

CONFIGURAZIONE SERVER E CLIENT

Kali (Server DNS, HTTP, HTTPS)

```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.32.100 netmask 255.255.255.0 broadcast 192.168.32.255  
    inet6 fe80::a00:27ff:fec7:e136 prefixlen 64 scopeid 0<link>  
    ether 08:00:27:c7:e1:36 txqueuelen 1000 (Ethernet)  
    RX packets 279 bytes 32888 (32.1 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 115 bytes 28759 (28.0 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 24 bytes 1240 (1.2 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 24 bytes 1240 (1.2 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Windows 7 (notare configurazione indirizzo IP server DNS)

```
C:\Windows\system32\cmd.exe  
Microsoft Windows [Version 6.1.7601]  
Copyright (c) 2009 Microsoft Corporation. All rights reserved.  
  
C:\Users\user>ipconfig /all  
  
Windows IP Configuration  
  
Host Name . . . . . : Windows  
Primary Dns Suffix . . . . . :  
Node Type . . . . . : Hybrid  
IP Routing Enabled. . . . . : No  
WINS Proxy Enabled. . . . . : No  
  
Ethernet adapter Local Area Connection:  
  
Connection-specific DNS Suffix . :  
Description . . . . . : Intel(R) PRO/1000 MT Desktop Adapter  
Physical Address. . . . . : 08-00-27-9B-CD-1D  
DHCP Enabled. . . . . : No  
Autoconfiguration Enabled . . . . : Yes  
Link-local IPv6 Address . . . . . : fe80::c949:a708:e4bd:7103%11(Preferred)  
IPv4 Address. . . . . : 192.168.32.101(Preferred)  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . : 192.168.32.1  
DHCPv6 IAID . . . . . : 235405351  
DHCPv6 Client DUID. . . . . : 00-01-00-01-2C-04-16-49-08-00-27-9B-CD-1D  
  
DNS Servers . . . . . : 192.168.32.100  
NetBIOS over Tcpip. . . . . : Enabled
```

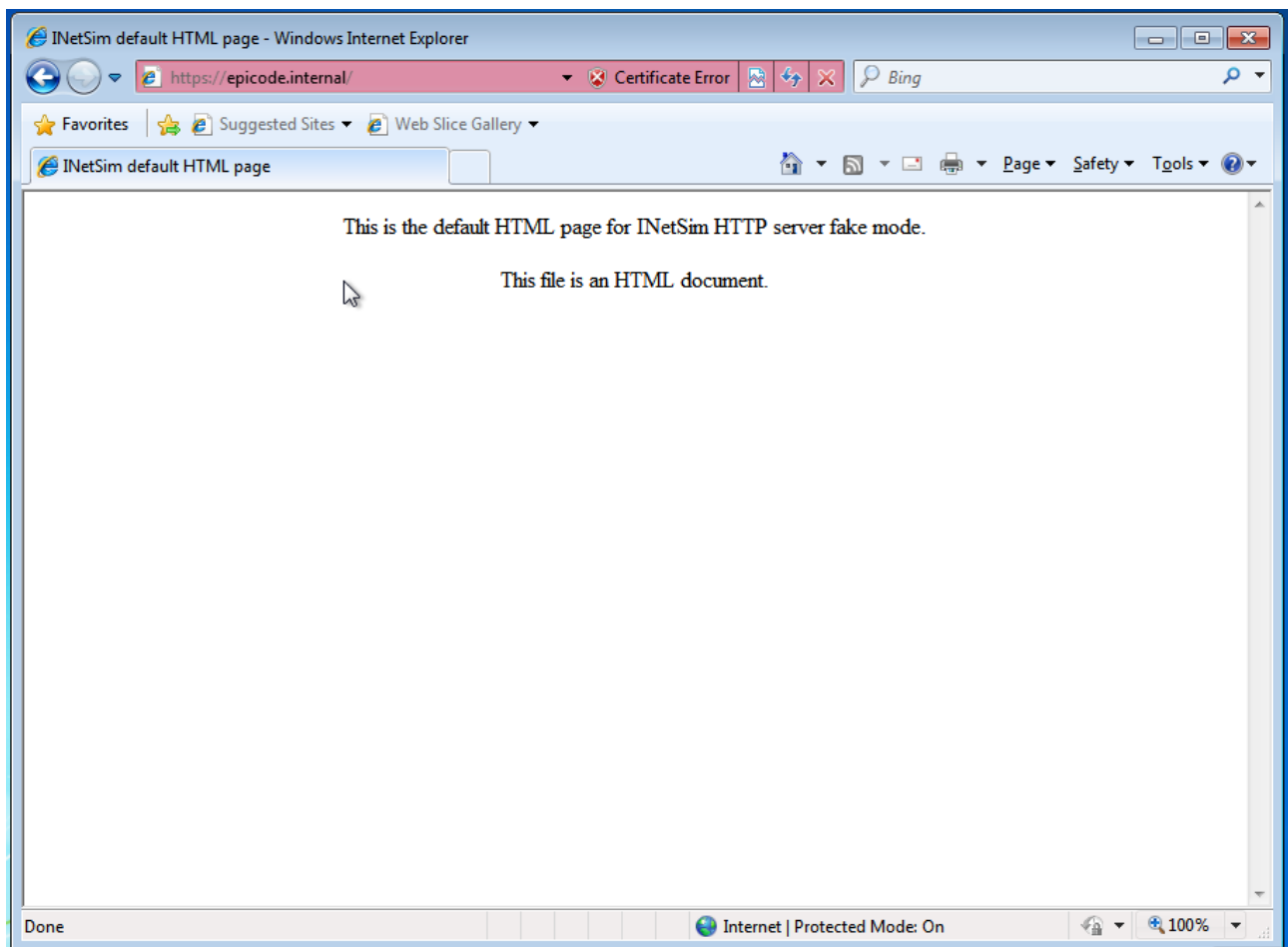
Configurazione hostname - indirizzo IP nel file di configurazione dell'utility Inetsim

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

AVVIO UTILITY INETSIM CON SERVIZI DI DNS E HTTPS

```
kali@kali: ~  
File Actions Edit View Help  
-(kali@kali)-[~]  
└─$ sudo inetsim  
[sudo] password for kali:  
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 1963) ==  
Session ID: 1963  
Listening on: 192.168.32.100  
Real Date/Time: 2023-06-18 10:38:27  
Fake Date/Time: 2023-06-18 10:38:27 (Delta: 0 seconds)  
Forking services ...  
  * dns_53_tcp_udp - started (PID 1965)  
  * https_443_tcp - started (PID 1966)  
done.  
Simulation running.  
█
```

RICHIESTA TRAMITE WEB BROWSER “epicode.internal”



INTERCETTAZIONE PACCHETTI CON WIRESHARK (HTTPS)

Wireshark interface showing network traffic capture on interface *eth0. The packet list displays 18 captured packets, including ARP requests, TCP SYN/ACK exchanges, and TLSv1 handshake messages.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	PcsCompu_9b:cd:1d	Broadcast	ARP	60	Who has 192.168.32.100? Tell 192.168.32.101
2	0.000019977	PcsCompu_c7:e1:36	PcsCompu_9b:cd:1d	ARP	42	192.168.32.100 is at 08:00:27:c7:e1:36
3	0.000191729	192.168.32.101	192.168.32.100	TCP	66	49221 → 443 [SYN] Seq=0 Win=8192 Len=0
4	0.000232556	192.168.32.100	192.168.32.101	TCP	66	443 → 49221 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0
5	0.000350267	192.168.32.101	192.168.32.100	TCP	60	49221 → 443 [ACK] Seq=1 Ack=1 Win=65535 Len=0
6	0.000681487	192.168.32.101	192.168.32.100	TLSv1	215	Client Hello
7	0.000700843	192.168.32.100	192.168.32.101	TCP	54	443 → 49221 [ACK] Seq=1 Ack=162 Win=65535 Len=0
8	0.033578664	192.168.32.100	192.168.32.101	TLSv1	1373	Server Hello, Certificate, Server Key Exchange, Change Cipher Spec, Encrypted Handshake
9	0.038578072	192.168.32.101	192.168.32.100	TLSv1	188	Client Key Exchange, Change Cipher Spec, Encrypted Handshake
10	0.039139453	192.168.32.100	192.168.32.101	TLSv1	113	Change Cipher Spec, Encrypted Handshake
11	0.041213534	192.168.32.101	192.168.32.100	TLSv1	395	Application Data
12	0.051913116	192.168.32.100	192.168.32.101	TLSv1	235	Application Data
13	0.053715433	192.168.32.100	192.168.32.101	TLSv1	384	Application Data, Encrypted Alert
14	0.053867332	192.168.32.101	192.168.32.100	TCP	60	49221 → 443 [ACK] Seq=637 Ack=1891 Win=65535 Len=0
15	0.053923990	192.168.32.101	192.168.32.100	TCP	60	49221 → 443 [FIN, ACK] Seq=637 Ack=1891 Win=65535 Len=0
16	0.053938430	192.168.32.100	192.168.32.101	TCP	54	443 → 49221 [ACK] Seq=1891 Ack=638 Win=65535 Len=0
17	5.055611964	PcsCompu_c7:e1:36	PcsCompu_9b:cd:1d	ARP	42	Who has 192.168.32.101? Tell 192.168.32.100
18	5.055803056	PcsCompu_9b:cd:1d	PcsCompu_c7:e1:36	ARP	60	192.168.32.101 is at 08:00:27:9b:cd:1d

Frame 3: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface eth0

Ethernet II, Src: PcsCompu_9b:cd:1d (08:00:27:9b:cd:1d), Dst: PcsCompu_c7:e1:36 (08:00:27:c7:e1:36)

Internet Protocol Version 4, Src: 192.168.32.101, Dst: 192.168.32.100

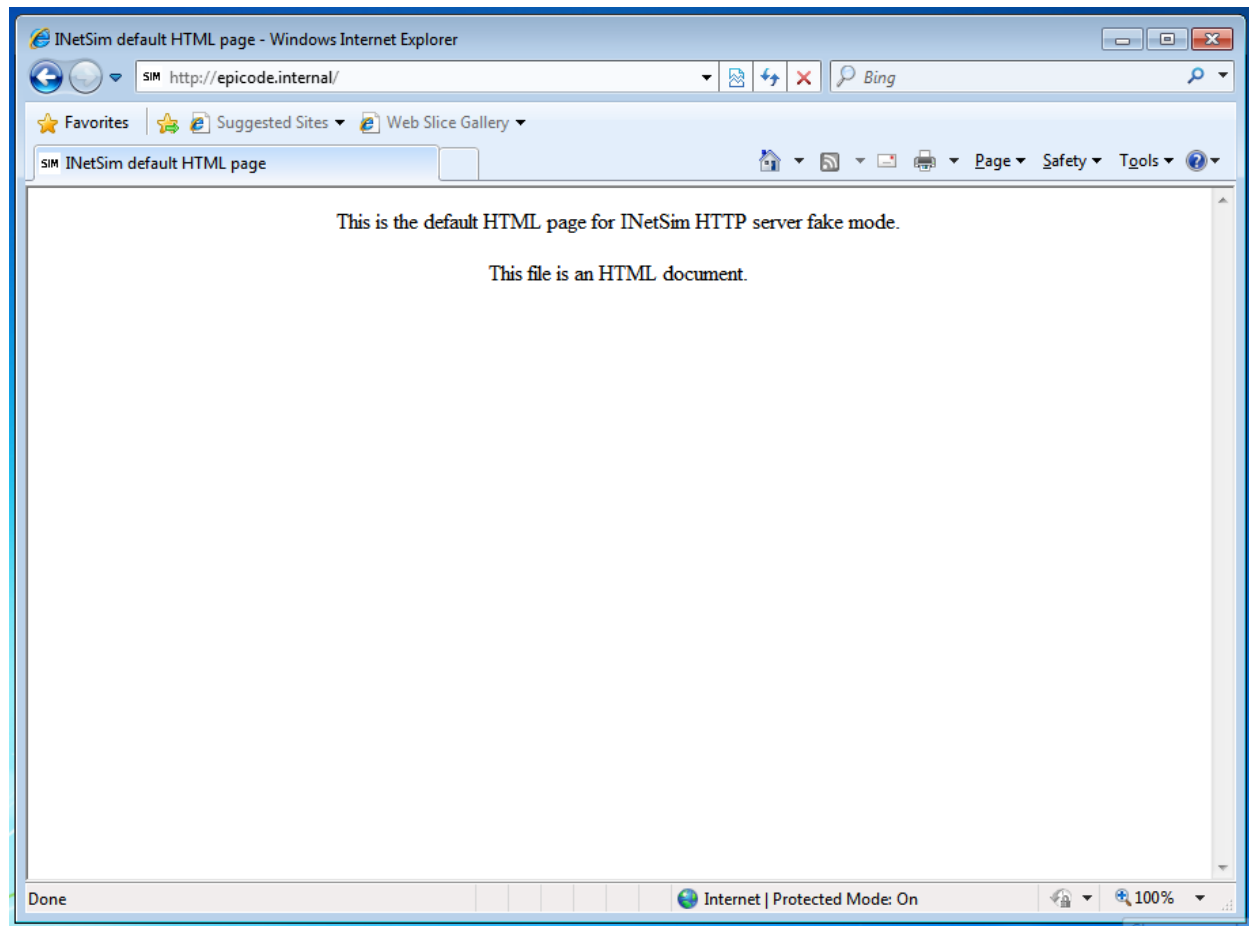
Transmission Control Protocol, Src Port: 49221, Dst Port: 443, Seq: 0, Len: 0

wireshark_eth0OIG61.pcapng | Packets: 18 · Displayed: 18 (100.0%) · Dropped: 0 (0.0%) | Profile: Default

AVVIO UTILITY INETSIM CON SERVIZI DI DNS E HTTP

```
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 4603) ==  
Session ID: 4603  
Listening on: 192.168.32.100  
Real Date/Time: 2023-06-18 13:41:37  
Fake Date/Time: 2023-06-18 13:41:37 (Delta: 0 seconds)  
Forking services ...  
* dns_53_tcp_udp - started (PID 4605)  
* http_80_tcp - started (PID 4606)  
done.  
Simulation running.  
█
```

RICHIESTA TRAMITE WEB BROWSER “epicode.internal”



INTERCETTAZIONE PACCHETTI CON WIRESHARK (HTTP)

[illegible]