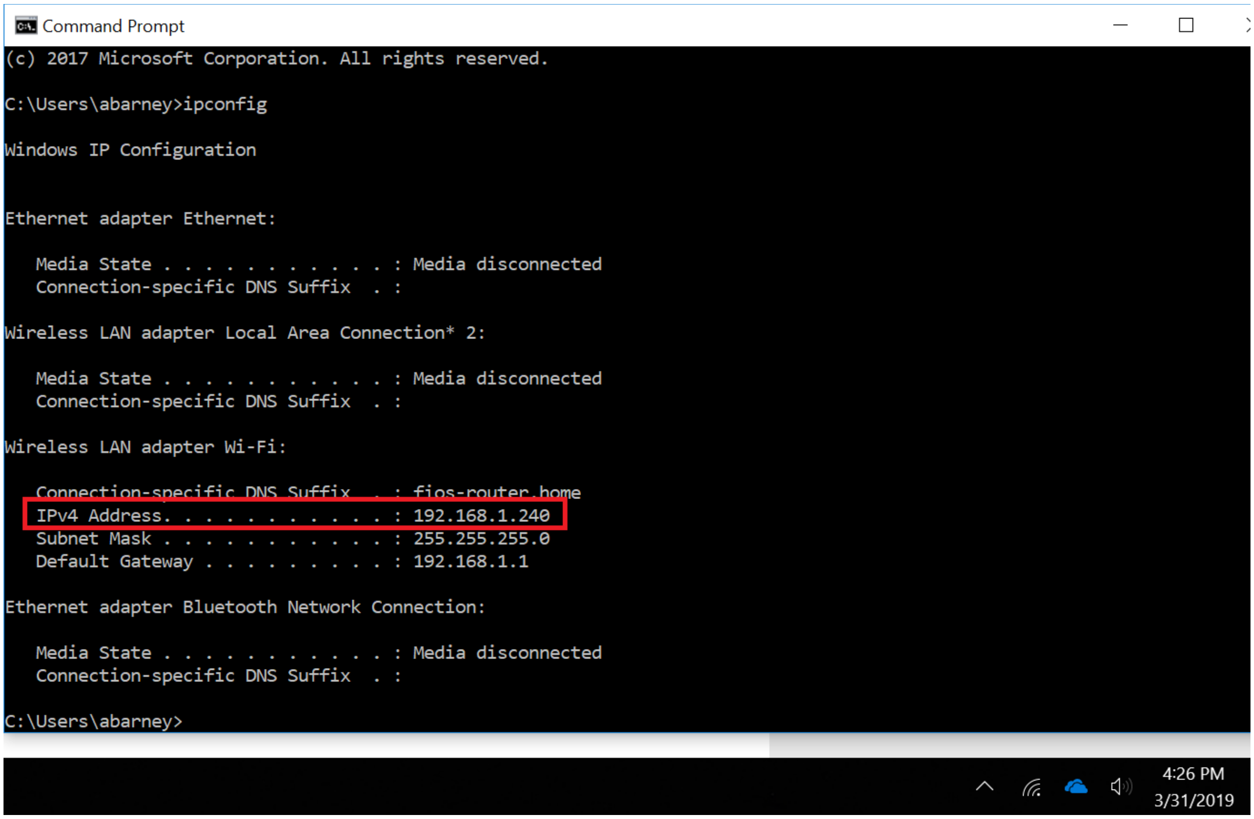
Lab 6

Computers IP Address?

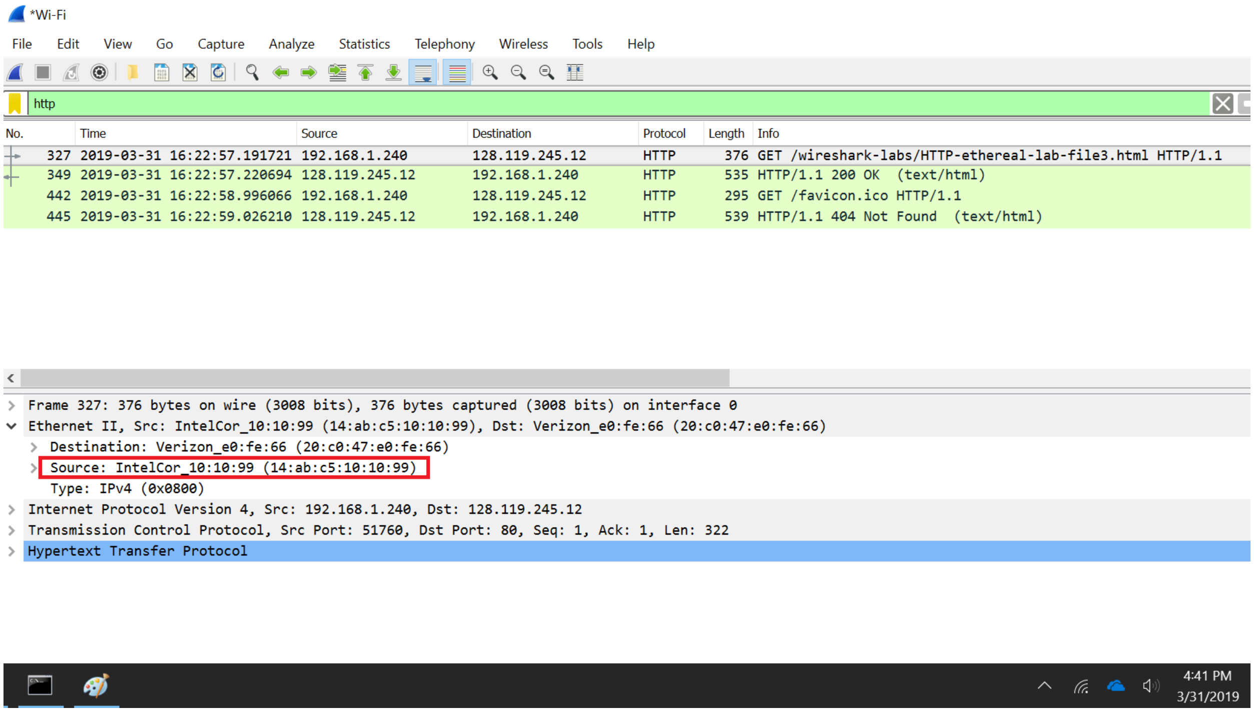
IP Address 192.168.1.240



```
(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>
```

1. What is the MAC address from your computer?

   14:AB:C5:10:10:99

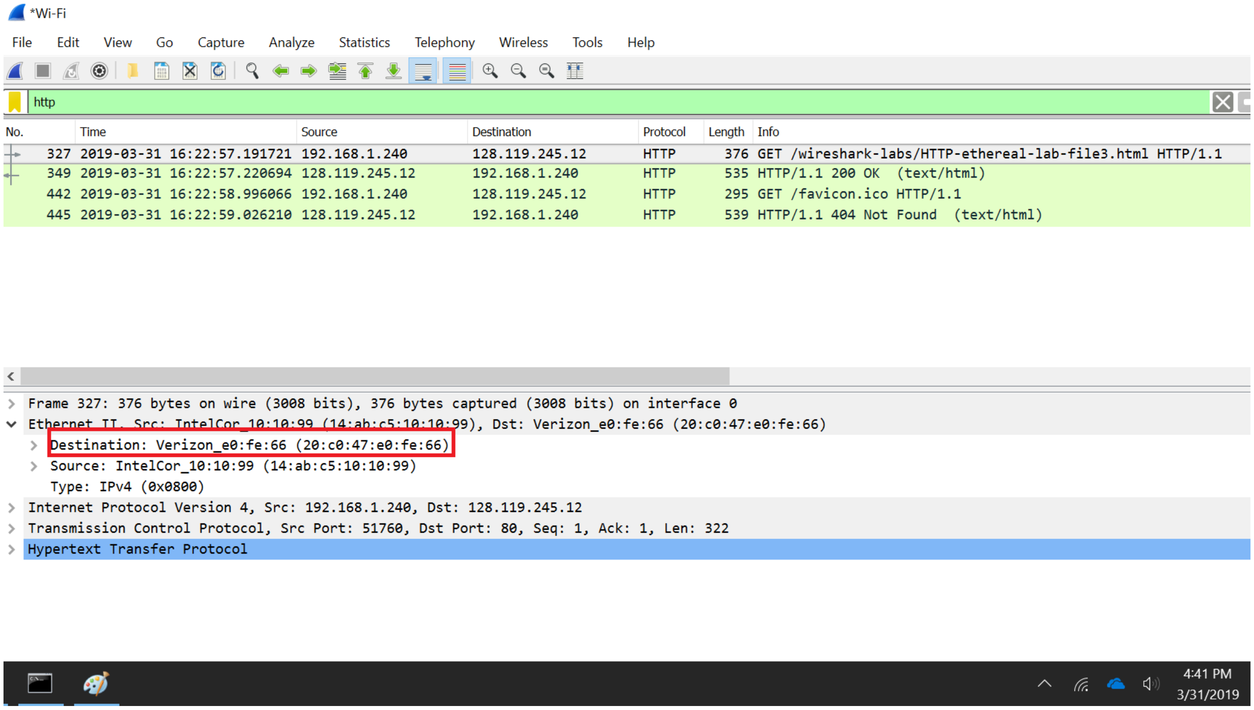


```
No.   Time                        Source          Destination     Protocol Length Info
  327 2019-03-31 16:22:57.191721 192.168.1.240   128.119.245.12  HTTP      376 GET /wireshark-labs/HTTP-ethereal-lab-file3.html HTTP/1.1
  349 2019-03-31 16:22:57.220694 128.119.245.12  192.168.1.240   HTTP      535 HTTP/1.1 200 OK  (text/html)
  442 2019-03-31 16:22:58.996066 192.168.1.240   128.119.245.12  HTTP      295 GET /favicon.ico HTTP/1.1
  445 2019-03-31 16:22:59.026210 128.119.245.12  192.168.1.240   HTTP      539 HTTP/1.1 404 Not Found  (text/html)
```

```
> Frame 327: 376 bytes on wire (3008 bits), 376 bytes captured (3008 bits) on interface 0
v Ethernet II, Src: IntelCor_10:10:99 (14:ab:c5:10:10:99), Dst: Verizon_e0:fe:66 (20:c0:47:e0:fe:66)
  > Destination: Verizon_e0:fe:66 (20:c0:47:e0:fe:66)
  > Source: IntelCor_10:10:99 (14:ab:c5:10:10:99)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 192.168.1.240, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 51760, Dst Port: 80, Seq: 1, Ack: 1, Len: 322
> Hypertext Transfer Protocol
```

2. What is the destination MAC address?

10:C0:47:E0:FE:66



```
No.   Time                        Source          Destination     Protocol Length Info
  327 2019-03-31 16:22:57.191721 192.168.1.240   128.119.245.12  HTTP      376 GET /wireshark-labs/HTTP-ethereal-lab-file3.html HTTP/1.1
  349 2019-03-31 16:22:57.220694 128.119.245.12  192.168.1.240   HTTP      535 HTTP/1.1 200 OK  (text/html)
  442 2019-03-31 16:22:58.996066 192.168.1.240   128.119.245.12  HTTP      295 GET /favicon.ico HTTP/1.1
  445 2019-03-31 16:22:59.026210 128.119.245.12  192.168.1.240   HTTP      539 HTTP/1.1 404 Not Found  (text/html)
```

```
> Frame 327: 376 bytes on wire (3008 bits), 376 bytes captured (3008 bits) on interface 0
v Ethernet II, Src: IntelCor_10:10:99 (14:ab:c5:10:10:99), Dst: Verizon_e0:fe:66 (20:c0:47:e0:fe:66)
  > Destination: Verizon_e0:fe:66 (20:c0:47:e0:fe:66)
  > Source: IntelCor_10:10:99 (14:ab:c5:10:10:99)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 192.168.1.240, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 51760, Dst Port: 80, Seq: 1, Ack: 1, Len: 322
> Hypertext Transfer Protocol
```

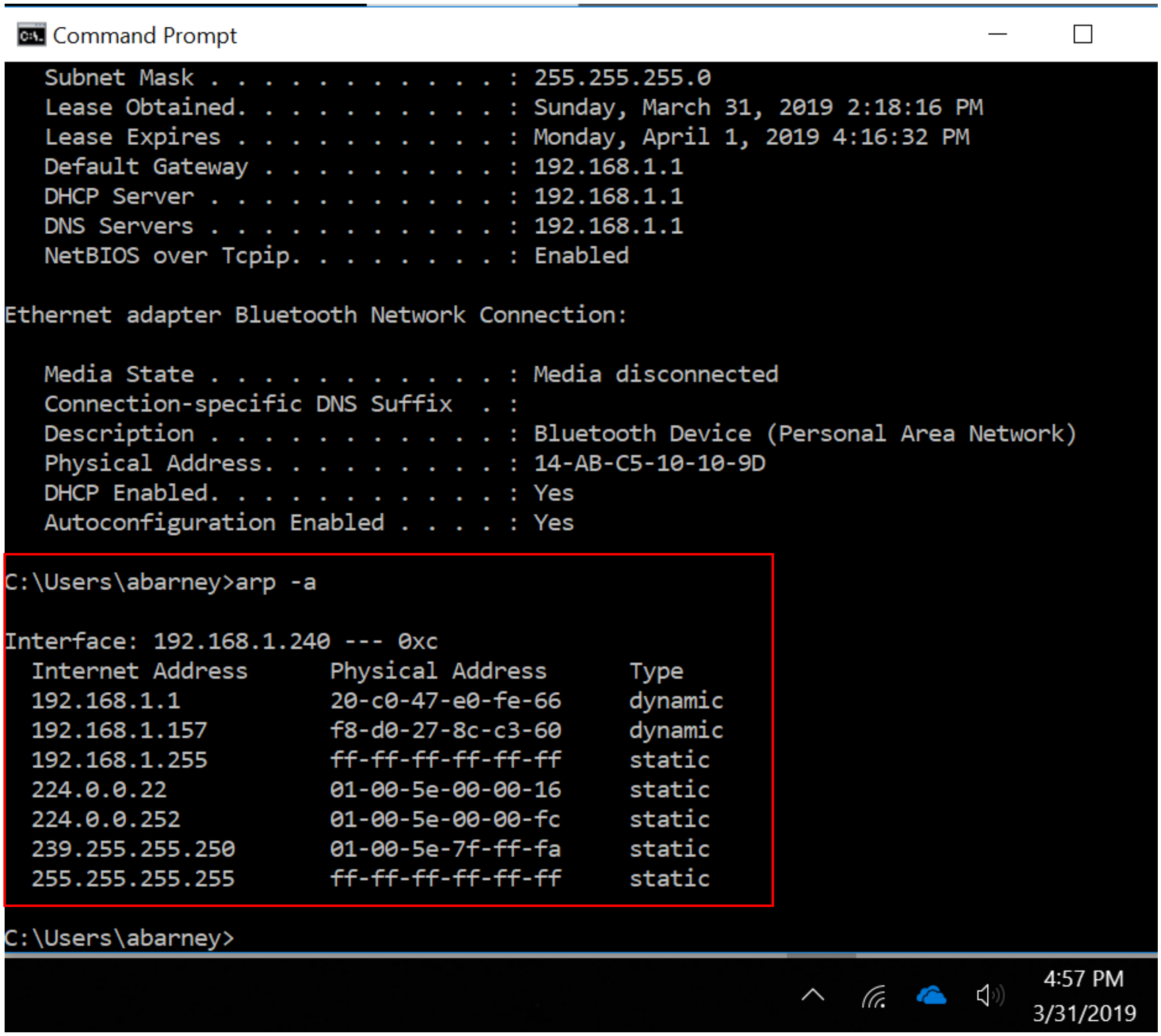
3. What device has the MAC address shown in the destination?

The first hop router, that is the Verizon ISP.

4. Explain the relationship between the destination MAC address and the destination IP address.

   The destination MAC address resides at layer 2, the destination IP resides at layer 3. The sender of the datagram needs to have both the destination IP and MAC address in its ARP table.

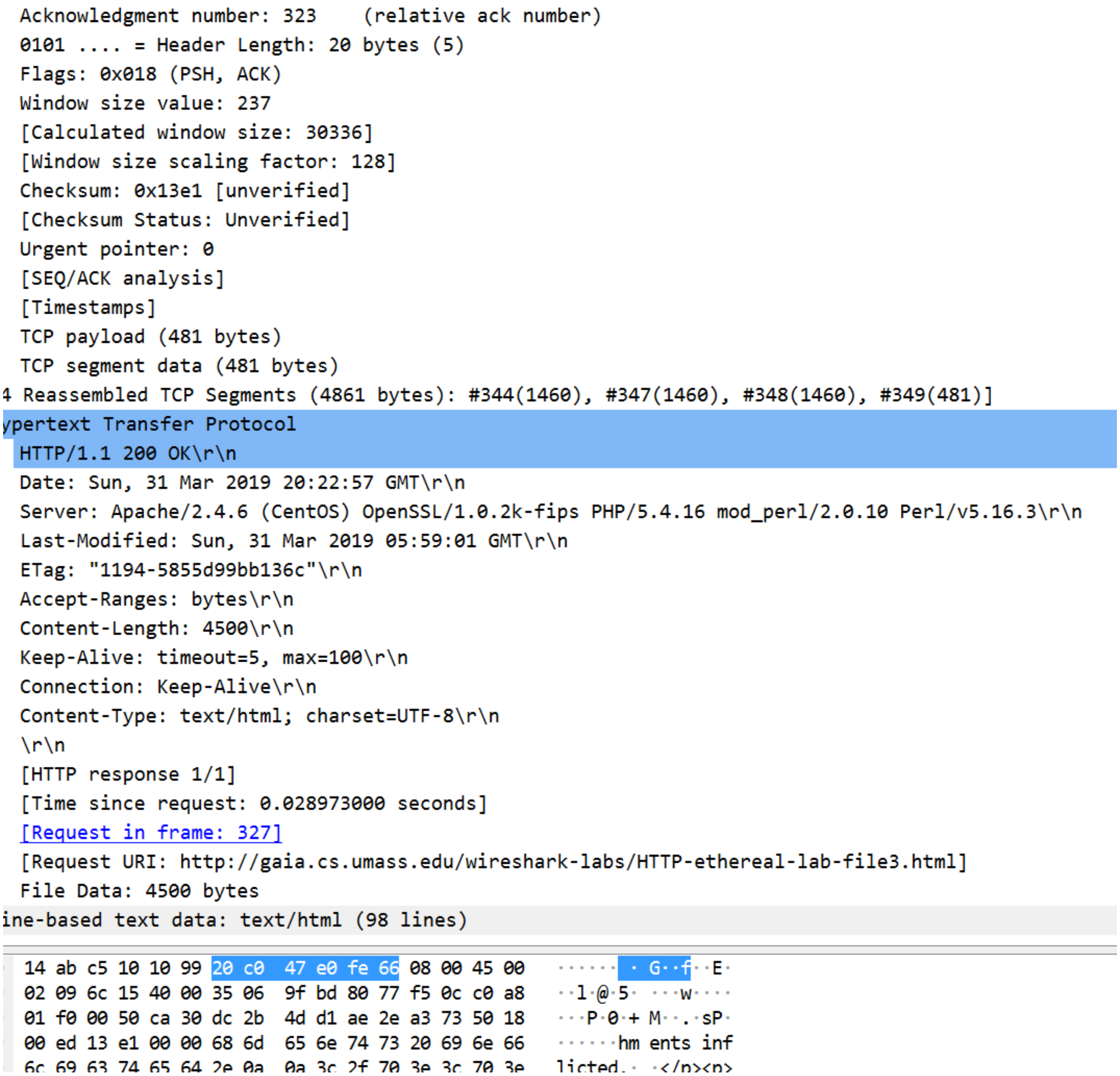
5. Using the terminal (cmd in Windows, Terminal in mac), run a command to display your full ARP list table. (Find out what the command is, and print a full screen shot of your result.)



```
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Sunday, March 31, 2019 2:18:16 PM
   Lease Expires . . . . . . . . . . : Monday, April 1, 2019 4:16:32 PM
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DNS Servers . . . . . . . . . . . : 192.168.1.1
   NetBIOS over Tcpip. . . . . . . . : Enabled

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Bluetooth Device (Personal Area Network)
   Physical Address. . . . . . . . . : 14-AB-C5-10-10-9D
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

C:\Users\abarney>arp -a

Interface: 192.168.1.240 --- 0xc
  Internet Address      Physical Address      Type
  192.168.1.1           20-c0-47-e0-fe-66     dynamic
  192.168.1.157         f8-d0-27-8c-c3-60     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\Users\abarney>
```

HTTP OK Print Out

```
No.     Time                          Source                Destination           Protocol Length Info
    349 2019-03-31 16:22:57.220694    128.119.245.12        192.168.1.240         HTTP     535    HTTP/1.1 200 OK  (text/html)
Frame 349: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface 0
    Interface id: 0 (\Device\NPF_{CBB16A1D-9E20-4EC2-82CA-4F266162421A})
        Interface name: \Device\NPF_{CBB16A1D-9E20-4EC2-82CA-4F266162421A}
    Encapsulation type: Ethernet (1)
    Arrival Time: Mar 31, 2019 16:22:57.220694000 Eastern Daylight Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1554063777.220694000 seconds
    [Time delta from previous captured frame: 0.000002000 seconds]
    [Time delta from previous displayed frame: 0.028973000 seconds]
    [Time since reference or first frame: 5.230534000 seconds]
    Frame Number: 349
    Frame Length: 535 bytes (4280 bits)
    Capture Length: 535 bytes (4280 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http:data-text-lines]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
Ethernet II, Src: Verizon_e0:fe:66 (20:c0:47:e0:fe:66), Dst: IntelCor_10:10:99 (14:ab:c5:10:10:99)
    Destination: IntelCor_10:10:99 (14:ab:c5:10:10:99)
        Address: IntelCor_10:10:99 (14:ab:c5:10:10:99)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source: Verizon_e0:fe:66 (20:c0:47:e0:fe:66)
        Address: Verizon_e0:fe:66 (20:c0:47:e0:fe:66)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
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)
        0000 00.. = Differentiated Services Codepoint: Default (0)
        .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 521
    Identification: 0x6c15 (27669)
    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: 0x9fbd [validation disabled]
    [Header checksum status: Unverified]
    Source: 128.119.245.12
    Destination: 192.168.1.240
Transmission Control Protocol, Src Port: 80, Dst Port: 51760, Seq: 4381, Ack: 323, Len: 481
    Source Port: 80
    Destination Port: 51760
    [Stream index: 28]
    [TCP Segment Len: 481]
    Sequence number: 4381    (relative sequence number)
    [Next sequence number: 4862    (relative sequence number)]
```



```
  Acknowledgment number: 323    (relative ack number)
  0101 .... = Header Length: 20 bytes (5)
  Flags: 0x018 (PSH, ACK)
  Window size value: 237
  [Calculated window size: 30336]
  [Window size scaling factor: 128]
  Checksum: 0x13e1 [unverified]
  [Checksum Status: Unverified]
  Urgent pointer: 0
  [SEQ/ACK analysis]
  [Timestamps]
  TCP payload (481 bytes)
  TCP segment data (481 bytes)
4 Reassembled TCP Segments (4861 bytes): #344(1460), #347(1460), #348(1460), #349(481)]
ypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
  Date: Sun, 31 Mar 2019 20:22:57 GMT\r\n
  Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
  Last-Modified: Sun, 31 Mar 2019 05:59:01 GMT\r\n
  ETag: "1194-5855d99bb136c"\r\n
  Accept-Ranges: bytes\r\n
  Content-Length: 4500\r\n
  Keep-Alive: timeout=5, max=100\r\n
  Connection: Keep-Alive\r\n
  Content-Type: text/html; charset=UTF-8\r\n
  \r\n
  [HTTP response 1/1]
  [Time since request: 0.028973000 seconds]
  [Request in frame: 327]
  [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-ethereal-lab-file3.html]
  File Data: 4500 bytes
ine-based text data: text/html (98 lines)

  14 ab c5 10 10 99 20 c0  47 e0 fe 66 08 00 45 00   ······ ·G··f··E·
  02 09 6c 15 40 00 35 06  9f bd 80 77 f5 0c c0 a8   ··l·@·5· ···w····
  01 f0 00 50 ca 30 dc 2b  4d d1 ae 2e a3 73 50 18   ···P·0·+ M··.·sP·
  00 ed 13 e1 00 00 68 6d  65 6e 74 73 20 69 6e 66   ······hm ents inf
  6c 69 63 74 65 64 2e 0a  0a 3c 2f 70 3e 3c 70 3e   licted.· ·</p><p>
```