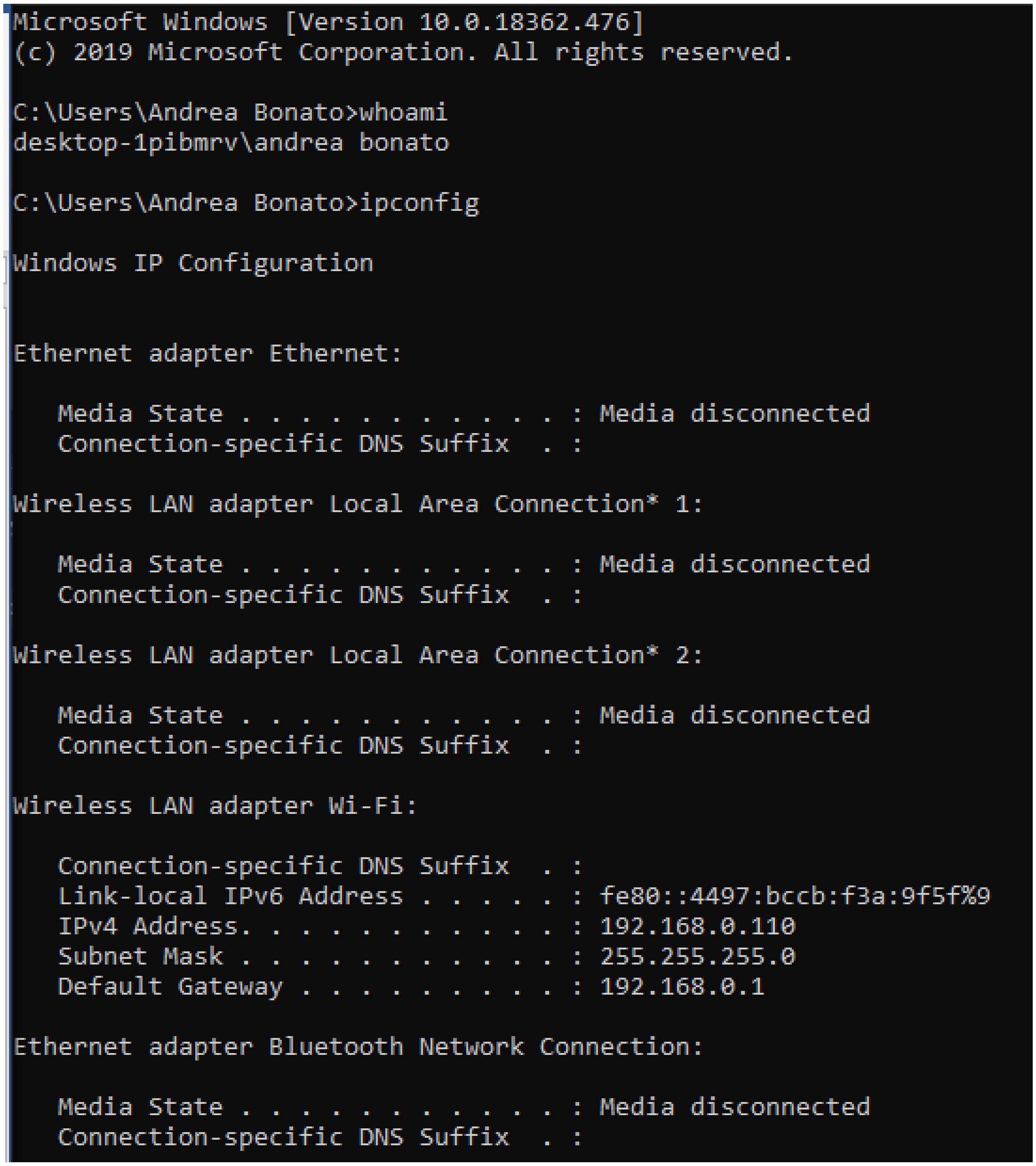
COMP-3670 Fall 2019 Assignment 3

Andrea Bonato

104760390



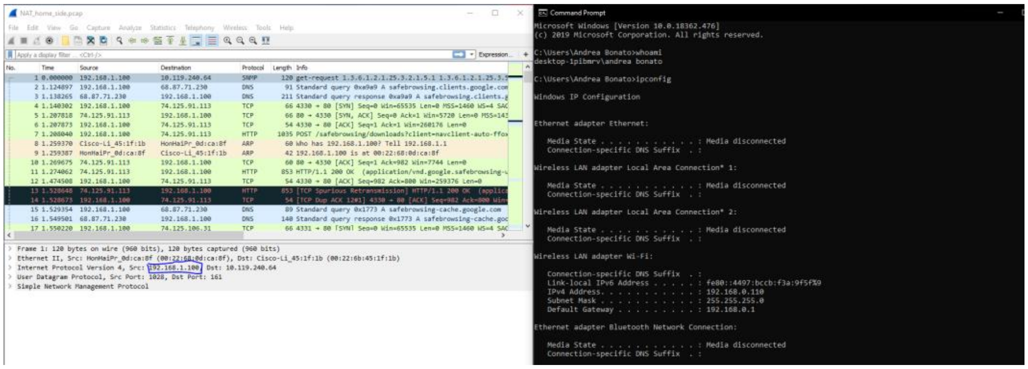
```
Microsoft Windows [Version 10.0.18362.476]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\Andrea Bonato>whoami
desktop-1pibmrv\andrea bonato

C:\Users\Andrea Bonato>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::4497:bccb:f3a:9f5f%9
   IPv4 Address. . . . . . . . . . . : 192.168.0.110
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
```

With this assignment, since I was unable to get a NAT device and unable to get two devices to continue with it, I did as the assignment prompted and used the traces that they provide.

Wireshark Lab: NAT

1. What is the IP address of the client?

The IP address of the client is 192.168.1.100 as shown in the screenshot below.



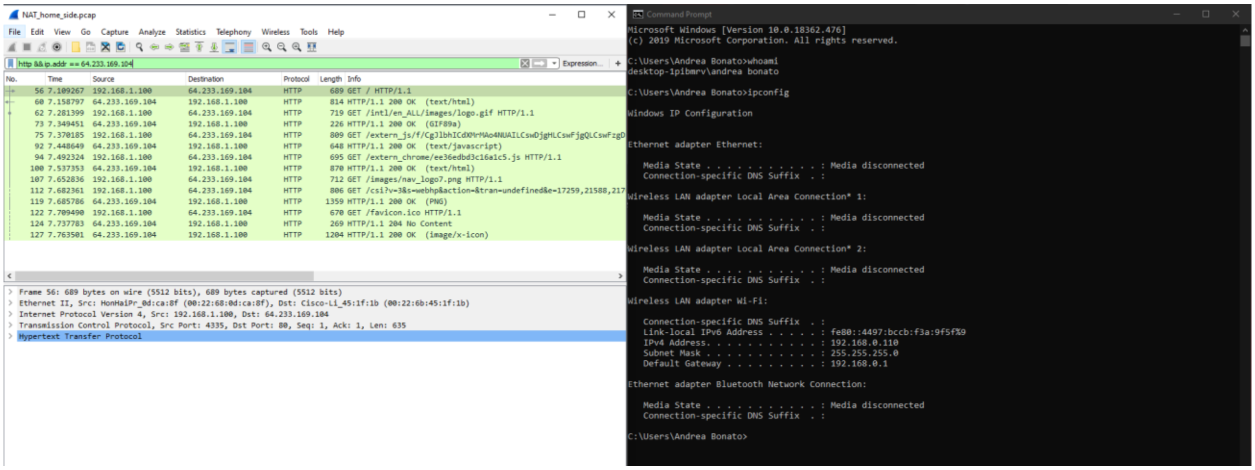
NAT_home_side.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...

```
No.  Time      Source             Destination        Protocol Length Info
   1 0.000000  192.168.1.100      10.119.240.64      SNMP     120 get-request 1.3.6.1.2.1.25.3.2.1.5.1 1.3.6.1.2.1.25.3.5
   2 1.124897  192.168.1.100      68.87.71.230       DNS       91 Standard query 0xa9a9 A safebrowsing.clients.google.com
   3 1.138265  68.87.71.230       192.168.1.100      DNS      211 Standard query response 0xa9a9 A safebrowsing.clients.g
   4 1.140302  192.168.1.100      74.125.91.113      TCP       66 4330 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=4 SAC
   5 1.207818  74.125.91.113      192.168.1.100      TCP       66 80 → 4330 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=143
   6 1.207873  192.168.1.100      74.125.91.113      TCP       54 4330 → 80 [ACK] Seq=1 Ack=1 Win=260176 Len=0
   7 1.208040  192.168.1.100      74.125.91.113      HTTP    1035 POST /safebrowsing/downloads?client=navclient-auto-ffox
   8 1.259370  Cisco-Li_45:1f:1b  HonHaiPr_0d:ca:8f  ARP       60 Who has 192.168.1.100? Tell 192.168.1.1
   9 1.259387  HonHaiPr_0d:ca:8f  Cisco-Li_45:1f:1b  ARP       42 192.168.1.100 is at 00:22:68:0d:ca:8f
  10 1.269675  74.125.91.113      192.168.1.100      TCP       60 80 → 4330 [ACK] Seq=1 Ack=982 Win=7744 Len=0
  11 1.274062  74.125.91.113      192.168.1.100      HTTP     853 HTTP/1.1 200 OK  (application/vnd.google.safebrowsing-u
  12 1.474508  192.168.1.100      74.125.91.113      TCP       54 4330 → 80 [ACK] Seq=982 Ack=800 Win=259376 Len=0
  13 1.528648  74.125.91.113      192.168.1.100      HTTP     853 [TCP Spurious Retransmission] HTTP/1.1 200 OK  (applica
  14 1.528673  192.168.1.100      74.125.91.113      TCP       54 [TCP Dup ACK 12#1] 4330 → 80 [ACK] Seq=982 Ack=800 Win=
  15 1.529354  192.168.1.100      68.87.71.230       DNS       89 Standard query 0x1773 A safebrowsing-cache.google.com
  16 1.549501  68.87.71.230       192.168.1.100      DNS      140 Standard query response 0x1773 A safebrowsing-cache.goo
  17 1.550220  192.168.1.100      74.125.106.31      TCP       66 4331 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=4 SAC

> Frame 1: 120 bytes on wire (960 bits), 120 bytes captured (960 bits)
> Ethernet II, Src: HonHaiPr_0d:ca:8f (00:22:68:0d:ca:8f), Dst: Cisco-Li_45:1f:1b (00:22:6b:45:1f:1b)
> Internet Protocol Version 4, Src: 192.168.1.100, Dst: 10.119.240.64
> User Datagram Protocol, Src Port: 1028, Dst Port: 161
> Simple Network Management Protocol
```

```
Microsoft Windows [Version 10.0.18362.476]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\Andrea Bonato>whoami
desktop-1pibmrv\andrea bonato

C:\Users\Andrea Bonato>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::4497:bccb:f3a:9f5f%9
   IPv4 Address. . . . . . . . . . . : 192.168.0.110
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
```

2. The client actually communicates with several different Google servers in order to implement "safe browsing." (See extra credit section at the end of this lab). The main Google server that will serve up the main Google web page has IP address 64.233.169.104. In order to display only those frames containing HTTP messages that are sent to/from this Google, server, enter the expression "http && ip.addr == 64.233.169.104" (without quotes) into the Filter: field in Wireshark .

The filter will be shown in the following screenshot:



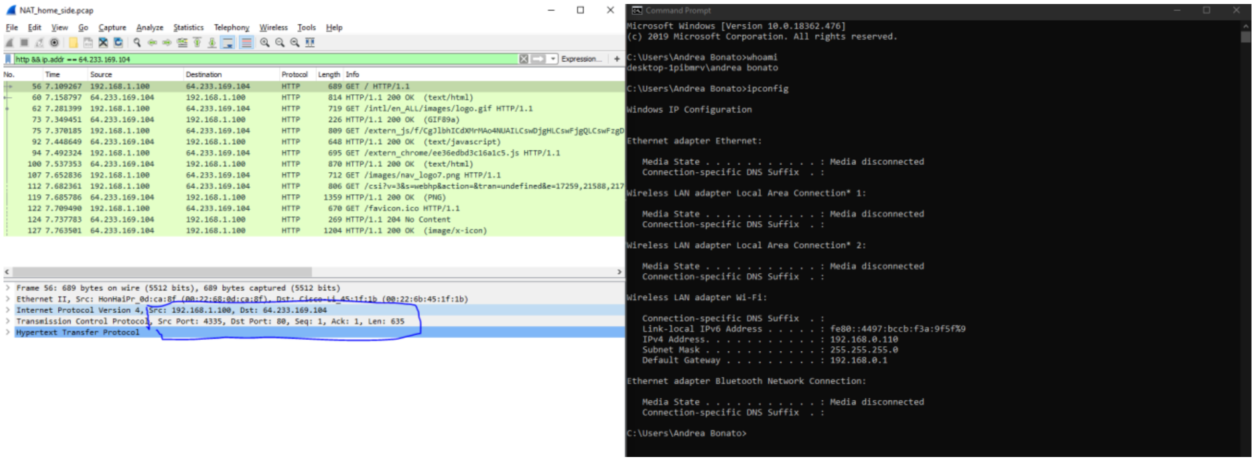
NAT_home_side.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...

```
http && ip.addr == 64.233.169.104

No.  Time      Source          Destination     Protocol Length Info
  56 7.109267  192.168.1.100   64.233.169.104  HTTP      689 GET / HTTP/1.1
  60 7.158797  64.233.169.104  192.168.1.100   HTTP      814 HTTP/1.1 200 OK  (text/html)
  62 7.281399  192.168.1.100   64.233.169.104  HTTP      719 GET /intl/en_ALL/images/logo.gif HTTP/1.1
  73 7.349451  64.233.169.104  192.168.1.100   HTTP      226 HTTP/1.1 200 OK  (GIF89a)
  75 7.370185  192.168.1.100   64.233.169.104  HTTP      809 GET /extern_js/f/CgJlbhICdXMrMAo4NUAILCswDjgHLCswFjgQLCswFzgD
  92 7.448649  64.233.169.104  192.168.1.100   HTTP      648 HTTP/1.1 200 OK  (text/javascript)
  94 7.492324  192.168.1.100   64.233.169.104  HTTP      695 GET /extern_chrome/ee36edbd3c16a1c5.js HTTP/1.1
 100 7.537353  64.233.169.104  192.168.1.100   HTTP      870 HTTP/1.1 200 OK  (text/html)
 107 7.652836  192.168.1.100   64.233.169.104  HTTP      712 GET /images/nav_logo7.png HTTP/1.1
 112 7.682361  192.168.1.100   64.233.169.104  HTTP      806 GET /csi?v=3&s=webhp&action=&tran=undefined&e=17259,21588,217
 119 7.685786  64.233.169.104  192.168.1.100   HTTP     1359 HTTP/1.1 200 OK  (PNG)
 122 7.709490  192.168.1.100   64.233.169.104  HTTP      670 GET /favicon.ico HTTP/1.1
 124 7.737783  64.233.169.104  192.168.1.100   HTTP      269 HTTP/1.1 204 No Content
 127 7.763501  64.233.169.104  192.168.1.100   HTTP     1204 HTTP/1.1 200 OK  (image/x-icon)

> Frame 56: 689 bytes on wire (5512 bits), 689 bytes captured (5512 bits)
> Ethernet II, Src: HonHaiPr_0d:ca:8f (00:22:68:0d:ca:8f), Dst: Cisco-Li_45:1f:1b (00:22:6b:45:1f:1b)
> Internet Protocol Version 4, Src: 192.168.1.100, Dst: 64.233.169.104
> Transmission Control Protocol, Src Port: 4335, Dst Port: 80, Seq: 1, Ack: 1, Len: 635
> Hypertext Transfer Protocol
```

```
Microsoft Windows [Version 10.0.18362.476]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\Andrea Bonato>whoami
desktop-1pibmrv\andrea bonato

C:\Users\Andrea Bonato>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::4497:bccb:f3a:9f5f%9
   IPv4 Address. . . . . . . . . . . : 192.168.0.110
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\Andrea Bonato>
```

3. Consider now the HTTP GET sent from the client to the Google server (whose IP address is IP address 64.233.169.104) at time 7.109267. What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP GET?

As shown in the screenshot below, the source IP is 192.168.1.100 and the destination IP is 64.233.169.104. The source port is 4335 and the destination port is 80.

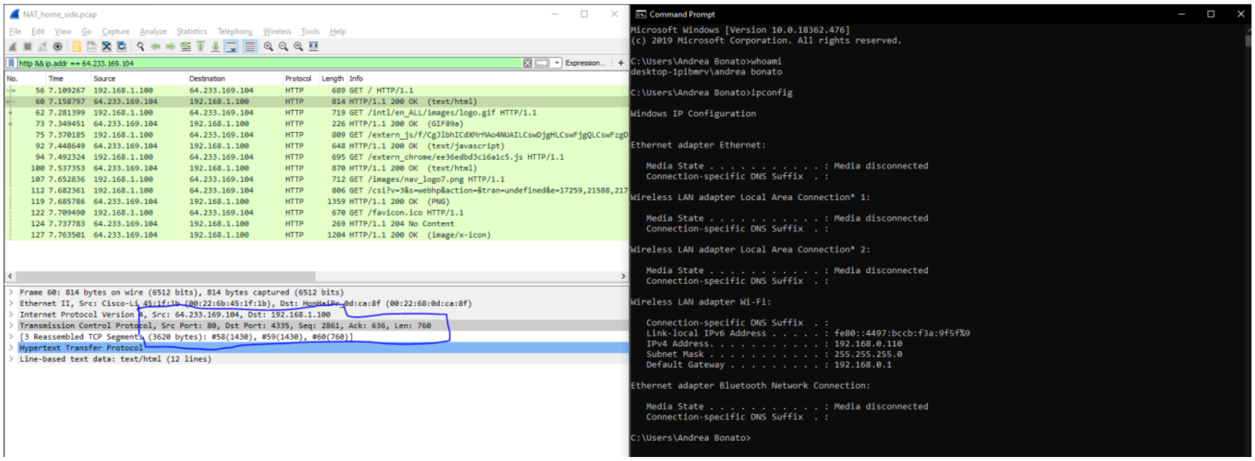

NAT_home_side.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
Command Prompt

```
http && ip.addr == 64.233.169.104

No.  Time      Source          Destination     Protocol Length Info
  56 7.109267  192.168.1.100   64.233.169.104  HTTP      689 GET / HTTP/1.1
  60 7.158797  64.233.169.104  192.168.1.100   HTTP      814 HTTP/1.1 200 OK  (text/html)
  62 7.281399  192.168.1.100   64.233.169.104  HTTP      719 GET /intl/en_ALL/images/logo.gif HTTP/1.1
  73 7.349451  64.233.169.104  192.168.1.100   HTTP      226 HTTP/1.1 200 OK  (GIF89a)
  75 7.370185  192.168.1.100   64.233.169.104  HTTP      809 GET /extern_js/f/CgJlbhICdXMrMAo4NUAILCswDjgHLCswFjgQLCswFzgD
  92 7.448649  64.233.169.104  192.168.1.100   HTTP      648 HTTP/1.1 200 OK  (text/javascript)
  94 7.492324  192.168.1.100   64.233.169.104  HTTP      695 GET /extern_chrome/ee36edbd3c16a1c5.js HTTP/1.1
 100 7.537353  64.233.169.104  192.168.1.100   HTTP      870 HTTP/1.1 200 OK  (text/html)
 107 7.652836  192.168.1.100   64.233.169.104  HTTP      712 GET /images/nav_logo7.png HTTP/1.1
 112 7.682361  192.168.1.100   64.233.169.104  HTTP      806 GET /csi?v=3&s=webhp&action=&tran=undefined&e=17259,21588,217
 119 7.685786  64.233.169.104  192.168.1.100   HTTP     1359 HTTP/1.1 200 OK  (PNG)
 122 7.709490  192.168.1.100   64.233.169.104  HTTP      670 GET /favicon.ico HTTP/1.1
 124 7.737783  64.233.169.104  192.168.1.100   HTTP      269 HTTP/1.1 204 No Content
 127 7.763501  64.233.169.104  192.168.1.100   HTTP     1204 HTTP/1.1 200 OK  (image/x-icon)

> Frame 56: 689 bytes on wire (5512 bits), 689 bytes captured (5512 bits)
> Ethernet II, Src: HonHaiPr_0d:ca:8f (00:22:68:0d:ca:8f), Dst: Cisco-Li_45:1f:1b (00:22:6b:45:1f:1b)
> Internet Protocol Version 4, Src: 192.168.1.100, Dst: 64.233.169.104
> Transmission Control Protocol, Src Port: 4335, Dst Port: 80, Seq: 1, Ack: 1, Len: 635
> Hypertext Transfer Protocol
```

```
Microsoft Windows [Version 10.0.18362.476]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\Andrea Bonato>whoami
desktop-1pibmrv\andrea bonato

C:\Users\Andrea Bonato>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::4497:bccb:f3a:9f5f%9
   IPv4 Address. . . . . . . . . . . : 192.168.0.110
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\Andrea Bonato>
```

4. At what time is the corresponding 200 OK HTTP message received from the Google server? What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP 200 OK message?

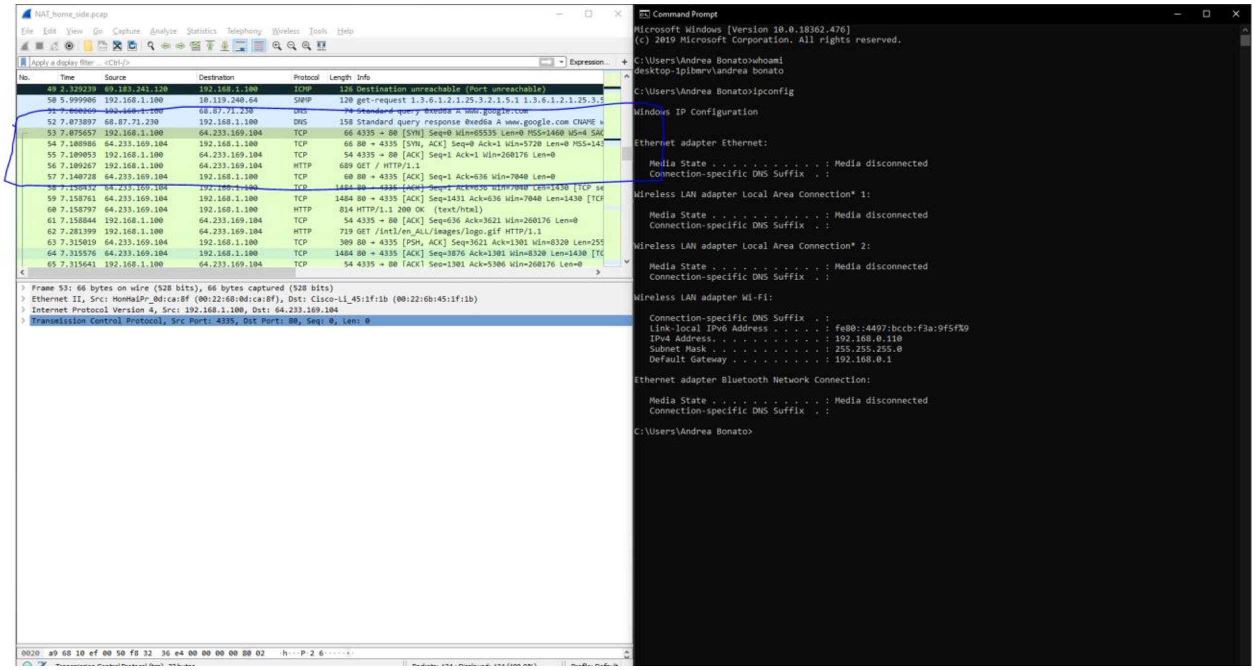
According to the screenshot below, the source IP address is 64.233.169.104 and the destination IP is 192.168.1.100. The source port is 80 and the destination port is 4335.


NAT_home_side.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
Command Prompt

```
http && ip.addr == 64.233.169.104

No.  Time      Source          Destination     Protocol Length Info
  56 7.109267  192.168.1.100   64.233.169.104  HTTP      689 GET / HTTP/1.1
  60 7.158797  64.233.169.104  192.168.1.100   HTTP      814 HTTP/1.1 200 OK  (text/html)
  62 7.281399  192.168.1.100   64.233.169.104  HTTP      719 GET /intl/en_ALL/images/logo.gif HTTP/1.1
  73 7.349451  64.233.169.104  192.168.1.100   HTTP      226 HTTP/1.1 200 OK  (GIF89a)
  75 7.370185  192.168.1.100   64.233.169.104  HTTP      809 GET /extern_js/f/CgJlbhICdXMrMAo4NUAILCswDjgHLCswFjgQLCswFzgD
  92 7.448649  64.233.169.104  192.168.1.100   HTTP      648 HTTP/1.1 200 OK  (text/javascript)
  94 7.492324  192.168.1.100   64.233.169.104  HTTP      695 GET /extern_chrome/ee36edbd3c16a1c5.js HTTP/1.1
 100 7.537353  64.233.169.104  192.168.1.100   HTTP      870 HTTP/1.1 200 OK  (text/html)
 107 7.652836  192.168.1.100   64.233.169.104  HTTP      712 GET /images/nav_logo7.png HTTP/1.1
 112 7.682361  192.168.1.100   64.233.169.104  HTTP      806 GET /csi?v=3&s=webhp&action=&tran=undefined&e=17259,21588,217
 119 7.685786  64.233.169.104  192.168.1.100   HTTP     1359 HTTP/1.1 200 OK  (PNG)
 122 7.709490  192.168.1.100   64.233.169.104  HTTP      670 GET /favicon.ico HTTP/1.1
 124 7.737783  64.233.169.104  192.168.1.100   HTTP      269 HTTP/1.1 204 No Content
 127 7.763501  64.233.169.104  192.168.1.100   HTTP     1204 HTTP/1.1 200 OK  (image/x-icon)

> Frame 60: 814 bytes on wire (6512 bits), 814 bytes captured (6512 bits)
> Ethernet II, Src: Cisco-Li_45:1f:1b (00:22:6b:45:1f:1b), Dst: HonHaiPr_0d:ca:8f (00:22:68:0d:ca:8f)
> Internet Protocol Version 4, Src: 64.233.169.104, Dst: 192.168.1.100
> Transmission Control Protocol, Src Port: 80, Dst Port: 4335, Seq: 2861, Ack: 636, Len: 760
> [3 Reassembled TCP Segments (3620 bytes): #58(1430), #59(1430), #60(760)]
> Hypertext Transfer Protocol
> Line-based text data: text/html (12 lines)
```

```
Microsoft Windows [Version 10.0.18362.476]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\Andrea Bonato>whoami
desktop-1pibmrv\andrea bonato

C:\Users\Andrea Bonato>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::4497:bccb:f3a:9f5f%9
   IPv4 Address. . . . . . . . . . . : 192.168.0.110
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\Andrea Bonato>
```

5. Recall that before a GET command can be sent to an HTTP server, TCP must first set up a connection using the three-way SYN/ACK handshake. At what time is the client-to-server TCP SYN segment sent that sets up the connection used by the GET sent at time 7.109267? What are the source and destination IP addresses and source and destination ports for the TCP SYN segment? What are the source and destination IP addresses and source and destination ports of the ACK sent in response to the SYN. At what time is this ACK received at the client? (Note: to find these segments you will need to clear the Filter expression you entered above in step 2. If you enter the filter "tcp", only TCP segments will be displayed by Wireshark).


NAT_home_side.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
Command Prompt

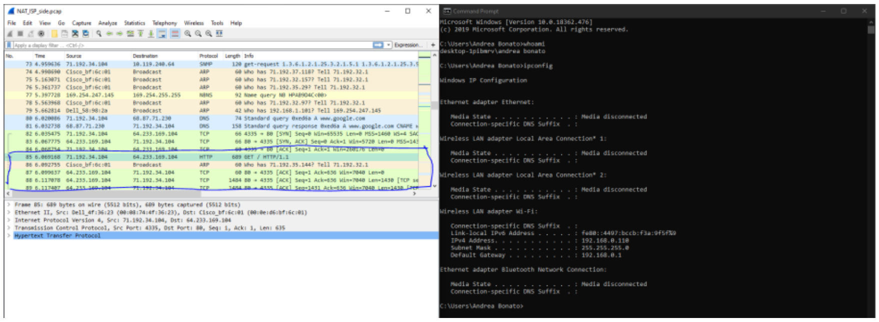
```
No.   Time      Source           Destination      Protocol Length Info
   49 2.329239  69.183.241.120   192.168.1.100    ICMP      126 Destination unreachable (Port unreachable)
   50 5.999906  192.168.1.100    10.119.240.64    SNMP      120 get-request 1.3.6.1.2.1.25.3.2.1.5.1 1.3.6.1.2.1.25.3.5
   51 7.060269  192.168.1.100    68.87.71.230     DNS        74 Standard query 0xed6a A www.google.com
   52 7.073897  68.87.71.230     192.168.1.100    DNS       158 Standard query response 0xed6a A www.google.com CNAME w
   53 7.075657  192.168.1.100    64.233.169.104   TCP        66 4335 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=4 SAC
   54 7.108986  64.233.169.104   192.168.1.100    TCP        66 80 → 4335 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=143
   55 7.109053  192.168.1.100    64.233.169.104   TCP        54 4335 → 80 [ACK] Seq=1 Ack=1 Win=260176 Len=0
   56 7.109267  192.168.1.100    64.233.169.104   HTTP      689 GET / HTTP/1.1
   57 7.140728  64.233.169.104   192.168.1.100    TCP        60 80 → 4335 [ACK] Seq=1 Ack=636 Win=7040 Len=0
   58 7.158432  64.233.169.104   192.168.1.100    TCP      1484 80 → 4335 [ACK] Seq=1 Ack=636 Win=7040 Len=1430 [TCP se
   59 7.158761  64.233.169.104   192.168.1.100    TCP      1484 80 → 4335 [ACK] Seq=1431 Ack=636 Win=7040 Len=1430 [TCF
   60 7.158797  64.233.169.104   192.168.1.100    HTTP      814 HTTP/1.1 200 OK  (text/html)
   61 7.158844  192.168.1.100    64.233.169.104   TCP        54 4335 → 80 [ACK] Seq=636 Ack=3621 Win=260176 Len=0
   62 7.281399  192.168.1.100    64.233.169.104   HTTP      719 GET /intl/en_ALL/images/logo.gif HTTP/1.1
   63 7.315019  64.233.169.104   192.168.1.100    TCP       309 80 → 4335 [PSH, ACK] Seq=3621 Ack=1301 Win=8320 Len=255
   64 7.315576  64.233.169.104   192.168.1.100    TCP      1484 80 → 4335 [ACK] Seq=3876 Ack=1301 Win=8320 Len=1430 [TC
   65 7.315641  192.168.1.100    64.233.169.104   TCP        54 4335 → 80 [ACK] Seq=1301 Ack=5306 Win=260176 Len=0

> Frame 53: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
> Ethernet II, Src: HonHaiPr_0d:ca:8f (00:22:68:0d:ca:8f), Dst: Cisco-Li_45:1f:1b (00:22:6b:45:1f:1b)
> Internet Protocol Version 4, Src: 192.168.1.100, Dst: 64.233.169.104
> Transmission Control Protocol, Src Port: 4335, Dst Port: 80, Seq: 0, Len: 0

0020  a9 68 10 ef 00 50 f8 32  36 e4 00 00 00 00 80 02   ·h···P·2 6·······
```

```
Microsoft Windows [Version 10.0.18362.476]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\Andrea Bonato>whoami
desktop-1pibmrv\andrea bonato

C:\Users\Andrea Bonato>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::4497:bccb:f3a:9f5f%9
   IPv4 Address. . . . . . . . . . . : 192.168.0.110
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\Andrea Bonato>
```

The time that the client-to-server TCP SYN segment is sent that sets up the connection used by the GET sent at time 7.109267 is 7.075657. The source IP address of the TCP SYN segment is 192.168.1.100 (port 4335) and the destination IP is 64.233.169.104 (port 80). The source IP address of the ACK segment is 64.233.169.104 (port 80) and the destination IP is 192.168.1.100 (port 4335). The ACK is received at 7.108986.

6. In the NAT_ISP_side trace file, find the HTTP GET message was sent from the client to the Google server at time 7.109267 (where t=7.109267 is time at which this was sent as recorded in the NAT_home_side trace file). At what time does this message appear in the NAT_ISP_side trace file? What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP GET (as recording in the NAT_ISP_side trace file)? Which of these fields are the same, and which are different, than in your answer to question 3 above?

The time at which this was sent was at 6.069168, as shown in the screenshot below. The source IP is 71.192.34.104, port 4335, and the destination IP is 64.233.169.104, port 80. The only field that changes is the source IP address. The destination, and the ports, are the same.


NAT_ISP_side.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+
Command Prompt

```
No.  Time     Source           Destination      Protocol Length Info
  73 4.959636 71.192.34.104    10.119.240.64    SNMP      120 get-request 1.3.6.1.2.1.25.3.2.1.5.1 1.3.6.1.2.1.25.3.5
  74 4.990690 Cisco_bf:6c:01   Broadcast        ARP        60 Who has 71.192.37.118? Tell 71.192.32.1
  75 5.163071 Cisco_bf:6c:01   Broadcast        ARP        60 Who has 71.192.32.157? Tell 71.192.32.1
  76 5.361737 Cisco_bf:6c:01   Broadcast        ARP        60 Who has 71.192.35.29? Tell 71.192.32.1
  77 5.397728 169.254.247.145  169.254.255.255  NBNS       92 Name query NB HPAB9D4C<00>
  78 5.563968 Cisco_bf:6c:01   Broadcast        ARP        60 Who has 71.192.32.97? Tell 71.192.32.1
  79 5.662814 Dell_58:98:2a    Broadcast        ARP        42 Who has 192.168.1.101? Tell 169.254.247.145
  80 6.020086 71.192.34.104    68.87.71.230     DNS        74 Standard query 0xed6a A www.google.com
  81 6.032738 68.87.71.230     71.192.34.104    DNS       158 Standard query response 0xed6a A www.google.com CNAME w
  82 6.035475 71.192.34.104    64.233.169.104   TCP        66 4335 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=4 SAC
  83 6.067775 64.233.169.104   71.192.34.104    TCP        66 80 → 4335 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=143
  84 6.068754 71.192.34.104    64.233.169.104   TCP        60 4335 → 80 [ACK] Seq=1 Ack=1 Win=260176 Len=0
  85 6.069168 71.192.34.104    64.233.169.104   HTTP      689 GET / HTTP/1.1
  86 6.092755 Cisco_bf:6c:01   Broadcast        ARP        60 Who has 71.192.35.144? Tell 71.192.32.1
  87 6.099637 64.233.169.104   71.192.34.104    TCP        60 80 → 4335 [ACK] Seq=1 Ack=636 Win=7040 Len=0
  88 6.117078 64.233.169.104   71.192.34.104    TCP      1484 80 → 4335 [ACK] Seq=1 Ack=636 Win=7040 Len=1430 [TCP se
  89 6.117407 64.233.169.104   71.192.34.104    TCP      1484 80 → 4335 [ACK] Seq=1431 Ack=636 Win=7040 Len=1430 [TCP
```

```
> Frame 85: 689 bytes on wire (5512 bits), 689 bytes captured (5512 bits)
> Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: Cisco_bf:6c:01 (00:0e:d6:bf:6c:01)
> Internet Protocol Version 4, Src: 71.192.34.104, Dst: 64.233.169.104
> Transmission Control Protocol, Src Port: 4335, Dst Port: 80, Seq: 1, Ack: 1, Len: 635
> Hypertext Transfer Protocol
```

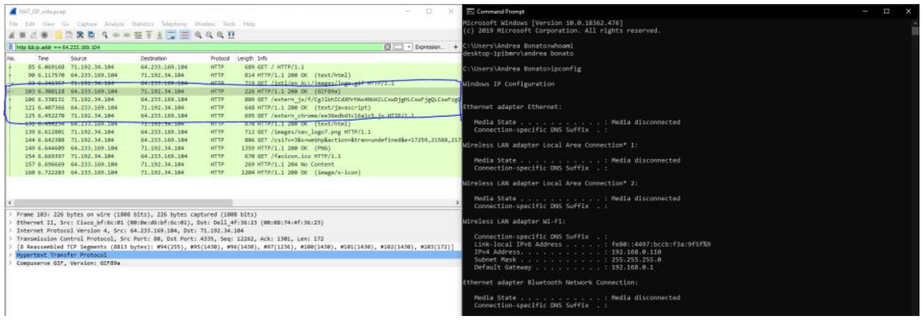
```
Microsoft Windows [Version 10.0.18362.476]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\Andrea Bonato>whoami
desktop-1pibmrv\andrea bonato

C:\Users\Andrea Bonato>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::4497:bccb:f3a:9f5f%9
   IPv4 Address. . . . . . . . . . . : 192.168.0.110
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\Andrea Bonato>
```

7. Are any fields in the HTTP GET message changed? Which of the following fields in the IP datagram carrying the HTTP GET are changed: Version, Header Length, Flags, Checksum. If any of these fields have changed, give a reason (in one sentence) stating why this field needed to change.

None of the fields in the HTTP GET message has changed. When comparing the fields itself in the datagram, the version, header length and flags did not change. However, the checksum flag did end up changing. This is because the source IP address changes, and the checksum includes the value of this specific IP address.

8. In the NAT_ISP_side trace file, at what time is the first 200 OK HTTP message received from the Google server? What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP 200 OK message? Which of these fields are the same, and which are different than your answer to question 4 above?

The time that the first 200 OK HTTP message was received was 6.308118. The source address for this was 64.233.169.104, port 80, and the destination IP was 71.192.34.104, port 4335. In this case, only the destination IP is different.

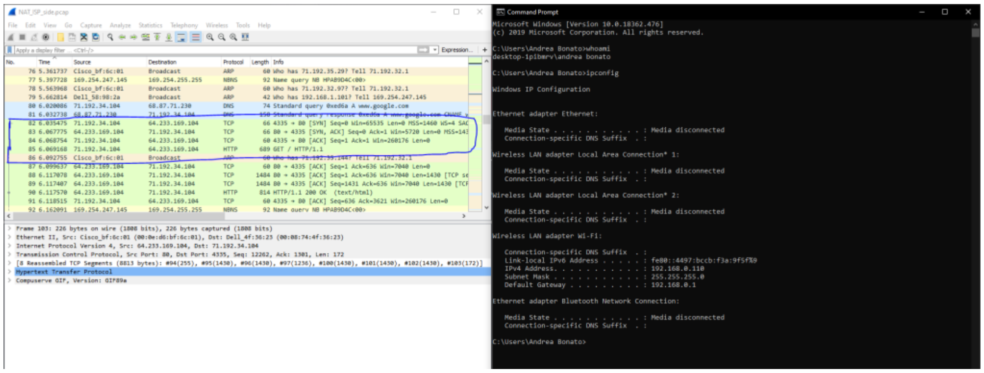


```
NAT_ISP_side.pcap
http && ip.addr == 64.233.169.104

No.  Time      Source          Destination     Protocol Length Info
  85 6.069168  71.192.34.104   64.233.169.104  HTTP      689 GET / HTTP/1.1
  90 6.117570  64.233.169.104  71.192.34.104   HTTP      814 HTTP/1.1 200 OK  (text/html)
  93 6.241357  71.192.34.104   64.233.169.104  HTTP      719 GET /intl/en_ALL/images/logo.gif HTTP/1.1
 103 6.308118  64.233.169.104  71.192.34.104   HTTP      226 HTTP/1.1 200 OK  (GIF89a)
 106 6.330131  71.192.34.104   64.233.169.104  HTTP      809 GET /extern_js/f/CgJlbhICdXMrMAo4NUAILCswDjgHLCswFjgQLCswFzgD
 121 6.407366  64.233.169.104  71.192.34.104   HTTP      648 HTTP/1.1 200 OK  (text/javascript)
 125 6.452270  71.192.34.104   64.233.169.104  HTTP      695 GET /extern_chrome/ee36edbd3c16e1c5.js HTTP/1.1
 131 6.496254  64.233.169.104  71.192.34.104   HTTP      870 HTTP/1.1 200 OK  (text/html)
 139 6.612801  71.192.34.104   64.233.169.104  HTTP      712 GET /images/nav_logo7.png HTTP/1.1
 144 6.642308  71.192.34.104   64.233.169.104  HTTP      806 GET /csi?v=3&s=webhp&action=&tran=undefined&e=17259,21588,217
 149 6.644609  64.233.169.104  71.192.34.104   HTTP     1359 HTTP/1.1 200 OK  (PNG)
 154 6.669397  71.192.34.104   64.233.169.104  HTTP      670 GET /favicon.ico HTTP/1.1
 157 6.696669  64.233.169.104  71.192.34.104   HTTP      269 HTTP/1.1 204 No Content
 160 6.722203  64.233.169.104  71.192.34.104   HTTP     1204 HTTP/1.1 200 OK  (image/x-icon)

> Frame 103: 226 bytes on wire (1808 bits), 226 bytes captured (1808 bits)
> Ethernet II, Src: Cisco_bf:6c:01 (00:0e:d6:bf:6c:01), Dst: Dell_4f:36:23 (00:08:74:4f:36:23)
> Internet Protocol Version 4, Src: 64.233.169.104, Dst: 71.192.34.104
> Transmission Control Protocol, Src Port: 80, Dst Port: 4335, Seq: 12262, Ack: 1301, Len: 172
> [8 Reassembled TCP Segments (8813 bytes): #94(255), #95(1430), #96(1430), #97(1236), #100(1430), #101(1430), #102(1430), #103(172)]
> Hypertext Transfer Protocol
> Compuserve GIF, Version: GIF89a
```

```
Command Prompt
Microsoft Windows [Version 10.0.18362.476]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\Andrea Bonato>whoami
desktop-1pibmrv\andrea bonato

C:\Users\Andrea Bonato>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::4497:bccb:f3a:9f5f%9
   IPv4 Address. . . . . . . . . . . : 192.168.0.110
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
```

9. In the NAT_ISP_side trace file, at what time were the client-to-server TCP SYN segment and the server-to-client TCP ACK segment corresponding to the segments in question 5 above captured? What are the source and destination IP addresses and source and destination ports for these two segments? Which of these fields are the same, and which are different than your answer to question 5 above?

The time that the client-to-server TCP SYN segment were captured was at 6.035475 and the TCP ACK was captured at 6.067775.



```
NAT_ISP_side.pcap
Apply a display filter ... <Ctrl-/>

No.  Time      Source           Destination      Protocol Length Info
  76 5.361737  Cisco_bf:6c:01   Broadcast        ARP       60 Who has 71.192.35.29? Tell 71.192.32.1
  77 5.397728  169.254.247.145  169.254.255.255  NBNS      92 Name query NB HPAB9D4C<00>
  78 5.563968  Cisco_bf:6c:01   Broadcast        ARP       60 Who has 71.192.32.97? Tell 71.192.32.1
  79 5.662814  Dell_58:98:2a    Broadcast        ARP       42 Who has 192.168.1.101? Tell 169.254.247.145
  80 6.020086  71.192.34.104    68.87.71.230     DNS       74 Standard query 0xed6a A www.google.com
  81 6.032738  68.87.71.230     71.192.34.104    DNS      150 Standard query response 0xed6a A www.google.com CNAME
  82 6.035475  71.192.34.104    64.233.169.104   TCP       66 4335 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=4 SAC
  83 6.067775  64.233.169.104   71.192.34.104    TCP       66 80 → 4335 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=143
  84 6.068754  71.192.34.104    64.233.169.104   TCP       60 4335 → 80 [ACK] Seq=1 Ack=1 Win=260176 Len=0
  85 6.069168  71.192.34.104    64.233.169.104   HTTP     689 GET / HTTP/1.1
  86 6.092755  Cisco_bf:6c:01   Broadcast        ARP       60 Who has 71.192.35.144? Tell 71.192.32.1
  87 6.099637  64.233.169.104   71.192.34.104    TCP       60 80 → 4335 [ACK] Seq=1 Ack=636 Win=7040 Len=0
  88 6.117078  64.233.169.104   71.192.34.104    TCP     1484 80 → 4335 [ACK] Seq=1 Ack=636 Win=7040 Len=1430 [TCP se
  89 6.117407  64.233.169.104   71.192.34.104    TCP     1484 80 → 4335 [ACK] Seq=1431 Ack=636 Win=7040 Len=1430 [TCP
  90 6.117570  64.233.169.104   71.192.34.104    HTTP     814 HTTP/1.1 200 OK  (text/html)
  91 6.118515  71.192.34.104    64.233.169.104   TCP       60 4335 → 80 [ACK] Seq=636 Ack=3621 Win=260176 Len=0
  92 6.162091  169.254.247.145  169.254.255.255  NBNS      92 Name query NB HPAB9D4C<00>

> Frame 103: 226 bytes on wire (1808 bits), 226 bytes captured (1808 bits)
> Ethernet II, Src: Cisco_bf:6c:01 (00:0e:d6:bf:6c:01), Dst: Dell_4f:36:23 (00:08:74:4f:36:23)
> Internet Protocol Version 4, Src: 64.233.169.104, Dst: 71.192.34.104
> Transmission Control Protocol, Src Port: 80, Dst Port: 4335, Seq: 12262, Ack: 1301, Len: 172
> [8 Reassembled TCP Segments (8813 bytes): #94(255), #95(1430), #96(1430), #97(1236), #100(1430), #101(1430), #102(1430), #103(172)]
> Hypertext Transfer Protocol
> Compuserve GIF, Version: GIF89a
```

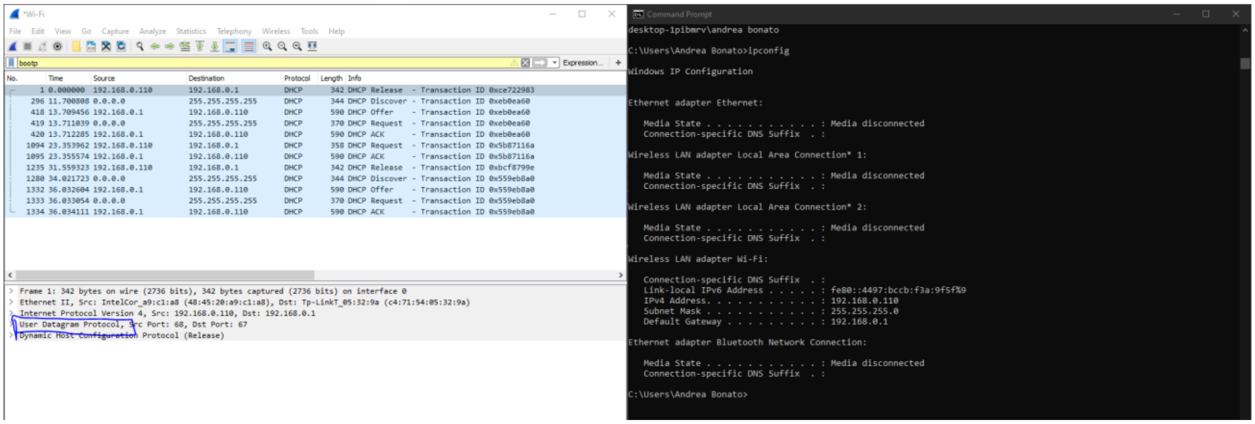
```
Command Prompt
Microsoft Windows [Version 10.0.18362.476]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\Andrea Bonato>whoami
desktop-1pibmrv\andrea bonato

C:\Users\Andrea Bonato>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::4497:bccb:f3a:9f5f%9
   IPv4 Address. . . . . . . . . . . : 192.168.0.110
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\Andrea Bonato>
```

The source IP for the SYN is 71.192.34.104, port 4335, and the destination IP is 64.233.69.104 port, 80. The source Ip for the ACK is 64.233.69.104, port 80, and the destination IP is 71.192.34.104, port 4335. In these cases, the port number remains the same, and in comparison to the solution in question 5, the source IP for the SYN source IP has changed and the destination IP for the ACK has also changed.

Wireshark Lab: DHCP

1. Are DHCP messages sent over UDP or TCP?

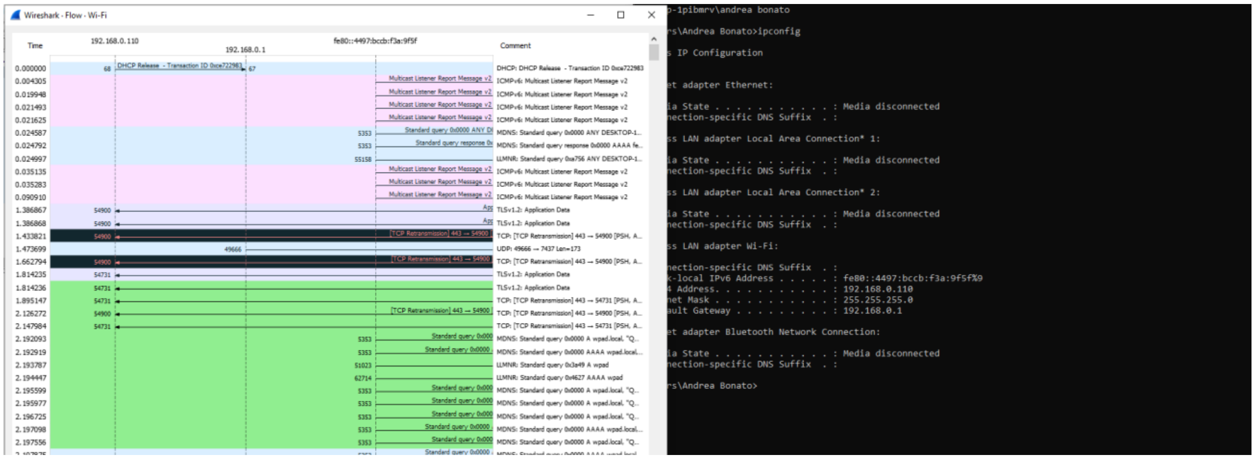
The messages are sent over UDP.


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
Command Prompt

```
bootp
No.   Time      Source        Destination     Protocol Length Info
   1 0.000000  192.168.0.110 192.168.0.1     DHCP     342 DHCP Release  - Transaction ID 0xce722983
 296 11.700808 0.0.0.0       255.255.255.255 DHCP     344 DHCP Discover - Transaction ID 0xeb0ea60
 418 13.709456 192.168.0.1   192.168.0.110   DHCP     590 DHCP Offer    - Transaction ID 0xeb0ea60
 419 13.711039 0.0.0.0       255.255.255.255 DHCP     370 DHCP Request  - Transaction ID 0xeb0ea60
 420 13.712285 192.168.0.1   192.168.0.110   DHCP     590 DHCP ACK      - Transaction ID 0xeb0ea60
1094 23.353962 192.168.0.110 192.168.0.1     DHCP     358 DHCP Request  - Transaction ID 0x5b87116a
1095 23.355574 192.168.0.1   192.168.0.110   DHCP     590 DHCP ACK      - Transaction ID 0x5b87116a
1235 31.559323 192.168.0.110 192.168.0.1     DHCP     342 DHCP Release  - Transaction ID 0xbcf8799e
1280 34.021723 0.0.0.0       255.255.255.255 DHCP     344 DHCP Discover - Transaction ID 0x559eb8a0
1332 36.032604 192.168.0.1   192.168.0.110   DHCP     590 DHCP Offer    - Transaction ID 0x559eb8a0
1333 36.033054 0.0.0.0       255.255.255.255 DHCP     370 DHCP Request  - Transaction ID 0x559eb8a0
1334 36.034111 192.168.0.1   192.168.0.110   DHCP     590 DHCP ACK      - Transaction ID 0x559eb8a0

> Frame 1: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
> Ethernet II, Src: IntelCor_a9:c1:a8 (48:45:20:a9:c1:a8), Dst: Tp-LinkT_05:32:9a (c4:71:54:05:32:9a)
> Internet Protocol Version 4, Src: 192.168.0.110, Dst: 192.168.0.1
> User Datagram Protocol, Src Port: 68, Dst Port: 67
> Dynamic Host Configuration Protocol (Release)
```

```
desktop-1pibmrv\andrea bonato

C:\Users\Andrea Bonato>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::4497:bccb:f3a:9f5f%9
   IPv4 Address. . . . . . . . . . . : 192.168.0.110
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\Andrea Bonato>
```

2. Draw a timing datagram illustrating the sequence of the first four-packet Discover/Offer/Request/ACK DHCP exchange between the client and server. For each packet, indicated the source and destination port numbers. Are the port numbers the same as in the example given in this lab assignment?

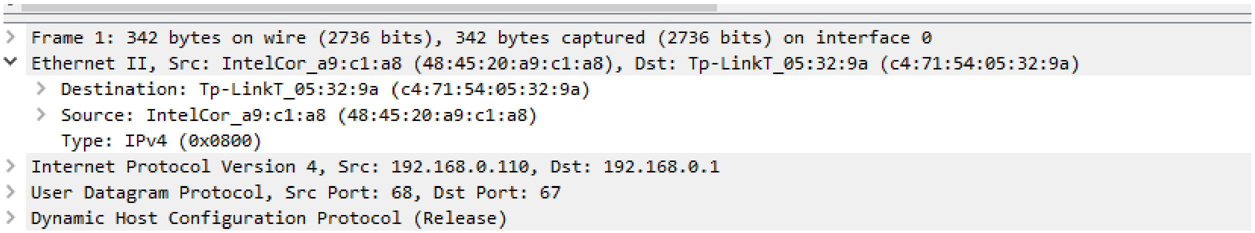

Wireshark - Flow - Wi-Fi
Time
192.168.0.110
192.168.0.1
fe80::4497:bccb:f3a:9f5f
Comment
DHCP Release - Transaction ID 0xce722983
Multicast Listener Report Message v2
Standard query 0x0000 ANY DE
Standard query response 0x
App
[TCP Retransmission] 443 → 54900
Standard query 0x000

```
0.000000   68 → 67   DHCP: DHCP Release  - Transaction ID 0xce722983
0.004305             ICMPv6: Multicast Listener Report Message v2
0.019948             ICMPv6: Multicast Listener Report Message v2
0.021493             ICMPv6: Multicast Listener Report Message v2
0.021625             ICMPv6: Multicast Listener Report Message v2
0.024587   5353      MDNS: Standard query 0x0000 ANY DESKTOP-1...
0.024792   5353      MDNS: Standard query response 0x0000 AAAA fe...
0.024997   55158     LLMNR: Standard query 0xa756 ANY DESKTOP-1...
0.035135             ICMPv6: Multicast Listener Report Message v2
0.035283             ICMPv6: Multicast Listener Report Message v2
0.090910             ICMPv6: Multicast Listener Report Message v2
1.386867   54900     TLSv1.2: Application Data
1.386868   54900     TLSv1.2: Application Data
1.433821   54900     TCP: [TCP Retransmission] 443 → 54900 [PSH, A...
1.473699   49666     UDP: 49666 → 7437 Len=173
1.662794   54900     TCP: [TCP Retransmission] 443 → 54900 [PSH, A...
1.814235   54731     TLSv1.2: Application Data
1.814236   54731     TLSv1.2: Application Data
1.895147   54731     TCP: [TCP Retransmission] 443 → 54731 [PSH, A...
2.126272   54900     TCP: [TCP Retransmission] 443 → 54900 [PSH, A...
2.147984   54731     TCP: [TCP Retransmission] 443 → 54731 [PSH, A...
2.192093   5353      MDNS: Standard query 0x0000 A wpad.local, "Q...
2.192919   5353      MDNS: Standard query 0x0000 AAAA wpad.local,...
2.193787   51023     LLMNR: Standard query 0x3a49 A wpad
2.194447   62714     LLMNR: Standard query 0x4627 AAAA wpad
2.195599   5353      MDNS: Standard query 0x0000 A wpad.local, "Q...
2.195977   5353      MDNS: Standard query 0x0000 A wpad.local, "Q...
2.196725   5353      MDNS: Standard query 0x0000 A wpad.local, "Q...
2.197098   5353      MDNS: Standard query 0x0000 AAAA wpad.local,...
2.197556   5353      MDNS: Standard query 0x0000 A wpad.local, "Q...
```

```
p-1pibmrv\andrea bonato

rs\Andrea Bonato>ipconfig

s IP Configuration


et adapter Ethernet:

ia State . . . . . . . . . . . : Media disconnected
nection-specific DNS Suffix  . :

ss LAN adapter Local Area Connection* 1:

ia State . . . . . . . . . . . : Media disconnected
nection-specific DNS Suffix  . :

ss LAN adapter Local Area Connection* 2:

ia State . . . . . . . . . . . : Media disconnected
nection-specific DNS Suffix  . :

ss LAN adapter Wi-Fi:

nection-specific DNS Suffix  . :
k-local IPv6 Address . . . . . : fe80::4497:bccb:f3a:9f5f%9
4 Address. . . . . . . . . . . : 192.168.0.110
net Mask . . . . . . . . . . . : 255.255.255.0
ault Gateway . . . . . . . . . : 192.168.0.1

et adapter Bluetooth Network Connection:

ia State . . . . . . . . . . . : Media disconnected
nection-specific DNS Suffix  . :

rs\Andrea Bonato>
```

3. What is the link-layer (e.g., Ethernet) address of your host?

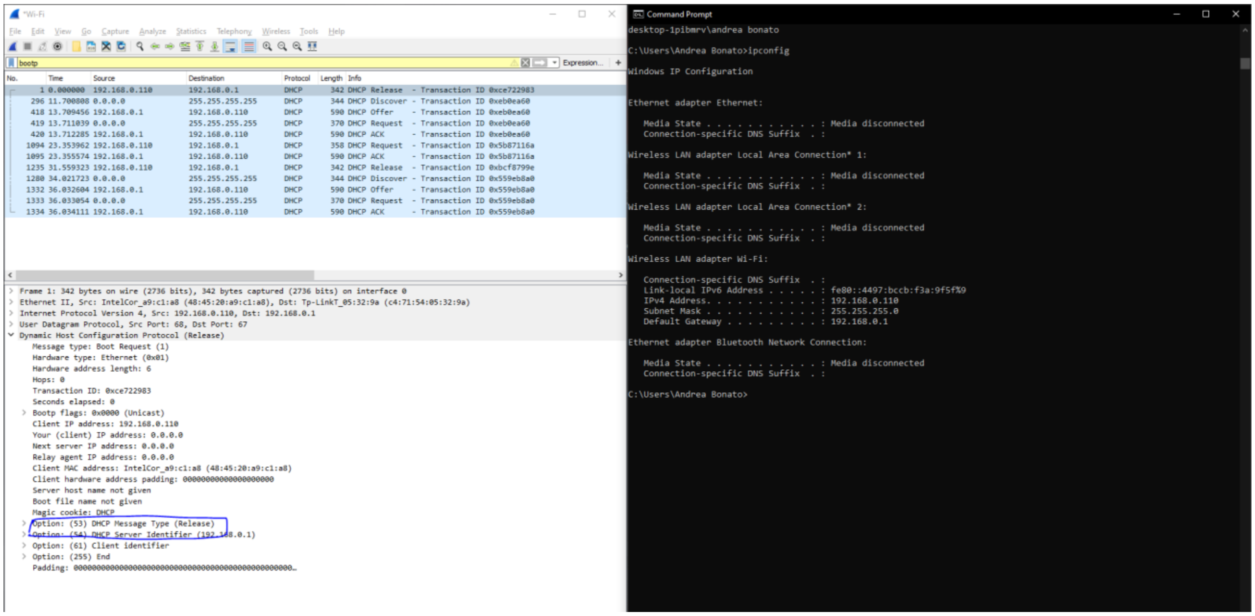
The link layer address of my workstation is 48:45:20:a9:c1:a8.



```
> Frame 1: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
v Ethernet II, Src: IntelCor_a9:c1:a8 (48:45:20:a9:c1:a8), Dst: Tp-LinkT_05:32:9a (c4:71:54:05:32:9a)
  > Destination: Tp-LinkT_05:32:9a (c4:71:54:05:32:9a)
  > Source: IntelCor_a9:c1:a8 (48:45:20:a9:c1:a8)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 192.168.0.110, Dst: 192.168.0.1
> User Datagram Protocol, Src Port: 68, Dst Port: 67
> Dynamic Host Configuration Protocol (Release)
```

4. What values in the DHCP discover message differentiate this message from the DHCP request message?

The value that differentiates this message from the DHCP request message to the discover message is the DHCP Message Type.



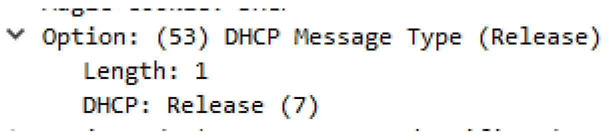
*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
Command Prompt

Filter: bootp

```
No.   Time      Source          Destination      Protocol Length Info
   1 0.000000  192.168.0.110   192.168.0.1      DHCP     342 DHCP Release  - Transaction ID 0xce722983
 296 11.700808 0.0.0.0         255.255.255.255  DHCP     344 DHCP Discover - Transaction ID 0xeb0ea60
 418 13.709456 192.168.0.1     192.168.0.110    DHCP     590 DHCP Offer    - Transaction ID 0xeb0ea60
 419 13.711039 0.0.0.0         255.255.255.255  DHCP     370 DHCP Request  - Transaction ID 0xeb0ea60
 420 13.712285 192.168.0.1     192.168.0.110    DHCP     590 DHCP ACK      - Transaction ID 0xeb0ea60
1094 23.353962 192.168.0.110   192.168.0.1      DHCP     358 DHCP Request  - Transaction ID 0x5b87116a
1095 23.355574 192.168.0.1     192.168.0.110    DHCP     590 DHCP ACK      - Transaction ID 0x5b87116a
1235 31.559323 192.168.0.110   192.168.0.1      DHCP     342 DHCP Release  - Transaction ID 0xbcf8799e
1280 34.021723 0.0.0.0         255.255.255.255  DHCP     344 DHCP Discover - Transaction ID 0x559eb8a0
1332 36.032604 192.168.0.1     192.168.0.110    DHCP     590 DHCP Offer    - Transaction ID 0x559eb8a0
1333 36.033054 0.0.0.0         255.255.255.255  DHCP     370 DHCP Request  - Transaction ID 0x559eb8a0
1334 36.034111 192.168.0.1     192.168.0.110    DHCP     590 DHCP ACK      - Transaction ID 0x559eb8a0
```

```
> Frame 1: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
> Ethernet II, Src: IntelCor_a9:c1:a8 (48:45:20:a9:c1:a8), Dst: Tp-LinkT_05:32:9a (c4:71:54:05:32:9a)
> Internet Protocol Version 4, Src: 192.168.0.110, Dst: 192.168.0.1
> User Datagram Protocol, Src Port: 68, Dst Port: 67
v Dynamic Host Configuration Protocol (Release)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xce722983
    Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
    Client IP address: 192.168.0.110
    Your (client) IP address: 0.0.0.0
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: IntelCor_a9:c1:a8 (48:45:20:a9:c1:a8)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Release)
  > Option: (54) DHCP Server Identifier (192.168.0.1)
  > Option: (61) Client identifier
  > Option: (255) End
    Padding: 000000000000000000000000000000000000000000000000…
```

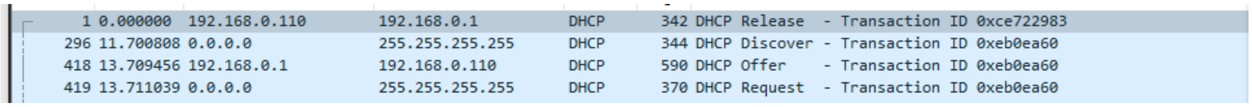
```
desktop-1pibmrv\andrea bonato

C:\Users\Andrea Bonato>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::4497:bccb:f3a:9f5f%9
   IPv4 Address. . . . . . . . . . . : 192.168.0.110
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\Andrea Bonato>
```



```
v Option: (53) DHCP Message Type (Release)
    Length: 1
    DHCP: Release (7)
```

5. What is the value of the Transaction-ID in each of the first four (Discover/Offer/Request/ACK) DHCP messages? What are the values of the Transaction-ID in the second set (Request/ACK) set of DHCP messages? What is the purpose of the Transaction-ID field?

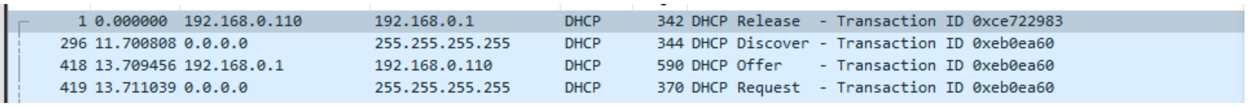
The value of the Transaction-ID in each of the first four is 0xce722983, and the rest is 0xeb0ea60.



```
  1 0.000000  192.168.0.110   192.168.0.1      DHCP   342 DHCP Release  - Transaction ID 0xce722983
296 11.700808 0.0.0.0         255.255.255.255  DHCP   344 DHCP Discover - Transaction ID 0xeb0ea60
418 13.709456 192.168.0.1     192.168.0.110    DHCP   590 DHCP Offer    - Transaction ID 0xeb0ea60
419 13.711039 0.0.0.0         255.255.255.255  DHCP   370 DHCP Request  - Transaction ID 0xeb0ea60
```

The values of the second Transaction-ID is 0xeb0ea60. A Transaction-ID is used to determine whether the requests are from the server and client.

6. A host uses DHCP to obtain an IP address, among other things. But a host's IP address is not confirmed until the end of the four-message exchange! If the IP address is not set until the end of the four-message exchange, then what values are used in the IP datagrams in the four-message exchange? For each of the four DHCP messages (Discover/Offer/Request/ACK DHCP), indicate the source and destination IP addresses that are carried in the encapsulating IP datagram.



```
    1 0.000000  192.168.0.110     192.168.0.1          DHCP      342 DHCP Release  - Transaction ID 0xce722983
  296 11.700808 0.0.0.0           255.255.255.255      DHCP      344 DHCP Discover - Transaction ID 0xeb0ea60
  418 13.709456 192.168.0.1       192.168.0.110        DHCP      590 DHCP Offer    - Transaction ID 0xeb0ea60
  419 13.711039 0.0.0.0           255.255.255.255      DHCP      370 DHCP Request  - Transaction ID 0xeb0ea60
```

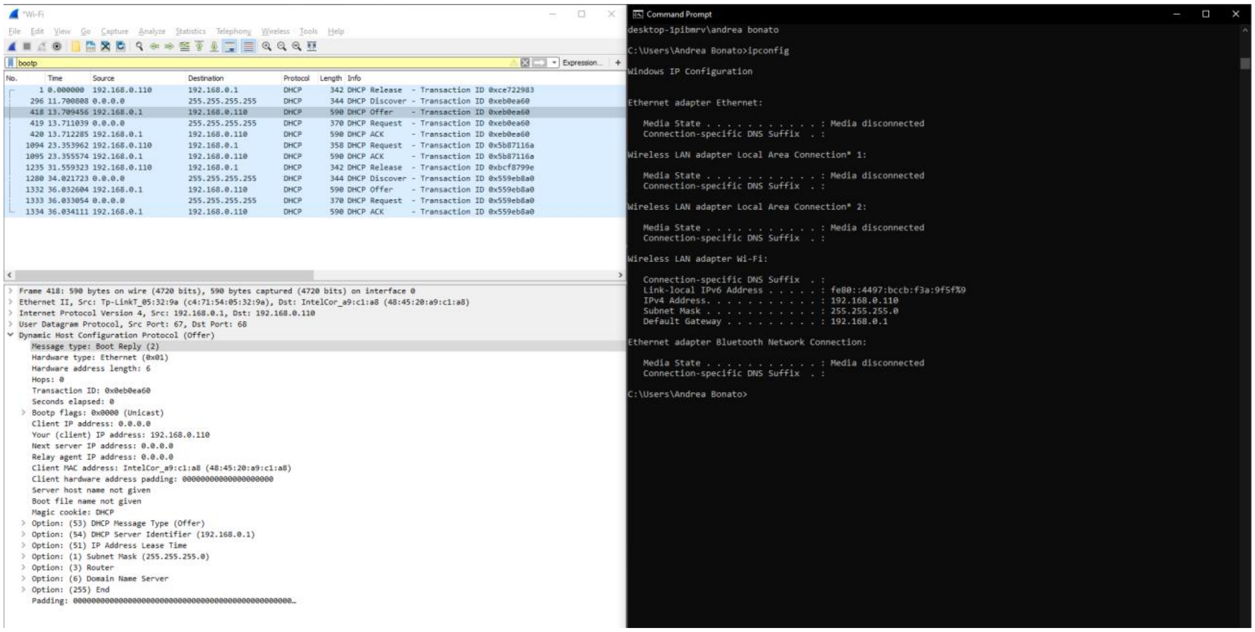
As shown above, the DCHP client and server both use 255.255.255.255 as the destination address. The client uses source IP addresses 0.0.0.0 and the actual server uses it's own IP.

7. What is the IP address of your DHCP server?

The address of the server is 192.168.0.1.

8. What IP address is the DHCP server offering to your host in the DHCP Offer message? Indicate which DHCP message contains the offered DHCP address.

The IP address that the DHCP server is offering is 192.168.0.110. The DHCP message type is equal to DHCP offer



*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
bootp
Expression…
+
Command Prompt

```
No.  Time      Source          Destination      Protocol Length Info
   1 0.000000  192.168.0.110   192.168.0.1      DHCP     342 DHCP Release  - Transaction ID 0xce722983
 296 11.700808 0.0.0.0         255.255.255.255  DHCP     344 DHCP Discover - Transaction ID 0xeb0ea60
 418 13.709456 192.168.0.1     192.168.0.110    DHCP     590 DHCP Offer    - Transaction ID 0xeb0ea60
 419 13.711039 0.0.0.0         255.255.255.255  DHCP     370 DHCP Request  - Transaction ID 0xeb0ea60
 420 13.712285 192.168.0.1     192.168.0.110    DHCP     590 DHCP ACK      - Transaction ID 0xeb0ea60
1094 23.353962 192.168.0.110   192.168.0.1      DHCP     358 DHCP Request  - Transaction ID 0x5b87116a
1095 23.355574 192.168.0.1     192.168.0.110    DHCP     590 DHCP ACK      - Transaction ID 0x5b87116a
1235 31.559323 192.168.0.110   192.168.0.1      DHCP     342 DHCP Release  - Transaction ID 0xbcf8799e
1280 34.021723 0.0.0.0         255.255.255.255  DHCP     344 DHCP Discover - Transaction ID 0x559eb8a0
1332 36.032604 192.168.0.1     192.168.0.110    DHCP     590 DHCP Offer    - Transaction ID 0x559eb8a0
1333 36.033054 0.0.0.0         255.255.255.255  DHCP     370 DHCP Request  - Transaction ID 0x559eb8a0
1334 36.034111 192.168.0.1     192.168.0.110    DHCP     590 DHCP ACK      - Transaction ID 0x559eb8a0
```

```
> Frame 418: 590 bytes on wire (4720 bits), 590 bytes captured (4720 bits) on interface 0
> Ethernet II, Src: Tp-LinkT_05:32:9a (c4:71:54:05:32:9a), Dst: IntelCor_a9:c1:a8 (48:45:20:a9:c1:a8)
> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.110
> User Datagram Protocol, Src Port: 67, Dst Port: 68
v Dynamic Host Configuration Protocol (Offer)
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x0eb0ea60
    Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 192.168.0.110
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: IntelCor_a9:c1:a8 (48:45:20:a9:c1:a8)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Offer)
  > Option: (54) DHCP Server Identifier (192.168.0.1)
  > Option: (51) IP Address Lease Time
  > Option: (1) Subnet Mask (255.255.255.0)
  > Option: (3) Router
  > Option: (6) Domain Name Server
  > Option: (255) End
    Padding: 000000000000000000000000000000000000000000000000…
```

```
desktop-1pibmrv\andrea bonato

C:\Users\Andrea Bonato>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::4497:bccb:f3a:9f5f%9
   IPv4 Address. . . . . . . . . . . : 192.168.0.110
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\Andrea Bonato>
```

9. In the example screenshot in this assignment, there is no relay agent between the host and the DHCP server. What values in the trace indicate the absence of a relay agent? Is there a relay agent in your experiment? If so, what is the IP address of the agent?

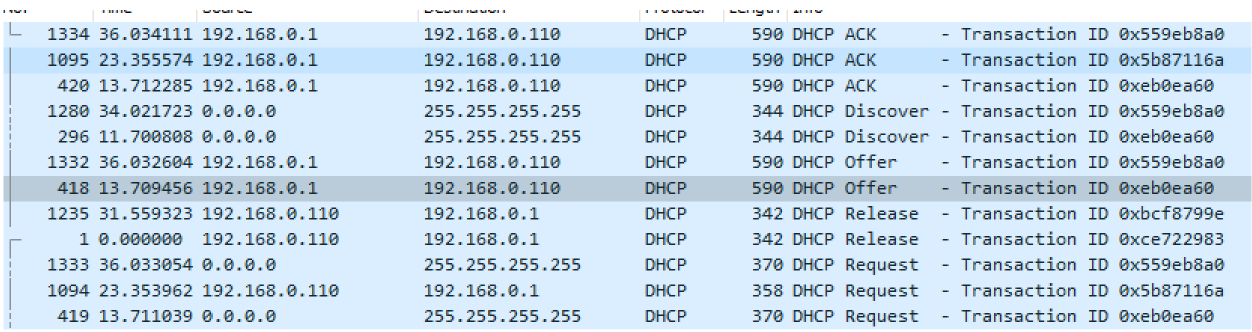
As shown in the screenshot in question 8, there is a relay agent, and it is set to the IP address 0.0.0.0. Thus, in my experiment there is a relay agent.

10. Explain the purpose of the router and subnet mask lines in the DHCP offer message.

The router line indicates what the default gateway should be to the client and the subnet mask lines determine which subnet mask the client should use.

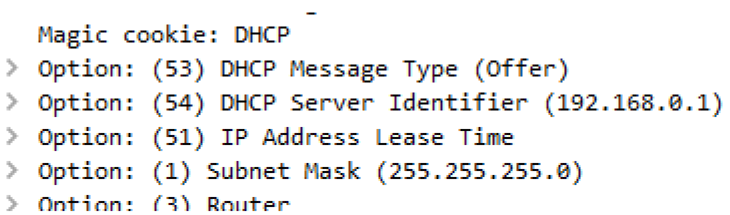
11. In the DHCP trace file noted in footnote 2, the DHCP server offers a specific IP address to the client (see also question 8. above). In the client's response to the first server OFFER message, does the client accept this IP address? Where in the client's RESPONSE is the client's requested address?

The host requests the offered IP address in the DHCP request message . The client's respone message is accepted in order to get to this section.



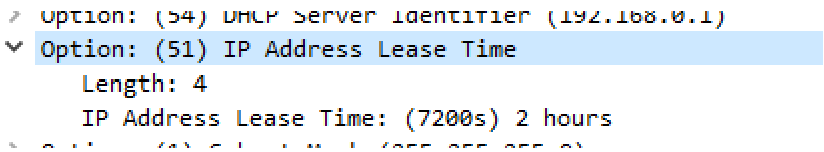
```
1334 36.034111 192.168.0.1      192.168.0.110      DHCP  590 DHCP ACK      - Transaction ID 0x559eb8a0
1095 23.355574 192.168.0.1      192.168.0.110      DHCP  590 DHCP ACK      - Transaction ID 0x5b87116a
 420 13.712285 192.168.0.1      192.168.0.110      DHCP  590 DHCP ACK      - Transaction ID 0xeb0ea60
1280 34.021723 0.0.0.0          255.255.255.255    DHCP  344 DHCP Discover - Transaction ID 0x559eb8a0
 296 11.700808 0.0.0.0          255.255.255.255    DHCP  344 DHCP Discover - Transaction ID 0xeb0ea60
1332 36.032604 192.168.0.1      192.168.0.110      DHCP  590 DHCP Offer    - Transaction ID 0x559eb8a0
 418 13.709456 192.168.0.1      192.168.0.110      DHCP  590 DHCP Offer    - Transaction ID 0xeb0ea60
1235 31.559323 192.168.0.110    192.168.0.1        DHCP  342 DHCP Release  - Transaction ID 0xbcf8799e
   1 0.000000  192.168.0.110    192.168.0.1        DHCP  342 DHCP Release  - Transaction ID 0xce722983
1333 36.033054 0.0.0.0          255.255.255.255    DHCP  370 DHCP Request  - Transaction ID 0x559eb8a0
1094 23.353962 192.168.0.110    192.168.0.1        DHCP  358 DHCP Request  - Transaction ID 0x5b87116a
 419 13.711039 0.0.0.0          255.255.255.255    DHCP  370 DHCP Request  - Transaction ID 0xeb0ea60
```

12. Explain the purpose of the lease time. How long is the lease time in your experiment?



```
  Magic cookie: DHCP
> Option: (53) DHCP Message Type (Offer)
> Option: (54) DHCP Server Identifier (192.168.0.1)
> Option: (51) IP Address Lease Time
> Option: (1) Subnet Mask (255.255.255.0)
> Option: (3) Router
```

The lease time is the amount of time that the DHCP server assigns an IP address to a client for. In this time, the server will not change the given address to another client, unless the client ha already given up the IP address that it was assigned.



```
> Option: (54) DHCP Server Identifier (192.168.0.1)
v Option: (51) IP Address Lease Time
    Length: 4
    IP Address Lease Time: (7200s) 2 hours
```

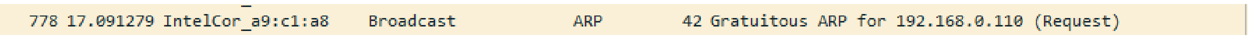
In this case, the lease time is 2 hours,

13. What is the purpose of the DHCP release message? Does the DHCP server issue an acknowledgment of receipt of the client's DHCP request? What would happen if the client's DHCP release message is lost?

As states in question 12, the lease time is the amount of time that the DHCP server takes between the assigning and requesting of the IP addresses. The DHCP release message is the message that the client sends to cancel its lease on the IP address given to it by the DHCP sever. However, the DHCP, in this case, did not acknowledge the request. In this case, because it was list, the DHCP server would have to wait the lease time to reassign the IP address.

14. Clear the bootp filter from your Wireshark window. Were any ARP packets sent or received during the DHCP packet-exchange period? If so, explain the purpose of those ARP packets.

In this case, there were several ARP requests made by the DHCP server.



```
778 17.091279 IntelCor_a9:c1:a8    Broadcast          ARP        42 Gratuitous ARP for 192.168.0.110 (Request)
```

The purpose of the ARP packets is to make sure that the IP addresses that are being assigned, isn't already assigned.