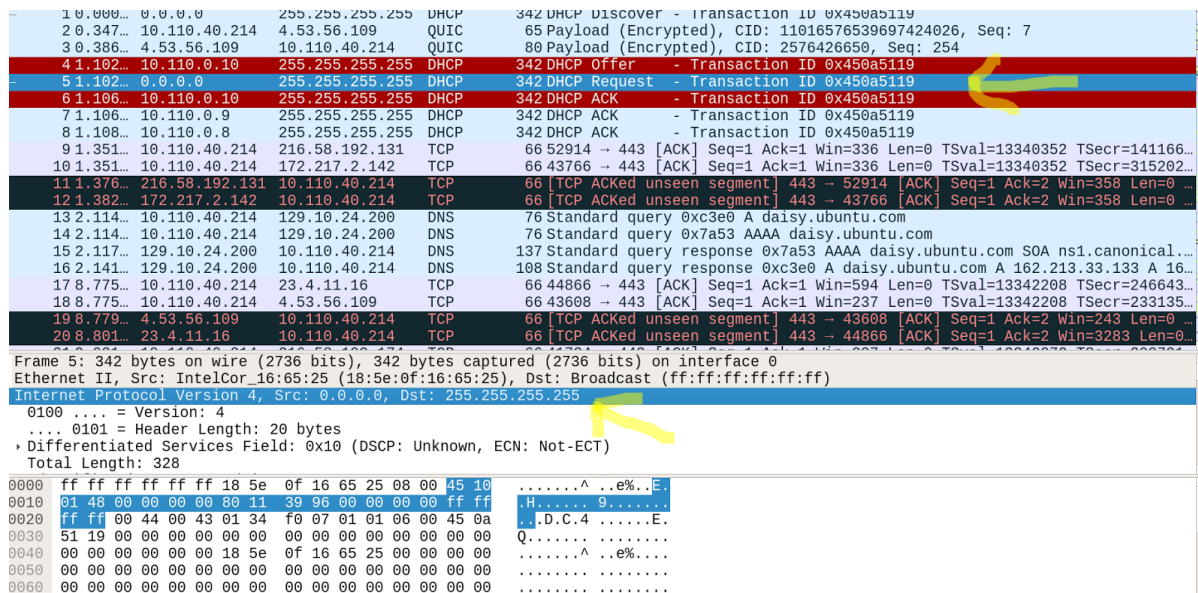


Name : Pushpinder Singh
NUID : 001906268
Class : CS6740

The first step after we ask the interface (wlp3s0 in my case) to connect/reconnect via dhcp is : dhclient wlp3s0. This gives result in wireshark something as follows :



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x450a5119
2	0.347	10.110.40.214	4.53.56.109	QUIC	65	Payload (Encrypted), CID: 11016576539697424026, Seq: 7
3	0.386	4.53.56.109	10.110.40.214	QUIC	80	Payload (Encrypted), CID: 2576426650, Seq: 254
4	1.102	10.110.0.10	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0x450a5119
5	1.102	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x450a5119
6	1.106	10.110.0.10	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0x450a5119
7	1.106	10.110.0.9	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0x450a5119
8	1.108	10.110.0.8	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0x450a5119
9	1.351	10.110.40.214	216.58.192.131	TCP	66	52914 → 443 [ACK] Seq=1 Ack=1 Win=336 Len=0 TSval=13340352 TSecr=141166...
10	1.351	10.110.40.214	172.217.2.142	TCP	66	43766 → 443 [ACK] Seq=1 Ack=1 Win=336 Len=0 TSval=13340352 TSecr=315202...
11	1.376	216.58.192.131	10.110.40.214	TCP	66	[TCP ACKed unseen segment] 443 → 52914 [ACK] Seq=1 Ack=2 Win=358 Len=0 ...
12	1.382	172.217.2.142	10.110.40.214	TCP	66	[TCP ACKed unseen segment] 443 → 43766 [ACK] Seq=1 Ack=2 Win=358 Len=0 ...
13	2.114	10.110.40.214	129.10.24.200	DNS	76	Standard query 0xc3e0 A daisy.ubuntu.com
14	2.114	10.110.40.214	129.10.24.200	DNS	76	Standard query 0x7a53 AAAA daisy.ubuntu.com
15	2.117	129.10.24.200	10.110.40.214	DNS	137	Standard query response 0x7a53 AAAA daisy.ubuntu.com SOA ns1.canonical...
16	2.141	129.10.24.200	10.110.40.214	DNS	108	Standard query response 0xc3e0 A daisy.ubuntu.com A 162.213.33.133 A 16...
17	8.775	10.110.40.214	23.4.11.16	TCP	66	44866 → 443 [ACK] Seq=1 Ack=1 Win=594 Len=0 TSval=13342208 TSecr=246643...
18	8.775	10.110.40.214	4.53.56.109	TCP	66	43608 → 443 [ACK] Seq=1 Ack=1 Win=237 Len=0 TSval=13342208 TSecr=233135...
19	8.779	4.53.56.109	10.110.40.214	TCP	66	[TCP ACKed unseen segment] 443 → 43608 [ACK] Seq=1 Ack=2 Win=243 Len=0 ...
20	8.801	23.4.11.16	10.110.40.214	TCP	66	[TCP ACKed unseen segment] 443 → 44866 [ACK] Seq=1 Ack=2 Win=3283 Len=0 ...

Frame 5: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
Ethernet II, Src: IntelCor_16:65:25 (18:5e:0f:16:65:25), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
0100 = Version: 4
.... 0101 = Header Length: 20 bytes
+ Differentiated Services Field: 0x10 (DSCP: Unknown, ECN: Not-ECT)
Total Length: 328

0000 ff ff ff ff ff ff 18 5e 0f 16 65 25 08 00 45 10^..e%..E.
0010 01 48 00 00 00 00 00 11 39 96 00 00 00 00 ff ff ..H.....9.....
0020 ff ff 00 44 00 43 01 34 f0 07 01 01 06 00 45 0a ...D.C.4.....E.
0030 51 19 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Q.....
0040 00 00 00 00 00 00 18 5e 0f 16 65 25 00 00 00 00^..e%.....
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

At first, dhcp uses default address and sends out message as broadcast and IP as 0.0.0.0, Dhcp then replies with an offer of an IP address which you can see above in red.

The Offer here is 10.110.40.214 which is indeed the ip address taken by my machine.

> ifconfig

```
wlp3s0  Link encap:Ethernet  HWaddr 18:5e:0f:16:65:25
        inet addr:10.110.40.214  Bcast:10.110.255.255  Mask:255.255.0.0
        inet6 addr: fe80::16e4:fa16:7480:7b1a/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:1637054 errors:0 dropped:0 overruns:0 frame:0
        TX packets:940280 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:1846534023 (1.8 GB)  TX bytes:323519734 (323.5 MB)
```

2) The second step i.e typing the Northeastern.edu in a web browser while capturing the packets in wireshark.

We notice a DNS query through default gateway to find the address of northeastern.edu

and the response thereafter usually contains the ip address of the desired name.

Here the Ip address is : 155.33.17.68.

3) Next comes the TCP protocol : It starts with the SYN/ACK packets between source and destination to initiate a session. We can confirm the SYN/ACK from flags in TCP packets
After successful acknowledgements,

No.	Time	Source	Destination	Protocol	Length	Info
44	13.13...	10.110.40.214	129.10.24.200	DNS	80	Standard query 0x82d5 A www.northeastern.edu
45	13.13...	10.110.40.214	129.10.24.200	DNS	77	Standard query 0x2407 A bcp.crwcdntrl.net
46	13.13...	10.110.40.214	129.10.24.200	DNS	78	Standard query 0x2b42 A cdn.inspectlet.com
47	13.13...	10.110.40.214	129.10.24.200	DNS	77	Standard query 0xef77 A track.hubspot.com
48	13.13...	10.110.40.214	216.58.192.142	QUIC	1392	Payload (Encrypted), CID: 4381629371485759687, Seq: 1
49	13.13...	129.10.24.200	10.110.40.214	DNS	96	Standard query response 0x82d5 A www.northeastern.edu A 155.33.17.68
50	13.13...	129.10.24.200	10.110.40.214	DNS	110	Standard query response 0x2b42 A cdn.inspectlet.com A 104.25.56.25 A 10...
51	13.13...	10.110.40.214	68.67.178.110	TCP	66	52302 → 443 [FIN, ACK] Seq=1 Ack=1 Win=349 Len=0 TSval=13343298 TSecr=1...
52	13.13...	10.110.40.214	54.90.148.22	TCP	66	47584 → 443 [FIN, ACK] Seq=1 Ack=1 Win=254 Len=0 TSval=13343298 TSecr=2...
53	13.13...	10.110.40.214	129.10.24.200	DNS	74	Standard query 0xe5df A fast.fonts.com
54	13.13...	10.110.40.214	129.10.24.200	DNS	78	Standard query 0xdf7e A graph.facebook.com
55	13.14...	10.110.40.214	129.10.24.200	DNS	83	Standard query 0x7ff1 A syndication.twitter.com
56	13.14...	10.110.40.214	155.33.17.68	TCP	74	58332 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=13343...
57	13.14...	10.110.40.214	155.33.17.68	TCP	74	58334 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=13343...
58	13.14...	10.110.40.214	155.33.17.68	TCP	74	58336 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=13343...
59	13.14...	10.110.40.214	155.33.17.68	TCP	74	58338 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=13343...
60	13.14...	10.110.40.214	155.33.17.68	TCP	74	58340 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=13343...
61	13.14...	10.110.40.214	155.33.17.68	TCP	74	58342 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=13343...
62	13.14...	10.110.40.214	155.33.17.68	TCP	74	46826 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1334...
63	13.14...	129.10.24.200	10.110.40.214	DNS	233	Standard query response 0x2407 A bcp.crwcdntrl.net CNAME g.crwcdntrl.ne...

• Frame 49: 96 bytes on wire (768 bits), 96 bytes captured (768 bits) on interface 0
• Ethernet II, Src: JuniperN_02:17:f0 (00:21:59:02:17:f0), Dst: IntelCor_16:65:25 (18:5e:0f:16:65:25)
• Internet Protocol Version 4, Src: 129.10.24.200, Dst: 10.110.40.214
• User Datagram Protocol, Src Port: 53 (53), Dst Port: 10099 (10099)
Source Port: 53
Destination Port: 10099
Length: 62

```
0000 18 5e 0f 16 65 25 00 21 59 02 17 f0 08 00 45 00  .^..e.! Y....E.
0010 00 52 30 fc 00 00 3f 11 7d 89 81 0a 18 c8 0a 6e  .R0...? }.....
0020 28 d6 00 35 27 73 00 3e a1 a1 82 d5 85 80 00 01  (.5's.> .....
0030 00 01 00 00 00 00 03 77 77 77 0c 6e 6f 72 74 68  ....w ww.north
0040 65 61 73 74 65 72 6e 03 65 64 75 00 00 01 00 01  eastern. edu....
0050 c0 0c 00 01 00 01 00 00 02 58 00 04 9b 21 11 44  ....X...!D
```

The web browser make an HTTP GET request via TCP from port 80 to neu.edu

1023	11.26...	155.33.17.68	10.110.40.214	TCP	74	80 → 59232 [SYN, ACK] Seq=0 Ack=1 Win=4158 Len=0 MSS=1386 TSval=1484632...
1024	11.26...	10.110.40.214	155.33.17.68	TCP	66	59232 → 80 [ACK] Seq=1 Ack=1 Win=29200 Len=0 TSval=14090059 TSecr=14846...
1025	11.26...	10.110.40.214	155.33.17.68	HTTP	381	GET / HTTP/1.1
1026	11.26...	155.33.17.68	10.110.40.214	TCP	66	80 → 59232 [ACK] Seq=1 Ack=316 Win=4473 Len=0 TSval=1484632543 TSecr=14...
1027	11.26...	155.33.17.68	10.110.40.214	HTTP	643	HTTP/1.1 301 Moved Permanently (text/html)
1028	11.26...	10.110.40.214	155.33.17.68	TCP	66	59232 → 80 [ACK] Seq=316 Ack=578 Win=30004 Len=0 TSval=14090060 TSecr=1...
1034	11.31...	10.110.40.214	155.33.17.68	TCP	74	59234 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=14090...
1035	11.32...	155.33.17.68	10.110.40.214	TCP	74	80 → 59234 [SYN, ACK] Seq=0 Ack=1 Win=4158 Len=0 MSS=1386 TSval=1484632...
1036	11.32...	10.110.40.214	155.33.17.68	TCP	66	59234 → 80 [ACK] Seq=1 Ack=1 Win=29200 Len=0 TSval=14090073 TSecr=14846...
1037	11.32...	10.110.40.214	155.33.17.68	HTTP	394	GET / HTTP/1.1
1038	11.32...	155.33.17.68	10.110.40.214	TCP	66	80 → 59234 [ACK] Seq=1 Ack=329 Win=4486 Len=0 TSval=1484632599 TSecr=14...
1039	11.33...	155.33.17.68	10.110.40.214	HTTP	1440	HTTP/1.1 200 OK (text/html)
1040	11.33...	10.110.40.214	155.33.17.68	TCP	66	59234 → 80 [ACK] Seq=329 Ack=1375 Win=31602 Len=0 TSval=14090075 TSecr=...

• Frame 1025: 381 bytes on wire (3048 bits), 381 bytes captured (3048 bits) on interface 0
• Ethernet II, Src: IntelCor_16:65:25 (18:5e:0f:16:65:25), Dst: IETF-VRRP-VRID_01 (00:00:5e:00:01:01)
• Internet Protocol Version 4, Src: 10.110.40.214, Dst: 155.33.17.68
• Transmission Control Protocol, Src Port: 59232 (59232), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 315
Source Port: 59232
Destination Port: 80
[Stream index: 28]

```
0000 00 00 5e 00 01 01 18 5e 0f 16 65 25 08 00 45 00  ..^...^ ..e..E.
0010 01 6f c5 b8 40 00 00 94 27 0a 6e 28 d6 9b 21  .o.@.@. .'.n(!
0020 11 44 e7 60 00 50 ff 31 3a fd 74 8d 7b 68 80 18  .D.`P.1 :.t.{h..
0030 72 10 d3 31 00 00 01 01 08 0a 00 d6 ff 4b 58 7d  r..1.... ..KX}
0040 b1 db 47 45 54 20 2f 20 48 54 54 50 2f 31 2e 31  ..GET / HTTP/1.1
0050 0d 0a 48 6f 73 74 3a 20 6e 65 75 2e 65 64 75 0d  ..Host: neu.edu.
0060 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a  .User-Agent: Moz
```

At this time the data is exchanged. At the end of communication, the web browser finishes the session with FYN/ACK packets.

WHOIS Info for neu.edu

Server Name: NEU.EDU.VN
Registrar: GODADDY.COM, LLC
Whois Server: whois.godaddy.com
Referral URL: <http://www.godaddy.com>

Domain Name: NEU.EDU
Registrar: EDUCAUSE
Sponsoring Registrar IANA ID: 365
Whois Server: whois.educause.net
Referral URL: <http://www.educause.edu/edudomain>
Name Server: NB4276.NEU.EDU
Name Server: NB4277.NEU.EDU
Name Server: NS20.CUSTOMER.LEVEL3.NET
Name Server: NS29.CUSTOMER.LEVEL3.NET
Status: ok <https://icann.org/epp#ok>
Updated Date: 25-mar-2016
Creation Date: 24-mar-1993
Expiration Date: 24-mar-2017

INFO via Arin.neu

Network	
Net Range	129.10.0.0 - 129.10.255.255
CIDR	129.10.0.0/16
Name	NORTHEASTERN-NET
Handle	NET-129-10-0-0-1
Parent	NET129 (NET-129-0-0-0-0)
Net Type	Direct Assignment
Origin AS	
Organization	Northeastern University (NORTHE-7)
Registration Date	1988-04-18
Last Updated	2008-12-09
Comments	
RESTful Link	https://whois.arin.net/rest/net/NET-129-10-0-0-1
Function	Point of Contact
Tech	ZN42-ARIN (ZN42-ARIN)

Using dig @amber.ccs.neu.edu ccs.neu.edu any
To get any information the DNS server has on it :

```

- Desktop/net_sec
> dig @amber.ccs.neu.edu ccs.neu.edu any

;<<> DiG 9.10.3-P4-Ubuntu <<> @amber.ccs.neu.edu ccs.neu.edu any
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 57915
;; flags: qr aa rd; QUERY: 1, ANSWER: 12, AUTHORITY: 0, ADDITIONAL: 6
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
; ccs.neu.edu.                IN      ANY

;; ANSWER SECTION:
ccs.neu.edu.                3600    IN      TXT      "MS=2B470A3FCBC85CBA5A7CC56291B911753B0AFF6B"
ccs.neu.edu.                300     IN      SOA      amber.ccs.neu.edu. hostmaster.ccs.neu.edu. 2016091500 10000 1800 604800 300
ccs.neu.edu.                300     IN      NS       dns1.easydns.net.
ccs.neu.edu.                300     IN      NS       dns1.easydns.com.
ccs.neu.edu.                300     IN      NS       amber.ccs.neu.edu.
ccs.neu.edu.                300     IN      NS       alderaan.ccs.neu.edu.
ccs.neu.edu.                300     IN      NS       asgard.ccs.neu.edu.
ccs.neu.edu.                300     IN      NS       joppa.ccs.neu.edu.
ccs.neu.edu.                300     IN      NS       dns3.easydns.ca.
ccs.neu.edu.                300     IN      A        129.10.116.51
ccs.neu.edu.                300     IN      MX       10 amber.ccs.neu.edu.
ccs.neu.edu.                300     IN      MX       50 ansible-smtp2.ccs.neu.edu.

;; ADDITIONAL SECTION:
amber.ccs.neu.edu.          300     IN      A        129.10.116.51
joppa.ccs.neu.edu.          300     IN      A        129.10.116.53
alderaan.ccs.neu.edu.       300     IN      A        129.10.116.80
asgard.ccs.neu.edu.         300     IN      A        129.10.116.61
ansible-smtp2.ccs.neu.edu.  300     IN      A        129.10.116.75

;; Query time: 18 msec
;; SERVER: 129.10.116.51#53(129.10.116.51)
;; WHEN: Fri Sep 23 19:32:16 EDT 2016
;; MSG SIZE rcvd: 458

```