

# Rapporto Server-Client in rete interna in HTTP

ASSEGNO GLI INDIRIZZI IP

Kali: ....32.100

Windows7: .....32.101

```
File Actions Edit View Help
zsh: corrupt history file /home/kali/.zsh_history
(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::50a8:c4c2:b70d:f025  prefixlen 64  scopeid 0x20<link>
    ether 08:00:27:1e:36:4a  txqueuelen 1000  (Ethernet)
    RX packets 96  bytes 8209 (8.0 KiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 51  bytes 9004 (8.7 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 0x10<host>
    loop txqueuelen 1000  (Local Loopback)
    RX packets 728  bytes 70016 (68.3 KiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 728  bytes 70016 (68.3 KiB)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

(kali@kali)-[~]
$
```

```

C:\Users\win7elle>ipconfig

Configurazione IP di Windows

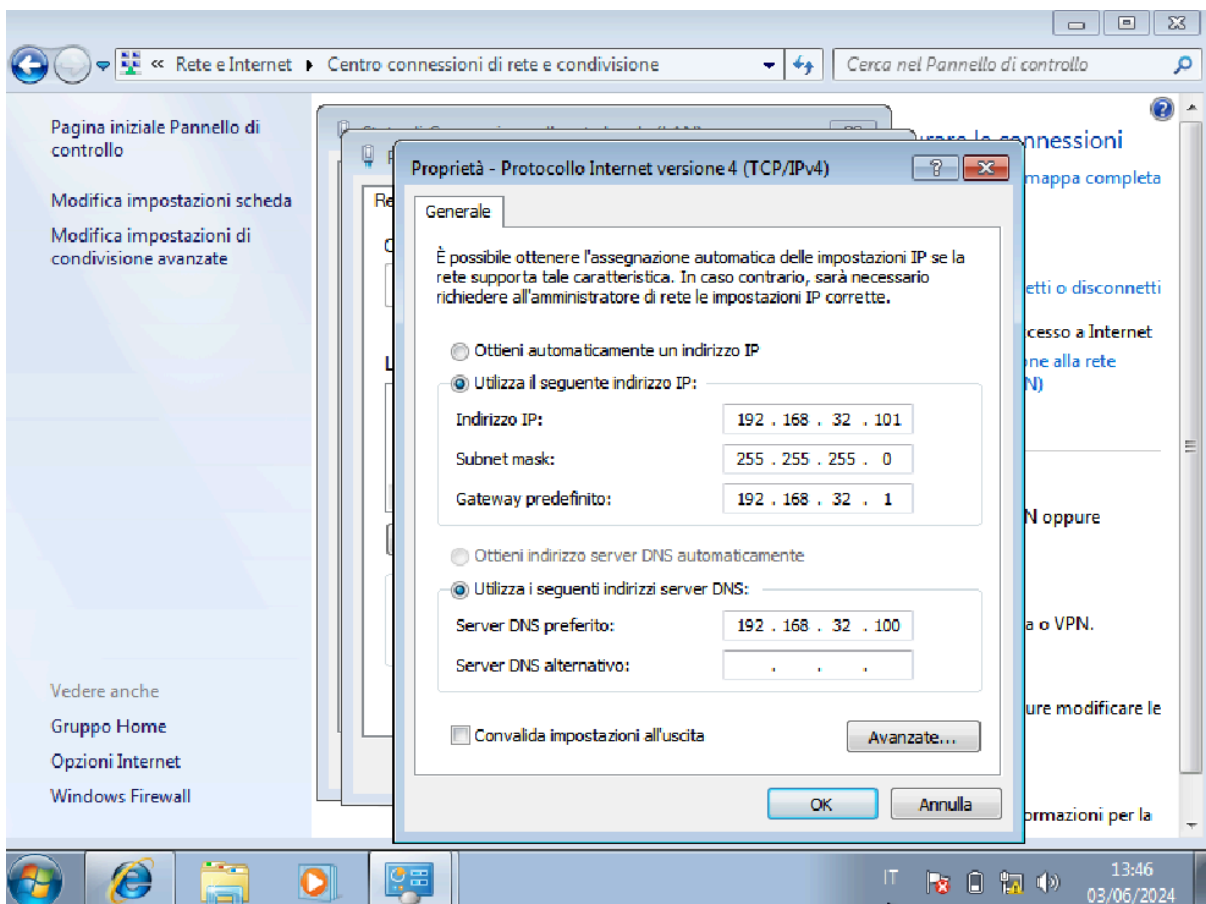
Scheda Ethernet Connessione alla rete locale (LAN):

    Suffisso DNS specifico per connessione:
    Indirizzo IPv6 locale rispetto al collegamento . : fe80::7d22:c6d6:2cf7:8e1d%11
    Indirizzo IPv4. . . . . : 192.168.32.101
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . : 192.168.32.1

Scheda Tunnel isatap.{16D93BD4-5A78-48F0-A3FA-8DC201BDBF78}:

    Stato supporto. . . . . : Supporto disconnesso
    Suffisso DNS specifico per connessione:

C:\Users\win7elle>
```



MODIFICO I FILE HOSTS

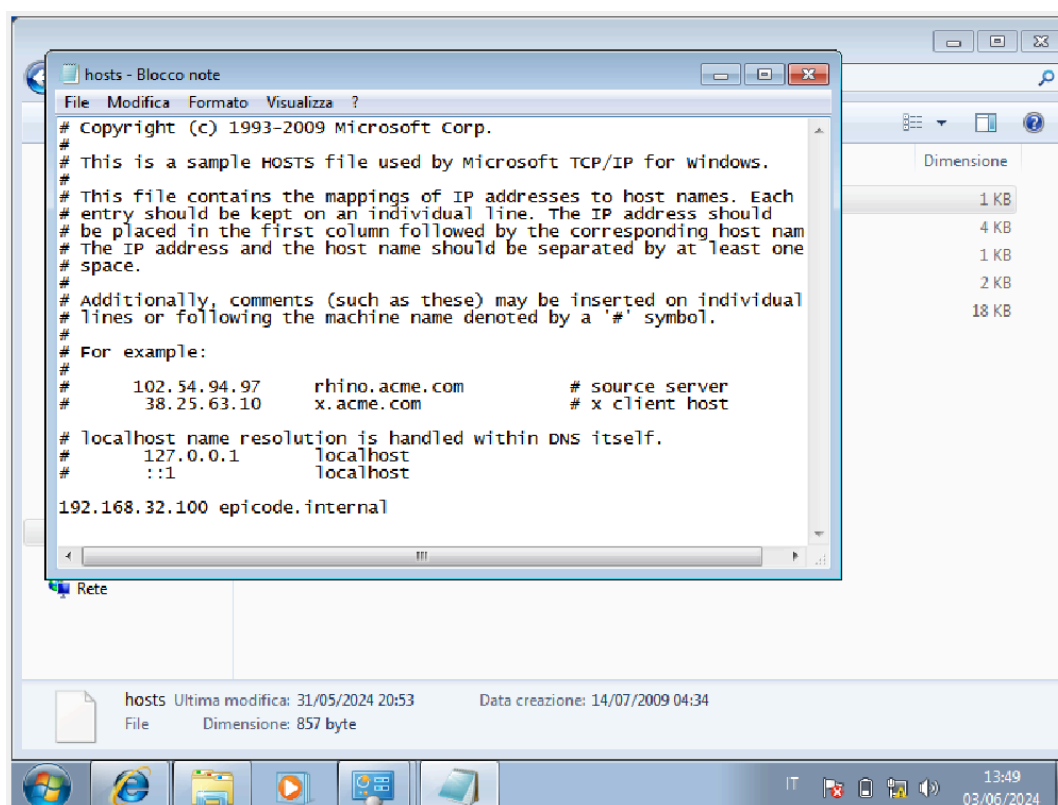
## In Kali:

IL FILE /etc/hosts

contiene una riga che affianca a 192.168.32.100 l'indirizzo  
epicode.internal

## In Windows7:

IL FILE si trova in System32/drivers e host.



## Simuliamo la pagina del Server

Ho semplicemente installato Apache2

Ho modificato il file interno ad Apache2:

/etc/apache2/sites-available/000-default.conf

Imitando la riga commentata #ServerName [www.example.com](http://www.example.com)

Ho fatto una riga: ServerName <http://epicode.internal>

**ORA PROVO UN PING, E PROVO A VISITARE LA PAGINA IN HTTP  
SULLE DUE MACCHINE.**

**SU KALI**

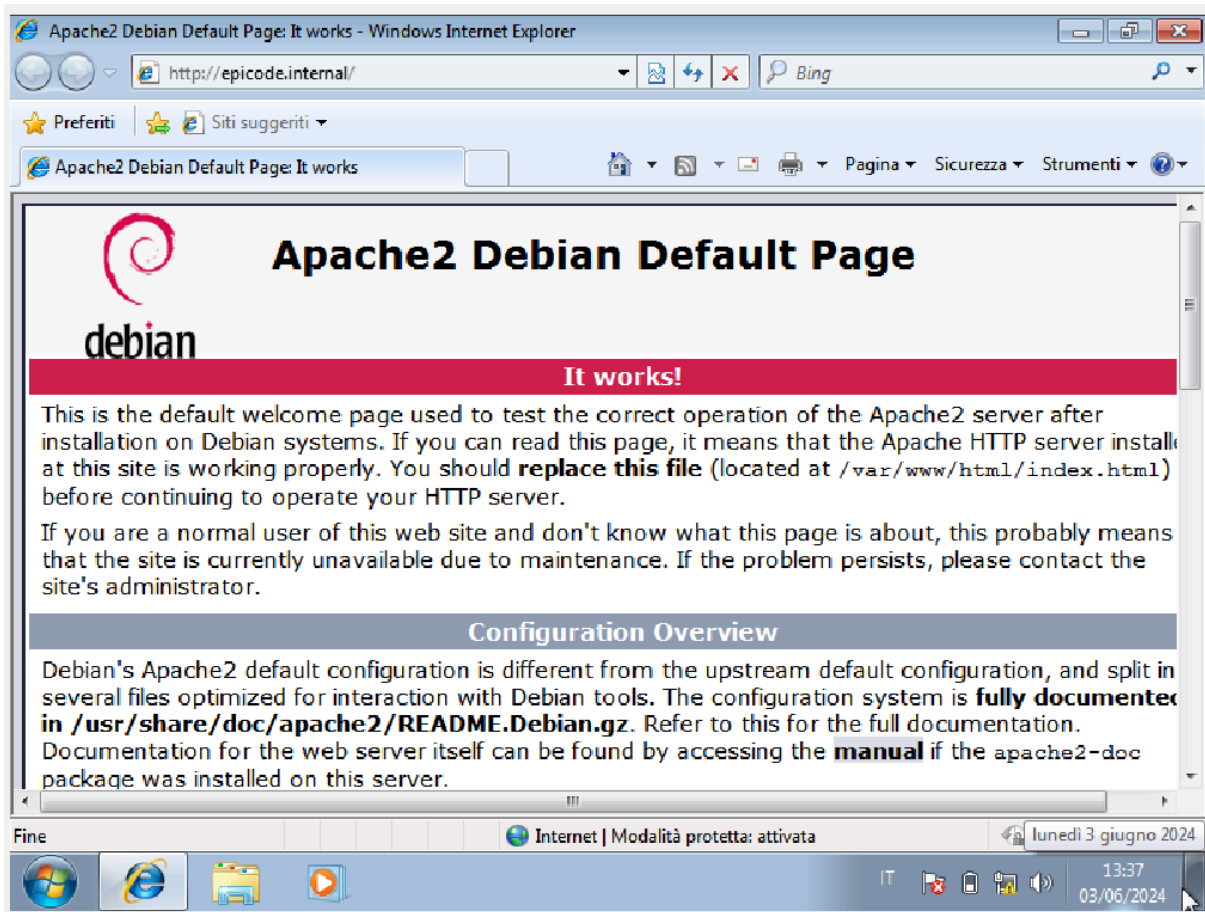
```
File Macchina Visualizza Inserimento Dispositivi Aiuto
zsh: corrupt history file /home/kali/.zsh_history
(kali@kali)-[~]
$ ping -c 6 epicode.internal
PING epicode.internal (192.168.32.100) 56(84) bytes of data:
64 bytes from epicode.internal (192.168.32.100): icmp_seq=1 ttl=64 time=0.127 ms
64 bytes from epicode.internal (192.168.32.100): icmp_seq=2 ttl=64 time=0.058 ms
64 bytes from epicode.internal (192.168.32.100): icmp_seq=3 ttl=64 time=0.037 ms
64 bytes from epicode.internal (192.168.32.100): icmp_seq=4 ttl=64 time=0.048 ms
64 bytes from epicode.internal (192.168.32.100): icmp_seq=5 ttl=64 time=0.071 ms
64 bytes from epicode.internal (192.168.32.100): icmp_seq=6 ttl=64 time=0.047 ms

— epicode.internal ping statistics —
6 packets transmitted, 6 received, 0% packet loss, time 5095ms
rtt min/avg/max/mdev = 0.037/0.064/0.127/0.029 ms
(kali@kali)-[~]
$
```

**FUNZIONA!**



SU WINDOWS 7 FUNZIONA!



CATTURA WIRESHARK

No.	Time	Source	Destination	Protocol	Length	Info
5	3.328379932	PCSystemtec_1e:36:4a	PCSystemtec_d9:8a:...	ARP	42	192.168.32.100 is at 08:00:27:1e:36:4a
6	3.329087108	192.168.32.101	192.168.32.100	DNS	76	Standard query 0x3829 A go.microsoft.com
7	3.329116423	192.168.32.100	192.168.32.101	ICMP	104	Destination unreachable (Port unreachable)
8	3.407390880	192.168.32.101	192.168.32.100	DNS	72	Standard query 0x2fe1 A www.bing.com
9	3.407425819	192.168.32.100	192.168.32.101	ICMP	100	Destination unreachable (Port unreachable)
10	4.312182312	192.168.32.101	192.168.32.100	DNS	76	Standard query 0x3829 A go.microsoft.com
11	4.312207525	192.168.32.100	192.168.32.101	ICMP	104	Destination unreachable (Port unreachable)
12	4.378600268	192.168.32.101	192.168.32.100	DNS	72	Standard query 0x2fe1 A www.bing.com
13	4.378637832	192.168.32.100	192.168.32.101	ICMP	100	Destination unreachable (Port unreachable)
14	5.311228085	192.168.32.101	192.168.32.100	DNS	76	Standard query 0x3829 A go.microsoft.com
15	5.311267835	192.168.32.100	192.168.32.101	ICMP	104	Destination unreachable (Port unreachable)
16	5.375091421	192.168.32.101	192.168.32.100	DNS	72	Standard query 0x2fe1 A www.bing.com
17	5.375142984	192.168.32.100	192.168.32.101	ICMP	100	Destination unreachable (Port unreachable)
18	7.310506765	192.168.32.101	192.168.32.100	DNS	76	Standard query 0x3829 A go.microsoft.com
19	7.310550860	192.168.32.100	192.168.32.101	ICMP	104	Destination unreachable (Port unreachable)
20	7.375480401	192.168.32.101	192.168.32.100	DNS	72	Standard query 0x2fe1 A www.bing.com
21	7.375519197	192.168.32.100	192.168.32.101	ICMP	100	Destination unreachable (Port unreachable)
22	8.003346096	192.168.32.101	192.168.32.100	TCP	60	49160 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM
23	8.003382030	192.168.32.100	192.168.32.101	TCP	66	80 → 49160 [SYN, ACK] Seq=0 Ack=1 Win=32120 Len=0 MSS=1460 SACK_PERM WS=1
24	8.003955224	192.168.32.101	192.168.32.100	TCP	60	49160 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
25	8.004154215	192.168.32.101	192.168.32.100	HTTP	561	GET / HTTP/1.1
26	8.004179702	192.168.32.100	192.168.32.101	TCP	54	80 → 49160 [ACK] Seq=1 Ack=508 Win=31872 Len=0
27	8.042451664	192.168.32.100	192.168.32.101	HTTP	3434	HTTP/1.1 200 OK (text/html)
28	8.043936255	192.168.32.101	192.168.32.100	TCP	60	49160 → 80 [ACK] Seq=508 Ack=3381 Win=65700 Len=0
29	8.075776689	192.168.32.101	192.168.32.100	HTTP	504	GET /icons/openlogo-75.png HTTP/1.1
30	8.076013325	192.168.32.100	192.168.32.101	HTTP	303	HTTP/1.1 304 Not Modified
31	8.278755460	192.168.32.101	192.168.32.100	TCP	60	49160 → 80 [ACK] Seq=958 Ack=3630 Win=65448 Len=0
32	11.308375527	192.168.32.101	192.168.32.100	DNS	76	Standard query 0x3829 A go.microsoft.com
33	11.308421845	192.168.32.100	192.168.32.101	ICMP	104	Destination unreachable (Port unreachable)
34	11.373438681	192.168.32.101	192.168.32.100	DNS	72	Standard query 0x2fe1 A www.bing.com
35	11.373475724	192.168.32.100	192.168.32.101	ICMP	100	Destination unreachable (Port unreachable)
36	13.079211836	192.168.32.100	192.168.32.101	TCP	54	80 → 49160 [FIN, ACK] Seq=3630 Ack=958 Win=31872 Len=0
37	13.080518572	192.168.32.101	192.168.32.100	TCP	60	49160 → 80 [ACK] Seq=958 Ack=3631 Win=65448 Len=0
38	15.374331681	192.168.32.101	192.168.32.255	NBNS	92	Name query NB WWW.BING.COM<00>
39	16.137557617	192.168.32.101	192.168.32.255	NBNS	92	Name query NB WWW.BING.COM<00>
40	16.070319785	192.168.32.101	192.168.32.255	NBNS	92	Name query NB WWW.BING.COM<00>
41	18.070891075	192.168.32.101	192.168.32.100	TCP	60	49160 → 80 [RST, ACK] Seq=958 Ack=3631 Win=0 Len=0

```

Frame 25: 561 bytes on wire (4488 bits), 561 bytes captured (4488 bits) on interface eth0, id 0
Ethernet II, Src: PCSSystemtec_d9:8a:ed (08:00:27:d9:8a:ed), Dst: PCSSystemtec_1e:36:4a (08:00:27:1e:36:4a)
  Destination: PCSSystemtec_1e:36:4a (08:00:27:1e:36:4a)
  Source: PCSSystemtec_d9:8a:ed (08:00:27:d9:8a:ed)
  Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.32.101, Dst: 192.168.32.100
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 547
  Identification: 0x008a (138)
  010. .... = Flags: 0x2, Don't fragment
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 128
  Protocol: TCP (6)
  Header Checksum: 0x3631 [validation disabled]

```

```

0000  08 00 27 1e 36 4a 08 00 27 d9 8a ed 08 00 45 00  ..'.6J.. '....E.
0010  02 23 00 8a 40 00 80 06 36 31 c0 a8 20 65 c0 a8  .#..@.. 61.. e..
0020  20 64 c0 08 00 50 4d 2a 4e a5 24 ec da 04 50 18  d...PM* N$. .P.
0030  40 29 a3 fa 00 00 47 45 54 20 2f 20 48 54 54 50  @)...GE T / HTTP
0040  2f 31 2e 31 0d 0a 41 63 63 65 70 74 3a 20 61 70  /1.1.Ac cept: ap
0050  70 6c 69 63 61 74 69 6f 6e 2f 78 2d 6d 73 2d 61  plicatio n/x-ms-a
0060  70 70 6c 69 63 61 74 69 6f 6e 2c 20 69 6d 61 67  pplicati on, imag
0070  65 2f 6a 70 65 67 2c 20 61 70 70 6c 69 63 61 74  e/jpeg, applicat
0080  69 6f 6e 2f 78 61 6d 6c 2b 78 6d 6c 2c 20 69 6d  ion/xaml+xml, im
0090  61 67 65 2f 67 69 66 2c 20 69 6d 61 67 65 2f 70  age/gif, image/p
00a0  6a 70 65 67 2c 20 61 70 70 6c 69 63 61 74 69 6f  jpeg, ap plicatio
00b0  6e 2f 78 2d 6d 73 2d 78 62 61 70 2c 20 2a 2f 2a  n/x-ms-x bap, */*
00c0  0d 0a 41 63 63 65 70 74 2d 4c 61 6e 67 75 61 67  .Accept -Languag
00d0  65 3a 20 69 74 0d 0a 55 73 65 72 2d 41 67 65 6e  e: it.U ser-Agen
00e0  74 3a 20 4d 6f 7a 69 6c 6c 61 2f 34 2e 30 20 28  t: Mozil la/4.0 (
00f0  63 6f 6d 70 61 74 69 62 6c 65 3b 20 4d 53 49 45  compatib le; MSIE
0100  20 38 2e 30 3b 20 57 69 6e 64 6f 77 73 20 4e 54  8.0; Wi ndows NT

```

No.: 25 · Time: 8.004154215 · Source: 192.168.32.101 · Destination: 192.168.32.100 · Protocol: HTTP · Length: 561 · Info: GET / HTTP/1.1

✓ Show packet bytes

IN QUESTO PACCHETTO CHE VA DA Windows7 a Kali,

- il Mac sorgente è: 08:00:27:d9:8a:ed
- il MAC destinazione è: 08:00:27:1e:36:4a

# Esercizio svolto con HTTPS

# Abilitiamo la crittografia SSL su Apache2

```
File Actions Edit View Help
zsh: corrupt history file /home/kali/.zsh_history
(kali@kali)-[~]
$ sudo a2enmod ssl
[sudo] password for kali:
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Module socache_shmcb already enabled
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create self-signed certificates.
To activate the new configuration, you need to run:
    systemctl restart apache2
(kali@kali)-[~]
$ systemctl restart apache2
```

## Adesso creiamo un certificato SSL autofirmato con OPENSSL

Il file che contiene il certificato si chiamerà apache-selfigned e si chiama uguale, cambia solo l'estensione, anche la chiave

[illegible]

AGGIORNAMO IL FILE CERTIFICATI DI APACHE2 TRASFORMANDO IN COMMENTI LE COSE VECCHIE:

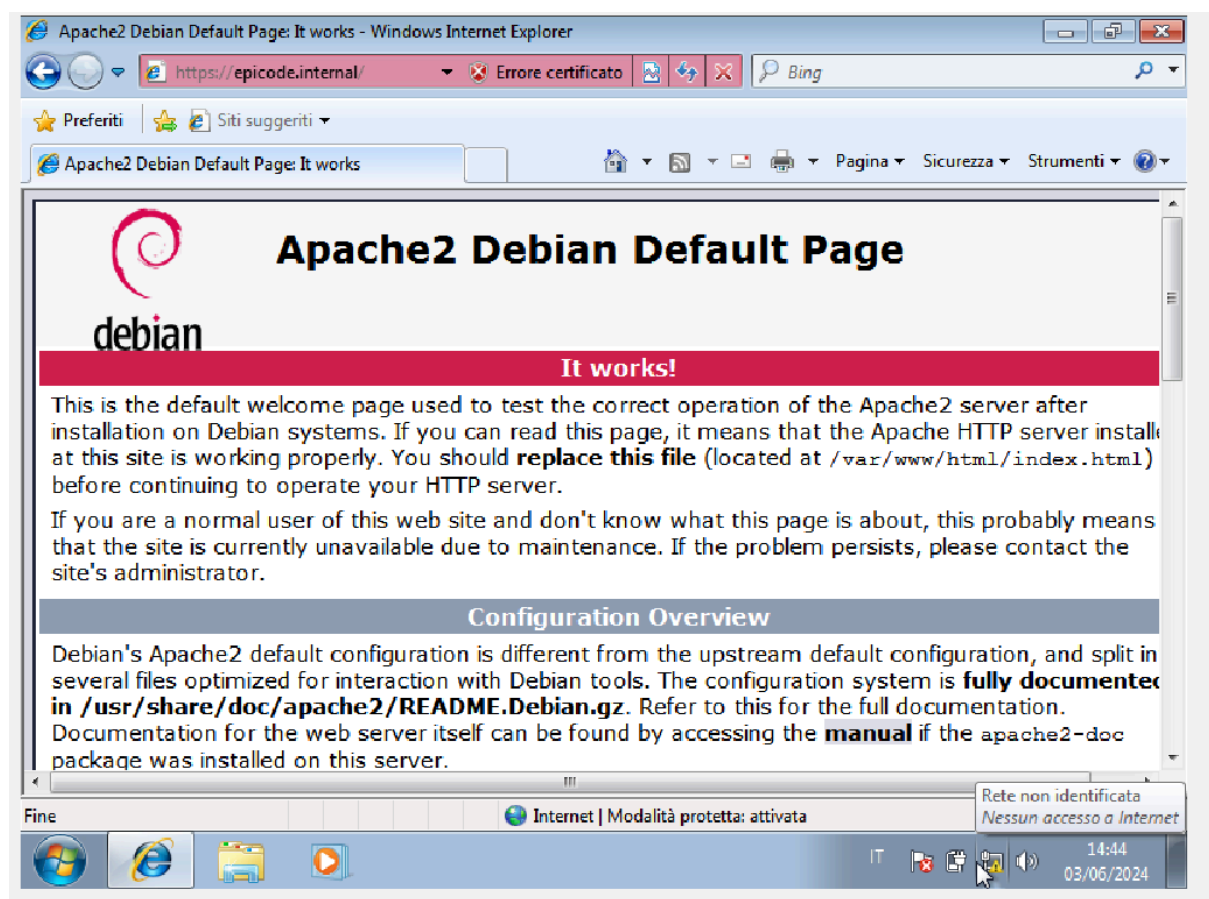
```
# /usr/share/doc/apache2/README.Debian.gz for more info.
# If both key and certificate are stored in the same file, only the
# SSLCertificateFile directive is needed.
####SSLCertificateFile /etc/ssl/certs/ssl-cert-snakeoil.pem
SSLCertificateFile /etc/ssl/certs/apache-selfsigned.crt
####SSLCertificateKeyFile /etc/ssl/private/ssl-cert-snakeoil.key
SSLCertificateKeyFile /etc/ssl/private/apache-selfsigned.key

# Server Certificate Chain:
# Point SSLCertificateChainFile at a file containing the
# concatenation of PEM encoded CA certificates which form the
# certificate chain for the server certificate. Alternatively
# the referenced file can be the same as SSLCertificateFile
# when the CA certificates are directly appended to the server
```



```
File Actions Edit View Help
zsh: corrupt history file /home/kali/.zsh_history
(kali@kali)-[~]
$ sudo a2ensite default-ssl.conf
[sudo] password for kali:
Enabling site default-ssl.
To activate the new configuration, you need to run:
    systemctl reload apache2
(kali@kali)-[~]
$ systemctl reload apache2
```

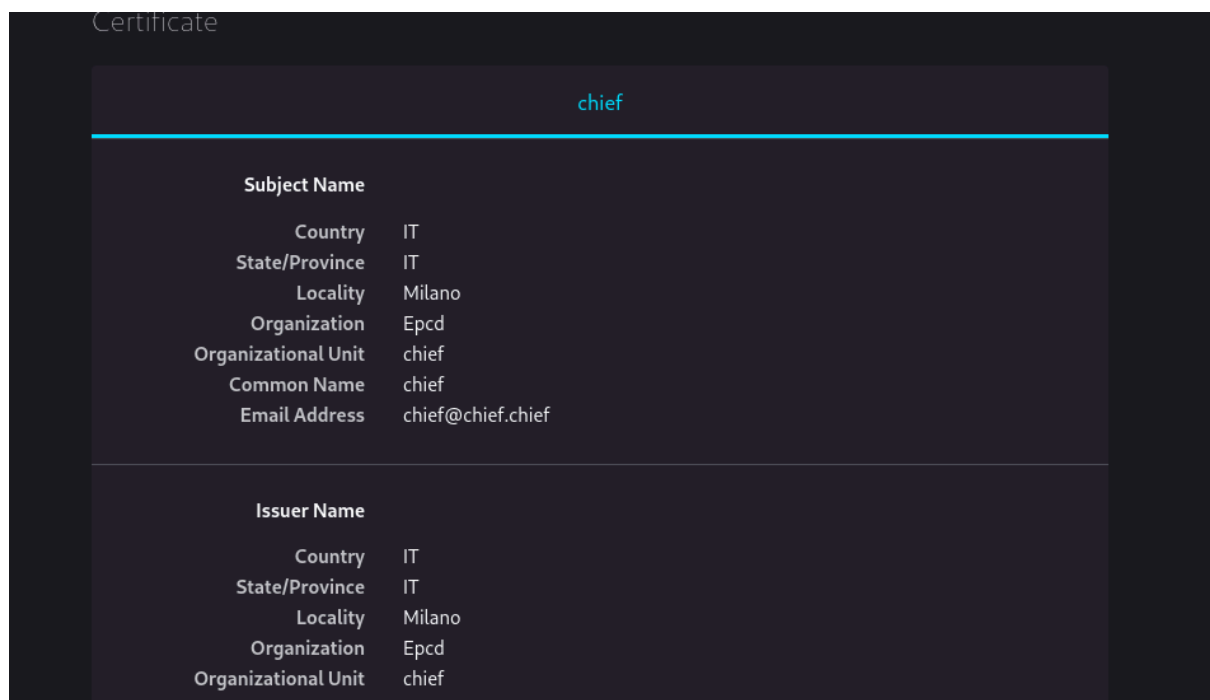
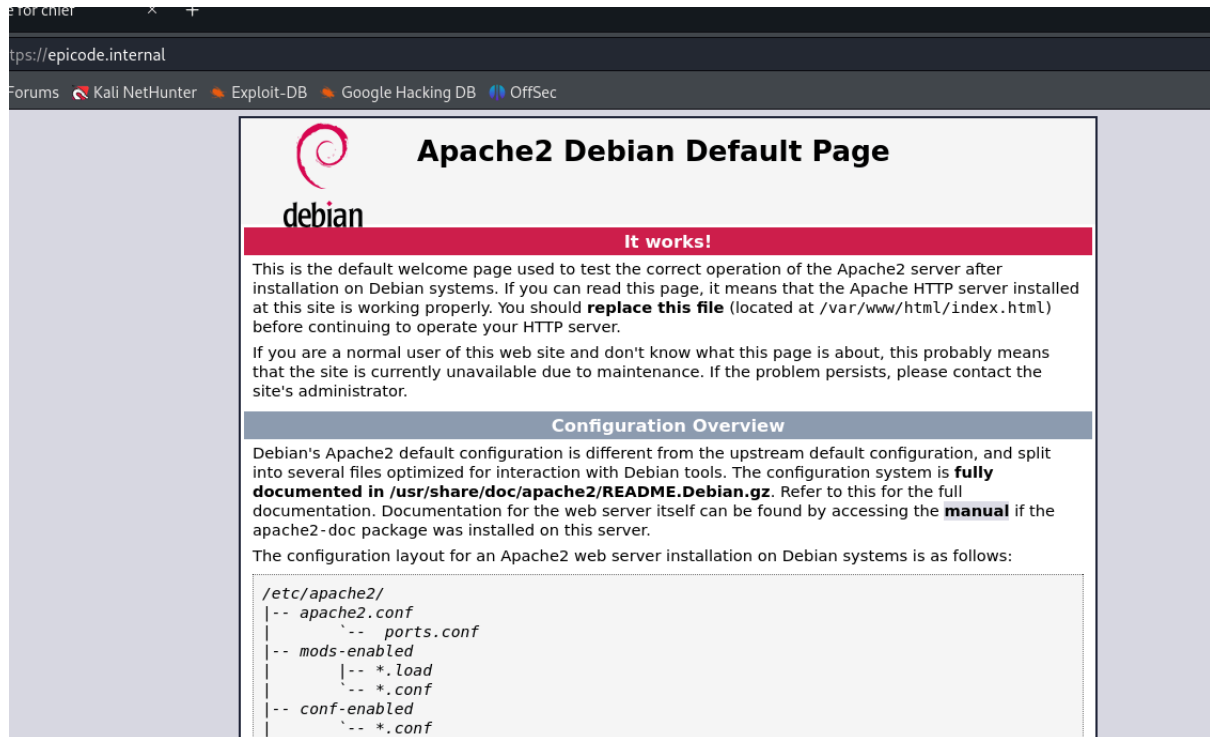
L'HTTP funziona, provo a visitare da Browser





# SU KALI, MOZILLA MI FA ANCHE VEDERE IL CERTIFICATO CON DATI FARLOCCHI CHE AVEVO CREATO CON OPENSSL

(organizzazione = epcd 😊)



# Faccio partire la CATTURA Wireshark

Noto che in HTTPS LA COMUNICAZIONE è criptata nonostante i MAC address siano i medesimi. infatti il protocollo che Wireshark mi visualizza è il TLS che serve per trasportare dati criptati in https.

```
» Frame 237: 215 bytes on wire (1720 bits), 215 bytes captured (1720 bits) on interface eth0, id 0
» Ethernet II, Src: PCSSystemtec_d9:8a:ed (08:00:27:d9:8a:ed), Dst: PCSSystemtec_1e:36:4a (08:00:27:1e:36:4a)
» Internet Protocol Version 4, Src: 192.168.32.101, Dst: 192.168.32.100
» Transmission Control Protocol, Src Port: 49170, Dst Port: 443, Seq: 1, Ack: 1, Len: 161
» Transport Layer Security

0000  08 00 27 1e 36 4a 08 00 27 d9 8a ed 08 00 45 00  ...'6J...E:
0010  00 c9 01 4c 40 00 00 06 36 c9 c0 a8 20 65 c0 a8  ...L@...6...e...
0020  20 64 c0 12 01 bb 13 17 70 95 e1 a5 d9 ff 50 18  ...d....p....P...
0030  40 29 19 12 00 00 16 03 01 00 9c 01 00 00 98 03  ...@).....
0040  01 66 5d c0 41 2c 8d 4b bb 45 c2 c0 14 a9 94 ee  ...f]_A_K_E.....
0050  d4 90 30 2d 5f a0 47 1f 54 3f f4 f5 5e 0f ac a7  ...-0_ _G_ T?..A...
0060  1d 20 17 58 0e 51 88 9f 7e 84 59 89 b5 91 e6 2a  ..._X Q_~Y.....*
0070  30 c1 c6 c9 9e 82 bc 4c 1e 49 e8 f7 64 ab f0 3f  ...0....L_I_d...?
0080  35 9a 00 18 00 2f 00 35 00 05 00 0a c0 13 c0 14  ...5..../5.....
0090  c0 09 c0 0a 00 32 00 38 00 13 00 04 01 00 00 37  .......2.8.....7
00a0  ff 01 00 01 00 00 00 00 15 00 13 00 00 10 65 70  ........ep
00b0  69 63 6f 64 65 2e 69 6e 74 65 72 6e 61 6c 00 05  ...icode.in ternal..
00c0  00 05 01 00 00 00 00 00 00 06 00 04 00 17 00  ........
00d0  18 00 0b 00 02 01 00 00 00 00 00 00 00 00 00 00  ...

Info.: 237 - Time: 752.332539823 - Source: 192.168.32.101 - Destination: 192.168.32.100 - Protocol: TLSv1 - Length: 215 - Info: Client Hello (SNL=epicode.internal)
/ Show packet bytes
```