# Network Protocol Analysis

***Contents***

* Network & Protocols
* Wireshark introduction
* Ip address spotting using Wireshark
* Use of Wireshark for filtering
* TCP 3 Way handshake
* Port Numbers
* Using http
* Making use of gzip
* Status Codes
* Following http stream
* FTP

***Networks & Protocols***

*Network -*

Systems that connect computers and devices, allowing them to communicate and share information. They can be as small as a home Wi-Fi setup or as large as the internet.

*Protocol –*

Protocols are rules or standards that define how data is transmitted over a network. They ensure that devices can understand and communicate with each other properly. Examples include TCP/IP for the internet and HTTP for web browsing.

***WIRESHARK***

*What is this tool ?*

Wireshark is a network analyzer tool. It captures and displays data exchanged between devices on a network, helping users troubleshoot issues, analyze communication patterns, and identify potential security issues. It's a valuable tool for understanding and monitoring network activities.

*Key Features include :*  Packet Capture, Protocol Support & Packet Inspection

***Spotting IP address of*** → <http://httpforever.com>

*Here is the IP address of the website obtained from Wireshark using the DNS protocol.*

*The same IP address can be obtained by pining the FQDN using the command prompt.*

*As you can see there is both the request as well as the response from the DNS server, this shows that*

*REQUEST – From source to the DNS server (here we need to keep in mind that the DNS is not the actual server but the middleman between the network)*

*RESPONSE – From DNS to source* *A screenshot of a computer

Description automatically generated*

***Cross Checking with CMD***

A screenshot of a computer

Description automatically generated

***Filtering***

Filtering the packets can be done using the following prompt

ip.addr == 146.190.62.39

Using this prompt, we can identify the required traffic to identify the 3-way handshake initiated with HTTPForever webserver

What is ip.addr?

"ip.addr" matches against both the [IP](https://wiki.wireshark.org/IP) source and destination addresses in the IP header. The same is true for "tcp.port", "udp.port", "eth.addr", and others. It's important to note that.

***TCP three-way handshake***

* A diagram of a server

  Description automatically generated1. SYN (Synchronize):

The client sends a SYN packet to the server, indicating its desire to initiate communication.

This packet includes a sequence number that the client will use to track the order of its data segments.

* 2. SYN-ACK (Synchronize-Acknowledge):

Upon receiving the SYN packet, the server sends a SYN-ACK packet back to the client.

This packet acknowledges the client's SYN with its own sequence number and includes an additional ACK (Acknowledgement) number.

The ACK number acknowledges the server's receipt of the client's SYN packet.

* 3. ACK (Acknowledge):

Finally, the client sends an ACK packet back to the server, acknowledging the server's SYN- ACK packet.

This completes the 3-way handshake and establishes a full-duplex connection between the two devices.

A screenshot of a computer

Description automatically generated

***Port Number***

Port number is like a unique address for different applications on your computer, allowing them to receive and send data independently.

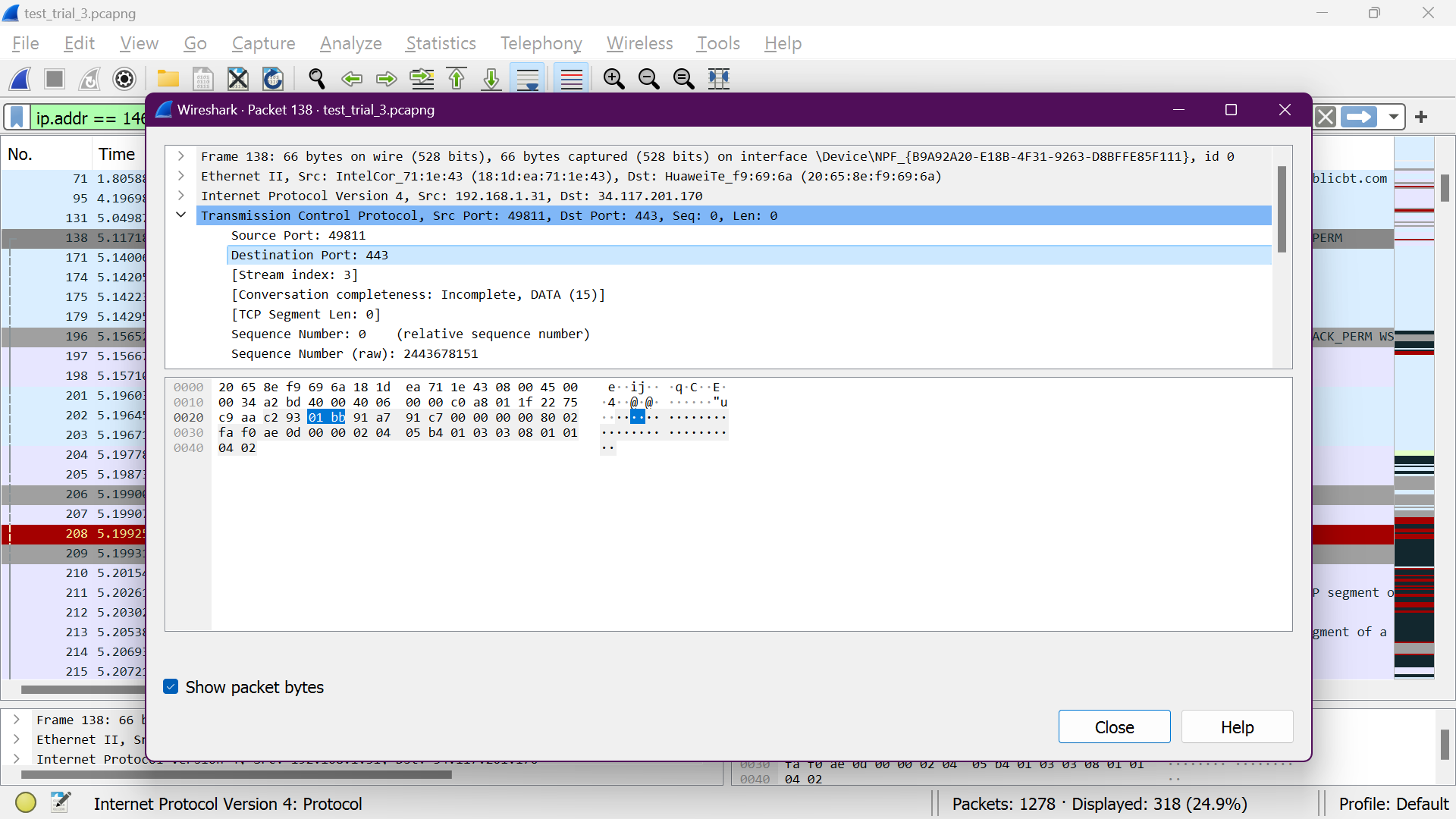
Think of it as mailboxes for different programs!

Using the Packets of SYN , SYN,ACK or ACK we can identify this property

There are 3 ranges of port numbers

A blue and white list with black text

Description automatically generated



***Status code***

Using http filtering we can obtain the GET request

A screenshot of a computer

Description automatically generated

http status codes are used as a server response to a browser's request

A screen shot of a computer status code

Description automatically generated

***Using http***

***A screenshot of a computer

Description automatically generated***

Browser language

Browser version

Version No.

***“Accept-Encoding: gzip”***

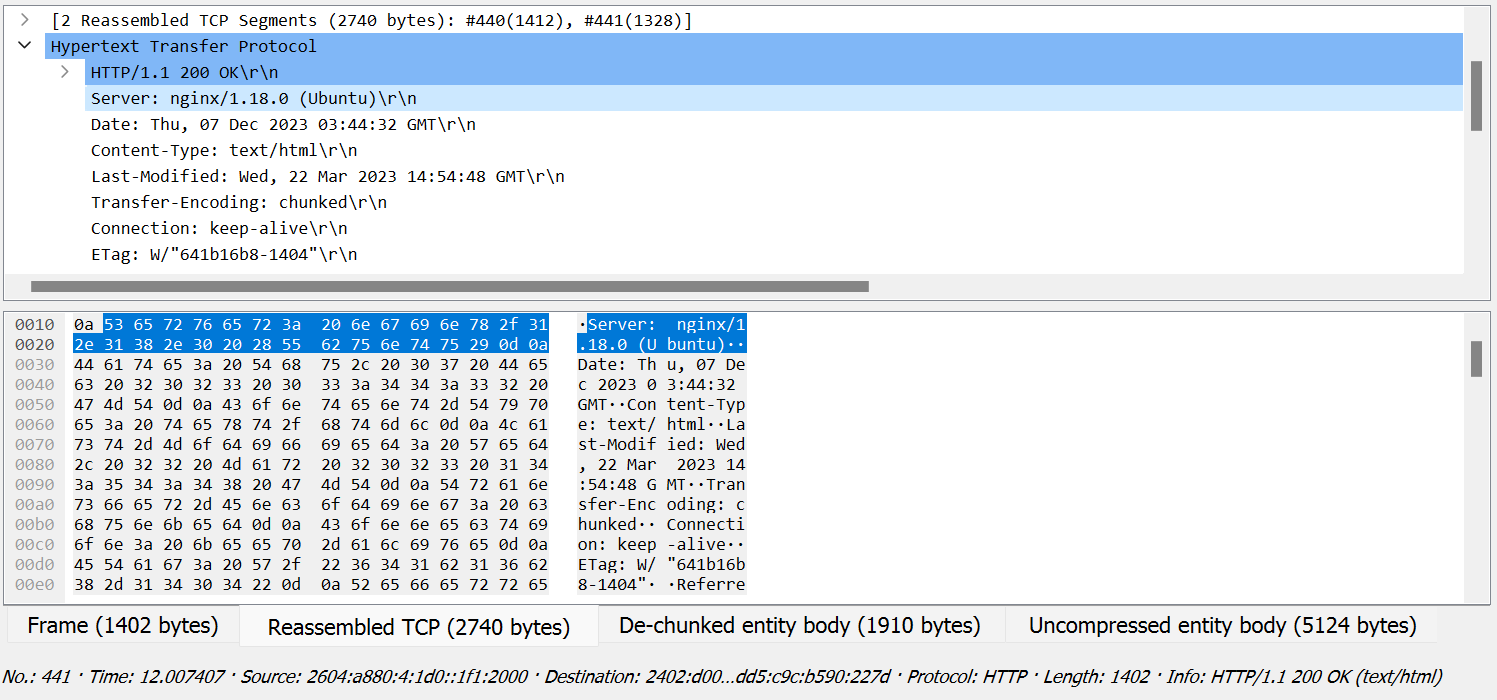
“Accept-Encoding: gzip" is a request header in HTTP telling the server the client can accept a compressed response using the gzip algorithm. This helps:

1. Reduce data transfer size: Compressed responses are smaller, leading to faster loading times and lower bandwidth usage.
2. Improve website performance: Smaller data decreases server load and improves responsiveness, enhancing user experience.
3. Wide compatibility: Most browsers and servers support gzip, making it a reliable practice.
4. User transparency: Users experience no difference in content despite the compression.

A screenshot of a computer

Description automatically generatedUsing "Accept-Encoding: gzip" is a simple and effective way to boost website performance and user satisfaction.

***Locating HTTP response***



***"Follow HTTP stream"***

Using the HTTP stream, we can identify the required data

Who is the author of this Website?

rel="author">scotthelme.co.uk 🡪 scotthelme

What copyright license is used?

<a href="https://creativecommons.org/licenses/by-sa/4.0/">CC BY-SA 4.0</a>

Link 🡪 https://creativecommons.org/licenses/

What is the country of origin of the author?

UK

***FTP***

The File Transfer Protocol (FTP) is a standard network protocol used for the transfer of computer files between a server and a client on a computer network. It is a widely used and established method for uploading and downloading files over the internet.

* Find more details at speedguide