Experiment No 1 - It is Practical 1.

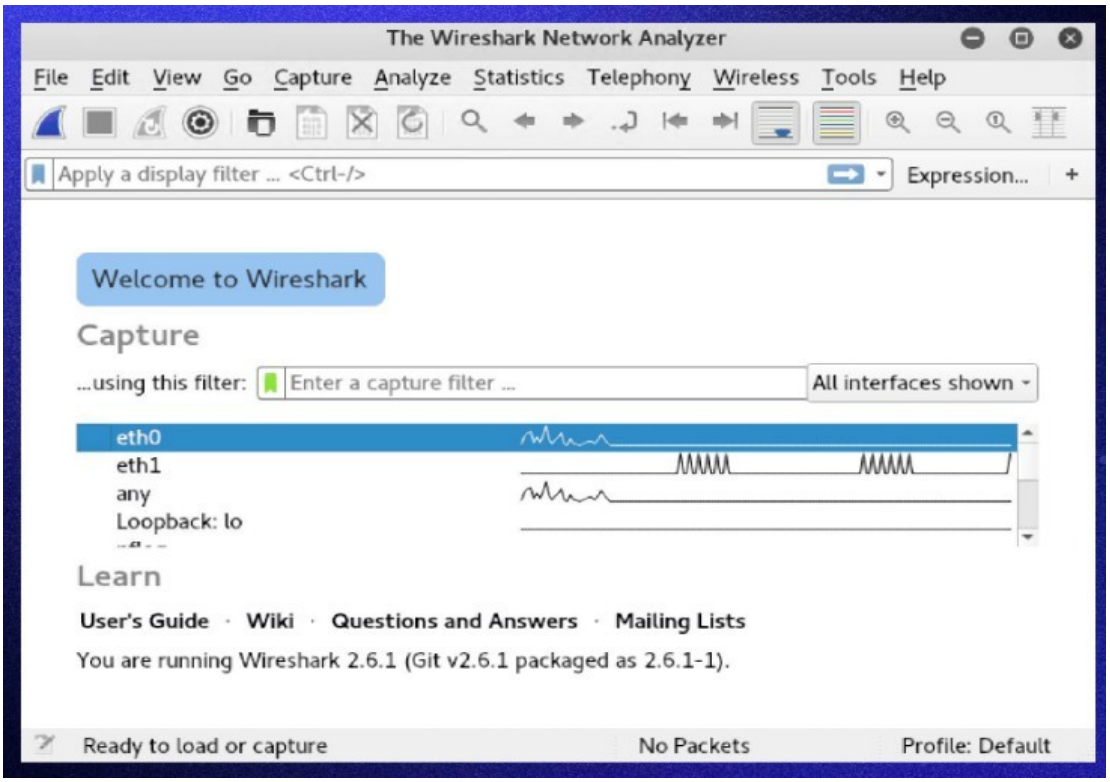
Cyber Security Workshop (Dr. A.P.J. Abdul Kalam Technical University)

Experiment No:1

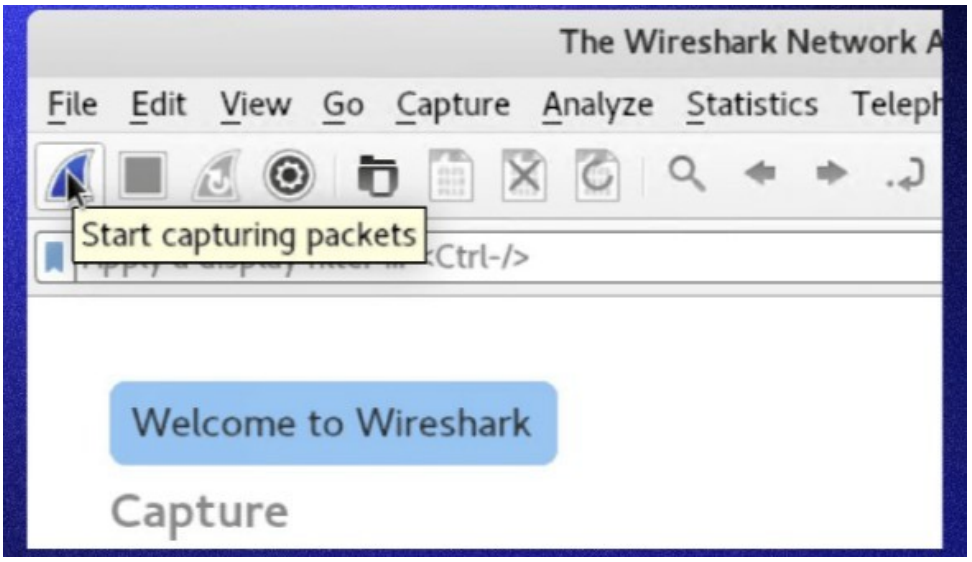
Aim: Basic Packet Inspection: Capture network traffic using Wire shark and analyze basic protocols like HTTP, DNS, and SMTP to understand how data is transmitted and received.

Solution

a. Open Wireshark.
b. The following screen showing a list of all the network connections you can monitor is displayed. You can select one or more of the network interfaces using shift+left-click or by clicking on the tab All Interfaces Shown

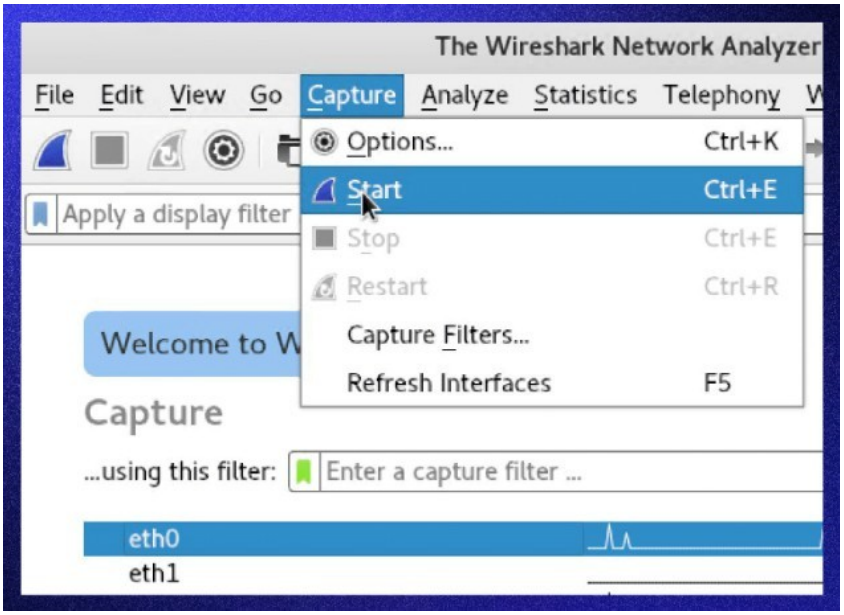


c. Once the network interface is selected, you can start the capture, and there are several ways to do that.
    i. Click the first button on the toolbar, titled "Start capturing packets."

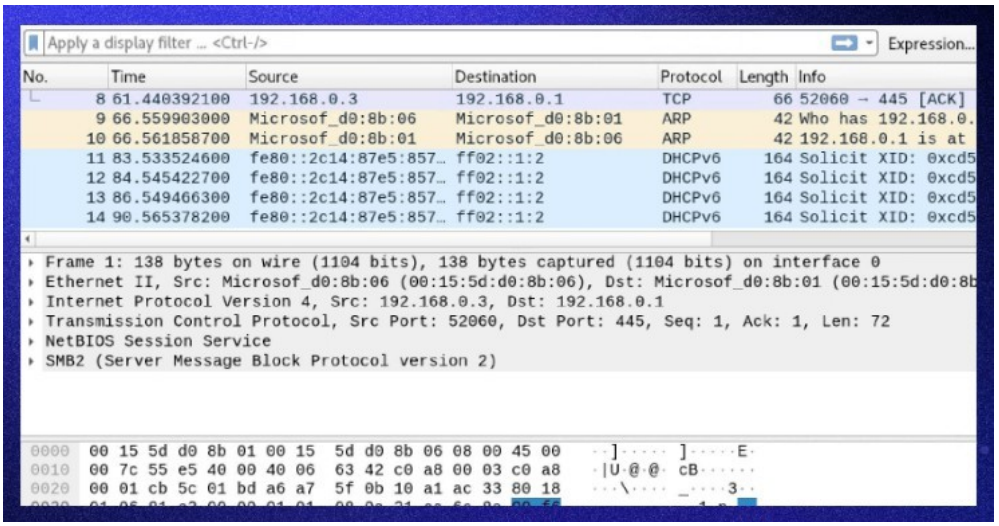


OR

you can select the menu item Capture-> Start



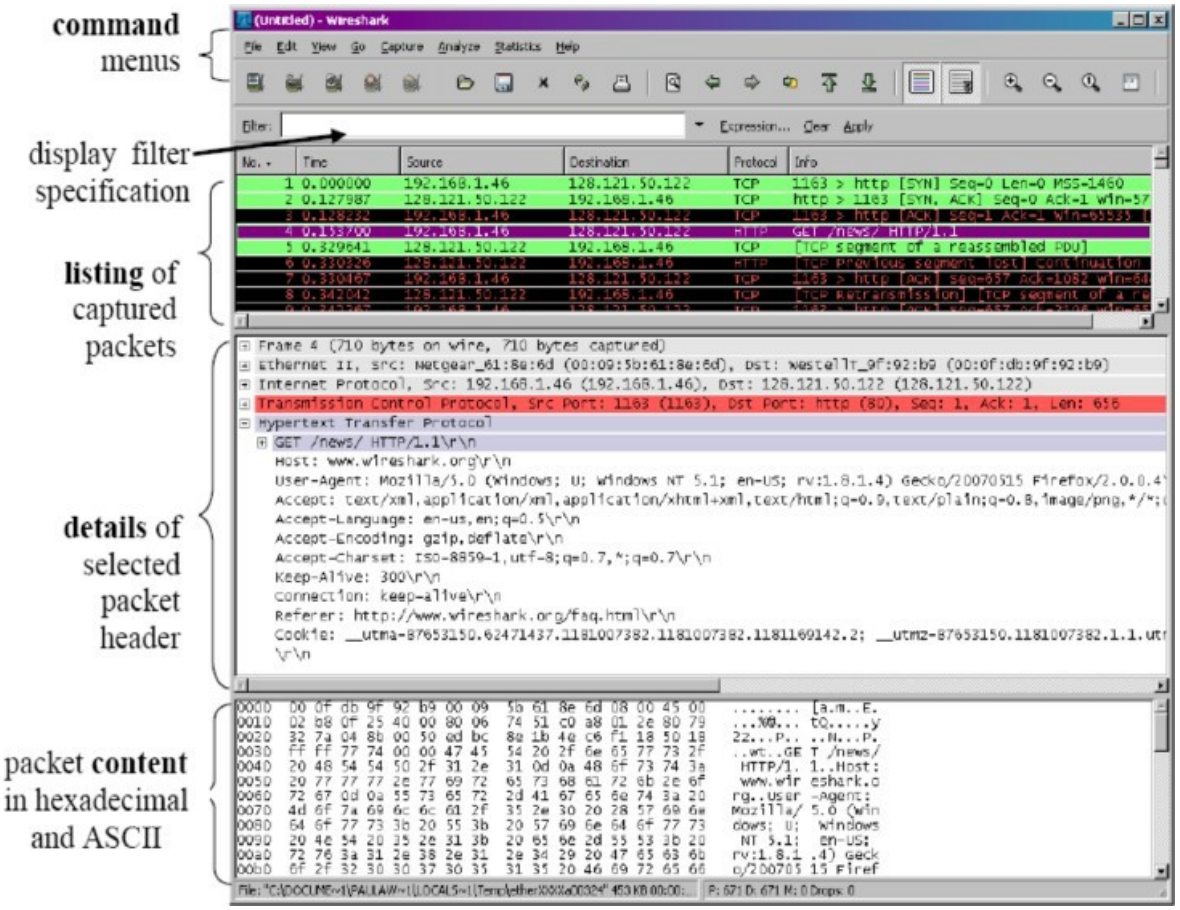
d. During the capture process, Wireshark will show the following screen



e. Once you have captured all the packets needed, use the same buttons or menu options to stop the capture as you did to begin.

Analyzing data packets on Wireshark: Wireshark Interface

Wireshark shows you three different panes for inspecting packet data. The Packet List, the top pane, lists all the packets in the capture. When you click on a packet, the other two panes change to show you the details about the selected packet. You can also tell if the packet is part of a conversation.



Here are details about each column in the top pane:

No.: This is the number order of the packet captured. The bracket indicates that this packet is part of a conversation.

Time: This column shows how long after you started the capture this particular packet was captured. You can change this value in the Settings menu to display a different option.

Source: This is the address of the system that sent the packet.

Destination: This is the address of the packet destination.

Protocol: This is the type of packet. For example: TCP, DNS, DHCPv6, or ARP.

Length: This column shows you the packet's length, measured in bytes.

Info: This column shows you more information about the packet contents, which will vary

depending on the type of packet.

Packet Details, the middle pane, shows you information about the packet depending on the packet type. You can right-click and create filters based on the highlighted text in this field.

The bottom pane, Packet Bytes, displays the packet exactly as it was captured in hexadecimal. When looking at a packet that is part of a conversation, you can right-click the packet and select Follow to see only the packets that are part of that conversation.

Wireshark filters

Filters allow you to view the capture the way you need to see it to troubleshoot the issues at hand. Below are several filters.

Wireshark capture filters

Capture filters limit the captured packets by the chosen filter. If the packets don't match the filter, Wireshark won't save them. Examples of capture filters include:

a. host IP-*address*: This filter limits the captured traffic to and from the IP address
b. net 192.168.0.0/24: This filter captures all traffic on the subnet
c. dst host IP-*address*: Capture packets sent to the specified host
d. port 53: Capture traffic on port 53 only
e. port not 53 and not arp: Capture all traffic except DNS and ARP traffic

Wireshark display filters

Wireshark display filters change the view of the capture during analysis. After you've stopped the packet capture, use display filters to narrow down the packets in the Packet List to troubleshoot

your issue.

a. ip.src==*IP-address* and ip.dst==*IP-address* This filter shows packets sent from one computer (ip.src) to another (ip.dst). You can also use ip.addr to show packets to and from that IP.

b. tcp.port eq 25: This filter will show you all traffic on port 25, which is usually SMTP traffic

c. icmp: This filter will show you only ICMP traffic in the capture, most likely they are pings

d. ip.addr != *IP_address*: This filter shows you all traffic except the traffic to or from the specified computer