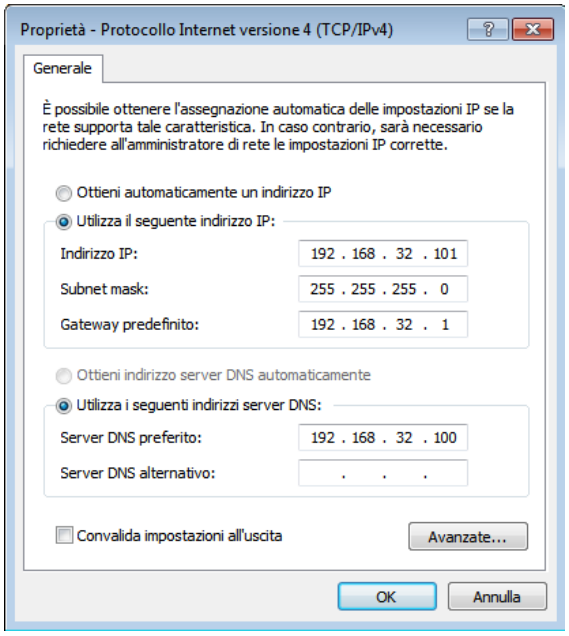
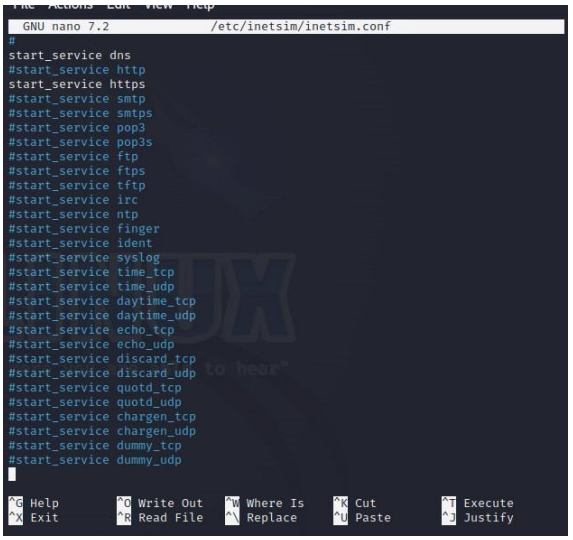
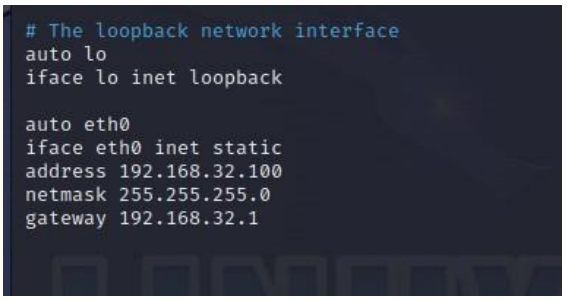
ESERCIZIO W4D4

Esecuzione:

1. Configurazione IP Kali Linux e Window:





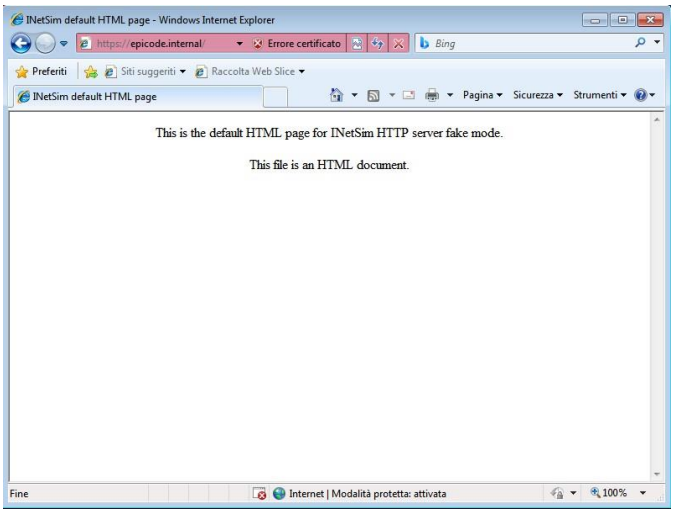


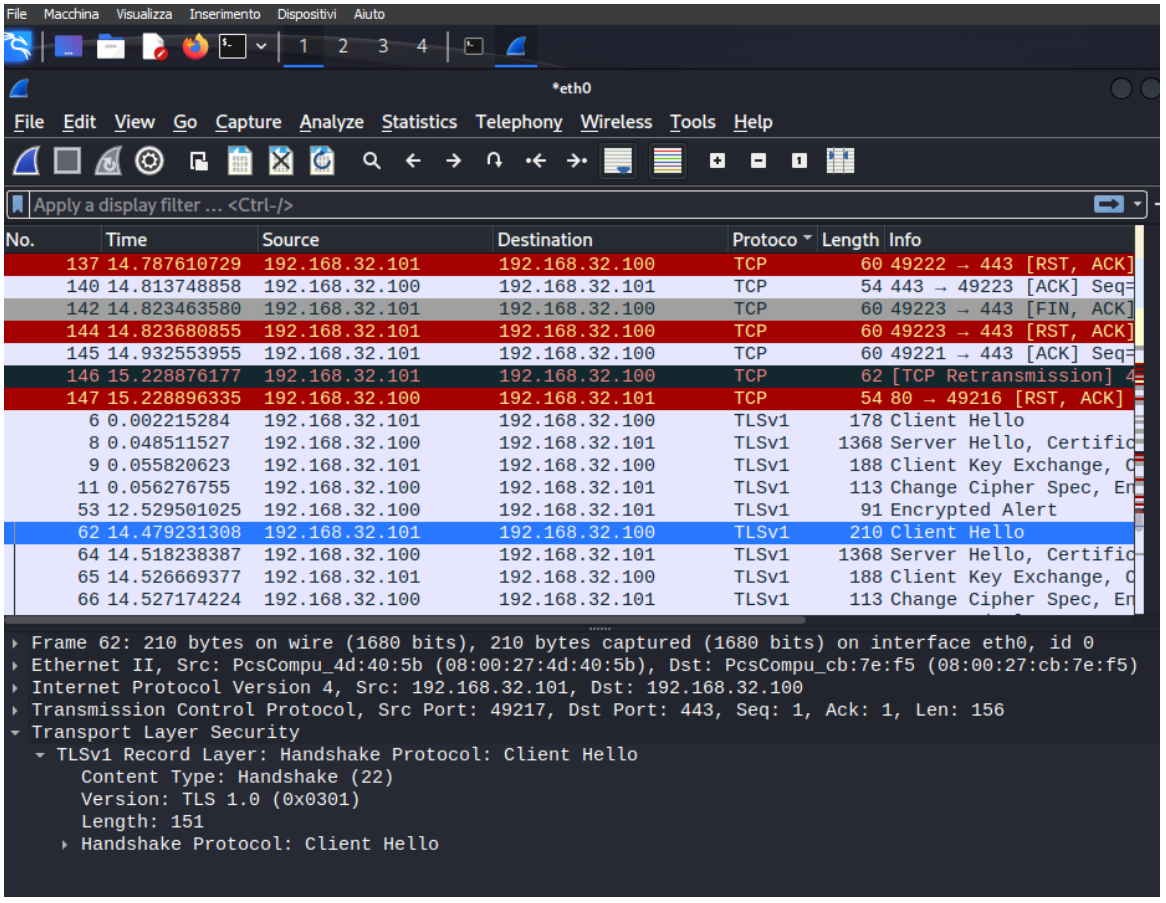
2. Fase 1: Comunicazione tramite HTTPS

Configurazione Iniziale:
Kali Linux e Windows 7 sono connessi nella stessa rete virtuale.

Richiesta HTTPS:
Il client Windows 7 richiede tramite web browser una risorsa all'hostname epicode.internal al server HTTPS di Kali Linux.

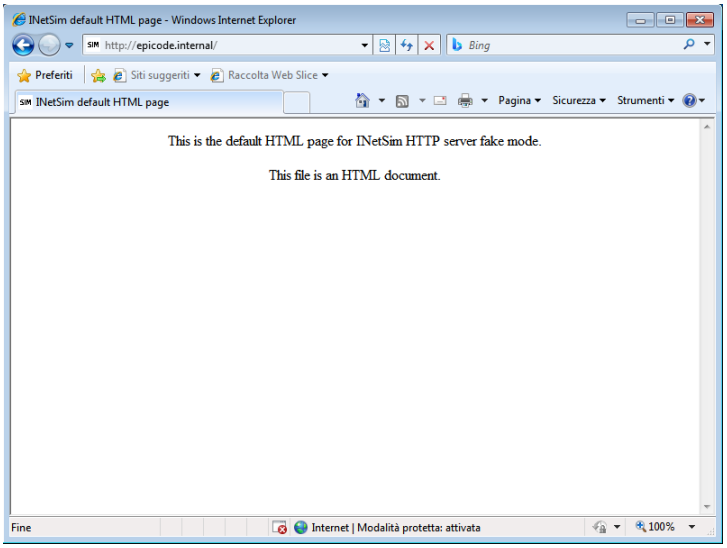
Utilizzando Wireshark, abbiamo intercettato la comunicazione.

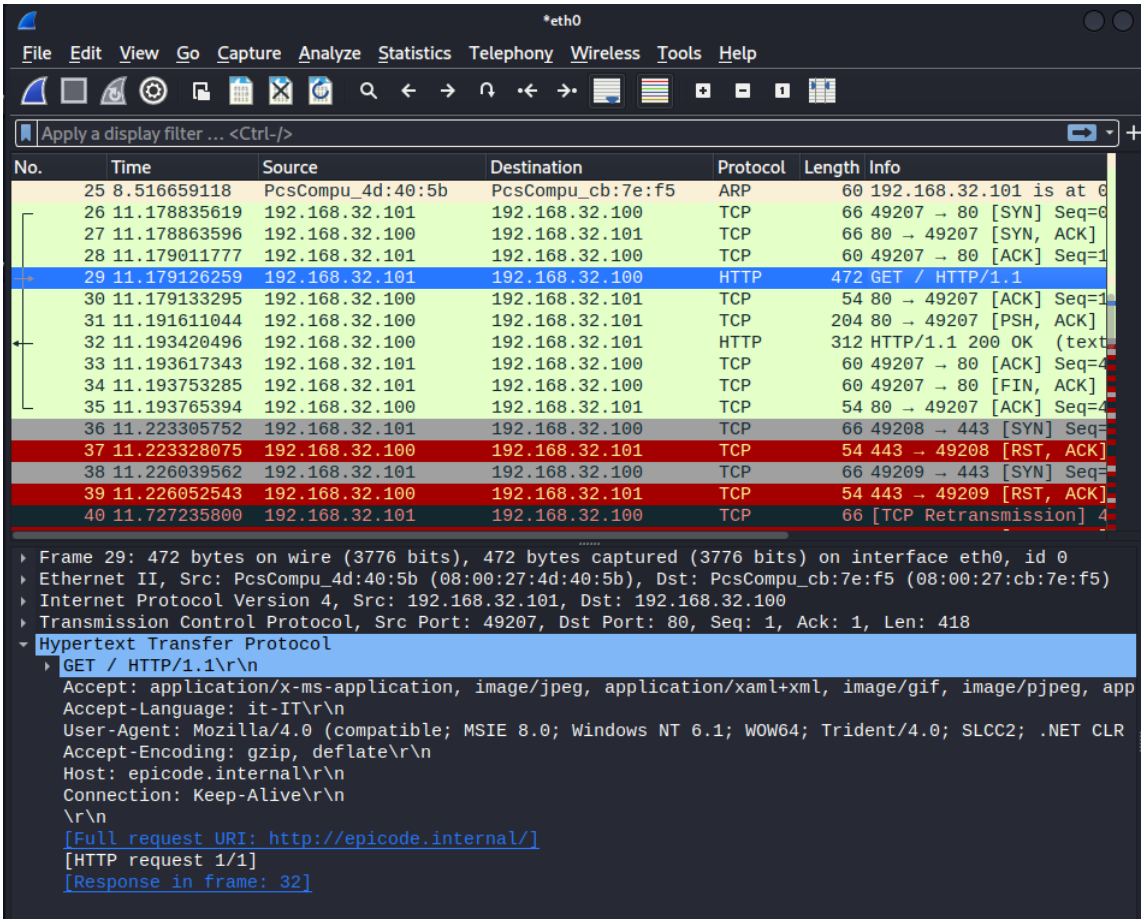




Fase 2: Comunicazione tramite HTTP

1. **Modifica del Server:**
   - Ho sostituito il server HTTPS con un server HTTP su Kali Linux.
2. **Richiesta HTTP:**
   - Il client (Windows 7) ha nuovamente emesso la richiesta tramite il web browser.
3. **Wireshark Capture (HTTP):**
   - La comunicazione è avvenuta nuovamente in maniera intercettabile.
   - Indirizzo MAC di origine: [MAC_Address_Client], Indirizzo MAC di destinazione: [MAC_Address_Server].
   - Contenuto della richiesta HTTP: [Contenuto_Richiesta_HTTP].





Configurazione dei Servizi DNS su Kali Linux:

- Ho impostato l'indirizzo IP predefinito del DNS su 192.168.32.100, in modo che Kali funga da server; l'indirizzo IP del DNS deve essere impostato con il proprio indirizzo IP.
- Il nome di dominio è "epcode.internal", come richiesto dall'esercizio.
- Nel file di configurazione del DNS, ho associato il nome di dominio all'indirizzo IP: epicode.internal.

1. **Analisi e Conclusioni**

- Quando si utilizza HTTPS, la richiesta viene crittografata, assicurando la sicurezza del contenuto, mentre con HTTP il contenuto è aperto e potenzialmente vulnerabile a intercettazioni.
- La distinzione chiave tra HTTPS e HTTP risiede nella sicurezza.
- Gli indirizzi MAC di sorgente e destinazione rimangono costanti durante tutte le fasi.
- La differenza principale tra HTTPS e HTTP non riguarda solo la sicurezza, ma HTTPS fornisce anche:
    - Verifica dell'identità e riservatezza dei dati.

- Crittografia del traffico.
- Controllo dell'integrità del traffico.