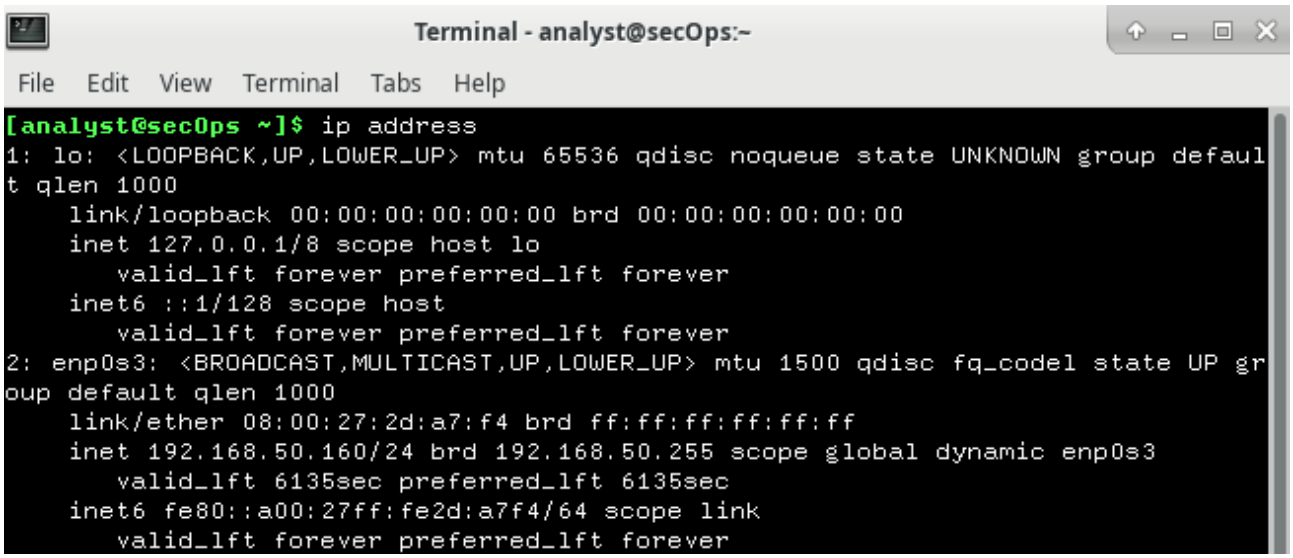
Utilizzo di Wireshark per Esaminare il Traffico HTTP e HTTPS

Capture and View HTTP Traffic

1. Ho aperto l'applicazione terminale e ho digitato il comando **ip address**.



I risultati sono : enp0s3 con indirizzo 192.168.50.160 e lo con indirizzo 127.0.0.1

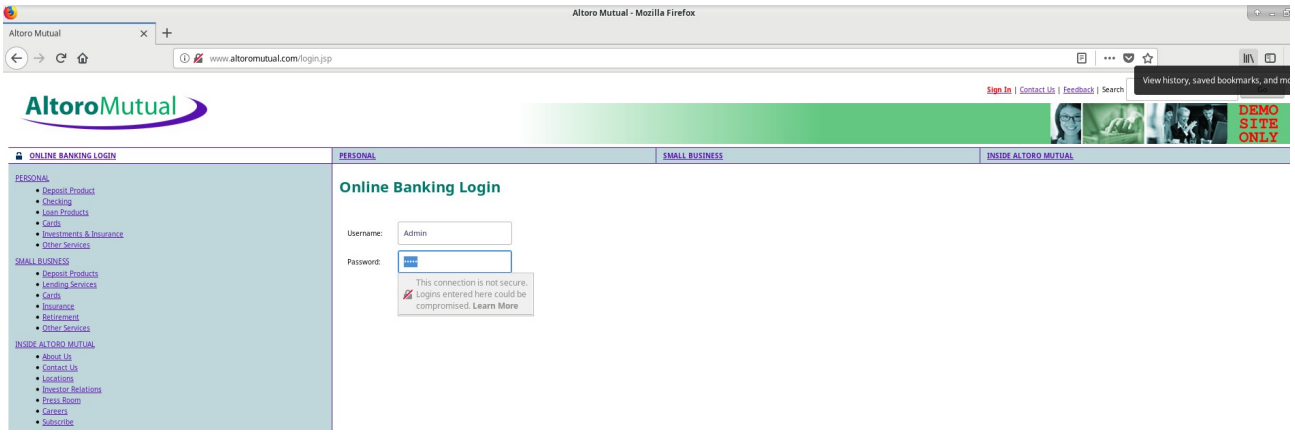
2. Ho digitato il comando **sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap** per intercettare il traffico sull'interfaccia enp0s3.

3. Ho aperto un browser web dalla barra di avvio all'interno della VM CyberOps Workstation. Sono andato all'indirizzo http://www.altoromutual.com/login.jsp.
Poiché questo sito utilizza HTTP, il traffico non è criptato. Ho cliccato sul campo della password per vedere il messaggio di avviso apparire.

Ho inserito il nome utente Admin con la password Admin e ho cliccato su Login.

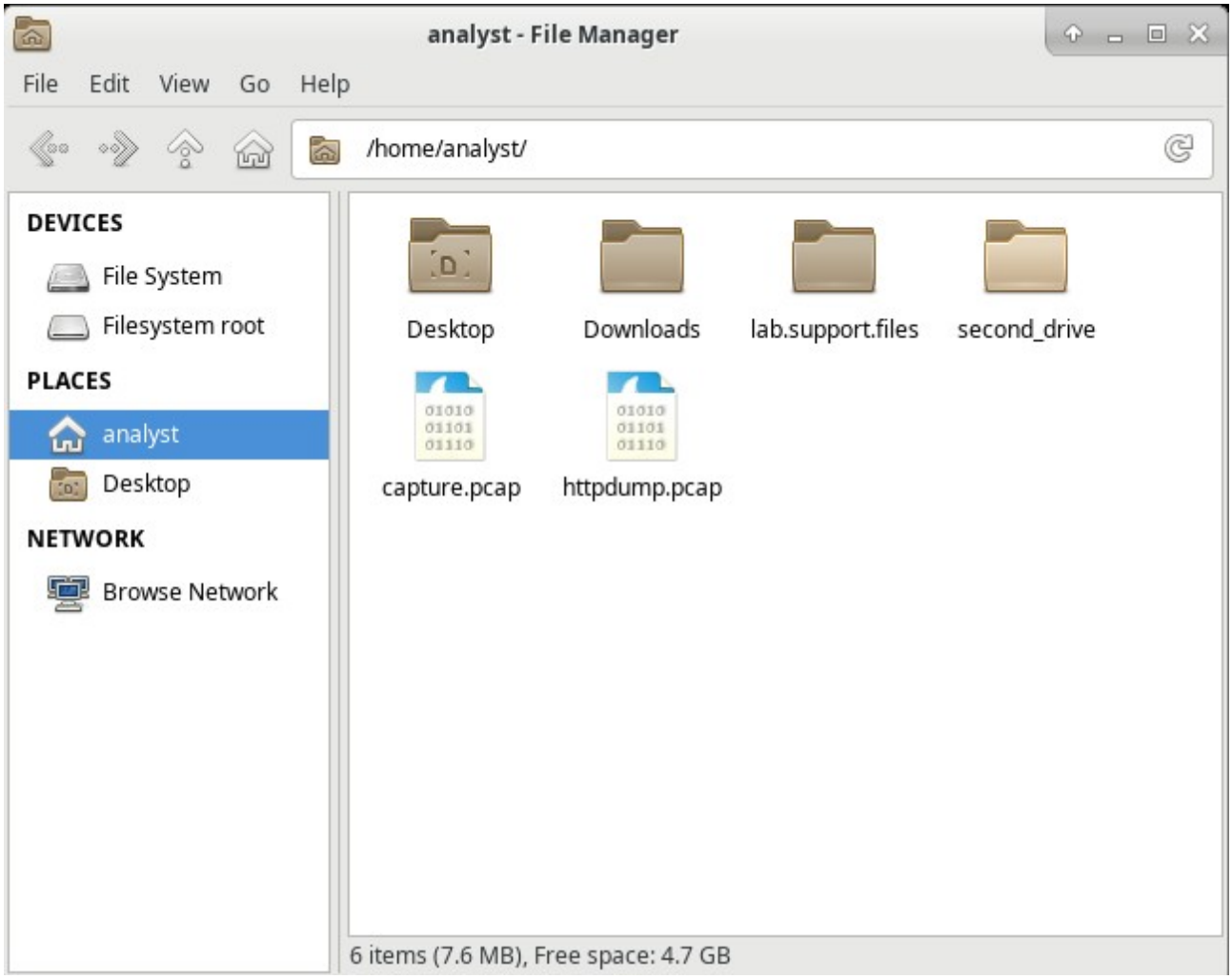
Dopo aver effettuato il login, ho chiuso il browser web.

Infine, sono tornato alla finestra del terminale dove stava girando tcpdump. Ho premuto CTRL+C per interrompere la cattura dei pacchetti.

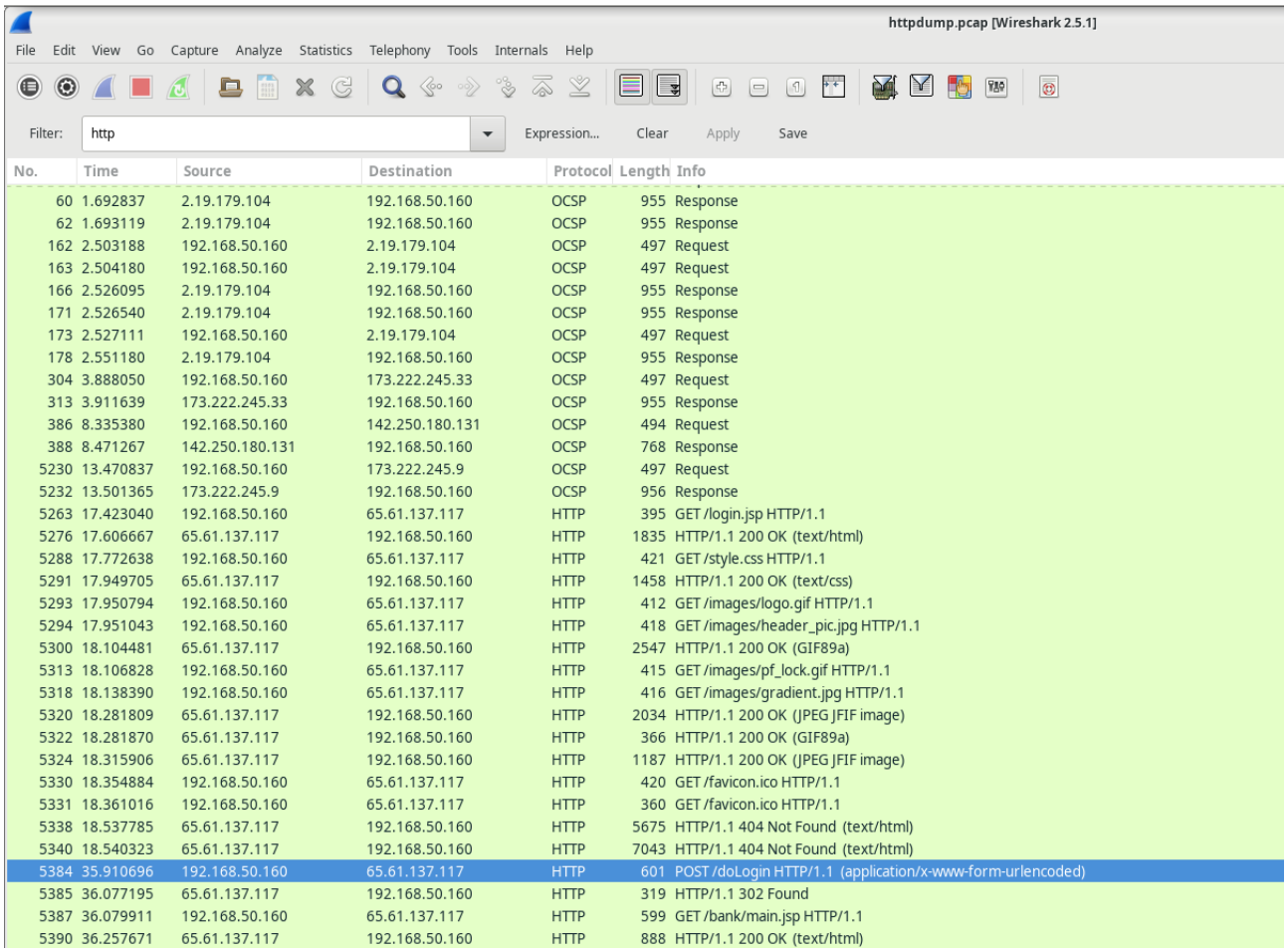



```
[analyst@secOps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
^C5529 packets captured
5529 packets received by filter
0 packets dropped by kernel
```

4. Ho cliccato sull'icona del **File Manager** sul desktop e ho navigato fino alla cartella home dell'utente analyst. Ho fatto doppio clic sul file **httpdump.pcap**. Nella finestra di dialogo **Apri con**, ho scorrere verso il basso fino a Wireshark e poi ho cliccato su **Apri**.



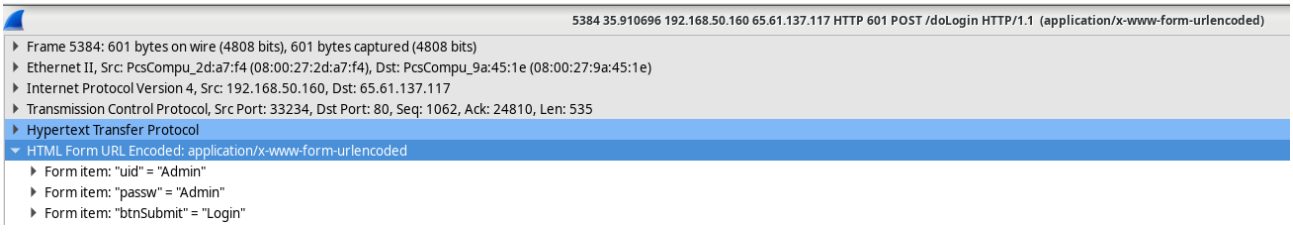
5. Nell'applicazione Wireshark, ho filtrato per **http** e ho cliccato su **Applica**.



No.	Time	Source	Destination	Protocol	Length	Info
60	1.692837	2.19.179.104	192.168.50.160	OCSP	955	Response
62	1.693119	2.19.179.104	192.168.50.160	OCSP	955	Response
162	2.503188	192.168.50.160	2.19.179.104	OCSP	497	Request
163	2.504180	192.168.50.160	2.19.179.104	OCSP	497	Request
166	2.526095	2.19.179.104	192.168.50.160	OCSP	955	Response
171	2.526540	2.19.179.104	192.168.50.160	OCSP	955	Response
173	2.527111	192.168.50.160	2.19.179.104	OCSP	497	Request
178	2.551180	2.19.179.104	192.168.50.160	OCSP	955	Response
304	3.888050	192.168.50.160	173.222.245.33	OCSP	497	Request
313	3.911639	173.222.245.33	192.168.50.160	OCSP	955	Response
386	8.335380	192.168.50.160	142.250.180.131	OCSP	494	Request
388	8.471267	142.250.180.131	192.168.50.160	OCSP	768	Response
5230	13.470837	192.168.50.160	173.222.245.9	OCSP	497	Request
5232	13.501365	173.222.245.9	192.168.50.160	OCSP	956	Response
5263	17.423040	192.168.50.160	65.61.137.117	HTTP	395	GET /login.jsp HTTP/1.1
5276	17.606667	65.61.137.117	192.168.50.160	HTTP	1835	HTTP/1.1 200 OK (text/html)
5288	17.772638	192.168.50.160	65.61.137.117	HTTP	421	GET /style.css HTTP/1.1
5291	17.949705	65.61.137.117	192.168.50.160	HTTP	1458	HTTP/1.1 200 OK (text/css)
5293	17.950794	192.168.50.160	65.61.137.117	HTTP	412	GET /images/logo.gif HTTP/1.1
5294	17.951043	192.168.50.160	65.61.137.117	HTTP	418	GET /images/header_pic.jpg HTTP/1.1
5300	18.104481	65.61.137.117	192.168.50.160	HTTP	2547	HTTP/1.1 200 OK (GIF89a)
5313	18.106828	192.168.50.160	65.61.137.117	HTTP	415	GET /images/pf_lock.gif HTTP/1.1
5318	18.138390	192.168.50.160	65.61.137.117	HTTP	416	GET /images/gradient.jpg HTTP/1.1
5320	18.281809	65.61.137.117	192.168.50.160	HTTP	2034	HTTP/1.1 200 OK (JPEG JFIF image)
5322	18.281870	65.61.137.117	192.168.50.160	HTTP	366	HTTP/1.1 200 OK (GIF89a)
5324	18.315906	65.61.137.117	192.168.50.160	HTTP	1187	HTTP/1.1 200 OK (JPEG JFIF image)
5330	18.354884	192.168.50.160	65.61.137.117	HTTP	420	GET /favicon.ico HTTP/1.1
5331	18.361016	192.168.50.160	65.61.137.117	HTTP	360	GET /favicon.ico HTTP/1.1
5338	18.537785	65.61.137.117	192.168.50.160	HTTP	5675	HTTP/1.1 404 Not Found (text/html)
5340	18.540323	65.61.137.117	192.168.50.160	HTTP	7043	HTTP/1.1 404 Not Found (text/html)
5384	35.910696	192.168.50.160	65.61.137.117	HTTP	601	POST /doLogin HTTP/1.1 (application/x-www-form-urlencoded)
5385	36.077195	65.61.137.117	192.168.50.160	HTTP	319	HTTP/1.1 302 Found
5387	36.079911	192.168.50.160	65.61.137.117	HTTP	599	GET /bank/main.jsp HTTP/1.1
5390	36.257671	65.61.137.117	192.168.50.160	HTTP	888	HTTP/1.1 200 OK (text/html)

6. Ho navigato tra i vari messaggi HTTP e ho selezionato il messaggio **POST**.

7. Nella finestra inferiore ho espanso la sezione **HTML Form URL Encoded: application/x-www-form-urlencoded**.

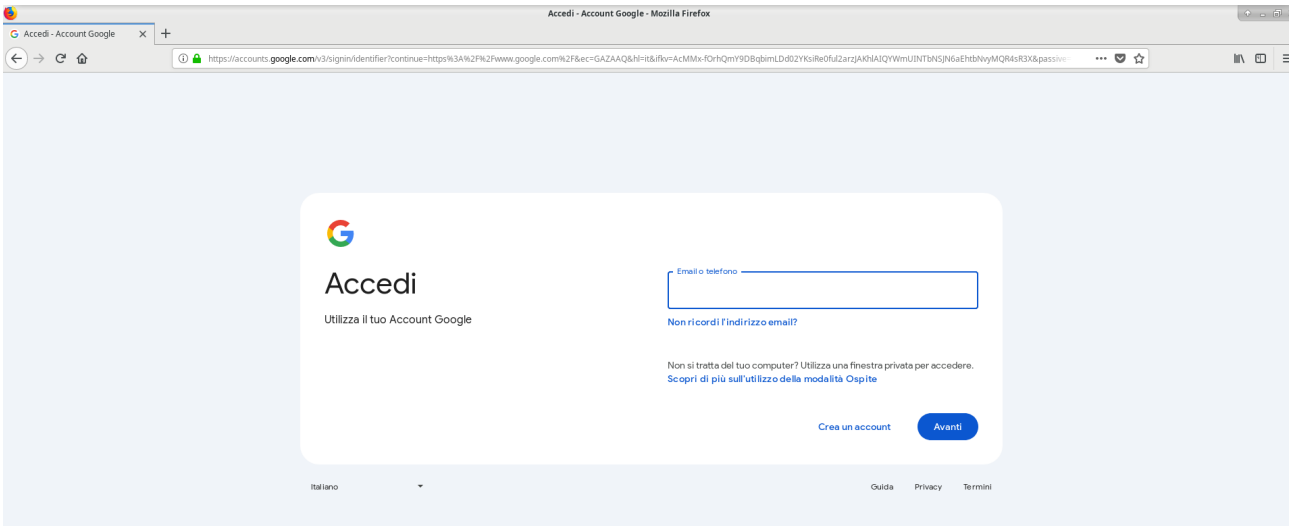


Vengono mostrati in chiaro uid e password.

Capture and View HTTPS Traffic

1. Ho digitato il comando **sudo tcpdump -i enp0s3 -s 0 -w httpsdump.pcap**. Quando mi è stata richiesta, ho inserito la password **cyberops** per l'utente **analyst**.

2. Ho aperto un browser web dalla barra di avvio all'interno della VM CyberOps Workstation. Sono andato all'indirizzo **www.google.com**



3. Ho effettuato il login, poi ho chiuso il browser web nella VM.
Sono tornato alla finestra del terminale dove stava girando tcpdump. Ho premuto **CTRL+C** per interrompere la cattura dei pacchetti.

```
[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
^C3853 packets captured
3855 packets received by filter
0 packets dropped by kernel
```

4. Nell'applicazione Wireshark, ho espanso verticalmente la finestra di cattura e poi ho filtrato il traffico per **HTTPS** tramite la porta **443**. Nella finestra inferiore, il messaggio è visualizzato. Dopo la sezione **TCP**, ora c'è una sezione **Secure Sockets Layer (SSL/TLS 1.2)** invece di **HTTP**. Ho completamente espanso la sezione **Secure Sockets Layer**.
Ho cliccato su **Encrypted Application Data**. Ho notato che il payload dei dati è criptato utilizzando **TLSv1.2** e non può essere visualizzato. Infine, ho chiuso tutte le finestre e ho spento la macchina virtuale.