```
import os
import socket
from struct import unpack

os.system("clear")
print("\n----------------------------------------------------")
print("\n------      SNIFFING PACKET AND ANALYZING     ------")
print("\n----------------------------------------------------\n")

# create an INET, raw socket
s = socket.socket(socket.AF_INET, socket.SOCK_RAW, socket.IPPROTO_TCP)

try:
    # receive a packet
    print("\n\n")
    packet = s.recvfrom(65565)
    print(packet)

    # packet string from tuple
    packet = packet[0]

    # take first 20 characters for the ip header
    ip_header = packet[0:20]
    print("\n\n")
    print(ip_header)

    # now unpack them :)
    iph = unpack('!BBHHHBBH4s4s', ip_header)

    version_ihl = iph[0]
    version = version_ihl >> 4
    ihl = version_ihl & 0xF

    iph_length = ihl * 4

    ttl = iph[5]
    protocol = iph[6]
    s_addr = socket.inet_ntoa(iph[8])
    d_addr = socket.inet_ntoa(iph[9])

    print('\nVersion : ' + str(version) + '\nIP Header Length : ' + str(ihl) + '\nTTL : ' + str(
        ttl) + '\nProtocol : ' + str(protocol) + '\nSource Address : ' + str(
        s_addr) + '\nDestination Address : ' + str(d_addr))

    tcp_header = packet[iph_length:iph_length + 20]

    # now unpack them :)
    tcph = unpack('!HHLLBBHHH', tcp_header)

    source_port = tcph[0]
    dest_port = tcph[1]
    sequence = tcph[2]
    acknowledgement = tcph[3]
    doff_reserved = tcph[4]
    tcph_length = doff_reserved >> 4

    print('\nSource Port : ' + str(source_port) + '\nDest Port : ' + str(dest_port) + '\nSequence Number : ' + str(
        sequence) + '\nAcknowledgement : ' + str(acknowledgement) + '\nTCP header length : ' + str(tcph_length))

    h_size = iph_length + tcph_length * 4
    data_size = len(packet) - h_size

    # get data from the packet
    data = packet[h_size:]

    print('\nData : ', str(data))
    print()

except socket.error as e:
    print("Socket error:", e)
finally:
    s.close()

print("--------------------- End of Sniffer Program ----------------------")
```

```
----------------------------------------------------

------      SNIFFING PACKET AND ANALYZING     ------

----------------------------------------------------



(b'E\x00\x03M\xccA@\x00@\x06\x13\x19\xac\x1c\x00\x0c\xac\x1c\x00\x0c#(\xdb\x9c\tZt\xa7\xacz\x97\xef\x80\x18\x02\x00[\x90\x00\x00\x01\x01


b'E\x00\x03M\xccA@\x00@\x06\x13\x19\xac\x1c\x00\x0c\xac\x1c\x00\x0c'

Version : 4
IP Header Length : 5
TTL : 64
Protocol : 6
Source Address : 172.28.0.12
Destination Address : 172.28.0.12

Source Port : 9000
Dest Port : 56220
Sequence Number : 156923047
Acknowledgement : 2893715439
TCP header length : 8

Data :  b'\x81~\x03\x15{"header": {"msg_id": "3a29937c-06a5df7c1b8a8c4c4d302acb_325", "msg_type": "stream", "username": "username", "ses

--------------------- End of Sniffer Program ----------------------
```