Ex.no: 5
09/08/24

Practical 5

Aim:

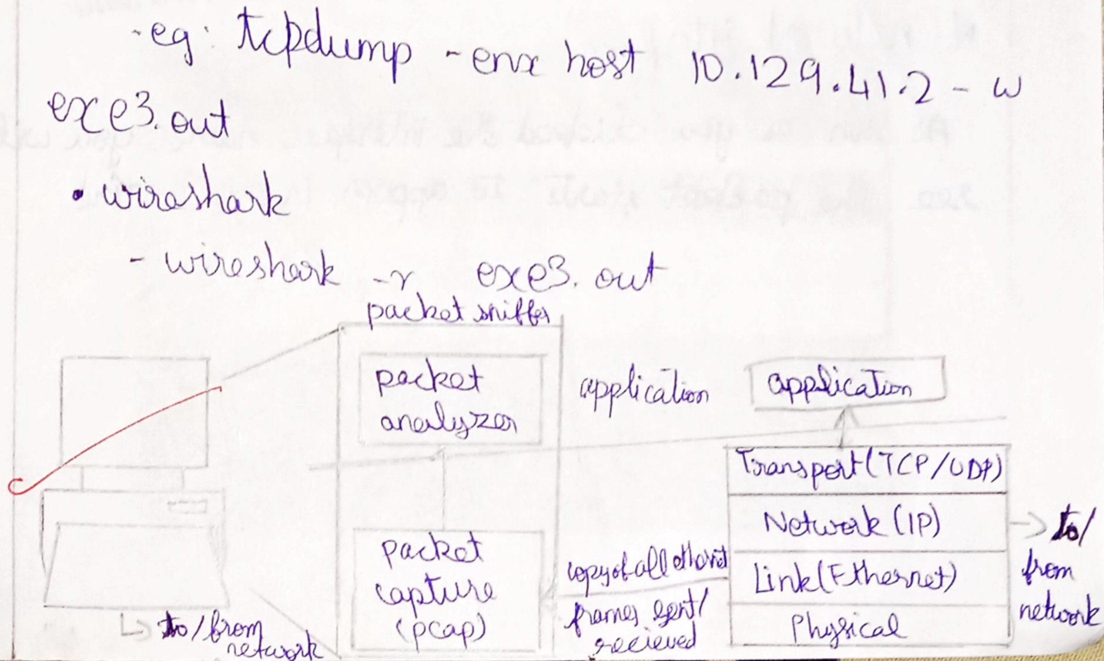
Experiment on Packet Capture tool : wireshark

Packet Sniffer

- Sniff message being sent/recieved from/by computer.
- Stores & Display content of various protocol
- Passive Program
  * never send packet itself
  * no packet addressed to it
  * recieved a copy of all packet

Packet Sniffer Structure Diagonostic Tools

- Tcpdump
  - eg: tcpdump -enx host 10.129.41.2 -w exe3.out
- wireshark
  - wireshark -r exe3.out



WireShark

- network analysis tool
- formerly known as Ethernet
- Capture packet in real-time & display in human readable form
- Include formats, filter, color coding, etc

Uses

- ~~Thro~~ Troubleshoot
- Examine security problems

Download WireShark

- download & install from www.wireshark.org

Capturing Packet

- Launch wireshark & double click on name of network interface.

As soon as you clicked the interface name, you will see the packet starts to appear in real-time

Colorcoding rules

Colours have been assigned for each packets ~~views~~

→ View → Coloring Rules

Filtering Packets

- Display orderly

→ type into filter box at top of window + clicking apply

TCP Conversation

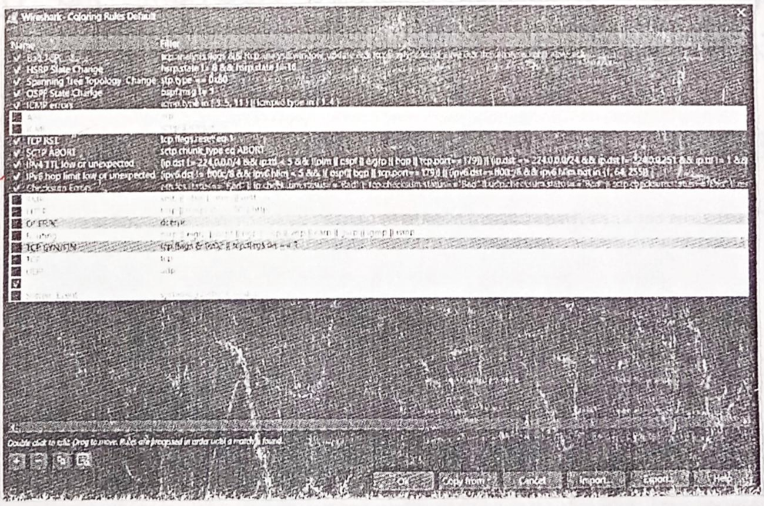
→~~B~~right click on a packet → follow → TCP stream

Inspect Packet

→ Click a packet to view details of packet + dig down

Flowgraph

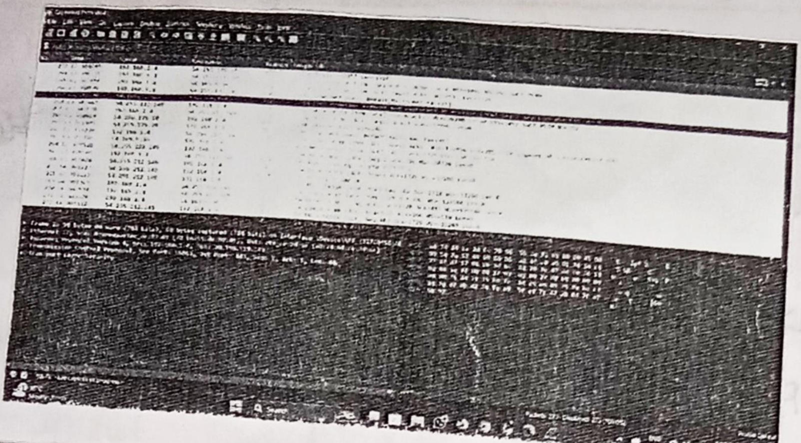
→ network interface → Statistics → Flow graph

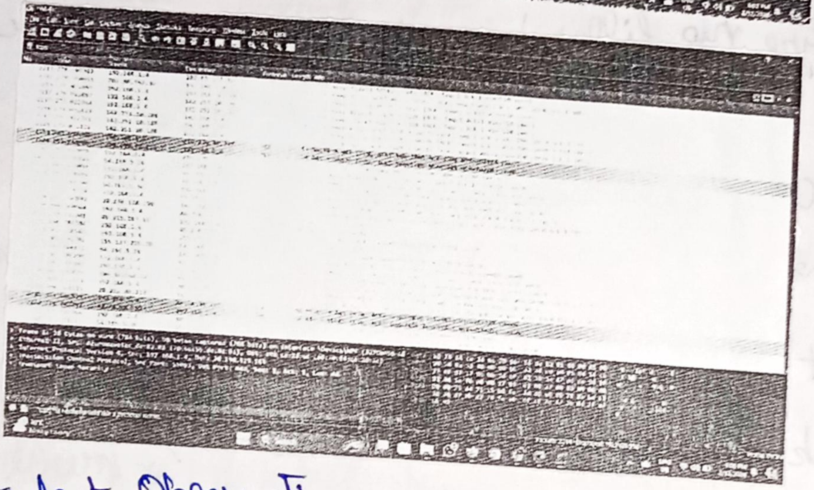


Wireshark · Coloring Rules Default

Name	Filter
✓ Bad TCP	tcp.analysis.flags && !tcp.analysis.window_update && [illegible]
✓ HSRP State Change	hsrp.state != 8 && hsrp.state != 16
✓ Spanning Tree Topology Change	stp.type == 0x80
✓ OSPF State Change	ospf.msg != 1
✓ ICMP errors	icmp.type in { 3..5, 11 } || icmpv6.type in { 1..4 }
ARP	arp
ICMP	icmp || icmpv6
✓ TCP RST	tcp.flags.reset eq 1
✓ SCTP ABORT	sctp.chunk_type eq ABORT
✓ IPv4 TTL low or unexpected	(ip.dst != 224.0.0.0/4 && ip.ttl < 5 && !(pim || ospf || eigrp || bgp || tcp.port==179)) || (ip.dst == 224.0.0.0/24 && ip.dst != 224.0.0.251 && ip.ttl != 1 &&
✓ IPv6 hop limit low or unexpected	(ipv6.dst != ff00::/8 && ipv6.hlim < 5 && !(ospf|| bgp || tcp.port==179)) || (ipv6.dst==ff00::/8 && ipv6.hlim not in {1, 64, 255})
✓ Checksum Errors	eth.fcs.status=="Bad" || ip.checksum.status=="Bad" || tcp.checksum.status=="Bad" || udp.checksum.status=="Bad" || sctp.checksum.status=="Bad" || [illegible]
SMB	smb || nbss || nbns || netbios
HTTP	http || tcp.port == 80 || http2
DCERPC	dcerpc
Routing	hsrp || eigrp || ospf || bgp || cdp || vrrp || carp || gvrp || igmp || ismp
TCP SYN/FIN	tcp.flags & 0x02 || tcp.flags.fin == 1
TCP	tcp
UDP	udp
☑	
System Event	systemd_journal || sysdig

Double click to edit. Drag to move. Rules are processed in order until a match is found.





Student Observation

1) What is promiscous mode?

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

2) Does ARP packet has transport layer header? Explain?

No, ARP packets do not have transport layer header.

3) Which transport Layer protocol is used by DNS

- UDP (user datagrapm Protocol)

4) ~~10~~ Port number used by Http protocol?

80

5) What is a broadcast ip address

Used to ~~to~~ send data to all devices on a network. For IPv4, it is highest address in a subnet.

9/8/24

Result:

Thus the expriment on packet capture using wireshark is studied