17.4.25 5. capturing and analysing packets with wireshark

Aim To perform experiments on packet capture tool wireshark.

packet sniffer

* Sniffs messages being sent / received from pc
* passive program
  → never sends packet in to packet

Tool

wire shark.

Description

wireshark a network analysis Tool formerly known as Ethereal, capture packets in real time.

Uses

* Network administrators
* network Security Engineers
* Developers : debug protocol
* people learn network protocol internals

Packet list pane

packet list pane displays all packets in current capture file, corresponds to one packet in capture file.

Packet details pane.

packet detail pane shows current packet in pane shows protocol fields and protocol of packet selected in packet list pane.

packet Bytes pane

packet bytes pane shows data of the current packet selected in the packet list pane in a Hexdump style.

Color coding

You will see probably highlighted packets in a variety of different colors. Wireshark uses color help you identify the types of traffic at glance. By default, light purple is TCP traffic, light blue is UDP traffic

filtering packets

If you are trying to inspect something specific, such as traffic a program sends color phase is done. still you will likely a large amount of packets to sift through.

Capturing and analysing packets

Procedure

1) select local area connection in wire shark

a) Go to capture → option.

3) Select stop capture after 10 packets

4) Then click Start Capture.

5) Save packets.

1. Create filter to display by TCP/UDP packets, unspect packets.

→ Select LAN in wireshark
→ Go to capture → option
→ select stop capture
→ Search Tcp packets in Search
→ To see flow graph.

Check statistics → flow graph.
→ save packets.

Procedure

→ select LAN in wireshark
→ Go to capture → option
→ select Tcp packets in Search fo
→ To see flow graph.
→ save packets.

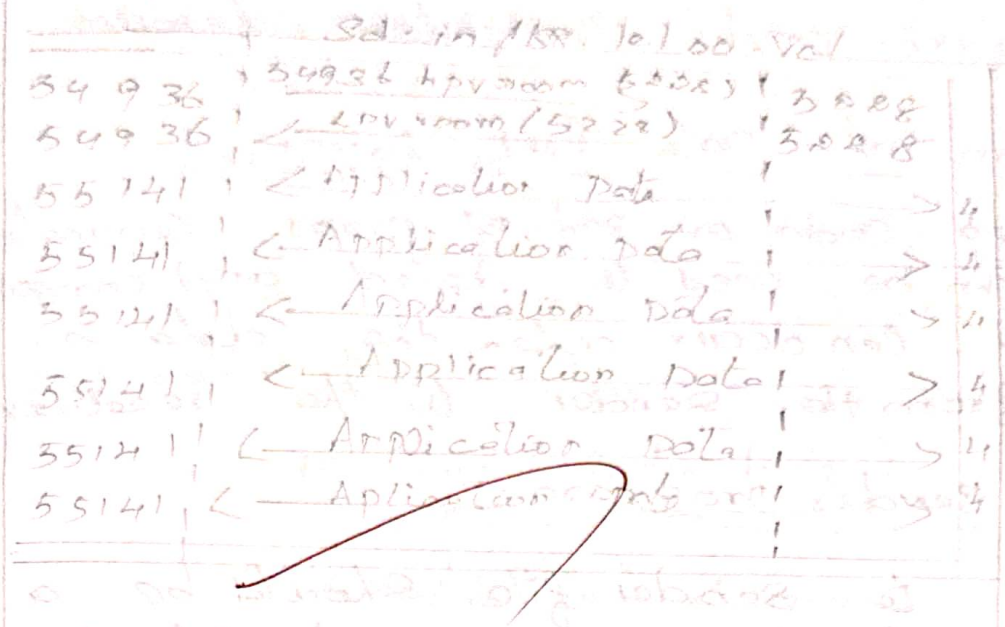
2) create a filter to display only ARP packets inspect.

Procedure

→ go to capture → option
→ select stop capture Auto for 100 packet
Then stop capture and search ARP packets and save.

Output

flow graph



Result.

Thus wireshark tool is used to handle and inspect packets.

14/X 8/20