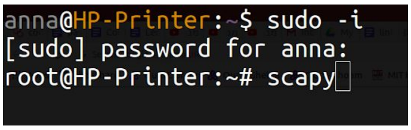
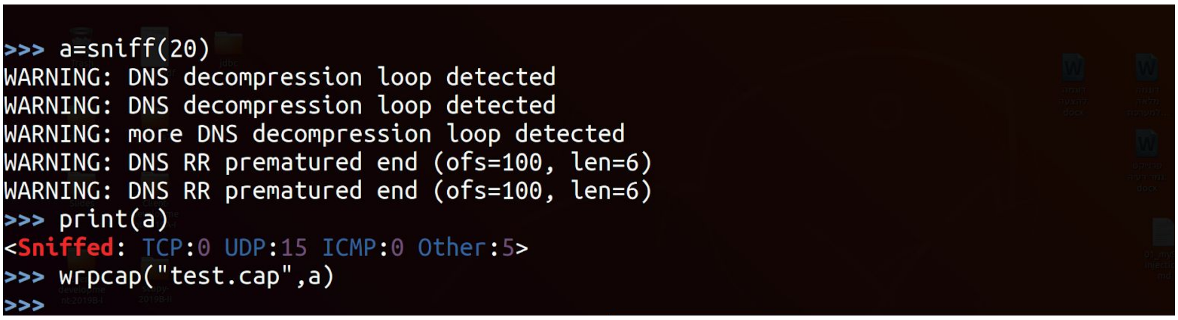
Importing and Exporting PCAP Data

Step 1 - run scapy as sudo



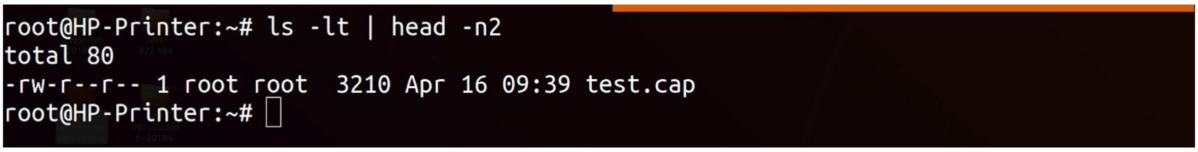
```
anna@HP-Printer:~$ sudo -i
[sudo] password for anna:
root@HP-Printer:~# scapy
```

Step 2 - sniff with scapy 20 packets, and save them to a “cap” file, named “test.cap”



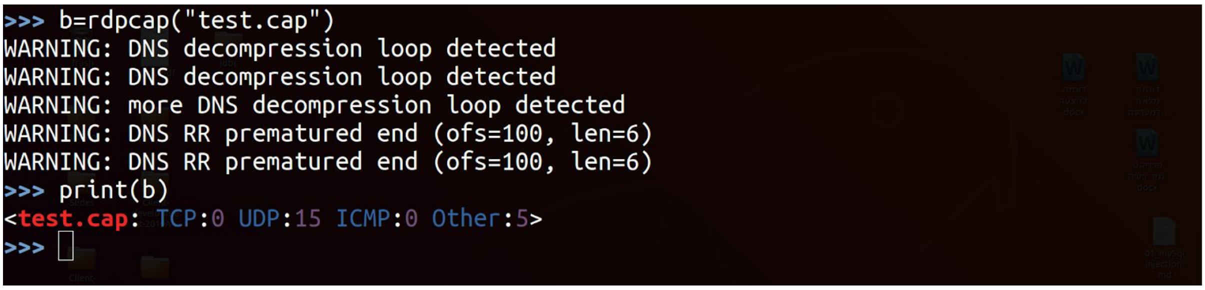
```
>>> a=sniff(20)
WARNING: DNS decompression loop detected
WARNING: DNS decompression loop detected
WARNING: more DNS decompression loop detected
WARNING: DNS RR prematured end (ofs=100, len=6)
WARNING: DNS RR prematured end (ofs=100, len=6)
>>> print(a)
<Sniffed: TCP:0 UDP:15 ICMP:0 Other:5>
>>> wrpcap("test.cap",a)
>>>
```

Step 3 - check from the terminal that “test.cap” created successfully



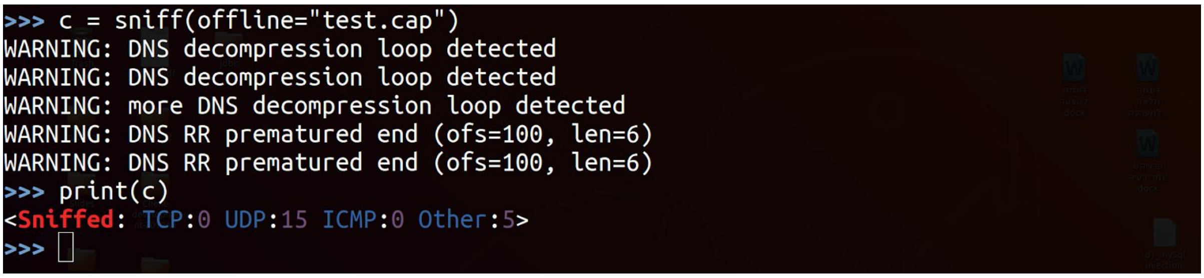
```
root@HP-Printer:~# ls -lt | head -n2
total 80
-rw-r--r-- 1 root root  3210 Apr 16 09:39 test.cap
root@HP-Printer:~#
```

Step 4 - first option to read with scapy the “test.cap” file



```
>>> b=rdpcap("test.cap")
WARNING: DNS decompression loop detected
WARNING: DNS decompression loop detected
WARNING: more DNS decompression loop detected
WARNING: DNS RR prematured end (ofs=100, len=6)
WARNING: DNS RR prematured end (ofs=100, len=6)
>>> print(b)
<test.cap: TCP:0 UDP:15 ICMP:0 Other:5>
>>>
```

Step 5 - second option to read with scapy the “test.cap” file



```
>>> c = sniff(offline="test.cap")
WARNING: DNS decompression loop detected
WARNING: DNS decompression loop detected
WARNING: more DNS decompression loop detected
WARNING: DNS RR prematured end (ofs=100, len=6)
WARNING: DNS RR prematured end (ofs=100, len=6)
>>> print(c)
<Sniffed: TCP:0 UDP:15 ICMP:0 Other:5>
>>>
```