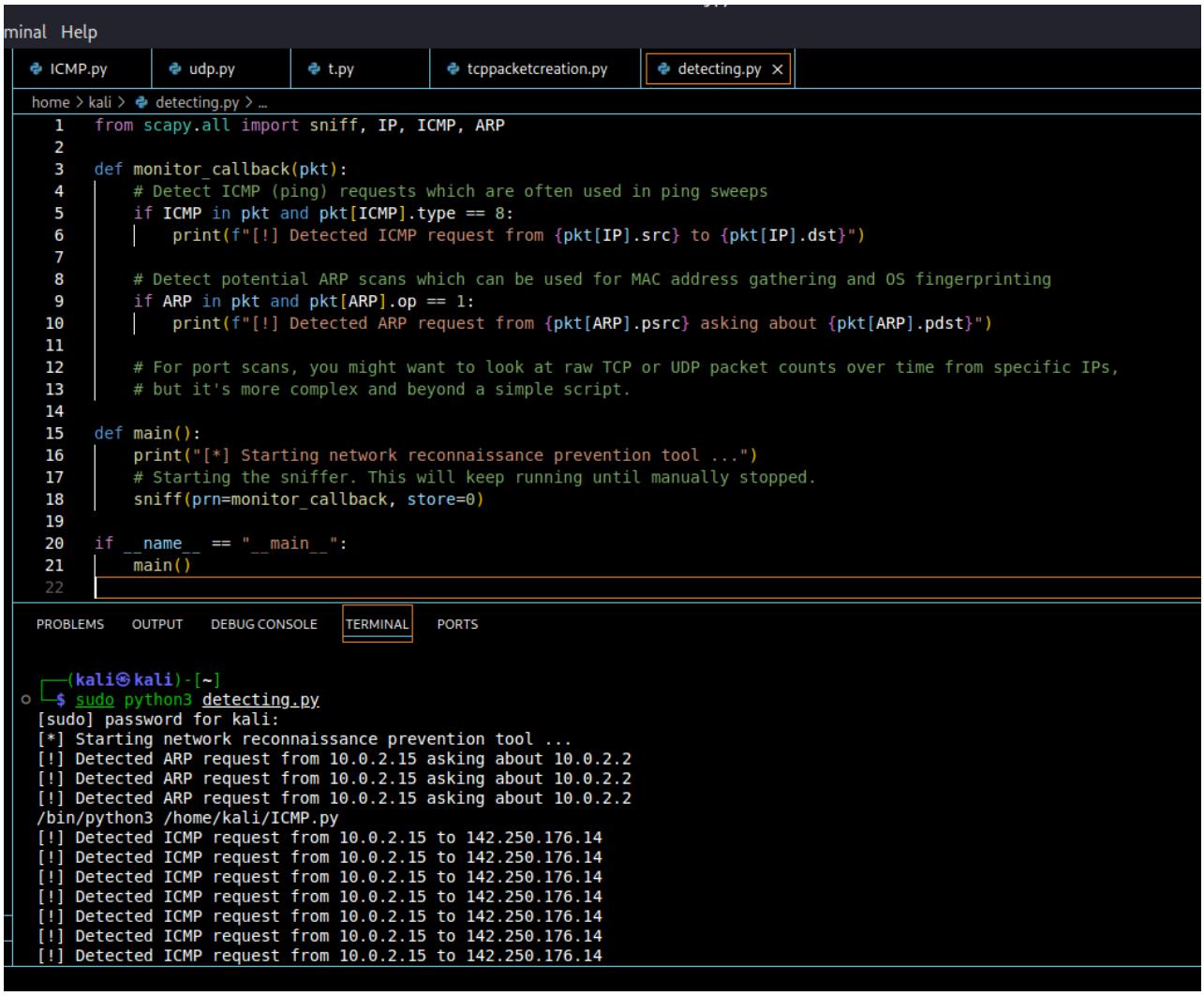
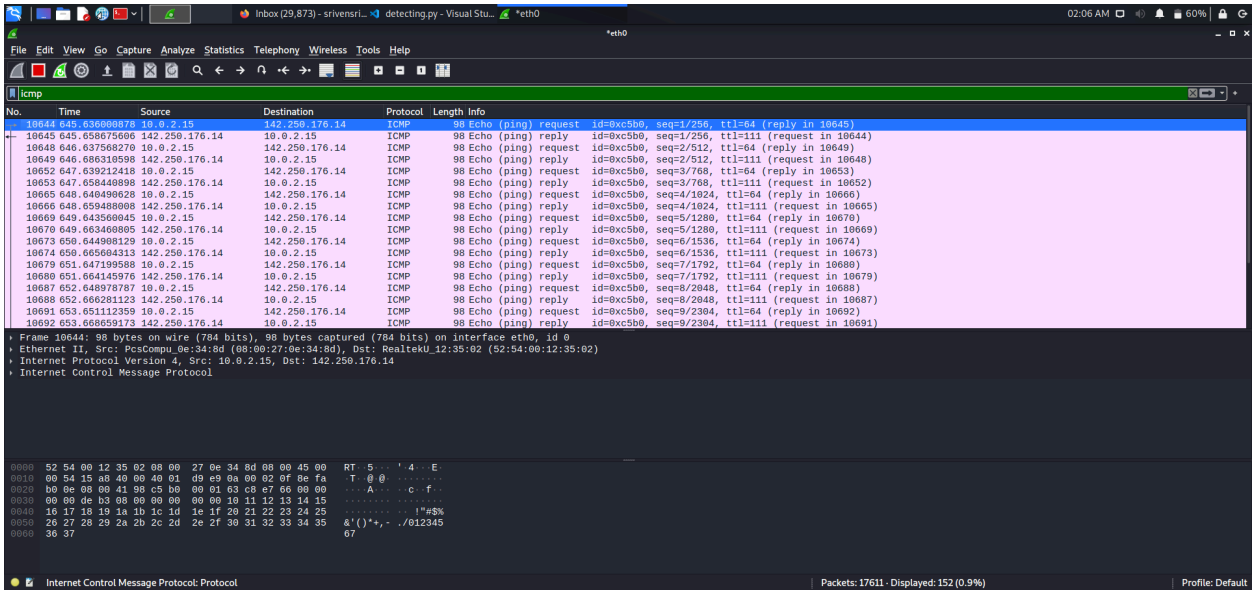
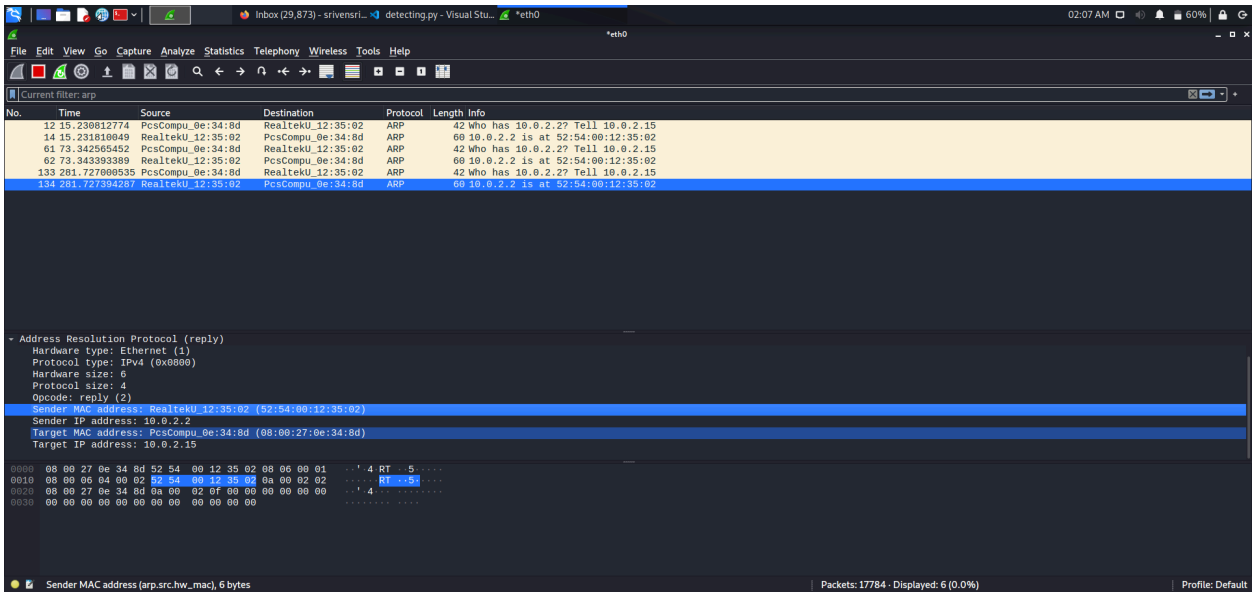
Detecting and Blocking Network Reconnaissance







Possibly integrate with firewall rules to automatically block IPs that exceed certain thresholds.

1.You can write a custom shell or Python script to monitor logs and dynamically add rules to block IPs using iptables or nftables.

sudo iptables -A INPUT -s <malicious_ip> -j DROP

2.Create a script that monitors /var/log/auth.log (for SSH) or any other log file.