**EX.NO. 5. WIRESHARK TOOL TO CAPTURE AND EXAMINE PACKETS**

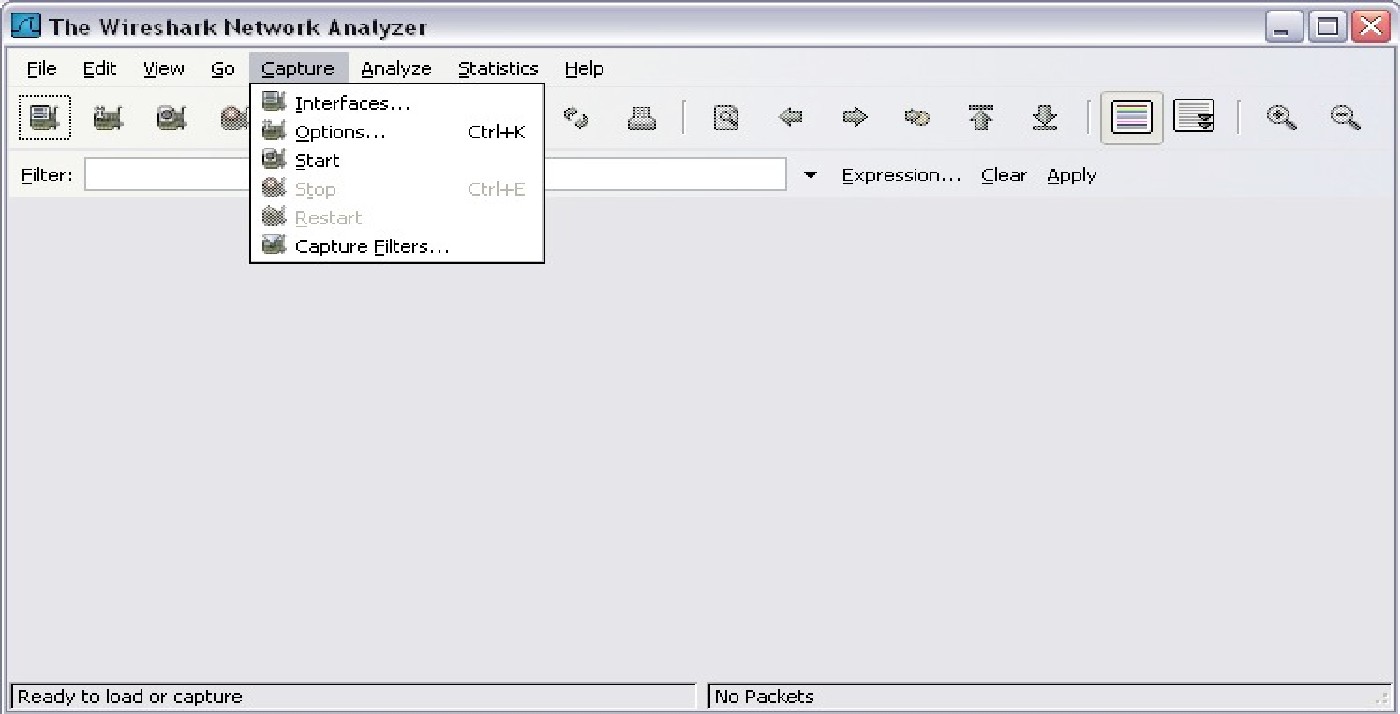
**AIM:**

To capture ping and traceroute PDUs using a network protocol analyzer and examine in

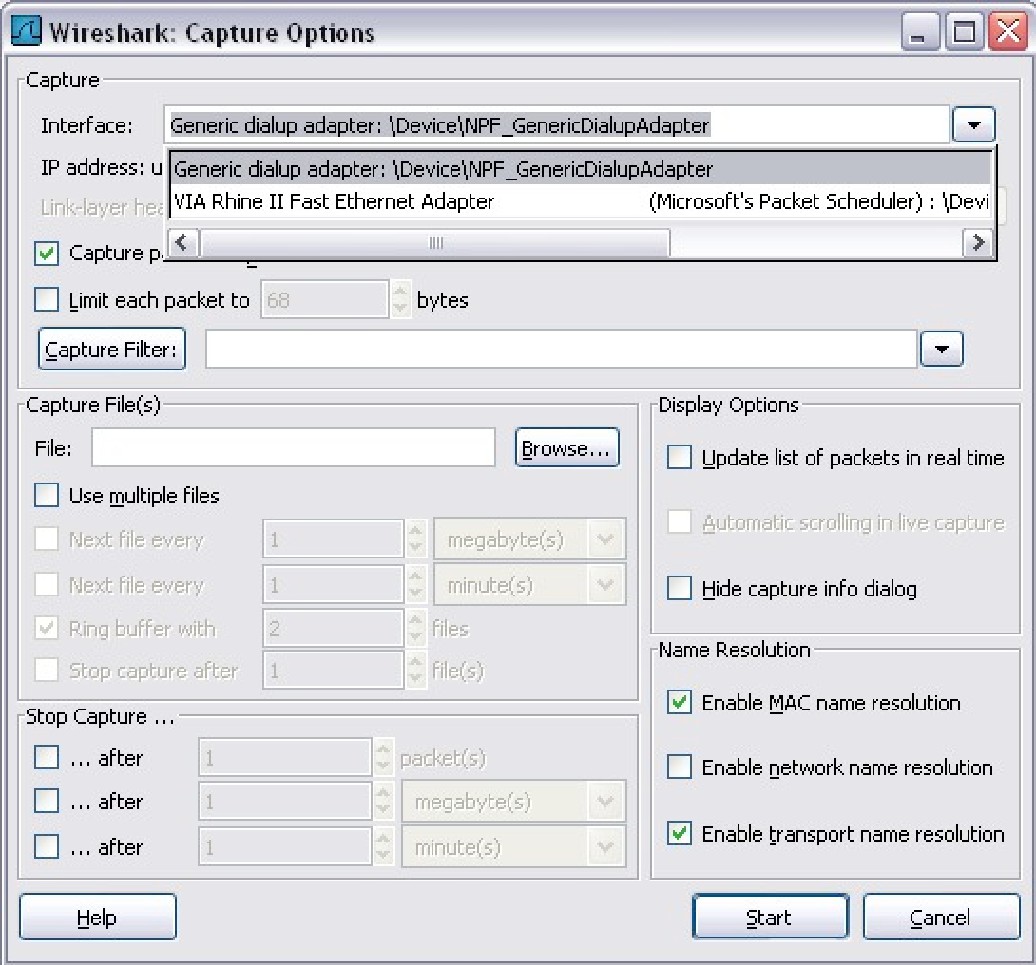
detail.

# WIRESHARK TOOL

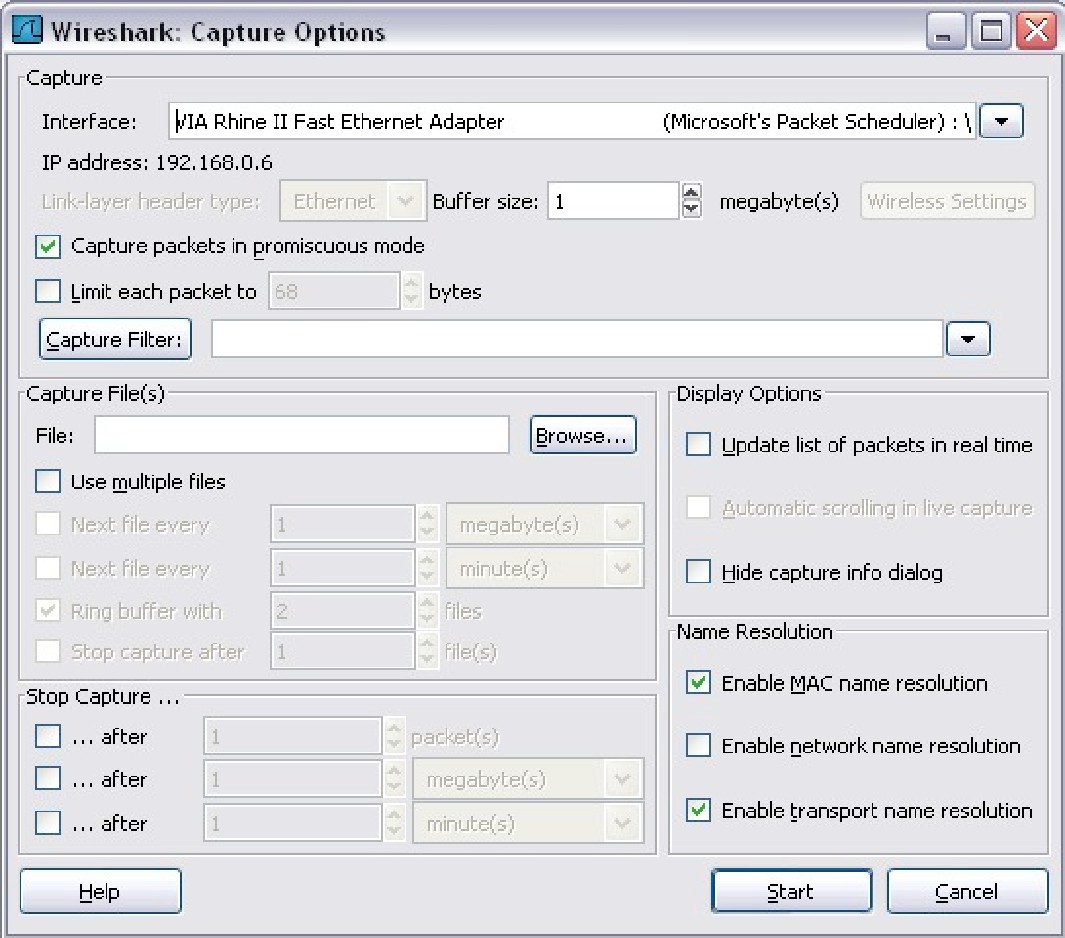
When Wireshark is launched, the screen below is displayed.



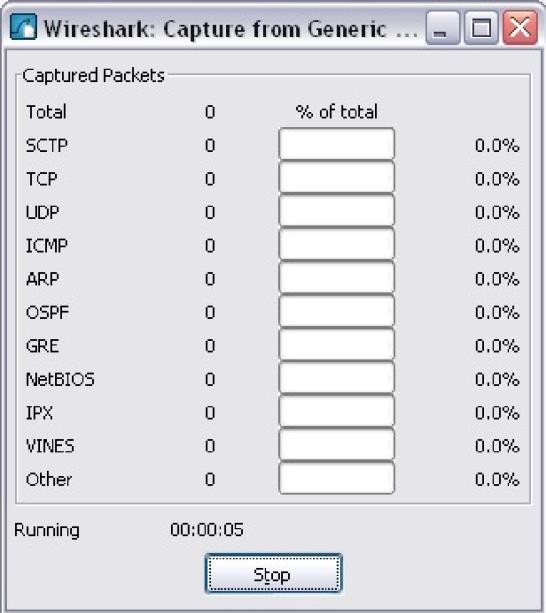
To start data capture it is first necessary to go to the **Capture** menu and select the **Options** choice. The **Options** dialog provides a range of settings and filters which determines which and how much data traffic is captured.



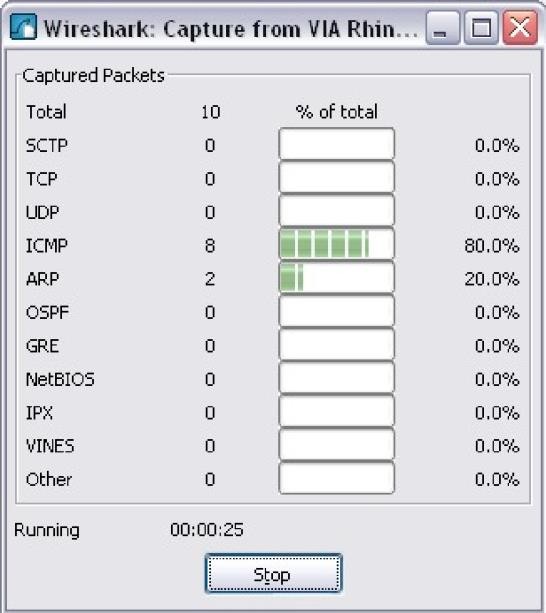
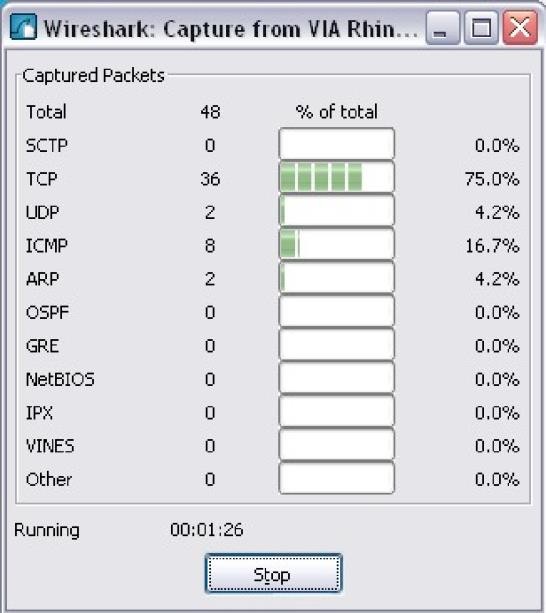
First, it is necessary to ensure that Wireshark is set to monitor the correct interface. From the **Interface** drop-down list, select the network adapter in use. Typically, for a computer this will be the connected Ethernet Adapter. Then other Options can be set. Among those available in **Capture Options,** the two highlighted below are worth examination.



Clicking on the **Start** button starts the data capture process and a message box displays the progress of this process.

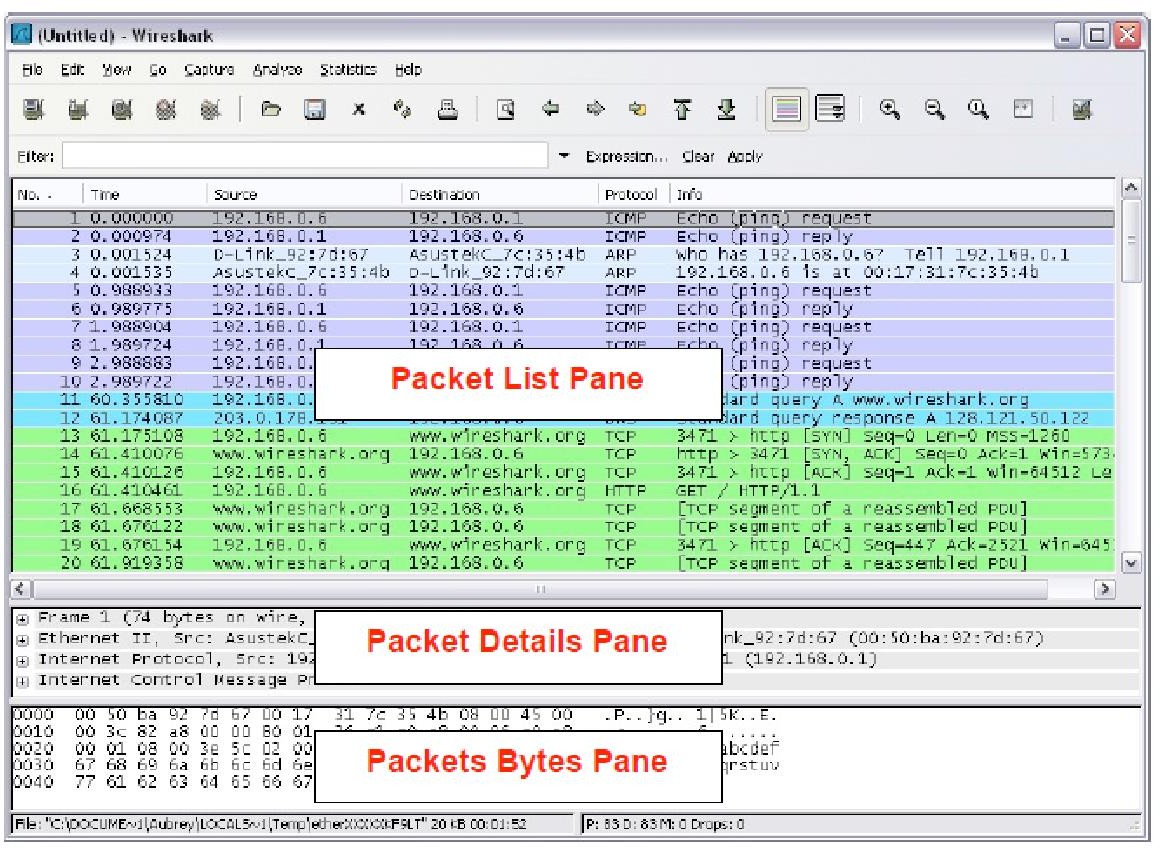


As data PDUs are captured, the types and number are indicated in the message box

The examples above show the capture of a ping process and then accessing a web page. When the

**Stop** button is clicked, the capture process is terminated and the main screen is displayed. This main display window of Wireshark has three panes.



The PDU (or Packet) List Pane at the top of the diagram displays a summary of each packet captured. By clicking on packets in this pane, you control what is displayed in the other two panes. The PDU (or Packet) Details Pane in the middle of the diagram displays the packet selected in the Packet List Pane in more detail.

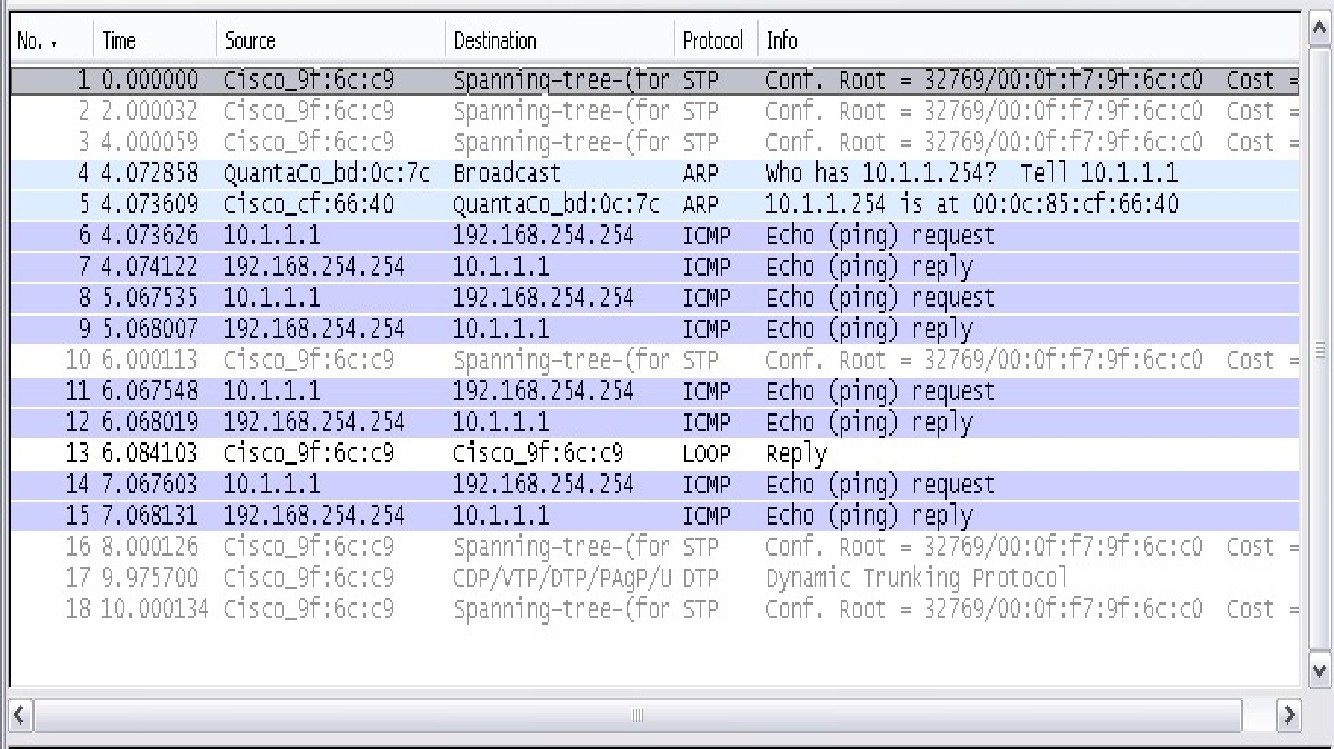
The PDU (or Packet) Bytes Pane at the bottom of the diagram displays the actual data (in hexadecimal form representing the actual binary) from the packet selected in the Packet List Pane, and highlights the field selected in the Packet Details Pane.

## Task 1: Ping PDU Capture

Step 1: After ensuring that the standard lab topology and configuration is correct, launch Wireshark on a computer in a lab pod. Set the Capture Options as described above in the overview and start the capture process. From the command line of the computer, ping the IP address of another network connected and powered on end device on in the lab topology. In this case, ping the Eagle Server at using the command ping 192.168.254.254. After receiving the successful replies to the ping in the command line window, stop the packet capture.

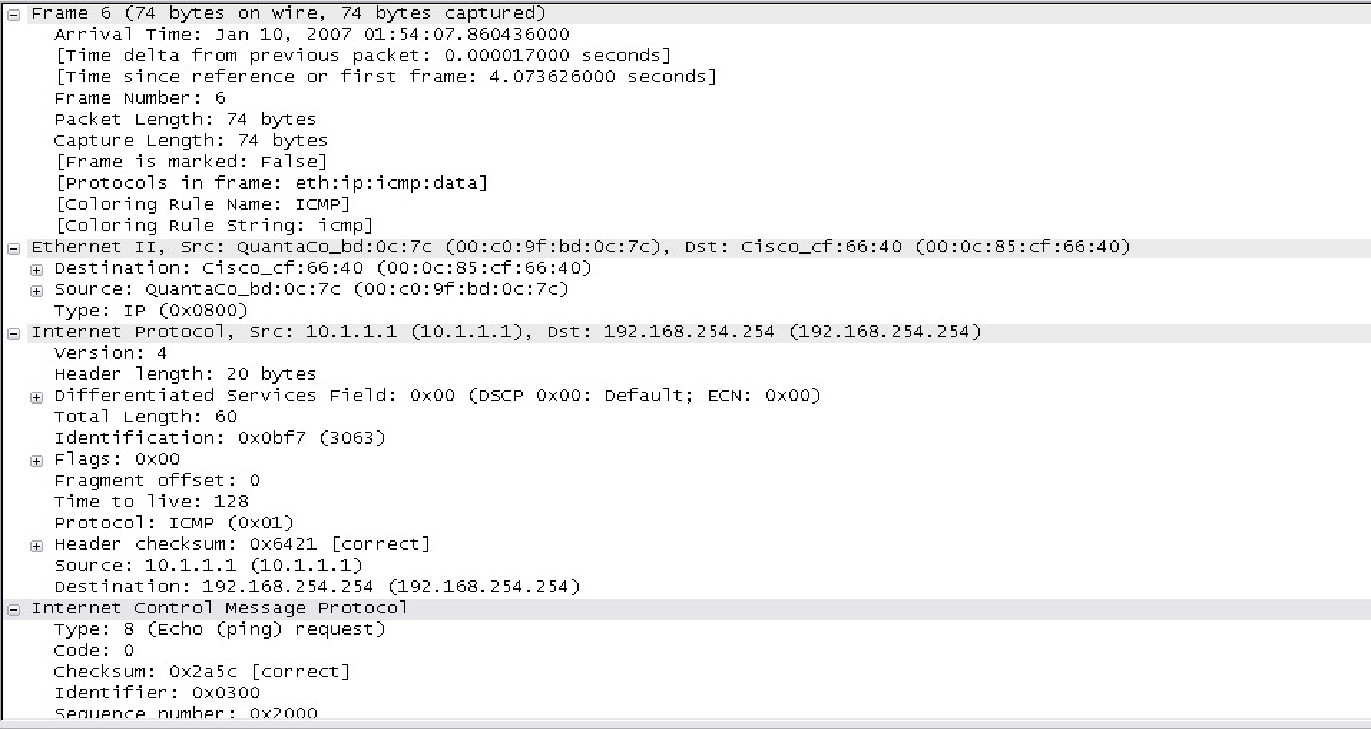
Step 2: Examine the Packet List pane.

The Packet List pane on Wireshark should now look something like this:



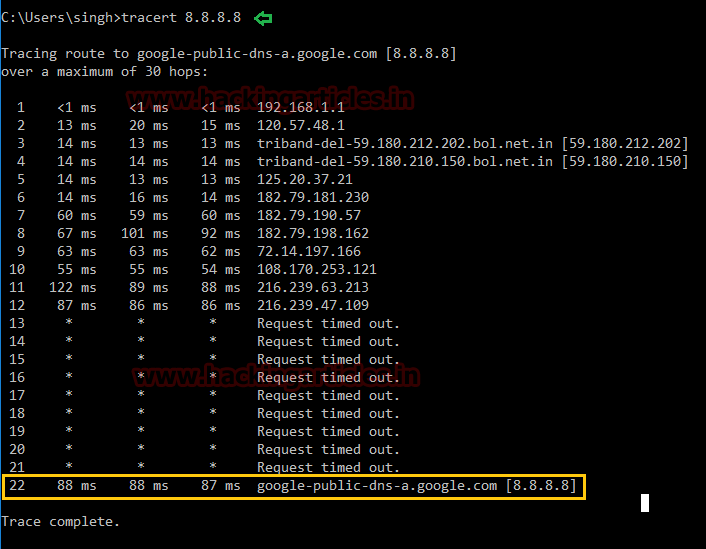
Look at the packets listed above; we are interested in packet numbers 6, 7, 8, 9, 11, 12, 14 and 15. Locate the equivalent packets on the packet list on your computer.

Step 3: Select (highlight) the first echo request packet on the list with the mouse. The Packet Detail pane will now display something similar to: Click on each of the four "+" to expand the information. The packet Detail Pane will now be similar to:



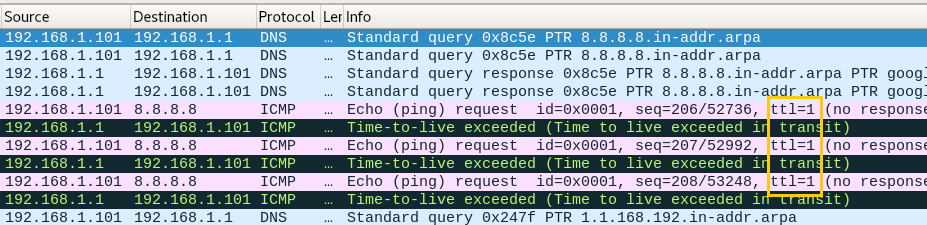
## Task 2: Traceroute PDU Capture

Traceroute generates a list of each hop by entering IP of routers that traversed between source and destination and average round-trip time. As a result **hop 22 denotes** entry of destination i.e. Google DNS. In order to notice the activity of traceroute, Wireshark runs in the background.

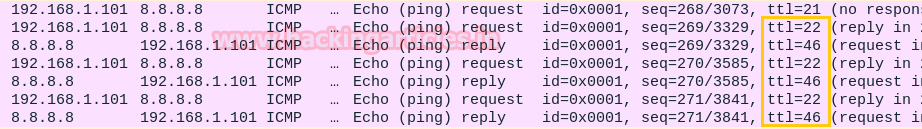


## At Wireshark the following points are notices:

* ICMP echo request packet is used instead of UDP to send DNS query.
* The packet first goes from source 192.168.1.101 to first router 192.168.1.1 having ICMP echo request packet with TTL=1
* The router will drop that packet and send ICMP Time Exceeded error message to the source.
* All this happens 3 times before the source machine sends next packet by incrementing TTL value by 1 i.e. TTL=2.



From this image we can observe ICMP echo reply message is sent from 8.8.8.8 (destination) to 192.168.1.101 (source) for TTL 22.



# RESULT:

Thus the capturing of ping and traceroute PDUs using a network protocol analyzer examined.