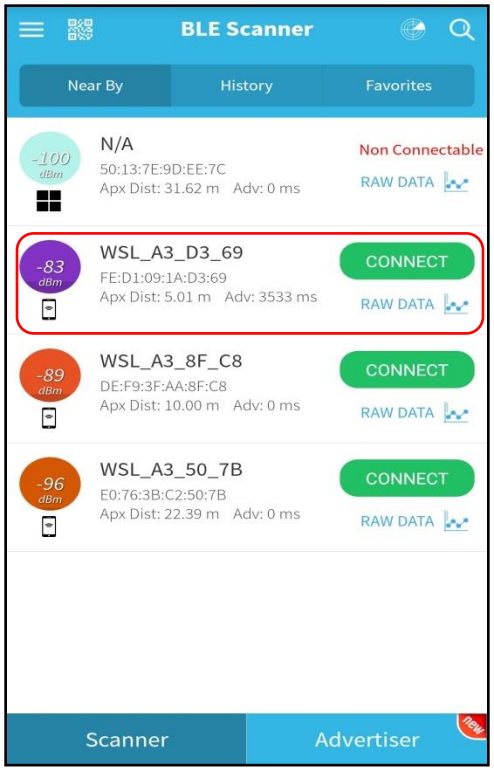
IoT (Internet of Things) Wireless & Cloud Computing Emerging Technologies Report

BLE Scanner :-

Scanner :-

Device WSL_A3_D3_69 is the closest among all as it has the highest RSSI value (-83).



Device Name : WSL_A3_D3_69

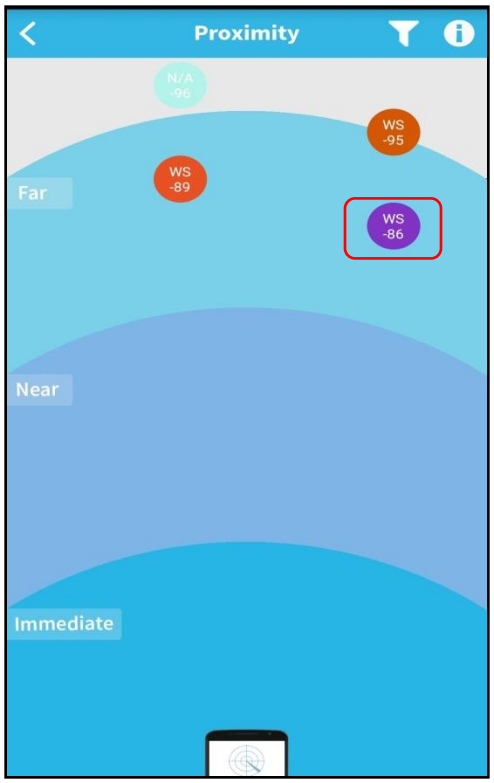
MAC Address : FE:D1:09:1A:D3:69

RSSI : -83

Raw Data :

Proximity :-

There are no “Immediate” or “Near” BLE devices available. All the BLE devices are at “Far” distance and beyond from the mobile device with the closest one being the one described above and now its RSSI is changed to -86.



Bluetooth 4.0 Scanner :-

Classic Scan :-

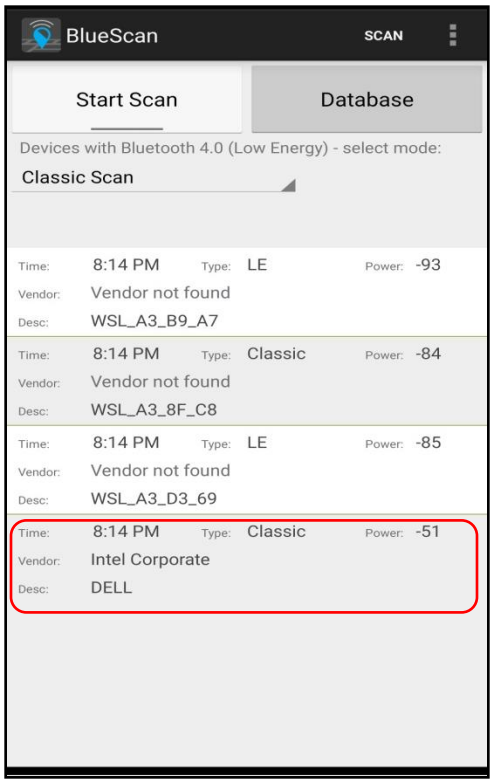
Both the devices with Bluetooth version more and less than 4.0 are listed here. For example, the details of one of the devices are as follows :-

Vendor : Intel Corporate

Desc : DELL

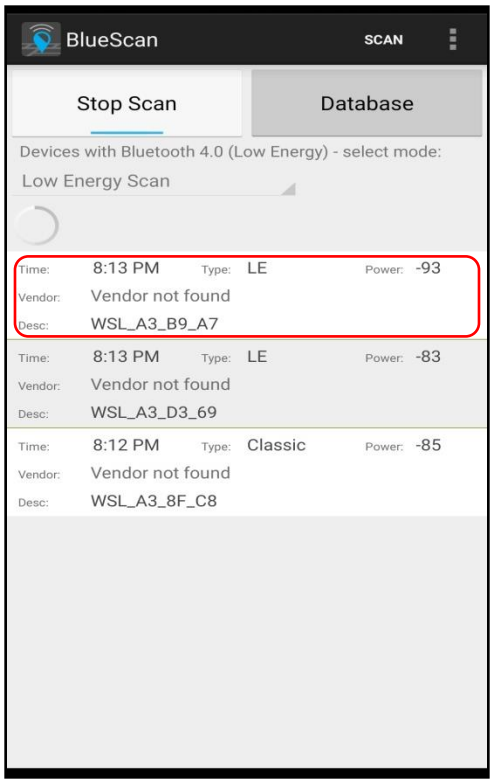
Type : Classic

Power (RSSI) : -51



Low Energy Scan :-

Devices with Bluetooth version 4.0 and above are listed here. For example, the details of one of the devices are as follows :-



Vendor : Not Found

Desc : WSL_A3_B9_A7

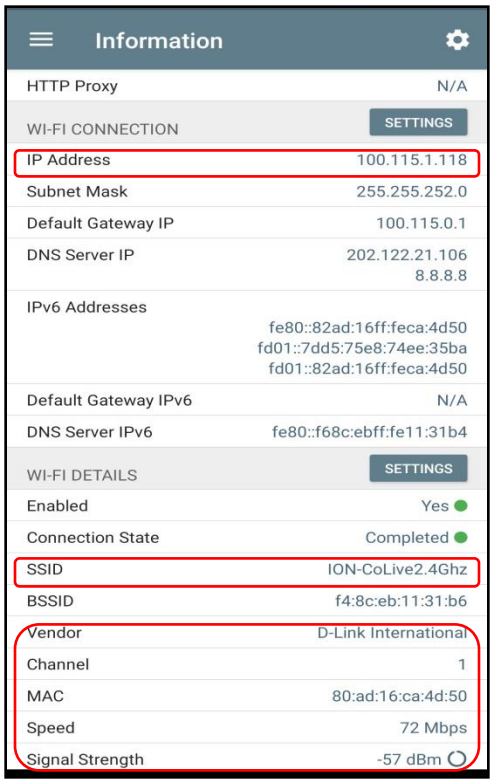
Type : LE

Power (RSSI) : -83

Network Analyzer :-

Wi-Fi Information :-

Following are the details of Wi-Fi network to which the mobile device is connected :-



SSID : ION-CoLive2.4GHz

Channel : 1

IP Address : 100.115.1.118

Speed : 72 Mbps

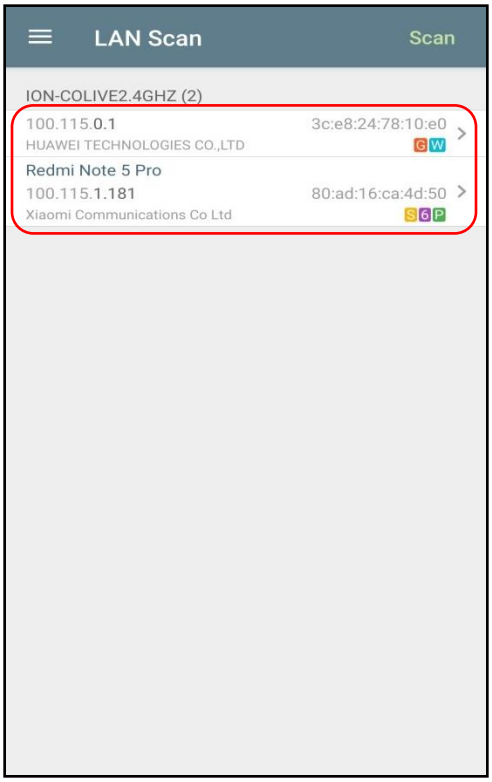
Signal Strength : -57 dBm

MAC Address of AP : 80:ad:16:ca:4d:50

Vendor : D-Link International

LAN Scan :-

Devices with following properties were captured in the LAN Scan :-



G : Gateway

W : Web Interface Available

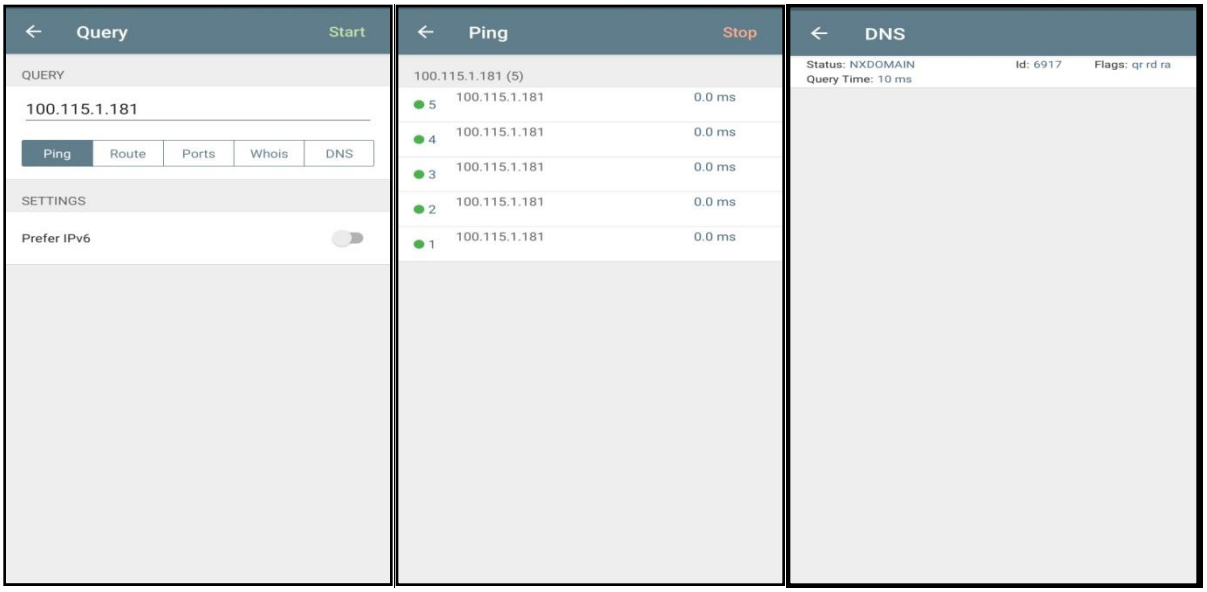
S : Scanning Device

6 : IPv6 Address Exists

P : Pingable

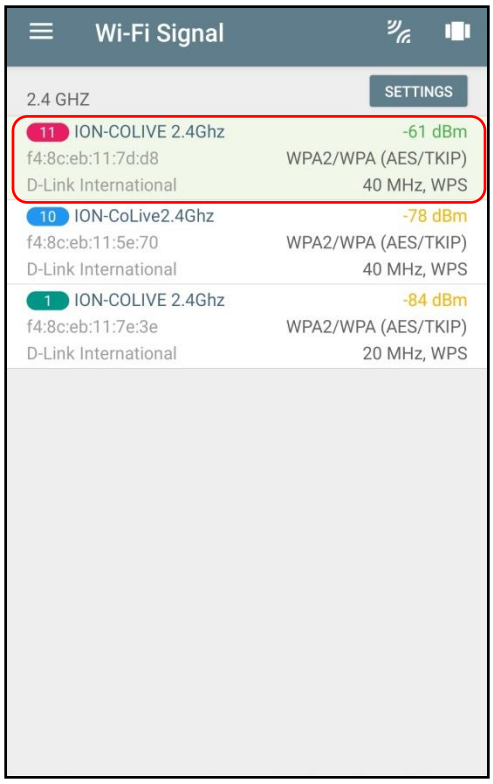
Query :-

Following queries were performed on the Redmi Note 5 Pro device :-



Wi-Fi Signal :-

3 Wi-Fi AP operating on 2.4 GHz band were detected. The details of one of the devices are as follows :-



RSSI : -61 dBm

SSID : ION-COLIVE 2.4GHz

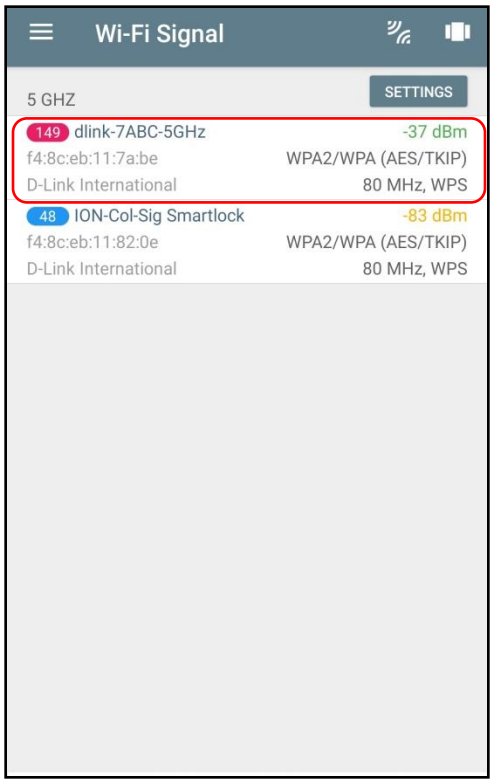
MAC Address of AP : f4:8c:eb:11:7d:d8

Bandwidth : 40 MHz

PHY Channel : 11th Channel

Encryption Scheme : WPA2/WPA (AES/TKIP)

2 Wi-Fi AP operating on 5 GHz band were detected. The details of one of the devices are as follows :-



RSSI : -37 dBm

SSID : dlink-7ABC-5GHz

MAC Address of AP : f4:8c:eb:11:7a:be

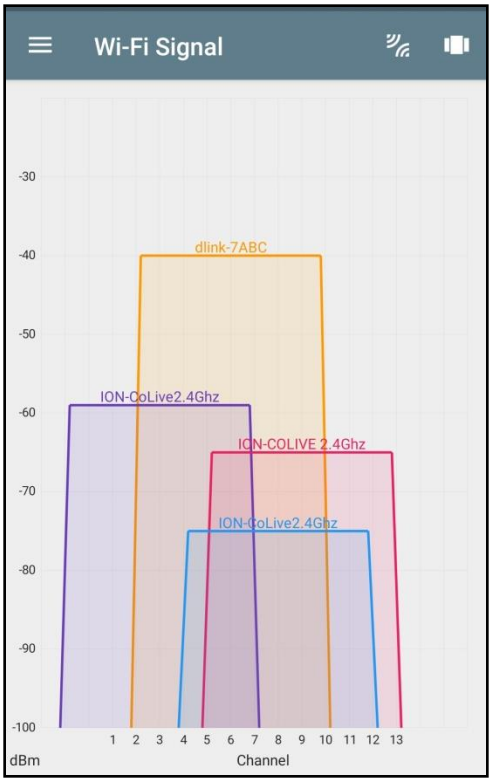
Bandwidth : 80 MHz

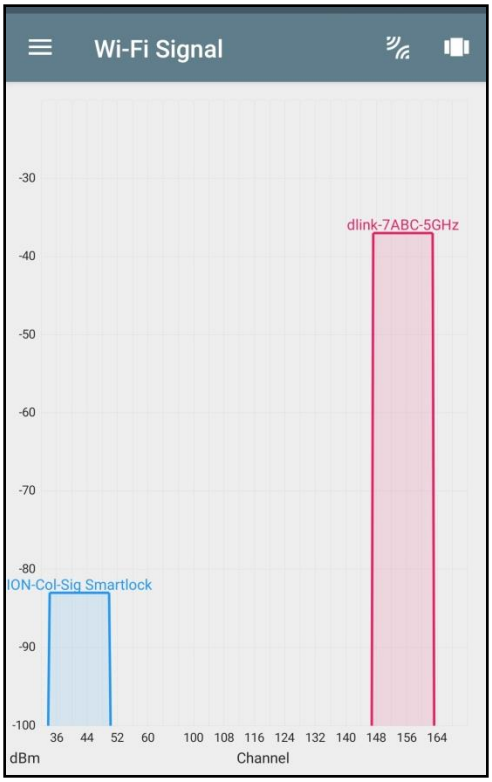
PHY Channel : 149th Channel

Encryption Scheme : WPA2/WPA (AES/TKIP)

Channel Graph :-

Following Channel Graphs were observed for both 2.4 and 5 GHz ISM bands. Even though the channels overlap, still we can see a clear distinction between them.



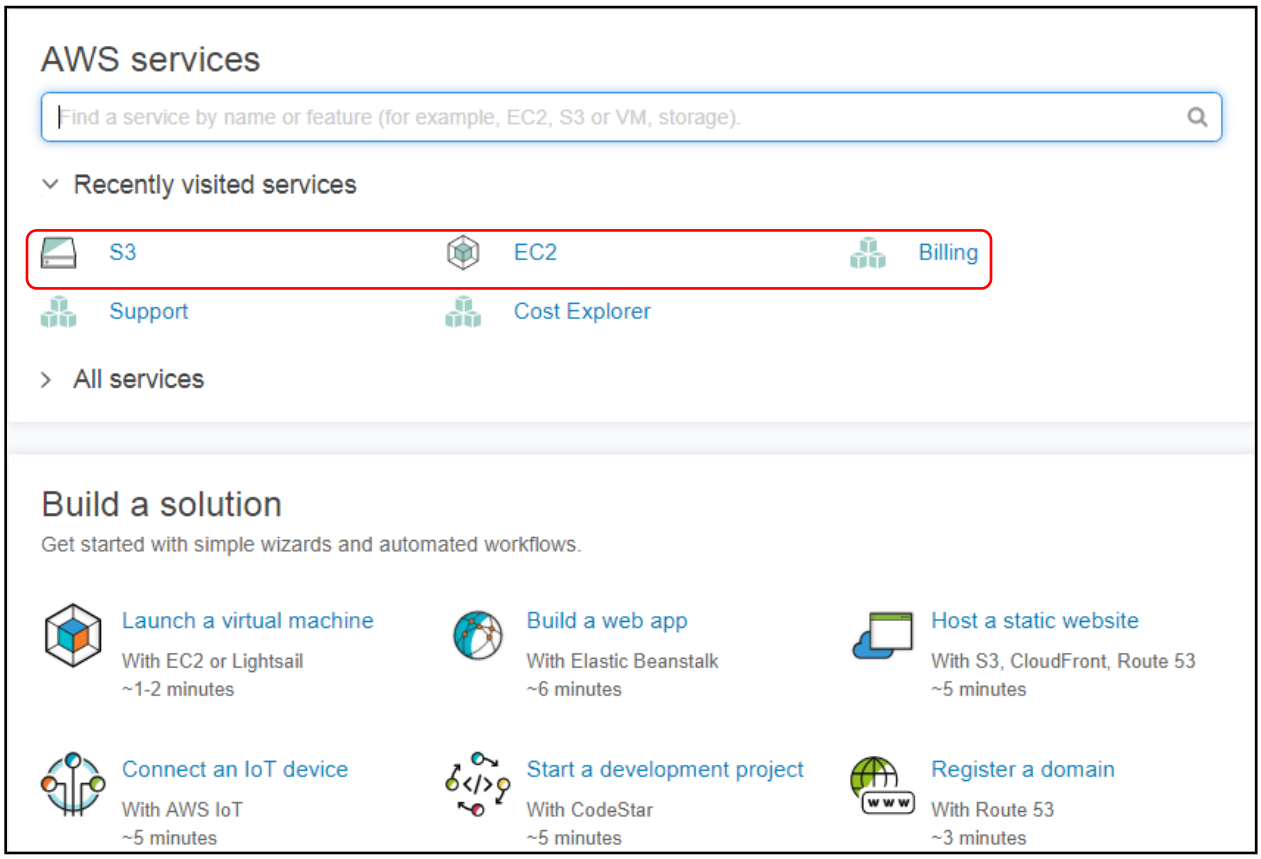


AWS EC2 :-

AWS Services :-

Explored some of the major AWS services such as :-

- Creating an instance using EC2 (Elastic Compute Cloud)
- Creating buckets and storing files using S3 (Simple Storage Service)
- Adding budget alarm using Billing interface



AWS EC2 Instance :-

The AMI that I chose had the following properties :-

Operating System : Linux

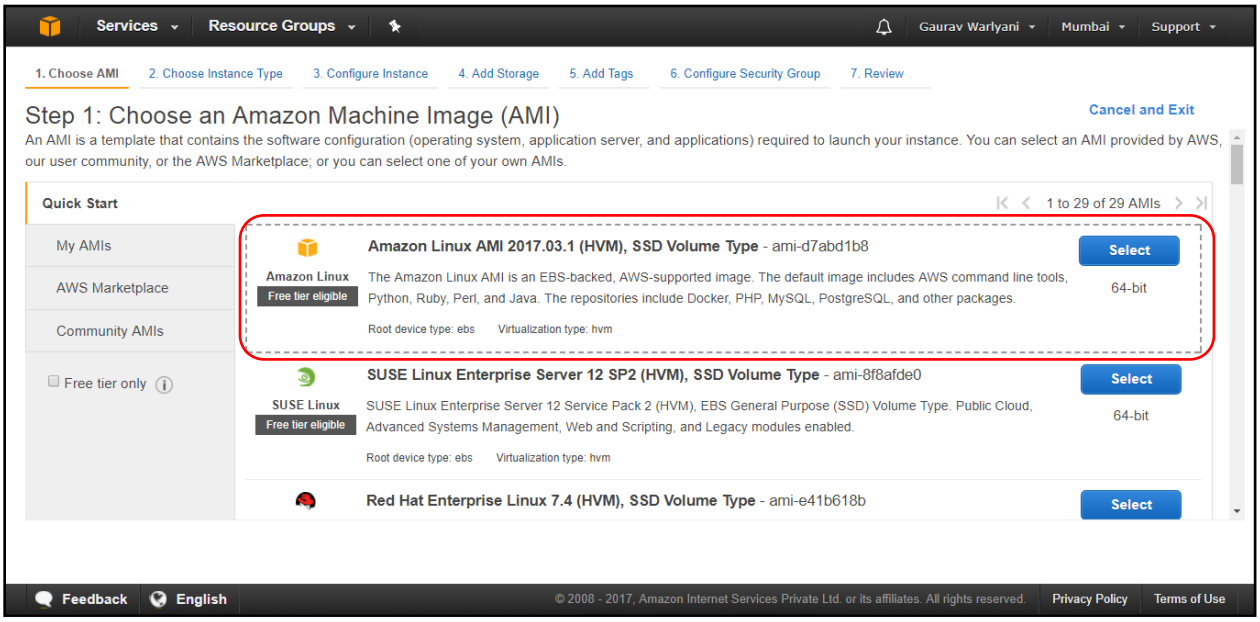
Instance Type : t2.micro

RAM : 1 GB

Internal HDD : 8GB

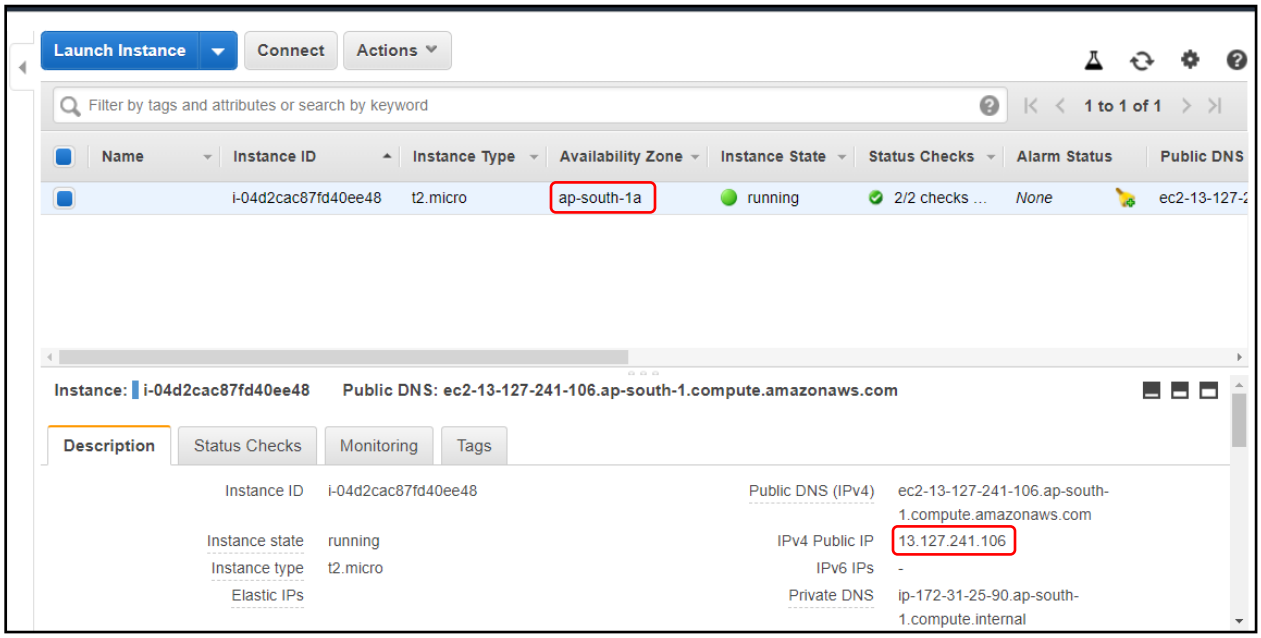
Processor : Intel 2.5 GHz

Security Group : HTTP, HTTPS and SSH (to access the Instance)



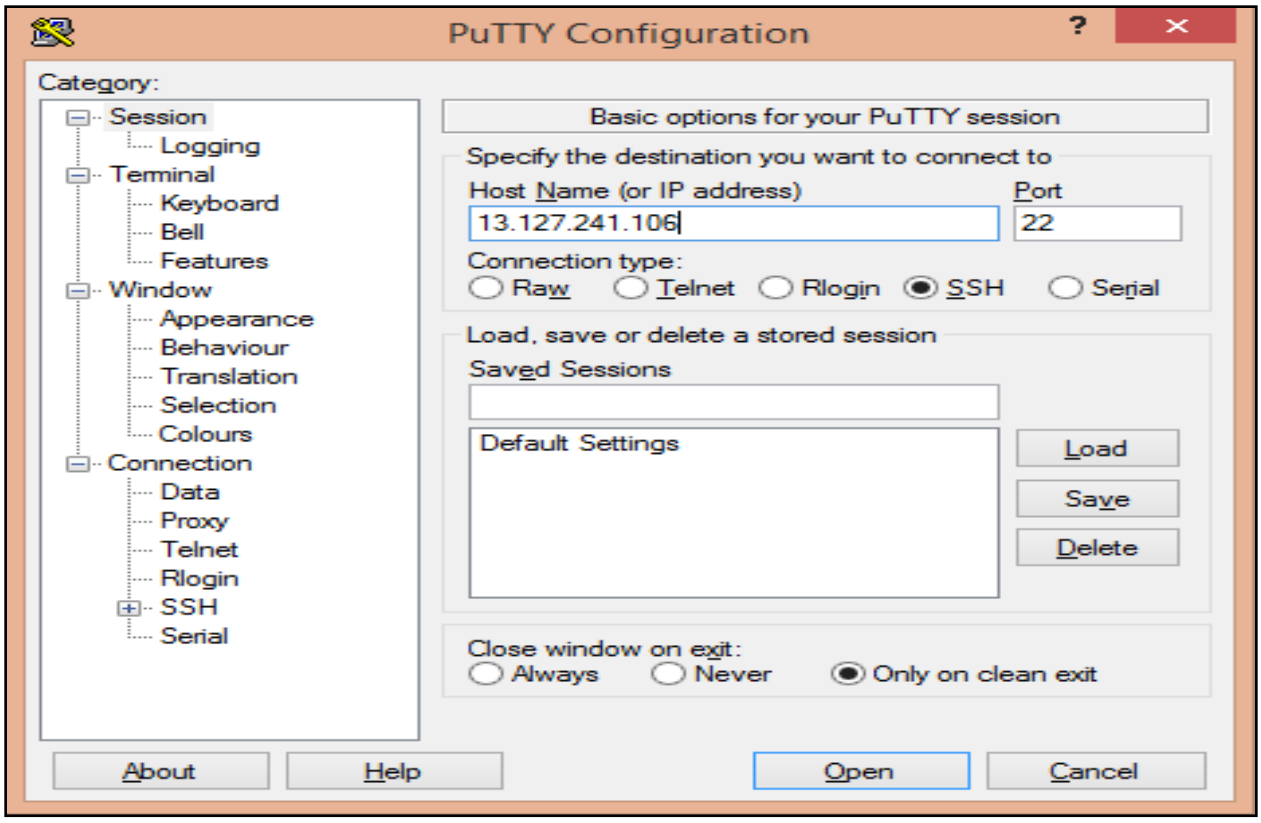
Launching the EC2 Instance :-

The instance was launched in the availability zone ap-south-1a (Asia Pacific) with IPv4 Public IP as : 13.127.241.106



Accessing the EC2 Instance :-

PPK file was generated via PuttyGen using the Public Key provided with AWS EC2 instance. Then, using Putty I was able to access my instance using the Public IP address and Port 22 (SSH).




```
[root@ip-172-31-25-90 ec2-user]# python BlockIP.py
[+] attempting to load demodata.pcap
[+] found valid header
[+] loaded 141 packets
[+] finished loading savefile.
little-endian capture file version 2.4
microsecond time resolution
snapshot length: 65535
linklayer type: LINKTYPE_ETHERNET
number of packets: 141

sudo -u root iptables -A INPUT -s 16.34.181.45 -j DROP
sudo -u root iptables -A INPUT -s 6.17.211.172 -j DROP
sudo -u root iptables -A INPUT -s 4.125.19.17 -j DROP
sudo -u root iptables -A INPUT -s 72.16.11.12 -j DROP
sudo -u root iptables -A INPUT -s 72.16.11.1 -j DROP
[root@ip-172-31-25-90 ec2-user]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  16.34.181.45         anywhere
DROP       all  --  6.17.211.172         anywhere
DROP       all  --  4.125.19.17          anywhere
DROP       all  --  h12.11.16.72.static.ip.windstream.net  anywhere
DROP       all  --  h1.11.16.72.static.ip.windstream.net  anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```