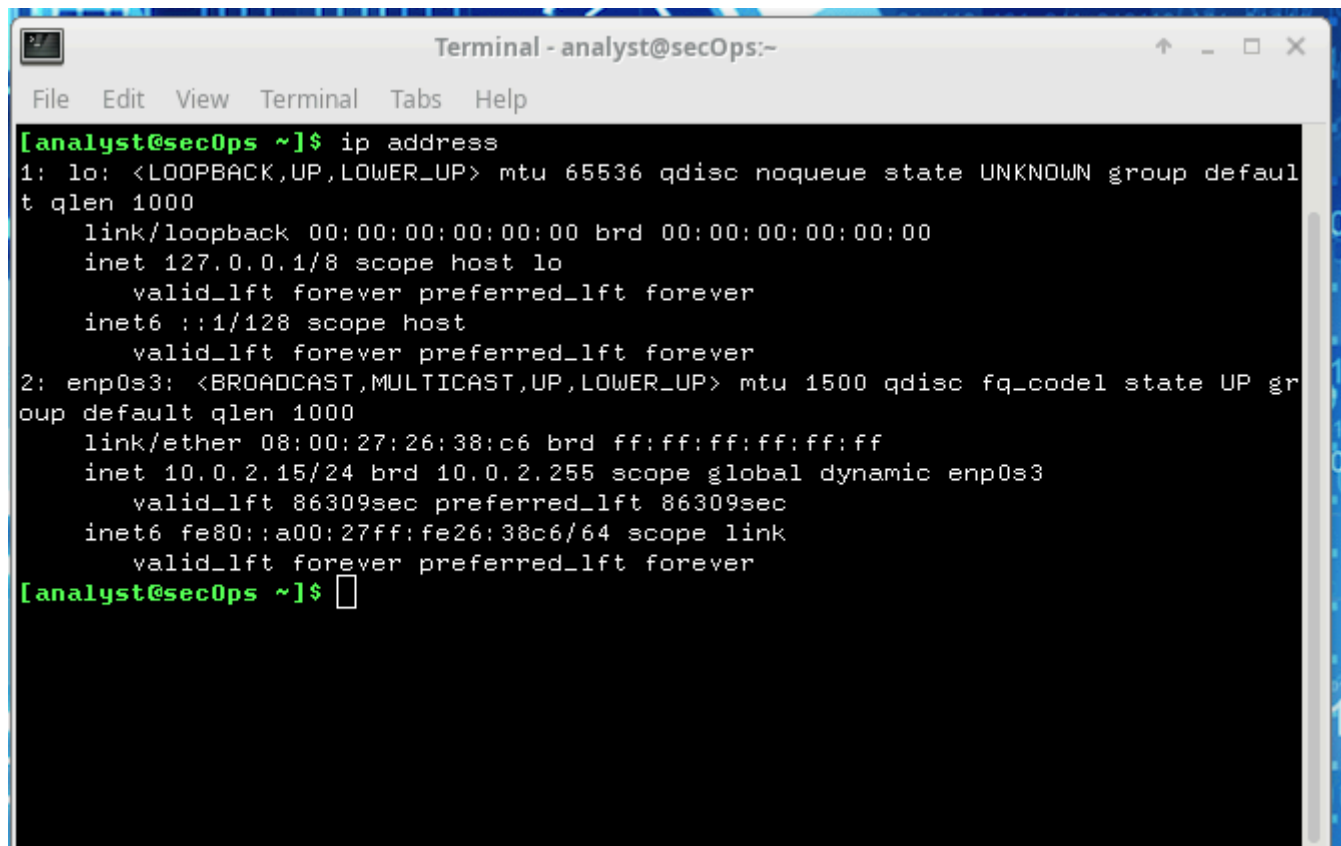


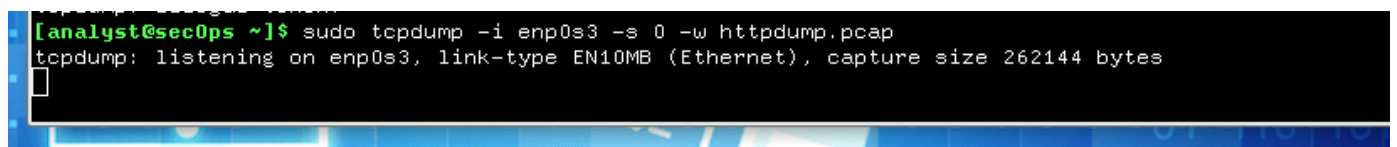
# HTTP e HTTPS

Lancio il comando `ip address` per vedere le mie config. di rete.



```
Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help
[analyst@secOps ~]$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:26:38:c6 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
        valid_lft 86309sec preferred_lft 86309sec
    inet6 fe80::a00:27ff:fe26:38c6/64 scope link
        valid_lft forever preferred_lft forever
[analyst@secOps ~]$
```

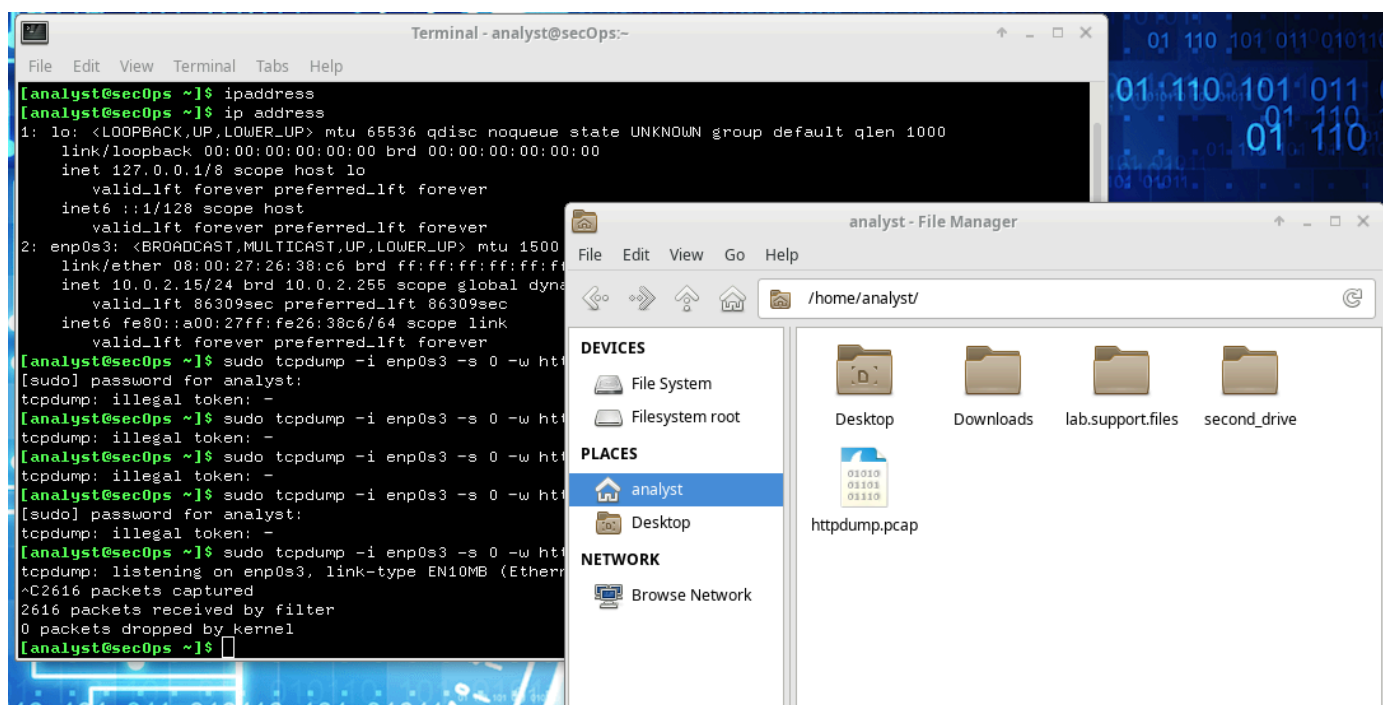
metto in ascolto il tcpdump col comando `sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap`



```
[analyst@secOps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
[analyst@secOps ~]$
```

vado su una pagina login suggerita dal laboratorio mi loggo e poi stoppo l'ascolto dalla console.

## Online Banking Login

Username: Password: 

Otengo le credenziali del login dal file di WireShark, task completa.

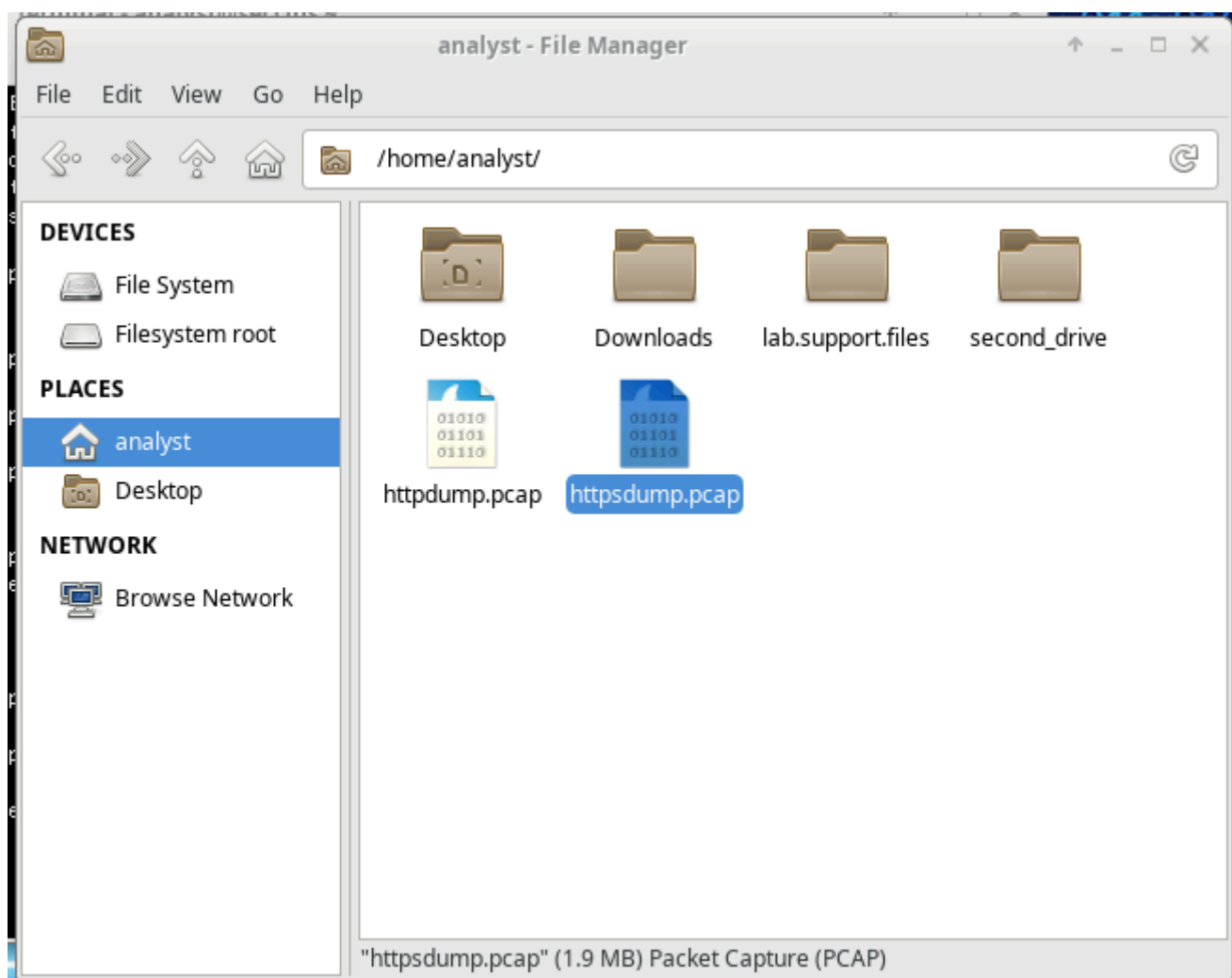
Time	Source	Destination	Protocol	Length	Info
2415	63.216113	10.0.2.15	HTTP	589	POST /doLogin HTTP/1.1 (application/x-www-form-urlencoded)
2419	63.364926	65.61.137.117	HTTP	315	HTTP/1.1 302 Found
2421	63.389554	65.61.137.117	HTTP	595	GET /bank/main.jsp HTTP/1.1
2425	63.544708	65.61.137.117	HTTP	3582	HTTP/1.1 200 OK (text/html)
Hypertext Transfer Protocol					
HTML Form URL Encoded: application/x-www-form-urlencoded					
Form item: "uid" = "Admin"					
Form item: "passw" = "Admin"					
Form item: "btnSubmit" = "Login"					

## HTTPS

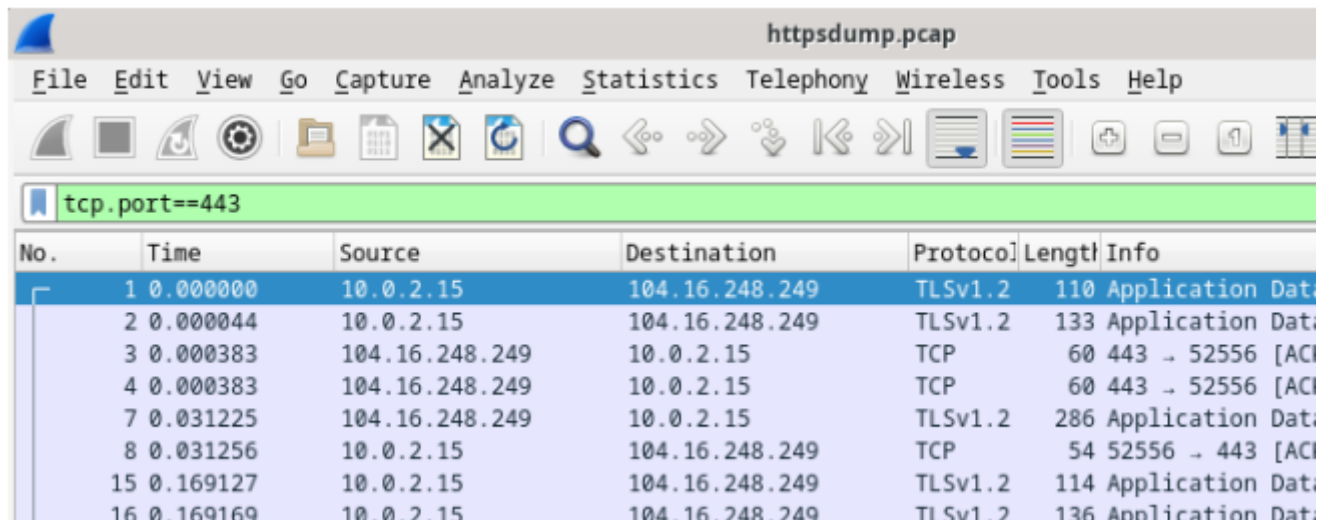
Stessa cosa ho fatto qui, ho avviato l'ascolto tcp dump.

```
Terminal - analyst@secOps:~  
File Edit View Terminal Tabs Help  
valid_lft forever preferred_lft forever  
inet6 ::1/128 scope host  
valid_lft forever preferred_lft forever  
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000  
link/ether 08:00:27:26:38:c6 brd ff:ff:ff:ff:ff:ff  
inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3  
valid_lft 86309sec preferred_lft 86309sec  
inet6 fe80::a00:27ff:fe26:38c6/64 scope link  
valid_lft forever preferred_lft forever  
[analyst@secOps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap  
[sudo] password for analyst:  
tcpdump: illegal token: -  
[analyst@secOps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap  
tcpdump: illegal token: -  
[analyst@secOps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap  
tcpdump: illegal token: -  
[analyst@secOps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap  
[sudo] password for analyst:  
tcpdump: illegal token: -  
[analyst@secOps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap  
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes  
^C2616 packets captured  
2616 packets received by filter  
0 packets dropped by kernel  
[analyst@secOps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap  
[sudo] password for analyst:  
[analyst@secOps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httpsdump.pcap  
[sudo] password for analyst:  
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
```

Mi sono loggato ad una pagina protetta HTTPS con un mio account ed ho ottenuto il file.



Ho analizzato i pacchetti per vedere se riuscissi anche qua a leggere i dati del login ma nulla TLS ha funzionato bene ;)



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.2.15	104.16.248.249	TLSv1.2	110	Application Data
2	0.000044	10.0.2.15	104.16.248.249	TLSv1.2	133	Application Data
3	0.000383	104.16.248.249	10.0.2.15	TCP	60	443 → 52556 [ACK]
4	0.000383	104.16.248.249	10.0.2.15	TCP	60	443 → 52556 [ACK]
7	0.031225	104.16.248.249	10.0.2.15	TLSv1.2	286	Application Data
8	0.031256	10.0.2.15	104.16.248.249	TCP	54	52556 → 443 [ACK]
15	0.169127	10.0.2.15	104.16.248.249	TLSv1.2	114	Application Data
16	0.169169	10.0.2.15	104.16.248.249	TLSv1.2	136	Application Data

▼ TLSv1.2 Record Layer: Application Data Protocol: http-over-tls  
Content Type: Application Data (23)  
Version: TLS 1.2 (0x0303)  
Length: 51  
Encrypted Application Data: 7fa9037731c6e38e6213aacc15a0a7281f94046fdb237be9...