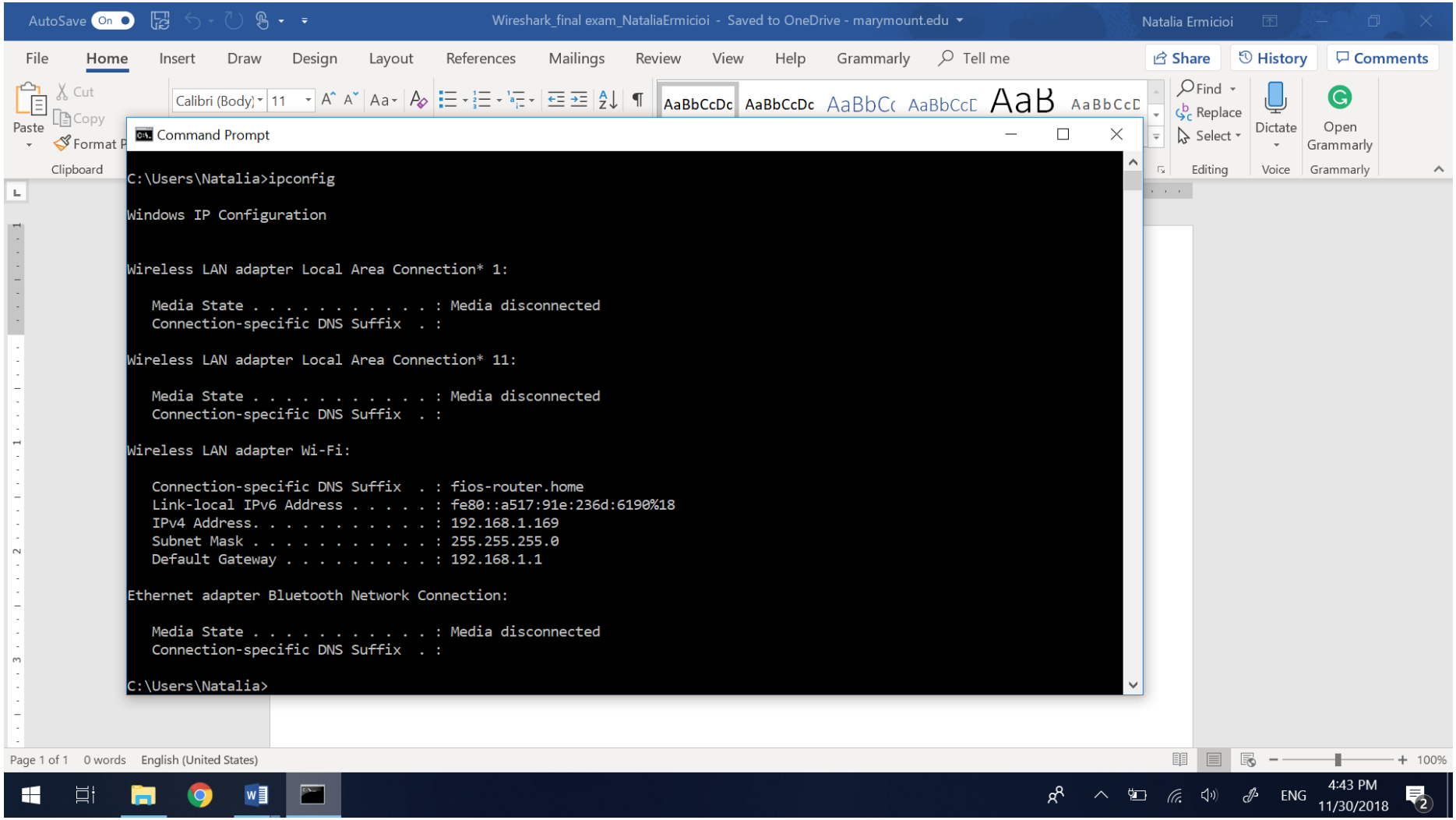
Wireshark – Final – Natalia Ermicioi

IP address: 192.168.1.169

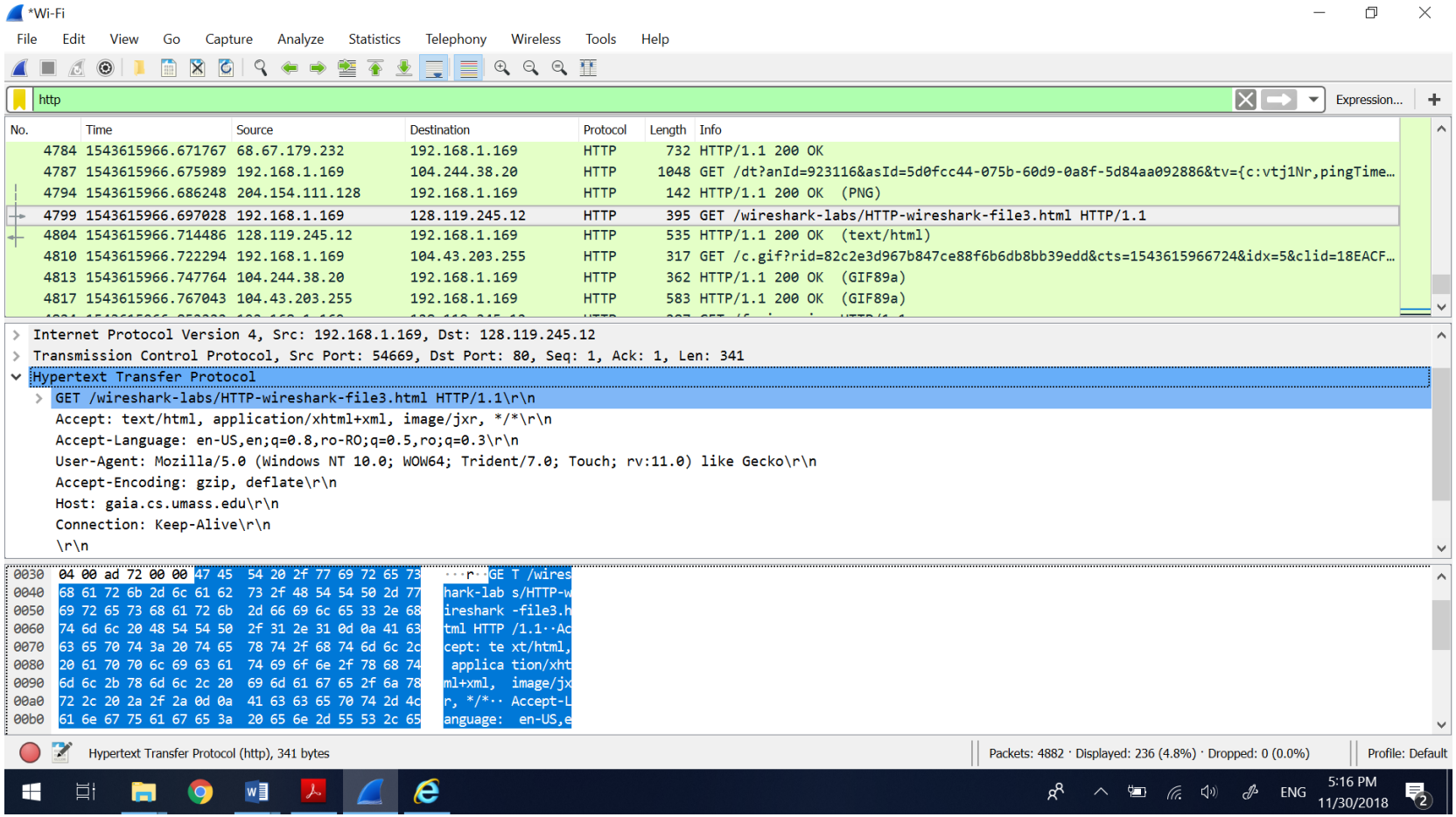


1. 1. How many HTTP GET request messages did your browser send?

Answer: 1

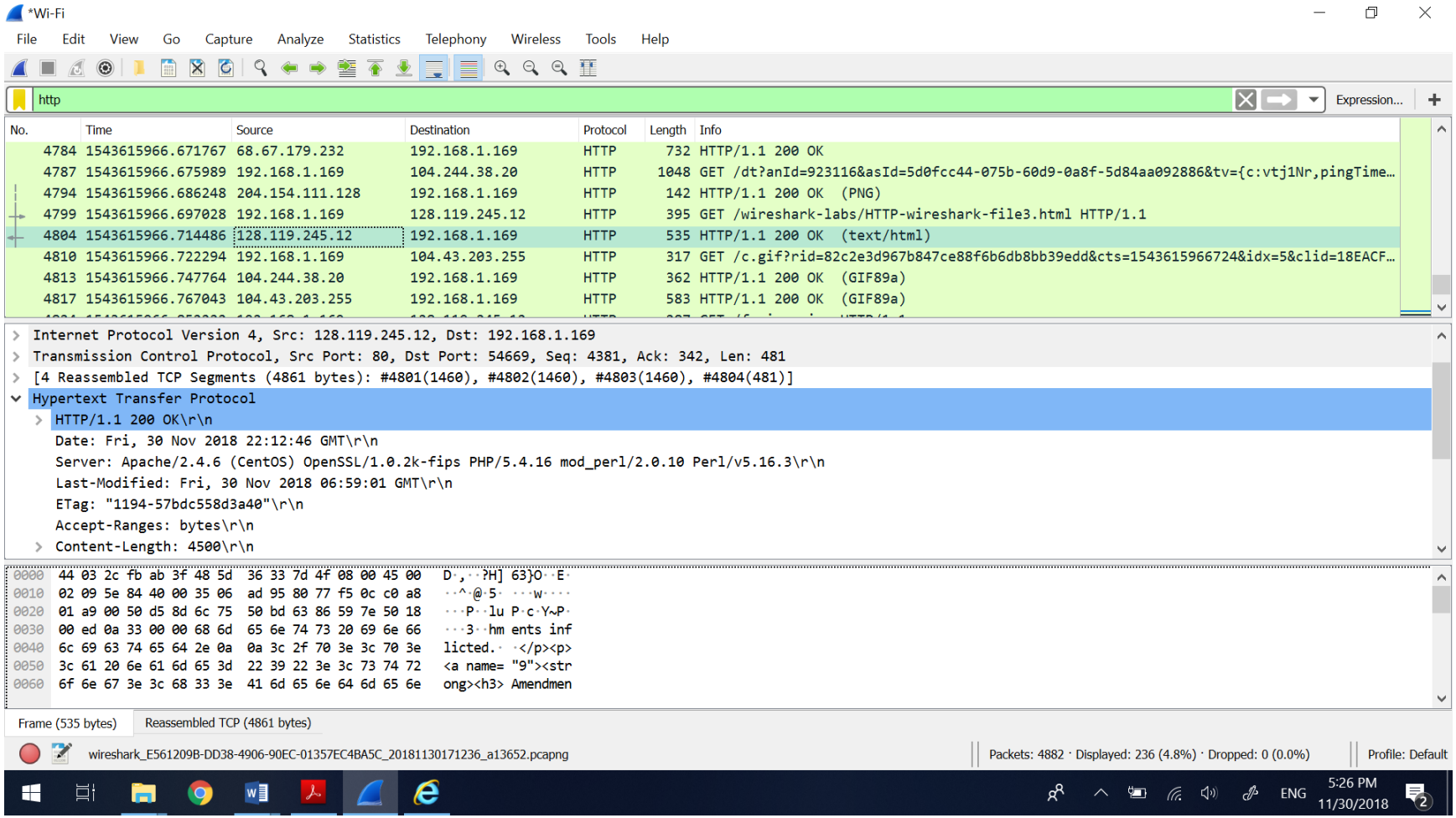
Which packet number in the trace contains the GET message for the Bill or Rights?

Answer: 4799



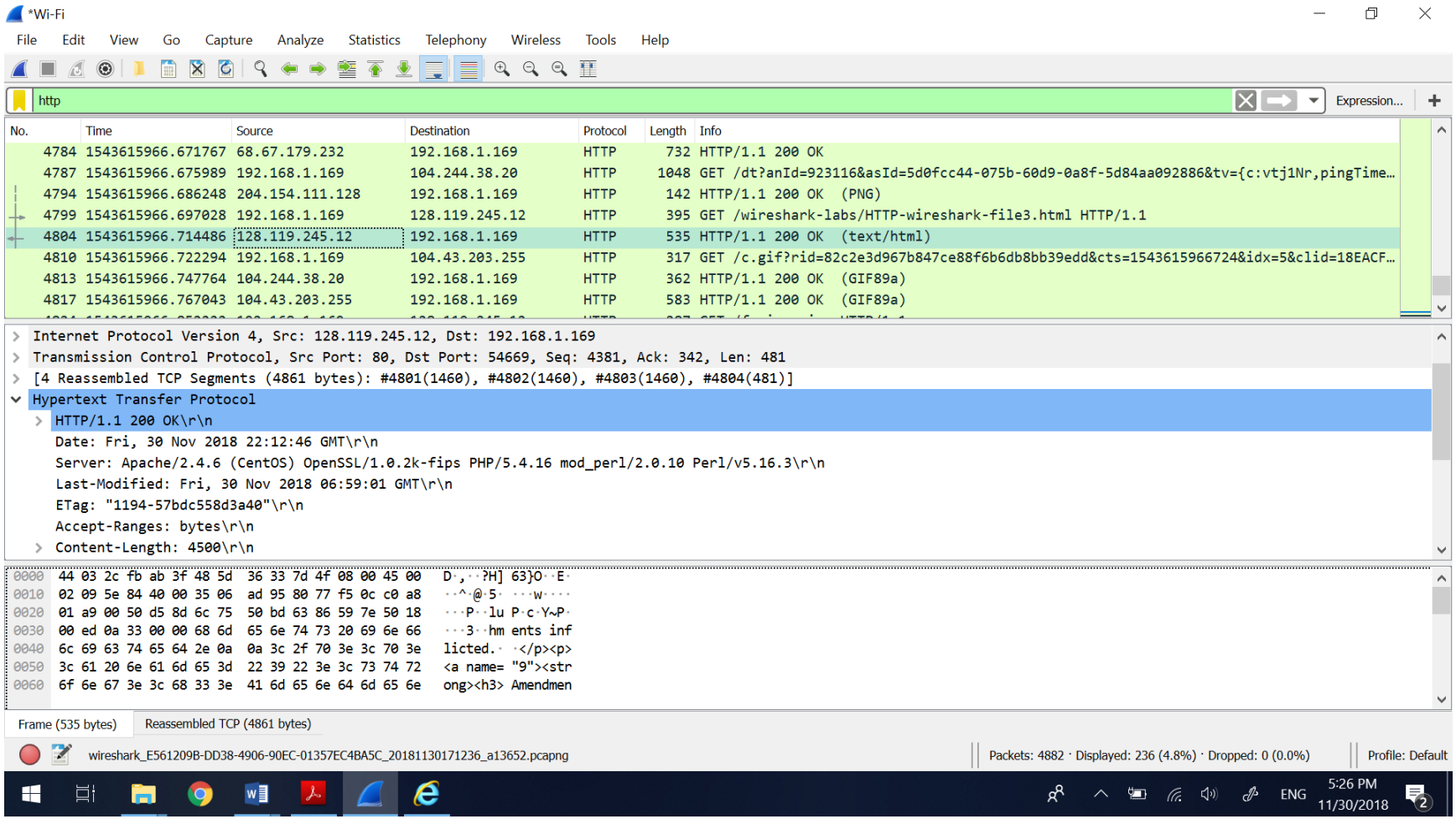
2. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?

Answer: 4804



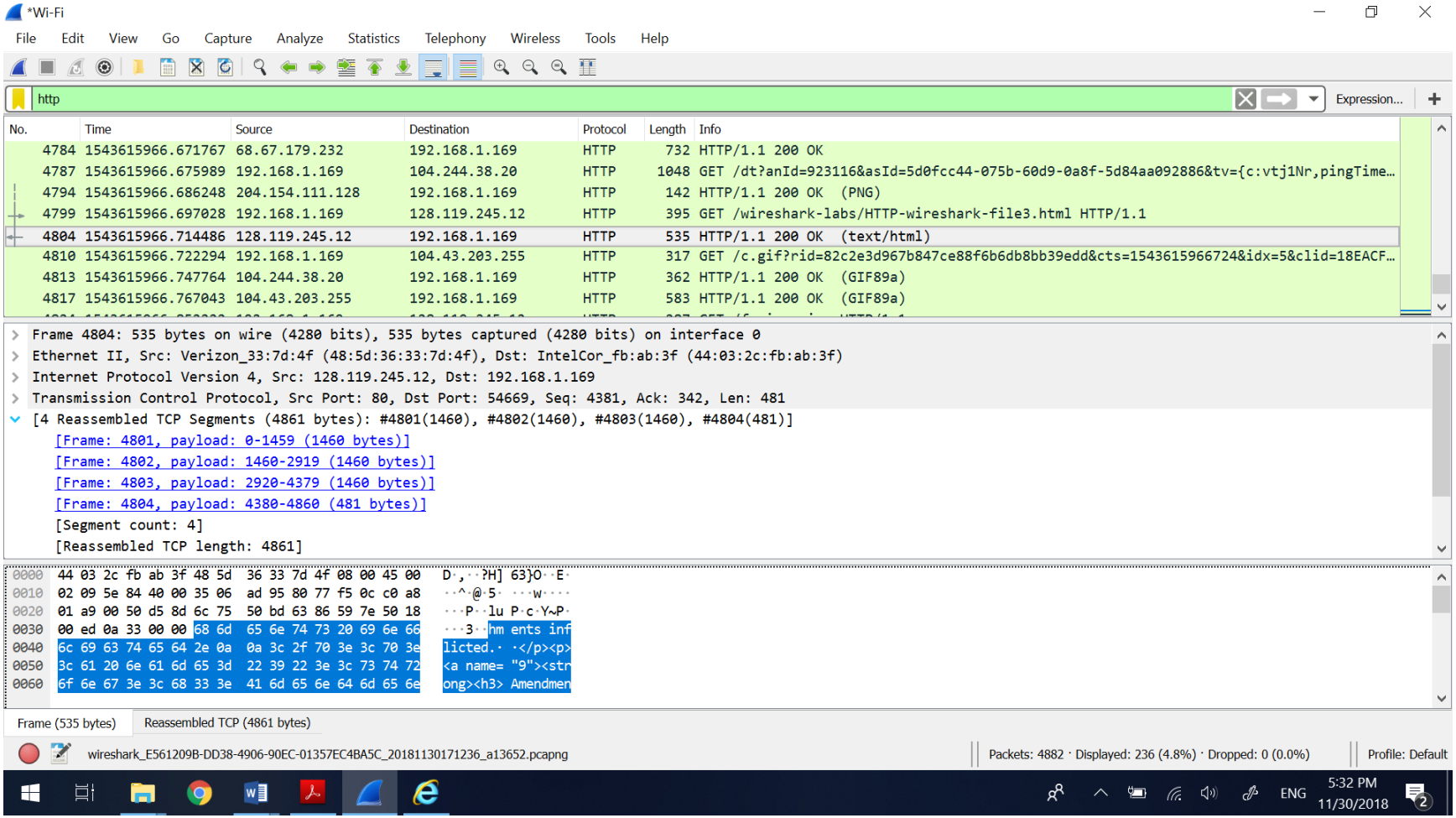
3. What is the status code and phrase in the response?

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



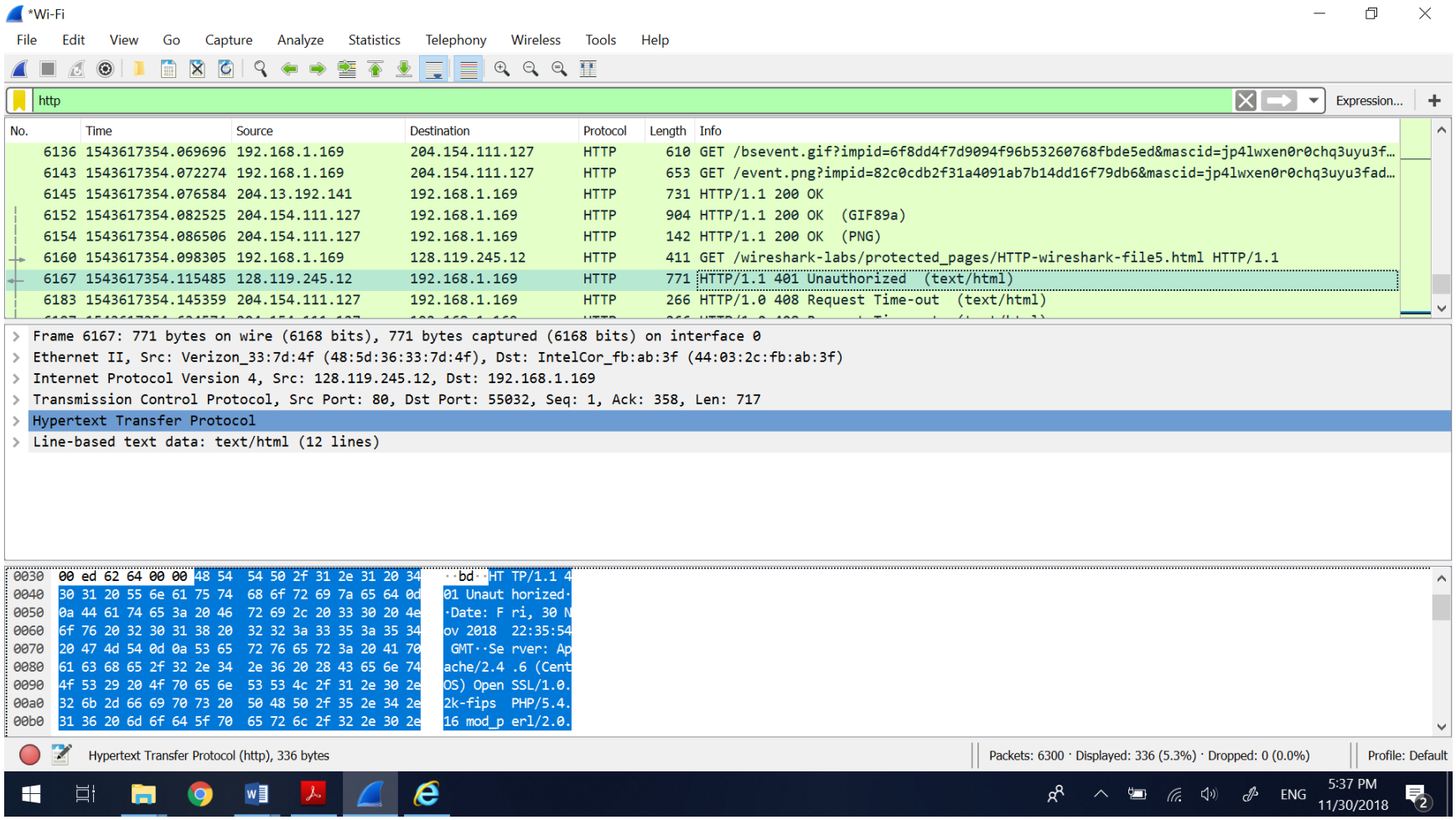
4. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?

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



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

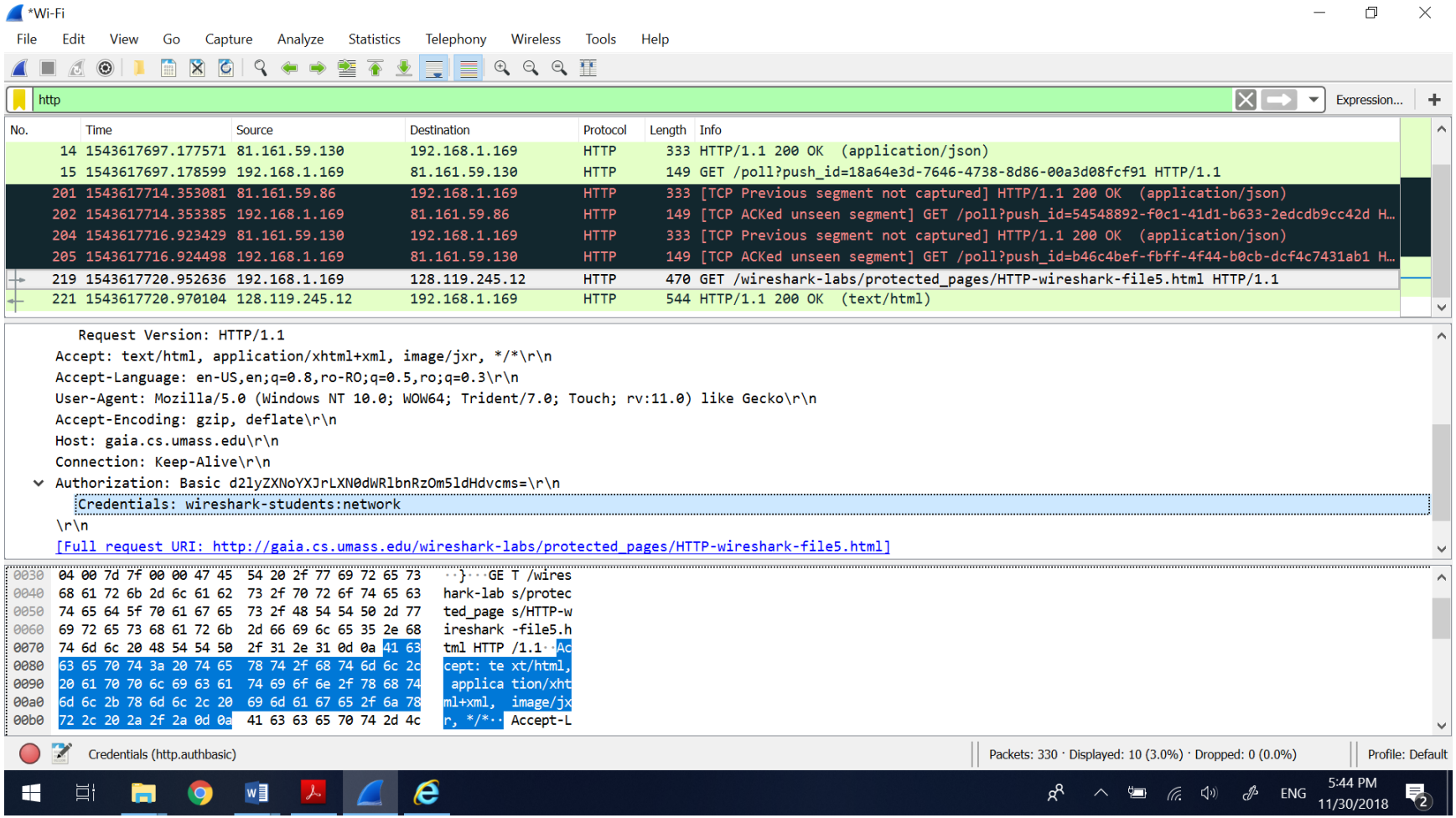
Answer: 6167 1543617354.115485 128.119.245.12 192.168.1.169 HTTP 771 HTTP/1.1 401 Unauthorized (text/html)



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

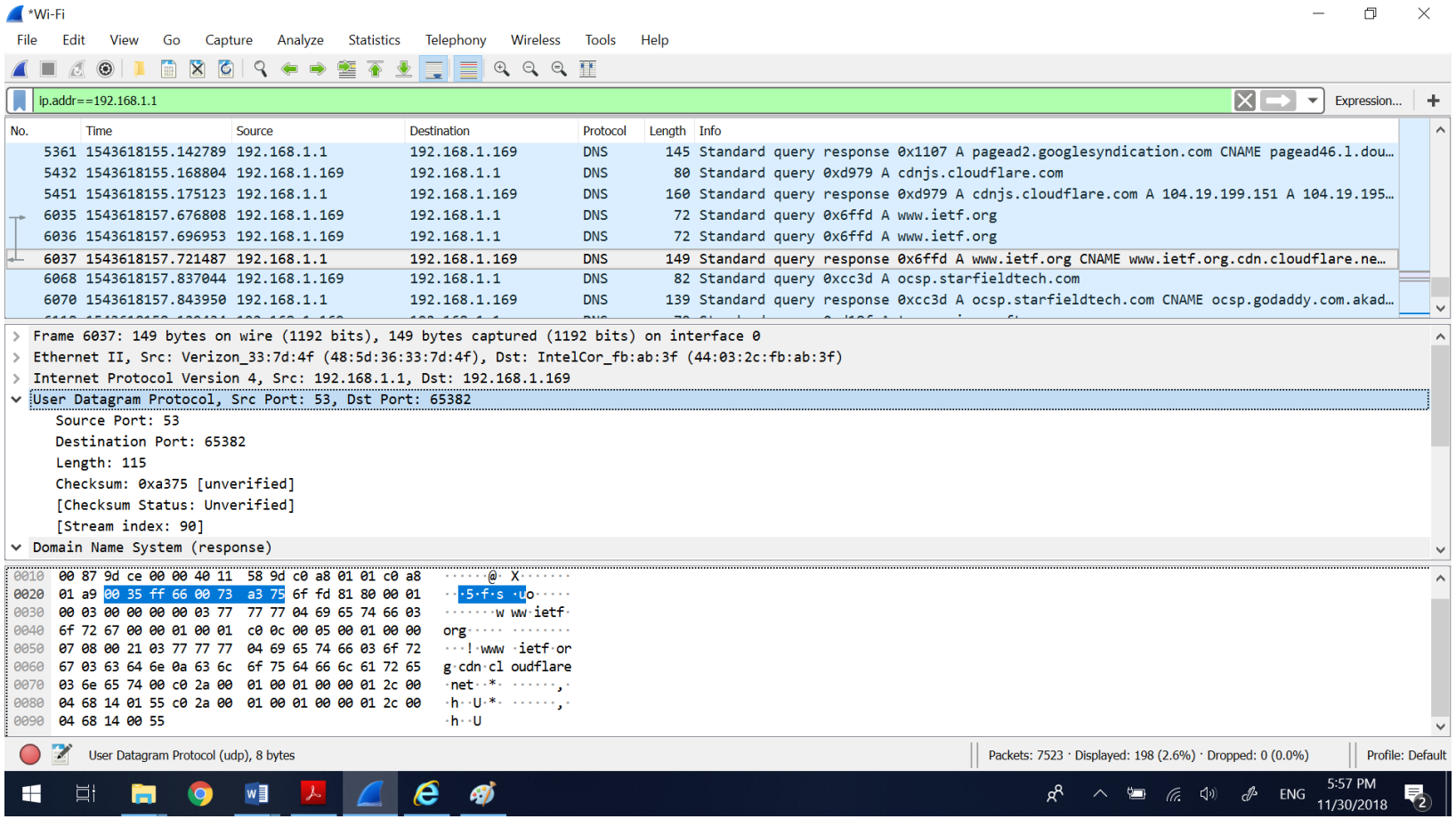


7. Locate the DNS query and response messages. Are they sent over UDP or TCP?

Answer: 6035 1543618157.676808 192.168.1.169 192.168.1.1 DNS 72 Standard query 0x6ffd A www.ietf.org

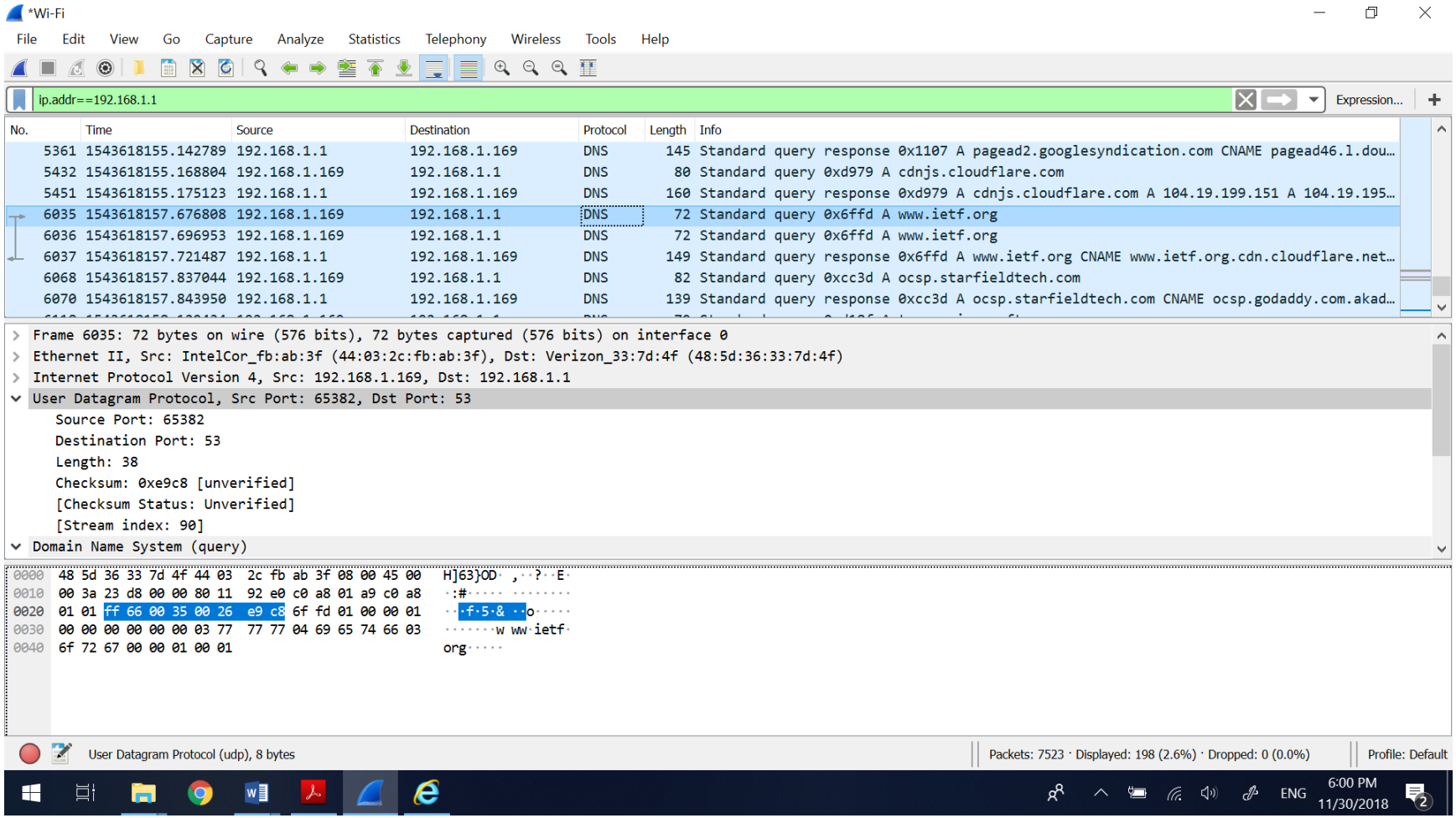
6037 1543618157.721487 192.168.1.1 192.168.1.169 DNS 149 Standard query response 0x6ffd A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.20.1.85 A 104.20.0.85

They are sent over UDP.



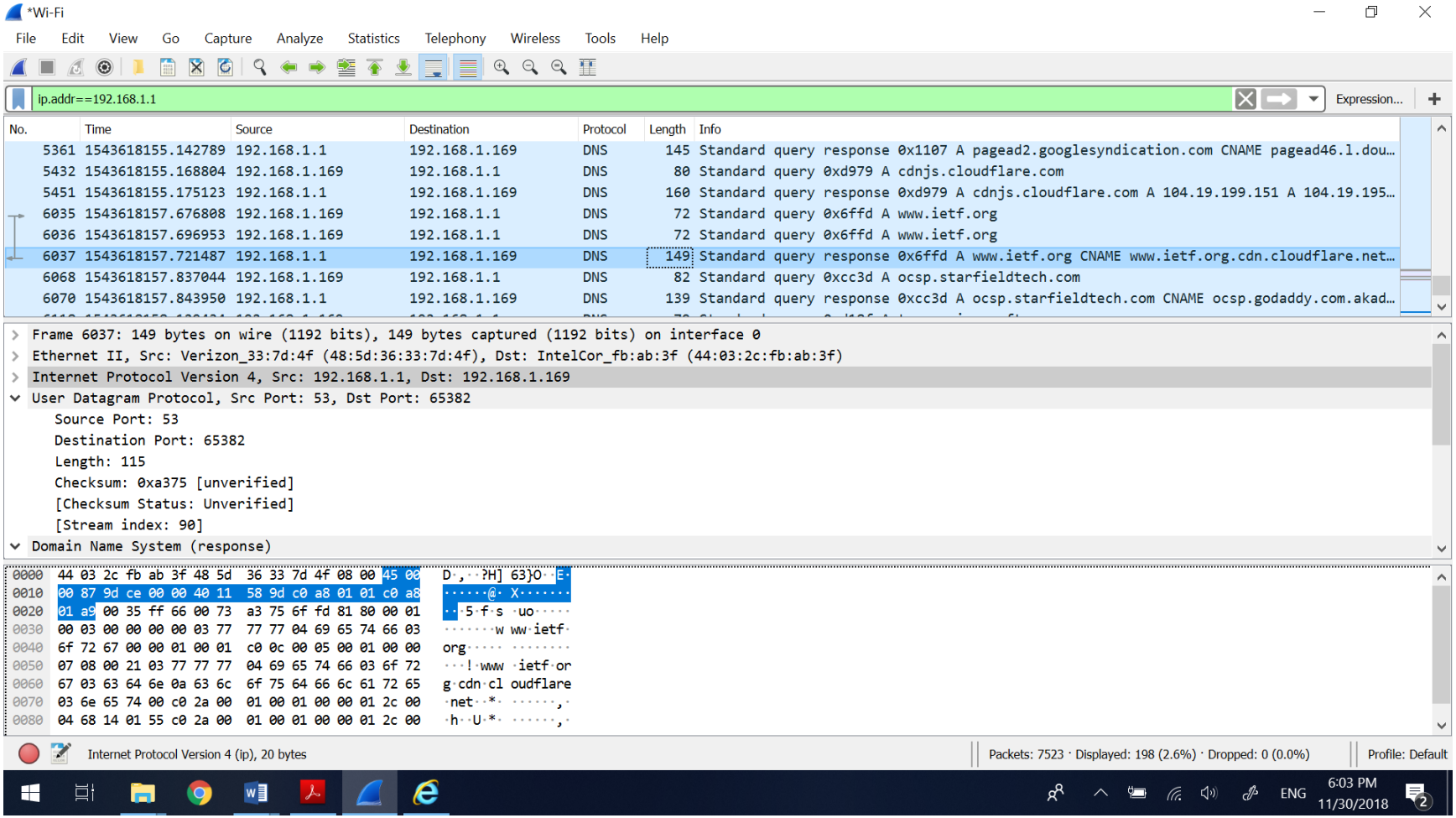
8. What is the destination port for the DNS query message?

Answer: Destination Port: 53 for Dst: 192.168.1.1



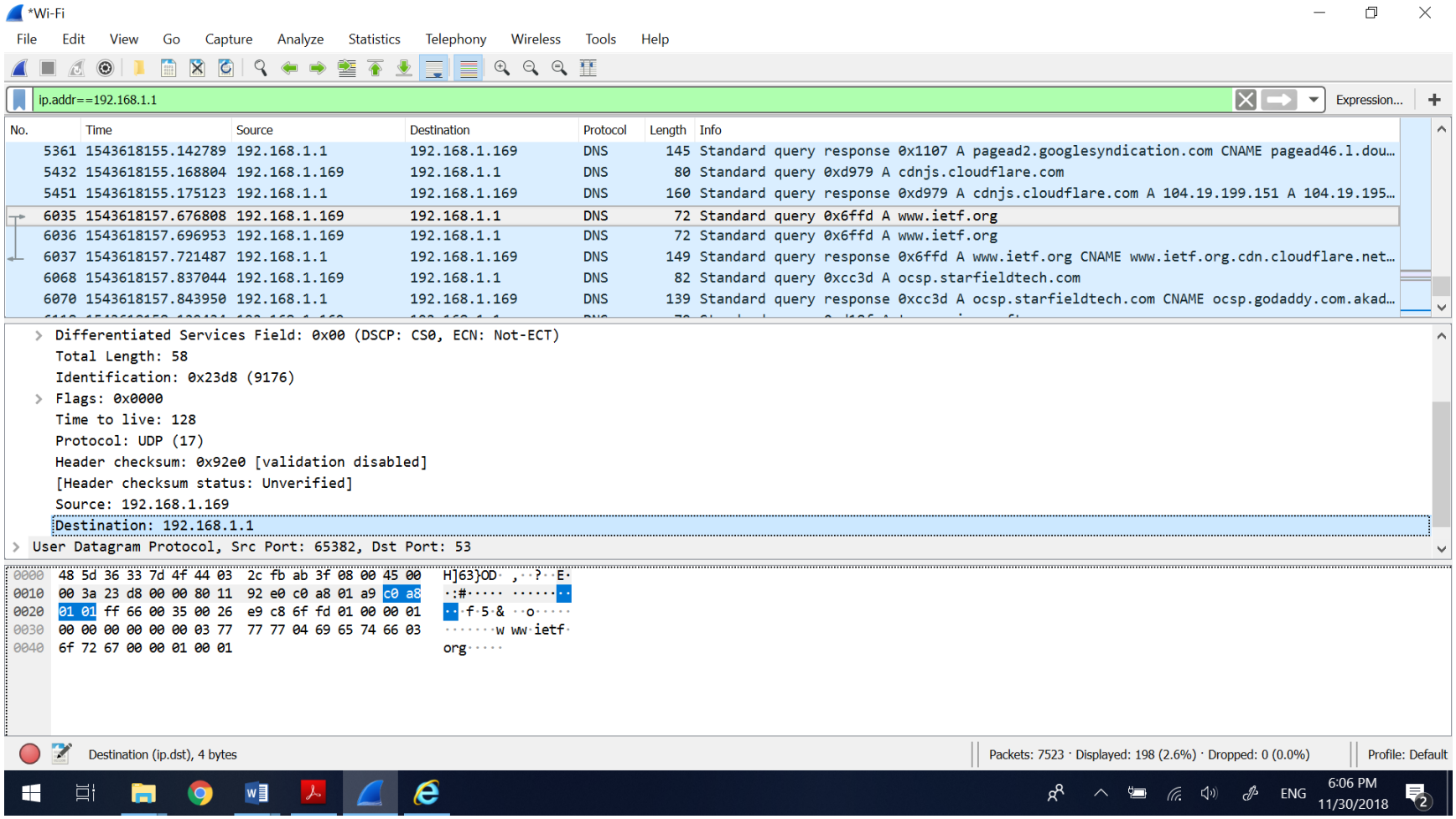
9. What is the source port of DNS response message?

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



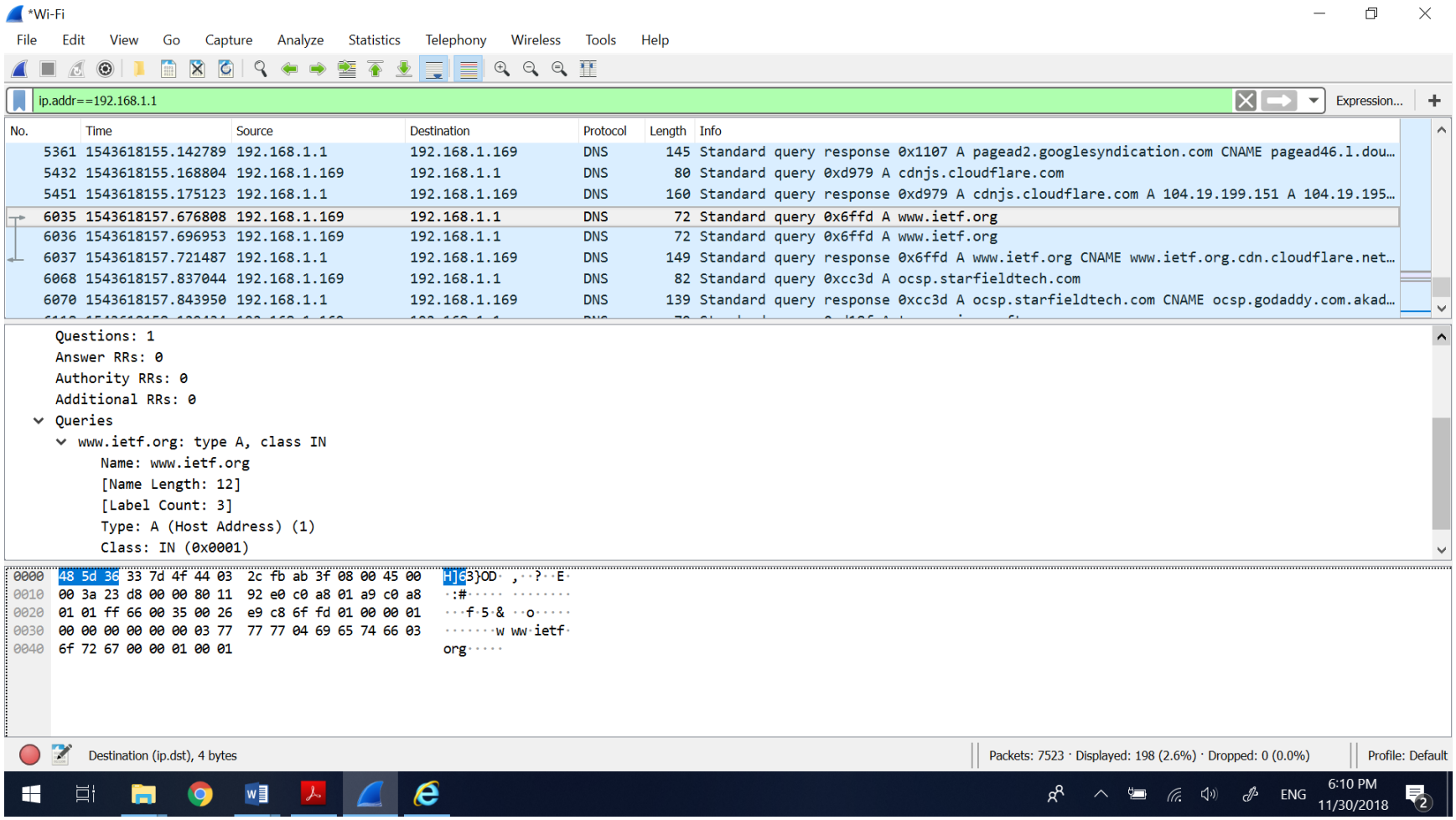
10. To what IP address is the DNS query message sent?

Answer: Destination: 192.168.1.1



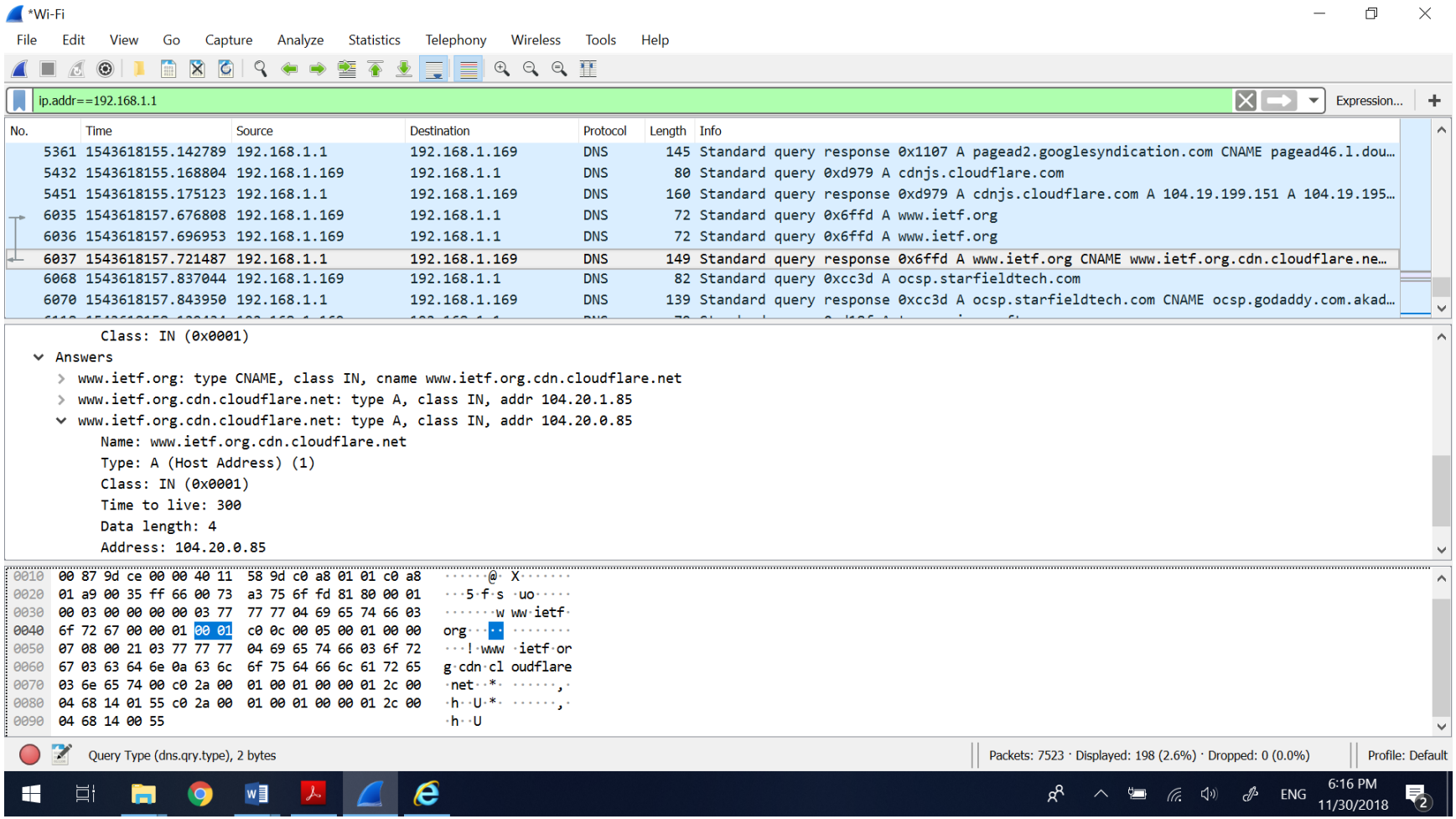
11. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

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

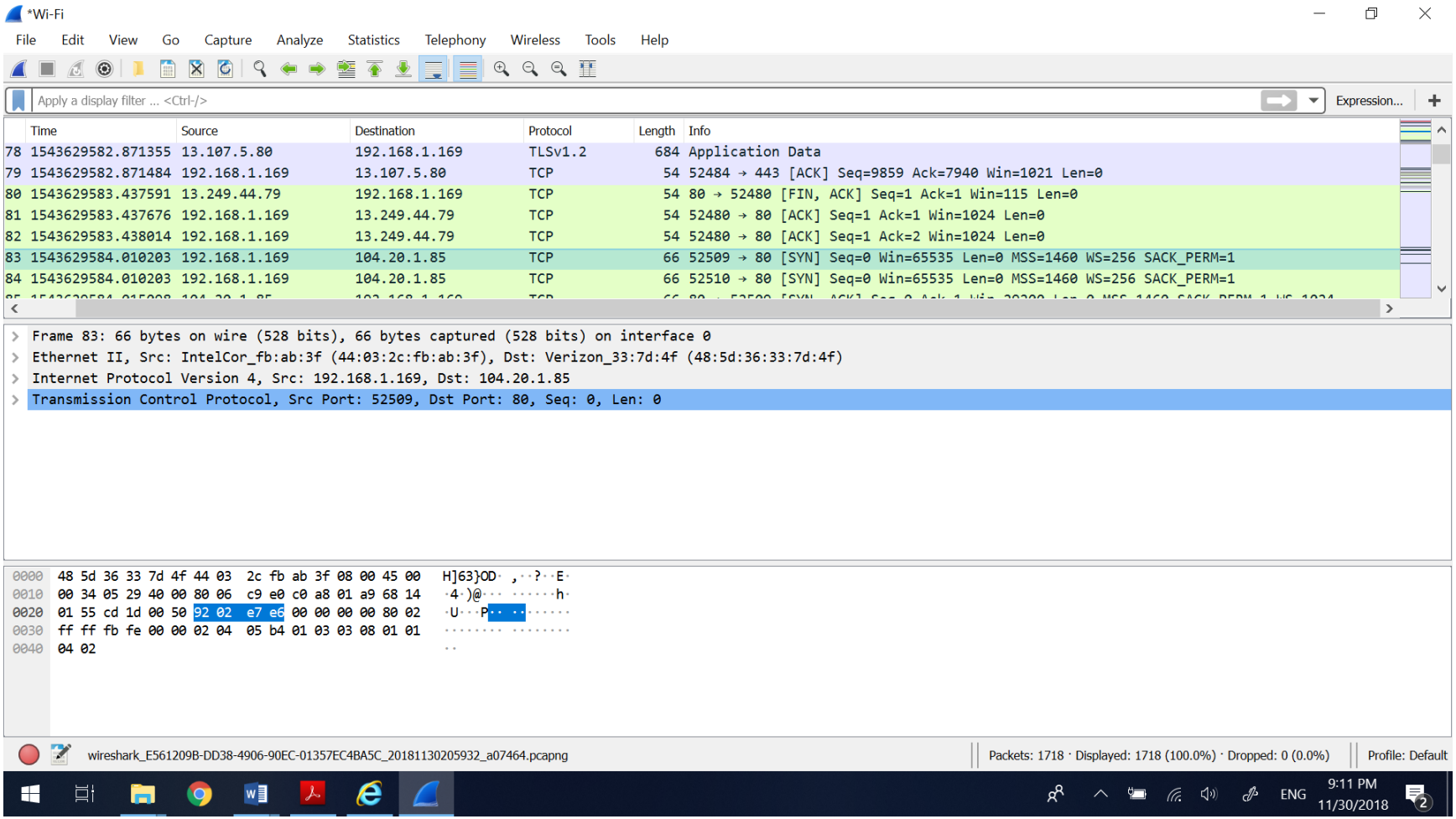


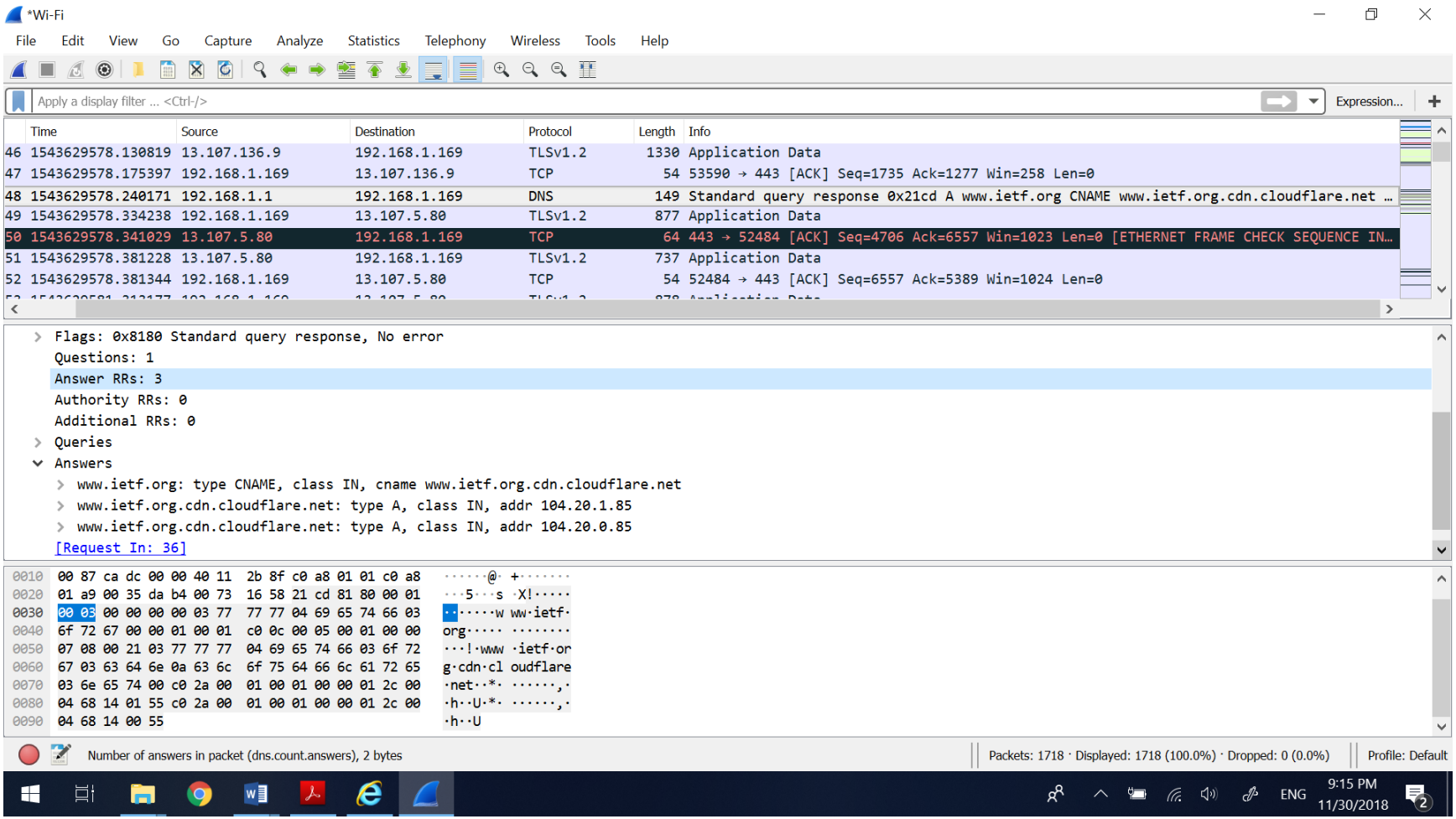
12. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

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



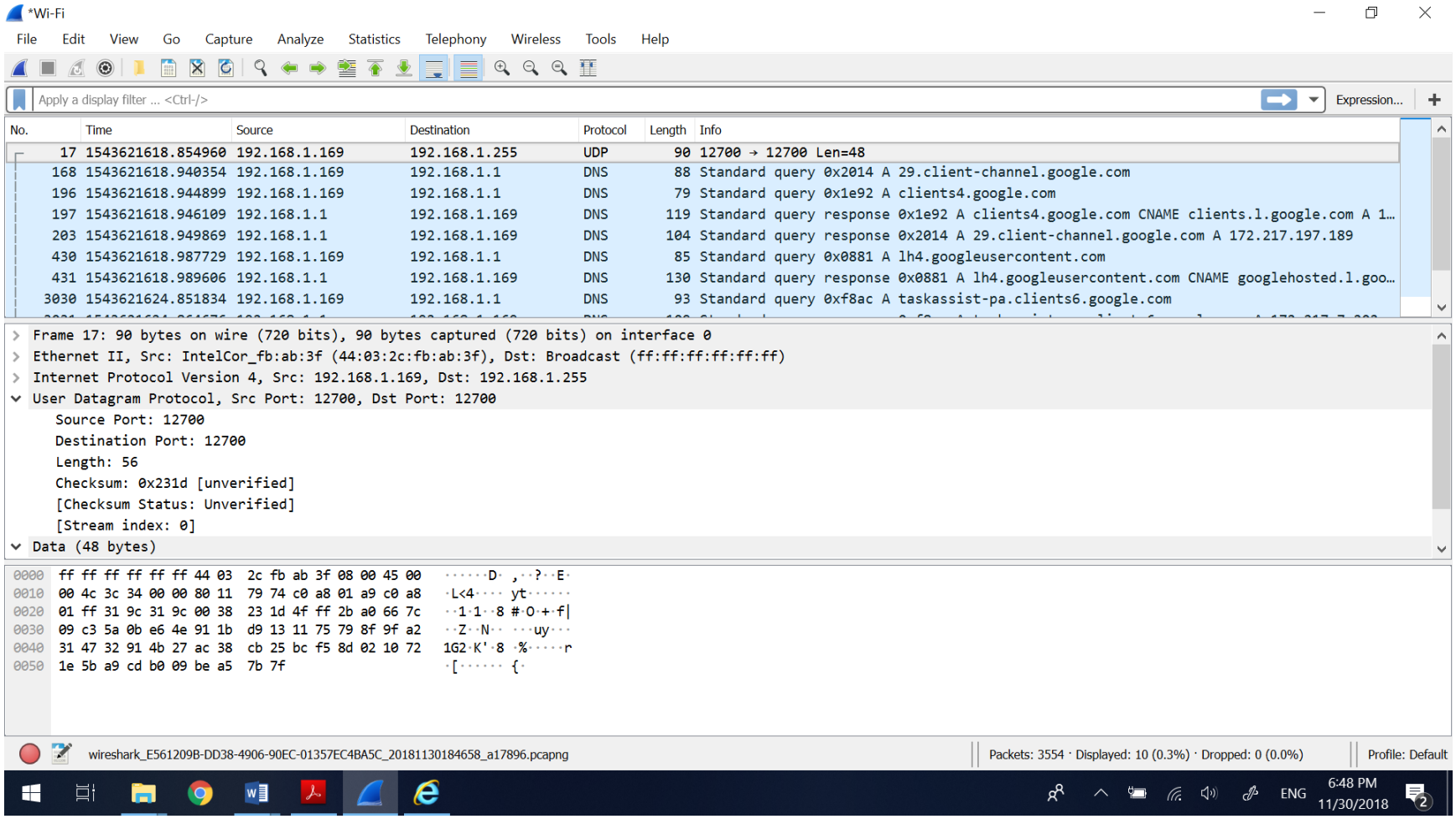
13. Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message? : Yes, the destination IP address of the SYN packet is 104.20.1.85, the same as the second answer in the DNS response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




*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
Flags: 0x8180 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 oudflare
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
ENG
9:15 PM
11/30/2018

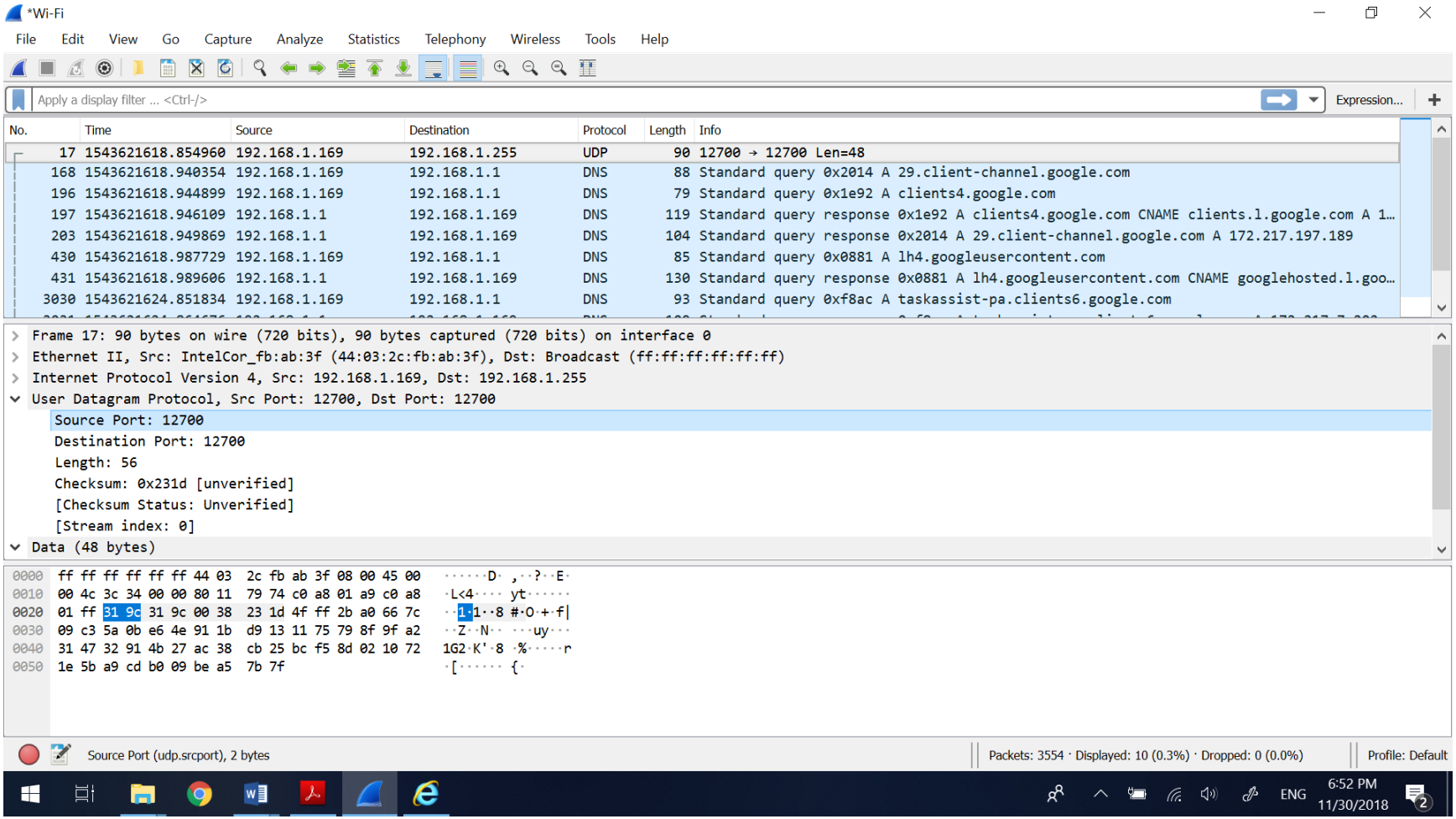
14. Select one UDP packet from your trace. From this packet, determine how many fields there are in the UDP header

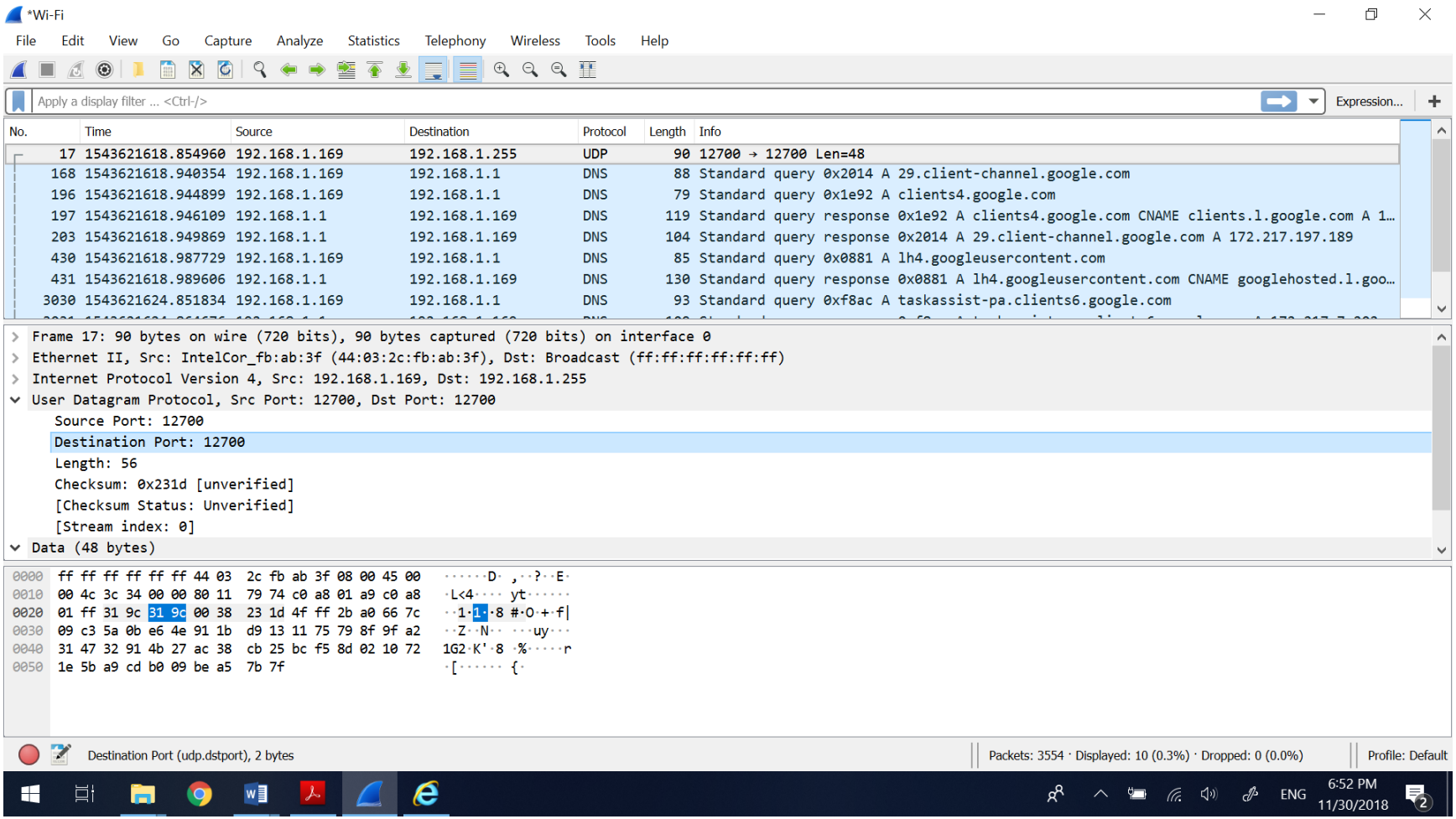
Answer: four (4): source port; destination port; length; checksum.

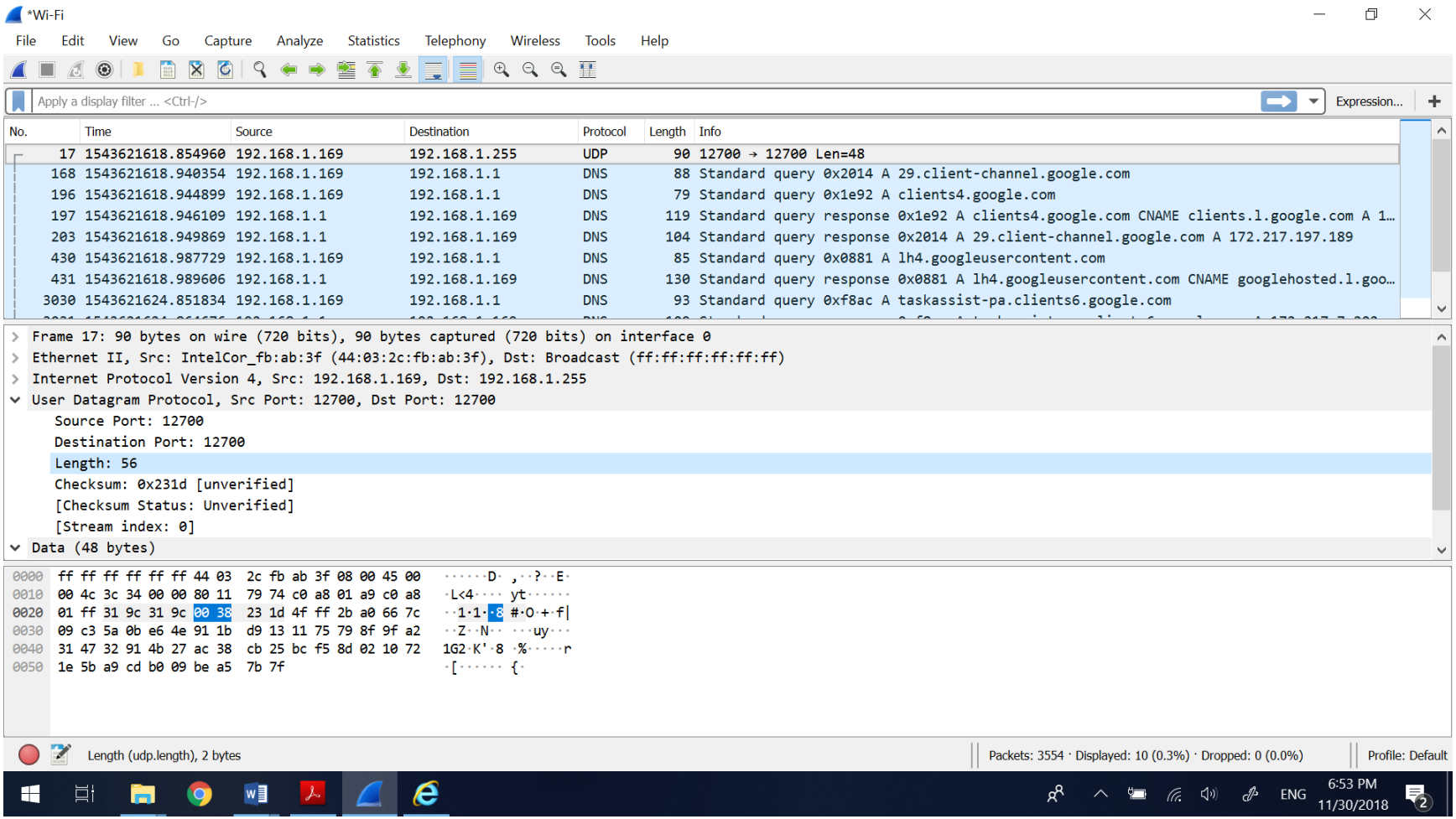


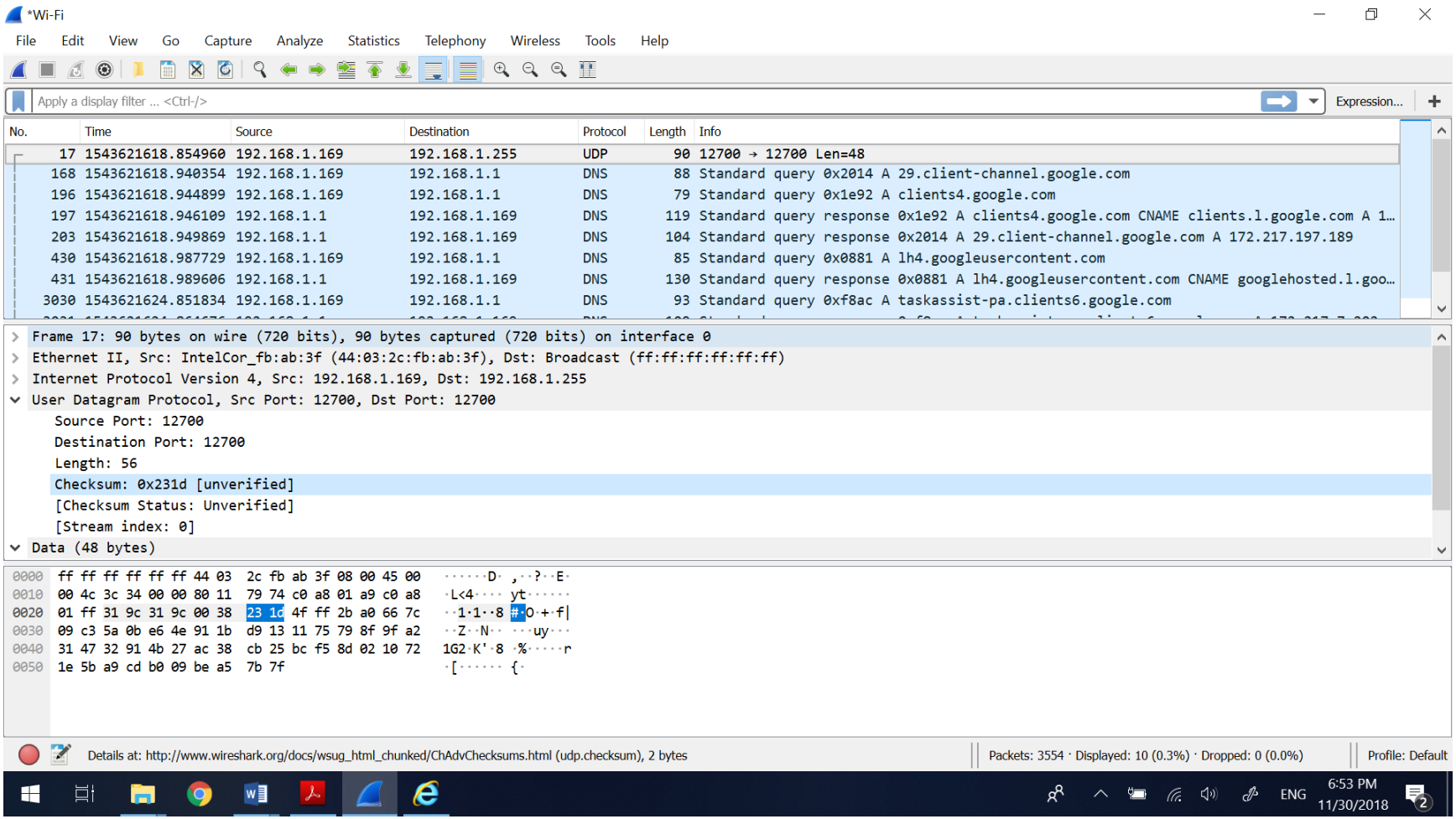
15. By consulting the displayed information in Wireshark's packet content field for this packet, determine the length (in bytes) of each of the UDP header fields.

Answer: each is 2 bytes.



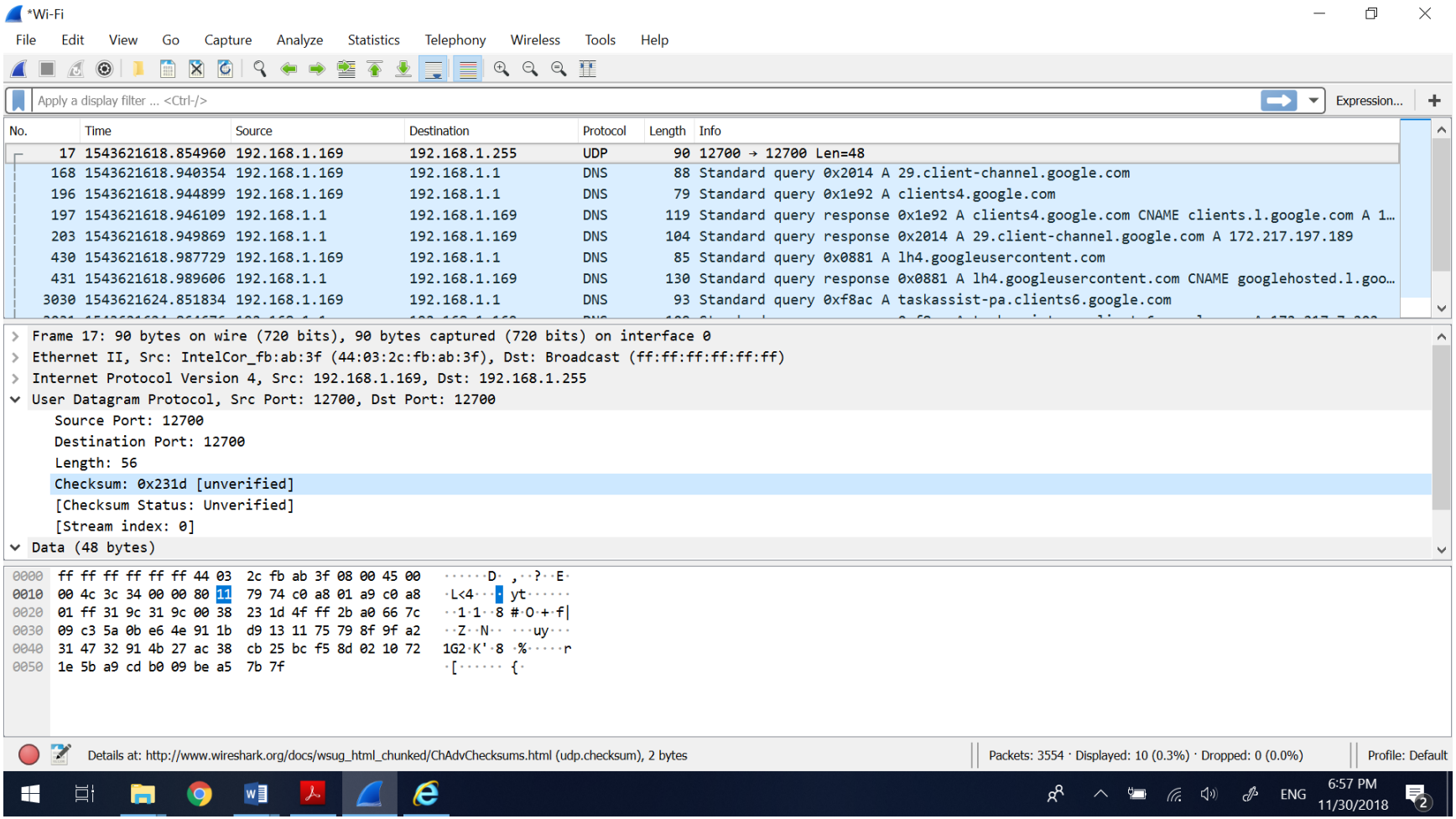

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
17 1543621618.854960 192.168.1.169 192.168.1.255 UDP 90 12700 → 12700 Len=48
168 1543621618.940354 192.168.1.169 192.168.1.1 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 1543621618.946109 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.l.goo…
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
0010 00 4c 3c 34 00 00 80 11 79 74 c0 a8 01 a9 c0 a8
0020 01 ff 31 9c 31 9c 00 38 23 1d 4f ff 2b a0 66 7c
0030 09 c3 5a 0b e6 4e 91 1b d9 13 11 75 79 8f 9f a2
0040 31 47 32 91 4b 27 ac 38 cb 25 bc f5 8d 02 10 72
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
ENG
6:52 PM
11/30/2018

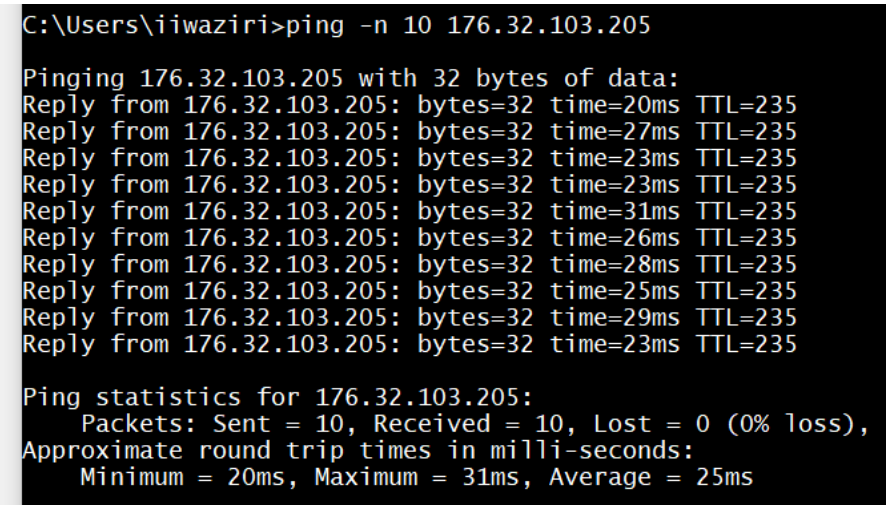

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
17 1543621618.854960 192.168.1.169 192.168.1.255 UDP 90 12700 → 12700 Len=48
168 1543621618.940354 192.168.1.169 192.168.1.1 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 1543621618.946109 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.l.goo…
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
0010 00 4c 3c 34 00 00 80 11 79 74 c0 a8 01 a9 c0 a8
0020 01 ff 31 9c 31 9c 00 38 23 1d 4f ff 2b a0 66 7c
0030 09 c3 5a 0b e6 4e 91 1b d9 13 11 75 79 8f 9f a2
0040 31 47 32 91 4b 27 ac 38 cb 25 bc f5 8d 02 10 72
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
ENG
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 1543621618.946109 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.l.goo…
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
0010 00 4c 3c 34 00 00 80 11 79 74 c0 a8 01 a9 c0 a8
0020 01 ff 31 9c 31 9c 00 38 23 1d 4f ff 2b a0 66 7c
0030 09 c3 5a 0b e6 4e 91 1b d9 13 11 75 79 8f 9f a2
0040 31 47 32 91 4b 27 ac 38 cb 25 bc f5 8d 02 10 72
0050 1e 5b a9 cd b0 09 be a5 7b 7f
Details at: 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
ENG
6:53 PM
11/30/2018

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 (playload+header) . Data is 48. Each header is 2. Therefore 48+2+2+2+2=56.





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

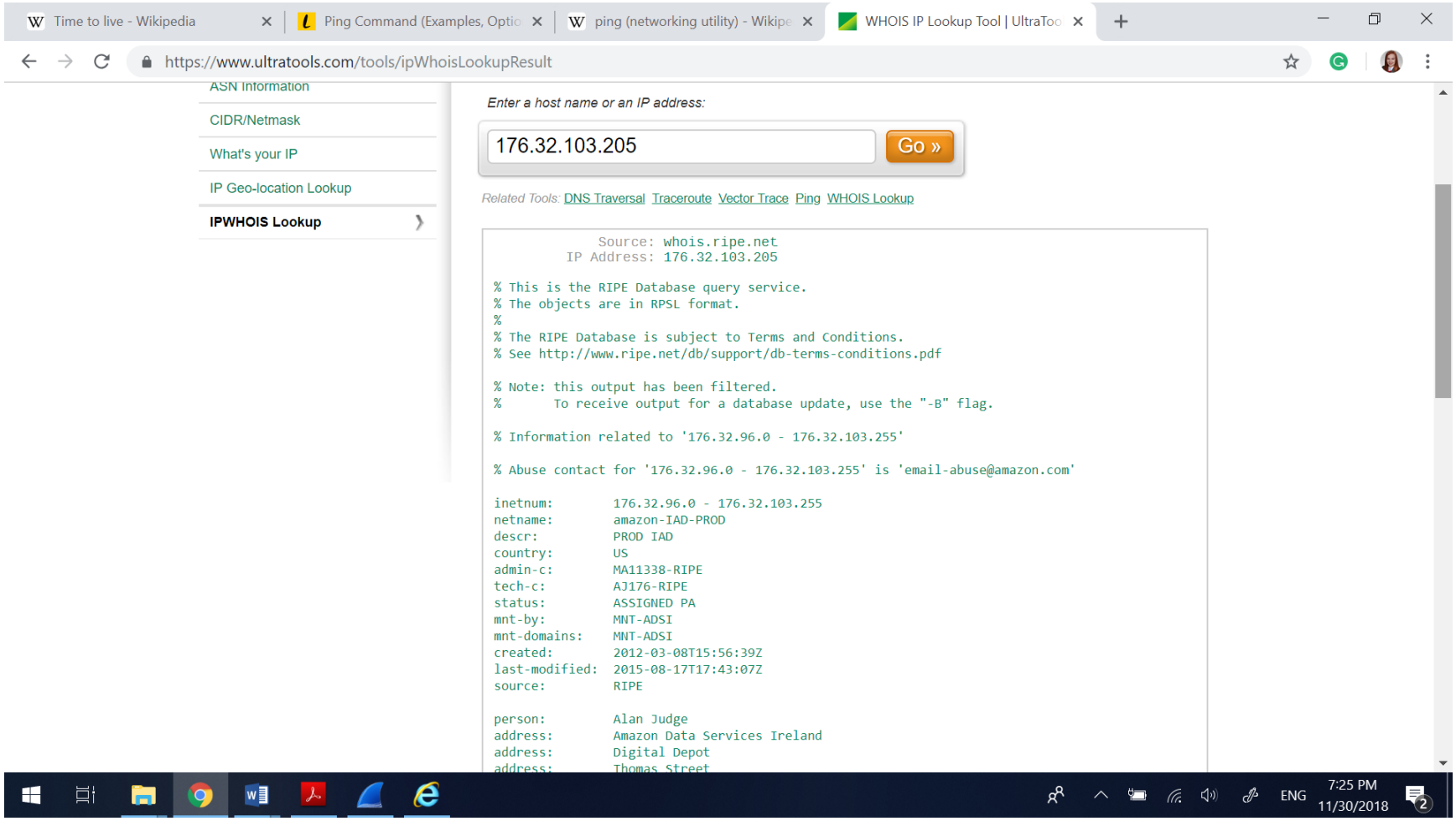
Answer: The ping command is used in the Command Prompt where the source “iiwasiri” reaches the destination IP 176.32.103.205. This computer is communication with another computer within the network. The command uses also -n count that is option that sets the number of ICMP Echo Requests to send, from 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?

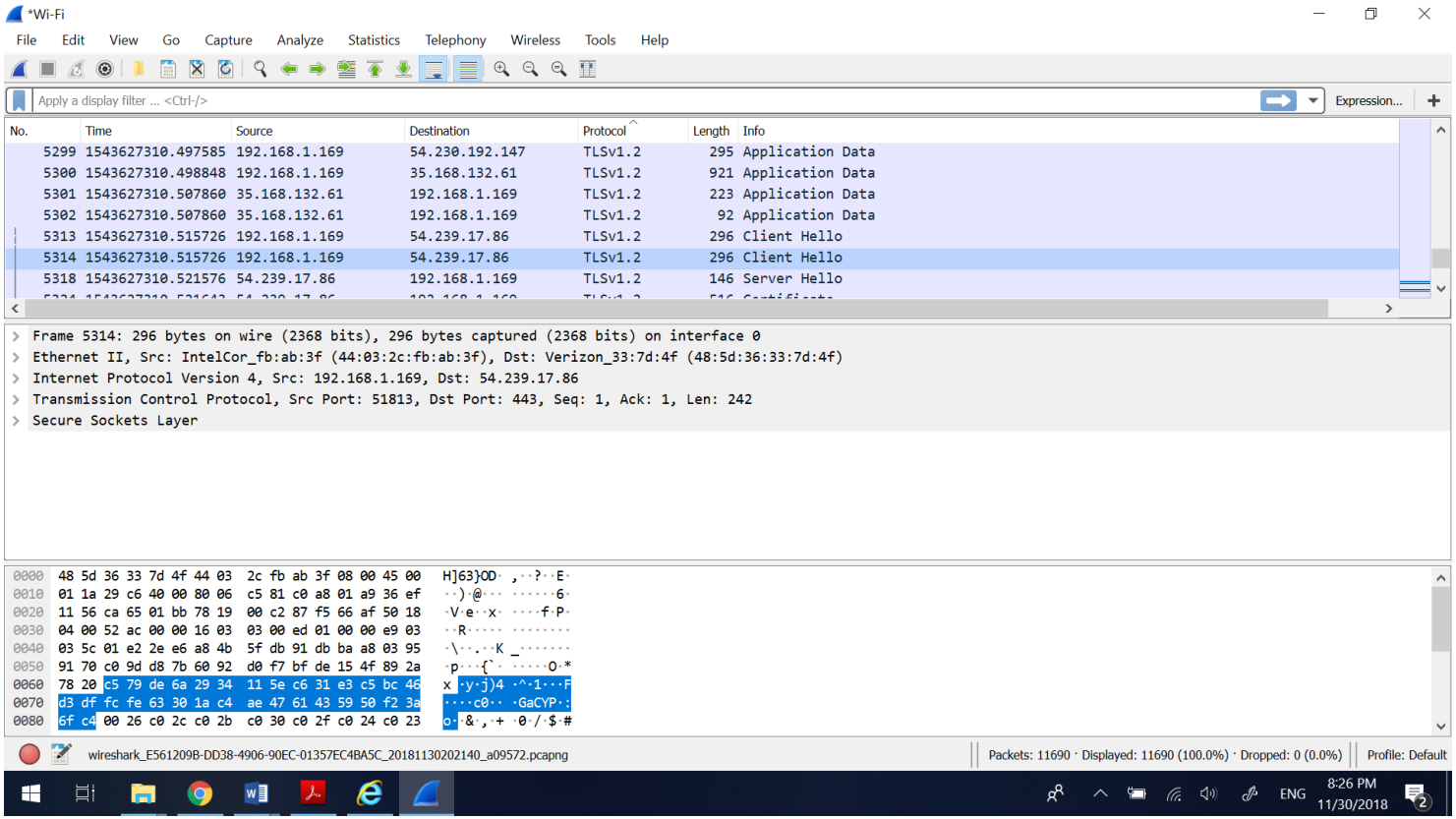
Answer: Amazon



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)

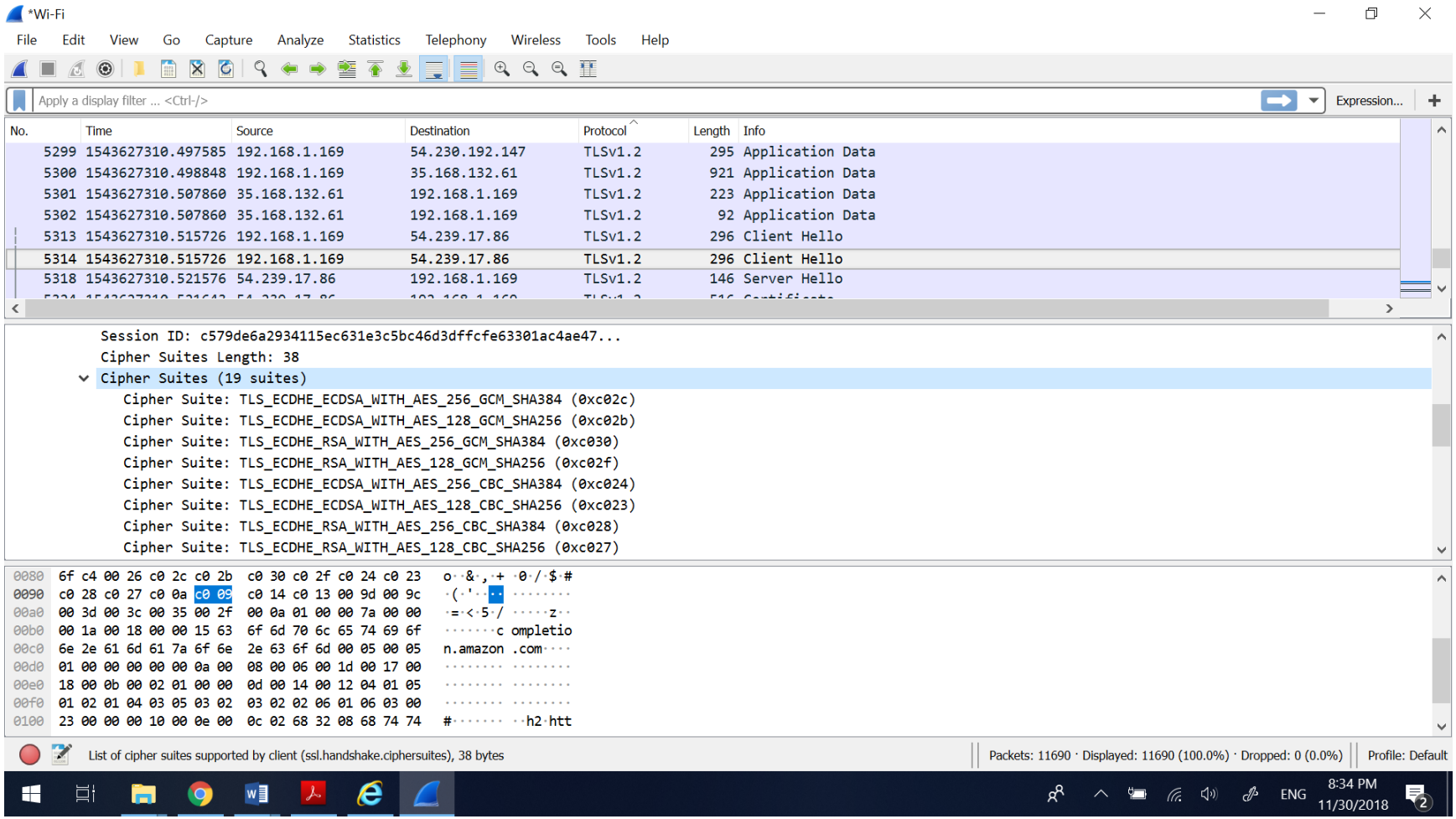
Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)

Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c)

Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)

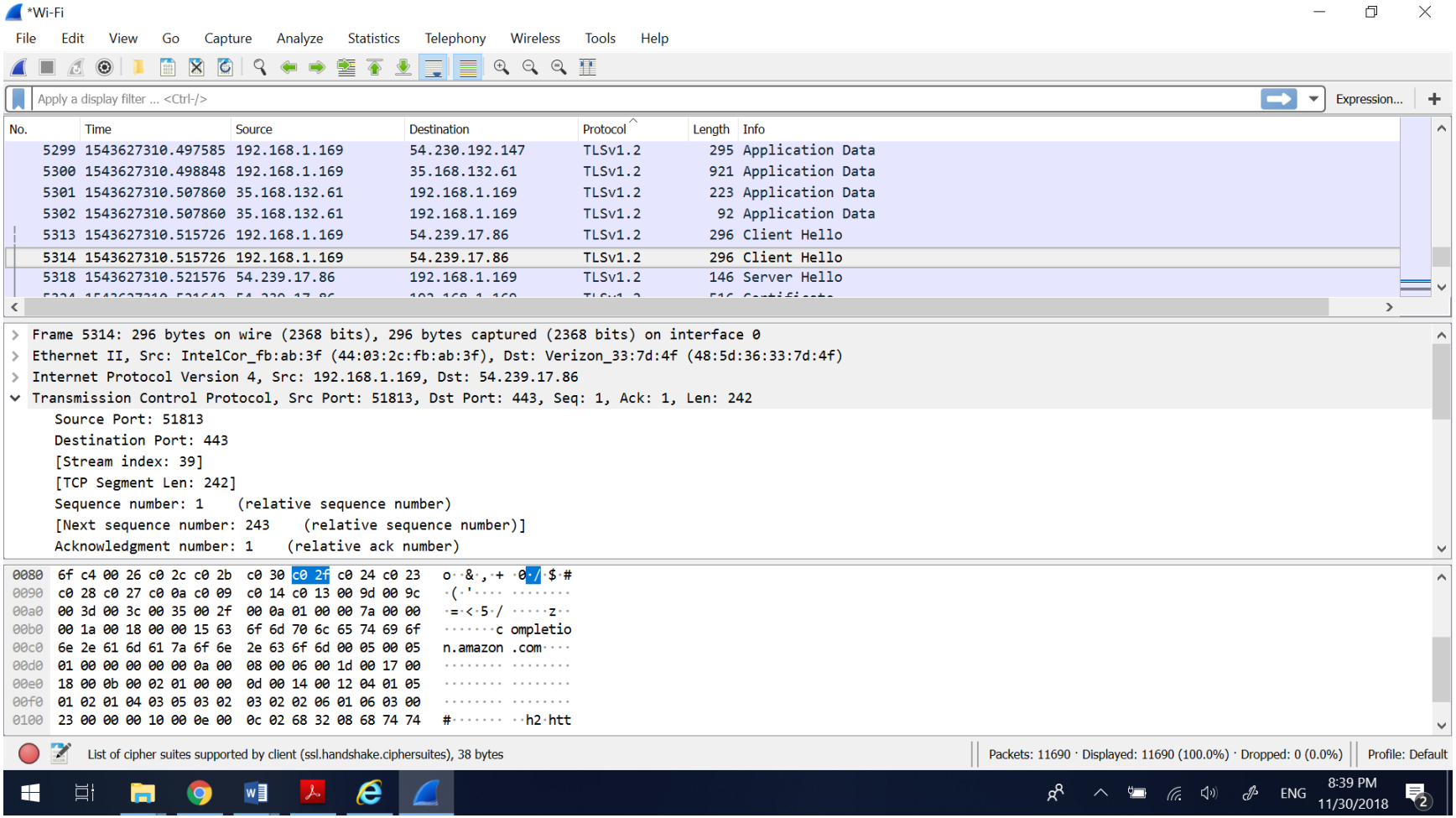
Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)

Cipher Suite: TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)



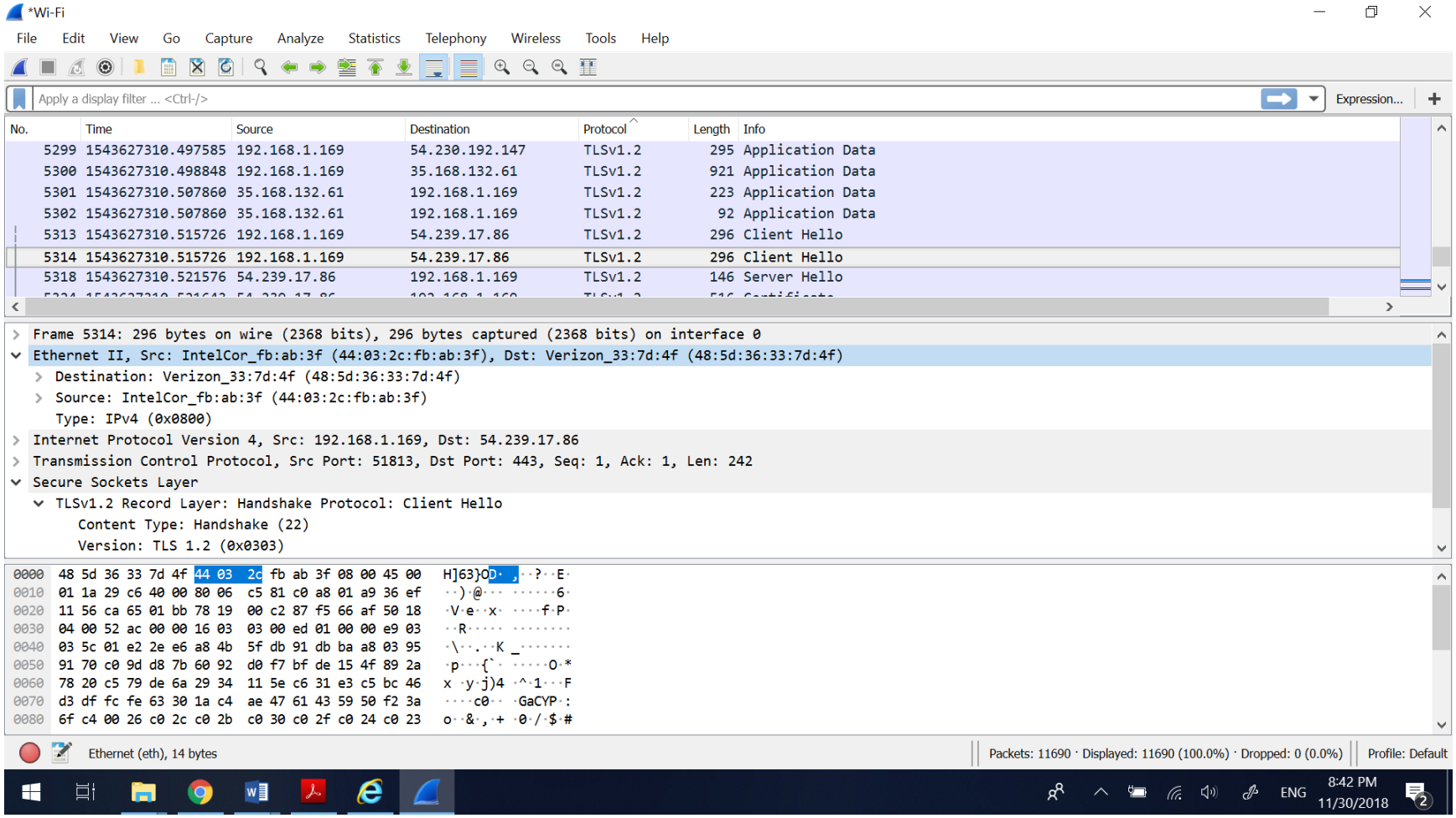
23. What TCP port number is used by the “Client Hello” packet, and why is it using that port number?

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



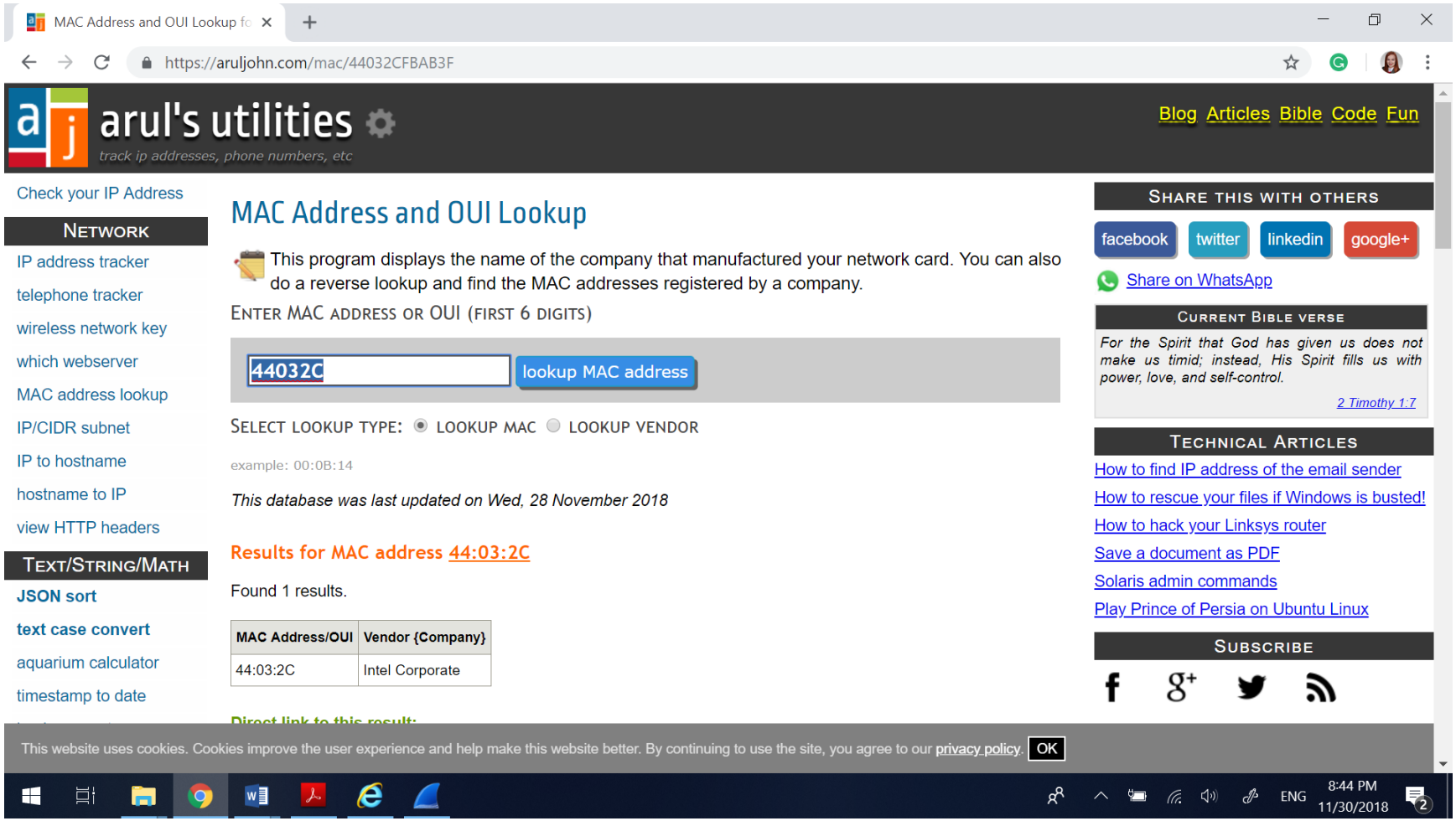
24. What are the source and destination MAC address?

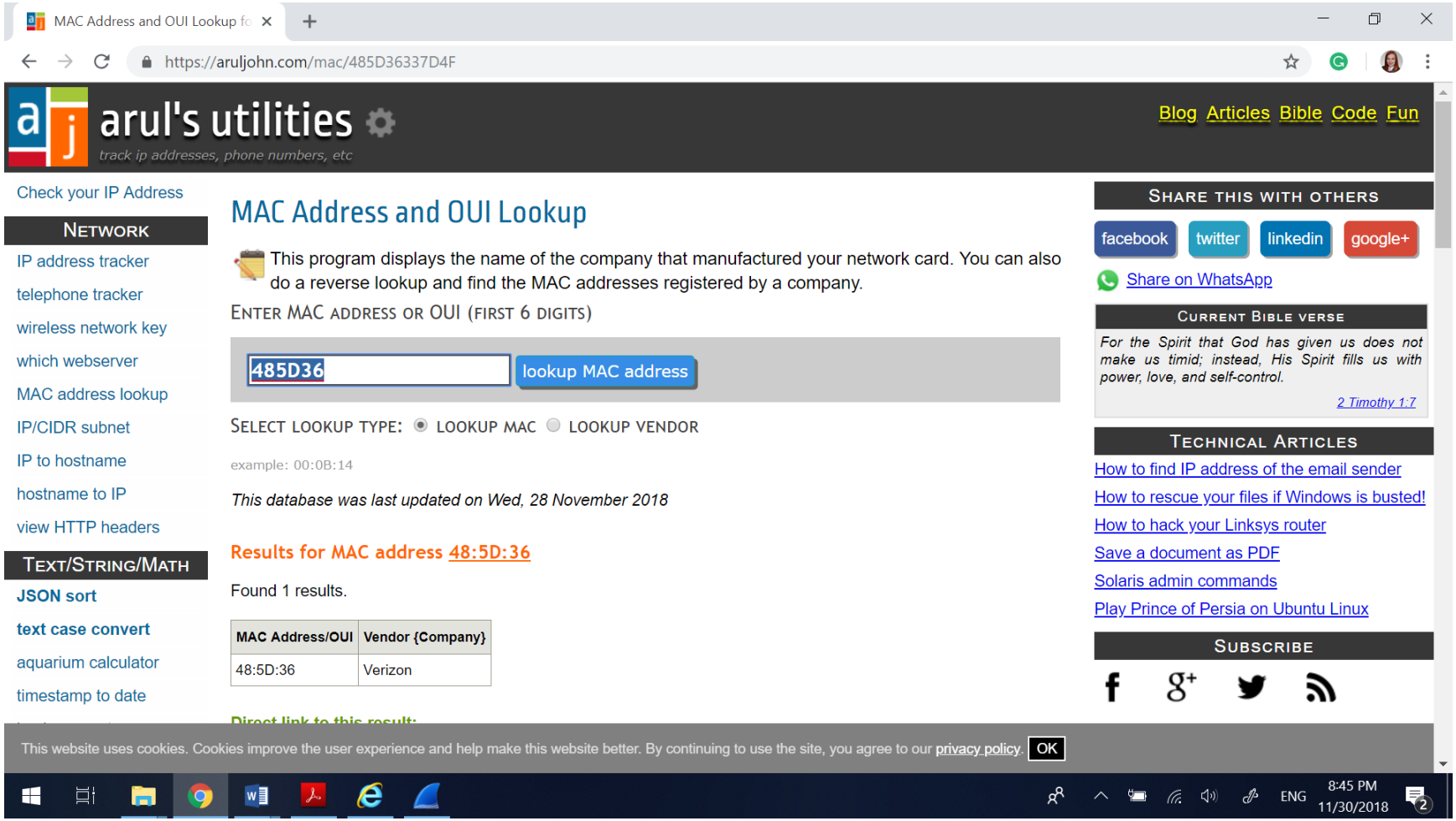
Answer:, Src: (44:03:2c:fb:ab:3f), Dst: (48:5d:36:33:7d:4f)



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

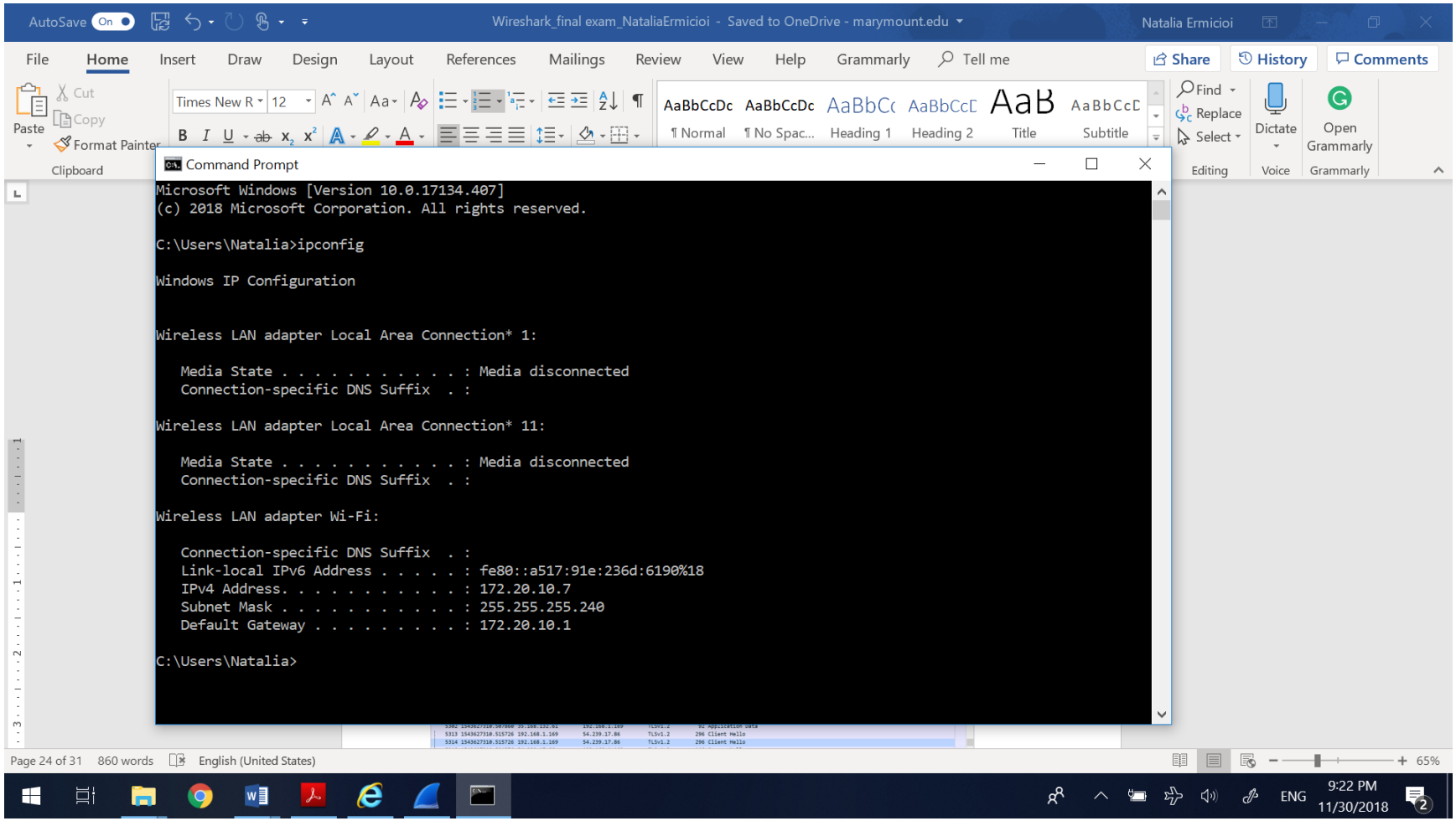
Answer: Intel & Verizon

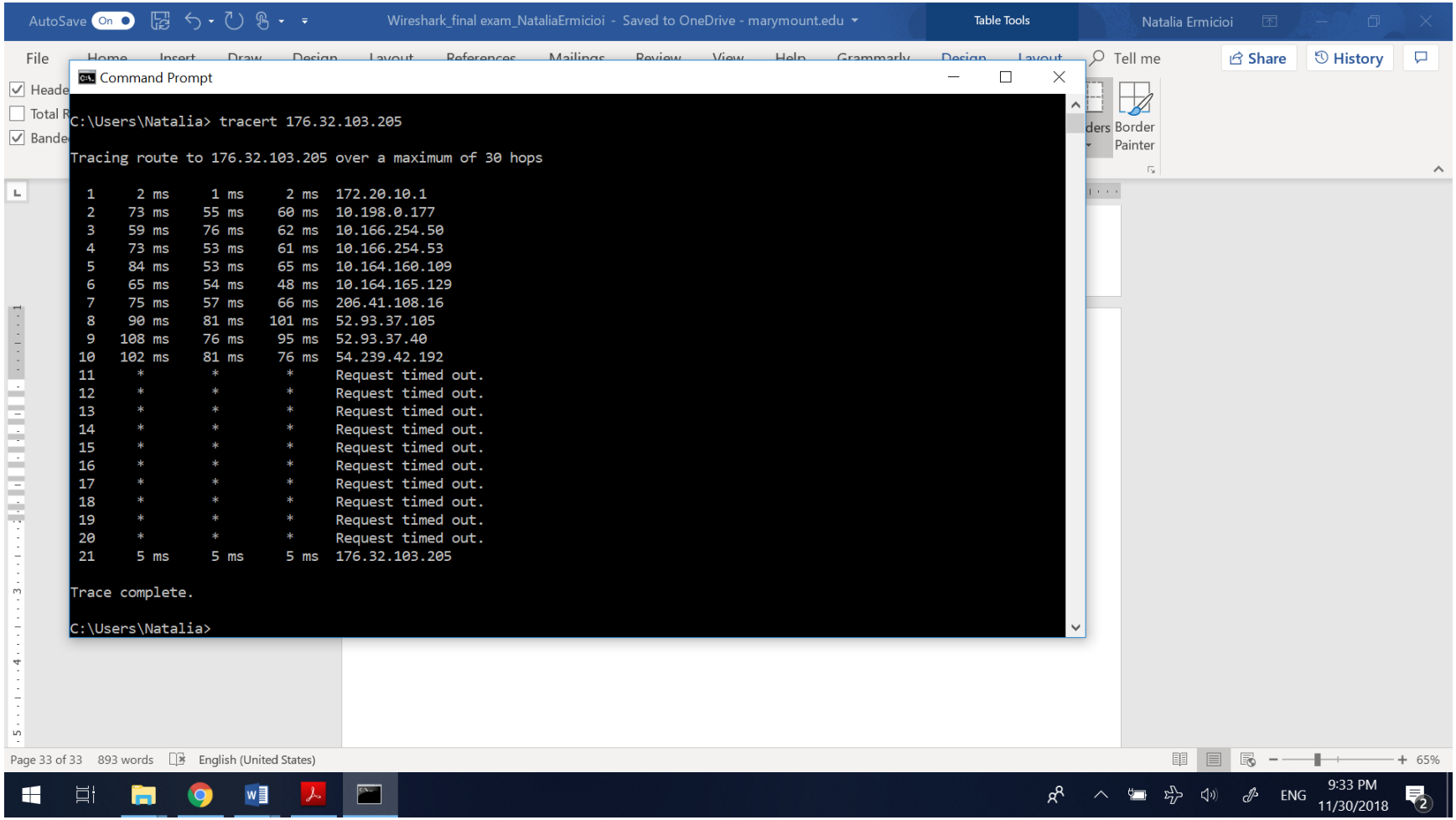



MAC Address and OUI Lookup
https://aruljohn.com/mac/485D36337D4F
arul's utilities
track ip addresses, phone numbers, etc
Blog Articles Bible Code Fun
Check your IP Address
NETWORK
IP address tracker
telephone tracker
wireless network key
which webserver
MAC address lookup
IP/CIDR subnet
IP to hostname
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
lookup MAC address
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
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
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
ENG
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_NataliaErmicioi - Saved to OneDrive - marymount.edu
Table Tools
Natalia Ermicioi
File
Tell me
Share
History
Command Prompt
C:\Users\Natalia> tracert 176.32.103.205
Tracing route to 176.32.103.205 over a maximum of 30 hops
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>
Border Painter
Page 33 of 33
893 words
English (United States)
65%
ENG
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