nslookup: search information about the mapping between domain name and its address

Server: 8.8.8.8

Address: 8.8.8.8#53

Non-authoritative answer:

Name: microsoft.com

Address: 134.170.185.46

Name: microsoft.com

Address: 134.170.188.221

server: the server address that we use to translate the domain name

address: #53 means the port we are communicating, it is common DNS port for query

canonical name: host name of the server

the two andress under show that the server use round robin to distribute server load

-type=MX : query mail exchanger

-type=NS : name server

-type=soa : (start of authority) technical information about the domain

origin: The authority from which the information originated.

mail addr: The e-mail address of the domain administrator (The first dot would be an @ symbol in an e-mail address, so here the e-mail address is msnhst@microsoft.com).

serial: Revision data for this information, in the form YYYYMMDDNN. Here, the information is current as of August 11, 2014; 02 means it was the second revision made on that day.

refresh: A number representing the interval, in seconds, after which the secondary name server will check the primary name server for an updated revision of this information. This information tells us that the secondary Microsoft name server's information is never more than two hours (7200 seconds) out of date.

retry: The secondary nameserver will wait this many seconds before attempting to reconnect to the primary name server after a failed attempt.

expire: The secondary nameserver's cache of the primary nameserver's information will always be considered invalid after this many seconds.

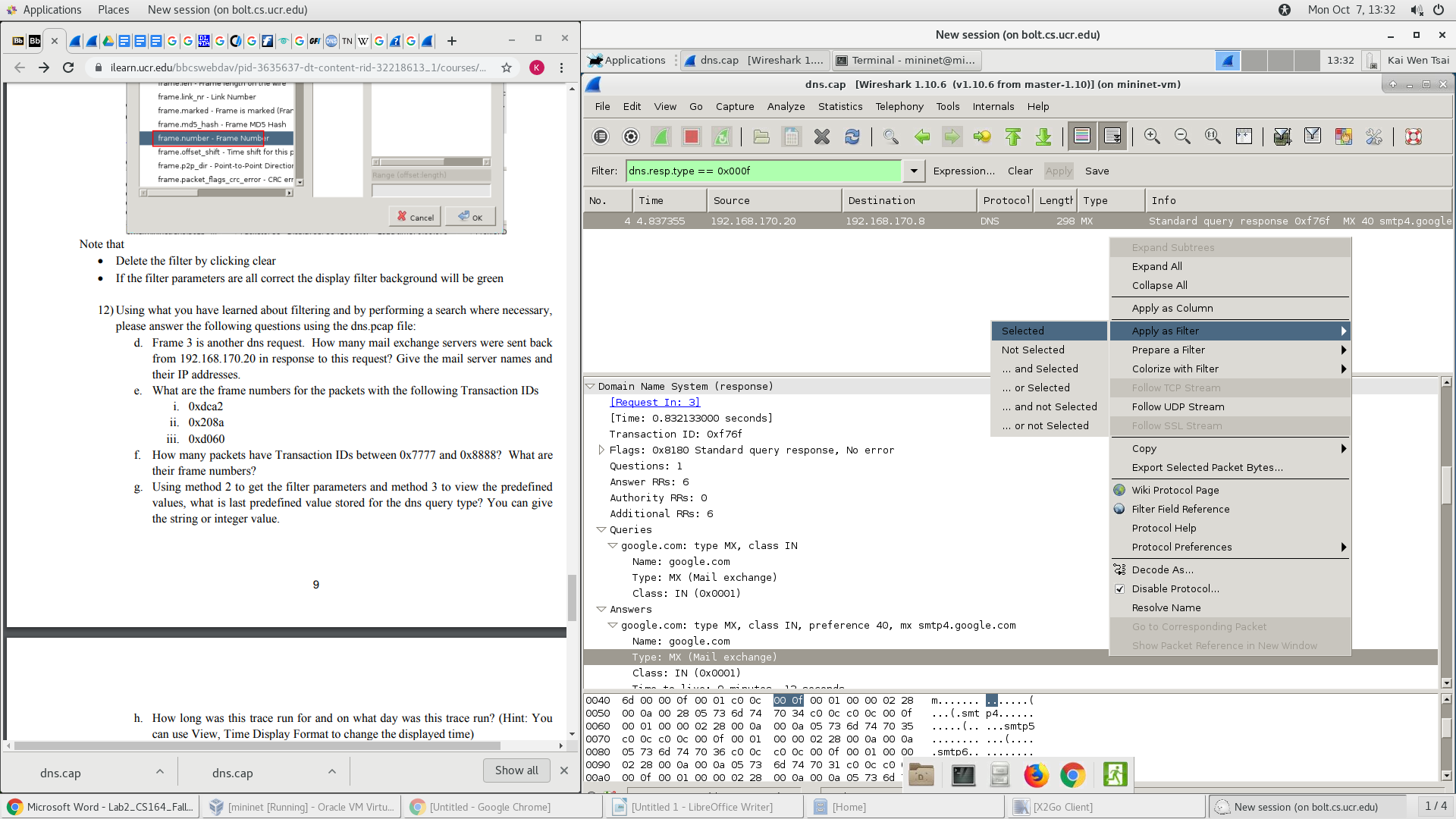
minimum: The secondary nameserver's cache of the primary nameserver's information should not be refreshed if this amount of time has not elapsed since the last refresh.

we can use revision search for IP to find the name for the IP

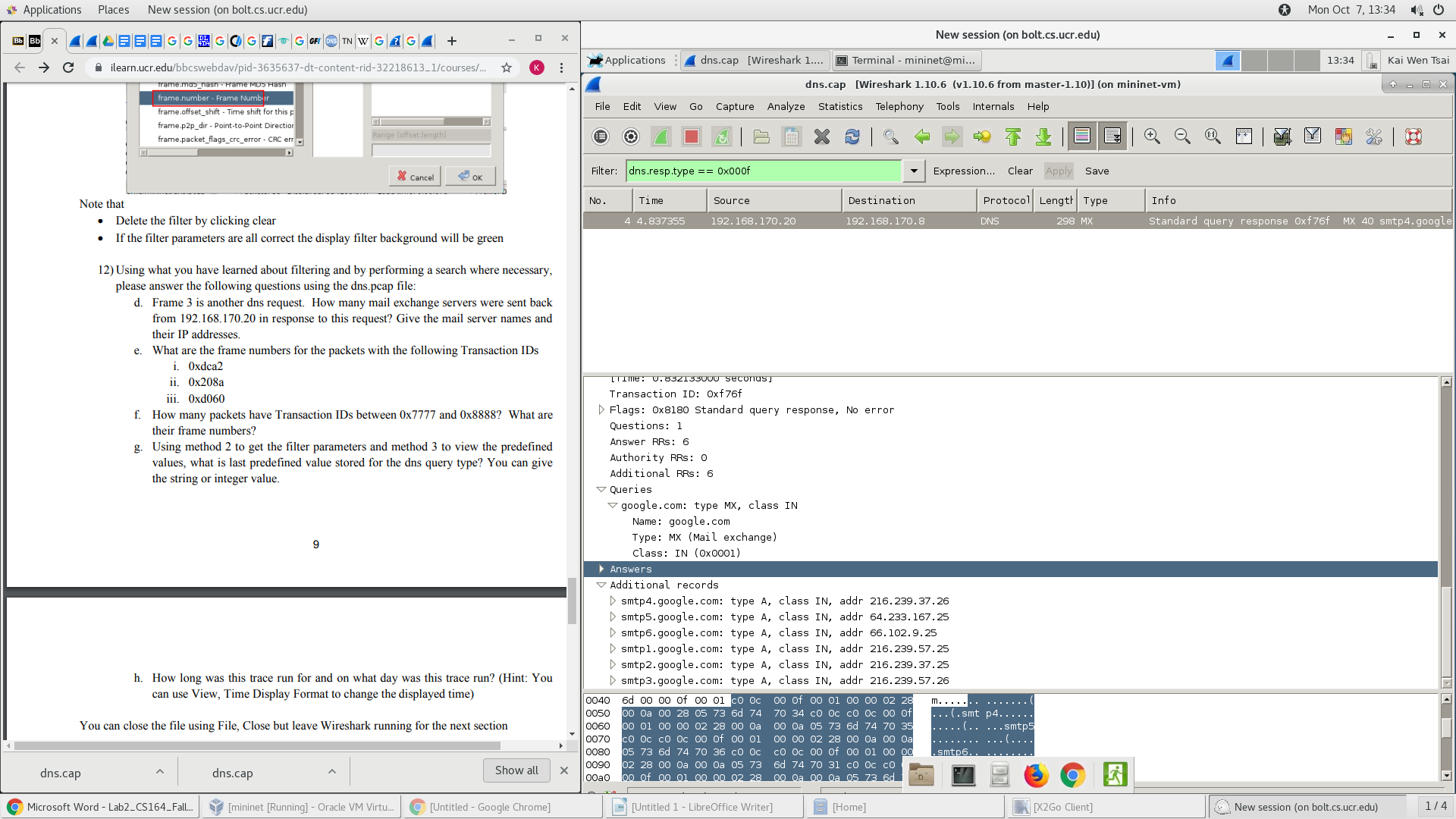
name of 8.8.8.8: google.com

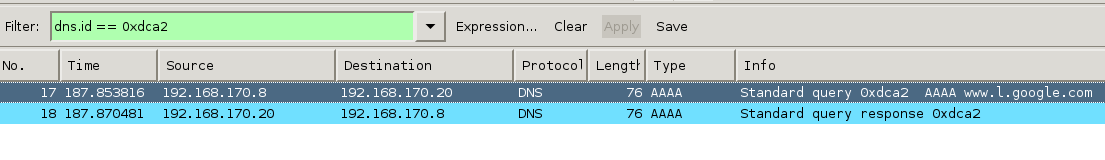
to take area of screenshot on linux: ctrl + shift + prtscn

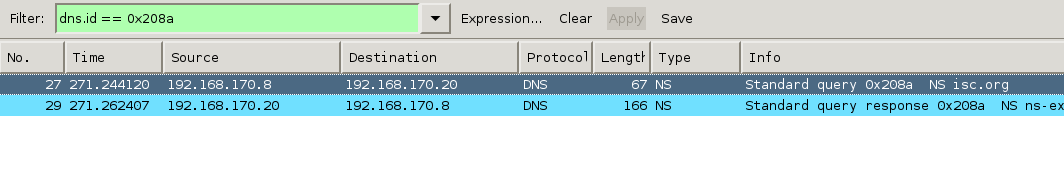
find response type that is mx:

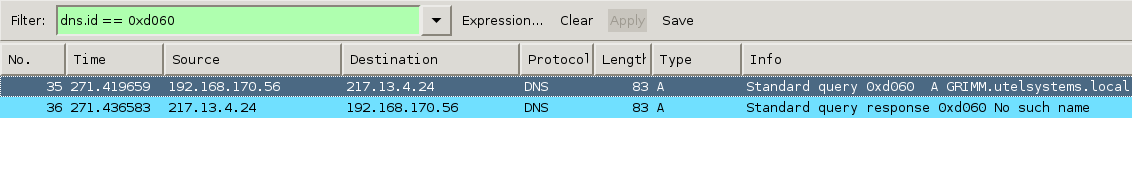


this is the name and type

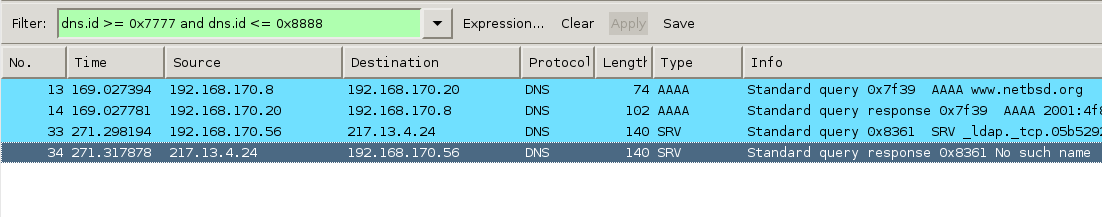




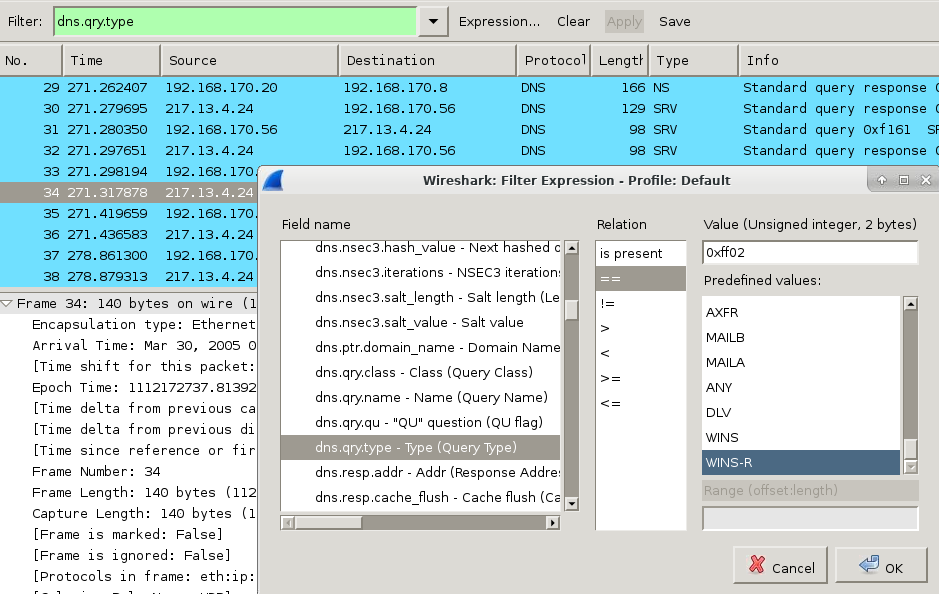




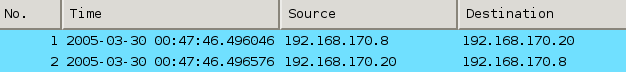
between



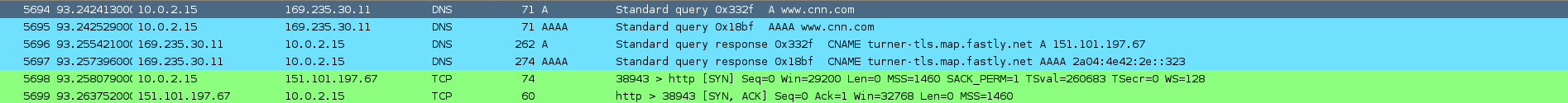
last in predefined value



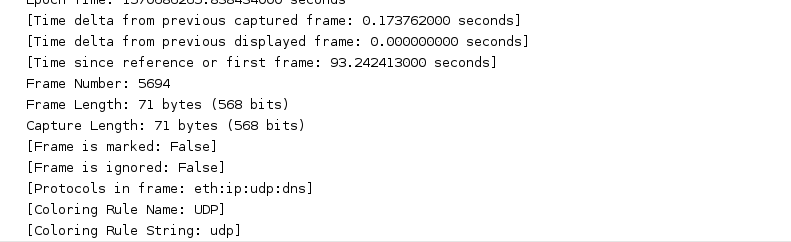
when trace start



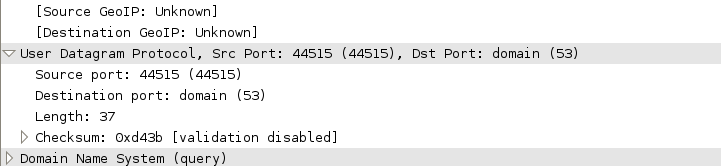
part3

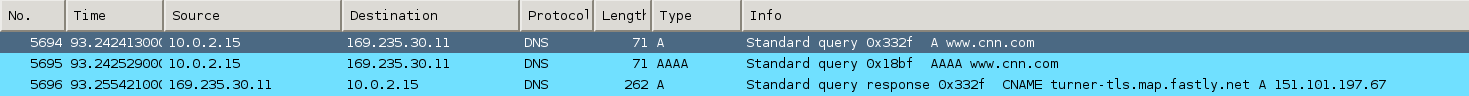
first package  


UDP



destination port:53

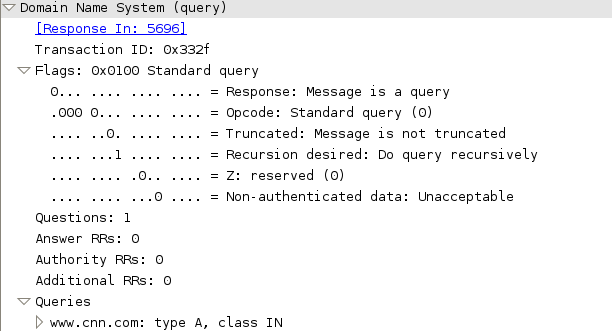




destination ip: 169.235.30.11

it goes through DNS to find the IP address based on the domain name we type in

query:

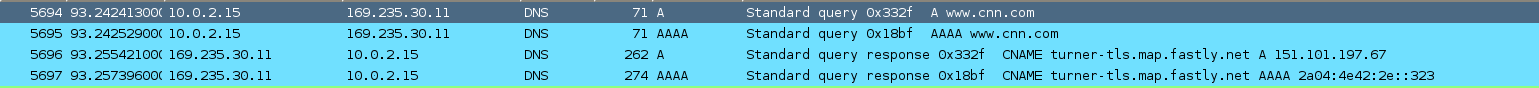


response is the feedback from the destination source when we send a request saying the connection is created

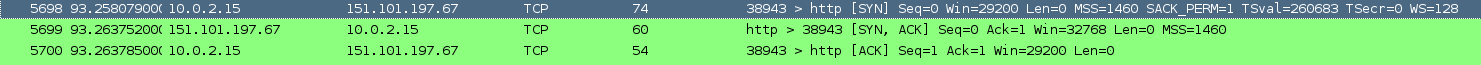


type A: is for ipv4 mapping

type AAA: for ipv6 mapping



three way handshake



after these

GET request , HTTP request and response



sequence number shows how much data have sent

Acknowledgment Numbers shows how much data have received

FIN flag tells no data is needed to send