**Lab 2a. Continue**

**16.** There are 3 HTTP GET request messages sent from my browser. IP addresses: 128.119.245.12, 128.119.245.12, 128.119.245.12

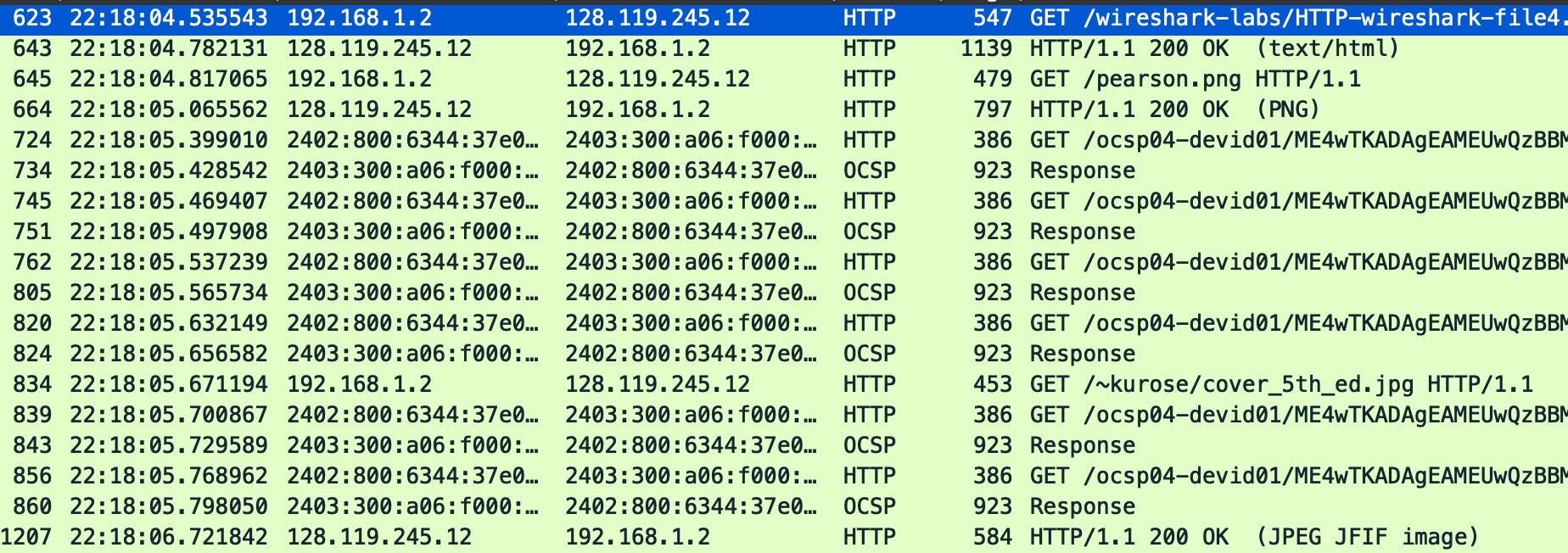
17. The two images were downloaded serially. The first image was requested and

retrieved with a status of 200 OK. Then the browser tried to download the

second image and had a response of 302 Found, which means the image

location moved. The browser had to then send another request to the new

destination to retrieve the second image, and it came back with a 200 OK.

**17.** Two images were downloaded serially, the first image was requested and retrieved with status 200 OK. Then browser tried to download second image and had response of 200 OK.

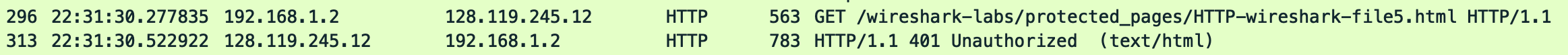
The two images were downloaded serially. The first image was requested and

retrieved with a status of 200 OK. Then the browser tried to download the

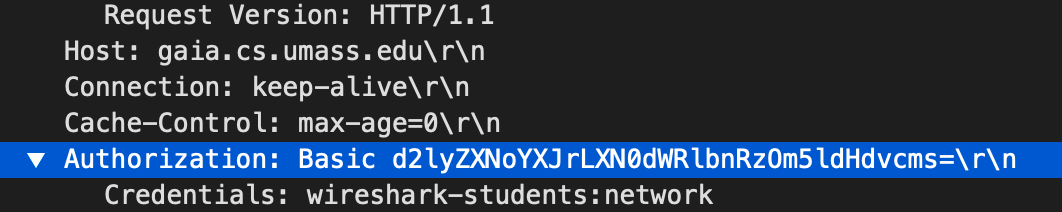
second image and had a response of 302 Found, which means the image

location moved. The browser had to then send another request to the new

destination to retrieve the second image, and it came back with a 200 OK.

**18.** 

**19.**

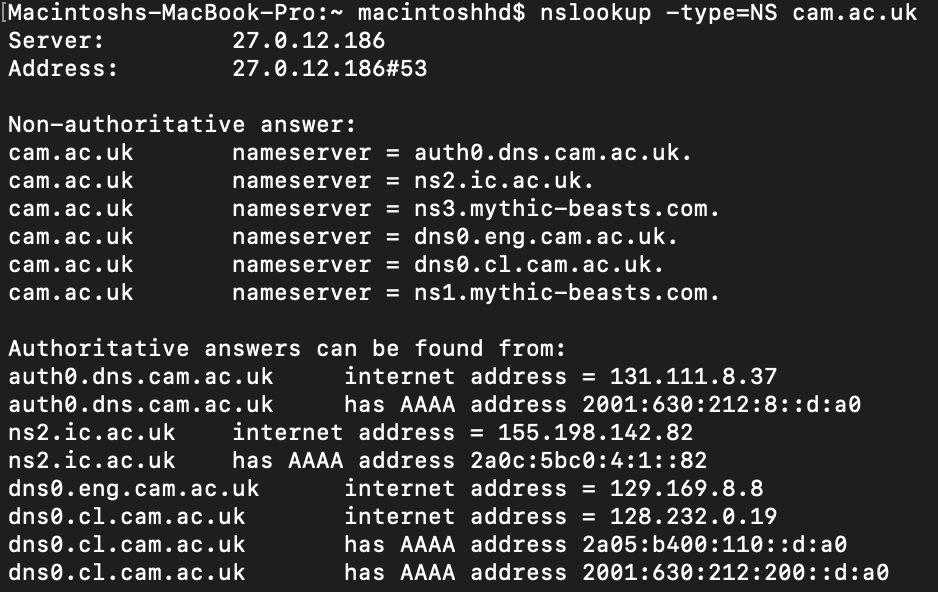


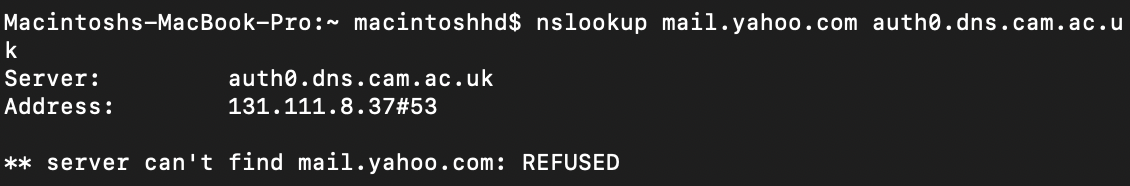
**LAB 2b. Wireshark DNS**

1. 

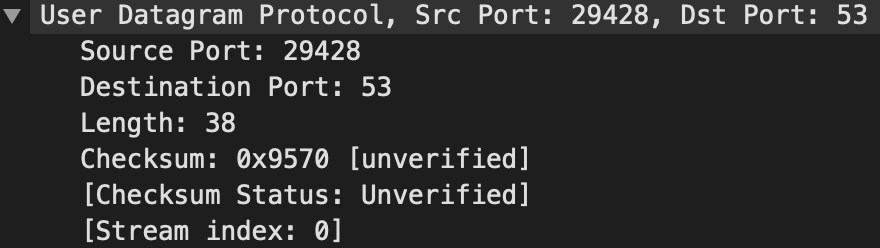
IP: 23.15.107.88

1. University of Cambridge was the target of this nslookup at [http://www.cam.ac.uk](http://www.cam.ac.uk/)



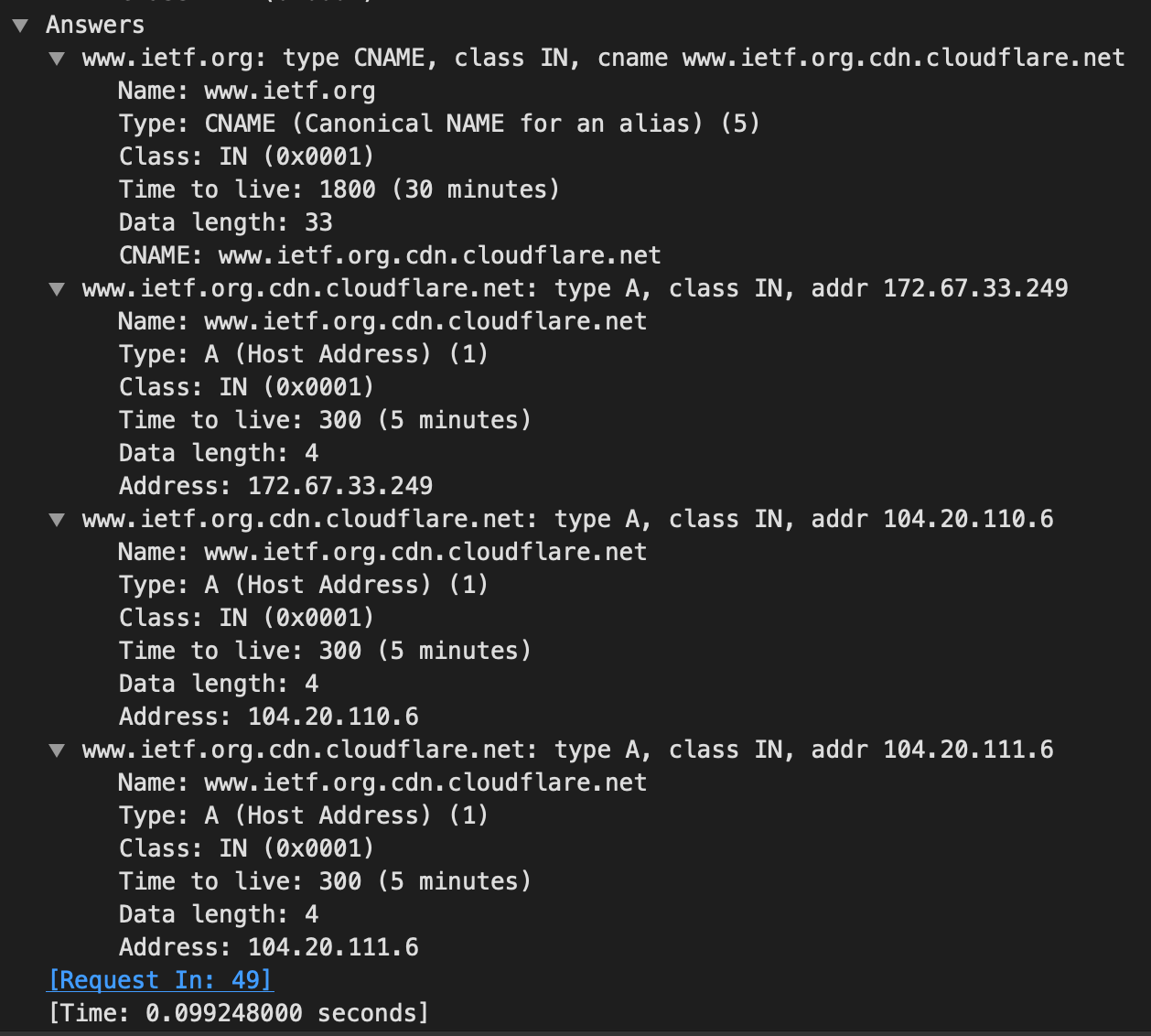
1. 
2. The query and response messages are sent via UDP





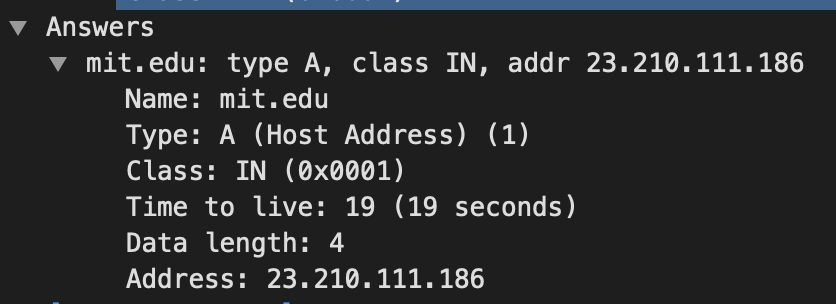
1. The destination port is port 53, and the source port is port 29428.
2. The DNS query message was sent to 203.113.188.1
3. 

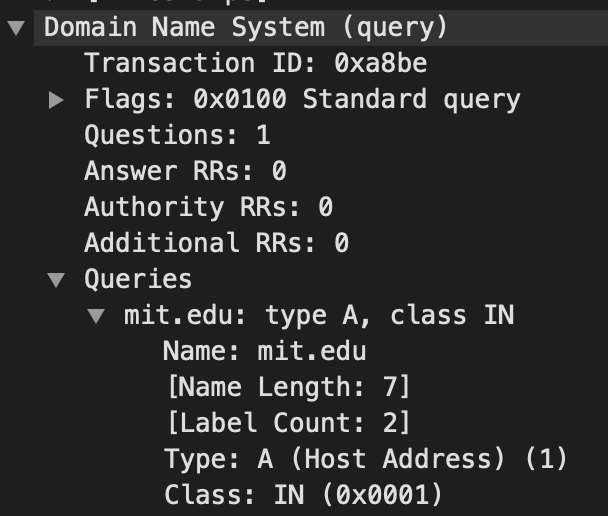
This query was a type A query. It did not contain any “answers”.



1. The destination IP address of the SYN packet corresponds to the address provided by the DNS response, 172.67.33.249
2. No
3. Destination port: 53, source port: 49290
4. IP address is the DNS query message sent: 27.0.12.186, which is the same as my local DNS server
5. The query is of type A and it doesn’t contain any answers

**14,15.**



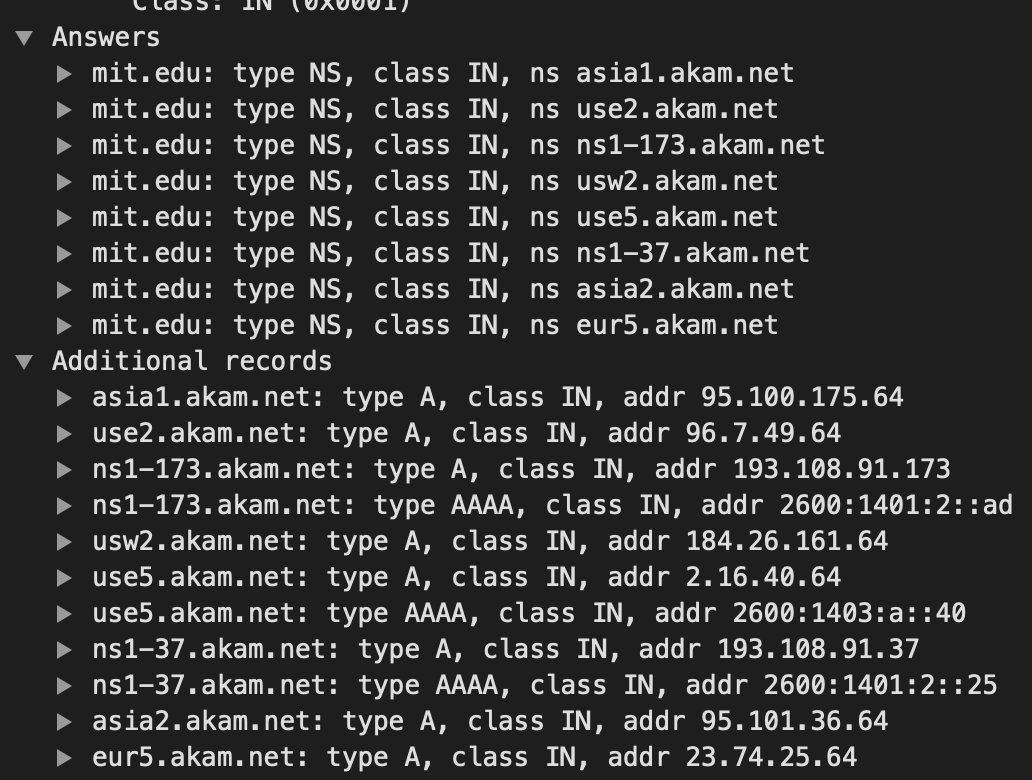


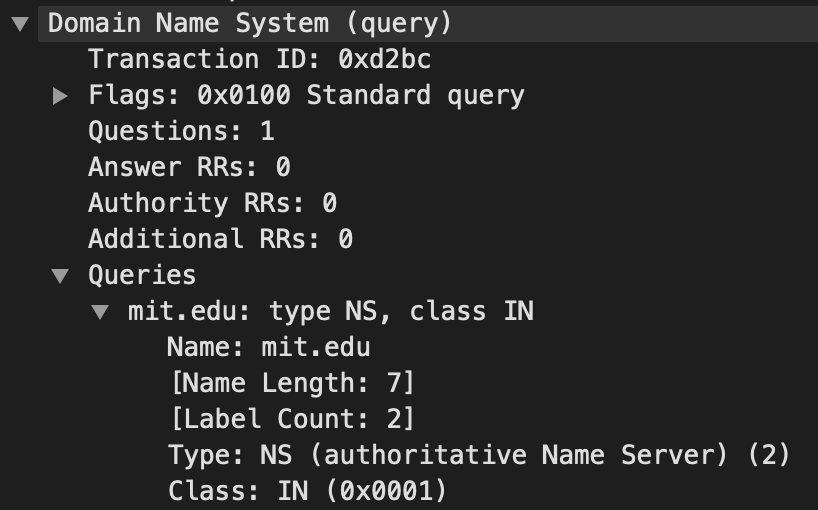


**16.** IP address is the DNS query message sent: 27.0.12.186 which is my default DNS server

**17.** The query is of type NS and it doesn’t contain any answers

**18.** The namesevers are asia1, use2, ns1-173, usw2, use5, ns1-37, asia2 and eur5. We can find their IP addresses if we expand the Additional records field in Wireshark as seen below.

**19.** 



 **20🡪23.**