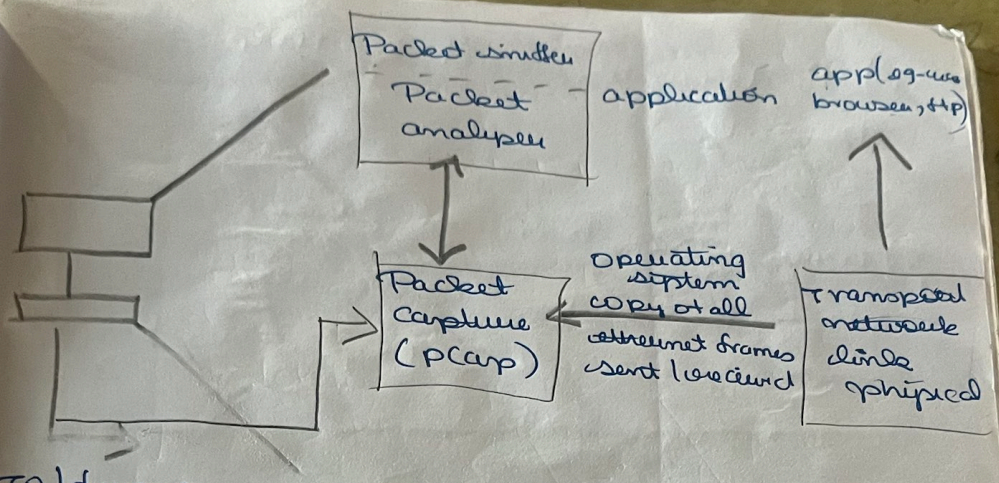
Exp No: 5 Wireshark
Date: 9.8.24

AIM: Experiment on packet capture tool: Wireshark.

Packet sniffer
- Sniff message being sent/received from/by computer
- Stores & display content of various protocol
- passive programs
  - → never send packet itself
  - → no packet addressed to it
  - → receive a copy of all packets

Packet sniffer structure diagonistic tools
- Tcpdump
  - eg: tcpdump -enx host 10.129.41.2 -w exe 3.out
- wireshark
  - wireshark - exe 3.out



Wireshark

→ network analysis tool

→ formerly known as ethereal

→ capture packets in real time & display in human readable form

→ include formats, filters, color coding etc

Uses

→ troubleshoot

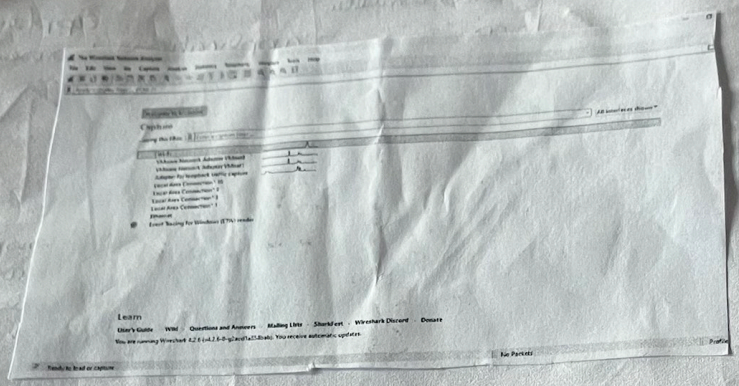
→ examine security problems

Download wireshark

→ download & install from www.wireshark.org

Capturing packets

→ Launch wireshark & double click on name of network interface



Colouring rules

* colours have been assigned for each packets view → colouring rules

Filtering Packets

* display orderly

→ type into filter box at top of window & clicking apply.

TCP conversation

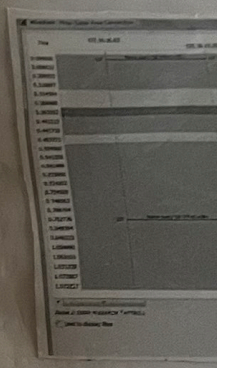
→ right click on a packet → follow → TCP stream

Inspect Packet

→ click a packet to view details of packet dig down

Flowgraph:

→ network



Student Obse

1) what is

A net

allows it

network

for it

2) Does

header?

No, A

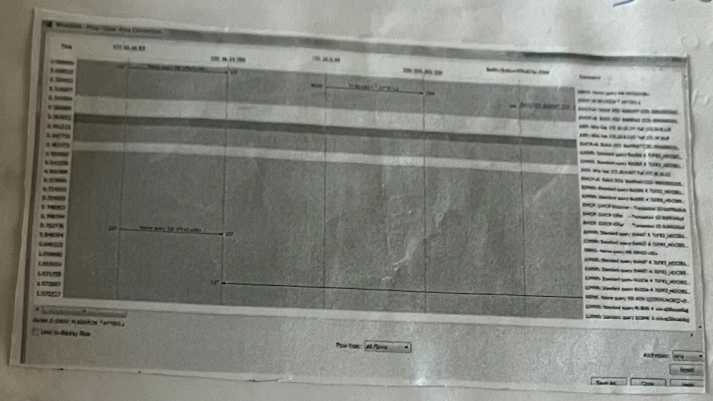
layer

3) Which

by o

Flowgraph:

→ network interface → statistics → flow graph



Student Observation:

1) What is promiscious mode?

A network interface card mode that allows it to capture all traffic on network not just the traffic intended for it own mac address.

2) Does ARP packets has transport layer header? explain.

No, ARP packets do not have transport layer header.

3) Which transport layer protocol is used by ON?

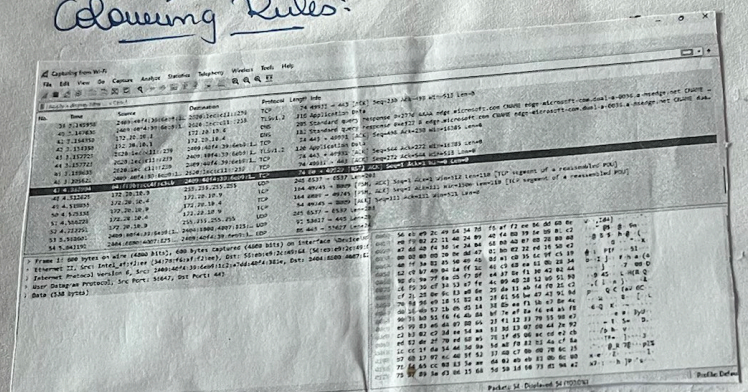
→ UDP (user datagram Protocol)

4) Port number used by HTTP protocol

→ 80

5) what is a broadcast IP address ? used to send data to all devices on a network. for IPV4 it is highest address in a subnet.

Observing Rules:



Result: 9/8/24

Thus the packet captivating tool wireshark is installed & studied

Ex.NO:

Date:

Aim: Write a
error detection
code. Make a
stream and

Error Correction

Hamming code is
that can be
the errors
transmitted
a technique
Correction

Create sender

→ Input to
length. Re
to binary

→ Apply h
and add

→ Save