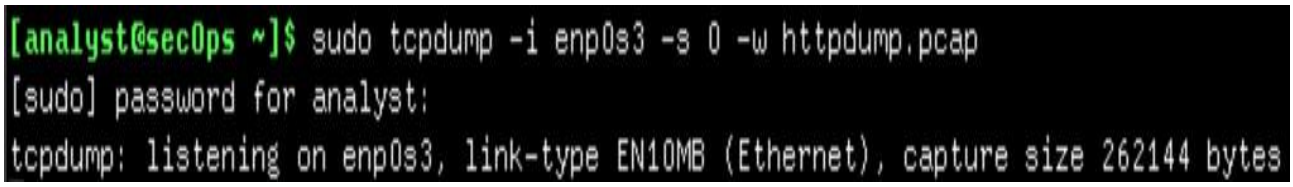
Relazione Wireshark Traffico http e HTTPS

Come primo passaggio e come illustrato nella seguente immagine, con il comando specifico per visualizzare gli indirizzi IP sia del localhost e della mia VM, utilizzo:

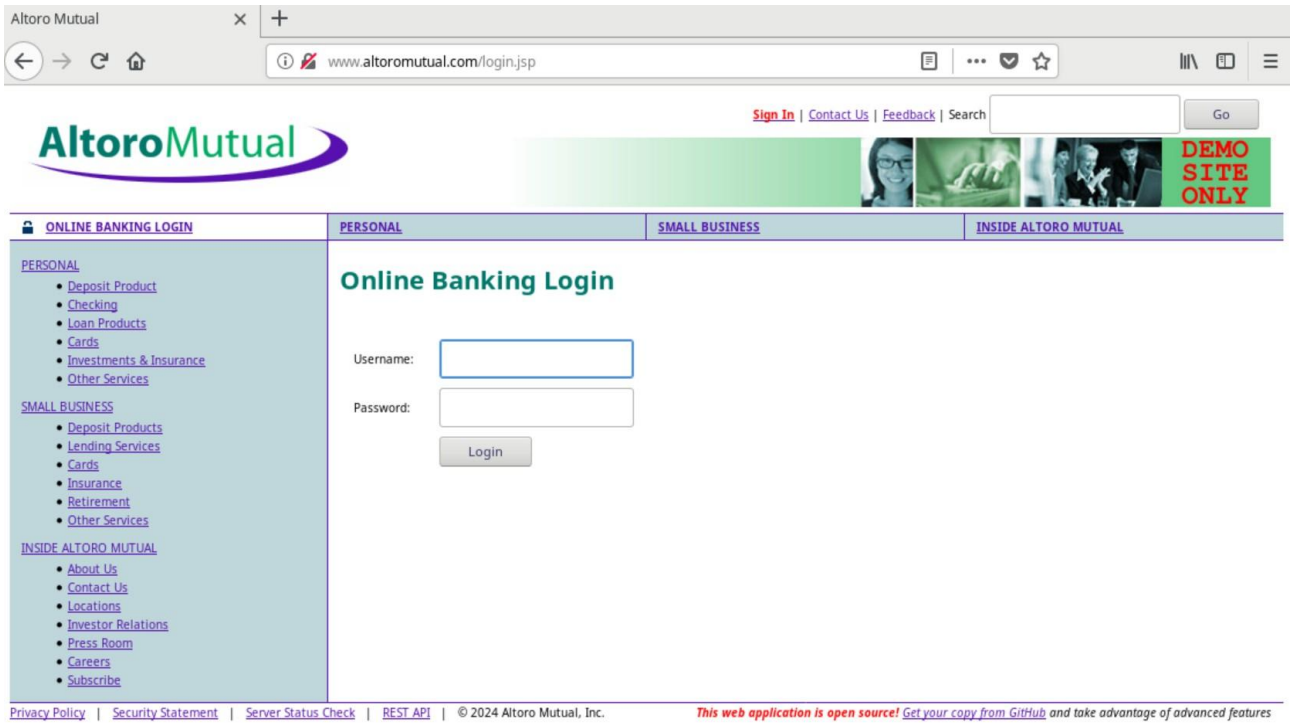
- **ip address**

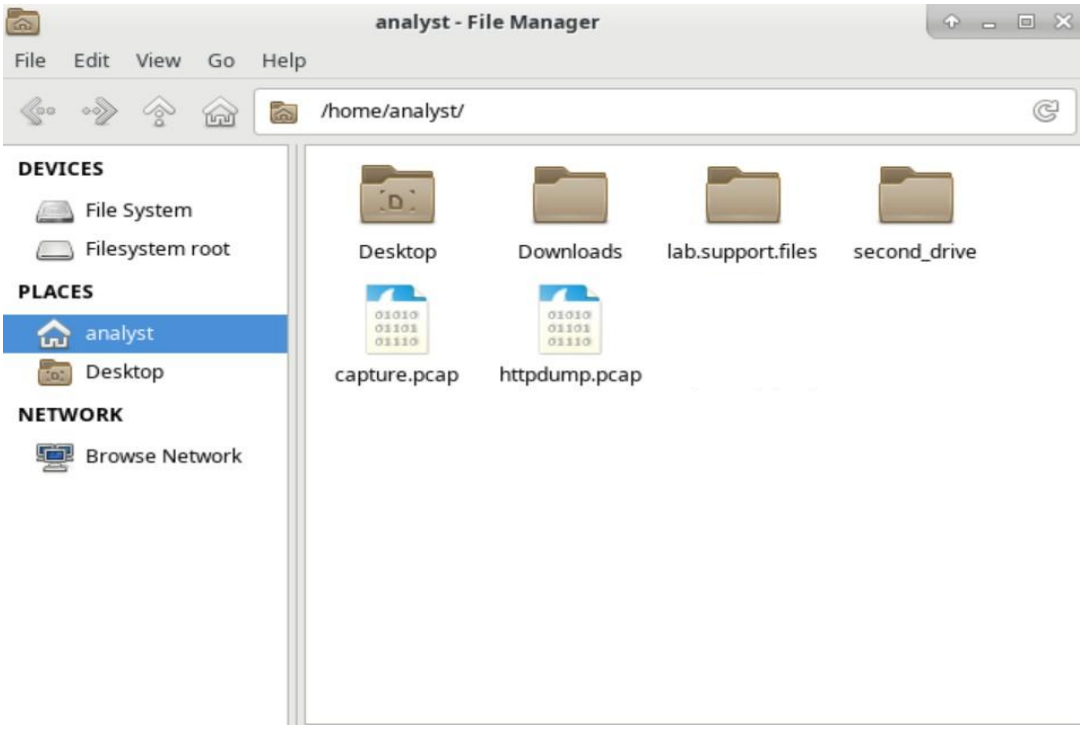
Nella seguente illustrazione ho utilizzato il comando specifico, per registrare il traffico di rete su l'intefaccia specifica, come descritta ed illustrata di seguito:

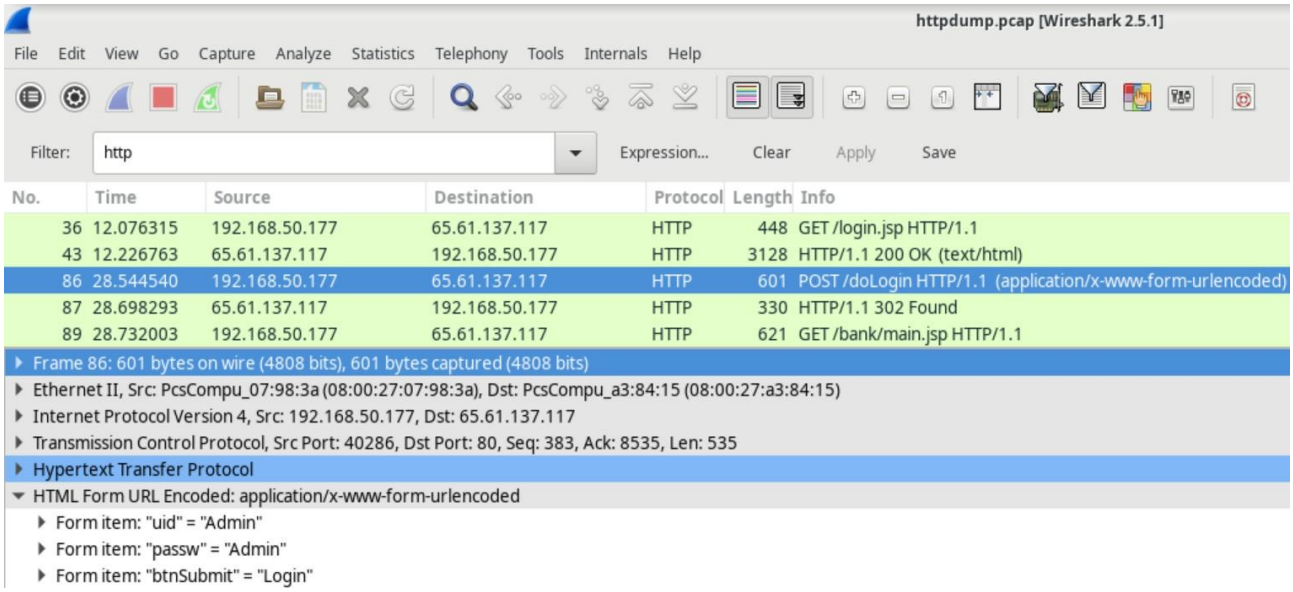
- **sudo tcpdump –i enp0s3 –s 0 –w httpdump.pcap**



Dopo aver utilizzato il comando illustrato in precedenza per registrare il traffico di rete sull'interfaccia **enp0s3**, vado sul sito di **AltoroMutual** e successivamente, dopo aver effettuato l'accesso al sito web, vado sul file creato in precedenza, con estensione **pcap** ed in fondo alla schermata del traffico di rete, vado sulla voce **HTML**, come illustrato nella prossima immagine:





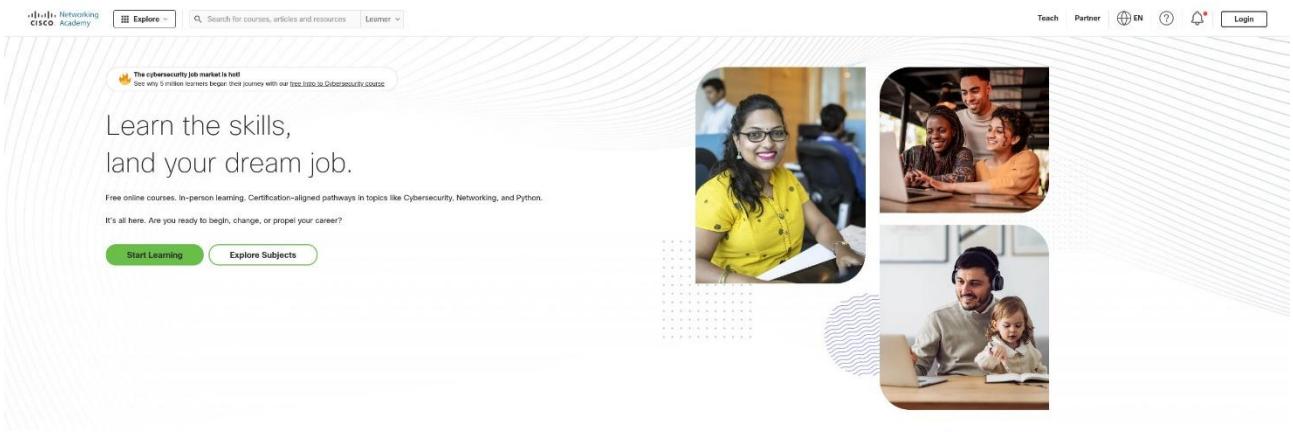


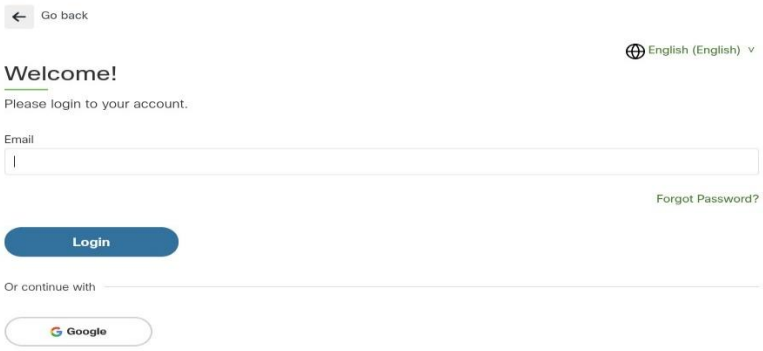
Dopo aver effettuato le operazioni sopra descritte ed illustrate per l'analisi del protocollo http, utilizzo il comando specifico per la registrazione del traffico di rete con protcollo HTTPS, come illustrato di seguito:

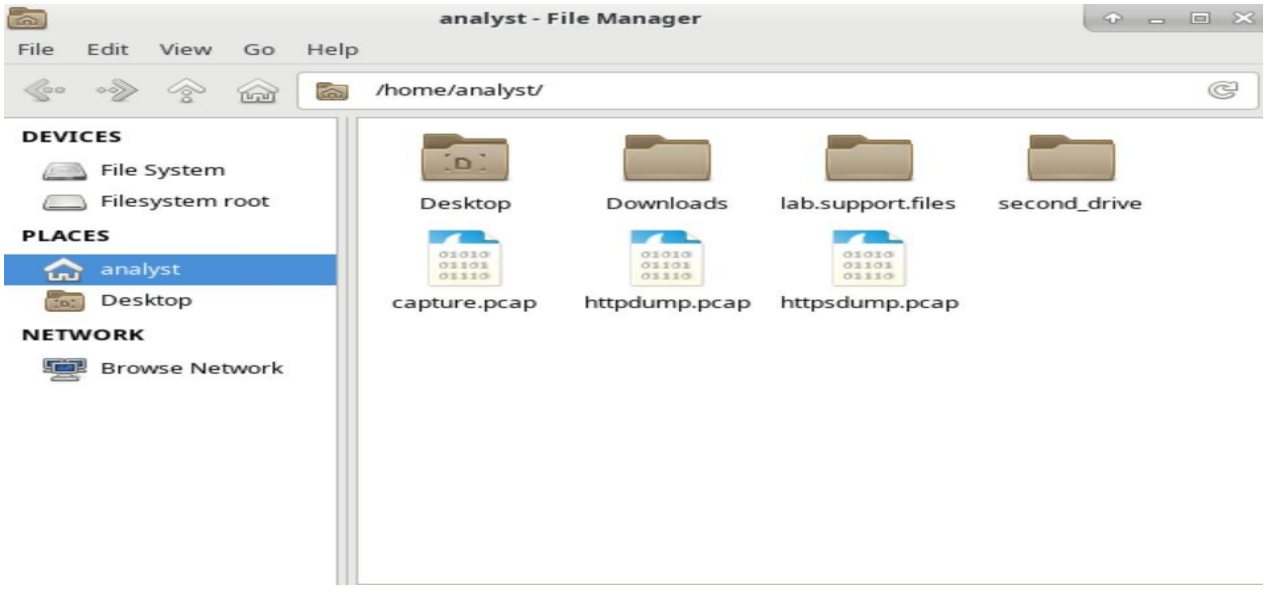
- **sudo tcpdump –i enp0s3 –s 0 –w httpsdump.pcap**

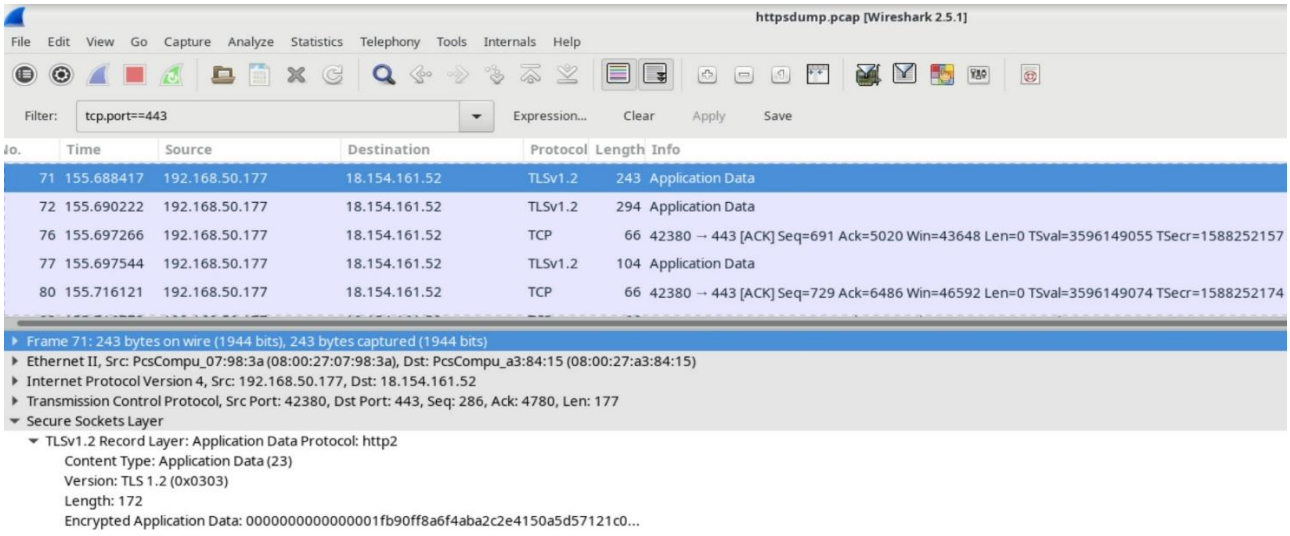
```
[analyst@secOps ~]$ sudo tcpdump -w enp0s3 -s 0 -w httpsdump.pcap
[sudo] password for analyst:
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
```

Dopo aver utilizzato il comando illustrato in precedenza per registrare il traffico di rete sull'interfaccia enp0s3, vado sul sito di **Netacad** e successivamente, dopo aver effettuato l'accesso al sito web, vado sul file creato in precedenza, con estensione **pcap** ed in fondo alla schermata del traffico di rete, vado sulla voce **HTML**, come illustrato nella prossima immagine:




Go back
English (English)
Welcome!
Please login to your account.
Email
Forgot Password?
Login
Or continue with
Google


analyst - File Manager
File Edit View Go Help
/home/analyst/
DEVICES
File System
Filesystem root
PLACES
analyst
Desktop
NETWORK
Browse Network
Desktop
Downloads
lab.support.files
second_drive
capture.pcap
httpdump.pcap
httpsdump.pcap


httpsdump.pcap [Wireshark 2.5.1]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: tcp.port==443
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
71 155.688417 192.168.50.177 18.154.161.52 TLSv1.2 243 Application Data
72 155.690222 192.168.50.177 18.154.161.52 TLSv1.2 294 Application Data
76 155.697266 192.168.50.177 18.154.161.52 TCP 66 42380 → 443 [ACK] Seq=691 Ack=5020 Win=43648 Len=0 TSval=3596149055 TSecr=1588252157
77 155.697544 192.168.50.177 18.154.161.52 TLSv1.2 104 Application Data
80 155.716121 192.168.50.177 18.154.161.52 TCP 66 42380 → 443 [ACK] Seq=729 Ack=6486 Win=46592 Len=0 TSval=3596149074 TSecr=1588252174
Frame 71: 243 bytes on wire (1944 bits), 243 bytes captured (1944 bits)
Ethernet II, Src: PcsCompu_07:98:3a (08:00:27:07:98:3a), Dst: PcsCompu_a3:84:15 (08:00:27:a3:84:15)
Internet Protocol Version 4, Src: 192.168.50.177, Dst: 18.154.161.52
Transmission Control Protocol, Src Port: 42380, Dst Port: 443, Seq: 286, Ack: 4780, Len: 177
Secure Sockets Layer
TLSv1.2 Record Layer: Application Data Protocol: http2
Content Type: Application Data (23)
Version: TLS 1.2 (0x0303)
Length: 172
Encrypted Application Data: 0000000000000001fb90ff8a6f4aba2c2e4150a5d57121c0...