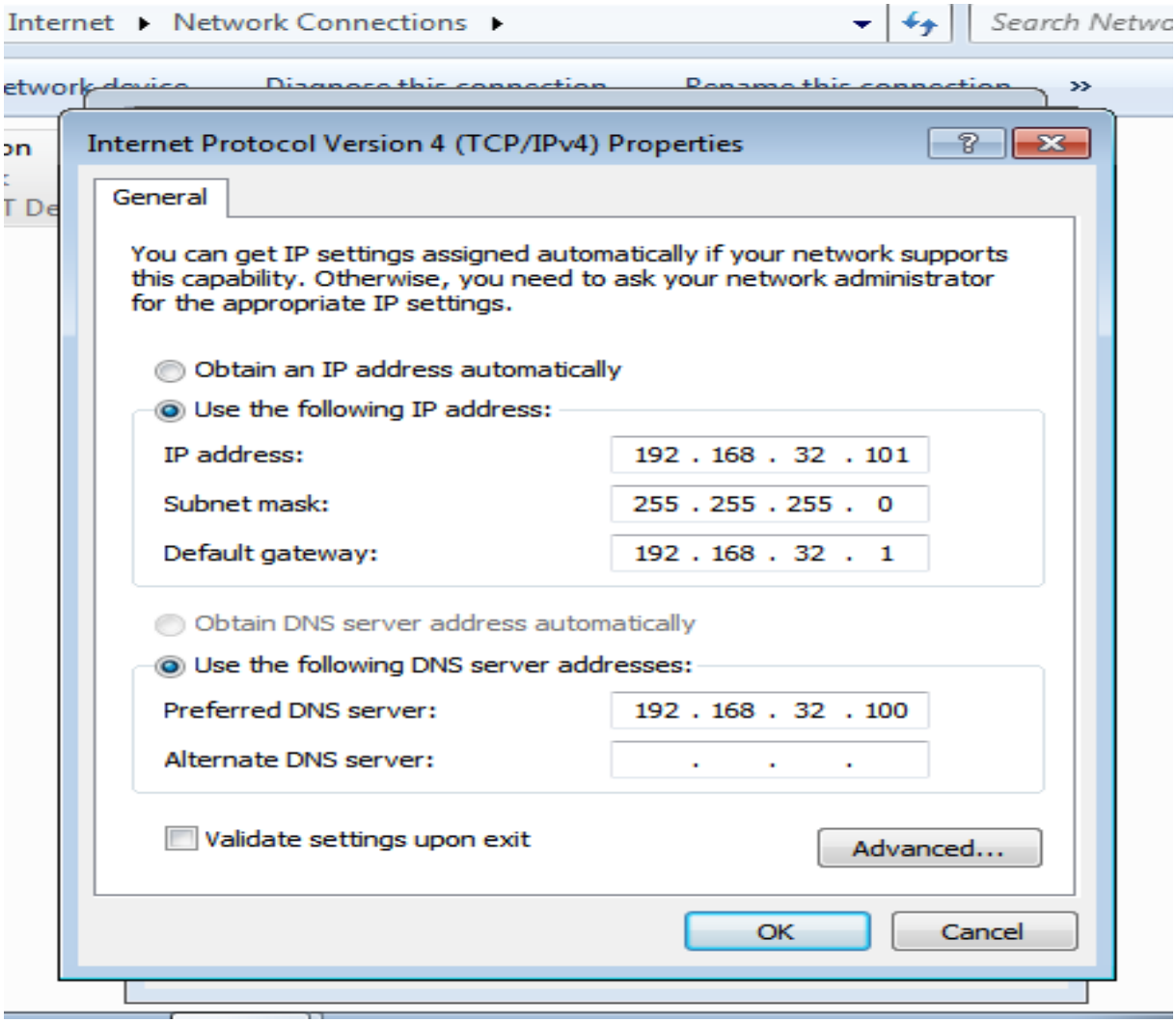
ESERCIZIO 27.01.2023

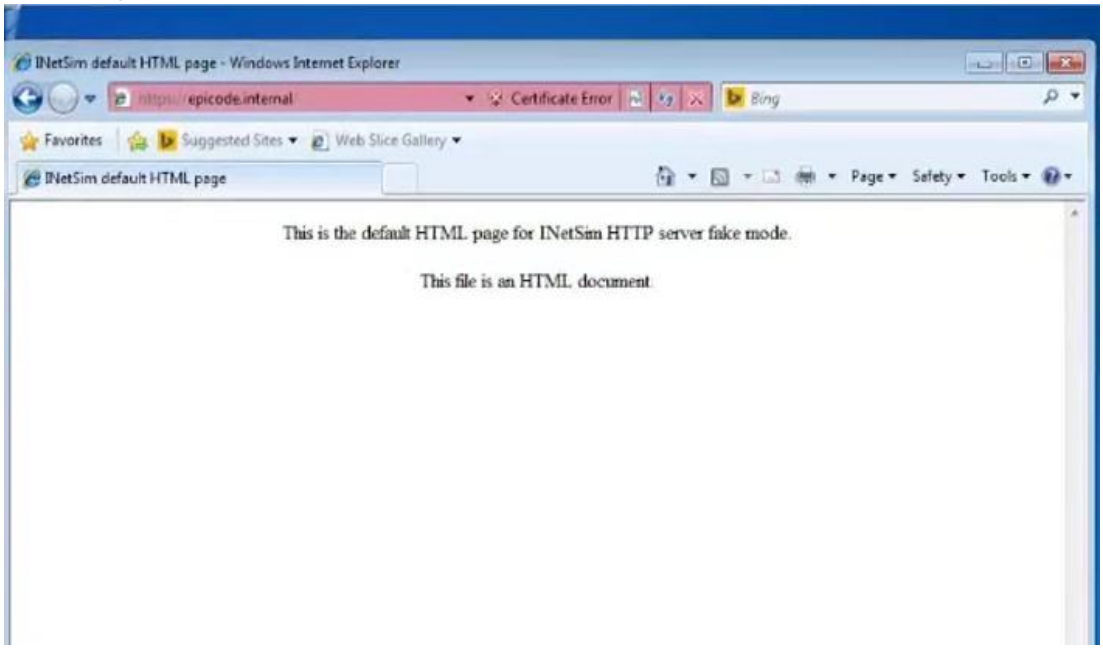
Per prima cosa ho configurato gli Ip statici di server e client, nello Screenshot mostro come ho fatto in Windows con ip 192.168.32.101, in Kali da terminale con il comando sudo nano etc/network/interfaces configurando ip 192.168.32.100



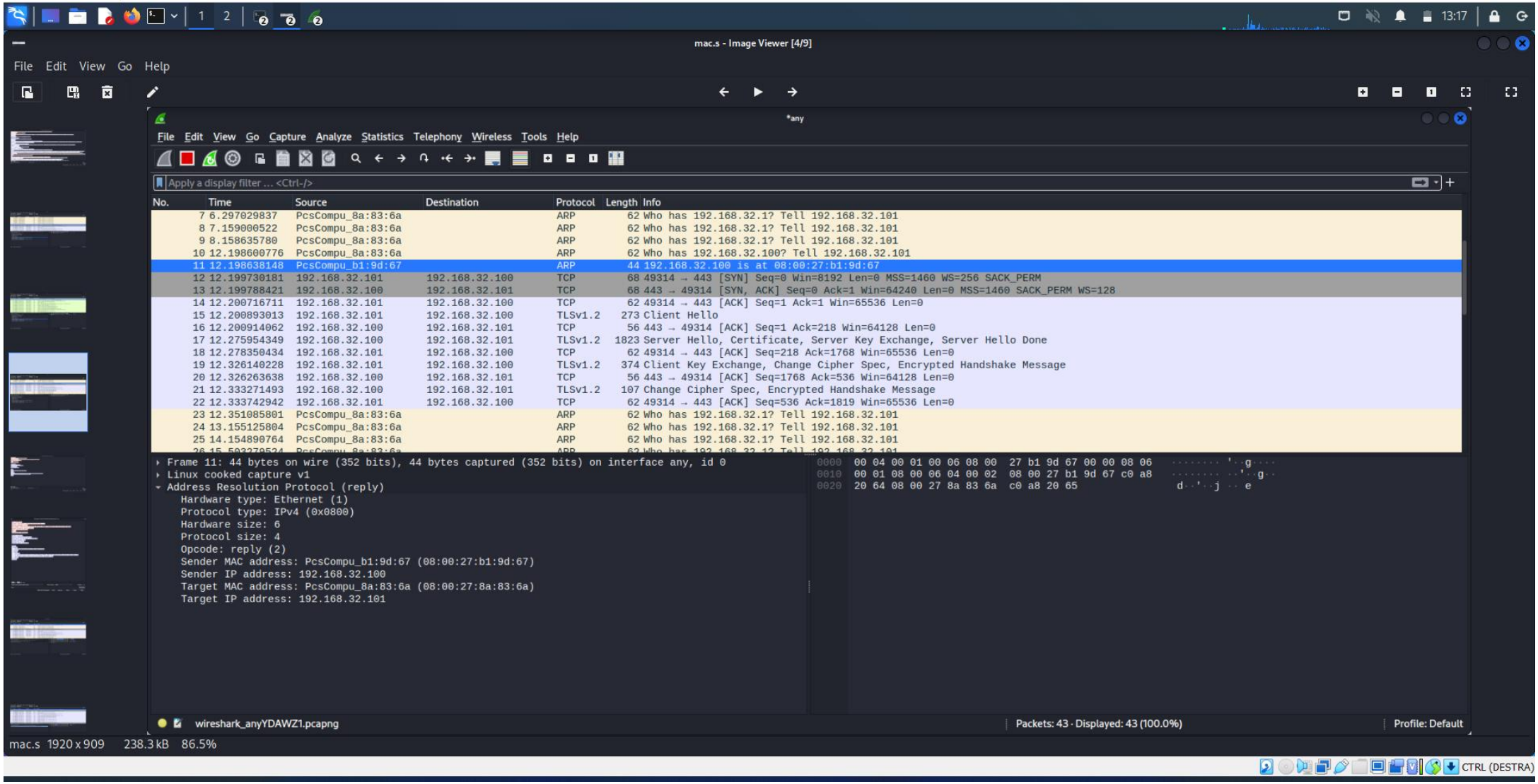
Dopo aver digitato il comando sudo nano etc/inetesim/inetsim.conf Ho-configurato in kali linux i servizi dns http e https. In seguito ho avviato il comando sudo inetsim per iniziare la simulazione

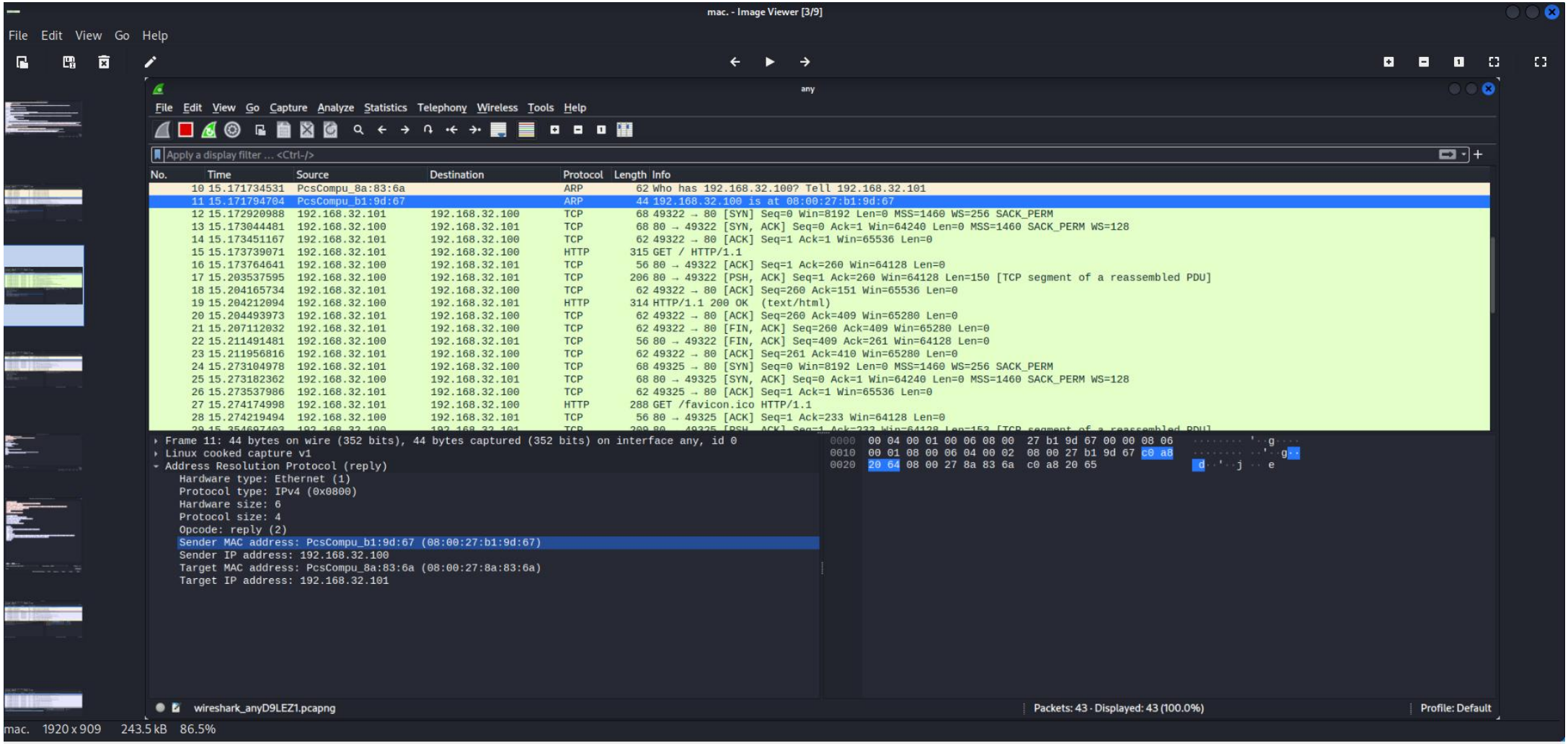
```
#
start_service dns
start_service http
start_service https
#start_service smtp
#start_service smtps
#start_service pop3
#start_service pop3s
#start_service ftp
#start_service ftps
#start_service tftp
#start_service irc
#start_service ntp
#start_service finger
#start_service ident
#start_service syslog
#start_service time_tcp
#start_service time_udp
#start_service daytime_tcp
#start_service daytime_udp
#start_service echo_tcp
Save modified buffer?
 Y Yes
 N No            ^C Cancel
```

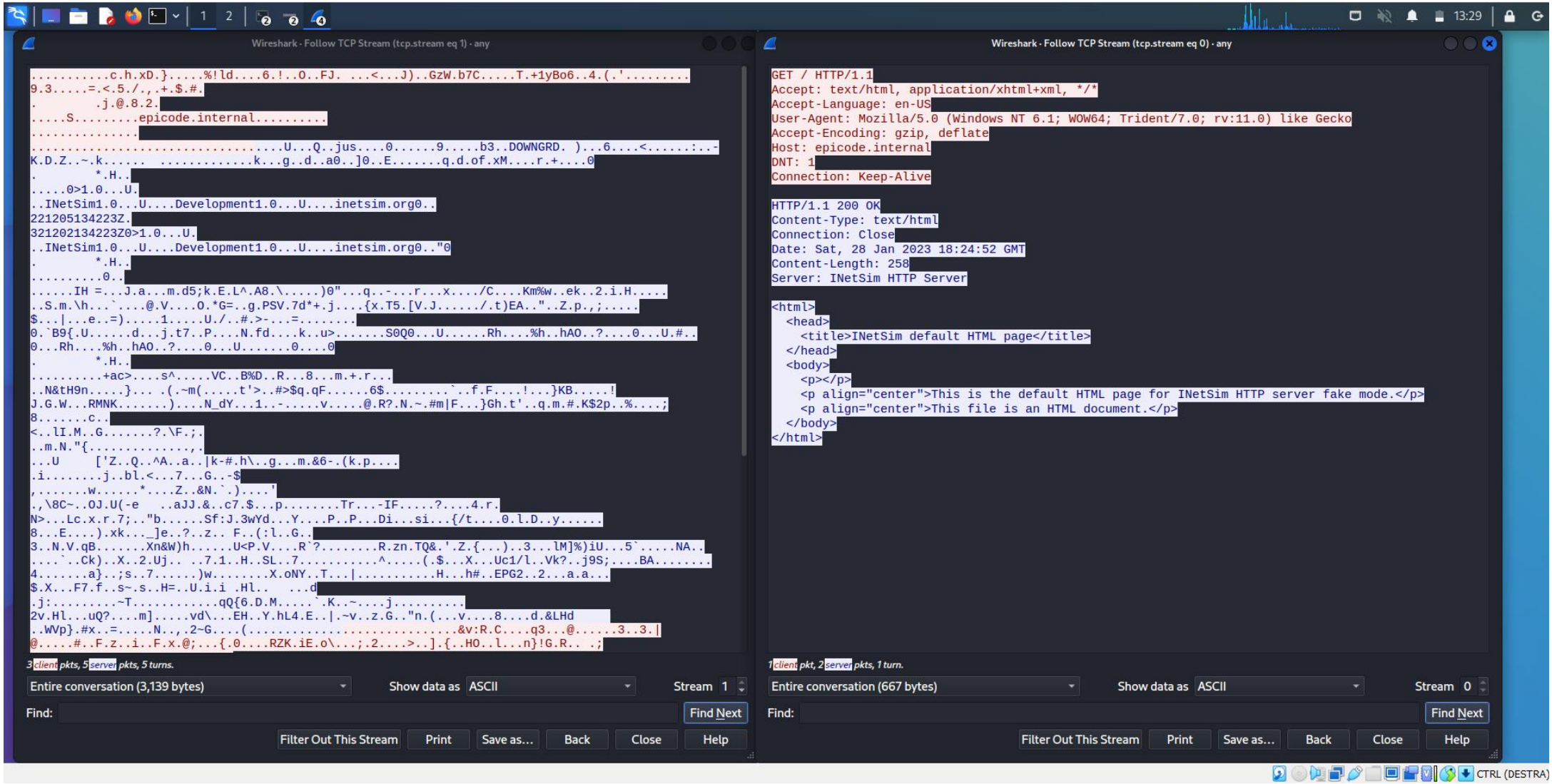
In questo passaggio ho cercato sulla barra di ricerca di explorer in windows il link https://epicode.internal e ho sniffato con wireshark, ho fatto lo stesso con http dato che avevo attivato entrambi i servizi



Negli screen a seguire mostro la cattura di wireshark, con gli indirizzi mac sorgente e destinazione in evidenza, di Http e Https.
Faccio vedere anche la differenza più grande tra le due catture. Controllando il pacchetto dati in http farà vedere il contenuto della richiesta in chiaro, mentre in https creare un messaggio cifrato prima di inviare i dati


mac.s - Image Viewer [4/9]
File Edit View Go Help
*any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
7 6.297029837 PcsCompu_8a:83:6a ARP 62 Who has 192.168.32.1? Tell 192.168.32.101
8 7.159000522 PcsCompu_8a:83:6a ARP 62 Who has 192.168.32.1? Tell 192.168.32.101
9 8.158635780 PcsCompu_8a:83:6a ARP 62 Who has 192.168.32.1? Tell 192.168.32.101
10 12.198600776 PcsCompu_8a:83:6a ARP 62 Who has 192.168.32.100? Tell 192.168.32.101
11 12.198638148 PcsCompu_b1:9d:67 ARP 44 192.168.32.100 is at 08:00:27:b1:9d:67
12 12.199730181 192.168.32.101 192.168.32.100 TCP 68 49314 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
13 12.199788421 192.168.32.100 192.168.32.101 TCP 68 443 → 49314 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
14 12.200716711 192.168.32.101 192.168.32.100 TCP 62 49314 → 443 [ACK] Seq=1 Ack=1 Win=65536 Len=0
15 12.200893013 192.168.32.101 192.168.32.100 TLSv1.2 273 Client Hello
16 12.200914062 192.168.32.100 192.168.32.101 TCP 56 443 → 49314 [ACK] Seq=1 Ack=218 Win=64128 Len=0
17 12.275954349 192.168.32.100 192.168.32.101 TLSv1.2 1823 Server Hello, Certificate, Server Key Exchange, Server Hello Done
18 12.278350434 192.168.32.101 192.168.32.100 TCP 62 49314 → 443 [ACK] Seq=218 Ack=1768 Win=65536 Len=0
19 12.326140228 192.168.32.101 192.168.32.100 TLSv1.2 374 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
20 12.326263638 192.168.32.100 192.168.32.101 TCP 56 443 → 49314 [ACK] Seq=1768 Ack=536 Win=64128 Len=0
21 12.333271493 192.168.32.100 192.168.32.101 TLSv1.2 107 Change Cipher Spec, Encrypted Handshake Message
22 12.333742942 192.168.32.101 192.168.32.100 TCP 62 49314 → 443 [ACK] Seq=536 Ack=1819 Win=65536 Len=0
23 12.351085801 PcsCompu_8a:83:6a ARP 62 Who has 192.168.32.1? Tell 192.168.32.101
24 13.155125804 PcsCompu_8a:83:6a ARP 62 Who has 192.168.32.1? Tell 192.168.32.101
25 14.154890764 PcsCompu_8a:83:6a ARP 62 Who has 192.168.32.1? Tell 192.168.32.101
Frame 11: 44 bytes on wire (352 bits), 44 bytes captured (352 bits) on interface any, id 0
Linux cooked capture v1
Address Resolution Protocol (reply)
Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: reply (2)
Sender MAC address: PcsCompu_b1:9d:67 (08:00:27:b1:9d:67)
Sender IP address: 192.168.32.100
Target MAC address: PcsCompu_8a:83:6a (08:00:27:8a:83:6a)
Target IP address: 192.168.32.101
0000 00 04 00 01 00 06 08 00 27 b1 9d 67 00 00 08 06
0010 00 01 08 00 06 04 00 02 08 00 27 b1 9d 67 c0 a8
0020 20 64 08 00 27 8a 83 6a c0 a8 20 65
wireshark_anyYDAWZ1.pcapng
Packets: 43 · Displayed: 43 (100.0%)
Profile: Default
mac.s 1920 x 909 238.3 kB 86.5%
CTRL (DESTRA)


mac. - Image Viewer [3/9]
File Edit View Go Help
any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
10 15.171734531 PcsCompu_8a:83:6a ARP 62 Who has 192.168.32.100? Tell 192.168.32.101
11 15.171794704 PcsCompu_b1:9d:67 ARP 44 192.168.32.100 is at 08:00:27:b1:9d:67
12 15.172920988 192.168.32.101 192.168.32.100 TCP 68 49322 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
13 15.173044481 192.168.32.100 192.168.32.101 TCP 68 80 → 49322 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
14 15.173451167 192.168.32.101 192.168.32.100 TCP 62 49322 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
15 15.173739071 192.168.32.101 192.168.32.100 HTTP 315 GET / HTTP/1.1
16 15.173764641 192.168.32.100 192.168.32.101 TCP 56 80 → 49322 [ACK] Seq=1 Ack=260 Win=64128 Len=0
17 15.203537595 192.168.32.100 192.168.32.101 TCP 206 80 → 49322 [PSH, ACK] Seq=1 Ack=260 Win=64128 Len=150 [TCP segment of a reassembled PDU]
18 15.204165734 192.168.32.101 192.168.32.100 TCP 62 49322 → 80 [ACK] Seq=260 Ack=151 Win=65536 Len=0
19 15.204212094 192.168.32.100 192.168.32.101 HTTP 314 HTTP/1.1 200 OK (text/html)
20 15.204493973 192.168.32.101 192.168.32.100 TCP 62 49322 → 80 [ACK] Seq=260 Ack=409 Win=65280 Len=0
21 15.207112032 192.168.32.101 192.168.32.100 TCP 62 49322 → 80 [FIN, ACK] Seq=260 Ack=409 Win=65280 Len=0
22 15.211491481 192.168.32.100 192.168.32.101 TCP 56 80 → 49322 [FIN, ACK] Seq=409 Ack=261 Win=64128 Len=0
23 15.211956816 192.168.32.101 192.168.32.100 TCP 62 49322 → 80 [ACK] Seq=261 Ack=410 Win=65280 Len=0
24 15.273104978 192.168.32.101 192.168.32.100 TCP 68 49325 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
25 15.273182362 192.168.32.100 192.168.32.101 TCP 68 80 → 49325 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
26 15.273537986 192.168.32.101 192.168.32.100 TCP 62 49325 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
27 15.274174998 192.168.32.101 192.168.32.100 HTTP 288 GET /favicon.ico HTTP/1.1
28 15.274219494 192.168.32.100 192.168.32.101 TCP 56 80 → 49325 [ACK] Seq=1 Ack=233 Win=64128 Len=0
Frame 11: 44 bytes on wire (352 bits), 44 bytes captured (352 bits) on interface any, id 0
Linux cooked capture v1
Address Resolution Protocol (reply)
Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: reply (2)
Sender MAC address: PcsCompu_b1:9d:67 (08:00:27:b1:9d:67)
Sender IP address: 192.168.32.100
Target MAC address: PcsCompu_8a:83:6a (08:00:27:8a:83:6a)
Target IP address: 192.168.32.101
0000 00 04 00 01 00 06 08 00 27 b1 9d 67 00 00 08 06
0010 00 01 08 00 06 04 00 02 08 00 27 b1 9d 67 c0 a8
0020 20 64 08 00 27 8a 83 6a c0 a8 20 65
wireshark_anyD9LEZ1.pcapng
Packets: 43 · Displayed: 43 (100.0%)
Profile: Default
mac. 1920 x 909 243.5 kB 86.5%


Wireshark · Follow TCP Stream (tcp.stream eq 1) · any
.....c.h.xD.}.....%!ld....6.!..O..FJ. ...<...J)..GzW.b7C.....T.+1yBo6..4.(.'.....
9.3....=.<.5./.,.+.$.#.
. .j.@.8.2.
.....S.....epicode.internal.....
.....
.....U...Q..jus....0.....9.....b3..DOWNGRD.)...6....<.....:..-
K.D.Z..~.k..... .....k...g..d..a0..]0..E.....q.d.of.xM....r.+....0
. *.H..
.....0>1.0...U.
..INetSim1.0...U....Development1.0...U....inetsim.org0..
221205134223Z.
321202134223Z0>1.0...U.
..INetSim1.0...U....Development1.0...U....inetsim.org0.."0
. *.H..
.....0..
.....IH =...J.a...m.d5;k.E.L^.A8.\.....)0"...q..-...r...x..../C....Km%w..ek..2.i.H.....
..S.m.\h...`....@.V....O.*G=..g.PSV.7d*+.j....{x.T5.[V.J...../.t)EA.."..Z.p.,;.....
$...|...e..=).....1.....U./..#.>-...=.....
0.`B9{.U.....d...j.t7..P....N.fd....k..u>.....S0Q0...U.....Rh....%h..hAO..?....0...U.#..
0...Rh....%h..hAO..?....0...U.....0....0
. *.H..
.....+ac>....s^.....VC..B%D..R...8...m.+.r...
..N&tH9n.....}... .(.~m(.....t'>..#>$q.qF.....6$.....`..f.F....!...}KB.....!
J.G.W...RMNK.....)....N_dY...1..-.....v.....@.R?.N.~.#m|F...}Gh.t'..q.m.#.K$2p..%....;
8.....c..
<..lI.M..G.....?.\F.;.
..m.N."{.....,.
...U ['Z..Q..^A..a..|k-#.h\..g...m.&6-.(k.p....
.i.....j..bl.<...7...G..-$
,.....w.....*....Z..&N.`.)....'
.,\8C~..OJ.U(-e ..aJJ.&..c7.$...p.....Tr...-IF.....?....4.r.
N>...Lc.x.r.7;.."b.....Sf:J.3wYd...Y....P..P...Di...si...{/t....0.l.D..y.....
8...E....).xk..._]e..?..z.. F..(:l..G..
3..N.V.qB.....Xn&W)h.....U<P.V....R`?.....R.zn.TQ&.'.Z.{...)..3...lM]%)iU...5`.....NA..
....`..Ck)..X..2.Uj.. ..7.1..H..SL..7.....^.....(.$...X...Uc1/l..Vk?..j9S;....BA.....
4.....a}..;s..7.....)w.....X.oNY..T...|.....H...h#..EPG2..2...a.a...
$.X...F7.f..s~.s..H=..U.i.i .Hl.. ...d
.j:.....~T.....qQ{6.D.M.....`.K..~....j.....
2v.Hl...uQ?....m].....vd\...EH..Y.hL4.E..|.~v..z.G.."n.(...v....8....d.&LHd
..WVp}.#x..=.....N..,.2~G....(.....&v:R.C....q3...@.....3..3.|
@.....#..F.z..i..F.x.@;...{.0....RZK.iE.o\..;.2....>..].{..HO..l...n}!G.R.. .;
3 client pkts, 5 server pkts, 5 turns.
Entire conversation (3,139 bytes)
Show data as ASCII
Stream 1
Find:
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help
Wireshark · Follow TCP Stream (tcp.stream eq 0) · any
GET / HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: epicode.internal
DNT: 1
Connection: Keep-Alive
HTTP/1.1 200 OK
Content-Type: text/html
Connection: Close
Date: Sat, 28 Jan 2023 18:24:52 GMT
Content-Length: 258
Server: INetSim HTTP Server
<html>
<head>
<title>INetSim default HTML page</title>
</head>
<body>

This is the default HTML page for INetSim HTTP server fake mode.
This file is an HTML document.
</body>
</html>
1 client pkt, 2 server pkts, 1 turn.
Entire conversation (667 bytes)
Show data as ASCII
Stream 0
Find:
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help