Report - Assignment 3

Rachit Garg (CS14B050)

January 25, 2017

1 Exercise 1

My teammates in the lab were CS14B034 Balaji Naik, and CS14B035 Amol Dumrewal.

2 Exercise 2

2.1 Initiation

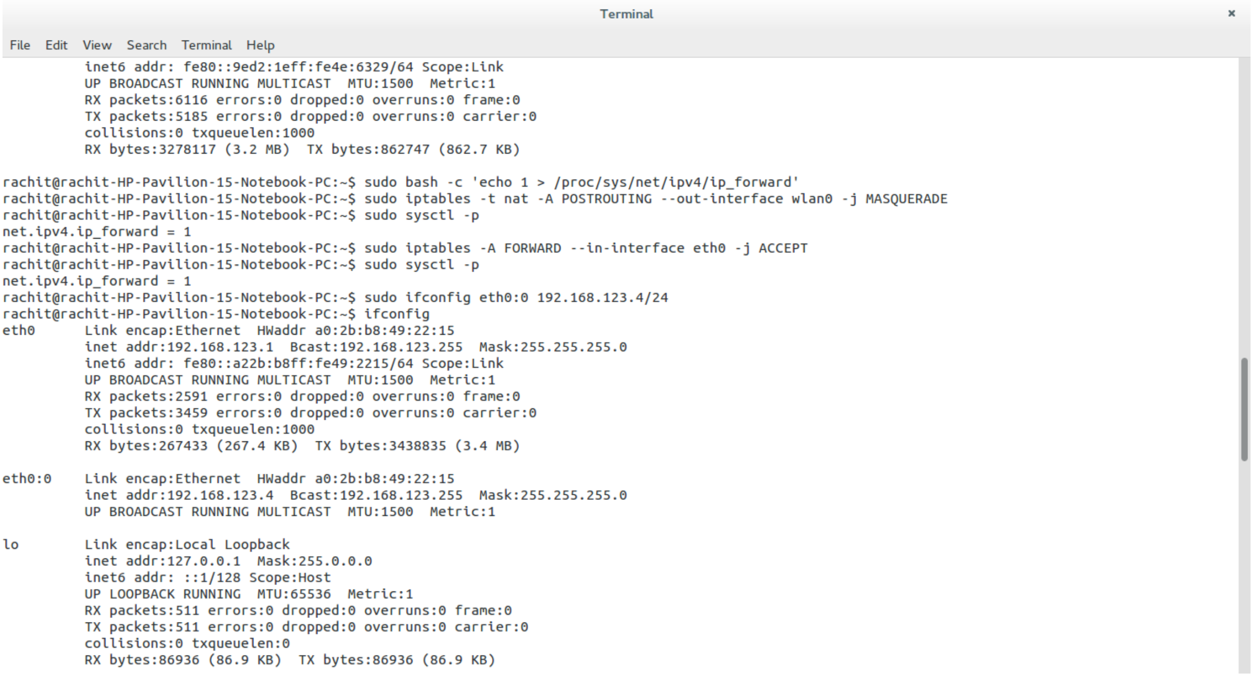
CS14B050's laptop was chosen as A and the one that makes an external connection and is connected with wifi. CS14B034's laptop was chosen as B and one that sets A's IP address in its gateway.

2.2 The task

1. We chose two ip addresses for A and B. A was chosen to be 192.168.123.1 ans B was chosen as 192.168.123.2.
   Command to change ip where x is the last digit is $ifconfig eth0 192.168.123.x netmask 255.255.255.0
2. Command at B's side is $route add default gw 192.168.123.1 eth0, where A's ip address is 192.168.123.1.
3. Switch on ip forwarding with the command $ sudo bash -c ’echo 1 > /proc/sys/net/ipv4/ip_forward’
   .
   This is an important step for transferring packets from the external network to the internal network.
4. Form a NAT interface at A, $sudo gedit $/etc/sysctl.conf$ and uncomment $net.ipv4.ip_forward =$ 1 in the file that is opened.
   Execute -
   - $sudo iptables -t nat -A POSTROUTING –out-interface wlan0 -j MASQUERADE
   - $sudo iptables -A FORWARD –in-interface eth0 -j ACCEPT
5. Modify $/etc/resolv.conf$ at B's side and change DNS to 10.6.0.11 (to resolve Domain names).

2.3 Home Task

1. Added an alias IP address of 192.168.123.4.
2. Changed B's gateway to 192.168.123.4 and connection showed a new eth0 ip in ifconfig. Figure 1



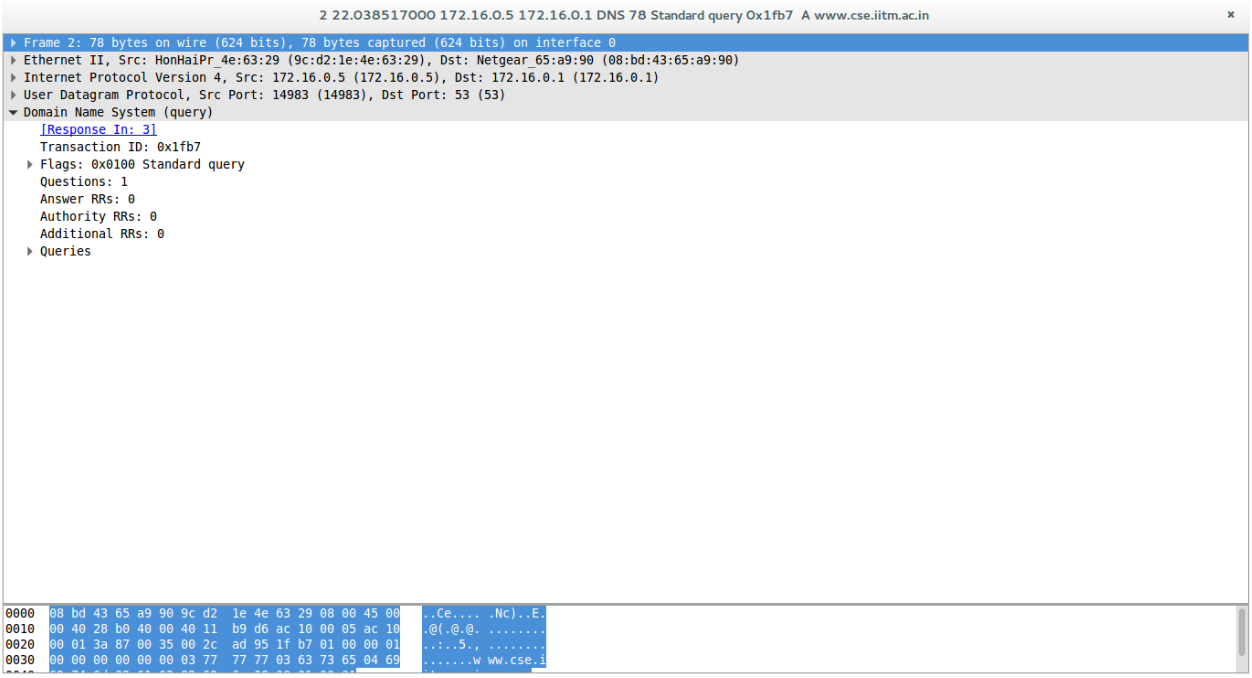
```
          inet6 addr: fe80::9ed2:1eff:fe4e:6329/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:6116 errors:0 dropped:0 overruns:0 frame:0
          TX packets:5185 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3278117 (3.2 MB)  TX bytes:862747 (862.7 KB)

rachit@rachit-HP-Pavilion-15-Notebook-PC:~$ sudo bash -c 'echo 1 > /proc/sys/net/ipv4/ip_forward'
rachit@rachit-HP-Pavilion-15-Notebook-PC:~$ sudo iptables -t nat -A POSTROUTING --out-interface wlan0 -j MASQUERADE
rachit@rachit-HP-Pavilion-15-Notebook-PC:~$ sudo sysctl -p
net.ipv4.ip_forward = 1
rachit@rachit-HP-Pavilion-15-Notebook-PC:~$ sudo iptables -A FORWARD --in-interface eth0 -j ACCEPT
rachit@rachit-HP-Pavilion-15-Notebook-PC:~$ sudo sysctl -p
net.ipv4.ip_forward = 1
rachit@rachit-HP-Pavilion-15-Notebook-PC:~$ sudo ifconfig eth0:0 192.168.123.4/24
rachit@rachit-HP-Pavilion-15-Notebook-PC:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr a0:2b:b8:49:22:15
          inet addr:192.168.123.1  Bcast:192.168.123.255  Mask:255.255.255.0
          inet6 addr: fe80::a22b:b8ff:fe49:2215/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2591 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3459 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:267433 (267.4 KB)  TX bytes:3438835 (3.4 MB)

eth0:0    Link encap:Ethernet  HWaddr a0:2b:b8:49:22:15
          inet addr:192.168.123.4  Bcast:192.168.123.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:511 errors:0 dropped:0 overruns:0 frame:0
          TX packets:511 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:86936 (86.9 KB)  TX bytes:86936 (86.9 KB)
```

Figure 1: The alias ip adress for eth0 connection is shown

3 Network forensics and sleuthing

3.1 Warming Up

1. Protocol used is udp(user datagram protocol). Filter used was udp. Figure 2



```
2 22.038517000 172.16.0.5 172.16.0.1 DNS 78 Standard query 0x1fb7  A www.cse.iitm.ac.in
```

```
▸ Frame 2: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface 0
▸ Ethernet II, Src: HonHaiPr_4e:63:29 (9c:d2:1e:4e:63:29), Dst: Netgear_65:a9:90 (08:bd:43:65:a9:90)
▸ Internet Protocol Version 4, Src: 172.16.0.5 (172.16.0.5), Dst: 172.16.0.1 (172.16.0.1)
▸ User Datagram Protocol, Src Port: 14983 (14983), Dst Port: 53 (53)
▾ Domain Name System (query)
    [Response In: 3]
    Transaction ID: 0x1fb7
  ▸ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▸ Queries
```

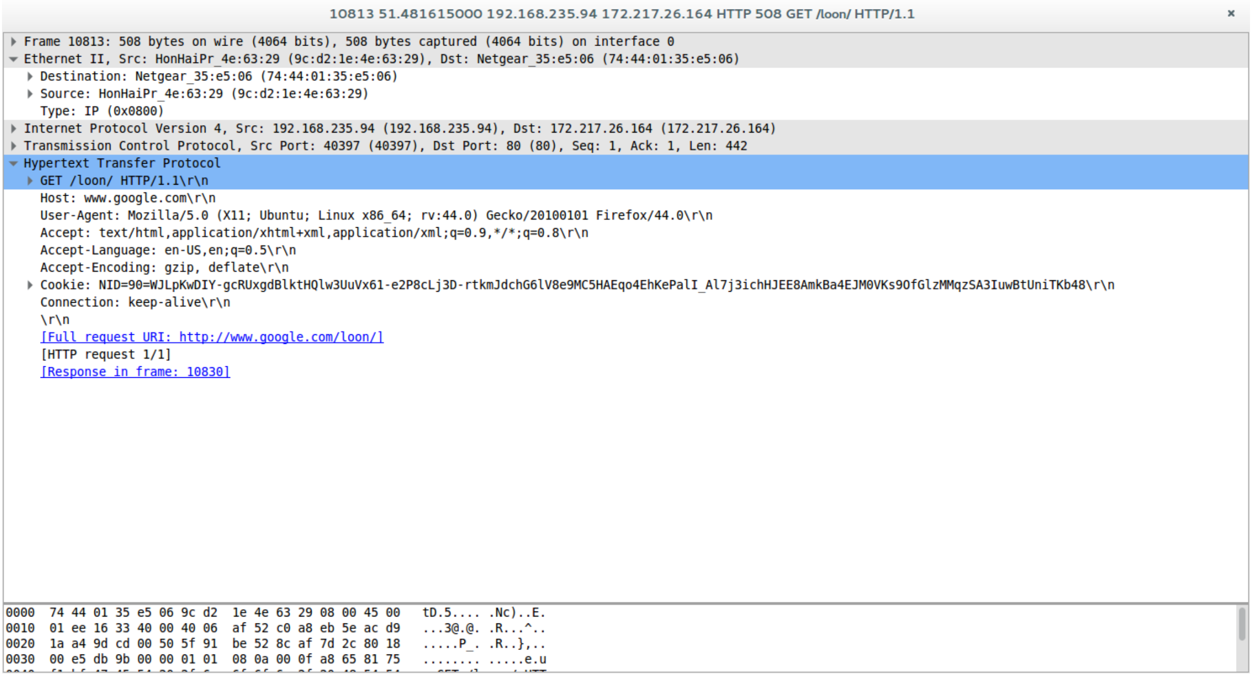
```
0000  08 bd 43 65 a9 90 9c d2  1e 4e 63 29 08 00 45 00   ..Ce.... .Nc)..E.
0010  00 40 28 b0 40 00 40 11  b9 d6 ac 10 00 05 ac 10   .@(.@.@. ........
0020  00 01 3a 87 00 35 00 2c  ad 95 1f b7 01 00 00 01   ..:..5., ........
0030  00 00 00 00 00 00 03 77  77 77 03 63 73 65 04 69   .......w ww.cse.i
```

Figure 2: The protocol name is shown with the dns request

2. MAC Address of target when requesting is $00:00:00\_00:00:00$, which is a gratitious arp request.
   MAC Address of source when reply is received is $3c:a8:2a:a9:dc:36$.

3. - In ICMP header file value present in type field of request is 8 and value in type field of reply is 0.
   - Size of data in bytes is 48.
   - Data being sent in hex is 8c 2b 07 00 00 00 00 00 10-37, in printable text is + !"#$%&'()*+,-./01234567.
   - Filter used here was ICMP.

4. HTTP protocol for the loon images were observed.
   User agent contained :- $''Mozilla/$5.0(X11: Ubuntu; Linux x86_64; rv:44.0)$Gecko/$20100101$Firefox/$44.0$\backslash r\backslash n$”
   It contained the web browser requesting the image and the system specifications such as 64 bit and operating system. Figure 3 Filter used was $http.request.method == ''GET$”

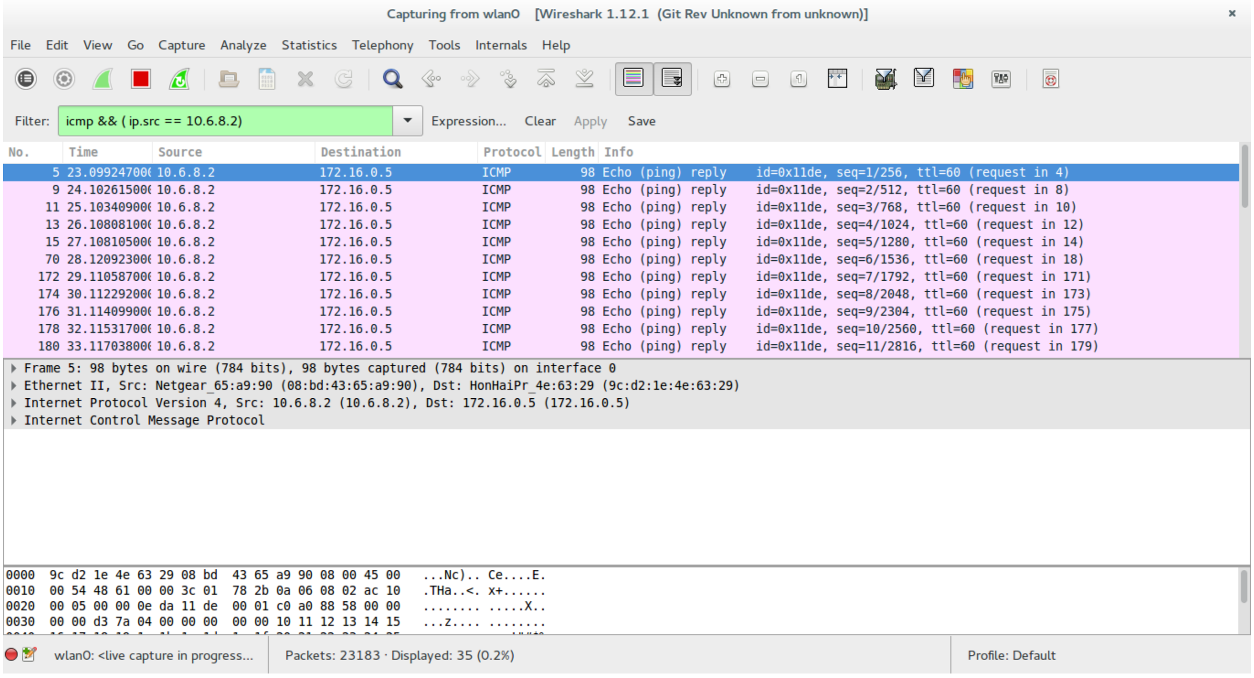


```
10813 51.481615000 192.168.235.94 172.217.26.164 HTTP 508 GET /loon/ HTTP/1.1
▸ Frame 10813: 508 bytes on wire (4064 bits), 508 bytes captured (4064 bits) on interface 0
▾ Ethernet II, Src: HonHaiPr_4e:63:29 (9c:d2:1e:4e:63:29), Dst: Netgear_35:e5:06 (74:44:01:35:e5:06)
  ▸ Destination: Netgear_35:e5:06 (74:44:01:35:e5:06)
  ▸ Source: HonHaiPr_4e:63:29 (9c:d2:1e:4e:63:29)
    Type: IP (0x0800)
▸ Internet Protocol Version 4, Src: 192.168.235.94 (192.168.235.94), Dst: 172.217.26.164 (172.217.26.164)
▸ Transmission Control Protocol, Src Port: 40397 (40397), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 442
▾ Hypertext Transfer Protocol
  ▸ GET /loon/ HTTP/1.1\r\n
    Host: www.google.com\r\n
    User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:44.0) Gecko/20100101 Firefox/44.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
  ▸ Cookie: NID=90=WJLpKwDIY-gcRUxgdBlktHQlw3UuVx61-e2P8cLj3D-rtkmJdchG6lV8e9MC5HAEqo4EhKePalI_Al7j3ichHJEE8AmkBa4EJM0VKs9OfGlzMMqzSA3IuwBtUniTKb48\r\n
    Connection: keep-alive\r\n
    \r\n
    [Full request URI: http://www.google.com/loon/]
    [HTTP request 1/1]
    [Response in frame: 10830]

0000  74 44 01 35 e5 06 9c d2  1e 4e 63 29 08 00 45 00   tD.5.... .Nc)..E.
0010  01 ee 16 33 40 00 40 06  af 52 c0 a8 eb 5e ac d9   ...3@.@. .R...^..
0020  1a a4 9d cd 00 50 5f 91  be 52 8c af 7d 2c 80 18   .....P_. .R..},..
0030  00 e5 db 9b 00 00 01 01  08 0a 00 0f a8 65 81 75   ........ .....e.u
```

Figure 3: The user agent in the http protocol with the loon images

5. Filters were experimented with in all four previous parts:-

    - For finding the reply scheme I used icmp && ip.src == 10.6.8.2 filter, the screenshot is shown below. Figure 4



Capturing from wlan0 [Wireshark 1.12.1 (Git Rev Unknown from unknown)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

Filter: icmp && (ip.src == 10.6.8.2)

```
No.   Time         Source      Destination   Protocol Length Info
    5 23.09924700( 10.6.8.2    172.16.0.5    ICMP       98 Echo (ping) reply   id=0x11de, seq=1/256, ttl=60 (request in 4)
    9 24.10261500( 10.6.8.2    172.16.0.5    ICMP       98 Echo (ping) reply   id=0x11de, seq=2/512, ttl=60 (request in 8)
   11 25.10340900( 10.6.8.2    172.16.0.5    ICMP       98 Echo (ping) reply   id=0x11de, seq=3/768, ttl=60 (request in 10)
   13 26.10808100( 10.6.8.2    172.16.0.5    ICMP       98 Echo (ping) reply   id=0x11de, seq=4/1024, ttl=60 (request in 12)
   15 27.10810500( 10.6.8.2    172.16.0.5    ICMP       98 Echo (ping) reply   id=0x11de, seq=5/1280, ttl=60 (request in 14)
   70 28.12092300( 10.6.8.2    172.16.0.5    ICMP       98 Echo (ping) reply   id=0x11de, seq=6/1536, ttl=60 (request in 18)
  172 29.11058700( 10.6.8.2    172.16.0.5    ICMP       98 Echo (ping) reply   id=0x11de, seq=7/1792, ttl=60 (request in 171)
  174 30.11229200( 10.6.8.2    172.16.0.5    ICMP       98 Echo (ping) reply   id=0x11de, seq=8/2048, ttl=60 (request in 173)
  176 31.11409900( 10.6.8.2    172.16.0.5    ICMP       98 Echo (ping) reply   id=0x11de, seq=9/2304, ttl=60 (request in 175)
  178 32.11531700( 10.6.8.2    172.16.0.5    ICMP       98 Echo (ping) reply   id=0x11de, seq=10/2560, ttl=60 (request in 177)
  180 33.11703800( 10.6.8.2    172.16.0.5    ICMP       98 Echo (ping) reply   id=0x11de, seq=11/2816, ttl=60 (request in 179)
```

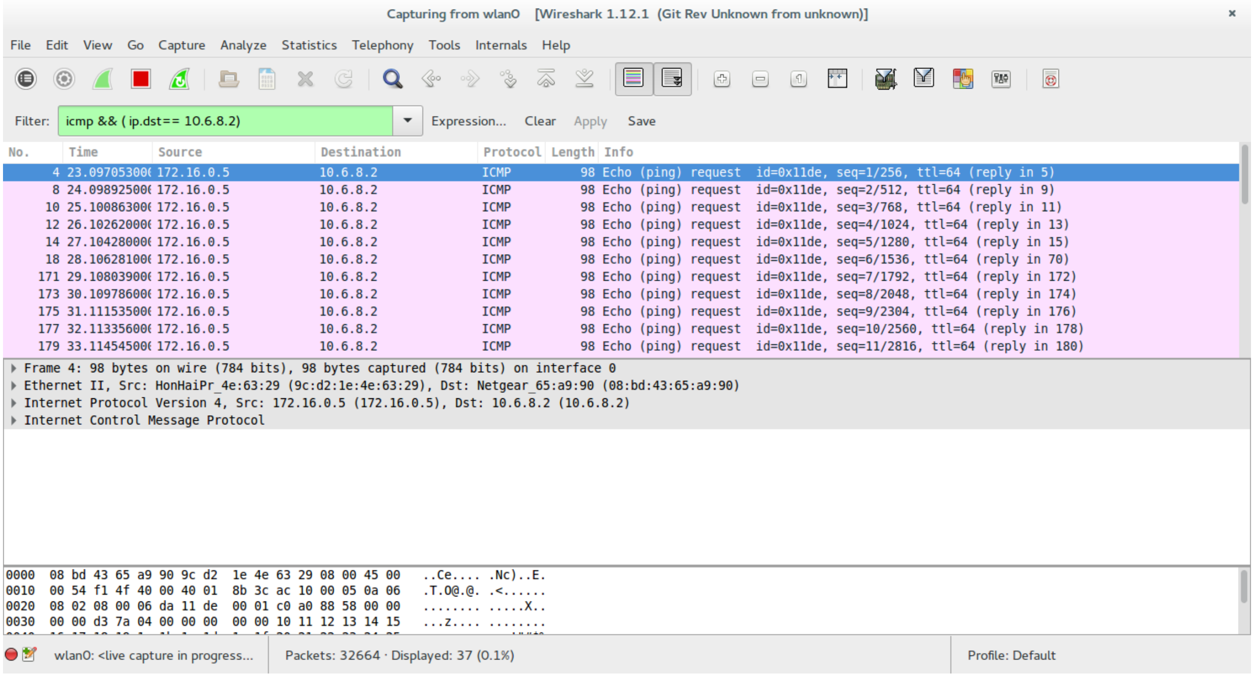
```
▸ Frame 5: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
▸ Ethernet II, Src: Netgear_65:a9:90 (08:bd:43:65:a9:90), Dst: HonHaiPr_4e:63:29 (9c:d2:1e:4e:63:29)
▸ Internet Protocol Version 4, Src: 10.6.8.2 (10.6.8.2), Dst: 172.16.0.5 (172.16.0.5)
▸ Internet Control Message Protocol
```

```
0000  9c d2 1e 4e 63 29 08 bd  43 65 a9 90 08 00 45 00   ...Nc).. Ce....E.
0010  00 54 48 61 00 00 3c 01  78 2b 0a 06 08 02 ac 10   .THa..<. x+......
0020  00 05 00 00 0e da 11 de  00 01 c0 a0 88 58 00 00   ........ .....X..
0030  00 00 d3 7a 04 00 00 00  00 00 10 11 12 13 14 15   ...z.... ........
```

wlan0: <live capture in progress... | Packets: 23183 · Displayed: 35 (0.2%) | Profile: Default

Figure 4: The filter is icmp && ip.src == 10.6.8.2

- And similarly for the reequest ip.dst == 10.6.8.2 was changed. Figure 5

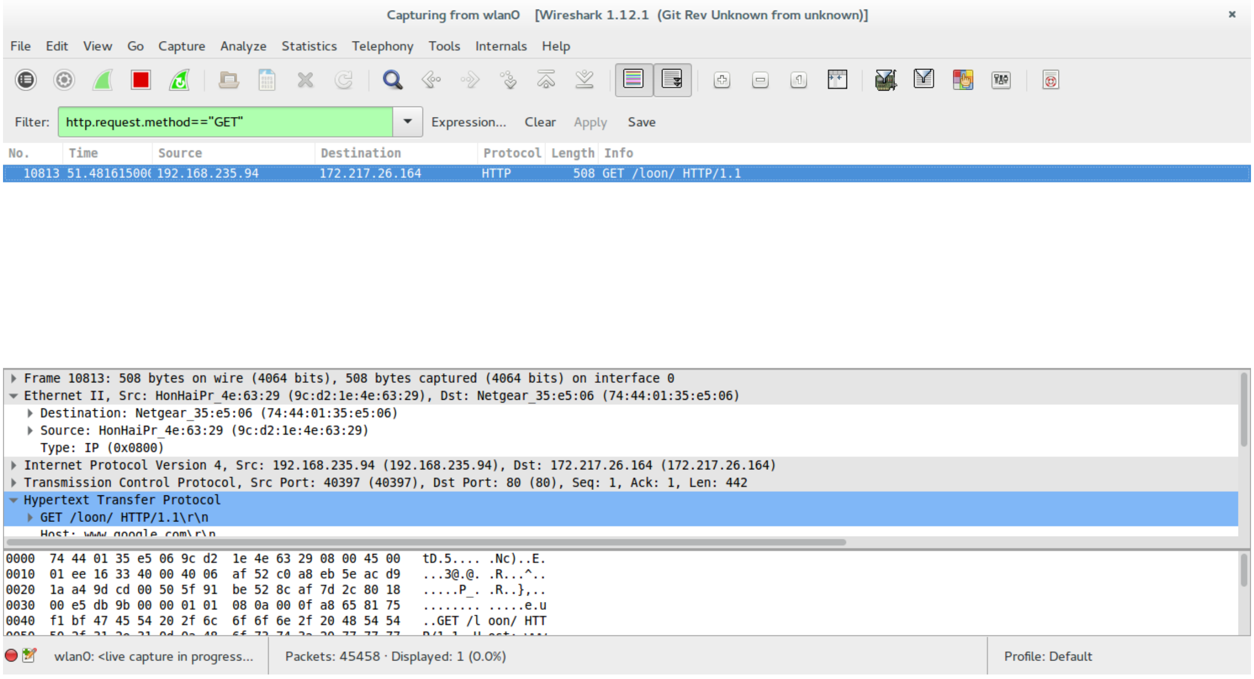


Capturing from wlan0 [Wireshark 1.12.1 (Git Rev Unknown from unknown)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: icmp && (ip.dst== 10.6.8.2)
Expression... Clear Apply Save
wlan0: <live capture in progress...
Packets: 32664 · Displayed: 37 (0.1%)
Profile: Default

```
No.    Time        Source         Destination     Protocol Length Info
     4 23.09705300( 172.16.0.5    10.6.8.2        ICMP        98 Echo (ping) request  id=0x11de, seq=1/256, ttl=64 (reply in 5)
     8 24.09892500( 172.16.0.5    10.6.8.2        ICMP        98 Echo (ping) request  id=0x11de, seq=2/512, ttl=64 (reply in 9)
    10 25.10086300( 172.16.0.5    10.6.8.2        ICMP        98 Echo (ping) request  id=0x11de, seq=3/768, ttl=64 (reply in 11)
    12 26.10262000( 172.16.0.5    10.6.8.2        ICMP        98 Echo (ping) request  id=0x11de, seq=4/1024, ttl=64 (reply in 13)
    14 27.10428000( 172.16.0.5    10.6.8.2        ICMP        98 Echo (ping) request  id=0x11de, seq=5/1280, ttl=64 (reply in 15)
    18 28.10628100( 172.16.0.5    10.6.8.2        ICMP        98 Echo (ping) request  id=0x11de, seq=6/1536, ttl=64 (reply in 70)
   171 29.10803900( 172.16.0.5    10.6.8.2        ICMP        98 Echo (ping) request  id=0x11de, seq=7/1792, ttl=64 (reply in 172)
   173 30.10978600( 172.16.0.5    10.6.8.2        ICMP        98 Echo (ping) request  id=0x11de, seq=8/2048, ttl=64 (reply in 174)
   175 31.11153500( 172.16.0.5    10.6.8.2        ICMP        98 Echo (ping) request  id=0x11de, seq=9/2304, ttl=64 (reply in 176)
   177 32.11335600( 172.16.0.5    10.6.8.2        ICMP        98 Echo (ping) request  id=0x11de, seq=10/2560, ttl=64 (reply in 178)
   179 33.11454500( 172.16.0.5    10.6.8.2        ICMP        98 Echo (ping) request  id=0x11de, seq=11/2816, ttl=64 (reply in 180)

▸ Frame 4: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
▸ Ethernet II, Src: HonHaiPr_4e:63:29 (9c:d2:1e:4e:63:29), Dst: Netgear_65:a9:90 (08:bd:43:65:a9:90)
▸ Internet Protocol Version 4, Src: 172.16.0.5 (172.16.0.5), Dst: 10.6.8.2 (10.6.8.2)
▸ Internet Control Message Protocol

0000  08 bd 43 65 a9 90 9c d2  1e 4e 63 29 08 00 45 00   ..Ce.... .Nc)..E.
0010  00 54 f1 4f 40 00 40 01  8b 3c ac 10 00 05 0a 06   .T.O@.@. .<......
0020  08 02 08 00 06 da 11 de  00 01 c0 a0 88 58 00 00   ........ .....X..
0030  00 00 d3 7a 04 00 00 00  00 00 10 11 12 13 14 15   ...z.... ........
```

Figure 5: The filter is icmp && ip.dst == 10.6.8.2

- http.request.method=="GET" filter was used in part 4. Figure 6



Filter: http.request.method=="GET"

No.	Time	Source	Destination	Protocol	Length	Info
10813	51.48161500(	192.168.235.94	172.217.26.164	HTTP	508	GET /loon/ HTTP/1.1

```
Frame 10813: 508 bytes on wire (4064 bits), 508 bytes captured (4064 bits) on interface 0
Ethernet II, Src: HonHaiPr_4e:63:29 (9c:d2:1e:4e:63:29), Dst: Netgear_35:e5:06 (74:44:01:35:e5:06)
  Destination: Netgear_35:e5:06 (74:44:01:35:e5:06)
  Source: HonHaiPr_4e:63:29 (9c:d2:1e:4e:63:29)
  Type: IP (0x0800)
Internet Protocol Version 4, Src: 192.168.235.94 (192.168.235.94), Dst: 172.217.26.164 (172.217.26.164)
Transmission Control Protocol, Src Port: 40397 (40397), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 442
Hypertext Transfer Protocol
  GET /loon/ HTTP/1.1\r\n
  Host: www.google.com\r\n
```

```
0000  74 44 01 35 e5 06 9c d2  1e 4e 63 29 08 00 45 00   tD.5.... .Nc)..E.
0010  01 ee 16 33 40 00 40 06  af 52 c0 a8 eb 5e ac d9   ...3@.@. .R...^..
0020  1a a4 9d cd 00 50 5f 91  be 52 8c af 7d 2c 80 18   .....P_. .R..},..
0030  00 e5 db 9b 00 00 01 01  08 0a 00 0f a8 65 81 75   ........ .....e.u
0040  f1 bf 47 45 54 20 2f 6c  6f 6f 6e 2f 20 48 54 54   ..GET /l oon/ HTT
0050  50 2f 31 2e 31 0d 0a 48  6f 73 74 3a 20 77 77 77   P/1.1..H ost: www
```

wlan0: <live capture in progress... | Packets: 45458 · Displayed: 1 (0.0%)

Figure 6: The filter is http.request.method=="GET"

3.2 Treasure Hunt

- To get the chat use the filter - ip.addr == 10.6.15.92 && udp.
- The chat is between Abhik and Bob. Abhik has ip 10.6.15.92 and Bob has ip 10.22.21.249.
- First message is - "Hi Abhik!.". Last message is ":).".
- They are discussing about TA work and a game. They transferred a file over a ftp server and client that their juniors developed.
- The type of file is jpeg.
- The file was split into 10 packets.
- The game that was being discussed was Watchdogs. Figure 7

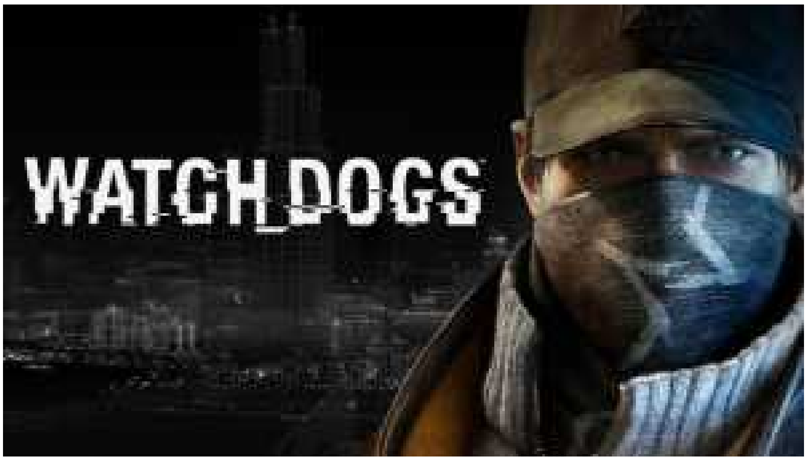


Figure 7: The image file of the game sent in the chat.