Network Traffic Analysis using Wireshark

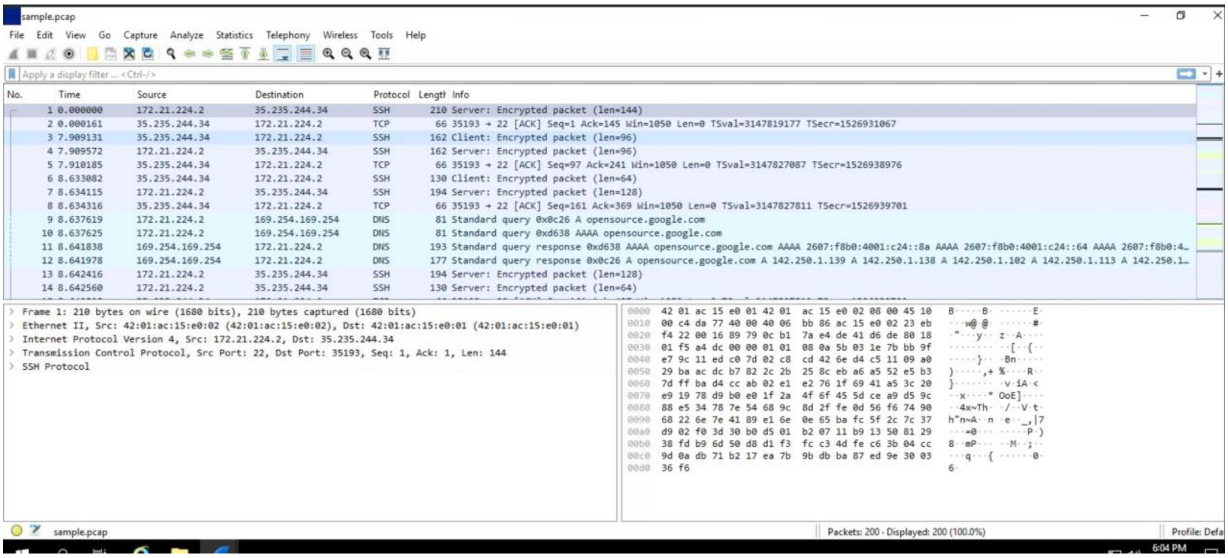
Project description

This simulation project puts the performer, **Maheswar Reddy Avula**, into the position of Security Analyst for an organization. Responsibilities include investigating network traffic by analyzing a network packet capture file that contains traffic data related to a user connecting to an internet site.

Explore data with Wireshark

Direction: The analyst must open a network packet capture file that contains data captured from a system that made web requests to a site using Wireshark.

The **sample.pcap** file was opened in Wireshark from the desktop as follows:



```
No.   Time        Source            Destination       Protocol Length Info
    1 0.000000    172.21.224.2      35.235.244.34     SSH      210 Server: Encrypted packet (len=144)
    2 0.000161    35.235.244.34     172.21.224.2      TCP       66 35193 → 22 [ACK] Seq=1 Ack=145 Win=1050 Len=0 TSval=3147819177 TSecr=1526931067
    3 7.909131    35.235.244.34     172.21.224.2      SSH      162 Client: Encrypted packet (len=96)
    4 7.909572    172.21.224.2      35.235.244.34     SSH      162 Server: Encrypted packet (len=96)
    5 7.910185    35.235.244.34     172.21.224.2      TCP       66 35193 → 22 [ACK] Seq=97 Ack=241 Win=1050 Len=0 TSval=3147827087 TSecr=1526938976
    6 8.633082    35.235.244.34     172.21.224.2      SSH      130 Client: Encrypted packet (len=64)
    7 8.634115    172.21.224.2      35.235.244.34     SSH      194 Server: Encrypted packet (len=128)
    8 8.634316    35.235.244.34     172.21.224.2      TCP       66 35193 → 22 [ACK] Seq=161 Ack=369 Win=1050 Len=0 TSval=3147827811 TSecr=1526939701
    9 8.637619    172.21.224.2      169.254.169.254   DNS       81 Standard query 0x0c26 A opensource.google.com
   10 8.637625    172.21.224.2      169.254.169.254   DNS       81 Standard query 0xd638 AAAA opensource.google.com
   11 8.641838    169.254.169.254   172.21.224.2      DNS      193 Standard query response 0xd638 AAAA opensource.google.com AAAA 2607:f8b0:4001:c24::8a AAAA 2607:f8b0:4001:c24::64 AAAA 2607:f8b0:4…
   12 8.641978    169.254.169.254   172.21.224.2      DNS      177 Standard query response 0x0c26 A opensource.google.com A 142.250.1.139 A 142.250.1.138 A 142.250.1.102 A 142.250.1.113 A 142.250.1…
   13 8.642416    172.21.224.2      35.235.244.34     SSH      194 Server: Encrypted packet (len=128)
   14 8.642560    172.21.224.2      35.235.244.34     SSH      130 Server: Encrypted packet (len=64)
```

```
> Frame 1: 210 bytes on wire (1680 bits), 210 bytes captured (1680 bits)
> Ethernet II, Src: 42:01:ac:15:e0:02 (42:01:ac:15:e0:02), Dst: 42:01:ac:15:e0:01 (42:01:ac:15:e0:01)
> Internet Protocol Version 4, Src: 172.21.224.2, Dst: 35.235.244.34
> Transmission Control Protocol, Src Port: 22, Dst Port: 35193, Seq: 1, Ack: 1, Len: 144
> SSH Protocol
```

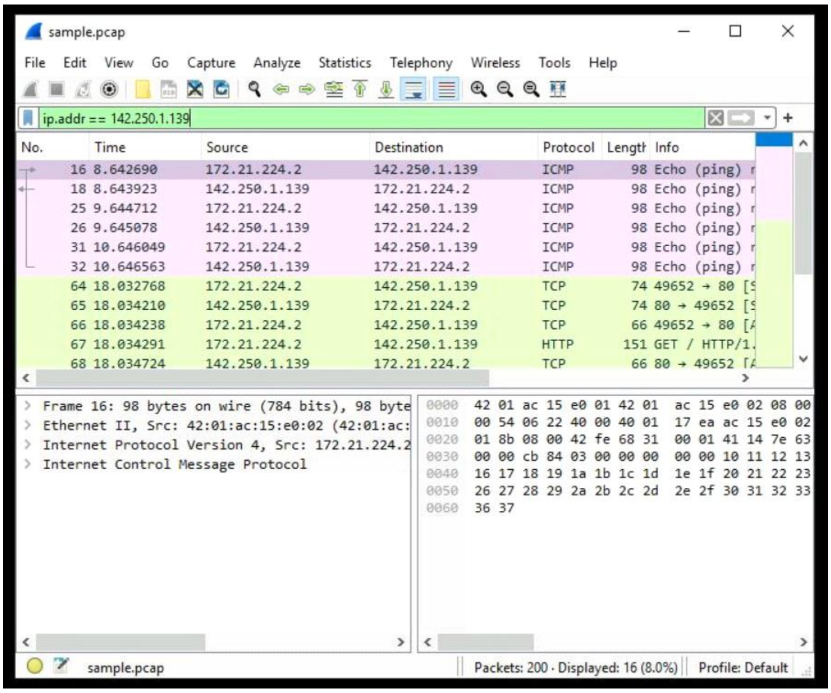
```
0000  42 01 ac 15 e0 01 42 01  ac 15 e0 02 08 00 45 10   B·····B·······E·
0010  00 c4 da 77 40 00 40 06  bb 86 ac 15 e0 02 23 eb   ···w@·@·······#·
0020  f4 22 00 16 89 79 0c b1  7a e4 de 41 d6 de 80 18   ·"···y··z··A····
0030  01 f5 a4 dc 00 00 01 01  08 0a 5b 03 1e 7b bb 9f   ··········[··{··
0040  e7 9c 11 ed c0 7d 02 c8  cd 42 6e d4 c5 11 09 a0   ·····}···Bn·····
0050  29 ba ac dc b7 82 2c 2b  25 8c eb a6 a5 52 e5 b3   )·····,+%····R··
0060  7d ff ba d4 cc ab 02 e1  e2 76 1f 69 41 a5 3c 20   }········v·iA·< 
0070  e9 19 78 d9 b0 e0 1f 2a  4f 6f 45 5d ce a9 d5 9c   ··x····*OoE]····
0080  88 e5 34 78 7e 54 68 9c  8d 2f fe 0d 56 f6 74 90   ··4x~Th··/··V·t·
0090  68 22 6e 7e 41 89 e1 6e  0e 65 ba fc 5f 2c 7c 37   h"n~A··n·e··_,|7
00a0  d9 02 f0 3d 30 b0 d5 01  b2 07 11 b9 13 50 81 29   ···=0········P·)
00b0  38 fd b9 6d 50 d8 d1 f3  fc c3 4d fe c6 3b 04 cc   8··mP·····M··;··
00c0  9d 0a db 71 b2 17 ea 7b  9b db ba 87 ed 9e 30 03   ···q···{······0·
00d0  36 f6                                              6·
```

All data fields like **No.**, **Time**, **Source**, **Destination**, **Protocol**, Length and **Info** are observed.

Apply a basic Wireshark filter and inspect a packet

Direction: The analyst must open a packet in Wireshark for more detailed exploration and filter the data to inspect the network layers and protocols contained in the packet.

The packets are first filtered for the IP address **142.250.1.139** as follows:



sample.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ip.addr == 142.250.1.139
```

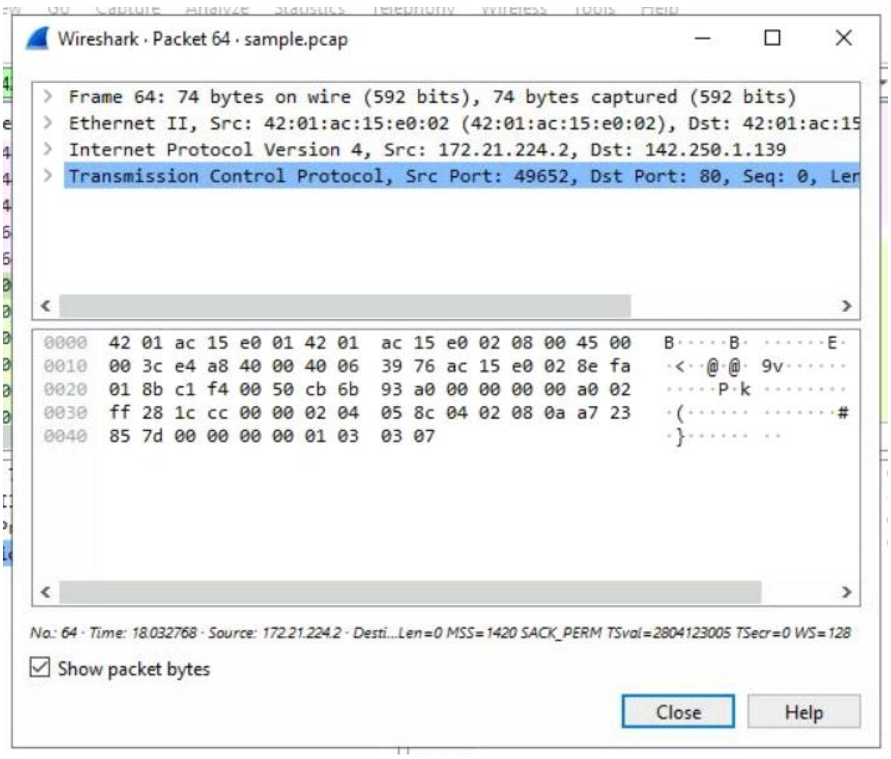
```
No.  Time          Source          Destination     Protocol Length Info
  16 8.642690      172.21.224.2    142.250.1.139   ICMP     98 Echo (ping) r
  18 8.643923      142.250.1.139   172.21.224.2    ICMP     98 Echo (ping) r
  25 9.644712      172.21.224.2    142.250.1.139   ICMP     98 Echo (ping) r
  26 9.645078      142.250.1.139   172.21.224.2    ICMP     98 Echo (ping) r
  31 10.646049     172.21.224.2    142.250.1.139   ICMP     98 Echo (ping) r
  32 10.646563     142.250.1.139   172.21.224.2    ICMP     98 Echo (ping) r
  64 18.032768     172.21.224.2    142.250.1.139   TCP      74 49652 → 80 [S
  65 18.034210     142.250.1.139   172.21.224.2    TCP      74 80 → 49652 [S
  66 18.034238     172.21.224.2    142.250.1.139   TCP      66 49652 → 80 [A
  67 18.034291     172.21.224.2    142.250.1.139   HTTP    151 GET / HTTP/1.
  68 18.034724     142.250.1.139   172.21.224.2    TCP      66 80 → 49652 [A
```

```
> Frame 16: 98 bytes on wire (784 bits), 98 byte
> Ethernet II, Src: 42:01:ac:15:e0:02 (42:01:ac:
> Internet Protocol Version 4, Src: 172.21.224.2
> Internet Control Message Protocol
```

```
0000  42 01 ac 15 e0 01 42 01  ac 15 e0 02 08 00
0010  00 54 06 22 40 00 40 01  17 ea ac 15 e0 02
0020  01 8b 08 00 42 fe 68 31  00 01 41 14 7e 63
0030  00 00 cb 84 03 00 00 00  00 00 10 11 12 13
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33
0060  36 37
```

sample.pcap | Packets: 200 · Displayed: 16 (8.0%) | Profile: Default

The first packet of the list is opened followed by the details pane window:



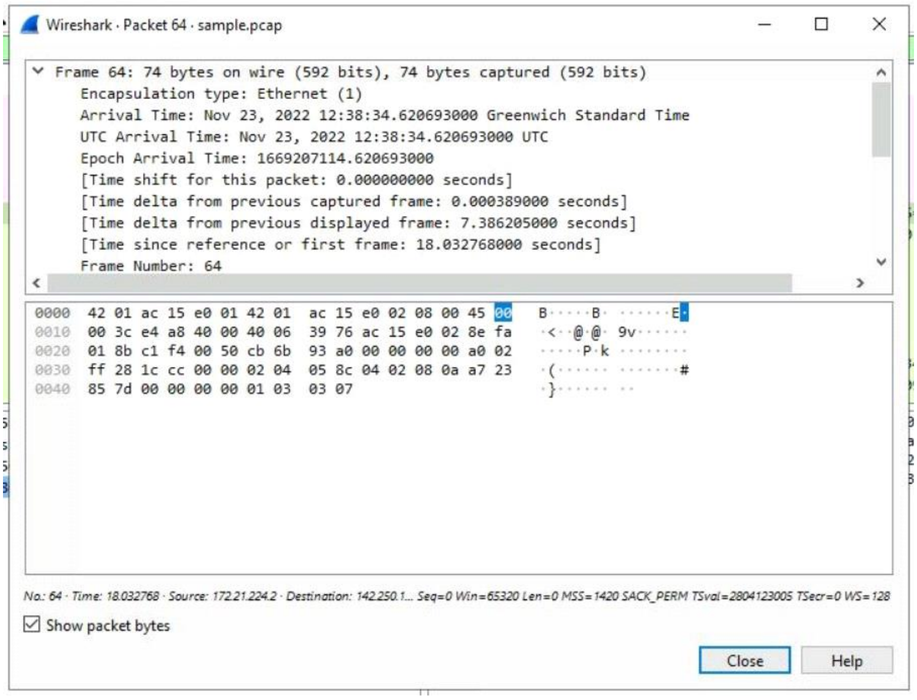
```
> Frame 64: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
> Ethernet II, Src: 42:01:ac:15:e0:02 (42:01:ac:15:e0:02), Dst: 42:01:ac:15
> Internet Protocol Version 4, Src: 172.21.224.2, Dst: 142.250.1.139
> Transmission Control Protocol, Src Port: 49652, Dst Port: 80, Seq: 0, Len
```

```
0000  42 01 ac 15 e0 01 42 01  ac 15 e0 02 08 00 45 00   B·····B· ······E·
0010  00 3c e4 a8 40 00 40 06  39 76 ac 15 e0 02 8e fa   ·<··@·@· 9v······
0020  01 8b c1 f4 00 50 cb 6b  93 a0 00 00 00 00 a0 02   ·····P·k ········
0030  ff 28 1c cc 00 00 02 04  05 8c 04 02 08 0a a7 23   ·(······ ·······#
0040  85 7d 00 00 00 00 01 03  03 07                     ·}······ ··
```

No.: 64 · Time: 18.032768 · Source: 172.21.224.2 · Desti...Len=0 MSS=1420 SACK_PERM TSval=2804123005 TSecr=0 WS=128

☑ Show packet bytes

It is observed that the upper section of this window contains subtrees where Wireshark provides an analysis of the various parts of the network packet. The lower section of the window contains the raw packet data displayed in hexadecimal and ASCII text. There is also placeholder text for fields where the character data does not apply, as indicated by the dot ("."). The **Frame**, **Internet Protocol Version 4**, and **Transmission Control Protocol** Subtrees are observed.

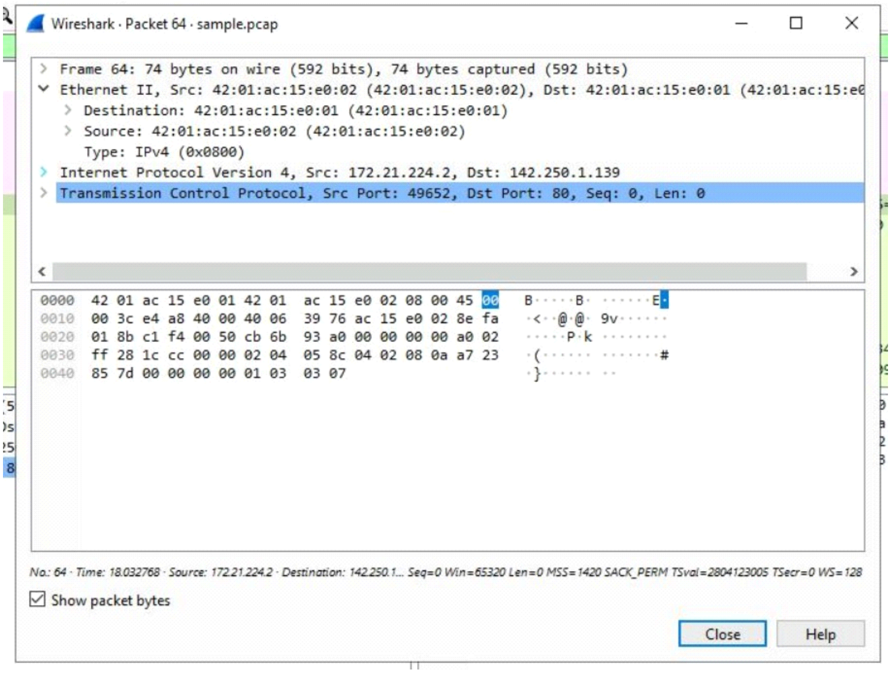


```
Frame 64: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Nov 23, 2022 12:38:34.620693000 Greenwich Standard Time
    UTC Arrival Time: Nov 23, 2022 12:38:34.620693000 UTC
    Epoch Arrival Time: 1669207114.620693000
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.000389000 seconds]
    [Time delta from previous displayed frame: 7.386205000 seconds]
    [Time since reference or first frame: 18.032768000 seconds]
    Frame Number: 64
```

```
0000  42 01 ac 15 e0 01 42 01  ac 15 e0 02 08 00 45 00   B·····B· ······E·
0010  00 3c e4 a8 40 00 40 06  39 76 ac 15 e0 02 8e fa   ·<··@·@· 9v······
0020  01 8b c1 f4 00 50 cb 6b  93 a0 00 00 00 00 a0 02   ·····P·k ········
0030  ff 28 1c cc 00 00 02 04  05 8c 04 02 08 0a a7 23   ·(······ ·······#
0040  85 7d 00 00 00 00 01 03  03 07                     ·}······ ··
```

No.: 64 · Time: 18.032768 · Source: 172.21.224.2 · Destination: 142.250.1... Seq=0 Win=65320 Len=0 MSS=1420 SACK_PERM TSval=2804123005 TSecr=0 WS=128

☑ Show packet bytes

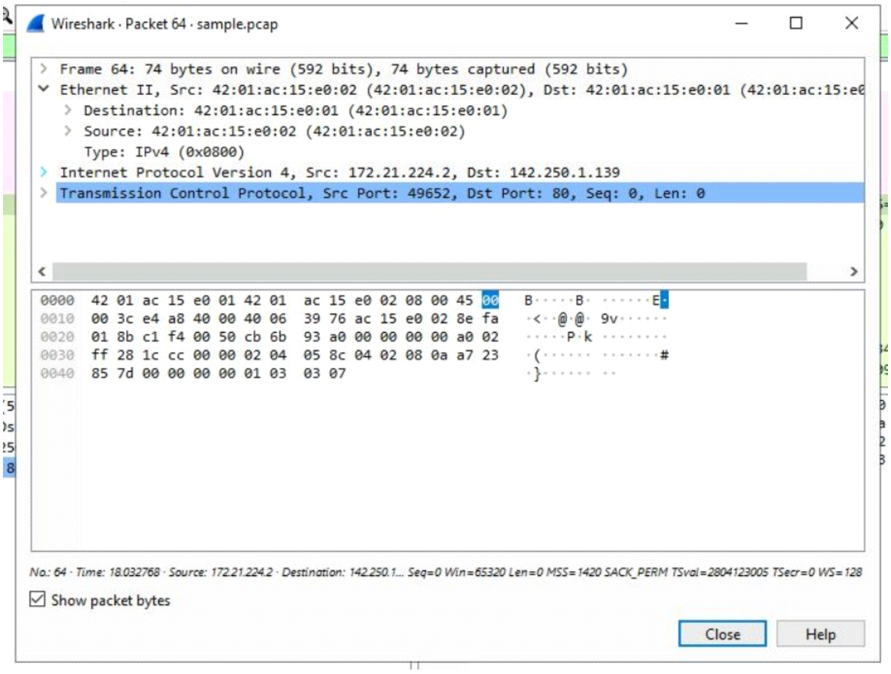


```
> Frame 64: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
v Ethernet II, Src: 42:01:ac:15:e0:02 (42:01:ac:15:e0:02), Dst: 42:01:ac:15:e0:01 (42:01:ac:15:e0
  > Destination: 42:01:ac:15:e0:01 (42:01:ac:15:e0:01)
  > Source: 42:01:ac:15:e0:02 (42:01:ac:15:e0:02)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 172.21.224.2, Dst: 142.250.1.139
> Transmission Control Protocol, Src Port: 49652, Dst Port: 80, Seq: 0, Len: 0
```

```
0000  42 01 ac 15 e0 01 42 01  ac 15 e0 02 08 00 45 00   B·····B· ······E·
0010  00 3c e4 a8 40 00 40 06  39 76 ac 15 e0 02 8e fa   ·<··@·@· 9v······
0020  01 8b c1 f4 00 50 cb 6b  93 a0 00 00 00 00 a0 02   ·····P·k ········
0030  ff 28 1c cc 00 00 02 04  05 8c 04 02 08 0a a7 23   ·(······ ·······#
0040  85 7d 00 00 00 00 01 03  03 07                     ·}······ ··
```

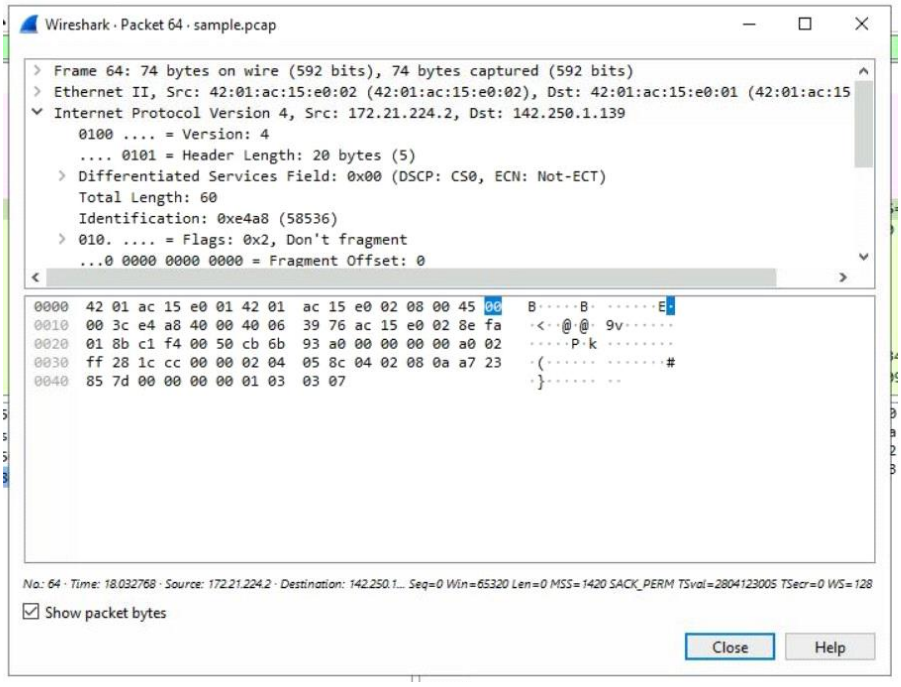
No.: 64 · Time: 18.032768 · Source: 172.21.224.2 · Destination: 142.250.1... Seq=0 Win=65320 Len=0 MSS=1420 SACK_PERM TSval=2804123005 TSecr=0 WS=128

☑ Show packet bytes



```
> Frame 64: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
v Ethernet II, Src: 42:01:ac:15:e0:02 (42:01:ac:15:e0:02), Dst: 42:01:ac:15:e0:01 (42:01:ac:15:e0
  > Destination: 42:01:ac:15:e0:01 (42:01:ac:15:e0:01)
  > Source: 42:01:ac:15:e0:02 (42:01:ac:15:e0:02)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 172.21.224.2, Dst: 142.250.1.139
> Transmission Control Protocol, Src Port: 49652, Dst Port: 80, Seq: 0, Len: 0

0000  42 01 ac 15 e0 01 42 01  ac 15 e0 02 08 00 45 00   B·····B· ······E·
0010  00 3c e4 a8 40 00 40 06  39 76 ac 15 e0 02 8e fa   ·<··@·@· 9v······
0020  01 8b c1 f4 00 50 cb 6b  93 a0 00 00 00 00 a0 02   ·····P·k ········
0030  ff 28 1c cc 00 00 02 04  05 8c 04 02 08 0a a7 23   ·(······ ·······#
0040  85 7d 00 00 00 00 01 03  03 07                     ·}······ ··

No.: 64 · Time: 18.032768 · Source: 172.21.224.2 · Destination: 142.250.1... Seq=0 Win=65320 Len=0 MSS=1420 SACK_PERM TSval=2804123005 TSecr=0 WS=128
```

☑ Show packet bytes



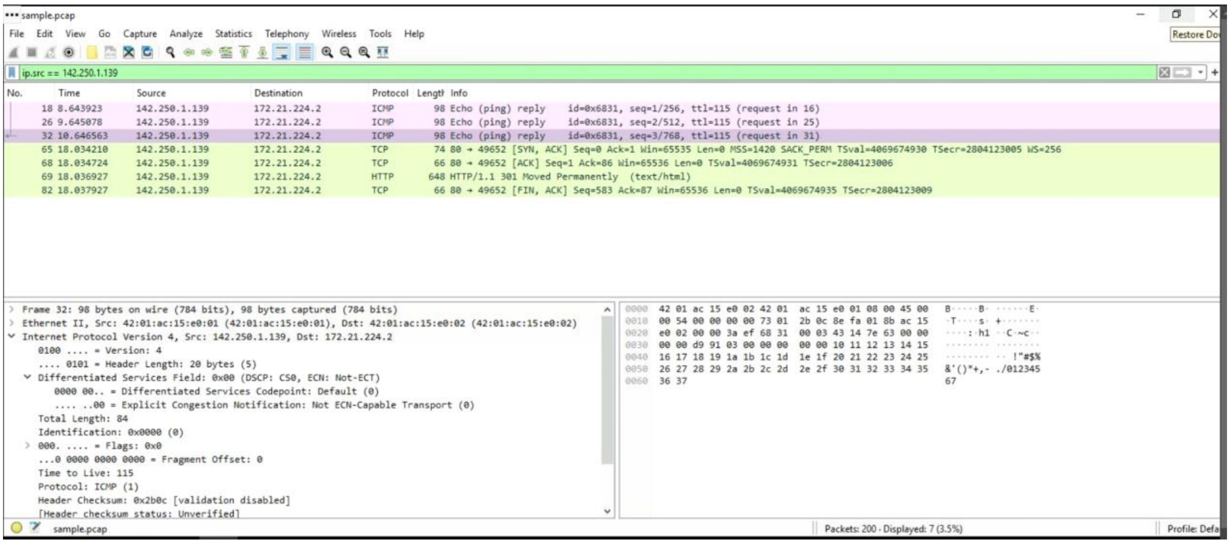
```
> Frame 64: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
> Ethernet II, Src: 42:01:ac:15:e0:02 (42:01:ac:15:e0:02), Dst: 42:01:ac:15:e0:01 (42:01:ac:15
v Internet Protocol Version 4, Src: 172.21.224.2, Dst: 142.250.1.139
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0xe4a8 (58536)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0

0000  42 01 ac 15 e0 01 42 01  ac 15 e0 02 08 00 45 00   B·····B· ······E·
0010  00 3c e4 a8 40 00 40 06  39 76 ac 15 e0 02 8e fa   ·<··@·@· 9v······
0020  01 8b c1 f4 00 50 cb 6b  93 a0 00 00 00 00 a0 02   ·····P·k ········
0030  ff 28 1c cc 00 00 02 04  05 8c 04 02 08 0a a7 23   ·(······ ·······#
0040  85 7d 00 00 00 00 01 03  03 07                     ·}······ ··

No.: 64 · Time: 18.032768 · Source: 172.21.224.2 · Destination: 142.250.1... Seq=0 Win=65320 Len=0 MSS=1420 SACK_PERM TSval=2804123005 TSecr=0 WS=128
```

☑ Show packet bytes

Use filters to select packets

Direction: The analyst must use filters to analyze specific network packets based on where the packets came from or where they were sent to.

Firstly, the packets were filtered for the source IP address **142.250.1.139** as follows:


••• sample.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Restore Do

```
ip.src == 142.250.1.139
```

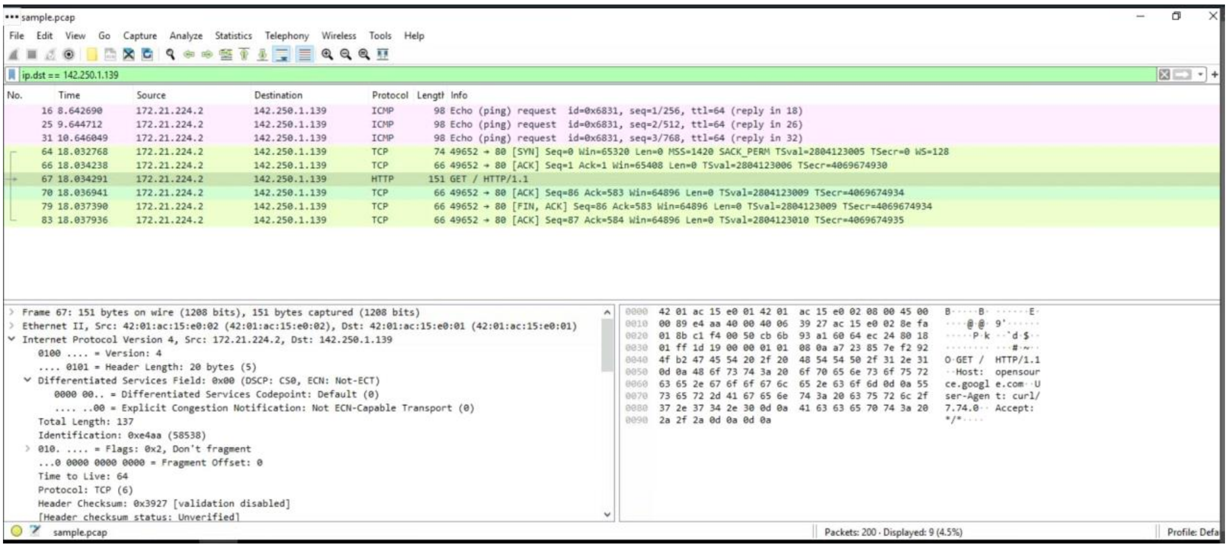
```
No.   Time         Source          Destination     Protocol Length Info
   18 8.643923     142.250.1.139   172.21.224.2    ICMP       98 Echo (ping) reply    id=0x6831, seq=1/256, ttl=115 (request in 16)
   26 9.645078     142.250.1.139   172.21.224.2    ICMP       98 Echo (ping) reply    id=0x6831, seq=2/512, ttl=115 (request in 25)
   32 10.646563    142.250.1.139   172.21.224.2    ICMP       98 Echo (ping) reply    id=0x6831, seq=3/768, ttl=115 (request in 31)
   65 18.034210    142.250.1.139   172.21.224.2    TCP        74 80 → 49652 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1420 SACK_PERM TSval=4069674930 TSecr=2804123005 WS=256
   68 18.034724    142.250.1.139   172.21.224.2    TCP        66 80 → 49652 [ACK] Seq=1 Ack=86 Win=65536 Len=0 TSval=4069674931 TSecr=2804123006
   69 18.036927    142.250.1.139   172.21.224.2    HTTP      648 HTTP/1.1 301 Moved Permanently  (text/html)
   82 18.037927    142.250.1.139   172.21.224.2    TCP        66 80 → 49652 [FIN, ACK] Seq=583 Ack=87 Win=65536 Len=0 TSval=4069674935 TSecr=2804123009
```

```
> Frame 32: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
> Ethernet II, Src: 42:01:ac:15:e0:01 (42:01:ac:15:e0:01), Dst: 42:01:ac:15:e0:02 (42:01:ac:15:e0:02)
v Internet Protocol Version 4, Src: 142.250.1.139, Dst: 172.21.224.2
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  v Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 84
    Identification: 0x0000 (0)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 115
    Protocol: ICMP (1)
    Header Checksum: 0x2b0c [validation disabled]
    [Header checksum status: Unverified]
```

```
0000  42 01 ac 15 e0 02 42 01  ac 15 e0 01 08 00 45 00   B·····B· ······E·
0010  00 54 00 00 00 00 73 01  2b 0c 8e fa 01 8b ac 15   ·T····s· +·······
0020  e0 02 00 00 3a ef 68 31  00 03 43 14 7e 63 00 00   ····:·h1 ··C·~c··
0030  00 00 d9 91 03 00 00 00  00 00 10 11 12 13 14 15   ········ ········
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ········ ·· !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345
0060  36 37                                              67
```

sample.pcap | Packets: 200 · Displayed: 7 (3.5%) | Profile: Defa

Then, the packets were filtered for the destination IP address **142.250.1.139** as follows:



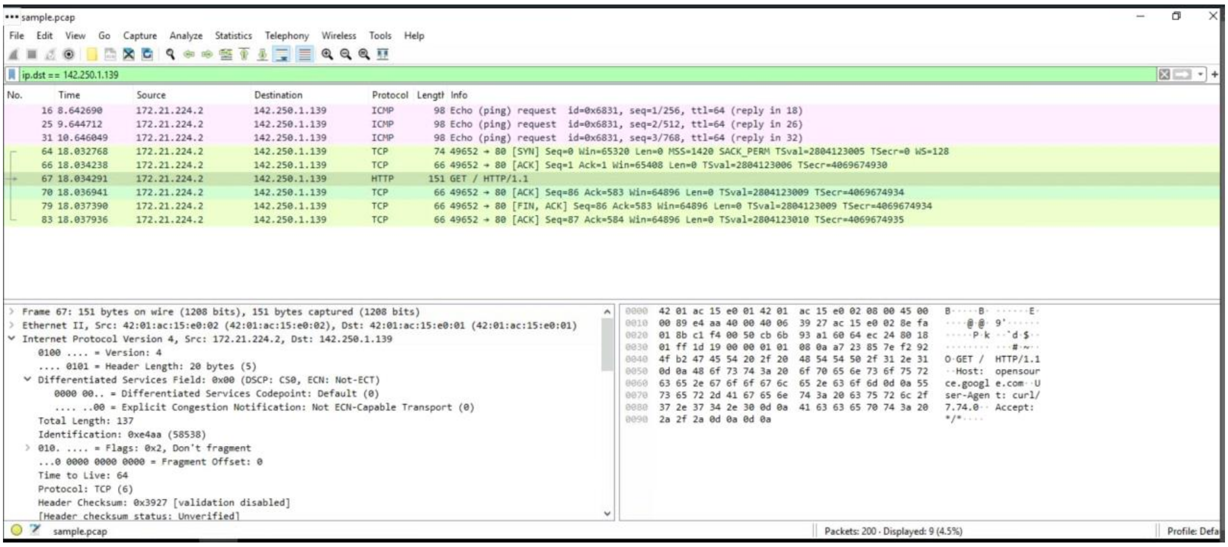
```
ip.dst == 142.250.1.139
```

```
No.   Time         Source          Destination     Protocol Length Info
   16 8.642690     172.21.224.2    142.250.1.139   ICMP       98 Echo (ping) request  id=0x6831, seq=1/256, ttl=64 (reply in 18)
   25 9.644712     172.21.224.2    142.250.1.139   ICMP       98 Echo (ping) request  id=0x6831, seq=2/512, ttl=64 (reply in 26)
   31 10.646049    172.21.224.2    142.250.1.139   ICMP       98 Echo (ping) request  id=0x6831, seq=3/768, ttl=64 (reply in 32)
   64 18.032768    172.21.224.2    142.250.1.139   TCP        74 49652 → 80 [SYN] Seq=0 Win=65320 Len=0 MSS=1420 SACK_PERM TSval=2804123005 TSecr=0 WS=128
   66 18.034238    172.21.224.2    142.250.1.139   TCP        66 49652 → 80 [ACK] Seq=1 Ack=1 Win=65408 Len=0 TSval=2804123006 TSecr=4069674930
   67 18.034291    172.21.224.2    142.250.1.139   HTTP      151 GET / HTTP/1.1
   70 18.036941    172.21.224.2    142.250.1.139   TCP        66 49652 → 80 [ACK] Seq=86 Ack=583 Win=64896 Len=0 TSval=2804123009 TSecr=4069674934
   79 18.037390    172.21.224.2    142.250.1.139   TCP        66 49652 → 80 [FIN, ACK] Seq=86 Ack=583 Win=64896 Len=0 TSval=2804123009 TSecr=4069674934
   83 18.037936    172.21.224.2    142.250.1.139   TCP        66 49652 → 80 [ACK] Seq=87 Ack=584 Win=64896 Len=0 TSval=2804123010 TSecr=4069674935
```

```
> Frame 67: 151 bytes on wire (1208 bits), 151 bytes captured (1208 bits)
> Ethernet II, Src: 42:01:ac:15:e0:02 (42:01:ac:15:e0:02), Dst: 42:01:ac:15:e0:01 (42:01:ac:15:e0:01)
v Internet Protocol Version 4, Src: 172.21.224.2, Dst: 142.250.1.139
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  v Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 137
    Identification: 0xe4aa (58538)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0x3927 [validation disabled]
    [Header checksum status: Unverified]
```

```
0000  42 01 ac 15 e0 01 42 01  ac 15 e0 02 08 00 45 00   B·····B· ······E·
0010  00 89 e4 aa 40 00 40 06  39 27 ac 15 e0 02 8e fa   ····@·@· 9'······
0020  01 8b c1 f4 00 50 cb 6b  93 a1 60 64 ec 24 80 18   ·····P·k ··`d·$··
0030  01 ff 1d 19 00 00 01 01  08 0a a7 23 85 7e f2 92   ········ ···#·~··
0040  4f b2 47 45 54 20 2f 20  48 54 54 50 2f 31 2e 31   O·GET /  HTTP/1.1
0050  0d 0a 48 6f 73 74 3a 20  6f 70 65 6e 73 6f 75 72   ··Host:  opensour
0060  63 65 2e 67 6f 6f 67 6c  65 2e 63 6f 6d 0d 0a 55   ce.googl e.com··U
0070  73 65 72 2d 41 67 65 6e  74 3a 20 63 75 72 6c 2f   ser-Agen t: curl/
0080  37 2e 37 34 2e 30 0d 0a  41 63 63 65 70 74 3a 20   7.74.0·· Accept: 
0090  2a 2f 2a 0d 0a 0d 0a                               */*····
```

sample.pcap | Packets: 200 · Displayed: 9 (4.5%) | Profile: Defa


••• sample.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.dst == 142.250.1.139

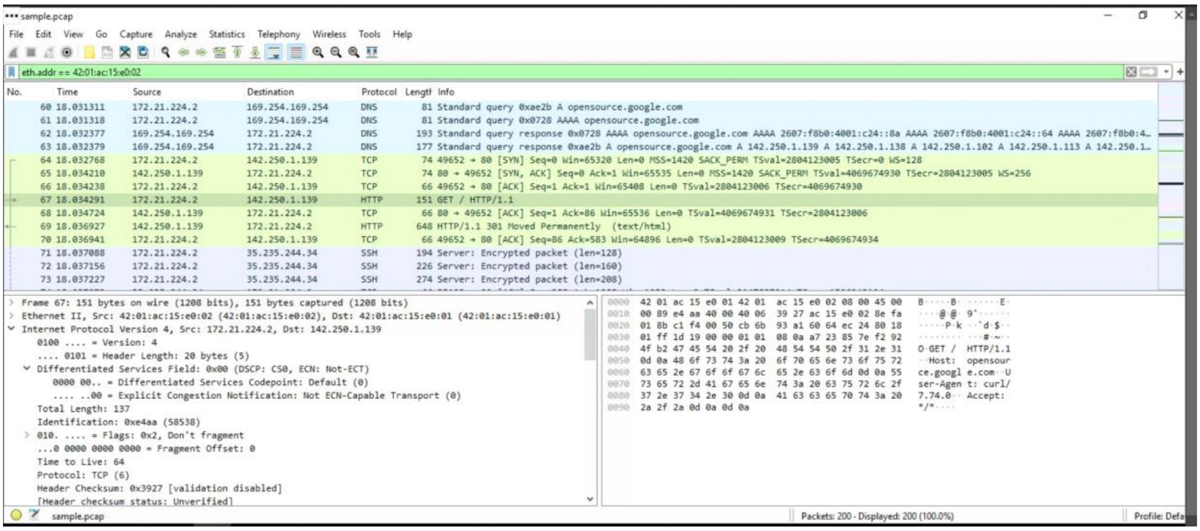
No.   Time   Source   Destination   Protocol Length Info
   16 8.642690   172.21.224.2   142.250.1.139   ICMP   98 Echo (ping) request id=0x6831, seq=1/256, ttl=64 (reply in 18)
   25 9.644712   172.21.224.2   142.250.1.139   ICMP   98 Echo (ping) request id=0x6831, seq=2/512, ttl=64 (reply in 26)
   31 10.646049   172.21.224.2   142.250.1.139   ICMP   98 Echo (ping) request id=0x6831, seq=3/768, ttl=64 (reply in 32)
   64 18.032768   172.21.224.2   142.250.1.139   TCP   74 49652 → 80 [SYN] Seq=0 Win=65320 Len=0 MSS=1420 SACK_PERM TSval=2804123005 TSecr=0 WS=128
   66 18.034238   172.21.224.2   142.250.1.139   TCP   66 49652 → 80 [ACK] Seq=1 Ack=1 Win=65408 Len=0 TSval=2804123006 TSecr=4069674930
   67 18.034291   172.21.224.2   142.250.1.139   HTTP   151 GET / HTTP/1.1
   70 18.036941   172.21.224.2   142.250.1.139   TCP   66 49652 → 80 [ACK] Seq=86 Ack=583 Win=64896 Len=0 TSval=2804123009 TSecr=4069674934
   79 18.037390   172.21.224.2   142.250.1.139   TCP   66 49652 → 80 [FIN, ACK] Seq=86 Ack=583 Win=64896 Len=0 TSval=2804123009 TSecr=4069674934
   83 18.037936   172.21.224.2   142.250.1.139   TCP   66 49652 → 80 [ACK] Seq=87 Ack=584 Win=64896 Len=0 TSval=2804123010 TSecr=4069674935

> Frame 67: 151 bytes on wire (1208 bits), 151 bytes captured (1208 bits)
> Ethernet II, Src: 42:01:ac:15:e0:02 (42:01:ac:15:e0:02), Dst: 42:01:ac:15:e0:01 (42:01:ac:15:e0:01)
v Internet Protocol Version 4, Src: 172.21.224.2, Dst: 142.250.1.139
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  v Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 137
    Identification: 0xe4aa (58538)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0x3927 [validation disabled]
    [Header checksum status: Unverified]

0000 42 01 ac 15 e0 01 42 01 ac 15 e0 02 08 00 45 00   B·····B· ······E·
0010 00 89 e4 aa 40 00 40 06 39 27 ac 15 e0 02 8e fa   ····@·@· 9'······
0020 01 8b c1 f4 00 50 cb 6b 93 a1 60 64 ec 24 80 18   ·····P·k ··`d·$··
0030 01 ff 1d 19 00 00 01 01 08 0a a7 23 85 7e f2 92   ········ ···#·~··
0040 4f b2 47 45 54 20 2f 20 48 54 54 50 2f 31 2e 31   O·GET / HTTP/1.1
0050 0d 0a 48 6f 73 74 3a 20 6f 70 65 6e 73 6f 75 72   ··Host: opensour
0060 63 65 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 0d 0a 55   ce.googl e.com··U
0070 73 65 72 2d 41 67 65 6e 74 3a 20 63 75 72 6c 2f   ser-Agen t: curl/
0080 37 2e 37 34 2e 30 0d 0a 41 63 63 65 70 74 3a 20   7.74.0·· Accept:
0090 2a 2f 2a 0d 0a 0d 0a   */*····

sample.pcap | Packets: 200 · Displayed: 9 (4.5%) | Profile: Defa

Then, the packets were filtered for the MAC address **42:01:ac:15:e0:02** as follows:


sample.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

eth.addr == 42:01:ac:15:e0:02

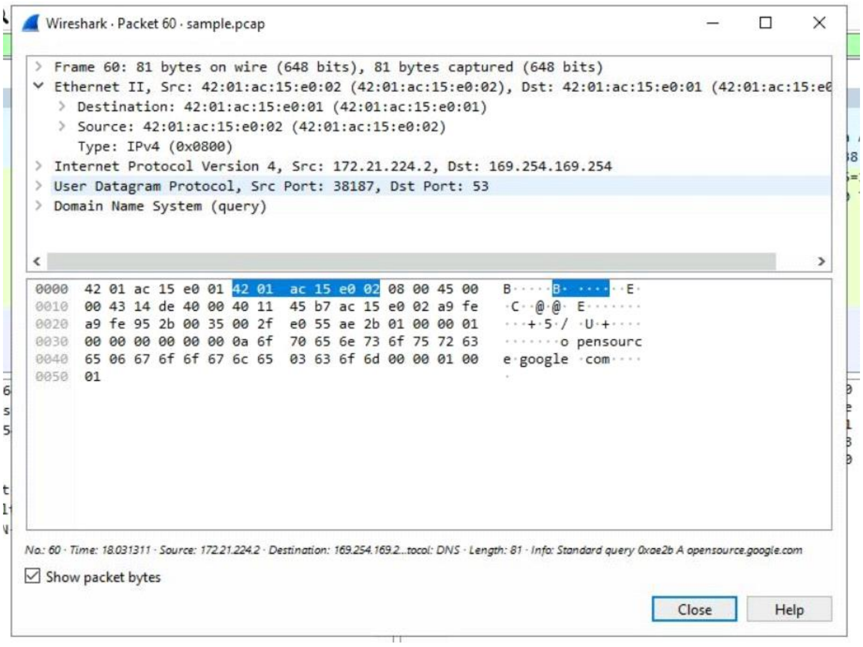
```
No.   Time       Source           Destination      Protocol Lengtł Info
   60 18.031311  172.21.224.2     169.254.169.254  DNS       81 Standard query 0xae2b A opensource.google.com
   61 18.031318  172.21.224.2     169.254.169.254  DNS       81 Standard query 0x0728 AAAA opensource.google.com
   62 18.032377  169.254.169.254  172.21.224.2     DNS      193 Standard query response 0x0728 AAAA opensource.google.com AAAA 2607:f8b0:4001:c24::8a AAAA 2607:f8b0:4001:c24::64 AAAA 2607:f8b0:4…
   63 18.032379  169.254.169.254  172.21.224.2     DNS      177 Standard query response 0xae2b A opensource.google.com A 142.250.1.139 A 142.250.1.138 A 142.250.1.102 A 142.250.1.113 A 142.250.1…
   64 18.032768  172.21.224.2     142.250.1.139    TCP       74 49652 → 80 [SYN] Seq=0 Win=65320 Len=0 MSS=1420 SACK_PERM TSval=2804123005 TSecr=0 WS=128
   65 18.034210  142.250.1.139    172.21.224.2     TCP       74 80 → 49652 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1420 SACK_PERM TSval=4069674930 TSecr=2804123005 WS=256
   66 18.034238  172.21.224.2     142.250.1.139    TCP       66 49652 → 80 [ACK] Seq=1 Ack=1 Win=65408 Len=0 TSval=2804123006 TSecr=4069674930
   67 18.034291  172.21.224.2     142.250.1.139    HTTP     151 GET / HTTP/1.1
   68 18.034724  142.250.1.139    172.21.224.2     TCP       66 80 → 49652 [ACK] Seq=1 Ack=86 Win=65536 Len=0 TSval=4069674931 TSecr=2804123006
   69 18.036927  142.250.1.139    172.21.224.2     HTTP     648 HTTP/1.1 301 Moved Permanently  (text/html)
   70 18.036941  172.21.224.2     142.250.1.139    TCP       66 49652 → 80 [ACK] Seq=86 Ack=583 Win=64896 Len=0 TSval=2804123009 TSecr=4069674934
   71 18.037088  172.21.224.2     35.235.244.34    SSH      194 Server: Encrypted packet (len=128)
   72 18.037156  172.21.224.2     35.235.244.34    SSH      226 Server: Encrypted packet (len=160)
   73 18.037227  172.21.224.2     35.235.244.34    SSH      274 Server: Encrypted packet (len=208)
```

```
> Frame 67: 151 bytes on wire (1208 bits), 151 bytes captured (1208 bits)
> Ethernet II, Src: 42:01:ac:15:e0:02 (42:01:ac:15:e0:02), Dst: 42:01:ac:15:e0:01 (42:01:ac:15:e0:01)
v Internet Protocol Version 4, Src: 172.21.224.2, Dst: 142.250.1.139
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  v Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 137
    Identification: 0xe4aa (58538)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0x3927 [validation disabled]
    [Header checksum status: Unverified]
```

```
0000  42 01 ac 15 e0 01 42 01  ac 15 e0 02 08 00 45 00   B·····B· ······E·
0010  00 89 e4 aa 40 00 40 06  39 27 ac 15 e0 02 8e fa   ····@·@· 9'······
0020  01 8b c1 f4 00 50 cb 6b  93 a1 60 64 ec 24 80 18   ·····P·k ··`d·$··
0030  01 ff 1d 19 00 00 01 01  08 0a a7 23 85 7e f2 92   ········ ···#·~··
0040  4f b2 47 45 54 20 2f 20  48 54 54 50 2f 31 2e 31   O·GET /  HTTP/1.1
0050  0d 0a 48 6f 73 74 3a 20  6f 70 65 6e 73 6f 75 72   ··Host:  opensour
0060  63 65 2e 67 6f 6f 67 6c  65 2e 63 6f 6d 0d 0a 55   ce.googl e.com··U
0070  73 65 72 2d 41 67 65 6e  74 3a 20 63 75 72 6c 2f   ser-Agen t: curl/
0080  37 2e 37 34 2e 30 0d 0a  41 63 63 65 70 74 3a 20   7.74.0·· Accept: 
0090  2a 2f 2a 0d 0a 0d 0a                               */*····
```

sample.pcap | Packets: 200 · Displayed: 200 (100.0%) | Profile: Defa

The first Packet in the list is selected and opened. The **Ethernet II** subtree is selected. The MAC address specified in the filter is listed as either the source or destination address in the expanded Ethernet II subtree:



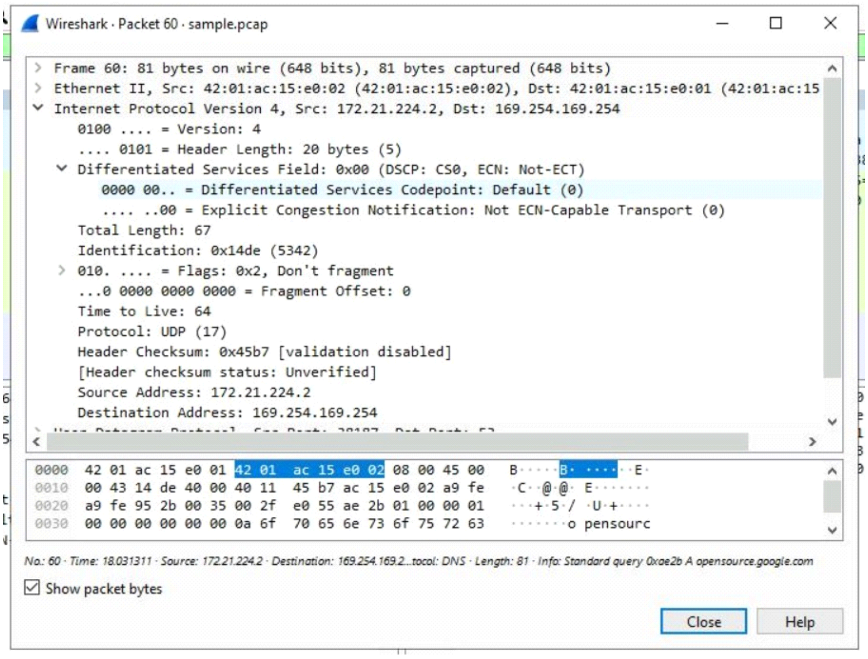
```
> Frame 60: 81 bytes on wire (648 bits), 81 bytes captured (648 bits)
v Ethernet II, Src: 42:01:ac:15:e0:02 (42:01:ac:15:e0:02), Dst: 42:01:ac:15:e0:01 (42:01:ac:15:e0
  > Destination: 42:01:ac:15:e0:01 (42:01:ac:15:e0:01)
  > Source: 42:01:ac:15:e0:02 (42:01:ac:15:e0:02)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 172.21.224.2, Dst: 169.254.169.254
> User Datagram Protocol, Src Port: 38187, Dst Port: 53
> Domain Name System (query)
```

```
0000  42 01 ac 15 e0 01 42 01  ac 15 e0 02 08 00 45 00   B·····B· ······E·
0010  00 43 14 de 40 00 40 11  45 b7 ac 15 e0 02 a9 fe   ·C··@·@· E·······
0020  a9 fe 95 2b 00 35 00 2f  e0 55 ae 2b 01 00 00 01   ···+·5·/ ·U·+····
0030  00 00 00 00 00 00 0a 6f  70 65 6e 73 6f 75 72 63   ·······o pensourc
0040  65 06 67 6f 6f 67 6c 65  03 63 6f 6d 00 00 01 00   e·google ·com····
0050  01                                                 ·
```

No.: 60 · Time: 18.031311 · Source: 172.21.224.2 · Destination: 169.254.169.2...tocol: DNS · Length: 81 · Info: Standard query 0xae2b A opensource.google.com

☑ Show packet bytes

Then, the **Internet Protocol Version 4** subtree is selected to observe the **Time to Live** and **Protocol** used:



Wireshark · Packet 60 · sample.pcap

```
> Frame 60: 81 bytes on wire (648 bits), 81 bytes captured (648 bits)
> Ethernet II, Src: 42:01:ac:15:e0:02 (42:01:ac:15:e0:02), Dst: 42:01:ac:15:e0:01 (42:01:ac:15
v Internet Protocol Version 4, Src: 172.21.224.2, Dst: 169.254.169.254
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  v Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 67
    Identification: 0x14de (5342)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: UDP (17)
    Header Checksum: 0x45b7 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 172.21.224.2
    Destination Address: 169.254.169.254
```

```
0000  42 01 ac 15 e0 01 42 01  ac 15 e0 02 08 00 45 00   B·····B· ······E·
0010  00 43 14 de 40 00 40 11  45 b7 ac 15 e0 02 a9 fe   ·C··@·@· E·······
0020  a9 fe 95 2b 00 35 00 2f  e0 55 ae 2b 01 00 00 01   ···+·5·/ ·U·+····
0030  00 00 00 00 00 00 0a 6f  70 65 6e 73 6f 75 72 63   ·······o pensourc
```

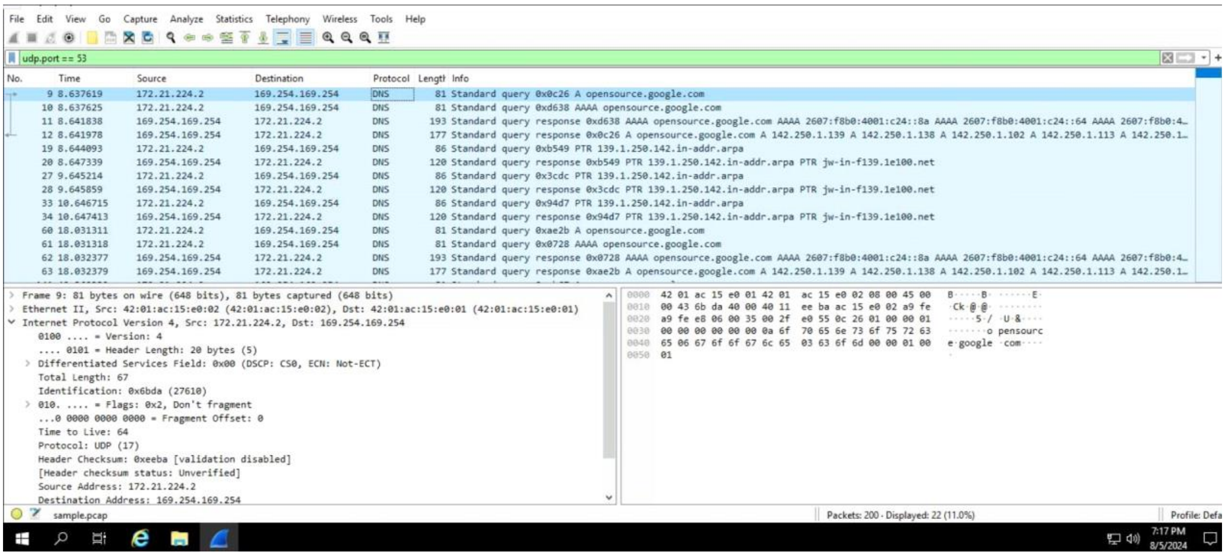
No.: 60 · Time: 18.031311 · Source: 172.21.224.2 · Destination: 169.254.169.2...tocol: DNS · Length: 81 · Info: Standard query 0xae2b A opensource.google.com

☑ Show packet bytes

Use filters to explore DNS packets

Direction: The analyst must use filters to select and examine DNS traffic and then drill down into the protocol to examine how the DNS packet data contains both **queries** and **answers**.

Packets are filtered for UDP traffic at port 53 as follows:



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

udp.port == 53

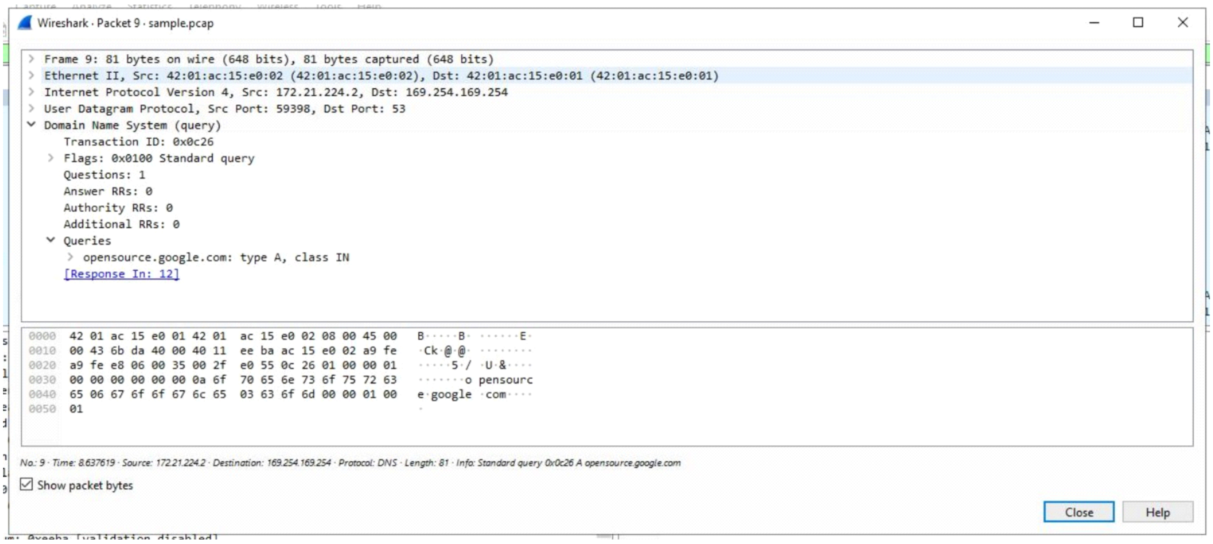
```
No.  Time        Source           Destination      Protocol Length Info
   9 8.637619    172.21.224.2     169.254.169.254  DNS       81 Standard query 0x0c26 A opensource.google.com
  10 8.637625    172.21.224.2     169.254.169.254  DNS       81 Standard query 0xd638 AAAA opensource.google.com
  11 8.641838    169.254.169.254  172.21.224.2     DNS      193 Standard query response 0xd638 AAAA opensource.google.com AAAA 2607:f8b0:4001:c24::8a AAAA 2607:f8b0:4001:c24::64 AAAA 2607:f8b0:4…
  12 8.641978    169.254.169.254  172.21.224.2     DNS      177 Standard query response 0x0c26 A opensource.google.com A 142.250.1.139 A 142.250.1.138 A 142.250.1.102 A 142.250.1.113 A 142.250.1…
  19 8.644093    172.21.224.2     169.254.169.254  DNS       86 Standard query 0xb549 PTR 139.1.250.142.in-addr.arpa
  20 8.647339    169.254.169.254  172.21.224.2     DNS      120 Standard query response 0xb549 PTR 139.1.250.142.in-addr.arpa PTR jw-in-f139.1e100.net
  27 9.645214    172.21.224.2     169.254.169.254  DNS       86 Standard query 0x3cdc PTR 139.1.250.142.in-addr.arpa
  28 9.645859    169.254.169.254  172.21.224.2     DNS      120 Standard query response 0x3cdc PTR 139.1.250.142.in-addr.arpa PTR jw-in-f139.1e100.net
  33 10.646715   172.21.224.2     169.254.169.254  DNS       86 Standard query 0x94d7 PTR 139.1.250.142.in-addr.arpa
  34 10.647413   169.254.169.254  172.21.224.2     DNS      120 Standard query response 0x94d7 PTR 139.1.250.142.in-addr.arpa PTR jw-in-f139.1e100.net
  60 18.031311   172.21.224.2     169.254.169.254  DNS       81 Standard query 0xae2b A opensource.google.com
  61 18.031318   172.21.224.2     169.254.169.254  DNS       81 Standard query 0x0728 AAAA opensource.google.com
  62 18.032377   169.254.169.254  172.21.224.2     DNS      193 Standard query response 0x0728 AAAA opensource.google.com AAAA 2607:f8b0:4001:c24::8a AAAA 2607:f8b0:4001:c24::64 AAAA 2607:f8b0:4…
  63 18.032379   169.254.169.254  172.21.224.2     DNS      177 Standard query response 0xae2b A opensource.google.com A 142.250.1.139 A 142.250.1.138 A 142.250.1.102 A 142.250.1.113 A 142.250.1…
```

```
> Frame 9: 81 bytes on wire (648 bits), 81 bytes captured (648 bits)
> Ethernet II, Src: 42:01:ac:15:e0:02 (42:01:ac:15:e0:02), Dst: 42:01:ac:15:e0:01 (42:01:ac:15:e0:01)
v Internet Protocol Version 4, Src: 172.21.224.2, Dst: 169.254.169.254
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 67
    Identification: 0x6bda (27610)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: UDP (17)
    Header Checksum: 0xeeba [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 172.21.224.2
    Destination Address: 169.254.169.254
```

```
0000  42 01 ac 15 e0 01 42 01  ac 15 e0 02 08 00 45 00   B·····B· ······E·
0010  00 43 6b da 40 00 40 11  ee ba ac 15 e0 02 a9 fe   ·Ck·@·@· ········
0020  a9 fe e8 06 00 35 00 2f  e0 55 0c 26 01 00 00 01   ·····5·/ ·U·&····
0030  00 00 00 00 00 00 0a 6f  70 65 6e 73 6f 75 72 63   ·······o pensourc
0040  65 06 67 6f 6f 67 6c 65  03 63 6f 6d 00 00 01 00   e·google ·com····
0050  01                                                 ·
```

sample.pcap | Packets: 200 · Displayed: 22 (11.0%) | Profile: Defa

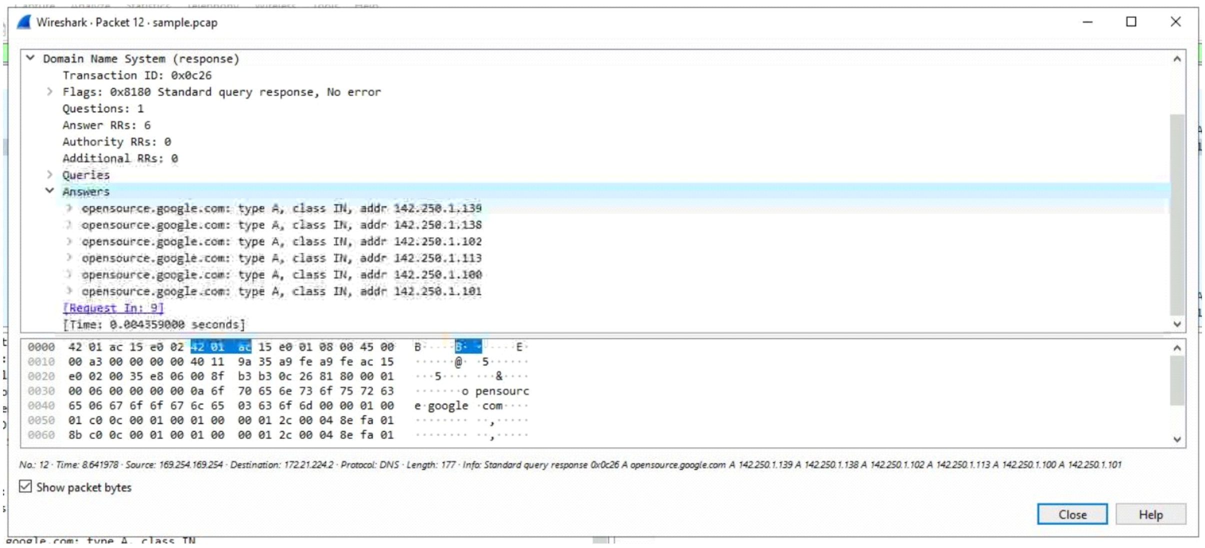
The first packet is opened and the **Domain Name System (query)** subtree is explored:



```
> Frame 9: 81 bytes on wire (648 bits), 81 bytes captured (648 bits)
> Ethernet II, Src: 42:01:ac:15:e0:02 (42:01:ac:15:e0:02), Dst: 42:01:ac:15:e0:01 (42:01:ac:15:e0:01)
> Internet Protocol Version 4, Src: 172.21.224.2, Dst: 169.254.169.254
> User Datagram Protocol, Src Port: 59398, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x0c26
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > opensource.google.com: type A, class IN
    [Response In: 12]

0000  42 01 ac 15 e0 01 42 01  ac 15 e0 02 08 00 45 00   B·····B· ······E·
0010  00 43 6b da 40 00 40 11  ee ba ac 15 e0 02 a9 fe   ·Ck·@·@· ········
0020  a9 fe e8 06 00 35 00 2f  e0 55 0c 26 01 00 00 01   ·····5·/ ·U·&····
0030  00 00 00 00 00 00 0a 6f  70 65 6e 73 6f 75 72 63   ·······o pensourc
0040  65 06 67 6f 6f 67 6c 65  03 63 6f 6d 00 00 01 00   e·google ·com····
0050  01                                                 ·

No.: 9 · Time: 8.637619 · Source: 172.21.224.2 · Destination: 169.254.169.254 · Protocol: DNS · Length: 81 · Info: Standard query 0x0c26 A opensource.google.com
```

☑ Show packet bytes

The queried website is observed to be opensource.google.com. Then the details pane is closed and the 4th packet in the list is opened and the **Domain Name System (query)** subtree is opened. The **Answers** subtree is explored:



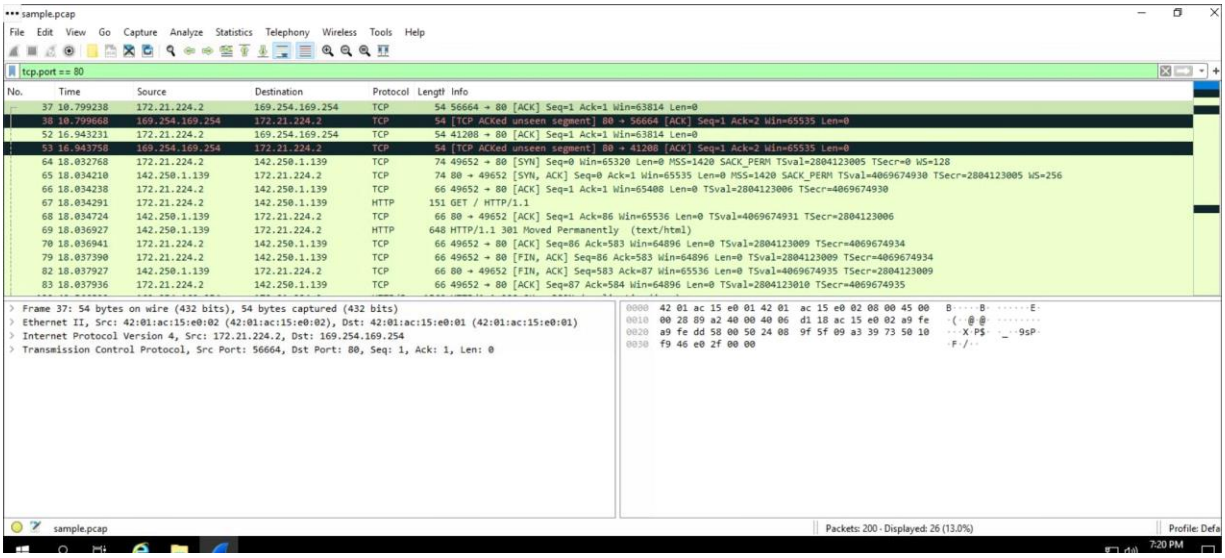
```
v Domain Name System (response)
    Transaction ID: 0x0c26
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 6
    Authority RRs: 0
    Additional RRs: 0
  > Queries
  v Answers
    > opensource.google.com: type A, class IN, addr 142.250.1.139
    > opensource.google.com: type A, class IN, addr 142.250.1.138
    > opensource.google.com: type A, class IN, addr 142.250.1.102
    > opensource.google.com: type A, class IN, addr 142.250.1.113
    > opensource.google.com: type A, class IN, addr 142.250.1.100
    > opensource.google.com: type A, class IN, addr 142.250.1.101
    [Request In: 9]
    [Time: 0.004359000 seconds]

0000  42 01 ac 15 e0 02 42 01  ac 15 e0 01 08 00 45 00   B·····B· ······E·
0010  00 a3 00 00 00 00 40 11  9a 35 a9 fe a9 fe ac 15   ······@· ·5······
0020  e0 02 00 35 e8 06 00 8f  b3 b3 0c 26 81 80 00 01   ···5···· ···&····
0030  00 06 00 00 00 00 0a 6f  70 65 6e 73 6f 75 72 63   ·······o pensourc
0040  65 06 67 6f 6f 67 6c 65  03 63 6f 6d 00 00 01 00   e·google ·com····
0050  01 c0 0c 00 01 00 01 00  00 01 2c 00 04 8e fa 01   ········ ··,·····
0060  8b c0 0c 00 01 00 01 00  00 01 2c 00 04 8e fa 01   ········ ··,·····

No.: 12 · Time: 8.641978 · Source: 169.254.169.254 · Destination: 172.21.224.2 · Protocol: DNS · Length: 177 · Info: Standard query response 0x0c26 A opensource.google.com A 142.250.1.139 A 142.250.1.138 A 142.250.1.102 A 142.250.1.113 A 142.250.1.100 A 142.250.1.101
```

☑ Show packet bytes

Use filters to explore TCP packets

Direction: The analyst must use additional filters to search for text that is present in payload data contained inside network packets.

The TCP traffic is for port 80 as follows:

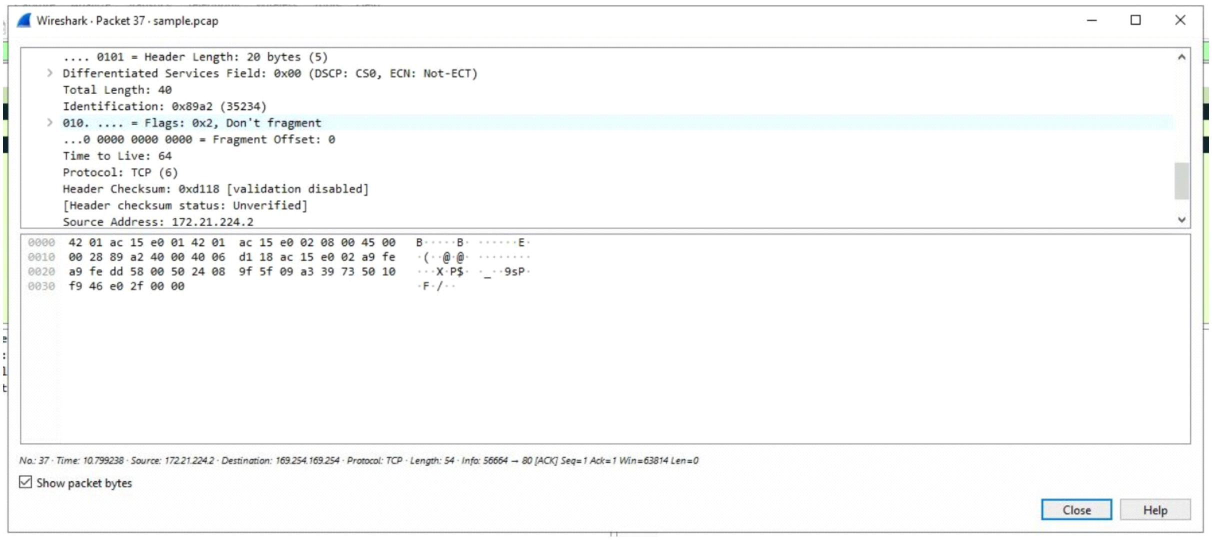

sample.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.port == 80

```
No.   Time       Source           Destination      Protocol Lengtl Info
   37 10.799238  172.21.224.2     169.254.169.254  TCP      54 56664 → 80 [ACK] Seq=1 Ack=1 Win=63814 Len=0
   38 10.799668  169.254.169.254  172.21.224.2     TCP      54 [TCP ACKed unseen segment] 80 → 56664 [ACK] Seq=1 Ack=2 Win=65535 Len=0
   52 16.943231  172.21.224.2     169.254.169.254  TCP      54 41208 → 80 [ACK] Seq=1 Ack=1 Win=63814 Len=0
   53 16.943758  169.254.169.254  172.21.224.2     TCP      54 [TCP ACKed unseen segment] 80 → 41208 [ACK] Seq=1 Ack=2 Win=65535 Len=0
   64 18.032768  172.21.224.2     142.250.1.139    TCP      74 49652 → 80 [SYN] Seq=0 Win=65320 Len=0 MSS=1420 SACK_PERM TSval=2804123005 TSecr=0 WS=128
   65 18.034210  142.250.1.139    172.21.224.2     TCP      74 80 → 49652 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1420 SACK_PERM TSval=4069674930 TSecr=2804123005 WS=256
   66 18.034238  172.21.224.2     142.250.1.139    TCP      66 49652 → 80 [ACK] Seq=1 Ack=1 Win=65408 Len=0 TSval=2804123006 TSecr=4069674930
   67 18.034291  172.21.224.2     142.250.1.139    HTTP    151 GET / HTTP/1.1
   68 18.034724  142.250.1.139    172.21.224.2     TCP      66 80 → 49652 [ACK] Seq=1 Ack=86 Win=65536 Len=0 TSval=4069674931 TSecr=2804123006
   69 18.036927  142.250.1.139    172.21.224.2     HTTP    648 HTTP/1.1 301 Moved Permanently  (text/html)
   70 18.036941  172.21.224.2     142.250.1.139    TCP      66 49652 → 80 [ACK] Seq=86 Ack=583 Win=64896 Len=0 TSval=2804123009 TSecr=4069674934
   79 18.037390  172.21.224.2     142.250.1.139    TCP      66 49652 → 80 [FIN, ACK] Seq=86 Ack=583 Win=64896 Len=0 TSval=2804123009 TSecr=4069674934
   82 18.037927  142.250.1.139    172.21.224.2     TCP      66 80 → 49652 [FIN, ACK] Seq=583 Ack=87 Win=65536 Len=0 TSval=4069674935 TSecr=2804123009
   83 18.037936  172.21.224.2     142.250.1.139    TCP      66 49652 → 80 [ACK] Seq=87 Ack=584 Win=64896 Len=0 TSval=2804123010 TSecr=4069674935
```

```
> Frame 37: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
> Ethernet II, Src: 42:01:ac:15:e0:02 (42:01:ac:15:e0:02), Dst: 42:01:ac:15:e0:01 (42:01:ac:15:e0:01)
> Internet Protocol Version 4, Src: 172.21.224.2, Dst: 169.254.169.254
> Transmission Control Protocol, Src Port: 56664, Dst Port: 80, Seq: 1, Ack: 1, Len: 0
```

```
0000  42 01 ac 15 e0 01 42 01  ac 15 e0 02 08 00 45 00   B·····B· ······E·
0010  00 28 89 a2 40 00 40 06  d1 18 ac 15 e0 02 a9 fe   ·(··@·@· ········
0020  a9 fe dd 58 00 50 24 08  9f 5f 09 a3 39 73 50 10   ···X·P$· ·_··9sP·
0030  f9 46 e0 2f 00 00                                  ·F·/··
```

The `first` packet in the list is opened and the **Time to Live** is observed to be 64 bytes:



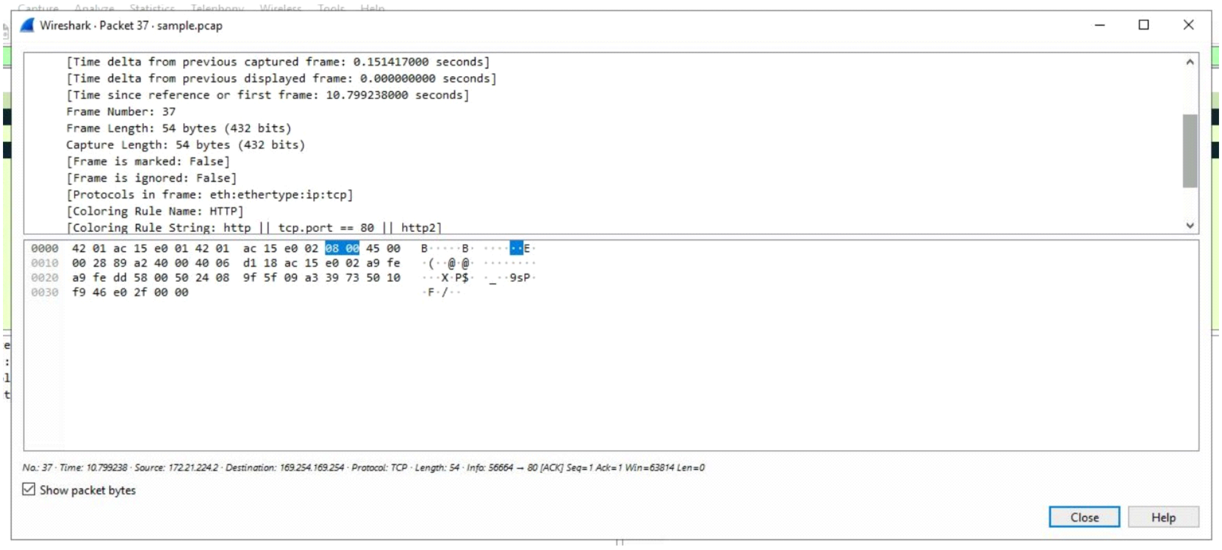
```
      .... 0101 = Header Length: 20 bytes (5)
    > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      Total Length: 40
      Identification: 0x89a2 (35234)
    > 010. .... = Flags: 0x2, Don't fragment
      ...0 0000 0000 0000 = Fragment Offset: 0
      Time to Live: 64
      Protocol: TCP (6)
      Header Checksum: 0xd118 [validation disabled]
      [Header checksum status: Unverified]
      Source Address: 172.21.224.2
```

```
0000  42 01 ac 15 e0 01 42 01  ac 15 e0 02 08 00 45 00   B·····B· ······E·
0010  00 28 89 a2 40 00 40 06  d1 18 ac 15 e0 02 a9 fe   ·(··@·@· ········
0020  a9 fe dd 58 00 50 24 08  9f 5f 09 a3 39 73 50 10   ···X·P$· ·_··9sP·
0030  f9 46 e0 2f 00 00                                  ·F·/··
```

No.: 37 · Time: 10.799238 · Source: 172.21.224.2 · Destination: 169.254.169.254 · Protocol: TCP · Length: 54 · Info: 56664 → 80 [ACK] Seq=1 Ack=1 Win=63814 Len=0

☑ Show packet bytes

Under the **Frame** subtree, the **Frame Length** is observed to be 54 bytes:



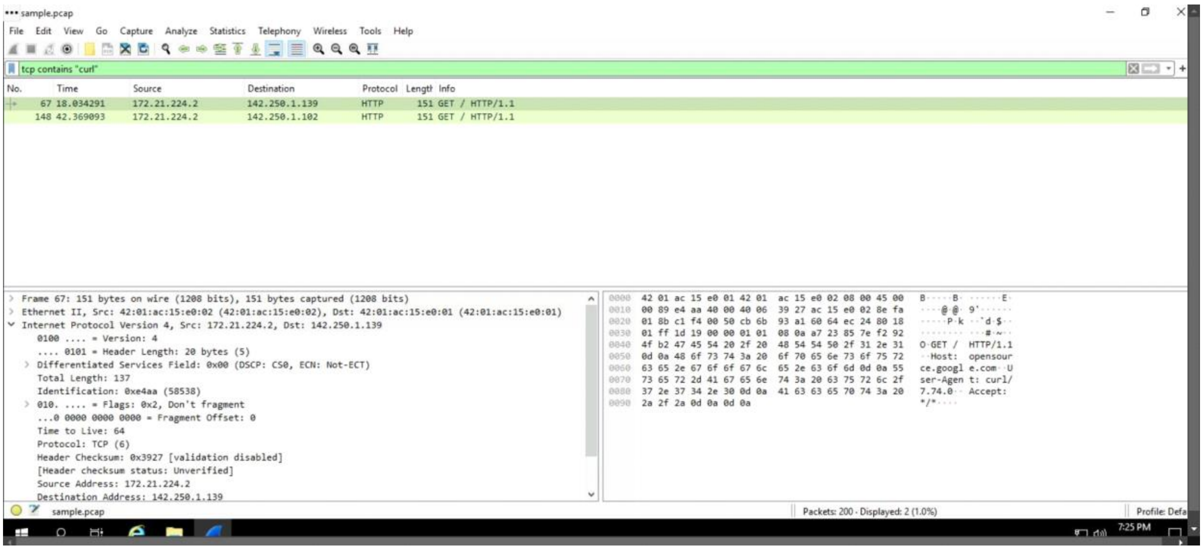
```
[Time delta from previous captured frame: 0.151417000 seconds]
[Time delta from previous displayed frame: 0.000000000 seconds]
[Time since reference or first frame: 10.799238000 seconds]
Frame Number: 37
Frame Length: 54 bytes (432 bits)
Capture Length: 54 bytes (432 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:tcp]
[Coloring Rule Name: HTTP]
[Coloring Rule String: http || tcp.port == 80 || http2]
```

```
0000  42 01 ac 15 e0 01 42 01  ac 15 e0 02 08 00 45 00   B·····B· ······E·
0010  00 28 89 a2 40 00 40 06  d1 18 ac 15 e0 02 a9 fe   ·(··@·@· ········
0020  a9 fe dd 58 00 50 24 08  9f 5f 09 a3 39 73 50 10   ···X·P$· ·_··9sP·
0030  f9 46 e0 2f 00 00                                  ·F·/··
```

No.: 37 · Time: 10.799238 · Source: 172.21.224.2 · Destination: 169.254.169.254 · Protocol: TCP · Length: 54 · Info: 56664 → 80 [ACK] Seq=1 Ack=1 Win=63814 Len=0

☑ Show packet bytes

The details are closed and filters are cleared. Then to search for specific text in a TCP packet, the **contains** filter is used:



tcp contains "curl"

```
No.     Time        Source          Destination      Protocol  Length  Info
   67   18.034291   172.21.224.2    142.250.1.139    HTTP      151     GET / HTTP/1.1
  148   42.369093   172.21.224.2    142.250.1.102    HTTP      151     GET / HTTP/1.1
```

```
> Frame 67: 151 bytes on wire (1208 bits), 151 bytes captured (1208 bits)
> Ethernet II, Src: 42:01:ac:15:e0:02 (42:01:ac:15:e0:02), Dst: 42:01:ac:15:e0:01 (42:01:ac:15:e0:01)
v Internet Protocol Version 4, Src: 172.21.224.2, Dst: 142.250.1.139
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 137
    Identification: 0xe4aa (58538)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0x3927 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 172.21.224.2
    Destination Address: 142.250.1.139
```

```
0000  42 01 ac 15 e0 01 42 01  ac 15 e0 02 08 00 45 00   B·····B· ······E·
0010  00 89 e4 aa 40 00 40 06  39 27 ac 15 e0 02 8e fa   ····@·@· 9'······
0020  01 8b c1 f4 00 50 cb 6b  93 a1 60 64 ec 24 80 18   ·····P·k ··`d·$··
0030  01 ff 1d 19 00 00 01 01  08 0a a7 23 85 7e f2 92   ········ ···#·~··
0040  4f b2 47 45 54 20 2f 20  48 54 54 50 2f 31 2e 31   O·GET /  HTTP/1.1
0050  0d 0a 48 6f 73 74 3a 20  6f 70 65 6e 73 6f 75 72   ··Host:  opensour
0060  63 65 2e 67 6f 6f 67 6c  65 2e 63 6f 6d 0d 0a 55   ce.googl e.com··U
0070  73 65 72 2d 41 67 65 6e  74 3a 20 63 75 72 6c 2f   ser-Agen t: curl/
0080  37 2e 37 34 2e 30 0d 0a  41 63 63 65 70 74 3a 20   7.74.0·· Accept: 
0090  2a 2f 2a 0d 0a 0d 0a                               */*····
```

Summary

Packet data was successfully analyzed and investigated using Wireshark filters like **==**, **contains** etc.. By filtering few commands, the packet analysis is successfully completed.