Assignment

Question -1

1) Python library Scapy, analyze the network packets associated with suspicious IP address

```
from scapy.all import*

def analyze_packets(ip_address):
packets = sniff(filters = "host" + ip_address, count= 1000)

print("Analyzing packets for IP address", ip_address)
print("Total packets captured:", len(packets))

# Analyze packet headers or payload
for packet in packets:
print(packet.summary())

# Replace "Suspicious_ip_adress" with actual IP address
Suspicious_ip_address = "x.x.x.x"
analyze_packets(suspicious_ip_address)
```

Expected Code

1)

```
from scapy.all import *

def packet_analysis(packet):

source_ip = packet[IP].src
destination_ip = packet[IP].dst
protocol = packet[IP].proto

# print packet details

print(f"Source IP: {source_ip}, Destination IP: {destination_ip},
      Protocol: {protocol}")

# Sniff network packets
def start_sniffing():

print("Starting packet sniffing...")

sniff(prn=packet_analysis, store=False)
```