PACKET SNIFFER

1. DEFINITION:

Packet sniffers are applications or utilities that read data packets traversing the network within the Transmission Control Protocol/Internet Protocol (TCP/IP) layer. When in the hands of network administrators, these tools “sniff” internet traffic in real-time, monitoring the data, which can then be interpreted to evaluate and diagnose performance problems within servers, networks, hubs and applications.

When packet sniffing is used by hackers to conduct unauthorized monitoring of internet activity, network administrators can use one of several methods for detecting sniffers on the network. Armed with this early warning, they can take steps to protect data from illicit sniffers.

Ways To protect networks from illicit sniffers:

- Do not use public Wi-Fi networks
- Rely on a trusted VPN connection
- Always deploy robust antivirus software
- Look for secure HTTPS protocols before surfing the web
- Don’t fall prey to social engineering tricks and traps

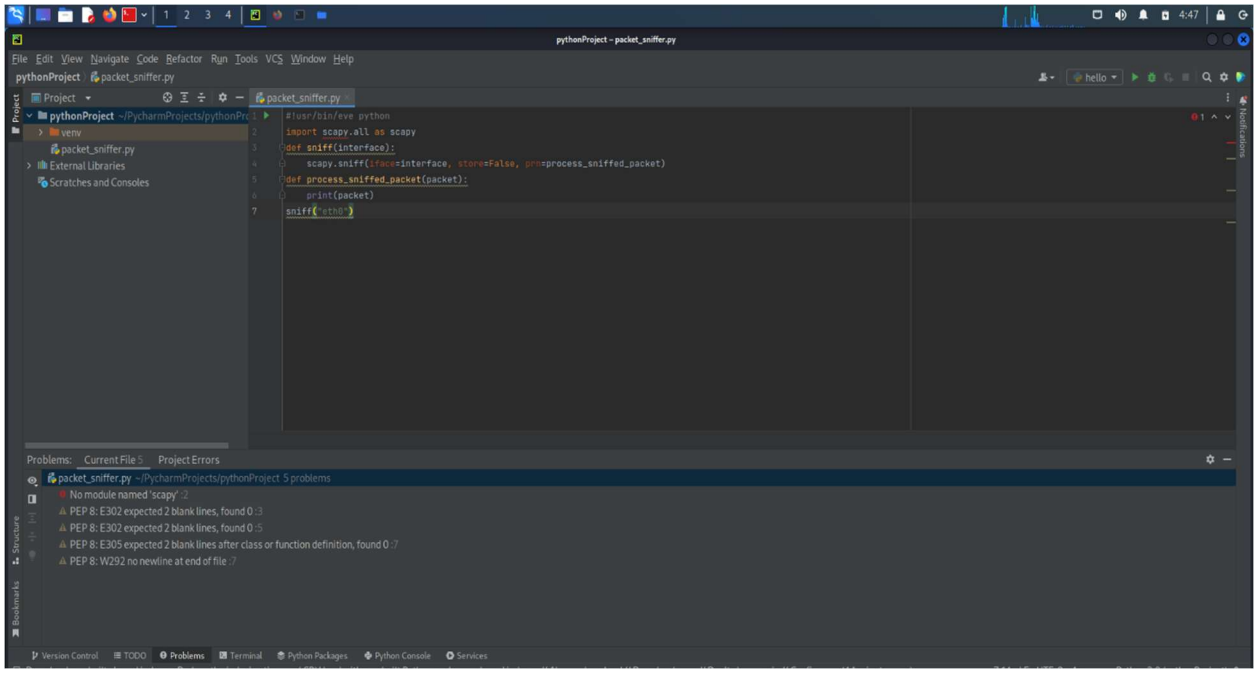
2. TOOLS REQURIED

- Kali Linux
- PyCharm
- Python3

3. PROCEDURE:

Step-1: Sniffing packets using Scapy:

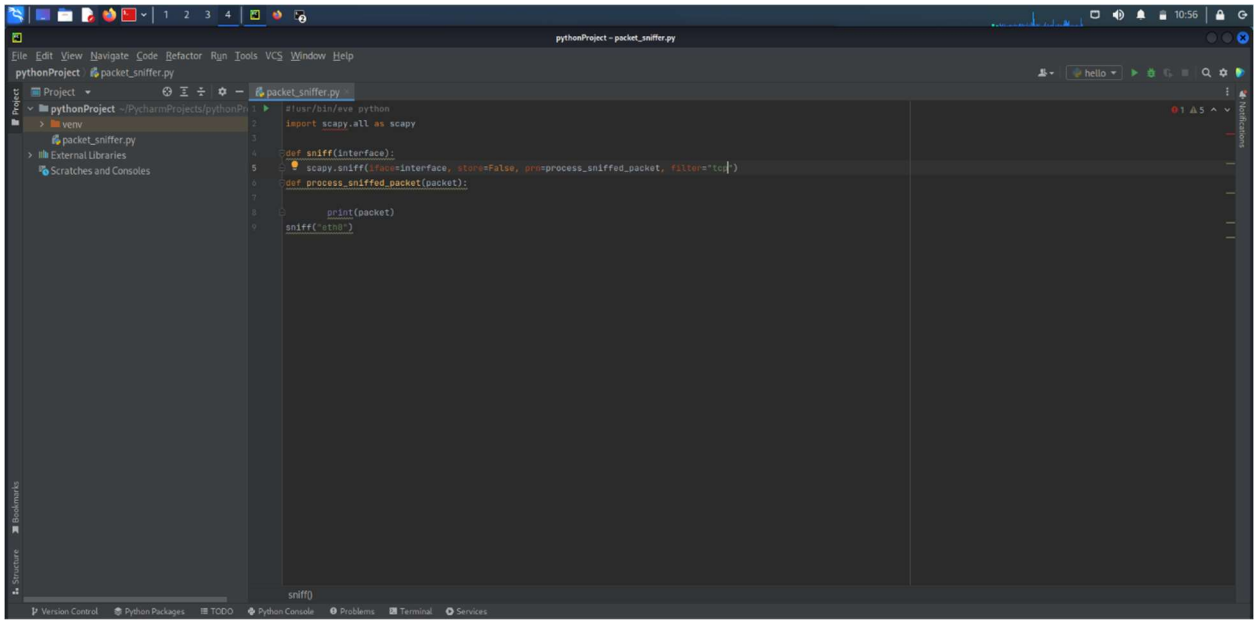
To sniff the packets, use the sniff () function. The sniff () function returns information about all the packets that has been sniffed. It can capture data sent to/ from interface.



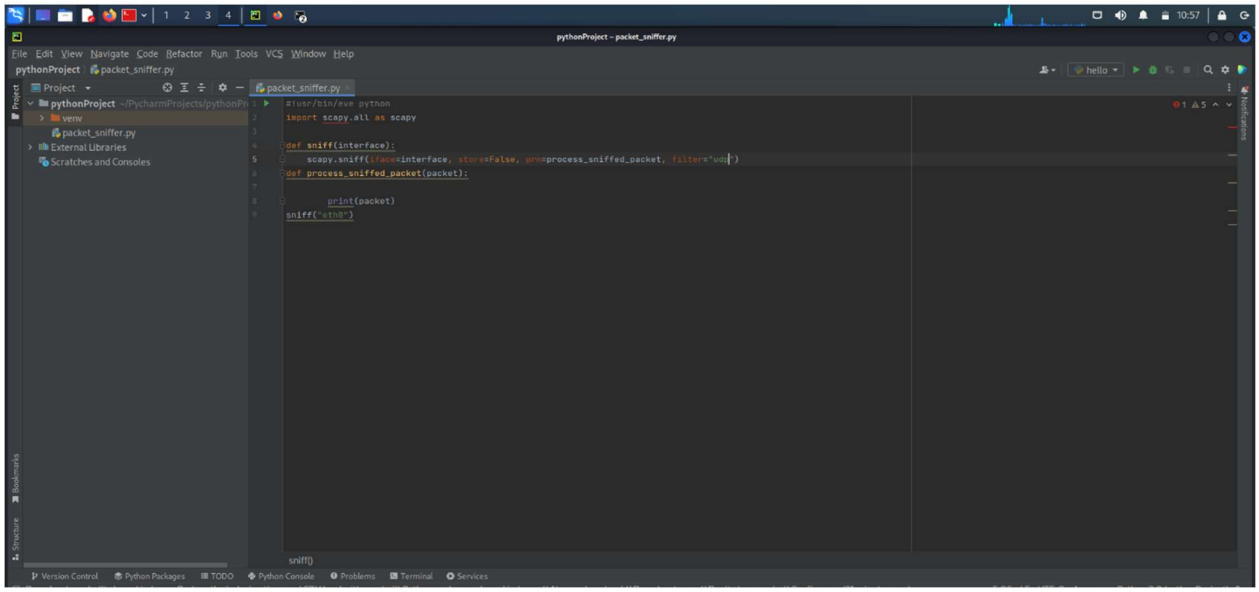
<u>Step-2:</u> Extracting data From a Specific Layer:

There are different layers like TCP, UDP, etc. We use filter=” layer name ” to extract data.

<u>UDP:</u>

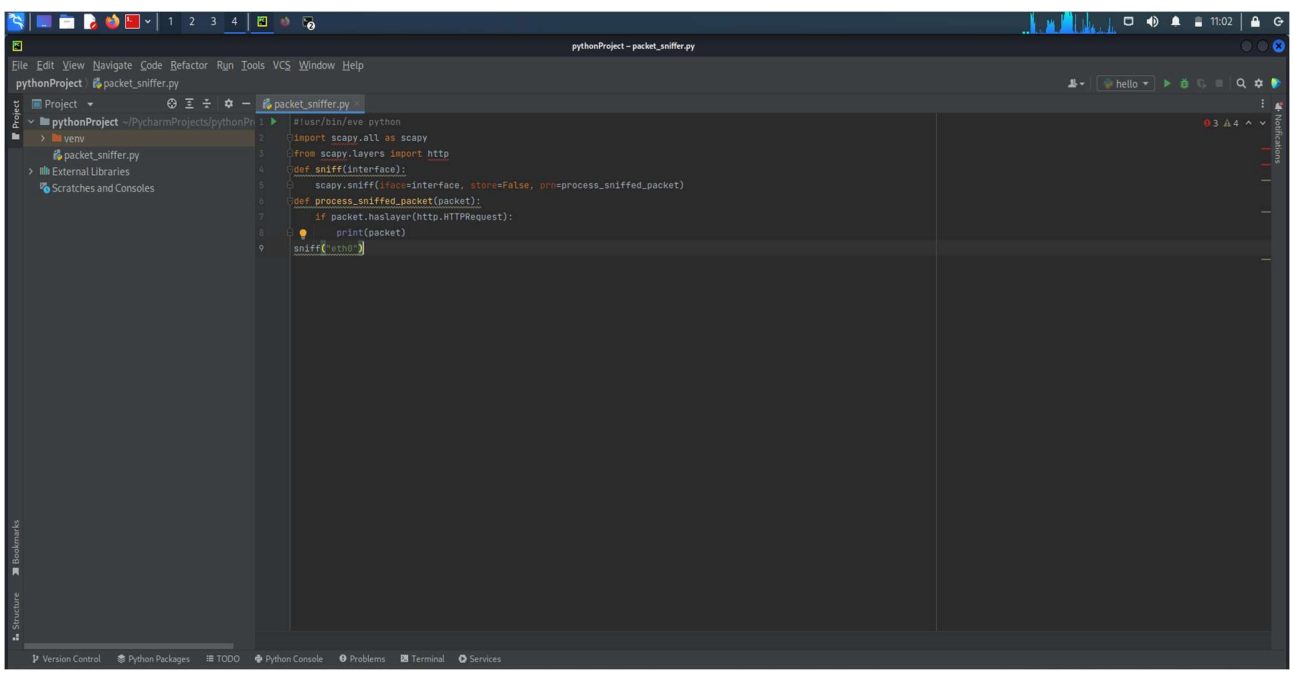


TCP:

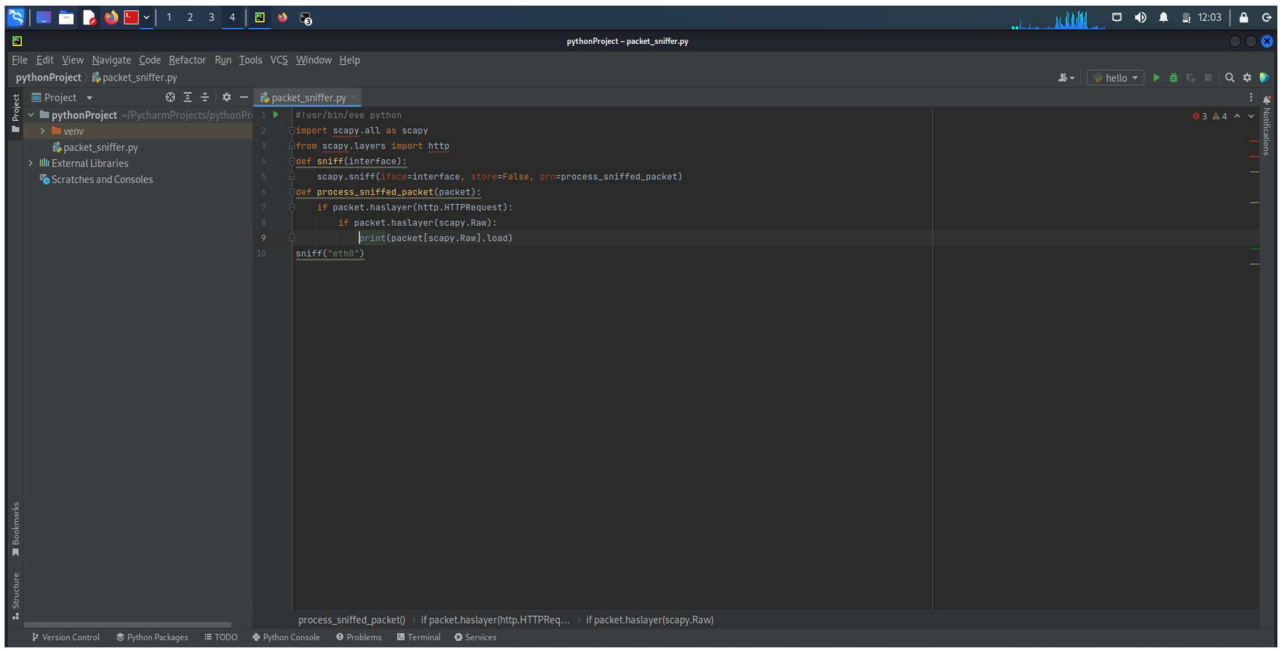


HTTP:

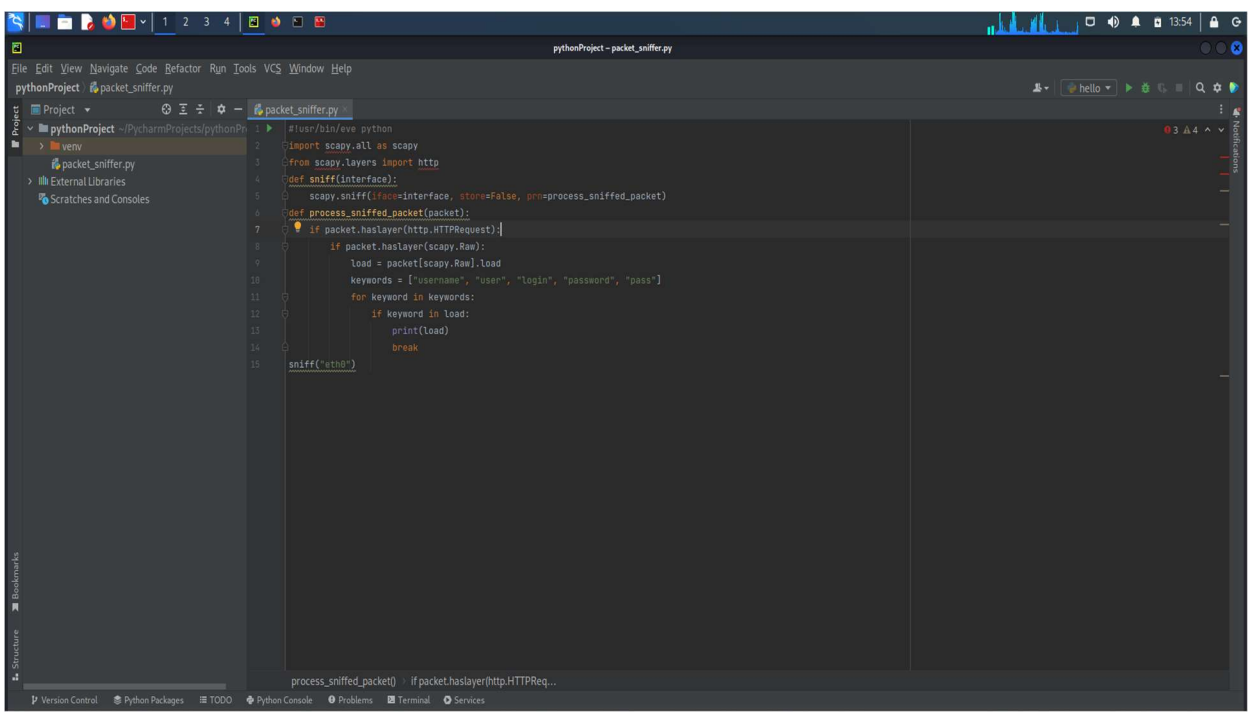
Scapy does not contain Http as default in its layer. So, we import http to scapy layer.



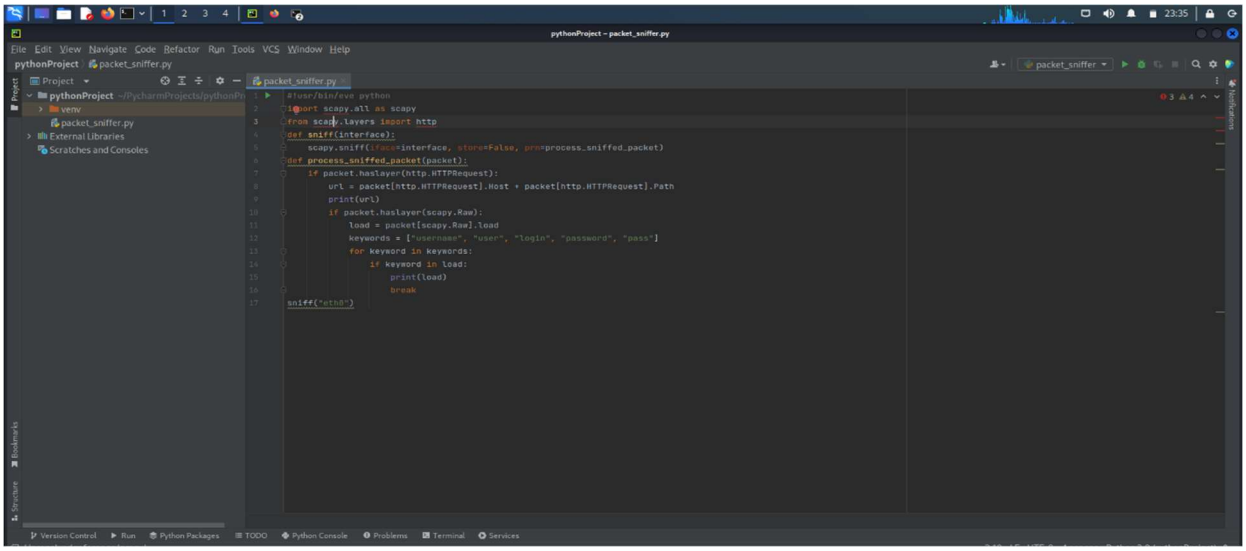
Step-3: Analyzing Sniffed Packets & Extracting Fields from Layers:



<u>Step-4:</u> Analyzing Fields and Extracting Passwords:

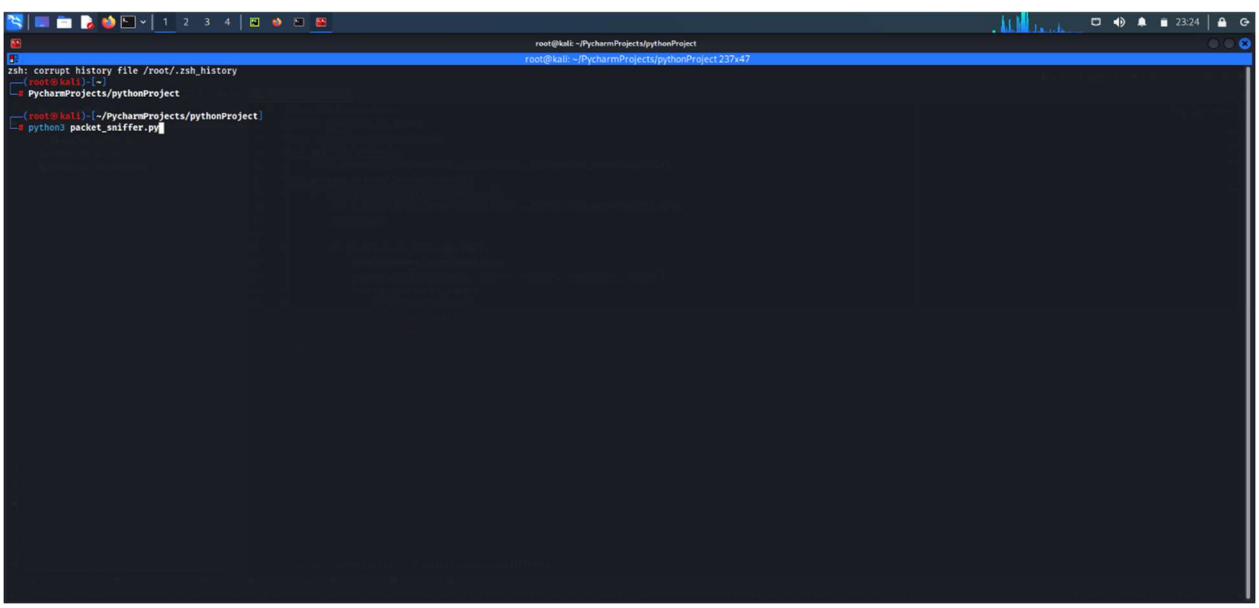


Step-5: Extracting URL:



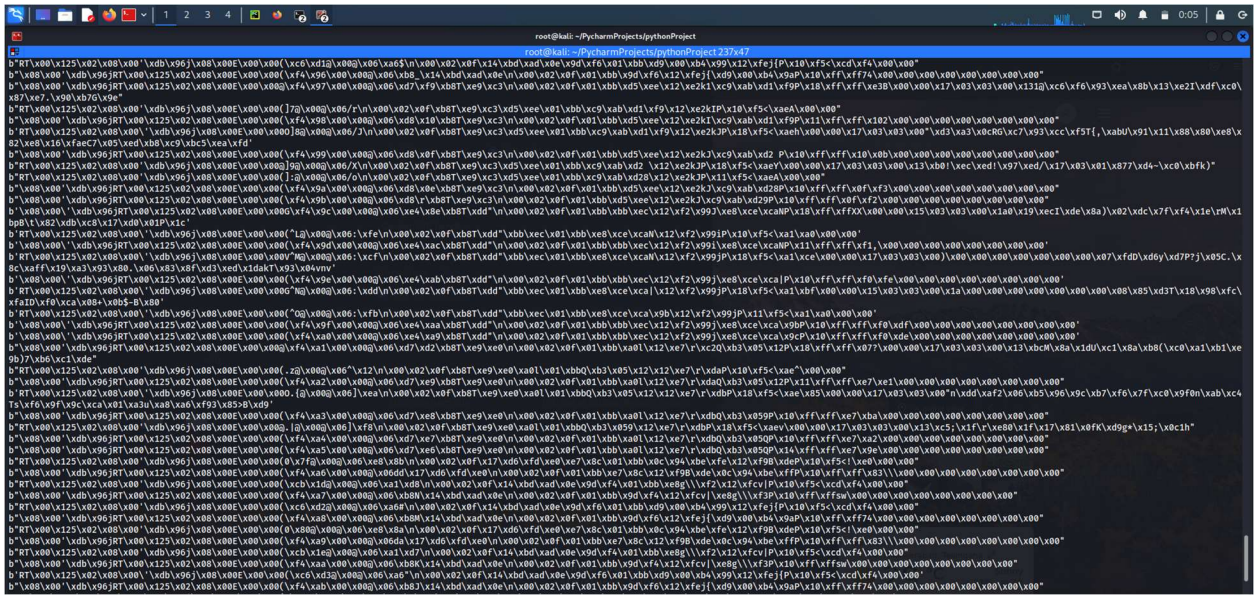
4. Execution:

Command: > python3 packet_sniffer.py

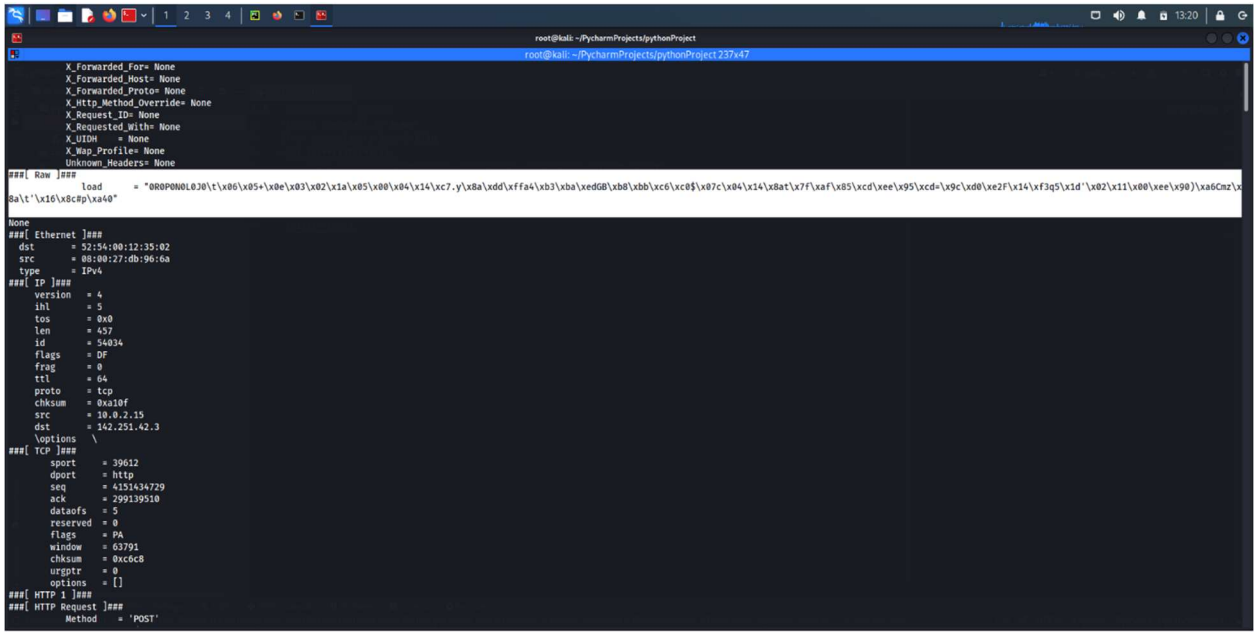


5. Output:

Step1:



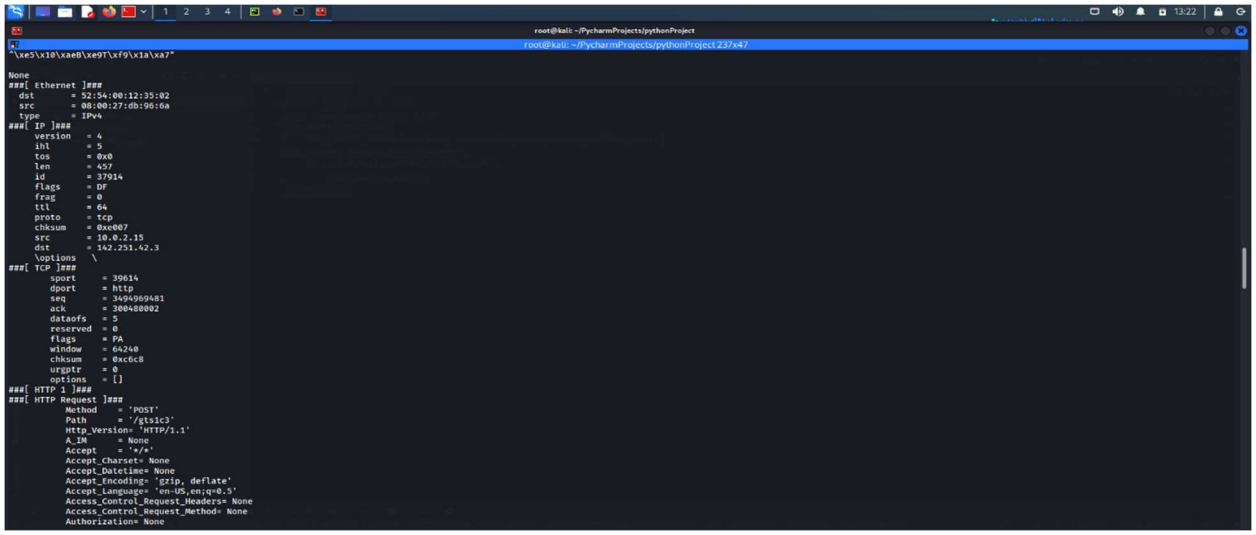
Step 2:



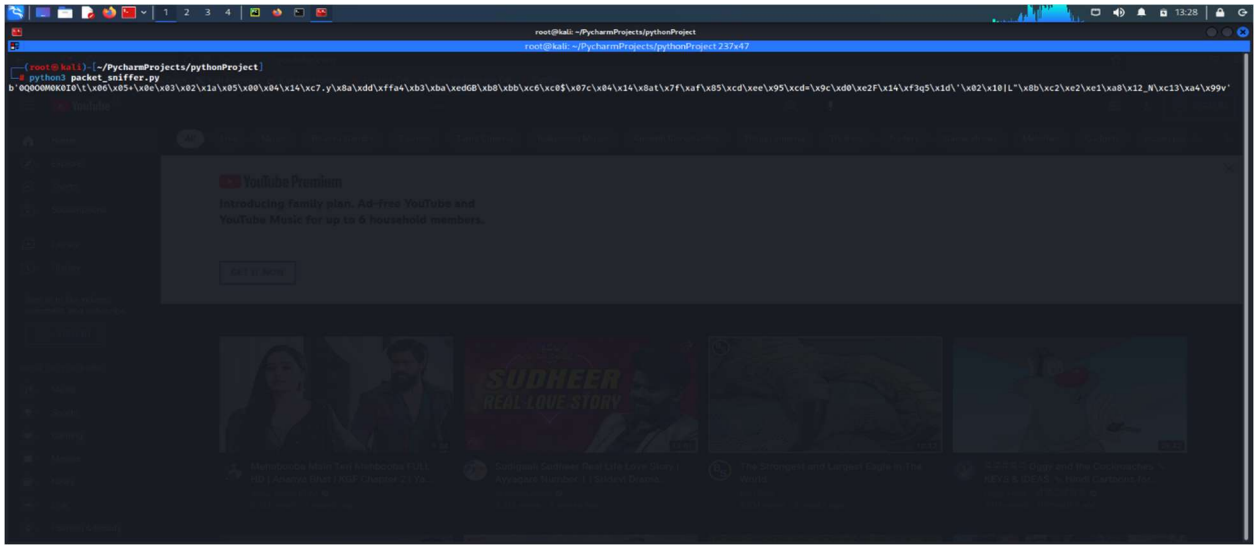
```
root@kali: ~/PycharmProjects/pythonProject
root@kali: ~/PycharmProjects/pythonProject 237x47
###[ HTTP Request ]###
          Method    = 'POST'
          Path      = '/gts1c3'
          Http_Version= 'HTTP/1.1'
          A_IM      = None
          Accept    = '*/*'
          Accept_Charset= None
          Accept_Datetime= None
          Accept_Encoding= 'gzip, deflate'
          Accept_Language= 'en-US,en;q=0.5'
          Access_Control_Request_Headers= None
          Access_Control_Request_Method= None
          Authorization= None
          Cache_Control= 'no-cache'
          Connection= 'keep-alive'
          Content_Length= '84'
          Content_MD5= None
          Content_Type= 'application/ocsp-request'
          Cookie    = None
          DNT       = None
          Date      = None
          Expect    = None
          Forwarded = None
          From      = None
          Front_End_Https= None
          HTTP2_Settings= None
          Host      = 'ocsp.pki.goog'
          If_Match  = None
          If_Modified_Since= None
          If_None_Match= None
          If_Range  = None
          If_Unmodified_Since= None
          Keep_Alive= None
          Max_Forwards= None
          Origin    = None
          Permanent = None
          Pragma    = 'no-cache'
          Proxy_Authorization= None
          Proxy_Connection= None
          Range     = None
          Referer   = None
          Save_Data = None
          TE        = None
          Upgrade   = None
          Upgrade_Insecure_Requests= None
          Upgrade_Insecure_Requests= None
          User_Agent= 'Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0'
```

```
root@kali: ~/PycharmProjects/pythonProject
root@kali: ~/PycharmProjects/pythonProject 237x47
          Upgrade_Insecure_Requests= None
          User_Agent= 'Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0'
          Via       = None
          Warning   = None
          X_ATT_DeviceId= None
          X_Correlation_ID= None
          X_Csrf_Token= None
          X_Forwarded_For= None
          X_Forwarded_Host= None
          X_Forwarded_Proto= None
          X_Http_Method_Override= None
          X_Request_ID= None
          X_Requested_With= None
          X_UIDH    = None
          X_Wap_Profile= None
          Unknown_Headers= None
###[ Raw ]###
          load      = "0R0P0N0L0J0\t\x06\x05+\x0e\x03\x02\x1a\x05\x00\x04\x14\xc7.y\x8a\xdd\xffa4\xb3\xba\xedGB\xb8\xbb\xc6\xc0$\x07c\x04\x14\x8at\x7f\xaf\x85\xcd\xee\x95\xcd=\x9c\xd0\xe2F\x14\xf3q5\x1d'\x02\x11\x00\xbb\xce\x11C6\x83
"\xe5\x10\xae8\xe9T\xf9\x1a\xa7"

None
###[ Ethernet ]###
  dst       = 52:54:00:12:35:02
  src       = 08:00:27:db:96:6a
  type      = IPv4
###[ IP ]###
     version   = 4
     ihl       = 5
     tos       = 0x0
     len       = 457
     id        = 25444
     flags     = DF
     frag      = 0
     ttl       = 64
     proto     = tcp
     chksum    = 0x10be
     src       = 10.0.2.15
     dst       = 142.251.42.3
     \options   \
###[ TCP ]###
        sport     = 39610
        dport     = http
        seq       = 3483548602
        ack       = 299077616
        dataofs   = 5
        reserved  = 0
        flags     = PA
```

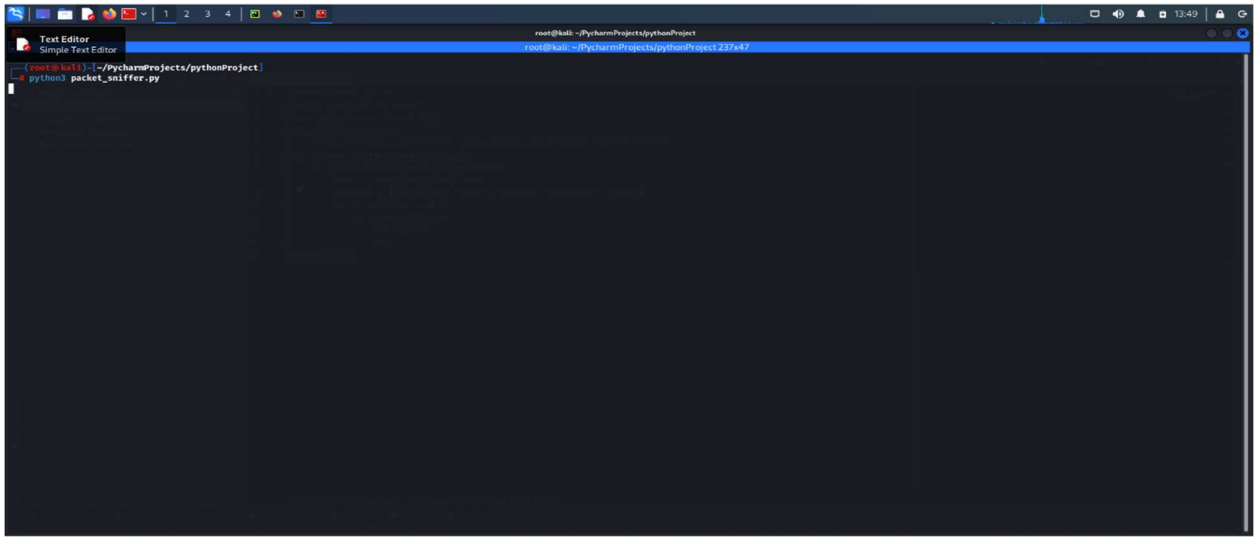

root@kali: ~/PycharmProjects/pythonProject
root@kali: ~/PycharmProjects/pythonProject 237x47
"\xe5\x10\xaeB\xe9T\xf9\x1a\xa7"
None
###[Ethernet]###
dst = 52:54:00:12:35:02
src = 08:00:27:db:96:6a
type = IPv4
###[IP]###
version = 4
ihl = 5
tos = 0x0
len = 457
id = 37914
flags = DF
frag = 0
ttl = 64
proto = tcp
chksum = 0xe007
src = 10.0.2.15
dst = 142.251.42.3
\options \
###[TCP]###
sport = 39614
dport = http
seq = 3494969481
ack = 300480002
dataofs = 5
reserved = 0
flags = PA
window = 64240
chksum = 0xc6c8
urgptr = 0
options = []
###[HTTP 1]###
###[HTTP Request]###
Method = 'POST'
Path = '/gts1c3'
Http_Version= 'HTTP/1.1'
A_IM = None
Accept = '*/*'
Accept_Charset= None
Accept_Datetime= None
Accept_Encoding= 'gzip, deflate'
Accept_Language= 'en-US,en;q=0.5'
Access_Control_Request_Headers= None
Access_Control_Request_Method= None
Authorization= None

Step 3:


root@kali: ~/PycharmProjects/pythonProject
root@kali: ~/PycharmProjects/pythonProject 237x47
(root@kali)-[~/PycharmProjects/pythonProject]
python3 packet_sniffer.py
b'0QOOAMOKDI0\l\x00\x05+\x0e\x03\x02\x1a\x05\x00\x04\x14\xc7.y\x8a\xdd\xffa4\xb3\xba\xedGB\xb8\xbb\xc6\xc0$\x07c\x04\x14\x8at\x7f\xaf\x85\xcd\xee\x95\xcd=\x9c\xd0\xe2F\x14\xf3q5\x1d\'\x02\x10|L"\x8b\xc2\xe2\xe1\xa8\x12_N\xc13\xa4\x99v'
Introducing family plan. Ad-free YouTube and
YouTube Music for up to 6 household members.
SUDHEER
REAL LOVE STORY

Step- 4:

There is no keywords in my raw so output is empty.



Step-5: