Aim:
Experiments on Packet capture kool
Wireshark del processo 1000
energy on the some law
Packet Sniffer
- Snills massages being sentlopeceived
- Sniffs massages being sent/received from/by your computer
- Store and display the contents of
the various protocol fields in
- Store and display the contents of the various protocol fields in the messages.
- Passive program
-> Non sends packets to itself
-> No packets addressed to it.
-> Receives a copy of all packets montagenes 97
Packet Sniffer Strutchure: Diagnostic Tools
. TCPdump sould was sold
· Wireshark
Packet sniffer
Packet application Application Analyzer application (Ex 1 20 12 brown)
Step dient) Flep dient)
Packet sure of states breaked breaked to
Capture 05
(pcap) copy all Ethernet Natwork (IP) frame sent (neceived Link (Ethern)
Physi cal
to/fnom retwork Lo/fnom retwork
Es/tnom

09/08/2024 Practical 5

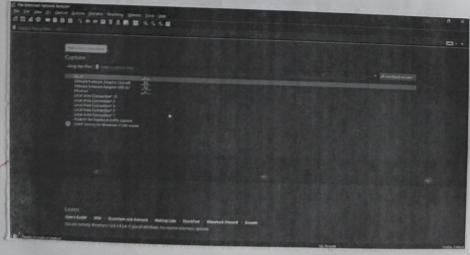
as Ethereal, captures packets in real time and display them in human-neadable format

What we can do?

- Capture network & traffic - Analyze problems
- Network admin: Trouble shoot network
- Develops: Debug protocol implementations Fillewig Padets

Capturing Packets

Lounch Wireshark and double-click the name of a network interface under Capture to start capturing packets on the interface.



Colour Coding

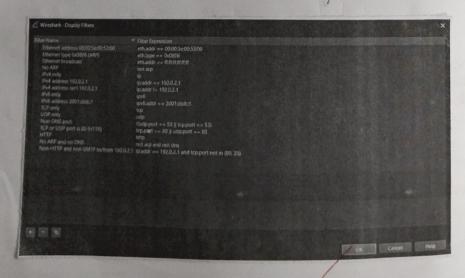
Wireshark uses colours to help you identify the types of traffic at a glance.

By at default, light pumple is TCP traffic, light blue is UDP traffic and black black identifies packets

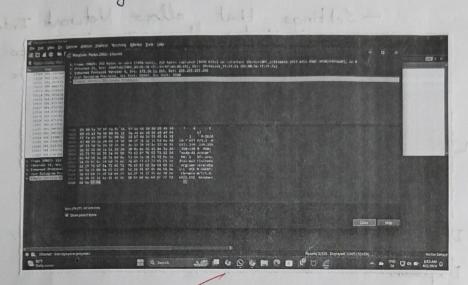


Filtering Packets

The most basic way to apply a filter is by typing it into the filter box at the top of the window and dicking apply.



Inspecting Packets Click a packet to select it and you can dig down to view its details.



No. The openale of dolo link layer

all by bear reduced the desperal of propered

5 what is a broadcast ip address?

Used to send a packet to all demices in the whoods regiment.

Wreshook took tras been experimented and packet transfer was been

Student Observation

1. What is promisions made in Wireshard?

- Settings that allow Network Interference Card that allows the device to capture all network-traffic on the segment it is connected to.

2. Which Enursport layer is used by DNS?

3. Does ARP packets has koransport leyear header?

No. The operate at data link layer and are used for mapping IP to MAC address

4. What is the port number used by http

5. What is a broadcast ip address?

Used to send a packet to all devices in the whork segment.

Result:

with and packet transfer has been experimented studied studied.