Lab 3

2 Networking

Manually configuring the IPs : **sudo ifconfig eth0 192.168.0.1 netmask 255.255.255.0**

- The interface that you want to change the IP for is eth0
- The IP you want to give the interface is 192.168.0.1
- The Subnet Mask you want to set for the interface is 255.255.255.0

Changing the Default Gateway of B : **sudo route add default gw 192.168.0.253 eth0**

Configuring NAT on A :
Allow IP forwarding : **echo 1 > /proc/sys/net/ipv4/ip_forward**

configure iptables to forward the packets from your internal network, on /dev/eth0, to your external network on /dev/wlan0 :

- **/sbin/iptables -t nat -A POSTROUTING -o wlan0 -j MASQUERADE**
- **/sbin/iptables -A FORWARD -i wlan0 -o eth0 -m state --state RELATED,ESTABLISHED -j ACCEPT**
- **/sbin/iptables -A FORWARD -i eth0 -o wlan0 -j ACCEPT**

Set the DNS server in B to the department DNS server - 10.6.0.11 : **Modify /etc/resolv.conf**

3 Network Forensics & Sleuthing

3.1

1. DNS Request and reply packets for www.cse.iitm.ac.in: What transport layer protocol does the DNS request use?
Ans : User Datagram Protocol (UDP)

2. ARP Request and response: What is the destination MAC address for ARP requests?
Ans :
Destination: D-LinkIn_9d:43:ba (e8:cc:18:9d:43:ba)

Source: LiteonTe_97:7b:ab (ac:e0:10:97:7b:ab)
Address Resolution Protocol (request)

3. ICMP Echo and Reply packets: What is the value present in the type field of the ICMP header in those packets? What is the size in bytes of the ICMP data field? What is the data being sent?
Ans :

Request

Type : 8 (Echo (ping) request)

Data : 48 bytes
48:0d:03:00:00:00:00:00:10:11:12:13:14:15:16:17:18:19:1a:1b:1c:1d:1e:1f:20:21:22:23:24:25:26:27:28:29:2a:2b:2c:2d:2e:2f:30:31:32:33:34:35:36:37

Reply

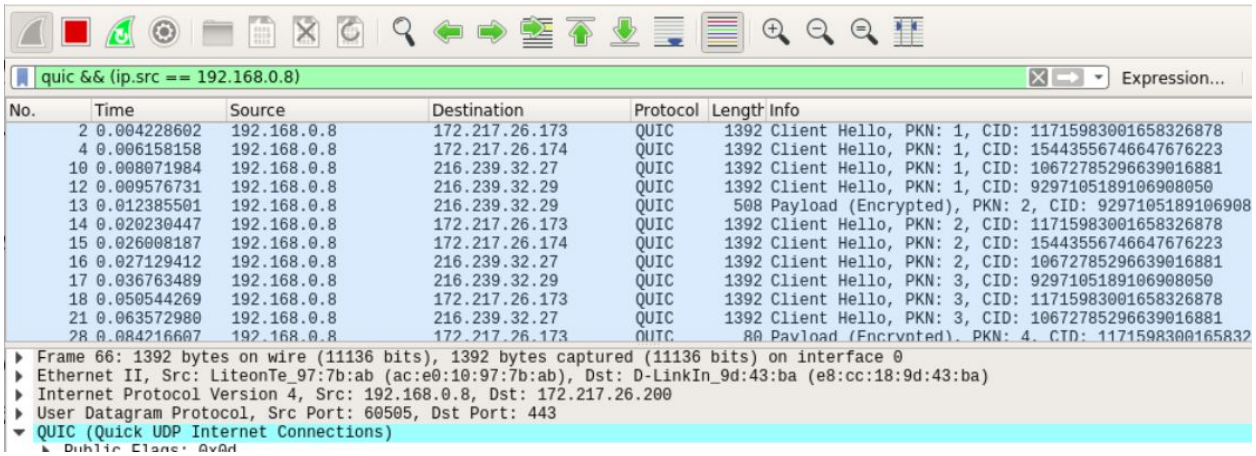
Type : 0 (Echo (ping) reply)

Data : 48 bytes
48:0d:03:00:00:00:00:00:10:11:12:13:14:15:16:17:18:19:1a:1b:1c:1d:1e:1f:20:21:22:23:24:25:26:27:28:29:2a:2b:2c:2d:2e:2f:30:31:32:33:34:35:36:37

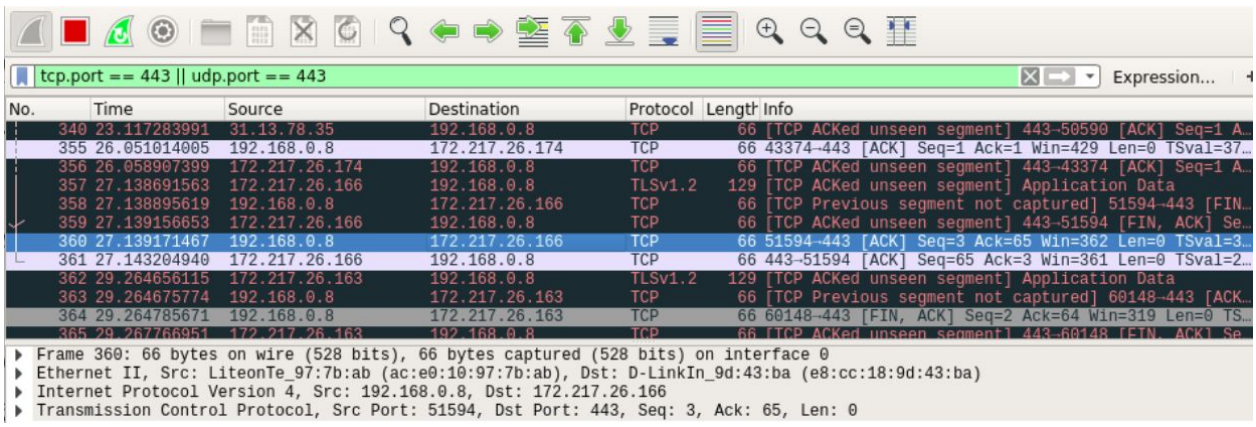
4. Open up your browser and visit http://www.google.com/loon/. Find the corresponding HTTP GET requests for images in the webpage in wireshark. What all information does the user-agent field in the HTTP header contain?
Ans :

5. Experiment with filters: Filters are extremely powerful and can simplify analysis if used intelligently. List any two filters your tried along with snapshots of the output.
Ans :

Filter : quic && (ip.src == 192.168.0.8)



Filter : tcp.port == 443 || udp.port == 443



3.2 The Treasure Hunt

1. What are the IP addresses and names of X and Y? What is the first and last message of the chat conversation?

Ans:

X : Bob 10.22.21.249

Y : Abhik 10.6.15.92

First message : Hi Abhik!

Last message : :)

```
Hi Abhik!
Hello Bob. What's up?
Nothing much. Doing some research. What about u?
Same here. I'm doing some TA work da. These juniors are N painful.
Hahahahaha, give them some hard assignments and pain them :P
Poor guys da. I'm not like Piney!
Or maybe I am! :P
Oh, and btw, I've been playing this new awesome game. It's brilliant!
Oh nice. What is it?
And I heard these juniors implemented an FTP Se
rver and client
I'm curious to try it out!
Hmmm, okay
I'm sending you a file
Okay
Got the file!
Oh! I see! So that's the game you were talking about!
Yep, it's a pretty awesome. Should play it soon.
:)
```

2. How many packets was the file that was transferred split into? Use the packet trace to reconstruct the entire file. What is the type of the file?

Ans:

Number of packets = 57332 to 57358 = 26 packets

Image File

3. What is the game that Bob was talking about?

Ans: Watch Dogs