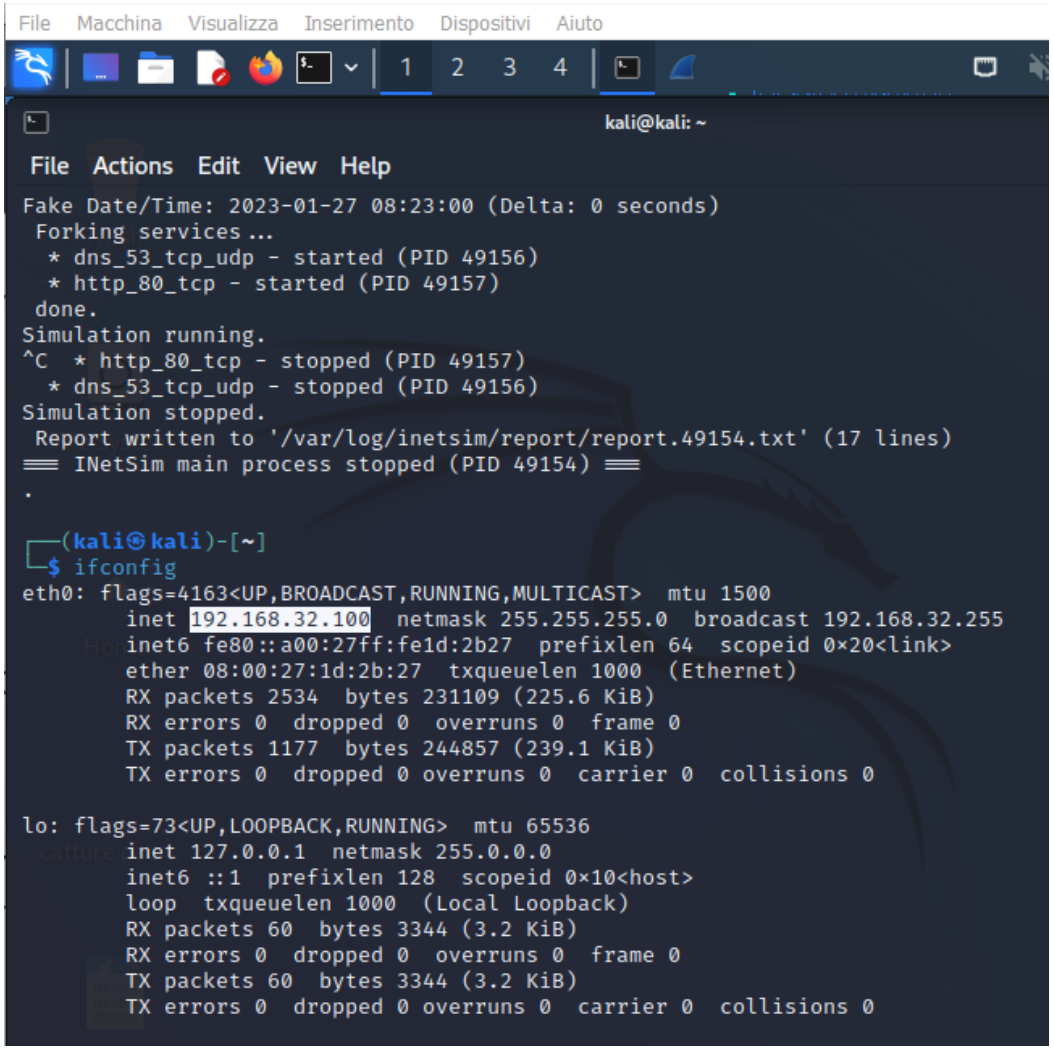
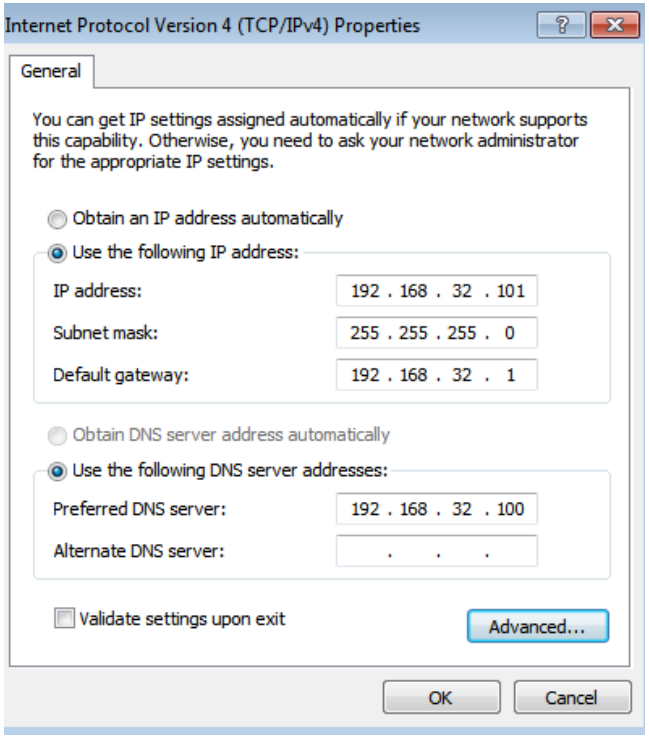
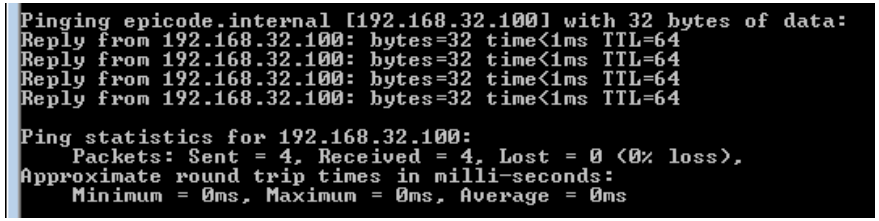






Modifica indirizzi IP e aggiunta server DNS su Windows (IP Kali)

Test di comunicazione con un ping

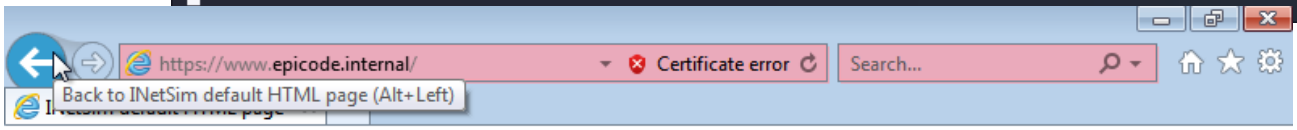
```
File  Actions  Edit  View  Help
 GNU nano 6.4                                  /etc/inetsim/inetsim.conf *
##########################################################
#
# INetSim configuration file
#
##########################################################


##########################################################
# Main configuration
##########################################################

########################################
# start_service
#
# 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
```

```
########################################
# 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: inetsim.org
#
dns_default_ip 192.168.32.100


########################################
# dns_default_hostname
#
# Default hostname to return with DNS replies
#
# Syntax: dns_default_hostname <hostname>
#
Default: www.epicode.internal
#
#dns_default_hostname somehost
```

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

```
┌──(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.
Warning: Unknown option 'Default:' in configuration file '/etc/inetsim/inetsim.conf' line 217
Configuration file parsed successfully.
=== INetSim main process started (PID 54791) ===
Session ID:     54791
Listening on:   192.168.32.100
Real Date/Time: 2023-01-27 08:45:43
Fake Date/Time: 2023-01-27 08:45:43 (Delta: 0 seconds)
 Forking services...
  * dns_53_tcp_udp - started (PID 54793)
  * https_443_tcp - started (PID 54794)
 done.
Simulation running.
```



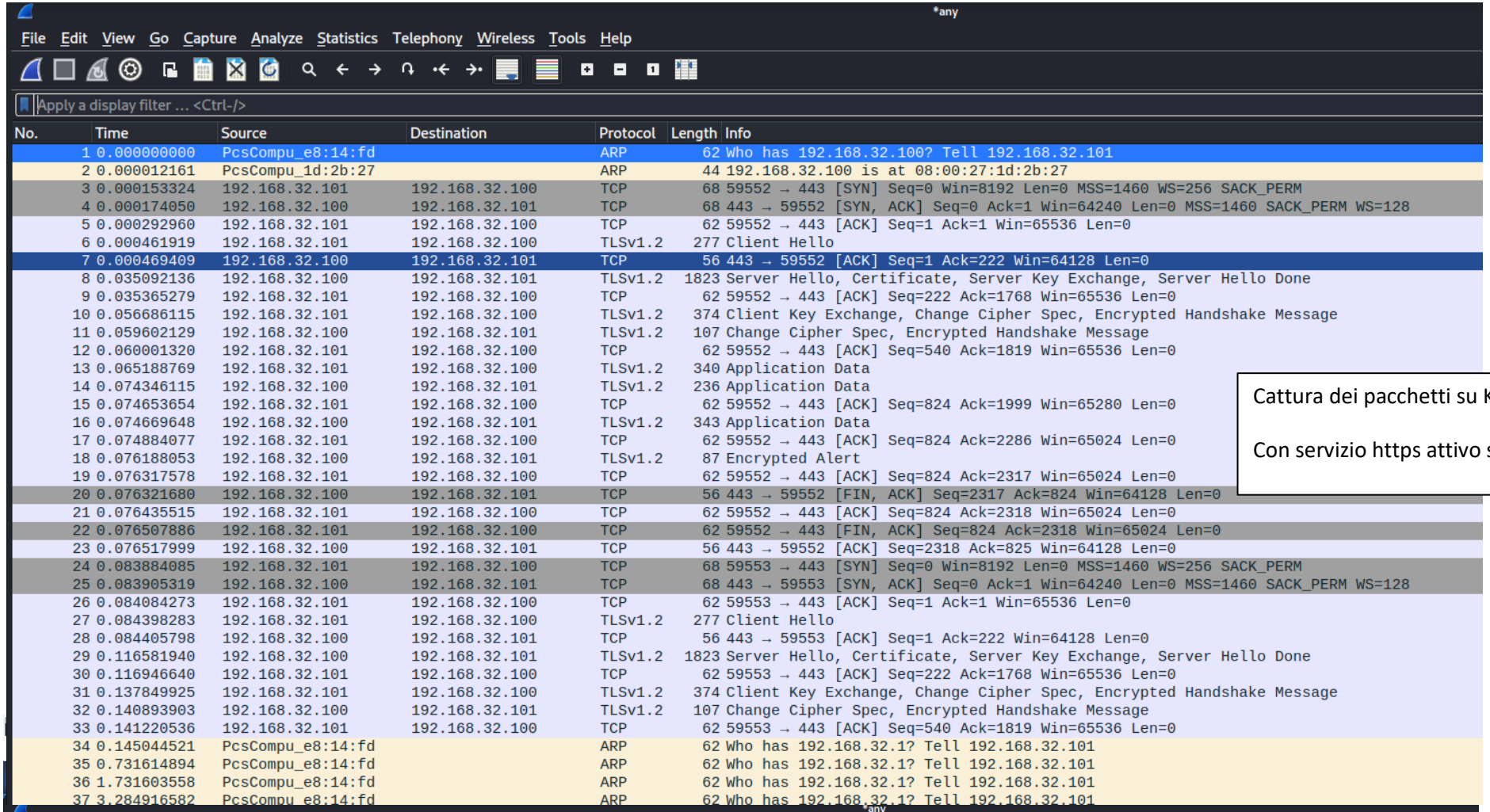
This is the default HTML page for INetSim HTTP server fake mode.

This file is an HTML document.

Modifica di inetsim in voci DNS e abilitazione servizi https e DNS.

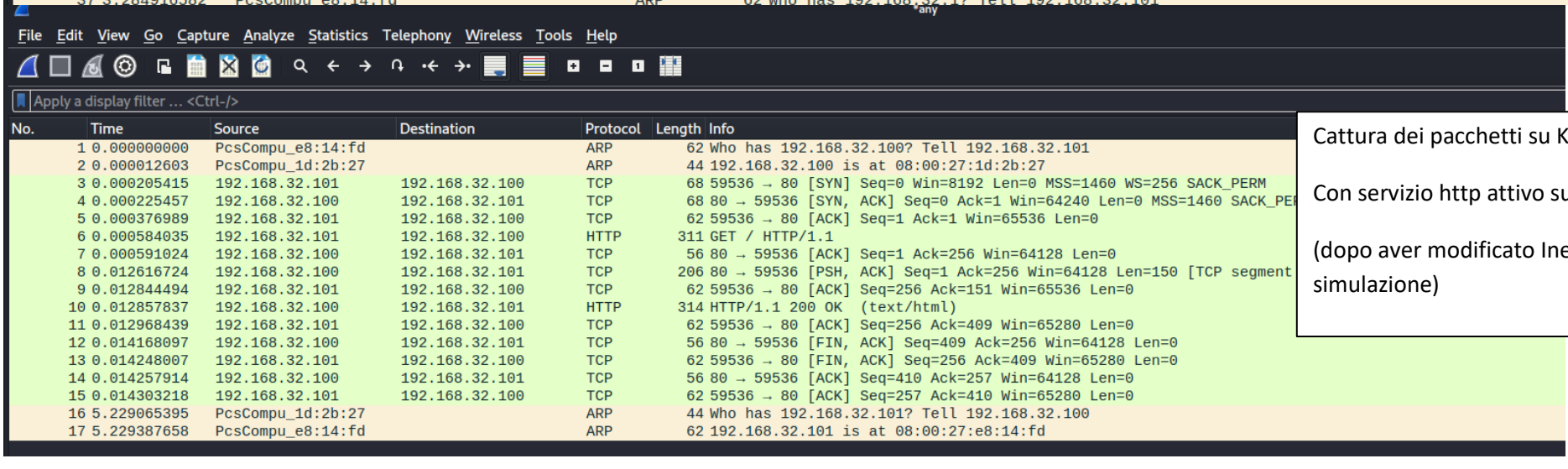
Attivazione simulazione

Ricerca di epicode.internal su browser di Windows



Cattura dei pacchetti su Kali con Whireshark

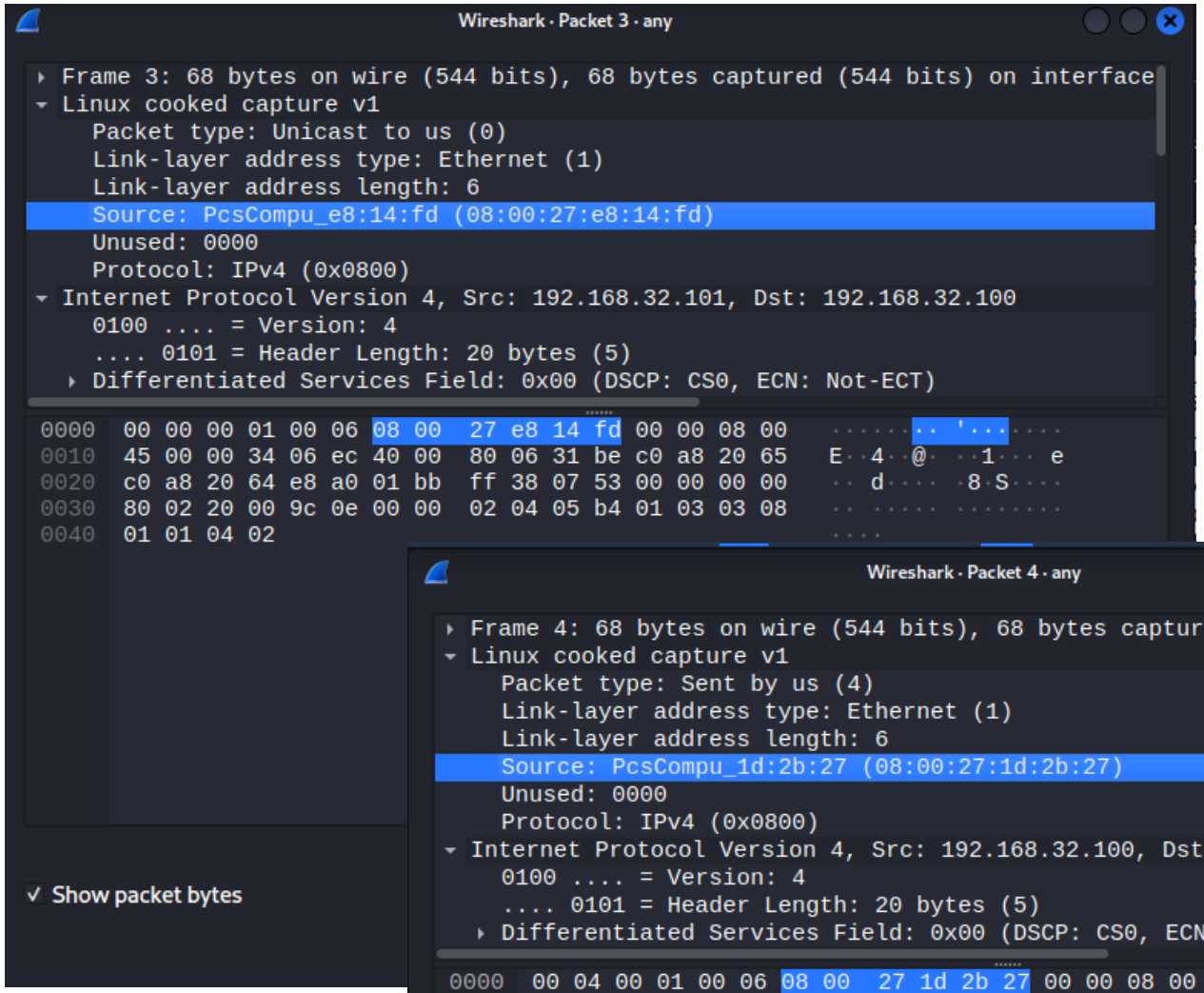
Con servizio https attivo su InetSim



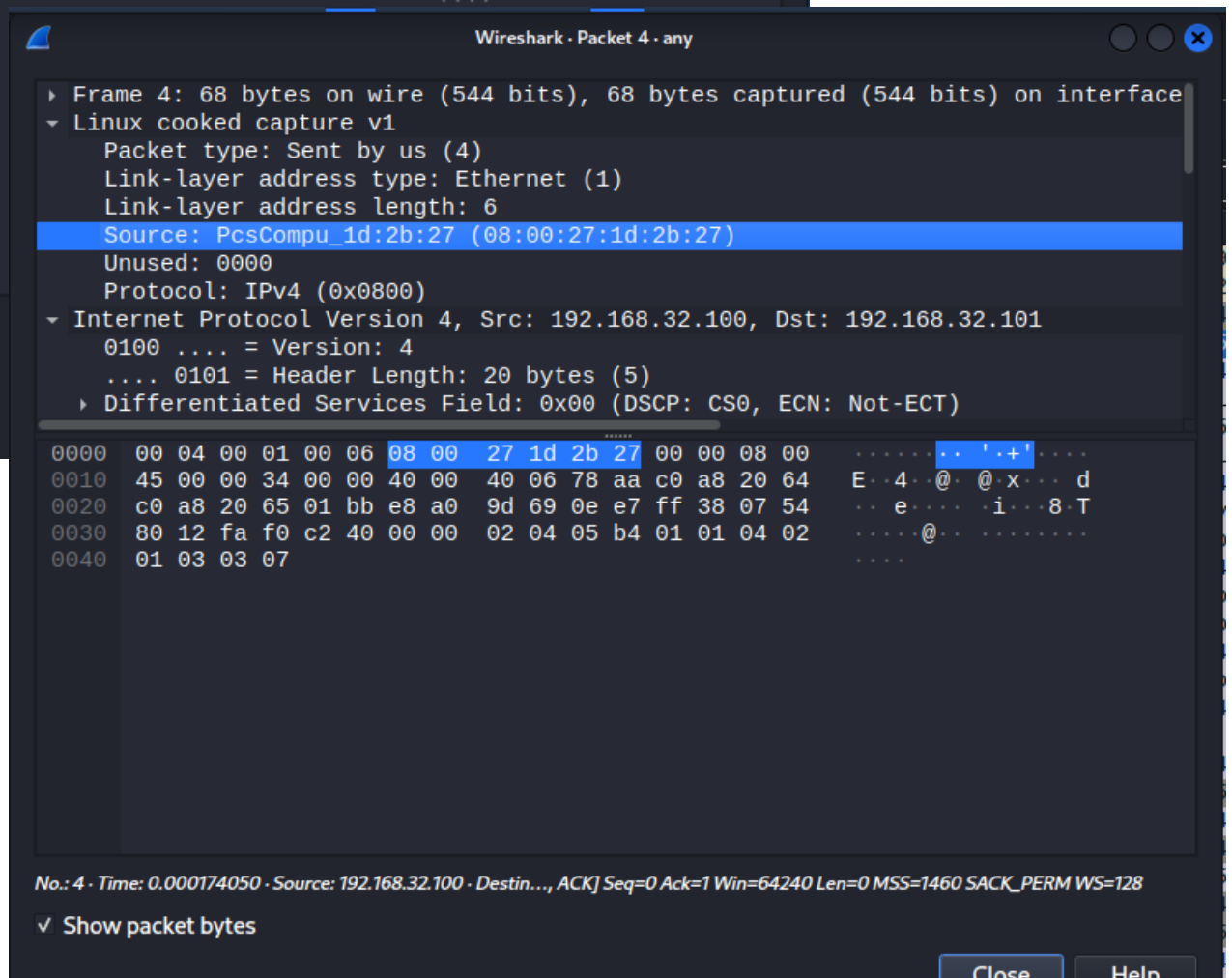
Cattura dei pacchetti su Kali con Whireshark

Con servizio http attivo su InetSim

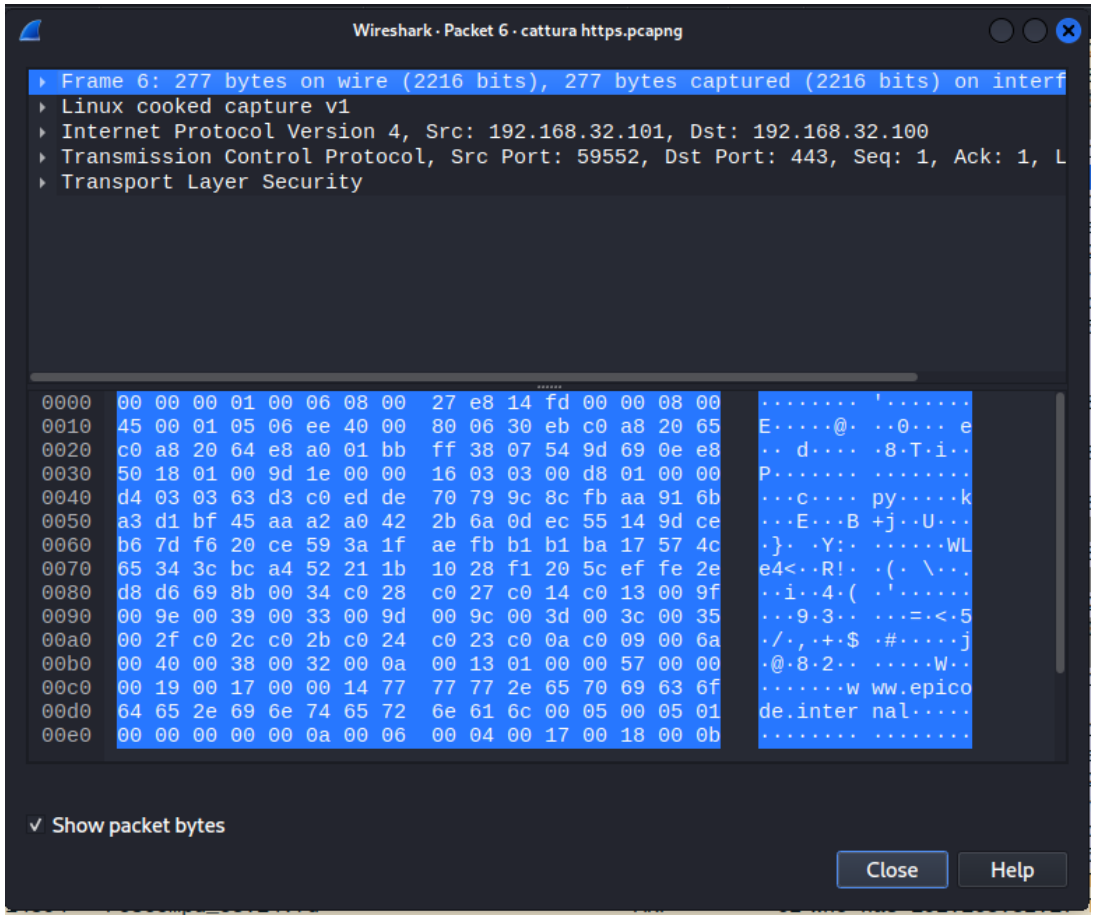
(dopo aver modificato InetSim e riavviato la simulazione)

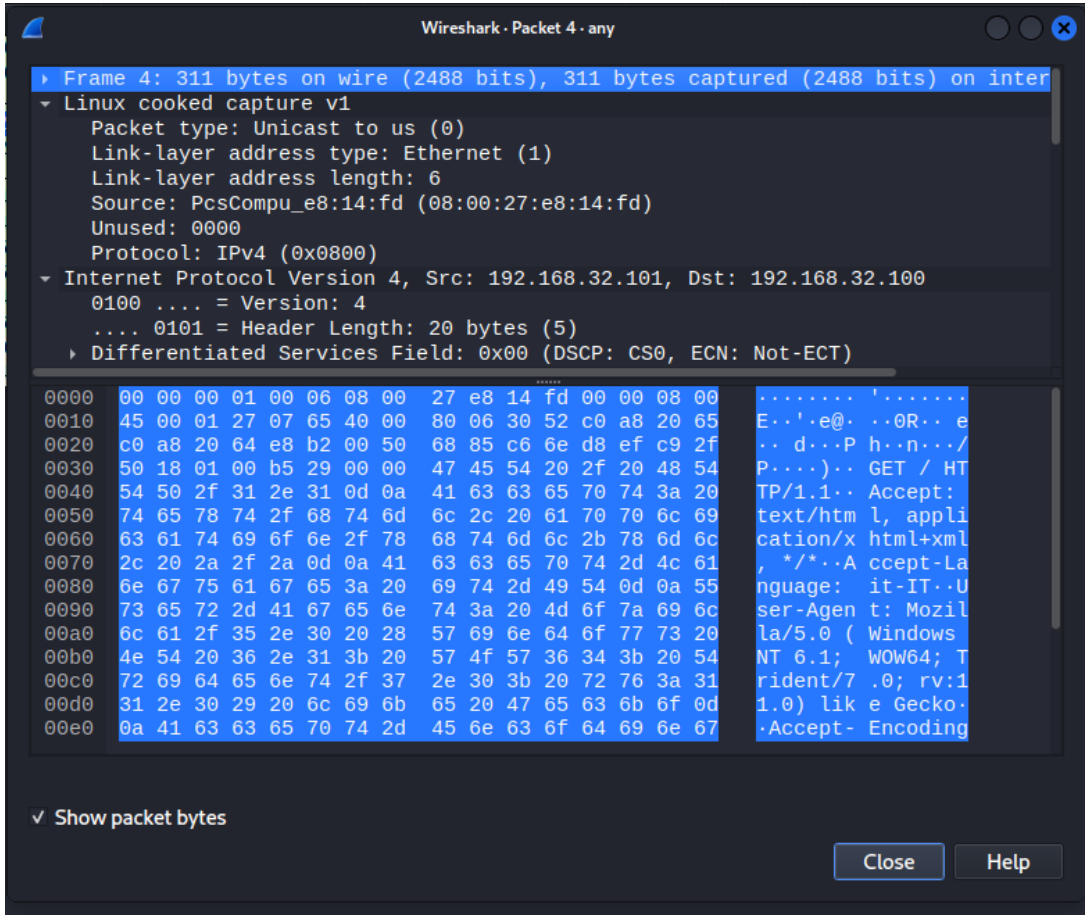


MAC Windows 7



MAC Kali Linux





Pacchetto cifratura dal protocollo di sicurezza di https

Pacchetto protocollo http

Pacchetto cifrato dal protocollo di sicurezza di https

Col protocollo http il contenuto del pacchetto rimane in chiaro, leggibile da Whireshark.

Questa oltre alla differenza di porte dedicate (443 per https e 80 per http), è la differenza più grande tra i due.