

Progetto: Acquisizione e Analisi del Traffico HTTP e HTTPS con Wireshark

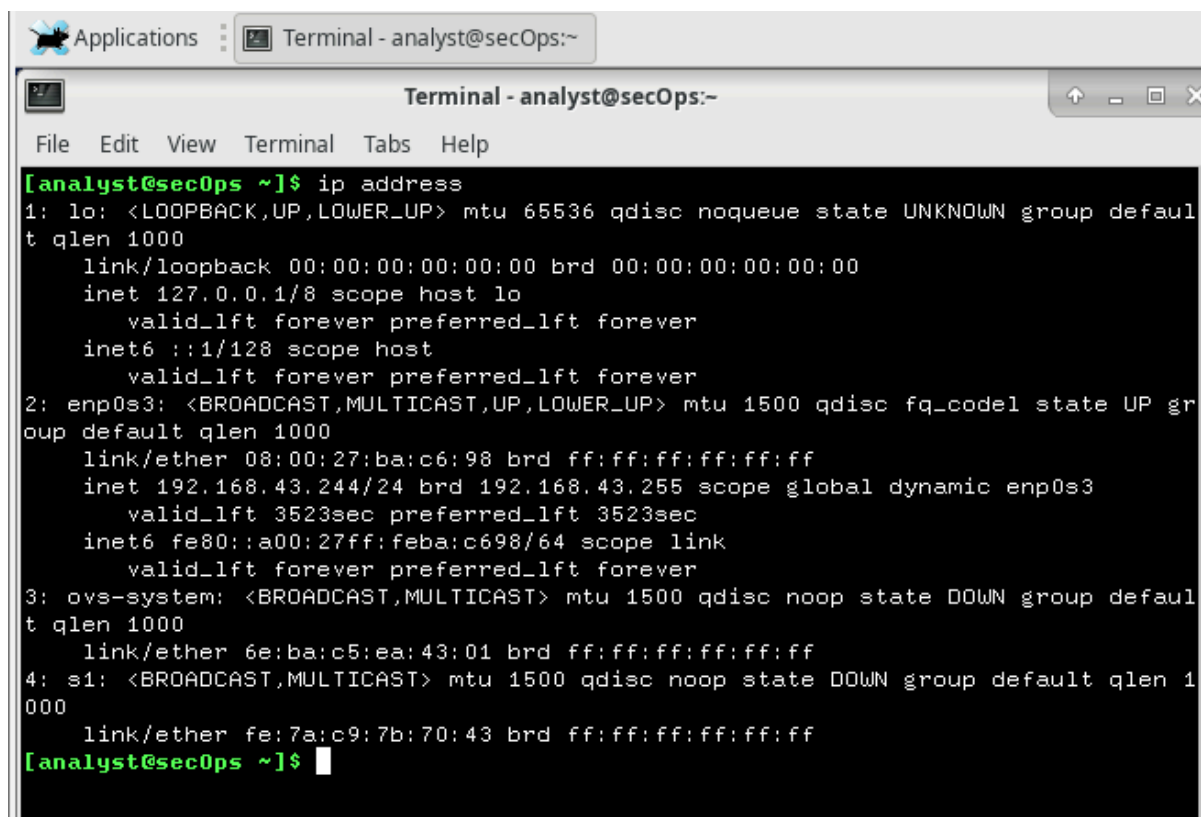
Obiettivo

In questo progetto, esploreremo l'utilizzo di **Wireshark** per catturare e analizzare il traffico di rete nei protocolli **HTTP** e **HTTPS**, mettendo in evidenza le differenze tra un protocollo non sicuro e uno crittografato. Attraverso l'analisi dei pacchetti acquisiti, potremo comprendere meglio il funzionamento della crittografia in HTTPS e i rischi legati all'uso di HTTP in contesti non sicuri.

Parte 1: Acquisire e Visualizzare il Traffico HTTP

Passaggio 1: Configurazione di Rete

Nello **Screenshot**, viene eseguito il comando `ip address`, che mostra i dettagli dell'interfaccia di rete del sistema. L'indirizzo IP assegnato all'interfaccia **enp0s3** è **192.168.43.244**. Questa configurazione è essenziale per identificare il dispositivo nel traffico di rete e capire su quale interfaccia catturare i pacchetti.

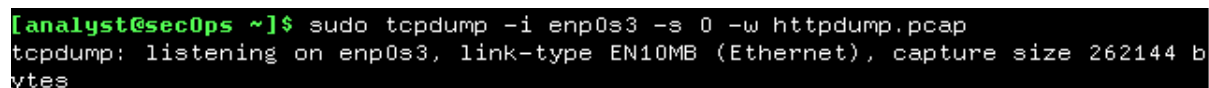
A screenshot of a terminal window titled "Terminal - analyst@secOps:~". The terminal shows the output of the command "ip address". The output lists network interfaces: "lo" (loopback), "enp0s3" (Ethernet), and "ovs-system" (Open vSwitch). Each interface entry includes details like MTU, state, group, and IP addresses (IPv4 and IPv6). The terminal prompt is "[analyst@secOps ~]\$".

```
[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:ba:c6:98 brd ff:ff:ff:ff:ff:ff
    inet 192.168.43.244/24 brd 192.168.43.255 scope global dynamic enp0s3
        valid_lft 3523sec preferred_lft 3523sec
    inet6 fe80::a00:27ff:feba:c698/64 scope link
        valid_lft forever preferred_lft forever
3: ovs-system: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 6e:ba:c5:ea:43:01 brd ff:ff:ff:ff:ff:ff
4: s1: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether fe:7a:c9:7b:70:43 brd ff:ff:ff:ff:ff:ff
[analyst@secOps ~]$
```

Passaggio 2: Avvio della Cattura del Traffico HTTP

Nello **Screenshot**, si avvia la cattura del traffico HTTP con il comando **tcpdump**:

```
sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap
```

A screenshot of a terminal window showing the execution of the command "sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap". The output shows "tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes". The terminal prompt is "[analyst@secOps ~]\$".

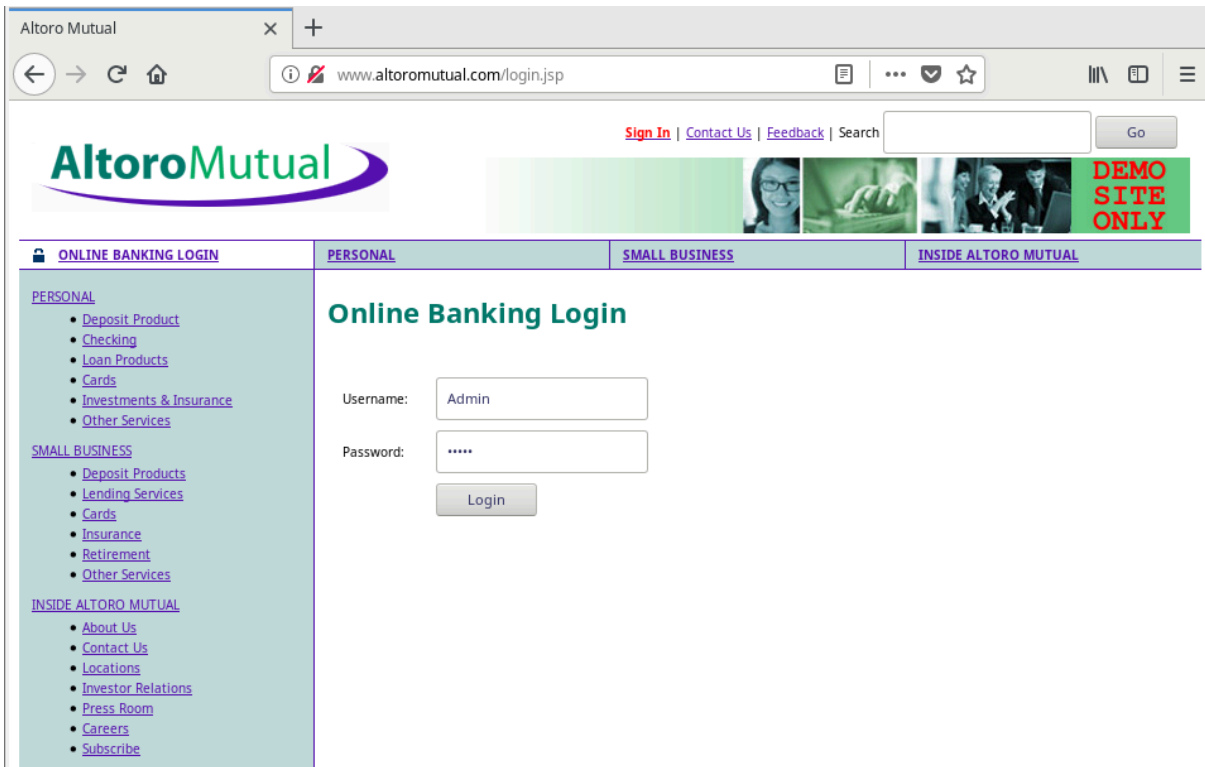
```
[analyst@secOps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
[analyst@secOps ~]$
```

Il comando specifica di catturare tutto il traffico sull'interfaccia **enp0s3** e salvarlo nel file **httpdump.pcap**. Questo file sarà successivamente analizzato in **Wireshark**.

Passaggio 3: Login su un Sito HTTP non Protetto

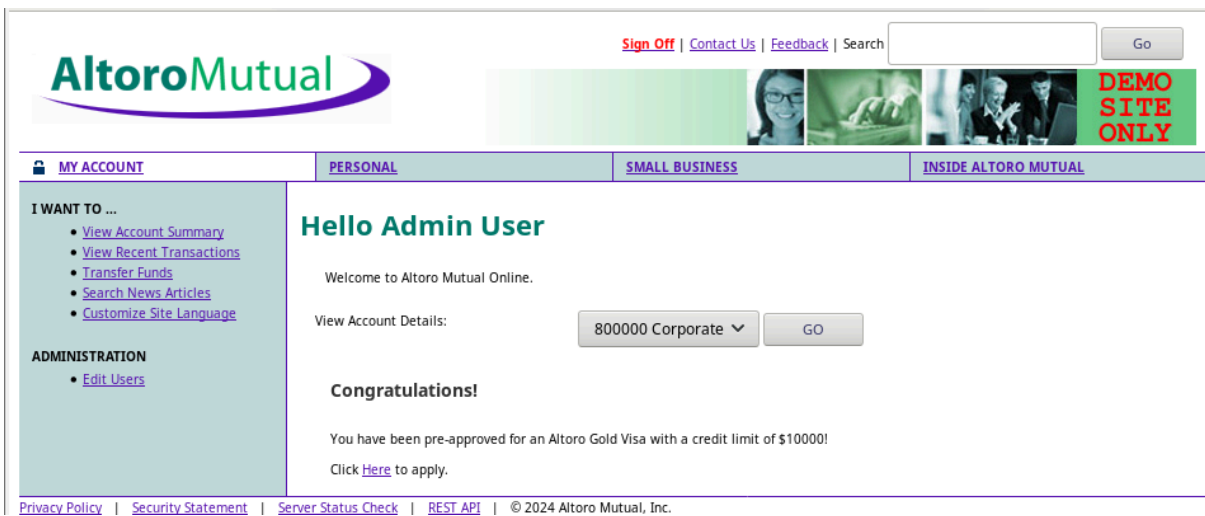
Nello **Screenshot**, viene mostrata la pagina di login del sito **Altoro Mutual**, accessibile tramite il protocollo HTTP. Il sito non utilizza HTTPS, quindi le

credenziali inserite nel form, come il nome utente **Admin** e la password, vengono inviate in chiaro sulla rete.



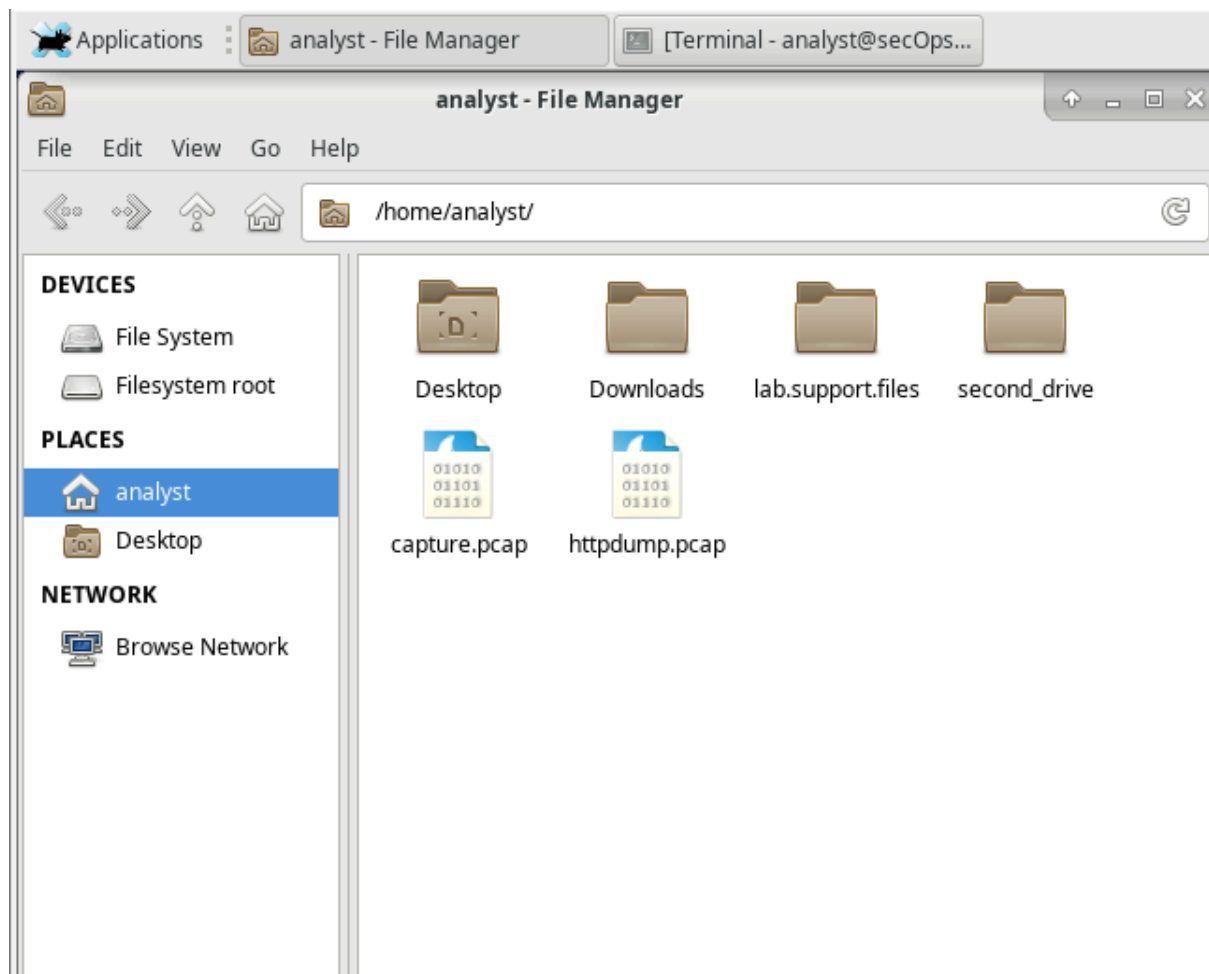
Passaggio 4: Accesso al Sito come Amministratore

Nello **Screenshot 4**, vediamo la schermata di successo del login, dove l'utente **Admin** ha effettuato l'accesso al conto aziendale da **800000 Corporate**. Questa fase indica il completamento del processo di login e il successo dell'operazione.



Passaggio 5: Visualizzazione del File di Cattura in Wireshark

Nello **Screenshot**, il file **httpdump.pcap** viene aperto in Wireshark. Nel gestore di file vediamo che il file è stato salvato insieme a un altro file di cattura **capture.pcap**, confermando che i pacchetti sono stati catturati correttamente e pronti per l'analisi.



Passaggio 6: Analisi dei Pacchetti HTTP

Nello **Screenshot**, all'interno di Wireshark viene applicato un filtro **HTTP** per visualizzare solo il traffico HTTP. Un pacchetto di interesse mostra una richiesta **POST** al percorso **/doLogin**. Analizzando il contenuto del pacchetto, possiamo vedere che le credenziali di accesso sono state trasmesse in chiaro.

No.	Time	Source	Destination	Protocol	Length	Info
3112	93.756923	192.168.43.244	192.229.221.95	OCSP	497	Request
3118	93.814189	192.229.221.95	192.168.43.244	OCSP	802	Response
3120	93.814286	192.229.221.95	192.168.43.244	OCSP	803	Response
3122	93.814319	192.229.221.95	192.168.43.244	OCSP	802	Response
3124	93.814350	192.229.221.95	192.168.43.244	OCSP	803	Response
3140	93.860464	192.229.221.95	192.168.43.244	OCSP	803	Response
3203	94.444415	192.168.43.244	34.107.221.82	HTTP	354	GET /success.txt HTTP/1.1
3230	94.676660	34.107.221.82	192.168.43.244	HTTP	282	HTTP/1.1 200 OK (text/plain)
4982	191.514082	192.168.43.244	23.220.255.60	OCSP	497	Request
4984	191.606838	23.220.255.60	192.168.43.244	OCSP	955	Response
5090	192.441934	192.168.43.244	23.220.255.34	OCSP	497	Request
5091	192.442256	192.168.43.244	23.220.255.34	OCSP	497	Request
5098	192.447506	192.168.43.244	23.220.255.34	OCSP	497	Request
5099	192.447841	192.168.43.244	23.220.255.34	OCSP	497	Request
5100	192.448084	192.168.43.244	23.220.255.34	OCSP	497	Request
5103	192.494632	23.220.255.34	192.168.43.244	OCSP	956	Response
5105	192.495414	23.220.255.34	192.168.43.244	OCSP	956	Response
5117	192.518648	23.220.255.34	192.168.43.244	OCSP	956	Response
5119	192.518755	23.220.255.34	192.168.43.244	OCSP	956	Response
5121	192.518786	23.220.255.34	192.168.43.244	OCSP	956	Response
6302	251.847855	192.168.43.244	65.61.137.117	HTTP	601	POST /doLogin HTTP/1.1 (application/x-www-form-urlencoded)
6303	252.050130	65.61.137.117	192.168.43.244	HTTP	290	HTTP/1.1 302 Found
6305	252.052696	192.168.43.244	65.61.137.117	HTTP	581	GET /bank/main.jsp HTTP/1.1
6307	252.253872	65.61.137.117	192.168.43.244	HTTP	5012	HTTP/1.1 200 OK (text/html)

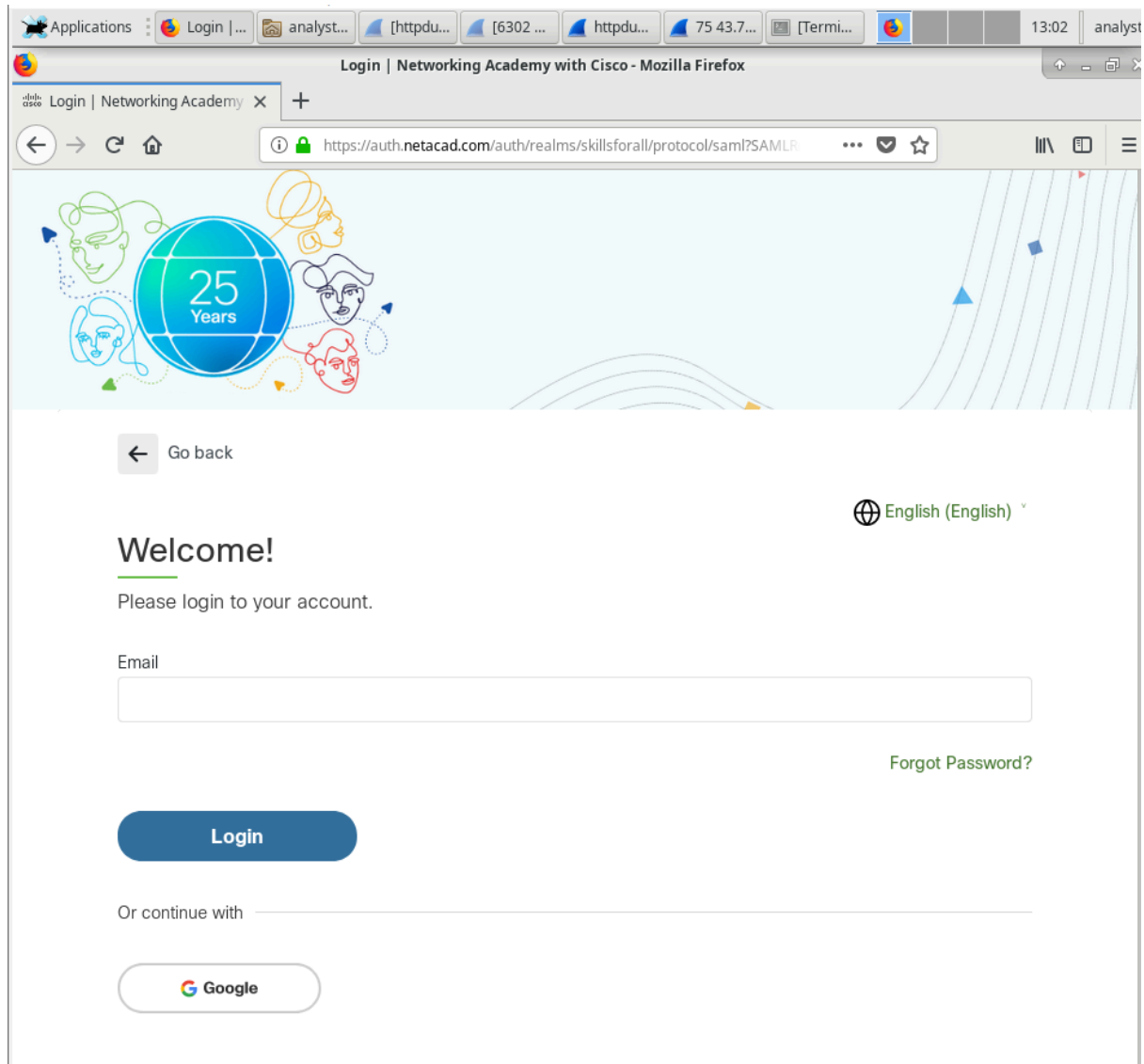
- **Screenshot** mostra ulteriori dettagli del pacchetto HTTP, confermando che le credenziali **username = Admin** e **password = Admin** sono visibili nel traffico intercettato. Questo dimostra la vulnerabilità del protocollo HTTP, che non protegge i dati sensibili trasmessi sulla rete.

6302 251.847855 192.168.43.244 65.61.137.117 HTTP 601 POST /doLogin HTTP/1.1 (application/x-www-form-urlencoded)	
▶	Frame 6302: 601 bytes on wire (4808 bits), 601 bytes captured (4808 bits)
▶	Ethernet II, Src: PcsCompu_ba:c6:98 (08:00:27:ba:c6:98), Dst: SamsungE_bc:fd:8f (68:e7:c2:bc:fd:8f)
▶	Internet Protocol Version 4, Src: 192.168.43.244, Dst: 65.61.137.117
▶	Transmission Control Protocol, Src Port: 47660, Dst Port: 80, Seq: 1, Ack: 1, 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"

Parte 2: Acquisire e Visualizzare il Traffico HTTPS

Passaggio 1: Apertura di un Sito Web HTTPS

Nello **Screenshot**, viene aperta una pagina di login del sito NetAcad, che utilizza HTTPS. Questo protocollo garantisce che le comunicazioni tra il client e il server siano protette tramite crittografia, impedendo a malintenzionati di intercettare e leggere i dati sensibili.



Il lucchetto verde visibile accanto all'URL nel browser conferma che la connessione è crittografata, e tutti i dati trasmessi saranno protetti. Questo è un esempio chiave del passaggio da una connessione non sicura a una connessione sicura.

Passaggio 2: Cattura del Traffico HTTPS

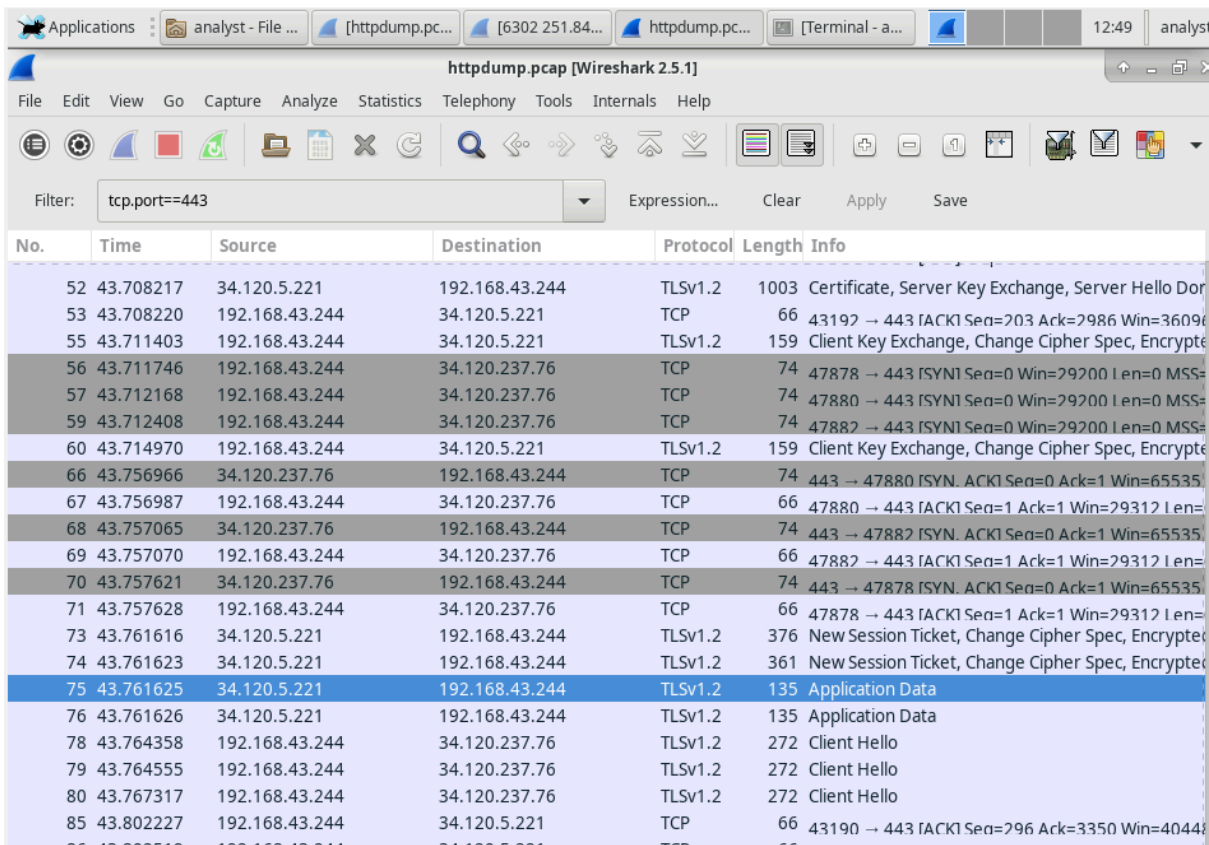
Nello **Screenshot**, il comando **tcpdump** viene utilizzato nuovamente per catturare il traffico HTTPS. In particolare, viene applicato un filtro per

monitorare solo il traffico sul porto **443**, che è il porto standard per le comunicazioni HTTPS. Il file risultante viene salvato in **httpdump.pcap**, pronto per essere analizzato.

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

Passaggio 3: Analisi del Traffico HTTPS in Wireshark

Nello **Screenshot**, Wireshark mostra il traffico **HTTPS** catturato. A differenza di HTTP, il contenuto del pacchetto è crittografato. Nello **Screenshot 10**, vediamo un pacchetto TLS con il protocollo **TLSv1.2** in azione. Il payload del pacchetto non è leggibile, indicando che la comunicazione è protetta da crittografia.



Passaggio 4: Differenze tra HTTP e HTTPS

Lo **Screenshot**, mostra ulteriori dettagli di un pacchetto TLS. Sebbene il pacchetto trasporti dati crittografati, non è possibile vedere il contenuto reale della comunicazione, proteggendo le informazioni sensibili come credenziali di accesso e altre transazioni. Questo rappresenta il vantaggio principale di HTTPS rispetto a HTTP.

