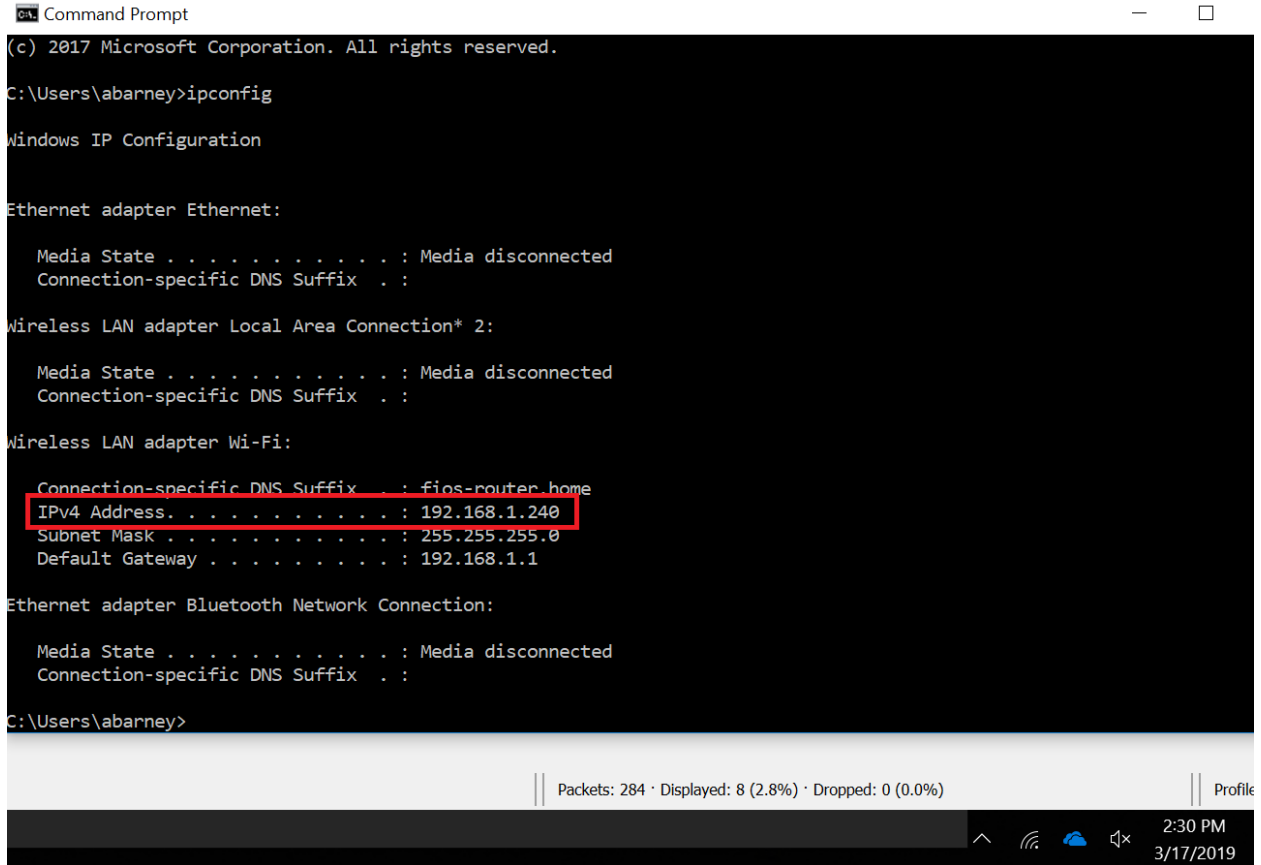


## Lab 4

IP Address: **192.168.1.240**



```
Command Prompt
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\abarney>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    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  . : fios-router.home
    IPv4 Address. . . . . : 192.168.1.240
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

Ethernet adapter Bluetooth Network Connection:

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

C:\Users\abarney>
```

Packets: 284 · Displayed: 8 (2.8%) · Dropped: 0 (0.0%)

2:30 PM  
3/17/2019

1. What is the IP address of your computer? Wireshark screenshot not, Terminal

**192.168.1.240**

\*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
23	2019-03-17 14:26:31.251954	192.168.1.240	92.242.140.21	HTTP	104	CCM_POST /bgb/handler.ashx?RequestType=LogIn
37	2019-03-17 14:26:34.713641	192.168.1.240	92.242.140.21	HTTP	549	GET /DeskAlerts//getalerts.aspx?uname=ABARNEY
42	2019-03-17 14:26:35.083104	92.242.140.21	192.168.1.240	HTTP	60	HTTP/1.1 200 OK (text/html)
147	2019-03-17 14:26:38.539009	192.168.1.240	128.119.245.12	HTTP	373	GET /wireshark-labs/HTTP-wireshark-file1.html
151	2019-03-17 14:26:38.725105	128.119.245.12	192.168.1.240	HTTP	540	HTTP/1.1 200 OK (text/html)
179	2019-03-17 14:26:39.067070	192.168.1.240	128.119.245.12	HTTP	295	GET /favicon.ico HTTP/1.1
181	2019-03-17 14:26:39.320071	128.119.245.12	192.168.1.240	HTTP	539	HTTP/1.1 404 Not Found (text/html)
188	2019-03-17 14:26:39.467673	128.119.245.12	192.168.1.240	HTTP	539	[TCP Spurious Retransmission] HTTP/1.1 404 Not Found

Internet Protocol Version 4, Src: 192.168.1.240, Dst: 128.119.245.12

- 0100 .... = Version: 4
- .... 0101 = Header Length: 20 bytes (5)
- > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 359
- Identification: 0x2842 (10306)
- > Flags: 0x4000, Don't fragment
- Time to live: 128
- Protocol: TCP (6)
- Header checksum: 0x9932 [validation disabled]
- [Header checksum status: Unverified]
- Source: 192.168.1.240
- Destination: 128.119.245.12
- > Transmission Control Protocol, Src Port: 54349, Dst Port: 80, Seq: 1, Ack: 1, Len: 319

0000 20 c0 47 e0 fe 66 14 ab c5 10 10 99 08 00 45 00 .G..f... ..E

0010 01 67 28 42 40 00 80 06 99 32 c0 a8 01 f0 80 77 g(B@... -2....w

0020 f5 0c d4 4d 00 50 3e 8a 23 a8 a8 7a 55 da 50 18 ...M.P>#..zU.P

0030 04 00 45 0e 00 00 47 45 54 20 2f 77 69 72 65 73 ..E...GE T /wires

0040 68 61 72 6b 2d 6c 61 62 73 2f 48 54 50 2d 77 hark-lab s/HTTP-w

0050 69 72 65 73 68 61 72 6b 2d 66 69 6c 65 31 2e 68 ireshark -file1.h

2:54 PM 3/17/2019

100%

2. What is the total length of the datagram?

**526 total length of datagram**

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
23	2019-03-17 14:26:31.251954	192.168.1.240	92.242.140.21	HTTP	104	CCM_POST /bgb/handler.ashx?RequestType
37	2019-03-17 14:26:34.713641	192.168.1.240	92.242.140.21	HTTP	549	GET /DeskAlerts//getalerts.aspx?uname:
42	2019-03-17 14:26:35.083104	92.242.140.21	192.168.1.240	HTTP	60	HTTP/1.1 200 OK (text/html)
147	2019-03-17 14:26:38.539009	192.168.1.240	128.119.245.12	HTTP	373	GET /wireshark-labs/HTTP-wireshark-fi
151	2019-03-17 14:26:38.725105	128.119.245.12	192.168.1.240	HTTP	540	HTTP/1.1 200 OK (text/html)
179	2019-03-17 14:26:39.067070	192.168.1.240	128.119.245.12	HTTP	295	GET /favicon.ico HTTP/1.1
181	2019-03-17 14:26:39.320071	128.119.245.12	192.168.1.240	HTTP	539	HTTP/1.1 404 Not Found (text/html)
188	2019-03-17 14:26:39.467673	128.119.245.12	192.168.1.240	HTTP	539	[TCP Spurious Retransmission] HTTP/1.

<

> Frame 151: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface 0

> Ethernet II, Src: Verizon\_e0:fe:66 (20:c0:47:e0:fe:66), Dst: IntelCor\_10:10:99 (14:ab:c5:10:10:99)

> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.240

0100 .... = Version: 4

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 526

Identification: 0x9996 (39318)

> Flags: 0x4000, Don't fragment

Time to live: 53

Protocol: TCP (6)

Header checksum: 0x7237 [validation disabled]

[Header checksum status: Unverified]

Source: 128.119.245.12

0010 02 0e 99 96 40 00 35 06 72 37 80 77 f5 0c c0 a8 ....C5- r7-w...

0020 01 f0 00 50 d4 4d a8 7a 55 da 3e 8a 24 e7 50 18 ...P-M-z U->\$-P-

0030 00 ed 9a e0 00 00 48 54 54 50 2f 31 2e 31 20 32 .....HT TP/1.1 2

0040 30 30 20 4f 4b 0d 0a 44 61 74 65 3a 20 53 75 6e 00 OK-D ate: Sun

0050 2c 20 31 37 20 4d 61 72 20 32 30 31 39 20 31 38 , 17 Mar 2019 18

0060 3a 32 36 3a 33 38 20 47 4d 54 0d 0a 53 65 72 76 :26:38 G MT-Serv

0070 65 72 3a 20 41 70 61 63 68 65 2f 32 2e 34 2e 36 er: Apac he/2.4.6

0080 20 28 43 65 6e 74 4f 53 29 20 4f 70 65 6e 53 53 (CentOS ) OpenSS

0090 4c 2f 31 2e 30 2e 32 6b 2d 66 69 70 73 20 50 48 L/1.0.2k -fips PH

0100 50 2f 33 2e 34 2e 31 38 20 6d 6f 64 5f 70 68 72 P/9.4.13 mod\_per

0110 6c 2f 32 2e 30 2e 31 30 20 50 65 72 6c 2f 76 35 1/2.0.10 Perl/v5

4:14 PM 3/17/2019

3. Has this IP datagram been fragmented?

**No, the more fragments flag has not been set.**

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
23	2019-03-17 14:26:31.251954	192.168.1.240	92.242.140.21	HTTP	104	CCM_POST /bgb/handler.ashx?RequestType=L
37	2019-03-17 14:26:34.713641	192.168.1.240	92.242.140.21	HTTP	549	GET /DeskAlerts//getalerts.aspx?uname=AB
42	2019-03-17 14:26:35.083104	92.242.140.21	192.168.1.240	HTTP	60	HTTP/1.1 200 OK (text/html)
147	2019-03-17 14:26:38.539009	192.168.1.240	128.119.245.12	HTTP	373	GET /wireshark-labs/HTTP-wireshark-file1
151	2019-03-17 14:26:38.725105	128.119.245.12	192.168.1.240	HTTP	540	HTTP/1.1 200 OK (text/html)
179	2019-03-17 14:26:39.067070	192.168.1.240	128.119.245.12	HTTP	295	GET /favicon.ico HTTP/1.1
181	2019-03-17 14:26:39.320071	128.119.245.12	192.168.1.240	HTTP	539	HTTP/1.1 404 Not Found (text/html)
188	2019-03-17 14:26:39.467673	128.119.245.12	192.168.1.240	HTTP	539	[TCP Spurious Retransmission] HTTP/1.1 4

0100 .... = Version: 4  
 .... 0101 = Header Length: 20 bytes (5)  
 > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
 Total Length: 526  
 Identification: 0x9996 (39318)  
 ✓ Flags: 0x4000, Don't fragment  
 0... .. = Reserved bit: Not set  
 .1... .. = Don't fragment: Set  
 ..0... .. = More fragments: Not set  
 ...0 0000 0000 0000 = Fragment offset: 0  
 Time to live: 53  
 Protocol: TCP (6)  
 Header checksum: 0x7237 [validation disabled]  
 [Header checksum status: Unverified]

0000 14 ab c5 10 10 99 20 c0 47 e0 fe 66 08 00 45 00 ... G f E  
 0010 02 00 00 00 00 00 00 00 00 00 00 00 00 00 ... 0 0 0 0

3:13 PM  
 3/17/2019

4. How many bytes are in the IP header?

**20 bytes in the IP header.**

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
23	2019-03-17 14:26:31.251954	192.168.1.240	92.242.140.21	HTTP	104	CCM_POST /bgb/handler.ashx?Req
37	2019-03-17 14:26:34.713641	192.168.1.240	92.242.140.21	HTTP	549	GET /DeskAlerts//getalerts.asp
42	2019-03-17 14:26:35.083104	92.242.140.21	192.168.1.240	HTTP	60	HTTP/1.1 200 OK (text/html)
147	2019-03-17 14:26:38.539009	192.168.1.240	128.119.245.12	HTTP	373	GET /wireshark-labs/HTTP-wires
151	2019-03-17 14:26:38.725105	128.119.245.12	192.168.1.240	HTTP	540	HTTP/1.1 200 OK (text/html)
179	2019-03-17 14:26:39.067070	192.168.1.240	128.119.245.12	HTTP	295	GET /favicon.ico HTTP/1.1
181	2019-03-17 14:26:39.320071	128.119.245.12	192.168.1.240	HTTP	539	HTTP/1.1 404 Not Found (text/
188	2019-03-17 14:26:39.467673	128.119.245.12	192.168.1.240	HTTP	539	[TCP Spurious Retransmission]

<

> Frame 151: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface 0

> Ethernet II, Src: Verizon\_e0:fe:66 (20:c0:47:e0:fe:66), Dst: IntelCor\_10:10:99 (14:ab:c5:10:10:99)

▼ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.240

0100 .... = Version: 4

... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 526

Identification: 0x9996 (39318)

▼ Flags: 0x4000, Don't fragment

0 .... = Reserved bit: Not set

.1... .... = Don't fragment: Set

0 .... = More fragments: Not set

3:23 PM 3/17/2019

5. How many bytes are in the payload of the IP datagram? Explain how you determine the number of payload bytes

506 in the payload of the IP datagram (Total length of 526, subtract 20 for the header)

\*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
23	2019-03-17 14:26:31.251954	192.168.1.240	92.242.140.21	HTTP	104	CCM_POST /bgb/handler.ashx?RequestType=Log
37	2019-03-17 14:26:34.713641	192.168.1.240	92.242.140.21	HTTP	549	GET /DeskAlerts//getalerts.aspx?uname=ABAR
42	2019-03-17 14:26:35.083104	92.242.140.21	192.168.1.240	HTTP	60	HTTP/1.1 200 OK (text/html)
147	2019-03-17 14:26:38.539009	192.168.1.240	128.119.245.12	HTTP	373	GET /wireshark-labs/HTTP-wireshark-file1.h
151	2019-03-17 14:26:38.725105	128.119.245.12	192.168.1.240	HTTP	540	HTTP/1.1 200 OK (text/html)
179	2019-03-17 14:26:39.067070	192.168.1.240	128.119.245.12	HTTP	295	GET /favicon.ico HTTP/1.1
181	2019-03-17 14:26:39.320071	128.119.245.12	192.168.1.240	HTTP	539	HTTP/1.1 404 Not Found (text/html)
188	2019-03-17 14:26:39.467673	128.119.245.12	192.168.1.240	HTTP	539	[TCP Spurious Retransmission] HTTP/1.1 404

<

> Frame 151: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface 0

> Ethernet II, Src: Verizon\_e0:fe:66 (20:c0:47:e0:fe:66), Dst: IntelCor\_10:10:99 (14:ab:c5:10:10:99)

✓ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.240

0100 .... = Version: 4

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 526

Identification: 0x9996 (39318)

> Flags: 0x4000, Don't fragment

Time to live: 53

Protocol: TCP (6)

Header checksum: 0x7237 [validation disabled]

[Header checksum status: Unverified]

Source: 128.119.245.12

0010 02 0e 99 96 40 00 35 06 72 37 80 77 f5 0c c0 a8 ...@.5. r7.w....

0020 01 f0 00 50 d4 4d a8 7a 55 da 3e 8a 24 e7 50 18 ...P.M.z U->\$.P.

0030 00 ed 9a e0 00 00 48 54 54 50 2f 31 2e 31 20 32 .....HT TP/1.1 2

0040 30 30 20 4f 4b 0d 0a 44 61 74 65 3a 20 53 75 6e 00 OK -D ate: Sun

0050 2c 20 31 37 20 4d 61 72 20 32 30 31 39 20 31 38 , 17 Mar 2019 18

0060 3a 32 36 3a 33 38 20 47 4d 54 0d 0a 53 65 72 76 :26:38 G MT Serv

3:43 PM 3/17/2019

No.	Time	Source	Destination	Protocol	Length	Info
151	2019-03-17 14:26:38.725105	128.119.245.12	192.168.1.240	HTTP	540	HTTP/1.1 200 OK (text/html)

Frame 151: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface 0  
 Ethernet II, Src: Verizon\_e0:fe:66 (20:c0:47:e0:fe:66), Dst: IntelCor\_10:10:99 (14:ab:c5:10:10:99)  
 Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.240  
 0100 .... = Version: 4  
 .... 0101 = Header Length: 20 bytes (5)  
 Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
 Total Length: 526  
 Identification: 0x9996 (39318)  
 Flags: 0x4000, Don't fragment  
   0... .... = Reserved bit: Not set  
   .1.. .... = Don't fragment: Set  
   ..0. .... = More fragments: Not set  
   ...0 0000 0000 0000 = Fragment offset: 0  
 Time to live: 53  
 Protocol: TCP (6)  
 Header checksum: 0x7237 [validation disabled]  
 [Header checksum status: Unverified]  
 Source: 128.119.245.12  
 Destination: 192.168.1.240  
 Transmission Control Protocol, Src Port: 80, Dst Port: 54349, Seq: 1, Ack: 320, Len: 486  
 Hypertext Transfer Protocol  
 Line-based text data: text/html (4 lines)