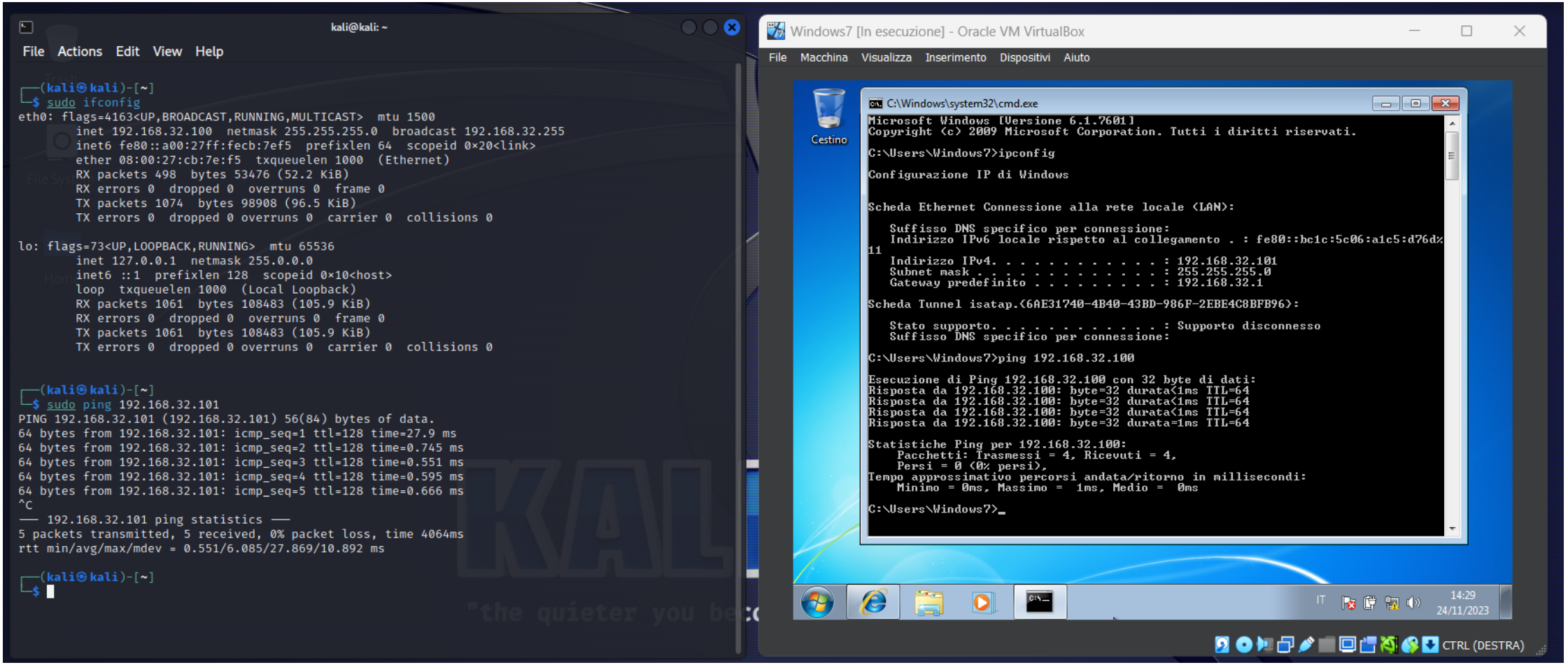
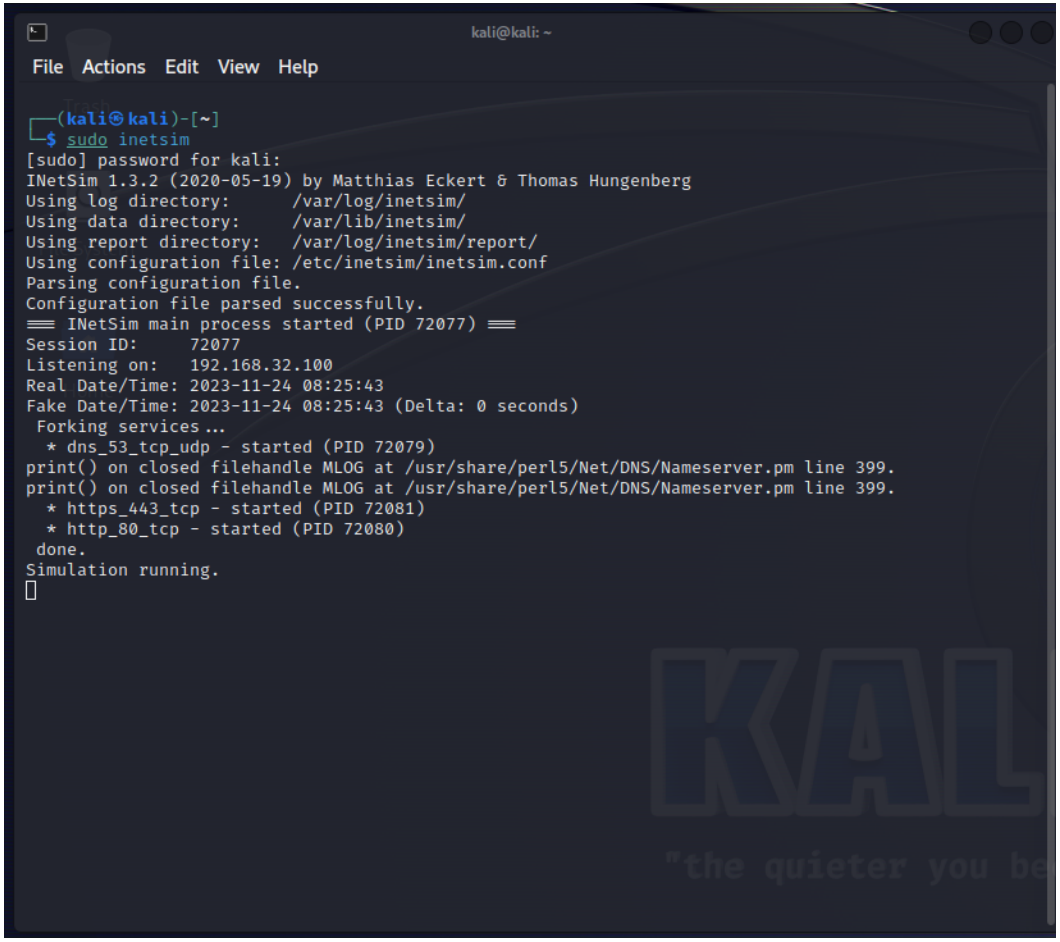
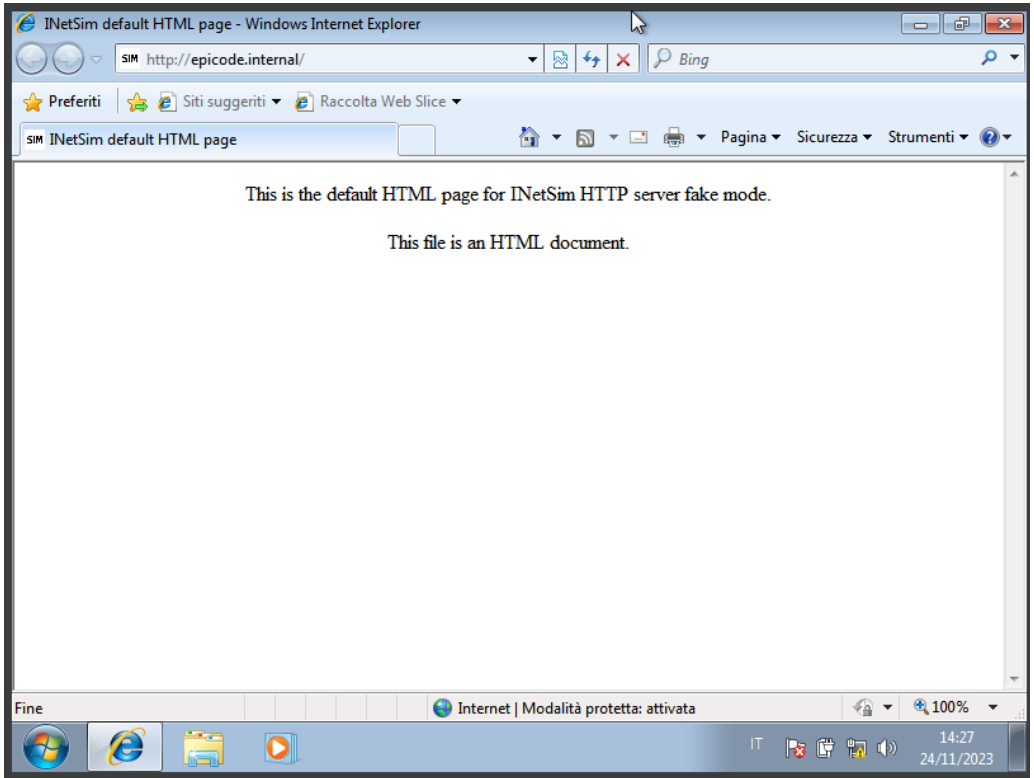
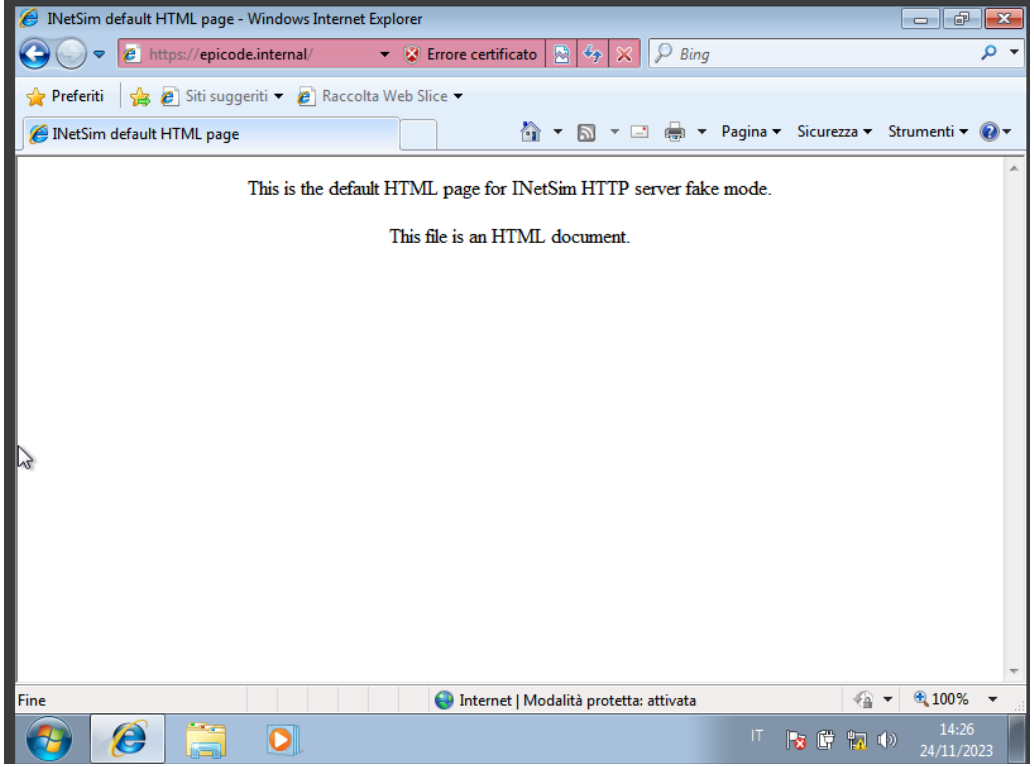
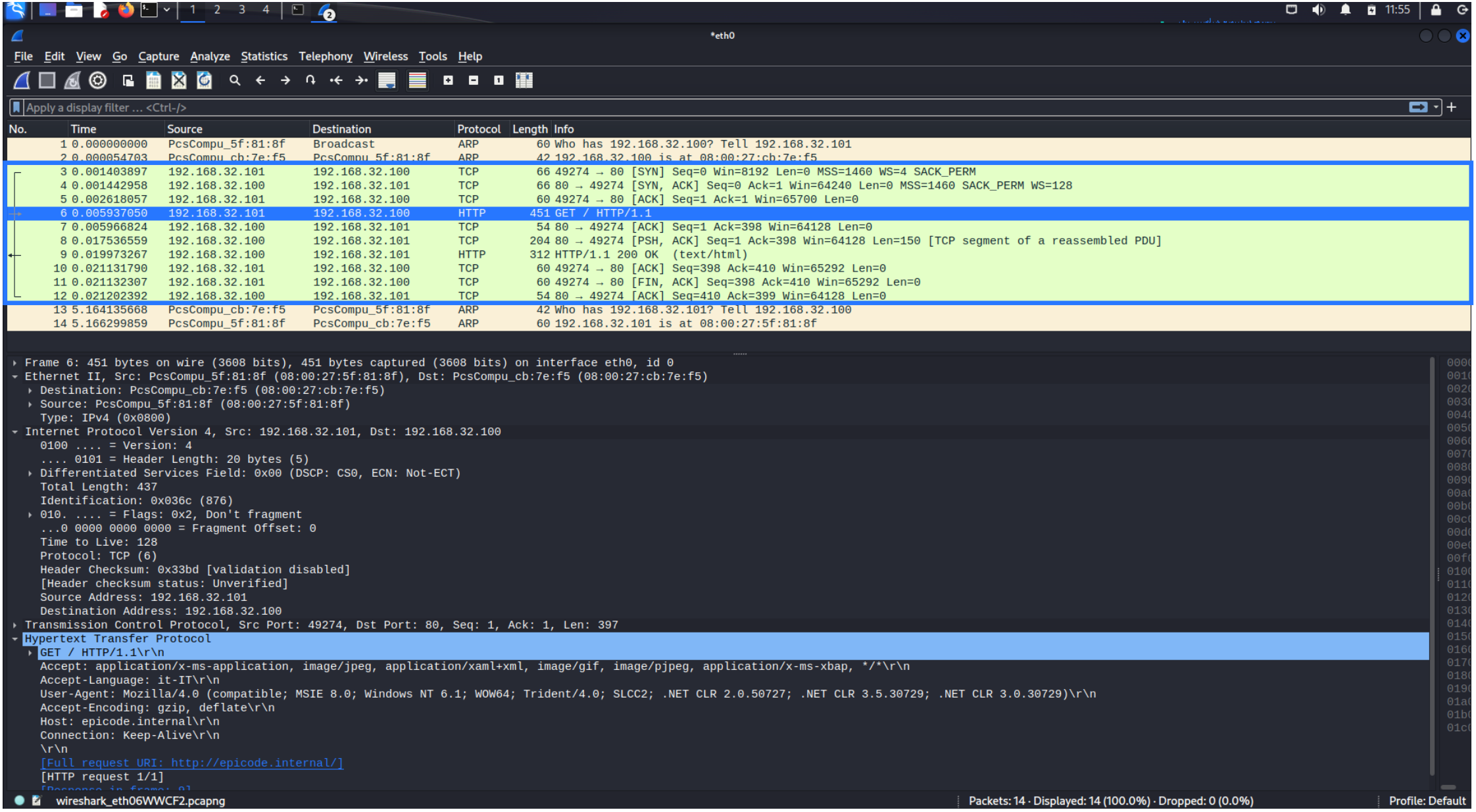

kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.32.100 netmask 255.255.255.0 broadcast 192.168.32.255
inet6 fe80::a00:27ff:fecb:7ef5 prefixlen 64 scopeid 0x20<link>
ether 08:00:27:cb:7e:f5 txqueuelen 1000 (Ethernet)
RX packets 498 bytes 53476 (52.2 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 1074 bytes 98908 (96.5 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 1061 bytes 108483 (105.9 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 1061 bytes 108483 (105.9 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
(kali㉿kali)-[~]
$ sudo 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=27.9 ms
64 bytes from 192.168.32.101: icmp_seq=2 ttl=128 time=0.745 ms
64 bytes from 192.168.32.101: icmp_seq=3 ttl=128 time=0.551 ms
64 bytes from 192.168.32.101: icmp_seq=4 ttl=128 time=0.595 ms
64 bytes from 192.168.32.101: icmp_seq=5 ttl=128 time=0.666 ms
^C
— 192.168.32.101 ping statistics —
5 packets transmitted, 5 received, 0% packet loss, time 4064ms
rtt min/avg/max/mdev = 0.551/6.085/27.869/10.892 ms
(kali㉿kali)-[~]
$
Windows7 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Cestino
C:\Windows\system32\cmd.exe
Microsoft Windows [Versione 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Tutti i diritti riservati.
C:\Users\Windows7>ipconfig
Configurazione IP di Windows
Scheda Ethernet Connessione alla rete locale (LAN):
Suffisso DNS specifico per connessione:
Indirizzo IPv6 locale rispetto al collegamento . : fe80::bc1c:5c06:a1c5:d76d%11
Indirizzo IPv4. . . . . : 192.168.32.101
Subnet mask . . . . . : 255.255.255.0
Gateway predefinito . . . . . : 192.168.32.1
Scheda Tunnel isatap.{6AE31740-4B40-43BD-986F-2EBE4C8BFB96}:
Stato supporto. . . . . : Supporto disconnesso
Suffisso DNS specifico per connessione:
C:\Users\Windows7>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<1ms 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
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 = 0ms, Massimo = 1ms, Medio = 0ms
C:\Users\Windows7>
IT
14:29
24/11/2023
CTRL (DESTRA)


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 72077) ===
Session ID: 72077
Listening on: 192.168.32.100
Real Date/Time: 2023-11-24 08:25:43
Fake Date/Time: 2023-11-24 08:25:43 (Delta: 0 seconds)
Forking services...
* dns_53_tcp_udp - started (PID 72079)
print() on closed filehandle MLOG at /usr/share/perl5/Net/DNS/Nameserver.pm line 399.
print() on closed filehandle MLOG at /usr/share/perl5/Net/DNS/Nameserver.pm line 399.
* https_443_tcp - started (PID 72081)
* http_80_tcp - started (PID 72080)
done.
Simulation running.

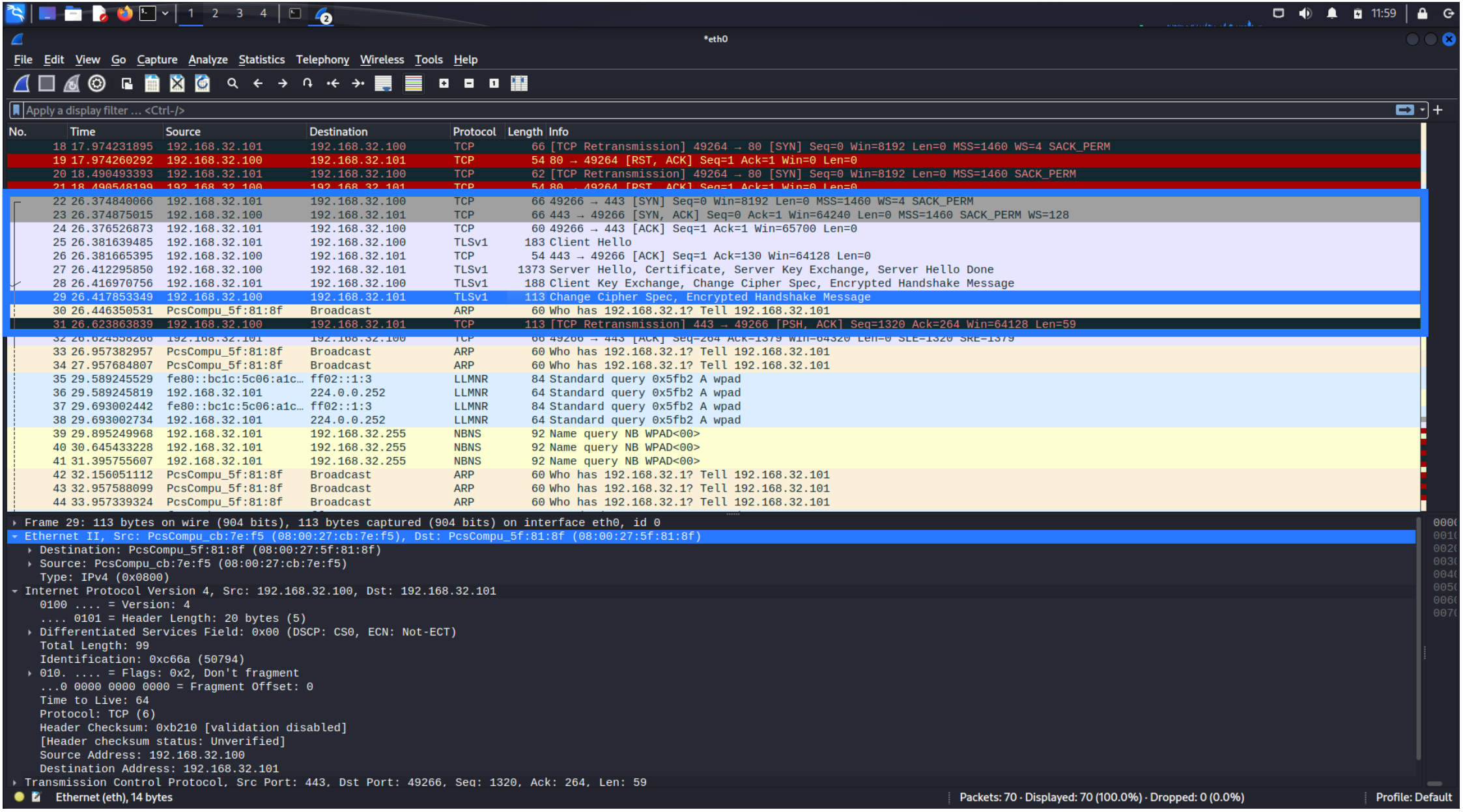

INetSim default HTML page - Windows Internet Explorer
http://epicode.internal/
Bing
Preferiti
Siti suggeriti
Raccolta Web Slice
INetSim default HTML page
Pagina
Sicurezza
Strumenti
This is the default HTML page for INetSim HTTP server fake mode.
This file is an HTML document.
Fine
Internet | Modalità protetta: attivata
100%
IT
14:27
24/11/2023


INetSim default HTML page - Windows Internet Explorer
https://epicode.internal/
Errore certificato
Bing
Preferiti
Siti suggeriti
Raccolta Web Slice
INetSim default HTML page
Pagina
Sicurezza
Strumenti
This is the default HTML page for INetSim HTTP server fake mode.
This file is an HTML document.
Fine
Internet | Modalità protetta: attivata
100%
IT
14:26
24/11/2023



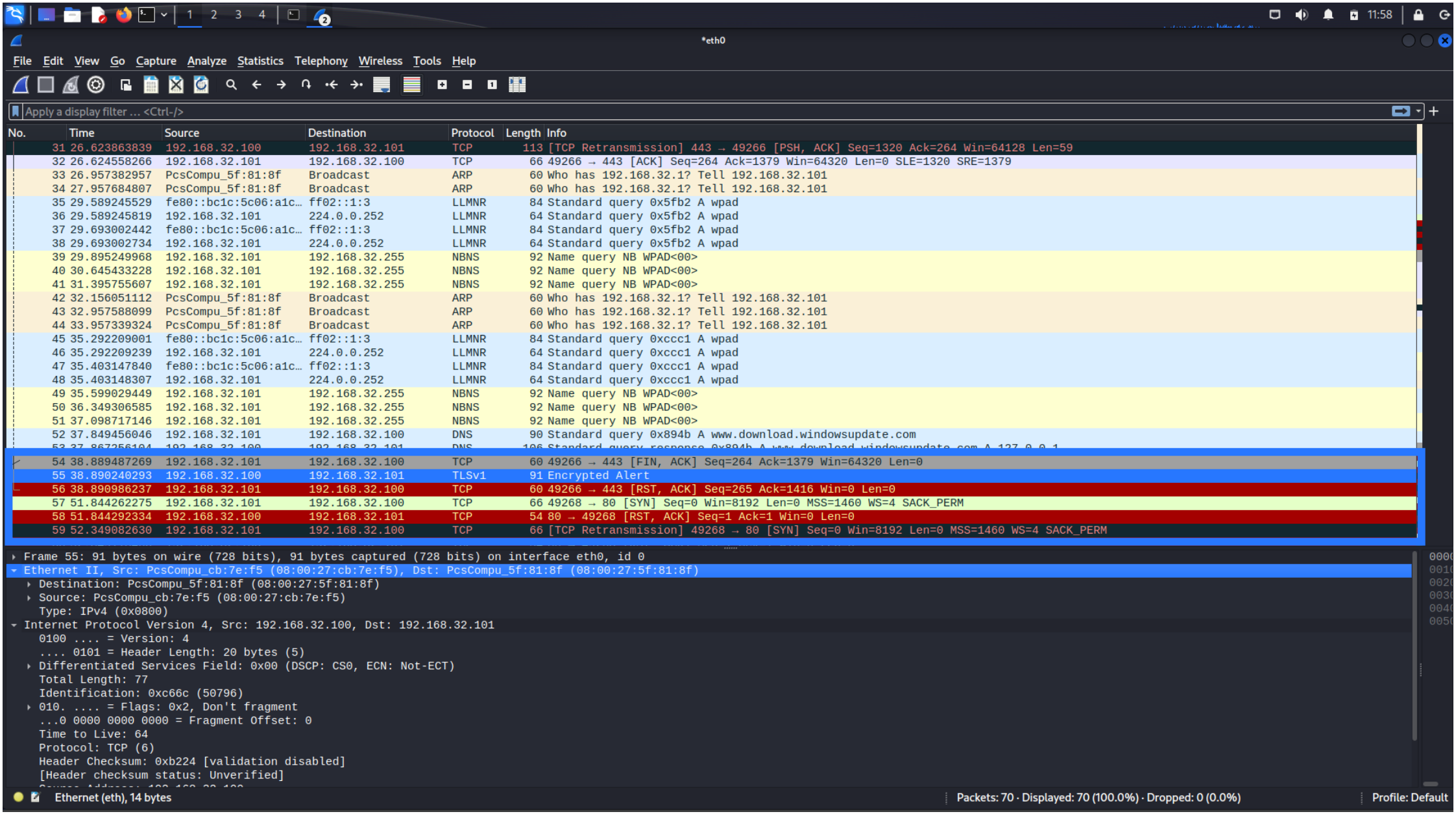
<u>RILEVATO IL PROTOCOLLO HTTP</u> , dove possiamo vedere tutto il contenuto .

Durante l'intercettazione dei dati grazie a Wireshark, si può notare che sia l'indizizzo IP che il contenuto sono visibili e non cifrati. I dati che viaggiano sulla rete sono esposti a potenziali attacchi per esempio quello di "man-in-the-middle", dove un utente malevolo intercetta i dati per rubarli ed utilizzare gli stessi in modo illecito.



RILEVATO IL PROTOCOLLO HTTPS, dove possiamo notare che i dati sono criptati.

Il traffico HTTPS mostra che il contenuto è cifrato, grazie al protocollo TLS, che fornisce un livello di sicurezza aggiuntivo nel caso degli attacchi provenienti da hacker malintenzionati. Ciò risulta fondamentale per quanto riguarda la trasmissione dei dati sensibili e personali, nonché password e dati finanziari.



Utilizzando il Wireshark e confrontando i due protocolli possiamo quindi affermare che , l'HTTP è esposto alla compromissione dei dati durante la loro trasmissione, invece l'HTTPS protegge il contenuto da potenziali minacce di intercettazione grazie alla crittografia della comunicazione. I MAC address sia di sorgente che della destinazione vengono evidenziati, ed è fondamentale per controllare e tracciare gli accessi ed i dispositivi all'interno di una rete.