

**Project:** Net crafts

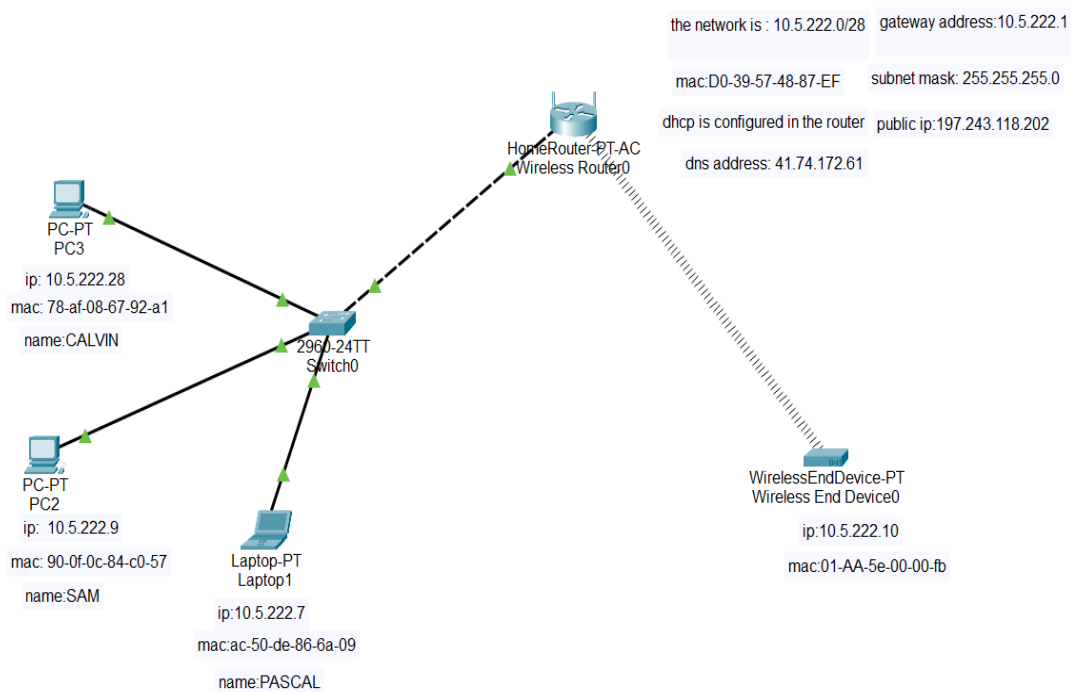
**NAME:** .....MUGISHA Pascal.....

**UNIT:** RW-CODING-ACADEMY-...II...

**S-code:** S.....25.....

## MAP THE NETWORK

The below network diagram depicts my network. The DHCP and DNS configurations are provided in a Wireless router.



## DHCP Configuration

Setup

Setup

Wireless

Security

Access Restrictions

Applications & Gaming

Administration

Status

Basic Setup

DDNS

MAC Address Clone

Advanced Routing

Internet Setup

Internet Connection type

Automatic Configuration - DHCP

Optional Settings (required by some internet service providers)

Host Name:

Domain Name:

MTU: Size: 1500

Network Setup

Router IP

IP Address:

10

5

222

1

Subnet Mask:

255.255.255.0

DHCP Server Settings

DHCP Server:

Enabled

Disabled

DHCP Reservation

Start IP Address:

10.5.222.100

Maximum number of Users:

28

IP Address Range:

10.5.222.100 - 127

Client Lease Time:

0

minutes (0 means one day)

Static DNS 1:

0

0

0

0

Static DNS 2:

0

0

0

0

Static DNS 3:

0

0

0

0

WINS:

0

0

0

0

ISP Vlans

Enabled

Disabled

Vlan IDs:

Internet: 10

VoIP: 20

IpTV: 30

Port Vlans:

Help...

MAC addresses were identified by running:

- arp -a
- ipconfig /all

**Getting manufacture based on MAC address:**

The screenshot shows a web browser at the URL `maclookup.app/search/result?mac=D0-39-57-48-87-EF`. The page has a blue header with the title "MAC Address Lookup" and a subtitle "Find the vendor name of a device by entering an OUI or a MAC address". Below this is a search bar with "MAC" selected and the address "D0-39-57-48-87-EF" entered. A search button with a magnifying glass icon is to the right. Below the search bar, a message says "Check an OUIs or a MAC address and display details like vendor name, location, MAC details, and more..." with a link "Search by Vendor Name?". The breadcrumb trail at the bottom of the header reads "Home / Search / Result (D0:39:57)".

The main content area displays the results for "Liteon Technology Corporation". There are two tabs: "Vendor" (selected) and "Details". Under the "Vendor" tab, the following information is shown:

- OUI: D0:39:57 (with a link icon)
- Vendor name: Liteon Technology Corporation (with a link icon)
- Address: (with a location pin icon and the text "AF")

To the right of the text is a map showing a location in Asia. An advertisement for "RequestInspector.com" is visible on the right side of the page, with the text "Collect and Inspect HTTP/Webhook Requests in Real Time". At the bottom right of the ad, it says "Ads by EthicalAds".

## COLLECTING INFORMATION

### 1. Using Shodan to collect information on my public IP address

The following screenshot indicates the results of searching the devices on my public IP address:

## 2. The results of checking the registrar of my public IP

The screenshot displays the Shodan search engine interface for the IP address 197.243.118.202. The browser's address bar shows the URL `shodan.io/host/197.243.118.202`. The Shodan navigation bar includes links for Shodan, Maps, Images, Monitor, Developer, and More... A search bar with the text "Search..." and a magnifying glass icon is also present.

The main content area features a satellite map of Rwanda. Below the map, the IP address **197.243.118.202** is prominently displayed. To the right of the IP, there are buttons for "Regular View" and "Raw Data".

Below the map, the "General Information" section provides details about the IP's location and ownership:

General Information	
Country	Rwanda
City	Kigali
Organization	BSC
ISP	KT RWANDA NETWORK Ltd
ASN	AS37228

To the right of the general information, the "Open Ports" section shows a list of open ports. A blue box highlights the number "264". Below this, the "Check Point Firewall" section displays the following information:

Check Point Firewall:  
Firewall Host: CP-CODING.ACADEMY  
SmartCenter Host: BSC-CP\_SMS

The bottom right corner of the interface shows the text "LAST SEEN: 2024" and a timestamp "2024-04-12T14:36:56".

```

(pascal@kali)-[~]
$ whois 197.243.118.202
% This is the AfrinIC Whois server.
% The AFRINIC whois database is subject to the following terms of Use. See https://afrinic.net/whois/terms

% Note: this output has been filtered.
% To receive output for a database update, use the "-B" flag.

% Information related to '197.243.118.0 - 197.243.118.255'

% No abuse contact registered for 197.243.118.0 - 197.243.118.255

inetnum:      197.243.118.0 - 197.243.118.255
netname:      TechnoLane
descr:        BSC
country:      RW
admin-c:      FN19-AFRINIC
tech-c:       FN19-AFRINIC
status:       ASSIGNED PA
mnt-by:       BSC-MNT
source:       AFRINIC # Filtered
parent:       197.243.0.0 - 197.243.127.255

person:       Faycal Ndingiza
address:       2F,TelecomHouse,BlvDeL'Umuganda
address:       Kacyiru-Kigali 7229
address:       Rwanda
phone:        tel:+250-788-301-540
nic-hdl:      FN19-AFRINIC
mnt-by:       GENERATED-GRHVMCBIQP3BSTRG0DKTZPSIFUAHNZ05-MNT
source:       AFRINIC # Filtered

% Information related to '197.243.118.0/24AS37619'

route:        197.243.118.0/24
descr:        BSC-NET-197.243.118.0/24
origin:       AS37619
mnt-by:       BSC-MNT
source:       AFRINIC # Filtered

```

### 3. Sniffing network

I sniffed my network by using Wireshark

**The Transmission Control Protocol (TCP)** is a fundamental communication protocol that forms the backbone of reliable data transfer on the internet