

Wireshark is a network analysis tool that allows users to monitor traffic that is outgoing on a given interface. It is a powerful tool that is widely considered to be one of the top tools to analyze network traffic. It gives users a large base of information including information at each network layer. It’s easy to setup and can be run on many operating systems, making it incredibly useful for network managers to use. It can also be used for malicious intent if the user so chooses to do so.

Wireshark sniffs the packets that go through the interface device, such as an Ethernet connection and gives information about the packets contents. The content in each packet is shown in the GUI main screen and is color coordinated based off of the protocol. It allows network managers to view what the source of each packet sent or received is, what the destination is, protocol, length, and a short info section on the main screen. There is also an option on the top to allow for packet filtering based on protocols and other options.

Once a packet is clicked on a smaller, lower, window opens in the Wireshark GUI which shows the packet details. Depending on what packet is checked there could be a variety of different information. Depending what type of protocol request is given changes the information in the packet detail window. If an HTTP packet is clicked, for example, users can look at the frame info, device used to transmit the data, the IP version being used and information about the packet, and what protocol is being used (either TCP or UDP for HTTP).

Clicking on any of the information in the packet detail window will drop down even more information about what is contained within each part of the packet. By clicking on what IP version is being used for example, will give information about things such as header length, total length, time to live, source, destination, and flags.

When connecting to a regular site, the ARP protocol is used to map the IPv4 address to the Ethernet address since, for this Wireshark analysis, Ethernet was used to connect to the internet. The ARP request shows the source MAC address and hardware as well as the destination MAC address and hardware.

A DNS request is first used to request a lookup for a given domain name. If google.com was searched, a DNS request is sent to try and determine the IP address of google.com. There is then a DNS response that informs the requester what the IP address of google is. The DNS request contains information about the source port which was 3163 and the destination is port 53. Port 3163 is a registered port that uses TCP and port 53 (server destination) is the port used for DNS requests. The DNS request also contains the source IP address and the destination IP address. The source IP in the Wireshark trace was 128.238.38.160 and the source address was 128.238.29.23.

The three way handshake is then initiated after the DNS response. For the three way handshake, a TCP connection is attempted with the source (usually a personal computer) tries to connect with the IP address of google. The server then responds with an ACK through TCP and the client replies with an ACK as well. Then a GET request is sent to get the page sent to the client. The TCP request contains the source IP and destination IP. The source IP is still 128.238.38.160 but the destination address is now 132.151.6.75. This is because the source is not trying to contact the DNS server but rather the server of the web service that it is trying to connect to. The ports used in the three way handshake are source port 3369 and destination port 80. Port 3369 is used for TCP connections and port 80 is used to listen for incoming TCP connections.

Wireshark is a powerful tool that allows users to see where packets are coming from and where they are going to on a network interface. This allows network specialists to analyze their traffic and see where it’s coming from, where it’s going to, the ports being used, interface used to connect and more. It can also be used to analyze packets to see if a DDoS attack is being attempted or malware is being sent over their networks. While Wireshark is helpful to analyze traffic and help improve network security, it can also be used for malicious attacks. Users could potentially use Wireshark to sniff people’s packets in say Starbucks to gain information about users in that Starbucks. This could allow malicious users to attack the users IPs they get from users computers and possibly cause a large amount of damage depending on what information they can extract from Wireshark. In the end, Wireshark is a powerful tool that, when used correctly, can help assist people trying to improve their networks.