

PROGETTO FINALE CONSEGNA - Domenico Vecchio

CONSEGNA:

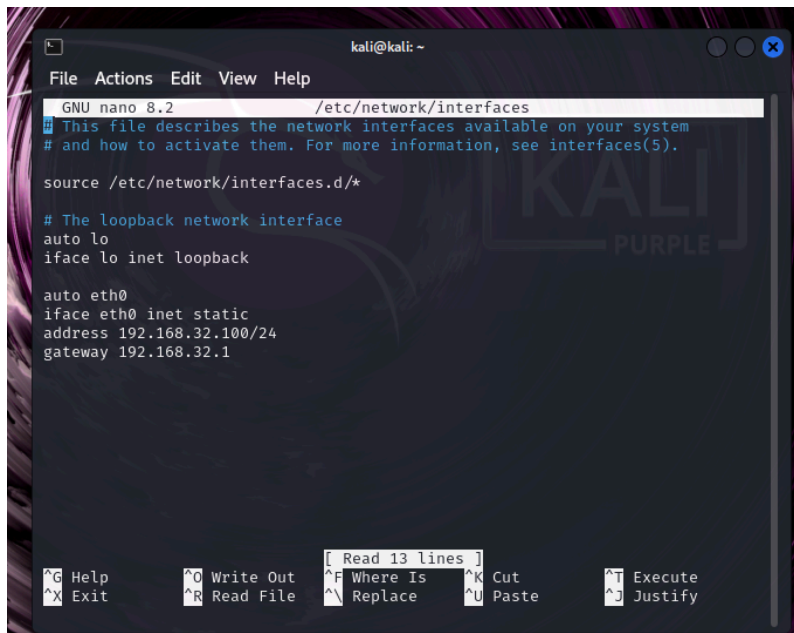
Requisiti e servizi:

- Kali Linux: IP 192.168.32.100
- Windows: IP 192.168.32.101
- HTTPS server: attivo
- Servizio DNS per risoluzione nomi di dominio: attivo.
- Simulare, in ambiente di laboratorio virtuale, un'architettura client server in cui un client con indirizzo 192.168.32.101 (Windows) richiede tramite web browser una risorsa all'hostname epicode.internal che risponde all'indirizzo 192.168.32.100 Kali.
- Si intercetti poi la comunicazione con Wireshark, evidenziando i MAC address di sorgente e destinazione ed il contenuto della richiesta HTTPS. Ripetere l'esercizio, sostituendo il server HTTPS, con un server HTTP.
- Si intercetti nuovamente il traffico, evidenziando le eventuali differenze tra il traffico appena catturato in HTTP ed il traffico precedente in HTTPS.
- Spiegare, motivandole, le principali differenze se presenti.

CONFIGURAZIONE IP KALI LINUX

Per configurare un ip statico su kali Linux (192.168.32.100) , bisogna accedere sul terminale e digitare il seguente comando :

sudo nano /etc/network/interfaces

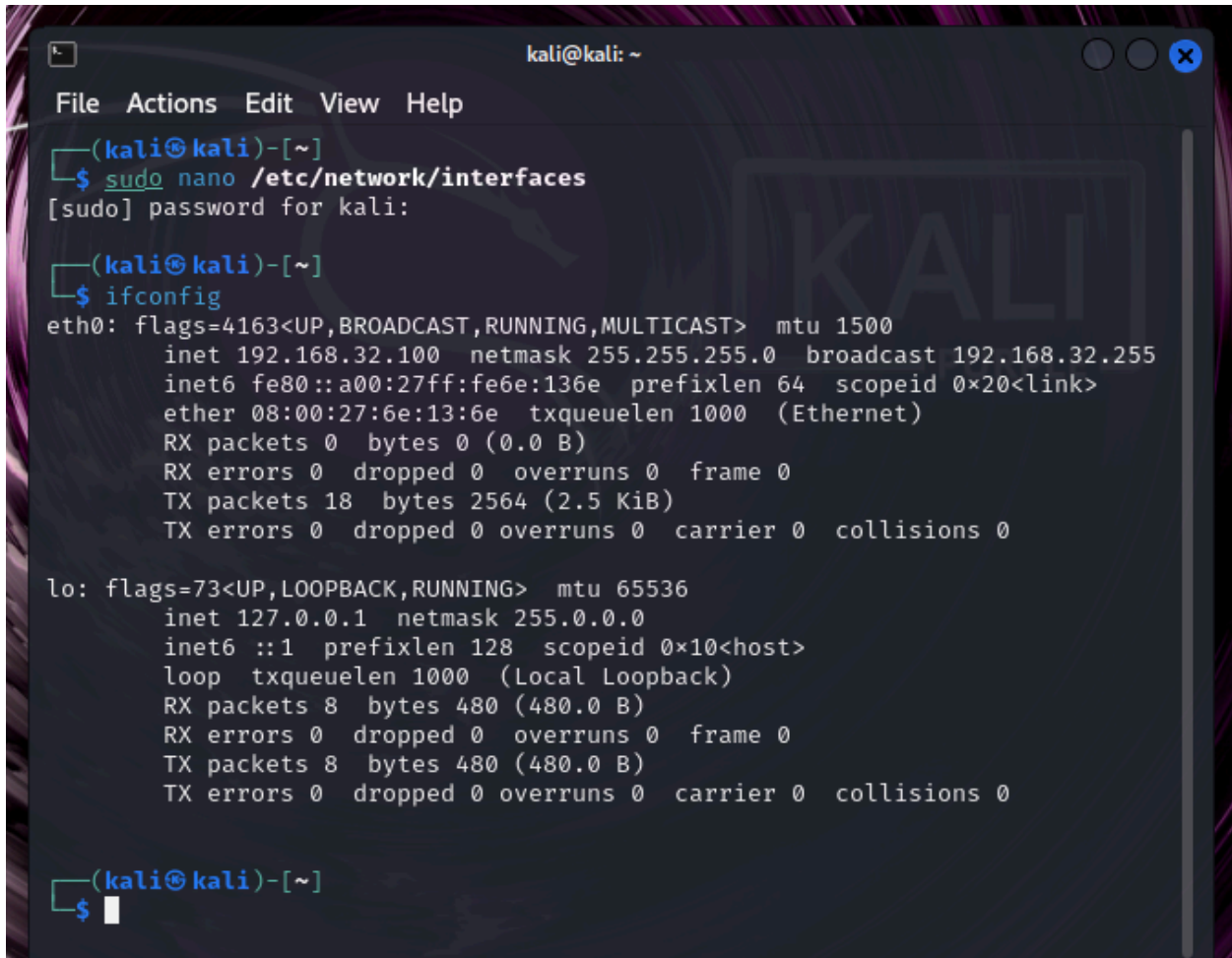


```
kali@kali: ~  
File Actions Edit View Help  
GNU nano 8.2 /etc/network/interfaces  
# This file describes the network interfaces available on your system  
# and how to activate them. For more information, see interfaces(5).  
  
source /etc/network/interfaces.d/*  
  
# The loopback network interface  
auto lo  
iface lo inet loopback  
  
auto eth0  
iface eth0 inet static  
address 192.168.32.100/24  
gateway 192.168.32.1  
  
[ Read 13 lines ]  
^G Help      ^O Write Out  ^F Where Is   ^K Cut        ^T Execute  
^X Exit      ^R Read File  ^N Replace    ^U Paste      ^J Justify
```

Verrà richiesta la password , inserire **kali**.

Una volta all'interno del file , inserire manualmente ip address (192.168.32.100) e il gateway (192.168.32.1) Salvare il file con CTRL+X , digitare Y (yes) e infine premere Invio.

Una volta configurato il file , digitare *ifconfig* , per visualizzare se l'indirizzo ip e il gateway sono stati assegnati correttamente .

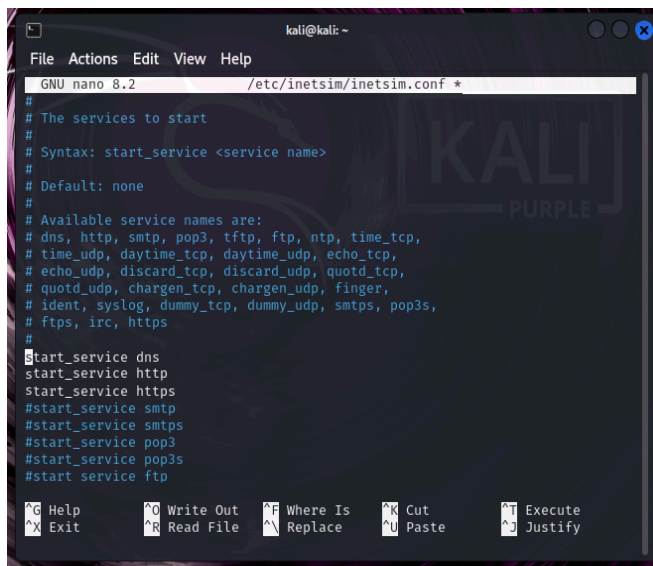
A terminal window titled 'kali@kali: ~' with a menu bar (File, Actions, Edit, View, Help). The user runs 'sudo nano /etc/network/interfaces', followed by a password prompt. Then, they run 'ifconfig'. The output shows details for 'eth0' (IP: 192.168.32.100, netmask: 255.255.255.0) and 'lo' (loopback, IP: 127.0.0.1).

```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ sudo nano /etc/network/interfaces  
[sudo] password for kali:  
  
(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:fe6e:136e  prefixlen 64  scopeid 0x20<link>  
    ether 08:00:27:6e:13:6e  txqueuelen 1000  (Ethernet)  
    RX packets 0  bytes 0 (0.0 B)  
    RX errors 0  dropped 0  overruns 0  frame 0  
    TX packets 18  bytes 2564 (2.5 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 8  bytes 480 (480.0 B)  
    RX errors 0  dropped 0  overruns 0  frame 0  
    TX packets 8  bytes 480 (480.0 B)  
    TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0  
  
(kali@kali)-[~]  
$
```

CONFIGURAZIONE SERVIZI DNS, http, HTTPS SU KALI LINUX

Per attivare questi servizi bisogna configurare il file di InetSim da Kali Linux.
Da terminale eseguire questo comando :

sudo nano /etc/inetsim/inetsim.conf



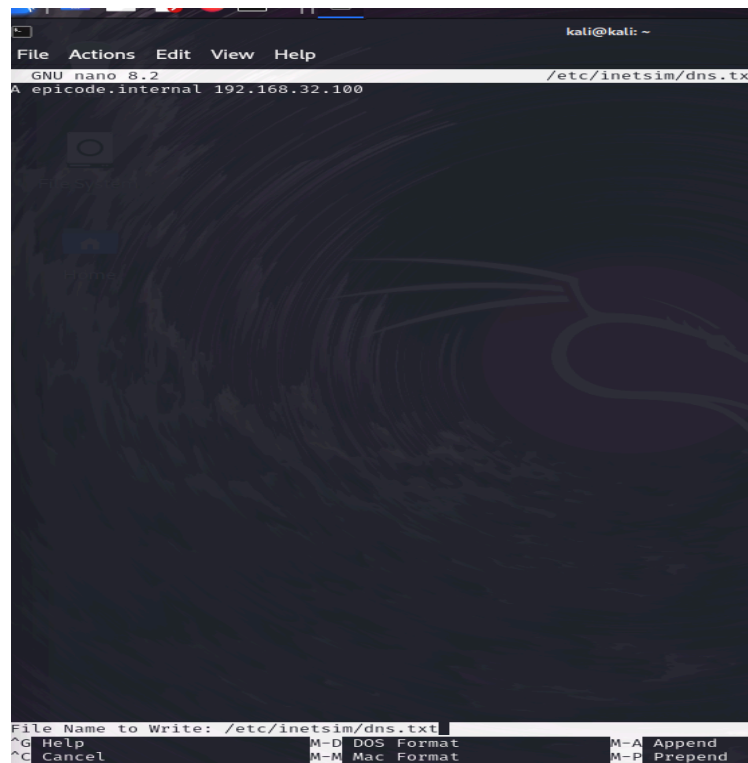
```
GNU nano 8.2 /etc/inetsim/inetsim.conf *
#
# The services to start
#
# Syntax: start_service <service name>
#
# Default: none
#
# Available service names are:
# dns, http, smtp, pop3, tftp, ftp, ntp, time_tcp,
# time_udp, daytime_tcp, daytime_udp, echo_tcp,
# echo_udp, discard_tcp, discard_udp, quotd_tcp,
# 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

^G Help      ^O Write Out  ^F Where Is   ^K Cut        ^T Execute
^X Exit      ^R Read File  ^N Replace    ^U Paste      ^J Justify
```

Una volta
all'interno per attivare i servizi bisogna
togliere “#” per attivare, in questo caso ci
servono;

-start_service_dns
-start_service_http
-start_service_https

Proseguendo nelle configurazioni , attivare
la porta 53.



```
GNU nano 8.2 /etc/inetsim/dns.txt
epicode.internal 192.168.32.100

File Name to Write: /etc/inetsim/dns.txt
^G Help      M-D DOS Format  M-A Append
^C Cancel    M-M Mac Format  M-P Prepend
```

All'interno del file dns.txt ,
specificare indirizzo e il nome
“epicode.internal” e
“192.168.32.100”

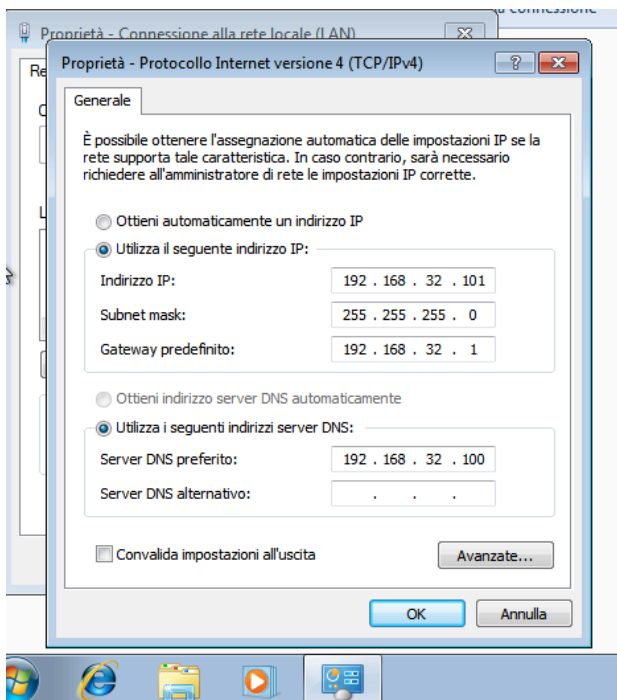
```
(kali@kali)-[~]
$ sudo inetsim
INetSim 1.3.2 (2020-05-19) by Matthias Eckert & Thomas Hungenberg
Using log directory: /var/log/inetsim/
Using data directory: /var/lib/inetsim/
Using report directory: /var/log/inetsim/report/
Using configuration file: /etc/inetsim/inetsim.conf
Parsing configuration file.
Configuration file parsed successfully.
== INetSim main process started (PID 12719) ==
Session ID: 12719
Listening on: 192.168.32.100
Real Date/Time: 2025-03-23 21:23:10
Fake Date/Time: 2025-03-23 21:23:10 (Delta: 0 seconds)
Forking services...
* dns_53_tcp_udp - started (PID 12729)
deprectated method; prefer start_server() at /usr/share/perl5/INetSim/DNS.pm line 69.
Attempt to start Net::DNS::Nameserver in a subprocess at /usr/share/perl5/INetSim/DNS.pm line 69.
* https_443_tcp - started (PID 12731)
* http_80_tcp - started (PID 12730)
done.
Simulation running.
```

Dopo avere salvato le configurazioni , avviare InetSim con il comando :

sudo inetsim

Se tutto è corretto verrà visualizzato indirizzo ip.

CONFIGURAZIONE DNS SU WINDOWS 7



Configurazione manuale del DNS:

Vai su **Pannello di Controllo -> Centro connessioni di rete e condivisione**.

Clicca su **Modifica impostazioni scheda**.

Seleziona la scheda di rete -> Proprietà.

Seleziona **Protocollo Internet versione 4 (TCP/IPv4)** -> Proprietà.

Imposta il **server DNS preferito** su **192.168.32.100**.

VERIFICA CHE LE MACCHINE SI PINGANO

Per verificare bisogna andare sul terminale e digitare *ping* (indirizzo ip della macchina)

nb : per far si che si pingano tra di loro bisogna settare su virtual box sulle impostazioni , che siano entrambi sulla rete interna con stesso nome nel mio caso (internall).

-disattivare anche il firewall su windows e utilizzare la regola allow_ping.

Come si vede dalle immagini le macchine comunicano fra di loro.

```
(kali@kali)-[~]
$ ping 192.168.32.101
PING 192.168.32.101 (192.168.32.101) 56(84) bytes of data.
64 bytes from 192.168.32.101: icmp_seq=1 ttl=128 time=4.25 ms
64 bytes from 192.168.32.101: icmp_seq=2 ttl=128 time=1.52 ms
64 bytes from 192.168.32.101: icmp_seq=3 ttl=128 time=26.8 ms
64 bytes from 192.168.32.101: icmp_seq=4 ttl=128 time=1.35 ms
64 bytes from 192.168.32.101: icmp_seq=5 ttl=128 time=1.18 ms
64 bytes from 192.168.32.101: icmp_seq=6 ttl=128 time=3.03 ms
64 bytes from 192.168.32.101: icmp_seq=7 ttl=128 time=1.33 ms
64 bytes from 192.168.32.101: icmp_seq=8 ttl=128 time=2.16 ms
^C
--- 192.168.32.101 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7024ms
rtt min/avg/max/mdev = 1.175/5.202/26.615/8.228 ms
(kali@kali)-[~]
```

```
C:\Windows\system32\cmd.exe

C:\Users\ vboxuser>ping 192.168.32.100

Esecuzione di Ping 192.168.32.100 con 32 byte di dati:
Risposta da 192.168.32.100: byte=32 durata=2ms TTL=64
Risposta da 192.168.32.100: byte=32 durata=2ms TTL=64
Risposta da 192.168.32.100: byte=32 durata=1ms TTL=64
Risposta da 192.168.32.100: byte=32 durata=1ms TTL=64

Statistiche Ping per 192.168.32.100:
    Pacchetti: Trasmessi = 4, Ricevuti = 4,
    Persi = 0 (0% persi),
    Tempo approssimativo percorsi andata/ritorno in millisecondi:
        Minimo = 1ms, Massimo = 2ms, Medio = 1ms

C:\Users\ vboxuser>_
```

INTERCETTAZIONE TRAFFICO WIRESHARK

Avviare WireShark , entrare sul browser e digitare 192.168.32.100.

HTTP

Avviare intercettazione con http , verificare i pacchetti catturati e verranno visualizzati i **MAC address** di sorgente (quella della macchina kali) e destinazione (quella del server).

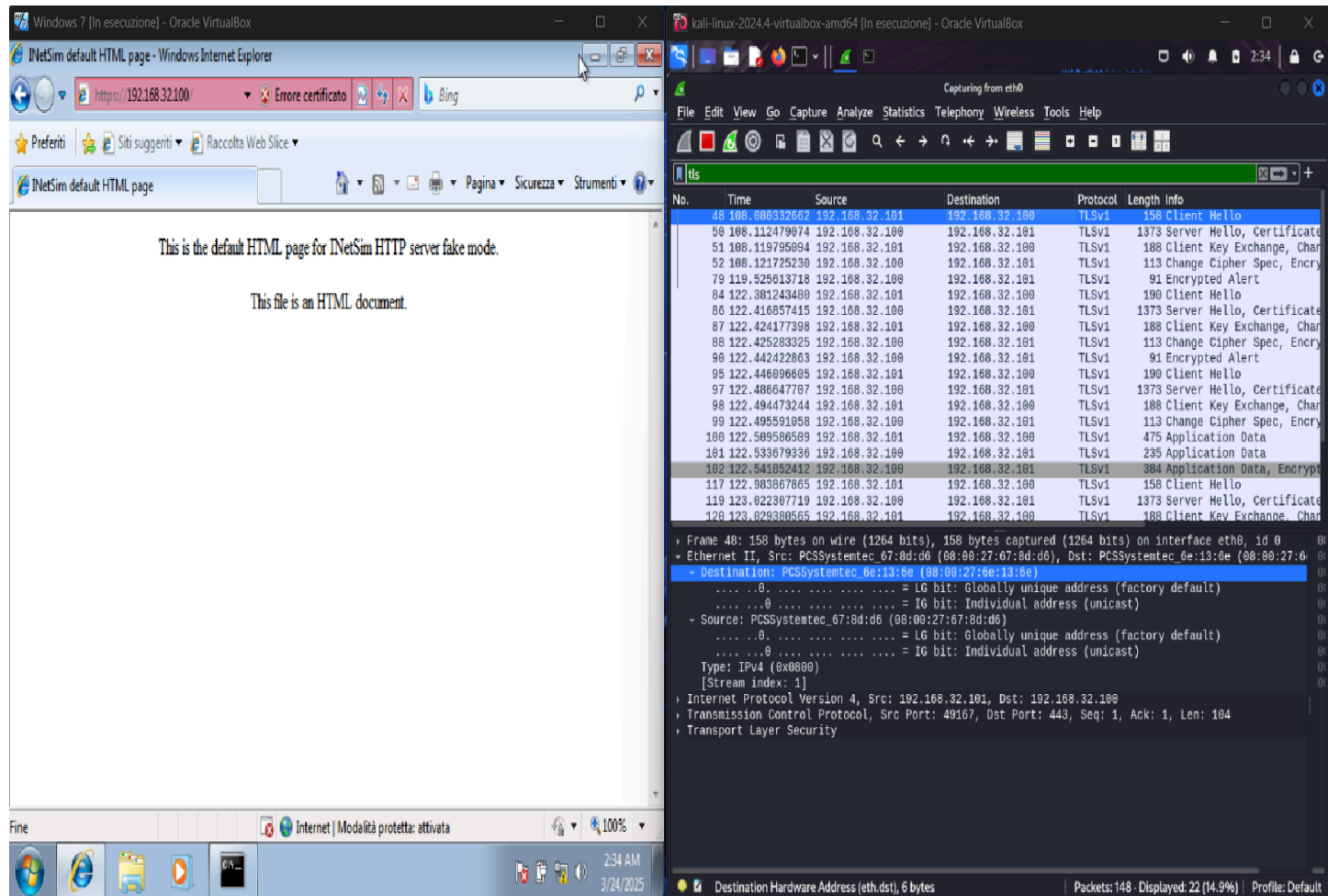
The screenshot displays two virtual machines running on Oracle VM VirtualBox. The left window shows a Windows 7 virtual machine with Internet Explorer open, displaying the default HTML page for the INetSim HTTP server. The right window shows a Kali Linux virtual machine with Wireshark open, capturing traffic on the eth0 interface. The packet list in Wireshark shows three HTTP GET requests to 192.168.32.100. The selected packet (No. 38) shows the Ethernet II header with source MAC 08:00:27:0e:13:6e and destination MAC 08:00:27:0e:8d:d6, followed by the IP and HTTP headers.

No.	Time	Source	Destination	Protocol	Length	Info
17	26.333199821	192.168.32.101	192.168.32.100	HTTP	449	GET / HTTP/1.1
20	26.384804489	192.168.32.100	192.168.32.101	HTTP	312	HTTP/1.1 200 OK [text/html]
35	26.473274540	192.168.32.101	192.168.32.100	HTTP	325	GET /favicon.ico HTTP/1.1
38	26.521395611	192.168.32.100	192.168.32.101	HTTP	252	HTTP/1.1 200 OK [image/x-ico]

Frame 38: 252 bytes on wire (2016 bits), 252 bytes captured (2016 bits) on interface eth0, id 0
Ethernet II, Src: PCSSystemtec_6e:13:6e (08:00:27:0e:13:6e), Dst: PCSSystemtec_07:8d:d6 (08:00:27:0e:8d:d6)
Destination: PCSSystemtec_07:8d:d6 (08:00:27:0e:8d:d6)
Source: PCSSystemtec_6e:13:6e (08:00:27:0e:13:6e)
Type: IPv4 (0x0800)
[Stream index: 1]
Internet Protocol Version 4, Src: 192.168.32.100, Dst: 192.168.32.101
Transmission Control Protocol, Src Port: 80, Dst Port: 49166, Seq: 154, Ack: 272, Len: 198
[2 Reassembled TCP Segments (351 bytes): #37(153), #38(198)]
Hypertext Transfer Protocol
Media Type

HTTPS

Ripetere i passaggi come in http , visualizzare i pacchetti , si vedrà che in https non si potrà vedere il testo perché è cifrato



In conclusione su **HTTPS (porta 443)** ,il contenuto è nascosto , poco utile senza chiave privata e il MAC address è visibile .

In **HTTP (porta 80)** , il contenuto è leggibile , MAC Address visibile e permette di vedere username e altri dati sensibili.