**Wireshark - Analyze Your First Packet**

**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:

1. Identify the source and destination IP addresses involved in this web browsing session.
2. Examine the protocols that are used when the user makes the connection to the website.
3. Analyze the data packet to identify the type of information sent and received by the systems that connect to each other when the network data is captured.

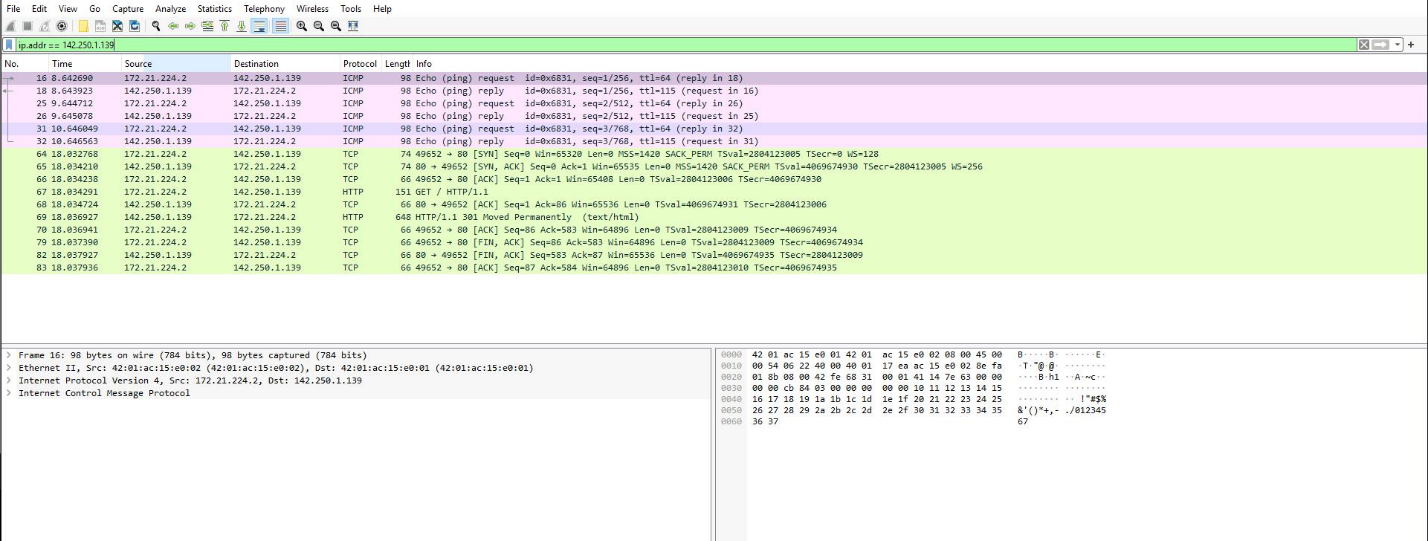
An overview of the key property columns listed for each packet:

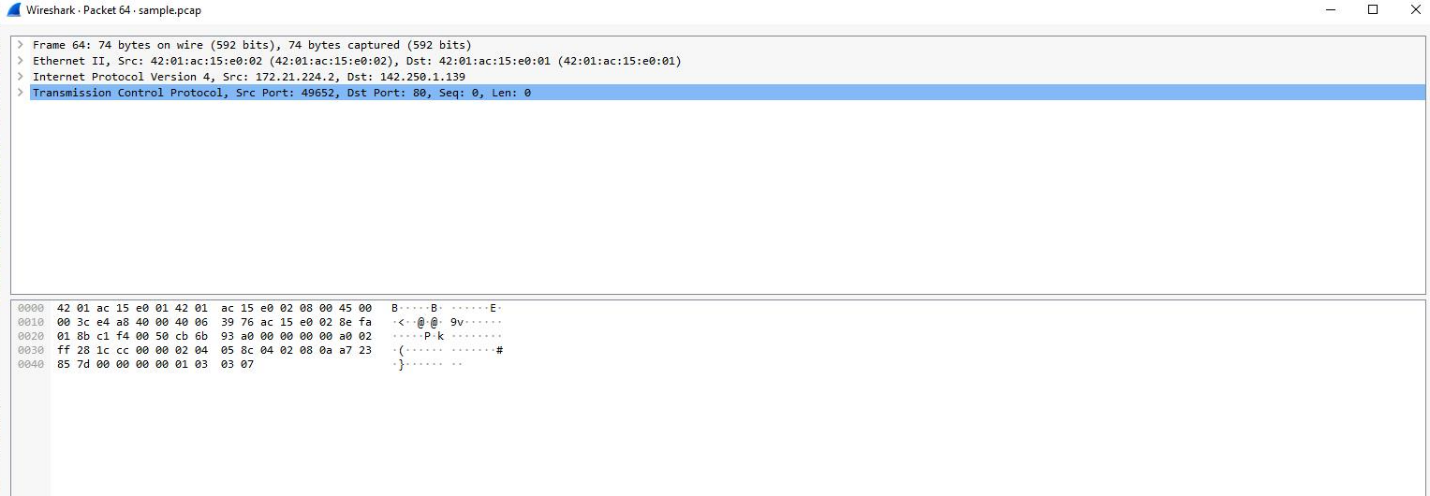
* No : The index number of the packet in this packet capture file.
* Time: The timestamp of the packet.
* Source: The source IP address.
* Destination: The destination IP address.
* Protocol: The protocol contained in the packet.
* Length: The total length of the packet.
* Info: Some infomation about the data in the packet (the payload) as interpreted by Wireshark.

**Solutions**

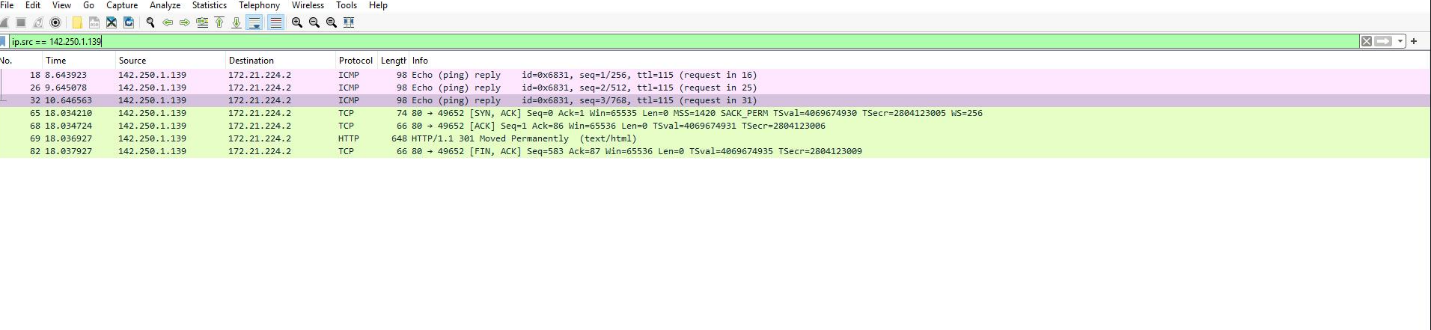
1. Identify the source and destination IP addresses involved in this web browsing session.

* On the title bar, type ip.addr == 142.250.1.139 to filter for traffic associated with a specific IP address. Select the first packet that contains TCP on the info field. addr means either the source or the destination IP.

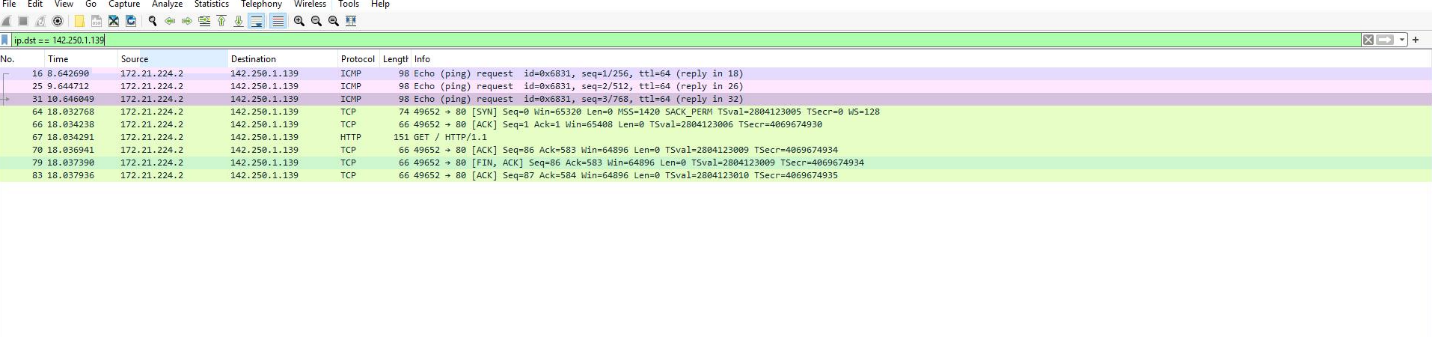
[](https://private-user-images.githubusercontent.com/135963482/302933804-0027d233-ae17-49a6-979c-1b8f3f003637.png?jwt=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJnaXRodWIuY29tIiwiYXVkIjoicmF3LmdpdGh1YnVzZXJjb250ZW50LmNvbSIsImtleSI6ImtleTUiLCJleHAiOjE3Njc2Nzc5NjYsIm5iZiI6MTc2NzY3NzY2NiwicGF0aCI6Ii8xMzU5NjM0ODIvMzAyOTMzODA0LTAwMjdkMjMzLWFlMTctNDlhNi05NzljLTFiOGYzZjAwMzYzNy5wbmc_WC1BbXotQWxnb3JpdGhtPUFXUzQtSE1BQy1TSEEyNTYmWC1BbXotQ3JlZGVudGlhbD1BS0lBVkNPRFlMU0E1M1BRSzRaQSUyRjIwMjYwMTA2JTJGdXMtZWFzdC0xJTJGczMlMkZhd3M0X3JlcXVlc3QmWC1BbXotRGF0ZT0yMDI2MDEwNlQwNTM0MjZaJlgtQW16LUV4cGlyZXM9MzAwJlgtQW16LVNpZ25hdHVyZT1mOTU1YjBmZjE2ZGNhMmVhYWM3OGQ5MTE2OGIxNzdiYTQ2MmRiZjkzMDNmMjJiYjkyYmUxYjZmZWFkZmI1ODBiJlgtQW16LVNpZ25lZEhlYWRlcnM9aG9zdCJ9.7JeReT1sKKFWPdIlBVFnz-z0JNWNpiTkShJpE1rdMBI)

[](https://private-user-images.githubusercontent.com/135963482/302933835-d2e2507c-ba58-4c4d-a6b5-43e511068100.png?jwt=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJnaXRodWIuY29tIiwiYXVkIjoicmF3LmdpdGh1YnVzZXJjb250ZW50LmNvbSIsImtleSI6ImtleTUiLCJleHAiOjE3Njc2Nzc5NjYsIm5iZiI6MTc2NzY3NzY2NiwicGF0aCI6Ii8xMzU5NjM0ODIvMzAyOTMzODM1LWQyZTI1MDdjLWJhNTgtNGM0ZC1hNmI1LTQzZTUxMTA2ODEwMC5wbmc_WC1BbXotQWxnb3JpdGhtPUFXUzQtSE1BQy1TSEEyNTYmWC1BbXotQ3JlZGVudGlhbD1BS0lBVkNPRFlMU0E1M1BRSzRaQSUyRjIwMjYwMTA2JTJGdXMtZWFzdC0xJTJGczMlMkZhd3M0X3JlcXVlc3QmWC1BbXotRGF0ZT0yMDI2MDEwNlQwNTM0MjZaJlgtQW16LUV4cGlyZXM9MzAwJlgtQW16LVNpZ25hdHVyZT00MjYyM2E2ZDE5ZTMzYjlhYmU3ZTk1ZDVjZmZlNDFkMTM0YmFkZDE2MmY2MzZiOWU2ZTM3NjY3NDdiYjFhNjA0JlgtQW16LVNpZ25lZEhlYWRlcnM9aG9zdCJ9.uhO2U97Ag-2_J1m7FgQBSpw25tjN_vzxKCcqNkU2bPM)

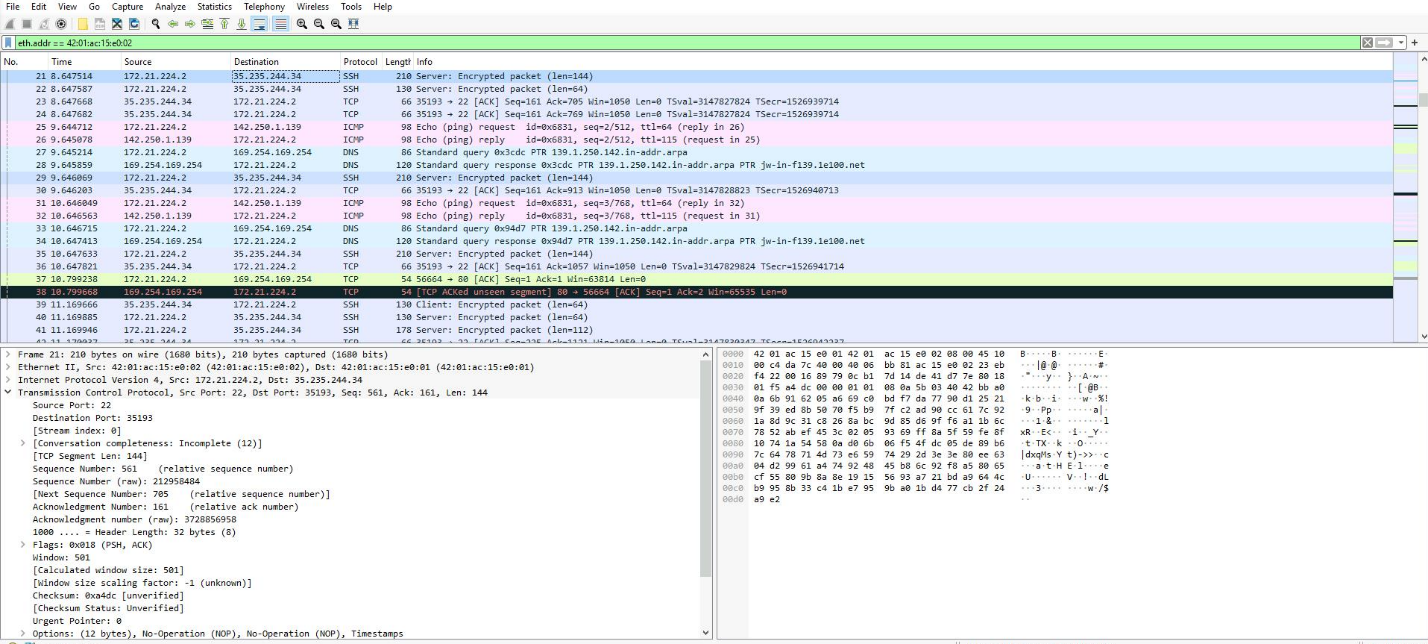
* On the title bar, type ip.src == 142.250.1.139 to filter for traffic associated with a specific IP address. src means it is where the packet comes from.

[](https://private-user-images.githubusercontent.com/135963482/302936581-48b3d84d-e5b1-4dc9-a6d8-363546b697bc.png?jwt=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJnaXRodWIuY29tIiwiYXVkIjoicmF3LmdpdGh1YnVzZXJjb250ZW50LmNvbSIsImtleSI6ImtleTUiLCJleHAiOjE3Njc2Nzc5NjYsIm5iZiI6MTc2NzY3NzY2NiwicGF0aCI6Ii8xMzU5NjM0ODIvMzAyOTM2NTgxLTQ4YjNkODRkLWU1YjEtNGRjOS1hNmQ4LTM2MzU0NmI2OTdiYy5wbmc_WC1BbXotQWxnb3JpdGhtPUFXUzQtSE1BQy1TSEEyNTYmWC1BbXotQ3JlZGVudGlhbD1BS0lBVkNPRFlMU0E1M1BRSzRaQSUyRjIwMjYwMTA2JTJGdXMtZWFzdC0xJTJGczMlMkZhd3M0X3JlcXVlc3QmWC1BbXotRGF0ZT0yMDI2MDEwNlQwNTM0MjZaJlgtQW16LUV4cGlyZXM9MzAwJlgtQW16LVNpZ25hdHVyZT1iM2Y5Nzk2MDU4NWE4MThkZDIyZmExYzI2N2I3NWMxNjlmMDUzY2M3MzFlZGFmYTc1MTlhNThlNjIwYjc2Y2ZhJlgtQW16LVNpZ25lZEhlYWRlcnM9aG9zdCJ9.jFMrfDRzdlQ-WPAZ9lsIOjQtZVuS1fgXA_pvNLVQTcM)

* On the title bar, type ip.dst == 142.250.1.139 to filter for traffic associated with a specific IP address. dst means it is where the packet goes to.

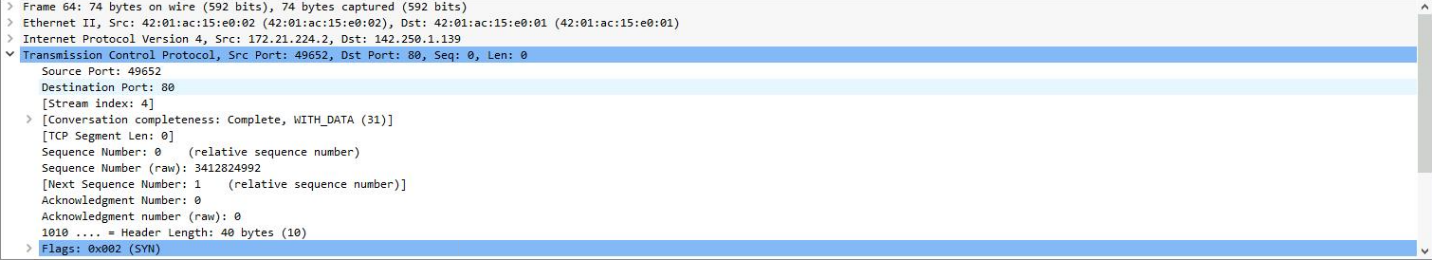
[](https://private-user-images.githubusercontent.com/135963482/302936769-19394509-d60b-48eb-9d41-176d5bffbc00.png?jwt=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJnaXRodWIuY29tIiwiYXVkIjoicmF3LmdpdGh1YnVzZXJjb250ZW50LmNvbSIsImtleSI6ImtleTUiLCJleHAiOjE3Njc2Nzc5NjYsIm5iZiI6MTc2NzY3NzY2NiwicGF0aCI6Ii8xMzU5NjM0ODIvMzAyOTM2NzY5LTE5Mzk0NTA5LWQ2MGItNDhlYi05ZDQxLTE3NmQ1YmZmYmMwMC5wbmc_WC1BbXotQWxnb3JpdGhtPUFXUzQtSE1BQy1TSEEyNTYmWC1BbXotQ3JlZGVudGlhbD1BS0lBVkNPRFlMU0E1M1BRSzRaQSUyRjIwMjYwMTA2JTJGdXMtZWFzdC0xJTJGczMlMkZhd3M0X3JlcXVlc3QmWC1BbXotRGF0ZT0yMDI2MDEwNlQwNTM0MjZaJlgtQW16LUV4cGlyZXM9MzAwJlgtQW16LVNpZ25hdHVyZT03ODRmZmVmOWM4YmY1ZTdhNWU2YWEzN2FlMTQ0MjM3ODMwYTVhMWMyMDVkOGM4YjNhZDU3NjU0N2EzNGVmNzhhJlgtQW16LVNpZ25lZEhlYWRlcnM9aG9zdCJ9.W04mPx6Q7myHrGQDYocuBFBC-41lm4RUk0hZ9n2p-QE)

* On the title bar, type eth.addr == 42:01:ac:15:e0:02 to filter for traffic associated with a specific Ethernet MAC address. addr means either the source or the destination IP.

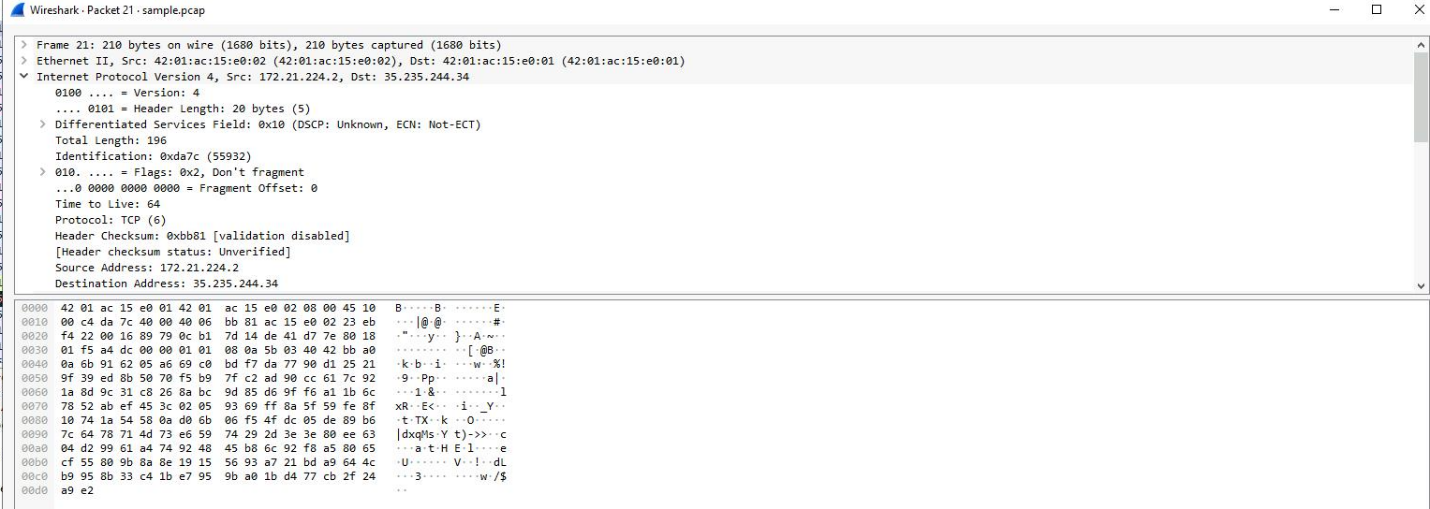
[](https://private-user-images.githubusercontent.com/135963482/302941001-4385847b-0f9f-4fe5-99af-2dc3792f64f1.png?jwt=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJnaXRodWIuY29tIiwiYXVkIjoicmF3LmdpdGh1YnVzZXJjb250ZW50LmNvbSIsImtleSI6ImtleTUiLCJleHAiOjE3Njc2Nzc5NjYsIm5iZiI6MTc2NzY3NzY2NiwicGF0aCI6Ii8xMzU5NjM0ODIvMzAyOTQxMDAxLTQzODU4NDdiLTBmOWYtNGZlNS05OWFmLTJkYzM3OTJmNjRmMS5wbmc_WC1BbXotQWxnb3JpdGhtPUFXUzQtSE1BQy1TSEEyNTYmWC1BbXotQ3JlZGVudGlhbD1BS0lBVkNPRFlMU0E1M1BRSzRaQSUyRjIwMjYwMTA2JTJGdXMtZWFzdC0xJTJGczMlMkZhd3M0X3JlcXVlc3QmWC1BbXotRGF0ZT0yMDI2MDEwNlQwNTM0MjZaJlgtQW16LUV4cGlyZXM9MzAwJlgtQW16LVNpZ25hdHVyZT01MTA3NWE4NTBhZGQ3MTNjYTAxYTEyMGU0OWZiN2ViZGU2NjkzZTIyYzNlOGRmYWQyOWIwMjkxN2ViNDQxOWZhJlgtQW16LVNpZ25lZEhlYWRlcnM9aG9zdCJ9.9o2YoswccAJs6hF-1XbmFq0F0Gq835XSpHrm9ovAt_s)

1. Examine the protocols that are used when the user makes the connection to the website.

* The TCP destination port of this TCP packet is 80 when ip.addr == 142.250.1.139 which contains the initial web request to an HTPP website that will typically be listening on TCP port 80.

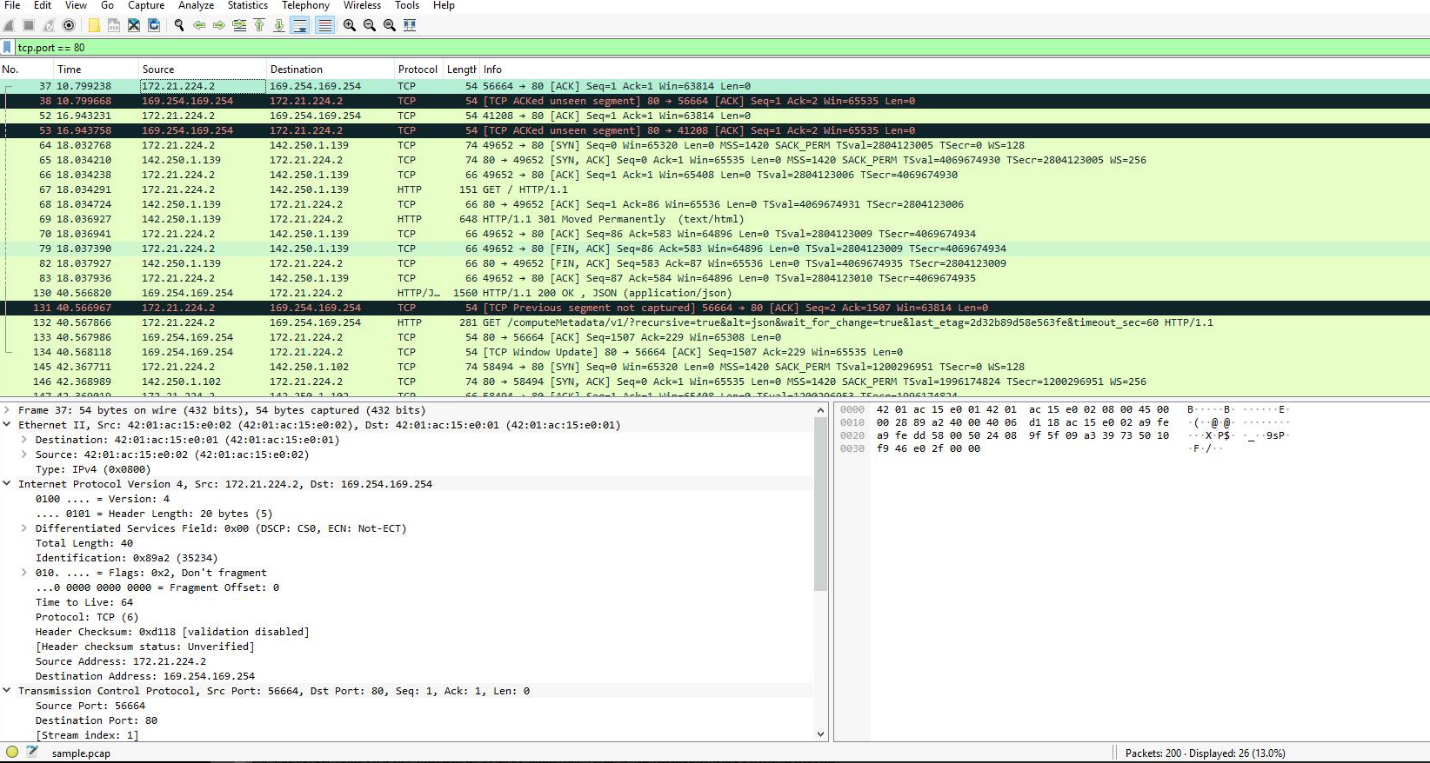
[](https://private-user-images.githubusercontent.com/135963482/302934005-5ce9594c-e9c3-49a2-9d93-cd0da4cb1e3b.png?jwt=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJnaXRodWIuY29tIiwiYXVkIjoicmF3LmdpdGh1YnVzZXJjb250ZW50LmNvbSIsImtleSI6ImtleTUiLCJleHAiOjE3Njc2Nzc5NjYsIm5iZiI6MTc2NzY3NzY2NiwicGF0aCI6Ii8xMzU5NjM0ODIvMzAyOTM0MDA1LTVjZTk1OTRjLWU5YzMtNDlhMi05ZDkzLWNkMGRhNGNiMWUzYi5wbmc_WC1BbXotQWxnb3JpdGhtPUFXUzQtSE1BQy1TSEEyNTYmWC1BbXotQ3JlZGVudGlhbD1BS0lBVkNPRFlMU0E1M1BRSzRaQSUyRjIwMjYwMTA2JTJGdXMtZWFzdC0xJTJGczMlMkZhd3M0X3JlcXVlc3QmWC1BbXotRGF0ZT0yMDI2MDEwNlQwNTM0MjZaJlgtQW16LUV4cGlyZXM9MzAwJlgtQW16LVNpZ25hdHVyZT00OGEyMTllM2UyMzkwZmUxYzExODdjNWE3Zjg3YTU3NDFmNWUwYmQ1NGFiMGY3Zjg2NWE2NjgwYzJmZGIzMDEwJlgtQW16LVNpZ25lZEhlYWRlcnM9aG9zdCJ9.OR_xOOrKOzdb4dZg4_YsBBkPdg31hZ7ryJFDbH7sSCA)

* The protocol destination port is TCP when Etherenet address was 42:01:ac:15:e0:02. Source address is 172.21.224.2 and the destination address is 35.235.244.34.

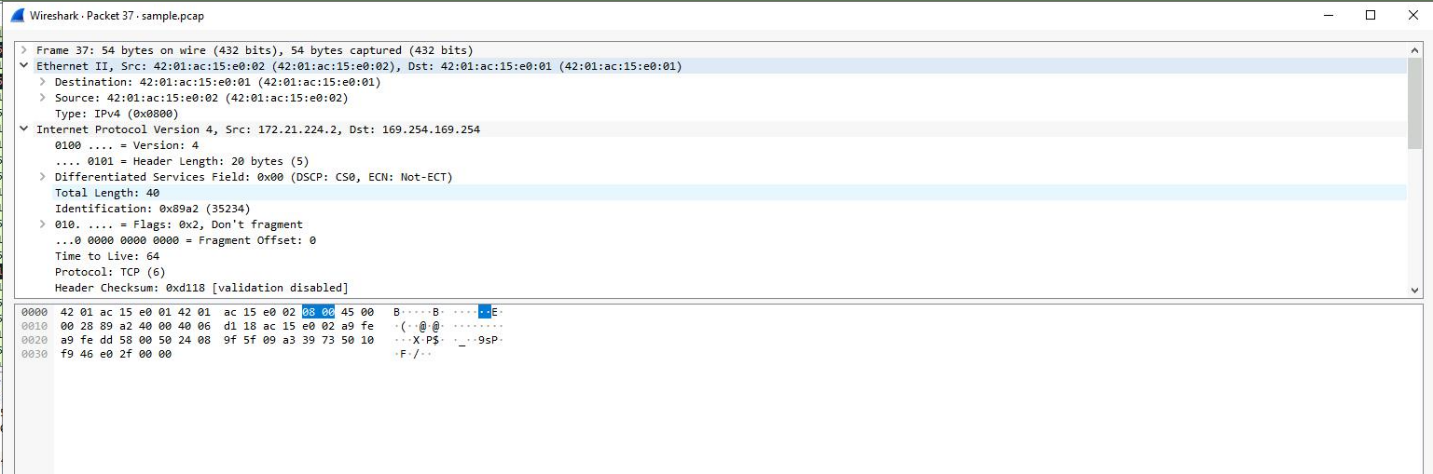
[](https://private-user-images.githubusercontent.com/135963482/302939715-263e55d9-e6e7-4204-b4c3-1215a69c98a1.png?jwt=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJnaXRodWIuY29tIiwiYXVkIjoicmF3LmdpdGh1YnVzZXJjb250ZW50LmNvbSIsImtleSI6ImtleTUiLCJleHAiOjE3Njc2Nzc5NjYsIm5iZiI6MTc2NzY3NzY2NiwicGF0aCI6Ii8xMzU5NjM0ODIvMzAyOTM5NzE1LTI2M2U1NWQ5LWU2ZTctNDIwNC1iNGMzLTEyMTVhNjljOThhMS5wbmc_WC1BbXotQWxnb3JpdGhtPUFXUzQtSE1BQy1TSEEyNTYmWC1BbXotQ3JlZGVudGlhbD1BS0lBVkNPRFlMU0E1M1BRSzRaQSUyRjIwMjYwMTA2JTJGdXMtZWFzdC0xJTJGczMlMkZhd3M0X3JlcXVlc3QmWC1BbXotRGF0ZT0yMDI2MDEwNlQwNTM0MjZaJlgtQW16LUV4cGlyZXM9MzAwJlgtQW16LVNpZ25hdHVyZT0zODkzMmI4NGIzYmJmYzY1YmY0YWU5MmE0MmI4MGFhNTdlZGNjN2E2ODFmNWVmMDE0OTNkOGNlZDhlNjM0Mjc2JlgtQW16LVNpZ25lZEhlYWRlcnM9aG9zdCJ9.78HH-iQziz8Jl3wxmkyUqEGsDxKlc3G3sEXM3nU32os)

1. Analyze the data packet to identify the type of information sent and received by the systems that connect to each other when the network data is captured.

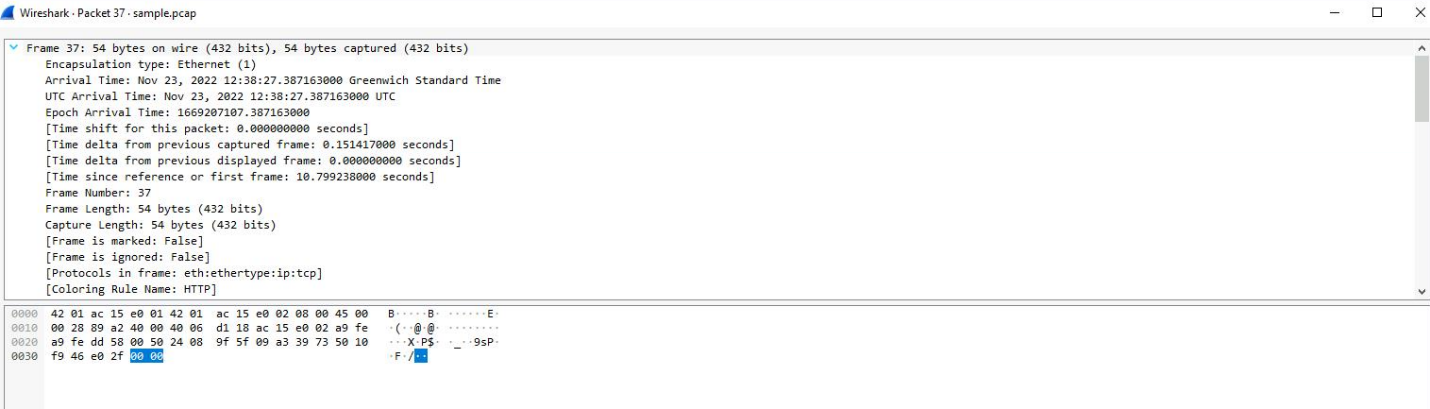
* On the title bar, type tcp.port == 80 to filter for traffic associated with a specific port number. tcp.port == 80 means only the tcp port is 80 will be shown.

[](https://private-user-images.githubusercontent.com/135963482/302944704-28081462-b634-4838-a307-b9574e7f3234.png?jwt=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJnaXRodWIuY29tIiwiYXVkIjoicmF3LmdpdGh1YnVzZXJjb250ZW50LmNvbSIsImtleSI6ImtleTUiLCJleHAiOjE3Njc2Nzc5NjYsIm5iZiI6MTc2NzY3NzY2NiwicGF0aCI6Ii8xMzU5NjM0ODIvMzAyOTQ0NzA0LTI4MDgxNDYyLWI2MzQtNDgzOC1hMzA3LWI5NTc0ZTdmMzIzNC5wbmc_WC1BbXotQWxnb3JpdGhtPUFXUzQtSE1BQy1TSEEyNTYmWC1BbXotQ3JlZGVudGlhbD1BS0lBVkNPRFlMU0E1M1BRSzRaQSUyRjIwMjYwMTA2JTJGdXMtZWFzdC0xJTJGczMlMkZhd3M0X3JlcXVlc3QmWC1BbXotRGF0ZT0yMDI2MDEwNlQwNTM0MjZaJlgtQW16LUV4cGlyZXM9MzAwJlgtQW16LVNpZ25hdHVyZT1kZjU5YTg1OWY2OTY4YzJiMzdkY2I2OTc4ODA0ZDlhYjdhNzZmOWE1MDdhZDNmNjQ3MzA0NDY2YmQzYmJkZDg5JlgtQW16LVNpZ25lZEhlYWRlcnM9aG9zdCJ9.5E1iZvGM7y5y5DiZFNNdAnctPTK0IXYo4i1cuBkl60o)

* When the filter tcp.port == 80 sets in play, the time to live is 64.
* Time to Live: A field in the Internet Protocol (IP) header that indicates the maximum amount of time an IP packet is allowed to exist in the network before it is discarded if it has not reached its destination. TTL is used to prevent packets from circulating indefinitely in the network, which could happen in the case of routing loops. It can be used as a basic security measure to limit how far packets can propagate through the network.

[](https://private-user-images.githubusercontent.com/135963482/302944581-1fe9ba32-926b-42f3-a39e-49da54240058.png?jwt=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJnaXRodWIuY29tIiwiYXVkIjoicmF3LmdpdGh1YnVzZXJjb250ZW50LmNvbSIsImtleSI6ImtleTUiLCJleHAiOjE3Njc2Nzc5NjYsIm5iZiI6MTc2NzY3NzY2NiwicGF0aCI6Ii8xMzU5NjM0ODIvMzAyOTQ0NTgxLTFmZTliYTMyLTkyNmItNDJmMy1hMzllLTQ5ZGE1NDI0MDA1OC5wbmc_WC1BbXotQWxnb3JpdGhtPUFXUzQtSE1BQy1TSEEyNTYmWC1BbXotQ3JlZGVudGlhbD1BS0lBVkNPRFlMU0E1M1BRSzRaQSUyRjIwMjYwMTA2JTJGdXMtZWFzdC0xJTJGczMlMkZhd3M0X3JlcXVlc3QmWC1BbXotRGF0ZT0yMDI2MDEwNlQwNTM0MjZaJlgtQW16LUV4cGlyZXM9MzAwJlgtQW16LVNpZ25hdHVyZT1iYzM4MTc5MmRlNTMyMmMzZmVkMWM4ZjBjMTUxNmRlOGI1NDMzYjcwMzU3YTk1N2QyOTM5Y2MwY2UyZWRmMzIzJlgtQW16LVNpZ25lZEhlYWRlcnM9aG9zdCJ9.wbNUdu6EIsTz9bw8y2R8Djnjg_uqarWlLqcVC8ehK-s)

* When the filter tcp.port == 80 sets in play, the Frame Number is 37 and Frame Length is 54 bytes.
* Frame Number: This is essentially the sequence number of a packet within a particular capture. It helps you identify and refer to packets more easily. In your case, a frame number of 37 means it's the 37th packet captured since the beginning of the capture session. This number is assigned sequentially as packets are captured, starting with the number 1 for the first packet.
* Frame Length: This indicates the size of the packet, including all headers and payload, measured in bytes. The frame length of 54 bytes means the total size of the packet is 54 bytes. This size includes everything from the lowest layer (physical layer) up to the highest layer present in the packet that Wireshark can decode. It's useful for understanding the size of the data being transmitted and can help in various analyses, such as identifying potential issues with packet sizes that might indicate fragmentation or other problems.

[](https://private-user-images.githubusercontent.com/135963482/302944127-107d084b-361e-4f74-98ea-c90c93fe1cae.png?jwt=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJnaXRodWIuY29tIiwiYXVkIjoicmF3LmdpdGh1YnVzZXJjb250ZW50LmNvbSIsImtleSI6ImtleTUiLCJleHAiOjE3Njc2Nzc5NjYsIm5iZiI6MTc2NzY3NzY2NiwicGF0aCI6Ii8xMzU5NjM0ODIvMzAyOTQ0MTI3LTEwN2QwODRiLTM2MWUtNGY3NC05OGVhLWM5MGM5M2ZlMWNhZS5wbmc_WC1BbXotQWxnb3JpdGhtPUFXUzQtSE1BQy1TSEEyNTYmWC1BbXotQ3JlZGVudGlhbD1BS0lBVkNPRFlMU0E1M1BRSzRaQSUyRjIwMjYwMTA2JTJGdXMtZWFzdC0xJTJGczMlMkZhd3M0X3JlcXVlc3QmWC1BbXotRGF0ZT0yMDI2MDEwNlQwNTM0MjZaJlgtQW16LUV4cGlyZXM9MzAwJlgtQW16LVNpZ25hdHVyZT1kODMyNGQzNGYyOTRkMDc1OGZmNjE2MjdjZjZkOGMzZTIxOTUyMGMxYzI1YzI2MDI0YjdmMzdiMTM0NTMyYjZjJlgtQW16LVNpZ25lZEhlYWRlcnM9aG9zdCJ9.8giJyW6smizdG71WzIzToJMQeVBkLpeyTltKLvaVKDQ)