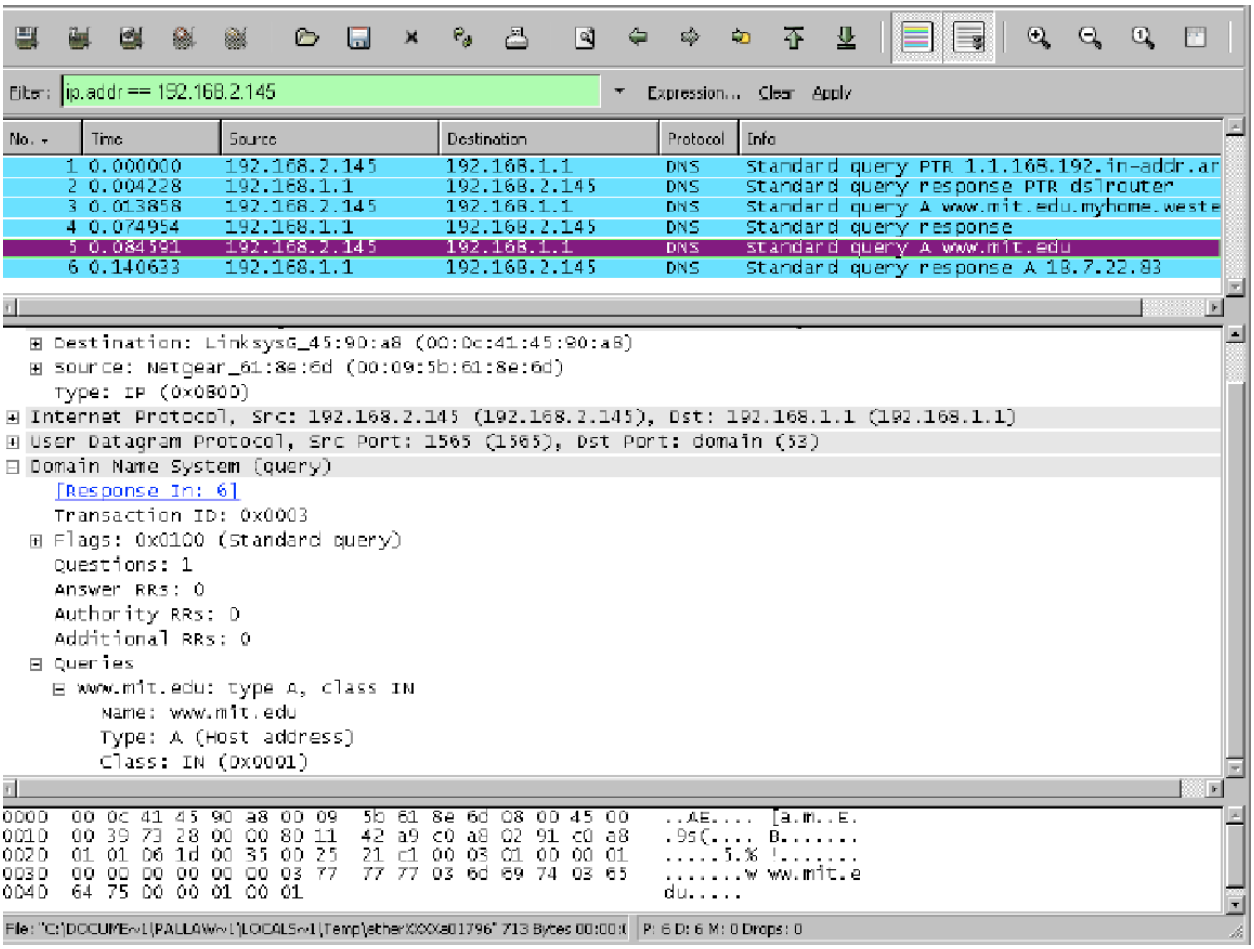
5. **Examine the DNS response message. How many "answers" are provided? What do each of these answers contain?**
   Ans: 3 Answers are provided.

```
Answers
  www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
      Name: www.ietf.org
      Type: CNAME (Canonical NAME for an alias) (5)
      Class: IN (0x0001)
      Time to live: 127 (2 minutes, 7 seconds)
      Data length: 33
      CNAME: www.ietf.org.cdn.cloudflare.net
  www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.45.99
      Name: www.ietf.org.cdn.cloudflare.net
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 17 (17 seconds)
      Data length: 4
      Address: 104.16.45.99
  www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.44.99
      Name: www.ietf.org.cdn.cloudflare.net
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 17 (17 seconds)
      Data length: 4
      Address: 104.16.44.99
  [Request In: 819]
  [Time: 0.104247000 seconds]
```

Now let's play with *nslookup*.

- Start packet capture.
- Do an *nslookup* on www.mit.edu
- Stop packet capture.

You should get a trace that looks something like the following:



We see from the above screenshot that *nslookup* actually sent three DNS queries and received three DNS responses. For the purpose of this assignment, in answering the following questions, ignore the first two sets of queries/responses, as they are specific to *nslookup* and are not normally generated by standard Internet applications. You should instead focus on the last query and response messages.

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

   Ans: Destination port of query: 53
   Source port of response: 53

2. **To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?**
The DNS query message is sent to 192.168.1.1. It is the same IP address as my local DNS server.

3. **Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?**
Ans: The type of DNS query is 'A' and DNS query message contains no answers.

4. **Examine the DNS response message. How many "answers" are provided? What do each of these answers contain? Provide a screenshot.**
4 Answers are provided.