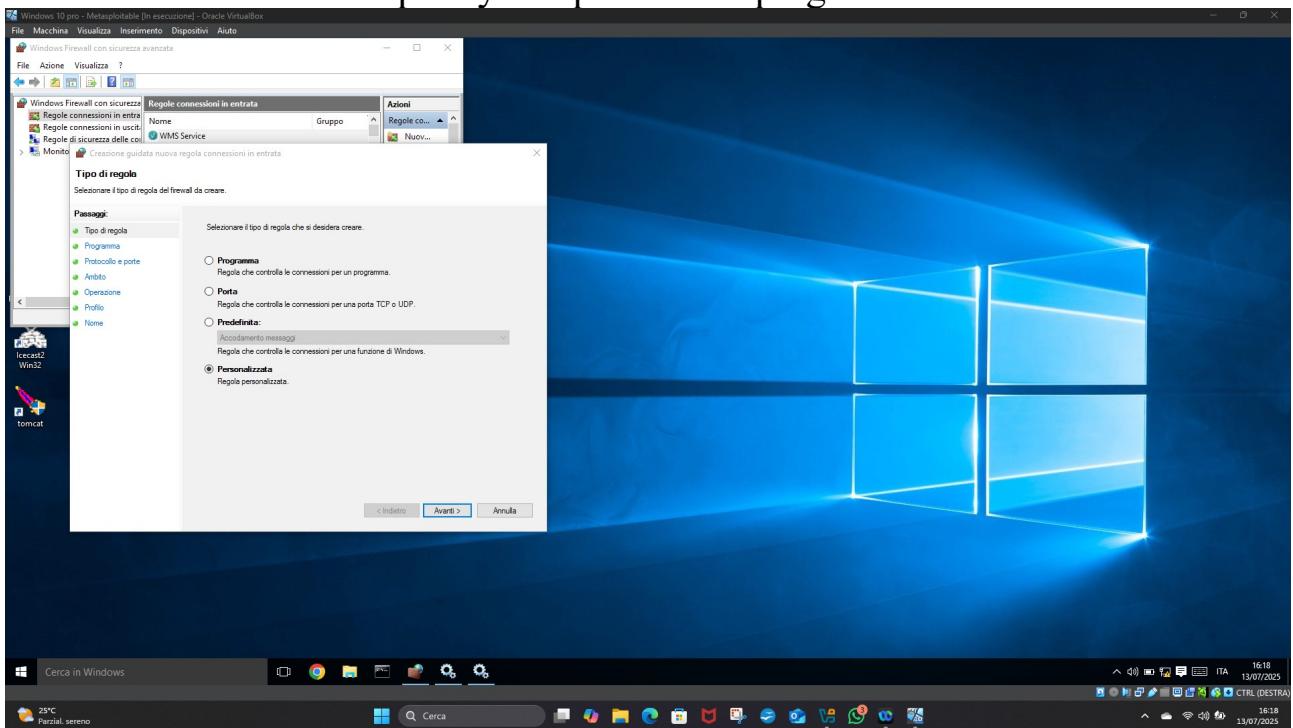


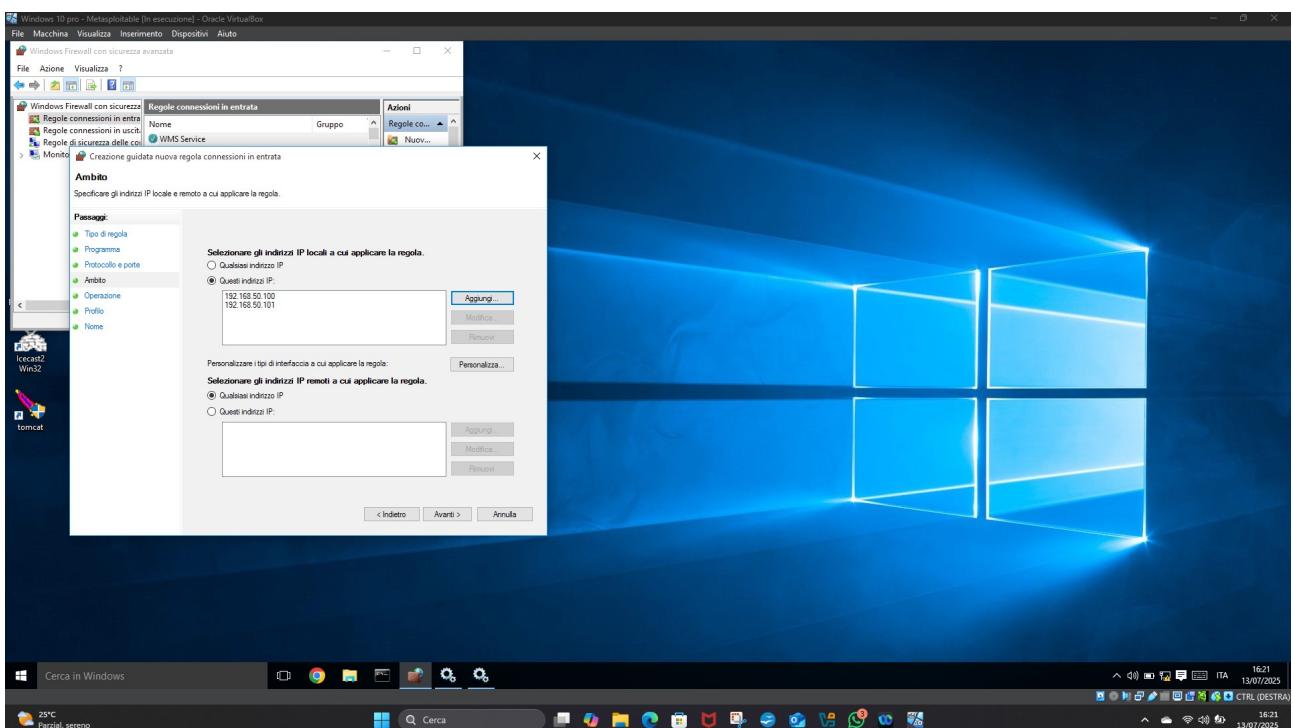
Creazione policy e Cattura pacchetti tramite Wireshark

Capitolo 1

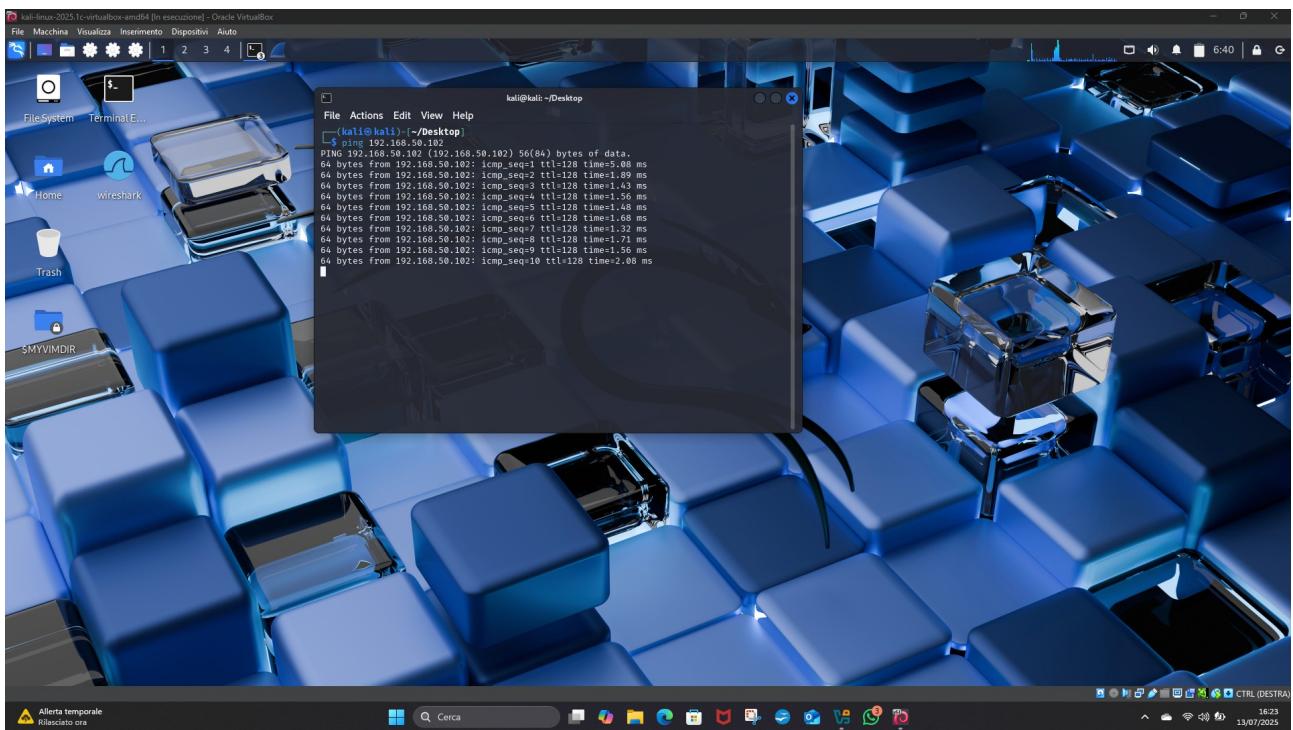
creazione di una policy che permetta il ping fra macchine virtuali



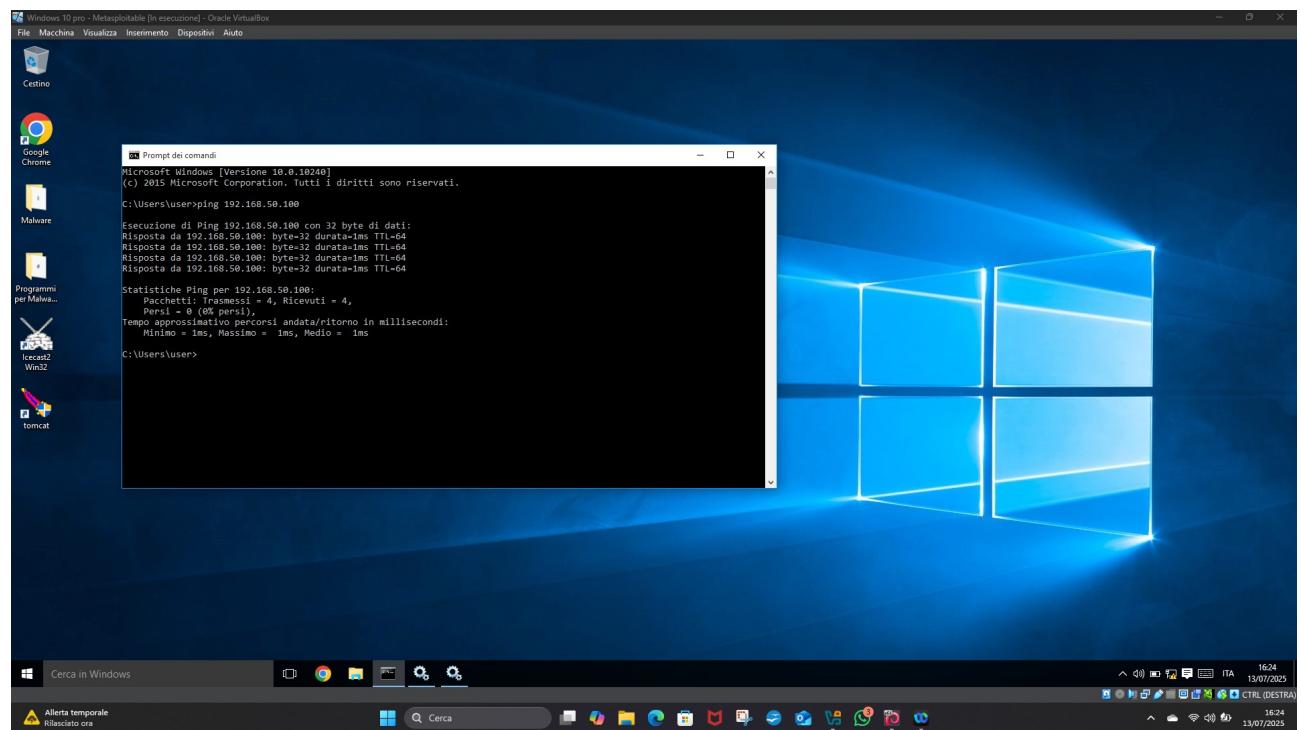
inserimento IP consentiti per la comunicazione
192.68.50.100 KALI
192.168.50.101 METASPLOITABLE



AVVIO PING DA KALI A WINDOWS

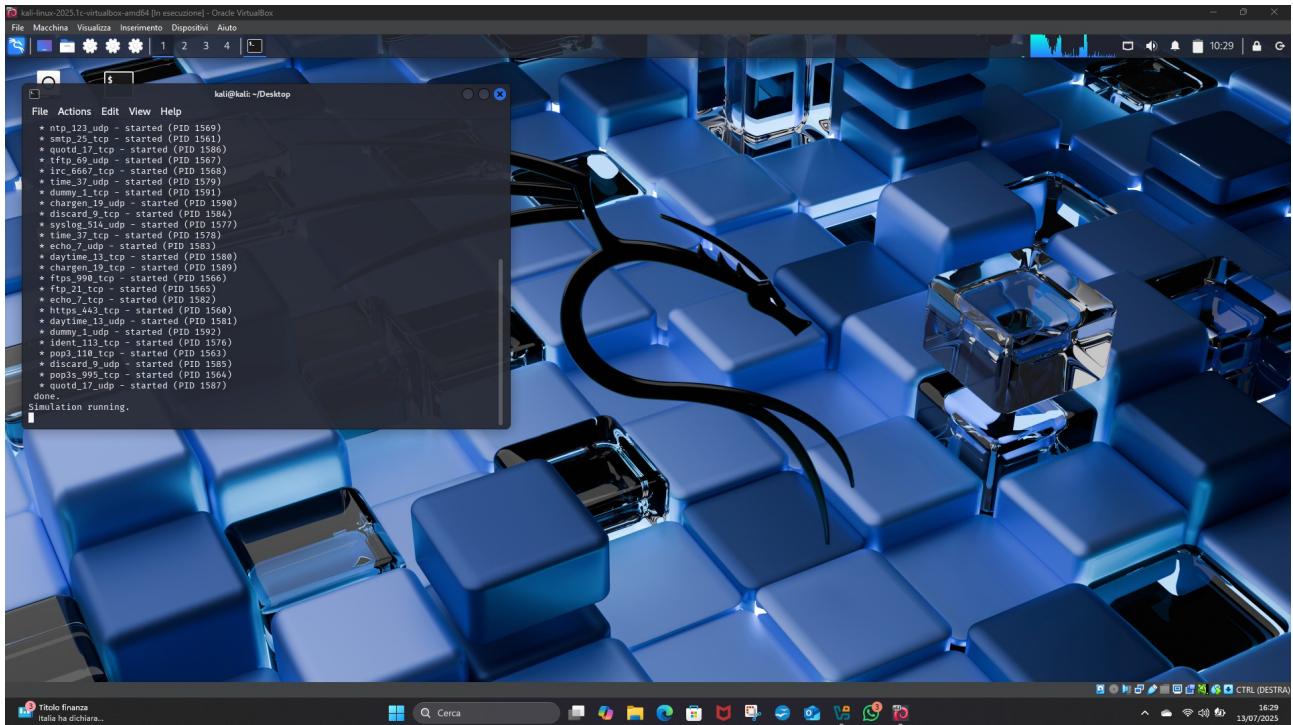


AVVIO PING DA WINDOWS A KALI

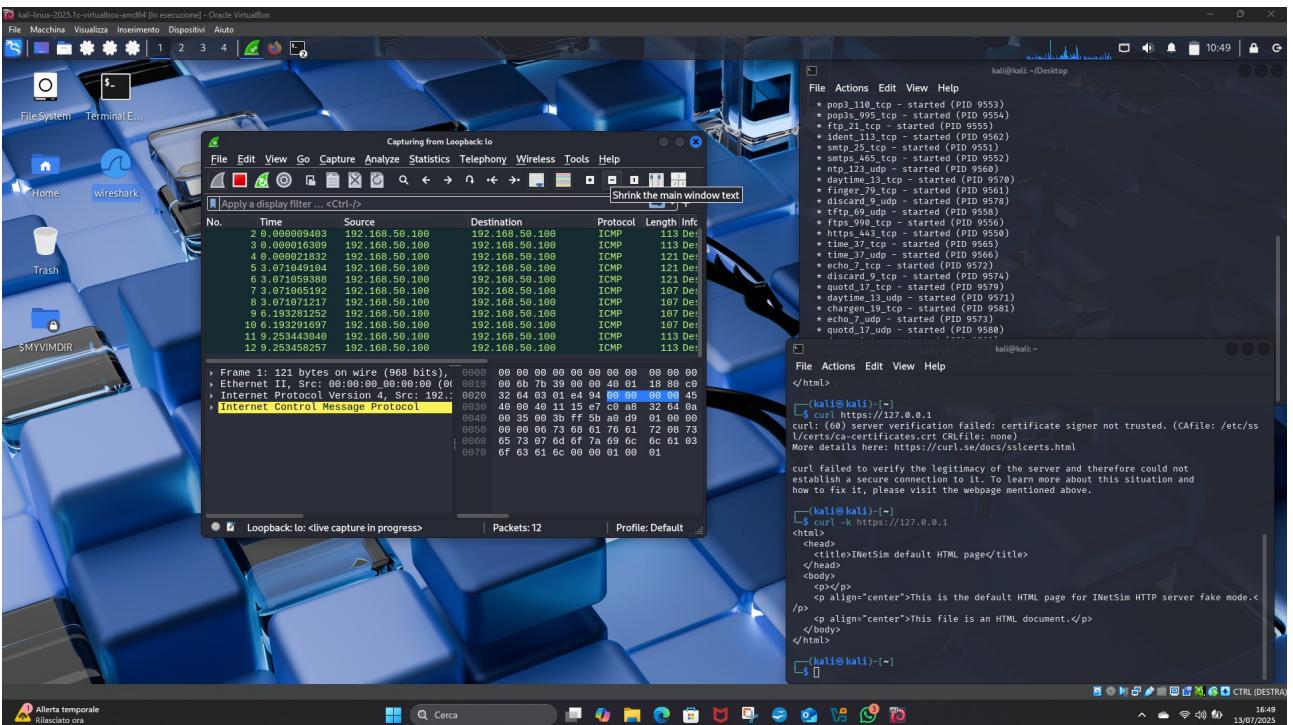


CAPITOLO 2 Avvio di INETSIM

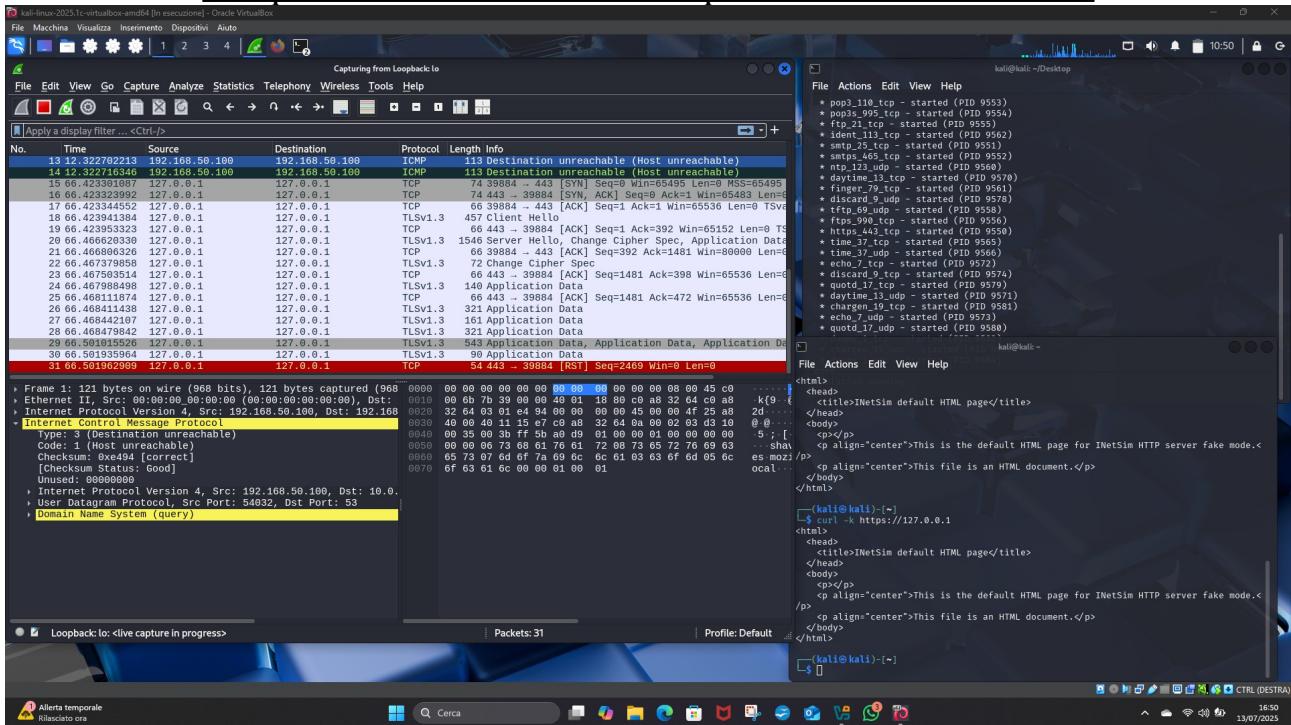
Inetsim è un app che simula servizi internet in un ambiente sicuro e isolato, essenziale per analisi di malware.



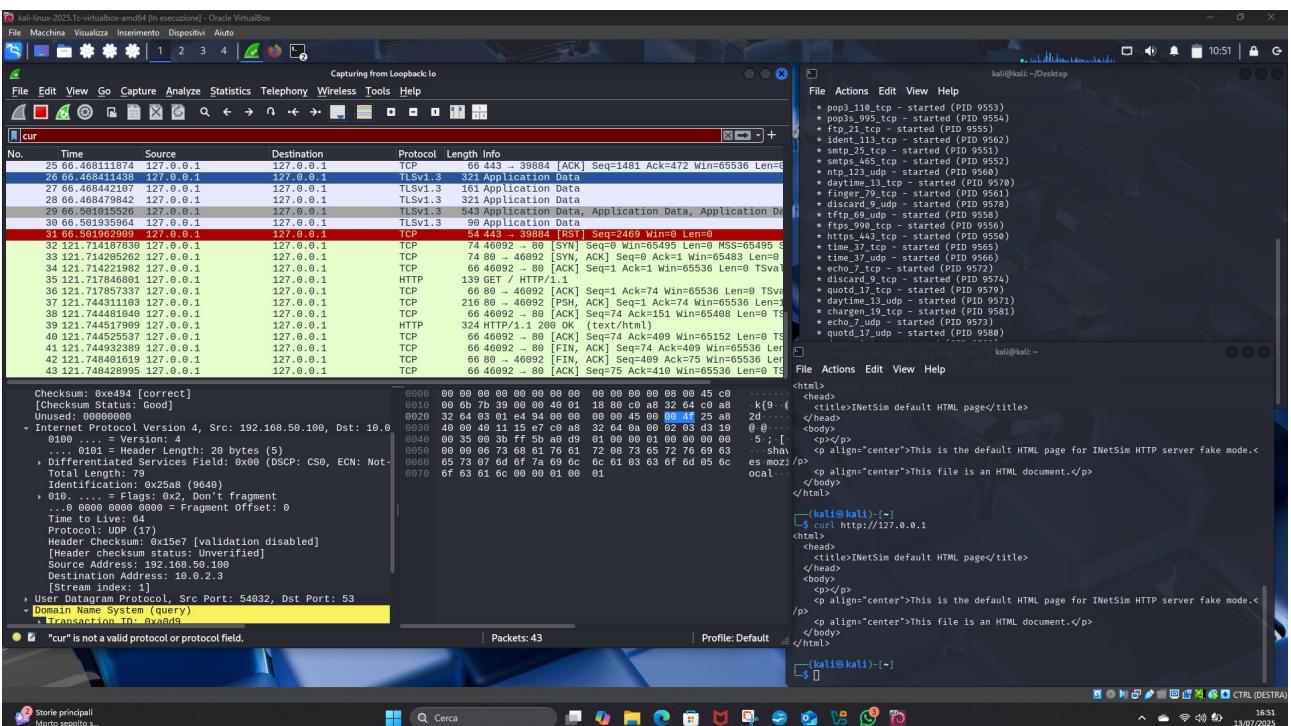
Tramite il comando curl si puo vedere tramite WIRESHARK cosa appare a schermo aprendo un https o un http



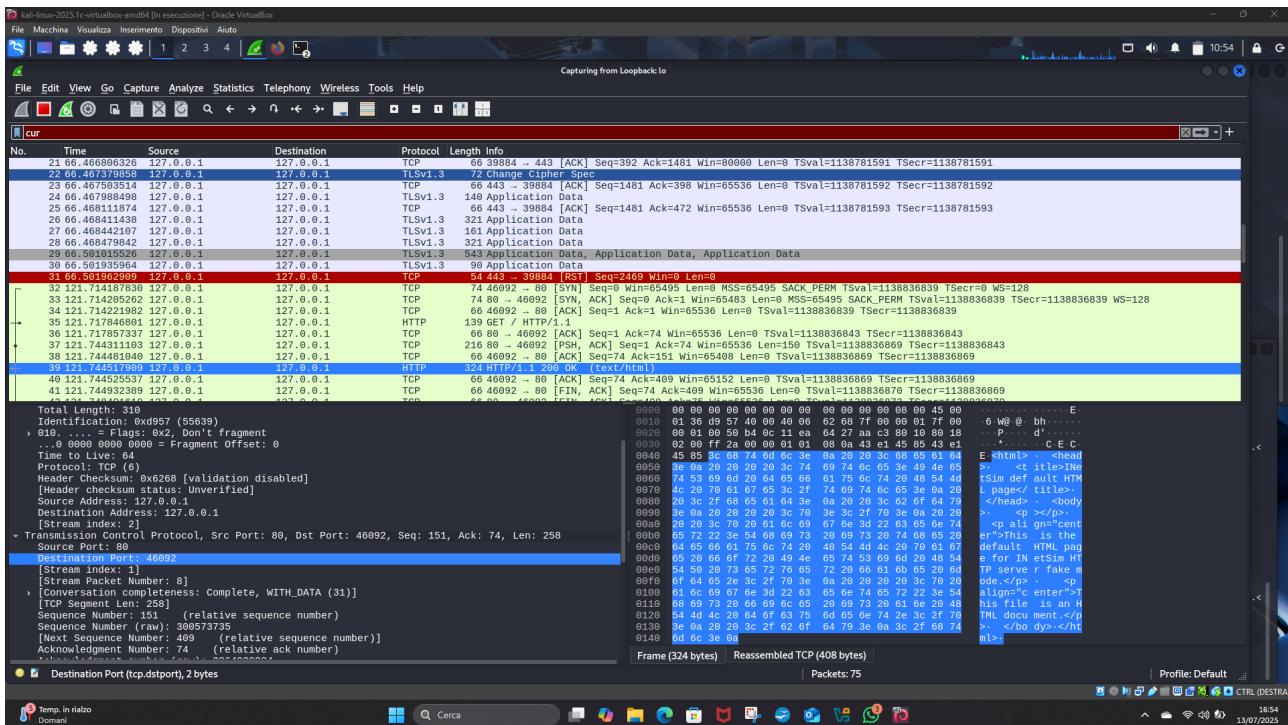
Nel primo caso (HTTPS) si notera' che siamo impossibilitati nel visionare completamente e liberamente i pacchetti inviati/ricevuti



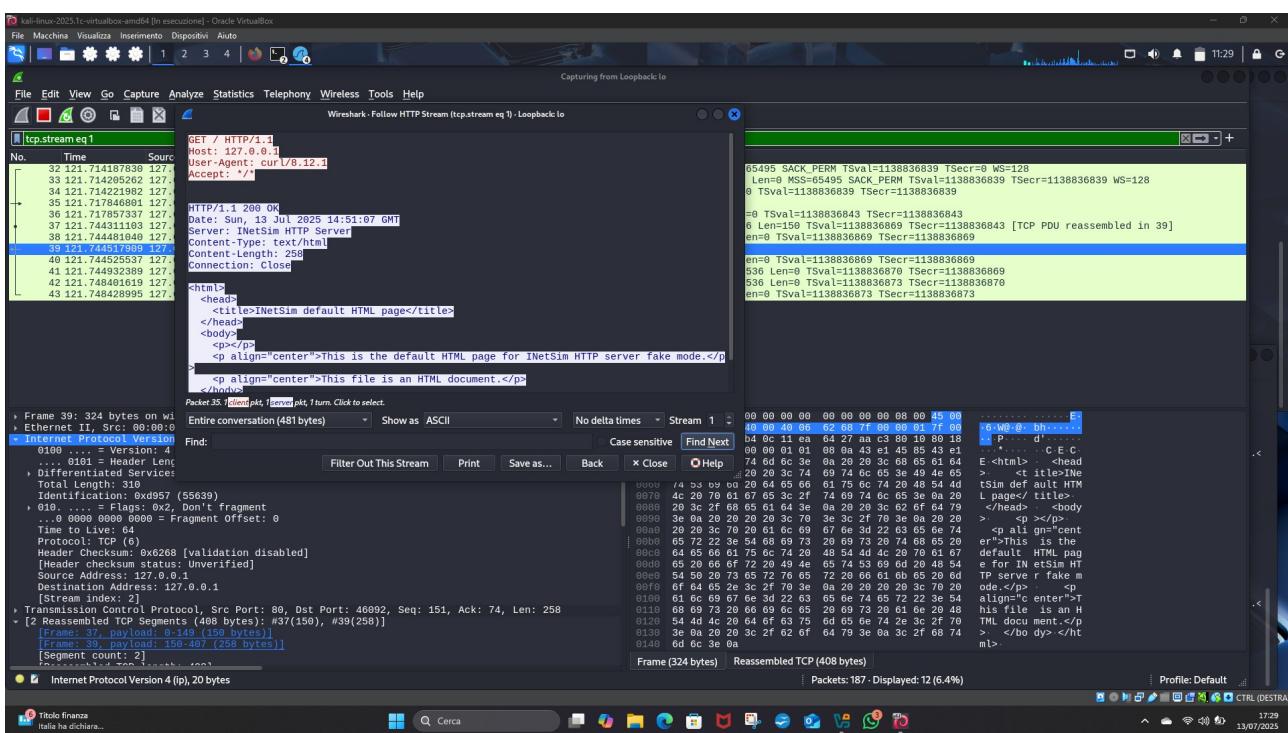
invece nel caso di HTTP saremo liberi di poter vedere qualsiasi pacchetto inviato e ricevuto



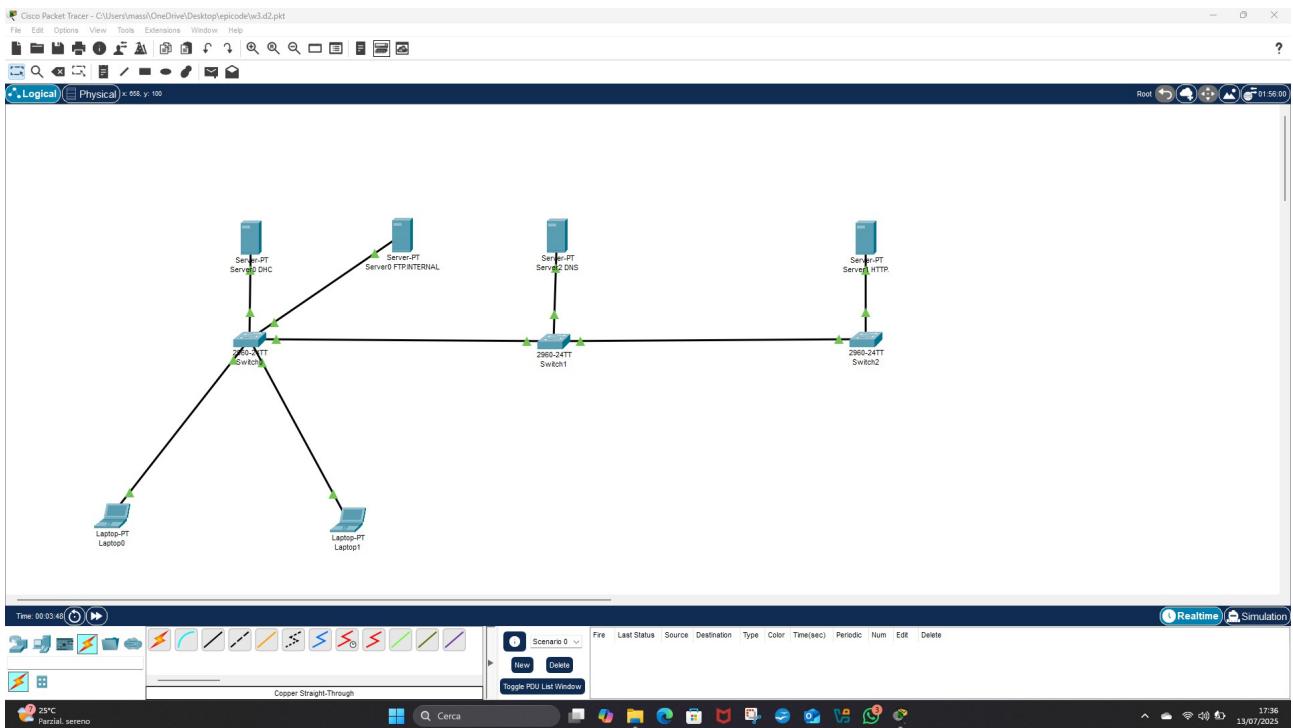
GRAZIE A WIRESHARK saremo in grado di vedere porte, source address destination address, messaggi di testo , qualsiasi cosa inviata e ricevuta



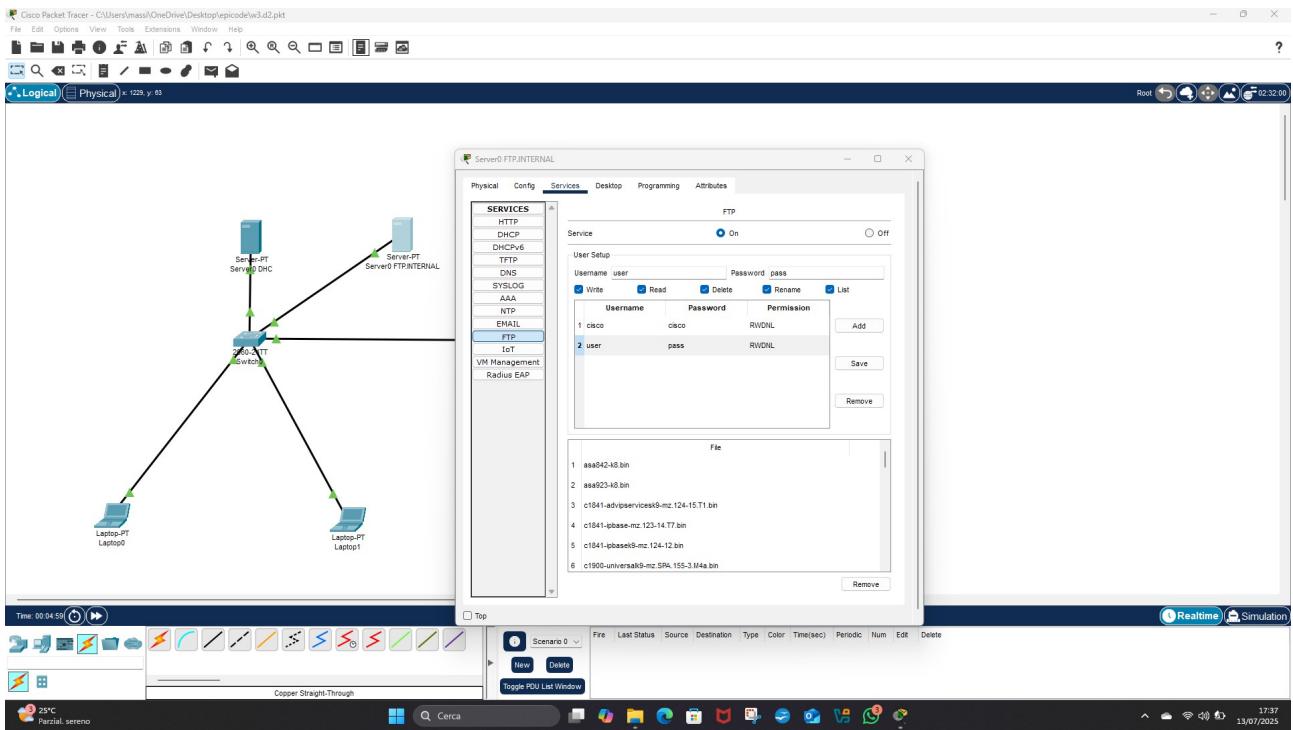
frame payload numero di byte

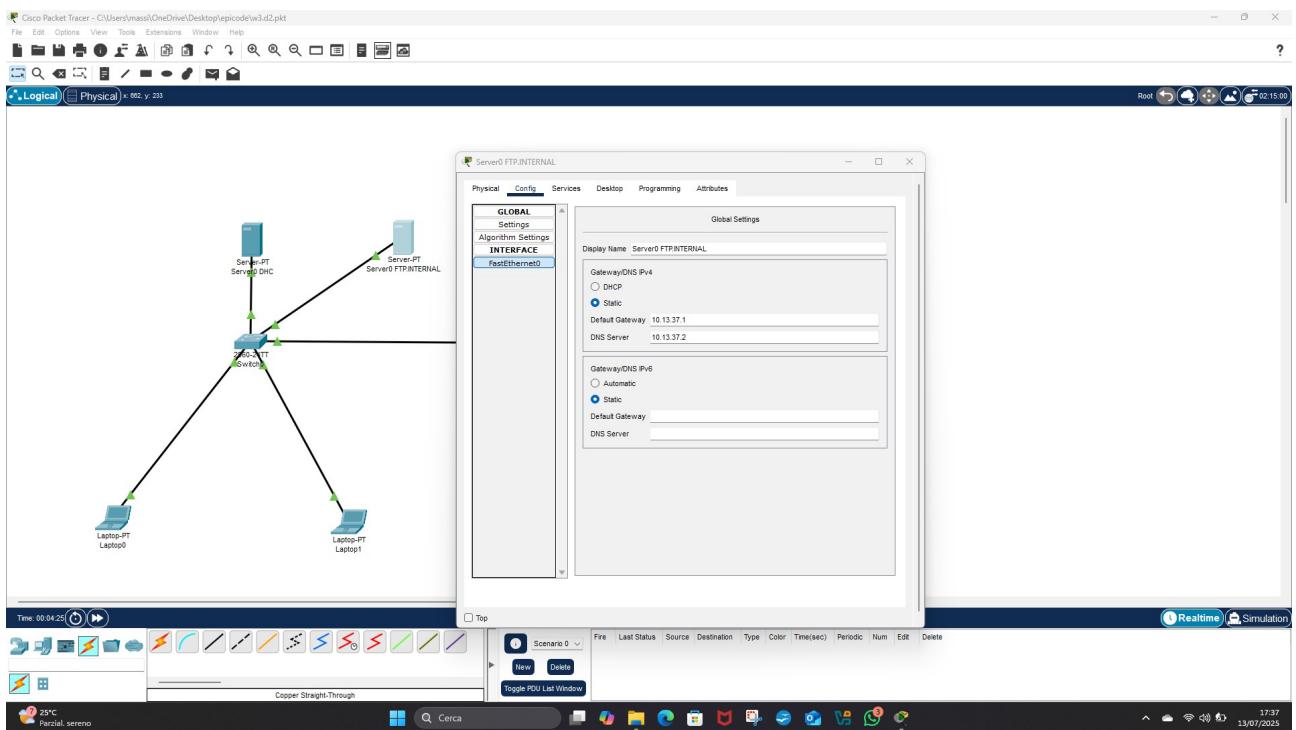


Extra W3D1 inserimento server FTP e download file



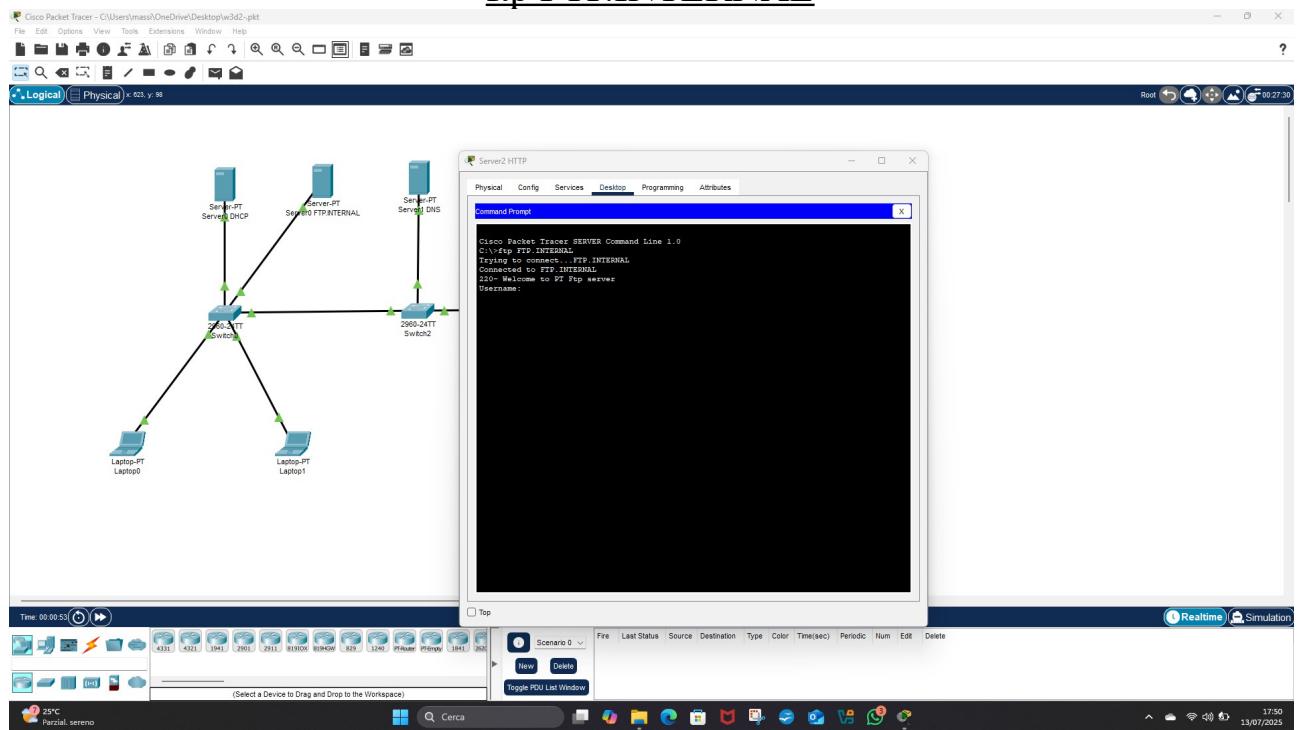
configurazione server ftp



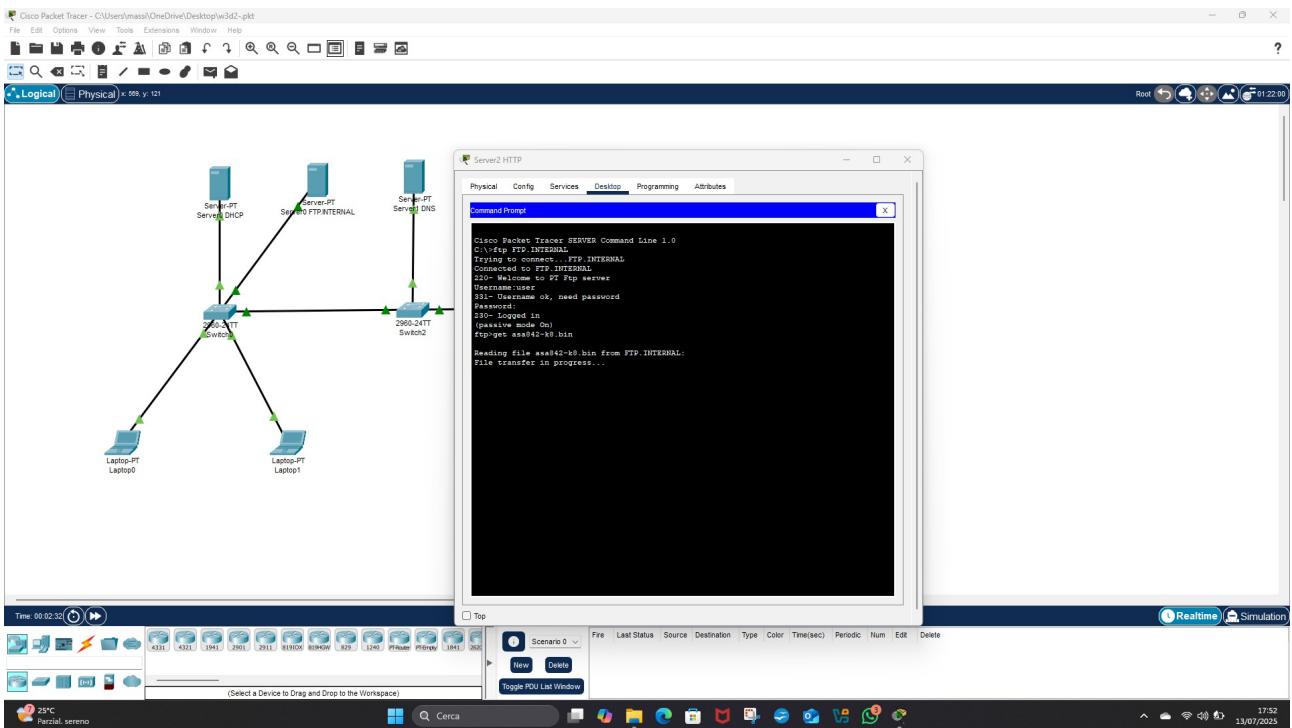


dopo aver abilitato il server Ftp e dopo la creazione di un account si aggiunge la voce DNS aggiungendo il nome ftp.internal e l'address poi si procede con il collegamento tramite prompt

ftp FTP.INTERNAL



PER SCARICARE IL FILE SI UTILIZZERA' IL COMANDO GET PIU "NOMEDEL FILE"



IN QUESTO CASO NON SONO RIUSCITO AD INSERIRE IN FILE E HO
PROCEDUTO CON LO SCARICARNE UNO GIA' PREIMPOSTATO
asa842-k8.bin

