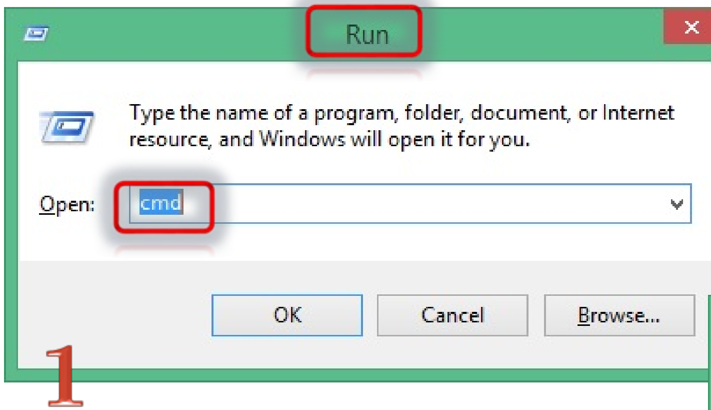
DHCP & WIRESHARK EXPERIMENT

Acknowledgement: Derived for the course by Ibrahim Aljubayri from exercises in Kurose and Ross text (See references provided in the first lecture)

DHCP Experiment

- In order to observe DHCP in action, we'll perform several DHCP-related commands and capture the DHCP messages exchanged as a result of executing these commands by using WireShark.

- We start by opening the Windows Command Prompt application.
- Go to Run → cmd

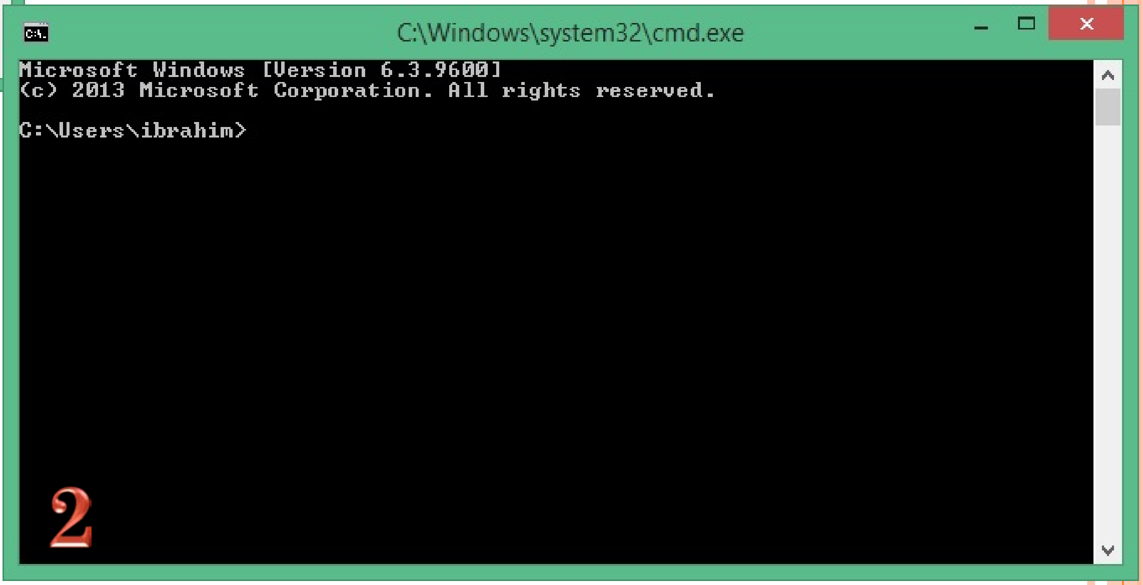


1

Run

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: cmd



2

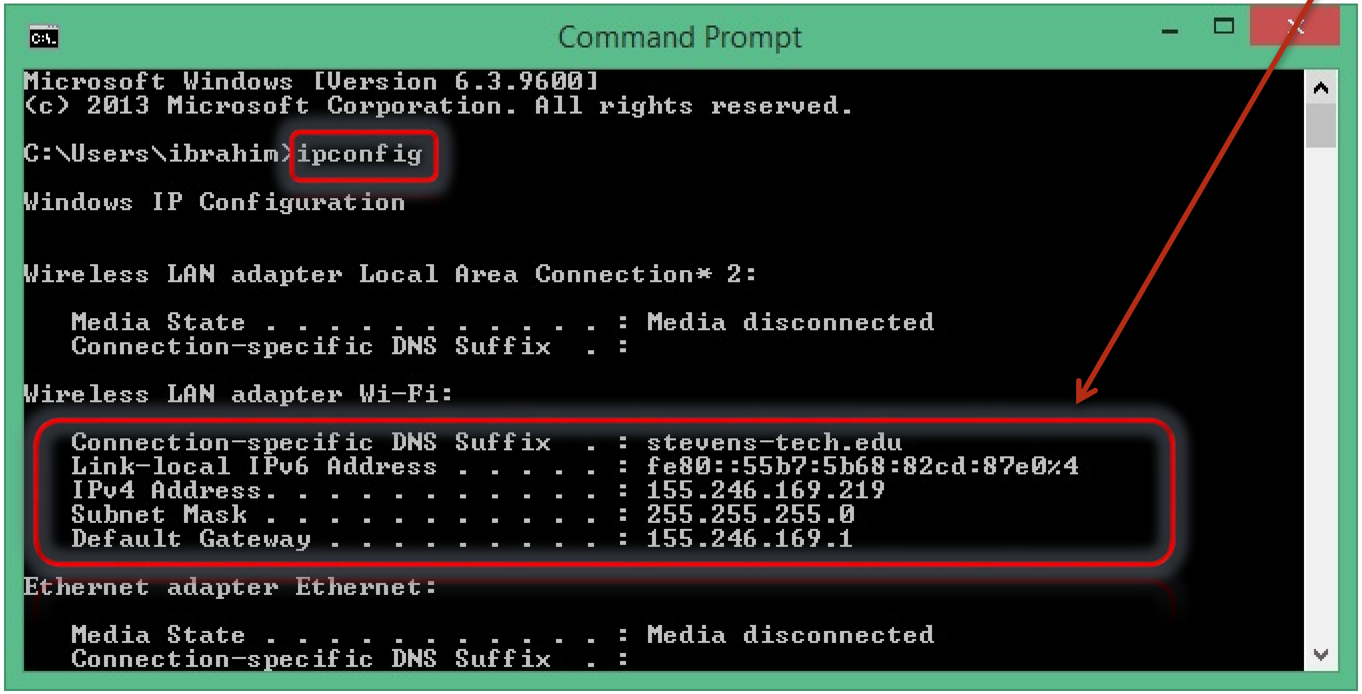
C:\Windows\system32\cmd.exe

```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\ibrahim>
```

Type in “ipconfig”

- This command will show you your current IP address. You got it dynamically as soon as you laptop discovered the DHCP server.

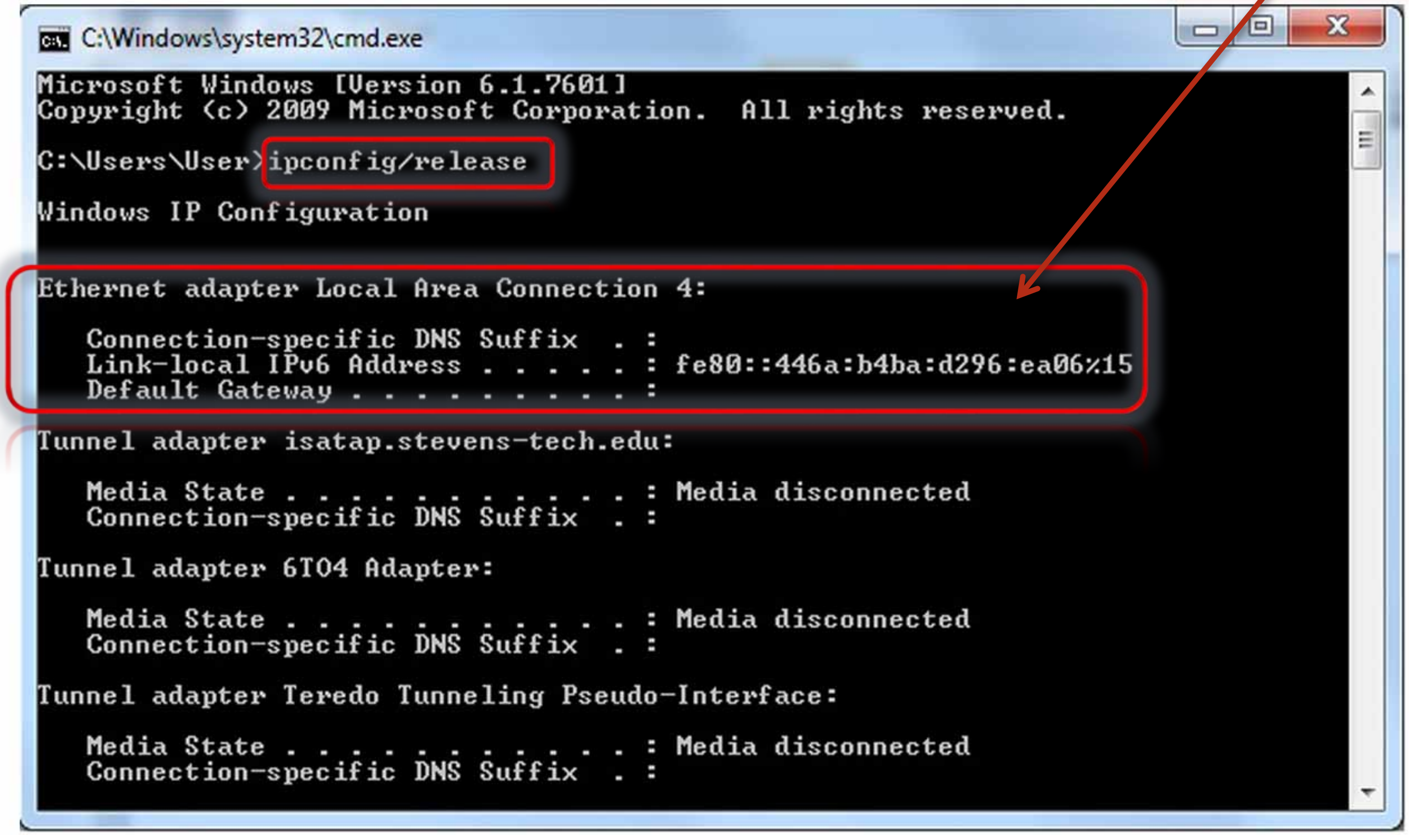
Dynamic IP address



```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\ibrahim>ipconfig

Windows IP Configuration


Wireless LAN adapter Local Area Connection* 2:

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

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : stevens-tech.edu
   Link-local IPv6 Address . . . . . : fe80::55b7:5b68:82cd:87e0%4
   IPv4 Address. . . . . . . . . . . : 155.246.169.219
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 155.246.169.1

Ethernet adapter Ethernet:

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

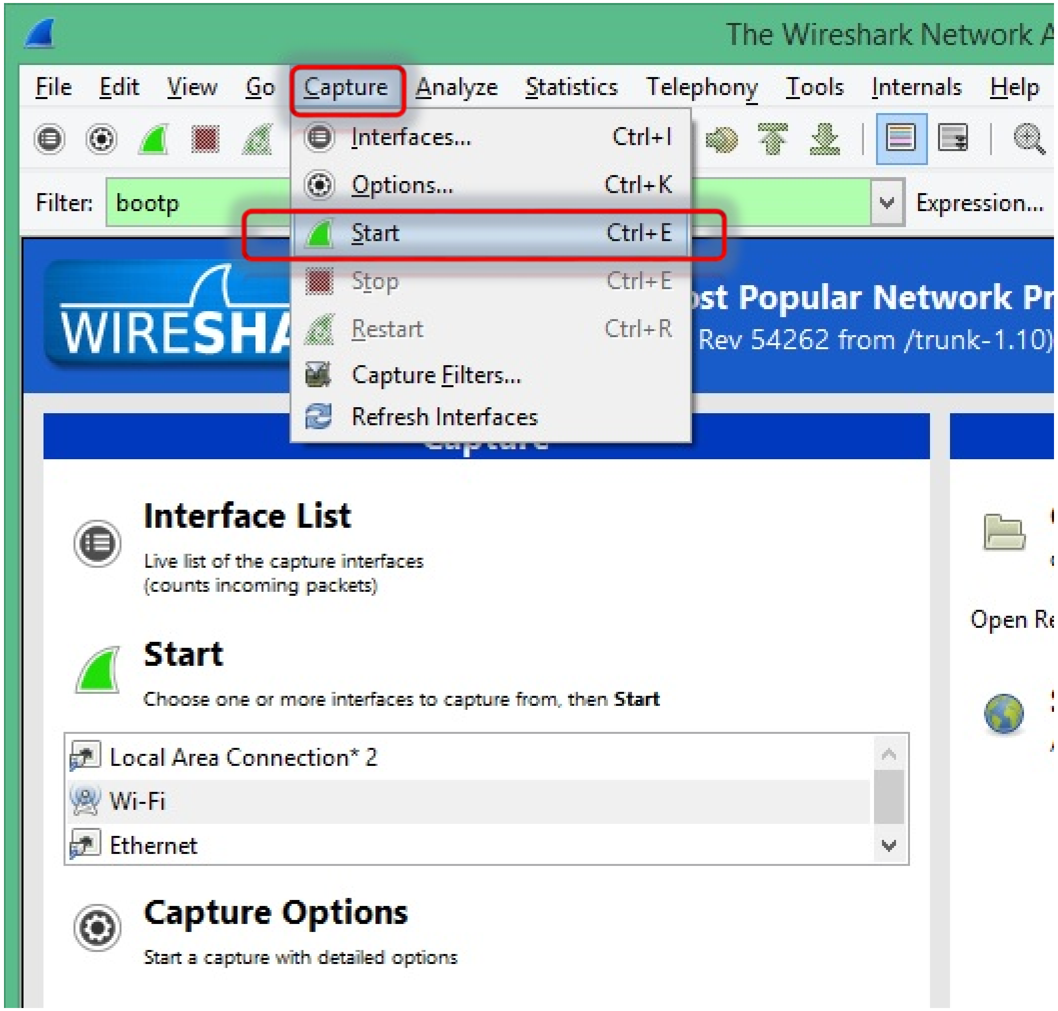
- Type in “ipconfig /release”
  - This command releases your current IP address. So, you have no IP address

No IP address



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\User>ipconfig/release

Windows IP Configuration


Ethernet adapter Local Area Connection 4:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::446a:b4ba:d296:ea06%15
   Default Gateway . . . . . . . . . :

Tunnel adapter isatap.stevens-tech.edu:

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

Tunnel adapter 6TO4 Adapter:

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

Tunnel adapter Teredo Tunneling Pseudo-Interface:

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

- Now start up the Wireshark packet sniffer, and begin Wireshark packet capture.



Filter: bootp

Interface List

Live list of the capture interfaces (counts incoming packets)

Start

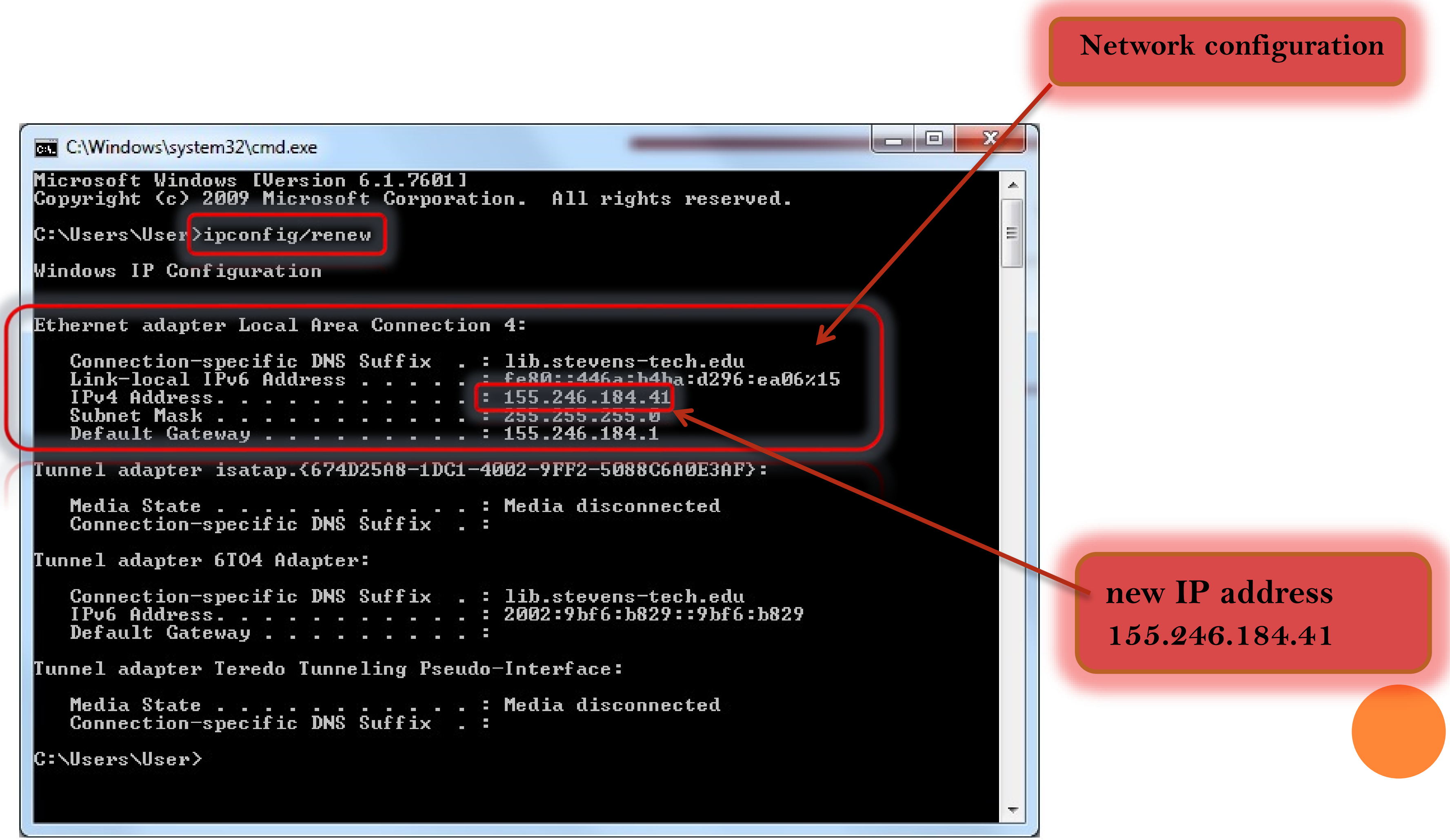
Choose one or more interfaces to capture from, then **Start**

Local Area Connection* 2
Wi-Fi
Ethernet

Capture Options

Start a capture with detailed options

- Now go back to the Windows Command Prompt and type “ipconfig /renew”.
  - This instructs your host to obtain a network configuration, including a new IP address.

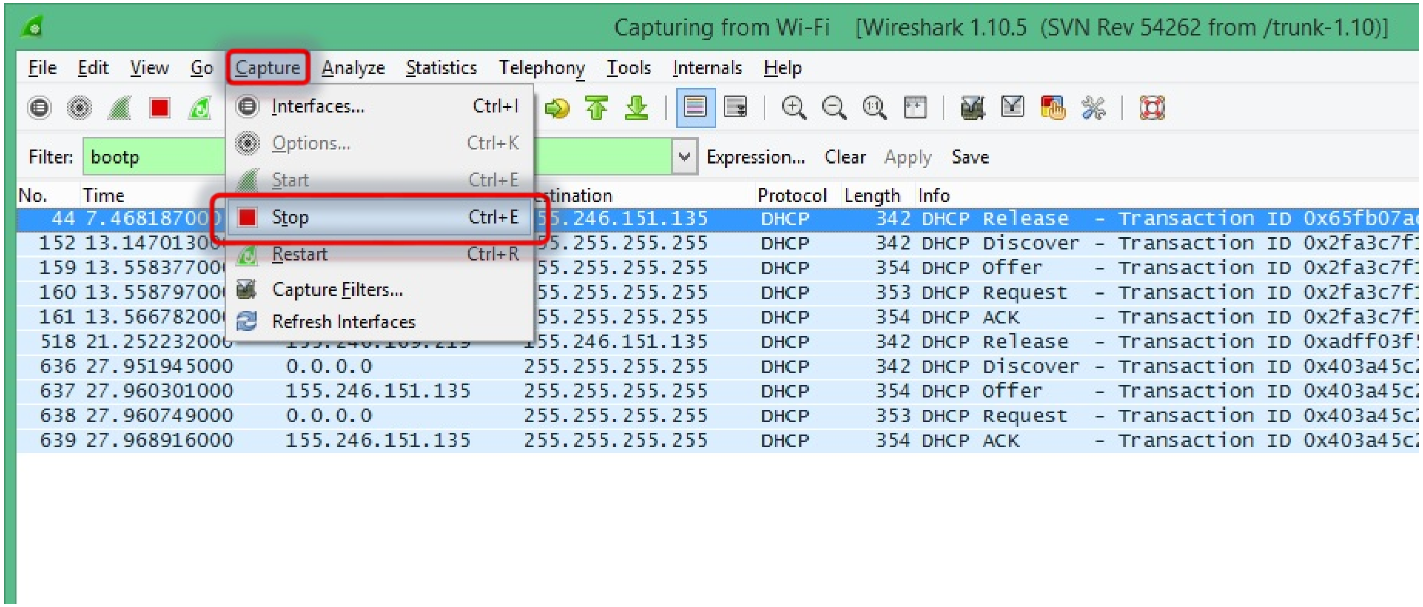


```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\User>ipconfig/renew

Windows IP Configuration


Ethernet adapter Local Area Connection 4:

   Connection-specific DNS Suffix  . : lib.stevens-tech.edu
   Link-local IPv6 Address . . . . . : fe80::446a:b4ba:d296:ea06%15
   IPv4 Address. . . . . . . . . . . : 155.246.184.41
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 155.246.184.1

Tunnel adapter isatap.{674D25A8-1DC1-4002-9FF2-5088C6A0E3AF}:

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

Tunnel adapter 6TO4 Adapter:

   Connection-specific DNS Suffix  . : lib.stevens-tech.edu
   IPv6 Address. . . . . . . . . . . : 2002:9bf6:b829::9bf6:b829
   Default Gateway . . . . . . . . . :

Tunnel adapter Teredo Tunneling Pseudo-Interface:

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

C:\Users\User>
```

Network configuration

new IP address
155.246.184.41

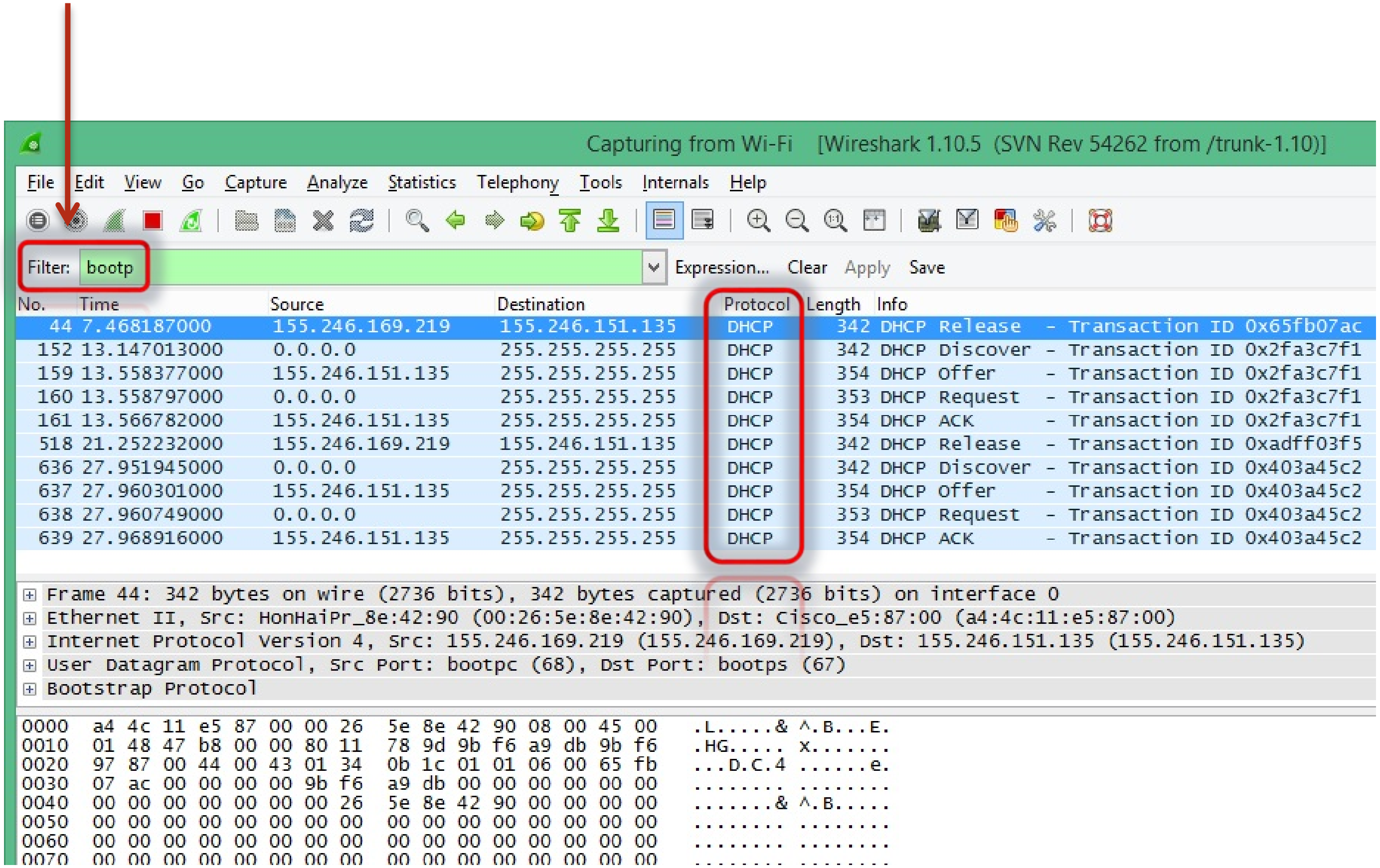
- Enter the command “ipconfig/release” to release the previously-allocated IP address to your computer.
- Finally, enter “ipconfig /renew” to again be allocated an IP address for your computer.
- Now go back to Wireshark and stop the packet capturing.



Filter: bootp

No.	Time		stination	Protocol	Length	Info
44	7.46818700		5.246.151.135	DHCP	342	DHCP Release - Transaction ID 0x65fb07a
152	13.14701300		5.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x2fa3c7f
159	13.55837700		55.255.255.255	DHCP	354	DHCP Offer - Transaction ID 0x2fa3c7f
160	13.55879700		55.255.255.255	DHCP	353	DHCP Request - Transaction ID 0x2fa3c7f
161	13.56678200		55.255.255.255	DHCP	354	DHCP ACK - Transaction ID 0x2fa3c7f
518	21.25223200	155.246.169.219	155.246.151.135	DHCP	342	DHCP Release - Transaction ID 0xadff03f
636	27.951945000	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x403a45c
637	27.960301000	155.246.151.135	255.255.255.255	DHCP	354	DHCP Offer - Transaction ID 0x403a45c
638	27.960749000	0.0.0.0	255.255.255.255	DHCP	353	DHCP Request - Transaction ID 0x403a45c
639	27.968916000	155.246.151.135	255.255.255.255	DHCP	354	DHCP ACK - Transaction ID 0x403a45c

- Now let’s take a look at the resulting WireShark window.
- Hint: To see only the DHCP packets, enter into the filter field “bootp”


Capturing from Wi-Fi [Wireshark 1.10.5 (SVN Rev 54262 from /trunk-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

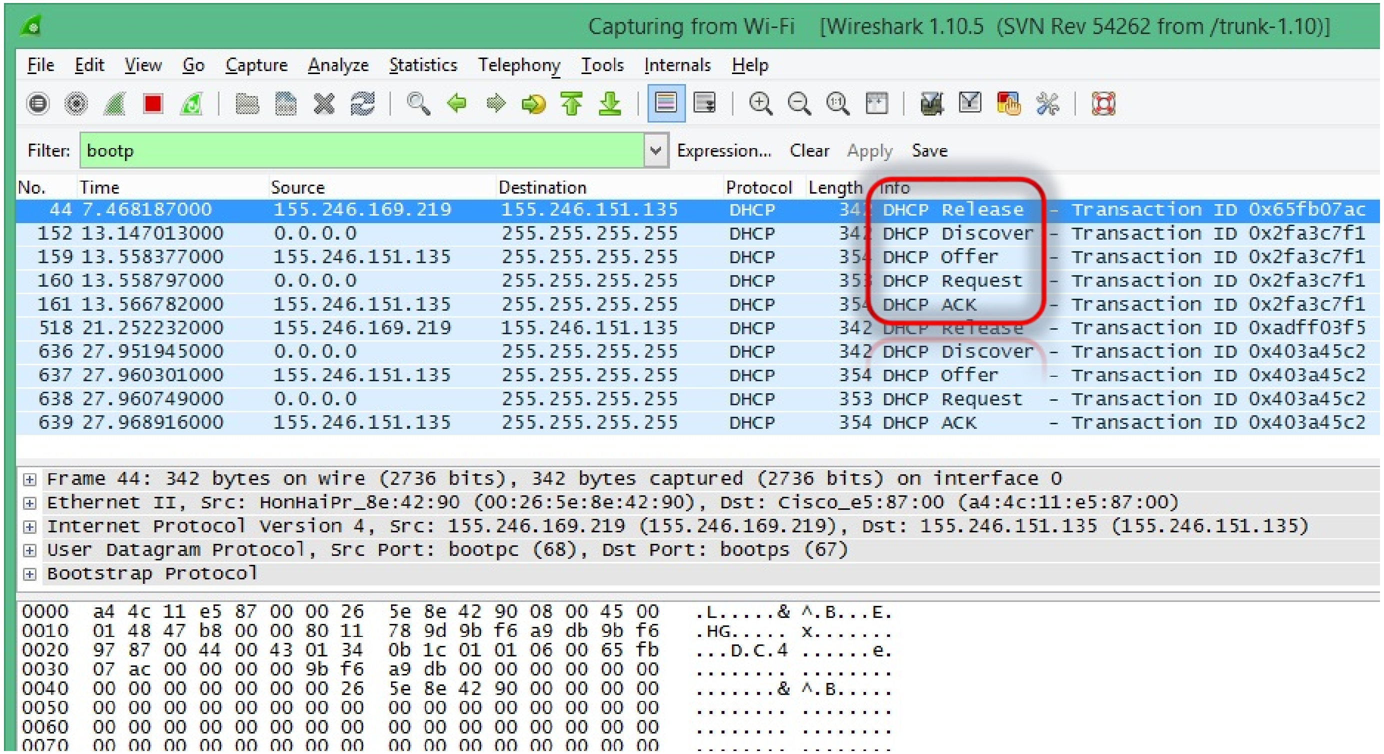
Filter: bootp

No.	Time	Source	Destination	Protocol	Length	Info
44	7.468187000	155.246.169.219	155.246.151.135	DHCP	342	DHCP Release - Transaction ID 0x65fb07ac
152	13.147013000	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x2fa3c7f1
159	13.558377000	155.246.151.135	255.255.255.255	DHCP	354	DHCP Offer - Transaction ID 0x2fa3c7f1
160	13.558797000	0.0.0.0	255.255.255.255	DHCP	353	DHCP Request - Transaction ID 0x2fa3c7f1
161	13.566782000	155.246.151.135	255.255.255.255	DHCP	354	DHCP ACK - Transaction ID 0x2fa3c7f1
518	21.252232000	155.246.169.219	155.246.151.135	DHCP	342	DHCP Release - Transaction ID 0xadff03f5
636	27.951945000	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x403a45c2
637	27.960301000	155.246.151.135	255.255.255.255	DHCP	354	DHCP Offer - Transaction ID 0x403a45c2
638	27.960749000	0.0.0.0	255.255.255.255	DHCP	353	DHCP Request - Transaction ID 0x403a45c2
639	27.968916000	155.246.151.135	255.255.255.255	DHCP	354	DHCP ACK - Transaction ID 0x403a45c2

```
⊞ Frame 44: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
⊞ Ethernet II, Src: HonHaiPr_8e:42:90 (00:26:5e:8e:42:90), Dst: Cisco_e5:87:00 (a4:4c:11:e5:87:00)
⊞ Internet Protocol Version 4, Src: 155.246.169.219 (155.246.169.219), Dst: 155.246.151.135 (155.246.151.135)
⊞ User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
⊞ Bootstrap Protocol
```

```
0000  a4 4c 11 e5 87 00 00 26  5e 8e 42 90 08 00 45 00   .L.....& ^.B...E.
0010  01 48 47 b8 00 00 80 11  78 9d 9b f6 a9 db 9b f6   .HG..... x.......
0020  97 87 00 44 00 43 01 34  0b 1c 01 01 06 00 65 fb   ...D.C.4 ......e.
0030  07 ac 00 00 00 00 9b f6  a9 db 00 00 00 00 00 00   ........ ........
0040  00 00 00 00 00 00 00 26  5e 8e 42 90 00 00 00 00   .......& ^.B.....
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   ........ ........
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
```

- We see from this Figure that the first “ipconfig/release” command caused four DHCP packets to be generated: a DHCP Discover packet, a DHCP Offer packet, a DHCP Request packet, and a DHCP ACK packet.



Capturing from Wi-Fi   [Wireshark 1.10.5 (SVN Rev 54262 from /trunk-1.10)]

Filter: bootp

```
No.  Time            Source            Destination       Protocol Length Info
  44 7.468187000     155.246.169.219   155.246.151.135   DHCP     342 DHCP Release  - Transaction ID 0x65fb07ac
 152 13.147013000    0.0.0.0           255.255.255.255   DHCP     342 DHCP Discover - Transaction ID 0x2fa3c7f1
 159 13.558377000    155.246.151.135   255.255.255.255   DHCP     354 DHCP Offer    - Transaction ID 0x2fa3c7f1
 160 13.558797000    0.0.0.0           255.255.255.255   DHCP     353 DHCP Request  - Transaction ID 0x2fa3c7f1
 161 13.566782000    155.246.151.135   255.255.255.255   DHCP     354 DHCP ACK      - Transaction ID 0x2fa3c7f1
 518 21.252232000    155.246.169.219   155.246.151.135   DHCP     342 DHCP Release  - Transaction ID 0xadff03f5
 636 27.951945000    0.0.0.0           255.255.255.255   DHCP     342 DHCP Discover - Transaction ID 0x403a45c2
 637 27.960301000    155.246.151.135   255.255.255.255   DHCP     354 DHCP Offer    - Transaction ID 0x403a45c2
 638 27.960749000    0.0.0.0           255.255.255.255   DHCP     353 DHCP Request  - Transaction ID 0x403a45c2
 639 27.968916000    155.246.151.135   255.255.255.255   DHCP     354 DHCP ACK      - Transaction ID 0x403a45c2
```

```
⊞ Frame 44: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
⊞ Ethernet II, Src: HonHaiPr_8e:42:90 (00:26:5e:8e:42:90), Dst: Cisco_e5:87:00 (a4:4c:11:e5:87:00)
⊞ Internet Protocol Version 4, Src: 155.246.169.219 (155.246.169.219), Dst: 155.246.151.135 (155.246.151.135)
⊞ User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
⊞ Bootstrap Protocol
```

```
0000  a4 4c 11 e5 87 00 00 26  5e 8e 42 90 08 00 45 00   .L.....& ^.B...E.
0010  01 48 47 b8 00 00 80 11  78 9d 9b f6 a9 db 9b f6   .HG..... x.......
0020  97 87 00 44 00 43 01 34  0b 1c 01 01 06 00 65 fb   ...D.C.4 ......e.
0030  07 ac 00 00 00 00 9b f6  a9 db 00 00 00 00 00 00   ........ ........
0040  00 00 00 00 00 00 00 26  5e 8e 42 90 00 00 00 00   .......& ^.B.....
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   ........ ........
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
```