**Exercise 1**

* A – Address record. Returns a 32-bit IPv4 address, most commonly used to map hostnames to an IP address of the host.
* CNAME – Canonical name record. Alias of one name to another.
* MX – Mail exchange record. List of mail exchange servers that accept email for a domain.
* NS - Name server record. Delegates a DNS zone to use the given authoritative name servers.
* PTR – PTR resource record. Pointer to a canonical name.
* SOA - Start of [a zone of] authority record. Specifies authoritative information about a DNS zone, including the primary name server, the email of the domain administrator, the domain serial number, and several timers relating to refreshing the zone.

**Exercise 2**

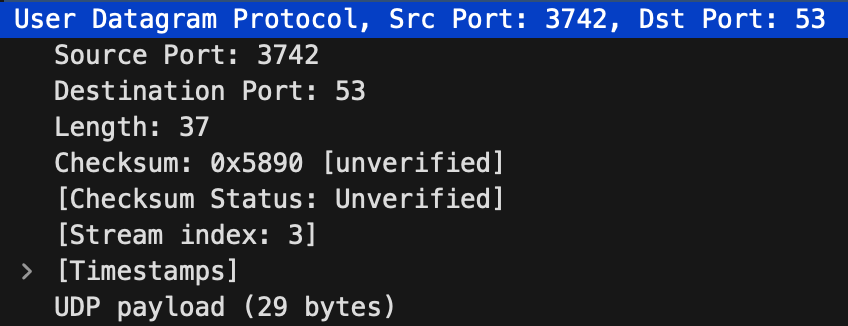
**A screenshot of a computer

Description automatically generated**

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

UDP

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



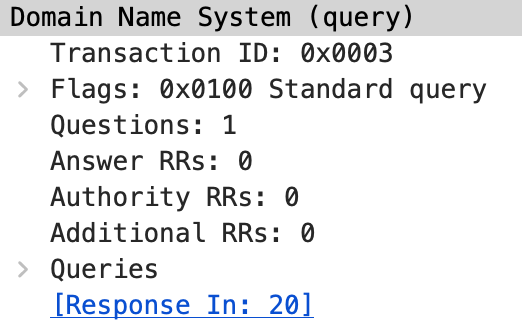
For the query message, source port is 3742, destination port is 53. For the response source port is 53 destination port is 3742.

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

****

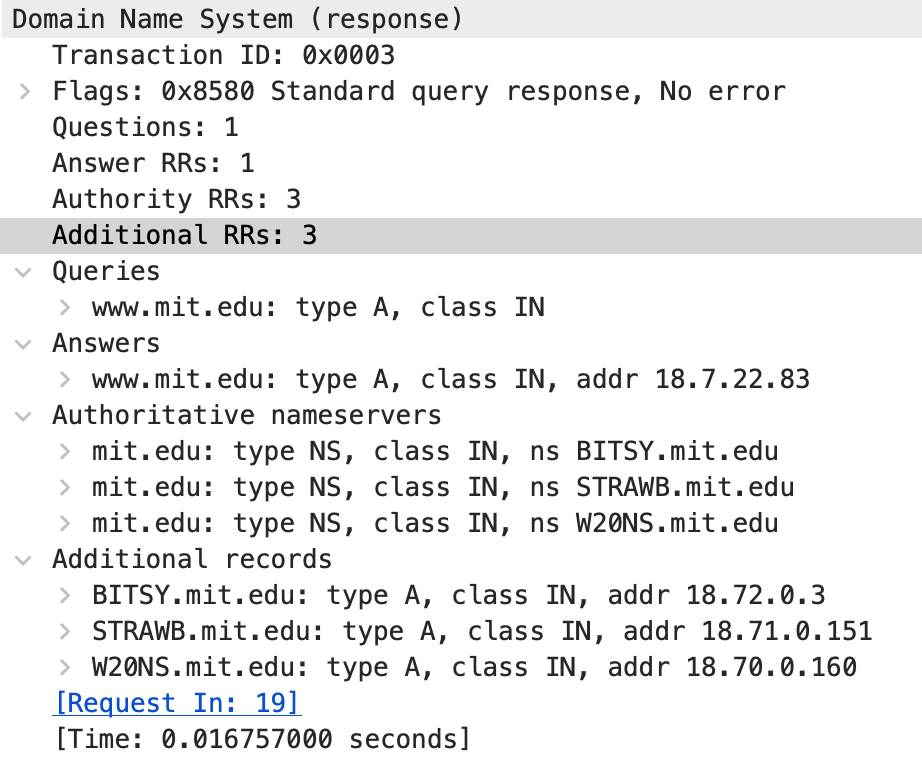
The IP address is 128.238.29.22. This is the same as the default DNS server, which means that we are sending the packet to our local DNS server.

**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”?**



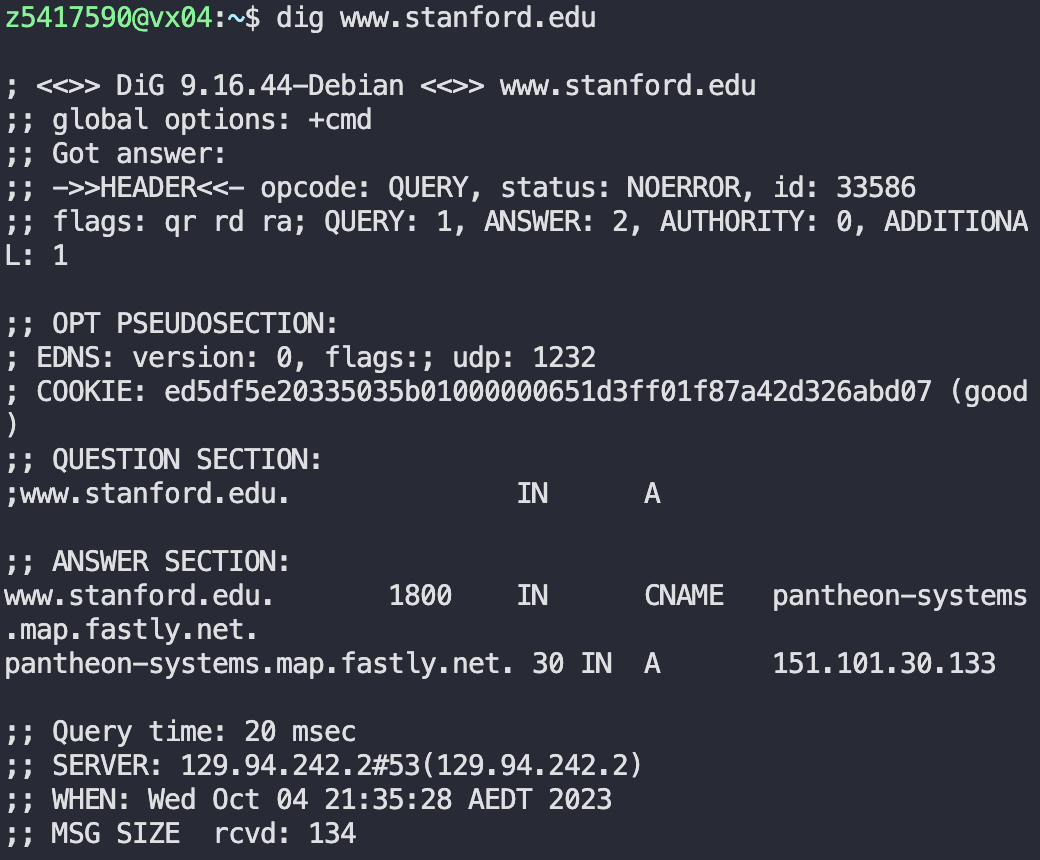
1 question contained in the DNS query message. The query message is of type A. The query message does not contain any answers.

**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?**

****

Answer contains the IP address of [www.mit.edu](http://www.mit.edu). Authoritative nameservers shows the three nameservers of mit.edu. Additional records shows the ip address of each of these nameservers.

**Exercise 3**



**Question 1. What is the IP address of www.stanford.edu? What type of DNS query is sent to get this answer?**

The IP address is 151.101.30.133. The DNS query is type A.

**Question 2. What is the canonical name for the Stanford webserver (i.e., www.stanford.edu )? Suggest a reason for having an alias for this server.**

The canonical name is pantheon-systems.map.fastly.net. The reason for having an alias is that it is easier to remember making it easier for users to access. Can also be useful in posting multiple services under one name.

**Question 3. What can you make of the rest of the response/what it is used for (i.e. the details available in the DNS response (cookie and other fields))?**

There are flags which tell us if it is authoritative or not. For the flags qr means A cookie is given for security reason and we can also find the DNS version. We can also find the message size being 134 bytes.

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

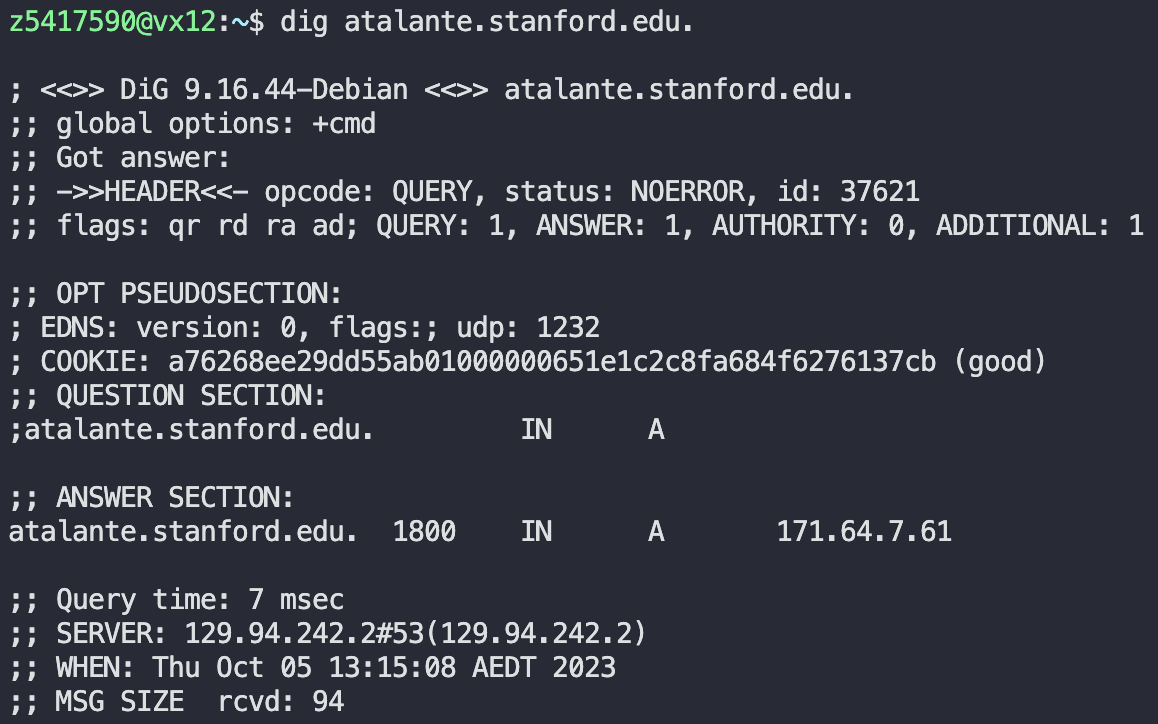
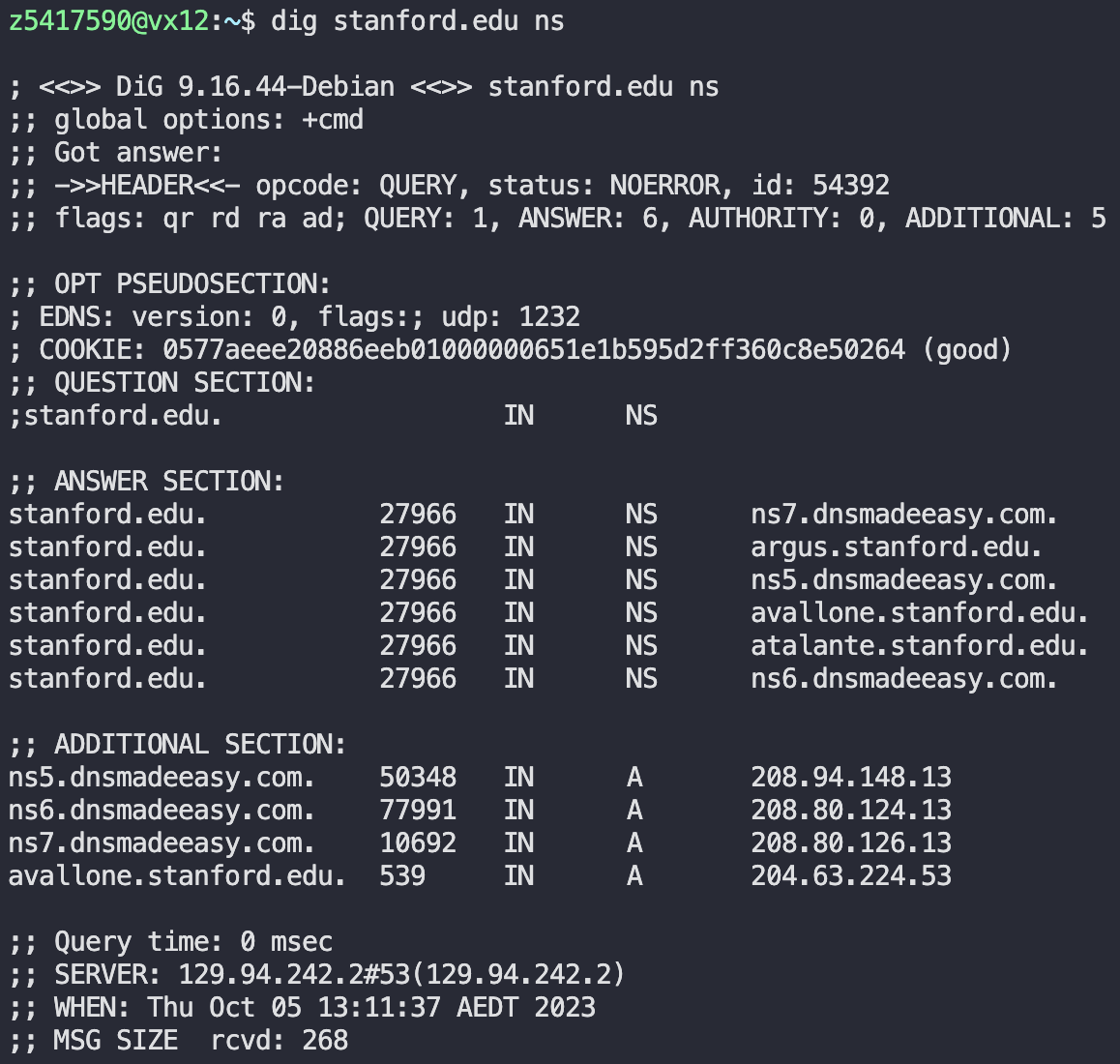
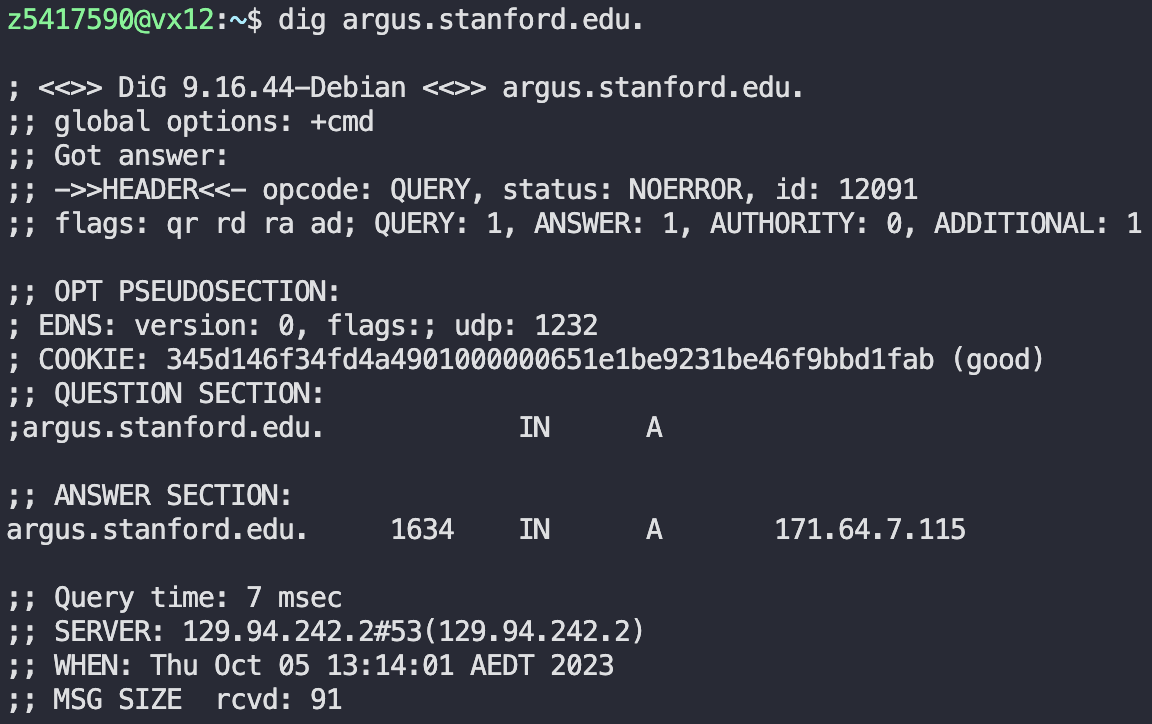
The IP address of my machine is 129.94.242.2 using the CSE servers.

**Question 5. What are the DNS nameservers for the "stanford.edu.” domain (note: the domain name is stanford.edu and not 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?**

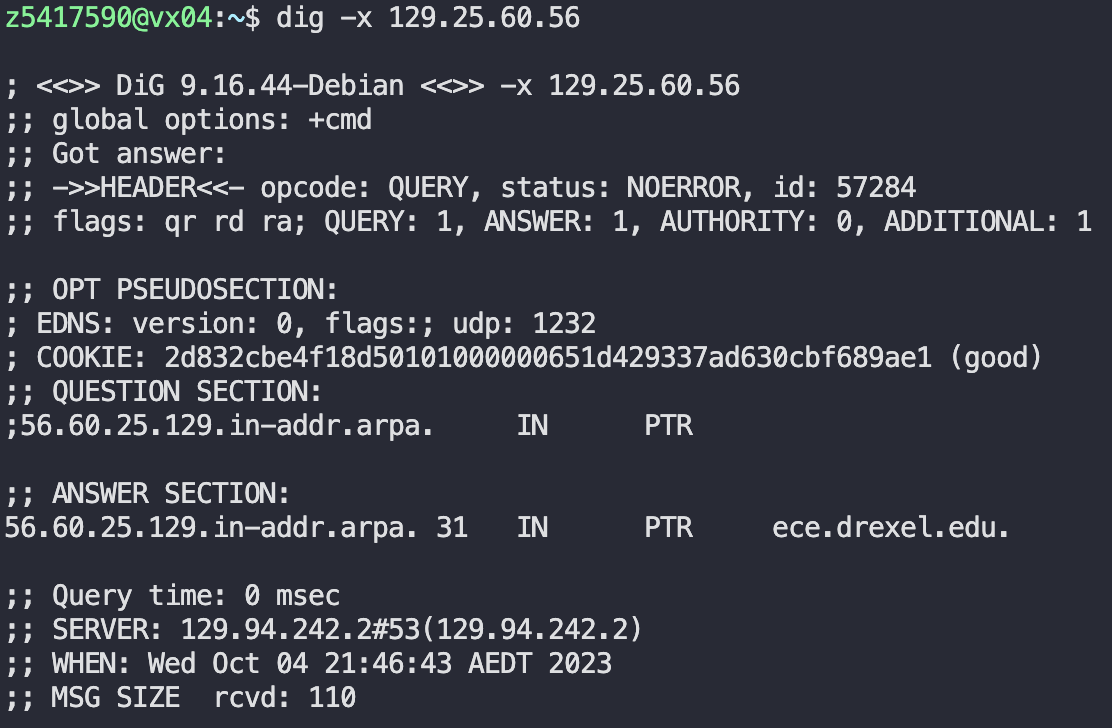
The DNS name servers and IP addresses of Stanford nameservers are:

* ns5.dnsmadeeasy.com.: 204.94.148.13
* ns6.dnsmadeeasy.com.: 208.80.124.13
* ns7.dnsmadeeasy.com.: 208.80.126.13
* avallone.stanford.edu.: 204.63.224.53
* argus.stanford.edu.: 171.64.7.115
* atalante.stanford.edu.: 171.64.7.61

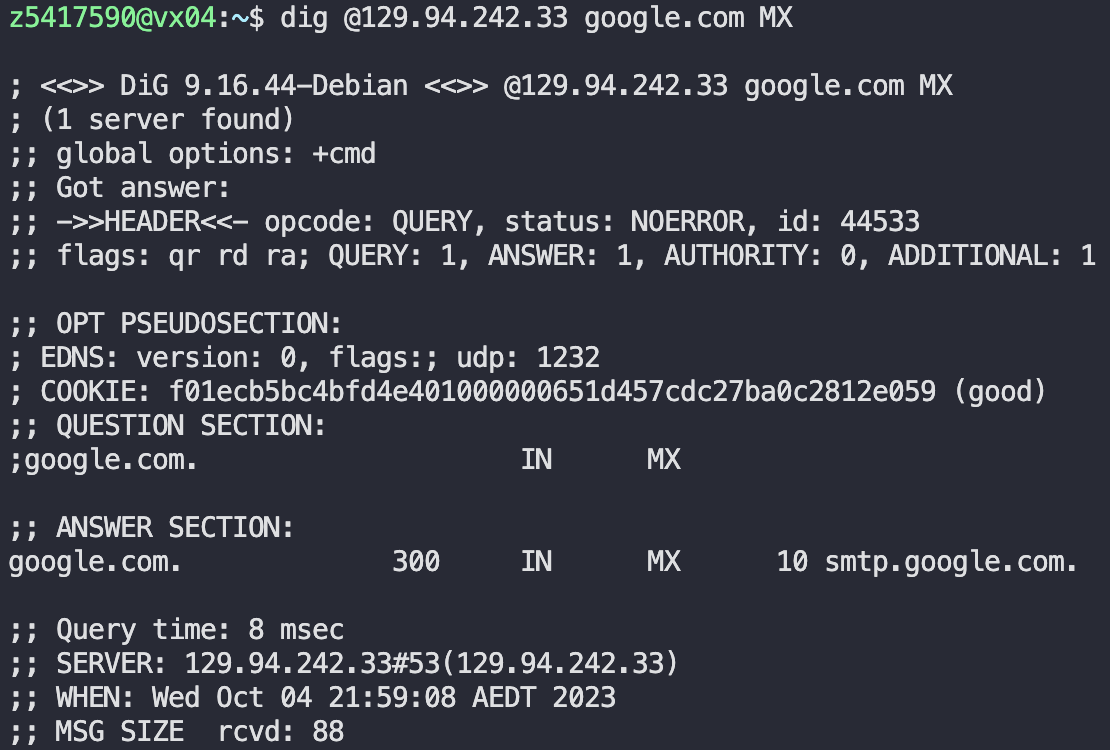
The DNS query sent to obtain this data is an NS query to obtain nameserver.

****

**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?**



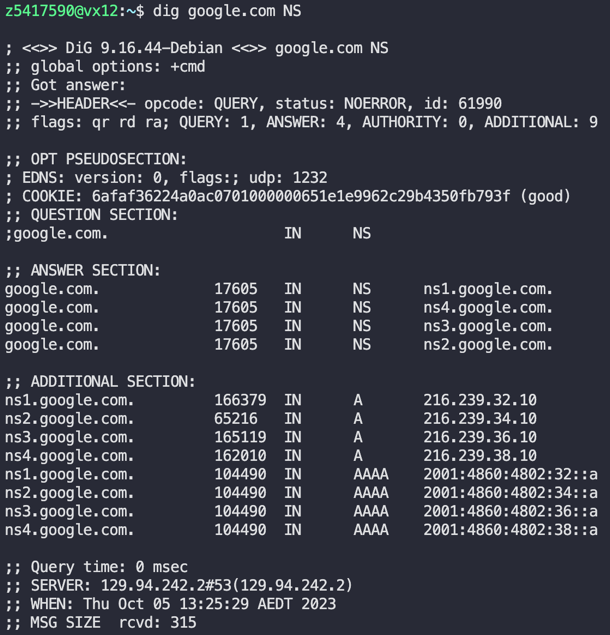
The DNS name associated with the IP address is ece.drexel.edu. The type of DNS query used was PTR.

**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 ). 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)** ****

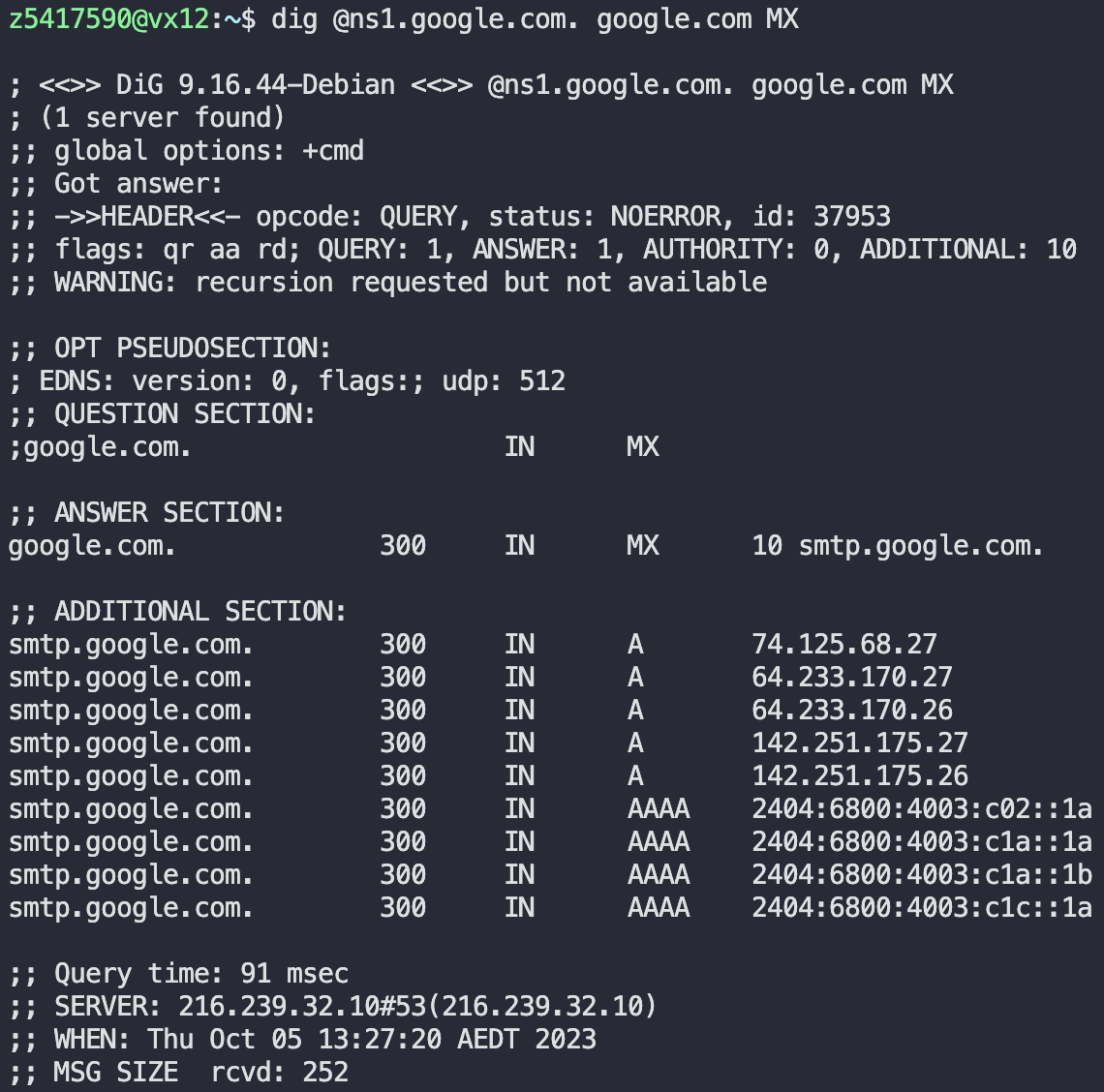
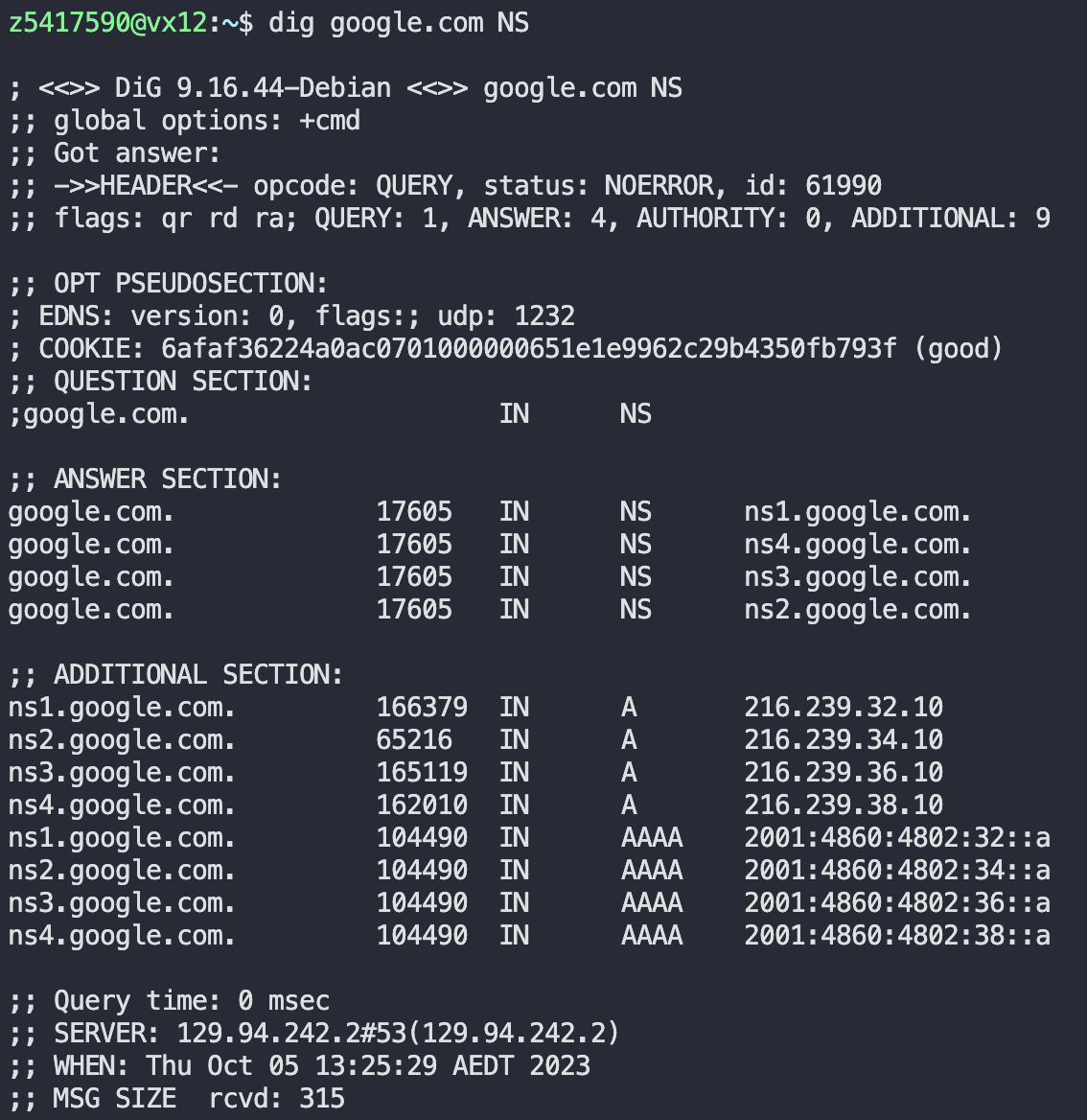
Did not get an authoritative answer. Examining the flags AA is not included which means that the response is not authoritative.

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

The answer is that Stanford refused to answer to us. As seen above the status: REFUSED. This was likely because we are not part of the Stanford network.

****

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

****

First find the name servers of google.com. Using one of these servers we can find the authoritative answer for the mail servers for google.com. We know it is authoritative because the flag has aa. The type of DNS query used is MX.

**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, flute00.cse.unsw.edu.au or flute01.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?**

6 DNS servers are queried to get the authoritative answer. The IP address of lyre00.cse.unsw.edu.au is 129.94.210.20.

|  |  |
| --- | --- |
|  | **DNS screenshots** |
| Root Domain |  |
| A root server  dig @a.root-servers.net. .au NS |  |
| q.au  dig @q.au. edu.au. NS |  |
| edu.au  dig @q.au. unsw.edu.au NS |  |
| Unsw.edu.au  dig @ns1.unsw.edu.au. cse.unsw.edu.au NS |  |
| Beethoven.orchestra.cse.unsw.edu.au  dig @beethoven.orchestra.cse.unsw.edu.au. lyre00.cse.unsw.edu.au A |  |

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

Yes, a machine can have several names or IP addresses. IP addresses can have multiples aliases associated with them.