**Configurazione DNS HTTPS ed wireshark**

**1)Cambiare indirizzo ip su kali**

Entro nel panello di comandi digito sudo nano /etc/network/interfaces.d/\*

Digito la password

Ed configuro.

Immagine che contiene testo

Descrizione generata automaticamente

Premo ctrl o per salvare ed invio .

Per uscire ctrl x

Cambio indirizzo ip di windows

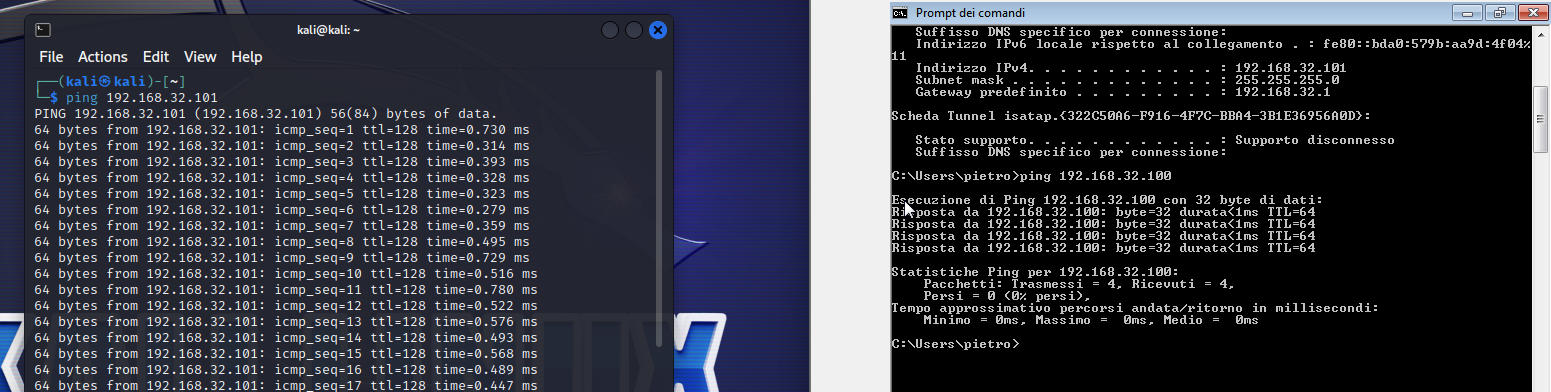
Vado su panello controllo dopo su rete e internet poi centro controllo connessioni , dopo di che su connessioni alla rete locale. proprietà; selezioni protocollo internet versione 4(tcp/ipv4) ed configuro.

Immagine che contiene testo

Descrizione generata automaticamente

Riavvio kali con sudo reboot

Ed controllo i Ping



**2)Setto la DNS**

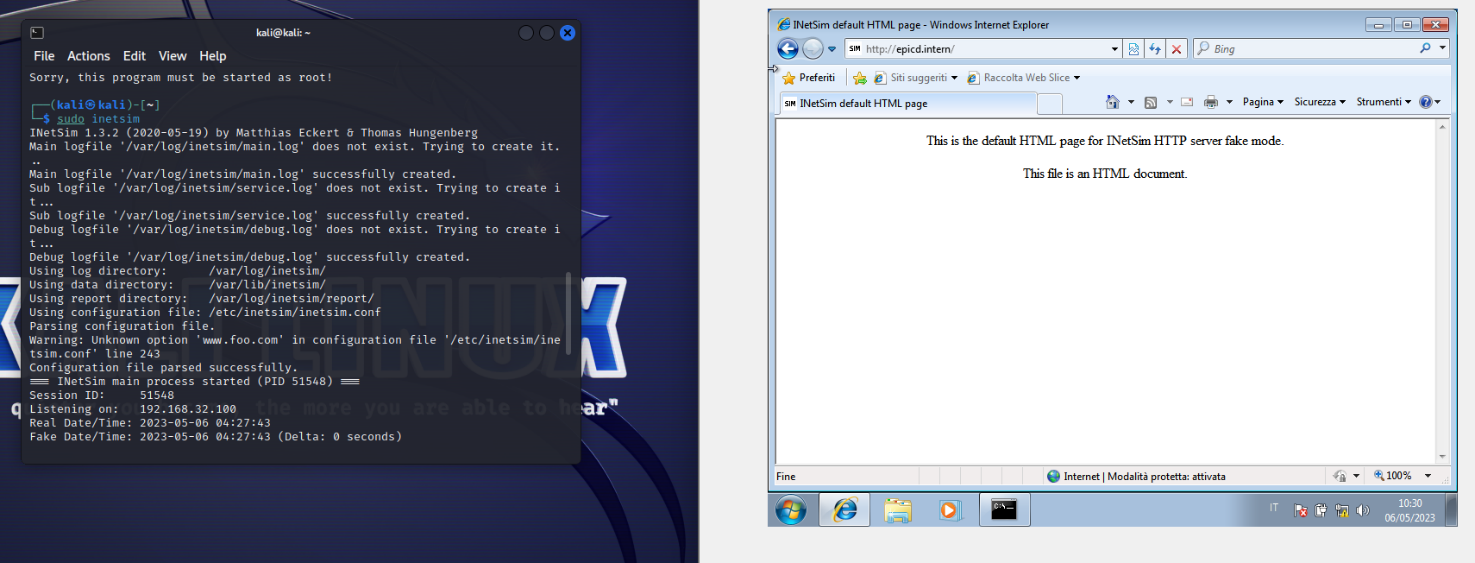
Inserendo a kali in nel panello di comando sudo nano /etc/inetsim/inetsim.conf

Inserisco

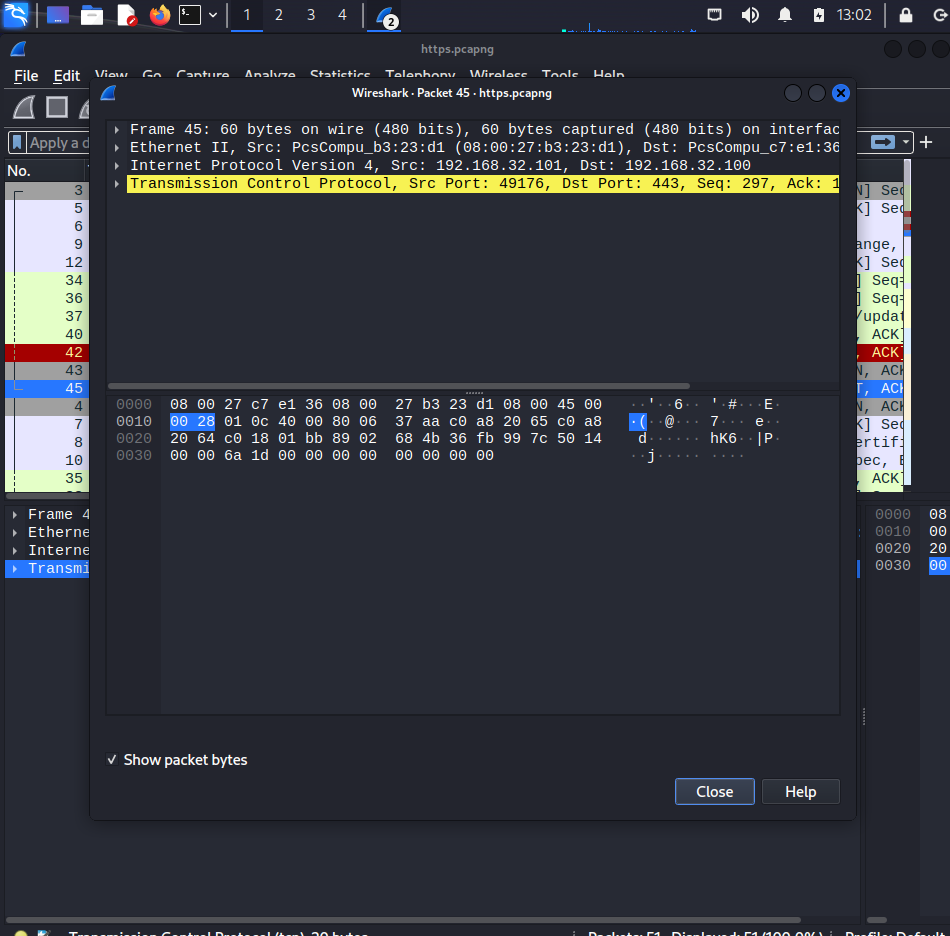
Immagine che contiene testo

Descrizione generata automaticamente

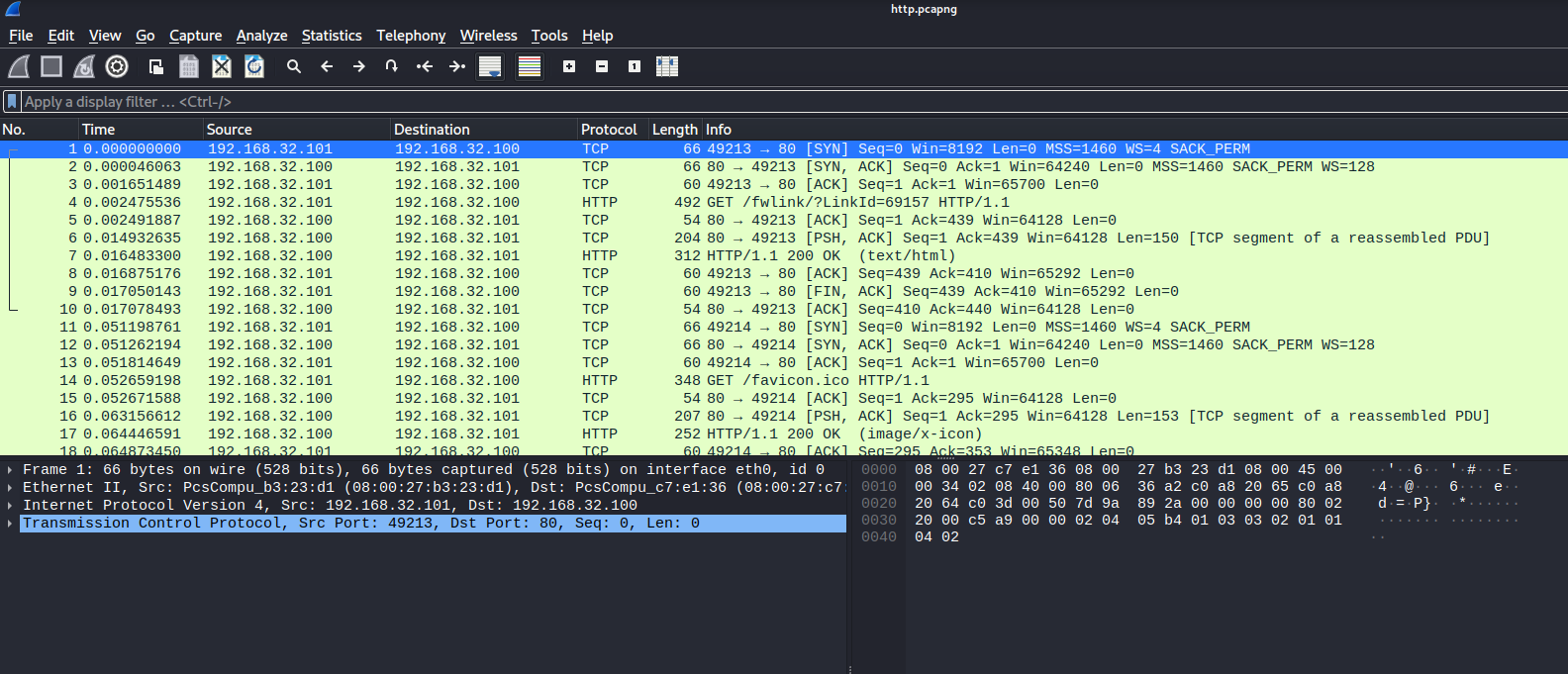
Avvio la simulazione con sudo inetsim



**3)Procedo con Wireshark**



Porta 433 per cui https noto che dei pacchetti sono criptati



Porta 80 e tutti i pacchetti sono leggibili .

**Http e https** sono due varianti dello stesso protocollo di telecomunicazione, ovvero quell’insieme di regole che definisce i metodi comunicativi tra due o più entità. Essi sono molto utilizzati durante la navigazione web medianti i più conosciuti browser, come Google Chrome, Microsoft Edge e Safari.

La principale differenza tra **http**(l’acronimo di **HyperText Transfer Protocol**) ed **https** (la cui **s** finale sta per **Secure**) risiede appunto nella maggiore sicurezza che quest’ultima variante di protocollo offre rispetto alla prima. Infatti, se nell’http lo scambio di risorse tra client e server avviene “in chiaro” (ovvero l’informazione che viene diffusa può essere letta da chi decide di intromettersi senza diritto nello scambio dei dati), nell’https la comunicazione è protetta grazie all’impiego di determinati certificati (come quello **SSL**, acronimo di **Secure Socket Layer**) .

**HTTPS = HTTP + SSL**

Per proteggere le informazioni potenzialmente sensibili dalla perdita, i siti web utilizzano i certificati SSL per creare una connessione sicura tra server web e browser, proteggendo la trasmissione di richieste e risposte HTTP.

L’ uso di un certificato SSL è la differenza fondamentale tra HTTP e HTTPS.

HTTPS crittografa il trasporto dei dati in modo che non sia visibile agli hacker o ad altri che monitorano la connessione. Ciò garantisce l’integrità dei dati e impedisce che le informazioni vengano modificate, danneggiate o rubate durante la trasmissione.

I protocolli SSL/TLS autenticano inoltre gli utenti per proteggere le informazioni e garantire che non vengano rivelate a utenti non autorizzati.