Wireshark: Open source application that can be used to capture and analyse network traffic. Need two IPv4 to identify host participating in packet exchange

Nslookup [url]: Identifies IP address of remote server

Ip.addr == [IP address] and [Protocol]: Filters based off IP and Protocol (HTTP/TCP/UDP/SSH etc). Can't by format like png html etc.

Cntrl +F: Filter by string text input

Ipconfig /flushdns: Flush caches dns info

Export Packet Bytes: Click on content →

so go to Packet details (bottom zone below the list of things) →

Right click the very bottom (Portable network graphic/Post office protocol/Line-based text data) → Export packet bytes + file format. This allows you to view the content whether it is a PNG or an Email or HTML etc

Source vs Destination on Wireshark:

- Source: who is sending the message
- Destination: who is receiving the message
- IE: If our IP is source → Website