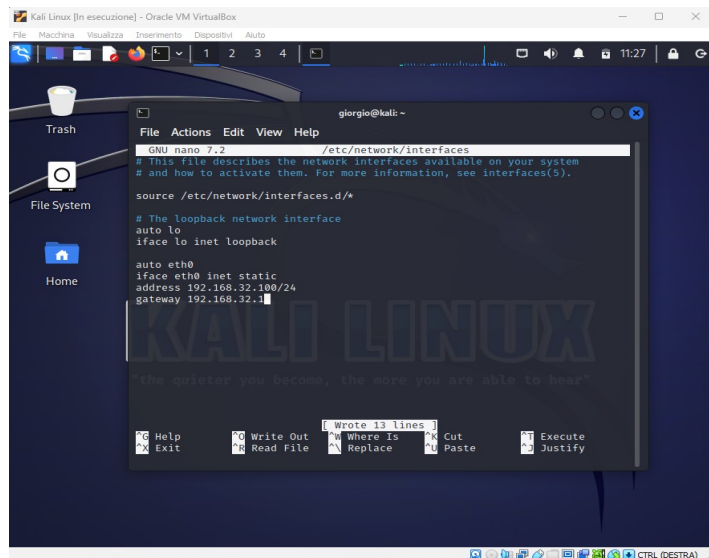


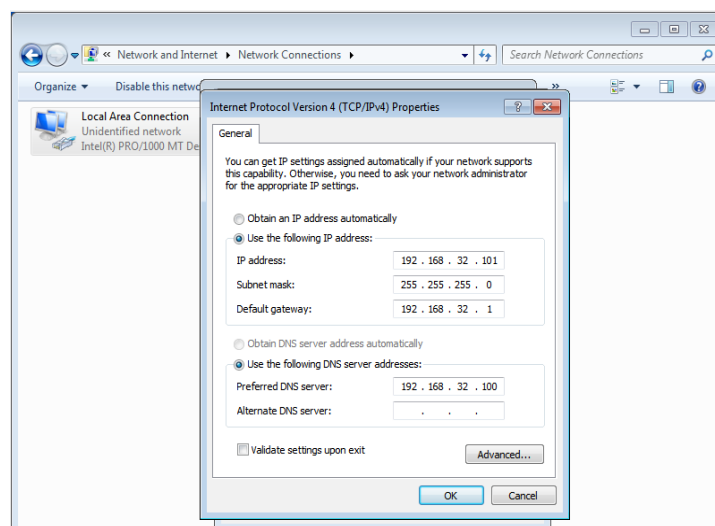
# PROGETTO S1/L5

## ESERCITAZIONE TRA CLIENT (WINDOWS 7) E SERVER (KALI LINUX)

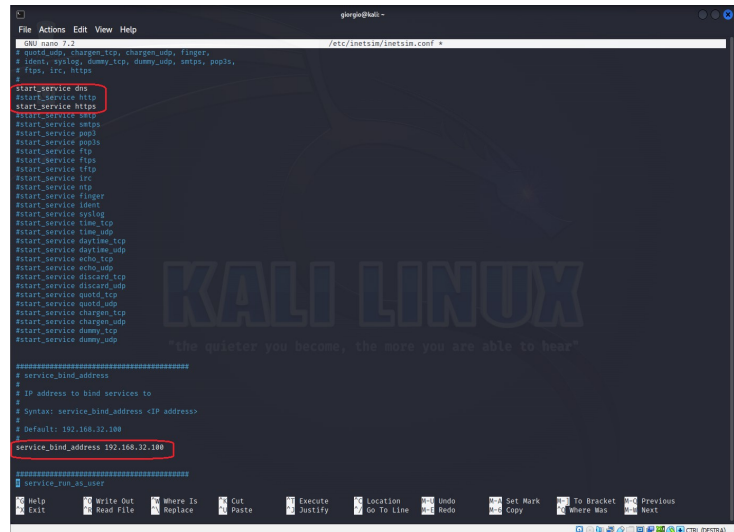
### 1. Settaggio IP su Kali



### 2. Settaggio IP su Windows 7



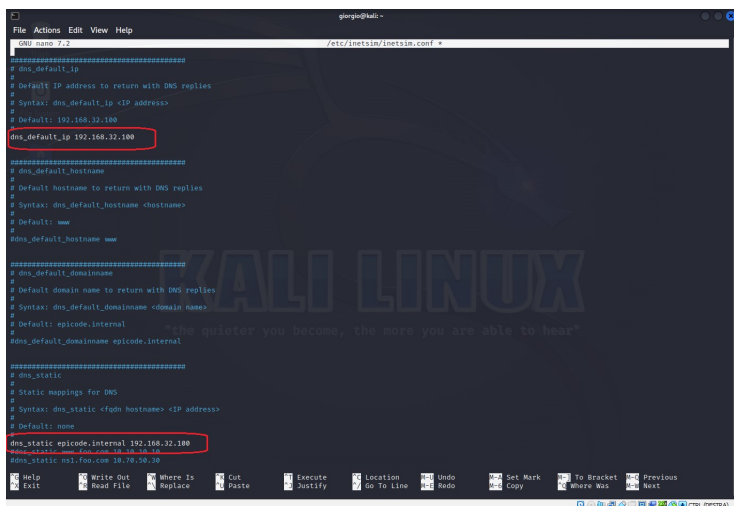
### 3. Attivazione servizio HTTPS e DNS



```
File Actions Edit View Help
GNU nano 2.2 /etc/inetSim/inetSim.conf
# quod_udp, chargen_tcp, chargen_udp, finger,
# dsnm, syslog, dummy_tcp, dummy_udp, snmp, pop3,
# ftp, irc, https
#
start_service dnsmasq
start_service httpd
start_service httpsd
start_service snmp
start_service pop3
start_service ftp
start_service irc
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 quod_tcp
start_service quod_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: 192.168.32.100
service_bind_address 192.168.32.100

#####
# service_run_as_user
#
# Help
# Exit
# Write Out
# Read File
# Where Is
# Replace
# Cut
# Paste
# Execute
# Justify
# Location
# Go To Line
# Undo
# Redo
# Set Mark
# Copy
# To Bracket
# Where Was
# Previous
# Next
CTRL EXTRAS
```



```
File Actions Edit View Help
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: 192.168.32.100
dns_default_ip 192.168.32.100

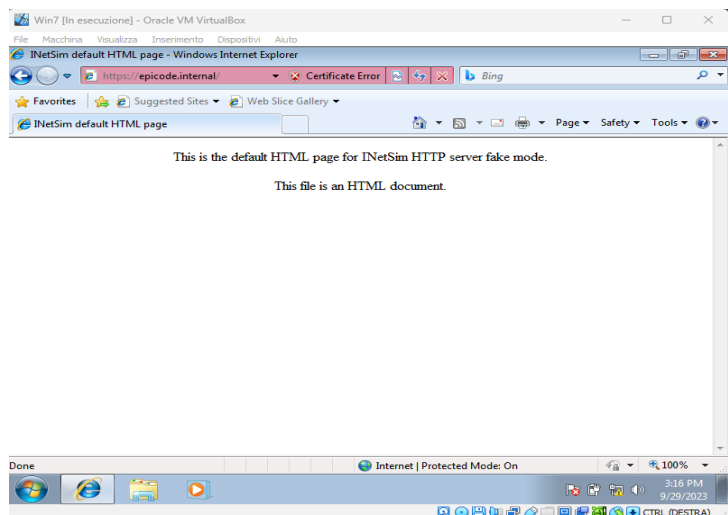
#####
# dns_default_hostname
#
# Default hostname to return with DNS replies
#
# Syntax: dns_default_hostname <hostname>
# Default: www
dns_default_hostname www

#####
# dns_default_domainname
#
# Default domain name to return with DNS replies
#
# Syntax: dns_default_domainname <domain name>
# Default: epicode.internal
dns_default_domainname epicode.internal

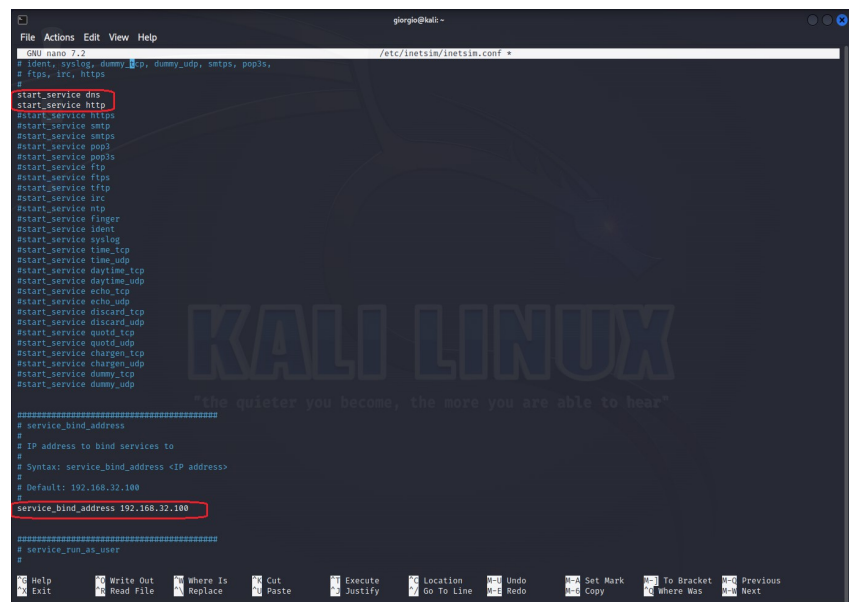
#####
# dns_static
#
# Static mappings for DNS
#
# Syntax: dns_static <fqdn hostname> <IP address>
# Default: none
dns_static epicode.internal 192.168.32.100
# dns_static mal.foo.com 38.79.29.28

#####
# Help
# Exit
# Write Out
# Read File
# Where Is
# Replace
# Cut
# Paste
# Execute
# Justify
# Location
# Go To Line
# Undo
# Redo
# Set Mark
# Copy
# To Bracket
# Where Was
# Previous
# Next
CTRL EXTRAS
```

### 4. Richiesta pagina tramite Web Browser Windows 7



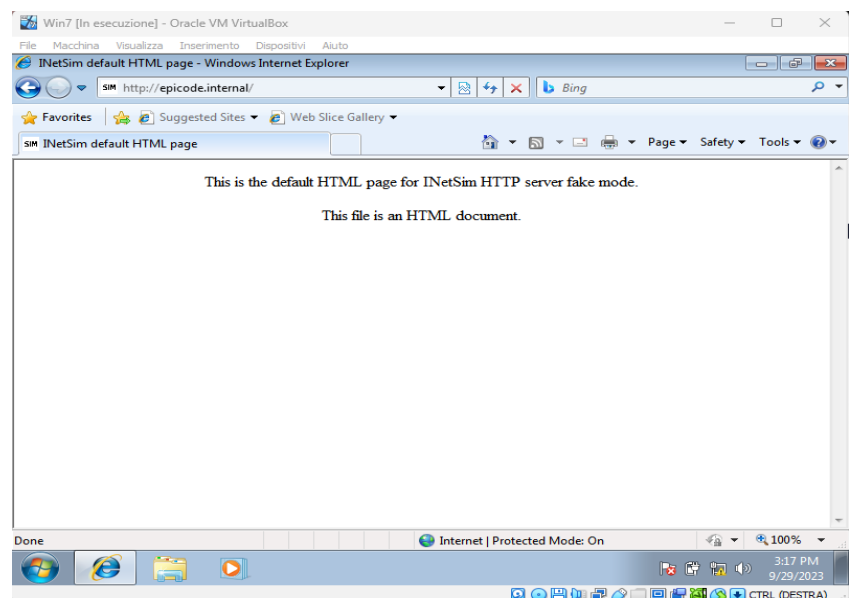
## 5. Attivazione servizio HTTP e DNS



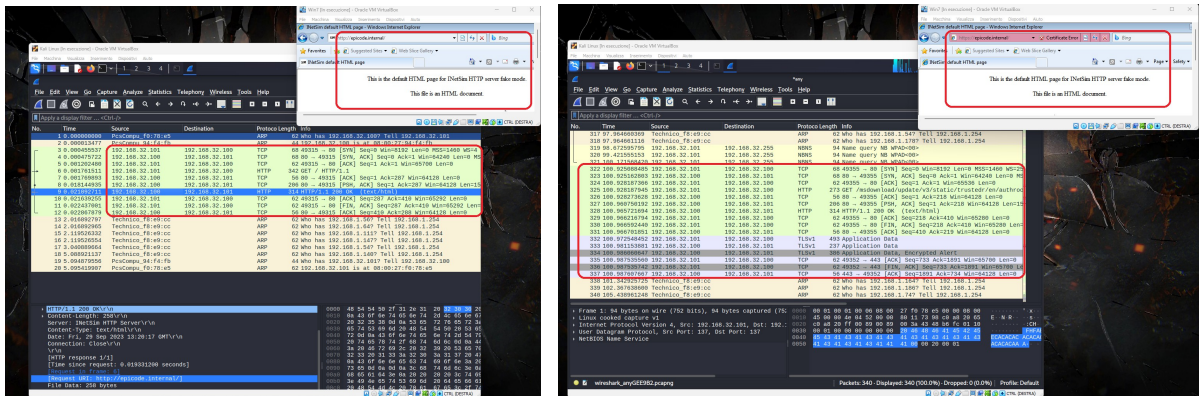
```
File Actions Edit View Help
GNU nano 7.2 /etc/inetd.conf
# ident, syslog, dummy, ftp, dummy_udp, smtp, pop3,
# ftps, irc, https
#
start_service dns
start_service http
start_service https
start_service smtp
start_service smtps
start_service pop3
start_service pop3s
start_service ftp
start_service ftps
start_service tftp
start_service tftp
start_service ntp
start_service ntp
start_service finger
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: 192.168.32.100
#
service_bind_address 192.168.32.100
=====
# service_run_as_user
#
Help      Write Out  Where Is   Cut        Execute    Location  Undo       Set Mark   To Bracket Previous
Exit      Read File  Replace    Paste      Justify    Go To Line Redo       Copy       Where Was  Next
```

## 6. Richiesta pagina tramite Web Browser Windows 7



## 7. Analisi tramite l'utilizzo di Wireshark della comunicazione intercettata



*Conclusione: Tramite l'utilizzo dello strumento Wireshark è possibile constatare la crittografia applicata al protocollo HTTPS, osservando l'immagine di destra si evince in particolare il protocollo TLS non presente con quello HTTP.*