

## Configurare inetsim su kali linux

```
start_service dns
#start_service http
start_service https
#start_service smtp
```

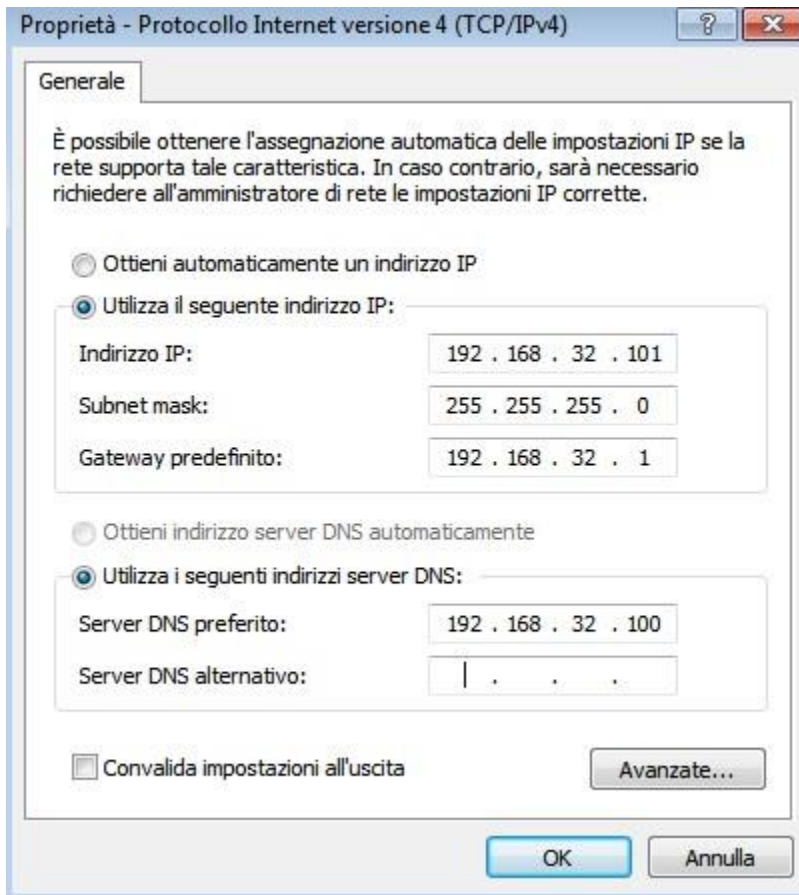
```
#####
# service_bind_address
#
# IP address to bind services to
#
# Syntax: service_bind_address <IP address>
#
# Default: 127.0.0.1
#
service_bind_address 192.168.32.100
```

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

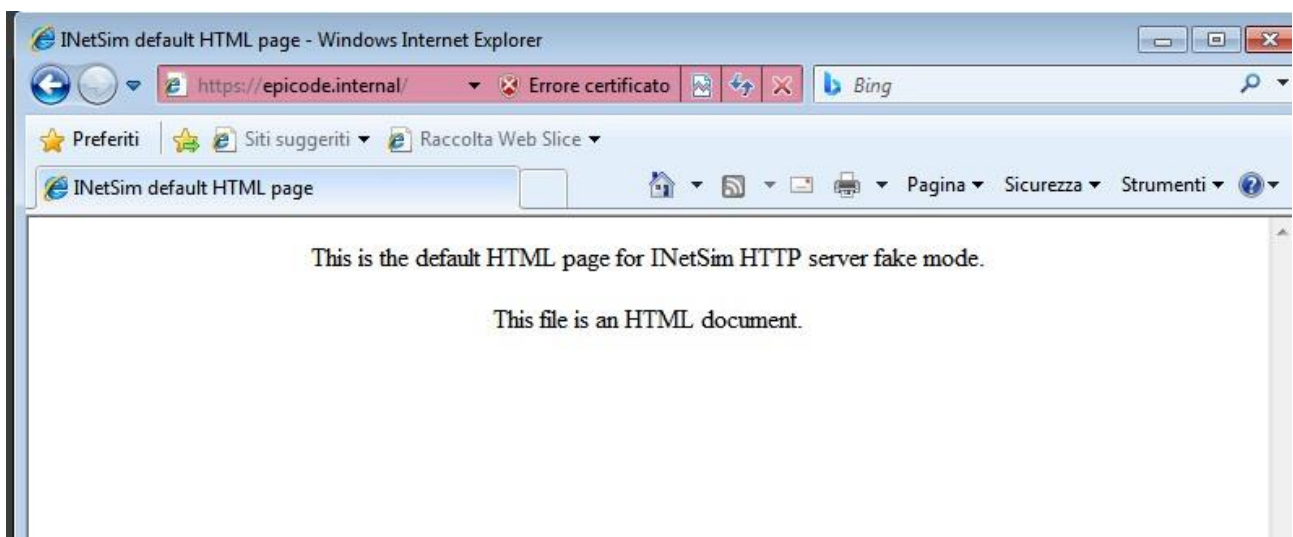
```
#####
# dns_default_domainname
#
# Default domain name to return with DNS replies
#
# Syntax: dns_default_domainname <domain name>
#
# Default: inetsim.org
#
dns_default_domainname epicode.internal

#####
# 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 ns1.foo.com 10.70.50.30
#dns_static ftp.bar.net 10.10.20.30
```

## Configurare windows 7



## Aprire il browser e inserire l'indirizzo https



Aprire wireshark su kali e vedere quanti pacchetti riesce a catturare dopo aver messo il link https su windows

The image shows the Wireshark network protocol analyzer interface. At the top, there's a menu bar with options like File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons for file operations and analysis. A search bar at the top of the packet list says "Apply a display filter ... <Ctrl-/>".

The main part of the interface is divided into two panes. The upper pane is the "Packet List" pane, which displays a table of captured packets. The lower pane is the "Packet Details" pane, which shows the hierarchical structure of the selected packet (packet 82).

**Packet List:**

No.	Time	Source	Destination	Protocol	Length	Info
79	205.190708883	PcsCompu_cc:7a:f4	Broadcast	ARP	60	Who has 192.
80	205.190722759	PcsCompu_6c:7f:7a	PcsCompu_cc:7a:f4	ARP	42	192.168.32.:
81	205.191433823	192.168.32.101	192.168.32.100	DNS	76	Standard que
82	205.191452391	192.168.32.100	192.168.32.101	ICMP	104	Destination
83	209.703316576	192.168.32.101	192.168.32.100	DNS	76	Standard que
84	209.703340651	192.168.32.100	192.168.32.101	ICMP	104	Destination
85	210.275368031	192.168.32.101	192.168.32.100	DNS	76	Standard que
86	210.275402640	192.168.32.100	192.168.32.101	ICMP	104	Destination
87	210.352229239	PcsCompu_6c:7f:7a	PcsCompu_cc:7a:f4	ARP	42	Who has 192.
88	210.352869478	PcsCompu_cc:7a:f4	PcsCompu_6c:7f:7a	ARP	60	192.168.32.:

**Packet Details (Packet 82):**

```

(1040 bits), 130 bytes captured (1040 bits) on interface eth0, id 0
3b:88:2d (08:00:27:8b:88:2d), Dst: IPv6mcast_16 (33:33:00:00:00:16)
Src: ::, Dst: ff02::16
Protocol v6
  
```

The bottom status bar shows "eth0: <live capture in progress>", "Packets: 145 · Displayed: 145 (100.0%)", and "Profile: Default".