M.V.Balaji
210905400

A. In the packet list pane, select the first DNS packet. In the packet detail pane, select the User Datagram Protocol. The UDP hexdump will be highlighted in the packet byte lane. Using the hexdump, Answer the following:

a. The source port number: 49892
b. The destination port number: 53
c. The total length of the user datagram: 47
d. The length of the data (UDP Payload): 39-8 (header information) bytes
e. Packet direction: Directed from client to server
f. Application-layer protocol: UDP
g. Checksum calculation: 0xa74d (unverified)

B. What are the source and destination IP addresses in the DNS query message? What are those addresses in the response message? What is the relationship between the two?

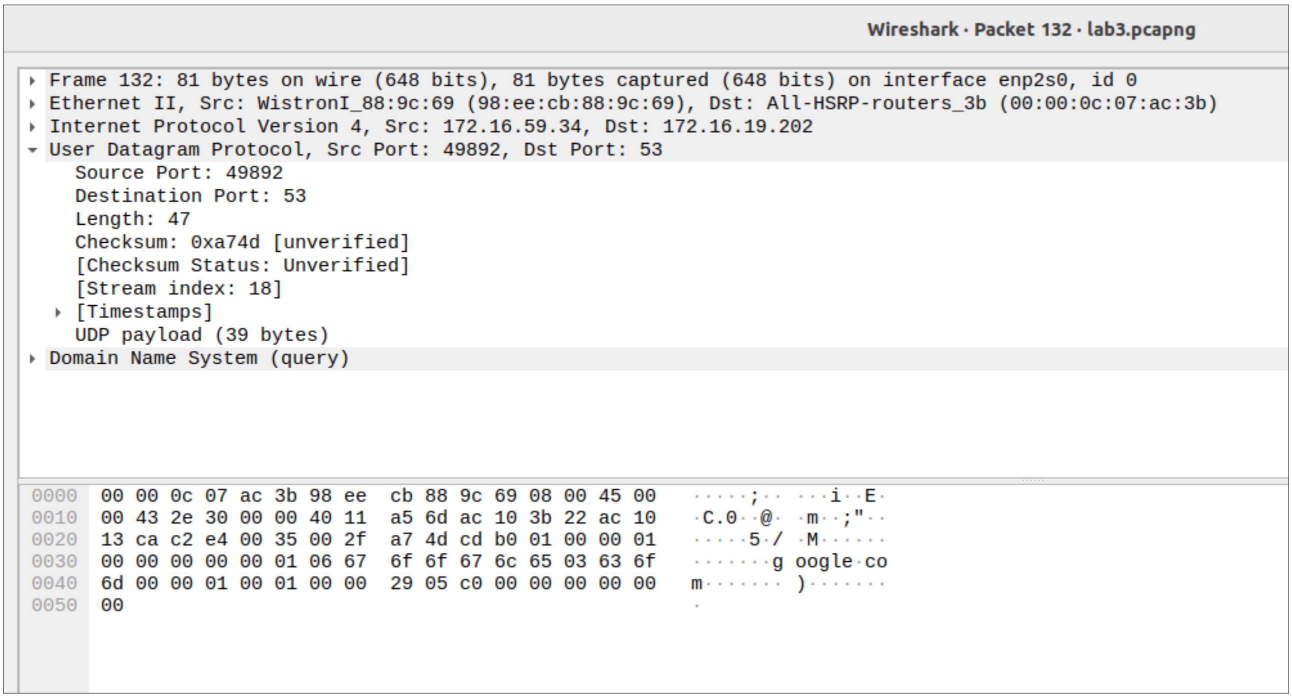
- Source: 172.16.59.34
- Destination: 172.16.59.202

C. What are the source and destination port numbers in the query message? What are those addresses in the response message? What is the relationship between the two? Which port number is a well-known port number?

- Source port number: 49892
- Destination port number: 53
- DNS Port 53 is a well known port number

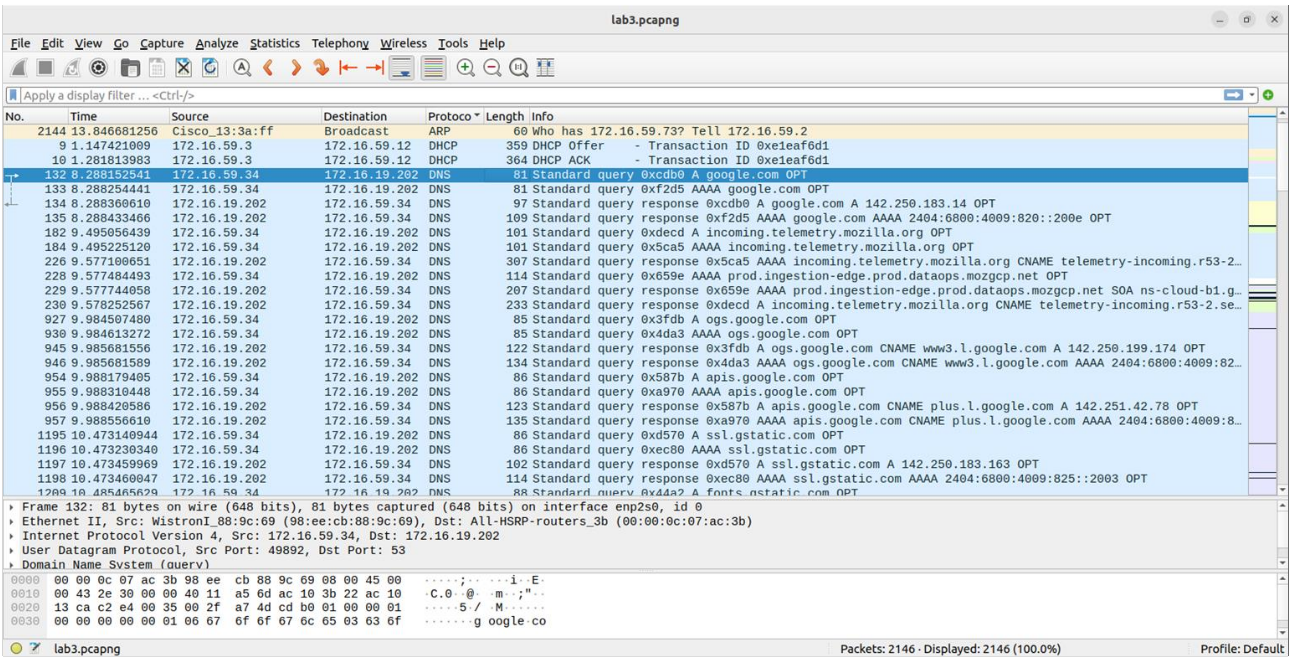
D. What is the length of the first packet? How many bytes of payload are carried by the first packet?

Length of 1st Packet:81. It is carrying 39 bytes of payload.



```
▸ Frame 132: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface enp2s0, id 0
▸ Ethernet II, Src: WistronI_88:9c:69 (98:ee:cb:88:9c:69), Dst: All-HSRP-routers_3b (00:00:0c:07:ac:3b)
▸ Internet Protocol Version 4, Src: 172.16.59.34, Dst: 172.16.19.202
▾ User Datagram Protocol, Src Port: 49892, Dst Port: 53
    Source Port: 49892
    Destination Port: 53
    Length: 47
    Checksum: 0xa74d [unverified]
    [Checksum Status: Unverified]
    [Stream index: 18]
  ▸ [Timestamps]
    UDP payload (39 bytes)
▸ Domain Name System (query)
```

```
0000  00 00 0c 07 ac 3b 98 ee  cb 88 9c 69 08 00 45 00   ·····;·· ···i··E·
0010  00 43 2e 30 00 00 40 11  a5 6d ac 10 3b 22 ac 10   ·C.0··@· ·m··;"··
0020  13 ca c2 e4 00 35 00 2f  a7 4d cd b0 01 00 00 01   ·····5·/ ·M······
0030  00 00 00 00 00 01 06 67  6f 6f 67 6c 65 03 63 6f   ·······g oogle·co
0040  6d 00 00 01 00 01 00 00  29 05 c0 00 00 00 00 00   m······· )·······
0050  00                                                 ·
```


lab3.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.  Time          Source          Destination     Protoco Length Info
2144 13.846681256  Cisco_13:3a:ff  Broadcast       ARP      60 Who has 172.16.59.73? Tell 172.16.59.2
   9 1.147421009   172.16.59.3     172.16.59.12    DHCP    359 DHCP Offer    - Transaction ID 0xe1eaf6d1
  10 1.281813983   172.16.59.3     172.16.59.12    DHCP    364 DHCP ACK      - Transaction ID 0xe1eaf6d1
 132 8.288152541   172.16.59.34    172.16.19.202   DNS      81 Standard query 0xcdb0 A google.com OPT
 133 8.288254441   172.16.59.34    172.16.19.202   DNS      81 Standard query 0xf2d5 AAAA google.com OPT
 134 8.288360610   172.16.19.202   172.16.59.34    DNS      97 Standard query response 0xcdb0 A google.com A 142.250.183.14 OPT
 135 8.288433466   172.16.19.202   172.16.59.34    DNS     109 Standard query response 0xf2d5 AAAA google.com AAAA 2404:6800:4009:820::200e OPT
 182 9.495056439   172.16.59.34    172.16.19.202   DNS     101 Standard query 0xdecd A incoming.telemetry.mozilla.org OPT
 184 9.495225120   172.16.59.34    172.16.19.202   DNS     101 Standard query 0x5ca5 AAAA incoming.telemetry.mozilla.org OPT
 226 9.577100651   172.16.19.202   172.16.59.34    DNS     307 Standard query response 0x5ca5 AAAA incoming.telemetry.mozilla.org CNAME telemetry-incoming.r53-2…
 228 9.577484493   172.16.59.34    172.16.19.202   DNS     114 Standard query 0x659e AAAA prod.ingestion-edge.prod.dataops.mozgcp.net OPT
 229 9.577744058   172.16.19.202   172.16.59.34    DNS     207 Standard query response 0x659e AAAA prod.ingestion-edge.prod.dataops.mozgcp.net SOA ns-cloud-b1.g…
 230 9.578252567   172.16.19.202   172.16.59.34    DNS     233 Standard query response 0xdecd A incoming.telemetry.mozilla.org CNAME telemetry-incoming.r53-2.se…
 927 9.984507480   172.16.59.34    172.16.19.202   DNS      85 Standard query 0x3fdb A ogs.google.com OPT
 930 9.984613272   172.16.59.34    172.16.19.202   DNS      85 Standard query 0x4da3 AAAA ogs.google.com OPT
 945 9.985681556   172.16.19.202   172.16.59.34    DNS     122 Standard query response 0x3fdb A ogs.google.com CNAME www3.l.google.com A 142.250.199.174 OPT
 946 9.985681589   172.16.19.202   172.16.59.34    DNS     134 Standard query response 0x4da3 AAAA ogs.google.com CNAME www3.l.google.com AAAA 2404:6800:4009:82…
 954 9.988179405   172.16.59.34    172.16.19.202   DNS      86 Standard query 0x587b A apis.google.com OPT
 955 9.988310448   172.16.59.34    172.16.19.202   DNS      86 Standard query 0xa970 AAAA apis.google.com OPT
 956 9.988420586   172.16.19.202   172.16.59.34    DNS     123 Standard query response 0x587b A apis.google.com CNAME plus.l.google.com A 142.251.42.78 OPT
 957 9.988556610   172.16.19.202   172.16.59.34    DNS     135 Standard query response 0xa970 AAAA apis.google.com CNAME plus.l.google.com AAAA 2404:6800:4009:8…
1195 10.473140944  172.16.59.34    172.16.19.202   DNS      86 Standard query 0xd570 A ssl.gstatic.com OPT
1196 10.473230340  172.16.59.34    172.16.19.202   DNS      86 Standard query 0xec80 AAAA ssl.gstatic.com OPT
1197 10.473459969  172.16.19.202   172.16.59.34    DNS     102 Standard query response 0xd570 A ssl.gstatic.com A 142.250.183.163 OPT
1198 10.473460047  172.16.19.202   172.16.59.34    DNS     114 Standard query response 0xec80 AAAA ssl.gstatic.com AAAA 2404:6800:4009:825::2003 OPT
1209 10.485465629  172.16.59.34    172.16.19.202   DNS      88 Standard query 0x44a2 A fonts.gstatic.com OPT
```

```
▸ Frame 132: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface enp2s0, id 0
▸ Ethernet II, Src: WistronI_88:9c:69 (98:ee:cb:88:9c:69), Dst: All-HSRP-routers_3b (00:00:0c:07:ac:3b)
▸ Internet Protocol Version 4, Src: 172.16.59.34, Dst: 172.16.19.202
▸ User Datagram Protocol, Src Port: 49892, Dst Port: 53
▸ Domain Name System (query)
```

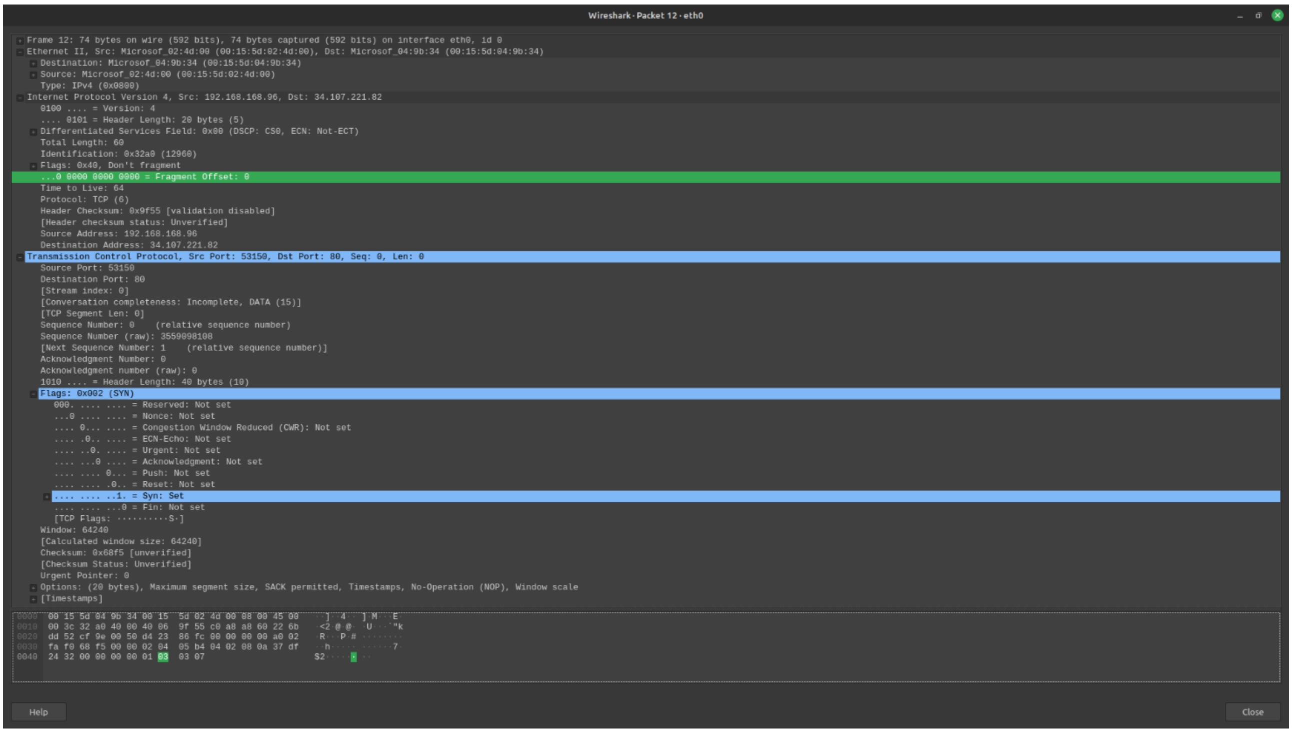
```
0000  00 00 0c 07 ac 3b 98 ee  cb 88 9c 69 08 00 45 00   ·····;·· ···i··E·
0010  00 43 2e 30 00 00 40 11  a5 6d ac 10 3b 22 ac 10   ·C.0··@· ·m··;"··
0020  13 ca c2 e4 00 35 00 2f  a7 4d cd b0 01 00 00 01   ·····5·/ ·M······
0030  00 00 00 00 00 01 06 67  6f 6f 67 6c 65 03 63 6f   ·······g oogle·co
```

2B. Analysing TCP packets using Wireshark:

Part I: Connection-Establishment Phase

Identify the TCP packets used for connection establishment. Note that the last packet used for connection establish may have the application-layer as the source protocol.Using the captured information, answer the following question in your lab report about packets used for connection establishment.

1. What are the socket addresses for each packet?
   - Source:53150
2. What flags are set in each packet?
   - Flags:0x002(SYN)
3. What are the sequence number and acknowledgment number of each packet?
   - Sequence Number:3339098108
   - Acknowledgment:0
4. What are the window size of each packet?
   - 64240



```
Frame 12: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth0, id 0
Ethernet II, Src: Microsof_02:4d:00 (00:15:5d:02:4d:00), Dst: Microsof_04:9b:34 (00:15:5d:04:9b:34)
  Destination: Microsof_04:9b:34 (00:15:5d:04:9b:34)
  Source: Microsof_02:4d:00 (00:15:5d:02:4d:00)
  Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.168.96, Dst: 34.107.221.82
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 60
  Identification: 0x32a0 (12960)
  Flags: 0x40, Don't fragment
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 64
  Protocol: TCP (6)
  Header Checksum: 0x9f55 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.168.96
  Destination Address: 34.107.221.82
Transmission Control Protocol, Src Port: 53150, Dst Port: 80, Seq: 0, Len: 0
  Source Port: 53150
  Destination Port: 80
  [Stream index: 0]
  [Conversation completeness: Incomplete, DATA (15)]
  [TCP Segment Len: 0]
  Sequence Number: 0    (relative sequence number)
  Sequence Number (raw): 3559098108
  [Next Sequence Number: 1    (relative sequence number)]
  Acknowledgment Number: 0
  Acknowledgment number (raw): 0
  1010 .... = Header Length: 40 bytes (10)
  Flags: 0x002 (SYN)
    000. .... .... = Reserved: Not set
    ...0 .... .... = Nonce: Not set
    .... 0... .... = Congestion Window Reduced (CWR): Not set
    .... .0.. .... = ECN-Echo: Not set
    .... ..0. .... = Urgent: Not set
    .... ...0 .... = Acknowledgment: Not set
    .... .... 0... = Push: Not set
    .... .... .0.. = Reset: Not set
    .... .... ..1. = Syn: Set
    .... .... ...0 = Fin: Not set
    [TCP Flags: ··········S·]
  Window: 64240
  [Calculated window size: 64240]
  Checksum: 0x68f5 [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP), Window scale
  [Timestamps]
```

```
0000  00 15 5d 04 9b 34 00 15  5d 02 4d 00 08 00 45 00   ··]··4·· ]·M···E·
0010  00 3c 32 a0 40 00 40 06  9f 55 c0 a8 a8 60 22 6b   ·<2·@·@· ·U···`"k
0020  dd 52 cf 9e 00 50 d4 23  86 fc 00 00 00 00 a0 02   ·R···P·# ········
0030  fa f0 68 f5 00 00 02 04  05 b4 04 02 08 0a 37 df   ··h····· ······7·
0040  24 32 00 00 00 00 01 03  03 07                     $2······ ··
```

Part II: Data-Transfer Phase

The data-transfer phase starts with an HTTP GET request message and ends with an HTTP OK message.Using the captured information, answer the following question in your lab report about packets used for data transfer.

1. What TCP flags are set in the first data-transfer packet (HTTP GET message)?
    - PSH and ACK
2. How many bytes are transmitted in this packet?
    - 359bytes
3. How often does the receiver generate an acknowledgment? To which acknowledgment rule(defined in Page 200 in the textbook) does your answer correspond to?
    - 0.005s

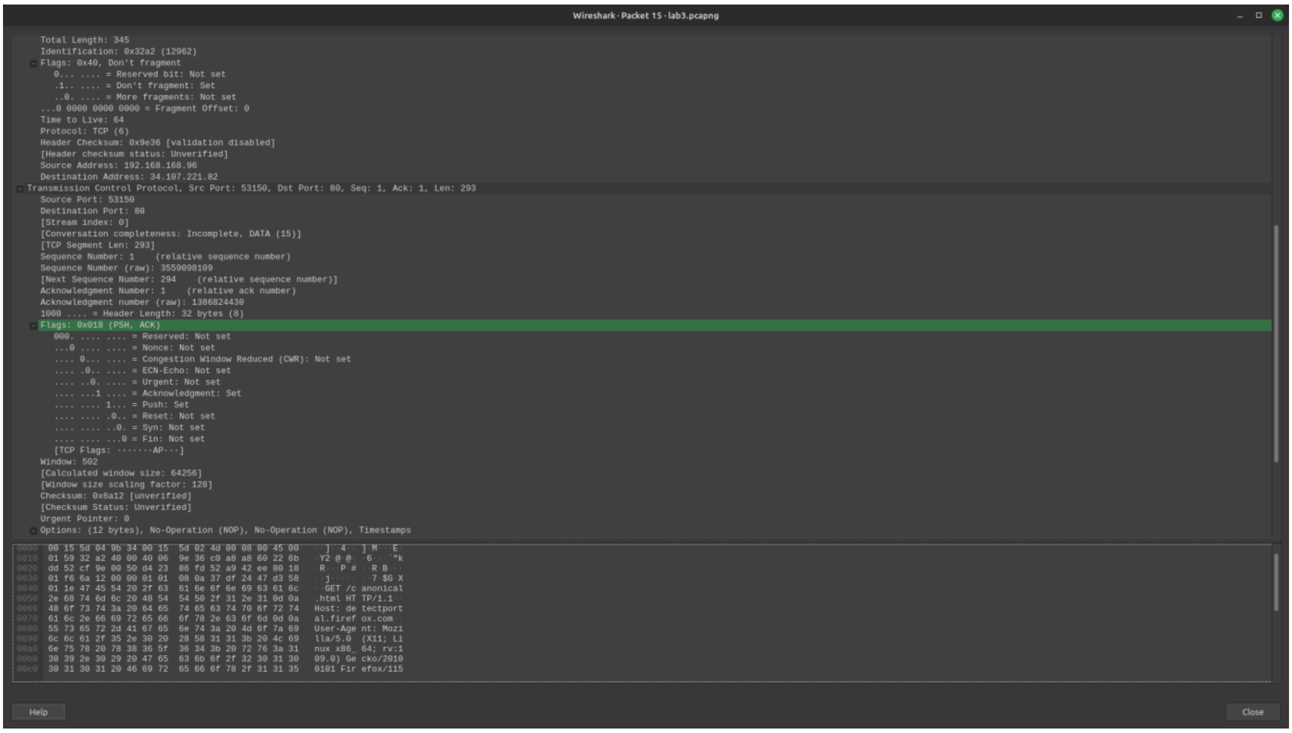
4. How many bytes are transmitted in each packet? How are the sequence and acknowledgment numbers related to number of bytes transmitted?
    - 359 bytes are transmitted each packet. The sequence number increases by the number of bytes transmitted, and the acknowledgment number increases by the number of bytes received.

5. What are the original window sizes that are set by the client and the server? Are these numbers expected? How do they change as more segments are received by the client?
    - Original Window Size:64256
    - Received Size:128
6. Explain how the window size is used in flow control?

- The client should be able to receive all windows while avoiding any congestion,so flow control is implemented to send a window soze better suited for the client

7. What is the purpose of the HTTP OK message in the data transfer phase?

- The HTTP OK message is a feedback about the request OK response indicates that a request has succeeded.



```
    Total Length: 345
    Identification: 0x32a2 (12962)
  ⊟ Flags: 0x40, 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: 64
    Protocol: TCP (6)
    Header Checksum: 0x9e36 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.168.96
    Destination Address: 34.107.221.82
⊟ Transmission Control Protocol, Src Port: 53150, Dst Port: 80, Seq: 1, Ack: 1, Len: 293
    Source Port: 53150
    Destination Port: 80
    [Stream index: 0]
    [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 293]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 3559098109
    [Next Sequence Number: 294    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 1386824430
    1000 .... = Header Length: 32 bytes (8)
  ⊟ Flags: 0x018 (PSH, ACK)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...1 .... = Acknowledgment: Set
      .... .... 1... = Push: Set
      .... .... .0.. = Reset: Not set
      .... .... ..0. = Syn: Not set
      .... .... ...0 = Fin: Not set
      [TCP Flags: ·······AP···]
    Window: 502
    [Calculated window size: 64256]
    [Window size scaling factor: 128]
    Checksum: 0x6a12 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  ⊟ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps

0000  00 15 5d 04 9b 34 00 15  5d 02 4d 00 08 00 45 00   ··]··4·· ]·M···E·
0010  01 59 32 a2 40 00 40 06  9e 36 c0 a8 a8 60 22 6b   ·Y2·@·@· ·6···`"k
0020  dd 52 cf 9e 00 50 d4 23  86 fd 52 a9 42 ee 80 18   ·R···P·# ··R·B···
0030  01 f6 6a 12 00 00 01 01  08 0a 37 df 24 47 d3 58   ··j····· ··7·$G·X
0040  01 1e 47 45 54 20 2f 63  61 6e 6f 6e 69 63 61 6c   ··GET /c anonical
0050  2e 68 74 6d 6c 20 48 54  54 50 2f 31 2e 31 0d 0a   .html HT TP/1.1··
0060  48 6f 73 74 3a 20 64 65  74 65 63 74 70 6f 72 74   Host: de tectport
0070  61 6c 2e 66 69 72 65 66  6f 78 2e 63 6f 6d 0d 0a   al.firef ox.com··
0080  55 73 65 72 2d 41 67 65  6e 74 3a 20 4d 6f 7a 69   User-Age nt: Mozi
0090  6c 6c 61 2f 35 2e 30 20  28 58 31 31 3b 20 4c 69   lla/5.0  (X11; Li
00a0  6e 75 78 20 78 38 36 5f  36 34 3b 20 72 76 3a 31   nux x86_ 64; rv:1
00b0  30 39 2e 30 29 20 47 65  63 6b 6f 2f 32 30 31 30   09.0) Ge cko/2010
00c0  30 31 30 31 20 46 69 72  65 66 6f 78 2f 31 31 35   0101 Fir efox/115
```

Part III: Connection Termination Phase

The data-transfer phase is followed by the connection termination phase. Note that some packets used in the connection-termination phase may have the source or sink protocol at the application layer. Find the packets used for connection termination.Using the captured information, answer the following question in your lab report about packets used for connection termination.

1. How many TCP segments are exchanged for this phase?

- 4 segments are exchanged in the connection termination phase. (FIN, ACK, FIN, ACK)

2. Which end point started the connection termination phase?

- Client

3. What flags are set in each of segments used for connection termination?

- FIN and ACK Flag