Report M1W4D5

Nell’esercizio di oggi metteremo insieme le competenze acquisite finora.
Lo studente verrà valutato sulla base della risoluzione al problema seguente.

Requisiti e servizi:

- Kali Linux IP 192.168.32.100
- Windows 7 IP 192.168.32.101
- HTTPS server: attivo
- Servizio DNS per risoluzione nomi di dominio: attivo

Traccia:

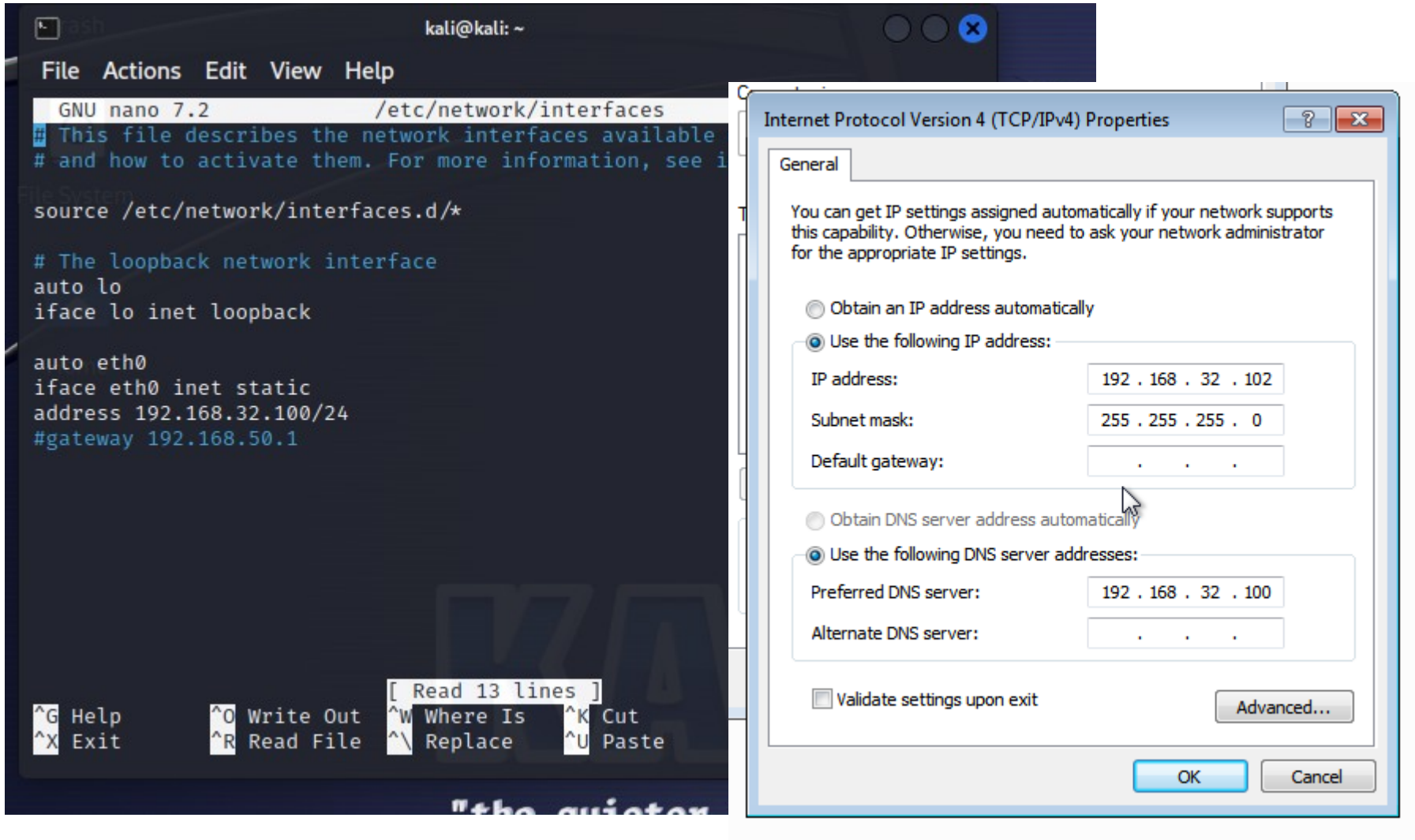
Simulare, in ambiente di laboratorio virtuale, un’architettura client server in cui un client con indirizzo 192.168.32.101 (Windows 7) richiede tramite web browser una risorsa all’hostname epicode.internal che risponde all’indirizzo 192.168.32.100 (Kali).

Si intercetti poi la comunicazione con Wireshark, evidenziando i MAC address di sorgente e destinazione ed il contenuto della richiesta HTTPS.

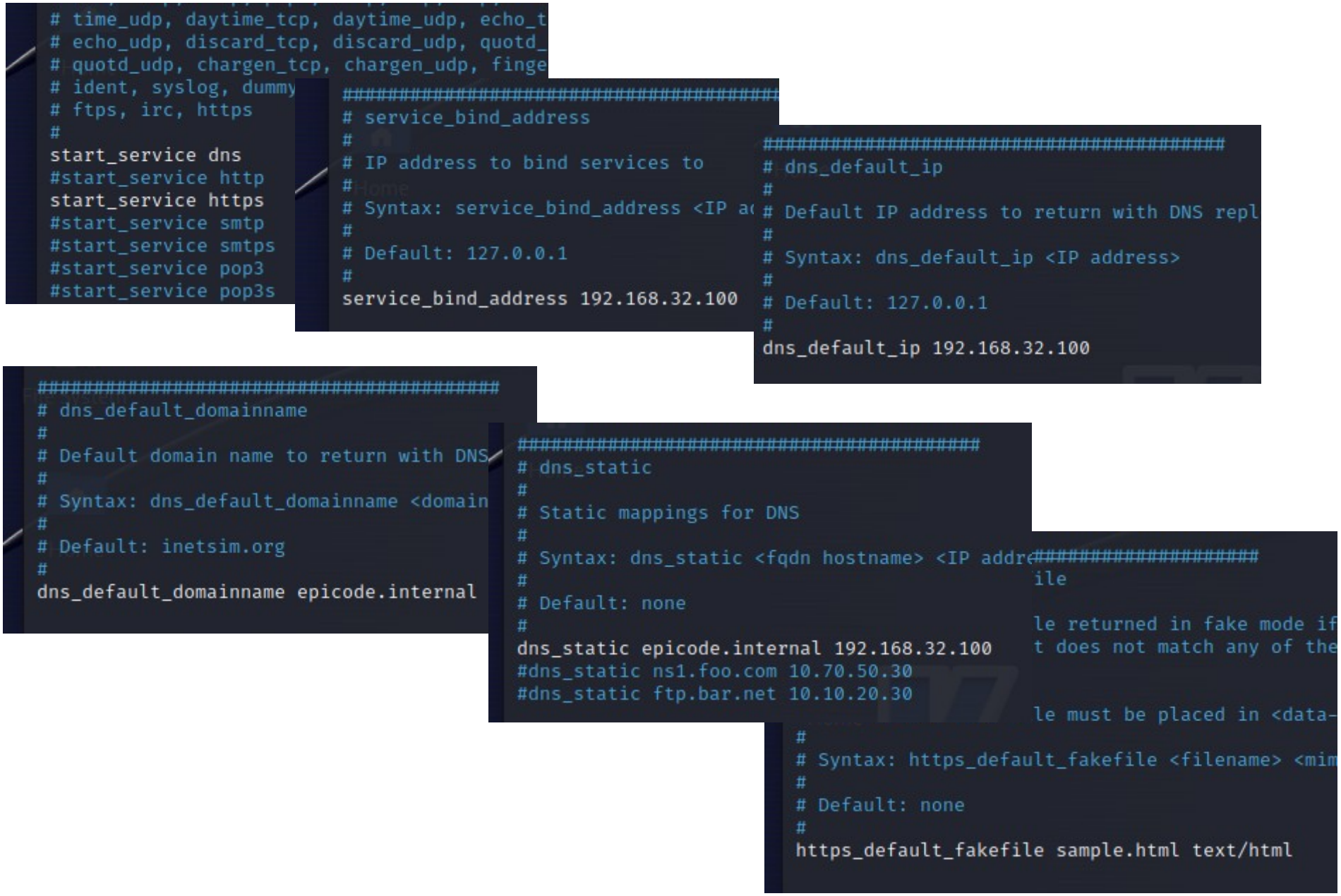
Ripetere l’esercizio, sostituendo il server HTTPS, con un server HTTP. Si intercetti nuovamente il traffico, evidenziando le eventuali differenze tra il traffico appena catturato in HTTP ed il traffico precedente in HTTPS. Spiegare, motivandole, le principali differenze se presenti.

- **CONFIGURAZIONI IP E INETSIM:**

Configuro le impostazioni di rete assegnando degli ip statici e facendo attenzione che l'indirizzo DNS di windows corrisponda all'indirizzo IP di kali per poter utilizzare il servizio di simulazione

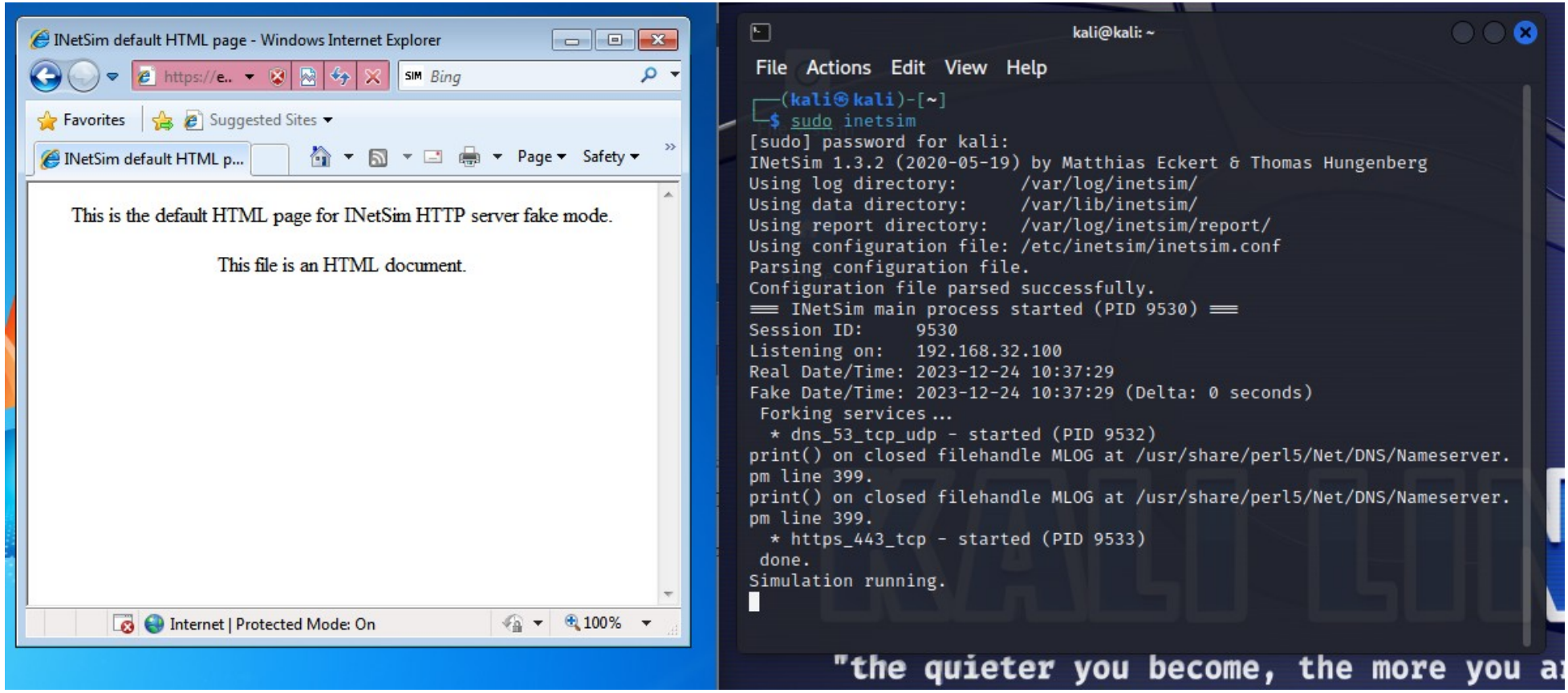


In questo caso devo configurare anche il servizio DNS di inetsim

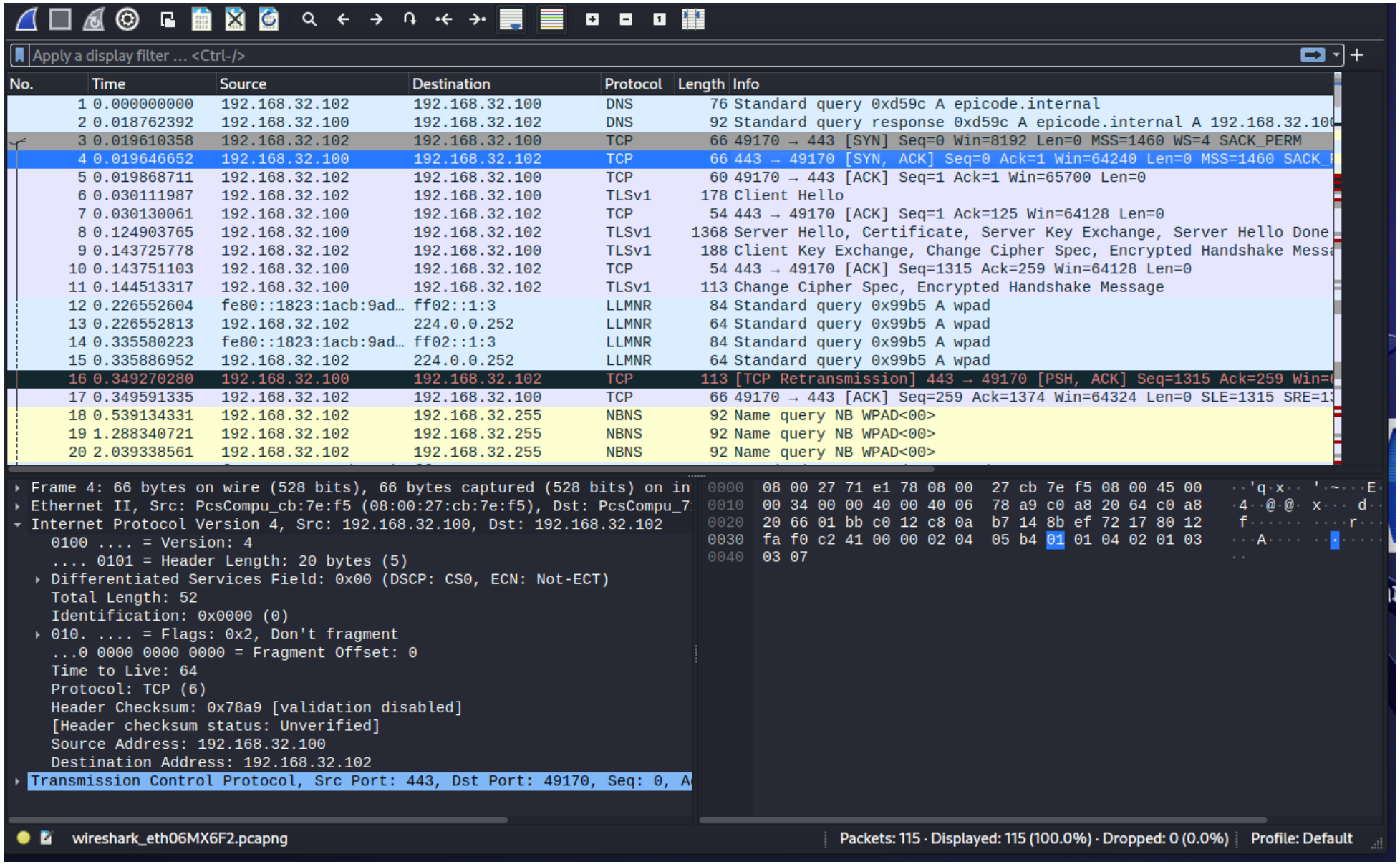


- **CATTURA PACCHETTI HTTPS CON WIRESHARK:**

Dopo aver avviato la simulazione Inetsim da terminale, apro wireshark su eth0 e carico la pagina https://epicode.internal su windows per catturarne i pacchetti

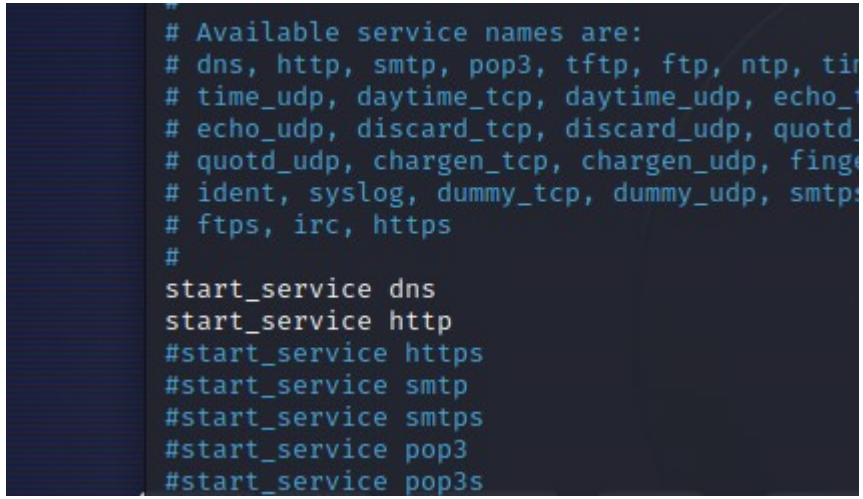


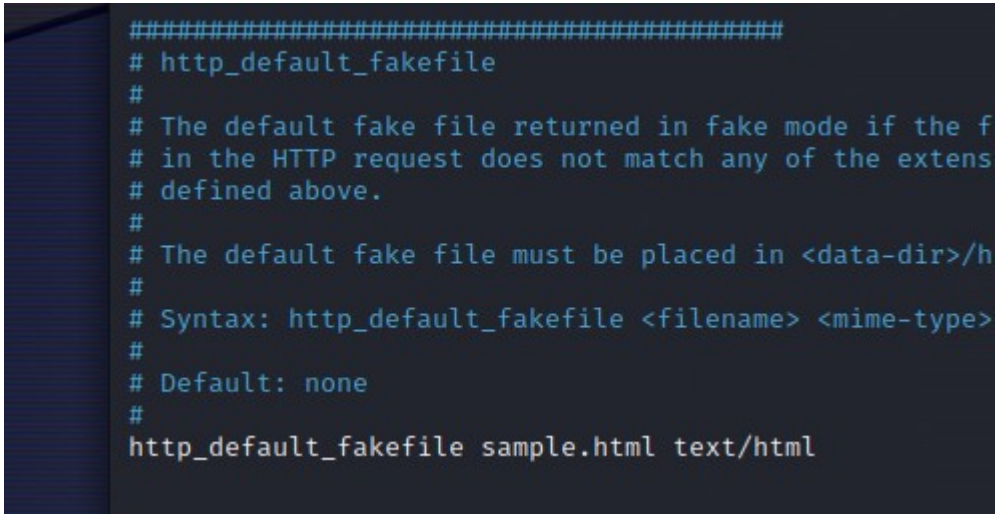
E quindi la cattura con wireshark:

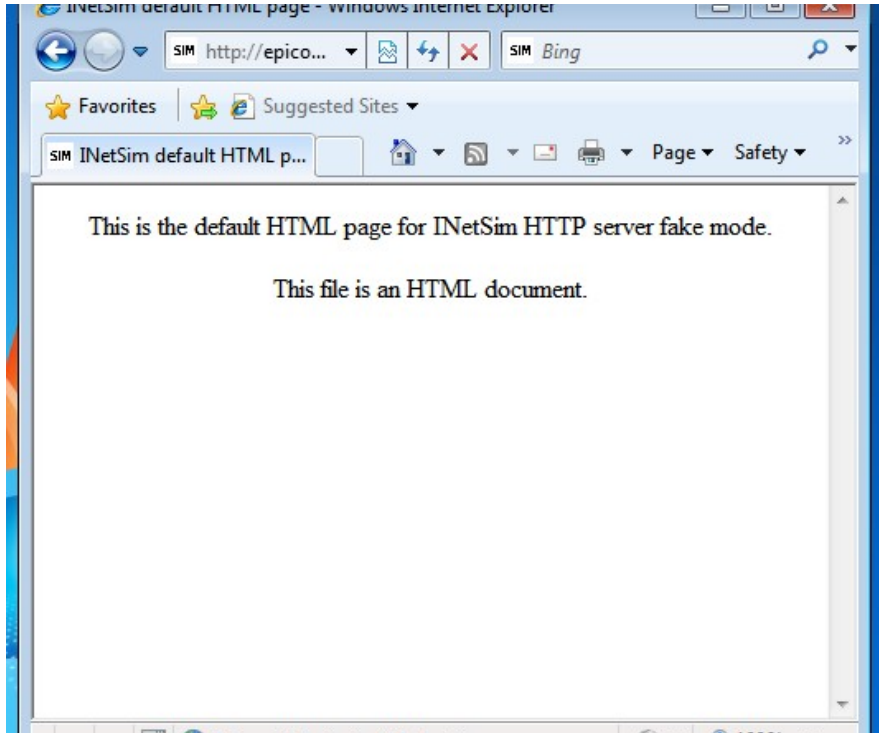


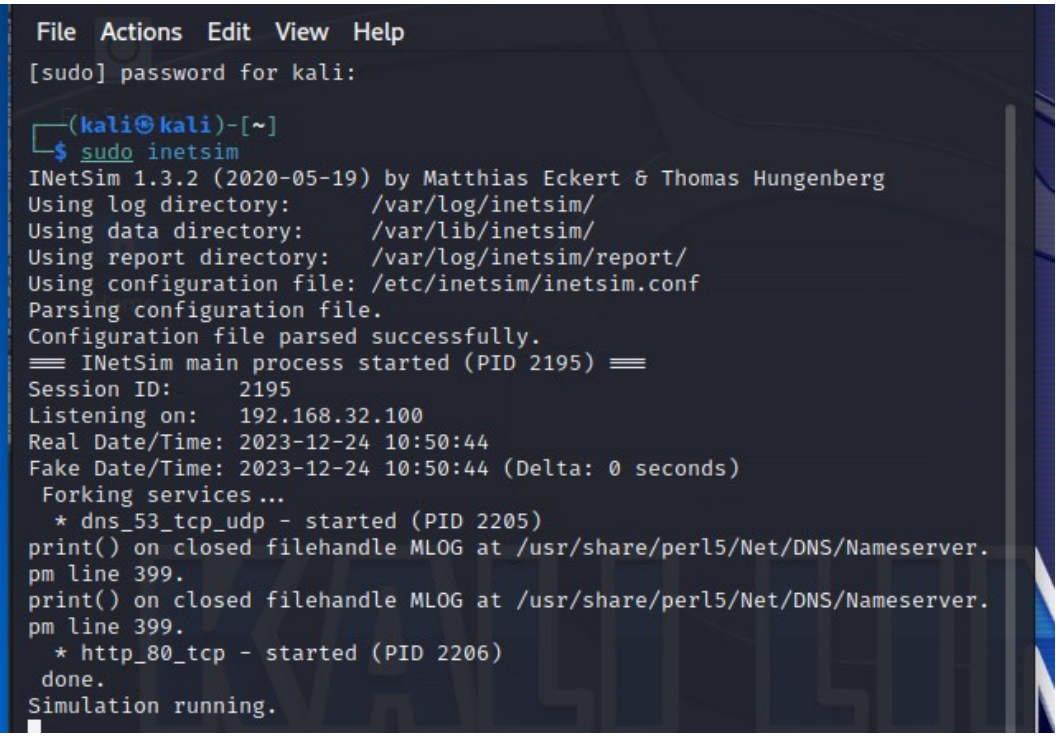
- **CATTURA PACCHETTI HTML CON WIRESHARK:**

Dopo aver modificato le impostazioni di simulazione ripeto il procedimento per l'indirizzo http://epicode.internal

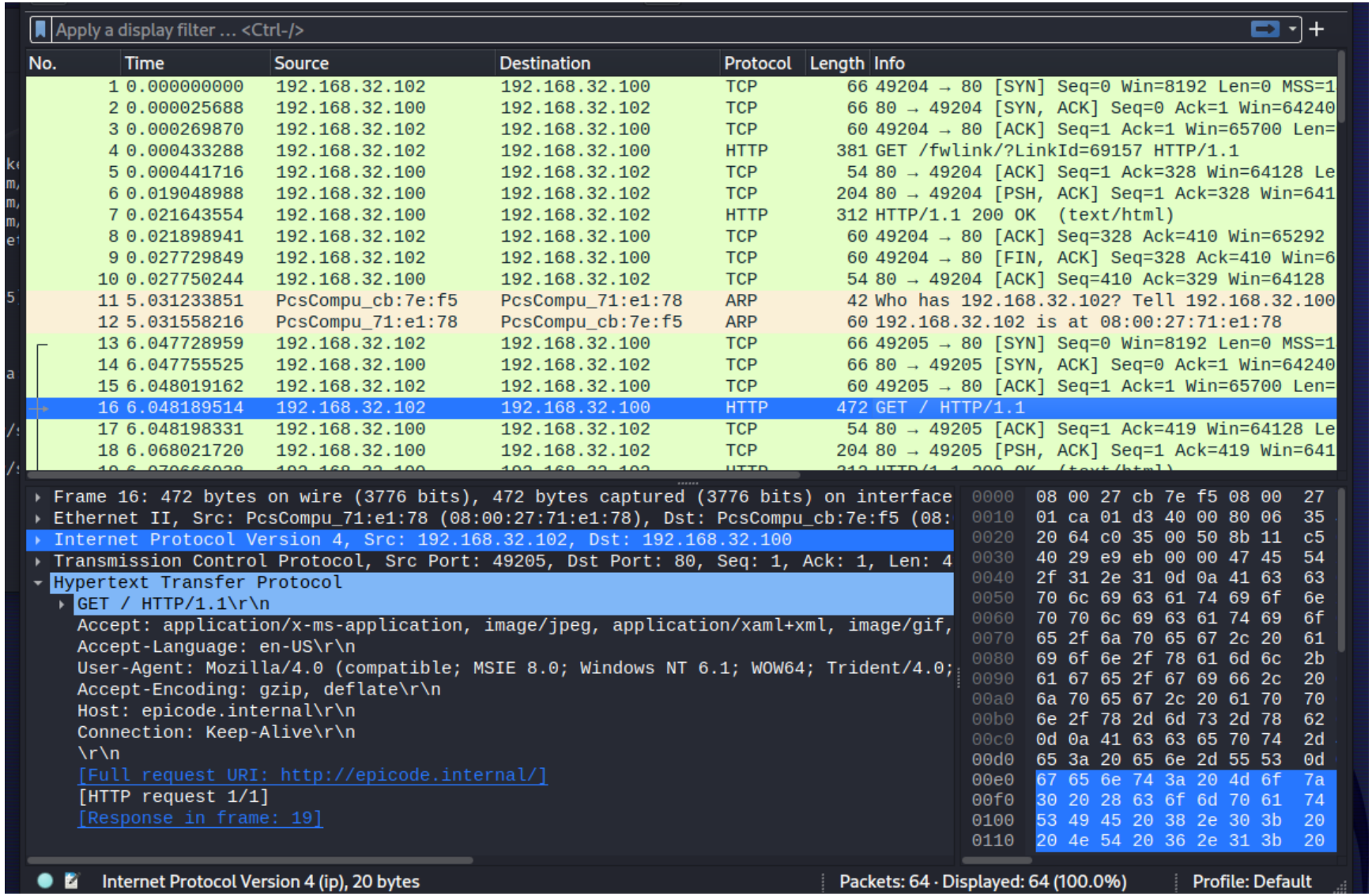








E quindi la cattura con wireshark:



- **CONCLUSIONI**:

Si possono notare grandi differenze:

- HTTPS:
  - sono evidenti i pacchetti cifrati con protocollo TLSv1
  - i pacchetti LLMNR e NBNS sono utilizzati per la risoluzione degli host-name
  - viene richiesto dal browser un certificato di sicurezza che il simulatore non è in grado di fornire
- HTTP:
  - i pacchetti del protocollo HTTP non essendo cifrati mostrano in chiaro l’indirizzo richiesto