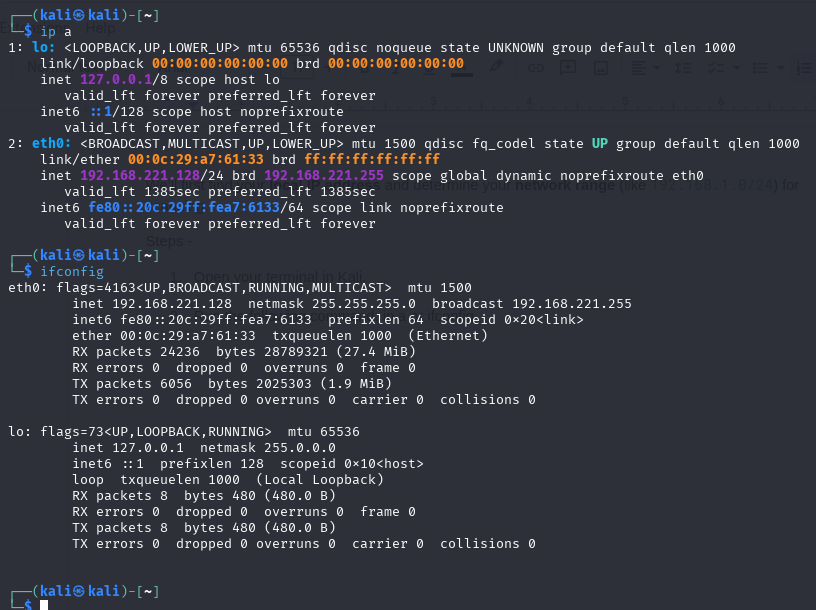
## **Nmap**

Step 1: Find Your Local IP Range

We’ll first find your **local IP address** and determine your **network range** (like 192.168.1.0/24) for scanning.

Steps -

1. Open your terminal in Kali.
2. Run the following command: ip a or ifconfig



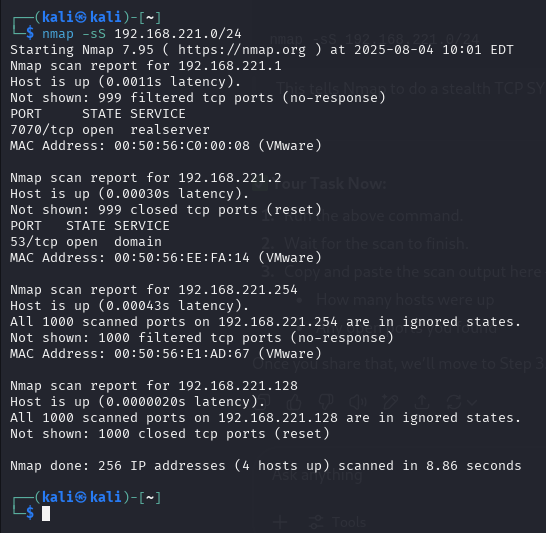
**local IP:** 192.168.221.128

**network range for scanning:** 192.168.221.0/24

Step 2: Perform a TCP SYN Scan Using Nmap

Now we’ll run a **TCP SYN scan** to find live hosts and open ports on our network. Use the following command:

nmap -sS 192.168.221.0/24



Active Hosts Found:

* **192.168.221.1** - Port 7070 open (service: realserver)
* **192.168.221.2** - Port 53 open (service: domain = DNS)
* **192.168.221.254** - No open ports, all filtered
* **192.168.221.128** (your machine) - All ports closed

Notes:

* 7070/tcp is commonly used by **proxy servers**, **streaming**, or custom services.
* 53/tcp is **DNS** — an essential service, often targeted.
* Filtered ports mean no response — likely blocked by a firewall or not listening.

**Step 3: Interpret Scan Results & Identify Potential Security Risks**

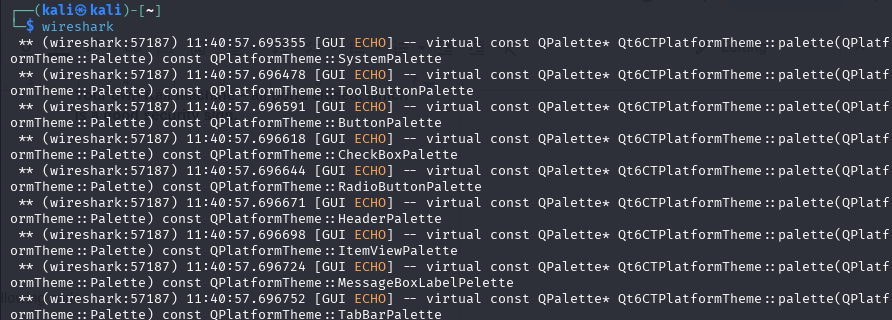
| **IP Address** | **Open Port** | **Service** | **Possible Risk Description** |
| --- | --- | --- | --- |
| **192.168.221.1** | **7070/tcp** | **realserver** | **Often used by proxy, streaming, or remote management tools. If misconfigured, it may expose internal services.** |
| **192.168.221.2** | **53/tcp** | **domain (DNS)** | **DNS is essential but can be exploited for data exfiltration (DNS tunneling), DoS, or poisoning if not secured.** |
| **192.168.221.254** | **—** | **—** | **All ports filtered – possibly a firewall/router blocking Nmap.** |
| **192.168.221.128** | **—** | **—** | **Your own Kali machine – all ports closed, which is a good security sign.** |

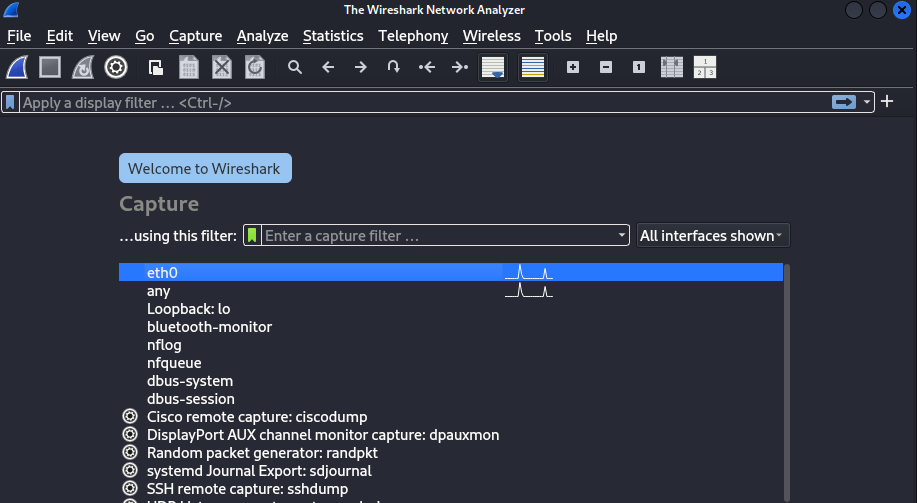
## **Wireshark**

Steps 1: To install wireshark, type the following code-

sudo wireshark

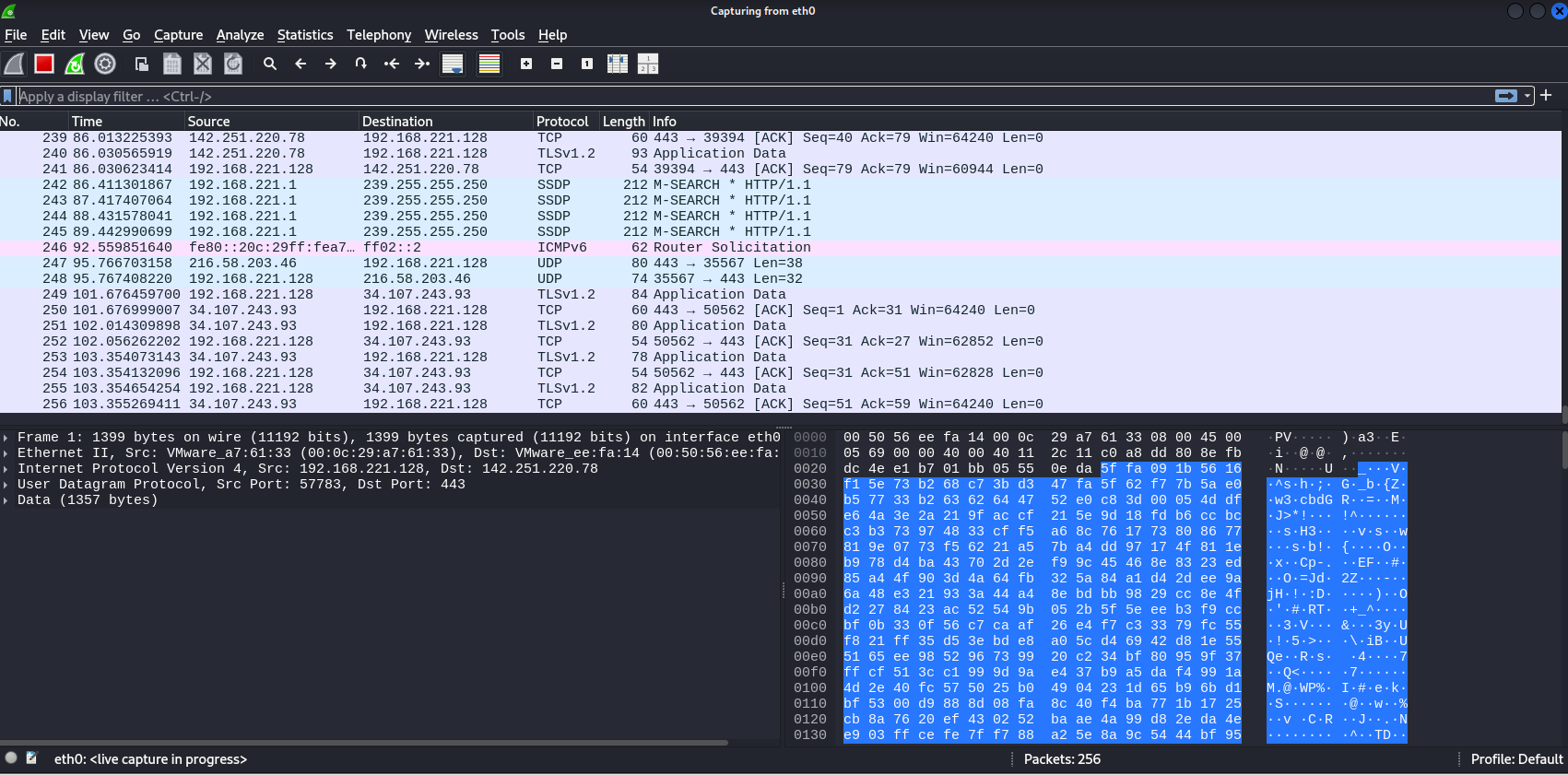
Then type ‘wireshark’





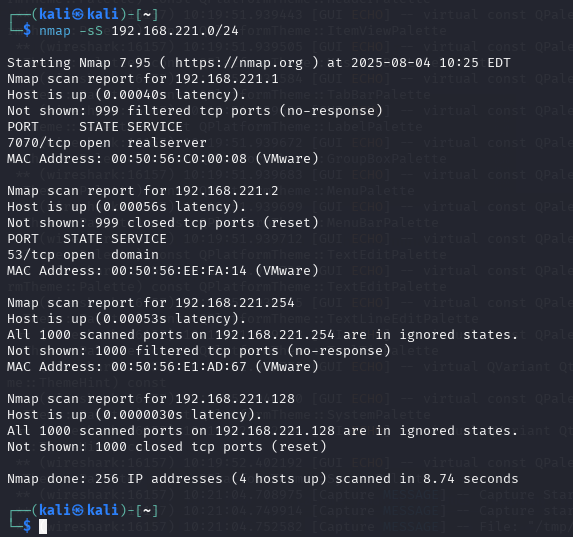
**Select the Correct Interface**

* Choose the **active interface** (probably eth0 in your case).
* Click the **blue shark fin icon** to start capturing packets.



**Step 2: Start the Nmap Scan in Another Terminal**

* Run: nmap -sS 192.168.221.0/24, in the terminal



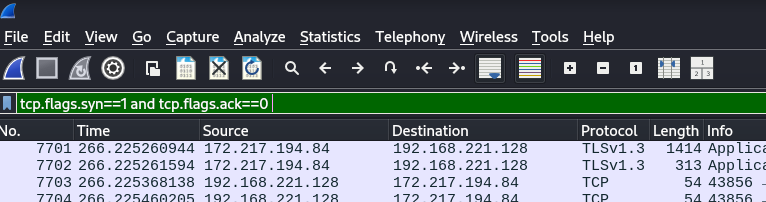
**Step 3: Stop Capture After the Scan Finishes**

* Click the **red square** to stop capture.

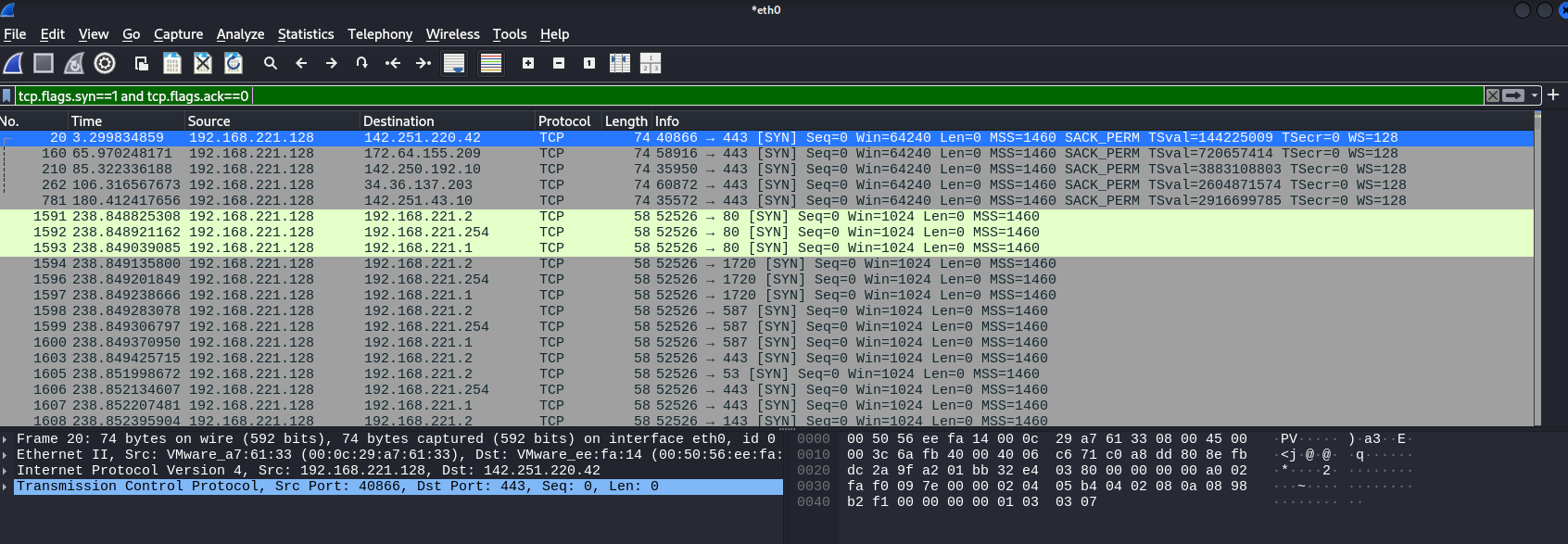
**Step 4: Filter for SYN Packets (Optional)**

* In Wireshark’s filter bar, enter:

tcp.flags.syn==1 and tcp.flags.ack==0



This shows SYN packets sent by Nmap (SYN scan = half-open TCP handshake).



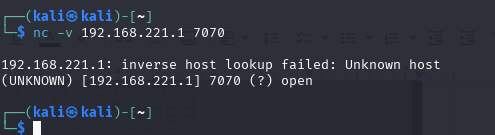
## **Netcat**

We’ll use Netcat to Probe an Open Port (Banner Grabbing), we’ll try to connect to one of the open ports found earlier with Nmap:

* **Target:** 192.168.221.1
* **Port:** 7070 (realserver)

Use the following command

nc -v 192.168.221.1 7070



Netcat output confirms:

* The **port is open** (7070 open ✅).
* **No banner or response** was received — meaning the service on that port might:  
  + Be a custom or proprietary protocol
  + Require specific input to reply
  + Be silently listening

## **Masscan**

Step 1: Install Masscan (if not already installed)

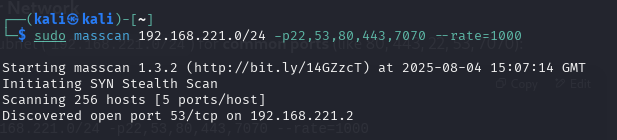
In Kali, run:

sudo apt install masscan

Step 2: Scan Your Network

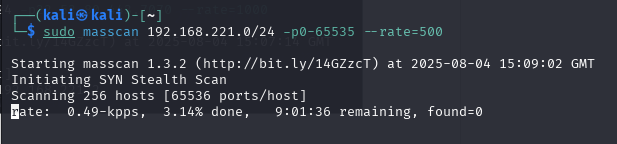
Let’s scan your same subnet (192.168.221.0/24) for **common ports** (like 80, 443, 22, 53, 7070):

sudo masscan 192.168.221.0/24 -p22,53,80,443,7070 --rate=1000



Step 3: Full Port Range Scan

You can scan *all 65535* ports, type the following code:



It takes hours..

All this confirms the same result from Nmap, validating that **192.168.221.2** is running a DNS service (TCP port 53 is open).

Result: Masscan did **not find 7070** open, which might be because:

* It's filtered from fast/stealthy scans
* Masscan dropped the packet before it completed a retry
* Nmap does deeper scans, while Masscan prioritizes speed