TASK-1

- BUILD A NETWORK SNIFFER IN PYTHON THAT CAPTURES AND ANALYZES NETWORK TRAFFIC.THS PROJECT WILL HELP YOU TO UNDERSTAND HOW DATA FLOWS ON A NETWORK AND HOW NETWORK PACKETS ARE STRUCTURED

WHAT IS NETWORK SNIFFER?

- SNIFFER:

A sniffer, also known as a packet analyzer or network analyzer, is a tool used to capture and analyze network traffic. It is a software or hardware tool that intercepts and records data packets transmitted between computers or devices on a network.Packet sniffers are commonly used for network troubleshooting, security analysis, and network optimization.

- NETWORK SNIFFER:
- A **network sniffer** "sniffs" or monitors network traffic for information (e.g., where it's coming from, which device, the protocol used, etc.). Network administrators can use this information to help optimize their environment.
- Types of sniffers:
- ARP spoofing
- Password Sniffer
- Mac Sniffers

A PYTHON PROGRAM THAT CAPTURES AND ANALYZES NETWORK TRAFFIC

```
import scapy.all as scapy
from scapy.layers import http
def process_packet(packet):
        if  packet.haslayer(http.HTTPRequest):
            print(packet[http.HTTPRequest].Host.decode())

def sniffing(interface):
scapy.sniff(iface=interface,store=False,prn=process_packet,filter='tcp')
sniffing('Wi-Fi')
```

NOTE: We have to replace Wi-Fi with Wi-Fi interface(like Wlan())

EXPLAINATION ABOUT CODE

- Import scapy.all as scapy:

Using scapy, a user will be able to send, sniff, dissect and forge network packets. Scapy also has the capability to store the sniffed packets in a pcap file.

➢ Scapy:

Scapy is a python package used to sniff, analyze, and send and receive arbitrary network packets. It comes with many of the common network layers built in. It can send packets at the "link layer", which means that even custom Wi-Fi packets are possible

➢ Scapy. Sniff():

Scapy's in-built sniff() function helps us capture all traffic: sniff() has count , filter , iface , lfilter , prn,timeout options. Can apply BPF filters . (Same as TCPDUMP).

➢ Interface:

The Wi-Fi interface module provides full Ethernet packet access. It's actually a Wireless Ethernet network where the Ethernet packets are exchanged in the same way as on wired networks.