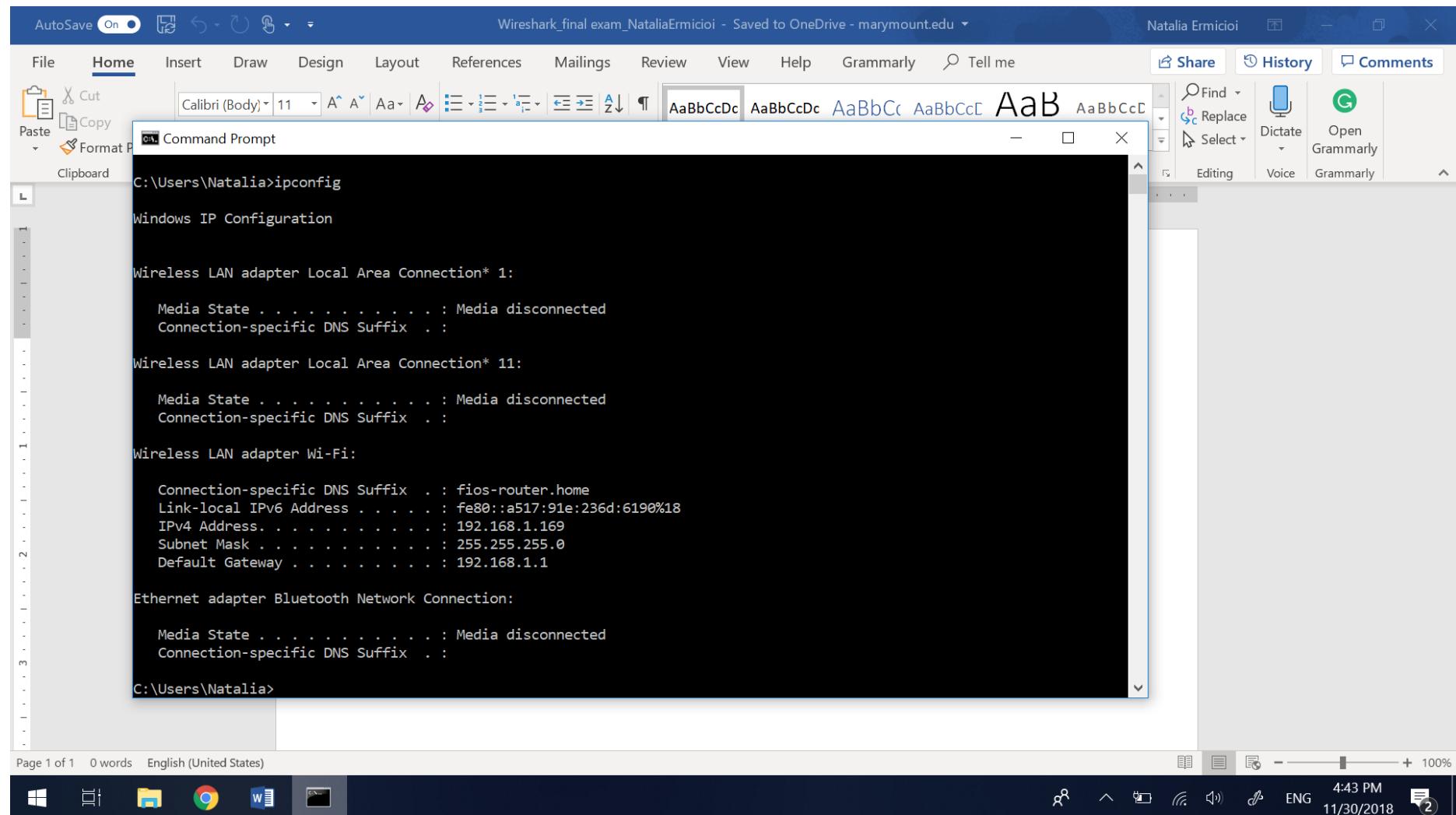


## Wireshark – Final – Natalia Ermicioi

IP address: 192.168.1.169



The screenshot shows a Microsoft Word document window titled "Wireshark\_final exam\_NataliaErmicioi - Saved to OneDrive - marymount.edu". The document contains the output of the "ipconfig" command run from the Windows Command Prompt. The output shows network configuration details for several adapters, including Local Area Connection\* 1, Local Area Connection\* 11, and Wi-Fi. The IP address 192.168.1.169 is listed under the Wi-Fi adapter's IPv4 Address.

```
C:\Users\Natalia>ipconfig

Windows IP Configuration

Wireless LAN adapter Local Area Connection* 1:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . .

Wireless LAN adapter Local Area Connection* 11:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . .

Wireless LAN adapter Wi-Fi:
  Connection-specific DNS Suffix . : fios-router.home
  Link-local IPv6 Address . . . . : fe80::a517:91e:236d:6190%18
  IPv4 Address . . . . . : 192.168.1.169
  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\Natalia>
```

1. 1. How many HTTP GET request messages did your browser send?

Answer: 1

Which packet number in the trace contains the GET message for the Bill or Rights?

Answer: 4799

The screenshot shows a Wireshark interface with the following details:

- Network Interface:** \*Wi-Fi
- Selected Protocol:** http
- Packets:** 4882 · Displayed: 236 (4.8%) · Dropped: 0 (0.0%)
- Selected Packet:** 4799 (GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1)
- Protocol Tree:** Shows the structure of the selected HTTP request, including headers like Accept, Accept-Language, User-Agent, Accept-Encoding, Host, and Connection.
- Hex Editor:** Shows the raw hex and ASCII representation of the selected packet.
- Bottom Status Bar:** Profile: Default, 5:16 PM, 11/30/2018, battery level, signal strength, and network status.

2. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?

Answer: 4804

The screenshot shows a Wireshark capture window titled '\*Wi-Fi'. The main pane displays a list of network packets. Packet 4804 is selected, showing an HTTP response from 192.168.1.169 to 128.119.245.12. The 'Info' column for this packet shows 'HTTP/1.1 200 OK (text/html)'. Below the list, the packet details, bytes, and hex panes are visible. The details pane shows the full HTTP response message:

```
> HTTP/1.1 200 OK\r\nDate: Fri, 30 Nov 2018 22:12:46 GMT\r\nServer: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\nLast-Modified: Fri, 30 Nov 2018 06:59:01 GMT\r\nETag: "1194-57bdc558d3a40"\r\nAccept-Ranges: bytes\r\nContent-Length: 4500\r\n
```

The bytes and hex panes show the raw binary data corresponding to the captured frame.

At the bottom, the status bar indicates: 'Frame (535 bytes) Reassembled TCP (4861 bytes)', 'Packets: 4882 · Displayed: 236 (4.8%) · Dropped: 0 (0.0%)', 'Profile: Default', and the system clock '5:26 PM 11/30/2018'.

3. What is the status code and phrase in the response?

Answer: 4804 1543615966.714486 128.119.245.12      192.168.1.169 HTTP 535      HTTP/1.1 200 OK (text/html)

The screenshot shows the Wireshark interface with the following details:

- Network Interface:** \*Wi-Fi
- Selected Filter:** http
- Packets List:** Shows a list of 236 selected packets. The packet at index 4804 is highlighted, which corresponds to the answer provided.
- Packet Details:** The selected packet (4804) is shown in detail:
  - Protocol: HTTP
  - Length: 535 bytes
  - Info: HTTP/1.1 200 OK (text/html)
- HTTP Headers:** The response includes the following headers:

```
Date: Fri, 30 Nov 2018 22:12:46 GMT\r\nServer: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\nLast-Modified: Fri, 30 Nov 2018 06:59:01 GMT\r\nETag: "1194-57bcd558d3a40"\r\nAccept-Ranges: bytes\r\nContent-Length: 4500\r\n
```
- Hex and ASCII Data:** The payload of the packet is displayed in hex and ASCII formats.
- Bottom Status Bar:** Shows the total number of packets (4882), displayed packets (236), dropped packets (0), and the profile (Default). It also shows the system date and time (5:26 PM, 11/30/2018).

4. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?

Answer: Four (4) TCP – 4801; 4802; 4803; 4804.

The screenshot shows a Wireshark capture window titled "http". The main pane displays a list of network frames, with frame 4804 selected. The details pane shows the frame structure:

- Frame 4804: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface 0
- Ethernet II, Src: Verizon\_33:7d:4f (48:5d:36:33:7d:4f), Dst: IntelCor\_fb:ab:3f (44:03:2c:fb:ab:3f)
- Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.169
- Transmission Control Protocol, Src Port: 80, Dst Port: 54669, Seq: 4381, Ack: 342, Len: 481

The expanded section "[4 Reassembled TCP Segments (4861 bytes): #4801(1460), #4802(1460), #4803(1460), #4804(481)]" shows the four segments:

- [Frame: 4801, payload: 0-1459 (1460 bytes)]
- [Frame: 4802, payload: 1460-2919 (1460 bytes)]
- [Frame: 4803, payload: 2920-4379 (1460 bytes)]
- [Frame: 4804, payload: 4380-4860 (481 bytes)]

The bytes pane shows the raw hex and ASCII data for the reassembled TCP segment:

|  |                   |
|--|-------------------|
| 0000 44 03 2c fb ab 3f 48 5d 36 33 7d 4f 08 00 45 00 | D,..?H] 63}0 ·E·  |
| 0010 02 09 5e 84 40 00 35 06 ad 95 80 77 f5 0c c0 a8 | ..^@ 5 ..W...     |
| 0020 01 a9 00 50 d5 8d 6c 75 50 bd 63 86 59 7e 50 18 | ...P..lu P:c~P~   |
| 0030 00 ed 0a 33 00 00 68 6d 65 6e 74 73 20 69 6e 66 | ...3..hm ents inf |
| 0040 6c 69 63 74 65 64 2e 0a 0a 3c 2f 70 3e 3c 70 3e | lited.. ~</p><p>  |
| 0050 3c 61 20 6e 61 6d 65 3d 22 39 22 3e 3c 73 74 72 | <a name= "9"><str |
| 0060 6f 6e 67 3e 3c 68 33 3e 41 6d 65 6e 64 6d 65 6e | ong><h3> Amendmen |

At the bottom, the status bar shows: Frame (535 bytes) Reassembled TCP (4861 bytes). The footer includes: Packets: 4882 · Displayed: 236 (4.8%) · Dropped: 0 (0.0%) · Profile: Default. The system tray shows the date and time: 5:32 PM 11/30/2018.

5. What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser?

Answer: 6167 1543617354.115485 128.119.245.12      192.168.1.169 HTTP 771      HTTP/1.1 401 Unauthorized (text/html)

The screenshot shows the Wireshark interface with the following details:

- Selected Packet:** Frame 6167 (HTTP/1.1 401 Unauthorized (text/html))
- Details Pane:** Shows the selected packet's details, including:
  - Frame 6167: 771 bytes on wire (6168 bits), 771 bytes captured (6168 bits) on interface 0
  - Ethernet II, Src: Verizon\_33:7d:4f (48:5d:36:33:7d:4f), Dst: IntelCor\_fb:ab:3f (44:03:2c:fb:ab:3f)
  - Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.169
  - Transmission Control Protocol, Src Port: 80, Dst Port: 55032, Seq: 1, Ack: 358, Len: 717
  - Hypertext Transfer Protocol
  - Line-based text data: text/html (12 lines)
- Hex and ASCII Panes:** Below the details pane, the hex and ASCII panes show the raw data of the selected packet.
- Bottom Status Bar:** Shows Packets: 6300 · Displayed: 336 (5.3%) · Dropped: 0 (0.0%) · Profile: Default.
- Taskbar:** Shows various application icons (Windows, File Explorer, Google Chrome, Microsoft Word, Paint, Internet Explorer) and system status indicators (Wi-Fi, battery, volume, network, date/time).

6. When your browser sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?

Answer: Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=

Credentials: wireshark-students:network

The screenshot shows a Wireshark capture window titled "http". The packet list pane displays several HTTP requests. The selected packet is number 219, which is a GET request to "http://gaia.cs.umass.edu/wireshark-labs/protected\_pages/HTTP-wireshark-file5.html". The details pane shows the request headers:

```
Request Version: HTTP/1.1
Accept: text/html, application/xhtml+xml, image/jxr, */*\r\n
Accept-Language: en-US,en;q=0.8,ro-RO;q=0.5,ro;q=0.3\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; Touch; rv:11.0) like Gecko\r\n
Accept-Encoding: gzip, deflate\r\n
Host: gaia.cs.umass.edu\r\n
Connection: Keep-Alive\r\n
Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
    Credentials: wireshark-students:network\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html]
```

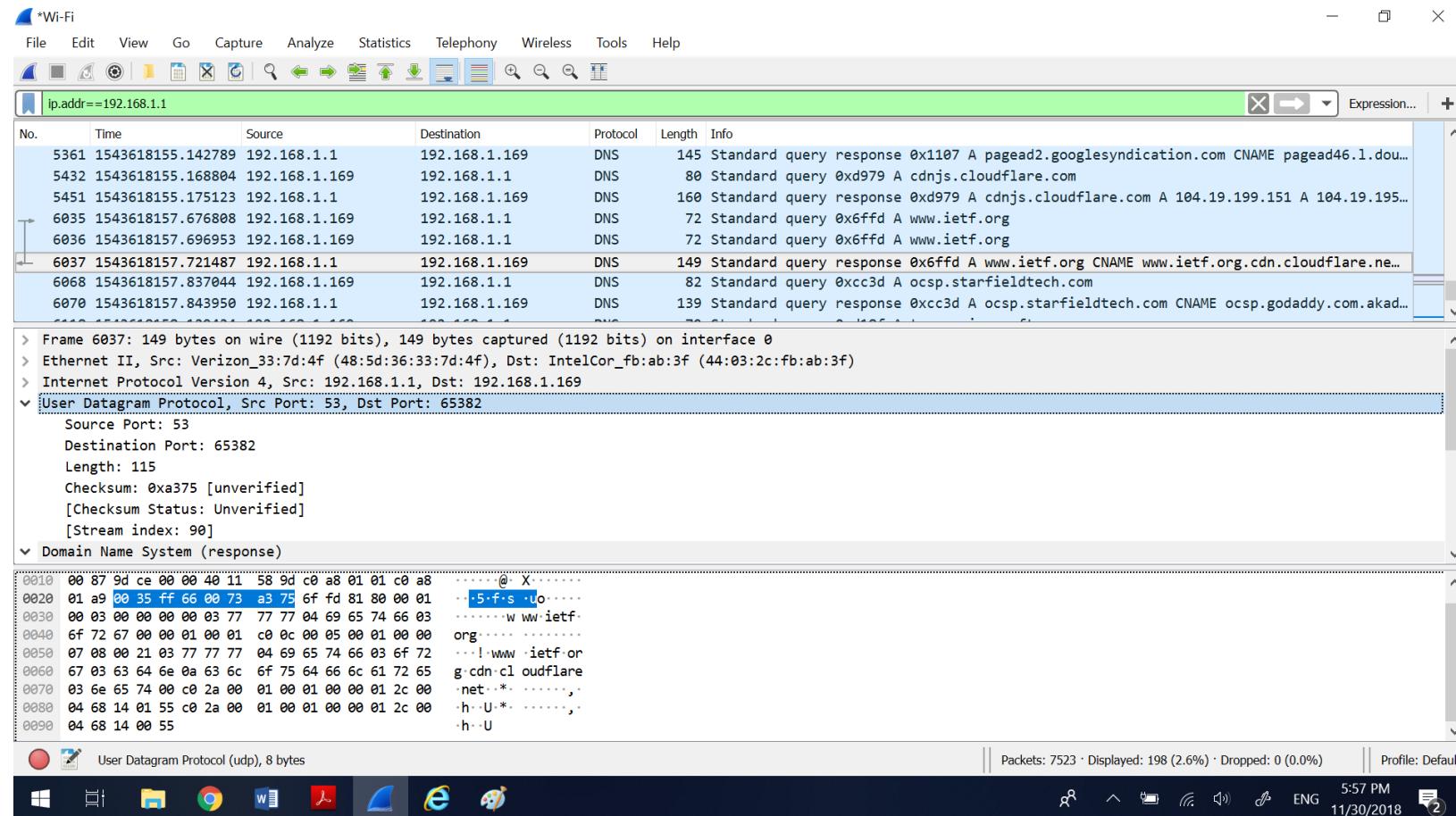
The bytes pane at the bottom shows the raw hex and ASCII data for the selected packet.

7. Locate the DNS query and response messages. Are they sent over UDP or TCP?

Answer: 6035 1543618157.676808 192.168.1.169 192.168.1.1 DNS 72 Standard query 0x6ffd A [www.ietf.org](http://www.ietf.org)

6037 1543618157.721487 192.168.1.1 192.168.1.169 DNS 149 Standard query response 0x6ffd A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.20.1.85 A 104.20.0.85

They are sent over UDP.



8. What is the destination port for the DNS query message?

Answer: Destination Port: 53 for Dst: 192.168.1.1

\*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr==192.168.1.1

| No.  | Time              | Source        | Destination   | Protocol | Length | Info   |
|------|-------------------|---------------|---------------|----------|--------|--|
| 5361 | 1543618155.142789 | 192.168.1.1   | 192.168.1.169 | DNS      | 145    | Standard query response 0x1107 A pagead2.googlesyndication.com CNAME pagead46.1.dou... |
| 5432 | 1543618155.168804 | 192.168.1.169 | 192.168.1.1   | DNS      | 80     | Standard query 0xd979 A cdnjs.cloudflare.com   |
| 5451 | 1543618155.175123 | 192.168.1.1   | 192.168.1.169 | DNS      | 160    | Standard query response 0xd979 A cdnjs.cloudflare.com A 104.19.199.151 A 104.19.195... |
| 6035 | 1543618157.676808 | 192.168.1.169 | 192.168.1.1   | DNS      | 72     | Standard query 0x6ffd A www.ietf.org   |
| 6036 | 1543618157.696953 | 192.168.1.169 | 192.168.1.1   | DNS      | 72     | Standard query 0x6ffd A www.ietf.org   |
| 6037 | 1543618157.721487 | 192.168.1.1   | 192.168.1.169 | DNS      | 149    | Standard query response 0x6ffd A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net... |
| 6068 | 1543618157.837044 | 192.168.1.169 | 192.168.1.1   | DNS      | 82     | Standard query 0xcc3d A ocsp.starfieldtech.com   |
| 6070 | 1543618157.843950 | 192.168.1.1   | 192.168.1.169 | DNS      | 139    | Standard query response 0xcc3d A ocsp.starfieldtech.com CNAME ocsp.godaddy.com.akad... |

> Frame 6035: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface 0

> Ethernet II, Src: IntelCor\_fb:ab:3f (44:03:2c:fb:ab:3f), Dst: Verizon\_33:7d:4f (48:5d:36:33:7d:4f)

> Internet Protocol Version 4, Src: 192.168.1.169, Dst: 192.168.1.1

User Datagram Protocol, Src Port: 65382, Dst Port: 53

Source Port: 65382  
Destination Port: 53  
Length: 38  
Checksum: 0xe9c8 [unverified]  
[Checksum Status: Unverified]  
[Stream index: 90]

Domain Name System (query)

| Hex  | Dec   | ASCII               |
|------|---|---------------------|
| 0000 | 48 5d 36 33 7d 4f 44 03 2c fb ab 3f 08 00 45 00 | H]63}OD` ,..?.. E.. |
| 0010 | 00 3a 23 d8 00 00 80 11 92 e0 c0 a8 01 a9 c0 a8 | :#..... .           |
| 0020 | 01 01 ff 66 00 35 00 26 e9 c8 6f fd 01 00 00 01 | ..f.5 & ..o....     |
| 0030 | 00 00 00 00 00 00 03 77 77 77 04 69 65 74 66 03 | .....w ww.ietf.     |
| 0040 | 6f 72 67 00 00 01 00 01                         | org....             |

User Datagram Protocol (udp), 8 bytes

Packets: 7523 · Displayed: 198 (2.6%) · Dropped: 0 (0.0%)

Profile: Default

Windows Taskbar icons: File Explorer, Google Chrome, Microsoft Word, Paint, Internet Explorer, and others.

System tray icons: Network, Battery, Volume, ENG, 6:00 PM, 11/30/2018, 2 notifications.

9. What is the source port of DNS response message?

Answer: Source Port: 53 for, Src: 192.168.1.1,

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr=192.168.1.1

| No.  | Time              | Source        | Destination   | Protocol | Length | Info   |
|------|-------------------|---------------|---------------|----------|--------|--|
| 5361 | 1543618155.142789 | 192.168.1.1   | 192.168.1.169 | DNS      | 145    | Standard query response 0x1107 A pagead2.googlesyndication.com CNAME pagead46.l.dou... |
| 5432 | 1543618155.168804 | 192.168.1.169 | 192.168.1.1   | DNS      | 80     | Standard query 0xd979 A cdnjs.cloudflare.com   |
| 5451 | 1543618155.175123 | 192.168.1.1   | 192.168.1.169 | DNS      | 160    | Standard query response 0xd979 A cdnjs.cloudflare.com A 104.19.199.151 A 104.19.195... |
| 6035 | 1543618157.676808 | 192.168.1.169 | 192.168.1.1   | DNS      | 72     | Standard query 0x6ffd A www.ietf.org   |
| 6036 | 1543618157.696953 | 192.168.1.169 | 192.168.1.1   | DNS      | 72     | Standard query 0x6ffd A www.ietf.org   |
| 6037 | 1543618157.721487 | 192.168.1.1   | 192.168.1.169 | DNS      | 149    | Standard query response 0x6ffd A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net... |
| 6068 | 1543618157.837044 | 192.168.1.169 | 192.168.1.1   | DNS      | 82     | Standard query 0xcc3d A ocsp.starfieldtech.com   |
| 6070 | 1543618157.843950 | 192.168.1.1   | 192.168.1.169 | DNS      | 139    | Standard query response 0xcc3d A ocsp.starfieldtech.com CNAME ocsp.godaddy.com.akad... |

Frame 6037: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface 0

Ethernet II, Src: Verizon\_33:7d:4f (48:5d:36:33:7d:4f), Dst: IntelCor\_fb:ab:3f (44:03:2c:fb:ab:3f)

Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.169

User Datagram Protocol, Src Port: 53, Dst Port: 65382

Source Port: 53  
Destination Port: 65382  
Length: 115  
Checksum: 0xa375 [unverified]  
[Checksum Status: Unverified]  
[Stream index: 90]

Domain Name System (response)

| Hex  | Dec   | ASCII             |
|------|---|-------------------|
| 0000 | 44 03 2c fb ab 3f 48 5d 36 33 7d 4f 08 00 45 00 | D,..?H] 63}O ·E·  |
| 0010 | 00 87 9d ce 00 00 40 11 58 9d c0 a8 01 01 c0 a8 | .....@ X.....     |
| 0020 | 01 a9 00 35 ff 66 00 73 a3 75 6f fd 81 80 00 01 | ..5.f s .uo....   |
| 0030 | 00 03 00 00 00 00 03 77 77 77 04 69 65 74 66 03 | .....w ww-ietf-   |
| 0040 | 6f 72 67 00 00 01 00 01 c0 0c 00 05 00 01 00 00 | org.....          |
| 0050 | 07 08 00 21 03 77 77 77 04 69 65 74 66 03 6f 72 | ..!ww ietf.or     |
| 0060 | 67 03 63 64 6e 0a 63 6c 6f 75 64 66 6c 61 72 65 | gcdn-cl oudfflare |
| 0070 | 03 6e 65 74 00 c0 2a 00 01 00 01 00 00 01 2c 00 | .net.* .....,-    |
| 0080 | 04 68 14 01 55 c0 2a 00 01 00 01 00 00 01 2c 00 | h·U* .....,-      |

Internet Protocol Version 4 (ip), 20 bytes

Packets: 7523 · Displayed: 198 (2.6%) · Dropped: 0 (0.0%) · Profile: Default

6:03 PM 11/30/2018

10. To what IP address is the DNS query message sent?

Answer: Destination: 192.168.1.1

The screenshot shows a Wireshark capture window titled "\*Wi-Fi". The filter bar at the top contains the expression "ip.addr==192.168.1.1". The main pane displays a list of network packets. A specific DNS query from 192.168.1.169 to 192.168.1.1 for the domain "www.ietf.org" is highlighted. The packet details view shows the DNS header fields: Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT), Total Length: 58, Identification: 0x23d8 (9176), Flags: 0x0000, Time to live: 128, Protocol: UDP (17), Header checksum: 0x92e0 [validation disabled] [Header checksum status: Unverified], Source: 192.168.1.169, and Destination: 192.168.1.1. The bytes and hex views show the corresponding binary data for this packet.

11. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

Answer: Type: A (Host Address). The query message has NO answers.

The screenshot shows a Wireshark capture window titled "Wi-Fi". The packet list pane displays several DNS requests and responses. A specific DNS query for "www.ietf.org" is highlighted, showing its details in the center pane:

- Questions: 1
- Answer RRs: 0
- Authority RRs: 0
- Additional RRs: 0
- Queries
  - www.ietf.org: type A, class IN
    - Name: www.ietf.org
    - [Name Length: 12]
    - [Label Count: 3]
    - Type: A (Host Address) (1)
    - Class: IN (0x0001)

The bottom pane shows the raw hex and ASCII representation of the selected DNS query packet. The ASCII dump shows the domain name "www.ietf.org".

Packet details:  
0000 48 5d 3c 33 7d 4f 44 03 2c fb ab 3f 08 00 45 00 H[63]OD ,..? E.  
0010 00 3a 23 d8 00 00 80 11 92 e0 c0 a8 01 a9 c0 a8 :#.....  
0020 01 01 ff 66 00 35 00 26 e9 c8 6f fd 01 00 00 01 ..f.5 & o....  
0030 00 00 00 00 00 00 03 77 77 77 04 69 65 74 66 03 .....w ww.ietf.  
0040 6f 72 67 00 00 01 00 01 org....

Bottom status bar: Destination (ip.dst), 4 bytes | Packets: 7523 · Displayed: 198 (2.6%) · Dropped: 0 (0.0%) | Profile: Default  
Windows taskbar icons: File Explorer, Google Chrome, Microsoft Word, Paint, Internet Explorer, Task View, Taskbar settings, Network, Battery, Volume, ENG, 6:10 PM, 11/30/2018, 2 notifications.

12. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

Answer: Three (3) answers. Each answer has: domain name; type, class; time to live; data length; ip address.

The screenshot shows a Wireshark capture window titled "\*Wi-Fi". A search filter bar at the top contains "ip.addr==192.168.1.1". The main pane displays a list of network packets. The selected packet (No. 6037) is highlighted in yellow and corresponds to the following details:

| No.  | Time              | Source        | Destination   | Protocol | Length | Info   |
|------|-------------------|---------------|---------------|----------|--------|--|
| 5361 | 1543618155.142789 | 192.168.1.1   | 192.168.1.169 | DNS      | 145    | Standard query response 0x1107 A pagead2.googlesyndication.com CNAME pagead46.1.dou... |
| 5432 | 1543618155.168804 | 192.168.1.169 | 192.168.1.1   | DNS      | 80     | Standard query 0xd979 A cdnjs.cloudflare.com   |
| 5451 | 1543618155.175123 | 192.168.1.1   | 192.168.1.169 | DNS      | 160    | Standard query response 0xd979 A cdnjs.cloudflare.com A 104.19.199.151 A 104.19.195... |
| 6035 | 1543618157.676808 | 192.168.1.169 | 192.168.1.1   | DNS      | 72     | Standard query 0x6ffd A www.ietf.org   |
| 6036 | 1543618157.696953 | 192.168.1.169 | 192.168.1.1   | DNS      | 72     | Standard query 0x6ffd A www.ietf.org   |
| 6037 | 1543618157.721487 | 192.168.1.1   | 192.168.1.169 | DNS      | 149    | Standard query response 0x6ffd A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net... |
| 6068 | 1543618157.837044 | 192.168.1.169 | 192.168.1.1   | DNS      | 82     | Standard query 0xcc3d A ocsp.starfieldtech.com   |
| 6070 | 1543618157.843950 | 192.168.1.1   | 192.168.1.169 | DNS      | 139    | Standard query response 0xcc3d A ocsp.starfieldtech.com CNAME ocsp.godaddy.com.akad... |

The detailed analysis pane shows the following for the selected DNS response:

- Class: IN (0x0001)
- Answers
  - > www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
  - > www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.1.85
  - & www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.0.85
    - Name: www.ietf.org.cdn.cloudflare.net
    - Type: A (Host Address) (1)
    - Class: IN (0x0001)
    - Time to live: 300
    - Data length: 4
    - Address: 104.20.0.85

The hex and ASCII panes below show the raw bytes of the DNS response message, which includes the header and the two A records for the www.ietf.org CNAME.

Packets: 7523 · Displayed: 198 (2.6%) · Dropped: 0 (0.0%) · Profile: Default

6:16 PM 11/30/2018

13. Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message? : Yes, the destination IP address of the SYN packet is 104.20.1.85, the same as the second answer in the DNS response message:

Frame 83: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0

Ethernet II, Src: IntelCor\_fb:ab:3f (44:03:2c:fb:ab:3f), Dst: Verizon\_33:7d:4f (48:5d:36:33:7d:4f)

Internet Protocol Version 4, Src: 192.168.1.169, Dst: 104.20.1.85

Transmission Control Protocol, Src Port: 52509, Dst Port: 80, Seq: 0, Len: 0

| Time                 | Source        | Destination   | Protocol | Length | Info   |
|----------------------|---------------|---------------|----------|--------|--|
| 78 1543629582.871355 | 13.107.5.80   | 192.168.1.169 | TLSv1.2  | 684    | Application Data   |
| 79 1543629582.871484 | 192.168.1.169 | 13.107.5.80   | TCP      | 54     | 52484 → 443 [ACK] Seq=9859 Ack=7940 Win=1021 Len=0                           |
| 80 1543629583.437591 | 13.249.44.79  | 192.168.1.169 | TCP      | 54     | 80 → 52480 [FIN, ACK] Seq=1 Ack=1 Win=115 Len=0                              |
| 81 1543629583.437676 | 192.168.1.169 | 13.249.44.79  | TCP      | 54     | 52480 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0                                  |
| 82 1543629583.438014 | 192.168.1.169 | 13.249.44.79  | TCP      | 54     | 52480 → 80 [ACK] Seq=1 Ack=2 Win=1024 Len=0                                  |
| 83 1543629584.010203 | 192.168.1.169 | 104.20.1.85   | TCP      | 66     | 52509 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1           |
| 84 1543629584.010203 | 192.168.1.169 | 104.20.1.85   | TCP      | 66     | 52510 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1           |
| 85 1543629584.010203 | 192.168.1.169 | 104.20.1.85   | TCP      | 66     | 80 → 52509 [SYN, ACK] Seq=0 Ack=1 Win=1024 Len=0 MSS=1460 SACK_PERM=1 WS=256 |

```

0000  48 5d 36 33 7d 4f 44 03  2c fb ab 3f 08 00 45 00  H]63)OD` ,..?..E:
0010  00 34 05 29 40 00 80 06  c9 e0 c0 a8 01 a9 68 14  .4-)@... ..h.
0020  01 55 cd 1d 00 50 92 02 e7 e6 00 00 00 00 80 02  .U..P... .....
0030  ff ff fb fe 00 00 02 04  05 b4 01 03 03 08 01 01  .....
0040  04 02  .. .

```

Packets: 1718 · Displayed: 1718 (100.0%) · Dropped: 0 (0.0%) · Profile: Default

\*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression... +

| Time | Source            | Destination   | Protocol      | Length  | Info  |
|------|-------------------|---------------|---------------|---------|---|
| 46   | 1543629578.130819 | 13.107.136.9  | 192.168.1.169 | TLSv1.2 | 1330 Application Data   |
| 47   | 1543629578.175397 | 192.168.1.169 | 13.107.136.9  | TCP     | 54 53590 → 443 [ACK] Seq=1735 Ack=1277 Win=258 Len=0  |
| 48   | 1543629578.240171 | 192.168.1.1   | 192.168.1.169 | DNS     | 149 Standard query response 0x21cd A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net ... |
| 49   | 1543629578.334238 | 192.168.1.169 | 13.107.5.80   | TLSv1.2 | 877 Application Data  |
| 50   | 1543629578.341029 | 13.107.5.80   | 192.168.1.169 | TCP     | 64 443 → 52484 [ACK] Seq=4706 Ack=6557 Win=1023 Len=0 [ETHERNET FRAME CHECK SEQUENCE IN...  |
| 51   | 1543629578.381228 | 13.107.5.80   | 192.168.1.169 | TLSv1.2 | 737 Application Data  |
| 52   | 1543629578.381344 | 192.168.1.169 | 13.107.5.80   | TCP     | 54 52484 → 443 [ACK] Seq=6557 Ack=5389 Win=1024 Len=0                                       |
| 53   | 1543629578.381344 | 192.168.1.169 | 13.107.5.80   | TLSv1.2 | 878 Application Data  |

<

Flags: 0x8100 Standard query response, No error  
 Questions: 1  
 Answer RRs: 3  
 Authority RRs: 0  
 Additional RRs: 0  
 > Queries  
 > Answers  
 > www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net  
 > www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.1.85  
 > www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.0.85  
[Request In: 36]

```

0010 00 87 ca dc 00 00 40 11 2b 8f c0 a8 01 01 c0 a8 .....@. +.....
0020 01 a9 00 35 da b4 00 73 16 58 21 cd 81 80 00 01 .....5..s .X!.....
0030 00 03 00 00 00 00 03 77 77 77 04 69 65 74 66 03 .....w ww.ietf...
0040 6f 72 67 00 00 01 00 01 c0 0c 00 05 00 01 00 00 org..... .....
0050 07 08 00 21 03 77 77 77 04 69 65 74 66 03 6f 72 .....!www .ietf.or...
0060 67 03 63 64 6e 0a 63 6c 6f 75 64 66 6c 61 72 65 g.cdn.cl oudfla...
0070 03 6e 65 74 00 c0 2a 00 01 00 01 00 00 01 2c 00 .net...*. ....,.
0080 04 68 14 01 55 c0 2a 00 01 00 01 00 00 01 2c 00 .h..U.*. ....,.
0090 04 68 14 00 55 .....h..U

```

Number of answers in packet (dns.count.answers), 2 bytes

Packets: 1718 · Displayed: 1718 (100.0%) · Dropped: 0 (0.0%) · Profile: Default

Windows Taskbar icons: File Explorer, Google Chrome, Microsoft Edge, File Manager, Task View, Network, Start button.

System tray icons: Volume, Battery, Signal strength, Network, Volume, ENG, 9:15 PM, 11/30/2018, 2 notifications.

14. Select one UDP packet from your trace. From this packet, determine how many fields there are in the UDP header

Answer: four (4): source port; destination port; length; checksum.

The screenshot shows the Wireshark interface with a list of network packets captured over a Wi-Fi interface. The selected packet is frame 17, a User Datagram Protocol (UDP) packet. The details pane shows the following information for this packet:

- Frame 17: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface 0
- Ethernet II, Src: IntelCor\_fb:ab:3f (44:03:2c:fb:ab:3f), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
- Internet Protocol Version 4, Src: 192.168.1.169, Dst: 192.168.1.255
- User Datagram Protocol, Src Port: 12700, Dst Port: 12700
  - Source Port: 12700
  - Destination Port: 12700
  - Length: 56
  - Checksum: 0x231d [unverified]  
[Checksum Status: Unverified]
  - [Stream index: 0]

The bytes pane displays the raw hex and ASCII data for the selected UDP packet. The hex dump shows the following structure:

| Hex  | ASCII            |
|--|------------------|
| 0000 ff ff ff ff ff ff 44 03 2c fb ab 3f 08 00 45 00 | .....D.,..?..E.  |
| 0010 00 4c 3c 34 00 00 80 11 79 74 c0 a8 01 a9 c0 a8 | .L<4.....yt..... |
| 0020 01 ff 31 9c 31 9c 00 38 23 1d 4f ff 2b a0 66 7c | ..1.1..8#.0.+f   |
| 0030 09 c3 5a 0b e6 4e 91 1b d9 13 11 75 79 8f 9f a2 | ..Z..N..u.y....  |
| 0040 31 47 32 91 4b 27 ac 38 cb 25 bc f5 8d 02 10 72 | 1G2.K'.8.%.....r |
| 0050 1e 5b a9 cd b0 09 be a5 7b 7f                   | :[.....{.        |

The status bar at the bottom indicates: Packets: 3554 · Displayed: 10 (0.3%) · Dropped: 0 (0.0%). The system tray shows the date and time as 6:48 PM 11/30/2018, along with other icons.

15. By consulting the displayed information in Wireshark's packet content field for this packet, determine the length (in bytes) of each of the UDP header fields.

Answer: each is 2 bytes.

The screenshot shows the Wireshark interface with the following details:

- File Menu:** File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help.
- Toolbar:** Standard icons for opening files, saving, zooming, and filtering.
- Display Filter:** Apply a display filter ... <Ctrl-/>
- Panels:**
  - Packet List:** Shows a list of captured packets. The selected packet is frame 17, which is a User Datagram Protocol (UDP) packet from source port 12700 to destination port 12700.
  - Selected Packet Details:** Displays detailed information about the selected UDP packet, including:
    - Frame 17: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface 0
    - Ethernet II, Src: IntelCor\_fb:ab:3f (44:03:2c:fb:ab:3f), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
    - Internet Protocol Version 4, Src: 192.168.1.169, Dst: 192.168.1.255
    - User Datagram Protocol, Src Port: 12700, Dst Port: 12700
      - Source Port: 12700
      - Destination Port: 12700
      - Length: 56
      - Checksum: 0x231d [unverified]
      - [Checksum Status: Unverified]
      - [Stream index: 0]
  - Selected Packet Bytes:** Shows the raw hex and ASCII representation of the selected UDP packet. The hex dump shows the bytes 0000 to 0050, and the ASCII dump shows the corresponding characters.
  - Bottom Status Bar:** Source Port (udp.srcport), 2 bytes | Packets: 3554 · Displayed: 10 (0.3%) · Dropped: 0 (0.0%) | Profile: Default | 6:52 PM 11/30/2018

\*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

| No.  | Time              | Source        | Destination   | Protocol | Length | Info   |
|------|-------------------|---------------|---------------|----------|--------|--|
| 17   | 1543621618.854960 | 192.168.1.169 | 192.168.1.255 | UDP      | 90     | 12700 → 12700 Len=48   |
| 168  | 1543621618.940354 | 192.168.1.169 | 192.168.1.1   | DNS      | 88     | Standard query 0x2014 A 29.client-channel.google.com                                   |
| 196  | 1543621618.944899 | 192.168.1.169 | 192.168.1.1   | DNS      | 79     | Standard query 0x1e92 A clients4.google.com  |
| 197  | 1543621618.946189 | 192.168.1.1   | 192.168.1.169 | DNS      | 119    | Standard query response 0x1e92 A clients4.google.com CNAME clients.l.google.com A 1... |
| 203  | 1543621618.949869 | 192.168.1.1   | 192.168.1.169 | DNS      | 104    | Standard query response 0x2014 A 29.client-channel.google.com A 172.217.197.189        |
| 430  | 1543621618.987729 | 192.168.1.169 | 192.168.1.1   | DNS      | 85     | Standard query 0x0881 A lh4.googleusercontent.com                                      |
| 431  | 1543621618.989606 | 192.168.1.1   | 192.168.1.169 | DNS      | 130    | Standard query response 0x0881 A lh4.googleusercontent.com CNAME googlehosted.lgoo...  |
| 3030 | 1543621624.851834 | 192.168.1.169 | 192.168.1.1   | DNS      | 93     | Standard query 0xf8ac A taskassist-pa.clients6.google.com                              |

> Frame 17: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface 0

> Ethernet II, Src: IntelCor\_fb:ab:3f (44:03:2c:fb:ab:3f), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

> Internet Protocol Version 4, Src: 192.168.1.169, Dst: 192.168.1.255

>User Datagram Protocol, Src Port: 12700, Dst Port: 12700

Source Port: 12700

Destination Port: 12700

Length: 56

Checksum: 0x231d [unverified]

[Checksum Status: Unverified]

[Stream index: 0]

Data (48 bytes)

|  |                   |
|--|-------------------|
| 0000 ff ff ff ff ff ff 44 03 2c fb ab 3f 08 00 45 00 | .....D ,..?..E    |
| 0010 00 4c 3c 34 00 80 11 79 74 c0 a8 01 a9 c0 a8    | .L<4 .. yt .....  |
| 0020 01 ff 31 9c 31 9c 00 38 23 1d 4f ff 2b a0 66 7c | .·1·.1·.8 #·0·+·f |
| 0030 09 c3 5a 0b e6 4e 91 1b d9 13 11 75 79 8f 9f a2 | .·Z·.N·. .uy ..   |
| 0040 31 47 32 91 4b 27 ac 38 cb 25 bc f5 8d 02 10 72 | 162·K·.8 % ..r    |
| 0050 1e 5b a9 cd b0 09 be a5 7b 7f                   | .[..... {.        |

Destination Port (udp.dstport), 2 bytes

Packets: 3554 · Displayed: 10 (0.3%) · Dropped: 0 (0.0%) · Profile: Default

Windows Taskbar icons: File Explorer, Google Chrome, File Cabinet, Microsoft Word, Microsoft Excel, Microsoft Powerpoint, Microsoft Edge, Microsoft Internet Explorer, Task View, System Tray icons: Volume, Battery, Network, Signal Strength, Volume, ENG, 6:52 PM, 11/30/2018, 2 notifications.

\*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

| No.  | Time              | Source        | Destination   | Protocol | Length | Info   |
|------|-------------------|---------------|---------------|----------|--------|--|
| 17   | 1543621618.854960 | 192.168.1.169 | 192.168.1.255 | UDP      | 90     | 12700 → 12700 Len=48   |
| 168  | 1543621618.940354 | 192.168.1.169 | 192.168.1.1   | DNS      | 88     | Standard query 0x2014 A 29.client-channel.google.com                                   |
| 196  | 1543621618.944899 | 192.168.1.169 | 192.168.1.1   | DNS      | 79     | Standard query 0x1e92 A clients4.google.com  |
| 197  | 1543621618.946189 | 192.168.1.1   | 192.168.1.169 | DNS      | 119    | Standard query response 0x1e92 A clients4.google.com CNAME clients.l.google.com A 1... |
| 203  | 1543621618.949869 | 192.168.1.1   | 192.168.1.169 | DNS      | 104    | Standard query response 0x2014 A 29.client-channel.google.com A 172.217.197.189        |
| 430  | 1543621618.987729 | 192.168.1.169 | 192.168.1.1   | DNS      | 85     | Standard query 0x0881 A lh4.googleusercontent.com                                      |
| 431  | 1543621618.989606 | 192.168.1.1   | 192.168.1.169 | DNS      | 130    | Standard query response 0x0881 A lh4.googleusercontent.com CNAME googlehosted.lgoo...  |
| 3030 | 1543621624.851834 | 192.168.1.169 | 192.168.1.1   | DNS      | 93     | Standard query 0xf8ac A taskassist-pa.clients6.google.com                              |

> Frame 17: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface 0

> Ethernet II, Src: IntelCor\_fb:ab:3f (44:03:2c:fb:ab:3f), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

> Internet Protocol Version 4, Src: 192.168.1.169, Dst: 192.168.1.255

>User Datagram Protocol, Src Port: 12700, Dst Port: 12700

Source Port: 12700

Destination Port: 12700

Length: 56

Checksum: 0x231d [unverified]

[Checksum Status: Unverified]

[Stream index: 0]

Data (48 bytes)

|  |                  |
|--|------------------|
| 0000 ff ff ff ff ff ff 44 03 2c fb ab 3f 08 00 45 00 | .....D. ,..?..E. |
| 0010 00 4c 3c 34 00 80 11 79 74 c0 a8 01 a9 c0 a8    | .L<4.....yt..... |
| 0020 01 ff 31 9c 31 9c 00 38 23 1d 4f ff 2b a0 66 7c | .·1·1··8 #·0·+·f |
| 0030 09 c3 5a 0b e6 4e 91 1b d9 13 11 75 79 8f 9f a2 | .·Z··N· ···uy··· |
| 0040 31 47 32 91 4b 27 ac 38 cb 25 bc f5 8d 02 10 72 | 162·K··8 % ···r  |
| 0050 1e 5b a9 cd b0 09 be a5 7b 7f                   | .[..... {.       |

Length (udp.length), 2 bytes

Packets: 3554 · Displayed: 10 (0.3%) · Dropped: 0 (0.0%) · Profile: Default

6:53 PM 11/30/2018

\*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

| No.  | Time              | Source        | Destination   | Protocol | Length | Info   |
|------|-------------------|---------------|---------------|----------|--------|--|
| 17   | 1543621618.854960 | 192.168.1.169 | 192.168.1.255 | UDP      | 90     | 12700 → 12700 Len=48   |
| 168  | 1543621618.940354 | 192.168.1.169 | 192.168.1.1   | DNS      | 88     | Standard query 0x2014 A 29.client-channel.google.com                                   |
| 196  | 1543621618.944899 | 192.168.1.169 | 192.168.1.1   | DNS      | 79     | Standard query 0x1e92 A clients4.google.com  |
| 197  | 1543621618.946189 | 192.168.1.1   | 192.168.1.169 | DNS      | 119    | Standard query response 0x1e92 A clients4.google.com CNAME clients.l.google.com A 1... |
| 203  | 1543621618.949869 | 192.168.1.1   | 192.168.1.169 | DNS      | 104    | Standard query response 0x2014 A 29.client-channel.google.com A 172.217.197.189        |
| 430  | 1543621618.987729 | 192.168.1.169 | 192.168.1.1   | DNS      | 85     | Standard query 0x0881 A lh4.googleusercontent.com                                      |
| 431  | 1543621618.989606 | 192.168.1.1   | 192.168.1.169 | DNS      | 130    | Standard query response 0x0881 A lh4.googleusercontent.com CNAME googlehosted.lgoo...  |
| 3030 | 1543621624.851834 | 192.168.1.169 | 192.168.1.1   | DNS      | 93     | Standard query 0xf8ac A taskassist-pa.clients6.google.com                              |

> Frame 17: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface 0

> Ethernet II, Src: IntelCor\_fb:ab:3f (44:03:2c:fb:ab:3f), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

> Internet Protocol Version 4, Src: 192.168.1.169, Dst: 192.168.1.255

>User Datagram Protocol, Src Port: 12700, Dst Port: 12700

Source Port: 12700  
Destination Port: 12700  
Length: 56  
Checksum: 0x231d [unverified]  
[Checksum Status: Unverified]  
[Stream index: 0]

Data (48 bytes)

|  |                |
|--|----------------|
| 0000 ff ff ff ff ff ff 44 03 2c fb ab 3f 08 00 45 00 | .....D ,..?..E |
| 0010 00 4c 3c 34 00 80 11 79 74 c0 a8 01 a9 c0 a8    | .L<4 ..yt..... |
| 0020 01 ff 31 9c 31 9c 00 38 23 1d 4f ff 2b a0 66 7c | .·1·1·8 #0+·f  |
| 0030 09 c3 5a 0b e6 4e 91 1b d9 13 11 75 79 8f 9f a2 | .·Z·N· ..uy... |
| 0040 31 47 32 91 4b 27 ac 38 cb 25 bc f5 8d 02 10 72 | 162·K·8 % ..·r |
| 0050 1e 5b a9 cd b0 09 be a5 7b 7f                   | .[-..... {.    |

Details at: [http://www.wireshark.org/docs/wsug\\_html\\_chunked/ChAdvChecksums.html](http://www.wireshark.org/docs/wsug_html_chunked/ChAdvChecksums.html) (udp.checksum), 2 bytes

Packets: 3554 · Displayed: 10 (0.3%) · Dropped: 0 (0.0%) · Profile: Default

Windows Taskbar icons: File Explorer, Google Chrome, File Manager, Task View, Microsoft Edge, and others. System tray icons: Volume, Network, Battery, and a notification for 2 new messages.

16. The value in the Length field is the length of what? Verify your claim with your captured UDP packet.

Answer: The UDP segment Length is 56 (payload+header) . Data is 48. Each header is 2. Therefore  $48+2+2+2=56$ .

The screenshot shows the Wireshark interface with the following details:

- Frame 17:** 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface 0
- Ethernet II:** Src: IntelCor\_fb:ab:3f (44:03:2c:fb:ab:3f), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
- Internet Protocol Version 4:** Src: 192.168.1.169, Dst: 192.168.1.255
- User Datagram Protocol:** Src Port: 12700, Dst Port: 12700
  - Source Port: 12700
  - Destination Port: 12700
  - Length: 56
  - Checksum: 0x231d [unverified]
  - [Checksum Status: Unverified]
  - [Stream index: 0]
- Data (48 bytes):**

|  |                |
|--|----------------|
| 0000 ff ff ff ff ff ff 44 03 2c fb ab 3f 08 00 45 00 | .....D ,..?E   |
| 0010 00 4c 3c 34 00 00 80 11 79 74 c0 a8 01 a9 c0 a8 | .L4...yt.....  |
| 0020 01 ff 31 9c 31 9c 00 38 23 1d 4f ff 2b a0 66 7c | .1.1.8 #.0.+f  |
| 0030 09 c3 5a 0b e6 4e 91 1b d9 13 11 75 79 8f 9f a2 | .Z-N..uy...    |
| 0040 31 47 32 91 4b 27 ac 38 cb 25 bc f5 8d 02 10 72 | 1G2.K'8 %....r |
| 0050 1e 5b a9 cd b0 09 be a5 7b 7f                   | .[.....{.      |

At the bottom, there is a status bar with the following information:  
Details at: [http://www.wireshark.org/docs/wsug\\_html\\_chunked/ChAdvChecksums.html](http://www.wireshark.org/docs/wsug_html_chunked/ChAdvChecksums.html) (udp.checksum), 2 bytes  
Packets: 3554 · Displayed: 10 (0.3%) · Dropped: 0 (0.0%) · Profile: Default  
Windows taskbar icons for File Explorer, Google Chrome, Microsoft Word, Microsoft Excel, and Internet Explorer.  
System tray icons for battery, signal strength, volume, and notifications (2).

```
C:\Users\iiwaziri>ping -n 10 176.32.103.205

Pinging 176.32.103.205 with 32 bytes of data:
Reply from 176.32.103.205: bytes=32 time=20ms TTL=235
Reply from 176.32.103.205: bytes=32 time=27ms TTL=235
Reply from 176.32.103.205: bytes=32 time=23ms TTL=235
Reply from 176.32.103.205: bytes=32 time=23ms TTL=235
Reply from 176.32.103.205: bytes=32 time=31ms TTL=235
Reply from 176.32.103.205: bytes=32 time=26ms TTL=235
Reply from 176.32.103.205: bytes=32 time=28ms TTL=235
Reply from 176.32.103.205: bytes=32 time=25ms TTL=235
Reply from 176.32.103.205: bytes=32 time=29ms TTL=235
Reply from 176.32.103.205: bytes=32 time=23ms TTL=235

Ping statistics for 176.32.103.205:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 20ms, Maximum = 31ms, Average = 25ms
```

17. Explain what happened in Figure 1. (pay close attention to the command.)

Answer: The ping command is used in the Command Prompt where the source “iiwasiri” reaches the destination IP 176.32.103.205. This computer is communication with another computer within the network. The command uses also -n count that is option that sets the number of ICMP Echo Requests to send, from 1 to 4294967295. The ping command will send 4 by default if -n isn't used. In this figure the -n is 10.

18. Which protocol is used to carry out the instruction in Figure 1.?

Answer: ICMP-- Internet Control Message Protocol.

## 19. Who owns the IP?

Answer: Amazon

The screenshot shows a web browser window with four tabs open:

- Time to live - Wikipedia
- Ping Command (Examples, Options)
- ping (networking utility) - Wikipedia
- WHOIS IP Lookup Tool | UltraTools

The main content area displays the results of a WHOIS lookup for the IP address 176.32.103.205. The search bar contains "176.32.103.205" and a "Go »" button. Below the search bar, there are links to related tools: DNS Traversal, Traceroute, Vector Trace, Ping, and WHOIS Lookup.

The WHOIS output is as follows:

```
Source: whois.ripe.net
IP Address: 176.32.103.205

% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See http://www.ripe.net/db/support/db-terms-conditions.pdf

% Note: this output has been filtered.
%       To receive output for a database update, use the "-B" flag.

% Information related to '176.32.96.0 - 176.32.103.255'

% Abuse contact for '176.32.96.0 - 176.32.103.255' is 'email-abuse@amazon.com'

inetnum:      176.32.96.0 - 176.32.103.255
netname:      amazon-IAD-PROD
descr:        PROD IAD
country:      US
admin-c:      MA11338-RIPE
tech-c:       AJ176-RIPE
status:       ASSIGNED PA
mnt-by:       MNT-ADSI
mnt-domains: MNT-ADSI
created:     2012-03-08T15:56:39Z
last-modified: 2015-08-17T17:43:07Z
source:       RIPE

person:       Alan Judge
address:      Amazon Data Services Ireland
address:      Digital Depot
address:      Thomas Street
```

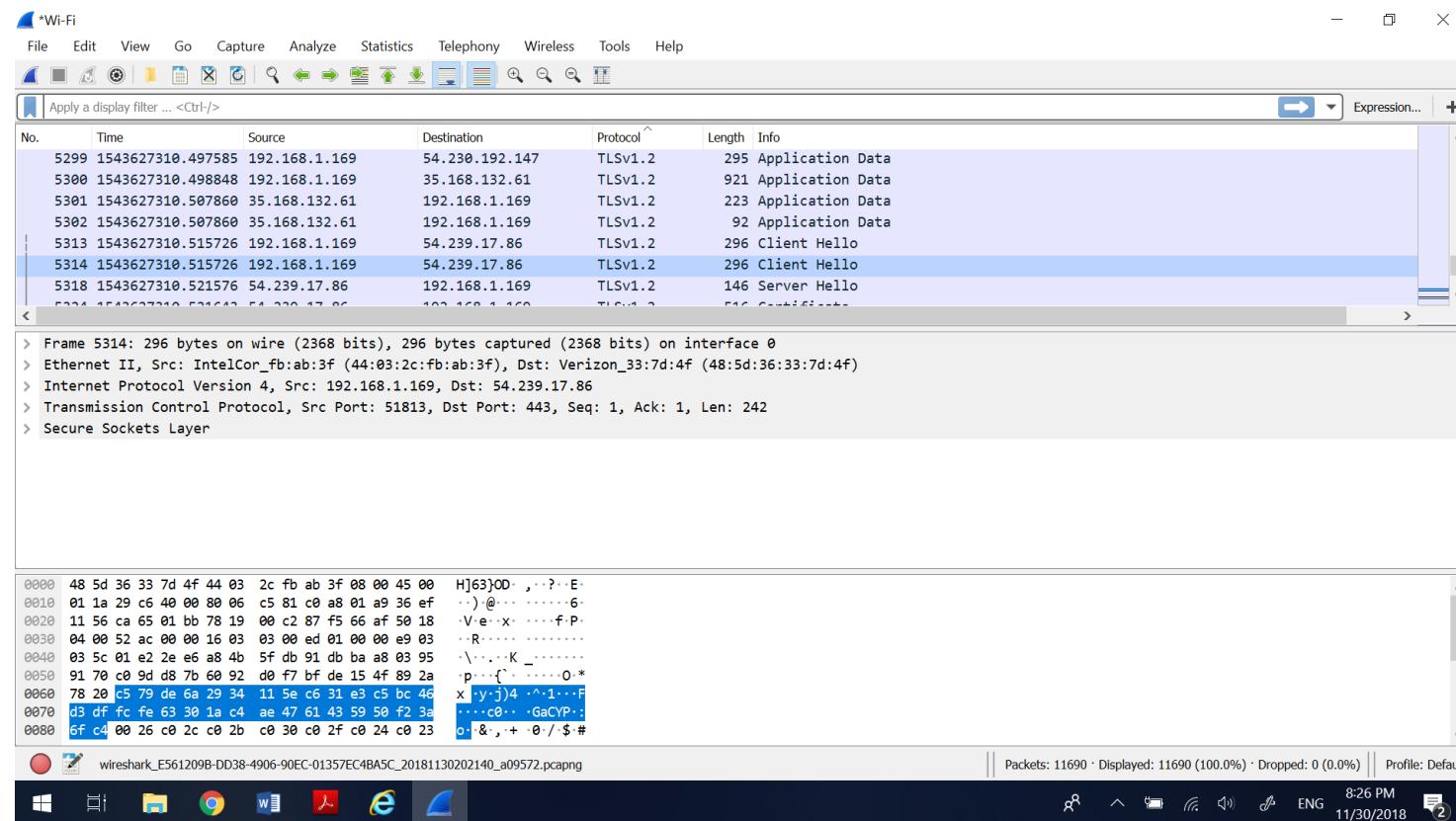
The taskbar at the bottom of the screen shows several pinned icons: File Explorer, Google Chrome, Microsoft Word, Microsoft Paint, Internet Explorer, and File Explorer again. The system tray indicates the date and time as 11/30/2018, 7:25 PM, with two notifications.

20. In addition to a screenshot, in a tabular form, list all the hops between your computer's IP and the IP address in Figure 1. The table should include the owner, and location of the IP address (Please see the last one)

21. What version of TLS does the IP above use? Hint: Visit the website of the owners IP address, and capture the "Client Hello" packet.

Answer: different AMAZON IP: 54.239.17.86

TLS version 1.2 - TLSv1.2      296      Client Hello



22. List all the algorithms listed in the Cipher Suite of the “Client Hello” packet in 21. **Answer:** Cipher Suites (19 suites)

Cipher Suite: TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384 (0xc02c)

Cipher Suite: TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256 (0xc02b)

Cipher Suite: TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384 (0xc030)

Cipher Suite: TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256 (0xc02f)

Cipher Suite: TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA384 (0xc024)

Cipher Suite: TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256 (0xc023)

Cipher Suite: TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384 (0xc028)

Cipher Suite: TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256 (0xc027)

Cipher Suite: TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA (0xc00a)

Cipher Suite: TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA (0xc009)

Cipher Suite: TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA (0xc014)

Cipher Suite: TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA (0xc013)

Cipher Suite: TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384 (0x009d)

Cipher Suite: TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256 (0x009c)

Cipher Suite: TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256 (0x003d)

Cipher Suite: TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256 (0x003c)

Cipher Suite: TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA (0x0035)

Cipher Suite: TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA (0x002f)

Cipher Suite: TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA (0x000a)

\*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression... +

| No.  | Time              | Source        | Destination    | Protocol | Length | Info             |
|------|-------------------|---------------|----------------|----------|--------|------------------|
| 5299 | 1543627310.497585 | 192.168.1.169 | 54.230.192.147 | TLSv1.2  | 295    | Application Data |
| 5300 | 1543627310.498848 | 192.168.1.169 | 35.168.132.61  | TLSv1.2  | 921    | Application Data |
| 5301 | 1543627310.507860 | 35.168.132.61 | 192.168.1.169  | TLSv1.2  | 223    | Application Data |
| 5302 | 1543627310.507860 | 35.168.132.61 | 192.168.1.169  | TLSv1.2  | 92     | Application Data |
| 5313 | 1543627310.515726 | 192.168.1.169 | 54.239.17.86   | TLSv1.2  | 296    | Client Hello     |
| 5314 | 1543627310.515726 | 192.168.1.169 | 54.239.17.86   | TLSv1.2  | 296    | Client Hello     |
| 5318 | 1543627310.521576 | 54.239.17.86  | 192.168.1.169  | TLSv1.2  | 146    | Server Hello     |
| 5324 | 1543627310.521642 | 54.239.17.86  | 192.168.1.169  | TLSv1.2  | 516    | Certificate      |

Session ID: c579de6a2934115ec631e3c5bc46d3dfffcfe63301ac4ae47...

Cipher Suites Length: 38

▼ Cipher Suites (19 suites)

- Cipher Suite: TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384 (0xc02c)
- Cipher Suite: TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256 (0xc02b)
- Cipher Suite: TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384 (0xc030)
- Cipher Suite: TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256 (0xc02f)
- Cipher Suite: TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA384 (0xc024)
- Cipher Suite: TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256 (0xc023)
- Cipher Suite: TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384 (0xc028)
- Cipher Suite: TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256 (0xc027)

```
0080 6f c4 00 26 c0 2c c0 2b c0 30 c0 2f c0 24 c0 23 o & , + 0 ./ $ #
0090 c0 28 c0 27 c0 0a c0 09 c0 14 c0 13 00 9d 00 9c ( . . . .
00a0 00 3d 00 3c 00 35 00 2f 00 00 01 00 00 7a 00 00 = < . / . . . z ..
00b0 00 1a 00 18 00 00 15 63 6f 6d 70 6c 65 74 69 6f . . . . . c ompletio
00c0 6e 2e 61 6d 61 7a 6f 6e 2e 63 6f 6d 00 05 00 05 n.amazon .com . .
00d0 01 00 00 00 00 0a 00 08 00 06 00 1d 00 17 00 . . . . . .
00e0 18 00 0b 00 02 01 00 00 0d 00 14 00 12 04 01 05 . . . . .
00f0 01 02 01 04 03 05 03 02 03 02 02 06 01 06 03 00 . . . . .
0100 23 00 00 00 10 00 0e 00 0c 02 68 32 08 68 74 74 # . . . . h2 . ht
```

List of cipher suites supported by client (ssl.handshake.ciphersuites), 38 bytes

Packets: 11690 · Displayed: 11690 (100.0%) · Dropped: 0 (0.0%) · Profile: Default

8:34 PM 11/30/2018

23. What TCP port number is used by the “Client Hello” packet, and why is it using that port number?

Answer: TCP port nr. 443. TCP port 443 is the standard TCP port used for website with SSL or TLS traffic.

The screenshot shows the Wireshark interface with the following details:

- Network Interface:** \*Wi-Fi
- File Menu:** File, Edit, View, Go, Capture, Analyze, Statistics, Telephoney, Wireless, Tools, Help
- Toolbar:** Apply a display filter ... <Ctrl-/>, Expression...
- Table:** Shows network traffic with columns: No., Time, Source, Destination, Protocol, Length, Info. The Client Hello packet (No. 5314) is highlighted.
- Packet Details:** Frame 5314: 296 bytes on wire (2368 bits), 296 bytes captured (2368 bits) on interface 0. It includes details about Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol.
- Hex Editor:** Displays the raw hex and ASCII data of the selected Client Hello packet.
- Status Bar:** Packets: 11690 · Displayed: 11690 (100.0%) · Dropped: 0 (0.0%) · Profile: Default
- Taskbar:** Shows icons for File Explorer, Google Chrome, Microsoft Edge, and FileZilla, along with system status icons (battery, signal, volume, network, etc.) and the date/time (8:39 PM, 11/30/2018).

## 24. What are the source and destination MAC address?

Answer:, Src: (44:03:2c:fb:ab:3f), Dst: (48:5d:36:33:7d:4f)

The screenshot shows a Wireshark capture window titled "Wi-Fi". The main pane displays a list of network frames. Frame 5314 is selected, showing details for an Ethernet II frame. The selected frame's bytes are shown in the bottom pane, with the source MAC address (44:03:2c:fb:ab:3f) highlighted in blue.

**Selected Frame Details:**

- Frame 5314: 296 bytes on wire (2368 bits), 296 bytes captured (2368 bits) on interface 0
- Ethernet II, Src: IntelCor\_fb:ab:3f (44:03:2c:fb:ab:3f), Dst: Verizon\_33:7d:4f (48:5d:36:33:7d:4f)
  - Destination: Verizon\_33:7d:4f (48:5d:36:33:7d:4f)
  - Source: IntelCor\_fb:ab:3f (44:03:2c:fb:ab:3f)
  - Type: IPv4 (0x0800)
- Internet Protocol Version 4, Src: 192.168.1.169, Dst: 54.239.17.86
- Transmission Control Protocol, Src Port: 51813, Dst Port: 443, Seq: 1, Ack: 1, Len: 242
- Secure Sockets Layer
  - TLSv1.2 Record Layer: Handshake Protocol: Client Hello
    - Content Type: Handshake (22)
    - Version: TLS 1.2 (0x0303)

**Selected Frame Bytes:**

| Hex  | Dec   | ASCII                  |
|------|---|------------------------|
| 0000 | 48 5d 36 33 7d 4f 44 03 2c fb ab 3f 08 00 45 00 | H]63}0D ..?..E..       |
| 0010 | 01 1a 29 c6 48 00 80 06 c5 81 c0 a8 01 a9 36 ef | ..)@.....6..           |
| 0020 | 11 56 ca 65 01 bb 78 19 00 c2 87 f5 66 af 50 18 | ..V..e..x.. ....f..P.. |
| 0030 | 04 00 52 ac 00 00 16 03 03 00 ed 01 00 00 e9 03 | ..R.....               |
| 0040 | 03 5c 01 e2 e6 a8 4b 5f db 91 db ba a8 03 95    | ..\\...K .....         |
| 0050 | 91 70 c0 9d d8 7b 60 92 d0 f7 bf de 15 4f 89 2a | p...{ ..O ..*          |
| 0060 | 78 20 c5 79 de 6a 29 34 11 5e c6 31 e3 c5 bc 46 | x ..y..j)4 ..^..1..F   |
| 0070 | d3 df fc fe 63 30 1a c4 ae 47 61 43 59 50 f2 3a | ....c0... .GaCYP..     |
| 0080 | 6f c4 00 26 c0 2c c0 2b c0 30 c0 2f c0 24 c0 23 | o ..& ..+ ..0 ..\$ ..# |

Packets: 11690 · Displayed: 11690 (100.0%) · Dropped: 0 (0.0%) · Profile: Default

8:42 PM 11/30/2018

25. Identify the company that manufactured the network cards with the MAC address identified in 8 above

Answer: Intel & Verizon

Screenshot of arul's utilities website showing the MAC Address and OUI Lookup tool.

The page title is "arul's utilities" with the subtitle "track ip addresses, phone numbers, etc".

The main content area is titled "MAC Address and OUI Lookup". It includes a description of the tool: "This program displays the name of the company that manufactured your network card. You can also do a reverse lookup and find the MAC addresses registered by a company." Below this is a form where the MAC address "44032C" is entered, and a button labeled "lookup MAC address" is visible.

A sidebar on the left lists various utility tools under "NETWORK" and "TEXT/STRING/MATH" categories.

A sidebar on the right includes links for "SHARE THIS WITH OTHERS" (facebook, twitter, linkedin, google+), a "CURRENT BIBLE VERSE" (2 Timothy 1:7), "TECHNICAL ARTICLES" (links to IP address of email sender, rescue files, hack router, save document as PDF, Solaris commands, and Prince of Persia game), and a "SUBSCRIBE" section with social media icons for Facebook, Google+, Twitter, and RSS feed.

At the bottom, there is a cookie consent message: "This website uses cookies. Cookies improve the user experience and help make this website better. By continuing to use the site, you agree to our [privacy policy](#). [OK](#)".

The taskbar at the bottom of the browser window shows various application icons (Windows, File Explorer, Google Chrome, Microsoft Word, Microsoft Excel, Microsoft Edge, and a blue shark icon).

MAC Address and OUI Lookup fc x +

https://aruljohn.com/mac/485D36337D4F

# arul's utilities

track ip addresses, phone numbers, etc

Check your IP Address

**NETWORK**

- IP address tracker
- telephone tracker
- wireless network key
- which webserver
- MAC address lookup
- IP/CIDR subnet
- IP to hostname
- hostname to IP
- view HTTP headers

**TEXT/STRING/MATH**

- JSON sort
- text case convert
- aquarium calculator
- timestamp to date

## MAC Address and OUI Lookup

This program displays the name of the company that manufactured your network card. You can also do a reverse lookup and find the MAC addresses registered by a company.

ENTER MAC ADDRESS OR OUI (FIRST 6 DIGITS)

485D36

SELECT LOOKUP TYPE:  LOOKUP MAC  LOOKUP VENDOR

example: 00:0B:14

*This database was last updated on Wed, 28 November 2018*

### Results for MAC address [48:5D:36](#)

Found 1 results.

| MAC Address/OUI | Vendor {Company} |
|-----------------|------------------|
| 48:5D:36        | Verizon          |

[Direct link to this result](#)

This website uses cookies. Cookies improve the user experience and help make this website better. By continuing to use the site, you agree to our [privacy policy](#).

SHARE THIS WITH OTHERS

[facebook](#) [twitter](#) [linkedin](#) [google+](#)

Share on WhatsApp

CURRENT BIBLE VERSE

*For the Spirit that God has given us does not make us timid; instead, His Spirit fills us with power, love, and self-control.*

[2 Timothy 1:7](#)

TECHNICAL ARTICLES

- [How to find IP address of the email sender](#)
- [How to rescue your files if Windows is busted!](#)
- [How to hack your Linksys router](#)
- [Save a document as PDF](#)
- [Solaris admin commands](#)
- [Play Prince of Persia on Ubuntu Linux](#)

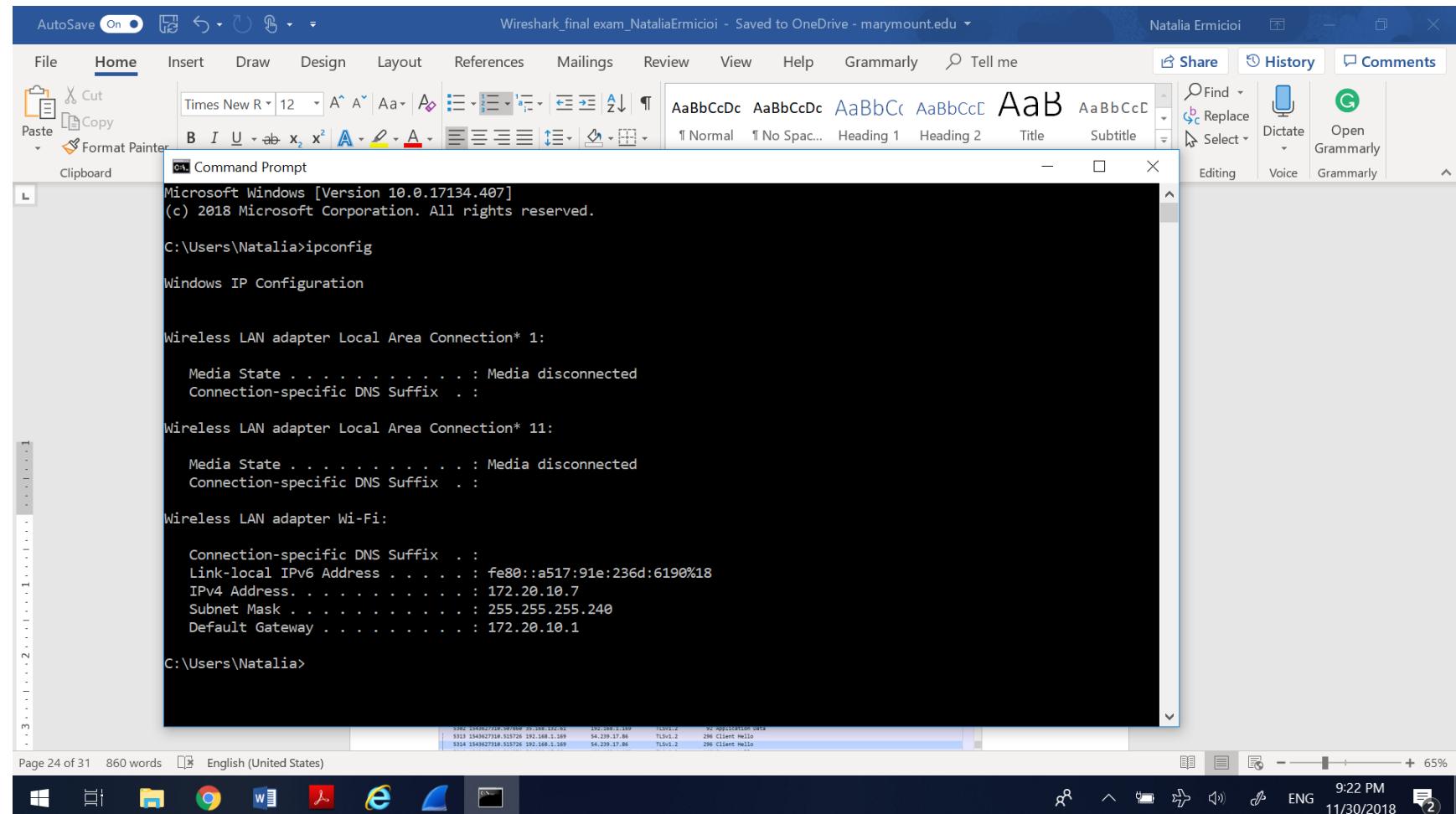
SUBSCRIBE

[!\[\]\(235bc52426e9c93b3d7d4df11f3f966b\_img.jpg\)](#) [!\[\]\(7cd98e86965561e187fe83822a690066\_img.jpg\)](#) [!\[\]\(406d4ef1ad5321782081829ae913d5cb\_img.jpg\)](#) [!\[\]\(0019a7d1c7cbe8539be377118ea4d9a8\_img.jpg\)](#)

8:45 PM 11/30/2018

Question 20: My home router has firewall and I can't traceroute. I did hotspot from my cellphone in order to traceroute.

New IP address: 172.20.10.7



AutoSave On Wireshark\_final\_exam\_NataliaErmicio - Saved to OneDrive - marymount.edu Table Tools

File Home Insert Design Layout References Mailings Review View Help Grammar Design Layout Tell me

Headers  Total Row  Bande

Command Prompt

C:\Users\Natalia> tracert 176.32.103.205

Tracing route to 176.32.103.205 over a maximum of 30 hops

| Hop | MS  | MS | MS | IP Address |                    |    |                |
|-----|-----|----|----|------------|--------------------|----|----------------|
| 1   | 2   | ms | 1  | ms         | 2                  | ms | 172.20.10.1    |
| 2   | 73  | ms | 55 | ms         | 60                 | ms | 10.198.0.177   |
| 3   | 59  | ms | 76 | ms         | 62                 | ms | 10.166.254.50  |
| 4   | 73  | ms | 53 | ms         | 61                 | ms | 10.166.254.53  |
| 5   | 84  | ms | 53 | ms         | 65                 | ms | 10.164.160.109 |
| 6   | 65  | ms | 54 | ms         | 48                 | ms | 10.164.165.129 |
| 7   | 75  | ms | 57 | ms         | 66                 | ms | 206.41.108.16  |
| 8   | 90  | ms | 81 | ms         | 101                | ms | 52.93.37.105   |
| 9   | 108 | ms | 76 | ms         | 95                 | ms | 52.93.37.40    |
| 10  | 102 | ms | 81 | ms         | 76                 | ms | 54.239.42.192  |
| 11  | *   | *  | *  |            | Request timed out. |    |                |
| 12  | *   | *  | *  |            | Request timed out. |    |                |
| 13  | *   | *  | *  |            | Request timed out. |    |                |
| 14  | *   | *  | *  |            | Request timed out. |    |                |
| 15  | *   | *  | *  |            | Request timed out. |    |                |
| 16  | *   | *  | *  |            | Request timed out. |    |                |
| 17  | *   | *  | *  |            | Request timed out. |    |                |
| 18  | *   | *  | *  |            | Request timed out. |    |                |
| 19  | *   | *  | *  |            | Request timed out. |    |                |
| 20  | *   | *  | *  |            | Request timed out. |    |                |
| 21  | 5   | ms | 5  | ms         | 5                  | ms | 176.32.103.205 |

Trace complete.

C:\Users\Natalia>

Page 33 of 33 893 words English (United States) + 65% 9:33 PM 11/30/2018

| IP Address     | Owner                                      | Location         |
|----------------|--|------------------|
| 172.20.10.1    | PRIVATE-ADDRESS-BBLK-RFC1918-IANA-RESERVED | LA, CA, USA      |
| 10.198.0.177   | PRIVATE-ADDRESS-ABLK-RFC1918-IANA-RESERVED | LA, CA, USA      |
| 10.166.254.50  | PRIVATE-ADDRESS-ABLK-RFC1918-IANA-RESERVED | LA, CA, USA      |
| 10.166.254.53  | PRIVATE-ADDRESS-ABLK-RFC1918-IANA-RESERVED | LA, CA, USA      |
| 10.164.160.109 | PRIVATE-ADDRESS-ABLK-RFC1918-IANA-RESERVED | LA, CA, USA      |
| 10.164.165.129 | PRIVATE-ADDRESS-ABLK-RFC1918-IANA-RESERVED | LA, CA, USA      |
| 206.41.108.16  | FL-IX-LAN                                  | Miami, FL, USA   |
| 52.93.37.105   | Amazon Technologies Inc.                   | Seattle, WA, USA |
| 52.93.37.40    | Amazon Technologies Inc.                   | Seattle, WA, USA |
| 54.239.42.192  | Amazon Technologies Inc.                   | Seattle, WA, USA |
| 176.32.103.205 | Amazon Technologies Inc.                   | Seattle, WA, USA |

\*\*\*\*\*Github: [https://github.com/n0e22710/wireshark\\_labs](https://github.com/n0e22710/wireshark_labs)