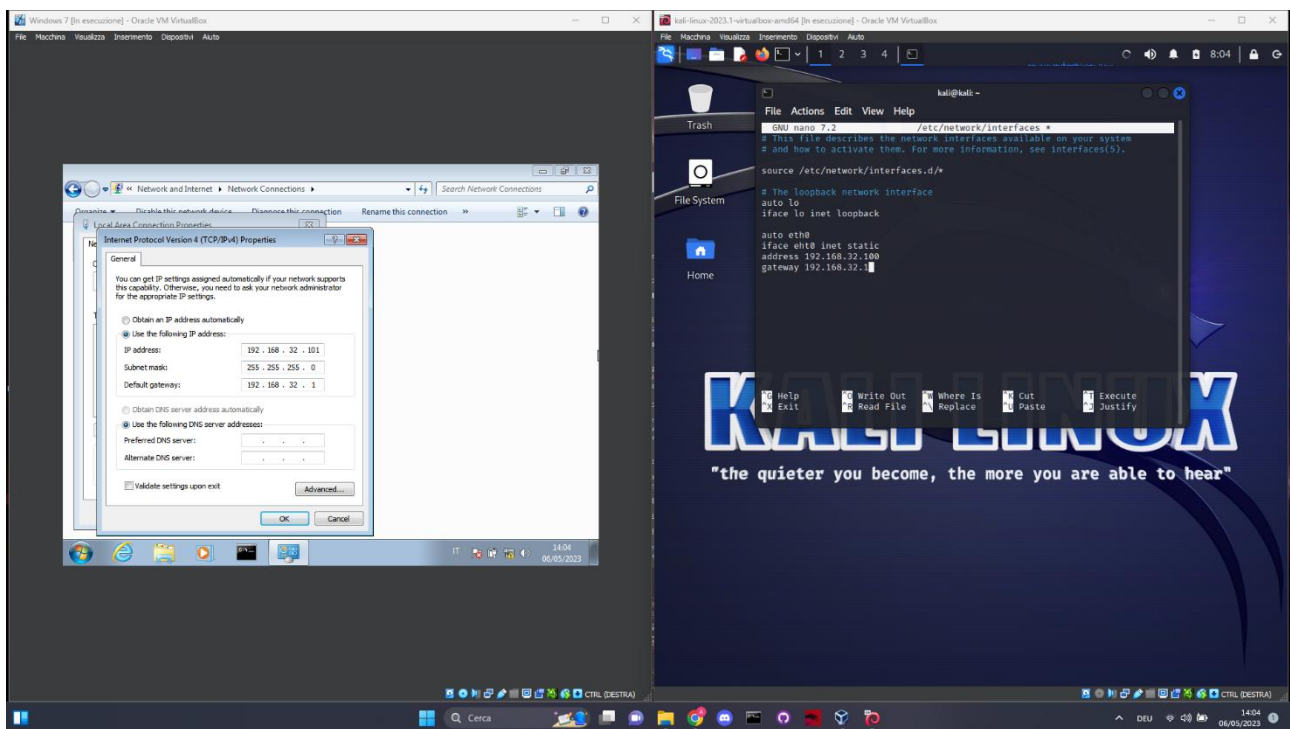
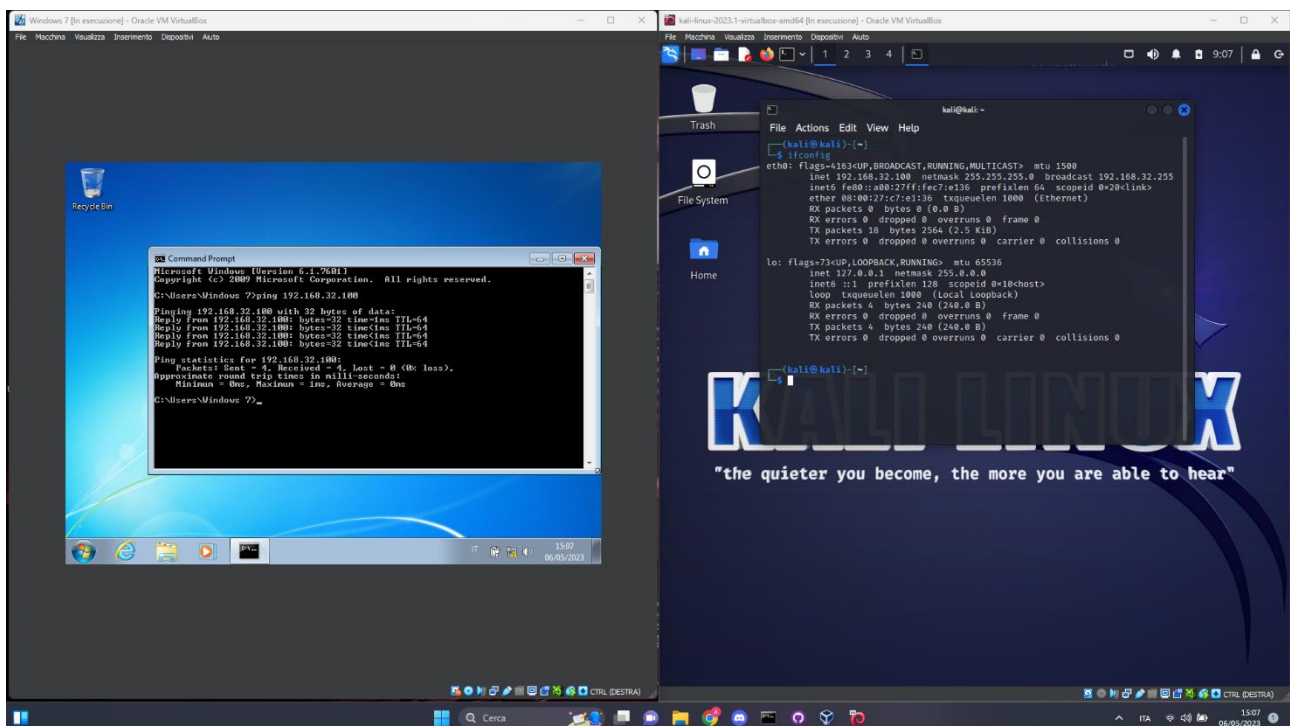


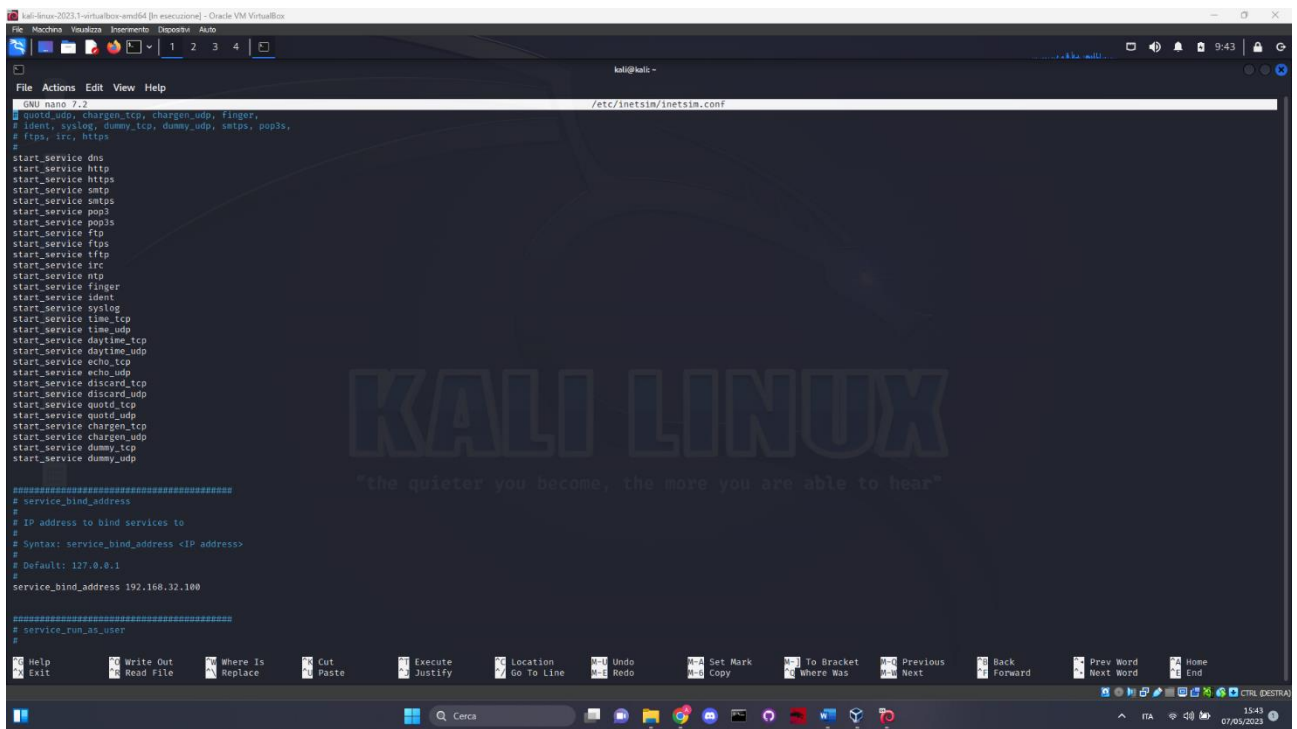
1. Il primo passaggio eseguito è stato il cambio dell'indirizzo IP delle macchine Kali Linux e Windows 7



2. Ho verificato il ping tra le due macchine



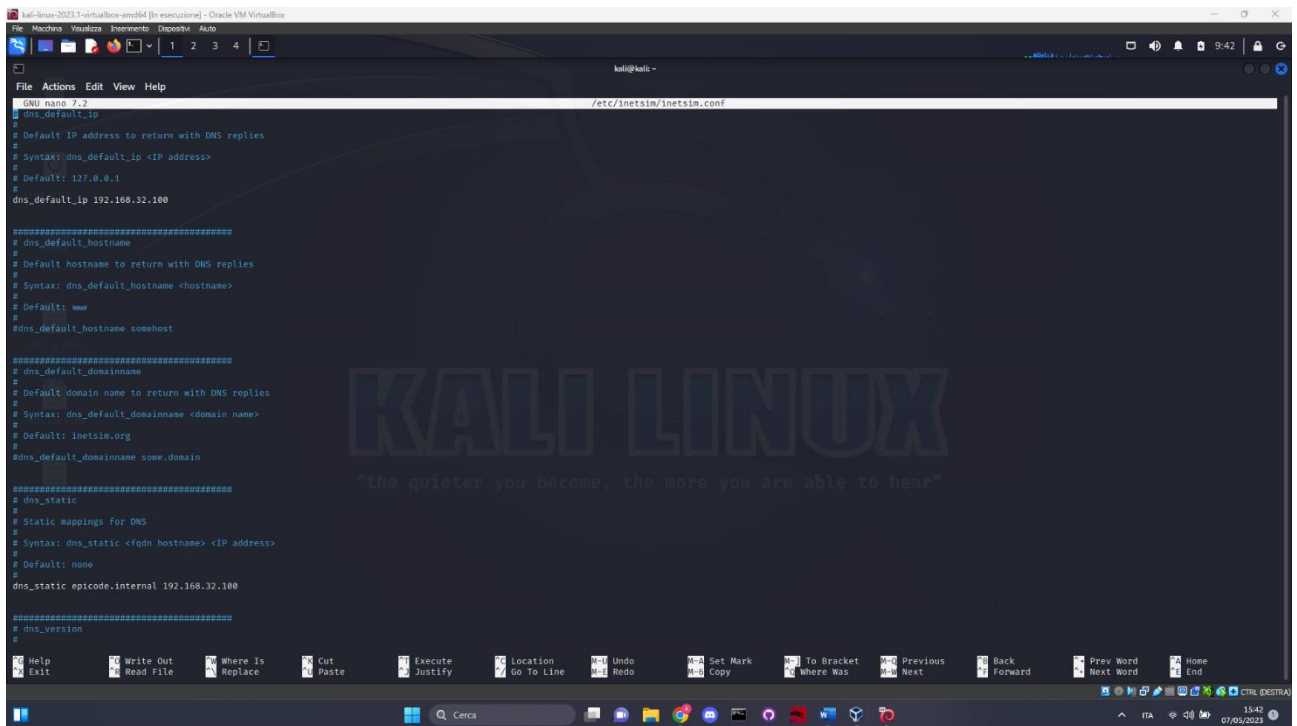
3. Ho attivato i server DNS, http e https e modificato i parametri DNS su inetsim.



```
GNU nano 2.2 /etc/inetsim/inetsim.conf
# Quoted udp, chargen_tcp, chargen_udp, finger,
# ident, syslog, dummy_tcp, dummy_udp, smtps, pop3s,
# ftps, irc, https
#
start_service dns
start_service http
start_service https
start_service smtp
start_service smtps
start_service pop3
start_service pop3s
start_service ftp
start_service tftp
start_service irc
start_service ntp
start_service mtp
start_service finger
start_service ident
start_service syslog
start_service time_tcp
start_service time_udp
start_service daytime_tcp
start_service daytime_udp
start_service echo_tcp
start_service echo_udp
start_service discard_tcp
start_service discard_udp
start_service quotd_tcp
start_service quotd_udp
start_service chargen_tcp
start_service chargen_udp
start_service dummy_tcp
start_service dummy_udp

=====
# service_bind_address
#
# IP address to bind services to
#
# Syntax: service_bind_address <IP address>
#
# Default: 127.0.0.1
#
service_bind_address 192.168.32.100

=====
# service_run_as_user
#
```



```
GNU nano 2.2 /etc/inetsim/inetsim.conf
# dns_default_ip
#
# Default IP address to return with DNS replies
#
# Syntax: dns_default_ip <IP address>
#
# Default: 127.0.0.1
#
dns_default_ip 192.168.32.100

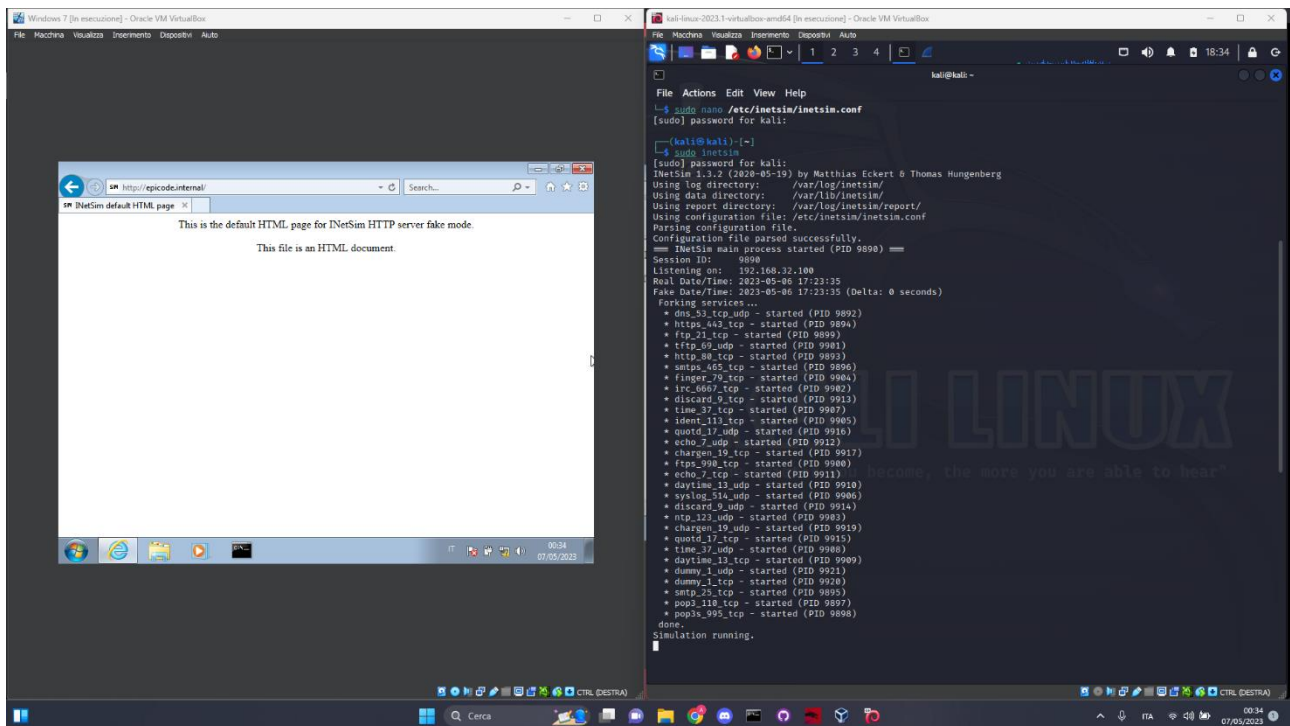
=====
# dns_default_hostname
#
# Default hostname to return with DNS replies
#
# Syntax: dns_default_hostname <hostname>
#
# Default: www
#
#dns_default_hostname somehost

=====
# dns_default_domainname
#
# Default domain name to return with DNS replies
#
# Syntax: dns_default_domainname <domain name>
#
# Default: inetsim.org
#
#dns_default_domainname some.domain

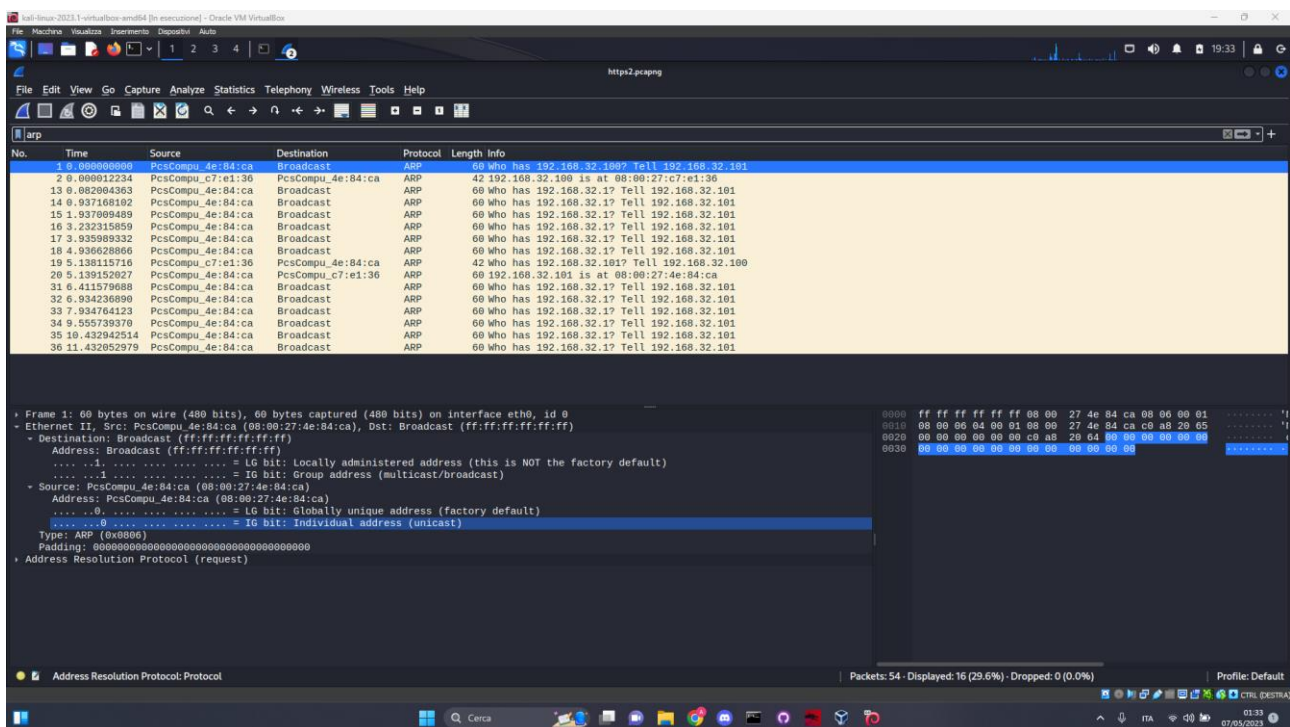
=====
# dns_static
#
# Static mappings for DNS
#
# Syntax: dns_static <fqdn hostname> <IP address>
#
# Default: none
#
dns_static epicode.internal 192.168.32.100

=====
# dns_version
#
```

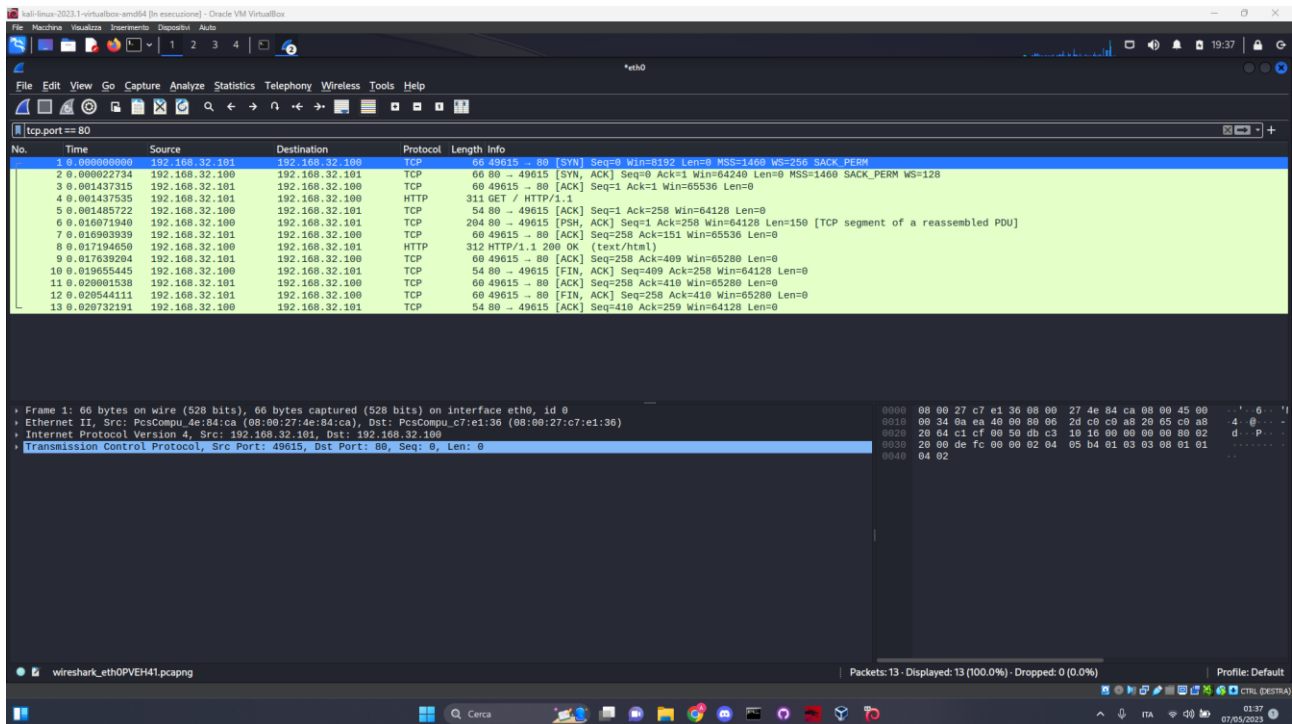
4. Ho iniziato la simulazione del server di inetsim e verificato che `epicode.internal` rispondesse all'indirizzo `192.168.32.100`



5. Dopo aver intercettato il traffico della richiesta https, ho filtrato il protocollo ARP per evidenziare i MAC di sorgente e destinazione del contenuto.



6. Ho ripetuto l'esercizio sostituendo il server https con uno http. Ho intercettato il traffico tramite l'utilizzo di Wireshark e filtrato con `tcp.port == 80`, la porta usata dal protocollo http.



7. Come possiamo vedere dalla schermata qui sopra e in quella successiva a questo testo, le principali differenze sono: ovviamente l'utilizzo di porte diverse e una maggiore sicurezza del server https. Questo è crittografato e durante l'intercettamento dei pacchetti con Wireshark ho ricevuto come risposta un Encryption Alert, a differenza del protocollo http dove ho ricevuta risposta con codice numerico 200 OK, ovvero risorsa trovata.

