Wireshark per esaminare il traffico HTTP e HTTPS.

1. **Configurazione di Wireshark**:

- **Obiettivo**: Raccogliere pacchetti di rete per analizzare il traffico HTTP e HTTPS.
- **Passaggi**:
  - Apri Wireshark e seleziona l'interfaccia di rete attiva (solitamente Wi-Fi o Ethernet).
  - Avvia la cattura cliccando sull'icona dello "squalo" verde in alto.
  - Naviga su alcuni siti Web HTTP e HTTPS per generare traffico.

Nota: Per visualizzare solo i pacchetti HTTP e HTTPS puoi impostare i filtri che descriviamo nei prossimi passaggi.

2. **Cattura e Analisi del Traffico HTTP**:

- **Obiettivo**: Osservare i dettagli del traffico HTTP, che viaggia in chiaro senza crittografia.
- **Passaggi**:
  - Inserisci il filtro http nella barra di ricerca di Wireshark per isolare i pacchetti HTTP.
  - Visita un sito web HTTP (ad esempio http://example.com) per generare il traffico.
  - Esamina i pacchetti catturati osservando le richieste e risposte HTTP. Ad esempio:
    - **Richiesta HTTP**:
      - Campo GET /index.html HTTP/1.1: identifica il tipo di richiesta e la risorsa richiesta.
      - Campo Host: example.com: indica il dominio richiesto.
    - **Risposta HTTP**:
      - Campo HTTP/1.1 200 OK: mostra lo stato della risposta (200 indica successo).
      - Campo Content-Type: text/html: descrive il tipo di contenuto.
  - **Analisi**: Dato che il traffico HTTP è in chiaro, noterai che i dati della richiesta e della risposta possono essere letti facilmente, come l'URL richiesto, le intestazioni, e i parametri di ricerca.

Tabella Esempio di una Richiesta HTTP:

Campo	Valore
Metodo	GET
URI	/index.html
Versione	HTTP/1.1
Host	example.com
Content-Type	text/html

3. **Cattura e Analisi del Traffico HTTPS**:

- **Obiettivo**: Comprendere il processo di handshake e l'invio di dati criptati nel protocollo HTTPS.
- **Passaggi**:
  - Inserisci il filtro tls o ssl nella barra di ricerca per visualizzare solo i pacchetti HTTPS.
  - Visita un sito web HTTPS (ad esempio https://example.com).
  - Esamina i pacchetti TLS, in particolare quelli legati all'handshake iniziale:
    - **ClientHello**: il client invia una lista di protocolli di crittografia supportati.
    - **ServerHello**: il server risponde scegliendo un protocollo crittografico condiviso.
    - **Certificate**: il server invia il proprio certificato per l'autenticazione.
    - **Key Exchange**: viene scambiata la chiave di crittografia per la sessione.
  - **Analisi**: Noterai che, a differenza di HTTP, il traffico HTTPS è criptato, quindi i dati effettivi della richiesta e risposta non sono leggibili.

Esempio di Pacchetti HTTPS:

Tipo di Pacchetto	Descrizione
ClientHello	Invia una lista di protocolli crittografici
ServerHello	Sceglie un protocollo crittografico
Certificate	Invia il certificato SSL del server
Key Exchange	Scambio della chiave di sessione

4. **Confronto Traffico HTTP e HTTPS**:

- Utilizzando Wireshark, puoi creare un **grafico temporale**per visualizzare il numero di pacchetti HTTP e HTTPS catturati nel tempo. Per farlo:
  - Vai su **Statistics > I/O Graphs**.
  - Aggiungi filtri per HTTP (http) e HTTPS (tls), visualizzandoli in colori diversi per un confronto diretto.
- Questo grafico mostrerà la frequenza e la distribuzione dei pacchetti HTTP e HTTPS, utile per identificare in modo visivo il tipo di traffico predominante.

5. **Esempio Pratico**:

- Immagina di voler accedere a http://testsite.com/login?user=test&password=1234 (un esempio non sicuro con HTTP).
- Su Wireshark, vedrai questi parametri visibili nel pacchetto HTTP. Con HTTPS, invece, tali dettagli sarebbero nascosti, essendo cifrati, proteggendo le credenziali dell'utente