ASSIGNMENT NO: 04

/*

Name: Alok Bhawankar

Roll No.: PD09

Subject: DFCL

*/

Problem Statement:

Write a Java/Python program to monitor and analyse Network Forensics, also perform investigation of various logs.

Objectives:

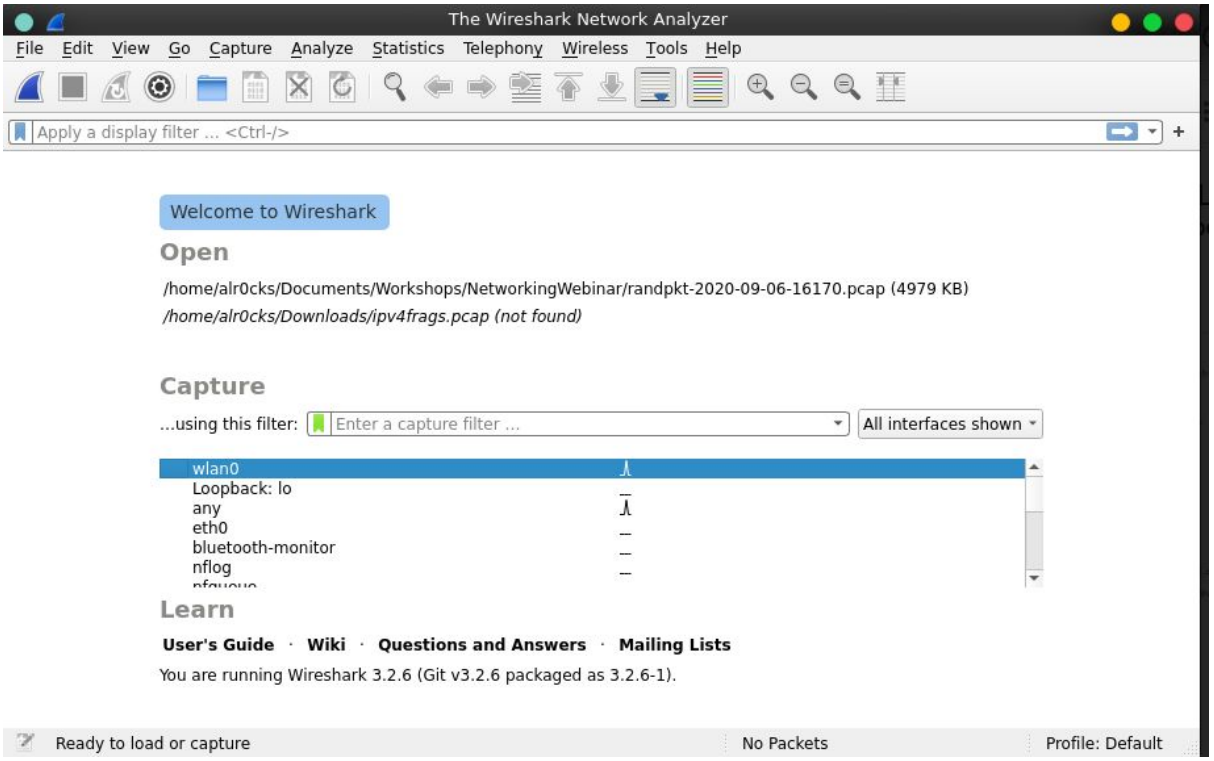
1. To study and explore Wireshark and its features.
2. To create analysis on Log Captured.

Theory:

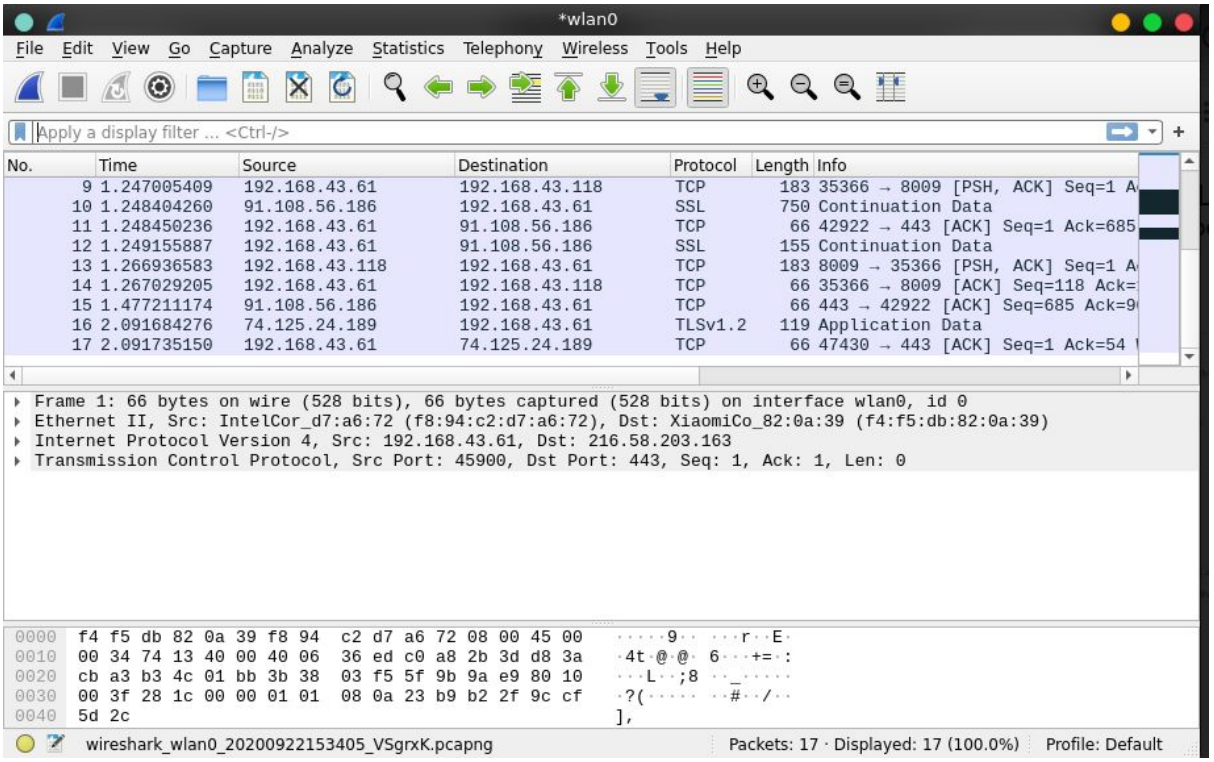
Wireshark supports feature such as:
1. Live capture and offline analysis.
2. Multi-platform support.
3. Rich VOIP Analysis.
4. Output can be exported to XML, PostScript, CSV, or plain text.
5. Decryption support for many protocols such as IPsec, Kerberos, SNMP, SSL/TLS and
WPA/WPA2.

Implementation:

1)Install Wireshark in the System.
2)Open Wireshark and start capturing packets.



3. Stop the capture of packets after browsing.



4. Save the captured packet as csv file.

5. Import the csv in python program.

6. Create a dataframe consisting of all features of csv

7. Search for the given input and display all the values of the matching row.

Code:

```
import pandas as pd

col_list = ["No.",
"Time","Source","Destination","Protocol","Length","Info"]
file=pd.read_csv("./file.csv", usecols=col_list)
file.head(20)

def source(ip1,file):
   selec = pd.DataFrame(file.loc[file['Source'] == ip1])
   return selec

def des(ip1,file):
   selec = pd.DataFrame(file.loc[file['Destination'] == ip1])
   return selec

def proto(ip1,file):
   selec = pd.DataFrame(file.loc[file['Protocol'] == ip1])
   return selec

def cleen(selec):
   rmv=[]
   for  i in range(len(selec)-2):
       if selec['Destination'][i]==selec['Destination'][i+1] and
selec['Destination'][i+1]==selec['Destination'][i+2]:
           rmv.append(i+1)
   selec = selec.drop(rmv)
   selec=selec.drop(["No."],axis=1)
   return selec


ip1="192.168.43.37"
selec=file
#Clean the continuous repetitive occurances of IP
slec=cleen(selec)

ip1="192.168.43.37"
selec=file

selec=source(ip1,slec)
selec.head(5)
```

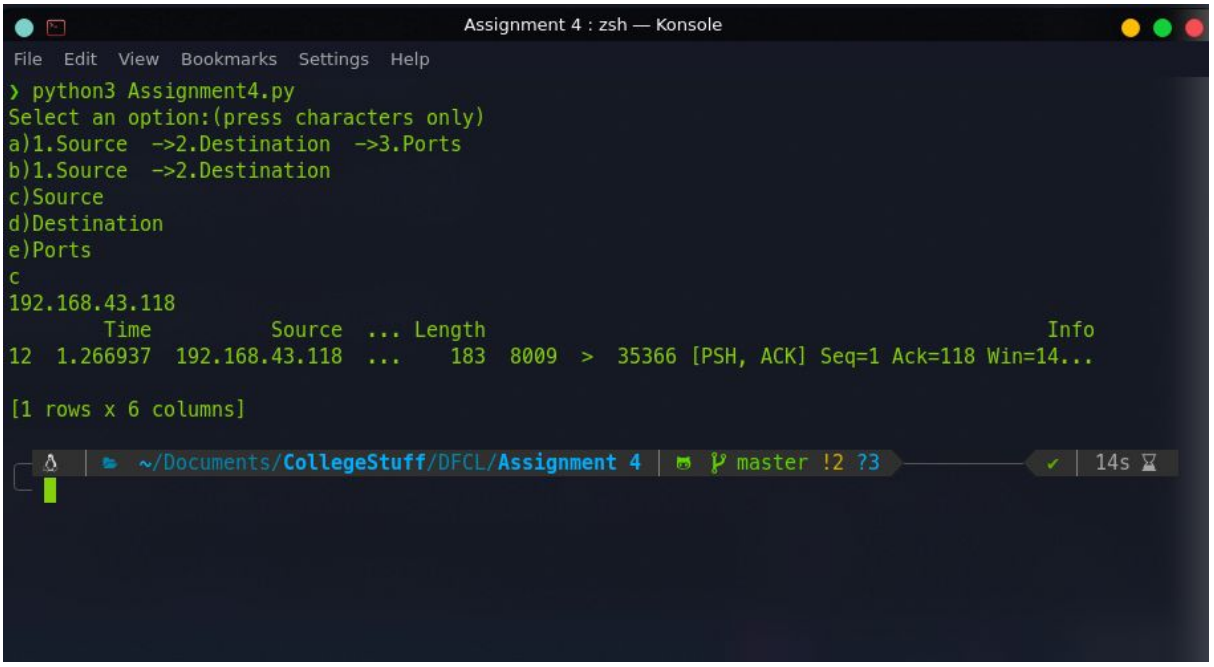
```
ip1="192.168.43.37"
selec=file
selec=des(ip1,slec)
selec.head(5)

ip1="UDP"
selec=file
selec=proto(ip1,slec)
selec.head(5)

print("Select an option:(press characters only)")
print("a)1.Source  ->2.Destination  ->3.Ports")
print("b)1.Source  ->2.Destination")
print("c)Source")
print("d)Destination")
print("e)Ports")
option=str(input())
selec=file
selec=cleen(selec)
if option=="a":
   sip=str(input())
   dip=str(input())
   pip=str(input())
   selec=source(sip,selec)
   selec=des(dip,selec)
   selec=proto(pip,selec)
   print(selec)
elif option=="b":
   sip=str(input())
   dip=str(input())
   selec=source(sip,selec)
   selec=des(dip,selec)
   print(selec)
elif option=="c":
   sip=str(input())
   selec=source(sip,selec)
   print(selec)
elif option=="d":
   dip=str(input())
   selec=des(dip,selec)
   print(selec)
elif option=="e":
```

```
    pip=str(input())
    selec=proto(pip,selec)
    print(selec)
else:
    print("Invalid Option!")
```

Dataset: Wireshark Packet Captured Dataset

Input: Source IP and/or Destination IP and/or Protocol

Output: Matched Dataset in CSV to the Input



Platform: Ubuntu 20.04

Programming Language Used: Python.

Conclusion: Hence, learned to use the Wireshark tool and analyze data through it.