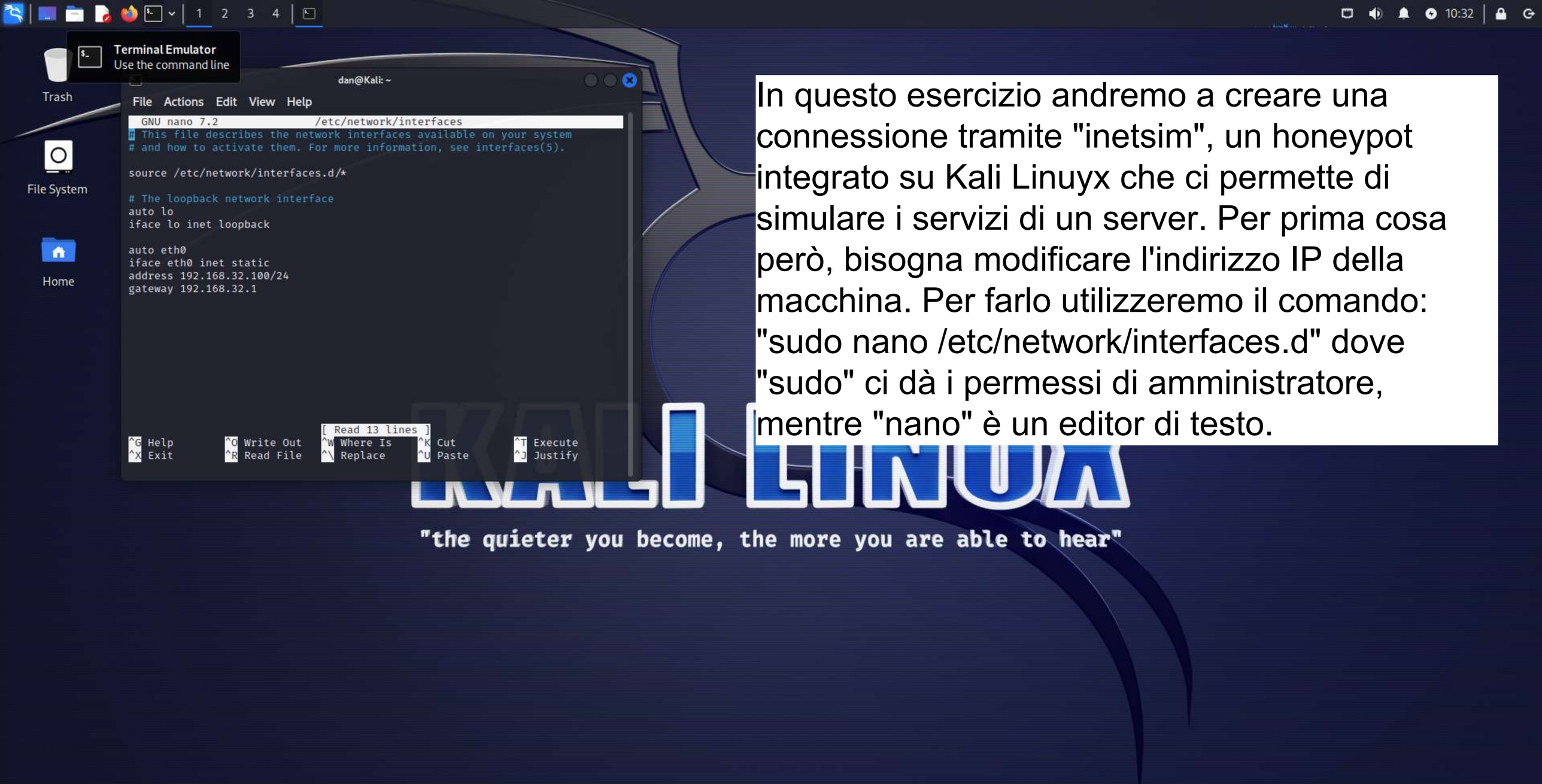
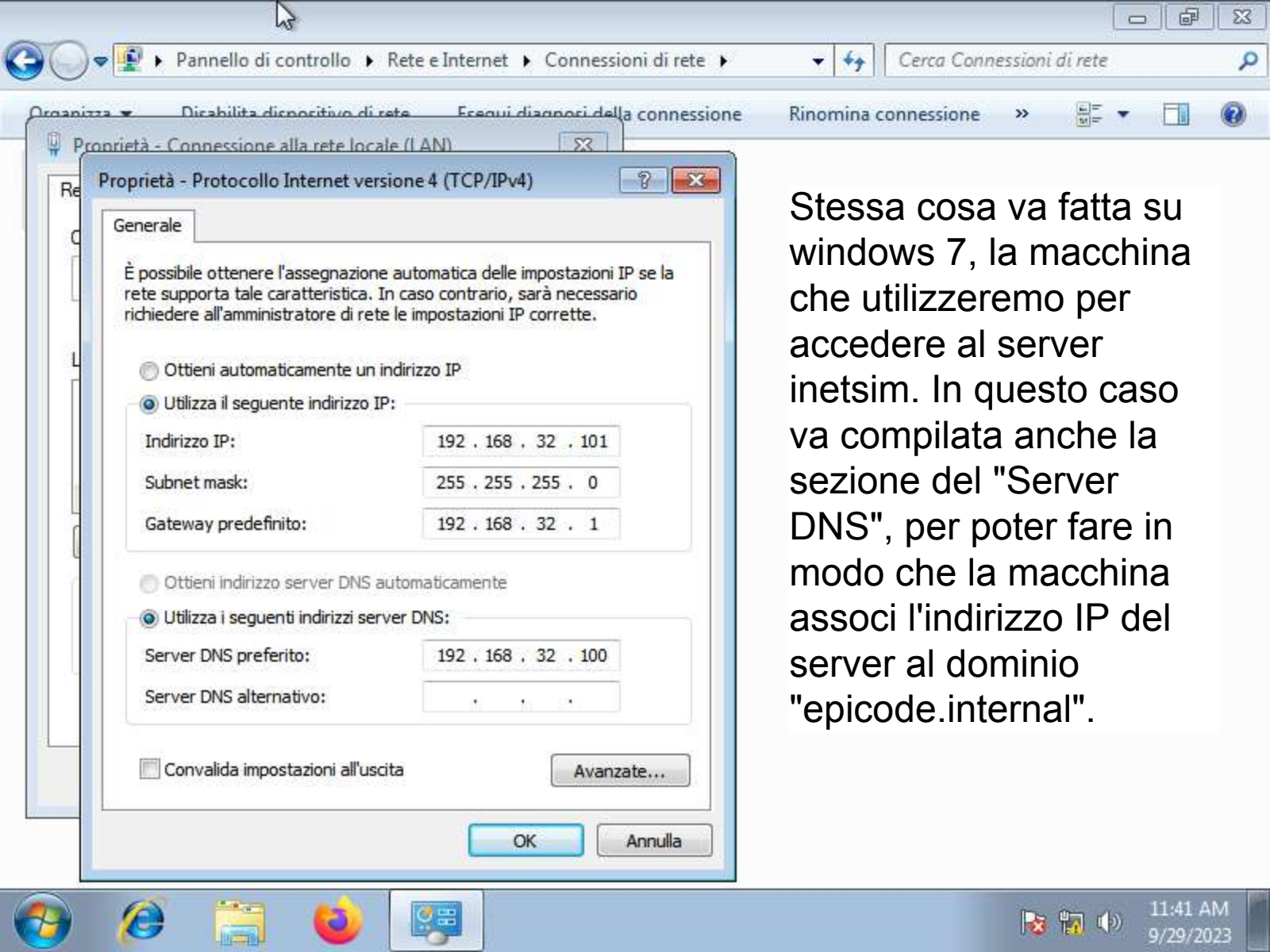
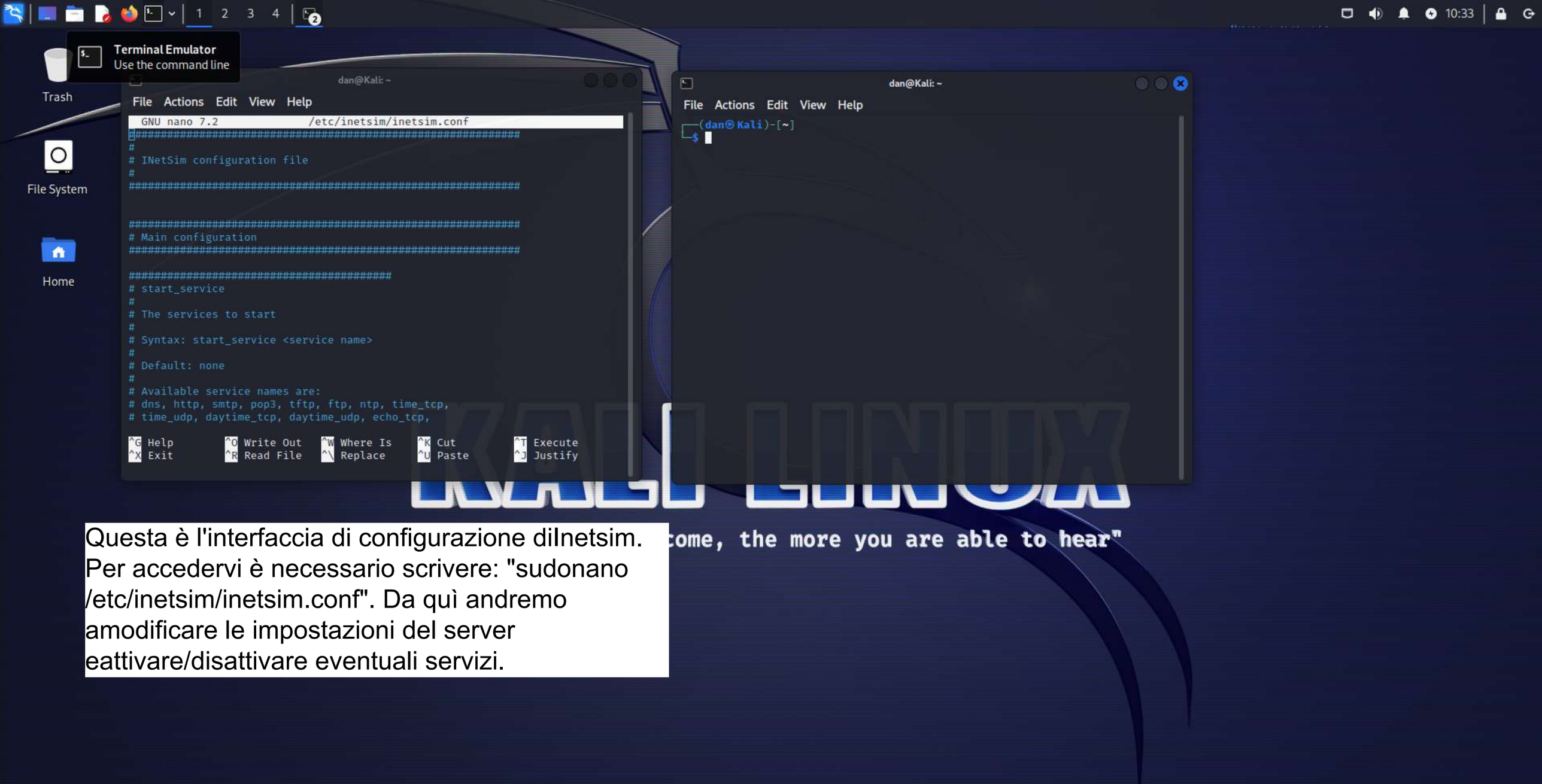


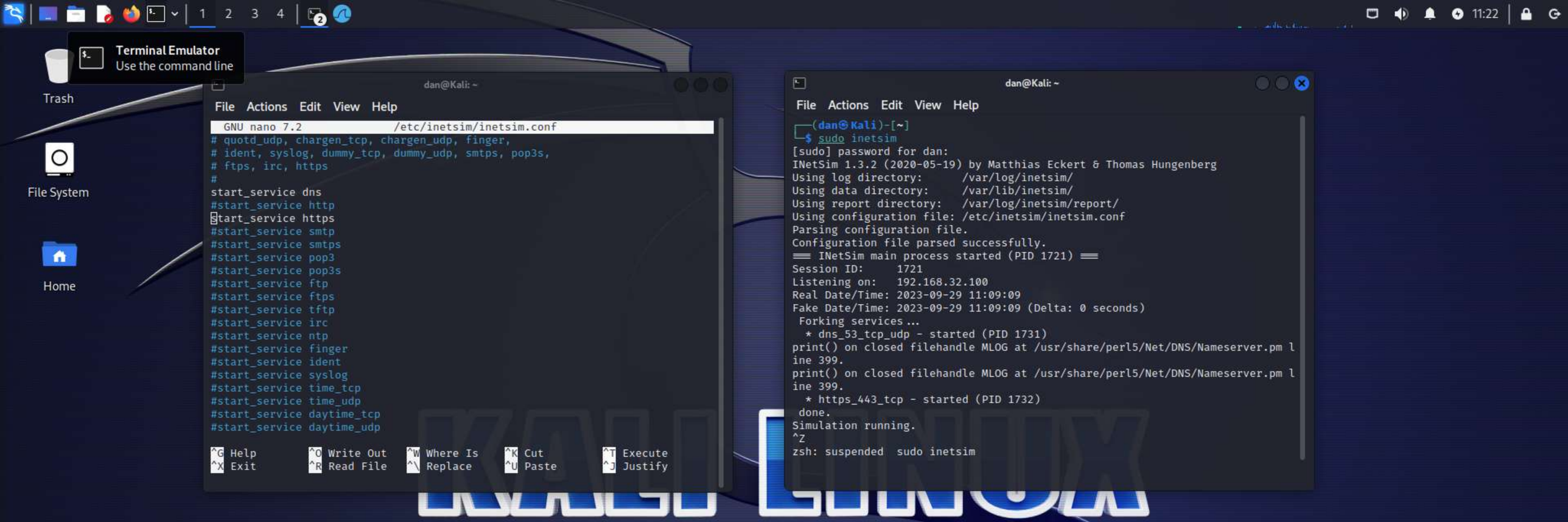
In questo esercizio andremo a creare una connessione tramite "inetsim", un honeypot integrato su Kali Linuyx che ci permette di simulare i servizi di un server. Per prima cosa però, bisogna modificare l'indirizzo IP della macchina. Per farlo utilizzeremo il comando: "sudo nano /etc/network/interfaces.d" dove "sudo" ci dà i permessi di amministratore, mentre "nano" è un editor di testo.



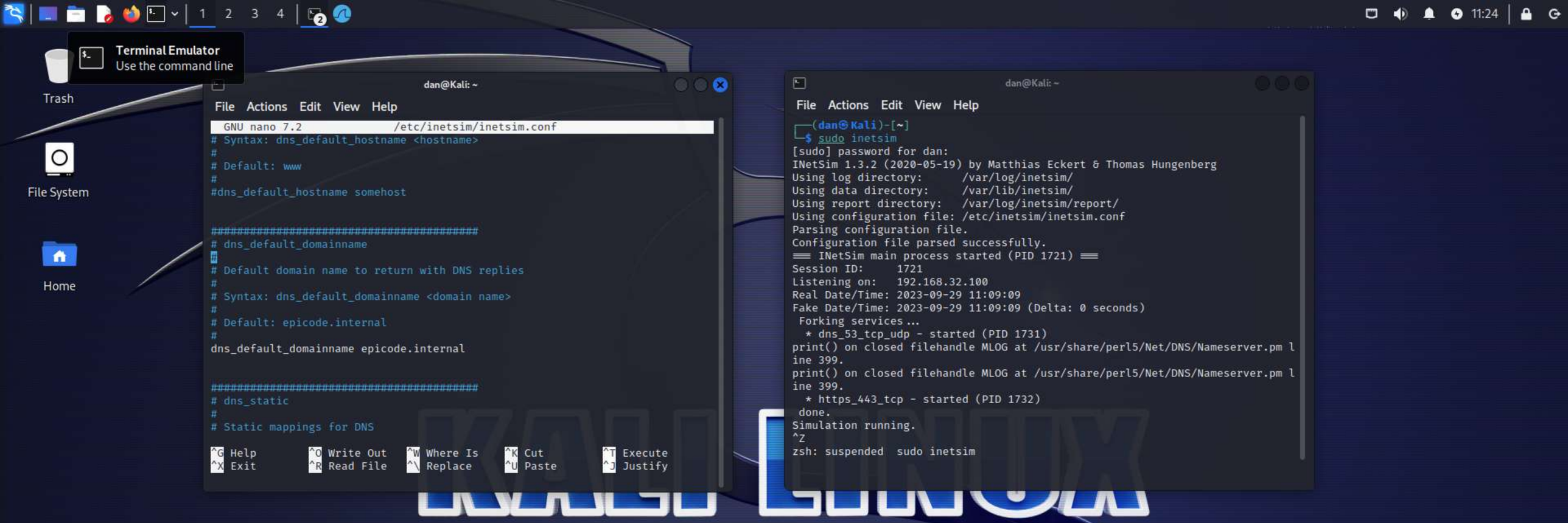
Stessa cosa va fatta su windows 7, la macchina che utilizzeremo per accedere al server inetsim. In questo caso va compilata anche la sezione del "Server DNS", per poter fare in modo che la macchina associ l'indirizzo IP del server al dominio "epicode.internal".



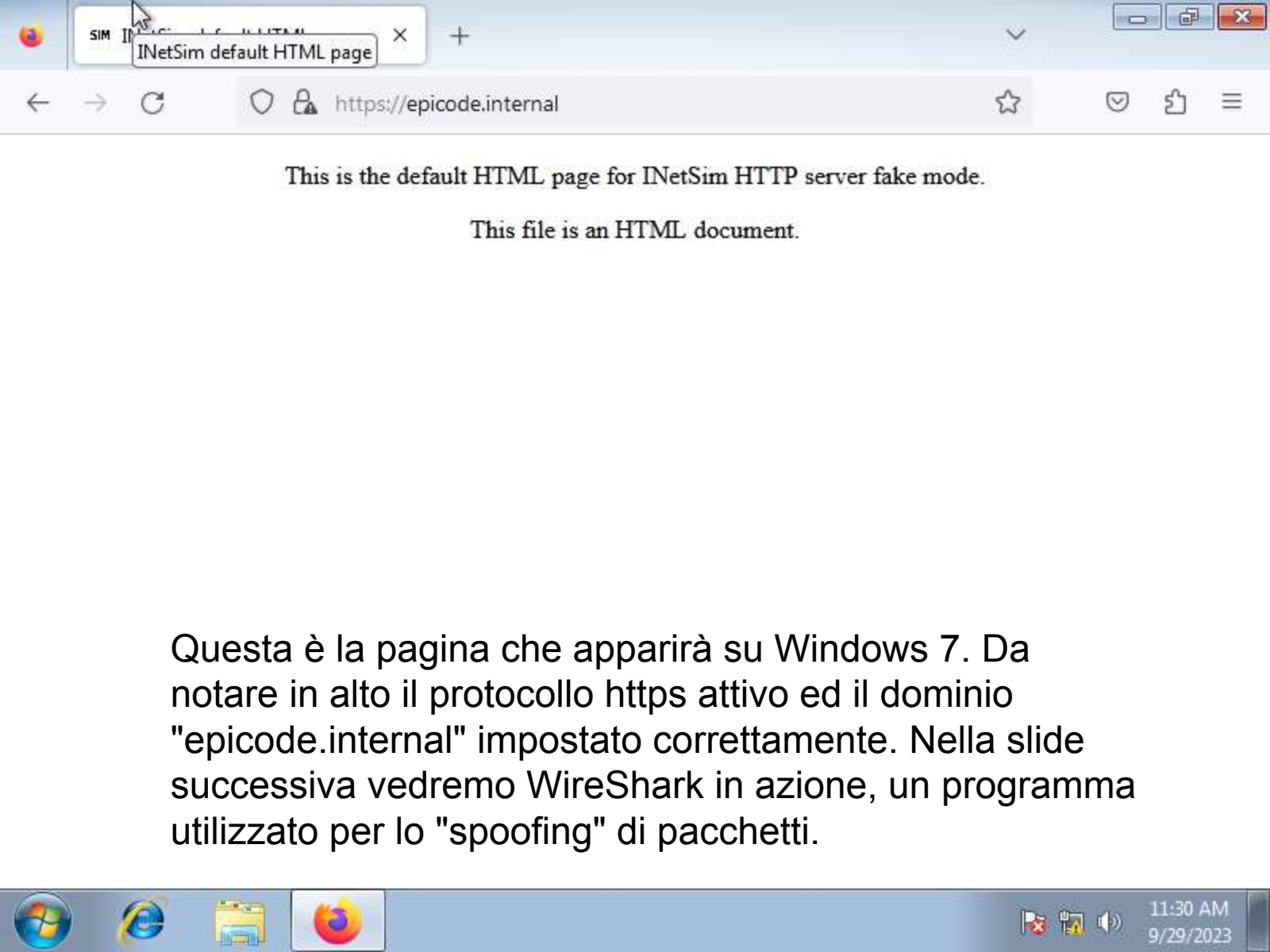
Questa è l'interfaccia di configurazione diInetsim. Per accedervi è necessario scrivere: "sudonano /etc/inetsim/inetsim.conf". Da qui andremo amodificare le impostazioni del server eattivare/disattivare eventuali servizi.



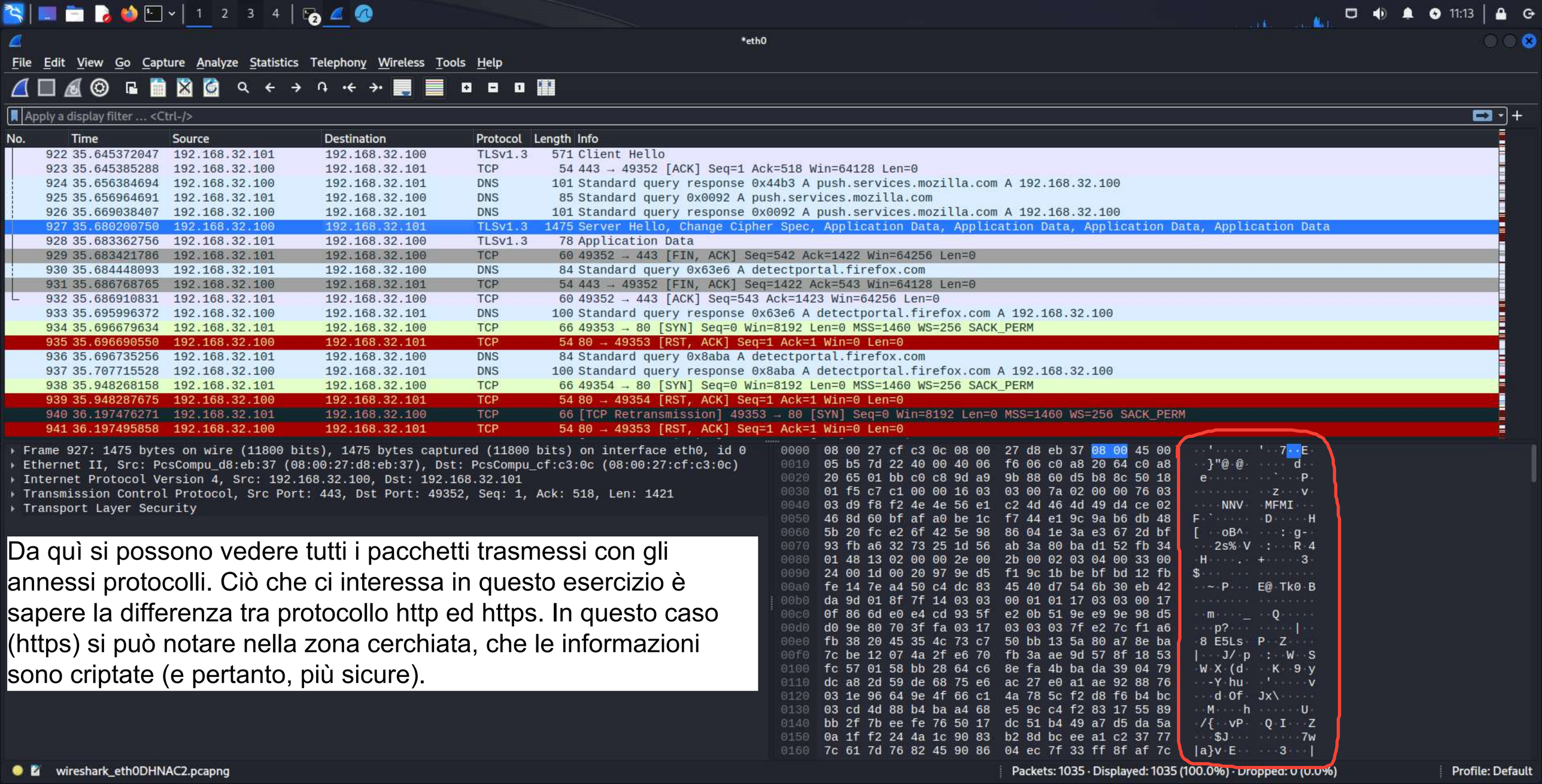
Quella a sinistra è la sezione dei servizi (che si trova nella pagina di configurazione di inetsim) in questo caso andremo ad attivare il servizio dns e https (successivamente proveremo col servizio http). Per farlo, basta usare il "#" prima dello "start_service" per disattivare o meno un servizio.



Ancora a sinistra, andremo a modificare il dominio, per poter effettivamente associarlo a l'indirizzo IP della macchina Linux. A destra invece c'è inetsim attivato, per farlo basta scrivere "sudo inetsim".

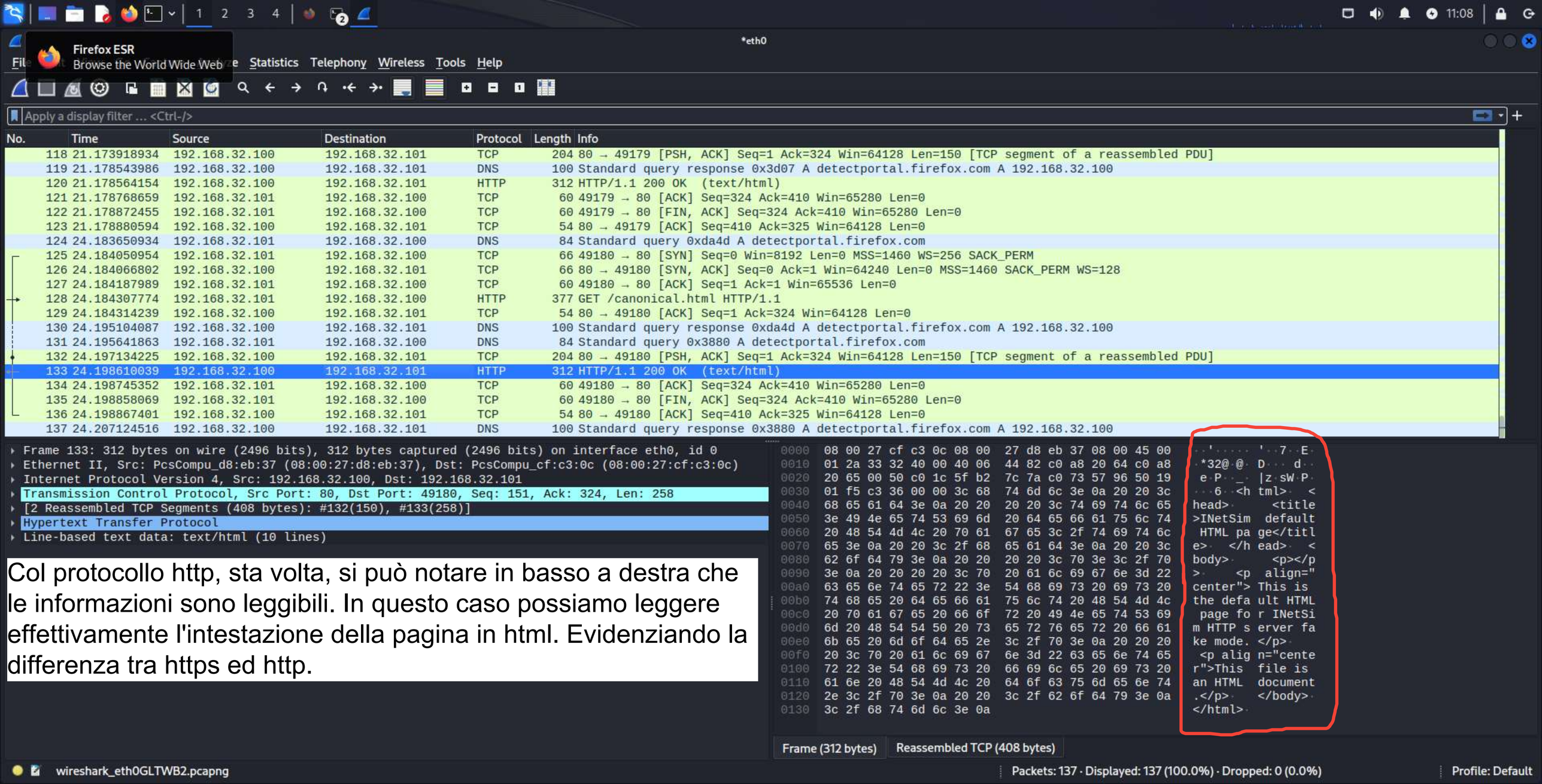


Questa è la pagina che apparirà su Windows 7. Da notare in alto il protocollo https attivo ed il dominio "epicode.internal" impostato correttamente. Nella slide successiva vedremo WireShark in azione, un programma utilizzato per lo "spoofing" di pacchetti.



Da quì si possono vedere tutti i pacchetti trasmessi con gli annessi protocolli. Ciò che ci interessa in questo esercizio è sapere la differenza tra protocollo http ed https. In questo caso (https) si può notare nella zona cerchiata, che le informazioni sono criptate (e pertanto, più sicure).

Questa è la stessa pagina di Windows 7, ma si può notare l'assenza del protocollo https in alto.



Col protocollo http, sta volta, si può notare in basso a destra che le informazioni sono leggibili. In questo caso possiamo leggere effettivamente l'intestazione della pagina in html. Evidenziando la differenza tra https ed http.