Description:

Wireshark Network Analysis Tool formely known as Ethereal Capture packets in Real time & Display wireless traffic & Inspect Individual packets

What we conduct wire shark.

→ Capture network traffic
→ Declare packets protal directly.
→ Analyse property.

Wire shark used for:

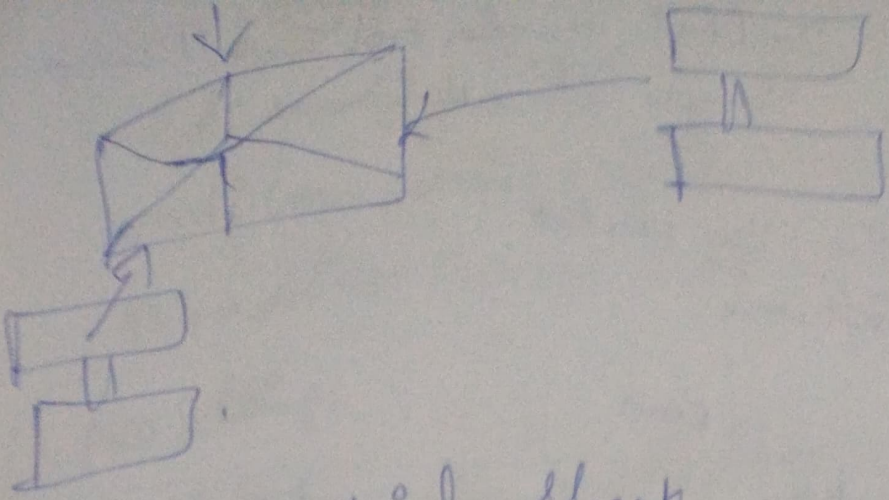
→ Network administrator trouble shoot Network problems.
→ people learns Network protocol.
→ Develop Debug protocol implement.

Getting wire shark:

Wire shark downloaded window across formits official websites unit or another Unilize system wireshark tshark package Responsibilites.

The packet list pane:

packet list pane Display all packets



Wide Shark

Aim: Experiment packet capture tools wireshark.

Packet Shiffer:

Shifter message being intercepted formely your Computer.

Store & Display Contet the various potential message.

Passive program:

→ Never send packet itself.

→ No packet address tool

→ passive copy all packet.

Packet Sniper Structe program Tcpredump

→ E. ptempdump ext flog 10.129.4.10

Wireshap - rexe 3-out.

Current Capture file. packet list pane each like corresponding packet Capture file.

Packet Details pane:

Packet Details pane shows the current packet more detailed fuction pane shows protocol packet selected packet list.

Packet Byte pane:

Packet byte Data Corresponding Packet hexdump style.

+ Sample Captures
+ Tokenizing packets.

2/19/24

6- Hamming Code.

Receiver.py:

```
def calc_parity_position(m):
    r=0
```