DOMS | Page No.
Date / /

practical - 5

Aim: Experiments on packet capture tool: wireshark.

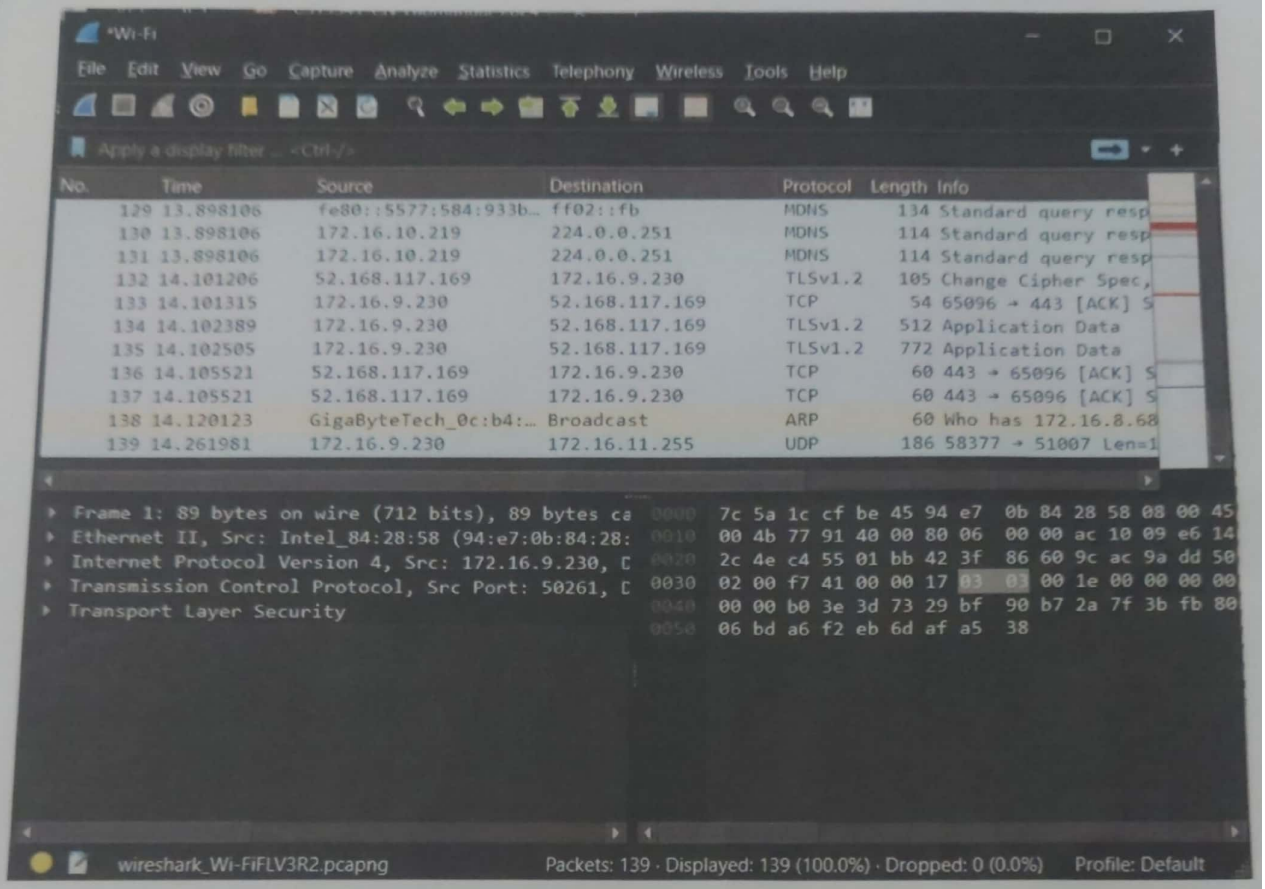
packet sniffer.

* Sniffs messages being sent/received from/by your computer.
* Store and display the contents of the various protocol fields in the messages.
* passive program.
  - never sends packets itself.
  - no packets addressed to it
  - receives a copy of all packets (sent/received).

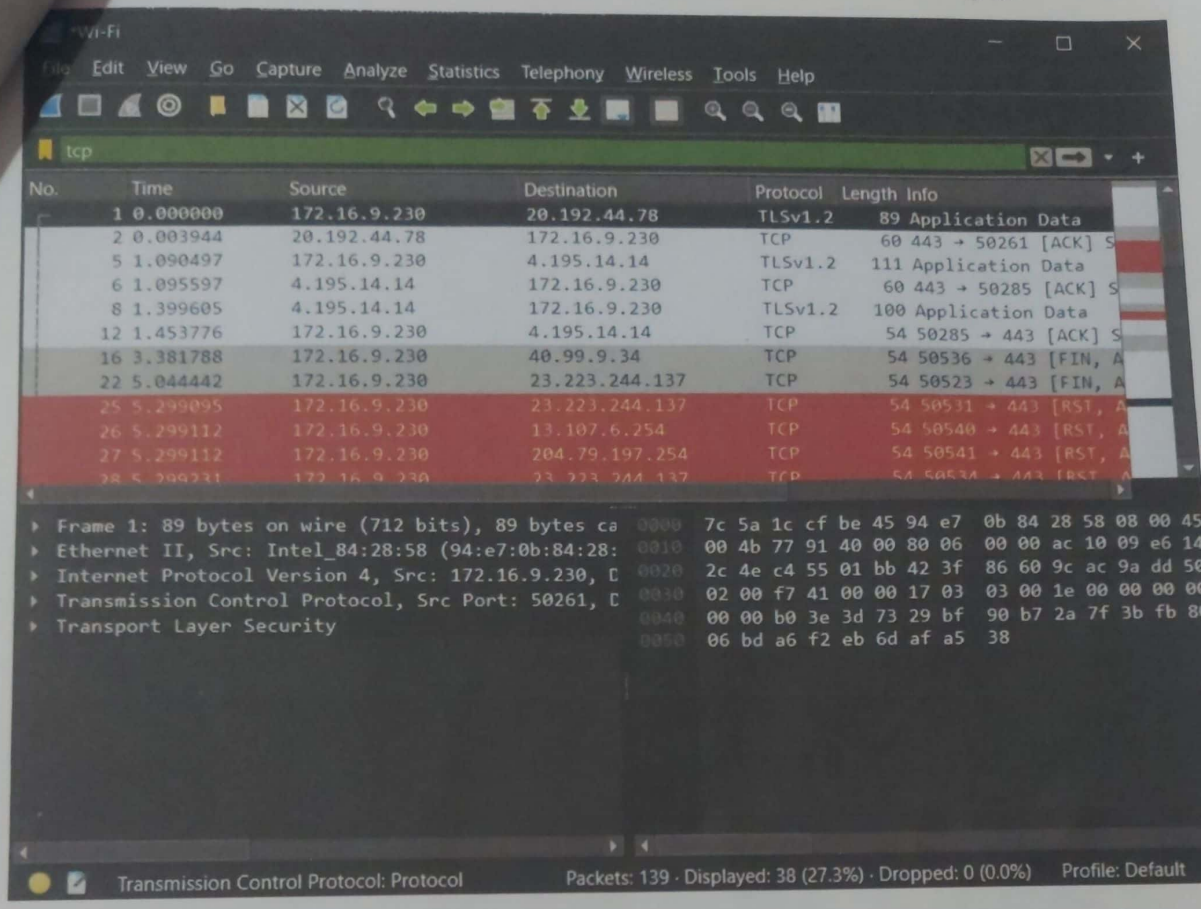
Packet Sniffer Structure Diagnostic tools

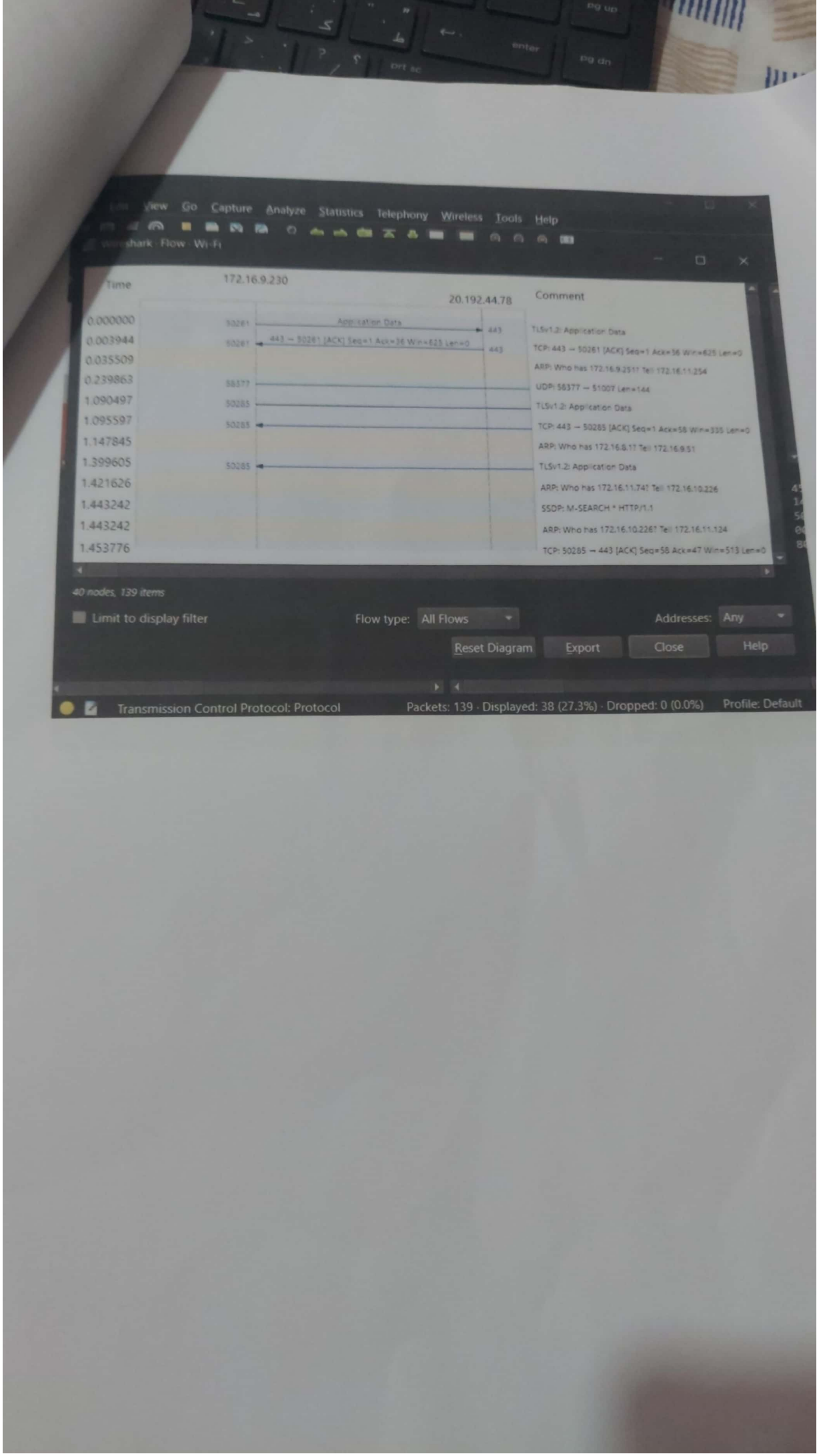
* Tcp dump.
  - Eg: tcpdump -enx host 10.129.41.2 -w exe3.out.
* wireshark.
  - wireshark -r exe3.out.

CAPTURING AND ANALYSING PACKETS USING WIRESHARK TOOL

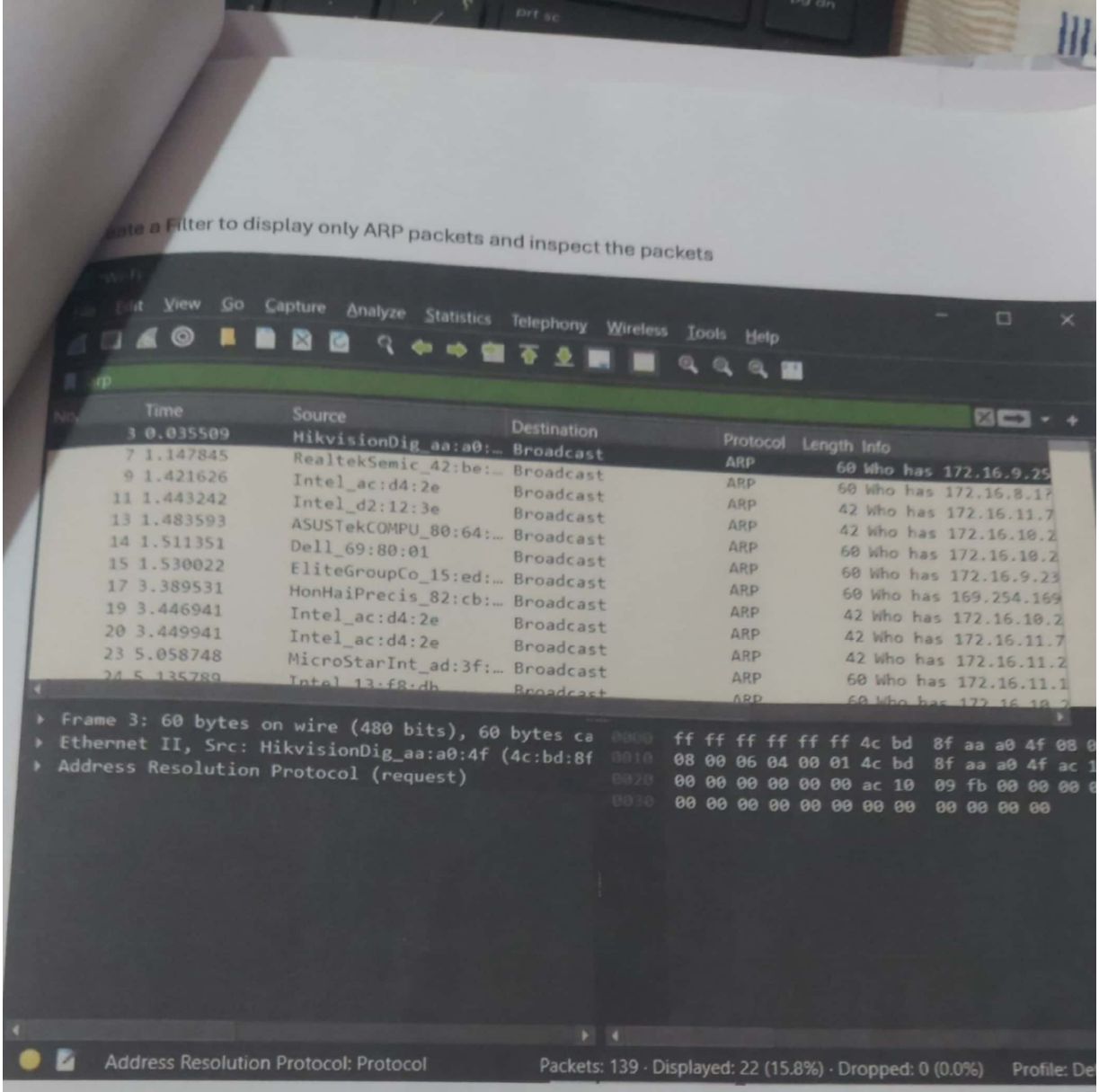


eate a Filter to display only TCP/UDP packets, inspect the packets and provide the flow graph

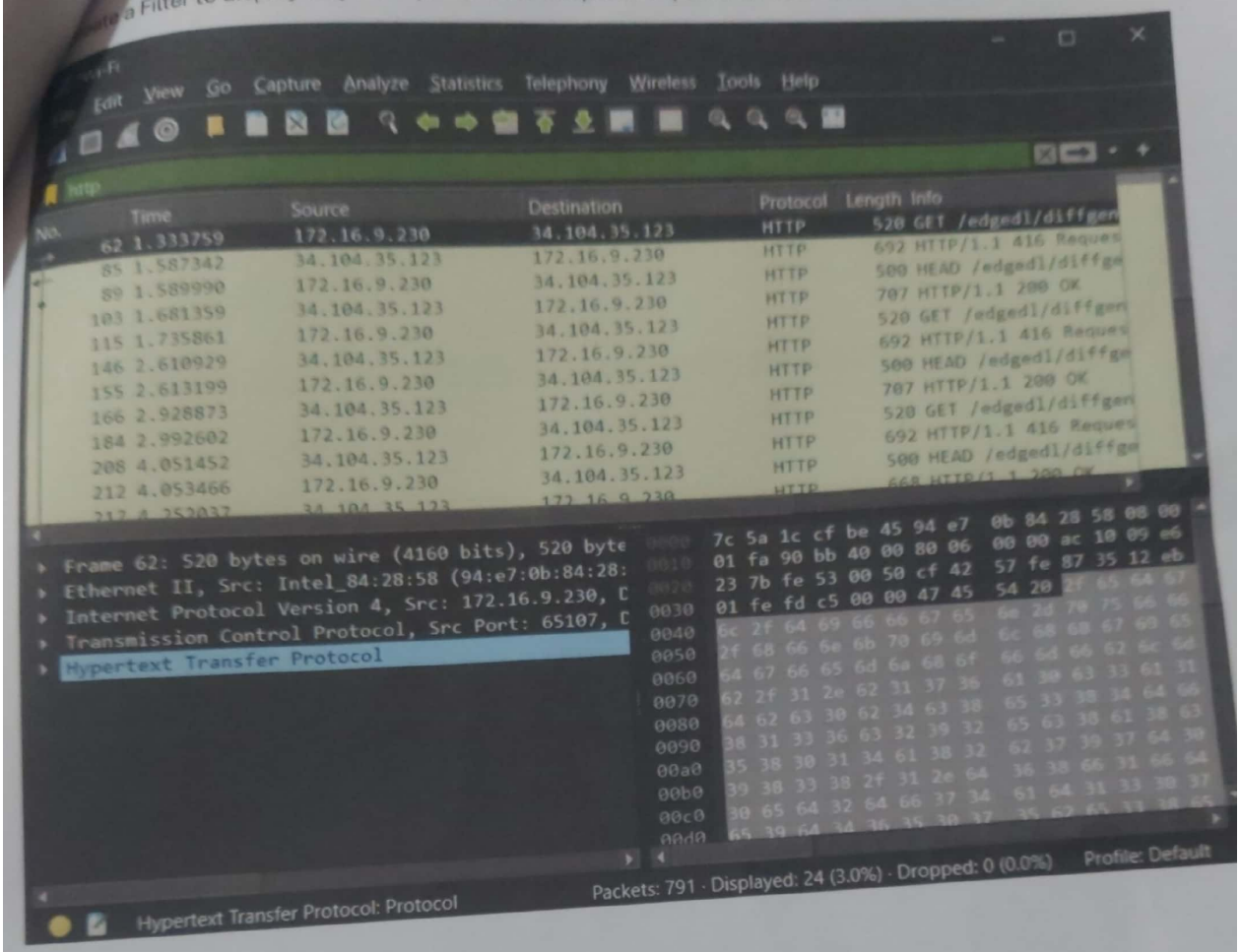




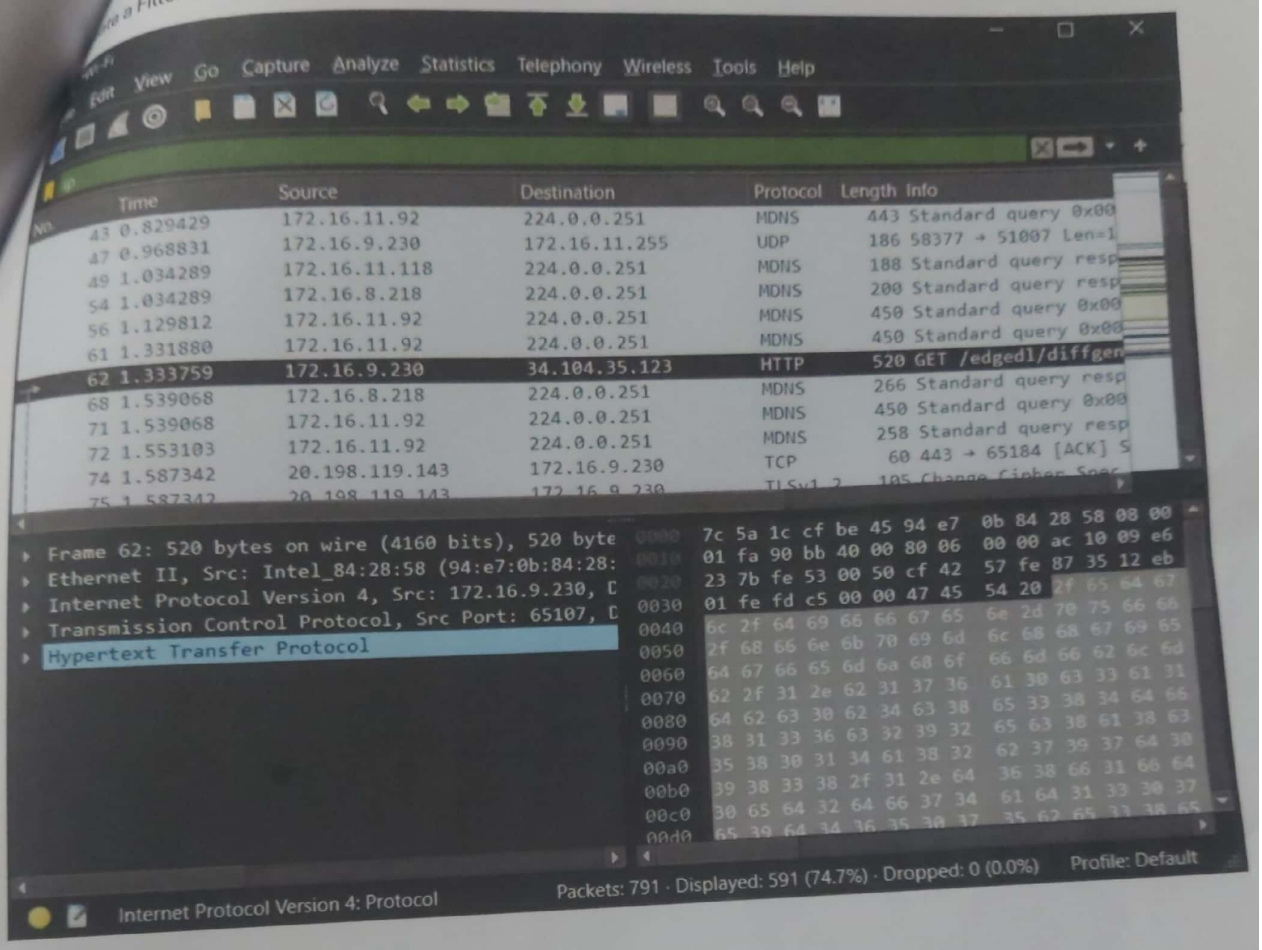
ate a Filter to display only ARP packets and inspect the packets



...a Filter to display only HTTP packets and inspect the packets Procedure.



...e a Filter to display only IP/ICMP packets and inspect the packets.



Result:

Thus the experiment is successfully executed and output is verified

17/8/24