Benchmark M1

esercitazione finale modulo 1

Ignazio Saba

INTRODUZIONE

in questa esercitazione simuliamo una comunicazione client server e ne catturiamo i risultati tramite wireshark

il server sarà simulato tramite kali e inetsim a cui attiveremo i servizi dns, http e https

il server sarà così configurato-

IP: 192.168.32.100

netmask: 255.255.255.0

gateway: 192.168.32.1

DNS: 192.168.32.100

il client sarà simulato tramite Windows 7 e sarà così configurato-

IP: 192.168.32.101

netmask: 255.255.255.0

gateway: 192.168.32.1

DNS: 192.168.32.100

configurazioni

network

```
  GNU nano 7.2
# This file describes the network inte
# and how to activate them. For more i

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
dns 192.168.32.100
```

inetsim services

```
# 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
#start_service ftps
#start_service tftp
#start_service irc
#start_service ntp
```

```
##########################################
# service_bind_address
#
# IP address to bind services to
#
# Syntax: service_bind_address <IP address>
#
# Default: 127.0.0.1
#
service_bind_address 0.0.0.0
```

```
##########################################
# dns_default_ip
#
# Default IP address to return with DNS replies
#
# Syntax: dns_default_ip <IP address>
#
# Default: 127.0.0.1
#
dns_default_ip 192.168.32.100
```

```
##########################################
# dns_default_domainname
#
# Default domain name to return with DNS replies
#
# Syntax: dns_default_domainname <domain name>
#
# Default: inetsim.org
#
dns_default_domainname epicode.internal
```

configurazioni

network windows 7

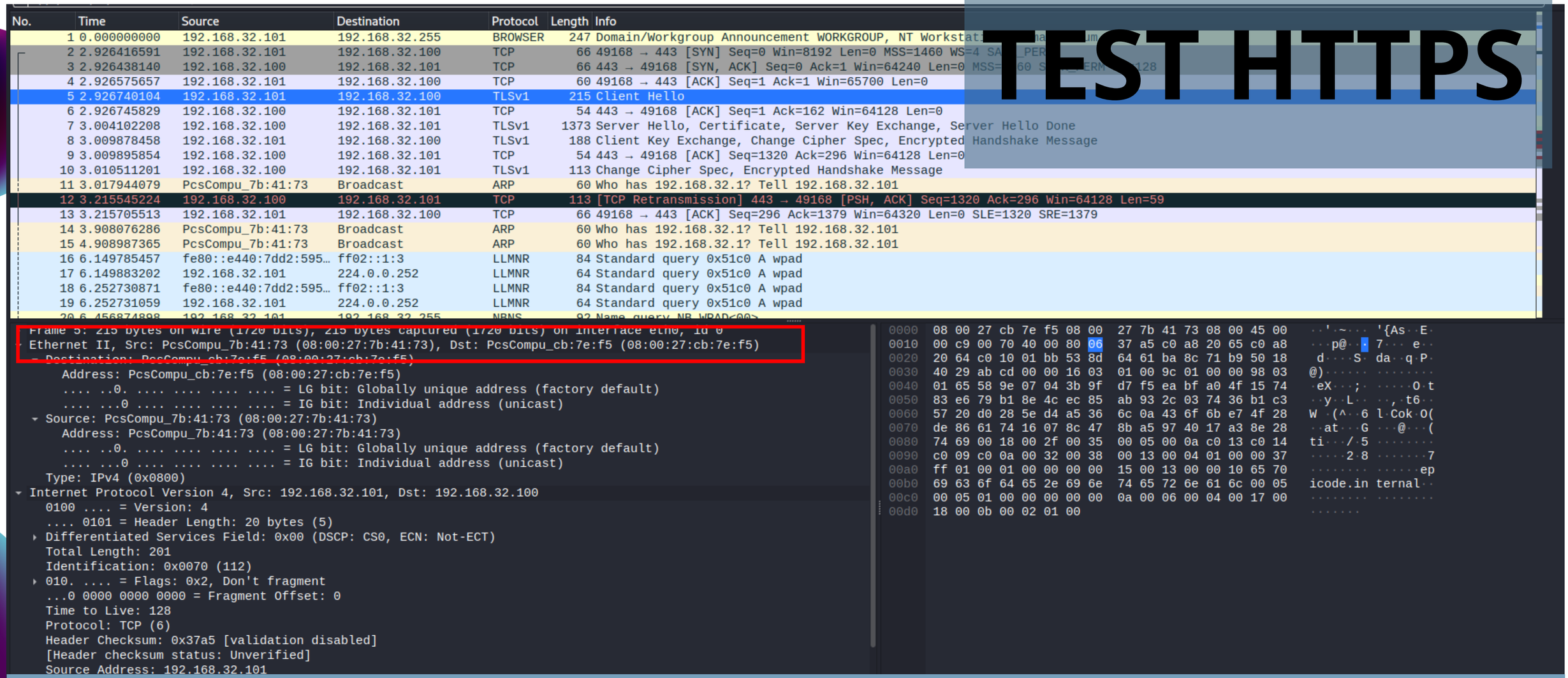
configurazioni

network windows 7

avvio servizi inetsim

```
┌──(kali㉿kali)-[/etc/inetsim]
└─$ 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 46002) ===
Session ID:     46002
Listening on:   0.0.0.0
Real Date/Time: 2023-11-18 07:48:58
Fake Date/Time: 2023-11-18 07:48:58 (Delta: 0 seconds)
 Forking services...
  * dns_53_tcp_udp - started (PID 46012)
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 46014)
  * http_80_tcp - started (PID 46013)
 done.
Simulation running.
```

TEST HTTPS

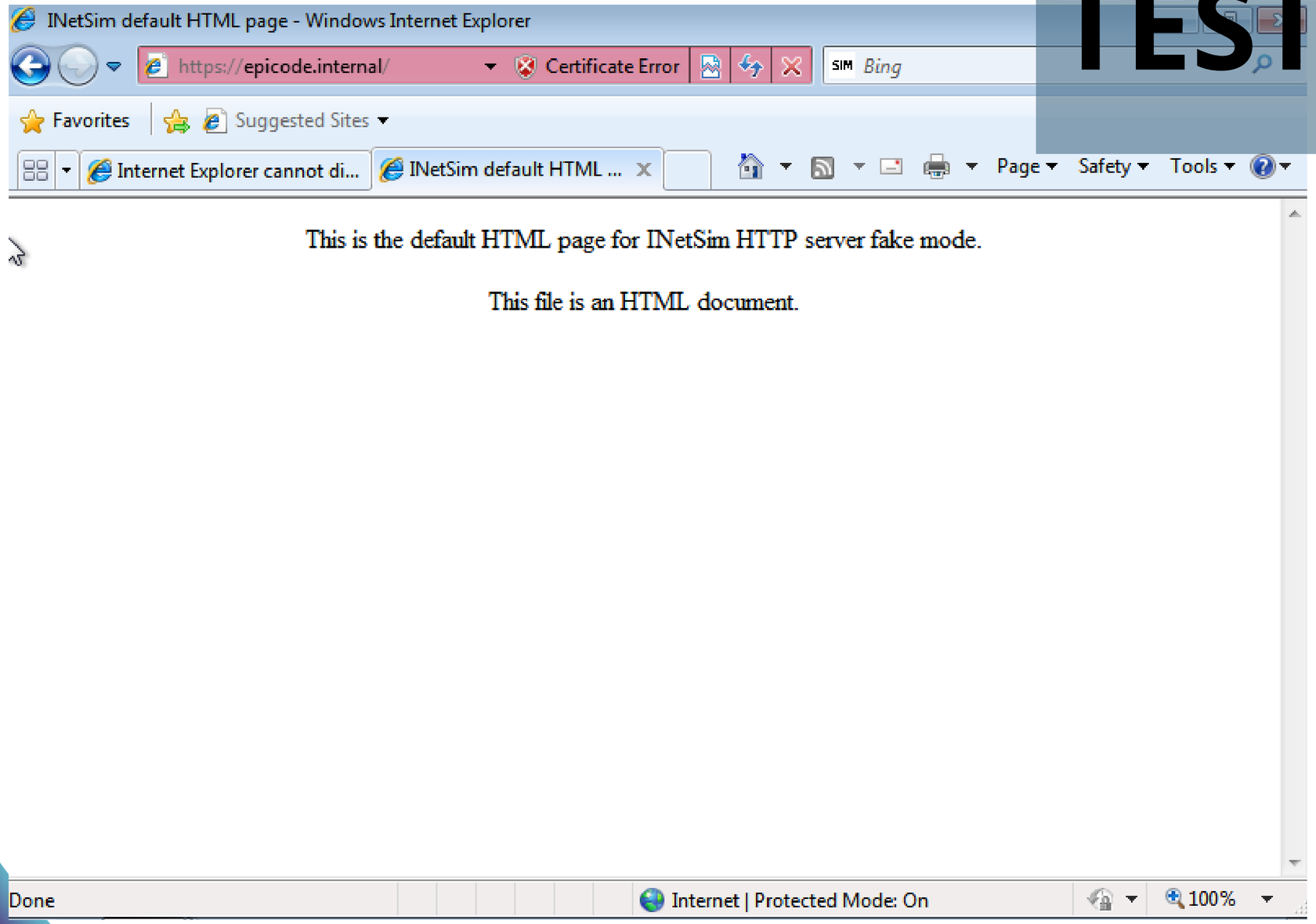


dalla riga 2 alla 4 possiamo vedere lo scambio di chiavi col tiple hand shake mentre le chiamate TLSV1 sono gli scambi dei pacchetti criptati

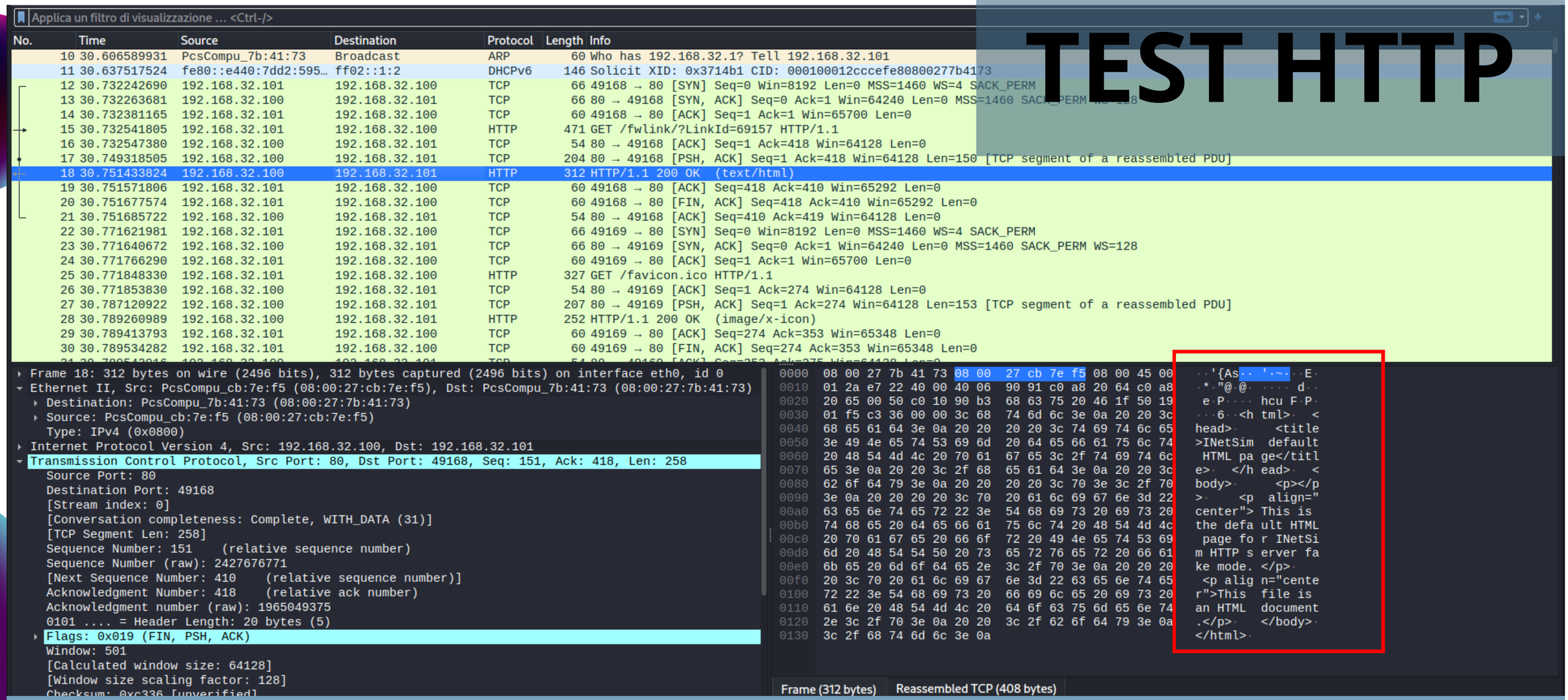
nel riquadro rosso vediamo i due mac address del client e server

source: 08:00:27:7b:41:73 destination: 08:00:27:cb:7e:f5

TEST HTTPS

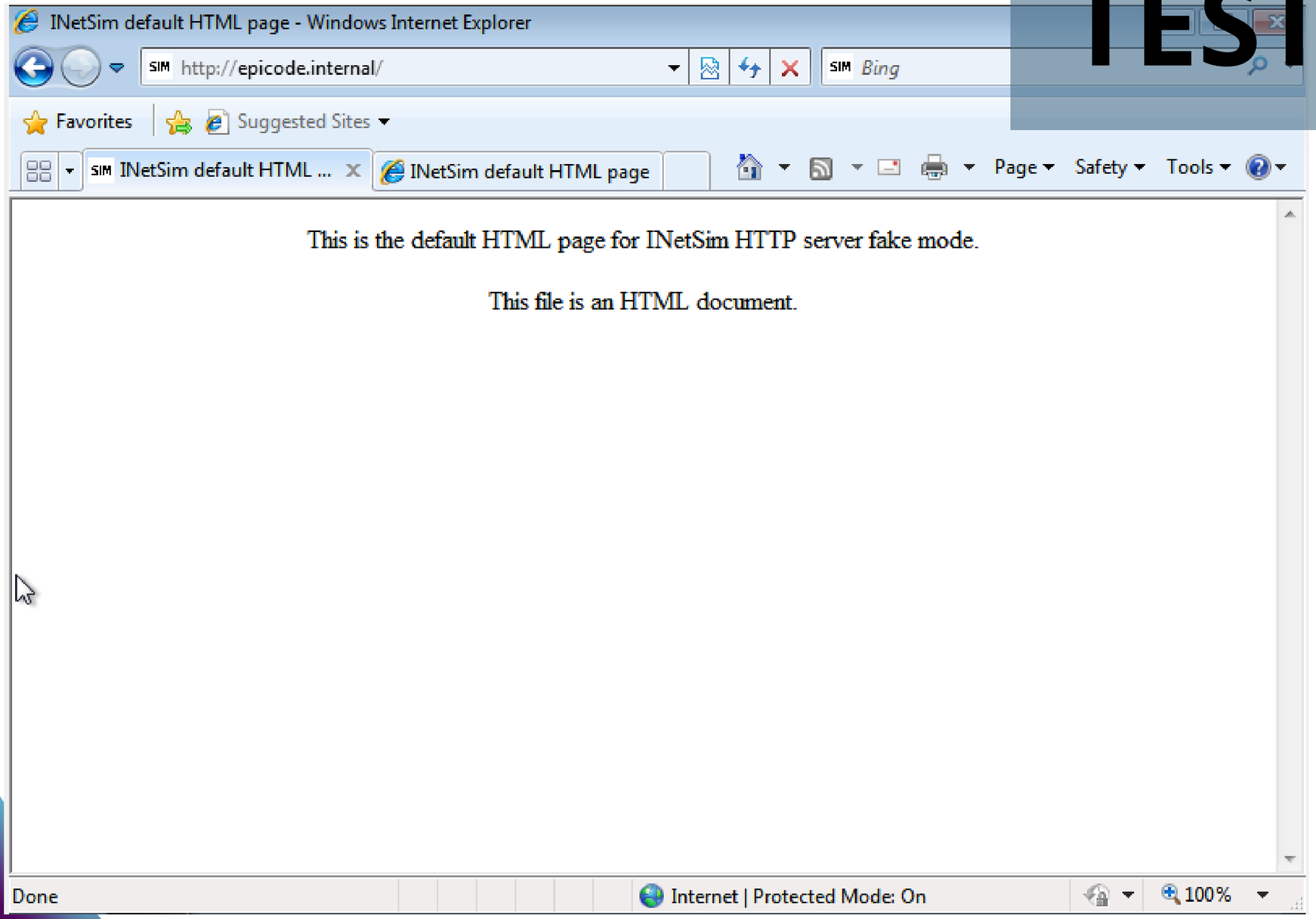

INetSim default HTML page - Windows Internet Explorer
https://epicode.internal/
Certificate Error
Bing
Favorites
Suggested Sites
Internet Explorer cannot di...
INetSim default HTML ...
Page
Safety
Tools
This is the default HTML page for INetSim HTTP server fake mode.
This file is an HTML document.
Done
Internet | Protected Mode: On
100%

TEST HTTP



A differenza delle chiamate https qui dopo lo scambio delle chiavi la trasmissione delle informazioni è in chiaro, come si può vedere nella riga selezionata, nel riquadro rosso vediamo il contenuto della pagina http

TEST HTTP


INetSim default HTML page - Windows Internet Explorer
http://epicode.internal/
Bing
Favorites
Suggested Sites
INetSim default HTML ...
INetSim default HTML page
Page
Safety
Tools
This is the default HTML page for INetSim HTTP server fake mode.
This file is an HTML document.
Done
Internet | Protected Mode: On
100%