

Laboratorio - Utilizzo di Wireshark per Esaminare il Traffico HTTP e HTTPS

In questo laboratorio, completa i seguenti obiettivi:

- Catturare e visualizzare il traffico HTTP
- Catturare e visualizzare il traffico HTTPS

Link relativo alla guida:

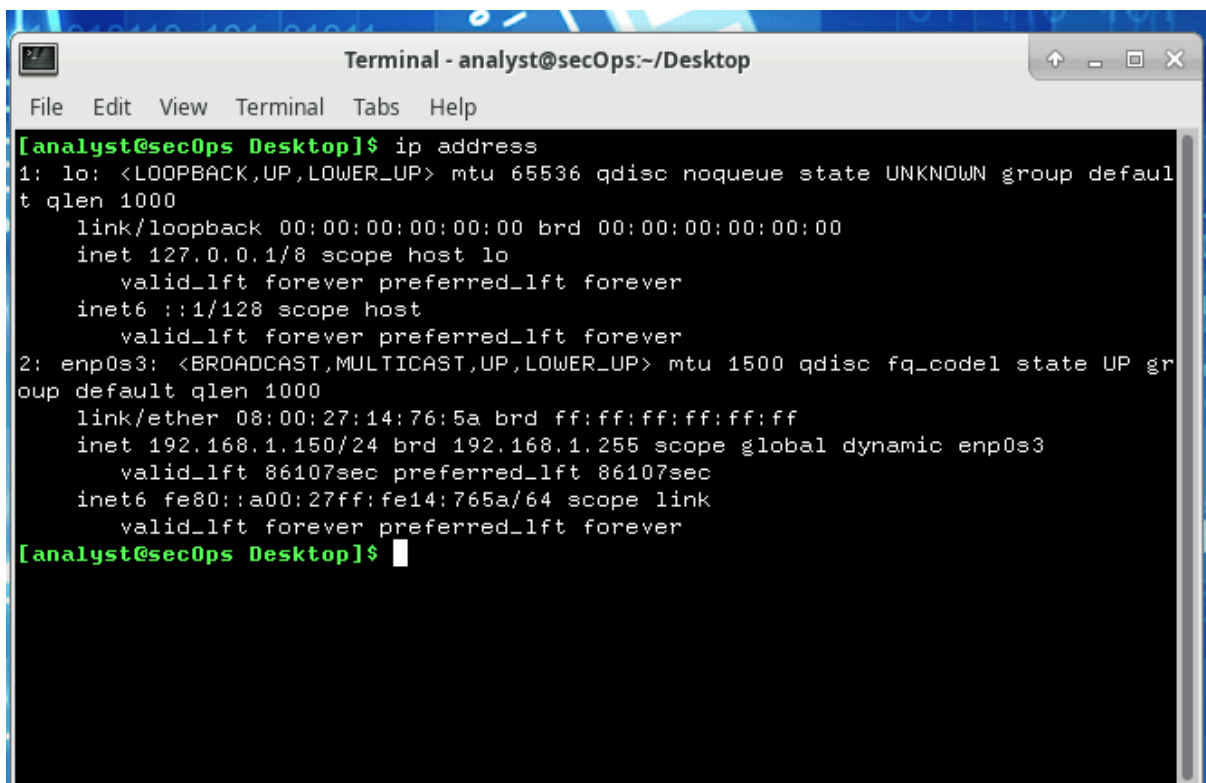
<https://itexamanswers.net/10-6-7-lab-using-wireshark-to-examine-http-and-https-traffic-answers.html>

Parte 1: Cattura e visualizza il traffico HTTP

In questa parte, utilizzerai tcpdump per catturare il contenuto del traffico HTTP. Utilizzerai le opzioni dei comandi per salvare il traffico in un file di cattura pacchetti (pcap). Questi record possono poi essere analizzati utilizzando diverse applicazioni che leggono i file pcap, tra cui Wireshark.

Passaggio 2: Apri un terminale e avvia tcpdump.

a. Apri un terminale e inserisci il comando `ip address`.



```
Terminal - analyst@secOps:~/Desktop
File Edit View Terminal Tabs Help
[analyst@secOps Desktop]$ 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 08:00:27:14:76:5a brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.150/24 brd 192.168.1.255 scope global dynamic enp0s3
        valid_lft 86107sec preferred_lft 86107sec
    inet6 fe80::a00:27ff:fe14:765a/64 scope link
        valid_lft forever preferred_lft forever
[analyst@secOps Desktop]$
```

Elenca le interfacce e i loro indirizzi IP visualizzati nell'output del comando `ip address`.

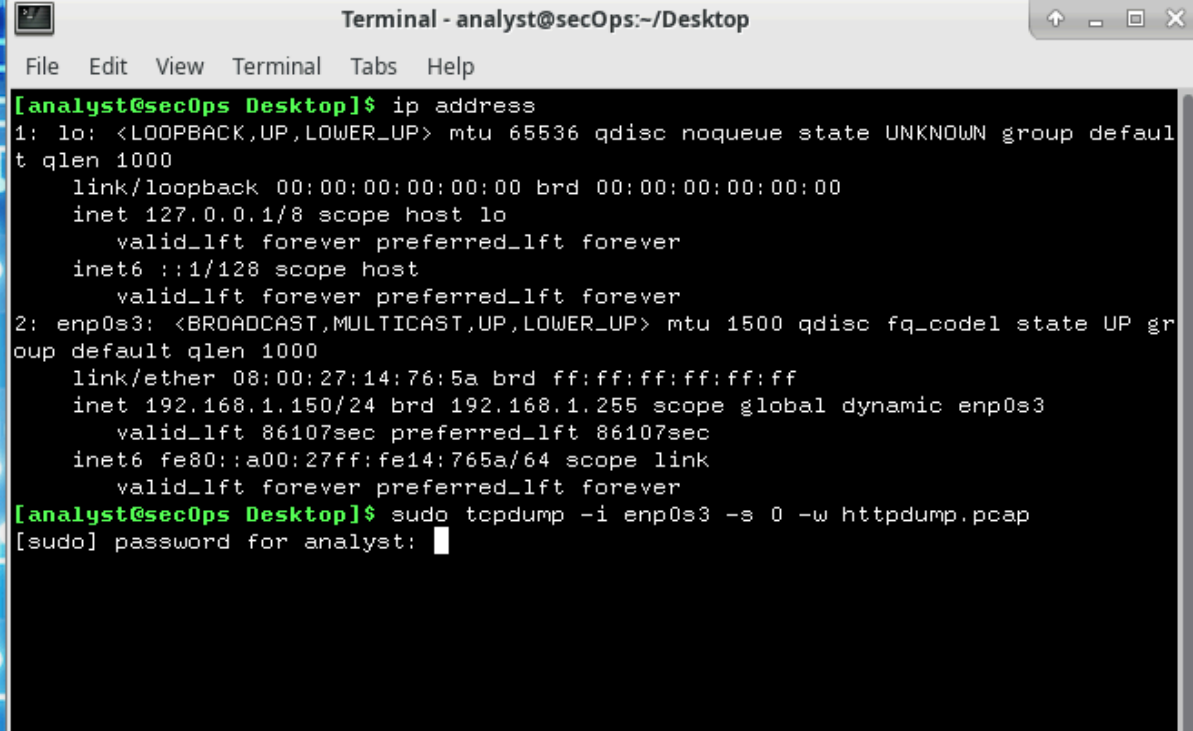
Le interfacce e i loro indirizzi IP visualizzati sono:

- **enp0s3** con indirizzo IP 192.168.1.150
- **lo** con indirizzo IP 127.0.0.1

Nel terminale, inserisci il comando:

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

Quando richiesto, inserisci la password `cyberops` per l'utente **analyst**.



```
Terminal - analyst@secOps:~/Desktop
File Edit View Terminal Tabs Help
[analyst@secOps Desktop]$ 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 08:00:27:14:76:5a brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.150/24 brd 192.168.1.255 scope global dynamic enp0s3
        valid_lft 86107sec preferred_lft 86107sec
    inet6 fe80::a00:27ff:fe14:765a/64 scope link
        valid_lft forever preferred_lft forever
[analyst@secOps Desktop]$ sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap
[sudo] password for analyst: 
```

Questo comando avvia tcpdump e registra il traffico di rete sull'interfaccia **enp0s3**.

L'opzione di comando **-i** permette di specificare l'interfaccia. Se non viene specificata, tcpdump catturerà tutto il traffico su tutte le interfacce.

L'opzione di comando **-s** specifica la lunghezza del campione per ogni pacchetto. È consigliabile limitare il valore di **snaplen** al numero più piccolo che catturerà le informazioni relative al protocollo di interesse. Impostando **snaplen** su 0, si imposta al valore predefinito di 262144, per garantire la compatibilità con le versioni più recenti e quelle più vecchie di tcpdump.

L'opzione di comando **-w** viene utilizzata per scrivere il risultato del comando tcpdump in un file. Aggiungere l'estensione **.pcap** assicura che i sistemi operativi e le applicazioni possano leggere il file. Tutto il traffico registrato verrà salvato nel file **httdump.pcap** nella directory home dell'utente **analyst**.

d. Apri un browser web dalla barra di avvio all'interno della CyberOps Workstation VM. Naviga su <http://www.altoromutual.com/login.jsp>.

Poiché questo sito web utilizza HTTP, il traffico non è criptato. Clicca sul campo della password per vedere il messaggio di avviso.

e. Inserisci come nome utente **Admin** e come password **Admin**, quindi clicca su **Login**.

f. Chiudi il browser web.

g. Torna alla finestra del terminale in cui tcpdump è in esecuzione. Inserisci **CTRL+C** per fermare la cattura dei pacchetti.

PERSONAL

Online Banking Login

Username:

Password:

This connection is not secure.
Logins entered here could be compromised. [Learn More](#)

Hello Admin User

Welcome to Altoro Mutual Online.

View Account Details:

800000 Corporate ▾

GO

Congratulations!

You have been pre-approved for an Altoro Gold Visa with a credit limit of \$10000!

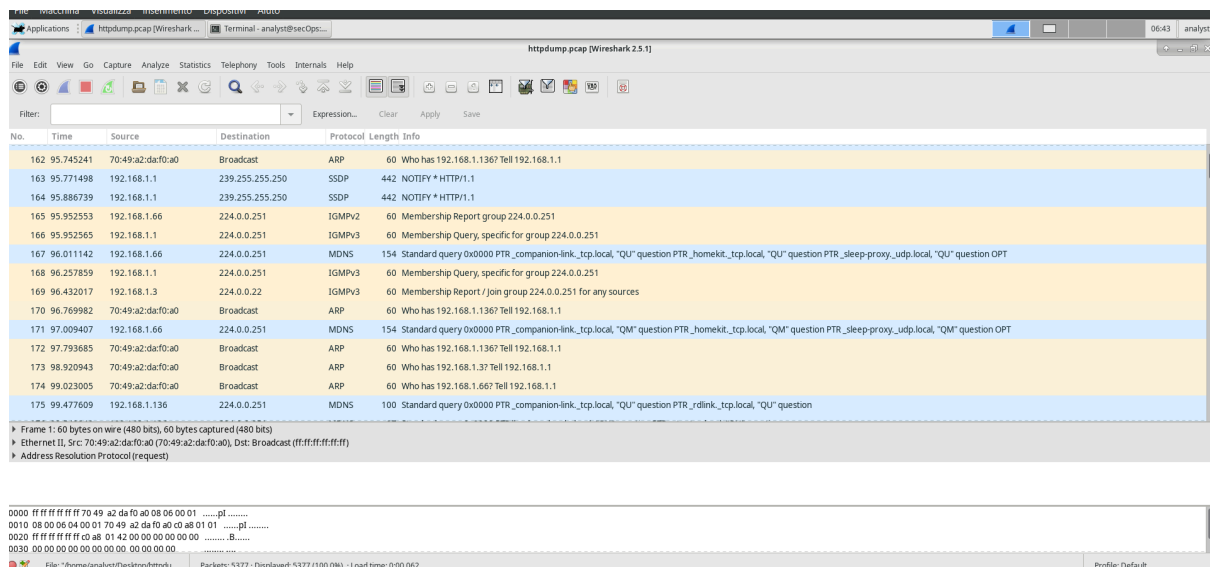
Click [Here](#) to apply.

```
validating forever preferred... forever
[analyst@secOps Desktop]$ sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap
[sudo] password for analyst:
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 b
ytes
^C5377 packets captured
5377 packets received by filter
0 packets dropped by kernel
[analyst@secOps Desktop]$
```

Passaggio 3: Visualizza la cattura HTTP.

Il comando tcpdump eseguito nel passaggio precedente ha salvato l'output in un file chiamato **httpdump.pcap**. Questo file si trova nella directory home dell'utente **analyst**.

a. Clicca sull'icona **File Manager** sulla scrivania e naviga nella cartella home dell'utente **analyst**. Fai doppio clic sul file **httpdump.pcap**, nella finestra di dialogo **Open With** scorri verso il basso e seleziona **Wireshark**, quindi clicca su **Open**.



Nell'applicazione Wireshark, filtra per **http** e clicca su **Apply**.

Filter:	http	▼	Expression...	Clear	Apply	Save
No.	Time	Source	Destination	Protocol	Length	Info
300	171.607773	192.168.1.150	34.107.221.82	HTTP	354	GET /success.txt HTTP/1.1
302	171.634650	34.107.221.82	192.168.1.150	HTTP	282	HTTP/1.1 200 OK (text/plain)
307	172.887997	192.168.1.150	34.107.221.82	HTTP	354	GET /success.txt HTTP/1.1
308	172.913664	34.107.221.82	192.168.1.150	HTTP	282	HTTP/1.1 200 OK (text/plain)
364	173.623735	192.168.1.150	95.100.181.26	OCSP	497	Request
367	173.625151	192.168.1.150	95.100.181.26	OCSP	497	Request
370	173.649652	95.100.181.26	192.168.1.150	OCSP	956	Response
373	173.653713	95.100.181.26	192.168.1.150	OCSP	956	Response
497	174.568496	192.168.1.150	95.100.181.26	OCSP	497	Request
498	174.568783	192.168.1.150	95.100.181.26	OCSP	497	Request
504	174.595737	95.100.181.26	192.168.1.150	OCSP	956	Response
507	174.598189	95.100.181.26	192.168.1.150	OCSP	956	Response
520	174.715937	192.168.1.150	95.100.181.26	OCSP	497	Request
531	174.742606	95.100.181.26	192.168.1.150	OCSP	956	Response
612	174.796641	192.168.1.150	142.250.180.163	OCSP	493	Request
614	174.927896	142.250.180.163	192.168.1.150	OCSP	767	Response
740	176.404732	192.168.1.150	65.61.137.117	HTTP	395	GET /login.jsp HTTP/1.1
833	176.558599	65.61.137.117	192.168.1.150	HTTP	8871	HTTP/1.1 200 OK (text/html)
851	176.694408	192.168.1.150	142.250.180.131	OCSP	493	Request
853	176.832753	142.250.180.131	192.168.1.150	OCSP	767	Response
3041	178.049002	192.168.1.150	65.61.137.117	HTTP	421	GET /style.css HTTP/1.1

Sfoglia i vari messaggi HTTP e seleziona il messaggio **POST**

4356	199.949793	23.40.158.218	192.168.1.150	OCSP	940	Response
4748	275.278734	192.168.1.150	65.61.137.117	HTTP	601	POST /doLogin HTTP/1.1 (application/x-www-form-urlencoded)
4753	275.436127	65.61.137.117	192.168.1.150	HTTP	327	HTTP/1.1 302 Found

Nel pannello inferiore, il messaggio viene visualizzato. Espandi la sezione **HTML Form URL Encoded: application/x-www-form-urlencoded**

▶ Hypertext Transfer Protocol
▼ HTML Form URL Encoded: application/x-www-form-urlencoded
▶ Form item: "uid" = "Admin"
▶ Form item: "passw" = "Admin"
▶ Form item: "btnSubmit" = "Login"

Il uid di Admin e la passw di Admin sono visualizzati all'interno della sezione espansa **HTML Form URL Encoded: application/x-www-form-urlencoded**.

Parte 2: Cattura e visualizza il traffico HTTPS

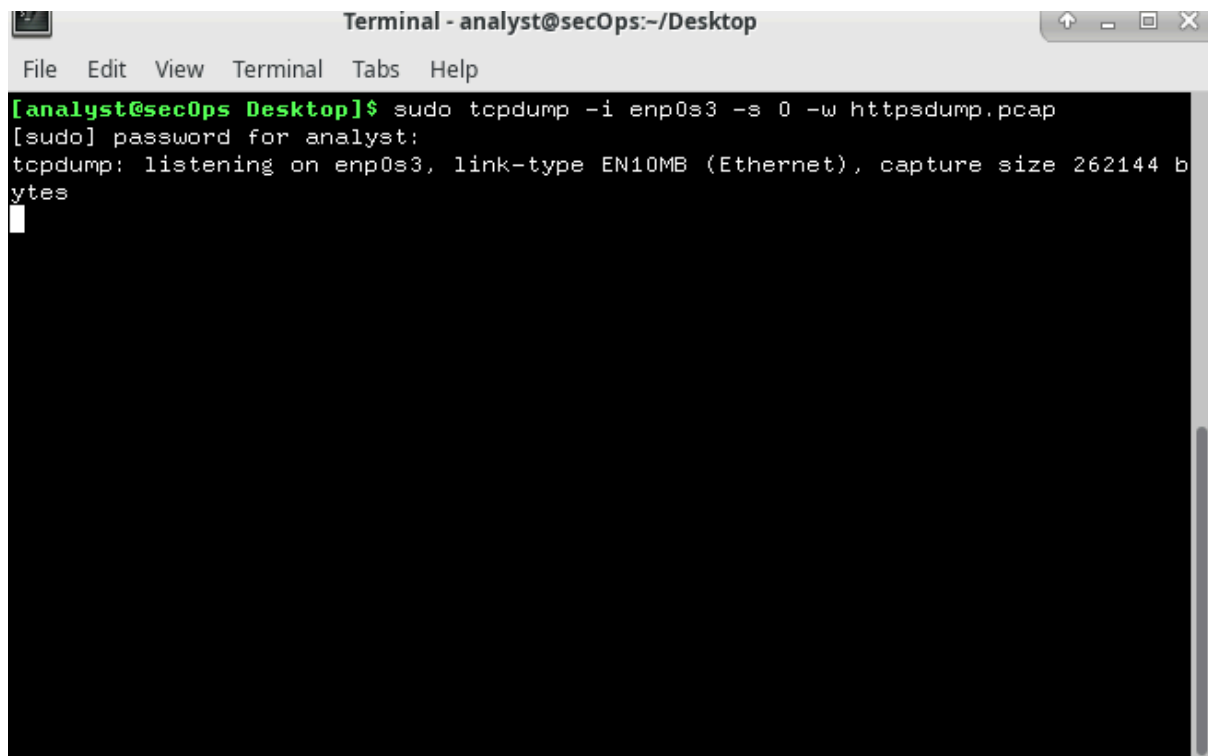
Ora utilizzerai tcpdump dalla linea di comando di una workstation Linux per catturare il traffico HTTPS. Dopo aver avviato tcpdump, genererai traffico HTTPS mentre tcpdump registra il contenuto del traffico di rete. Questi record saranno poi analizzati utilizzando Wireshark.

Passaggio 1: Avvia tcpdump all'interno di un terminale.

a. Mentre sei nell'applicazione terminale, inserisci il comando:

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

Quando richiesto, inserisci la password **cyberops** per l'utente **analyst**.



```
Terminal - analyst@secOps:~/Desktop
File Edit View Terminal Tabs Help
[analyst@secOps Desktop]$ 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
█
```

Questo comando avvierà tcpdump e registrerà il traffico di rete sull'interfaccia **enp0s3** della workstation Linux. Se la tua interfaccia è diversa da **enp0s3**, assicurati di modificarla nel comando sopra.

Tutto il traffico registrato sarà salvato nel file **httpsdump.pcap** nella directory home dell'utente **analyst**.

b. Apri un browser web dalla barra di avvio all'interno della CyberOps Workstation VM. Naviga su www.netacad.com.

Nota: Se ricevi una pagina “**Secure Connection Failed**”, probabilmente significa che la data e l'ora sono errate. Aggiorna il giorno e l'ora con il seguente comando, modificando con il giorno e l'ora correnti:

```
sudo date MMDDhhmm[[CC]YY][.ss]
```

Cosa noti riguardo l'URL del sito web?

Il sito web sta utilizzando HTTPS e c'è un lucchetto, il che indica che la connessione è sicura e crittografata.

Passaggio 2: Visualizza la cattura HTTPS.

Il comando tcpdump eseguito nel Passaggio 1 ha salvato l'output in un file chiamato **httpsdump.pcap**. Questo file si trova nella directory home dell'utente **analyst**.

a. Clicca sull'icona **Filesystem** sulla scrivania e naviga nella cartella home dell'utente **analyst**. Apri il file **httpsdump.pcap**.

Nell'applicazione Wireshark, espandi la finestra di cattura verticalmente e poi filtra il traffico HTTPS tramite la porta 443.

Inserisci il filtro `tcp.port==443` e clicca su Apply.

Filter:	tcp.port == 443			Expression...	Clear	Apply	Save
No.	Time	Source	Destination	Protocol	Length	Info	
35	11.914290	192.168.1.150	104.18.32.137	TLSv1.2	112	Application Data	
36	11.940494	104.18.32.137	192.168.1.150	TCP	66	443 → 35390 [ACK] Seq=1 Ack=47 Win=10 Len=0 TSval=757221353 TSecr=1641852797	
37	11.940511	104.18.32.137	192.168.1.150	TLSv1.2	112	Application Data	
38	11.940519	192.168.1.150	104.18.32.137	TCP	66	35390 → 443 [ACK] Seq=47 Ack=47 Win=325 Len=0 TSval=1641852823 TSecr=757221353	
41	12.915486	192.168.1.150	104.18.32.137	TLSv1.2	112	Application Data	
42	12.915943	192.168.1.150	104.85.9.21	TLSv1.2	112	Application Data	
43	12.916142	192.168.1.150	13.226.175.91	TLSv1.2	112	Application Data	
44	12.942654	13.226.175.91	192.168.1.150	TCP	66	443 → 40528 [ACK] Seq=1 Ack=47 Win=137 Len=0 TSval=561712394 TSecr=1348668535	
45	12.942672	13.226.175.91	192.168.1.150	TLSv1.2	112	Application Data	
46	12.942679	192.168.1.150	13.226.175.91	TCP	66	40528 → 443 [ACK] Seq=47 Ack=47 Win=1222 Len=0 TSval=1348668562 TSecr=561712394	
47	12.945143	104.18.32.137	192.168.1.150	TLSv1.2	112	Application Data	

Sfoglia i vari messaggi HTTPS e seleziona un messaggio Application Data.

Nel pannello inferiore, che messaggio viene visualizzato.

Ciò che ha sostituito la sezione HTTP presente nel file di cattura precedente è la sezione Secure Sockets Layer (SSL/TLS 1.2), che appare dopo la sezione TCP, invece della sezione HTTP.

▼ 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: 00000000000000061596a6438c808dbeab13d1c3a518ed59...

Clicca su **Encrypted Application Data**.

I dati dell'applicazione sono in formato **plaintext** o leggibili?

I dati dell'applicazione sono in formato cifrato e non possono essere visualizzati, poiché il payload dei dati è criptato utilizzando **TLSv1.2**.

Quali sono i vantaggi dell'utilizzo di HTTPS invece di HTTP?

Quando si utilizza HTTPS, il payload dei dati di un messaggio è criptato e può essere visualizzato solo dai dispositivi che fanno parte della conversazione crittografata.

Tutti i siti web che utilizzano HTTPS sono considerati affidabili?

No, perché siti web dannosi possono utilizzare HTTPS per sembrare legittimi pur continuando a catturare i dati degli utenti e le credenziali di accesso.