Video - Sample IPv4 Headers in Wireshark (6 min)

Let's see how network layer information can be seen and analyzed in a Wireshark packet capture. I have a screenshot from a Wireshark packet capture. And you can see that the second packet that's been captured has been highlighted, and then in the packet details window, the network layer information has been expanded to show us all of the things happening at the network layer.

So let's see what's happening in this particular packet that we're examining. We can see that, first of all, the network layer protocol, or Internet layer protocol, that we are dealing with was Internet protocol version 4, IPv4. We can also see that the source IP address was 192.168.1.109. You can see it also highlighted up here in the packet list window area and that the destination IP address was 192.168.1.1. And we can also see that up here. We can see that, at the higher layer, this is TCP protocol packet. But if we limit ourselves to just the IPv4 fields, or the IPv4 information, we can see the different types of control information that's contained in every IPv4 packet.

For instance, the version number, which is 4, identifying this as an IPv4, as opposed to IPv6 packet. The header length, or the length of the header-- this the minimum size of an IPv4 header. The differentiated services field, which is used for packet prioritization and is useful for applications like voice over IP. The total length of the packet, the identification number, which is used for fragmentation. The flags, you can see that the DF bit has been set, which stands for "don't fragment." This packet is not large enough or is not identified for fragmentation. A fragment offset, the TTL, or time to live, which is set to 128. Every time a packet is routed from one hop to the next, the TTL number is reduced. When the TTL number reaches 0, the packet is dropped, insuring that packets don't circulate on the Internet forever on an endless loop. The TTL value is also used in ICMP trace routes and pings. The protocol field lets us know the type of information to expect in the data portion of the packet. A 6 identities the data portion of this packet as being a TCP packet. The header checksum field, which allows routers to check to see if there are any errors or inconsistency in the IP header. If there is, the packet will be dropped.

And then, lastly, the source and destination IP addresses, which are the most important part of the IPv4 packet. Let's take a look at two more screenshots of Wireshark packet captures, and we'll see some similarities and differences. The next screenshot shows us that now we're looking at the eighth packet captured. The packet's source IP address is also 192.188.1.109, and the destination IP address is 192.168.1.1, except this packet is an HTTP GET request. So this is a request to a web server located at 192.168.1.1. You can see that the network layer, or Internet layer information, has been expanded, that it's also the IP version 4 protocol, and that we have similar information in the different fields.

Notice under the total length field that this packet is 411 bytes, compared to the previous packet, which was only 52 bytes. You can tell that this packet has a lot more information, or is a much larger packet, than the previous one. If we look below the Internet protocol version 4 information, we can see the TCP information and then below that that there's hypertext transfer protocol, or HTTP protocol, information in this packet as well. I'll move forward to the next packet, and you can see that this packet is the 16th packet captured right up here. It's also from host 192.168.1.109 to host 192.168.1.1, except this is the ICMP protocol. You can see from the information in the packet list window that this in an echo, or ping, request. If we look in the Internet protocol version 4 information in the details area, we can see some minor differences. The version is still 4. The header length is still 20 bytes. But we can see that the flags are slightly different and that the protocol field is now set to 1, indicating that the data portion of this packet is an ICMP protocol message. Notice that in the details window at the bottom here is an expanded area to look at the header information specific to ICMP.