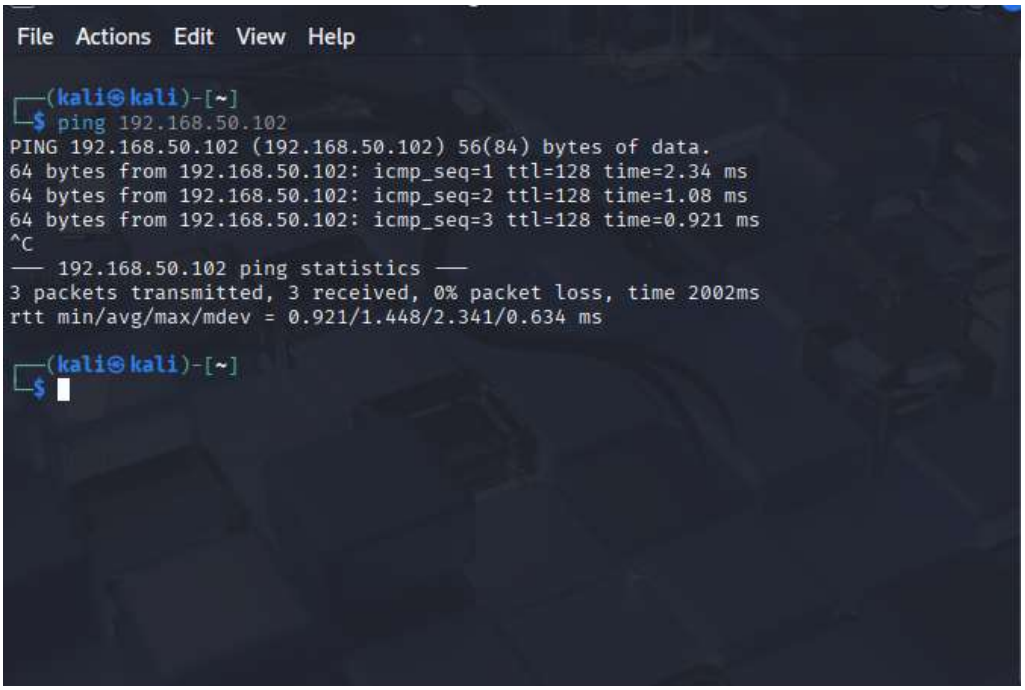
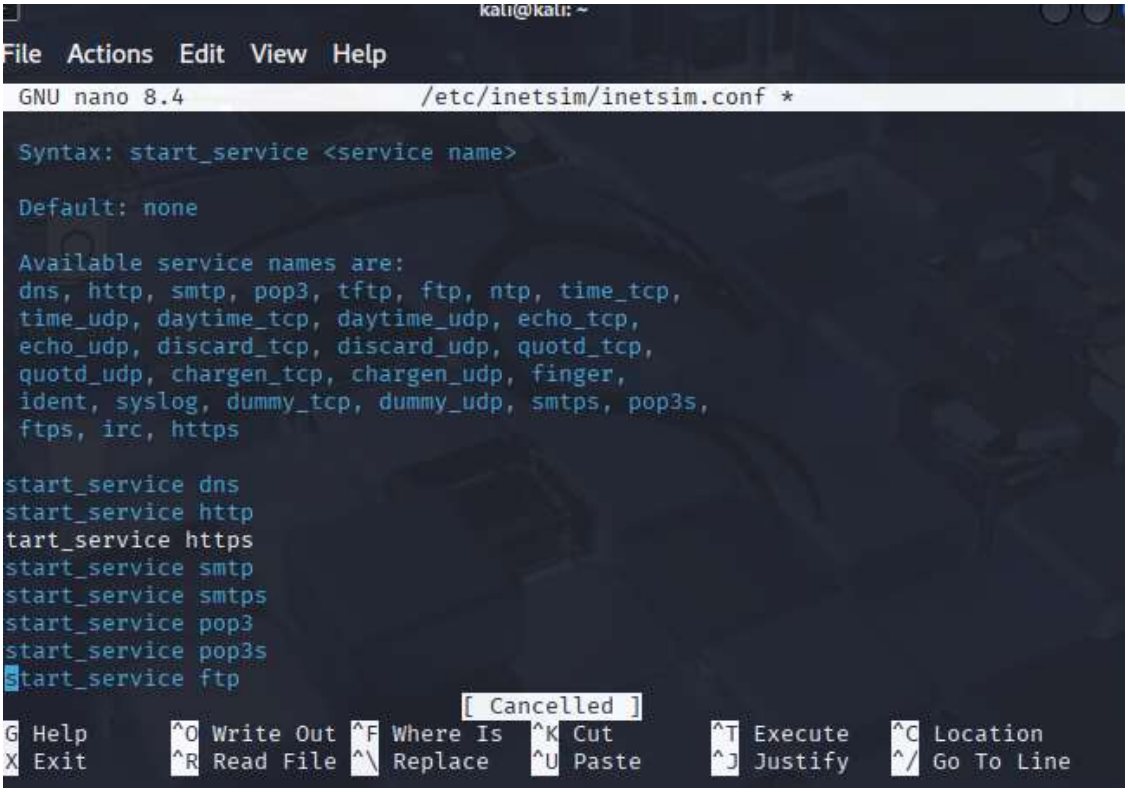
Policy e Packet captur

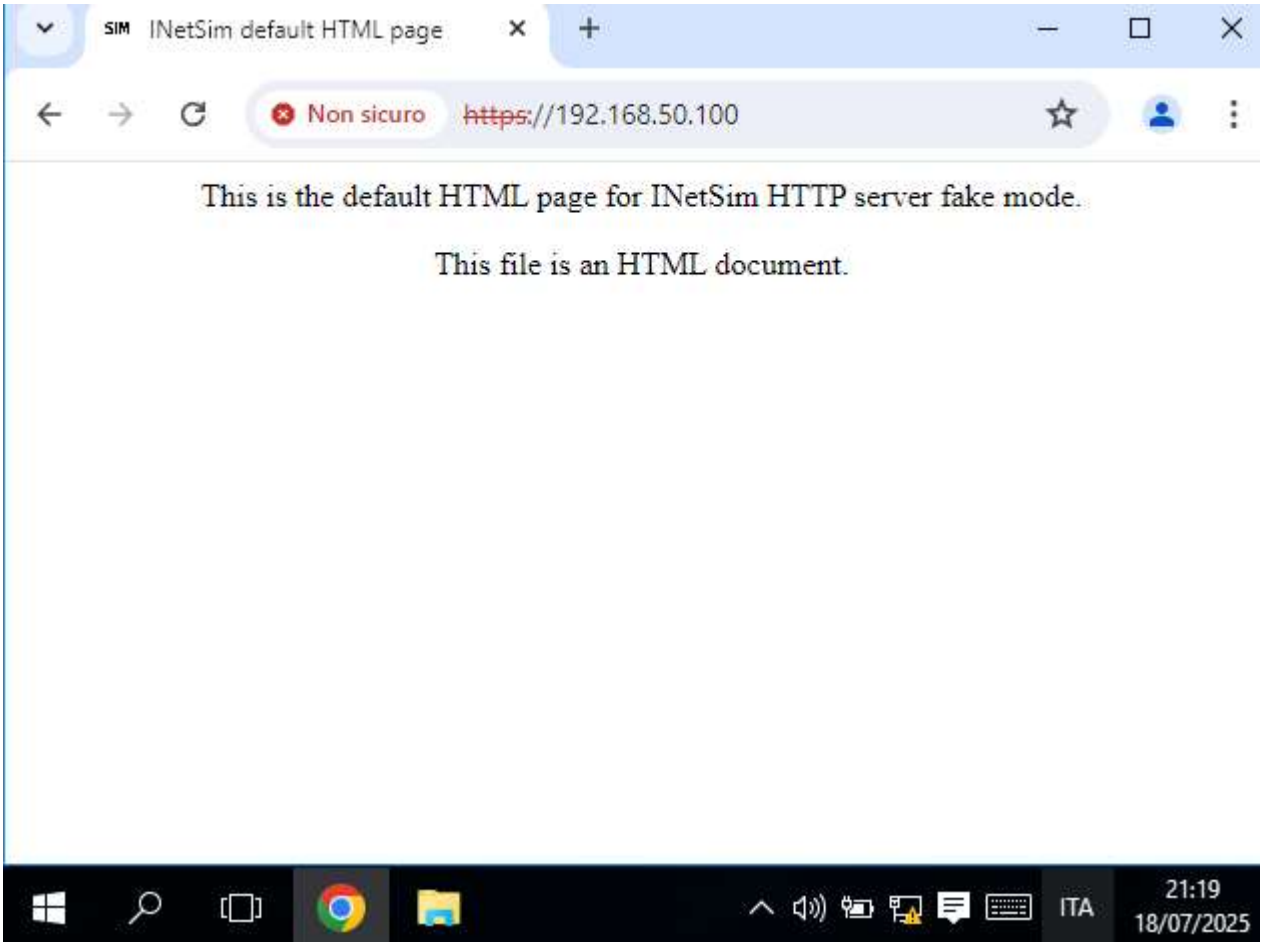
Come prima cosa controlliamo che la kali comunica con windows con il comando PING



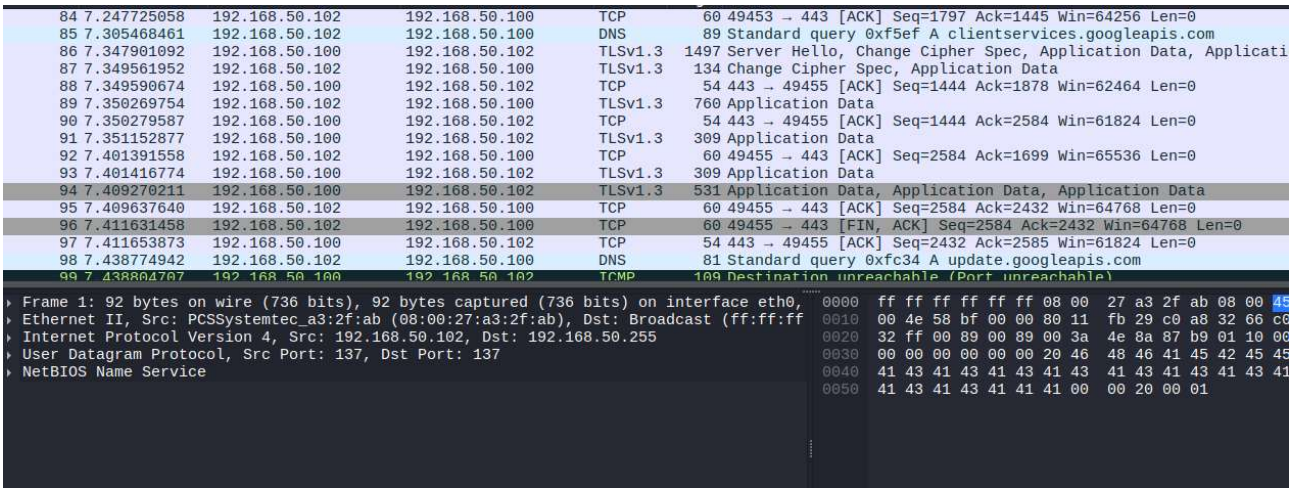
Come seconda cosa configuriamo il file inetsim.conf per utilizzare solo il servizio HTTPS



Facciamo partire inetti dalla kali e dalla macchina windows andremo sul browser e cercheremo l'indirizzo ip della macchina kali con un servizio HTTPS attivo



Come possiamo vedere tutto funziona perfettamente. Ora controlliamo dalla kali il traffico di rete con wireshark

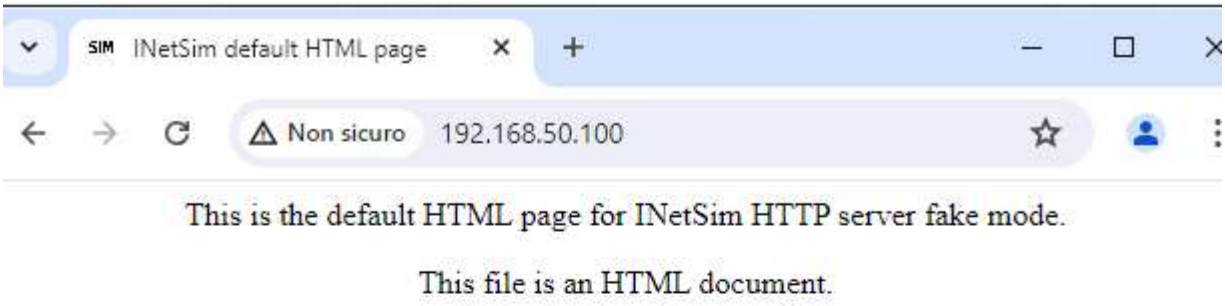


E da qui possiamo analizzare i pacchetti che partono che si comunicano le due macchine.

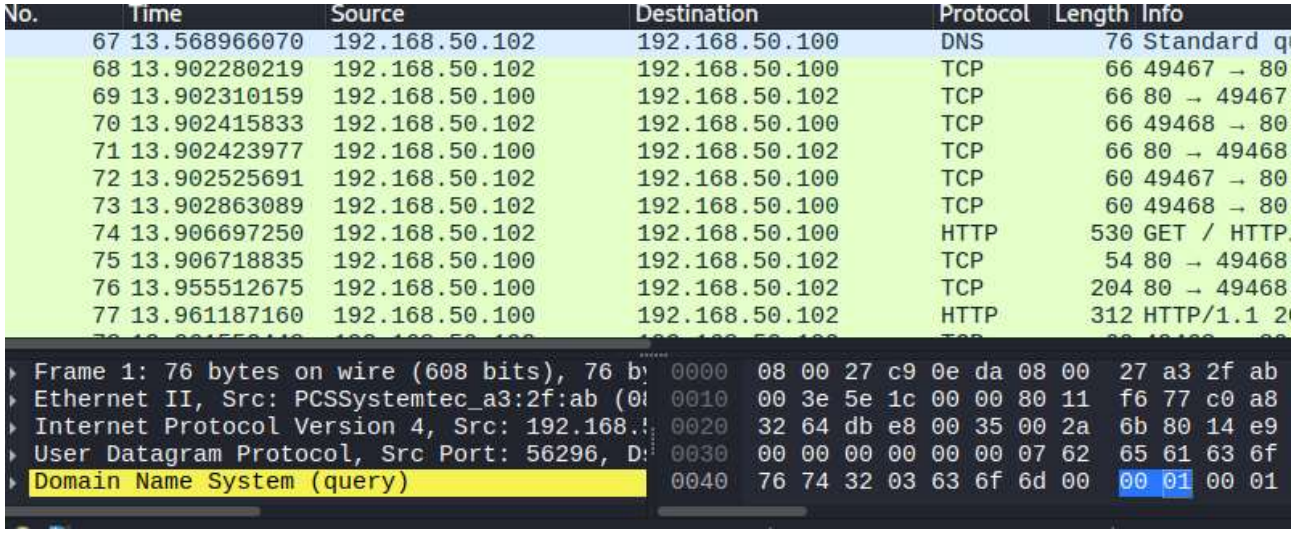
Possiamo rifare la stessa cosa con un altro servizio invece che HTTPS possiamo usare http quindi dobbiamo modificare il file inetti.conf per attivare il servizio http

Cerchiamo dal browser di windows la stessa cosa ma con protocollo

http invece che HTTPS



E poi andremo a vedere le differenze da wireshark controllando il contenuto dei pacchetti



No.	Time	Source	Destination	Protocol	Length	Info
67	13.568966070	192.168.50.102	192.168.50.100	DNS	76	Standard q
68	13.902280219	192.168.50.102	192.168.50.100	TCP	66	49467 → 80
69	13.902310159	192.168.50.100	192.168.50.102	TCP	66	80 → 49467
70	13.902415833	192.168.50.102	192.168.50.100	TCP	66	49468 → 80
71	13.902423977	192.168.50.100	192.168.50.102	TCP	66	80 → 49468
72	13.902525691	192.168.50.102	192.168.50.100	TCP	60	49467 → 80
73	13.902863089	192.168.50.102	192.168.50.100	TCP	60	49468 → 80
74	13.906697250	192.168.50.102	192.168.50.100	HTTP	530	GET / HTTP
75	13.906718835	192.168.50.100	192.168.50.102	TCP	54	80 → 49468
76	13.955512675	192.168.50.100	192.168.50.102	TCP	204	80 → 49468
77	13.961187160	192.168.50.100	192.168.50.102	HTTP	312	HTTP/1.1 2

```
▸ Frame 1: 76 bytes on wire (608 bits), 76 b
▸ Ethernet II, Src: PCSSystemtec_a3:2f:ab (0
▸ Internet Protocol Version 4, Src: 192.168.
▸ User Datagram Protocol, Src Port: 56296, D
▸ Domain Name System (query)
```

```
0000  08 00 27 c9 0e da 08 00  27 a3 2f ab
0010  00 3e 5e 1c 00 00 80 11  f6 77 c0 a8
0020  32 64 db e8 00 35 00 2a  6b 80 14 e9
0030  00 00 00 00 00 00 07 62  65 61 63 6f
0040  76 74 32 03 63 6f 6d 00  00 01 00 01
```