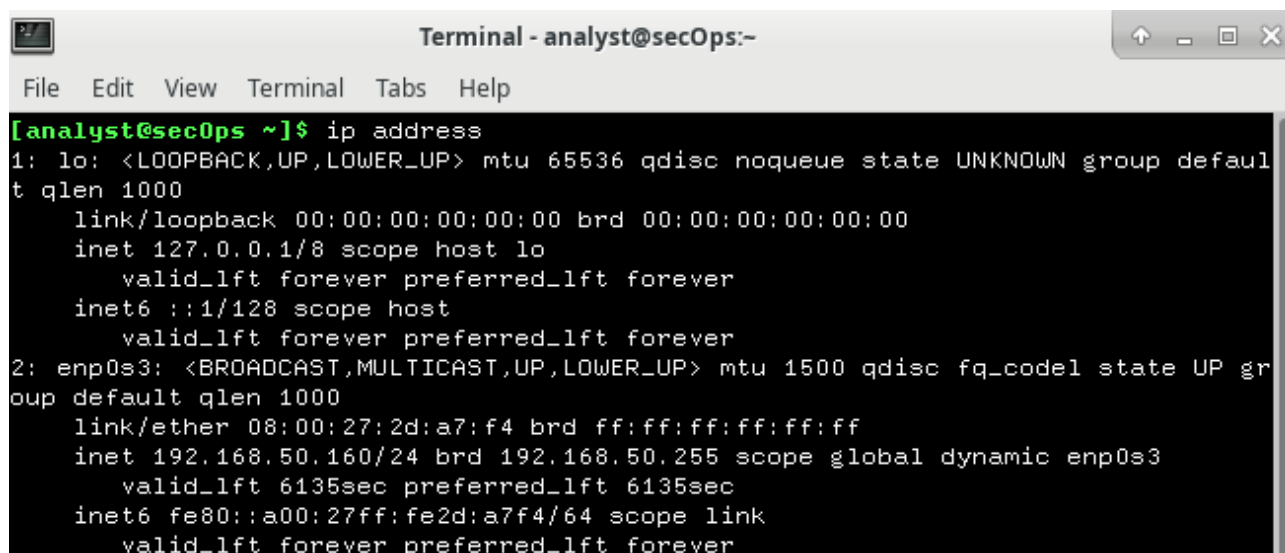


Utilizzo di Wireshark per Esaminare il Traffico HTTP e HTTPS

Capture and View HTTP Traffic

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



```
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 08:00:27:2d:a7:f4 brd ff:ff:ff:ff:ff:ff  
    inet 192.168.50.160/24 brd 192.168.50.255 scope global dynamic enp0s3  
        valid_lft 6135sec preferred_lft 6135sec  
    inet6 fe80::a00:27ff:fe2d:a7f4/64 scope link  
        valid_lft forever preferred_lft forever
```

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

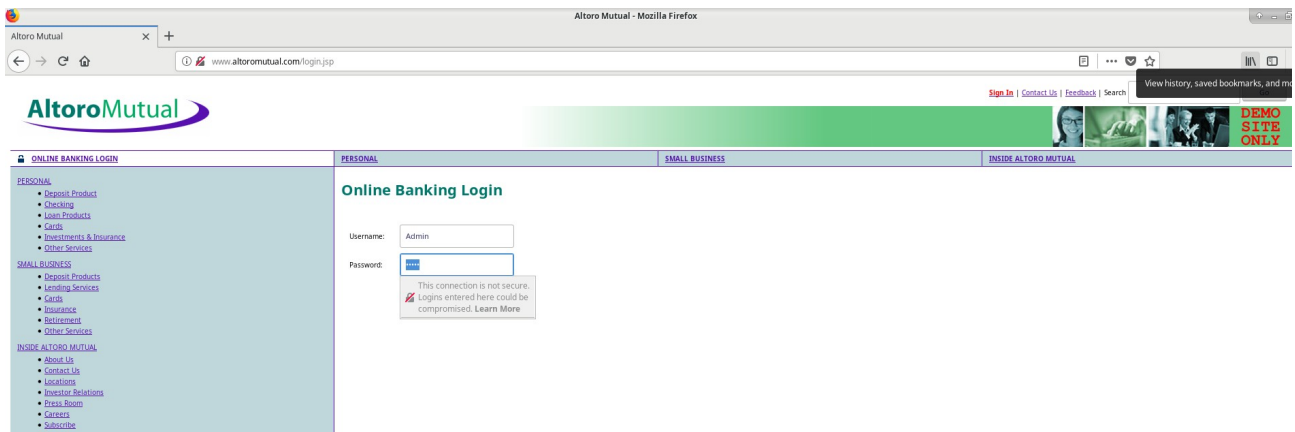
2. Ho digitato il comando **sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap** per intercettare il traffico sull'interfaccia enp0s3.

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.

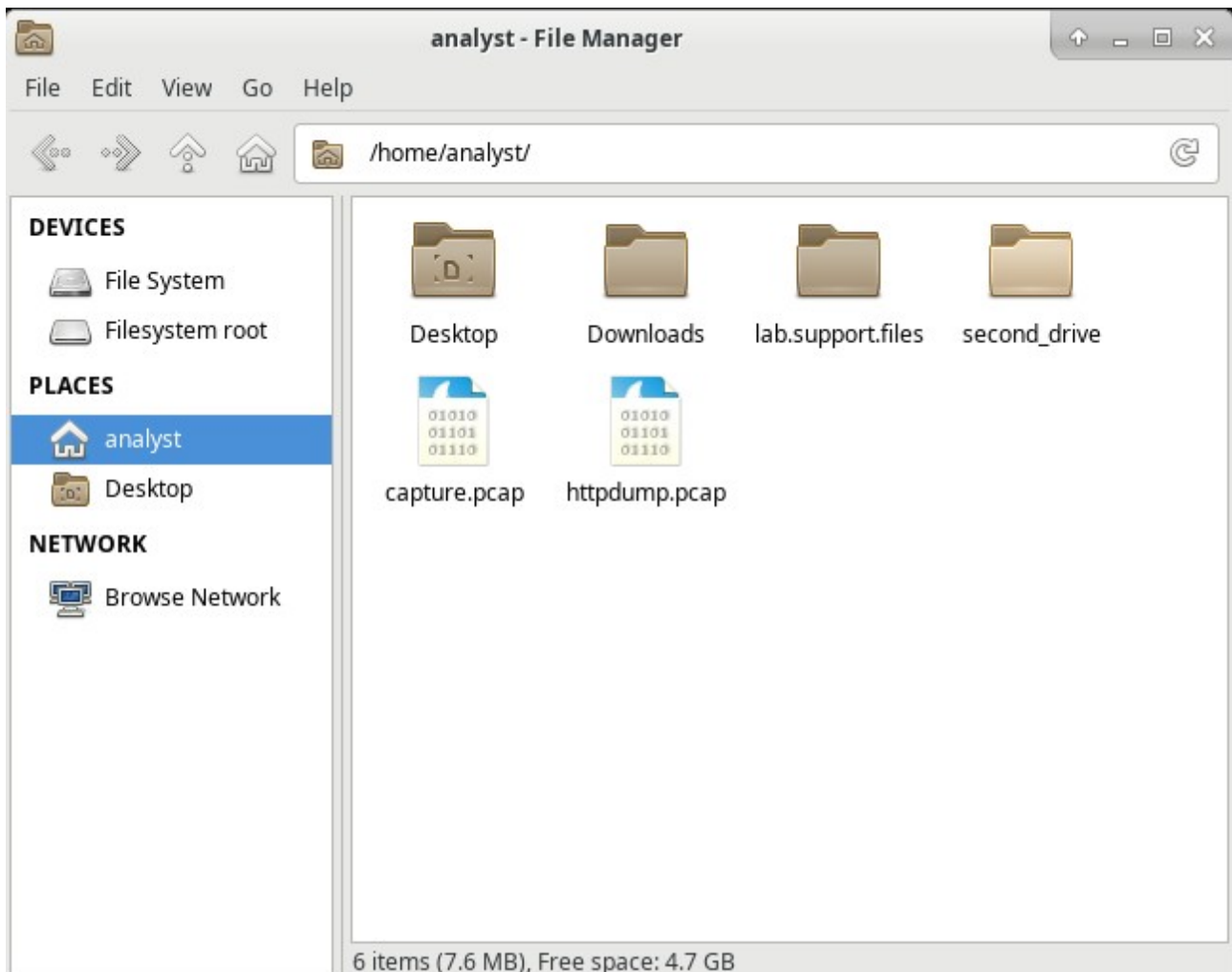
Dopo aver effettuato il login, ho chiuso il browser web.

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

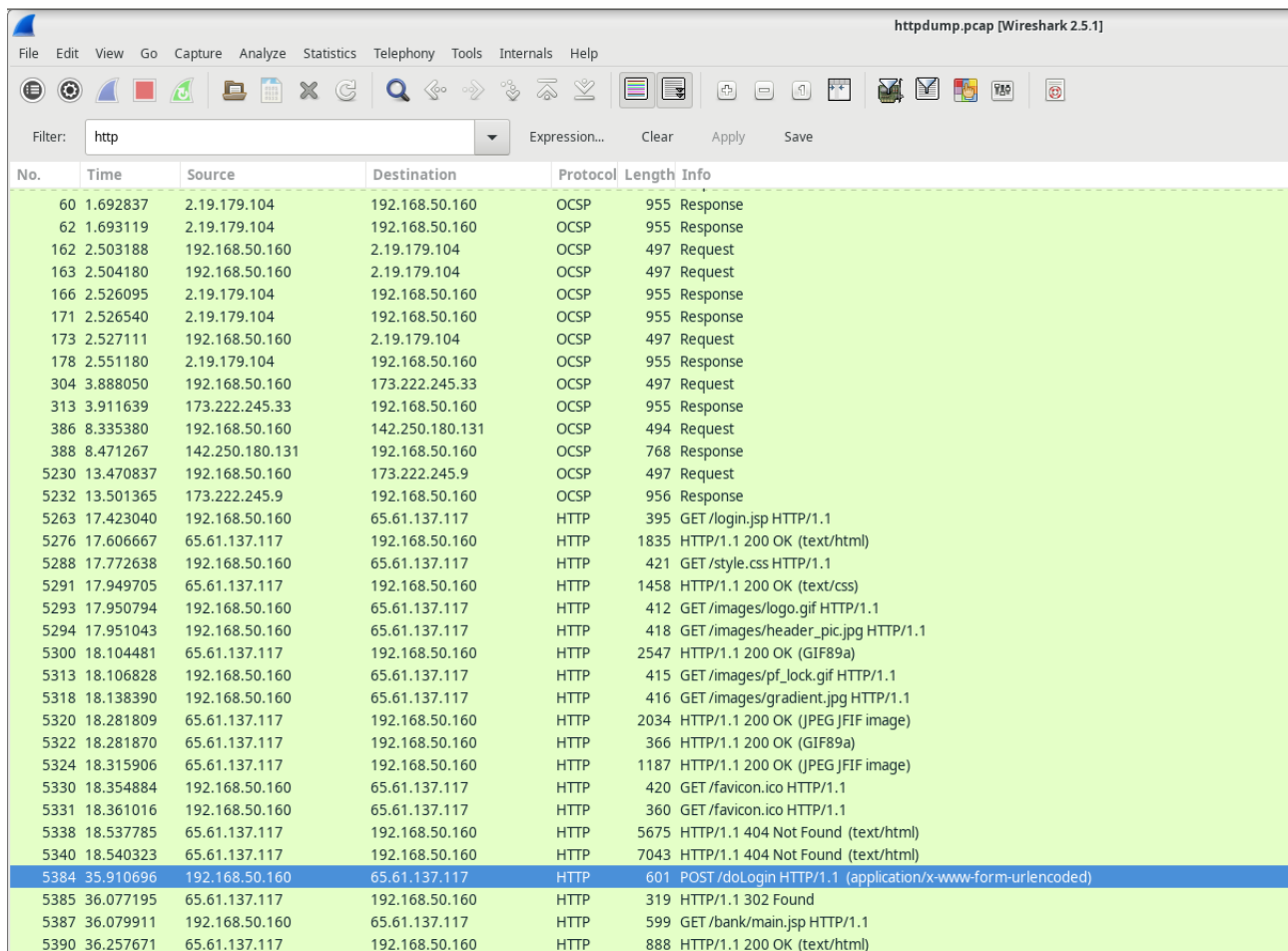


```
[analyst@secOps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
^C5529 packets captured
5529 packets received by filter
0 packets dropped by kernel
```

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**.

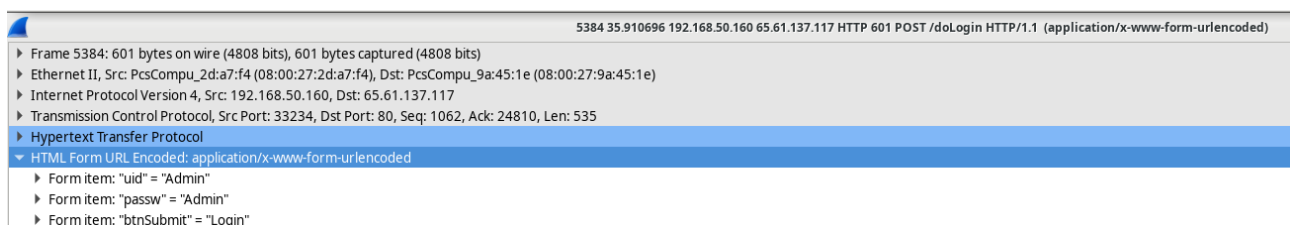


The image shows the Wireshark 2.5.1 interface with the packet list filtered by 'http'. The table below represents the data shown in the packet list pane.

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**.



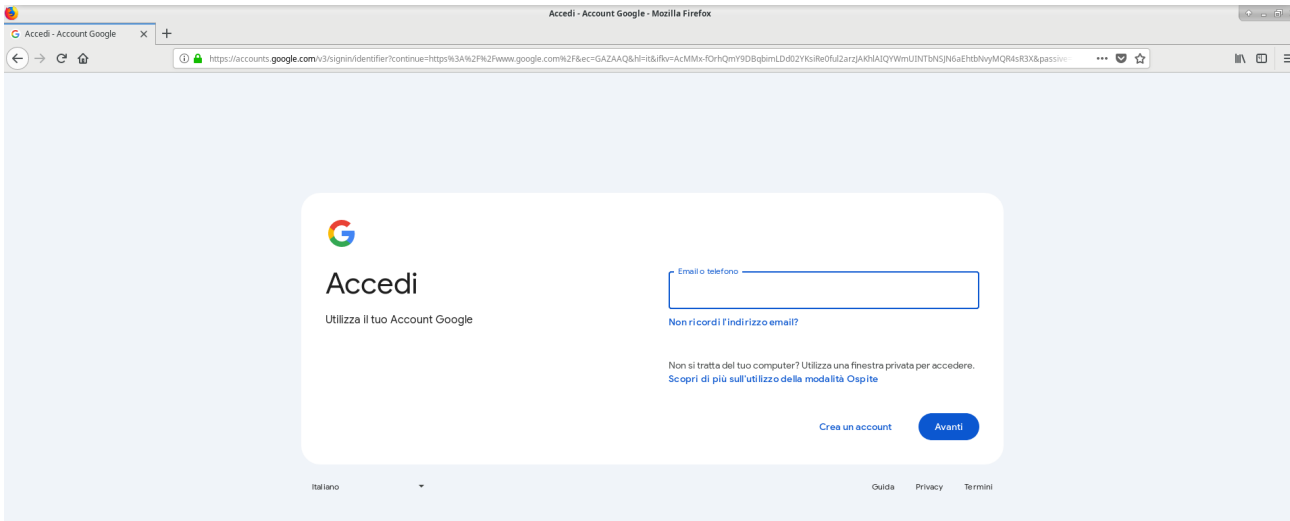
The image shows the expanded details of the selected POST packet (No. 5384). The table below represents the data shown in the packet details pane.

5384 35.910696 192.168.50.160 65.61.137.117 HTTP 601 POST /doLogin HTTP/1.1 (application/x-www-form-urlencoded)	
▶	Frame 5384: 601 bytes on wire (4808 bits), 601 bytes captured (4808 bits)
▶	Ethernet II, Src: PcsCompu_2d:a7:f4 (08:00:27:2d:a7:f4), Dst: PcsCompu_9a:45:1e (08:00:27:9a:45:1e)
▶	Internet Protocol Version 4, Src: 192.168.50.160, Dst: 65.61.137.117
▶	Transmission Control Protocol, Src Port: 33234, Dst Port: 80, Seq: 1062, Ack: 24810, Len: 535
▶	Hypertext Transfer Protocol
▼	HTML Form URL Encoded: application/x-www-form-urlencoded
▶	Form item: "uid" = "Admin"
▶	Form item: "passw" = "Admin"
▶	Form item: "btnSubmit" = "Login"

Vengono mostrati in chiaro uid e password.

Capture and View HTTPS Traffic

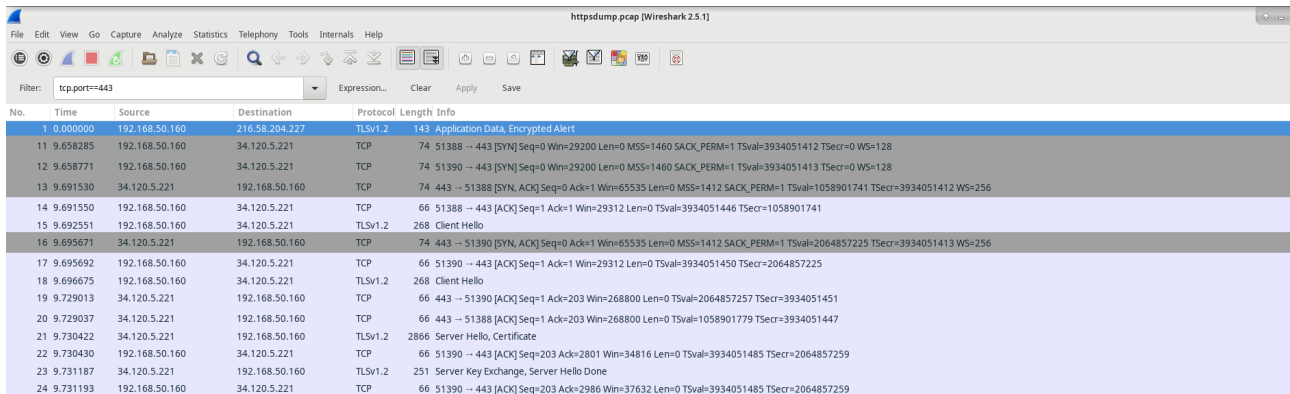
1. Ho digitato il comando `sudo tcpdump -i enp0s3 -s 0 -w httpsdump.pcap`. Quando mi è stata richiesta, ho inserito la password **cyberops** per l'utente **analyst**.
2. Ho aperto un browser web dalla barra di avvio all'interno della VM CyberOps Workstation. Sono andato all'indirizzo www.google.com



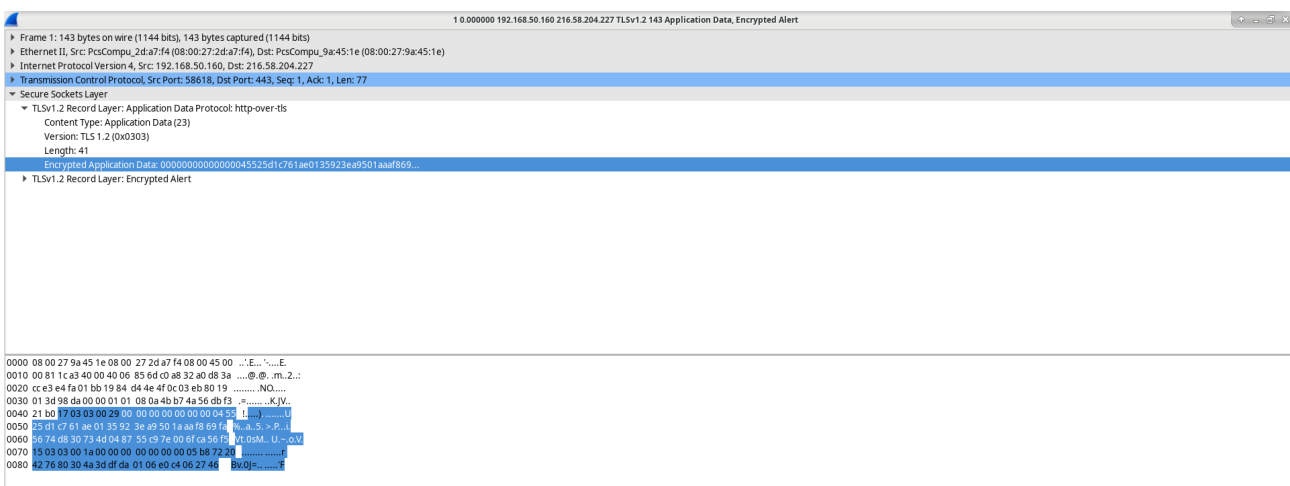
3. Ho effettuato il login, poi ho chiuso il browser web nella VM. Sono tornato alla finestra del terminale dove stava girando tcpdump. Ho premuto **CTRL+C** per interrompere la cattura dei pacchetti.

```
[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.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.50.160	216.58.204.227	TLSv1.2	143	Application Data, Encrypted Alert
11	9.658285	192.168.50.160	34.120.5.221	TCP	74	51388 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=3934051412 TSecr=0 WS=128
12	9.658771	192.168.50.160	34.120.5.221	TCP	74	51390 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=3934051413 TSecr=0 WS=128
13	9.691530	34.120.5.221	192.168.50.160	TCP	74	443 → 51388 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM=1 TSval=1058901741 TSecr=3934051412 WS=256
14	9.691550	192.168.50.160	34.120.5.221	TCP	66	51388 → 443 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=3934051446 TSecr=1058901741
15	9.692551	192.168.50.160	34.120.5.221	TLSv1.2	268	Client Hello
16	9.695671	34.120.5.221	192.168.50.160	TCP	74	443 → 51390 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM=1 TSval=2064857225 TSecr=3934051413 WS=256
17	9.695692	192.168.50.160	34.120.5.221	TCP	66	51390 → 443 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=3934051450 TSecr=2064857225
18	9.696675	192.168.50.160	34.120.5.221	TLSv1.2	268	Client Hello
19	9.729013	34.120.5.221	192.168.50.160	TCP	66	443 → 51390 [ACK] Seq=1 Ack=203 Win=268800 Len=0 TSval=2064857257 TSecr=3934051451
20	9.729037	34.120.5.221	192.168.50.160	TCP	66	443 → 51388 [ACK] Seq=1 Ack=203 Win=268800 Len=0 TSval=1058901779 TSecr=3934051447
21	9.730422	34.120.5.221	192.168.50.160	TLSv1.2	2866	Server Hello, Certificate
22	9.730430	192.168.50.160	34.120.5.221	TCP	66	51390 → 443 [ACK] Seq=203 Ack=2801 Win=34816 Len=0 TSval=3934051485 TSecr=2064857259
23	9.731187	34.120.5.221	192.168.50.160	TLSv1.2	251	Server Key Exchange, Server Hello Done
24	9.731193	192.168.50.160	34.120.5.221	TCP	66	51390 → 443 [ACK] Seq=203 Ack=2986 Win=37632 Len=0 TSval=3934051485 TSecr=2064857259



1 0.000000 192.168.50.160 216.58.204.227 TLSv1.2 143 Application Data, Encrypted Alert	
Frame 1: 143 bytes on wire (1144 bits), 143 bytes captured (1144 bits)	
Ethernet II, Src: PcsCompu_2d:a7:f4 (08:00:27:2d:a7:f4), Dst: PcsCompu_9a:45:1e (08:00:27:9a:45:1e)	
Internet Protocol Version 4, Src: 192.168.50.160, Dst: 216.58.204.227	
Transmission Control Protocol, Src Port: 58618, Dst Port: 443, Seq: 1, Ack: 1, Len: 77	
Secure Sockets Layer	
TLSv1.2 Record Layer: Application Data Protocol: http-over-tls	
Content Type: Application Data (23)	
Version: TLS 1.2 (0x0303)	
Length: 41	
Encrypted Application Data: 000000000000000045525d1c761ae0135923ea9501aaaf869...	
TLSv1.2 Record Layer: Encrypted Alert	

0000	08 00 27 9a 45 1e 08 00 27 2d a7 f4 08 00 45 00 ...E.....E.
0010	00 81 1c a3 40 00 40 06 85 6d c0 a8 32 a0 d8 3a@.@..m..z..
0020	cc e3 e4 fa 01 bb 19 84 04 4e 4f 0c 03 eb 80 19NQ.....
0030	01 3d 98 da 00 00 01 01 08 0a 4b b7 4a 56 eb f9K.V.....
0040	21 b0 17 03 03 00 25 00 00 00 00 00 00 04 55U.....
0050	25 d1 c7 61 ae 01 35 92 3e a9 50 1a aa f8 69 faa..5..>P..U
0060	26 74 08 30 73 4d 04 87 55 c9 7e 00 6f ca 56 f9VL0SM..U--oV
0070	5 03 03 00 1a 00 00 00 00 00 00 05 b8 72 2bf.....
0080	22 76 80 30 4a 3d df da 01 06 e0 e4 06 27 46BUD.....f