TASK 01 : BASIC NETWORK SNIFFER

I create a python program to detect and capture the Network packets

As you can see here

```
import socket
import struct
import sys

def main():
    if len(sys.argv) < 2:
        print("Usage: python sniffer.py <interface> [verbose]")
        sys.exit(1)

    interface = sys.argv[1]
    verbose = len(sys.argv) > 2 and sys.argv[2].lower() == "verbose"

    # Create a raw socket
    try:
        sniffer = socket.socket(socket.AF_INET, socket.SOCK_RAW,
socket.IPPROTO_IP)
    except PermissionError:
        print("Error: This script must be run as administrator or with root
privileges.")
        sys.exit(1)

    # Bind to the specified interface
    try:
        sniffer.bind((interface, 0))
    except socket.error as e:
        print(f"Error: Failed to bind to interface '{interface}'. Details: {e}")
        sys.exit(1)

    # Include the IP headers in the capture
    sniffer.setsockopt(socket.IPPROTO_IP, socket.IP_HDRINCL, 1)

    # Enable promiscuous mode (Windows only)
    if sys.platform == "win32":
```

```
        sniffer.ioctl(socket.SIO_RCVALL, socket.RCVALL_ON)

    try:
        print(f"Sniffer is running on interface '{interface}'... Press Ctrl+C to
stop.")
        while True:
            # Receive packets
            raw_packet = sniffer.recvfrom(65565)
            packet = raw_packet[0]

            # Extract and display the IP header
            ip_header = packet[0:20]
            unpacked_header = struct.unpack("!BBHHHBBH4s4s", ip_header)
            source_ip = socket.inet_ntoa(unpacked_header[8])
            destination_ip = socket.inet_ntoa(unpacked_header[9])

            if verbose:
                print(f"Packet: {source_ip} -> {destination_ip}")
    except KeyboardInterrupt:
        print("\nStopping sniffer...")

    finally:
        # Disable promiscuous mode (Windows only)
        if sys.platform == "win32":
            sniffer.ioctl(socket.SIO_RCVALL, socket.RCVALL_OFF)

if __name__ == "__main__":
    main()
```

- **this is the code you have to save this file as sniffer .py . in notepad .**

once you save it then

- **then Open powershell and run as administrator**
- **run the ipconfig in PowerShell and note the ip of the desired interface .**

```
PS C:\Users\dell> ipconfig
```

run the ipconfig in powershell

```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::1041:1c8:6bcb:9e02%8
   IPv4 Address. . . . . . . . . . . : 192.168.0.114
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1
```

And note ip so the ip is 192.168.0.114 .

TO RUN THE COMMAND

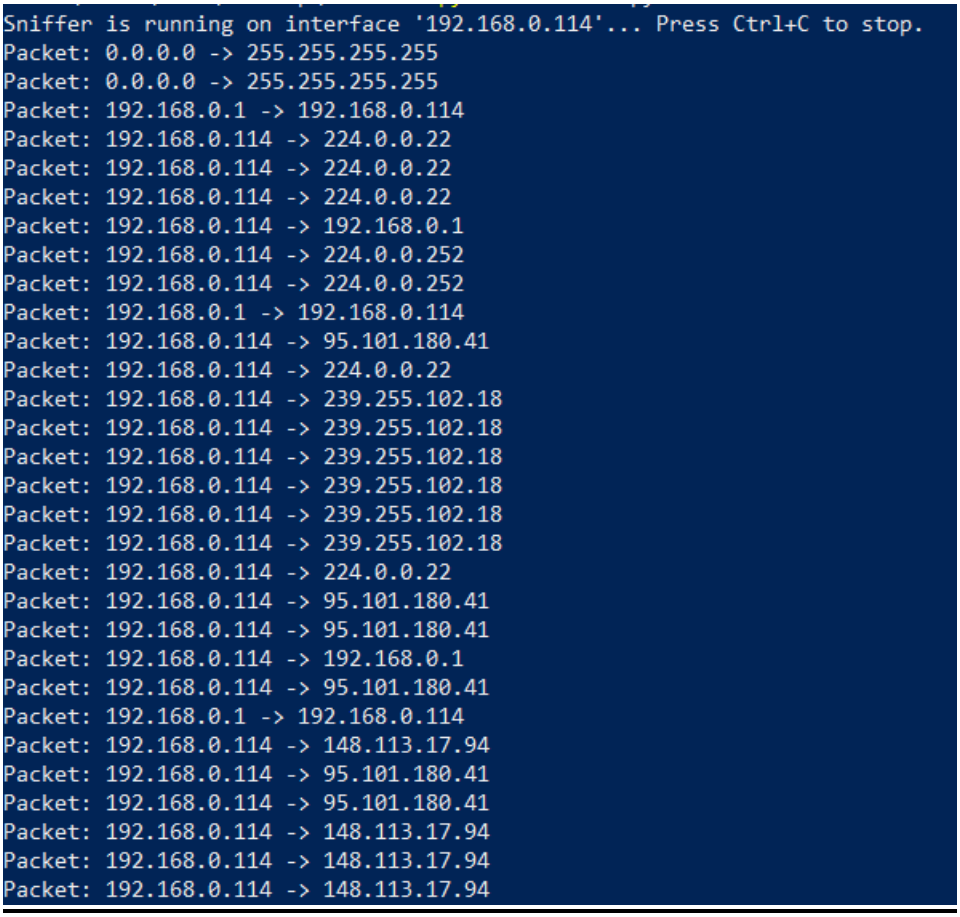
First go to file location of that program through powershell

```
PS C:\> cd /Users/dell/Desktop/sniffer
```

Now run the command to capture packet

```
PS C:\Users\dell\Desktop\sniffer> python sniffer.py 192.168.0.114 verbose
```

It Captures and detect packets


Sniffer is running on interface '192.168.0.114'... Press Ctrl+C to stop.
Packet: 0.0.0.0 -> 255.255.255.255
Packet: 0.0.0.0 -> 255.255.255.255
Packet: 192.168.0.1 -> 192.168.0.114
Packet: 192.168.0.114 -> 224.0.0.22
Packet: 192.168.0.114 -> 224.0.0.22
Packet: 192.168.0.114 -> 224.0.0.22
Packet: 192.168.0.114 -> 192.168.0.1
Packet: 192.168.0.114 -> 224.0.0.252
Packet: 192.168.0.114 -> 224.0.0.252
Packet: 192.168.0.1 -> 192.168.0.114
Packet: 192.168.0.114 -> 95.101.180.41
Packet: 192.168.0.114 -> 224.0.0.22
Packet: 192.168.0.114 -> 239.255.102.18
Packet: 192.168.0.114 -> 239.255.102.18
Packet: 192.168.0.114 -> 239.255.102.18
Packet: 192.168.0.114 -> 239.255.102.18
Packet: 192.168.0.114 -> 239.255.102.18
Packet: 192.168.0.114 -> 239.255.102.18
Packet: 192.168.0.114 -> 224.0.0.22
Packet: 192.168.0.114 -> 95.101.180.41
Packet: 192.168.0.114 -> 95.101.180.41
Packet: 192.168.0.114 -> 192.168.0.1
Packet: 192.168.0.114 -> 95.101.180.41
Packet: 192.168.0.1 -> 192.168.0.114
Packet: 192.168.0.114 -> 148.113.17.94
Packet: 192.168.0.114 -> 95.101.180.41
Packet: 192.168.0.114 -> 95.101.180.41
Packet: 192.168.0.114 -> 148.113.17.94
Packet: 192.168.0.114 -> 148.113.17.94
Packet: 192.168.0.114 -> 148.113.17.94