Analyze Packet Using Wireshark

Scenario

In this scenario, you're a security analyst investigating traffic to a website.

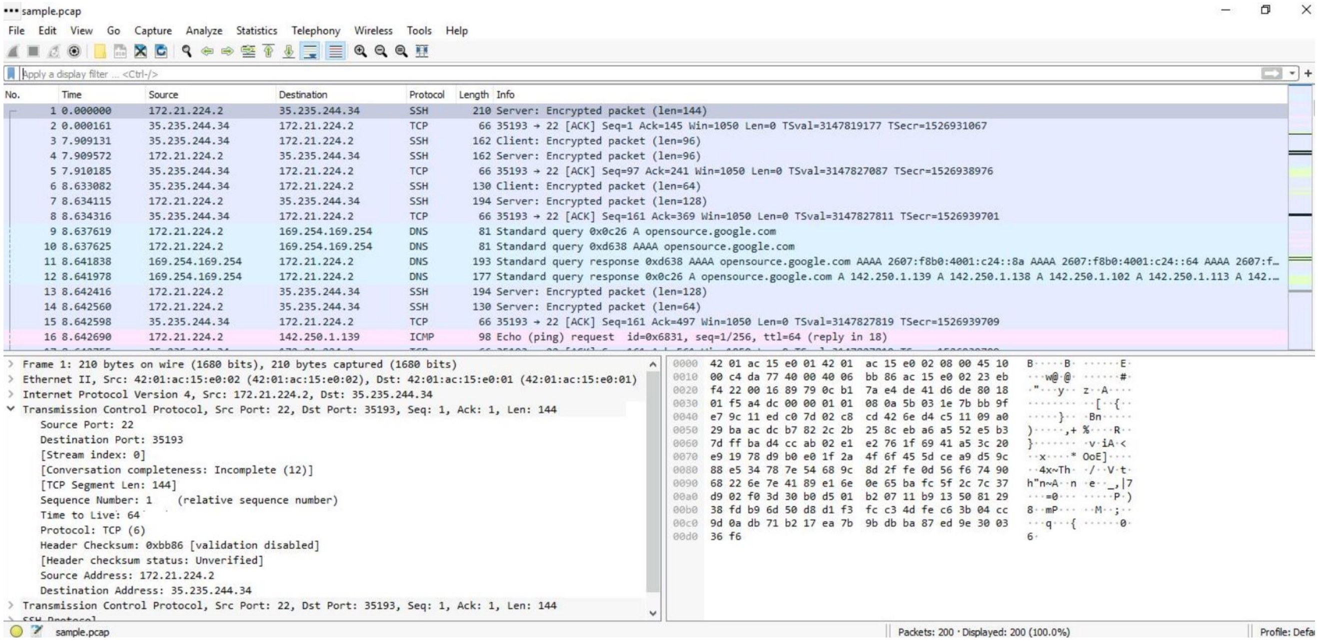
You'll analyze a network packet capture file that contains traffic data related to a user connecting to an internet site. The ability to filter network traffic using packet sniffers to gather relevant information is an essential skill as a security analyst.

You must filter the data in order to:

- identify the source and destination IP addresses involved in this web browsing session,
- examine the protocols that are used when the user makes the connection to the website, and
- analyze some of the data packets to identify the type of information sent and received by the systems that connect to each other when the network data is captured.

Here's how you'll do this: **First**, you'll open the packet capture file and explore the basic Wireshark graphic user interface. **Second**, you'll open a detailed view of a single packet and explore how to examine the various protocol and data layers inside a network packet. **Third**, you'll apply filters to select and inspect packets based on specific criteria. **Fourth**, you'll filter and inspect UDP DNS traffic to examine protocol data. **Finally**, you'll apply filters to TCP packet data to search for specific payload text data.

You're ready to use Wireshark to inspect network packet data!

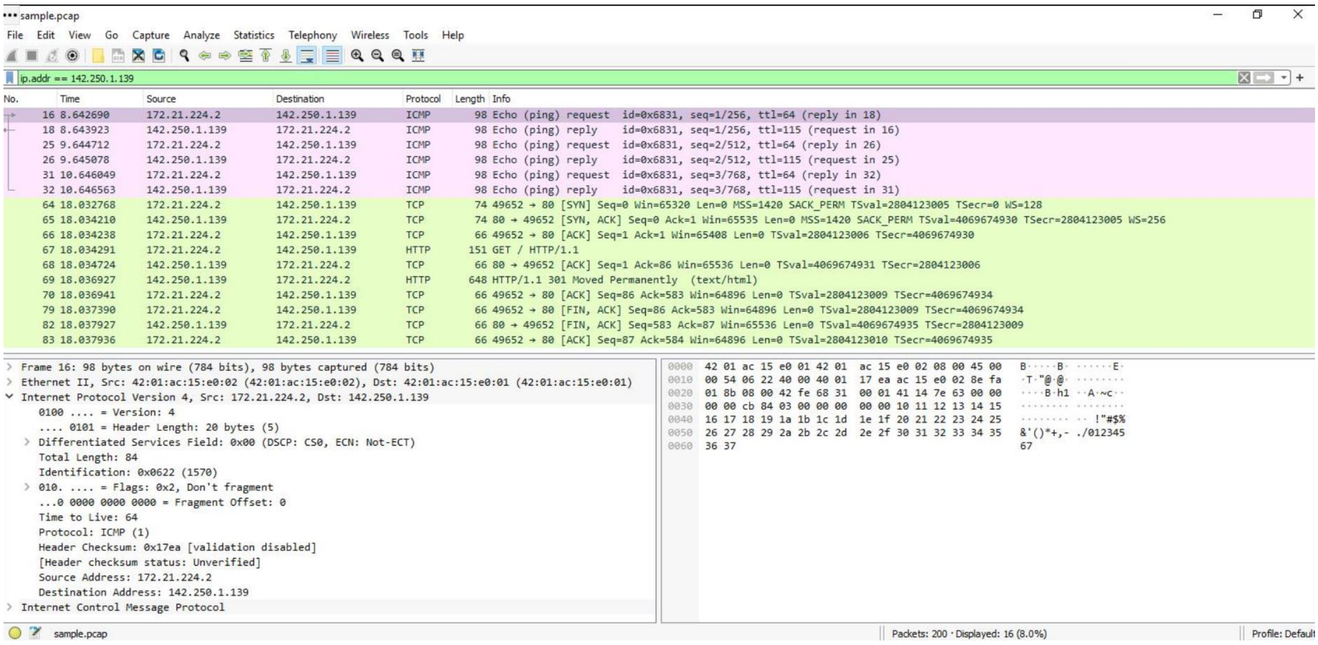

sample.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
sample.pcap
Packets: 200 · Displayed: 200 (100.0%)
Profile: Defa

```
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:f…
   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.…
   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)
   15 8.642598   35.235.244.34    172.21.224.2     TCP       66 35193 → 22 [ACK] Seq=161 Ack=497 Win=1050 Len=0 TSval=3147827819 TSecr=1526939709
   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)
```

```
> 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
v Transmission Control Protocol, Src Port: 22, Dst Port: 35193, Seq: 1, Ack: 1, Len: 144
    Source Port: 22
    Destination Port: 35193
    [Stream index: 0]
    [Conversation completeness: Incomplete (12)]
    [TCP Segment Len: 144]
    Sequence Number: 1    (relative sequence number)
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0xbb86 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 172.21.224.2
    Destination Address: 35.235.244.34
> Transmission Control Protocol, Src Port: 22, Dst Port: 35193, Seq: 1, Ack: 1, Len: 144
```

```
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·
```

Figure 1 Packets to be analyzed

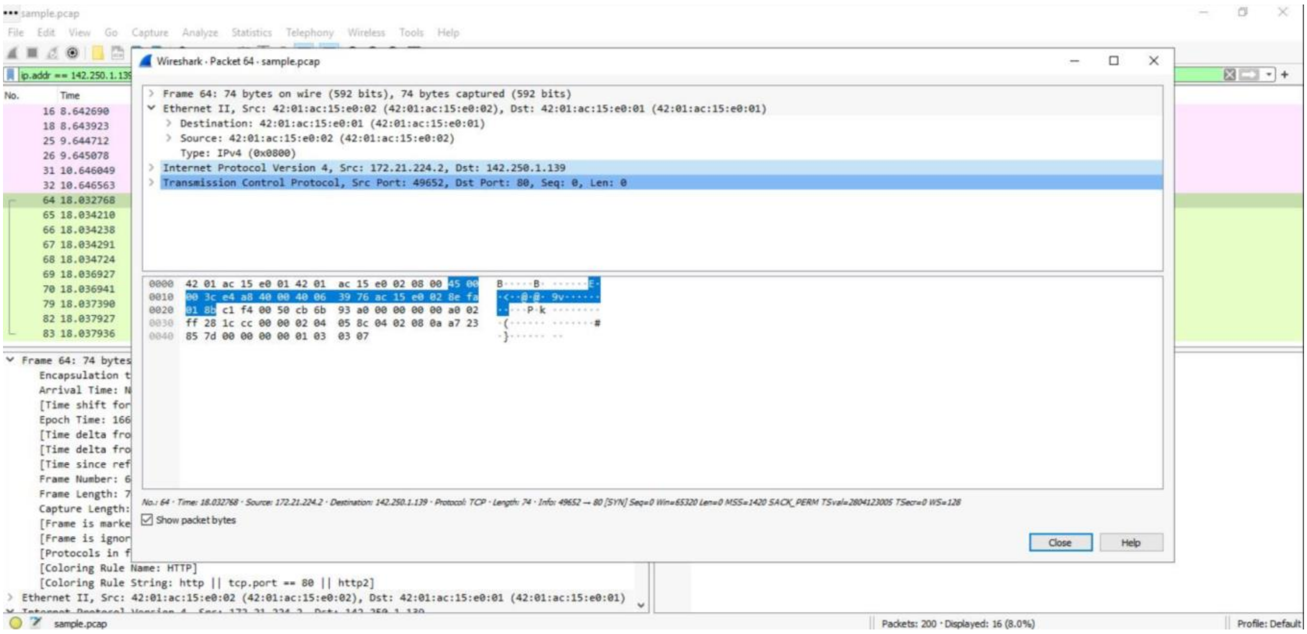

sample.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 142.250.1.139
sample.pcap
Packets: 200 · Displayed: 16 (8.0%)
Profile: Default

```
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)
   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)
   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)
   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)
   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)
   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)
   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 16: 98 bytes on wire (784 bits), 98 bytes captured (784 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: 84
    Identification: 0x0622 (1570)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: ICMP (1)
    Header Checksum: 0x17ea [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 172.21.224.2
    Destination Address: 142.250.1.139
> Internet Control Message Protocol
```

```
0000  42 01 ac 15 e0 01 42 01  ac 15 e0 02 08 00 45 00   B·····B· ······E·
0010  00 54 06 22 40 00 40 01  17 ea ac 15 e0 02 8e fa   ·T·"@·@· ········
0020  01 8b 08 00 42 fe 68 31  00 01 41 14 7e 63 00 00   ····B·h1 ··A·~c··
0030  00 00 cb 84 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
```

Figure 2 Applying display filtering


sample.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Packet 64 · sample.pcap
Show packet bytes
Close
Help

```
ip.addr == 142.250.1.139
No.   Time
 16 8.642690
 18 8.643923
 25 9.644712
 26 9.645078
 31 10.646049
 32 10.646563
 64 18.032768
 65 18.034210
 66 18.034238
 67 18.034291
 68 18.034724
 69 18.036927
 70 18.036941
 79 18.037390
 82 18.037927
 83 18.037936
```

```
> 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:e0:01)
  > 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                     ·}······ ··
```

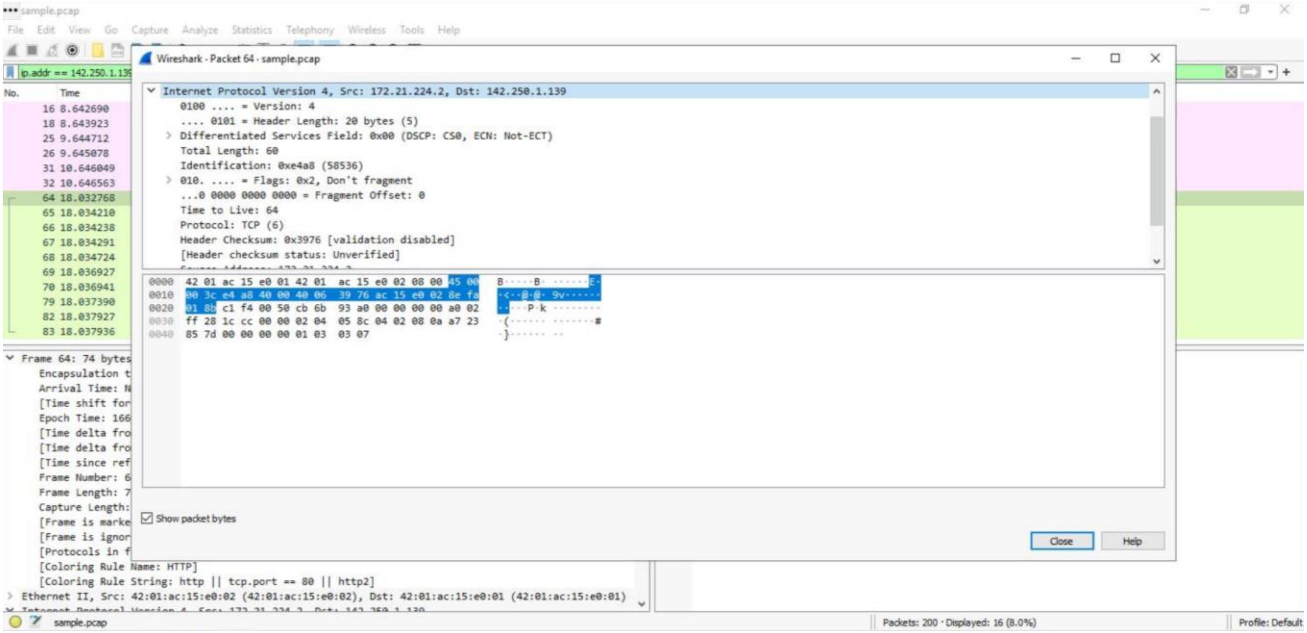
No.: 64 · Time: 18.032768 · Source: 172.21.224.2 · Destination: 142.250.1.139 · Protocol: TCP · Length: 74 · Info: 49652 → 80 [SYN] Seq=0 Win=65320 Len=0 MSS=1420 SACK_PERM TSval=2804123005 TSecr=0 WS=128

☑ Show packet bytes

```
v Frame 64: 74 bytes
    Encapsulation t
    Arrival Time: N
    [Time shift for
    Epoch Time: 166
    [Time delta fro
    [Time delta fro
    [Time since ref
    Frame Number: 6
    Frame Length: 7
    Capture Length:
    [Frame is marke
    [Frame is ignor
    [Protocols in f
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
> 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)
```

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

Figure 3 Ethernet II


sample.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Packet 64 · sample.pcap
Show packet bytes
Close
Help

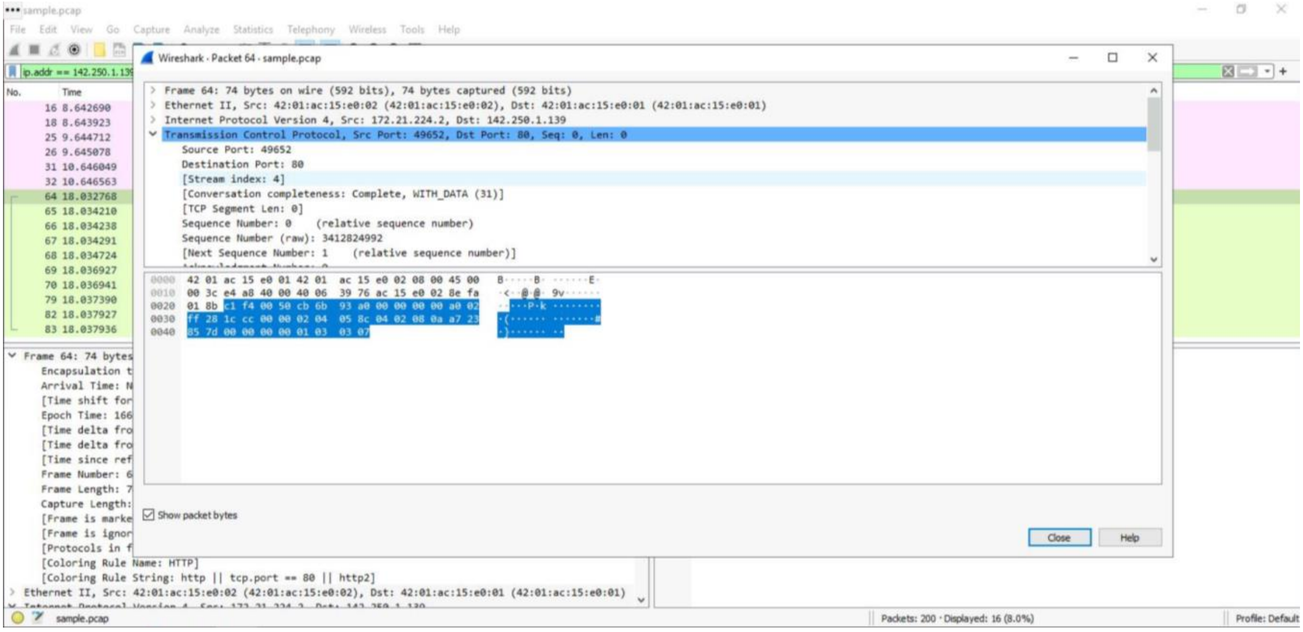
```
v Internet Protocol Version 4, Src: 172.21.224.2, Dst: 142.250.1.139
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0xe4a8 (58536)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0x3976 [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 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                     ·}······ ··
```

☑ Show packet bytes

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

Figure 4 IPv4


sample.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Packet 64 · sample.pcap
Close
Help
sample.pcap
Profile: Default

ip.addr == 142.250.1.139

```
No.    Time
 16 8.642690
 18 8.643923
 25 9.644712
 26 9.645078
 31 10.646049
 32 10.646563
 64 18.032768
 65 18.034210
 66 18.034238
 67 18.034291
 68 18.034724
 69 18.036927
 70 18.036941
 79 18.037390
 82 18.037927
 83 18.037936
```

```
> 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:e0:01)
> Internet Protocol Version 4, Src: 172.21.224.2, Dst: 142.250.1.139
v Transmission Control Protocol, Src Port: 49652, Dst Port: 80, Seq: 0, Len: 0
    Source Port: 49652
    Destination Port: 80
    [Stream index: 4]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 3412824992
    [Next Sequence Number: 1    (relative sequence number)]
```

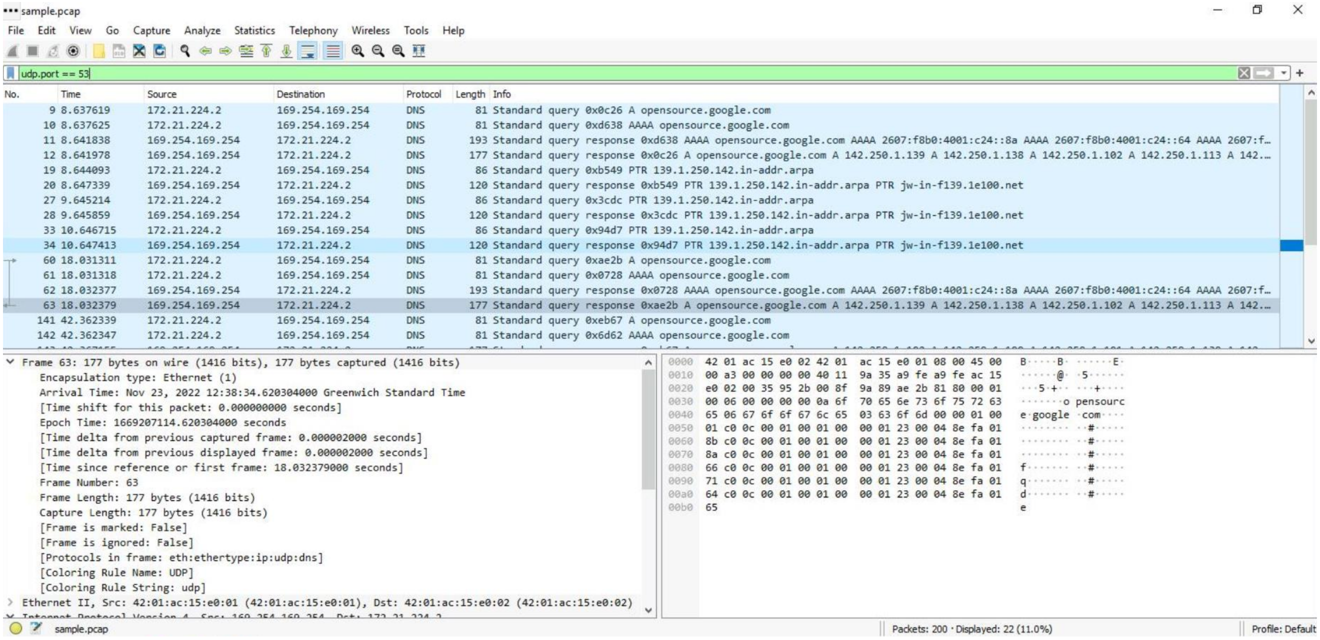
```
0000  42 01 ac 15 e0 01 42 01  ac 15 e0 02 08 00 45 00   B·····B· ······E·
0010  00 3c e4 a8 40 00 40 06  39 76 ac 15 e0 02 8e fa   ·<··@·@· 9v······
0020  01 8b c1 f4 00 50 cb 6b  93 a0 00 00 00 00 a0 02   ·····P·k ········
0030  ff 28 1c cc 00 00 02 04  05 8c 04 02 08 0a a7 23   ·(······ ·······#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

☑ Show packet bytes

```
v Frame 64: 74 bytes
    Encapsulation t
    Arrival Time: N
    [Time shift for
    Epoch Time: 166
    [Time delta fro
    [Time delta fro
    [Time since ref
    Frame Number: 6
    Frame Length: 7
    Capture Length:
    [Frame is marke
    [Frame is ignor
    [Protocols in f
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
> 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)
```

Packets: 200 · Displayed: 16 (8.0%)

Figure 5 TCP


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

udp.port == 53

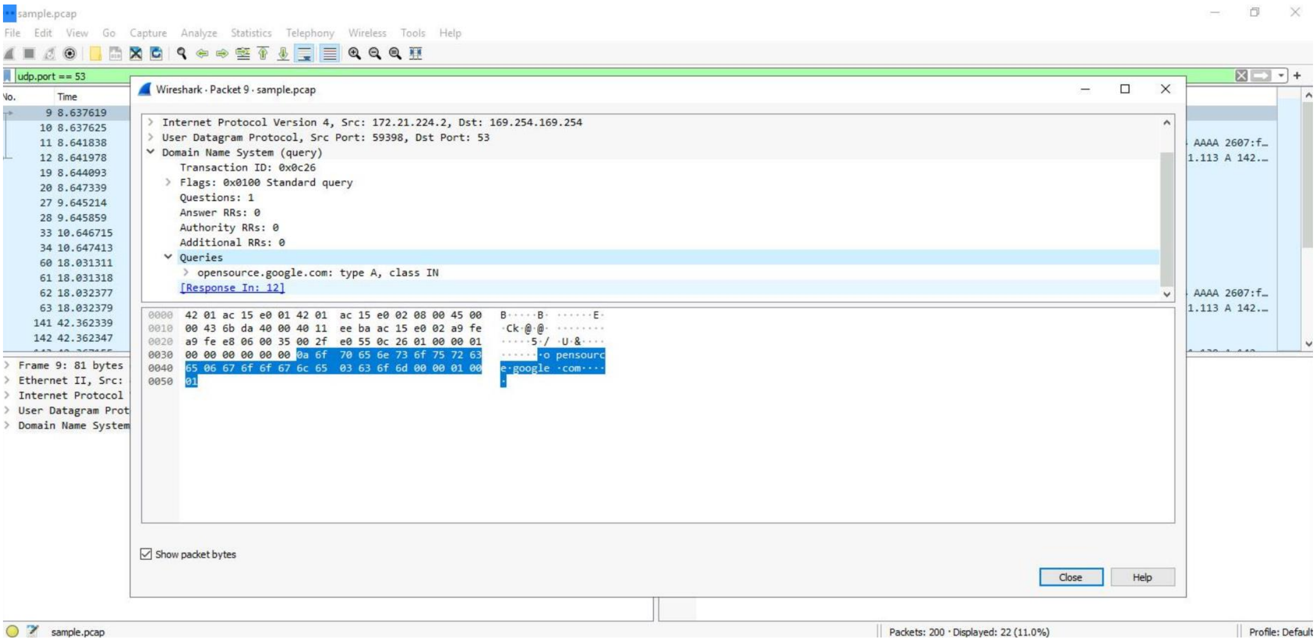
```
No.   Time       Source           Destination      Protocol Length Info
  9 8.637619    172.21.224.2     169.254.169.254  DNS       81 Standard query 0x0c26 A opensource.google.com
 10 8.637625    172.21.224.2     169.254.169.254  DNS       81 Standard query 0xd638 AAAA opensource.google.com
 11 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:f…
 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.…
 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:f…
 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.…
141 42.362339   172.21.224.2     169.254.169.254  DNS       81 Standard query 0xeb67 A opensource.google.com
142 42.362347   172.21.224.2     169.254.169.254  DNS       81 Standard query 0x6d62 AAAA opensource.google.com
```

```
v Frame 63: 177 bytes on wire (1416 bits), 177 bytes captured (1416 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Nov 23, 2022 12:38:34.620304000 Greenwich Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1669207114.620304000 seconds
    [Time delta from previous captured frame: 0.000002000 seconds]
    [Time delta from previous displayed frame: 0.000002000 seconds]
    [Time since reference or first frame: 18.032379000 seconds]
    Frame Number: 63
    Frame Length: 177 bytes (1416 bits)
    Capture Length: 177 bytes (1416 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:udp:dns]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
> 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)
```

```
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 95 2b 00 8f  9a 89 ae 2b 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 23 00 04 8e fa 01   ········ ··#·····
0060  8b c0 0c 00 01 00 01 00  00 01 23 00 04 8e fa 01   ········ ··#·····
0070  8a c0 0c 00 01 00 01 00  00 01 23 00 04 8e fa 01   ········ ··#·····
0080  66 c0 0c 00 01 00 01 00  00 01 23 00 04 8e fa 01   f······· ··#·····
0090  71 c0 0c 00 01 00 01 00  00 01 23 00 04 8e fa 01   q······· ··#·····
00a0  64 c0 0c 00 01 00 01 00  00 01 23 00 04 8e fa 01   d······· ··#·····
00b0  65                                                 e
```

Packets: 200 · Displayed: 22 (11.0%)

Figure 6 Using filters to explore DNS packets


sample.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Packet 9 · sample.pcap
Close
Help
sample.pcap

```
udp.port == 53

No.  Time
  9 8.637619
 10 8.637625
 11 8.641838
 12 8.641978
 19 8.644093
 20 8.647339
 27 9.645214
 28 9.645859
 33 10.646715
 34 10.647413
 60 18.031311
 61 18.031318
 62 18.032377
 63 18.032379
141 42.362339
142 42.362347

> Frame 9: 81 bytes
> Ethernet II, Src:
> Internet Protocol
> User Datagram Prot
> Domain Name System
```

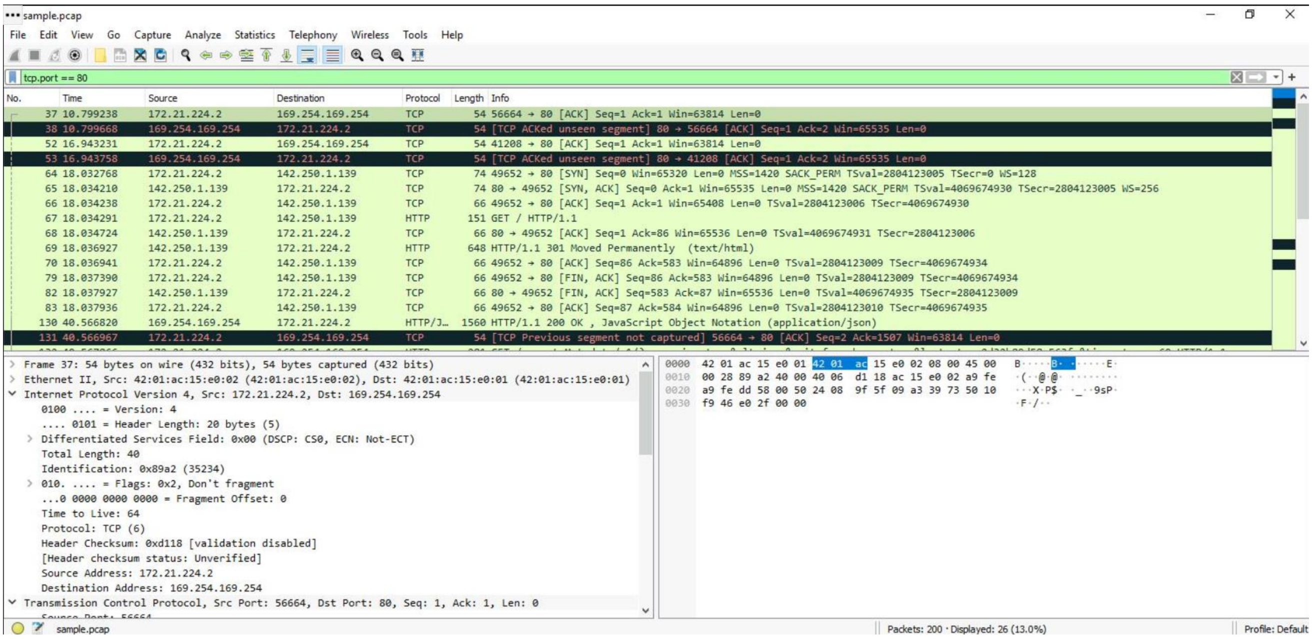
```
> Internet Protocol Version 4, Src: 172.21.224.2, Dst: 169.254.169.254
> User Datagram Protocol, Src Port: 59398, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x0c26
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v 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                                                 ·
```

☑ Show packet bytes

AAAA 2607:f…
1.113 A 142.…

Packets: 200 · Displayed: 22 (11.0%) Profile: Default

Figure 7 DNS queries


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

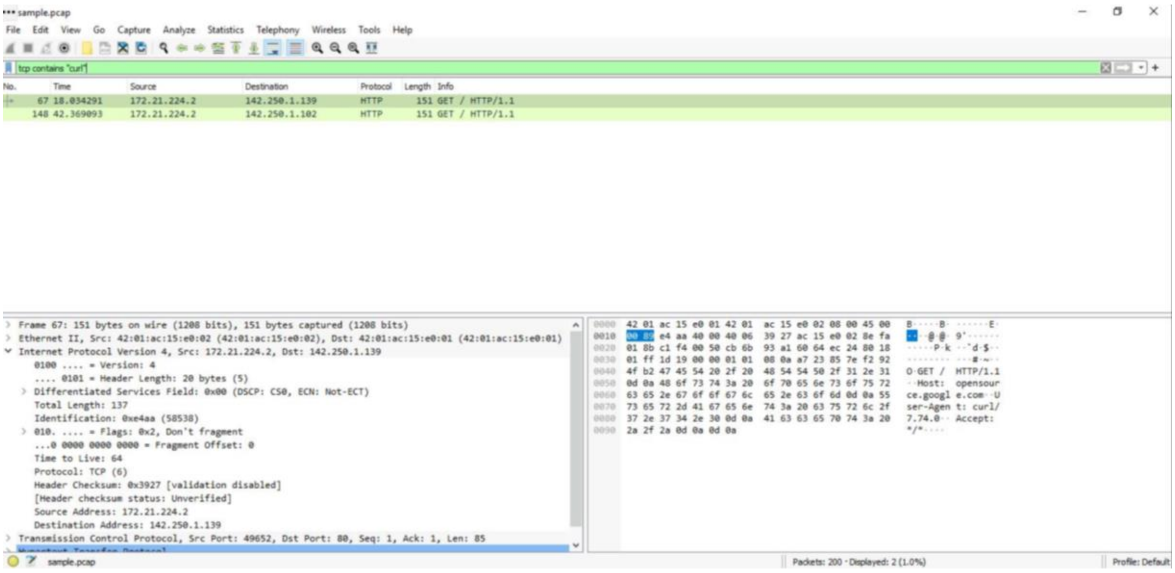
```
tcp.port == 80

No.  Time       Source           Destination      Protocol Length 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
130 40.566820  169.254.169.254  172.21.224.2     HTTP/J…  1560 HTTP/1.1 200 OK , JavaScript Object Notation (application/json)
131 40.566967  172.21.224.2     169.254.169.254  TCP        54 [TCP Previous segment not captured] 56664 → 80 [ACK] Seq=2 Ack=1507 Win=63814 Len=0
```

```
> 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)
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: 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
    Destination Address: 169.254.169.254
v 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·/··
```

Packets: 200 · Displayed: 26 (13.0%) Profile: Default

Figure 8 TCP filtering


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

```
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
> Transmission Control Protocol, Src Port: 49652, Dst Port: 80, Seq: 1, Ack: 1, Len: 85
> Hypertext Transfer Protocol
```

```
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: 2 (1.0%)          Profile: Default
```

Figure 9 TCP filtering with keyword "curl"