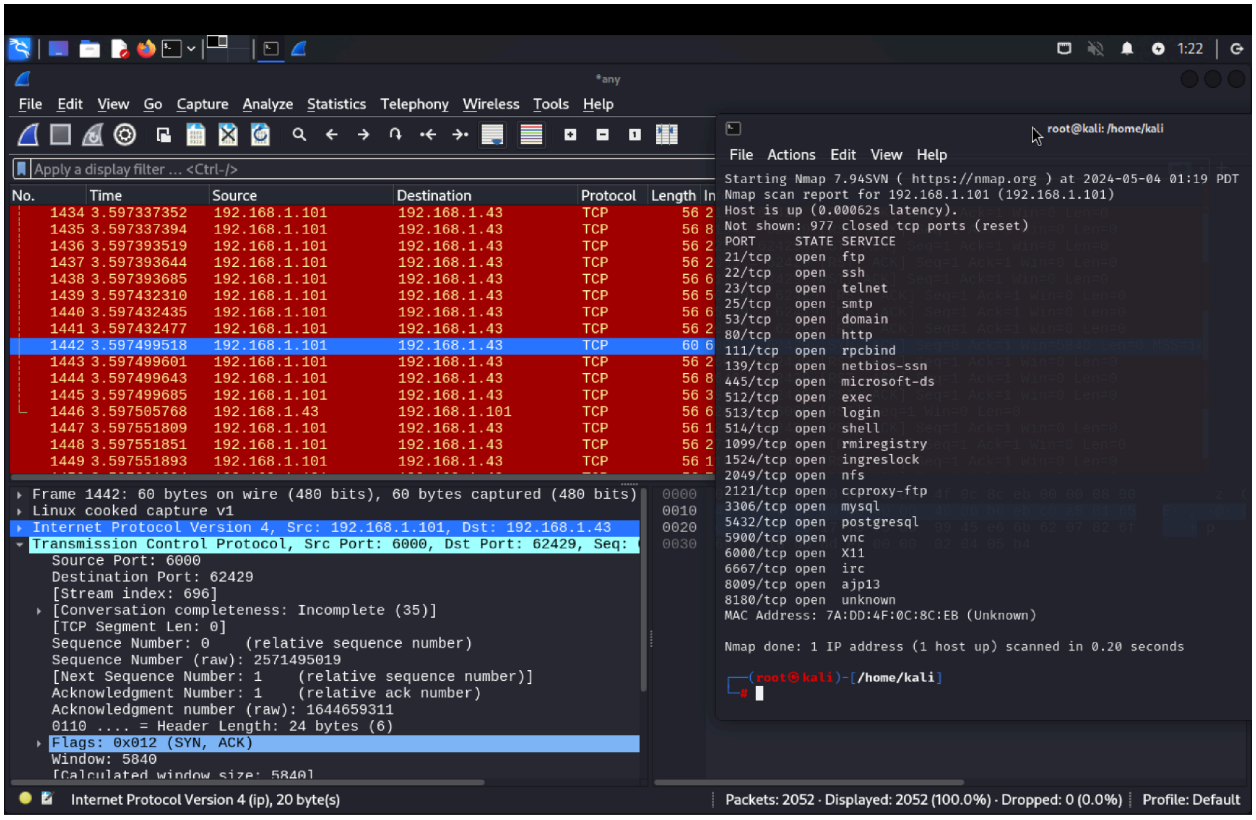
Network Scan Report

Target IP Address: 192.168.1.101 (Metasploitable)

1. TCP SYN Scan:

Command: `nmap -sS 192.168.1.101`

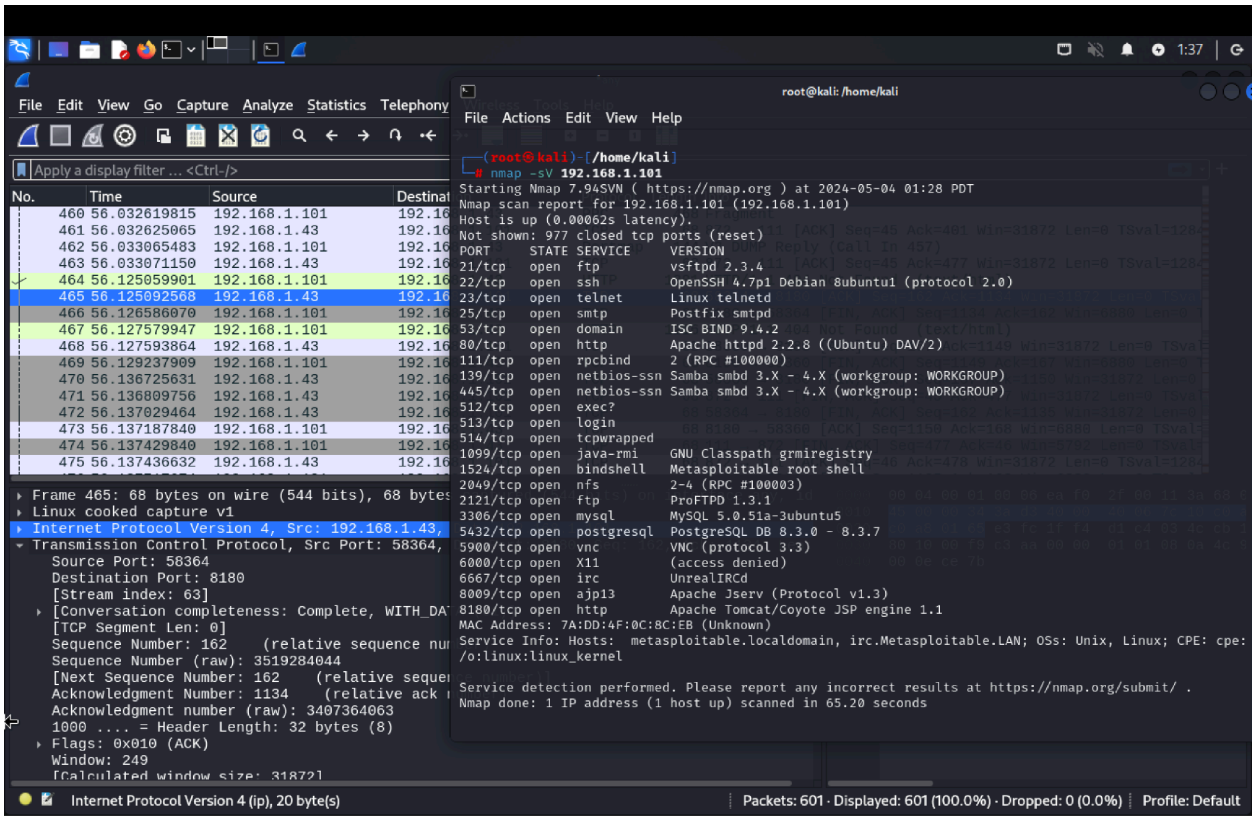
: This command performs a TCP SYN scan on the target IP address to identify open ports.



2. Full Scan with Version Detection:

Command: `nmap -sV 192.168.1.101`

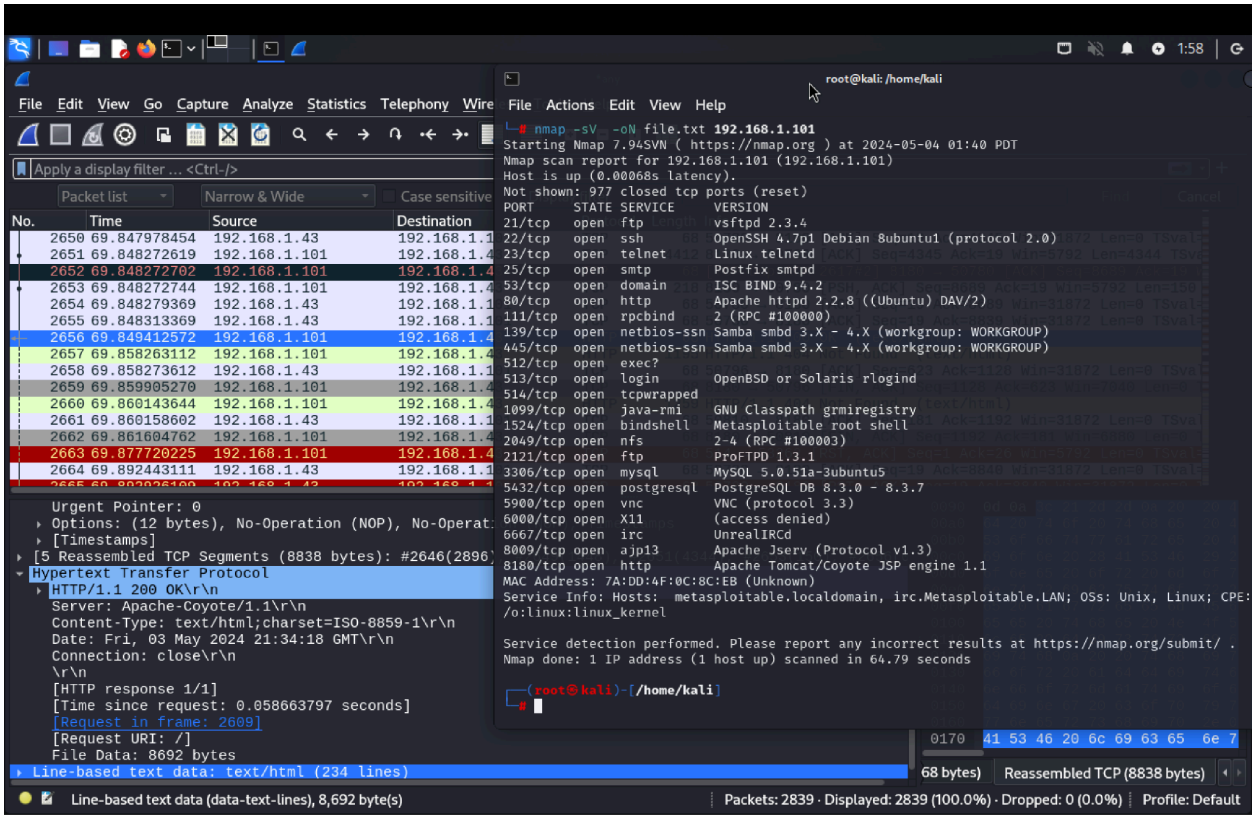
This command conducts a full scan on the target IP address, including version detection to identify services running on open ports.



3. Output to File:

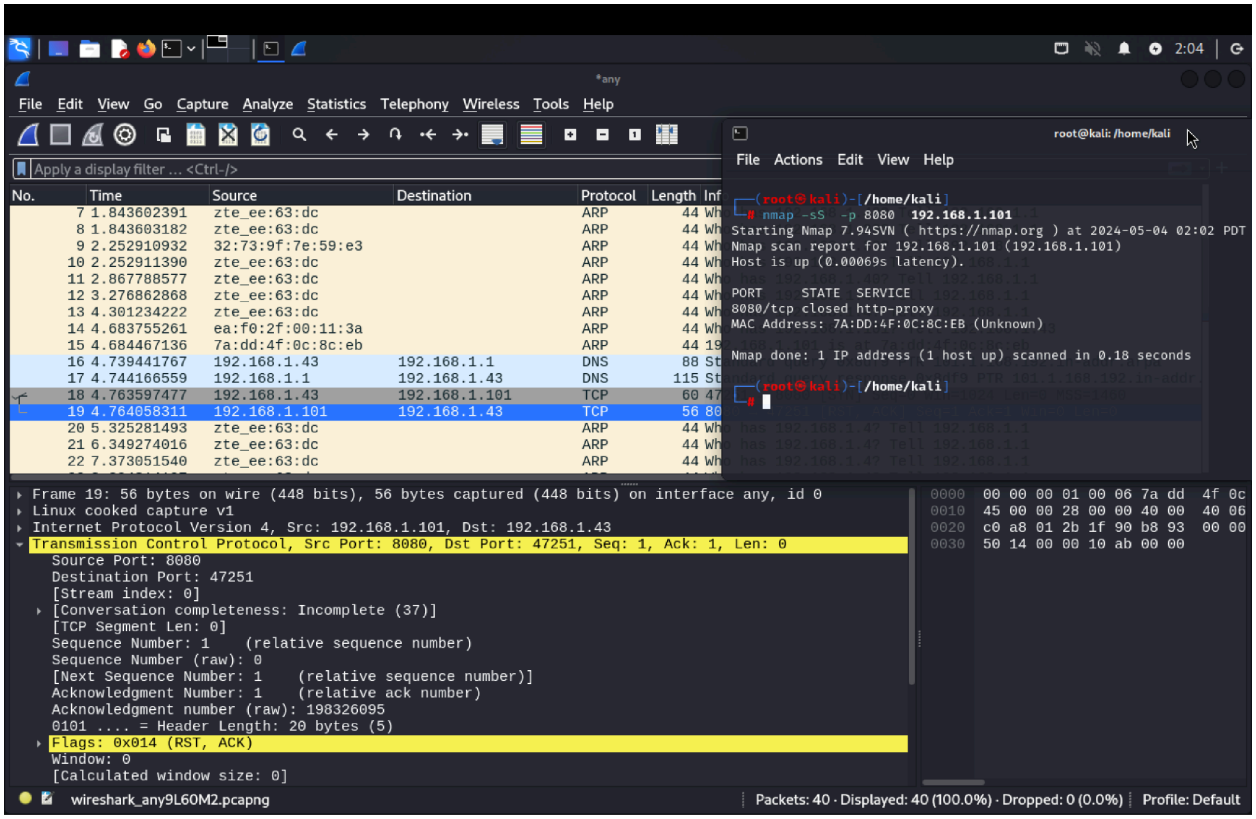
Command: `nmap -sV -oN file.txt 192.168.1.101`

This command performs a full scan with version detection on the target IP address and saves the output to a file named "file.txt".



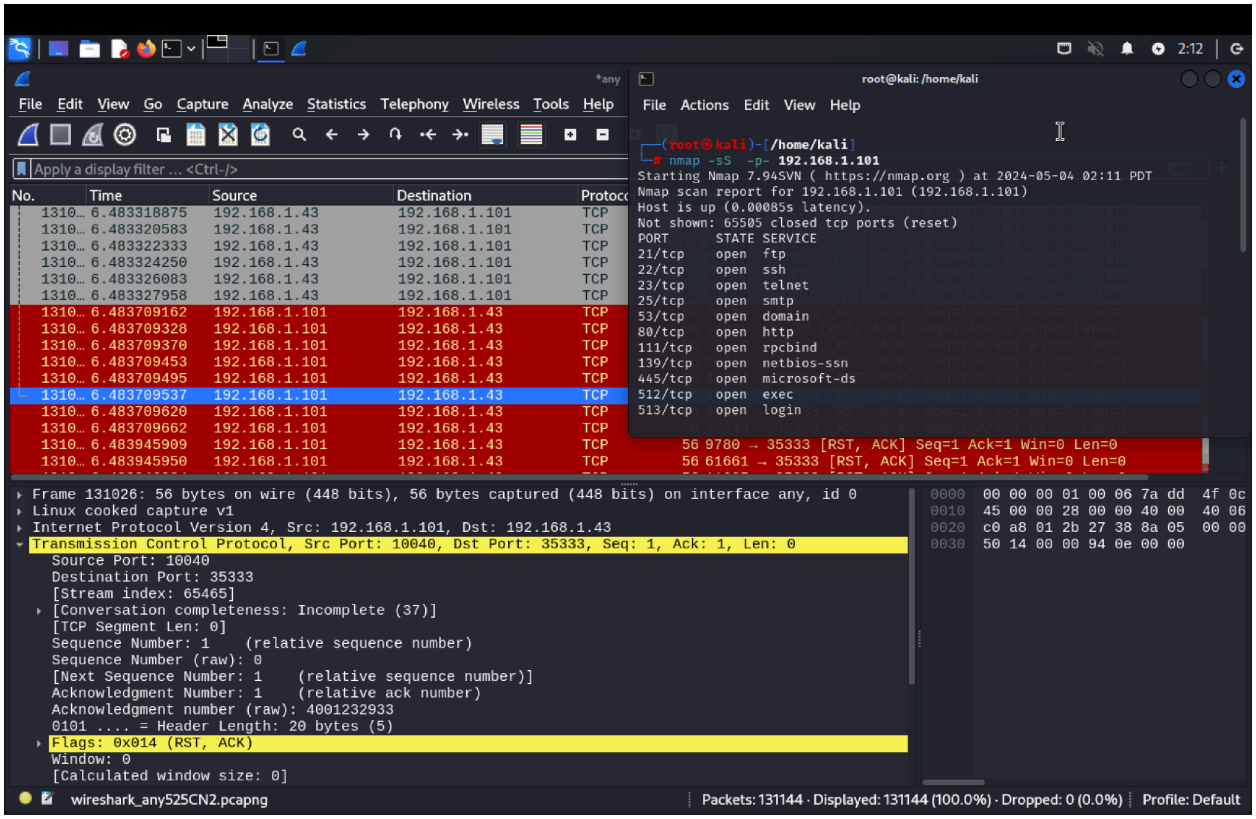
4. Port Scan (Port 8080):

Command: `nmap -sS -p 8080 192.168.1.101
This command scans port 8080 on the target IP address using TCP SYN scan.



5. Full Port Scan:

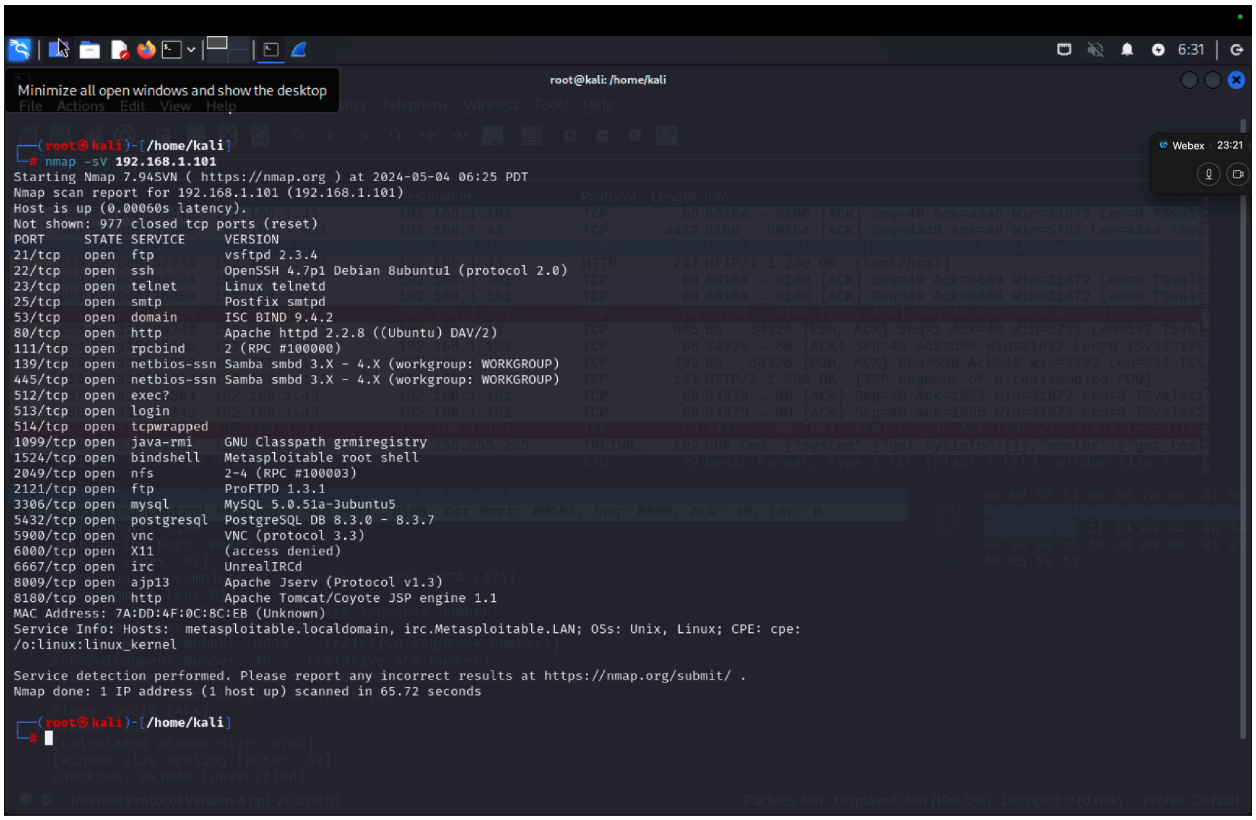
Command: `nmap -sS -p- 192.168.1.101`
This command performs a full port scan on the target IP address to identify all open ports.



7. Operating System Scan:

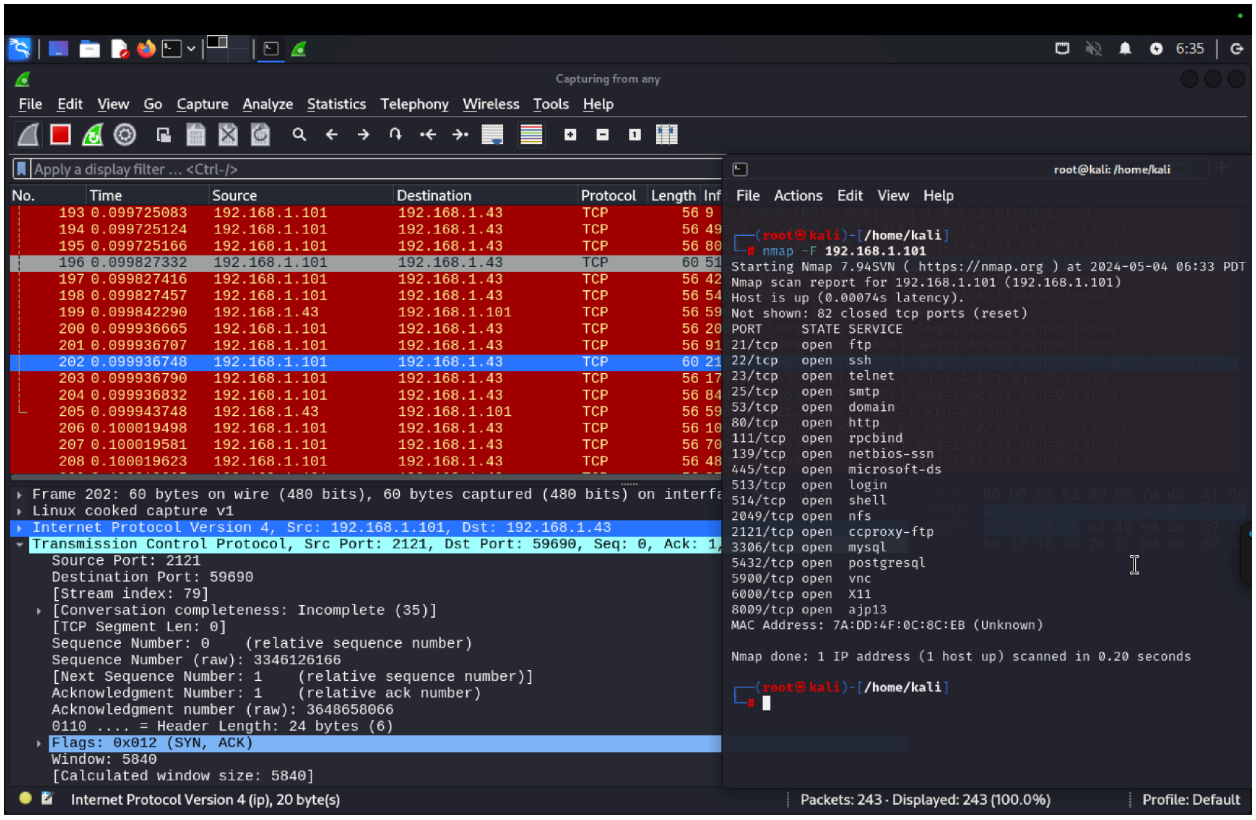
Command: `nmap -O 192.168.1.101`

This command performs an operating system scan on the target IP address to identify the operating system running on the host.



8. Version Detection Scan:

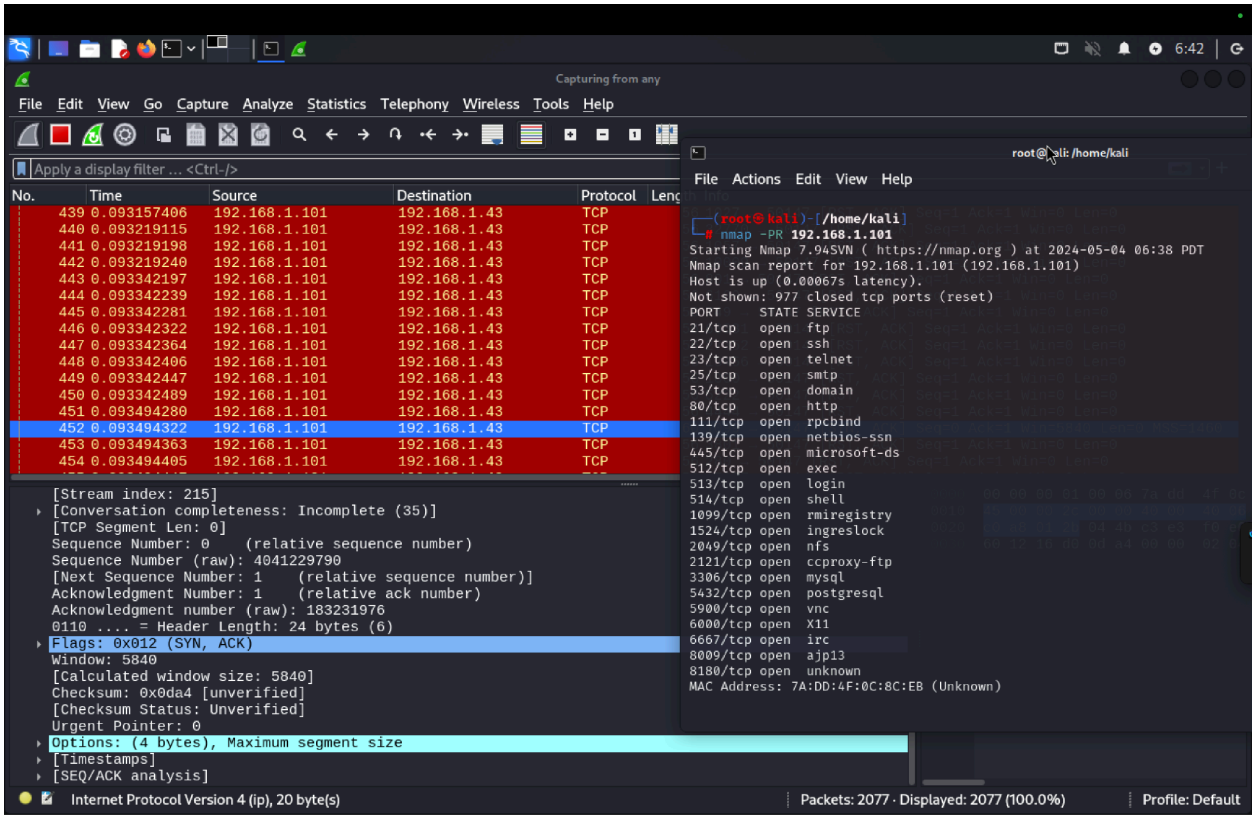
Command: `nmap -sV 192.168.1.101`
This command performs a version detection scan on the target IP address to identify services and their versions running on open ports.



9. Common Ports Scan (Top 100):

Command: `nmap -F 192.168.1.101`

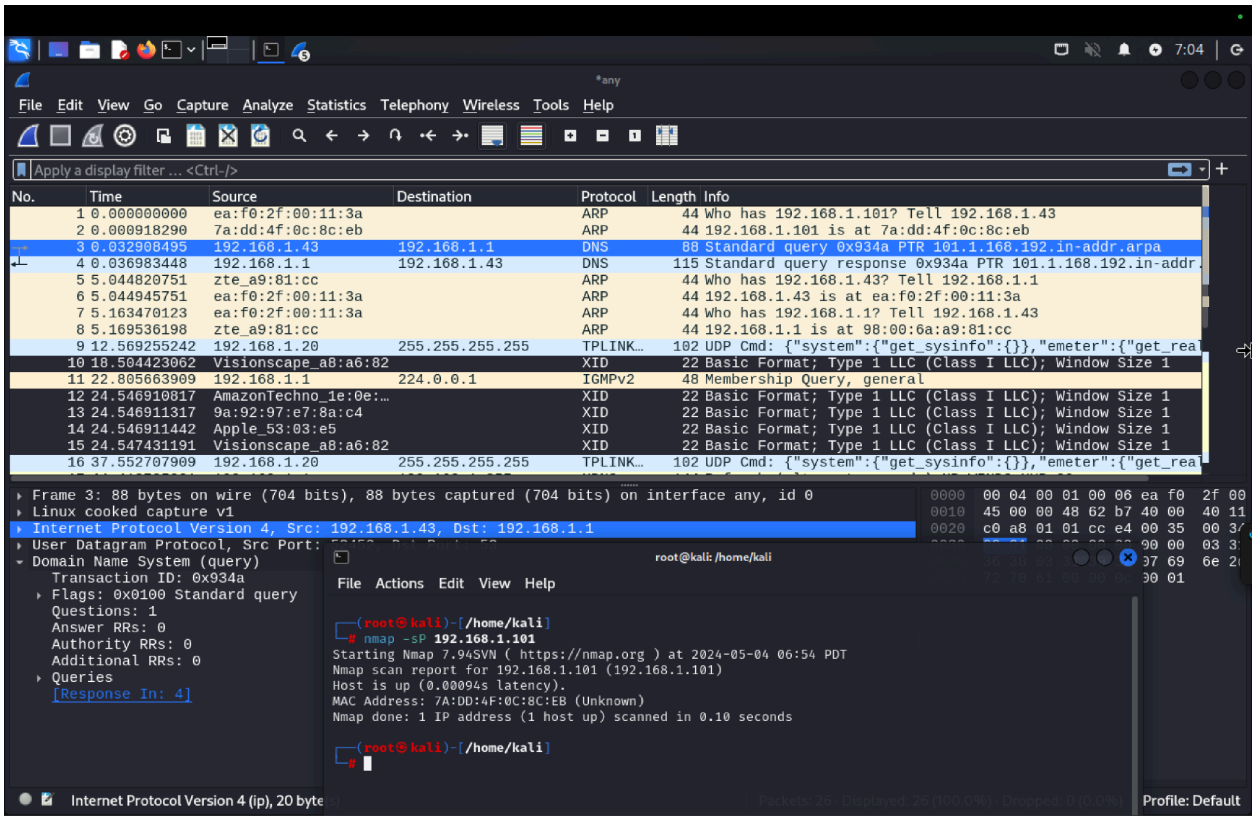
This command conducts a scan on the top 100 common ports on the target



10. ARP Scan:

Command: `nmap -PR 192.168.1.101`

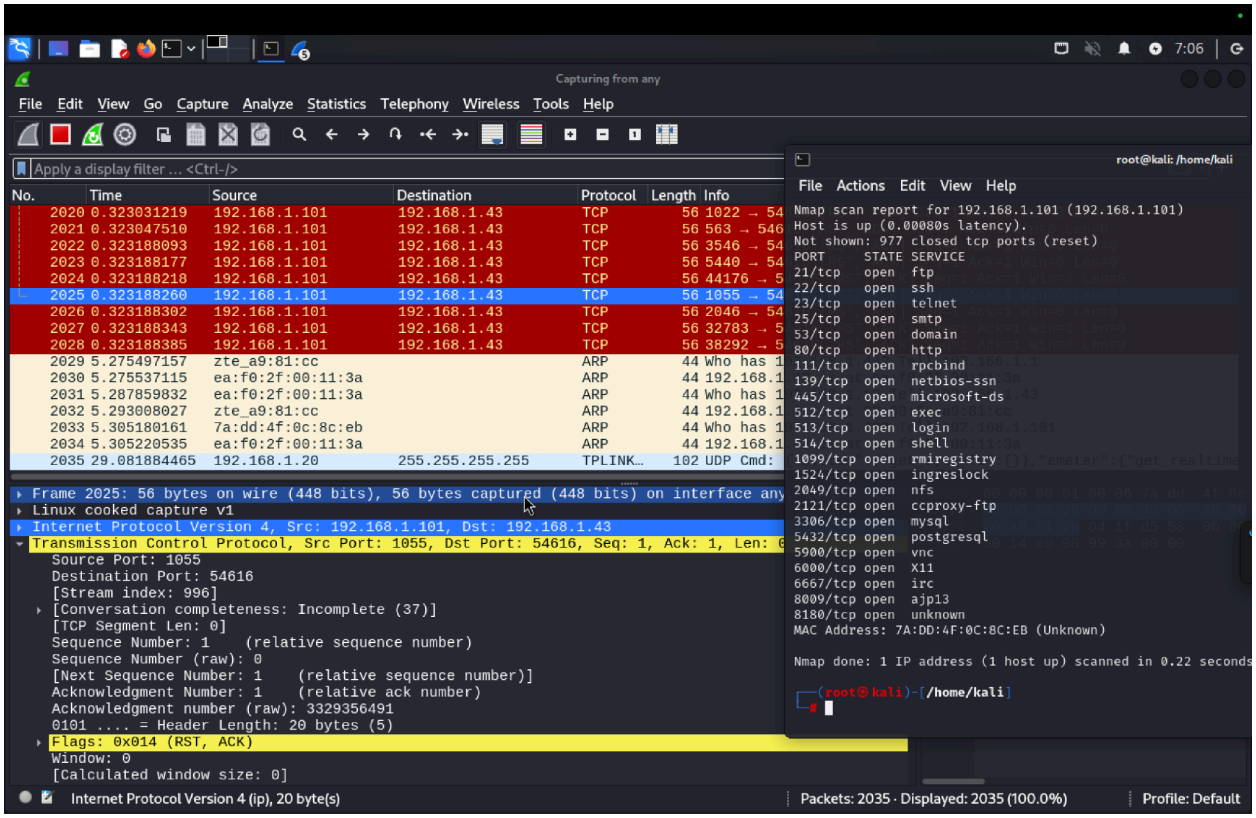
This command performs an ARP scan on the target IP address to discover hosts within the local network.



11. Ping Scan:

Command: `nmap -sP 192.168.1.101`

This command conducts a ping scan on the target IP address to determine if the hosts are alive.



12. Scan without Ping:

Command: `nmap -PN 192.168.1.101`

This command performs a scan on the target IP address without sending ICMP echo requests.