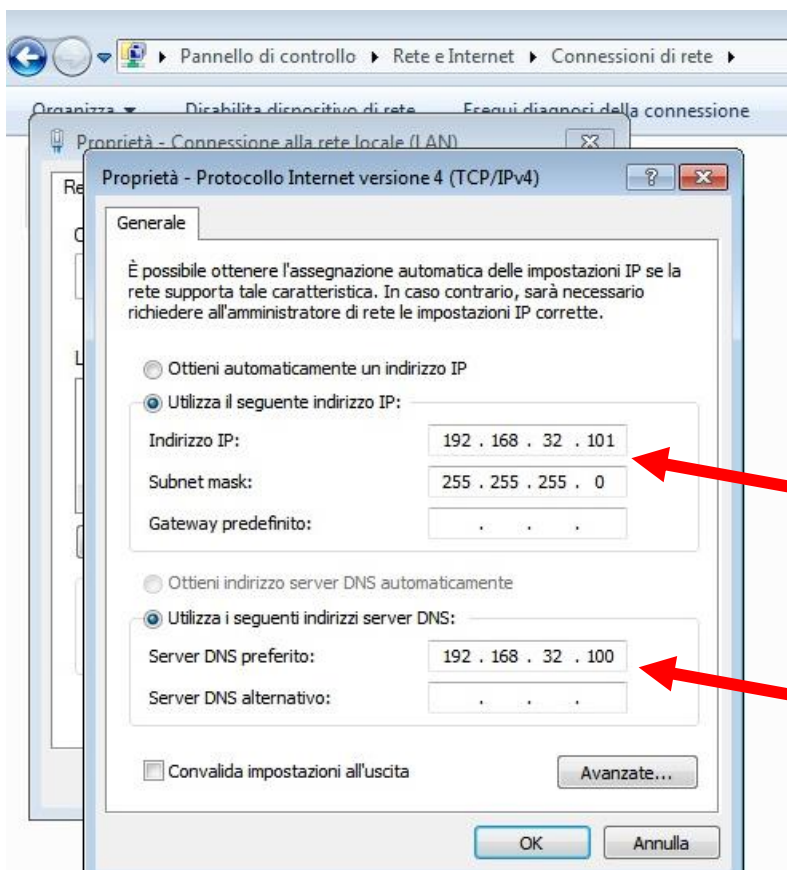
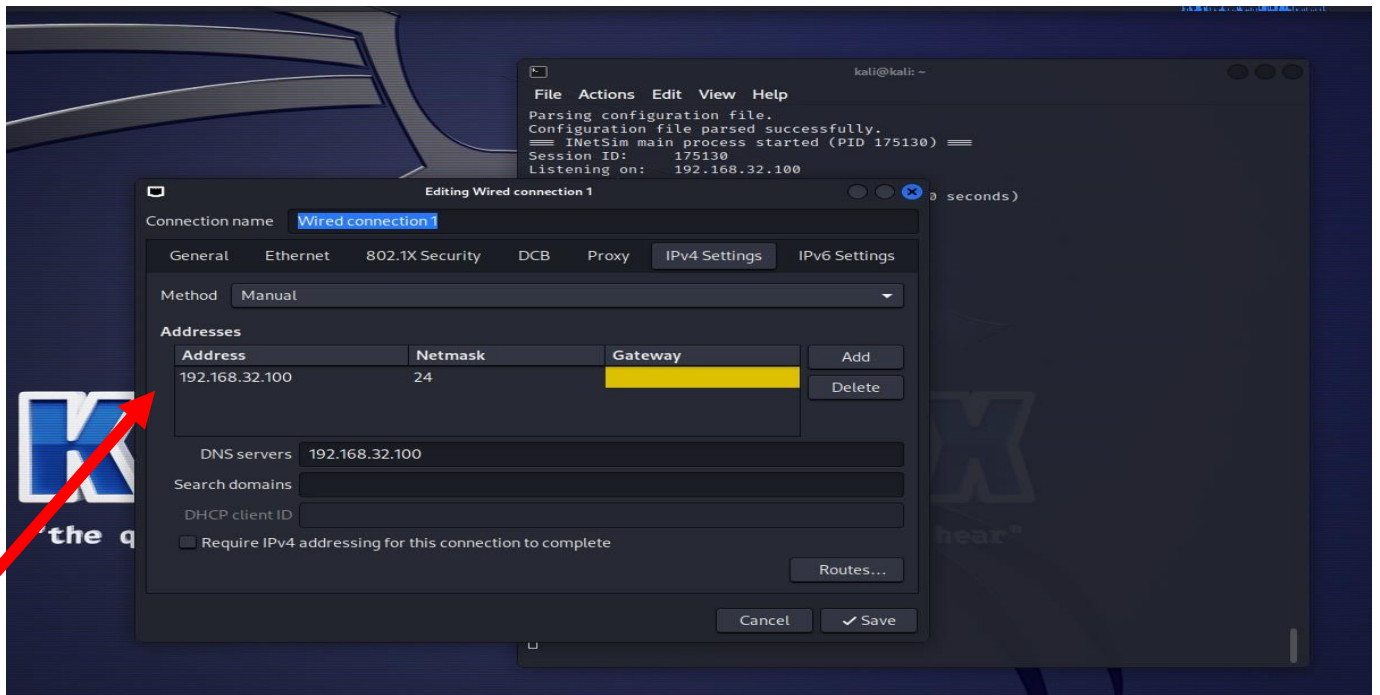


HOMEWORK 05/05/2023

STEP 1:

- **Kali Linux:** modifica IP in **192.168.32.100** e DNS servers in **192.168.32.100**
- **Windows 7:** modifica IP **192.168.32.101** e DNS server predefinito in **192.168.32.100**



STEP 2:

- Ho avviato Kali con permessi di root mediante comando ***sudo mousepad /etc/inetsim/inetsim.config*** (figura 1);
- (Previa rimozione di Modifica stringa #) service_bind_address con IP di Kali Linux ***192.168.32.100*** (figura 2);
- (Previa rimozione di #) Modifica stringa dns_default_ip con IP di Kali Linux ***192.168.32.100*** (figura 3);
- (Previa rimozione di #) Modifica stringa dns_static in ***epicode.internal 192.168.32.100*** (figura 4);
- Ho avviato la simulazione del server tramite Inetsim con il comando ***sudo inetsim*** (figura 5);

Figura 1 Ho avviato Kali con permessi di root mediante comando ***sudo mousepad /etc/inetsim/inetsim.config***

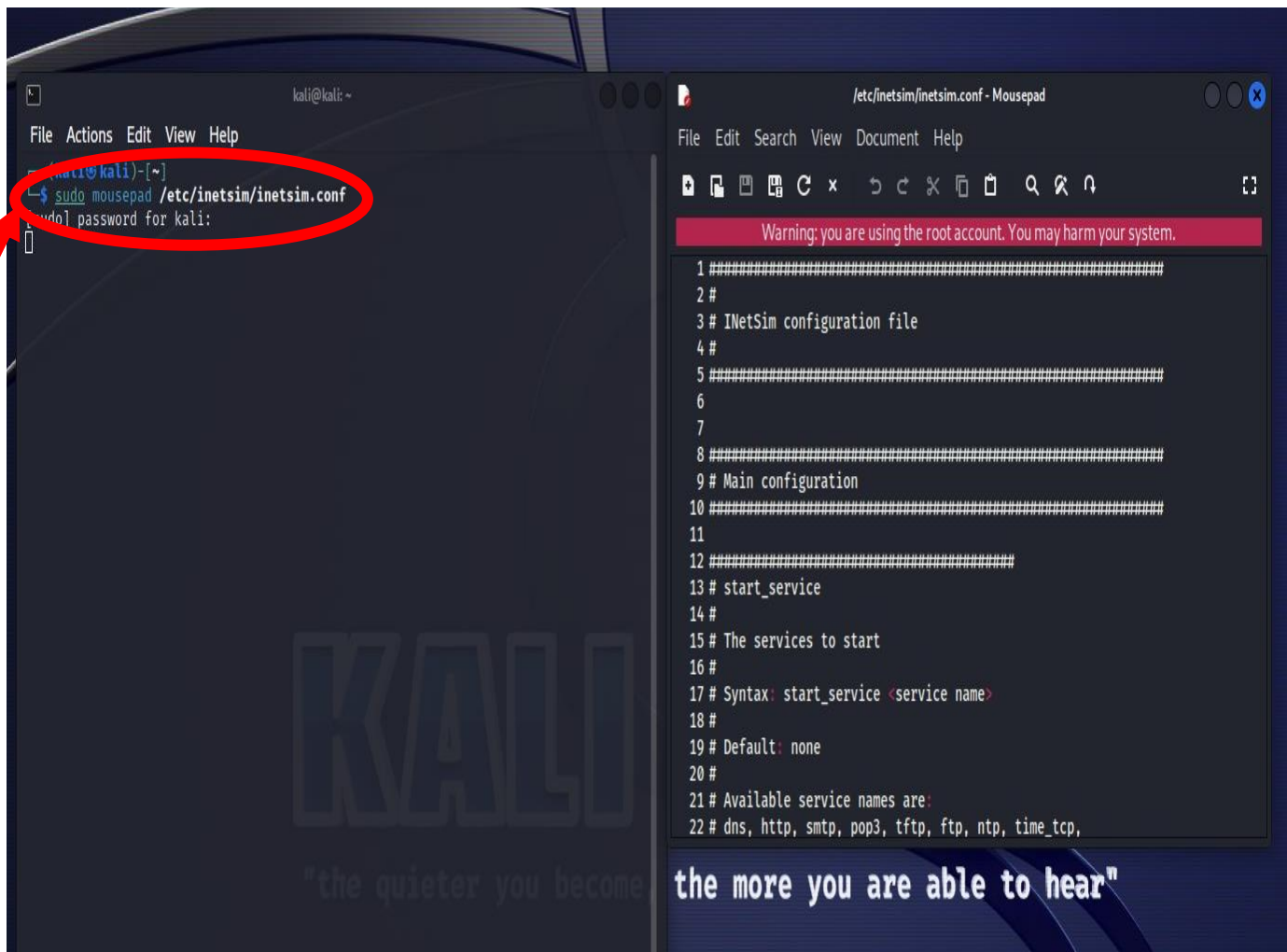
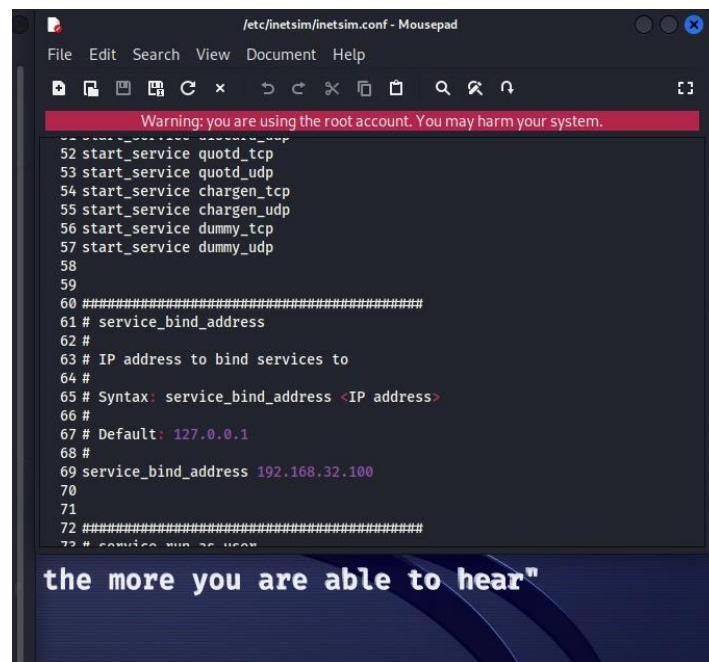


Figura 2 (Previa rimozione di #) Modifica stringa service_bind_address con IP di Kali Linux 192.168.32.100

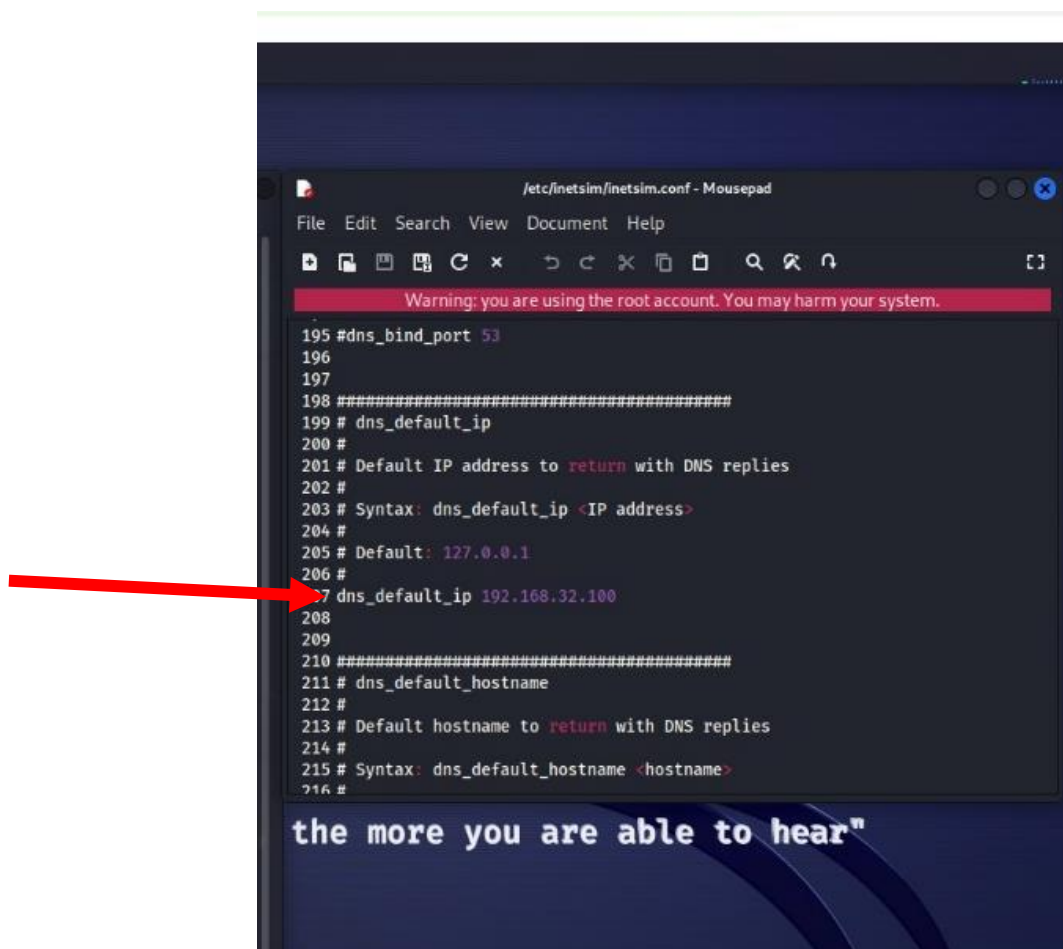


```
Warning: you are using the root account. You may harm your system.

52 start_service quotd_tcp
53 start_service quotd_udp
54 start_service chargen_tcp
55 start_service chargen_udp
56 start_service dummy_tcp
57 start_service dummy_udp
58
59
60 #####
61 # service_bind_address
62 #
63 # IP address to bind services to
64 #
65 # Syntax: service_bind_address <IP address>
66 #
67 # Default: 127.0.0.1
68 #
69 service_bind_address 192.168.32.100
70
71
72 #####
73 # service_bind_address

the more you are able to hear"
```

Figura 3 (Previa rimozione di #) Modifica stringa dns_default_ip con IP di Kali Linux 192.168.32.100

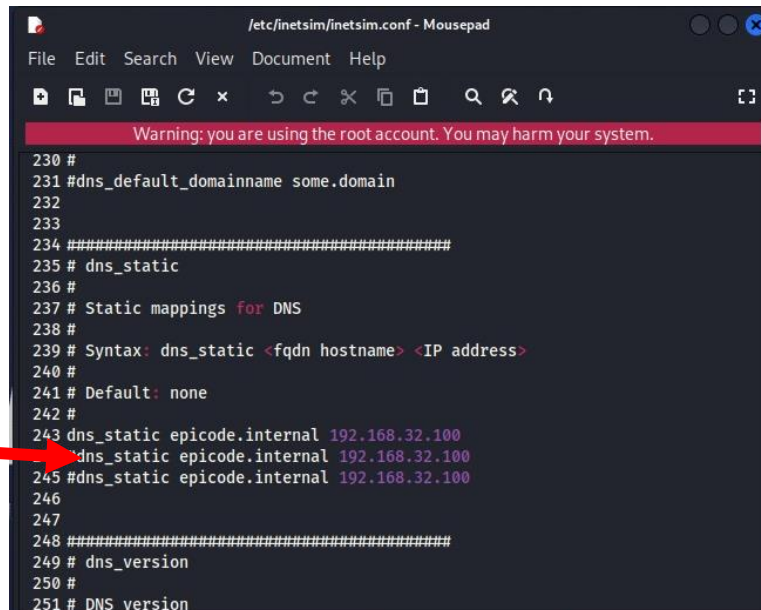


```
Warning: you are using the root account. You may harm your system.

195 #dns_bind_port 53
196
197
198 #####
199 # dns_default_ip
200 #
201 # Default IP address to return with DNS replies
202 #
203 # Syntax: dns_default_ip <IP address>
204 #
205 # Default: 127.0.0.1
206 #
207 dns_default_ip 192.168.32.100
208
209
210 #####
211 # dns_default_hostname
212 #
213 # Default hostname to return with DNS replies
214 #
215 # Syntax: dns_default_hostname <hostname>
216 #

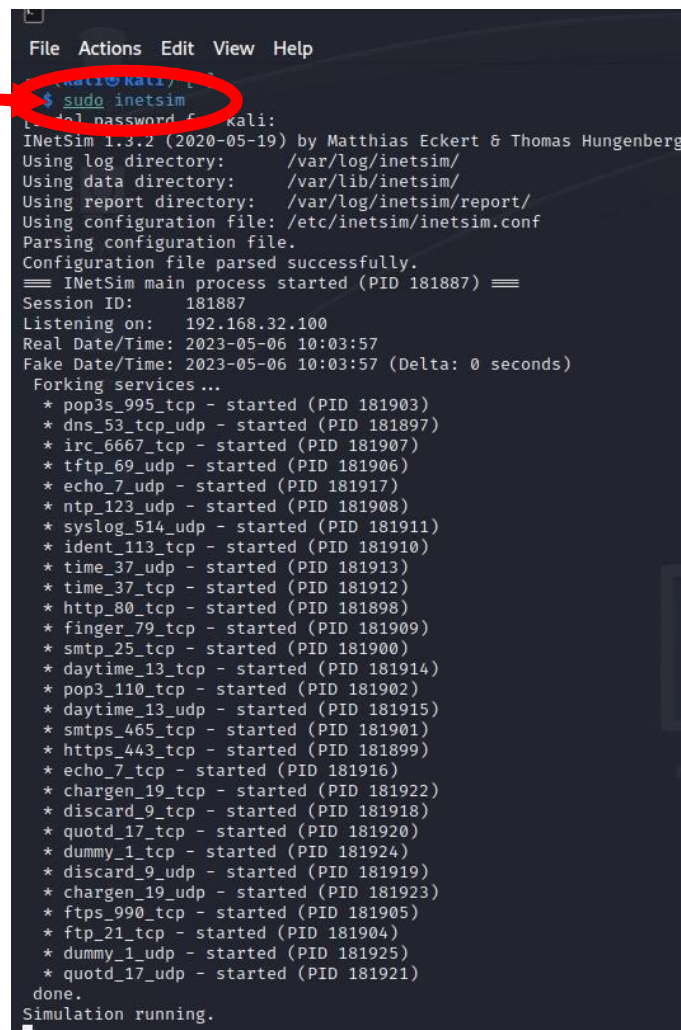
the more you are able to hear"
```

**Figura 4 (Previa rimozione di #) Modifica dns_static in epicode.internal
192.168.32.100**



```
/etc/inetsim/inetsim.conf - Mousepad
File Edit Search View Document Help
Warning: you are using the root account. You may harm your system.
230 #
231 #dns_default_domainname some.domain
232
233
234 #####
235 # dns_static
236 #
237 # Static mappings for DNS
238 #
239 # Syntax: dns_static <fqdn hostname> <IP address>
240 #
241 # Default: none
242 #
243 dns_static epicode.internal 192.168.32.100
244 dns_static epicode.internal 192.168.32.100
245 #dns_static epicode.internal 192.168.32.100
246
247
248 #####
249 # dns_version
250 #
251 # DNS version
```

Figura 5 Ho avviato la simulazione del server tramite Inetsim con il comando sudo inetsim



```
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 181887) ==
Session ID: 181887
Listening on: 192.168.32.100
Real Date/Time: 2023-05-06 10:03:57
Fake Date/Time: 2023-05-06 10:03:57 (Delta: 0 seconds)
Forking services ...
* pop3s_995_tcp - started (PID 181903)
* dns_53_tcp_udp - started (PID 181897)
* irc_6667_tcp - started (PID 181907)
* tftp_69_udp - started (PID 181906)
* echo_7_udp - started (PID 181917)
* ntp_123_udp - started (PID 181908)
* syslog_514_udp - started (PID 181911)
* ident_113_tcp - started (PID 181910)
* time_37_udp - started (PID 181913)
* time_37_tcp - started (PID 181912)
* http_80_tcp - started (PID 181898)
* finger_79_tcp - started (PID 181909)
* smtp_25_tcp - started (PID 181900)
* daytime_13_tcp - started (PID 181914)
* pop3_110_tcp - started (PID 181902)
* daytime_13_udp - started (PID 181915)
* smtps_465_tcp - started (PID 181901)
* https_443_tcp - started (PID 181899)
* echo_7_tcp - started (PID 181916)
* chargen_19_tcp - started (PID 181922)
* discard_9_tcp - started (PID 181918)
* quotd_17_tcp - started (PID 181920)
* dummy_1_tcp - started (PID 181924)
* discard_9_udp - started (PID 181919)
* chargen_19_udp - started (PID 181923)
* ftps_990_tcp - started (PID 181905)
* ftp_21_tcp - started (PID 181904)
* dummy_1_udp - started (PID 181925)
* quotd_17_udp - started (PID 181921)
done.
Simulation running.
```


STEP 3:

- Ho raggiunto <https://epicode.internal> da Win 7 (figura 6);
- Ho intercettato la comunicazione con Wireshark, dalla quale ho acquisito MAC address di sorgente e di destinazione (figura 7).

Figura 6 Ho raggiunto <https://epicode.internal> da Win 7

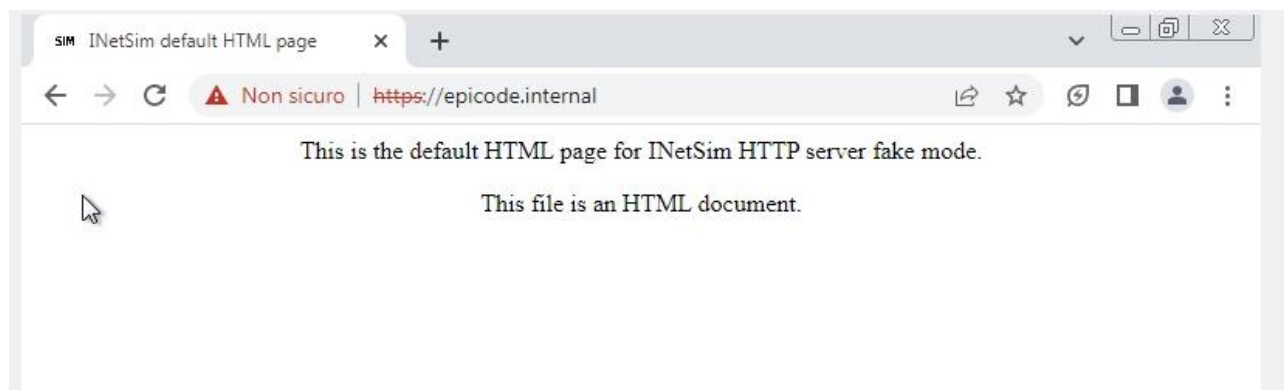
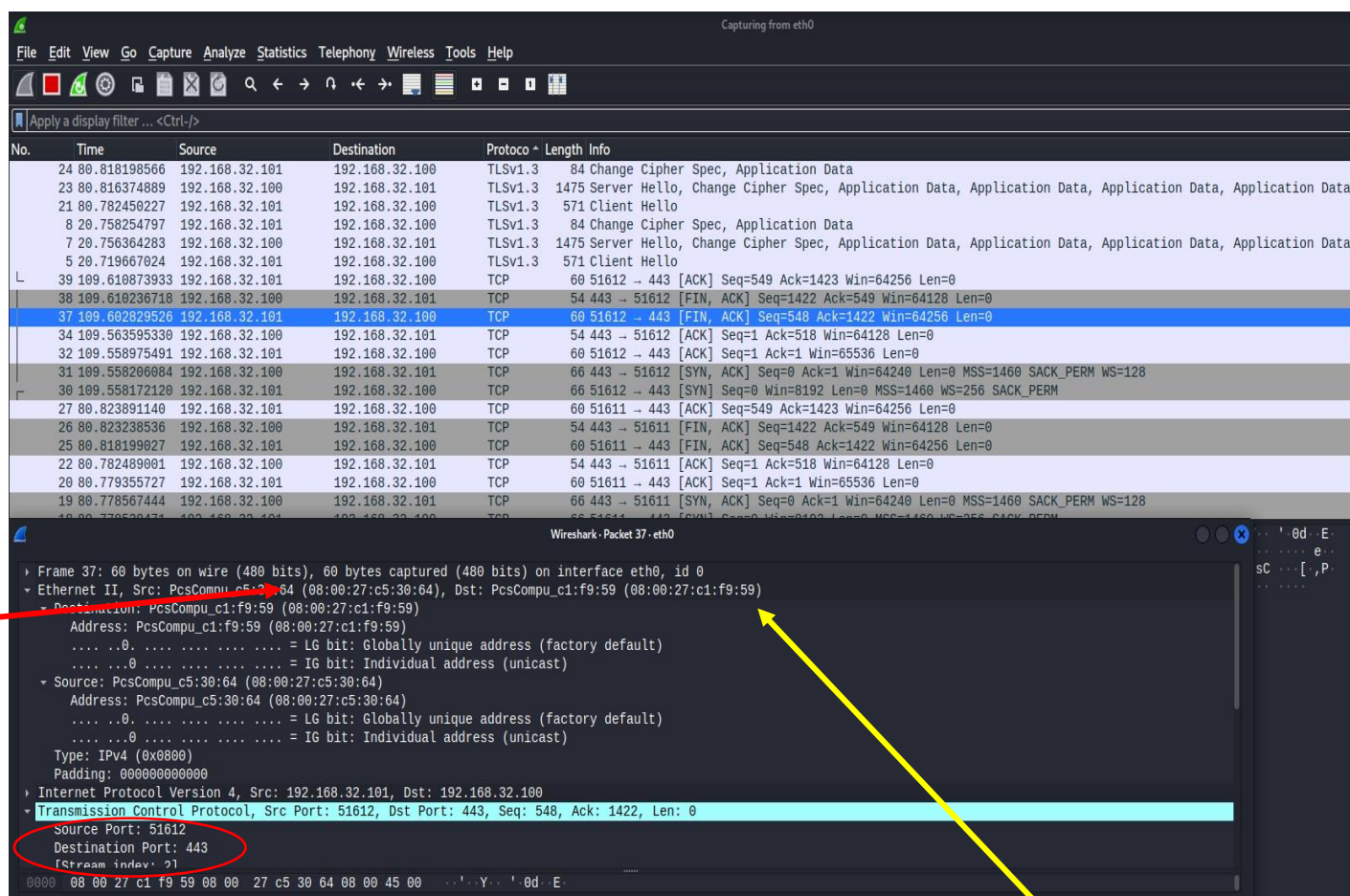


Figura 7 Ho intercettato la comunicazione con Wireshark, dalla quale ho acquisito MAC address di sorgente e di destinazione (in rosso MAC Win 7, in giallo MAC KALI LINUX)



STEP 4:

- Ho sostituito il server https con il server HTTPS e ho raggiunto <http://epicode.internal> da Win 7 (figura 8);
- Ho intercettato la comunicazione con Wireshark, dalla quale ho acquisito MAC address di sorgente e di destinazione (in rosso MAC Win 7, in giallo MAC Kali Linux). Acquisiti anche da protocollo ARP (rappresentato dall'ovale verde)

Figura 8 Ho sostituito il server https con il server HTTPS e ho raggiunto <http://epicode.internal> da Win 7

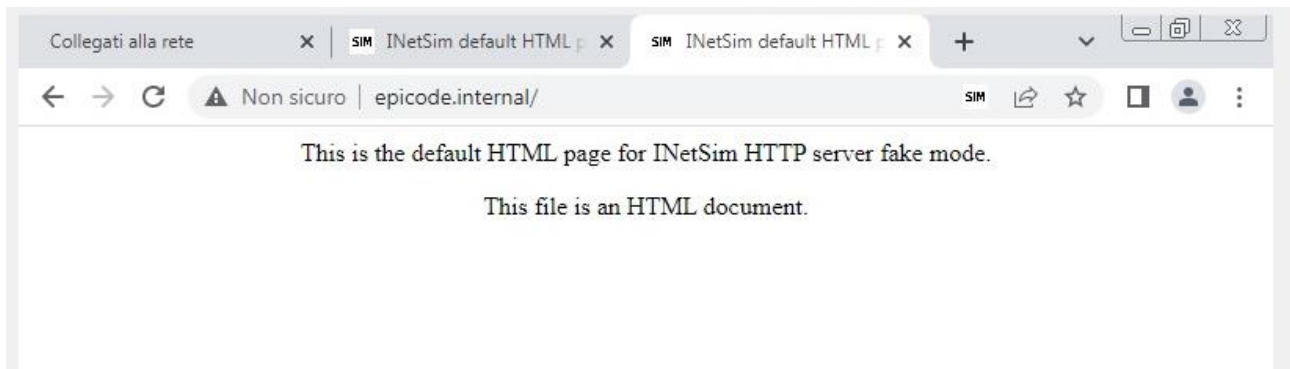
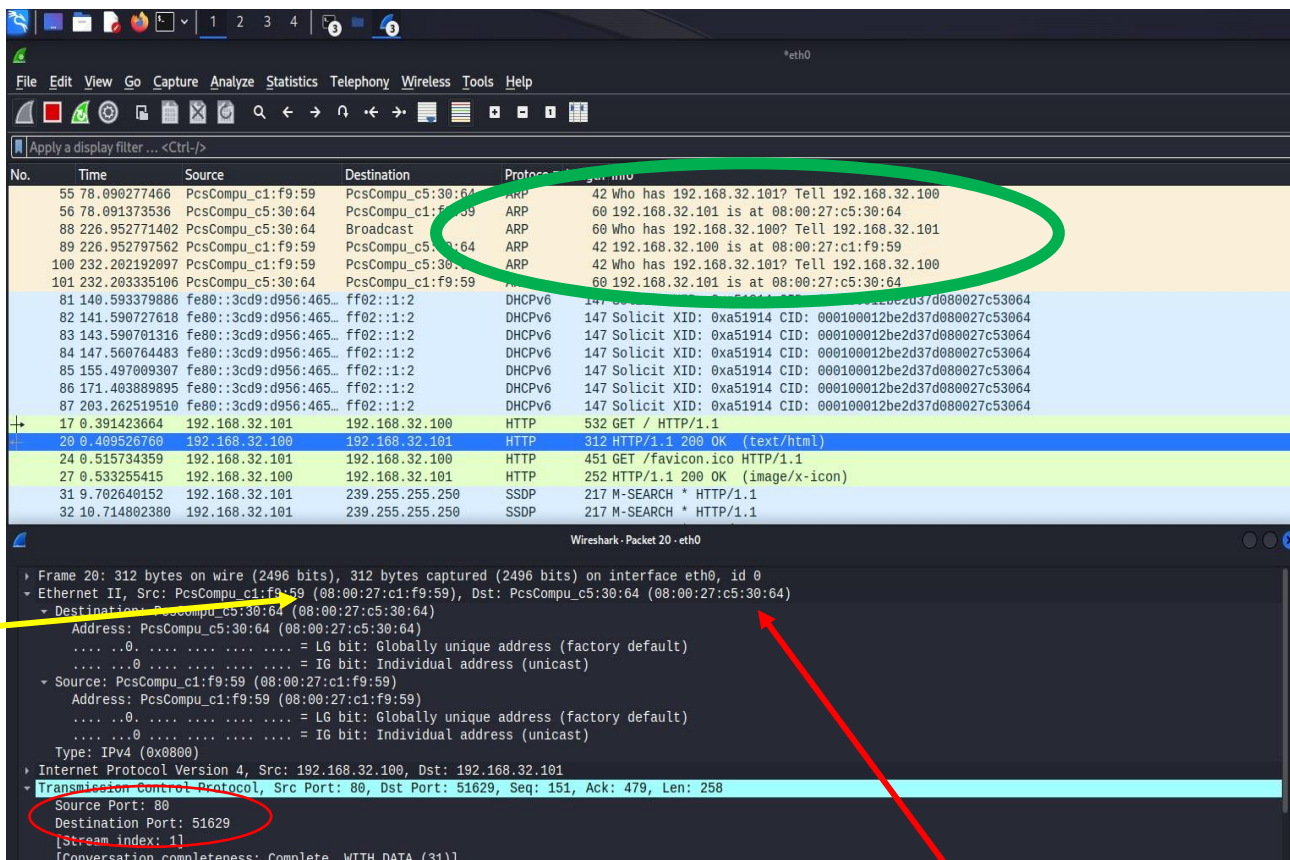


Figura 9 Ho intercettato la comunicazione con Wireshark, dalla quale ho acquisito MAC address di sorgente e di destinazione, (in rosso MAC Win 7, in giallo MAC Kali Linux). Acquisiti anche da protocollo ARP (rappresentato dall'ovale verde)



STEP 5:

- **DIFFERENZA 1:** nel raggiungimento del server https sono stato avvisato di una connessione non privata e non sicura, avviso questo che non mi è giunto quando ho raggiunto il server http.
- **DIFFERENZA 2:** su Wireshark ho rintracciato il protocollo TLSv.1.3 quando ho fatto l'accesso al server https, mentre il protocollo presente sul server http è per l'appunto http. Premesso ciò, ho impostato il filtro **tcp.stream**, grazie al quale ho avuto accesso alla comunicazione che hanno avuto client e server, notando una sostanziale differenza. Nel server http ho trovato la comunicazione in chiaro che client e server hanno avuto (figura 10), mentre, con lo stesso procedimento sul server https, ho notato che la comunicazione è stata **crittografata** (figura 11).

Figura 10 tcp.stream su server http

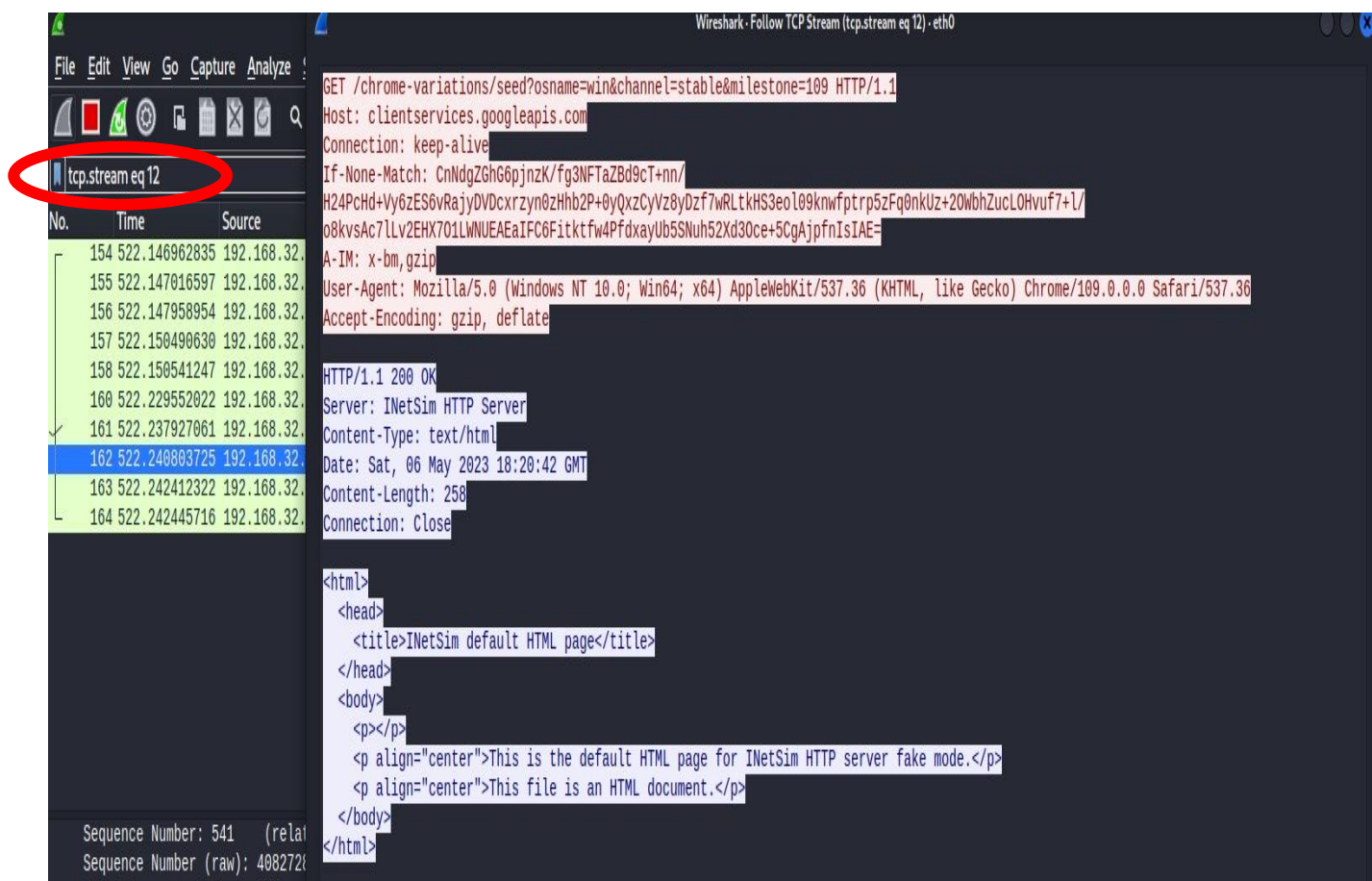


Figura 11 tcp.stream su server https

Wireshark - Follow TCP Stream (tcp.stream eq 0) - eth0

File Edit View Go Capture Analyze

tcp.stream eq 0

No.	Time	Source
42	33.923761214	192.168.32.
43	33.923825988	192.168.32.
44	33.926051691	192.168.32.
46	33.932845164	192.168.32.
49	34.059773571	192.168.32.
50	34.062022248	192.168.32.
51	34.081722921	192.168.32.
52	34.086088083	192.168.32.
45	33.932801441	192.168.32.
47	34.057440292	192.168.32.
48	34.059720831	192.168.32.

.....;..X...f=] .4^.....X.....U .A.nS.U/.0.z9...@...LC
..).+./.,.0...../5...ZZ.Di.....h2.#.....
.....3.+.).....!.....F.>0W.,... (6.....r.(.d.
.....www.google.com.+...
.....h2.http/
1.1.....
.....Z...v....r...<C~!.!...Y...f..V].X.A.nS..
....z9...@...LC
..).+....3.\$... .h.A.....*.&F..0..h...]8.V.....A.9.....~...Z.....J.....(.....<...a..3.....xC.?,
s..N5A0]&7..b-Gy;.....s`.0...a..P..Z.....d.....I..\"# .{T_E;W
?^....."zY.'K.....^.....~N_~%Vy(5u*.n\i.....w.2l..\"?...PE../NI..9.w..>.Q-K.v..T'.....I.D=;H g....OnJ.{.`..n..
3.....'x.G.....T.Z.0{.....z.*..H...hj8r..2...U..TI.in...7..0x.....%...o.9n.....fC..lvdBF.....?cg.@%.0i=a.....[.=H-..
.....'...<:??^\$.9...#R...R...D.....J.;.(...:e.9.U,..
..|.M..... L.G..nsh....
bK....(0~.\".L..I.]..0.t....J...~ ..&\$.....0.H.r.:|t.....9.:.*C.?#.^.L..2.k`..N309.....7 ..?
..} B..yQ..G,..NPn.....f+L8F.<x.vf.i....v.c\$w.....r+.....~...+.....\\...|..=iPe../Q..5_*.t..8x.....D.d.T
..R.T.....Qq'..-\\..W...a..R!.....>.....*P..I:H[\".....<..\\..?7wap}>.....U.....K.]c!...K...k.
+RCx.y\\....Z.D.EbN.....U^..R../:.....!2p...<].)T....H.?.....r0.2....a...`C..
.....{Y.l...h.*wV.q.Q'.3.\".:^Gn...oQ.).....xY..C. 3.....m.1.t....m.....Kx{.....-...!b}J..j#.\"m..
[.w.Y.....(r...wuYk.....J.....m.....\".-]9_>.....%W.0'Db.).FW9... ..0..C/!{..I...Zw/..).|x...+=A'...N
....^.....E.i5e.....V8n... ..:.)if...?z..
..|..
Dj..&....2(\"9feU...>.f...Gw8.#...E...Ql.i0p..I...GN...w\"...QI.+U..H]...k.Vd.M...mn=\".../F{U9nzj6T.vu.....Go.....y.C....

Frame 44: 60 bytes on wire (480

