CAPTURING AND ANALYSING PACKETS USING WIRESHARK TOOL

To filter, capture, view, packets in Wireshark Tool.

Capture 100 packets from the Ethernet: IEEE 802.3 LAN Interface and save it.

Procedure

> Select Local Area Connection in Wireshark.
> Go to capture ⬚ option
> Select stop capture automatically after 100 packets.
> Then click Start capture.
> Save the packets.

1. Create a Filter to display only TCP/UDP packets, inspect the packets and provide

the flow graph

Procedure

> Select Local Area Connection in Wireshark.
> Go to capture ⬚ option
> Select stop capture automatically after 100 packets.
> Then click Start capture.
> Search TCP packets in search bar.
> To see flow graph click Statistics Flow graph.
> Save the packets.

2. Create a Filter to display only ARP packets and inspect the packets.

Procedure

> Go to capture option
> Select stop capture automatically after 100 packets.
> Then click Start capture.
> Search ARP packets in search bar.
> Save the packets.

3. Create a Filter to display only DNS packets and provide the flow graph.

Procedure

> Go to capture option
> Select stop capture automatically after 100 packets.
> Then click Start capture.
> Search DNS packets in search bar.
> To see flow graph click Statistics Flow graph.
> Save the packets.

4. Create a Filter to display only HTTP packets and inspect the packets

Procedure

> Select Local Area Connection in Wireshark.

> Go to capture option
> Select stop capture automatically after 100 packets.
> Then click Start capture.
> Search HTTP packets in search bar.
> Save the packets.

5. Create a Filter to display only IP/ICMP packets and inspect the packets.

Procedure

> Select Local Area Connection in Wireshark.
> Go to capture ⬚ option
> Select stop capture automatically after 100 packets.
> Then click Start capture.
> Search ICMP/IP packets in search bar.
> save the packets

6. Create a Filter to display only DHCP packets and inspect the packets.

Procedure

> Select Local Area Connection in Wireshark.
> Go to capture ⬚ option
> Select stop capture automatically after 100 packets.
> Then click Start capture.
> Search DHCP packets in search bar.
> Save the packets