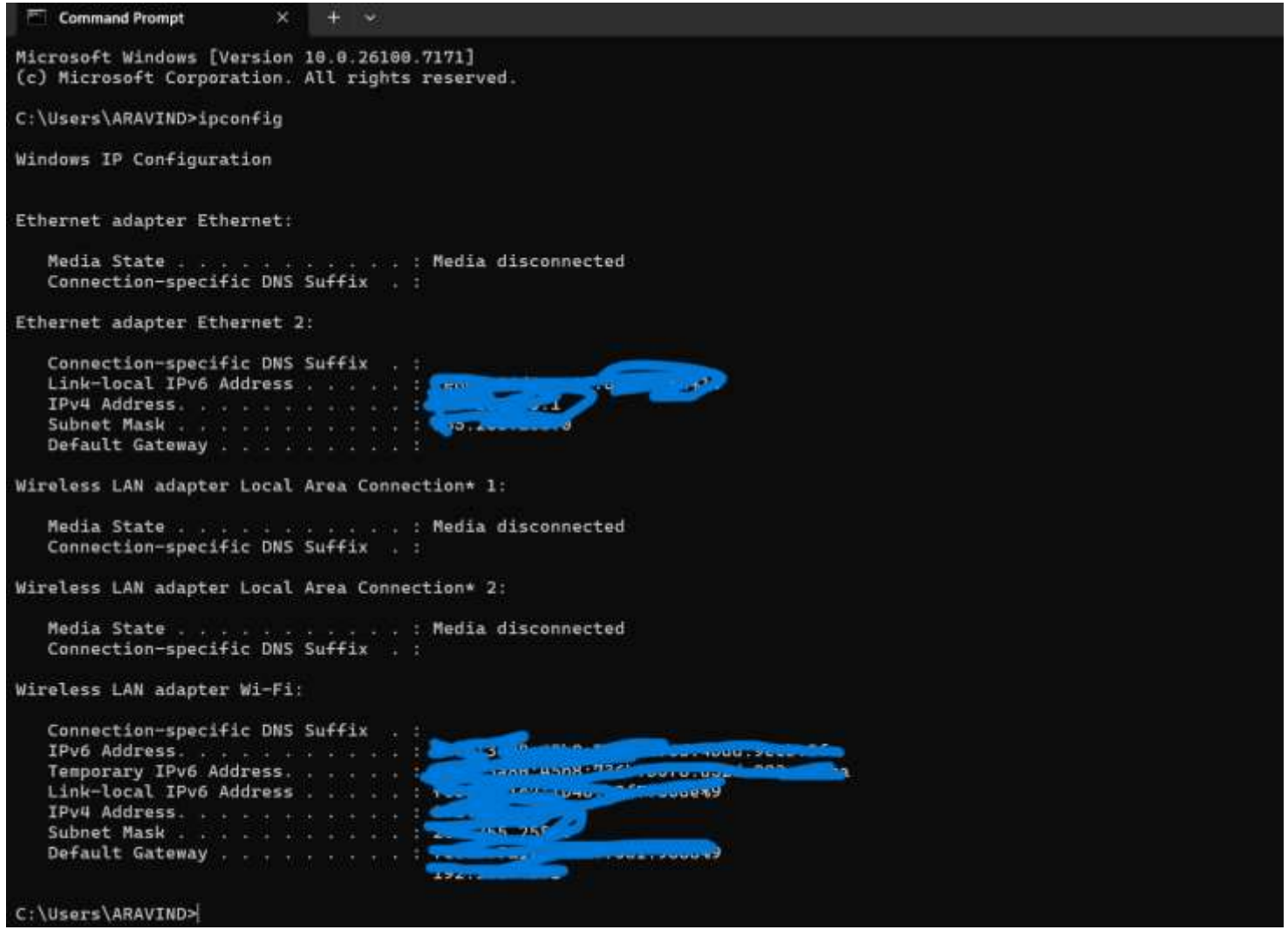
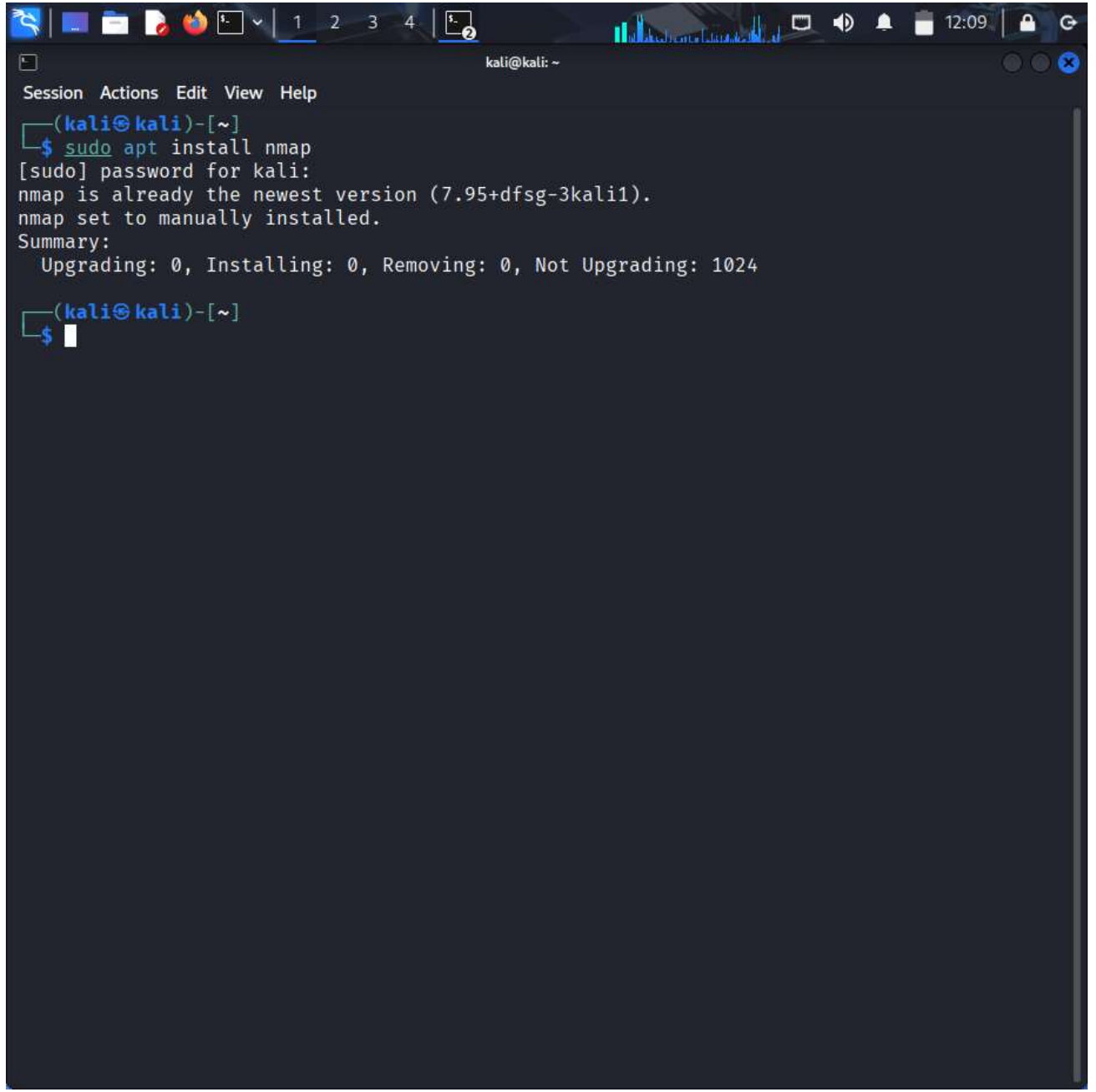
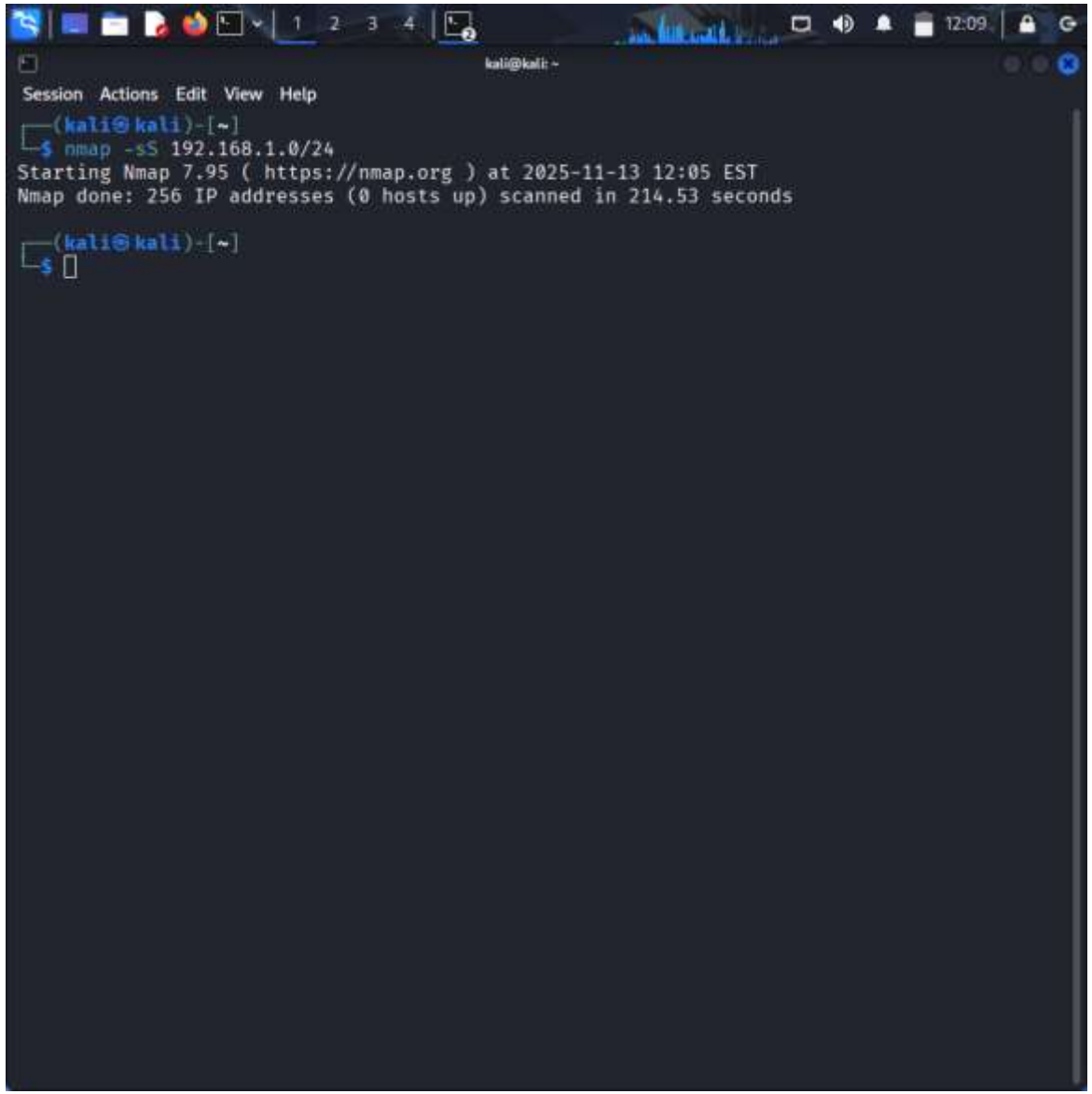
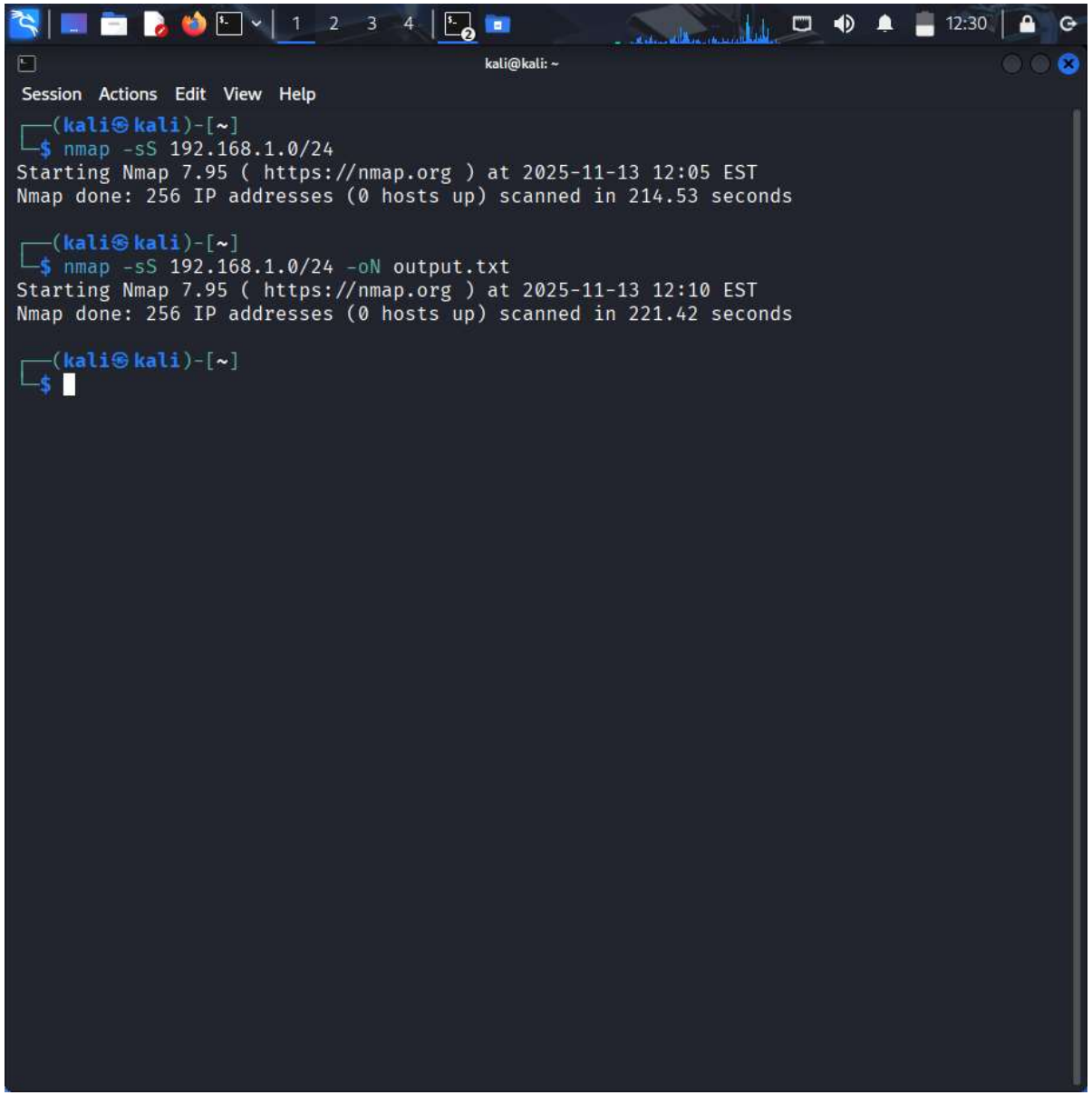
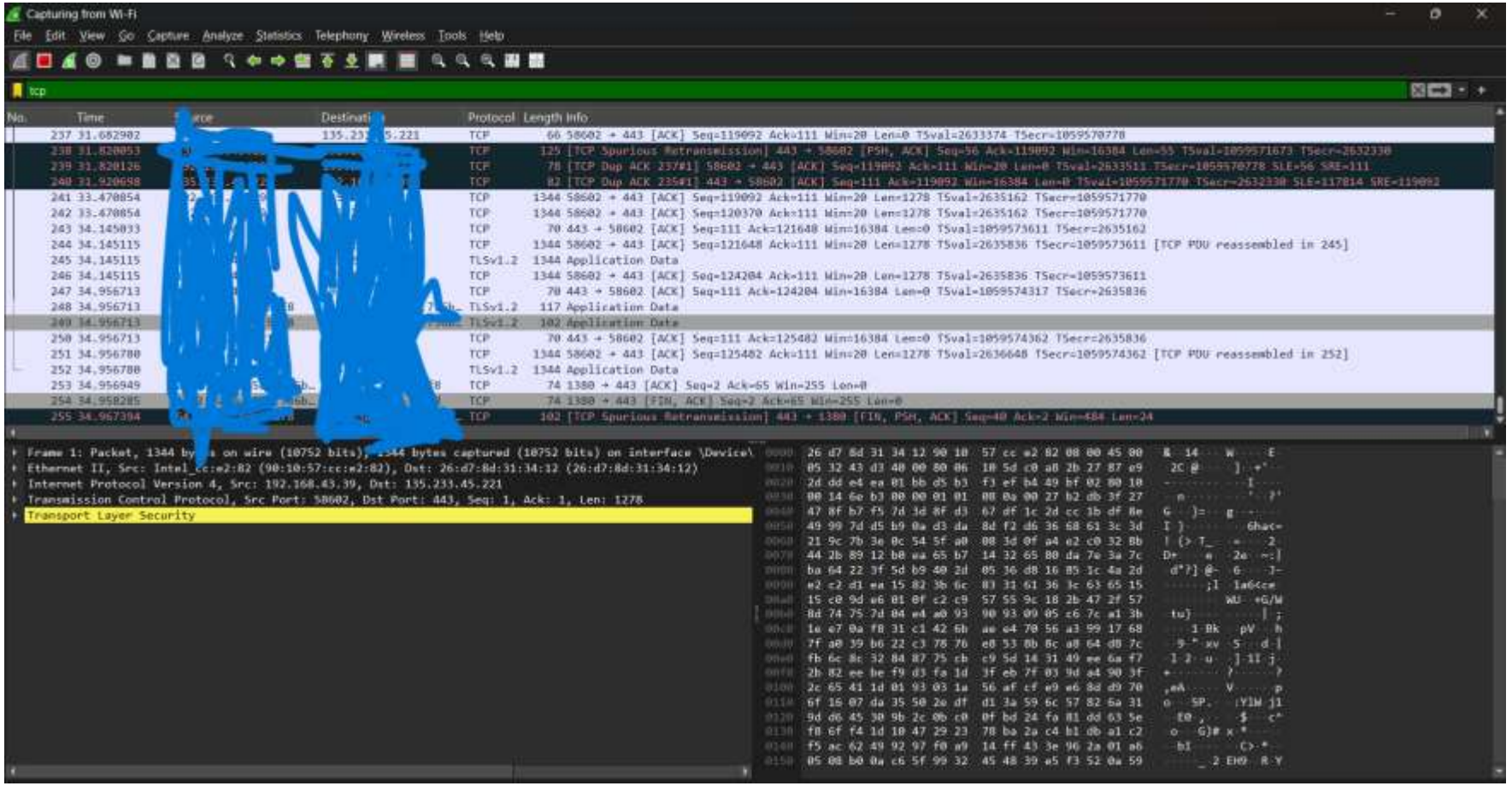
Task -1


Command Prompt
Microsoft Windows [Version 10.0.26100.7171]
(c) Microsoft Corporation. All rights reserved.
C:\Users\ARAVIND>ipconfig
Windows IP Configuration
Ethernet adapter Ethernet:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Ethernet adapter Ethernet 2:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . :
IPv4 Address. . . . . :
Subnet Mask . . . . . :
Default Gateway . . . . . :
Wireless LAN adapter Local Area Connection* 1:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Wireless LAN adapter Local Area Connection* 2:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Wireless LAN adapter Wi-Fi:
Connection-specific DNS Suffix . :
IPv6 Address. . . . . :
Temporary IPv6 Address. . . . . :
Link-local IPv6 Address . . . . . :
IPv4 Address. . . . . :
Subnet Mask . . . . . :
Default Gateway . . . . . :
C:\Users\ARAVIND>


1 2 3 4
12:09
kali@kali: ~
Session Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ sudo apt install nmap
[sudo] password for kali:
nmap is already the newest version (7.95+dfsg-3kali1).
nmap set to manually installed.
Summary:
Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 1024
┌──(kali㉿kali)-[~]
└─$


1 2 3 4
12:09
kali@kali: ~
Session Actions Edit View Help
(kali㉿kali)-[~]
$ nmap -sS 192.168.1.0/24
Starting Nmap 7.95 (https://nmap.org) at 2025-11-13 12:05 EST
Nmap done: 256 IP addresses (0 hosts up) scanned in 214.53 seconds
(kali㉿kali)-[~]
$


1 2 3 4
12:30
kali@kali: ~
Session Actions Edit View Help
(kali㉿kali)-[~]
$ nmap -sS 192.168.1.0/24
Starting Nmap 7.95 (https://nmap.org) at 2025-11-13 12:05 EST
Nmap done: 256 IP addresses (0 hosts up) scanned in 214.53 seconds
(kali㉿kali)-[~]
$ nmap -sS 192.168.1.0/24 -oN output.txt
Starting Nmap 7.95 (https://nmap.org) at 2025-11-13 12:10 EST
Nmap done: 256 IP addresses (0 hosts up) scanned in 221.42 seconds
(kali㉿kali)-[~]
$


Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp
No. Time Source Destination Protocol Length Info
237 31.682902 135.233.45.221 TCP 66 58602 → 443 [ACK] Seq=119092 Ack=111 Win=20 Len=0 TSval=2633374 TSecr=1059570770
238 31.820053 TCP 125 [TCP Spurious Retransmission] 443 → 58602 [PSH, ACK] Seq=56 Ack=119092 Win=16384 Len=55 TSval=1059571673 TSecr=2632330
239 31.820126 TCP 78 [TCP Dup ACK 237#1] 58602 → 443 [ACK] Seq=119092 Ack=111 Win=20 Len=0 TSval=2633511 TSecr=1059570778 SLE=56 SRE=111
240 31.920698 TCP 82 [TCP Dup ACK 235#1] 443 → 58602 [ACK] Seq=111 Ack=119092 Win=16384 Len=0 TSval=1059571770 TSecr=2632330 SLE=117814 SRE=119092
241 33.470854 TCP 1344 58602 → 443 [ACK] Seq=119092 Ack=111 Win=20 Len=1278 TSval=2635162 TSecr=1059571770
242 33.470854 TCP 1344 58602 → 443 [ACK] Seq=120370 Ack=111 Win=20 Len=1278 TSval=2635162 TSecr=1059571770
243 34.145033 TCP 70 443 → 58602 [ACK] Seq=111 Ack=121648 Win=16384 Len=0 TSval=1059573611 TSecr=2635162
244 34.145115 TCP 1344 58602 → 443 [ACK] Seq=121648 Ack=111 Win=20 Len=1278 TSval=2635836 TSecr=1059573611 [TCP PDU reassembled in 245]
245 34.145115 TLSv1.2 1344 Application Data
246 34.145115 TCP 1344 58602 → 443 [ACK] Seq=124204 Ack=111 Win=20 Len=1278 TSval=2635836 TSecr=1059573611
247 34.956713 TCP 70 443 → 58602 [ACK] Seq=111 Ack=124204 Win=16384 Len=0 TSval=1059574317 TSecr=2635836
248 34.956713 TLSv1.2 117 Application Data
249 34.956713 TLSv1.2 102 Application Data
250 34.956713 TCP 70 443 → 58602 [ACK] Seq=111 Ack=125482 Win=16384 Len=0 TSval=1059574362 TSecr=2635836
251 34.956780 TCP 1344 58602 → 443 [ACK] Seq=125482 Ack=111 Win=20 Len=1278 TSval=2636648 TSecr=1059574362 [TCP PDU reassembled in 252]
252 34.956780 TLSv1.2 1344 Application Data
253 34.956949 TCP 74 1380 → 443 [ACK] Seq=2 Ack=65 Win=255 Len=0
254 34.958285 TCP 74 1380 → 443 [FIN, ACK] Seq=2 Ack=65 Win=255 Len=0
255 34.967394 TCP 102 [TCP Spurious Retransmission] 443 → 1380 [FIN, PSH, ACK] Seq=48 Ack=2 Win=484 Len=24
Frame 1: Packet, 1344 by s on wire (10752 bits), 1344 bytes captured (10752 bits) on interface \Device\
Ethernet II, Src: Intel_cc:e2:82 (90:10:57:cc:e2:82), Dst: 26:d7:8d:31:34:12 (26:d7:8d:31:34:12)
Internet Protocol Version 4, Src: 192.168.43.39, Dst: 135.233.45.221
Transmission Control Protocol, Src Port: 58602, Dst Port: 443, Seq: 1, Ack: 1, Len: 1278
Transport Layer Security