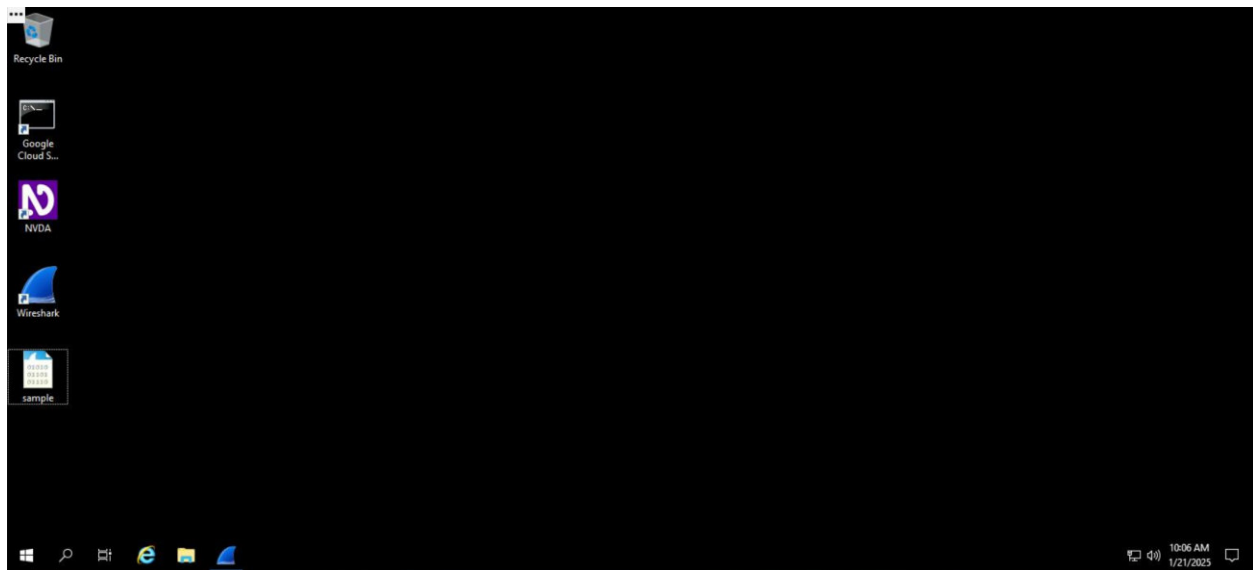


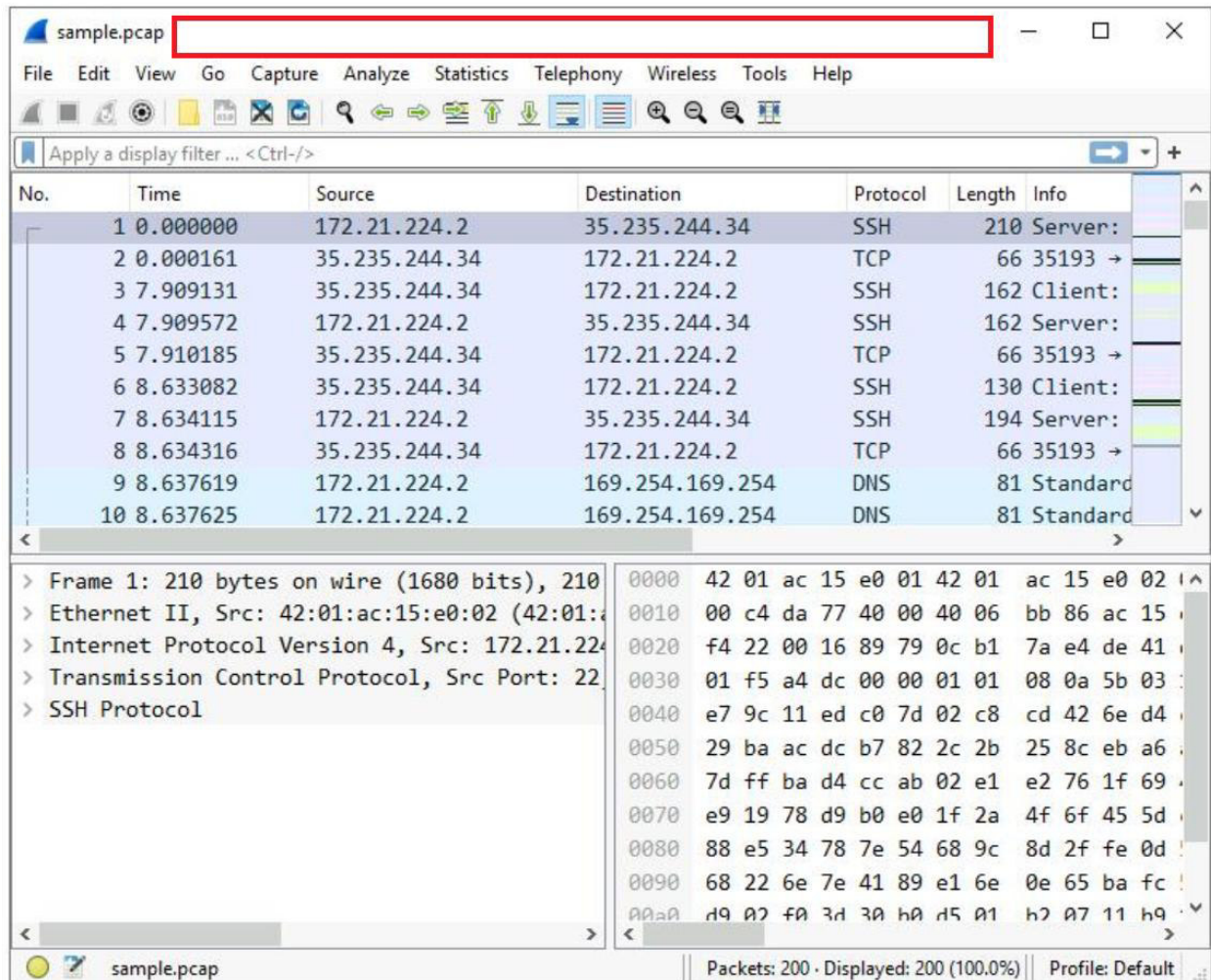
Task 1. Explore data with Wireshark

In this task, you must open a network packet capture file that contains data captured from a system that made web requests to a site. You need to open this data with Wireshark to get an overview of how the data is presented in the application.

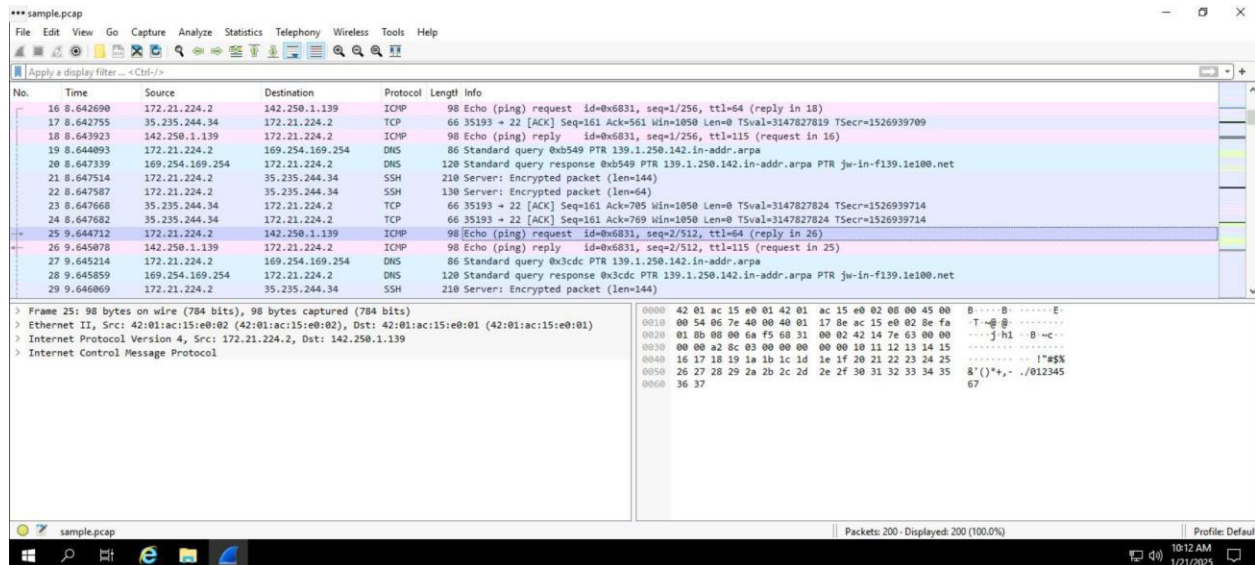
1. To open the packet capture file, double-click the **sample** file on the Windows desktop. This will start Wireshark.



2. Double-click the Wireshark title bar next to the **sample.pcap** filename to maximize the Wireshark application window.



3. Scroll down the packet list until a packet is listed where the info column starts with the words 'Echo (ping) request'.



Task 2. Apply a basic Wireshark filter and inspect a packet

In this task, you'll open a packet in Wireshark for more detailed exploration and filter the data to inspect the network layers and protocols contained in the packet.

1. Enter the following filter for traffic associated with a specific IP address. Enter this into the **Apply a display filter...** text box immediately above the list of packets:

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

Copied!

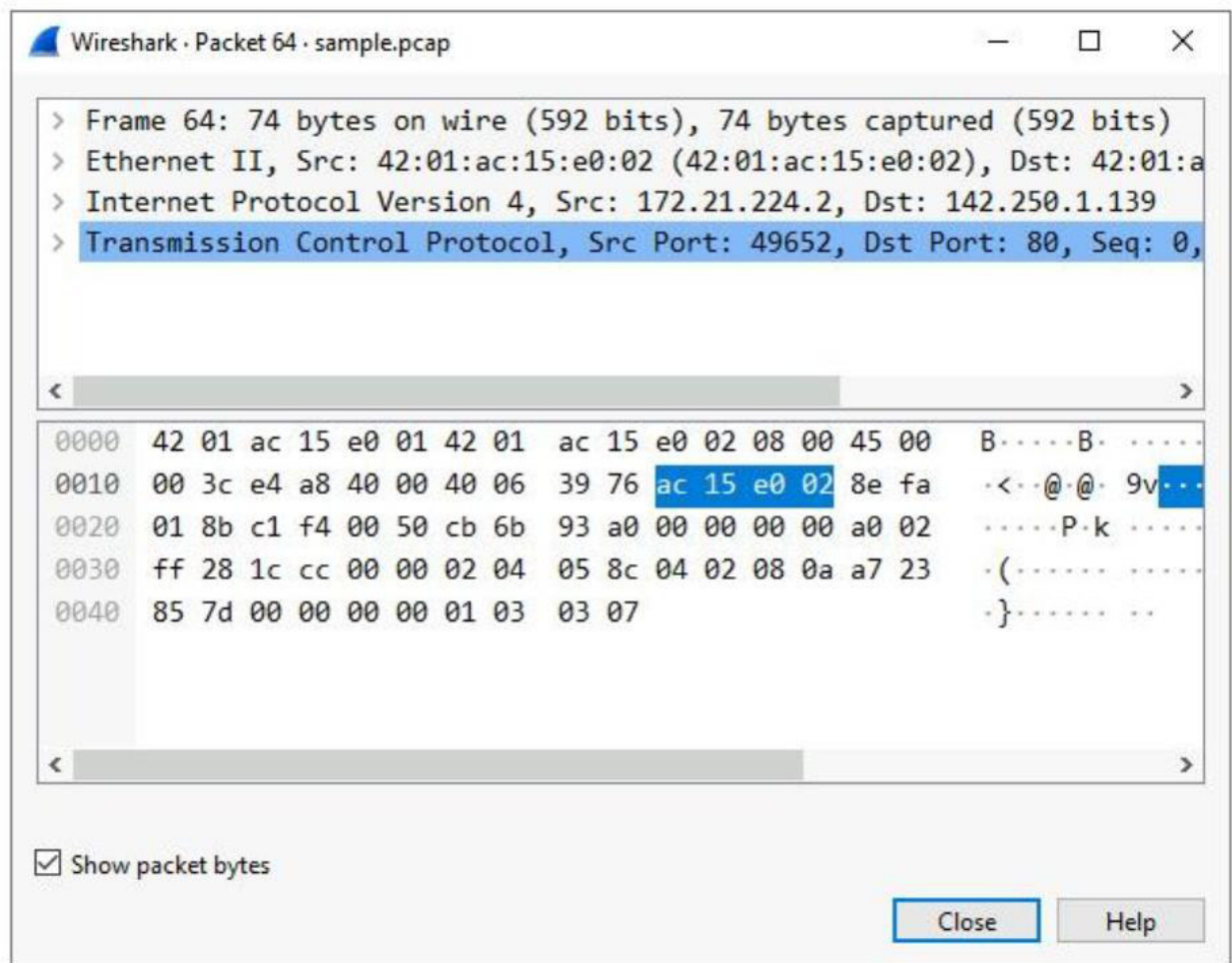
content_copy

2. Press **ENTER** or click the **Apply display filter** icon in the filter text box.

The list of packets displayed is now significantly reduced and contains only packets where either the source or the destination IP address matches the address you entered. Now only two packet colors are used: **light pink** for ICMP protocol packets and **light green** for TCP (and HTTP, which is a subset of TCP) packets.

3. Double-click the first packet that lists **TCP** as the protocol.

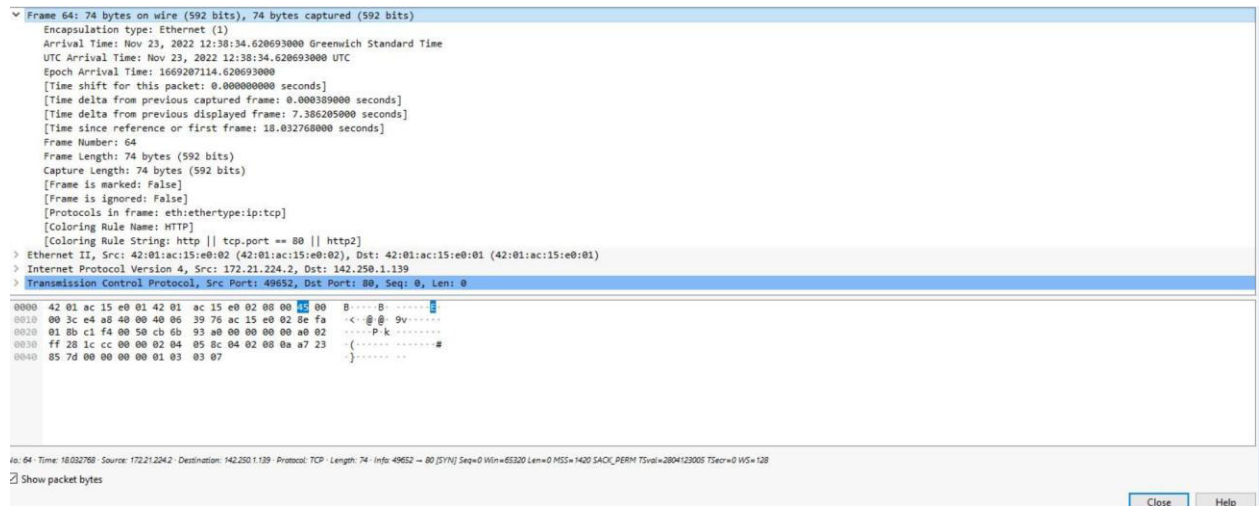
This opens a packet details pane window:



The upper section of this window contains subtrees where Wireshark will provide you with 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 (".").

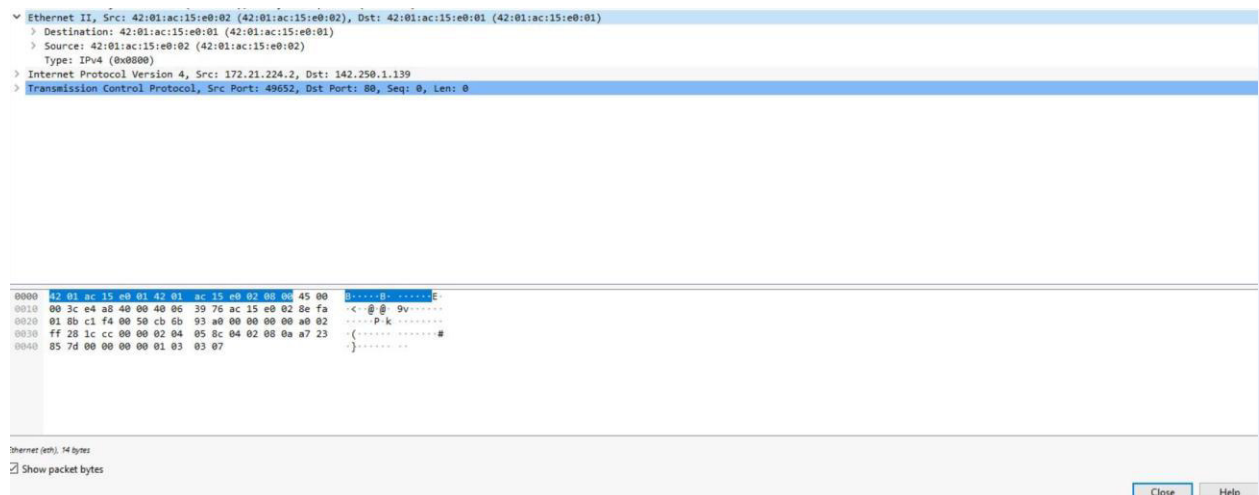
Note: The details pane is located at the bottom portion of the main Wireshark window. It can also be accessed in a new window by double clicking a packet.

4. Double-click the first subtree in the upper section. This starts with the word **Frame**.



This provides you with details about the overall network packet, or frame, including the frame length and the arrival time of the packet. At this level, you're viewing information about the entire packet of data.

5. Double-click **Frame** again to collapse the subtree and then double-click the **Ethernet II** subtree.



This item contains details about the packet at the Ethernet level, including the source and destination MAC addresses and the type of internal protocol that the Ethernet packet contains.

6. Double-click **Ethernet II** again to collapse that subtree and then double-click the **Internet Protocol Version 4** subtree.

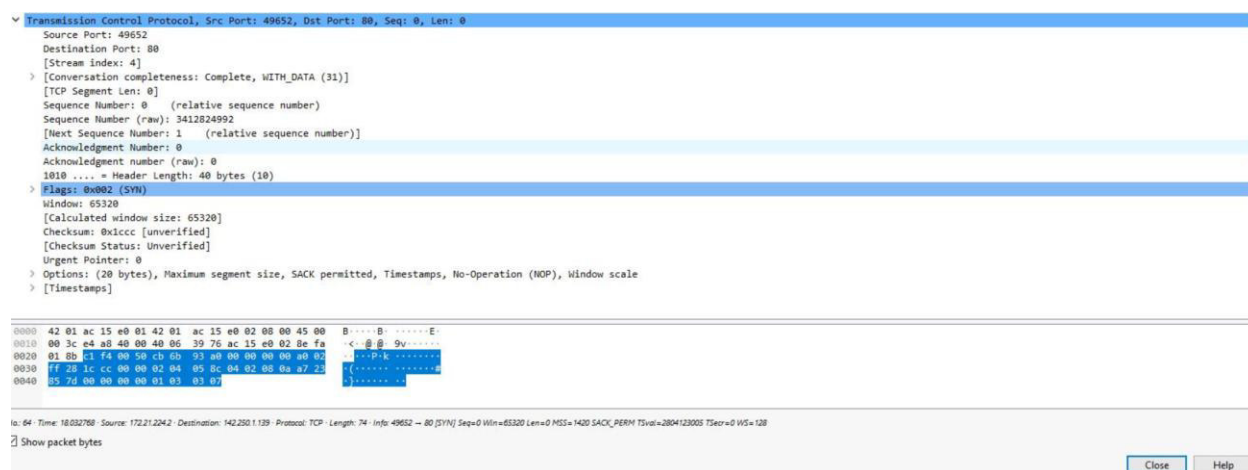


This provides packet data about the Internet Protocol (IP) data contained in the Ethernet packet. It contains information such as the source and destination IP addresses and the Internal Protocol (for example, TCP or UDP), which is carried inside the IP packet.

Note: The Internet Protocol Version 4 subtree is Internet Protocol Version 4 (IPv4). The third subtree label reflects the protocol.

The source and destination IP addresses shown here match the source and destination IP addresses in the summary display for this packet in the main Wireshark window.

7. Double-click **Internet Protocol Version 4** again to collapse that subtree and then double-click the **Transmission Control Protocol** subtree.



This provides detailed information about the TCP packet, including the source and destination TCP ports, the TCP sequence numbers, and the TCP flags.

The source port and destination port listed here match the source and destination ports in the info column of the summary display for this packet in the list of all of the packets in the main Wireshark window.

8. In the **Transmission Control Protocol** subtree, scroll down and double-click **Flags**.

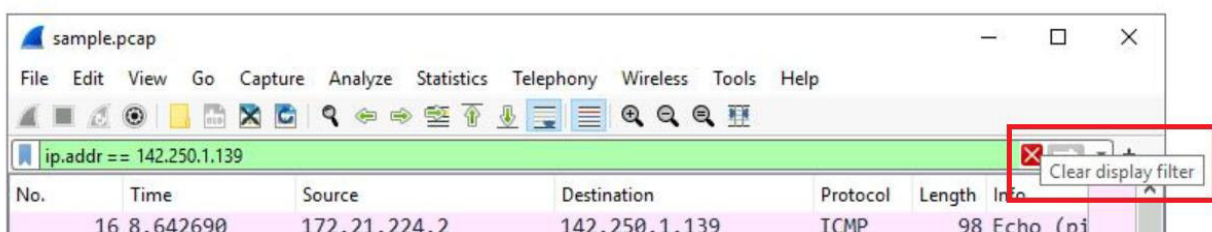
```

▼ Flags: 0x002 (SYN)
  000. .... = Reserved: Not set
  ...0 .... = Accurate ECN: Not set
  .... 0... = Congestion Window Reduced: 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: 65320
[Calculated window size: 65320]
Checksum: 0x1ccc [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
> Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP), Window scale
> [Timestamps]
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 .....).

```

This provides a detailed view of the TCP flags set in this packet.

9. Click the **X Clear display filter** icon in the Wireshark filter bar to clear the IP address filter.



All the packets have returned to the display.

If you ever accidentally close the Wireshark application, you can reopen it by double-clicking the **sample** file on the desktop.

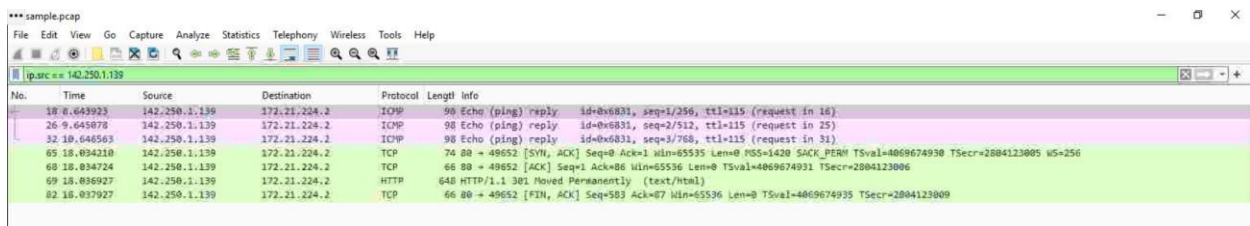
Task 3. Use filters to select packets

In this task, you'll use filters to analyze specific network packets based on where the packets came from or where they were sent to. You'll explore how to select packets using either their physical Ethernet Media Access Control (MAC) address or their Internet Protocol (IP) address.

1. Enter the following filter to select traffic for a specific source IP address only.

Enter this into the **Apply a display filter...** text box immediately above the list of packets:

```
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=1/356, ttl=115 (request in 16)
26	9.045878	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 W=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

2. Press **ENTER** or click the **Apply display filter** icon in the filter text box.

A filtered list is returned with fewer entries than before. It contains only packets that came from **142.250.1.139**.

3. Click the **X Clear display filter** icon in the Wireshark filter bar to clear the IP address filter.
4. Enter the following filter to select traffic for a specific destination IP address only:

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

- Press **ENTER** or click the **Apply display filter** icon in the filter text box.



The screenshot shows the Wireshark interface with the filter bar set to `ip.dst == 142.250.1.139`. The packet list contains several entries, with the following table representing the data shown:

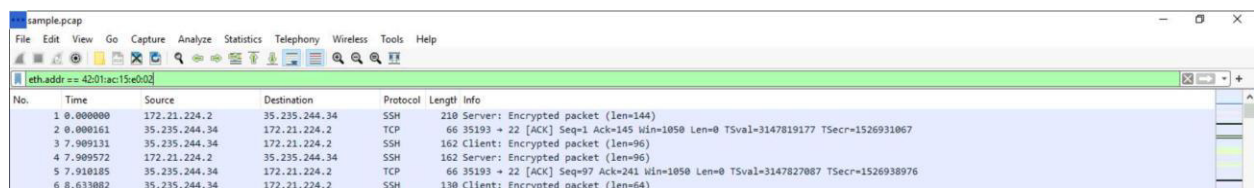
No.	Time	Source	Destination	Protocol	Length	Info
16	8.642690	172.21.224.2	142.250.1.139	ICMP	98	Echo (ping) request id=0x6831, seq=1/256, ttl=64 (reply in 18)
25	9.644712	172.21.224.2	142.250.1.139	ICMP	98	Echo (ping) request id=0x6831, seq=2/512, ttl=64 (reply in 26)
31	10.646049	172.21.224.2	142.250.1.139	ICMP	98	Echo (ping) request id=0x6831, seq=3/768, ttl=64 (reply in 32)
64	18.832768	172.21.224.2	142.250.1.139	TCP	74	49652 → 80 [SYN] Seq=0 Win=65536 Len=0 MSS=1420 SACK_PERM TSval=2804123005 TSecr=0 WS=128
66	18.834238	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	18.834291	172.21.224.2	142.250.1.139	HTTP	151	GET / HTTP/1.1
70	18.836941	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	18.837390	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	18.837936	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

A filtered list is returned that contains only packets that were sent to **142.250.1.139**.

- Click the **X Clear display filter** icon in the Wireshark filter bar to clear the IP address filter.
- Enter the following filter to select traffic to or from a specific Ethernet MAC address. This filters traffic related to one MAC address, regardless of the other protocols involved:

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

- Press **ENTER** or click the **Apply display filter** icon in the filter text box.

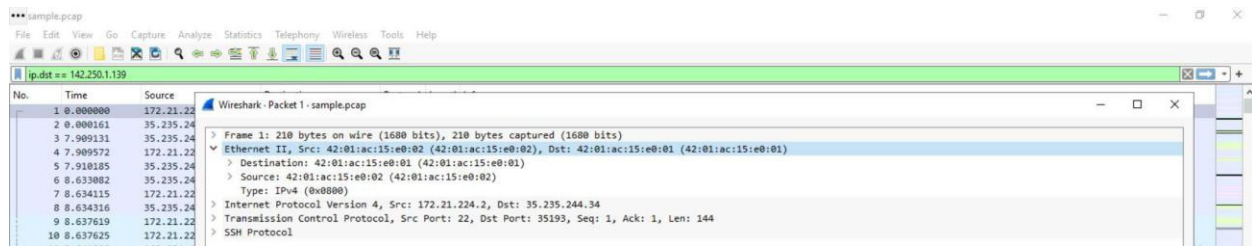


The screenshot shows the Wireshark interface with the filter bar set to `eth.addr == 42:01:ac:15:e0:02`. The packet list contains several entries, with the following table representing the data shown:

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)

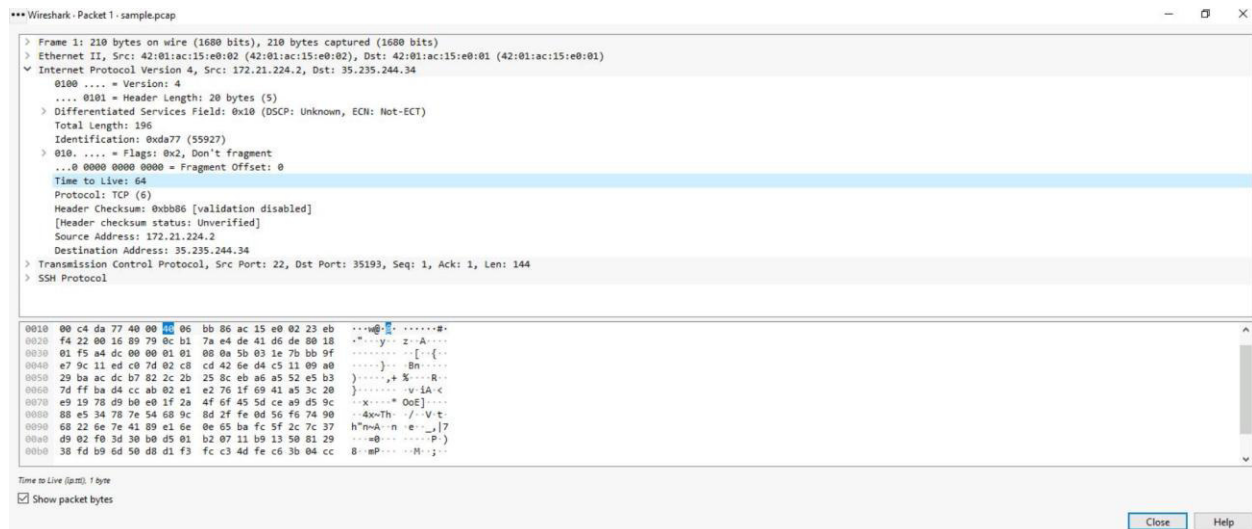
- Double-click the first packet in the list. You may need to scroll back to display the first packet in the filtered list.
- Double-click the **Ethernet II** subtree if it is not already open.

The MAC address you specified in the filter is listed as either the source or destination address in the expanded Ethernet II subtree.



11. Double-click the **Ethernet II** subtree to close it.

12. Double-click the **Internet Protocol Version 4** subtree to expand it and scroll down until the **Time to Live** and **Protocol** fields appear.



The **Protocol** field in the **Internet Protocol Version 4** subtree indicates which IP internal protocol is contained in the packet.

Task 4. Use filters to explore DNS packets

In this task, you'll use filters to select and examine DNS traffic. Once you've selected sample DNS traffic, you'll drill down into the protocol to examine how the DNS packet data contains both queries (names of internet sites that are being looked up) and answers (IP addresses that are being sent back by a DNS server when a name is successfully resolved).

1. Enter the following filter to select UDP port 53 traffic. DNS traffic uses UDP port 53, so this will list traffic related to DNS queries and responses only. Enter this into the **Apply a display filter...** text box immediately above the list of packets:

```
udp.port == 53
```

2. Press **ENTER** or click the **Apply display filter** icon in the filter text box.

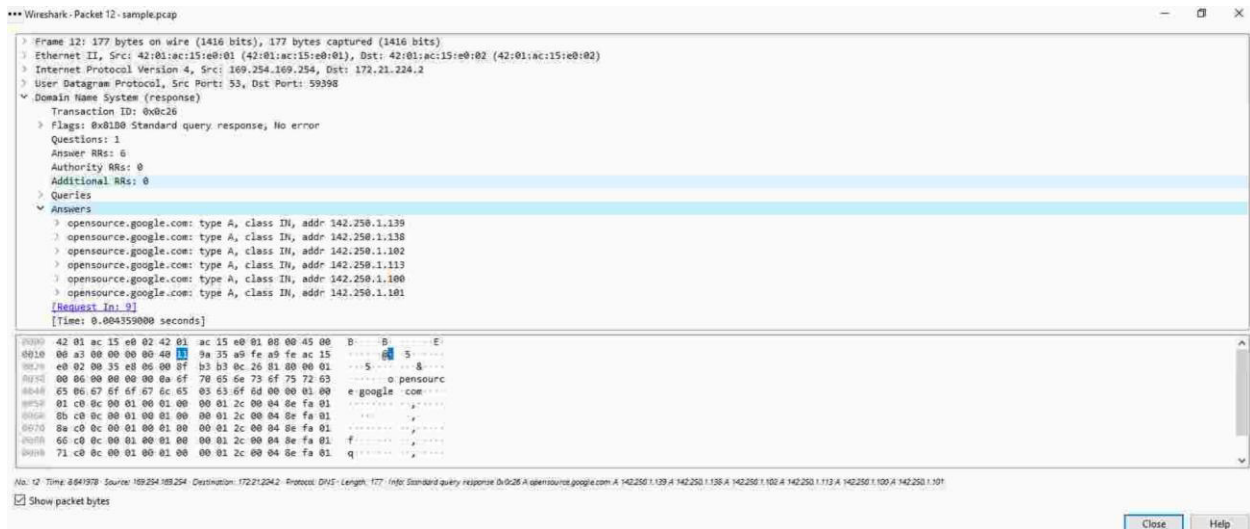
The screenshot displays the Wireshark interface with a packet capture named 'sample.pcap'. The filter bar at the top is set to 'udp.port == 53'. The packet list pane shows five packets:

No.	Time	Source	Destination	Protocol	Length	Info
8	0.637619	172.21.224.2	169.254.169.254	DNS	81	Standard query 0xc26 A opendns.google.com
9	0.637625	172.21.224.2	169.254.169.254	DNS	81	Standard query 0xd638 AAAA opendns.google.com
10	0.641838	169.254.169.254	172.21.224.2	DNS	193	Standard query response 0xd638 AAAA opendns.google.com AAAA 2607:f8b0:4001:c24::8a AAAA 2607:f8b0:4001:c24::64 AAAA 2607:f8b0:4001:c24::10
11	0.641978	169.254.169.254	172.21.224.2	DNS	177	Standard query response 0xc26 A opendns.google.com A 142.250.1.139 A 142.250.1.138 A 142.250.1.102 A 142.250.1.113 A 142.250.1.114 A 142.250.1.115 A 142.250.1.116 A 142.250.1.117 A 142.250.1.118 A 142.250.1.119 A 142.250.1.120 A 142.250.1.121 A 142.250.1.122 A 142.250.1.123 A 142.250.1.124 A 142.250.1.125 A 142.250.1.126 A 142.250.1.127 A 142.250.1.128 A 142.250.1.129 A 142.250.1.130 A 142.250.1.131 A 142.250.1.132 A 142.250.1.133 A 142.250.1.134 A 142.250.1.135 A 142.250.1.136 A 142.250.1.137 A 142.250.1.138 A 142.250.1.139 A 142.250.1.140 A 142.250.1.141 A 142.250.1.142 A 142.250.1.143 A 142.250.1.144 A 142.250.1.145 A 142.250.1.146 A 142.250.1.147 A 142.250.1.148 A 142.250.1.149 A 142.250.1.150 A 142.250.1.151 A 142.250.1.152 A 142.250.1.153 A 142.250.1.154 A 142.250.1.155 A 142.250.1.156 A 142.250.1.157 A 142.250.1.158 A 142.250.1.159 A 142.250.1.160 A 142.250.1.161 A 142.250.1.162 A 142.250.1.163 A 142.250.1.164 A 142.250.1.165 A 142.250.1.166 A 142.250.1.167 A 142.250.1.168 A 142.250.1.169 A 142.250.1.170 A 142.250.1.171 A 142.250.1.172 A 142.250.1.173 A 142.250.1.174 A 142.250.1.175 A 142.250.1.176 A 142.250.1.177 A 142.250.1.178 A 142.250.1.179 A 142.250.1.180 A 142.250.1.181 A 142.250.1.182 A 142.250.1.183 A 142.250.1.184 A 142.250.1.185 A 142.250.1.186 A 142.250.1.187 A 142.250.1.188 A 142.250.1.189 A 142.250.1.190 A 142.250.1.191 A 142.250.1.192 A 142.250.1.193 A 142.250.1.194 A 142.250.1.195 A 142.250.1.196 A 142.250.1.197 A 142.250.1.198 A 142.250.1.199 A 142.250.1.200 A 142.250.1.201 A 142.250.1.202 A 142.250.1.203 A 142.250.1.204 A 142.250.1.205 A 142.250.1.206 A 142.250.1.207 A 142.250.1.208 A 142.250.1.209 A 142.250.1.210 A 142.250.1.211 A 142.250.1.212 A 142.250.1.213 A 142.250.1.214 A 142.250.1.215 A 142.250.1.216 A 142.250.1.217 A 142.250.1.218 A 142.250.1.219 A 142.250.1.220 A 142.250.1.221 A 142.250.1.222 A 142.250.1.223 A 142.250.1.224 A 142.250.1.225 A 142.250.1.226 A 142.250.1.227 A 142.250.1.228 A 142.250.1.229 A 142.250.1.230 A 142.250.1.231 A 142.250.1.232 A 142.250.1.233 A 142.250.1.234 A 142.250.1.235 A 142.250.1.236 A 142.250.1.237 A 142.250.1.238 A 142.250.1.239 A 142.250.1.240 A 142.250.1.241 A 142.250.1.242 A 142.250.1.243 A 142.250.1.244 A 142.250.1.245 A 142.250.1.246 A 142.250.1.247 A 142.250.1.248 A 142.250.1.249 A 142.250.1.250 A 142.250.1.251 A 142.250.1.252 A 142.250.1.253 A 142.250.1.254 A 142.250.1.255 A 142.250.1.256 A 142.250.1.257 A 142.250.1.258 A 142.250.1.259 A 142.250.1.260 A 142.250.1.261 A 142.250.1.262 A 142.250.1.263 A 142.250.1.264 A 142.250.1.265 A 142.250.1.266 A 142.250.1.267 A 142.250.1.268 A 142.250.1.269 A 142.250.1.270 A 142.250.1.271 A 142.250.1.272 A 142.250.1.273 A 142.250.1.274 A 142.250.1.275 A 142.250.1.276 A 142.250.1.277 A 142.250.1.278 A 142.250.1.279 A 142.250.1.280 A 142.250.1.281 A 142.250.1.282 A 142.250.1.283 A 142.250.1.284 A 142.250.1.285 A 142.250.1.286 A 142.250.1.287 A 142.250.1.288 A 142.250.1.289 A 142.250.1.290 A 142.250.1.291 A 142.250.1.292 A 142.250.1.293 A 142.250.1.294 A 142.250.1.295 A 142.250.1.296 A 142.250.1.297 A 142.250.1.298 A 142.250.1.299 A 142.250.1.300 A 142.250.1.301 A 142.250.1.302 A 142.250.1.303 A 142.250.1.304 A 142.250.1.305 A 142.250.1.306 A 142.250.1.307 A 142.250.1.308 A 142.250.1.309 A 142.250.1.310 A 142.250.1.311 A 142.250.1.312 A 142.250.1.313 A 142.250.1.314 A 142.250.1.315 A 142.250.1.316 A 142.250.1.317 A 142.250.1.318 A 142.250.1.319 A 142.250.1.320 A 142.250.1.321 A 142.250.1.322 A 142.250.1.323 A 142.250.1.324 A 142.250.1.325 A 142.250.1.326 A 142.250.1.327 A 142.250.1.328 A 142.250.1.329 A 142.250.1.330 A 142.250.1.331 A 142.250.1.332 A 142.250.1.333 A 142.250.1.334 A 142.250.1.335 A 142.250.1.336 A 142.250.1.337 A 142.250.1.338 A

3. Double-click the first packet in the list to open the detailed packet window.
4. Scroll down and double-click the **Domain Name System (query)** subtree to expand it.
5. Scroll down and double-click **Queries**.

You'll notice that the name of the website that was queried is **opensource.google.com**.

- Click the **X** icon to close the detailed packet inspection window.
- Double-click the fourth packet in the list to open the detailed packet window.
- Scroll down and double-click the **Domain Name System (query)** subtree to expand it.
- Scroll down and double-click **Answers**, which is in the **Domain Name System (query)** subtree.



The Answers data includes the name that was queried (**opensource.google.com**) and the addresses that are associated with that name.

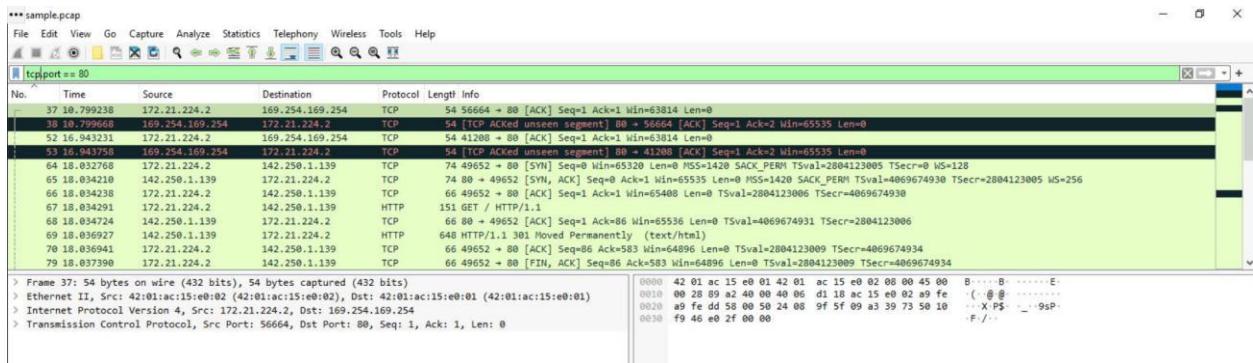
Task 5. Use filters to explore TCP packets

In this task, you'll use additional filters to select and examine TCP packets. You'll learn how to search for text that is present in payload data contained inside network packets. This will locate packets based on something such as a name or some other text that is of interest to you.

1. Enter the following filter to select TCP port **80** traffic. TCP port **80** is the default port that is associated with web traffic:

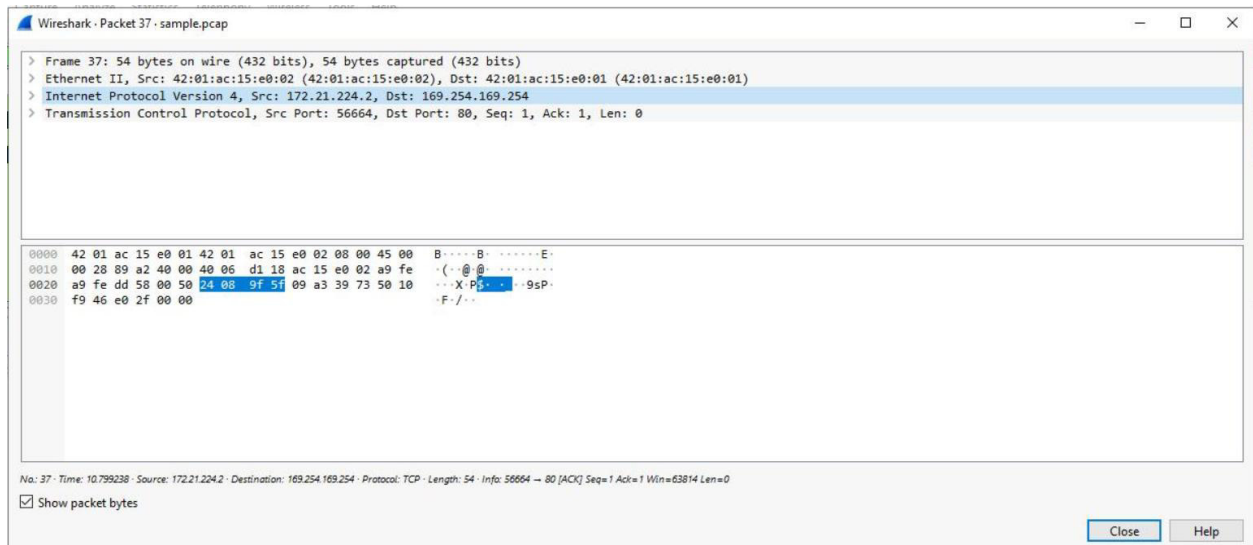
`tcp.port == 80`

2. Press **ENTER** or click the **Apply display filter** icon in the filter text box.



Quite a few packets were created when the user accessed the web page <http://opensource.google.com>.

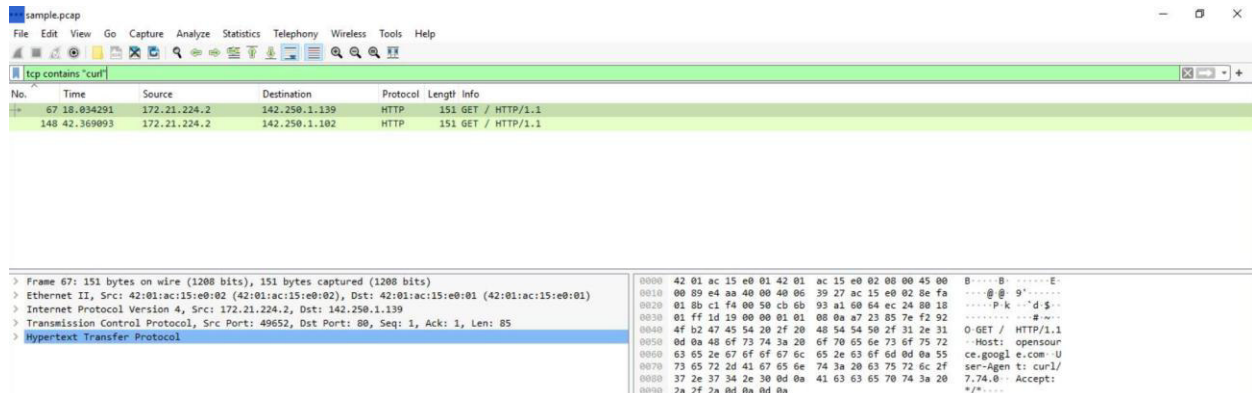
3. Double-click the first packet in the list. The **Destination IP** address of this packet is **169.254.169.254**.



4. Enter the following filter to select TCP packet data that contains specific text data.

`tcp contains "curl"`

5. Press **ENTER** or click the **Apply display filter** icon in the filter text box.



Conclusion

I now have practical experience using Wireshark to

- open saved packet capture files,
- view high-level packet data, and
- use filters to inspect detailed packet data.

This is an important milestone on my journey toward understanding how to use network packet analysis tools to examine network traffic!