

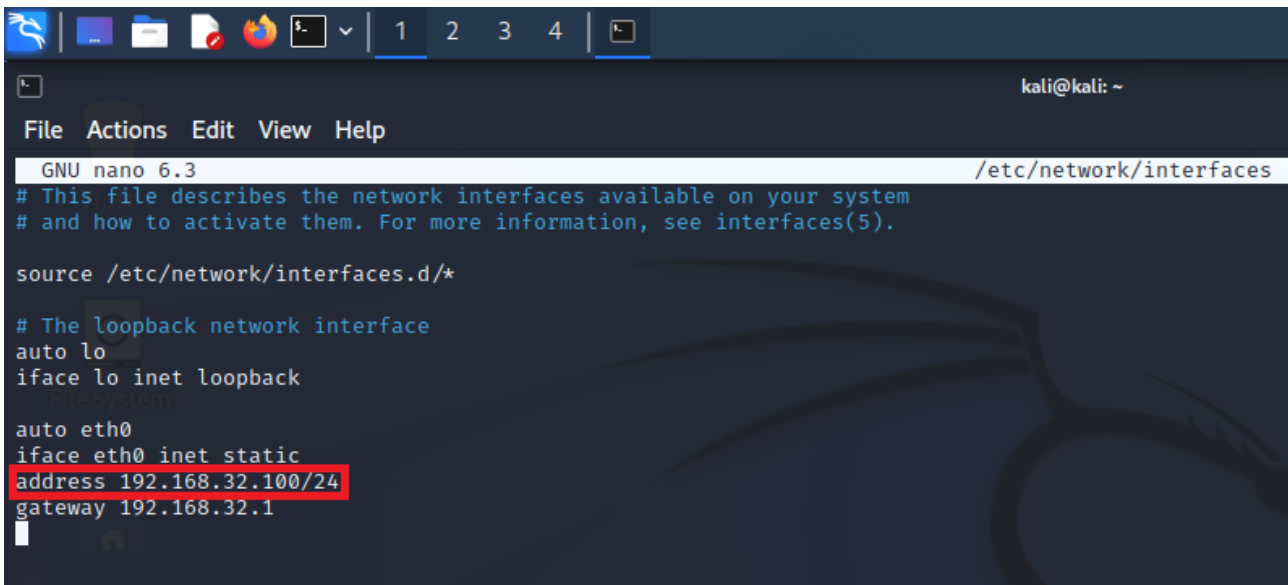
## SIMULAZIONE DI UN'ARCHITETTURA DI RETE CLIENT/SERVER E INTERCETTAZIONE DEL TRAFFICO DI RETE SU SERVER HTTPS E HTTP CON WIRESHARK

### Azioni richieste:

1. Assegnare l'indirizzo IP 192.168.32.100 alla macchina Kali Linux e configurare INetSim con i servizi HTTPS, HTTP e DNS
2. Assegnare l'indirizzo IP 192.168.32.101 alla macchina Windows 7
3. Navigazione web su epicode.internal da macchina Windows 7 su server HTTPS e HTTP
4. Intercettazione del traffico di rete con Wireshark
5. Identificazione e verifica degli indirizzi MAC

### 1. Configurazione di Kali Linux

#### 1.1 Assegnazione dell'IP statico 192.168.32.100



```

kali@kali: ~
File Actions Edit View Help
GNU nano 6.3 /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
address 192.168.32.100/24
gateway 192.168.32.1

```

#### 1.2 Configurazione INetSim:

- 1.2.1 Attivazione servizi HTTPS, HTTP e DNS: modifichiamo il file di configurazione di INetSim eseguendo il comando **sudo nano /etc/inetsim/inetsim.conf** per attivare i servizi di nostro interesse

```
kali@kali: ~
File Actions Edit View Help
GNU nano 6.3 /etc/inetsim/inetsim.conf *
#####
# Main configuration
#####
#
#####
# start_service
#
# The services to start
#
# Syntax: start_service <service name>
#
# Default: none
#
# Available service names are:
# dns, http, smtp, pop3, tftp, ftp, ntp, time_tcp,
# time_udp, daytime_tcp, daytime_udp, echo_tcp,
# echo_udp, discard_tcp, discard_udp, quotd_tcp,
# quotd_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
```

### 1.2.2 Configurazione server DNS per la risoluzione del nome di dominio **epicode.internal**

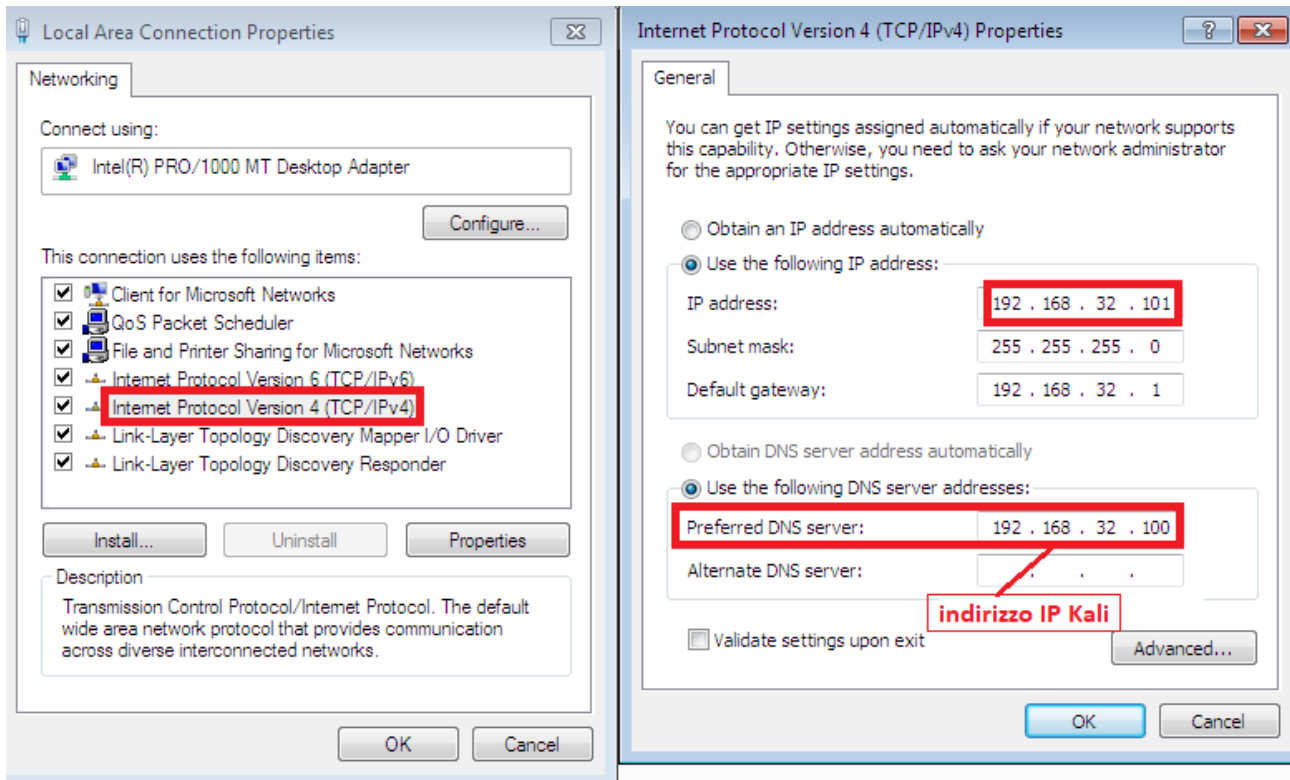
```
#####
# dns_static
#
# Static mappings for DNS
#
# Syntax: dns_static <fqdn hostname> <IP address>
#
# Default: none
#
#dns_static www.foo.com 10.10.10.10
#dns_static ns1.foo.com 10.70.50.30
#dns_static ftp.bar.net 10.10.20.30
dns_static epicode.internal 192.168.32.100
#####
```

### 1.2.3 Modifica del service bind address con il valore dell'IP precedentemente assegnato a Kali

```
#####
# 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
```

## 2. Configurazione delle impostazioni di rete sulla macchina Windows 7

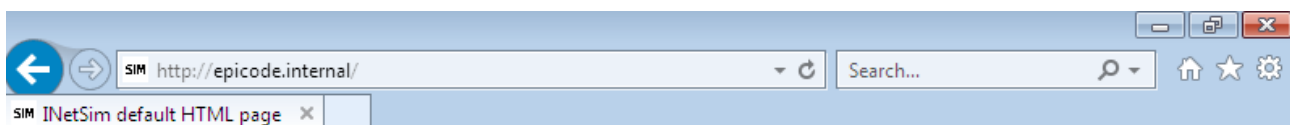
Modifichiamo le impostazioni di rete inserendo l'indirizzo IP richiesto 192.168.32.101 e inserendo l'IP di Kali come server DNS



## 3. Navigazione web su epicode.internal da macchina Windows 7 su server HTTPS e HTTP



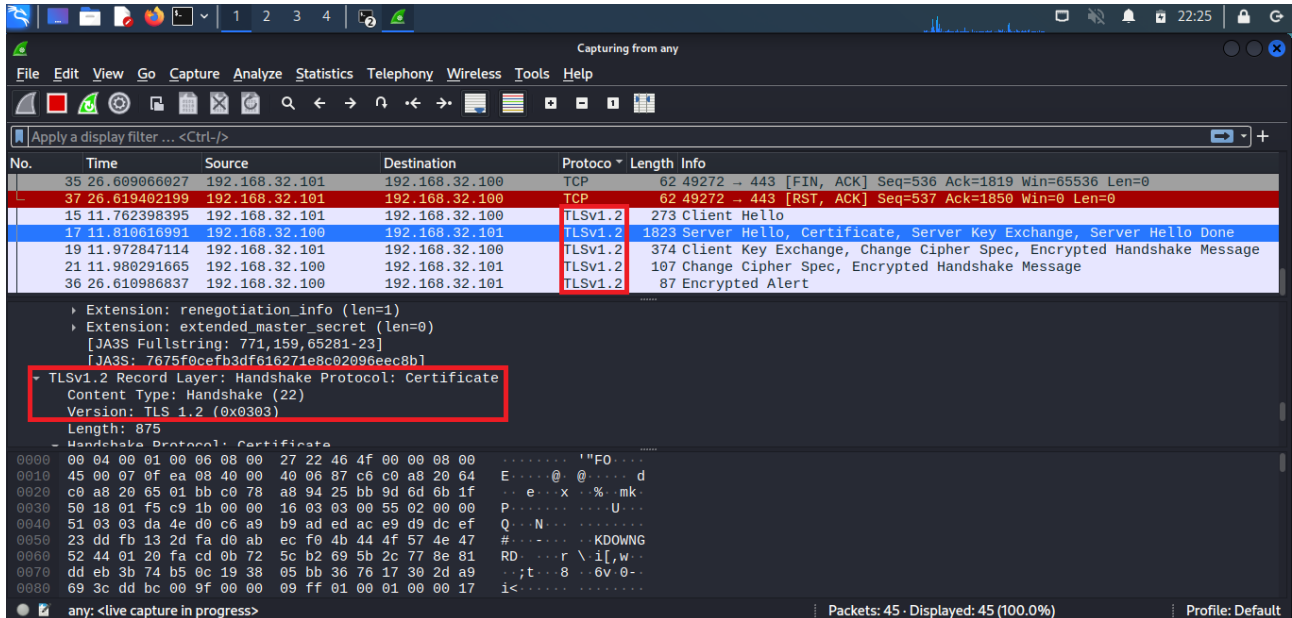
This file is an HTML document.



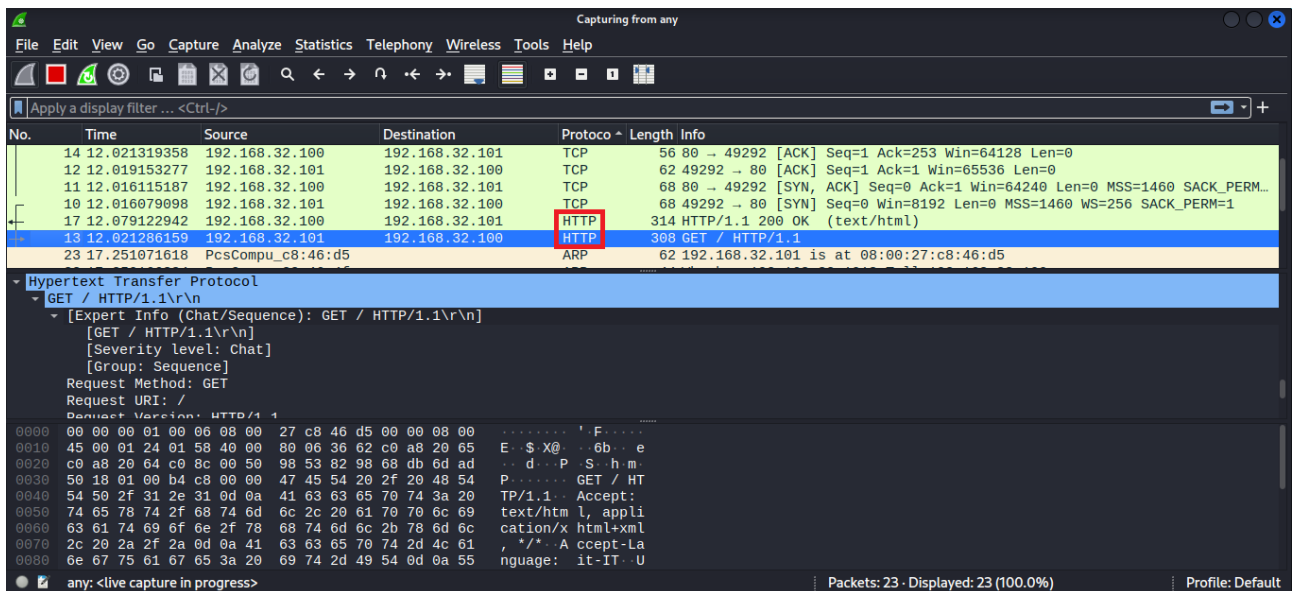
This file is an HTML document.

## 4. Intercettazione del traffico di rete con Wireshark

### 4.1 Cattura del traffico di rete – richiesta HTTPS



### 4.2 Cattura del traffico di rete – richiesta HTTP

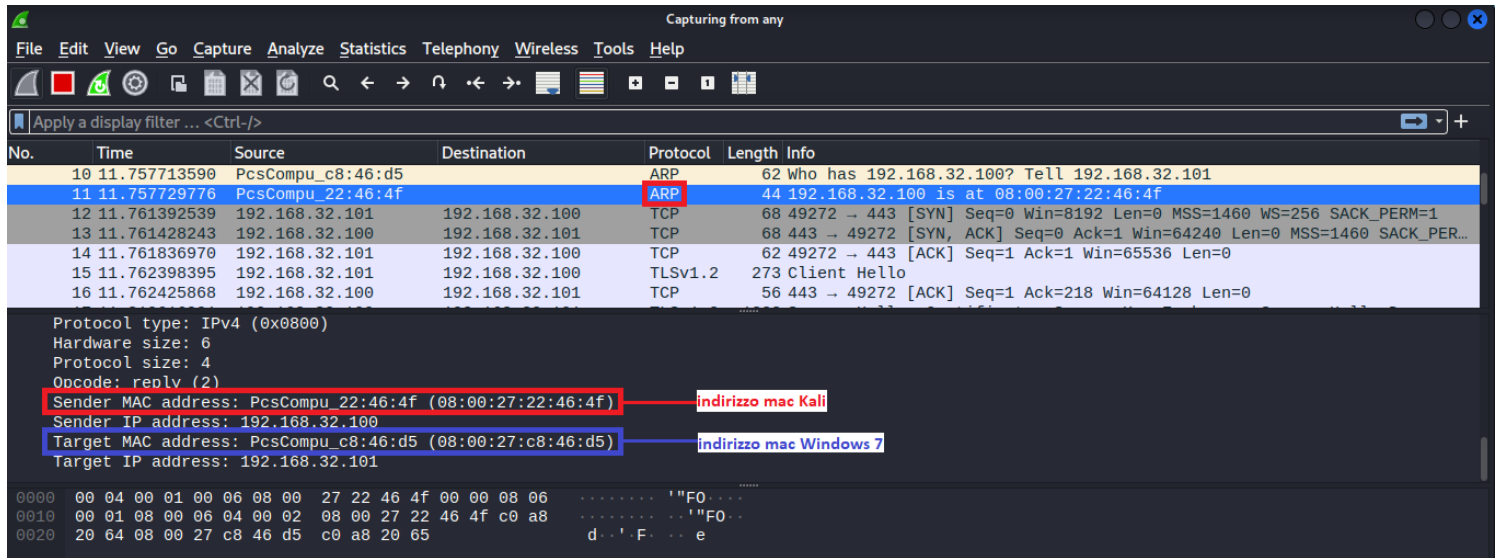


In entrambe le catture viene intercettato traffico con protocollo TCP e ARP. Inoltre, nella richiesta HTTP vengono catturati pacchetti con protocollo HTTP, mentre nella richiesta HTTPS questi ultimi sono sostituiti da pacchetti con protocollo TLS, il che ci dà evidenza della crittografia dei dati scambiati che caratterizza le richieste HTTPS.

## 5. Identificazione e verifica degli indirizzi MAC

### 5.1 Identificazione

Nella figura seguente, è possibile rilevare gli indirizzi MAC di entrambe le macchine coinvolte: i dati sono inclusi all'interno del pacchetto ARP di risposta inviato da Kali a Windows 7 in seguito alla richiesta di quest'ultima macchina.



### 5.2 Verifica

Verifichiamo gli indirizzi MAC rilevati eseguendo il comando **ipconfig** da Windows e **ifconfig** da Kali

