E2

Question 1: What transport layer protocol is being used by the DNS messages?

A: The protocol is UDP

Question 2: What are the source and destination port for the DNS query message and the corresponding response?

A: DNS query message:

Source port: 3742

destination port: 53

DNS response message:  
 source port: 53

destination port: 3742


Question 3: To what IP address is the DNS query message sent? Is this the same as the default local DNS server?

A: IP address: 128.238.38.160



Yes, it is same.



Question 4: How many “questions” are contained in the DNS query message? What “Type” of DNS queries are they? Does the query message also contain any “answers”?

A: One question, no answer

The question is a standard query for the DNS record type A (IPv4 address) and class IN (Internet)

文本

描述已自动生成

Question 5: Examine the DNS response message. Provide details of the contents of the “Answers”, “Authority” and “Additional Information” fields. What can you infer from these?

A: In “Answers”: IP address associated with the hostname www.mit.edu is 18.7.22.83



In “Authority”: the RRs indicate that authoritative name servers for the "mit.edu" domain are ns BITSY.mit.edu, ns STRAWB.mit.edu, and ns W20NS.mit.edu.

图形用户界面, 文本, 应用程序

描述已自动生成

In “Additional Information”: We may assume that the authoritative name servers for the "mit.edu" domain are dispersed across a number of IP addresses

文本

描述已自动生成

E3:

Question 1. What is the IP address of [www.stanford.edu](http://www.stanford.edu/)? What type of DNS query is sent to get this answer?

A: 手机屏幕截图

描述已自动生成

IP address is 151.101.30.133, it is A record query. The A record maps a domain name to an IPv4 address.

Question 2. What is the canonical name for the Stanford webserver (i.e., [www.stanford.edu](http://www.stanford.edu/))? Suggest a reason for having an alias for this serve

A: pantheon-systems.map.fastly.net.

So, if we use an alias, we don’t need to update every client that uses the server’s IP address when changing the IP address.

Question 3. What can you make of the rest of the response (i.e. the details available in the Authority and Additional sections)?

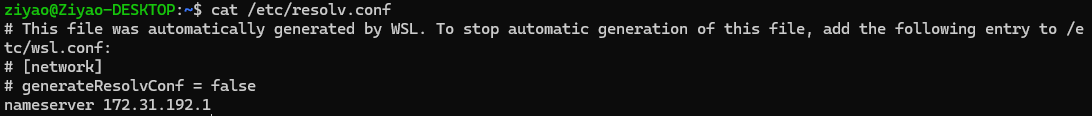
A:

Authority section: The authoritative nameservers for the fastly.net domain are shown in the response's Authority section. If the domain's nameservers are not already cached, this information will help recursive nameservers discover them.

Additional section: The IP addresses of the nameservers provided in the Authority section are included in the Additional portion of the answer. This information is supplied to assist resolvers in contacting the authoritative nameservers in order to retrieve the necessary DNS records.

Question 4. What is the IP address of the local nameserver for your machine?

A: It is 172.31.192.1



Question 5. What are the DNS nameservers for the "stanford.edu.” domain (note: the domain name is stanford.edu and not [www.stanford.edu](http://www.stanford.edu/). This is an example of what is referred to as the apex/naked domain)? Find their IP addresses. What type of DNS query is sent to obtain this information?

A:

表格

描述已自动生成

There are 6 nameservers:

ns7.dnsmadeeasy.com 208.80.126.13,

atalante.stanford.edu 171.64.7.61,

ns5.dnsmadeeasy.com 208.94.148.13,

ns6.dnsmadeeasy.com 208.80.124.13,

avallone.stanford.edu 204.63.224.53,

argus.stanford.edu 171.64.7.115.

NS query, asks the authoritative DNS server for the domain to provide the list servers that are responsible for the domain.

Question 6. What is the DNS name associated with the IP address 129.25.60.56 ? What type of DNS query is sent to obtain this information?

A:

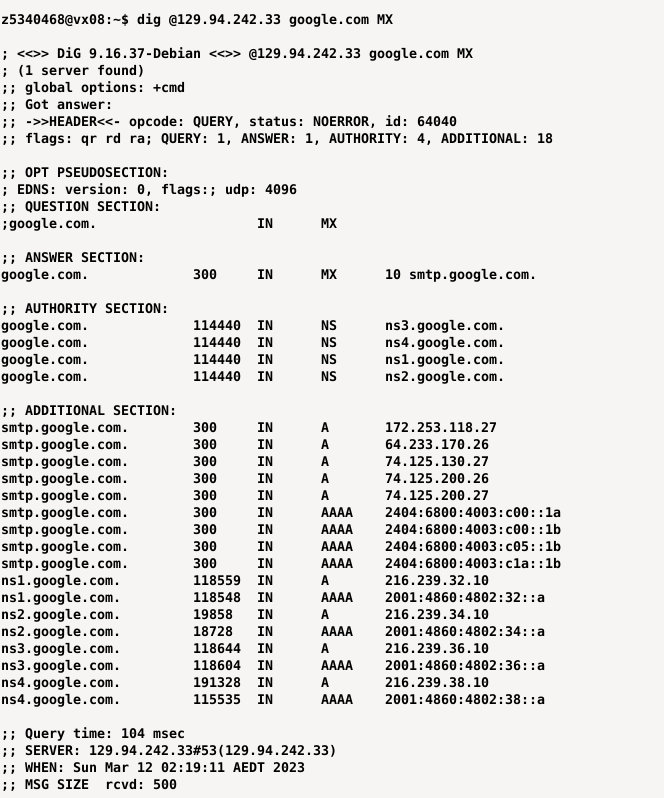
文本

描述已自动生成

Name is ece.drexel.edu. The type of DNS query sent to obtain this information was a PTR (pointer) query.

Question 7. Run, dig and query the CSE nameserver (129.94.242.33) for the mail servers for google.com (again, the domain name is google.com, not [www.google.com](http://www.google.com/)). Did you get an authoritative answer? Why? (HINT: Just because a response contains information in the authoritative part of the DNS response message does not mean it came from an authoritative name server. You should examine the flags in the response message to determine the answer)

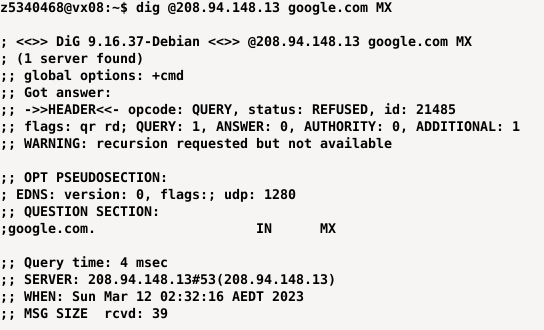
A:



In authoritative section, there are four authoritative nameservers for the google.com domain: ns1.google.com, ns2.google.com, ns3.google.com, and ns4.google.com.The CSE nameserver is not authoritative for the google.com domain because there is a ‘ra’ response in flag. ‘ra’ flag means the server supports recursive queries and ‘rd’ flag means the query was made with the recursive option.

Question 8. Repeat the above (i.e. Question 7) but use one of the nameservers obtained in Question 5. What is the result?

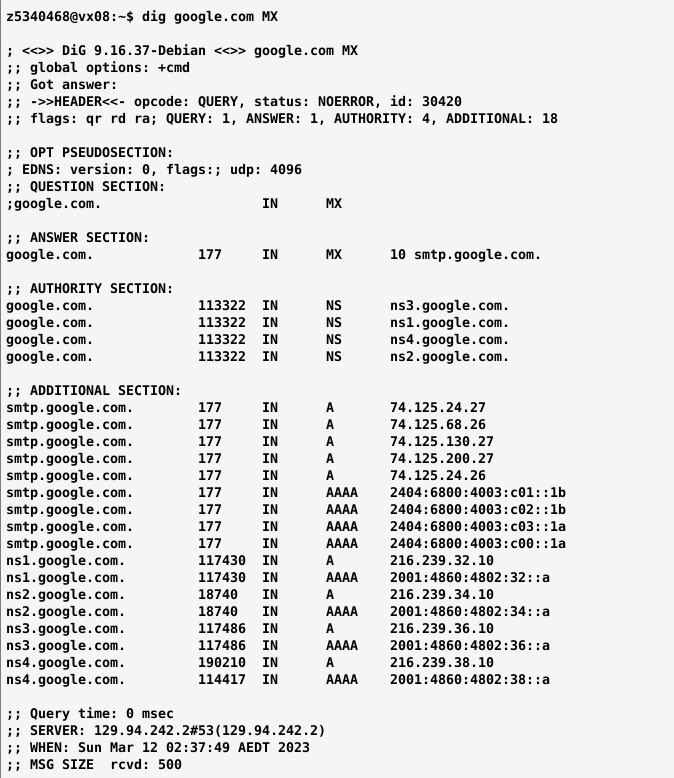
A:



There is a ‘REFUSED’ status, which means that the DNS server received the query but refused to give an answer. According to the ‘WARNING’, the DNS server does not support received queries, so it just provides answers for the domains for which it is authoritative.

Question 9. Obtain the authoritative answer for the mail servers for google.com. What type of DNS query is sent to obtain this information?

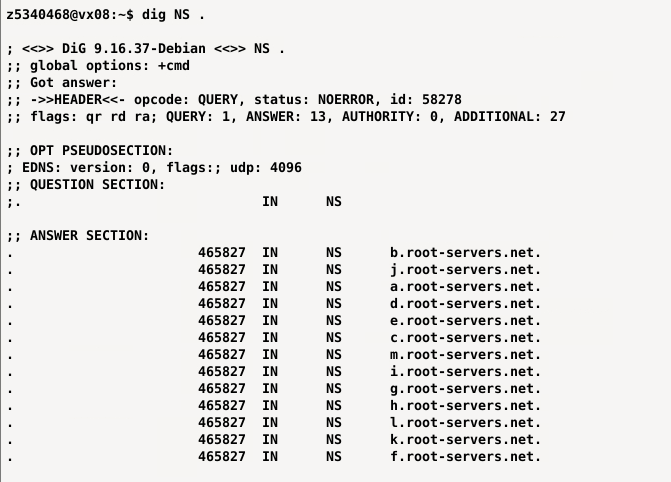
A:



It should be MX type.

Question 10. In this exercise, you simulate the iterative DNS query process to find the IP address of your machine (e.g. lyre00.cse.unsw.edu.au). If you are using VLAB Then find the IP address of one of the following: lyre00.cse.unsw.edu.au, lyre01.cse.unsw.edu.au, drum00.cse.unsw.edu.au or drum01.cse.unsw.edu.au. First, find the name server (query type NS) of the "." domain (root domain). Query this nameserver to find the authoritative name server for the "au." domain. Query this second server to find the authoritative nameserver for the "edu.au." domain. Now query this nameserver to find the authoritative nameserver for "unsw.edu.au". Next query the nameserver of unsw.edu.au to find the authoritative name server of cse.unsw.edu.au. Now query the nameserver of cse.unsw.edu.au to find the IP address of your host. How many DNS servers do you have to query to get the authoritative answer?

A:



表格

描述已自动生成

手机屏幕截图

描述已自动生成

手机屏幕截图

描述已自动生成

手机屏幕截图

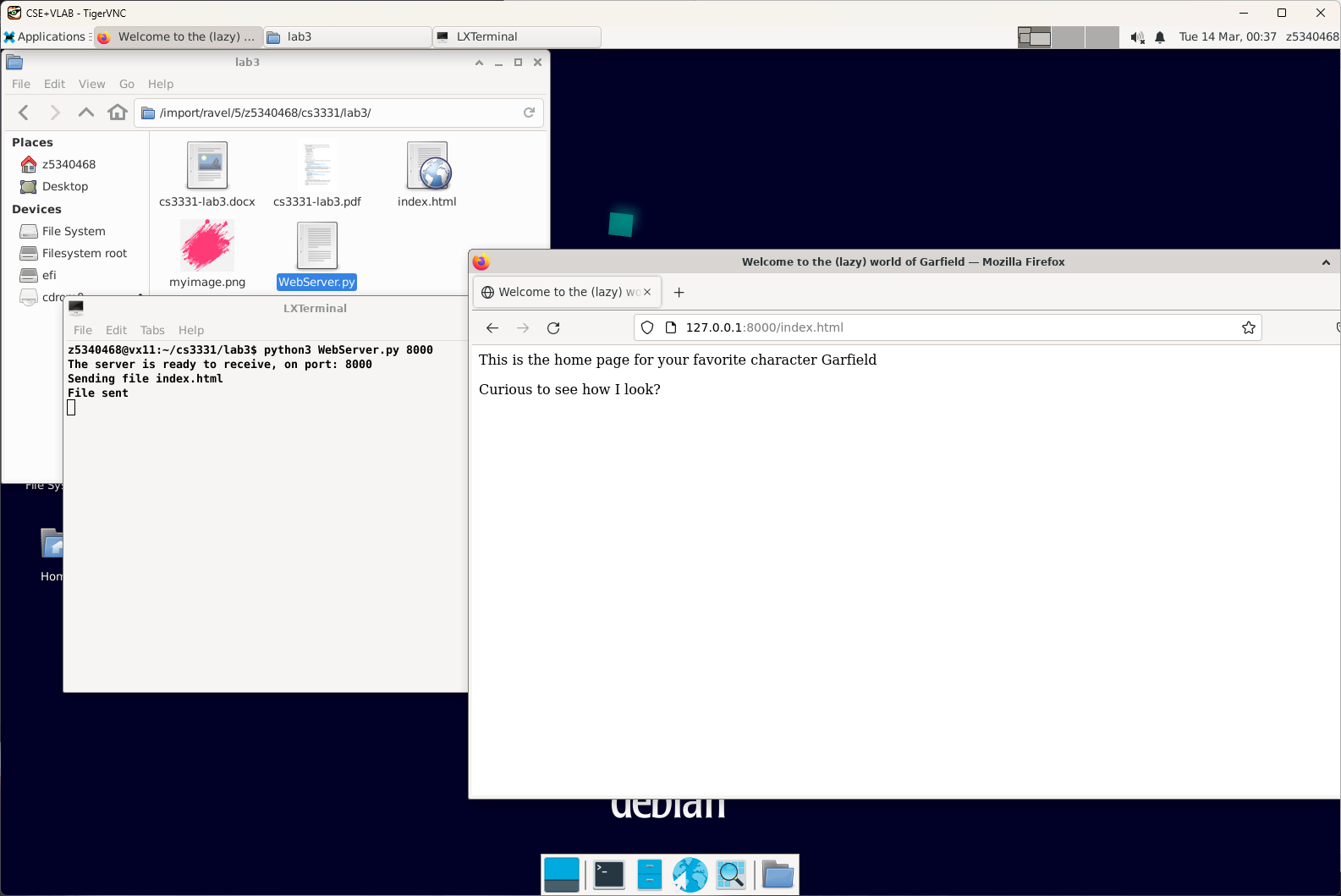
描述已自动生成

There are 5 steps.

Question 11. Can one physical machine have several names and/or IP addresses associated with it?

A: Yes it is, for load balancing or fault-tolerant.

E4:



图形用户界面, 应用程序, PowerPoint

描述已自动生成

图形用户界面, 应用程序

描述已自动生成