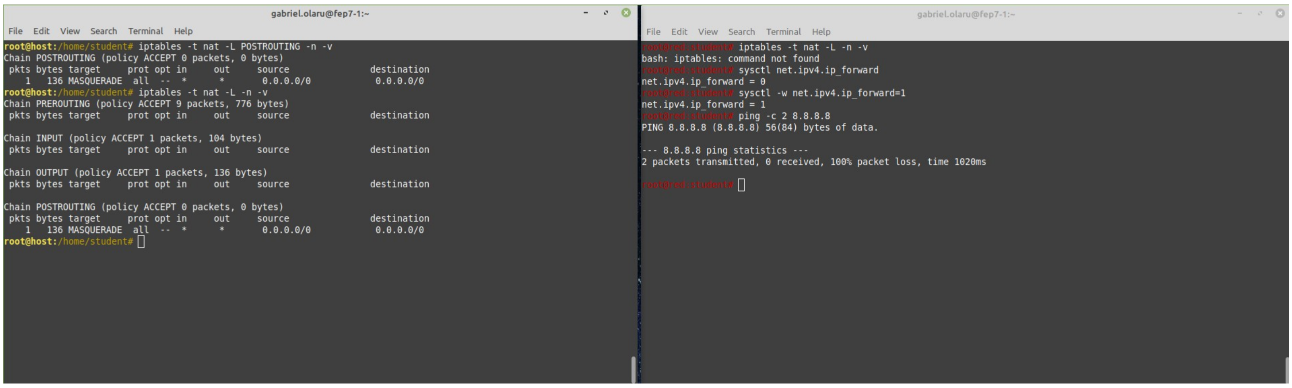
Olaru Gabriel Iulian
334 CC
Lab 09

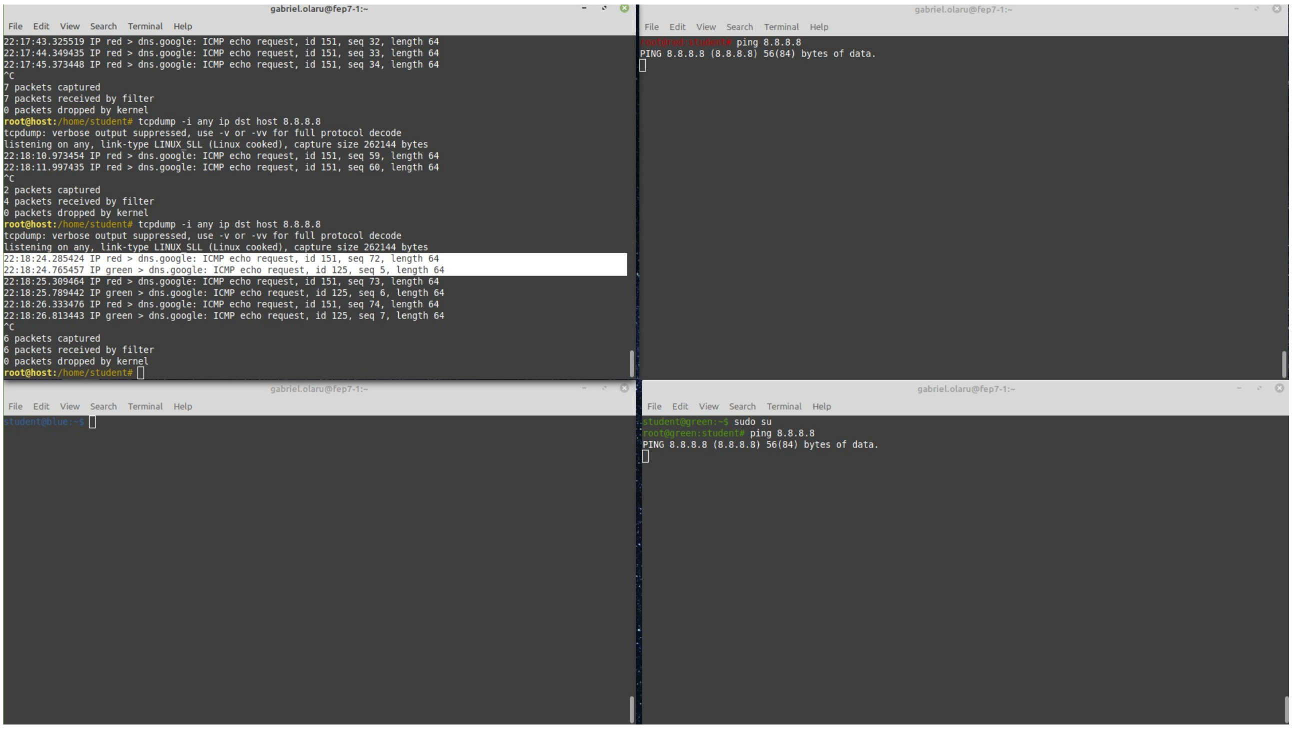
EX1


gabriel.olaru@fep7-1:~
File Edit View Search Terminal Help
gabriel.olaru@fep7-1:~
File Edit View Search Terminal Help

```
root@host:/home/student# iptables -t nat -L POSTROUTING -n -v
Chain POSTROUTING (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    1   136 MASQUERADE  all  --  *      *       0.0.0.0/0            0.0.0.0/0
root@host:/home/student# iptables -t nat -L -n -v
Chain PREROUTING (policy ACCEPT 9 packets, 776 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain INPUT (policy ACCEPT 1 packets, 104 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 1 packets, 136 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain POSTROUTING (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    1   136 MASQUERADE  all  --  *      *       0.0.0.0/0            0.0.0.0/0
root@host:/home/student# 
```

```
root@red:student# iptables -t nat -L -n -v
bash: iptables: command not found
root@red:student# sysctl net.ipv4.ip_forward
net.ipv4.ip_forward = 0
root@red:student# sysctl -w net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
root@red:student# ping -c 2 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.

--- 8.8.8.8 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 1020ms

root@red:student# 
```

EX2:



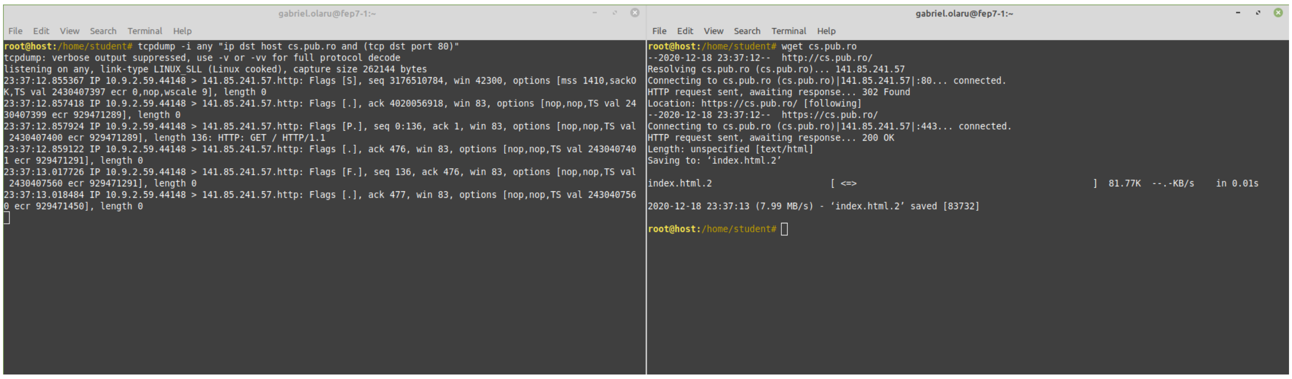
```
22:17:43.325519 IP red > dns.google: ICMP echo request, id 151, seq 32, length 64
22:17:44.349435 IP red > dns.google: ICMP echo request, id 151, seq 33, length 64
22:17:45.373448 IP red > dns.google: ICMP echo request, id 151, seq 34, length 64
^C
7 packets captured
7 packets received by filter
0 packets dropped by kernel
root@host:/home/student# tcpdump -i any ip dst host 8.8.8.8
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type LINUX_SLL (Linux cooked), capture size 262144 bytes
22:18:10.973454 IP red > dns.google: ICMP echo request, id 151, seq 59, length 64
22:18:11.997435 IP red > dns.google: ICMP echo request, id 151, seq 60, length 64
^C
2 packets captured
4 packets received by filter
0 packets dropped by kernel
root@host:/home/student# tcpdump -i any ip dst host 8.8.8.8
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type LINUX_SLL (Linux cooked), capture size 262144 bytes
22:18:24.285424 IP red > dns.google: ICMP echo request, id 151, seq 72, length 64
22:18:24.765457 IP green > dns.google: ICMP echo request, id 125, seq 5, length 64
22:18:25.309464 IP red > dns.google: ICMP echo request, id 151, seq 73, length 64
22:18:25.789442 IP green > dns.google: ICMP echo request, id 125, seq 6, length 64
22:18:26.333476 IP red > dns.google: ICMP echo request, id 151, seq 74, length 64
22:18:26.813443 IP green > dns.google: ICMP echo request, id 125, seq 7, length 64
^C
6 packets captured
6 packets received by filter
0 packets dropped by kernel
root@host:/home/student# 
```

```
root@red:student# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
```

```
student@blue:~$ 
```

```
student@green:~$ sudo su
root@green:student# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
```

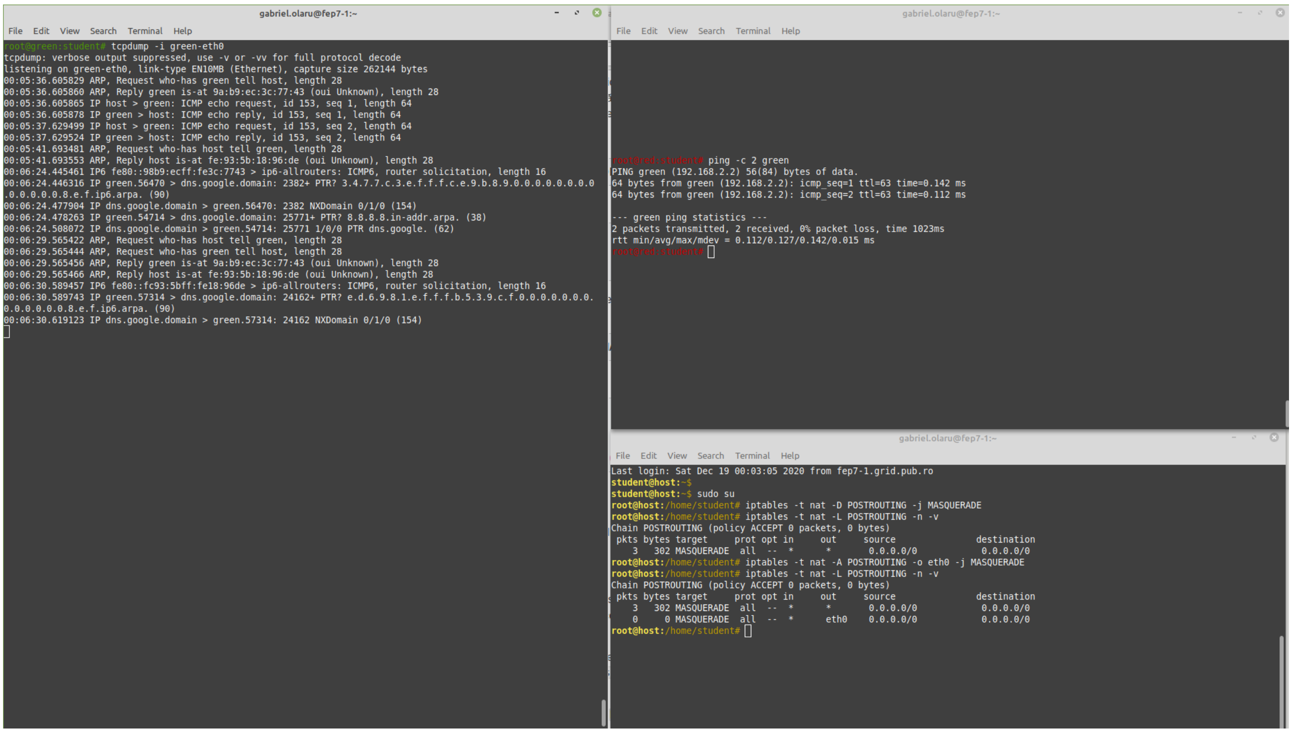
EX3:



```
root@host:/home/student# tcpdump -i any "ip dst host cs.pub.ro and (tcp dst port 80)"
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type LINUX_SLL (Linux cooked), capture size 262144 bytes
23:37:12.855367 IP 10.9.2.59.44148 > 141.85.241.57.http: Flags [S], seq 3176510784, win 42300, options [mss 1410,sackO
K,TS val 2430407397 ecr 0,nop,wscale 9], length 0
23:37:12.857418 IP 10.9.2.59.44148 > 141.85.241.57.http: Flags [.], ack 4020056918, win 83, options [nop,nop,TS val 24
30407399 ecr 929471289], length 0
23:37:12.857924 IP 10.9.2.59.44148 > 141.85.241.57.http: Flags [P.], seq 0:136, ack 1, win 83, options [nop,nop,TS val
 2430407400 ecr 929471289], length 136: HTTP: GET / HTTP/1.1
23:37:12.859122 IP 10.9.2.59.44148 > 141.85.241.57.http: Flags [.], ack 476, win 83, options [nop,nop,TS val 243040740
1 ecr 929471291], length 0
23:37:13.017726 IP 10.9.2.59.44148 > 141.85.241.57.http: Flags [F.], seq 136, ack 476, win 83, options [nop,nop,TS val
 2430407560 ecr 929471291], length 0
23:37:13.018484 IP 10.9.2.59.44148 > 141.85.241.57.http: Flags [.], ack 477, win 83, options [nop,nop,TS val 243040756
0 ecr 929471450], length 0
```

```
root@host:/home/student# wget cs.pub.ro
--2020-12-18 23:37:12--  http://cs.pub.ro/
Resolving cs.pub.ro (cs.pub.ro)... 141.85.241.57
Connecting to cs.pub.ro (cs.pub.ro)|141.85.241.57|:80... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://cs.pub.ro/ [following]
--2020-12-18 23:37:12--  https://cs.pub.ro/
Connecting to cs.pub.ro (cs.pub.ro)|141.85.241.57|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: ‘index.html.2’

index.html.2                  [ <=>                                            ]  81.77K  --.-KB/s    in 0.01s

2020-12-18 23:37:13 (7.99 MB/s) - ‘index.html.2’ saved [83732]

root@host:/home/student# 
```

Ex4:

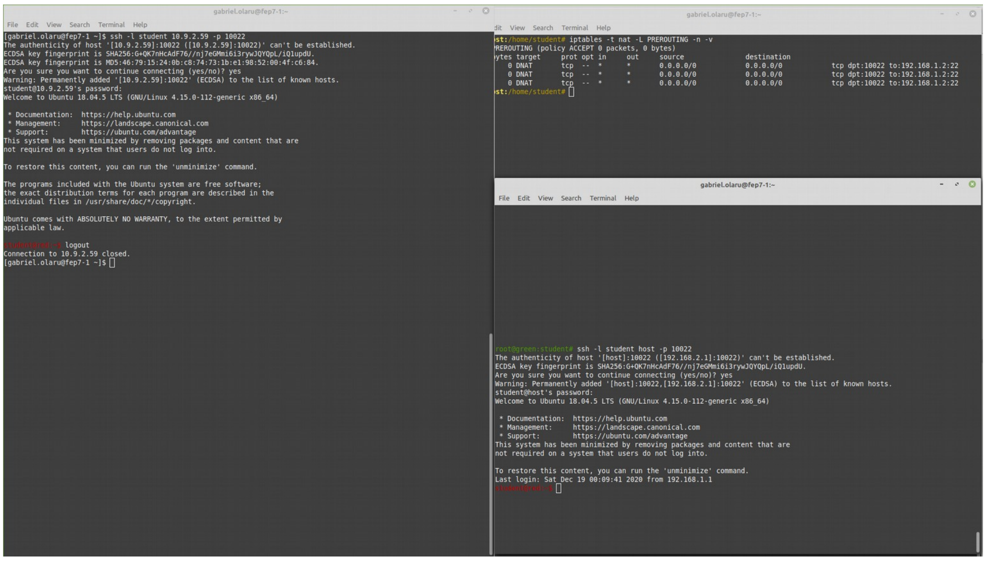


```
root@green:student# tcpdump -i green-eth0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on green-eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
00:05:36.605829 ARP, Request who-has green tell host, length 28
00:05:36.605860 ARP, Reply green is-at 9a:b9:ec:3c:77:43 (oui Unknown), length 28
00:05:36.605865 IP host > green: ICMP echo request, id 153, seq 1, length 64
00:05:36.605878 IP green > host: ICMP echo reply, id 153, seq 1, length 64
00:05:37.629499 IP host > green: ICMP echo request, id 153, seq 2, length 64
00:05:37.629524 IP green > host: ICMP echo reply, id 153, seq 2, length 64
00:05:41.693481 ARP, Request who-has host tell green, length 28
00:05:41.693553 ARP, Reply host is-at fe:93:5b:18:96:de (oui Unknown), length 28
00:06:24.445461 IP6 fe80::98b9:ecff:fe3c:7743 > ip6-allrouters: ICMP6, router solicitation, length 16
00:06:24.446316 IP green.56470 > dns.google.domain: 2382+ PTR? 3.4.7.7.c.3.e.f.f.f.c.e.9.b.8.9.0.0.0.0.0.0.0.0
.0.0.0.0.0.8.e.f.ip6.arpa. (90)
00:06:24.477904 IP dns.google.domain > green.56470: 2382 NXDomain 0/1/0 (154)
00:06:24.478263 IP green.54714 > dns.google.domain: 25771+ PTR? 8.8.8.8.in-addr.arpa. (38)
00:06:24.508072 IP dns.google.domain > green.54714: 25771 1/0/0 PTR dns.google. (62)
00:06:29.565422 ARP, Request who-has host tell green, length 28
00:06:29.565444 ARP, Request who-has green tell host, length 28
00:06:29.565456 ARP, Reply green is-at 9a:b9:ec:3c:77:43 (oui Unknown), length 28
00:06:29.565466 ARP, Reply host is-at fe:93:5b:18:96:de (oui Unknown), length 28
00:06:30.589457 IP6 fe80::fc93:5bff:fe18:96de > ip6-allrouters: ICMP6, router solicitation, length 16
00:06:30.589743 IP green.57314 > dns.google.domain: 24162+ PTR? e.d.6.9.8.1.e.f.f.f.b.5.3.9.c.f.0.0.0.0.0.0.0.
0.0.0.0.0.0.0.8.e.f.ip6.arpa. (90)
00:06:30.619123 IP dns.google.domain > green.57314: 24162 NXDomain 0/1/0 (154)
```

```
root@red:student# ping -c 2 green
PING green (192.168.2.2) 56(84) bytes of data.
64 bytes from green (192.168.2.2): icmp_seq=1 ttl=63 time=0.142 ms
64 bytes from green (192.168.2.2): icmp_seq=2 ttl=63 time=0.112 ms

--- green ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1023ms
rtt min/avg/max/mdev = 0.112/0.127/0.142/0.015 ms
root@red:student#
```

```
Last login: Sat Dec 19 00:03:05 2020 from fep7-1.grid.pub.ro
student@host:~$
student@host:~$ sudo su
root@host:/home/student# iptables -t nat -D POSTROUTING -j MASQUERADE
root@host:/home/student# iptables -t nat -L POSTROUTING -n -v
Chain POSTROUTING (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    3   302 MASQUERADE  all  --  *      *       0.0.0.0/0            0.0.0.0/0
root@host:/home/student# iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
root@host:/home/student# iptables -t nat -L POSTROUTING -n -v
Chain POSTROUTING (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    3   302 MASQUERADE  all  --  *      *       0.0.0.0/0            0.0.0.0/0
    0     0 MASQUERADE  all  --  *      eth0    0.0.0.0/0            0.0.0.0/0
root@host:/home/student#
```

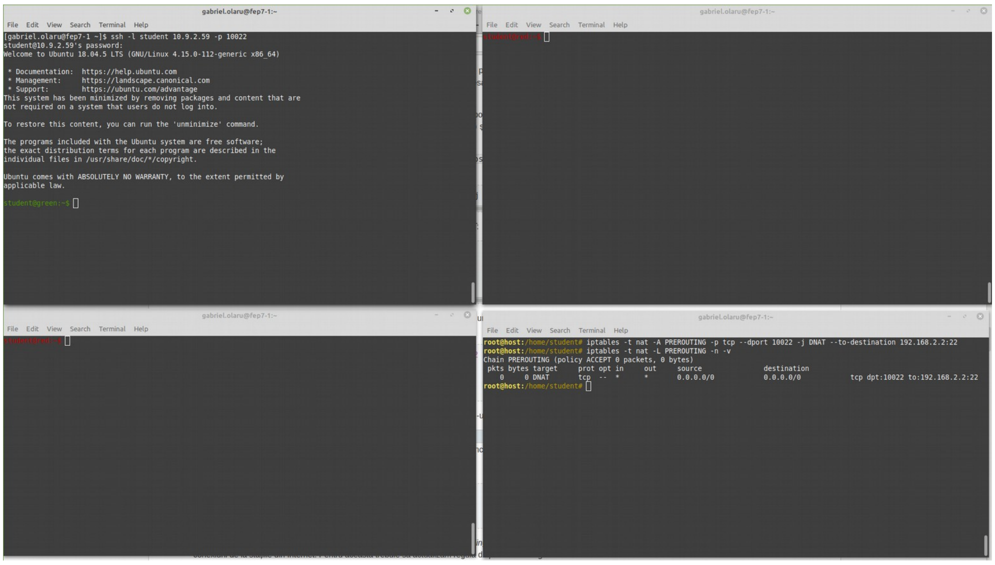
Ex5:



```
[gabriel.olaru@fep7-1 ~]$ ssh -l student 10.9.2.59 -p 10022
The authenticity of host '[10.9.2.59]:10022 ([10.9.2.59]:10022)' can't be established.
ECDSA key fingerprint is SHA256:G+QK7nHcAdF76//nj7eGMmi6i3rywJQYQpL/iQ1updU.
ECDSA key fingerprint is MD5:46:79:15:24:0b:c8:74:73:1b:e1:98:52:00:4f:c6:84.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[10.9.2.59]:10022' (ECDSA) to the list of known hosts.
student@10.9.2.59's password:
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-112-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

student@red:~$ logout
Connection to 10.9.2.59 closed.
[gabriel.olaru@fep7-1 ~]$
```

```
st:/home/student# iptables -t nat -L PREROUTING -n -v
PREROUTING (policy ACCEPT 0 packets, 0 bytes)
ytes target     prot opt in     out     source               destination
   0 DNAT       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:10022 to:192.168.1.2:22
   0 DNAT       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:10022 to:192.168.1.2:22
   0 DNAT       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:10022 to:192.168.1.2:22
st:/home/student#
```

```
root@green:student# ssh -l student host -p 10022
The authenticity of host '[host]:10022 ([192.168.2.1]:10022)' can't be established.
ECDSA key fingerprint is SHA256:G+QK7nHcAdF76//nj7eGMmi6i3rywJQYQpL/iQ1updU.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[host]:10022,[192.168.2.1]:10022' (ECDSA) to the list of known hosts.
student@host's password:
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-112-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Sat Dec 19 00:09:41 2020 from 192.168.1.1
student@red:~$
```



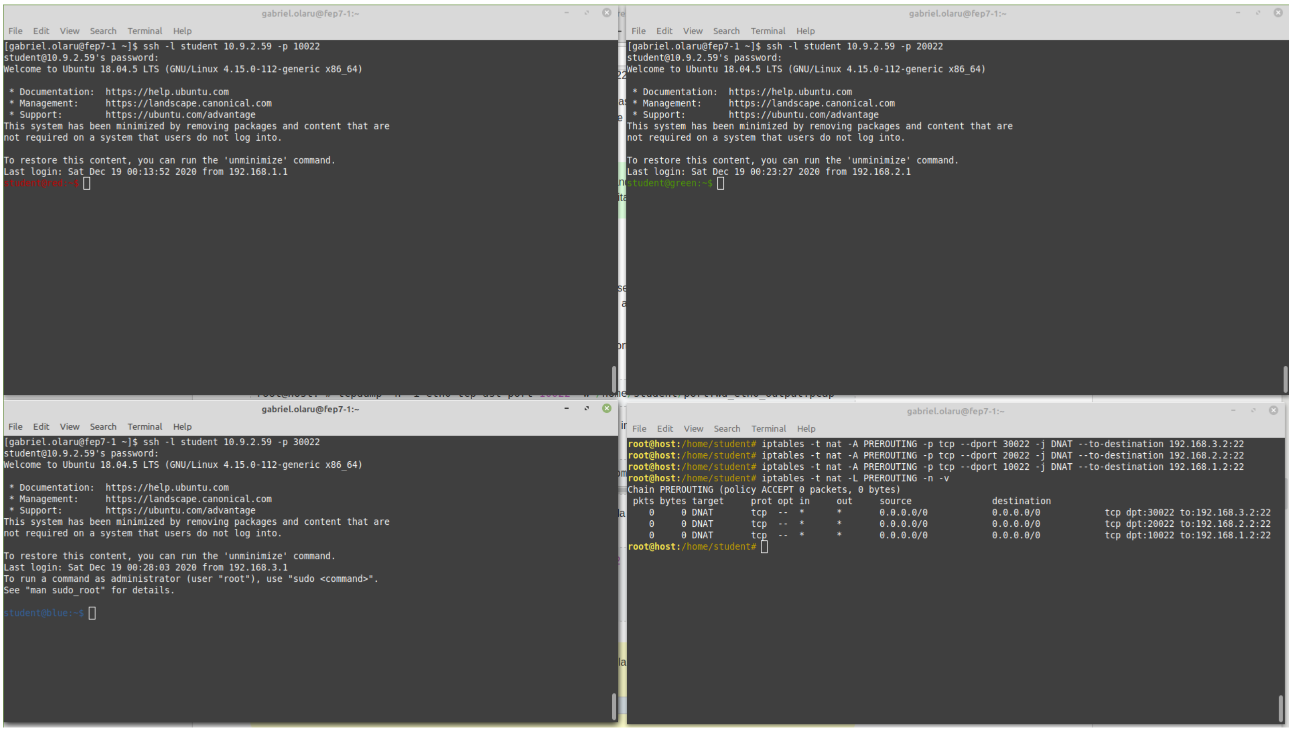
```
[gabriel.olaru@fep7-1 ~]$ ssh -l student 10.9.2.59 -p 10022
student@10.9.2.59's password:
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-112-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

student@green:~$
```

```
student@red:~$
```

```
student@red:~$
```

```
root@host:/home/student# iptables -t nat -A PREROUTING -p tcp --dport 10022 -j DNAT --to-destination 192.168.2.2:22
root@host:/home/student# iptables -t nat -L PREROUTING -n -v
Chain PREROUTING (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DNAT       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:10022 to:192.168.2.2:22
root@host:/home/student#
```

EX6:



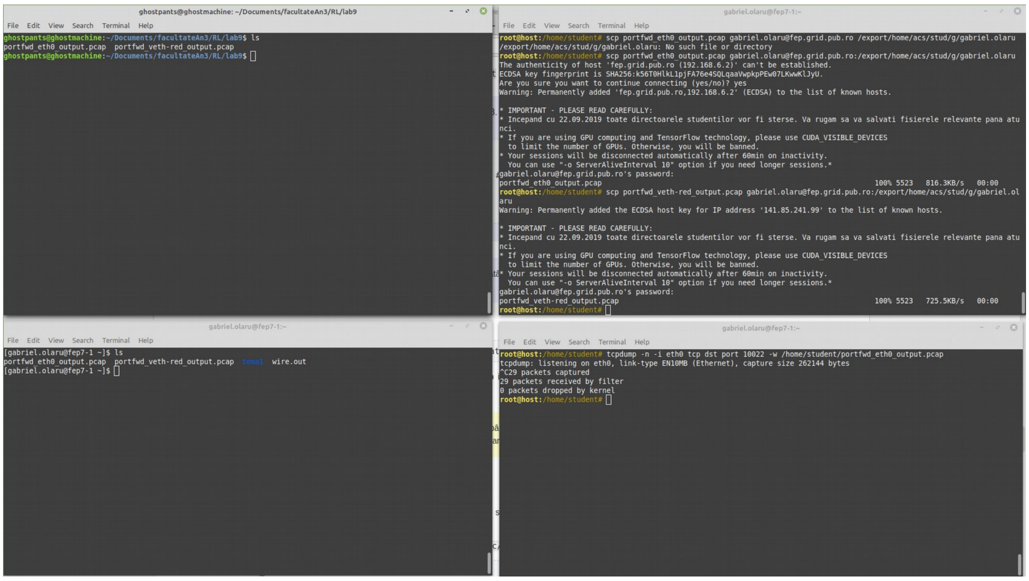
```
[gabriel.olaru@fep7-1 ~]$ ssh -l student 10.9.2.59 -p 10022
student@10.9.2.59's password:
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-112-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Sat Dec 19 00:13:52 2020 from 192.168.1.1
student@red:~$ 
```

```
[gabriel.olaru@fep7-1 ~]$ ssh -l student 10.9.2.59 -p 20022
student@10.9.2.59's password:
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-112-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Sat Dec 19 00:23:27 2020 from 192.168.2.1
student@green:~$ 
```

```
[gabriel.olaru@fep7-1 ~]$ ssh -l student 10.9.2.59 -p 30022
student@10.9.2.59's password:
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-112-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Sat Dec 19 00:28:03 2020 from 192.168.3.1
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

student@blue:~$ 
```

```
root@host:/home/student# iptables -t nat -A PREROUTING -p tcp --dport 30022 -j DNAT --to-destination 192.168.3.2:22
root@host:/home/student# iptables -t nat -A PREROUTING -p tcp --dport 20022 -j DNAT --to-destination 192.168.2.2:22
root@host:/home/student# iptables -t nat -A PREROUTING -p tcp --dport 10022 -j DNAT --to-destination 192.168.1.2:22
root@host:/home/student# iptables -t nat -L PREROUTING -n -v
Chain PREROUTING (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DNAT       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:30022 to:192.168.3.2:22
    0     0 DNAT       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:20022 to:192.168.2.2:22
    0     0 DNAT       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:10022 to:192.168.1.2:22
root@host:/home/student# 
```

EX7:

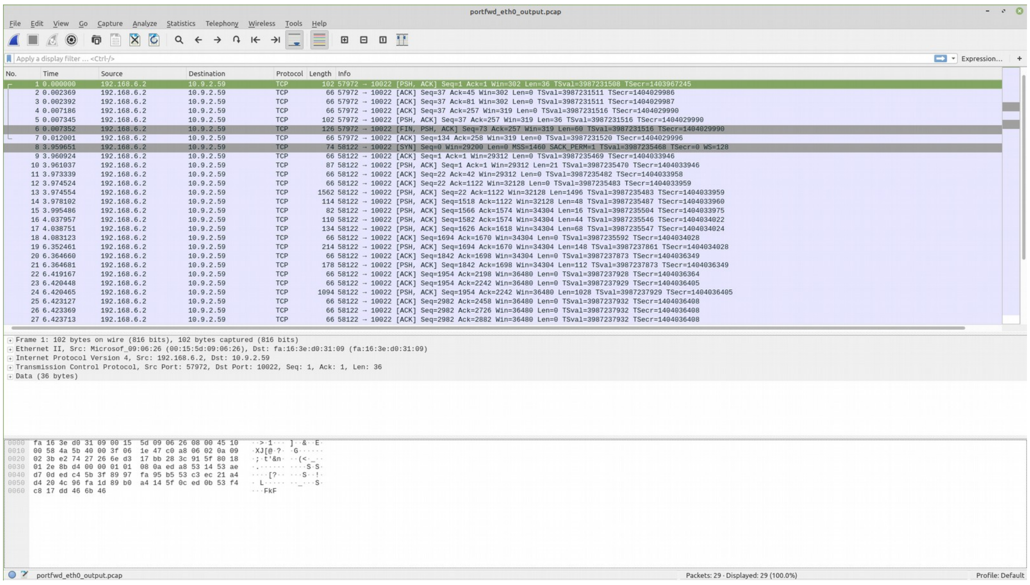

ghostpants@ghostmachine: ~/Documents/facultateAn3/RL/lab9
gabriel.olaru@fep7-1:~
File Edit View Search Terminal Help

```
ghostpants@ghostmachine:~/Documents/facultateAn3/RL/lab9$ ls
portfwd_eth0_output.pcap  portfwd_veth-red_output.pcap
ghostpants@ghostmachine:~/Documents/facultateAn3/RL/lab9$ 
```

```
root@host:/home/student# scp portfwd_eth0_output.pcap gabriel.olaru@fep.grid.pub.ro /export/home/acs/stud/g/gabriel.olaru
/export/home/acs/stud/g/gabriel.olaru: No such file or directory
root@host:/home/student# scp portfwd_eth0_output.pcap gabriel.olaru@fep.grid.pub.ro:/export/home/acs/stud/g/gabriel.olaru
The authenticity of host 'fep.grid.pub.ro (192.168.6.2)' can't be established.
ECDSA key fingerprint is SHA256:k56T0HlkL1pjFA76e4SQLqaaVwpkpPEw07LKwwKlJyU.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'fep.grid.pub.ro,192.168.6.2' (ECDSA) to the list of known hosts.

* IMPORTANT - PLEASE READ CAREFULLY:
* Incepand cu 22.09.2019 toate directoarele studentilor vor fi sterse. Va rugam sa va salvati fisierele relevante pana atu
nci.
* If you are using GPU computing and TensorFlow technology, please use CUDA_VISIBLE_DEVICES
  to limit the number of GPUs. Otherwise, you will be banned.
* Your sessions will be disconnected automatically after 60min on inactivity.
  You can use "-o ServerAliveInterval 10" option if you need longer sessions.*
gabriel.olaru@fep.grid.pub.ro's password:
portfwd_eth0_output.pcap                                                     100% 5523   816.3KB/s   00:00
root@host:/home/student# scp portfwd_veth-red_output.pcap gabriel.olaru@fep.grid.pub.ro:/export/home/acs/stud/g/gabriel.ol
aru
Warning: Permanently added the ECDSA host key for IP address '141.85.241.99' to the list of known hosts.

* IMPORTANT - PLEASE READ CAREFULLY:
* Incepand cu 22.09.2019 toate directoarele studentilor vor fi sterse. Va rugam sa va salvati fisierele relevante pana atu
nci.
* If you are using GPU computing and TensorFlow technology, please use CUDA_VISIBLE_DEVICES
  to limit the number of GPUs. Otherwise, you will be banned.
* Your sessions will be disconnected automatically after 60min on inactivity.
  You can use "-o ServerAliveInterval 10" option if you need longer sessions.*
gabriel.olaru@fep.grid.pub.ro's password:
portfwd_veth-red_output.pcap                                                 100% 5523   725.5KB/s   00:00
root@host:/home/student# 
```

```
[gabriel.olaru@fep7-1 ~]$ ls
portfwd_eth0_output.pcap  portfwd_veth-red_output.pcap  tema1  wire.out
[gabriel.olaru@fep7-1 ~]$ 
```

```
root@host:/home/student# tcpdump -n -i eth0 tcp dst port 10022 -w /home/student/portfwd_eth0_output.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C29 packets captured
29 packets received by filter
0 packets dropped by kernel
root@host:/home/student# 
```

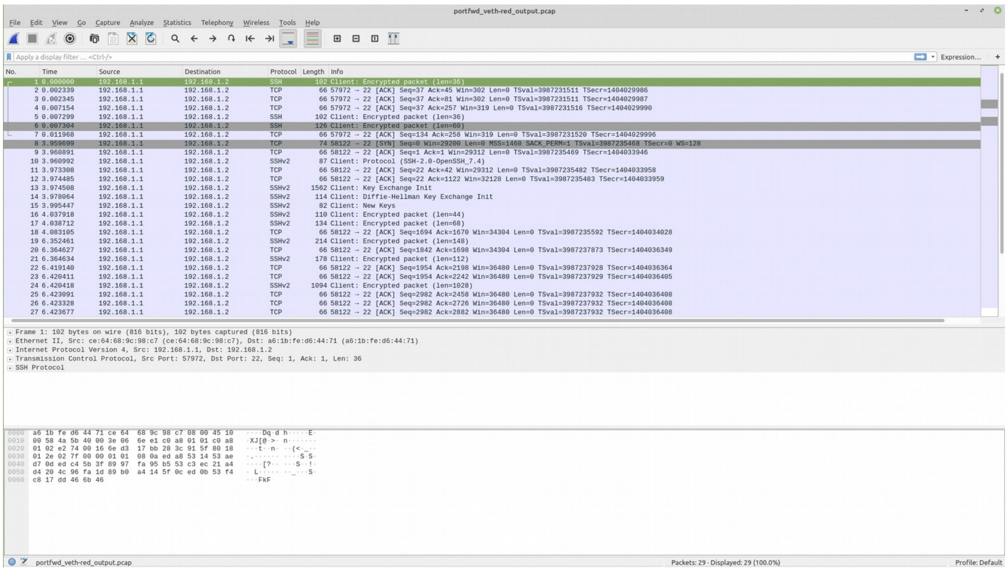

portfwd_eth0_output.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Expression…

```
No.  Time      Source       Destination Protocol Length Info
   1 0.000000  192.168.6.2  10.9.2.59   TCP       102 57972 → 10022 [PSH, ACK] Seq=1 Ack=1 Win=302 Len=36 TSval=3987231508 TSecr=1403967245
   2 0.002369  192.168.6.2  10.9.2.59   TCP        66 57972 → 10022 [ACK] Seq=37 Ack=45 Win=302 Len=0 TSval=3987231511 TSecr=1404029986
   3 0.002392  192.168.6.2  10.9.2.59   TCP        66 57972 → 10022 [ACK] Seq=37 Ack=81 Win=302 Len=0 TSval=3987231511 TSecr=1404029987
   4 0.007186  192.168.6.2  10.9.2.59   TCP        66 57972 → 10022 [ACK] Seq=37 Ack=257 Win=319 Len=0 TSval=3987231516 TSecr=1404029990
   5 0.007345  192.168.6.2  10.9.2.59   TCP       102 57972 → 10022 [PSH, ACK] Seq=37 Ack=257 Win=319 Len=36 TSval=3987231516 TSecr=1404029990
   6 0.007352  192.168.6.2  10.9.2.59   TCP       126 57972 → 10022 [FIN, PSH, ACK] Seq=73 Ack=257 Win=319 Len=60 TSval=3987231516 TSecr=1404029990
   7 0.012001  192.168.6.2  10.9.2.59   TCP        66 57972 → 10022 [ACK] Seq=134 Ack=258 Win=319 Len=0 TSval=3987231520 TSecr=1404029996
   8 3.959651  192.168.6.2  10.9.2.59   TCP        74 58122 → 10022 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=3987235468 TSecr=0 WS=128
   9 3.960924  192.168.6.2  10.9.2.59   TCP        66 58122 → 10022 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=3987235469 TSecr=1404033946
  10 3.961037  192.168.6.2  10.9.2.59   TCP        87 58122 → 10022 [PSH, ACK] Seq=1 Ack=1 Win=29312 Len=21 TSval=3987235470 TSecr=1404033946
  11 3.973339  192.168.6.2  10.9.2.59   TCP        66 58122 → 10022 [ACK] Seq=22 Ack=42 Win=29312 Len=0 TSval=3987235482 TSecr=1404033958
  12 3.974524  192.168.6.2  10.9.2.59   TCP        66 58122 → 10022 [ACK] Seq=22 Ack=1122 Win=32128 Len=0 TSval=3987235483 TSecr=1404033959
  13 3.974554  192.168.6.2  10.9.2.59   TCP      1562 58122 → 10022 [PSH, ACK] Seq=22 Ack=1122 Win=32128 Len=1496 TSval=3987235483 TSecr=1404033959
  14 3.978102  192.168.6.2  10.9.2.59   TCP       114 58122 → 10022 [PSH, ACK] Seq=1518 Ack=1122 Win=32128 Len=48 TSval=3987235487 TSecr=1404033960
  15 3.995486  192.168.6.2  10.9.2.59   TCP        82 58122 → 10022 [PSH, ACK] Seq=1566 Ack=1574 Win=34304 Len=16 TSval=3987235504 TSecr=1404033975
  16 4.037957  192.168.6.2  10.9.2.59   TCP       110 58122 → 10022 [PSH, ACK] Seq=1582 Ack=1574 Win=34304 Len=44 TSval=3987235546 TSecr=1404034022
  17 4.038751  192.168.6.2  10.9.2.59   TCP       134 58122 → 10022 [PSH, ACK] Seq=1626 Ack=1618 Win=34304 Len=68 TSval=3987235547 TSecr=1404034024
  18 4.083123  192.168.6.2  10.9.2.59   TCP        66 58122 → 10022 [ACK] Seq=1694 Ack=1670 Win=34304 Len=0 TSval=3987235592 TSecr=1404034028
  19 6.352461  192.168.6.2  10.9.2.59   TCP       214 58122 → 10022 [PSH, ACK] Seq=1694 Ack=1670 Win=34304 Len=148 TSval=3987237861 TSecr=1404034028
  20 6.364660  192.168.6.2  10.9.2.59   TCP        66 58122 → 10022 [ACK] Seq=1842 Ack=1698 Win=34304 Len=0 TSval=3987237873 TSecr=1404036349
  21 6.364681  192.168.6.2  10.9.2.59   TCP       178 58122 → 10022 [PSH, ACK] Seq=1842 Ack=1698 Win=34304 Len=112 TSval=3987237873 TSecr=1404036349
  22 6.419167  192.168.6.2  10.9.2.59   TCP        66 58122 → 10022 [ACK] Seq=1954 Ack=2198 Win=36480 Len=0 TSval=3987237928 TSecr=1404036364
  23 6.420448  192.168.6.2  10.9.2.59   TCP        66 58122 → 10022 [ACK] Seq=1954 Ack=2242 Win=36480 Len=0 TSval=3987237929 TSecr=1404036405
  24 6.420465  192.168.6.2  10.9.2.59   TCP      1094 58122 → 10022 [PSH, ACK] Seq=1954 Ack=2242 Win=36480 Len=1028 TSval=3987237929 TSecr=1404036405
  25 6.423127  192.168.6.2  10.9.2.59   TCP        66 58122 → 10022 [ACK] Seq=2982 Ack=2458 Win=36480 Len=0 TSval=3987237932 TSecr=1404036408
  26 6.423369  192.168.6.2  10.9.2.59   TCP        66 58122 → 10022 [ACK] Seq=2982 Ack=2726 Win=36480 Len=0 TSval=3987237932 TSecr=1404036408
  27 6.423713  192.168.6.2  10.9.2.59   TCP        66 58122 → 10022 [ACK] Seq=2982 Ack=2882 Win=36480 Len=0 TSval=3987237932 TSecr=1404036408
```

```
+ Frame 1: 102 bytes on wire (816 bits), 102 bytes captured (816 bits)
+ Ethernet II, Src: Microsof_09:06:26 (00:15:5d:09:06:26), Dst: fa:16:3e:d0:31:09 (fa:16:3e:d0:31:09)
+ Internet Protocol Version 4, Src: 192.168.6.2, Dst: 10.9.2.59
+ Transmission Control Protocol, Src Port: 57972, Dst Port: 10022, Seq: 1, Ack: 1, Len: 36
+ Data (36 bytes)
```

```
0000  fa 16 3e d0 31 09 00 15  5d 09 06 26 08 00 45 10   ··>·1···  ]··&··E·
0010  00 58 4a 5b 40 00 3f 06  1e 47 c0 a8 06 02 0a 09   ·XJ[@·?·  ·G······
0020  02 3b e2 74 27 26 6e d3  17 bb 28 3c 91 5f 80 18   ·;·t'&n·  ··(<·_··
0030  01 2e 8b d4 00 00 01 01  08 0a ed a8 53 14 53 ae   ·.······  ····S·S·
0040  d7 0d ed c4 5b 3f 89 97  fa 95 b5 53 c3 ec 21 a4   ····[?··  ···S··!·
0050  d4 20 4c 96 fa 1d 89 b0  a4 14 5f 0c ed 0b 53 f4   · L·····  ··_···S·
0060  c8 17 dd 46 6b 46                                  ···FkF
```

portfwd_eth0_output.pcap   Packets: 29 · Displayed: 29 (100.0%)   Profile: Default


portfwd_veth-red_output.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Expression…

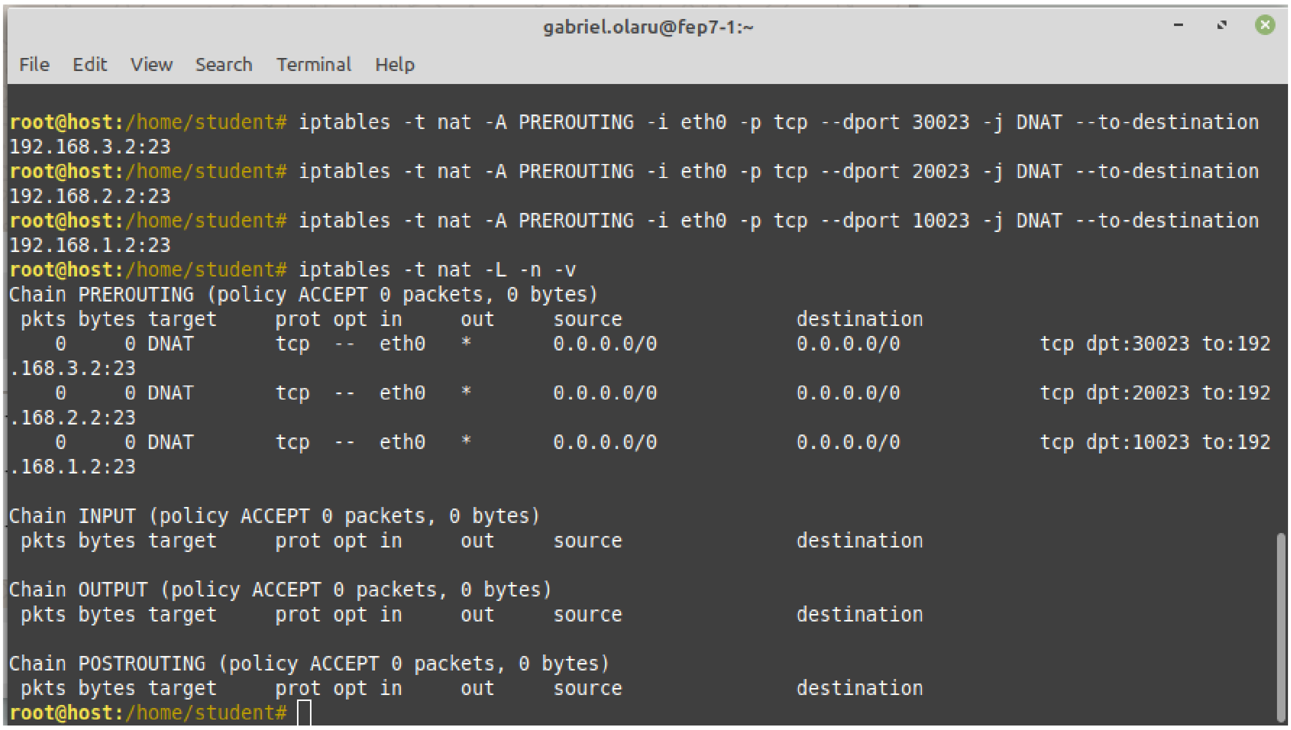
```
No.  Time      Source       Destination  Protocol Length Info
   1 0.000000  192.168.1.1  192.168.1.2  SSH       102 Client: Encrypted packet (len=36)
   2 0.002339  192.168.1.1  192.168.1.2  TCP        66 57972 → 22 [ACK] Seq=37 Ack=45 Win=302 Len=0 TSval=3987231511 TSecr=1404029986
   3 0.002345  192.168.1.1  192.168.1.2  TCP        66 57972 → 22 [ACK] Seq=37 Ack=81 Win=302 Len=0 TSval=3987231511 TSecr=1404029987
   4 0.007154  192.168.1.1  192.168.1.2  TCP        66 57972 → 22 [ACK] Seq=37 Ack=257 Win=319 Len=0 TSval=3987231516 TSecr=1404029990
   5 0.007299  192.168.1.1  192.168.1.2  SSH       102 Client: Encrypted packet (len=36)
   6 0.007304  192.168.1.1  192.168.1.2  SSH       126 Client: Encrypted packet (len=60)
   7 0.011968  192.168.1.1  192.168.1.2  TCP        66 57972 → 22 [ACK] Seq=134 Ack=258 Win=319 Len=0 TSval=3987231520 TSecr=1404029996
   8 3.959699  192.168.1.1  192.168.1.2  TCP        74 58122 → 22 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=3987235468 TSecr=0 WS=128
   9 3.960891  192.168.1.1  192.168.1.2  TCP        66 58122 → 22 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=3987235469 TSecr=1404033946
  10 3.960992  192.168.1.1  192.168.1.2  SSHv2      87 Client: Protocol (SSH-2.0-OpenSSH_7.4)
  11 3.973308  192.168.1.1  192.168.1.2  TCP        66 58122 → 22 [ACK] Seq=22 Ack=42 Win=29312 Len=0 TSval=3987235482 TSecr=1404033958
  12 3.974485  192.168.1.1  192.168.1.2  TCP        66 58122 → 22 [ACK] Seq=22 Ack=1122 Win=32128 Len=0 TSval=3987235483 TSecr=1404033959
  13 3.974508  192.168.1.1  192.168.1.2  SSHv2    1562 Client: Key Exchange Init
  14 3.978064  192.168.1.1  192.168.1.2  SSHv2     114 Client: Diffie-Hellman Key Exchange Init
  15 3.995447  192.168.1.1  192.168.1.2  SSHv2      82 Client: New Keys
  16 4.037918  192.168.1.1  192.168.1.2  SSHv2     110 Client: Encrypted packet (len=44)
  17 4.038712  192.168.1.1  192.168.1.2  SSHv2     134 Client: Encrypted packet (len=68)
  18 4.083105  192.168.1.1  192.168.1.2  TCP        66 58122 → 22 [ACK] Seq=1694 Ack=1670 Win=34304 Len=0 TSval=3987235592 TSecr=1404034028
  19 6.352461  192.168.1.1  192.168.1.2  SSHv2     214 Client: Encrypted packet (len=148)
  20 6.364627  192.168.1.1  192.168.1.2  TCP        66 58122 → 22 [ACK] Seq=1842 Ack=1698 Win=34304 Len=0 TSval=3987237873 TSecr=1404036349
  21 6.364634  192.168.1.1  192.168.1.2  SSHv2     178 Client: Encrypted packet (len=112)
  22 6.419140  192.168.1.1  192.168.1.2  TCP        66 58122 → 22 [ACK] Seq=1954 Ack=2198 Win=36480 Len=0 TSval=3987237928 TSecr=1404036364
  23 6.420411  192.168.1.1  192.168.1.2  TCP        66 58122 → 22 [ACK] Seq=1954 Ack=2242 Win=36480 Len=0 TSval=3987237929 TSecr=1404036405
  24 6.420418  192.168.1.1  192.168.1.2  SSHv2    1094 Client: Encrypted packet (len=1028)
  25 6.423091  192.168.1.1  192.168.1.2  TCP        66 58122 → 22 [ACK] Seq=2982 Ack=2458 Win=36480 Len=0 TSval=3987237932 TSecr=1404036408
  26 6.423328  192.168.1.1  192.168.1.2  TCP        66 58122 → 22 [ACK] Seq=2982 Ack=2726 Win=36480 Len=0 TSval=3987237932 TSecr=1404036408
  27 6.423677  192.168.1.1  192.168.1.2  TCP        66 58122 → 22 [ACK] Seq=2982 Ack=2882 Win=36480 Len=0 TSval=3987237932 TSecr=1404036408
```

```
+ Frame 1: 102 bytes on wire (816 bits), 102 bytes captured (816 bits)
+ Ethernet II, Src: ce:64:68:9c:98:c7 (ce:64:68:9c:98:c7), Dst: a6:1b:fe:d6:44:71 (a6:1b:fe:d6:44:71)
+ Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.2
+ Transmission Control Protocol, Src Port: 57972, Dst Port: 22, Seq: 1, Ack: 1, Len: 36
+ SSH Protocol
```

```
0000  a6 1b fe d6 44 71 ce 64  68 9c 98 c7 08 00 45 10   ····Dq·d h·····E·
0010  00 58 4a 5b 40 00 3e 06  6e e1 c0 a8 01 01 c0 a8   ·XJ[@·>·  n·······
0020  01 02 e2 74 00 16 6e d3  17 bb 28 3c 91 5f 80 18   ···t··n·  ··(<·_··
0030  01 2e 02 7f 00 00 01 01  08 0a ed a8 53 14 53 ae   ·.······  ····S·S·
0040  d7 0d ed c4 5b 3f 89 97  fa 95 b5 53 c3 ec 21 a4   ····[?··  ···S··!·
0050  d4 20 4c 96 fa 1d 89 b0  a4 14 5f 0c ed 0b 53 f4   · L·····  ··_···S·
0060  c8 17 dd 46 6b 46                                  ···FkF
```

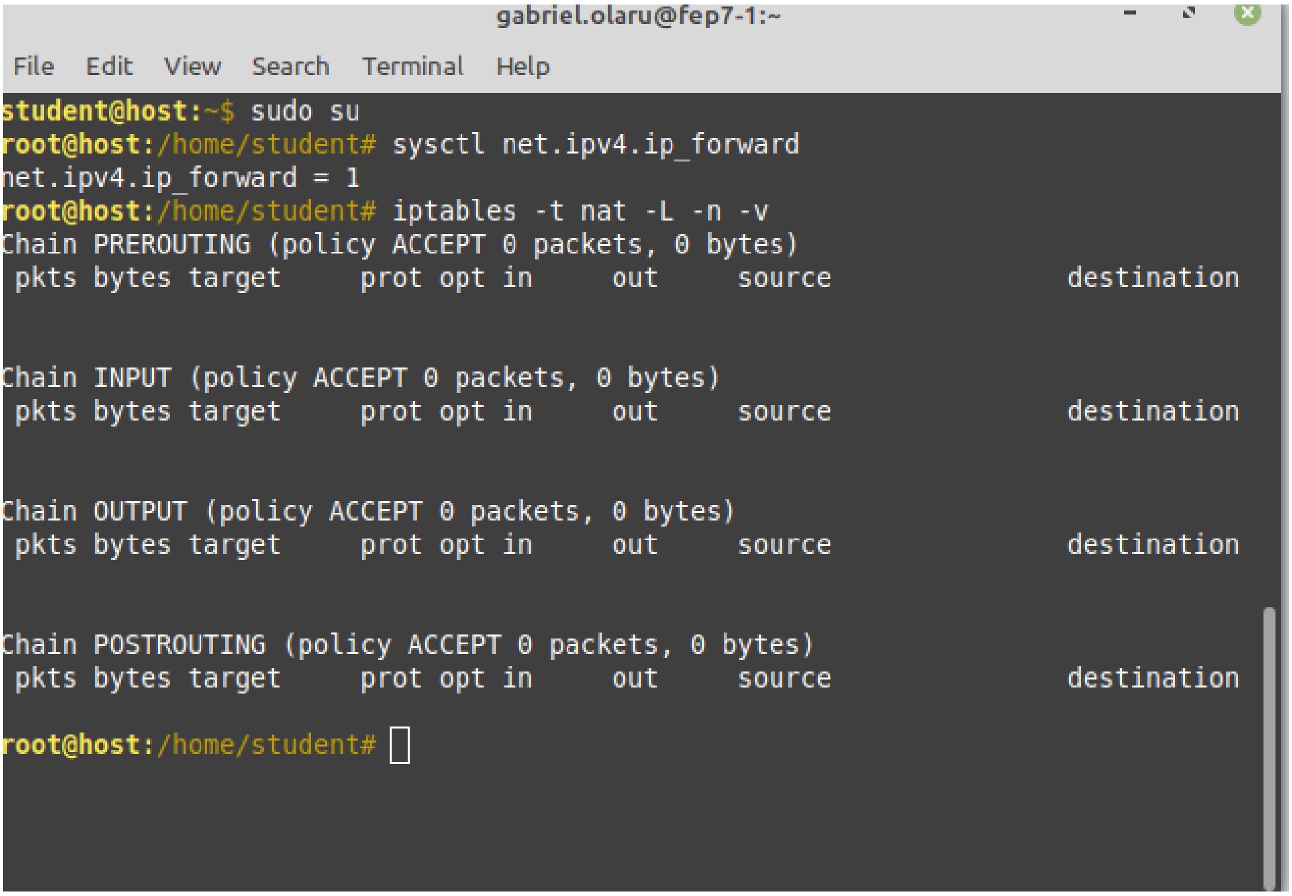
portfwd_veth-red_output.pcap   Packets: 29 · Displayed: 29 (100.0%)   Profile: Default

EX8:



```
root@host:/home/student# iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 30023 -j DNAT --to-destination
192.168.3.2:23
root@host:/home/student# iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 20023 -j DNAT --to-destination
192.168.2.2:23
root@host:/home/student# iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 10023 -j DNAT --to-destination
192.168.1.2:23
root@host:/home/student# iptables -t nat -L -n -v
Chain PREROUTING (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DNAT       tcp  --  eth0   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:30023 to:192
.168.3.2:23
    0     0 DNAT       tcp  --  eth0   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:20023 to:192
.168.2.2:23
    0     0 DNAT       tcp  --  eth0   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:10023 to:192
.168.1.2:23

Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain POSTROUTING (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
root@host:/home/student# 
```

EX9:



```
student@host:~$ sudo su
root@host:/home/student# sysctl net.ipv4.ip_forward
net.ipv4.ip_forward = 1
root@host:/home/student# iptables -t nat -L -n -v
Chain PREROUTING (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain POSTROUTING (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

root@host:/home/student# 
```