**Name:Naval Kishore Jangid**

**Registration Number:20154171**

**Branch:CSE**

**Week #1 assignment for Networking Lab**

**Exercise # 1 Tracing DNS with Wireshark**

**Answer the following questions using dns-ethereal-trace-1 file:**

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

Ans:UDP

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

**response message?**

Ans:Source port is res-sap(3163)

Destination port is domain(53)

**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 IP address DNS query is sent to is 128.238.29.23(128.238.29.23)

Source IP address is 128.238.38.160(128.238.38.160)

**4. Examine the DNS query message. What “Type” of DNS query is it? Does the query message**

**contain any “answers”?**

Ans: DNS query is of Type A. It contains 0 answers.

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

Ans:It contains 2 answers. The answers contain:

[www.ietf.org](http://www.ietf.org/) type A,class IN, addr 132.151.6.75

[www.ietf.org](http://www.ietf.org/) type A,class IN addr 65.246.255.51

**6. Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?**

Ans:No, the destination IP address of the SYN packet doesn't correspond to any of the IP addresses provided in the DNS response message.

**7. This web page contains images. Before retrieving each image, does your host issue new DNS**

**queries?**

Ans:No,before retrieving each image, the host doesn't issue new DNS queries because HTTP connection is persistent.

**Answer the following questions using dns-ethereal-trace-2 file:**

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

**response message?**

Ans:The destination port for DNS query message is 'domain' and the source port of DNS response message is 'domain'.

**9. To what IP address is the DNS query message sent? Is this the IP address of your default**

**local DNS server?**

Ans: DNS query message is sent to 128.238.29.22. Yes.

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

Ans: First query is of type PTR and second and third are of type A.

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

Ans: In the first response there is 1 answer,in the second there are 0 answers and in the third there is 1 answer.

First response answer:22.29.238.128.in-addr.arpa:type PTR,class IN,dns-prime.poly.edu

Third response answer:[www.mit.edu](http://www.mit.edu/):type A,class IN,addr 18.7.22.83

**Answer the following questions using *dns-ethereal-trace-3* file:**

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

Ans:It was sent to 128.238.29.22 which is my default DNS server.

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

Ans:It’s a type NS DNS query that doesn’t contain any answers.

**15. Examine the DNS response message. What MIT nameservers does the response message provide? Does this response message also provide the IP addresses of the MIT namesers?**

Ans:The nameservers are bitsy, strawb and w20ns. We can find their IP addresses if we expand the Additional records field in Wireshark as seen below.

**Answer the following questions using *dns-ethereal-trace-4* file:**

**17. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? If not, what does the IP address correspond to?**

Ans:The query is sent to 18.72.0.3 which corresponds to bitsy.mit.edu.

**18. Examine the DNS query message. What “Type” of DNS query is it? Does the**

**query message contain any “answers”?**

Ans:It’s a standard type A query that doesn’t contain any answers.

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

Ans:One answer provided in the DNS response message. It contains the following:

Answers

[www.aiit.or.kr](http://www.aiit.or.kr): type A, class inet, addr 222.106.36.102

Name: [www.aiit.or.kr](http://www.aiit.or.kr)

Type: Host address

Class: inet

Time to live: 1 hour

Data length: 4

Addr: 222.106.36.102

**Exercise # 2 Tracing UDP with Wireshark**

**Answer the following questions using *udp-wireshark-trace* file:**

**1. Select *one* UDP packet from your trace. From this packet, determine how many fields there are in the UDP header. (You shouldn’t look in the textbook! Answer these questions directly from what you observe in the packet trace.) Name these fields.**

Ans:The UDP header consists of 4 fields: Source Port, Destination Port, Length and

Checksum.

**2. By consulting the displayed information in Wireshark’s packet content field for this packet, determine the length (in bytes) of each of the UDP header fields.**

Ans:The length in bytes of each of the header fields is as follows: (i) Source Port: 2

bytes, (ii) Destination Port: 2 bytes, (iii) Length: 2 bytes and (iv) Checksum: 2 bytes

**3. The value in the Length field is the length of what? (You can consult the text for this answer). Verify your claim with your captured UDP packet.**

Ans:: The value of the Length field (28 bytes) is the total length of the UDP segment,

i.e. including the header and payload. Each of the 4 header fields is 2 bytes long as

discussed above. Further, the payload of the UDP segment is 20 bytes. Thus, 20 + 4(2)

= 28 bytes.

**4. What is the maximum number of bytes that can be included in a UDP payload? (Hint: theanswer to this question can be determined by your answer to 2. above)**

Ans:The maximum size of a UDP segment (including headers) is 65535 bytes

(2^16 -1 bytes). Thus the maximum size of the UDP payload can be 65527 bytes. Of

course in a real network, the MTU of the underlying network will limit the maximum

size to a much smaller value.

**5. What is the largest possible source port number? (Hint: see the hint in 4.)**

Ans:The largest possible source port number is 65535 (2^16 -1).

**6. What is the protocol number for UDP? Give your answer in both hexadecimal and decimal notation. To answer this question, you’ll need to look into the Protocol field of the IP datagram containing this UDP segment (see Figure 4.13 in the text, and the discussion of IP header fields).**

Ans:The IP protocol number for UDP is 0x11 hex, and that translates to 17 in decimal.

**7. Examine a pair of UDP packets in which your host sends the first UDP packet and the second**

**UDP packet is a reply to this first UDP packet. (Hint: for a second packet to be sent in**

**response to a first packet, the sender of the first packet should be the destination of the second packet). Describe the relationship between the port numbers in the two packets.**

Ans:The source and destination port numbers for the first UDP packet in the trace

are 3740 and 53 (used for DNS) respectively. The second UDP packet has the source

port number as 53 and the destination port number as 3740, which is reverse of the first

packet. This indicates that the two packets are part of a query-response exchange, which

is indeed the case – the first packet is a DNS query and the second packet is a DNS

response