Exemplar: Analyze your first packet with Wireshark

Activity overview

As a security analyst, you'll need to analyze network traffic in order to learn what type of traffic is being sent to and from systems on the networks you'll be working with.

Previously, you learned about packet capture and analysis. Analyzing packets can help security teams interpret and understand network communications. Network protocol analyzers such as Wireshark, which has a graphical user interface or GUI, can help you examine packet data during your investigations. Since network packet data is complex, network protocol analyzers (packet sniffers) like Wireshark are designed to help you find patterns and filter the data in order to focus on the network traffic that is most relevant to your security investigations.

Now you'll use Wireshark to inspect packet data and apply filters to sort through packet information efficiently.

In this lab activity, you'll use Wireshark to examine a sample packet capture file and filter the network traffic data.

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.

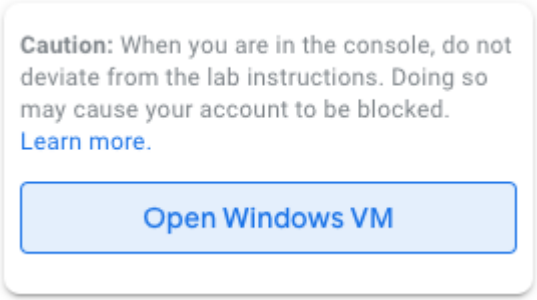
You're ready to use Wireshark to inspect network packet data!

Disclaimer: For optimal performance and compatibility, it is recommended to use either **Google Chrome** or **Mozilla Firefox** browsers while accessing the labs.

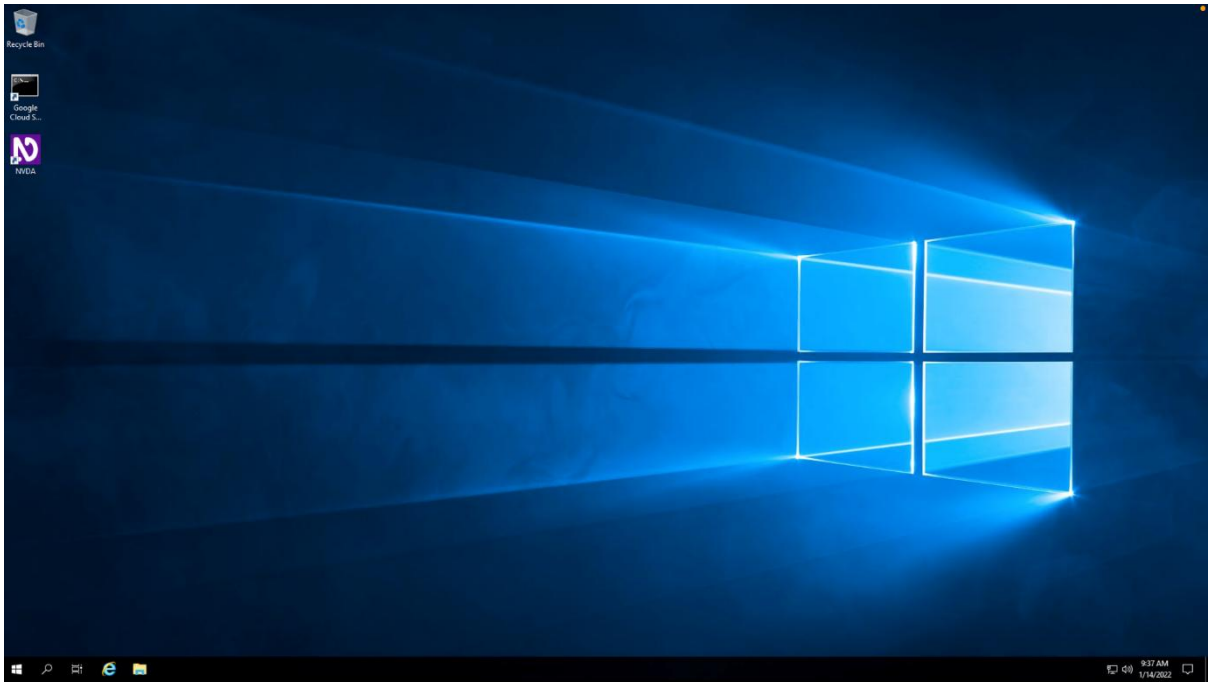
Start the lab

You'll need to start the lab before you can access the materials. To do this, click the green "Start Lab" button at the top of the screen.

After you click the "Start Lab" button, you will see a panel appear below where the start lab button was that has an **Open Windows VM** button.



Click the **Open Windows VM** button and a new tab will open with a visual interface for Windows OS, where you will be performing further steps in the lab. You should have a visual interface for Windows that looks like this:



Note: If the Windows VM becomes stuck and disconnects automatically, you can reconnect in the following ways:

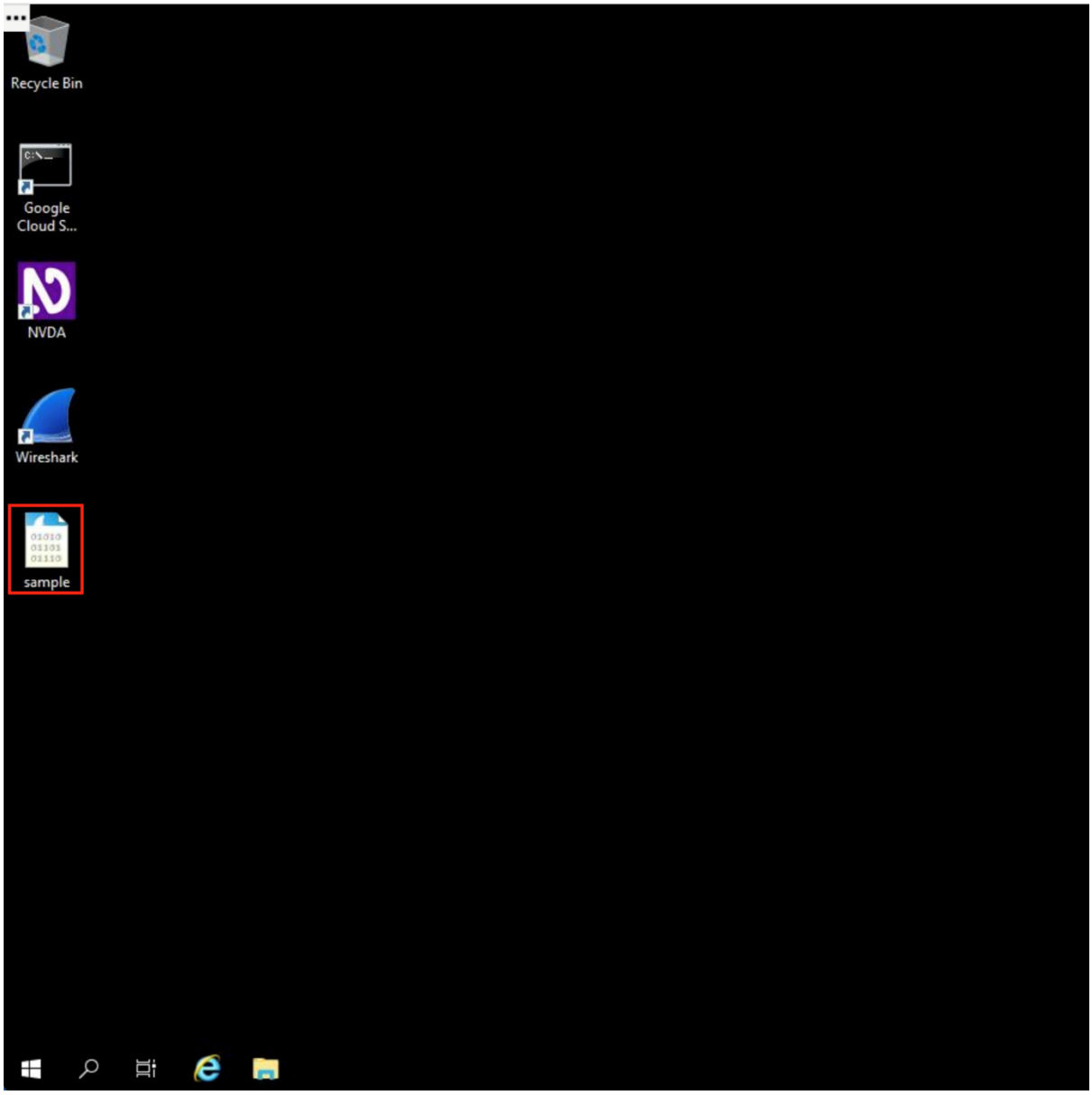
1. Return to the lab page, and click **Open Windows VM** again. This will reconnect you to the same Windows VM.
2. Use the following credentials on the login page and leave the other fields unchanged:

Server	localhost
Username	qwiklabs
Password	qwiklabs-bb-fa75b845-0b0a-49c6-b19b-510ee08190fe

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.

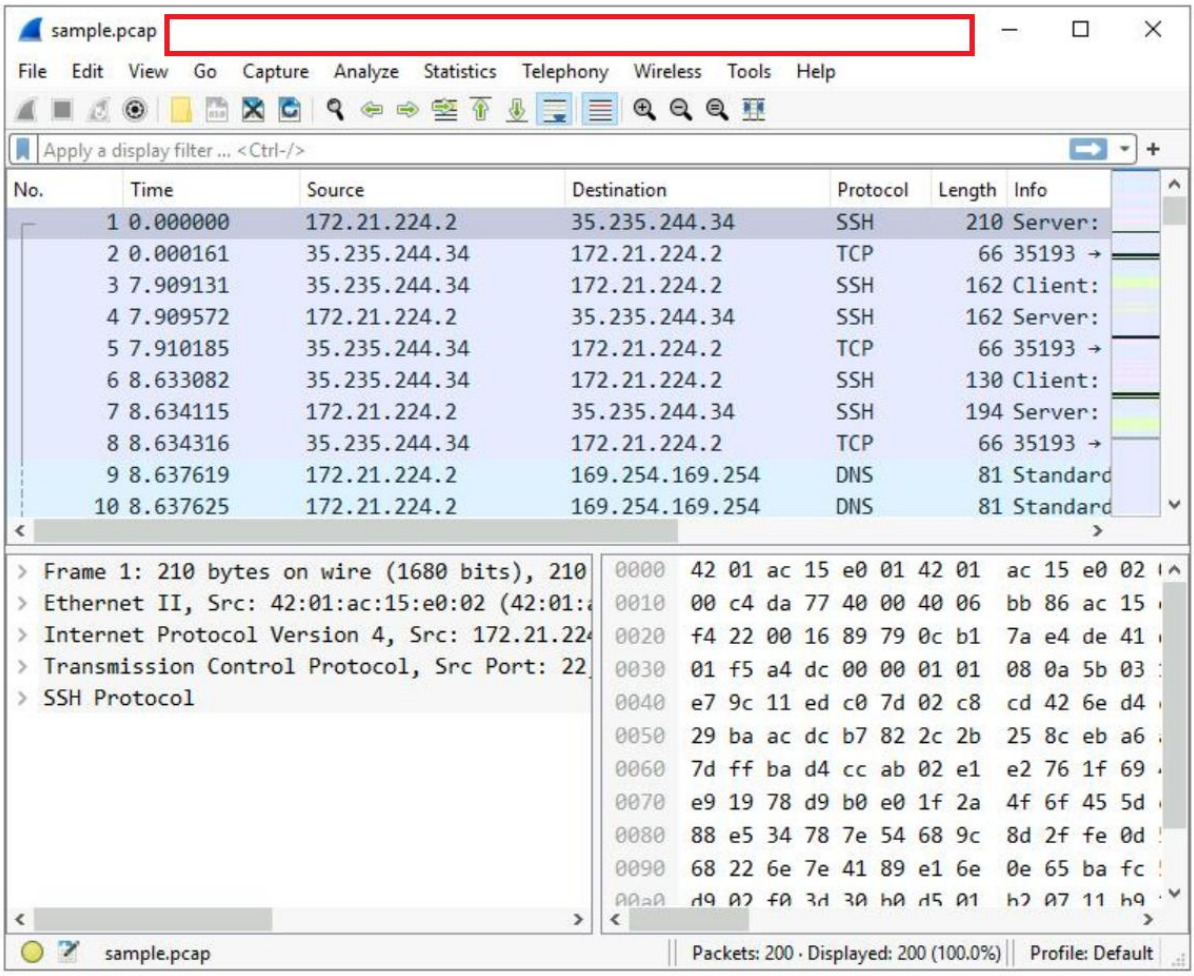


The packet capture file has the Wireshark packet capture file icon, which shows a shark's fin swimming above three rows of binary digits. The packet capture file has a **.pcap** file extension that is hidden by default by Windows Explorer and on the desktop view.

Note: *A* ***Software Update*** *dialog box may appear, notifying you that a new version of Wireshark is available. Click* ***Skip this version****.*

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

Not all the data packets are the same color. Coloring rules are used to provide high-level visual cues to help you quickly classify the different types of data. Since network packet

capture files can contain large amounts of data, you can use coloring rules to quickly identify the data that is relevant to you. The example packet lists a group of light blue packets that all contain DNS traffic, followed by green packets that contain a mixture of TCP and HTTP protocol traffic.

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

What is the protocol of the first packet in the list where the info column starts with the words 'Echo (ping) request'?

HTTP

SSH

ICMP

TCP

Submit

Answer: ICMP is the protocol type listed for the first (and all) packets that contain 'Echo (ping) request' in the info column.

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:

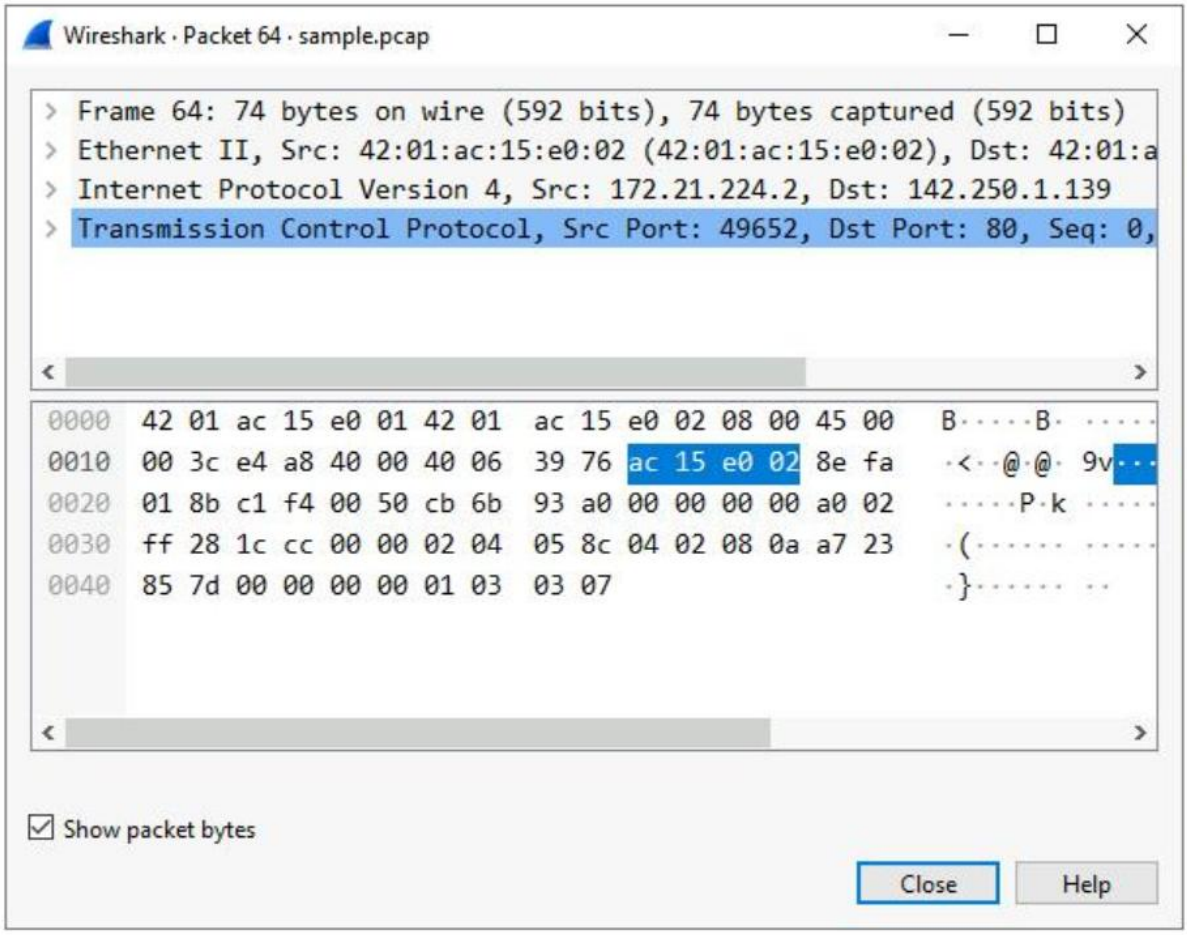
ip.addr == 142.250.1.139

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.

What is the TCP destination port of this TCP packet?

200

53

66

80

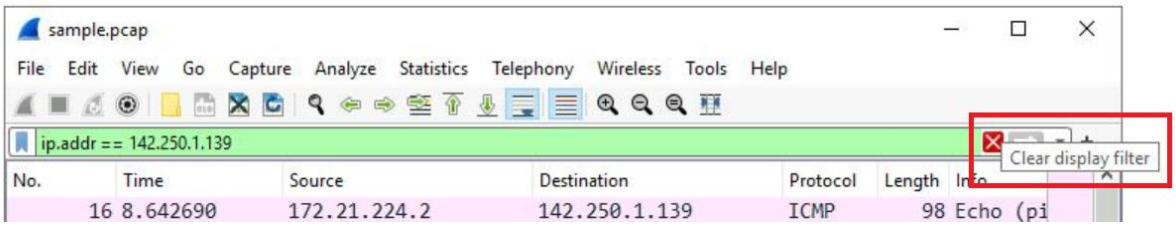
Submit

Answer: Port 80 is the TCP destination port for this packet. It contains the initial web request to an HTTP website that will typically be listening on TCP port 80.

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.



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

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

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

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

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

7. 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

8. Press **ENTER** or click the **Apply display filter** icon in the filter text box.
9. Double-click the first packet in the list. You may need to scroll back to display the first packet in the filtered list.
10. 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.

What is the protocol contained in the Internet Protocol Version 4 subtree from the first packet related to MAC address 42:01:ac:15:e0:02?

ESP

TCP

UDP

ICMP

Submit

Answer: TCP is the internal protocol contained in the first packet from MAC address 42:01:ac:15:e0:02.

13. Click the **X** icon to close the detailed packet inspection window.
14. Click the **X Clear display filter** icon in the Wireshark filter bar to clear the MAC address filter.

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.
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**.

6. Click the **X** icon to close the detailed packet inspection window.
7. Double-click the fourth packet in the list to open the detailed packet window.
8. Scroll down and double-click the **Domain Name System (query)** subtree to expand it.
9. 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.

Which of these IP addresses is displayed in the expanded Answers section for the DNS query for opensource.google.com?

142.250.1.139

139.1.250.142

172.21.224.1

169.254.169.254

Submit

Answer: The IP address 142.250.1.139 is displayed in the expanded Answers section for the DNS query for **opensource.google.com**.

10. Click the **X** icon to close the detailed packet inspection window.
11. Click the **X Clear display filter** icon in the Wireshark filter bar to clear the filter.

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**.

What is the Time to Live value of the packet as specified in the Internet Protocol Version 4 subtree?

32

128

64

16

Submit

Answer: The Time to Live value is 64. This property is contained in the Internet Protocol Version 4 subtree, which is the third subtree listed in the detailed packet inspection window.

What is the Frame Length of the packet as specified in the Frame subtree?

40 bytes

54 bytes

74 bytes

60 bytes

Submit

Answer: The Frame Length is 54 bytes. This property is contained in the Frame subtree, which is the first subtree listed in the detailed packet inspection window.

What is the Header Length of the packet as specified in the Internet Protocol Version 4 subtree?

74 bytes

20 bytes

60 bytes

54 bytes

Submit

Answer: The Header Length is 20 bytes. This property is defined in the Internet Protocol Version 4 subtree, which is the fourth subtree listed in the detailed packet inspection window.

What is the Destination Address as specified in the Internet Protocol Version 4 subtree?

239.1.250.142

172.21.224.2

142.250.1.139

169.254.169.254

Submit

Answer: The Destination Address is 169.254.169.254. This property is defined in the Internet Protocol Version 4 subtree, which is the third subtree listed in the detailed packet inspection window.

4. Click the **X** icon to close the detailed packet inspection window.
5. Click the **X Clear display filter** icon in the Wireshark filter bar to clear the filter.
6. Enter the following filter to select TCP packet data that contains specific text data.

tcp contains "curl"

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

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

Conclusion

Great work!

You 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 your journey toward understanding how to use network packet analysis tools to examine network traffic!

End your lab

Before you end the lab, make sure you're satisfied that you've completed all the tasks, and follow these steps:

1. Click **End Lab**. A pop-up box will appear. Click **Submit** to confirm that you're done. Ending the lab will remove your access to the Bash shell. You won't be able to access the work you've completed in it again.
2. Another pop-up box will ask you to rate the lab and provide feedback comments. You can complete this if you choose to.
3. Close the browser tab containing the lab to return to your course.
4. Refresh the browser tab for the course to mark the lab as complete.