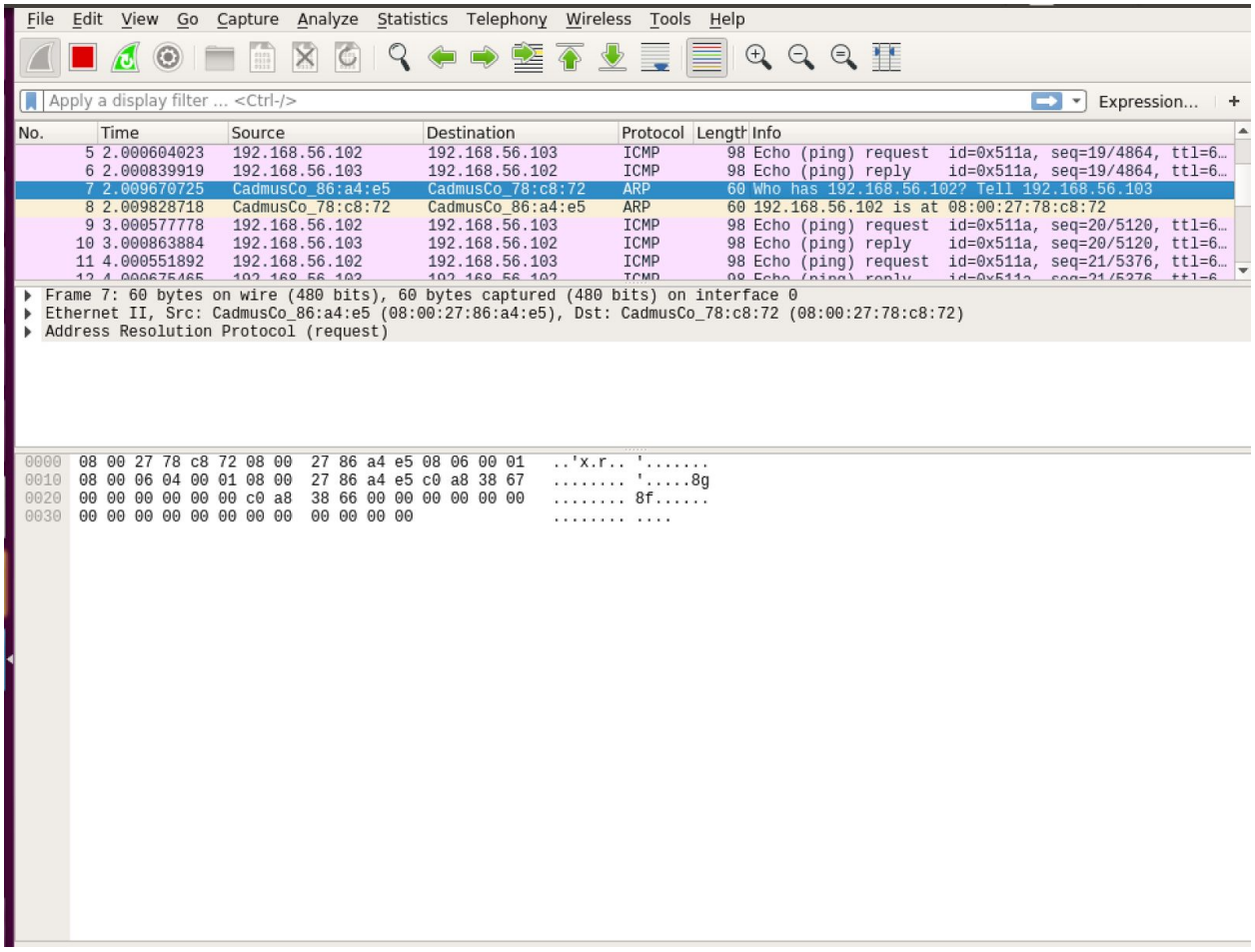
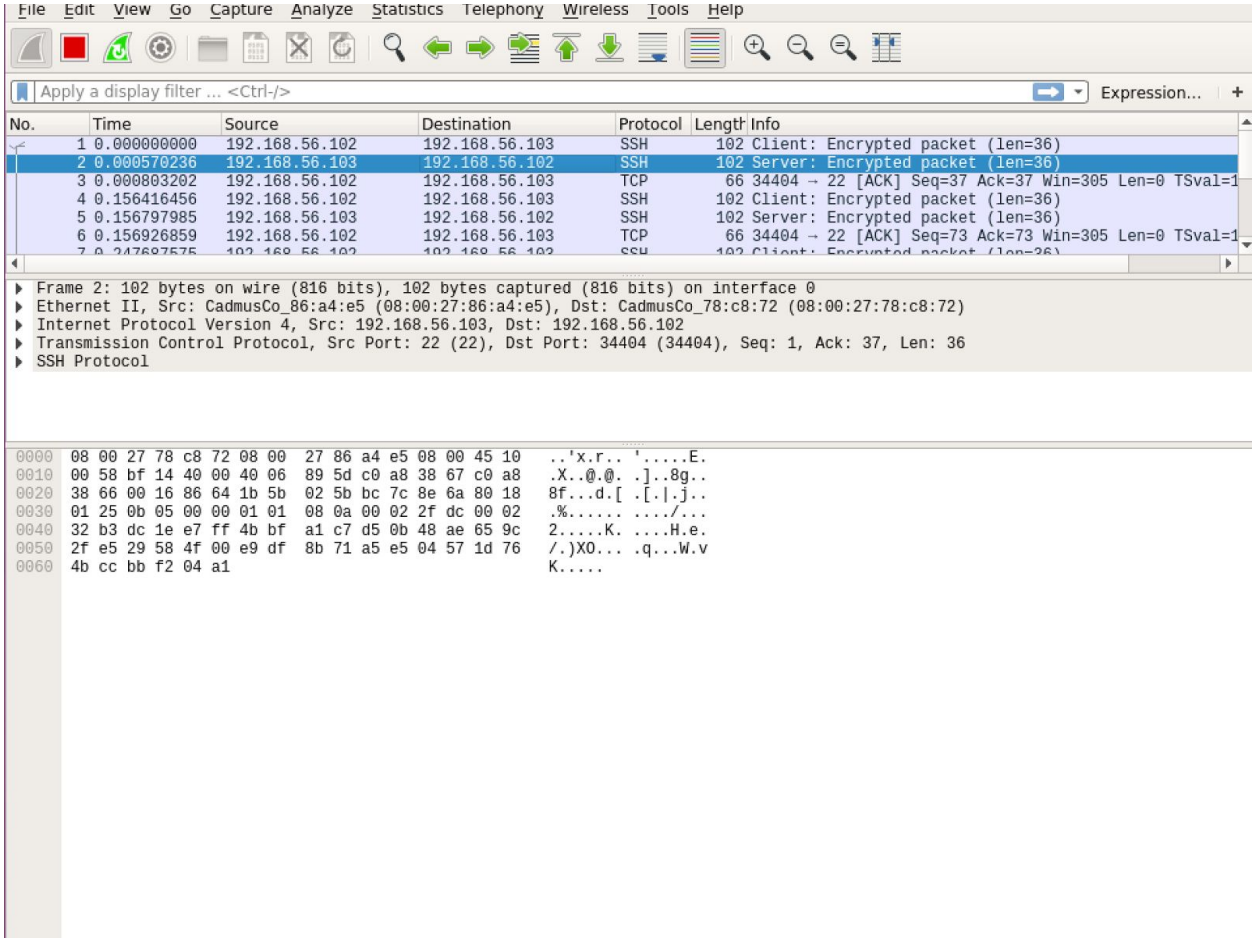
Lab 1: Sniff-then-spoof

ARP

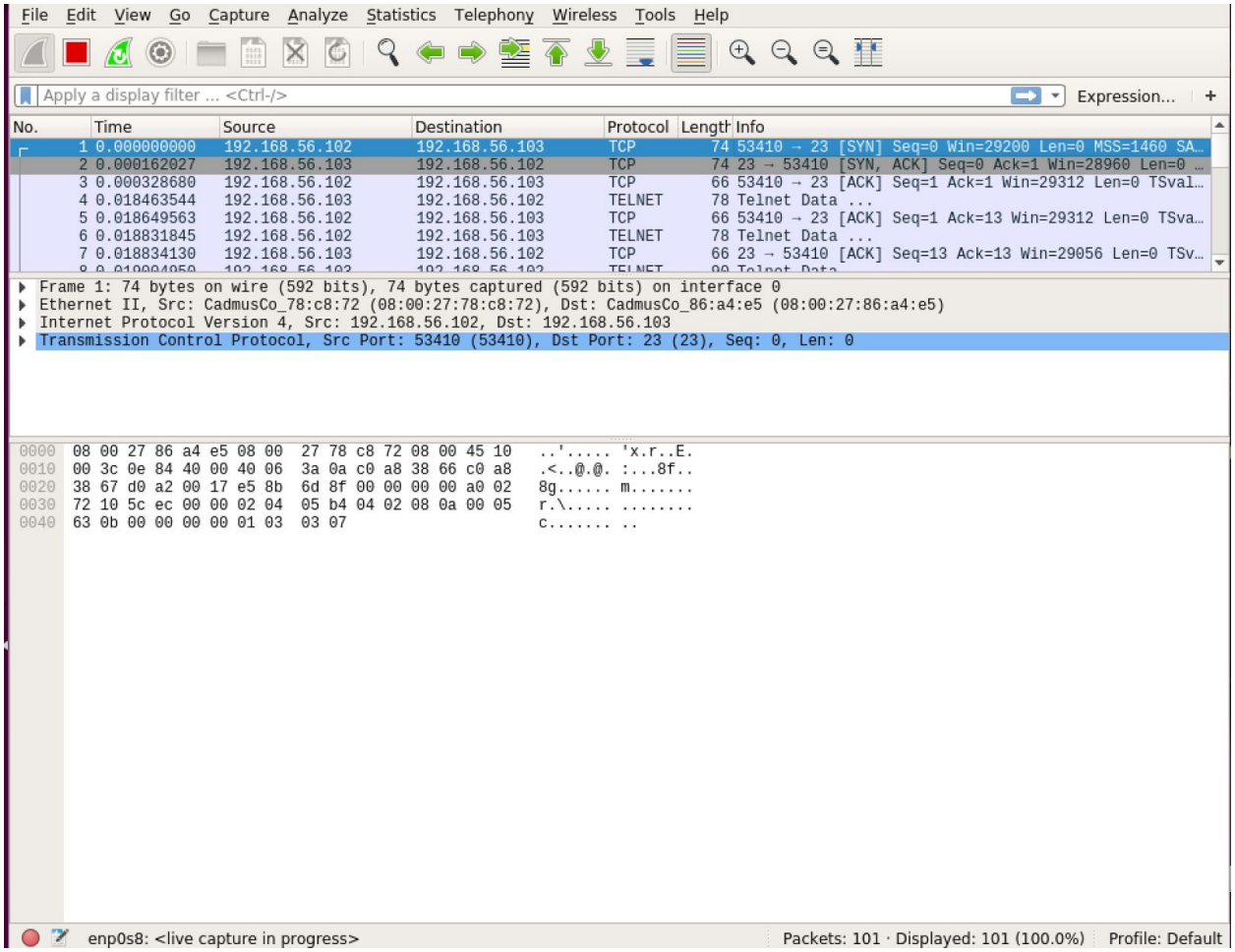


SSH



Data is encrypted

Telnet



Data is not encrypted

It was possible to discover the password by looking at each message (each message sent one character)

```
..'x.r.. '.....E.
.@f.@.@. ....8g..
8f....NG ...tY\..
..6..... ........
.'..Pass word:
```

```
..'..... 'x.r..E.
.5..@.@. ....8f..
8g.....t Y\NG....
...G.... ........
..d
```

```
..'..... 'x.r..E.
.5..@.@. ....8f..
8g.....t Y]NG....
........ ........
.Qi
```

```
..'..... 'x.r..E.
.5..@.@. ....8f..
8g.....t Y^NG....
...a.... ........
.cg
```

```
..'..... 'x.r..E.
.5..@.@. ....8f..
8g.....t Y_NG....
... .... ........
..i
```

```
..'..... 'x.r..E.
.5..@.@. ....8f..
8g.....t Y`NG....
........ .....1..
..s
```

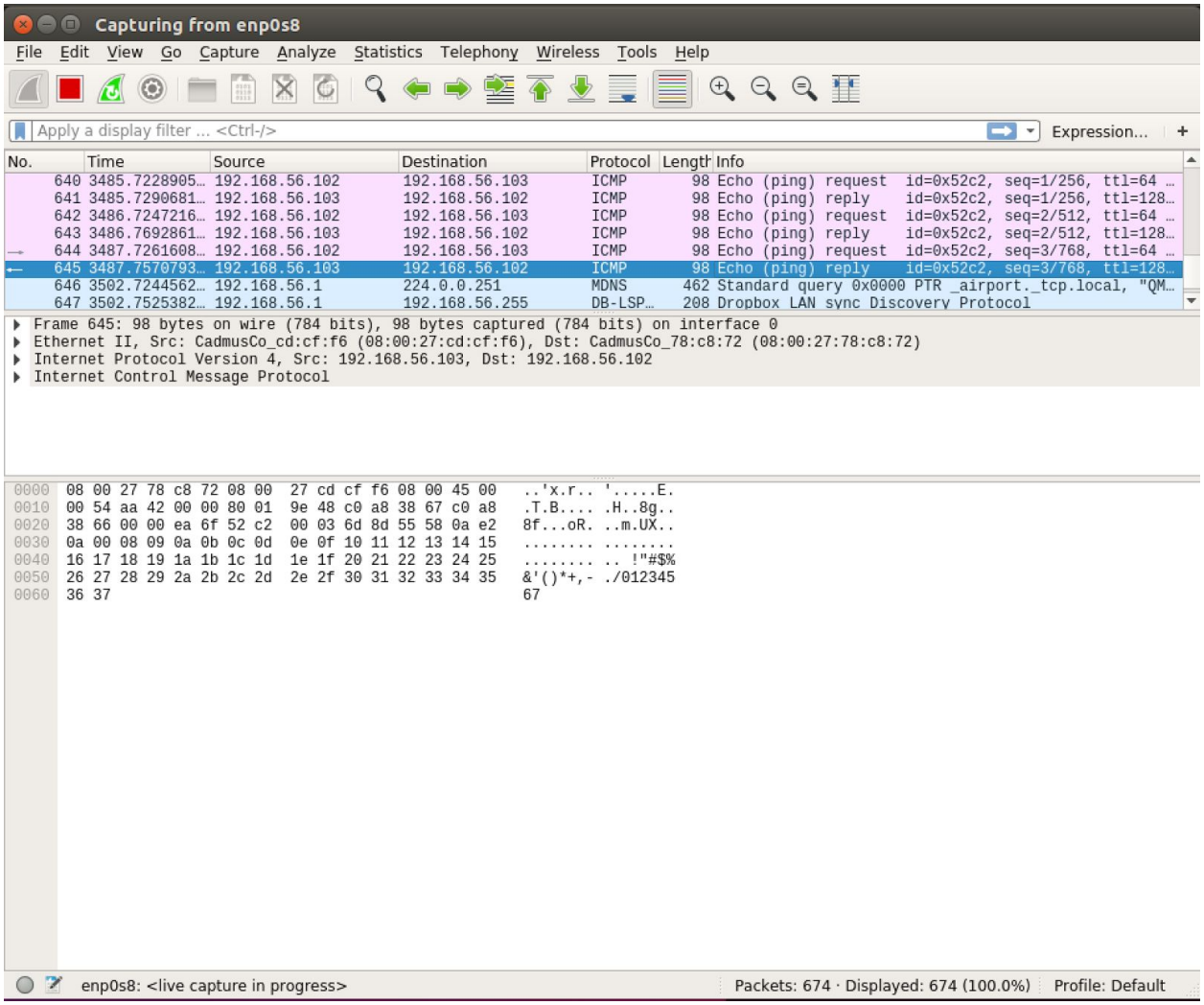
```
..'..... 'x.r..E.
.5..@.@. ....8f..
8g.....t YaNG....
........ .....K..
..e
```

```
..'..... 'x.r..E.
.5..@.@. ....8f..
8g.....t YbNG....
...3.... ........
..c
```

```
..'..... 'x.r..E.
.6..@.@. ....8f..
8g.....t YcNG....
........ ........
.1..
```

(\r)

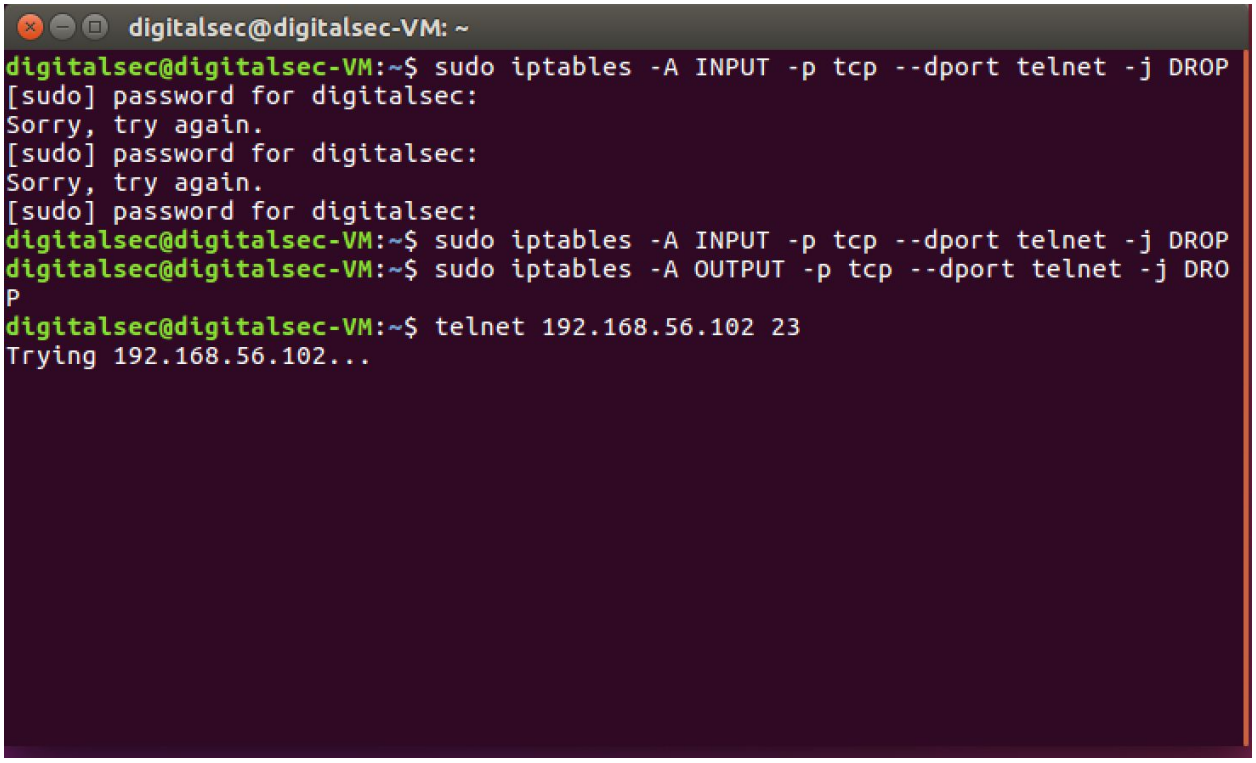
ARP impersonation



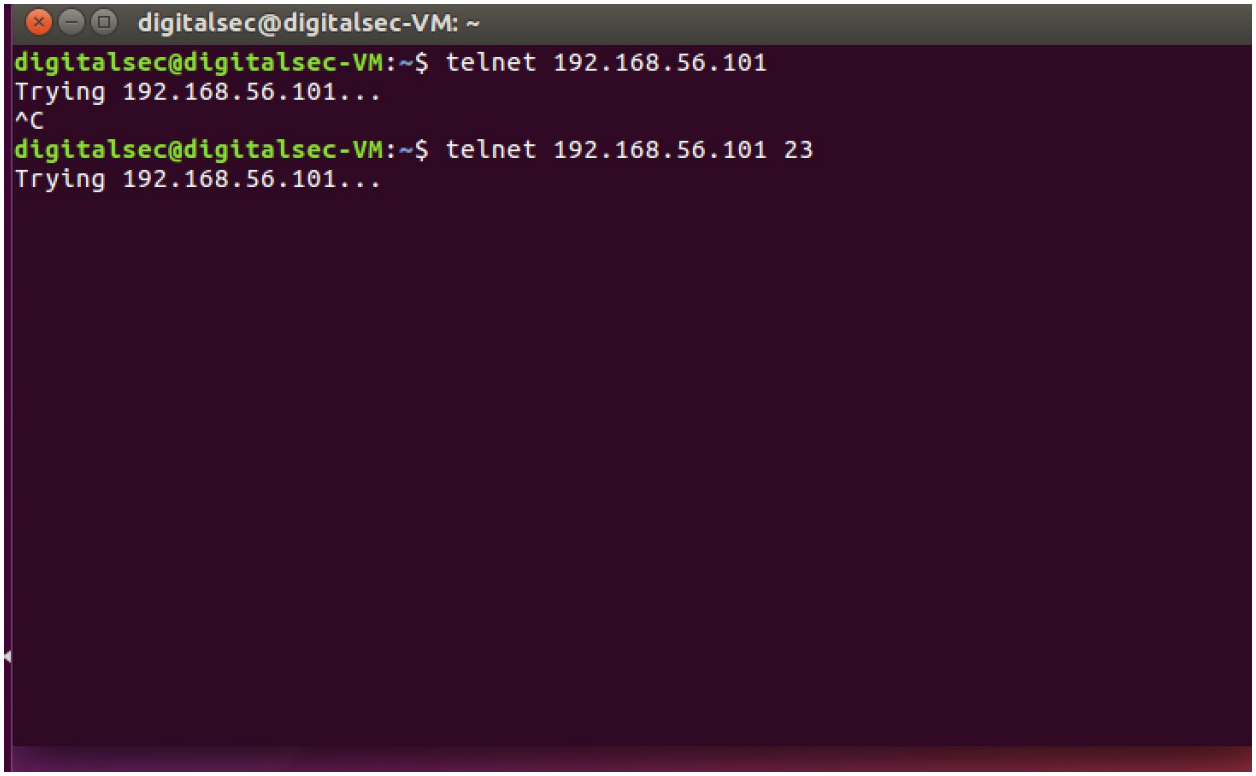
08:00:27:cd:cf:f6 is 192.168.56.100 and is impersonating 192.168.56.103

Lab 2: Firewall

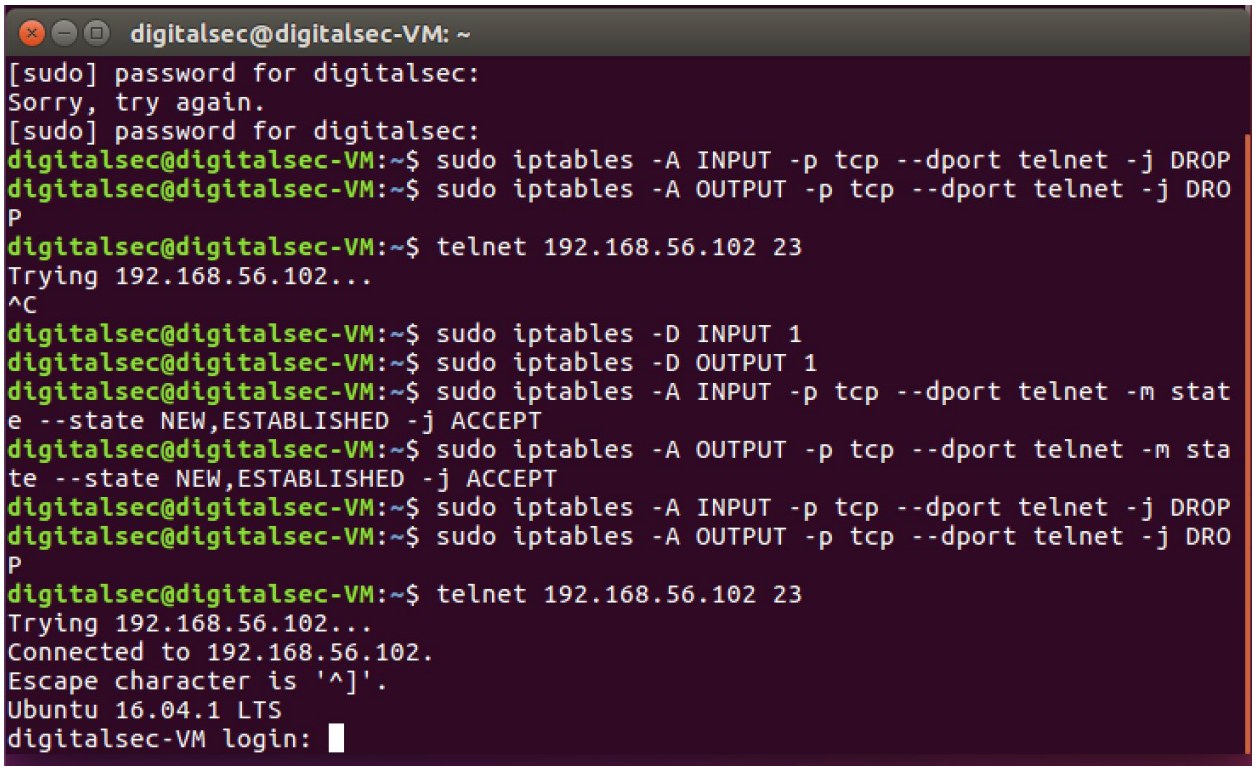
Blocked



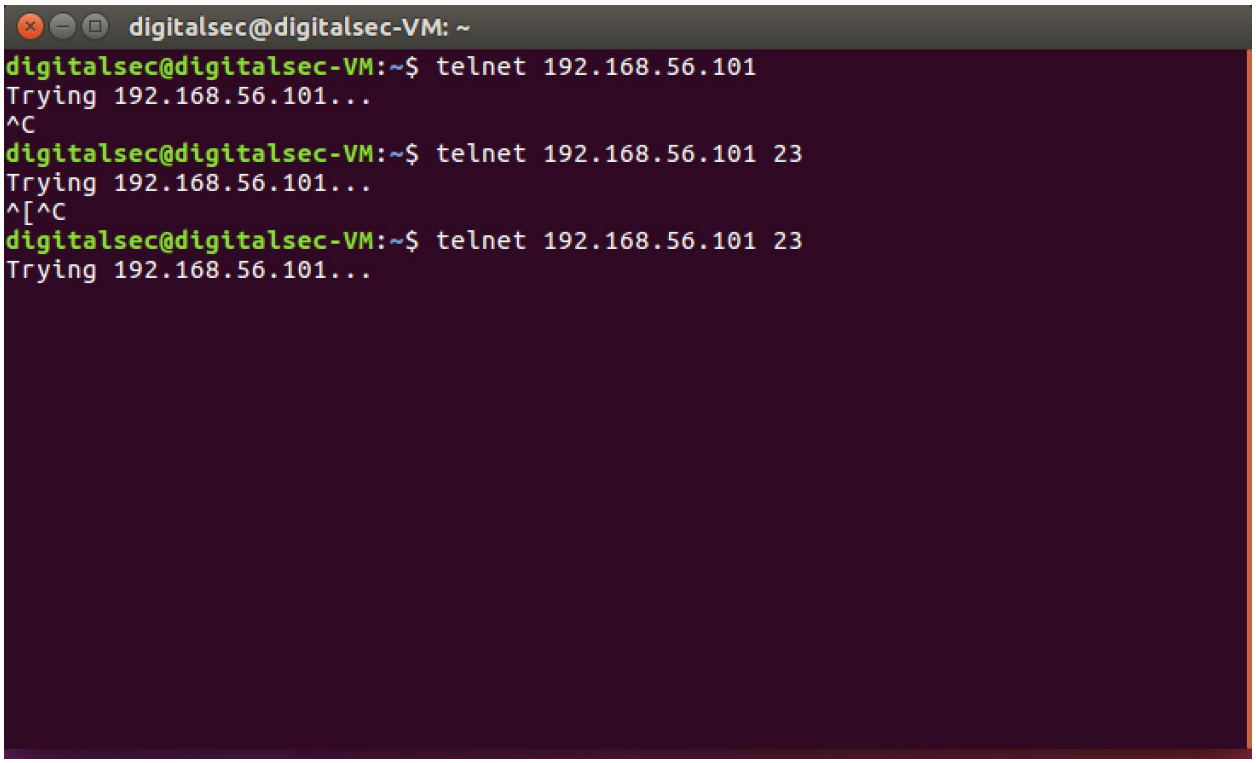
Blocked



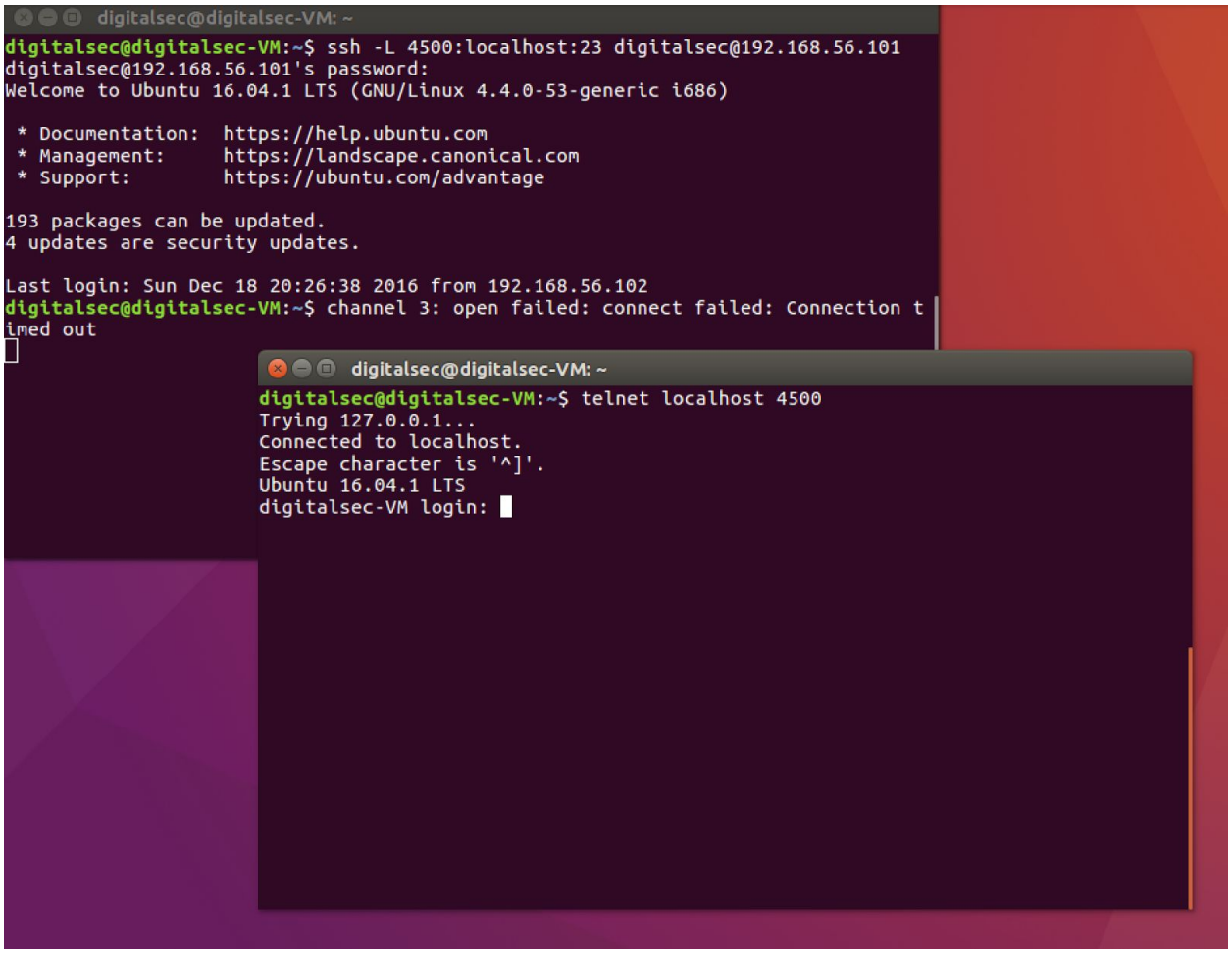
Not blocked



Blocked

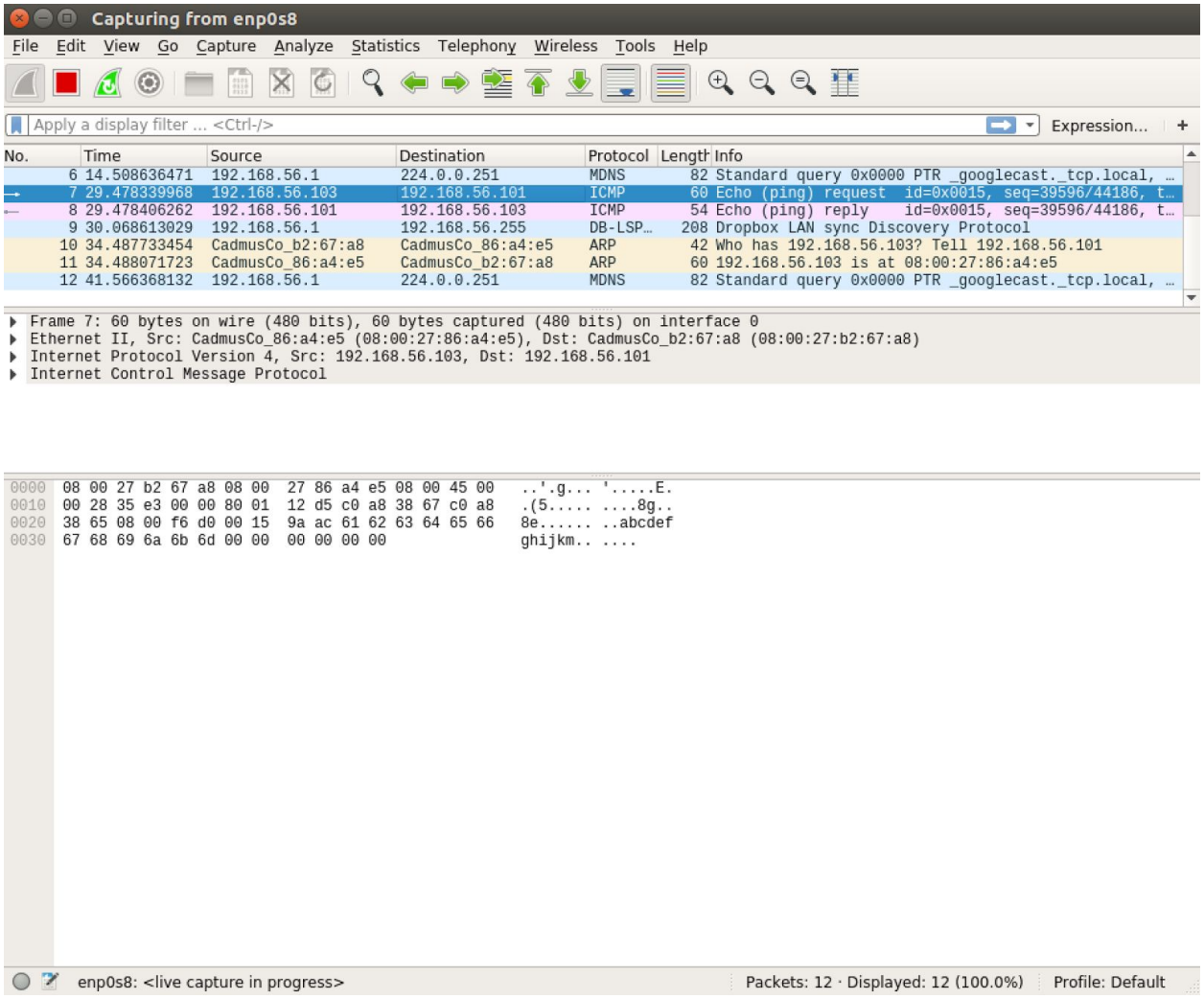


Tunneling


digitalsec@digitalsec-VM: ~
digitalsec@digitalsec-VM:~$ ssh -L 4500:localhost:23 digitalsec@192.168.56.101
digitalsec@192.168.56.101's password:
Welcome to Ubuntu 16.04.1 LTS (GNU/Linux 4.4.0-53-generic i686)
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/advantage
193 packages can be updated.
4 updates are security updates.
Last login: Sun Dec 18 20:26:38 2016 from 192.168.56.102
digitalsec@digitalsec-VM:~$ channel 3: open failed: connect failed: Connection t
imed out
digitalsec@digitalsec-VM: ~
digitalsec@digitalsec-VM:~$ telnet localhost 4500
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
Ubuntu 16.04.1 LTS
digitalsec-VM login:

Lab 3: DoS

Ponging 103 from 102



SYN flooding 103