Lab-2 DNS

A screenshot of a computer

Description automatically generated

1. Run nslookup to obtain the IP address of the web server for the Indian  
   Institute of Technology in Bombay, India: www.iitb.ac.in. What is the IP address  
   of [www.iitb.ac.in](http://www.iitb.ac.in)

Server: 192.168.0.1

Address: 192.168.0.1#53

Non-authoritative answer:

Name: www.iitb.ac.in

Address: 103.21.124.10

1. What is the IP address of the DNS server that provided the answer to your  
   nslookup command in question 1 above?
   1. 192.168.0.1
2. Did the answer to your nslookup command in question 1 above come from an  
   authoritative or non-authoritative server?
   1. Non-authoritative
3. Use the nslookup command to determine the name of the authoritative name  
   server for the iit.ac.in domain. What is that name? (If there are more than one  
   authoritative servers, what is the name of the first authoritative server returned by  
   nslookup )? If you had to find the IP address of that authoritative name server,  
   how would you do so?

Authoritative answers can be found from:

iitb.ac.in

origin = dns1.iitb.ac.in

mail addr = postmaster.iitb.ac.in

serial = 2013071001

refresh = 16384

retry = 2048

expire = 1048576

* 1. minimum = 3960
  2. I would find the IP address by the SOA record get the primary name server and then do another nslookup with the original ip address and specify this name server

A screenshot of a computer

Description automatically generated

1. Locate the first DNS query message resolving the name gaia.cs.umass.edu. What  
   is the packet number in the trace for the DNS query message? Is this query4  
   message sent over UDP or TCP?
   1. The message is sent over UDP
2. Now locate the corresponding DNS response to the initial DNS query. What is the  
   packet number in the trace for the DNS response message? Is this response  
   message received via UDP or TCP?
   1. 20, the response is received via UDP

A screenshot of a computer

Description automatically generated

1. What is the destination port for the DNS query message? What is the source port  
   of the DNS response message?
   1. Destination is 53, Source is 578979
2. To what IP address is the DNS query message sent?
   1. 192.168.0.1
3. Examine the DNS query message. How many “questions” does this DNS message  
   contain? How many “answers” answers does it contain? Why?
   1. 1 Question, 0 answers. This is because it is trying to find an answer for it question.
4. Examine the DNS response message to the initial query message. How many  
   “questions” does this DNS message contain? How many “answers” answers does  
   it contain? Why?
   1. There is 1 question and 4 answers. This is because there were 4 different answers to the original 1 question.
5. The web page for the base file http://gaia.cs.umass.edu/kurose\_ross/ references  
   the image object http://gaia.cs.umass.edu/kurose\_ross/  
   header\_graphic\_book\_8E\_2.jpg , which, like the base webpage, is on  
   gaia.cs.umass.edu. What is the packet number in the trace for the initial HTTP  
   GET request for the base file http://gaia.cs.umass.edu/kurose\_ross/? What is the  
   packet number in the trace of the DNS query made to resolve gaia.cs.umass.edu  
   so that this initial HTTP request can be sent to the gaia.cs.umass.edu IP address?  
   What is the packet number in the trace of the received DNS response? What is the  
   packet number in the trace for the HTTP GET request for the image object http://  
   gaia.cs.umass.edu/kurose\_ross/header\_graphic\_book\_8E\_3.jpg? What is the  
   packet number in the DNS query made to resolve gaia.cs.umass.edu so that this  
   second HTTP request can be sent to the gaia.cs.umass.edu IP address? Discuss  
   how DNS caching affects the answer to this last question.
   1. Packet number 217
   2. Packet number 19
   3. Packet number 20
   4. Packet number 317
   5. Packet number 214

A screenshot of a computer

Description automatically generated

1. What is the destination port for the DNS query message? What is the source port  
   of the DNS response message?
   1. Source Port: 50154
   2. Destination Port: 53
2. To what IP address is the DNS query message sent? Is this the IP address of your  
   default local DNS server?
   1. 192.168.0.1, yes this is my default local DNS server

1. Examine the DNS query message. What “Type” of DNS query is it? Does the  
   query message contain any “answers”?
   1. The query is a standard query, it contains no answers.
2. Examine the DNS response message to the query message. How many  
   “questions” does this DNS response message contain? How many “answers”?
   1. There is one question and one answer.

A screenshot of a computer

Description automatically generated

1. To what IP address is the DNS query message sent? Is this the IP address of your  
   default local DNS server?
   1. The IP address is 128.119.8.148, this is not the default local DNS server.
2. Examine the DNS query message. How many questions does the query have?  
   Does the query message contain any “answers”?
   1. 1 question no answers.
3. Examine the DNS response message. How many answers does the response  
   have? If any, what information is contained in the answers? How many additional  
   resource records are returned? What additional information is included in these  
   additional resource records?
   1. There is no response received from umass.