Differenze di traffico tra HTTP e HTTPS

1. **Visibilità del Contenuto dei Pacchetti:**
   - **HTTP**
     Tutti i dati sono inviati in chiaro. Ciò significa che puoi vedere tutto il contenuto della richiesta e della risposta, inclusi i dati delle intestazioni (headers) e il corpo del messaggio (body). Puoi vedere informazioni come URL, parametri GET, dati POST, cookie e contenuti delle pagine web.
   - **HTTPS**
     I dati sono crittografati utilizzando SSL/TLS. Pertanto, non puoi vedere il contenuto delle richieste e delle risposte. Quello che vedrai sono pacchetti crittografati che contengono dati illeggibili senza la chiave di decrittazione.

2. **Struttura del Traffico:**
   - **HTTP**
     Le comunicazioni avvengono direttamente tra client e server senza ulteriori passaggi. Puoi osservare facilmente l'handshake TCP seguito dall'invio e ricezione dei dati HTTP.
   - **HTTPS**
     Prima di inviare dati HTTP, avviene un handshake SSL/TLS. Questo handshake include scambi di chiavi e certificati per stabilire una connessione sicura. Vedrai pacchetti che rappresentano questo handshake iniziale, come il "ClientHello", "ServerHello", scambio di chiavi, e messaggi di "Finished" che indicano la fine dell'handshake.

3. **Intestazioni e Metadati:**
   - **HTTP**
     Le intestazioni HTTP sono visibili e possono includere informazioni sensibili come i cookie, l'user-agent, referrer, e altre informazioni di tracciamento.
   - **HTTPS**
     Le intestazioni HTTP sono crittografate e quindi non visibili. Tuttavia, le intestazioni del livello di trasporto (IP e TCP)

rimangono visibili, quindi puoi vedere gli indirizzi IP e le porte utilizzate, ma non il contenuto delle intestazioni HTTP.

4.**Performance:**

- **HTTP**
  Non c'è overhead di crittografia, quindi le richieste e risposte possono essere leggermente più veloci in termini di latenza, ma la mancanza di sicurezza è un rischio significativo.

- **HTTPS**
  L'overhead della crittografia può introdurre un piccolo ritardo aggiuntivo, soprattutto durante l'handshake SSL/TLS. Tuttavia, il beneficio di avere una comunicazione sicura giustifica questo overhead.

5. **Sicurezza:**

- **HTTP**
  Non offre nessuna protezione contro intercettazioni (sniffing) e attacchi man-in-the-middle. I dati in transito possono essere letti e modificati da chiunque intercetti il traffico.
- **HTTPS**
  Fornisce sicurezza tramite crittografia, autenticazione del server e integrità dei dati. Solo il client e il server possono decifrare i dati trasmessi, prevenendo intercettazioni e modifiche da parte di terzi.

Esempi Visivi con Wireshark:

- **HTTP**
  Puoi vedere direttamente le richieste GET/POST e le risposte con tutti i dati visibili in chiaro.
- **HTTPS**
  Vedrai pacchetti TLS con dati criptati. Il contenuto HTTP sarà protetto all'interno dei pacchetti TLS e non sarà leggibile direttamente.

In conclusione, la principale differenza tra il traffico HTTP e HTTPS è la crittografia che HTTPS introduce. Questo cambia drasticamente la visibilità e la sicurezza del traffico. Mentre HTTP ti permette di vedere

tutto il contenuto in chiaro, HTTPS nasconde queste informazioni proteggendole da potenziali intercettatori.