**Lab 7-I DNS**

Name – Sati, Ankit Date – 12/22/2021

Section - 001

Total in points (Maximum 100 points)–

Professors Comments –

Affirmation of Independent Effort – Ankit Sati

1. Run nslookup to obtain the IP address of a Web server in Asia. What is the IP?

**Answer - asia1.akam.net internet address = 95.100.175.64**

1. Run nslookup to determine the authoritative DNS servers for a university in Europe.

**Answer - eur5.akam.net internet address = 23.74.25.64**

1. Run nslookup so that one of the DNS servers obtained in Question 2 is queried for?

**Answer -** **C:\windows\system32>nslookup www.aiit.or.kr bitsy.mit.edu**

**DNS request timed out.**

**timeout was 2 seconds.**

**Server: UnKnown**

**Address: 18.0.72.3**

1. the mail servers for Yahoo! mail. What is its IP address?Locate the DNS query and response messages. Are then sent over UDP or TCP?

**Answer - It is using UDP for both the query and response messages.**

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

**Answer - Both ports are 53.**

1. 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 - The DNS query is sent to 10.7.40.3 which is the local DNS server of the computer. Yes, the IP addresses are the same.**

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

**Answer - It is a Type A DNS query and there are no answers in the query.**

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

**Answer - The DNS response message has 3 answers. The first answer is telling us the Canonical Name and what its real domain name is. The second answer is the IP address of the real domain name. The third answer is the second IP address of the domain name, as there are two IP’s associated within that domain (104.20.1.85 & 104.20.0.85).**

1. This web page contains images. Before retrieving each image, does your host issue new DNS queries?

**Answer - No, there are no new DNS queries issued before retrieving each image.**

1. Provide a screenshot

Graphical user interface, text, application, table

Description automatically generated

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

**Answer - The Destination and Source ports are 53.**

1. 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 sent to 10.7.40.3 which is the local DNS server IP.**

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

**Answer - The DNS Query is Type A, it does not contain any answers.**

Question 13 - Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

**Answer -**

**The DNS Response message contains 2 answers. The first answer is the Canonical name and the real domain name. The second answer is the IP address of the domain**

**Question 14**

Provide a screenshot.

Graphical user interface, text, application

Description automatically generated

**Question 15 -** To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

**Answer –**

**Yes it is sent to the default DNS server which is 10.7.40.3**

**Question 16 -** Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

**Answer –**

**It is a type NS query and there are no answers.**

**Question 17 -** Examine the DNS response message. What UBC name servers does the response message provide? Does this response message also provide the IP addresses of the UBC name servers?

**Answer –**

**The name servers it provides are dns3.ubc.ca, and hub.ubc.ca, it does not provide the IP address of the name servers.**

**Question 18 - Provide a screenshot.**

Graphical user interface, text, application, email

Description automatically generated

**Question 19 -** 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?

**Answer-**

**The DNS query message is sent to 137.82.1.1 which is not the IP address of the local DNS server. The IP address corresponds to the hub.ubc.ca name server and its DNS which we are querying to.**

**Question 20**- Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

**Answer-**

The query message is a Type A DNS query and it does not contain any

answers.

**The query message is a Type A DNS query and it does not contain any answers.**

**Question 21 -** Examine the DNS response message. How many “answers” are provided? What does each of these answers contain?

**Answer-**

**There is one answer which contains the ucalgary.ca domain name, and its IP address. It is a Type A DNS record and contains information within it.**

**Question 22 - Provide a screenshot.**

Graphical user interface, text, application

Description automatically generated