Date: 9:8:24 Capture 6001: wire Shark

AIM!

Experiment on Packet capture tool: wire shark

## Packet Snitfer

- · Sniffs messages being sent/received from/by
  your computer
- Protocol field in the messages.
- · Passive Program
  - never sends Packets itself
  - no packets addressed to it
  - receives a copy of all Packets (Sent/received)

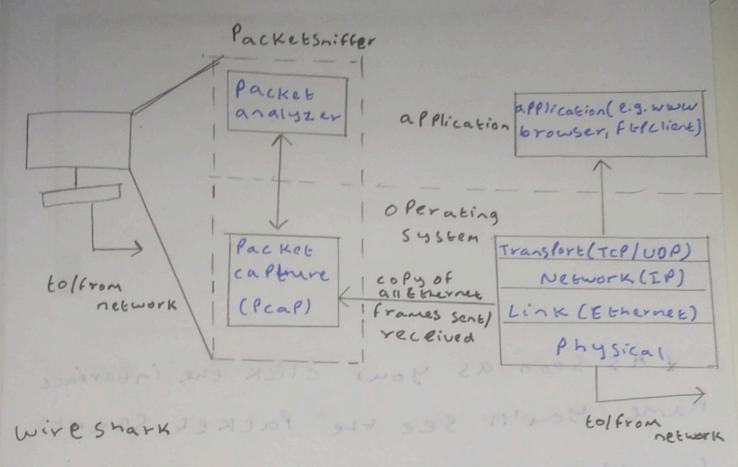
Packet Sniffer Structure Diagnostic Tools

· TCPdump

- 6.9. Ecpdamp -enx host 10.129.41.2-wexes,

· wires hark

- wire Shark - r exe3.out



- \* network analysis, tool
- \* formerly knows as Ethereal
- \* capture Packets in real time display in human readable born
- \* include bormais, bilter, color coding etc.

Download wire Shark

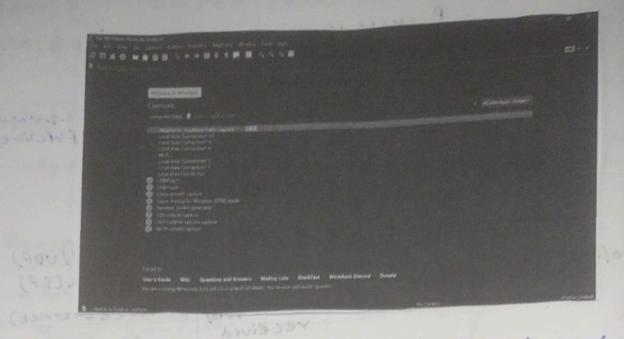
· download & install from www.wire Shark.org

Calturing Pockets

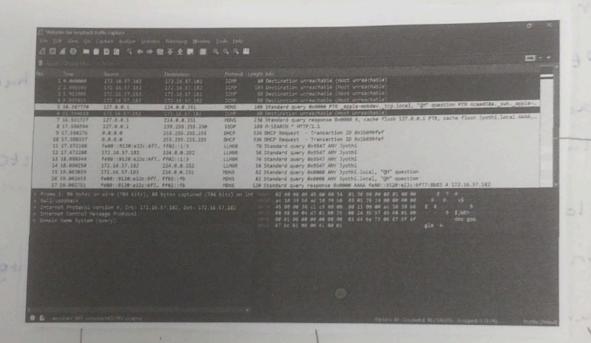
ne twork theerface. In a double click on name of

on graph

Es established ave



\* As soon as your click the interface name you'll see me lacker Starts to affear in red time to make the



Packet details Packet

Byte

li'st

Flow graph

> network interface >> Statistics -> blow graph

Treshark & , Asuble Click on, France of

		PLANTAGE STATEMENT STATEME		
				The Chinase American London Commission
				Contraction or Committee Stort over payer
				Coll Secretar constitute (from prescripting
				Tim Original Confederate State Association
			OCCUPANT DESCRIPTION	sales former and helpfully appropriate the
THE PERSON NAMED IN				A last Constitution (Completed Street Assessment
			CONTRACTOR OF THE PARTY OF THE	make the control and control and a control of
		HUMOSTATA	and the second second	SCHOOLSE SERVICE - MISSELF
				SAN SAN AGAIN STORES CO. CO.
				DATE DATE Report - Township of Street,
				Challe charles and course per John
				Commence of the Parish Street,
-				Writing (product) from grappy into chaps
				The spirit density and traffit the rate
	Spiritual and Section and Assessment Coll spiritual	3 200		report general intelligence on married all and
				Water designed their property and cheer have able about
				SACREC CONTRACTOR OF THE PARTY SACRED
-	AND THE RESIDENCE OF THE PARTY			DOME SHARP FORCE TOWNS THE OWN DATE (AND THE OWN)
				Change Schools are orders to a read
				The same terrator and pages on the
550				Laboration - sand train-1
	5.16 5.08 5.09	See that you have been a facilities and the second of the		See

Student observation.

1) what is Promiscous modely

A network Internet courd mode that allow it to capture an traffic allow it to capture an mace address intended for its own mace address

2) Dose ARP Packets has transport layer header? Explain

No ARP Packets do not have transfort

layer header

3. which transport layer rotocol
is used by DNS.

UDP (User data gram Proto Col)

4) Port number used by HTTP
Protocol

-> 80

S) what is a broadcast IP address user to send data to all device on a metwork or IPv4, Intis. nights a address in a subres.

A NEW WORK LANGE COUNT MODE PAGE

ON TELLED COUNTY AND FILE

LEGAL FOR THE COUNTY AND FORESE

cose ARP Packets has transport laser

AZP PACKETS de noue have bransper

yer heading

Result:

thus the Packet capturing too wire share is installed & Studied.