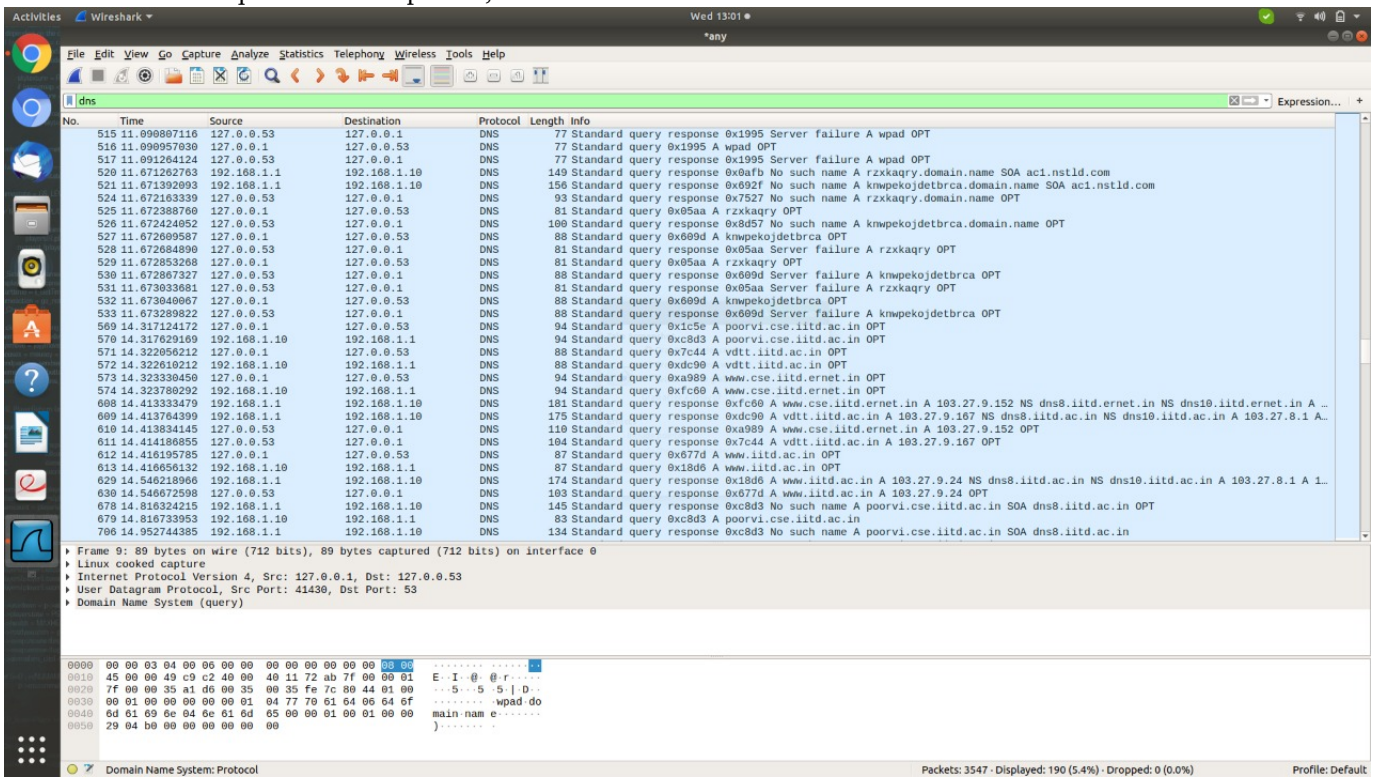
1 Q1

1.1 subpart a

Yes, I could find DNS queries and responses for www.cse.iitd.ac.in
The DNS server used was 192.168.1.11
There were several queries and responses, out of which 2 are shown in the screenshot.



For the following queries, time taken for the DNS request-response to complete was :
1. 0x09b9 took 0.081258836 ms
2. 0x9aee took 0.080320496 ms

The other requests were sent to poorvi.iitd.ac.in and iitd.ernet.in

1.2 subpart b

Number of GET requests : 30
This tells us that web pages are not composed of one or elements, there are many constituents of any webpage and all of them have to be loaded for the webpage to display completely in the browser.

When there are mutliple objects, they are requested on different TCP connections and pipelined so that less time is required for loading all of them. After obtaining the content objects from different TCP connections, the HTML, CSS and javascript script files are processed to DOM, CSSDOM and finally into a rendering tree. This is a part of the procedure to build up the webpage.

1.3 subpart c

Number of TCP connections that were opened between my browser and the web-server = 7
All of them were distinct wrt (source IP, destination IP, source port, destination port)

1.4 subpart d

Yes, several content objects are fetched over the same TCP connection.
There were 7 connections and over 1000 packets over the 7 of them only

1.5 subpart e

Handshake time			
Source Port	SYN	ACK	Latency
51840	5.453978758	6.530710991	1.076732233
51842	5.455578484	5.586028334	0.130449850
51852	14.113987664	14.209731696	0.095744032
51854	14.123186099	14.209898963	0.086712864
51856	14.125629608	14.209909908	0.084280300
51858	14.125905676	14.209935313	0.084029637
51860	14.136883448	14.209950757	0.073067309

Latencies are sufficiently large for the TCP connections, so in order to optimize loading contents of a webpage, a browser genrally keeps the TCP connection alive and downloads multiple objects over it. It can also make use of cache.

1.6 subpart f

page load time = $14.550804308 - 5.453978758 = 92.09682555$

1.7 subpart g

For www.indianexpress.com, I could filter only 2 HTTP entries. So there wasn't any HTTP traffic for www.indianexpress.com
I could not see any HTML/CSS/Javscript files being transferred
Yes, I could see the contents of HTML and Javascript files like .js files, .png images etc for www.cse.iitd.ac.in

This happens because the content of www.indianexpress.com is encrypted and hence not visible from wireshark. This is probably because of restrictions from the indian express server itself since the site contains several advertisements hyperlinked to other web servers of amazon, facebook etc. and there must be privacy protection norms imposed by them. There aren't any ads on www.cse.iitd.ac.in, so there is no encryption of the content and it is easily visible in wireshark

2 Q2

2.1 subpart a

Yes,I was able to see the different content objects in the browser, which I was earlier not able to see through Wireshark for www.indianexpress.com

2.2 subpart b

Number of content objects downloaded (till the load time) = 361
They are many of them from amazon web services, doubleclick.net, www.amazon.com, www.api.google.com, google ads services

The purpose of these objects are : Google API : fonts DoubleClick : advertisements AWS : web services Google Ads : advertisements

2.3 subpart c

Large object : mungerviolence.jpg
size = 31.4 kilo bytes Queued at : 116.91 ms
Started at : 235.64 ms

In resource scheduling,
queueing took 118.73 ms

In Connection Start,
stalled had duration 87.45 ms

In Request/Response,
Request sent took 23.61 ms
Waiting (TTFB) took 2.01 ms
Content Download took 16.51 ms

Total = 238.31 ms

Average throughput = 4823348.69 bytes/second = 1.8134 MBps

2.4 subpart d

Total amount of content downloaded for www.indianexpress.com = 9.7 MB
Total amount of content downloaded for www.nytimes.com = 25.1 MB

Page Load time for www.indianexpress.com (approx 4s) was also less than www.nytimes.com (approx 15s)

There is more latency in case of www.nytimes.com because it takes more hops to reach a foreign host server compared to the host of www.indianexpress.com

Also, websites have to be created to be able to adapt on different web browsers at different locations across the globe. The amount of content downloaded for nytimes was more because the host server might have a higher bandwidth which enables sending more content but rendering of the website is also dependent on the browser and network from where we access it. So websites have to be created such that they are very adaptive and the related content (which might be hosted on different domains) can be easily downloaded at different locations.

2.5 subpart e

Yes, I agree that from a user-experience point of view, since web-pages are constituted of many small objects and which could be hosted on multiple domains, factors like the roundtrip delay and optimizations by the browser to pipeline downloads of multiple objects, are more important than the network throughput that is obtained.

Throughput only indicates the efficiency of downloading the content, but pipelining downloads of multiple objects significantly affects the total time to load the page and navigate to hyperlinks. So, those factors are more important for user experience.

2.6 subpart f

I experimented with different custom networks.
The screenshot of Regular 2G is shown below :

Chrome is able to emulate different networks because it puts in browser level delays to simulate the different networks. There are sometimes large content objects like high resolution images and videos which require computational power and memory for processing and display. So when many such objects are being received in parallel, it is possible that the device's computational power is than the power required. So this may affect user experience since objects are not rendered onto the webpage display at the same speed at which they are being received.

Other than just transmission/receipt of data, web browsers also have to render content, sometimes there may be problems related to some content not being supported by a particular browser.

2.7 subpart g

There are requests going to ad.doubleclick.net and analytics.google.com

The third party domains accessed are :
https://googleads.g.doubleclick.net/pagead/id
https://fonts.gstatic.com/s/opensans/v16/mem8YaGs126MiZpBA-UFVZ0b.woff2
https://connect.facebook.net/en.US/fbevents.js

The info is about location of user, number of times the user visits the site, type of device used, email address etc.
Images, password, are stored as cookies locally

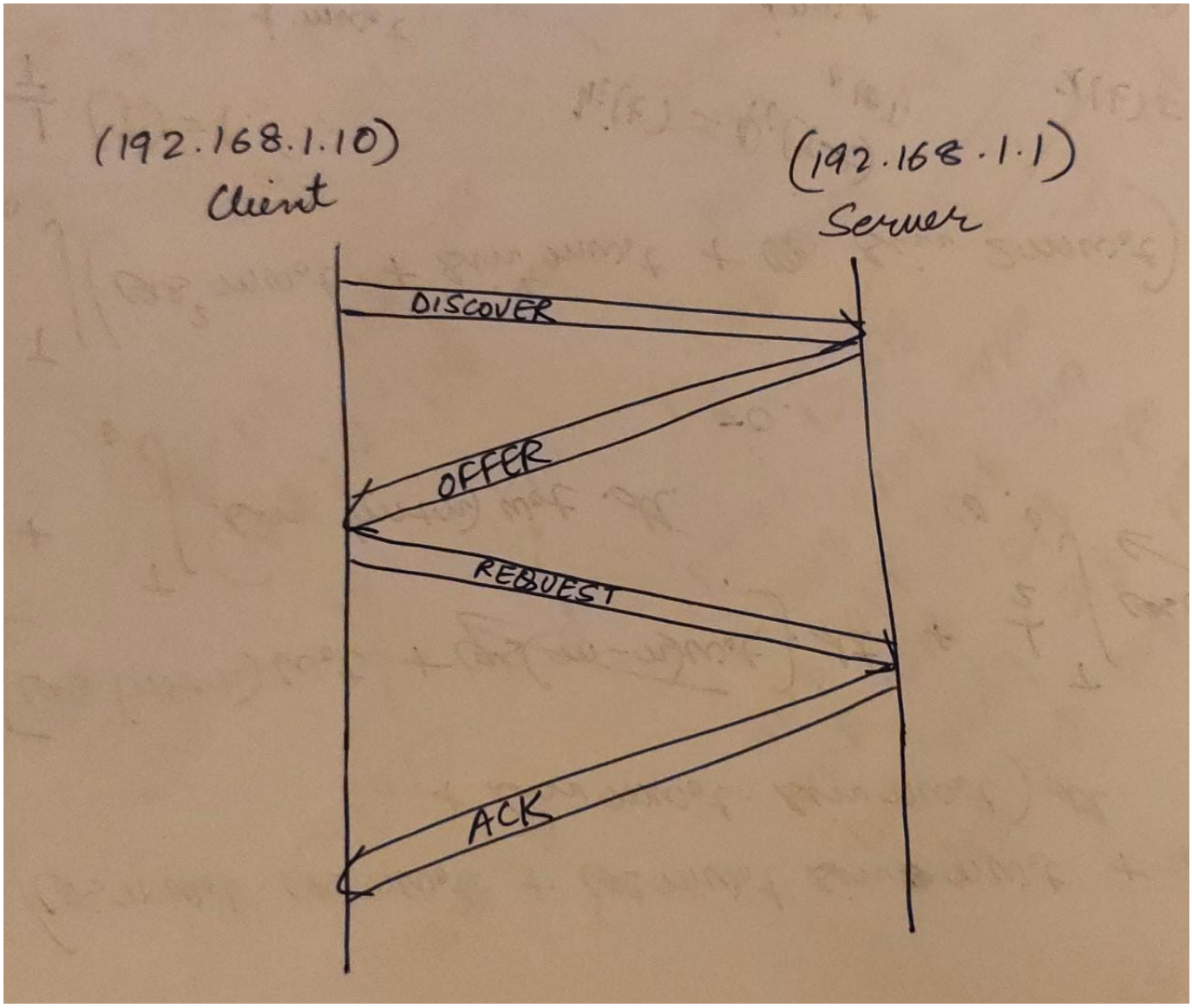
I don't have third party cookies blocked

3 Q3

3.1 subpart a

4 DHCP packets are seen :
discover, offer, request, ack
Protocol through which DHCP operates is User Datagram Protocol (UDP)

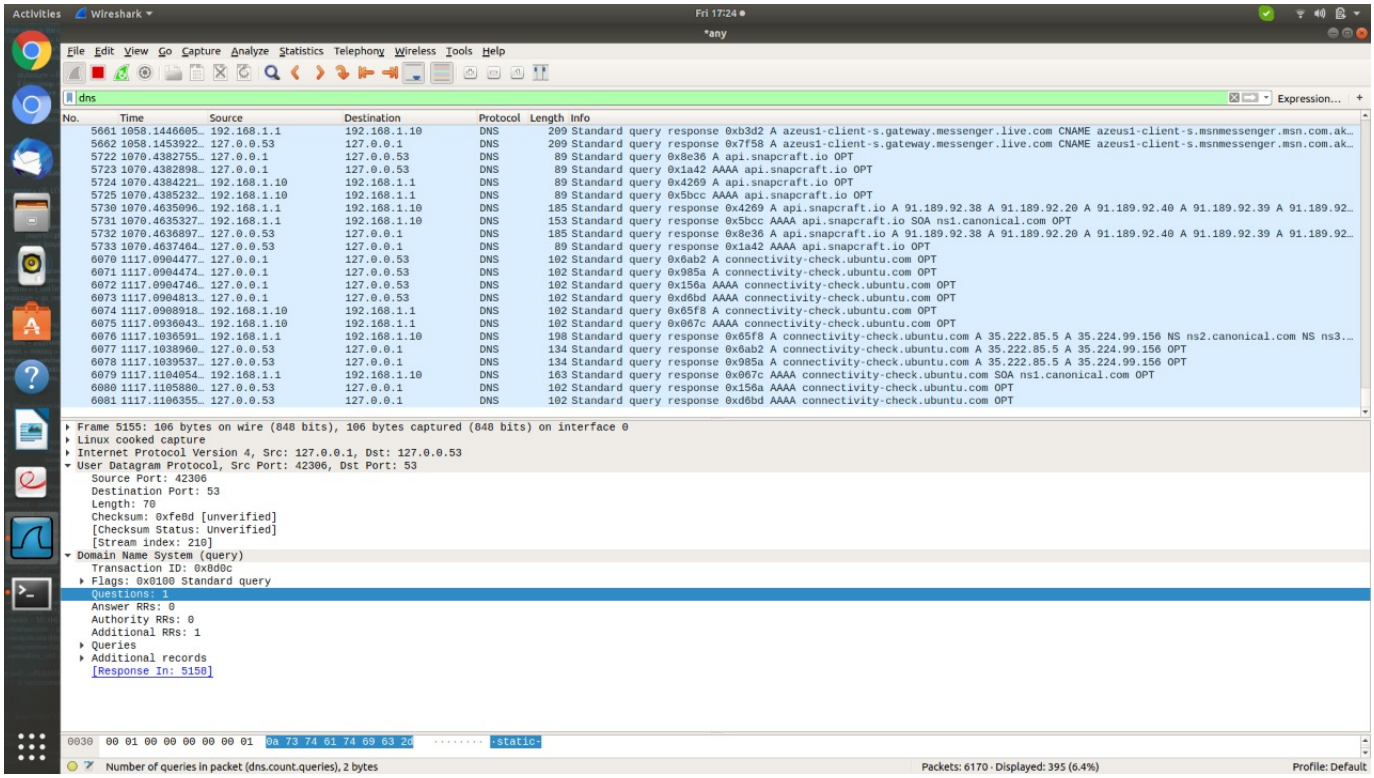
Transaction Diagram of DHCP messages :



Underlying Transport Layer Protocol is UDP and Bootstrap protocol

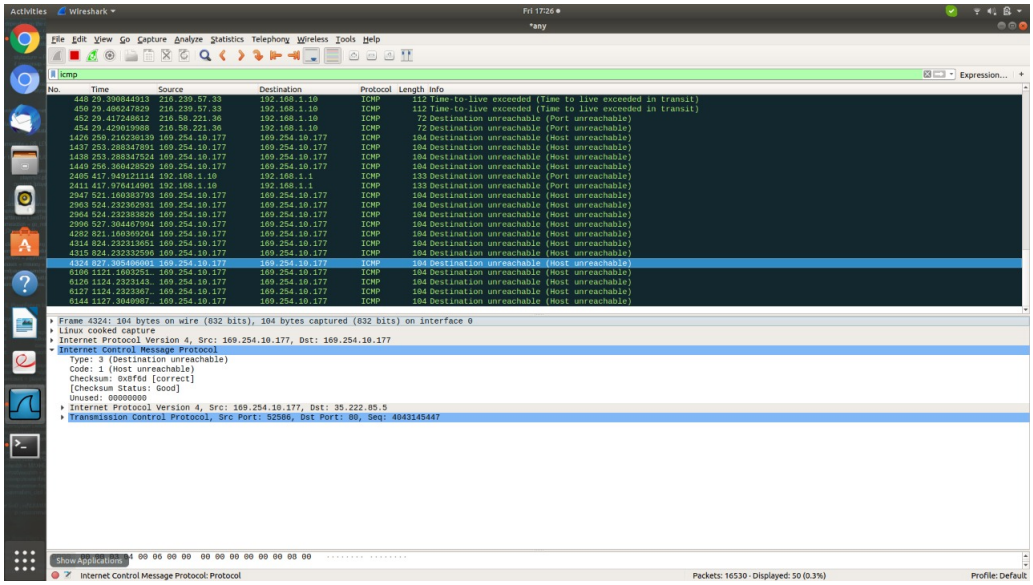
3.2 subpart b

While tracerouting to www.google.com, there are several DNS messages sent and received by my system, mostly about ip address check from domain name.



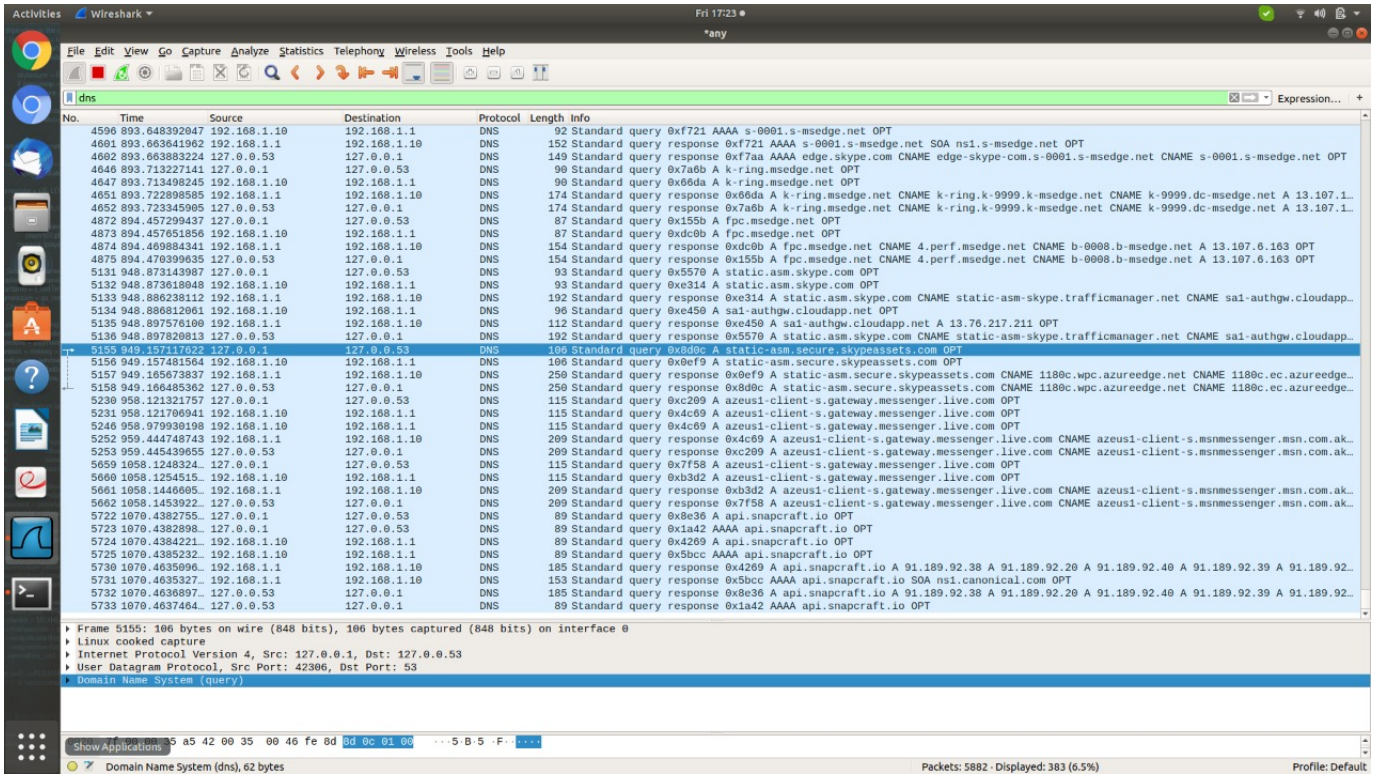
3.3 subpart c

For ICMP messages, mostly reachability is being checked by traceroute messages
The screenshot attached below :



3.4 subpart d

Protocols used for streaming data on : 1. Youtube : UDP 2. Zoom : UDP
So, mostly for data streaming, the underline protocol is UDP.


Activities
Wireshark
Fri 17:23
*any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
Expression...
No. Time Source Destination Protocol Length Info
4596 893.648392047 192.168.1.10 192.168.1.1 DNS 92 Standard query 0xf721 AAAA s-0001.s-msedge.net OPT
4601 893.663641962 192.168.1.1 192.168.1.10 DNS 152 Standard query response 0xf721 AAAA s-0001.s-msedge.net SOA ns1.s-msedge.net OPT
4602 893.663883224 127.0.0.53 127.0.0.1 DNS 149 Standard query response 0xf7aa AAAA edge.skype.com CNAME edge-skype-com.s-0001.s-msedge.net CNAME s-0001.s-msedge.net OPT
4646 893.713227141 127.0.0.1 127.0.0.53 DNS 90 Standard query 0x7a6b A k-ring.msedge.net OPT
4647 893.713498245 192.168.1.10 192.168.1.1 DNS 90 Standard query 0x66da A k-ring.msedge.net OPT
4651 893.722898585 192.168.1.1 192.168.1.10 DNS 174 Standard query response 0x66da A k-ring.msedge.net CNAME k-ring.k-9999.k-msedge.net CNAME k-9999.dc-msedge.net A 13.107.1…
4652 893.723345905 127.0.0.53 127.0.0.1 DNS 174 Standard query response 0x7a6b A k-ring.msedge.net CNAME k-ring.k-9999.k-msedge.net CNAME k-9999.dc-msedge.net A 13.107.1…
4872 894.457299437 127.0.0.1 127.0.0.53 DNS 87 Standard query 0x155b A fpc.msedge.net OPT
4873 894.457651856 192.168.1.10 192.168.1.1 DNS 87 Standard query 0xdc0b A fpc.msedge.net OPT
4874 894.469884341 192.168.1.1 192.168.1.10 DNS 154 Standard query response 0xdc0b A fpc.msedge.net CNAME 4.perf.msedge.net CNAME b-0008.b-msedge.net A 13.107.6.163 OPT
4875 894.470399635 127.0.0.53 127.0.0.1 DNS 154 Standard query response 0x155b A fpc.msedge.net CNAME 4.perf.msedge.net CNAME b-0008.b-msedge.net A 13.107.6.163 OPT
5131 948.873143987 127.0.0.1 127.0.0.53 DNS 93 Standard query 0x5570 A static.asm.skype.com OPT
5132 948.873618048 192.168.1.10 192.168.1.1 DNS 93 Standard query 0xe314 A static.asm.skype.com OPT
5133 948.886238112 192.168.1.1 192.168.1.10 DNS 192 Standard query response 0xe314 A static.asm.skype.com CNAME static-asm-skype.trafficmanager.net CNAME sa1-authgw.cloudapp…
5134 948.886812061 192.168.1.10 192.168.1.1 DNS 96 Standard query 0xe450 A sa1-authgw.cloudapp.net OPT
5135 948.897576100 192.168.1.1 192.168.1.10 DNS 112 Standard query response 0xe450 A sa1-authgw.cloudapp.net A 13.76.217.211 OPT
5136 948.897820813 127.0.0.53 127.0.0.1 DNS 192 Standard query response 0x5570 A static.asm.skype.com CNAME static-asm-skype.trafficmanager.net CNAME sa1-authgw.cloudapp…
5155 949.157117622 127.0.0.1 127.0.0.53 DNS 106 Standard query 0x8d0c A static-asm.secure.skypeassets.com OPT
5156 949.157481564 192.168.1.10 192.168.1.1 DNS 106 Standard query 0x0ef9 A static-asm.secure.skypeassets.com OPT
5157 949.165673837 192.168.1.1 192.168.1.10 DNS 250 Standard query response 0x0ef9 A static-asm.secure.skypeassets.com CNAME 1180c.wpc.azureedge.net CNAME 1180c.ec.azureedge…
5158 949.166485362 127.0.0.53 127.0.0.1 DNS 250 Standard query response 0x8d0c A static-asm.secure.skypeassets.com CNAME 1180c.wpc.azureedge.net CNAME 1180c.ec.azureedge…
5230 958.121321757 127.0.0.1 127.0.0.53 DNS 115 Standard query 0xc209 A azeus1-client-s.gateway.messenger.live.com OPT
5231 958.121706941 192.168.1.10 192.168.1.1 DNS 115 Standard query 0x4c69 A azeus1-client-s.gateway.messenger.live.com OPT
5246 958.979930198 192.168.1.10 192.168.1.1 DNS 115 Standard query 0x4c69 A azeus1-client-s.gateway.messenger.live.com OPT
5252 959.444748743 192.168.1.1 192.168.1.10 DNS 209 Standard query response 0x4c69 A azeus1-client-s.gateway.messenger.live.com CNAME azeus1-client-s.msnmessenger.msn.com.ak…
5253 959.445439655 127.0.0.53 127.0.0.1 DNS 209 Standard query response 0xc209 A azeus1-client-s.gateway.messenger.live.com CNAME azeus1-client-s.msnmessenger.msn.com.ak…
5659 1058.1248324… 127.0.0.1 127.0.0.53 DNS 115 Standard query 0x7f58 A azeus1-client-s.gateway.messenger.live.com OPT
5660 1058.1254515… 192.168.1.10 192.168.1.1 DNS 115 Standard query 0xb3d2 A azeus1-client-s.gateway.messenger.live.com OPT
5661 1058.1446605… 192.168.1.1 192.168.1.10 DNS 209 Standard query response 0xb3d2 A azeus1-client-s.gateway.messenger.live.com CNAME azeus1-client-s.msnmessenger.msn.com.ak…
5662 1058.1453922… 127.0.0.53 127.0.0.1 DNS 209 Standard query response 0x7f58 A azeus1-client-s.gateway.messenger.live.com CNAME azeus1-client-s.msnmessenger.msn.com.ak…
5722 1070.4382755… 127.0.0.1 127.0.0.53 DNS 89 Standard query 0x8e36 A api.snapcraft.io OPT
5723 1070.4382898… 127.0.0.1 127.0.0.53 DNS 89 Standard query 0x1a42 AAAA api.snapcraft.io OPT
5724 1070.4384221… 192.168.1.10 192.168.1.1 DNS 89 Standard query 0x4269 A api.snapcraft.io OPT
5725 1070.4385232… 192.168.1.10 192.168.1.1 DNS 89 Standard query 0x5bcc AAAA api.snapcraft.io OPT
5730 1070.4635096… 192.168.1.1 192.168.1.10 DNS 185 Standard query response 0x4269 A api.snapcraft.io A 91.189.92.38 A 91.189.92.20 A 91.189.92.40 A 91.189.92.39 A 91.189.92…
5731 1070.4635327… 192.168.1.1 192.168.1.10 DNS 153 Standard query response 0x5bcc AAAA api.snapcraft.io SOA ns1.canonical.com OPT
5732 1070.4636897… 127.0.0.53 127.0.0.1 DNS 185 Standard query response 0x8e36 A api.snapcraft.io A 91.189.92.38 A 91.189.92.20 A 91.189.92.40 A 91.189.92.39 A 91.189.92…
5733 1070.4637464… 127.0.0.53 127.0.0.1 DNS 89 Standard query response 0x1a42 AAAA api.snapcraft.io OPT
Frame 5155: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface 0
Linux cooked capture
Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.53
User Datagram Protocol, Src Port: 42306, Dst Port: 53
Domain Name System (query)
Show Applications
Domain Name System (dns), 62 bytes
Packets: 5882 · Displayed: 383 (6.5%)
Profile: Default