**CYBER SECURITY LAB 3**

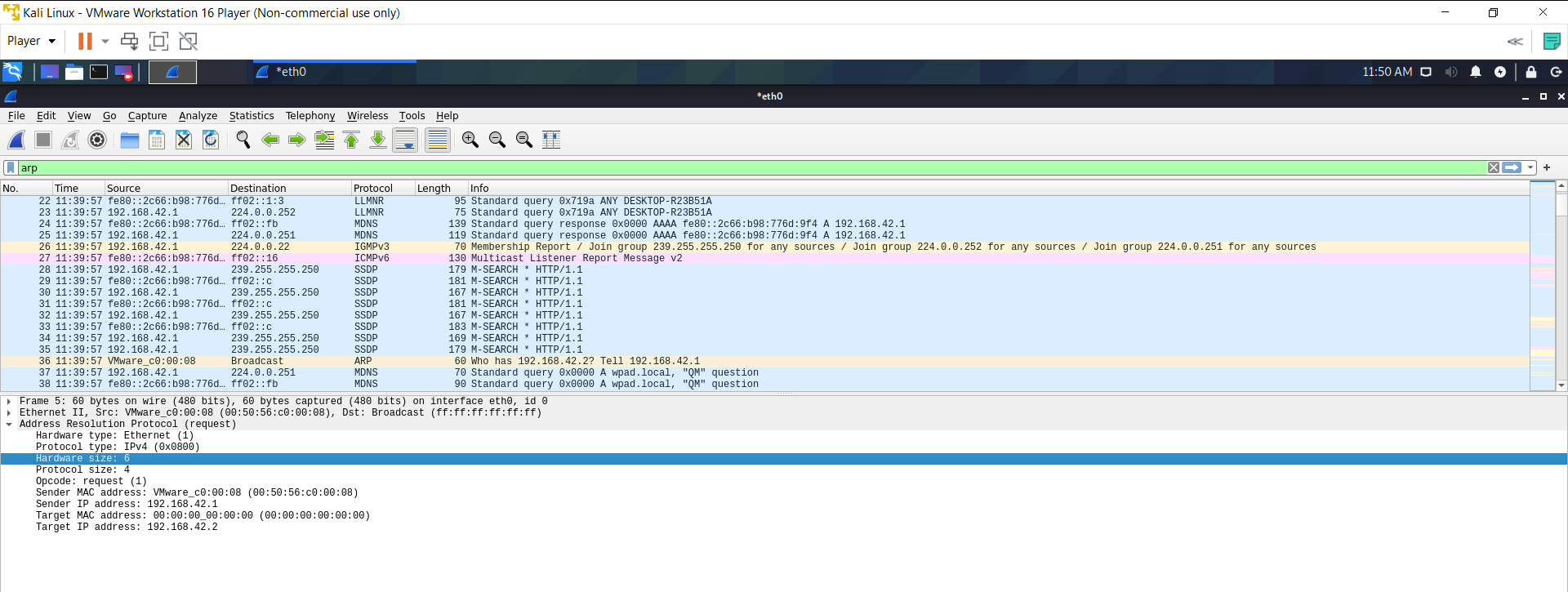
**WIRESHARK COMMANDS**

**NAME : SREENIDHI GANACHARI**

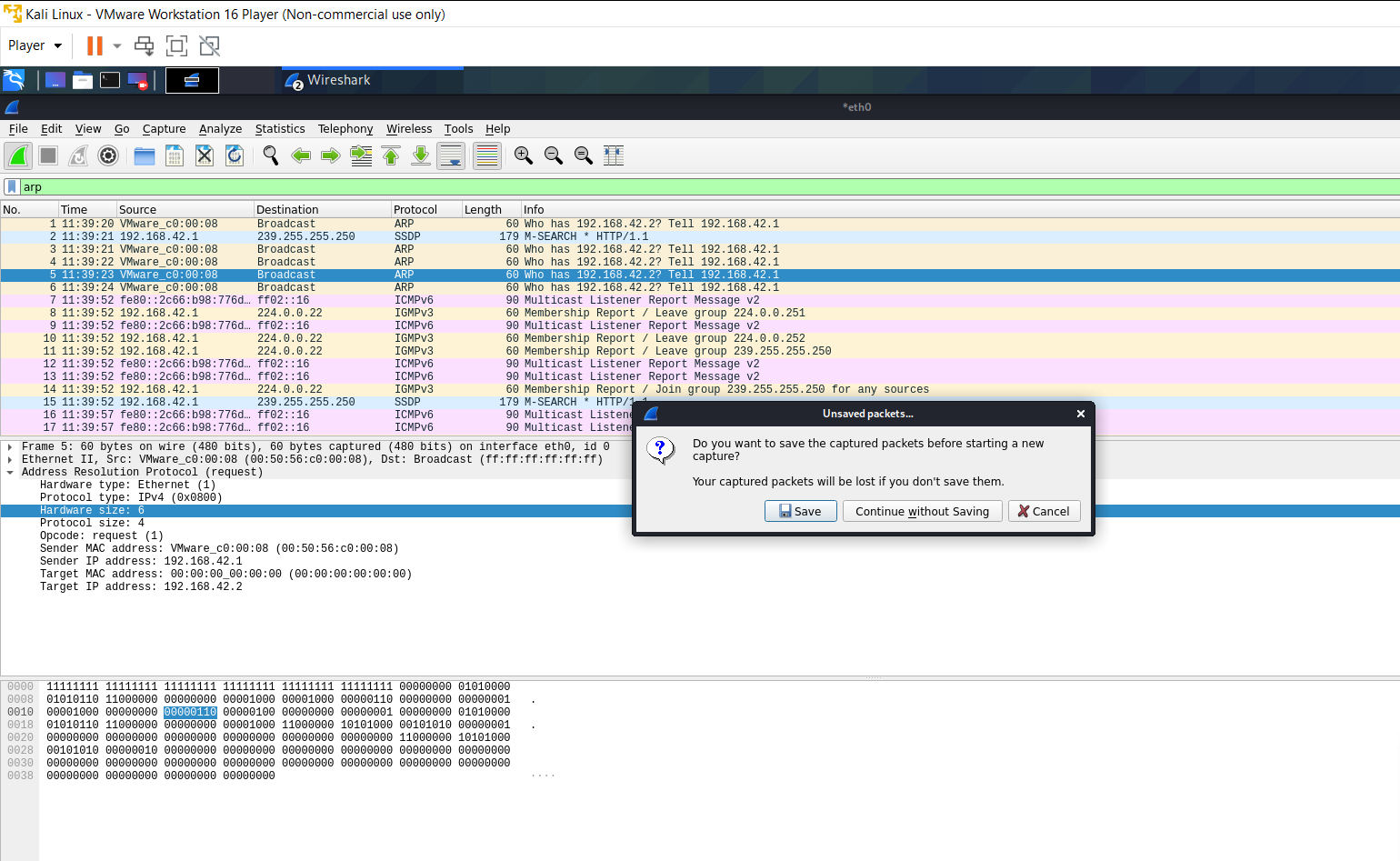
**REGISTRATION NUMBER : 19BCE7230**

Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education. Wireshark lets the user put network interface controllers into promiscuous mode (if supported by the network interface controller), so they can see all the traffic visible on that interface including unicast traffic not sent to that network interface controller's MAC address. However, when capturing with a packet analyzer in promiscuous mode on a port on a network switch, not all traffic through the switch is necessarily sent to the port where the capture is done, so capturing in promiscuous mode is not necessarily sufficient to see all network traffic.

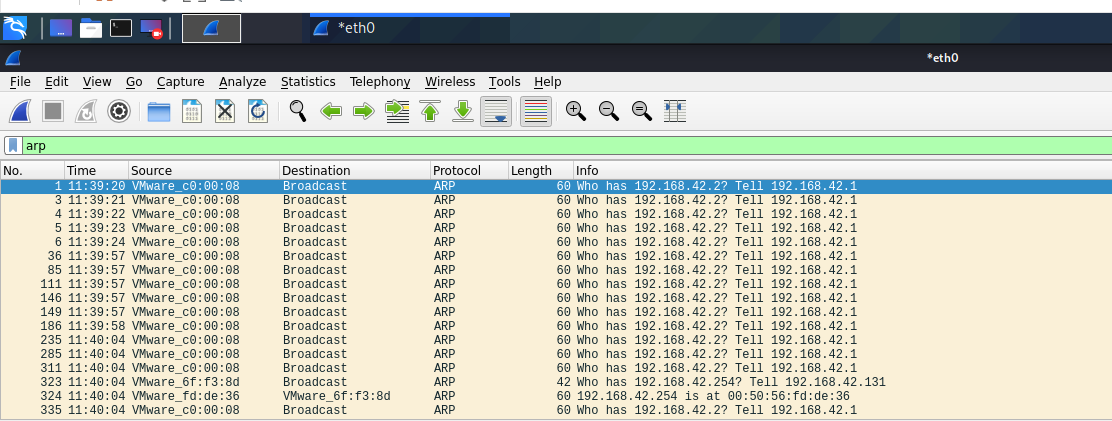
1) The captured packets are visible when we run “**Start Capturing packets**”



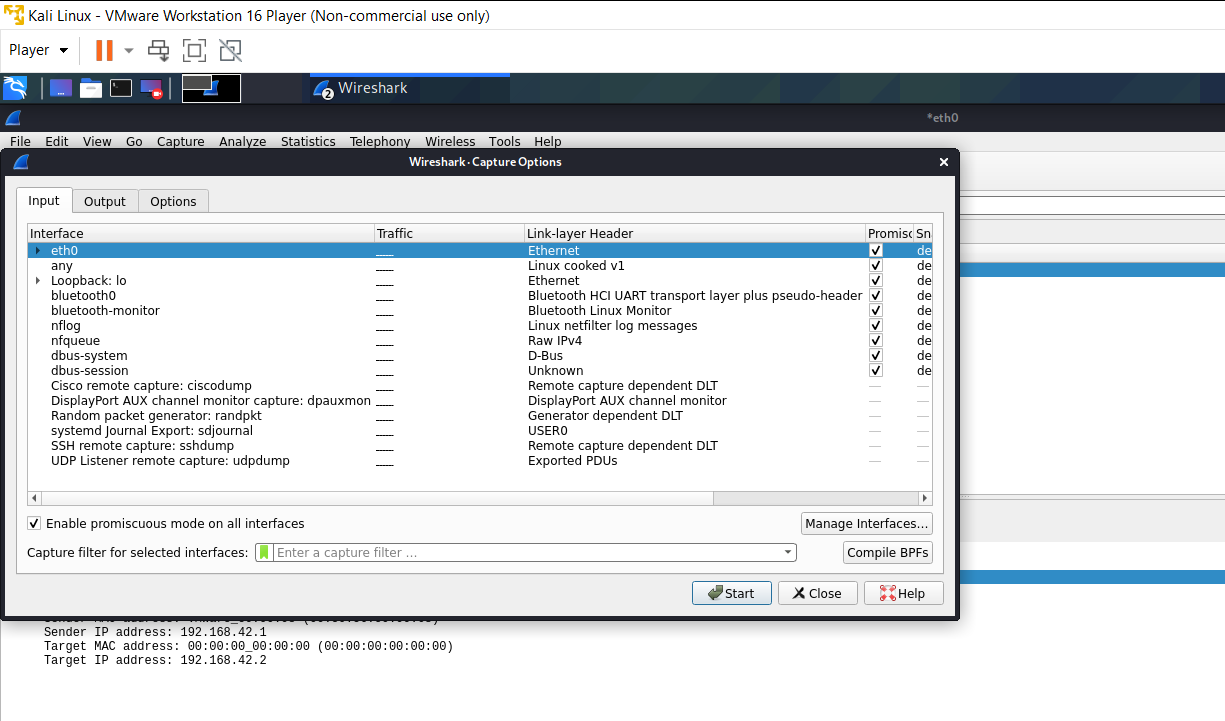
2) We can **save the packets** captured in the shown way



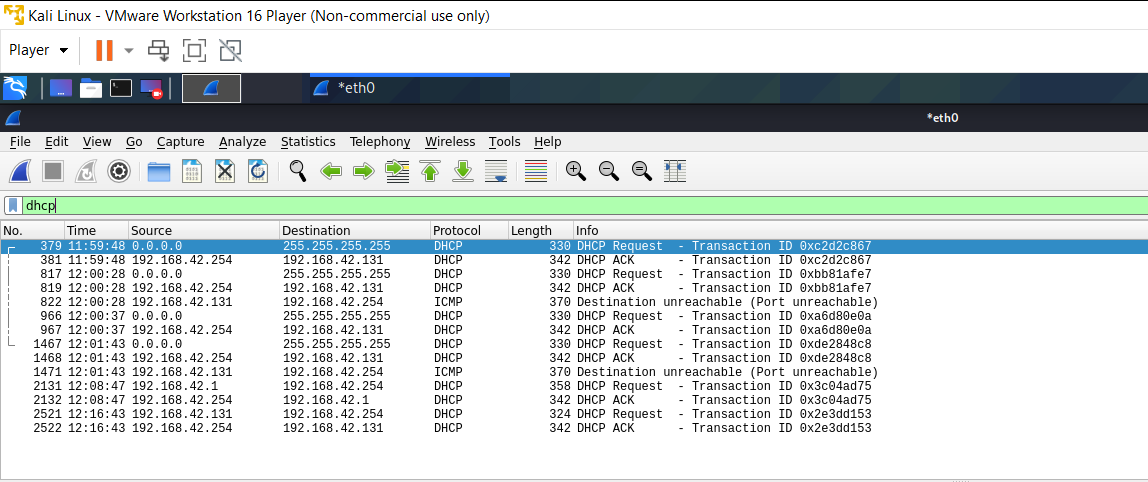
3) We can view the required protocol captured packets by searching for them - **ARP**



4) This shows the **Wireshark capture options**



5) **DHCP**



6) **UDP**

