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

IP address of the www.sina.com.cn is 36.51.254.37

mac:~ duan$ nslookup www.sina.com.cn

Server: 192.168.1.1

Address: 192.168.1.1#53

Non-authoritative answer:

www.sina.com.cn canonical name = spool.grid.sinaedge.com.

Name: spool.grid.sinaedge.com

Address: 36.51.254.37

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

The authoritative DNS servers for London University are ns0.ulcc.ac.uk and ns1.ulcc.ac.uk

mac:~ duan$ nslookup -type=NS london.ac.uk

Server: 192.168.1.1

Address: 192.168.1.1#53

Non-authoritative answer:

london.ac.uk nameserver = ns0.ulcc.ac.uk.

london.ac.uk nameserver = ns1.ulcc.ac.uk.

Authoritative answers can be found from:

ns0.ulcc.ac.uk internet address = 193.63.88.11

1. Run *nslookup* so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! mail. What is its IP address?

Its IP addresses are 94.245.120.74 and 213.199.154.138

mac:~ duan$ nslookup -type=MX london.ac.uk ns0.ulcc.ac.uk

Server: ns0.ulcc.ac.uk

Address: 193.63.88.11#53

london.ac.uk mail exchanger = 0 london-ac-uk.mail.protection.outlook.com.

mac:~ duan$ nslookup london-ac-uk.mail.protection.outlook.com

Server: 192.168.1.1

Address: 192.168.1.1#53

Non-authoritative answer:

Name: london-ac-uk.mail.protection.outlook.com

Address: 94.245.120.74

Name: london-ac-uk.mail.protection.outlook.com

Address: 213.199.154.138

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

UDP

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

Destination port is 53, and source port is 40049

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?

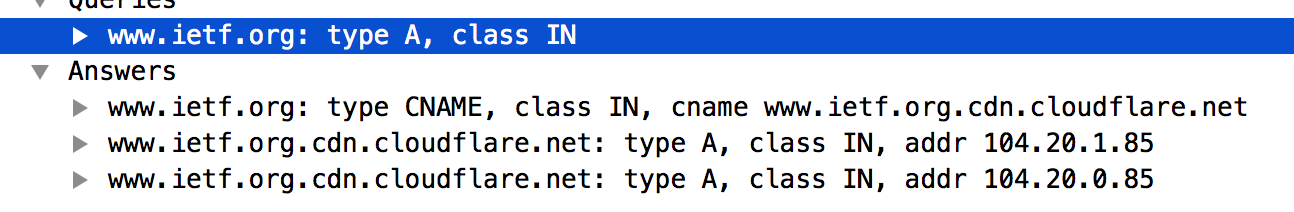
The IP address is 192.168.1.1. It is the same as my local DNS server.

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

The type is ‘A’. The message does not contain any answers.

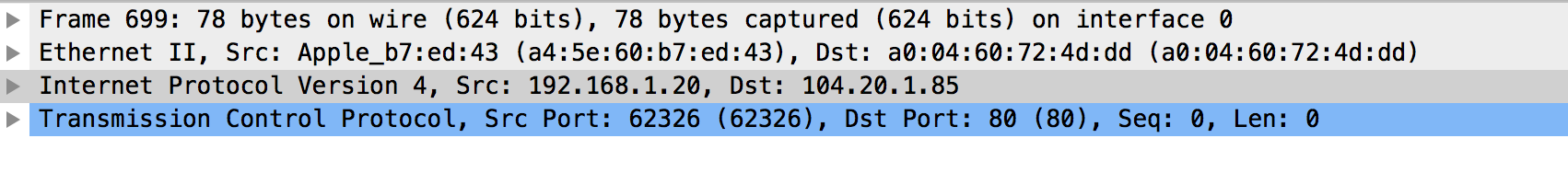
1. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

It contains three answers. One is cname of the hostname, the other two are addresses of the cname. All of them are shown in the following figure.



1. 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?

Yes, it uses the first IP provided by DNS response message.



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

No, because the hostname was the same.

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

Destination port is 53, and source port is 65279

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

The IP address is 192.168.1.1. It is the same as my local DNS server.

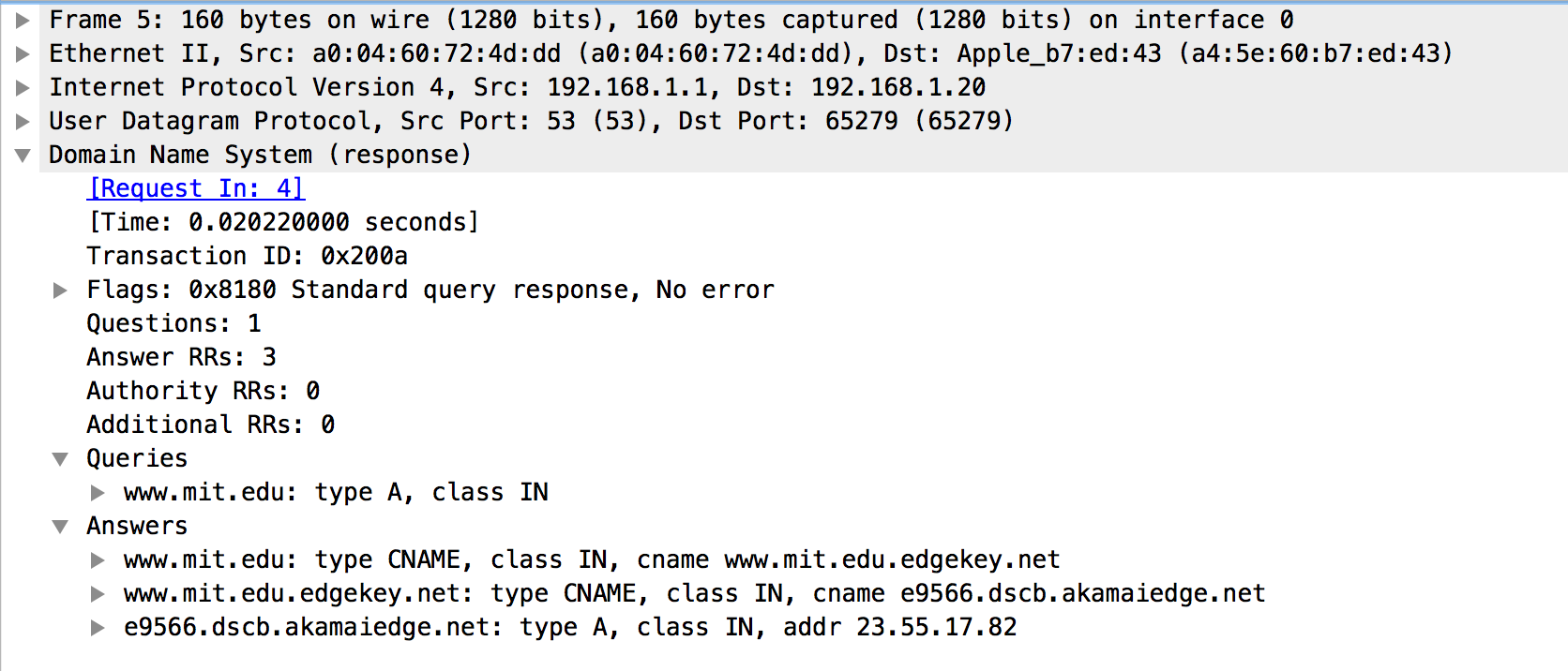
1. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

The type is ‘A’. The message does not contain any answers.

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

There are 3 answers in the response message. One is cname of the hostname, the other two are addresses of the cname.

1. Provide a screenshot.



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

The IP address is 192.168.1.1. It is the same as my local DNS server.

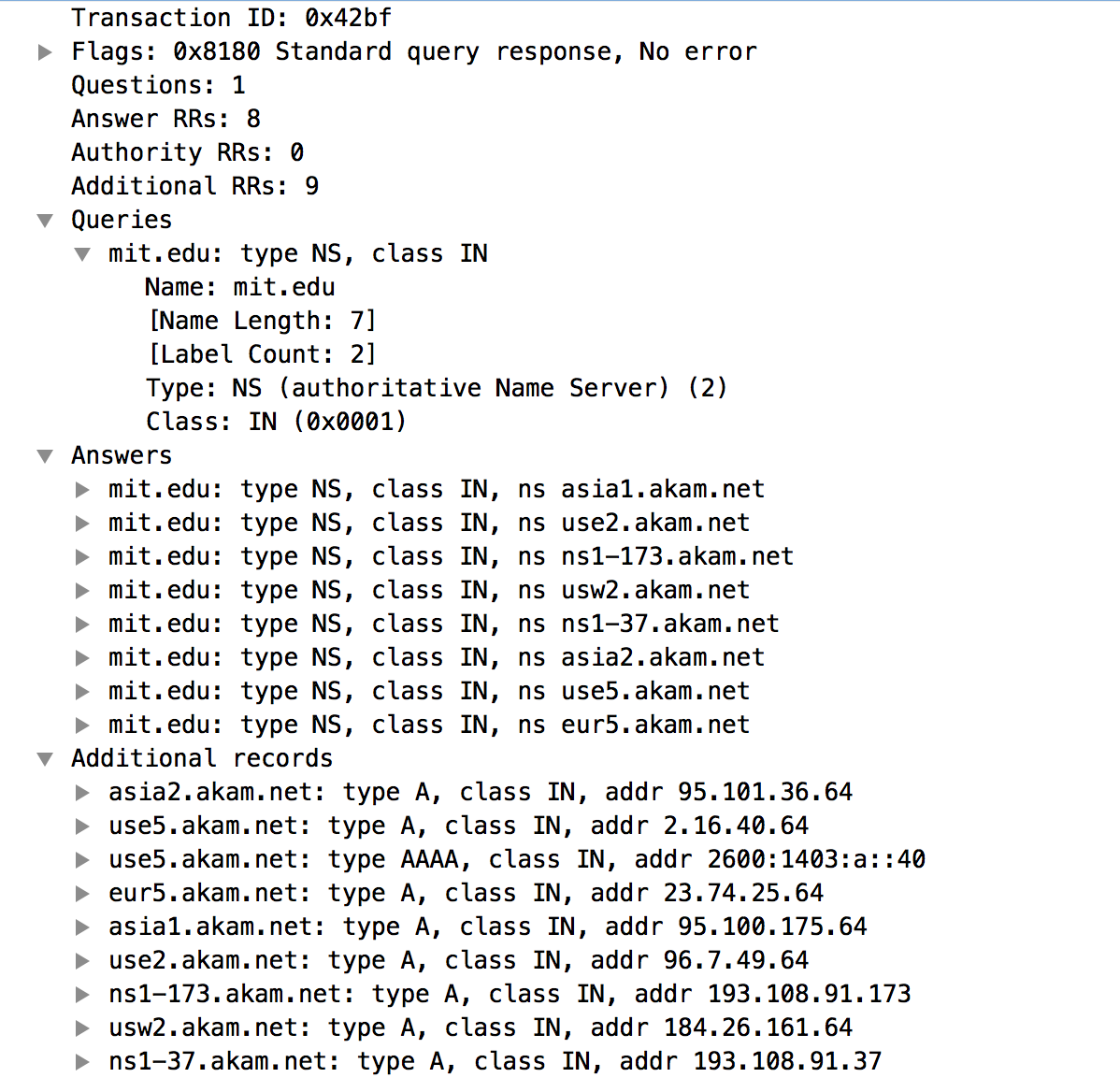
1. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

The type is ‘NS’. The message does not contain any answers.

1. 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 namservers?

The response provides eight MIT nameservers and also their IP addresses.

1. Provide a screenshot.



1. 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?

The query message is sent to 18.72.0.3, which is the IP address of bitsy.mit.edu, is not IP address of my local DNS server.

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

The type is ‘A’. The message does not contain any answers.

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

No response. My system is OSX. I started another Ubuntu 16.04 virtual machine, there is still no response. I created a virtual machine on AWS and there was still no response.

1. Provide a screenshot.

