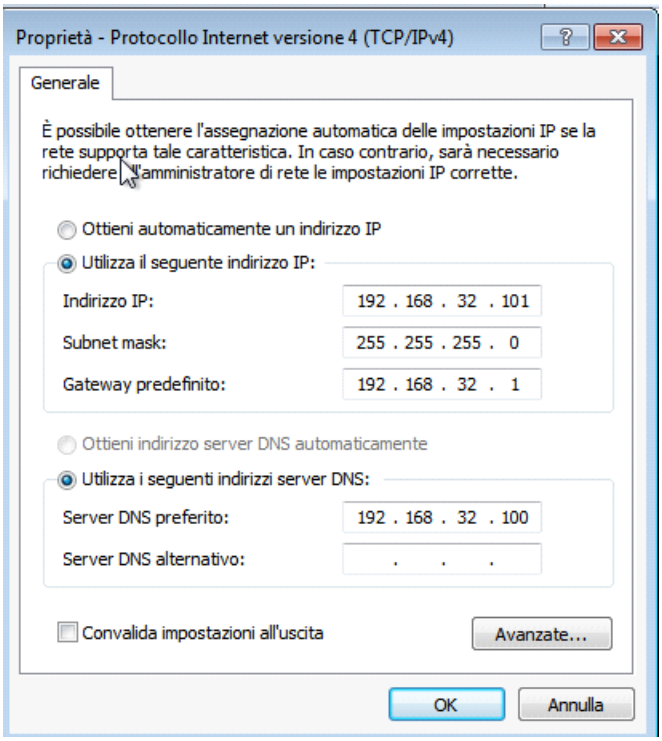
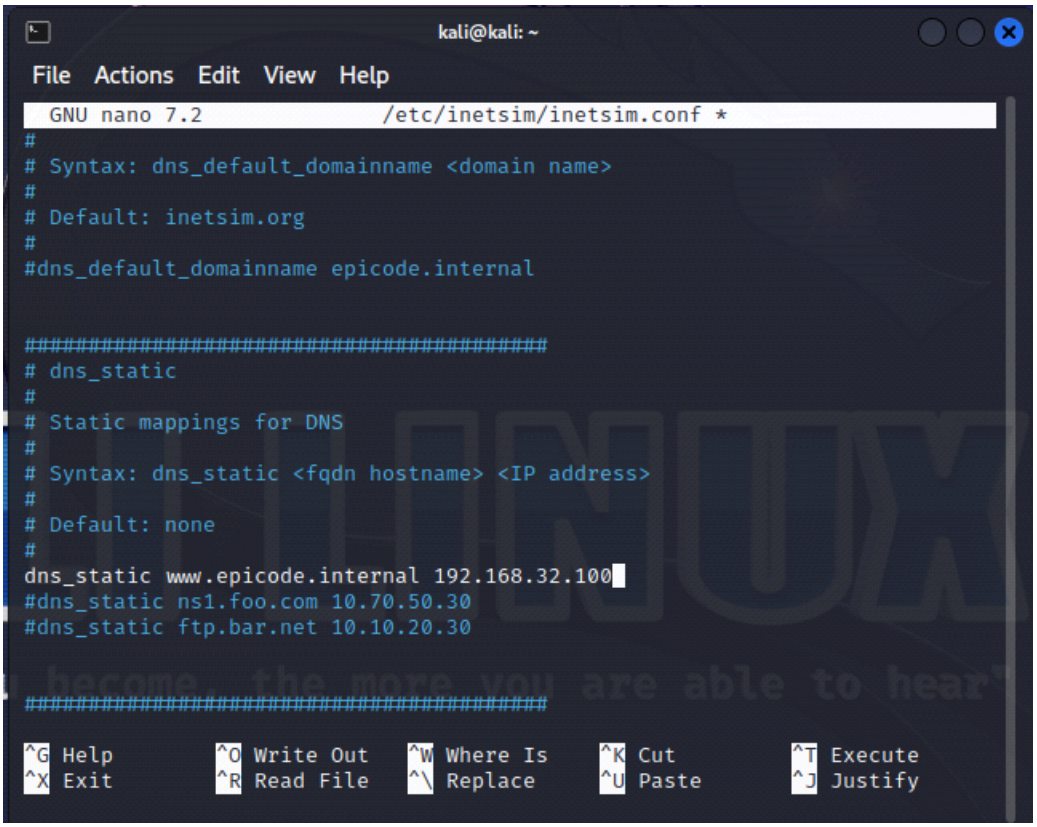
Simulazione servizi DNS, HTTPS, HTTP e utilizzo di Wireshark

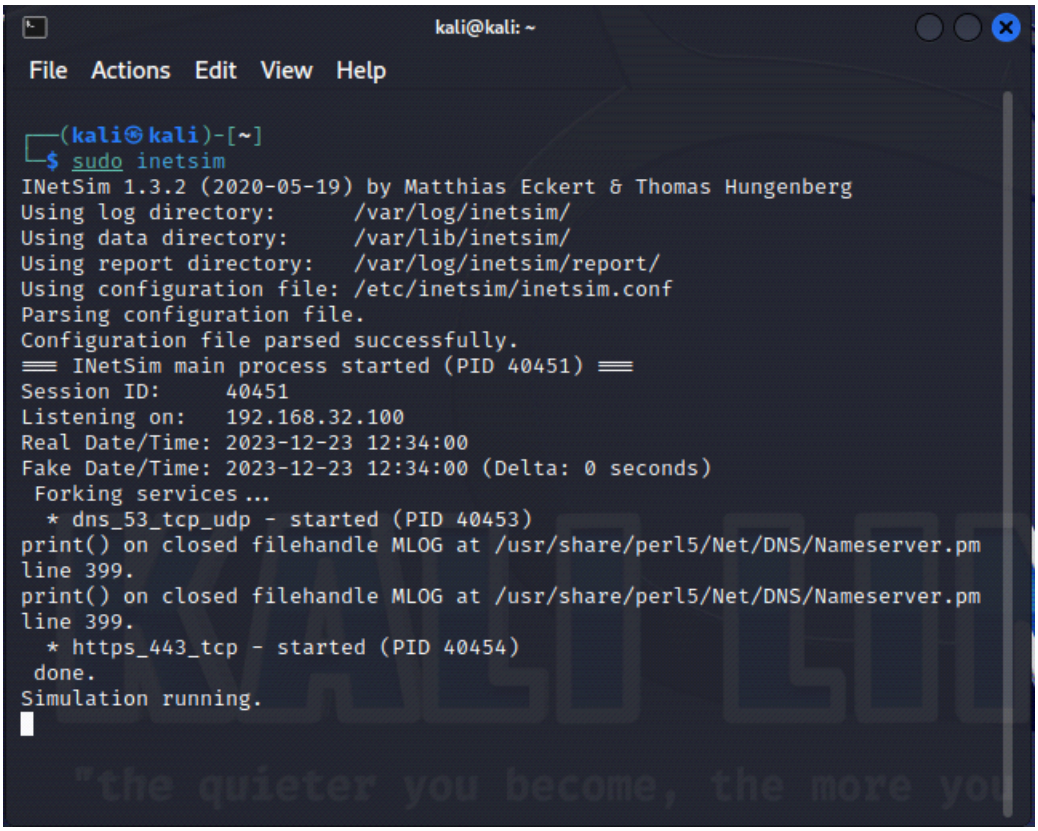
Prima di tutto si sono configurati gli IP per l'esercizio su Kali e Windows 7 , inoltre su quest'ultimo si è iserito l'indirizzo del server DNS che verrà successivamente simulato su Kali.

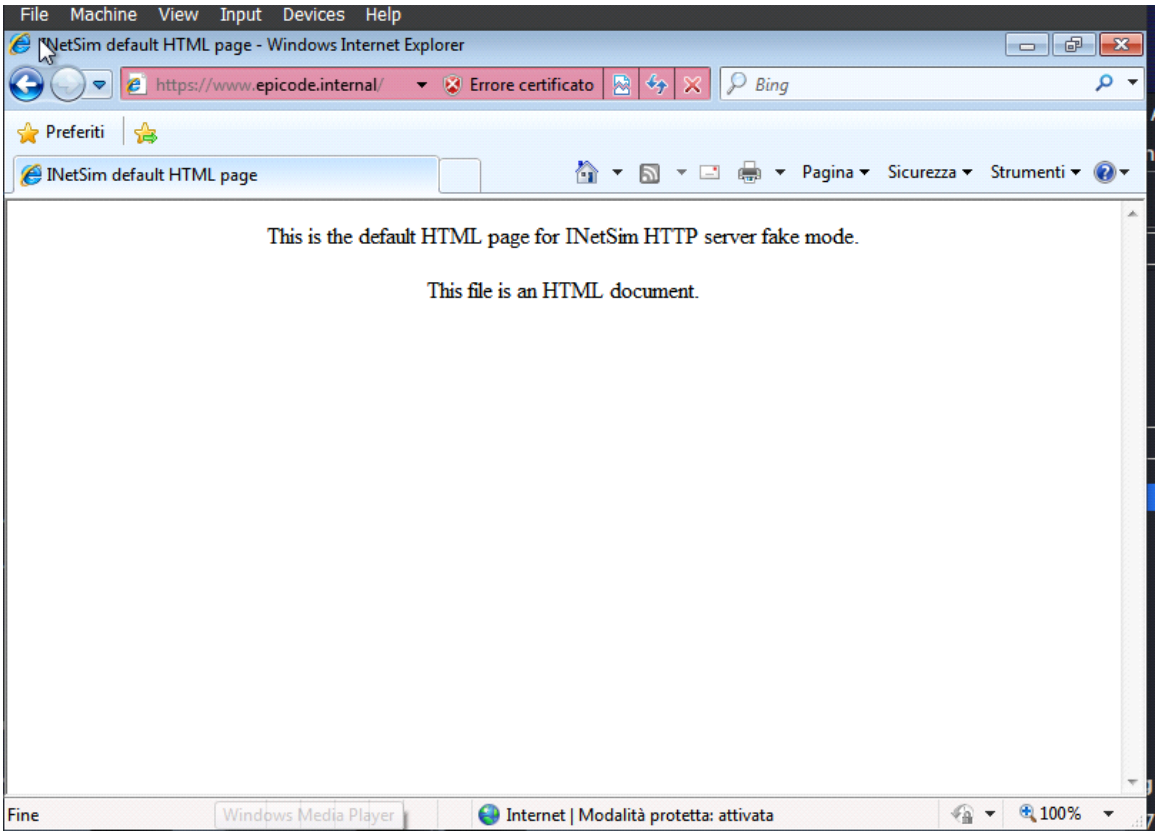


Su Kali si è poi configurato il servizio di DNS con assegnazione dell'indirizzo IP 192.168.32.100 alla risorsa www.epicode.internal

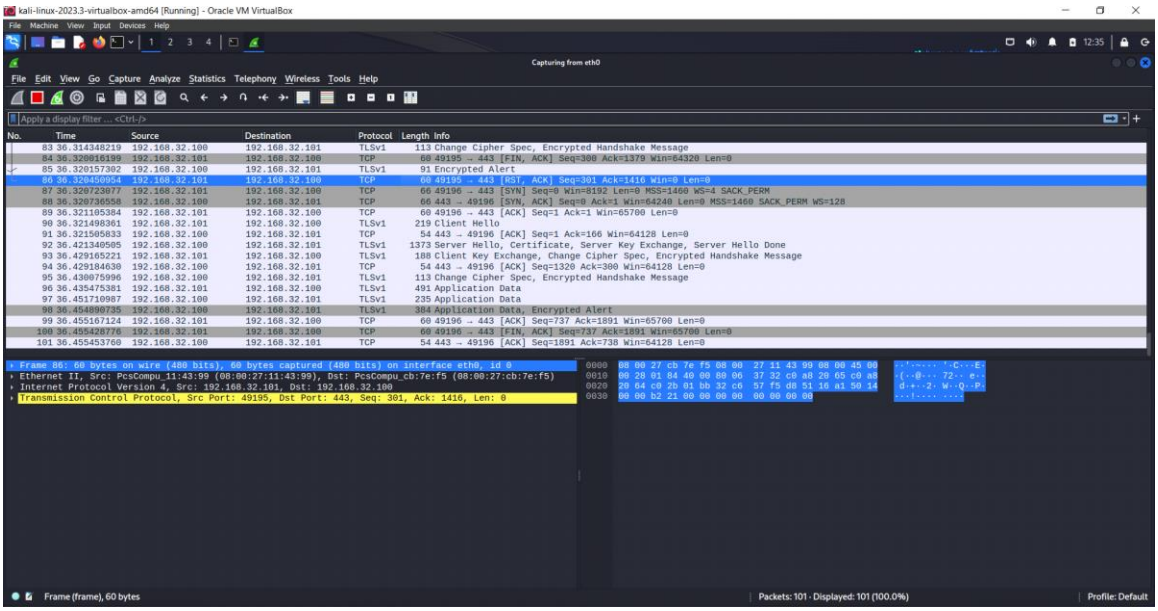


Poi si è simulato un servizio HTTPS dalla macchina Kali e si è fatta una richiesta dalla macchina Windows 7 per la risorsa epicode.internal

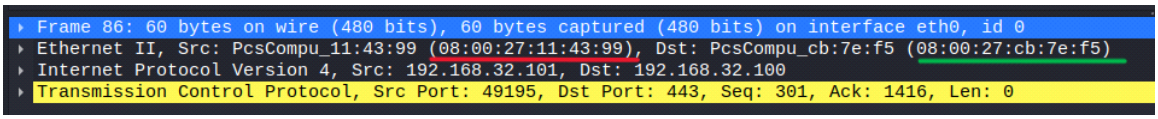

kali@kali: ~
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ sudo inetsim
INetSim 1.3.2 (2020-05-19) by Matthias Eckert & Thomas Hungenberg
Using log directory: /var/log/inetsim/
Using data directory: /var/lib/inetsim/
Using report directory: /var/log/inetsim/report/
Using configuration file: /etc/inetsim/inetsim.conf
Parsing configuration file.
Configuration file parsed successfully.
=== INetSim main process started (PID 40451) ===
Session ID: 40451
Listening on: 192.168.32.100
Real Date/Time: 2023-12-23 12:34:00
Fake Date/Time: 2023-12-23 12:34:00 (Delta: 0 seconds)
Forking services ...
* dns_53_tcp_udp - started (PID 40453)
print() on closed filehandle MLOG at /usr/share/perl5/Net/DNS/Nameserver.pm line 399.
print() on closed filehandle MLOG at /usr/share/perl5/Net/DNS/Nameserver.pm line 399.
* https_443_tcp - started (PID 40454)
done.
Simulation running.



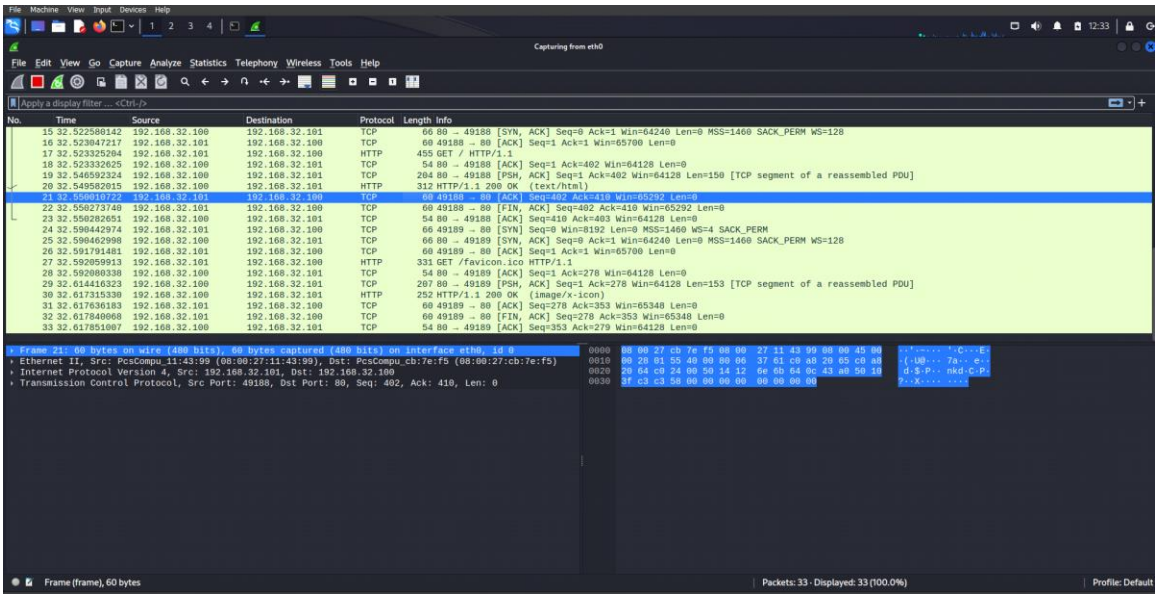
Si è poi utilizzato il tool Wireshark per la cattura e l'analisi dei pacchetti del traffico HTTPS



Nella figura che segue si può notare sottolineato in rosso l'indirizzo MAC della sorgente ed in verde l'indirizzo MAC del client che ha fatto la richiesta del servizio HTTPS



Si è poi effettuato lo stesso procedimento ma con un servizio HTTP, che ha restituito il seguente traffico



La differenza principale tra i due servizi si può notare nell'utilizzo del protocollo TLS all'interno del servizio HTTPS tramite il quale viene data più sicurezza al traffico e alla lettura dei pacchetti. Mentre utilizzando l'HTTP si può visualizzare il contenuto dei pacchetti non essendo protetti da alcun protocollo.