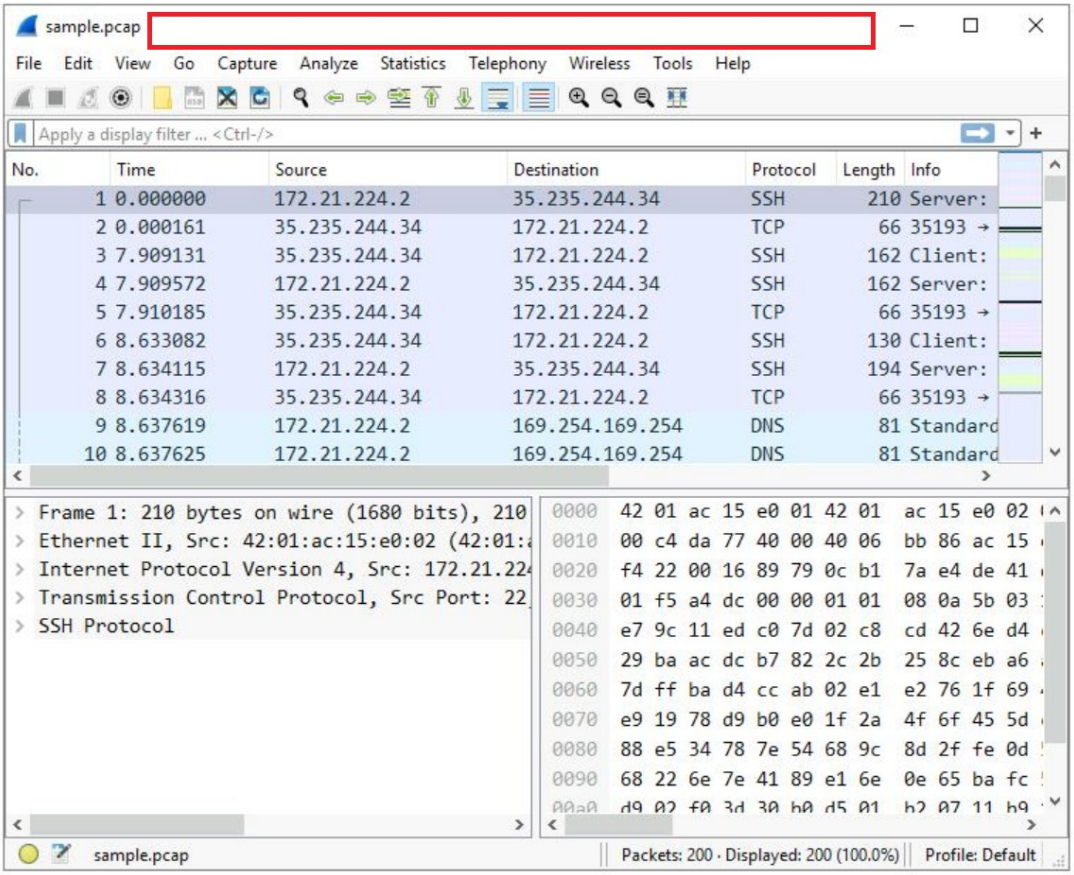
Explore data with Wireshark

1.Open the packet capture file by double-clicking the file called **sample** on the Windows desktop. Wireshark starts.

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



A lot of network packet traffic is listed, which is why you'll apply filters to find the information needed in an upcoming step.

For now, here is an overview of the key property columns listed for each packet:

- **No.** : The index number of the packet in this packet capture file
- **Time**: The timestamp of the packet
- **Source**: The source IP address
- **Destination**: The destination IP address

•**Protocol**: The protocol contained in the packet

•**Length**: The total length of the packet

•**Info**: Some infomation about the data in the packet (the payload) as interpreted by Wireshark

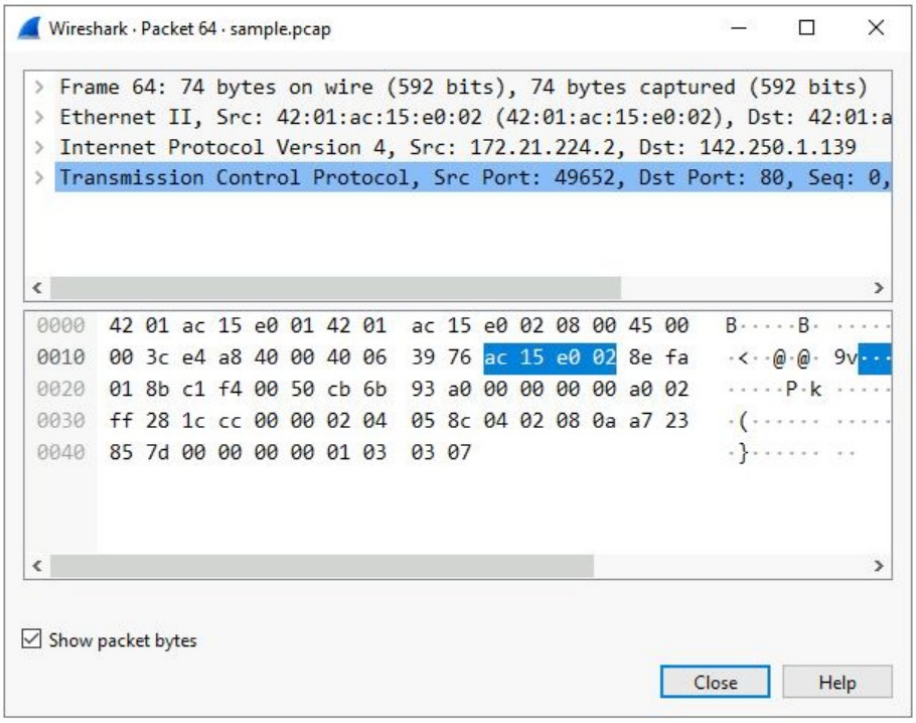
Apply a basic Wireshark filter and inspect a packet

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

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

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

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



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.

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

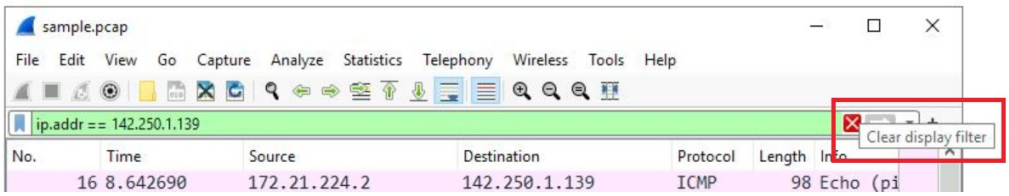
This provides detailed information about the TCP packet, including the source and destination TCP ports, the TCP sequence numbers, and the TCP flags.

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

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

9.Click the **X** icon to close the detailed packet inspection window.

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



Use filters to select packets

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
```

2. Enter the following filter to select traffic for a specific destination IP address only:

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

3.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
```

Use filters to explore DNS packets

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.

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

2.Scroll down and double-click the **Domain Name System (query)** subtree to expand it.

3.Scroll down and double-click **Queries**.

4.Click the **X** icon to close the detailed packet inspection window.

5.Double-click the fourth packet in the list to open the detailed packet window.

6.Scroll down and double-click the **Domain Name System (query)** subtree to expand it.

7.Scroll down and double-click **Answers**, which is in the **Domain Name System (query)** subtree.

Use filters to explore TCP packets

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
```

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

```
tcp contains "curl"
```

This filters to packets containing web requests made with the `curl` command in this sample packet capture file.