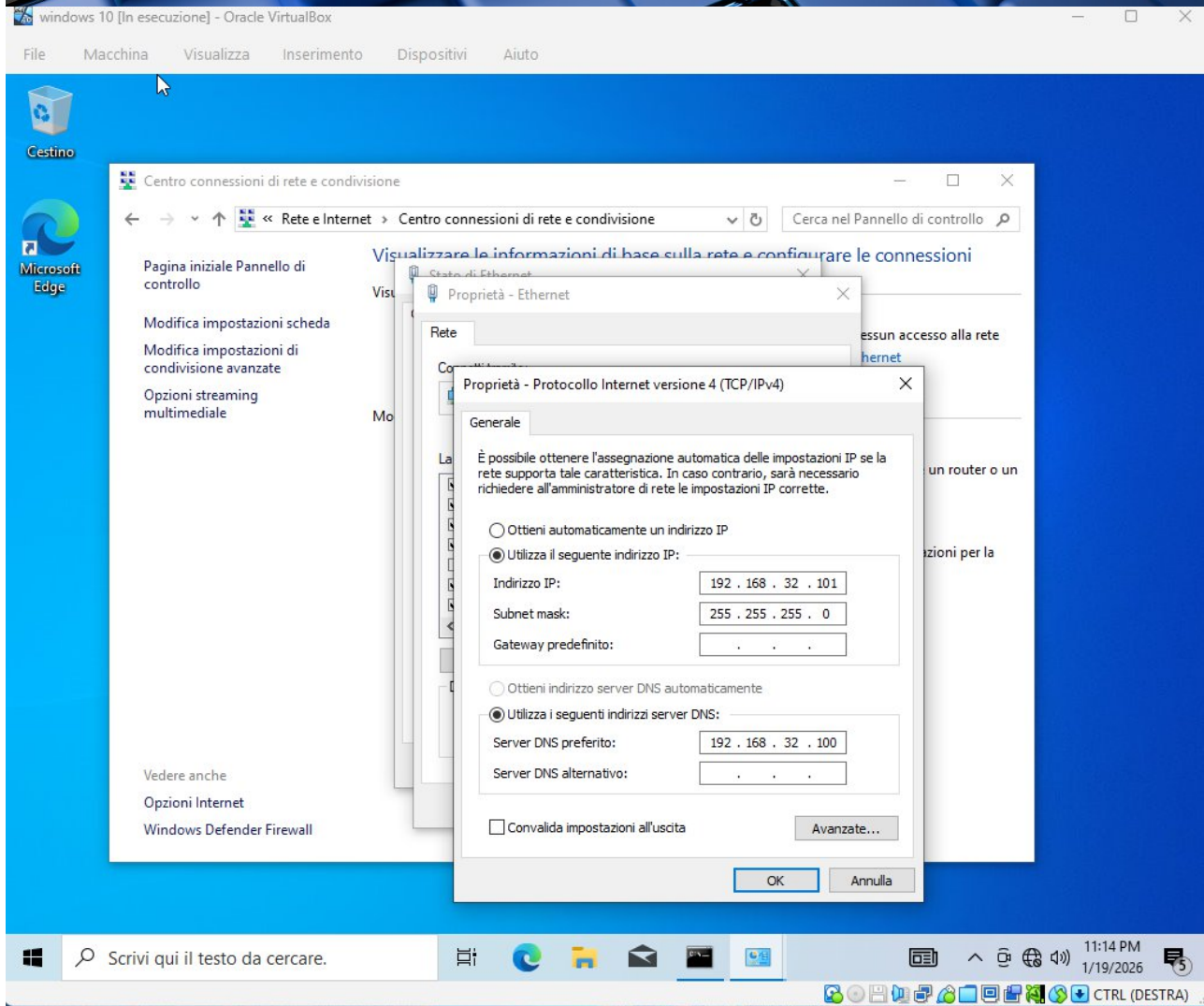
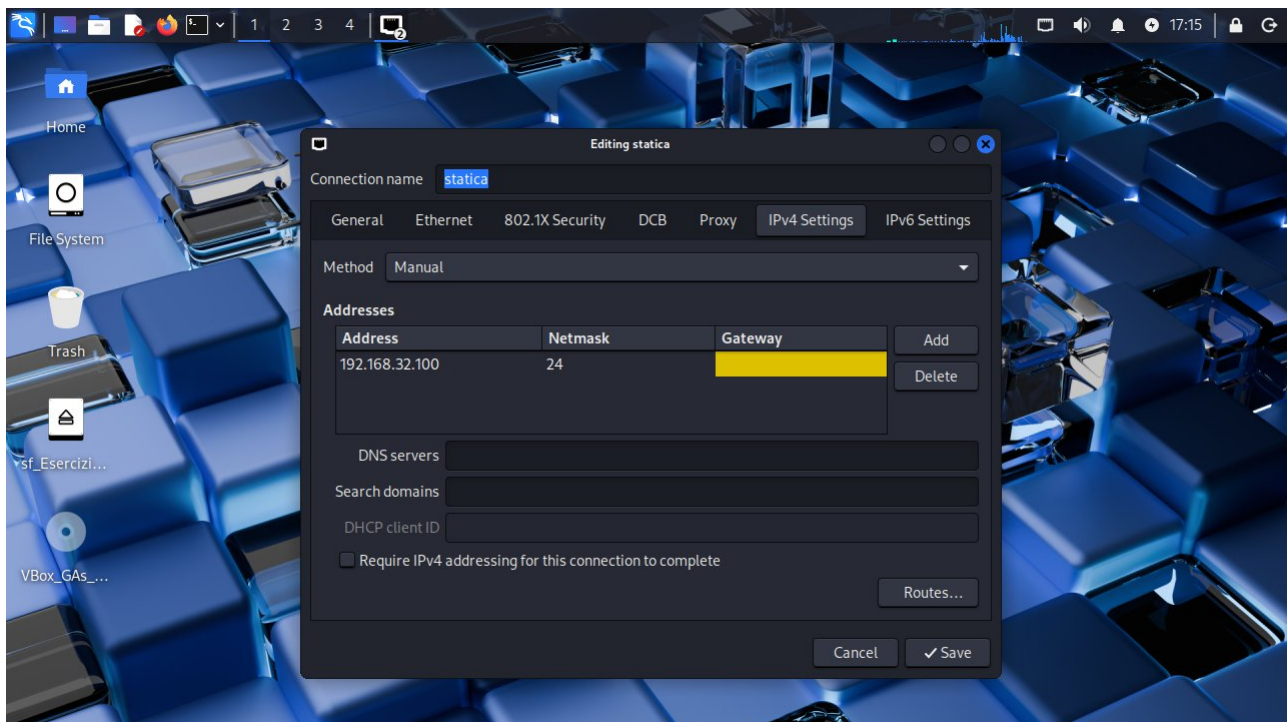


REPORT ORICCHIO ANTONIO PROGETTO FINALE

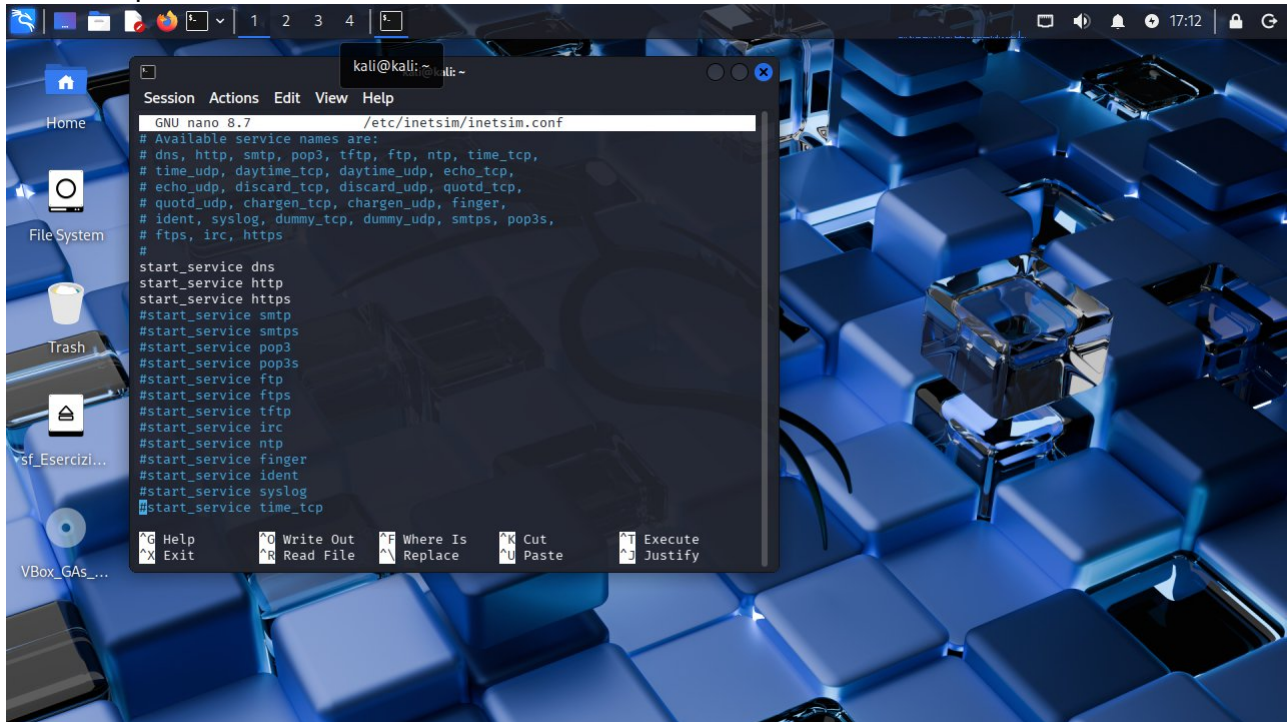
Si richiedevano due macchine:

-Windows IP 192.168.32.101

-Linux IP 192.168.32.100



Servizi https attivi

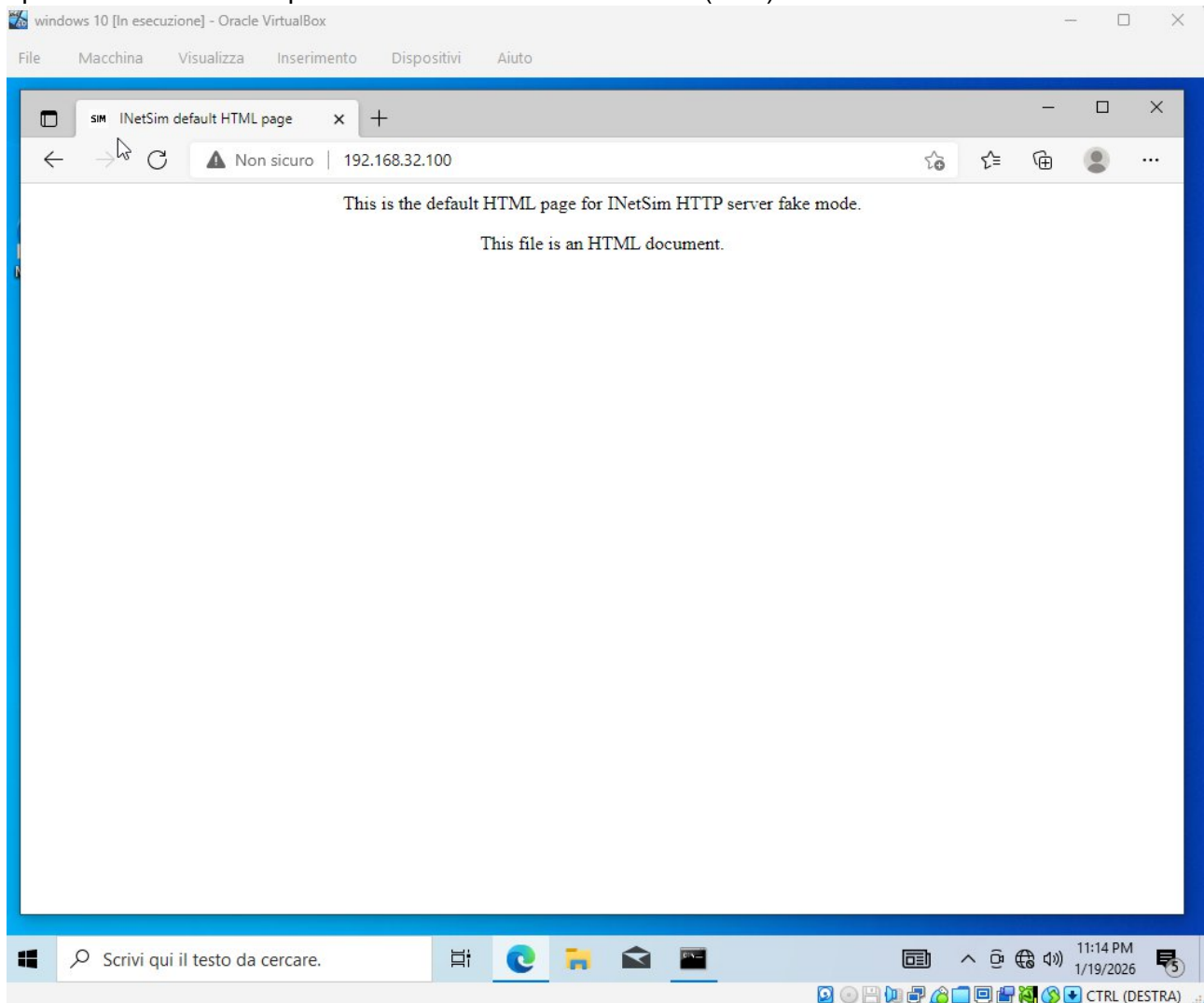


Servizio DNS attivo



Simulare, in ambiente di laboratorio virtuale, un'architettura client server in cui un client con indirizzo 192.168.32.101 (Windows) richiede tramite web browser una risorsa all'hostname

epicode.internal che risponde all'indirizzo 192.168.32.100(Kali).



Si intercetti poi la comunicazione con Wireshark, evidenziando i MAC address di sorgente e destinazione ed il contenuto della richiesta HTTPS.

Nella prima cattura vediamo indirizzo MAC mittente https: 08:00:27:39:d5:b5

Capturing from eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.port == 443 || udp.port == 443

No.	Time	Source	Destination	Protocol	Length	Info
111	15.856174480	192.168.32.101	192.168.32.100	TCP	66	60733 → 443 [SYN] Seq=0 Win=64
112	15.856199603	192.168.32.100	192.168.32.101	TCP	66	443 → 60733 [SYN, ACK] Seq=0 A
113	15.856848499	192.168.32.101	192.168.32.100	TCP	60	60733 → 443 [ACK] Seq=1 Ack=1
114	15.857139760	192.168.32.101	192.168.32.100	TCP	66	58900 → 443 [SYN] Seq=0 Win=64
115	15.857149615	192.168.32.100	192.168.32.101	TCP	66	443 → 58900 [SYN, ACK] Seq=0 A
116	15.857673917	192.168.32.101	192.168.32.100	TCP	60	58900 → 443 [ACK] Seq=1 Ack=1
117	15.904548896	192.168.32.101	192.168.32.100	TLSv1.3	571	Client Hello
118	15.904565224	192.168.32.100	192.168.32.101	TCP	54	443 → 58900 [ACK] Seq=1 Ack=51
119	15.905802165	192.168.32.101	192.168.32.100	TLSv1.3	571	Client Hello
120	15.905847859	192.168.32.100	192.168.32.101	TCP	54	443 → 60733 [ACK] Seq=1 Ack=51
121	15.907497569	192.168.32.100	192.168.32.101	TLSv1.3	1497	Server Hello, Change Cipher Sp
122	15.907950588	192.168.32.100	192.168.32.101	TLSv1.3	1497	Server Hello, Change Cipher Sp
123	15.960472530	192.168.32.101	192.168.32.100	TCP	60	60733 → 443 [ACK] Seq=518 Ack=

28 bits), 66 bytes captured (528 bits) on interface eth0
5 (08:00:27:39:d5:b5), Dst: PCSSystemtec_63:b0:05 (08:00:27:39:d5:b5)
bit: Globally unique address (factory default)
bit: Individual address (unicast)
:27:39:d5:b5)
bit: Globally unique address (factory default)
bit: Individual address (unicast)

168.32.101, Dst: 192.168.32.100
t: 60733, Dst Port: 443, Seq: 0, Len: 0

This shows the raw value of the acknowledgment number (tcp.ack_raw), 4 bytes Packets: 180 · Displayed: 36 (20.0%) Profile: Default

Nella seconda cattura possiamo notare il medesimo MAC mittente ma stavolta su http

Capturing from eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.port == 80 || udp.port == 80

No.	Time	Source	Destination	Protocol	Length	Info
133	32.546090016	192.168.32.101	192.168.32.100	TCP	66	57171 → 80 [SYN] Seq=0 Win=642
134	32.546111827	192.168.32.100	192.168.32.101	TCP	66	80 → 57171 [SYN, ACK] Seq=0 Ac
135	32.546795141	192.168.32.101	192.168.32.100	TCP	60	57171 → 80 [ACK] Seq=1 Ack=1 W
136	32.547177429	192.168.32.101	192.168.32.100	TCP	66	54614 → 80 [SYN] Seq=0 Win=642
137	32.547187924	192.168.32.100	192.168.32.101	TCP	66	80 → 54614 [SYN, ACK] Seq=0 Ac
138	32.547530152	192.168.32.101	192.168.32.100	TCP	60	54614 → 80 [ACK] Seq=1 Ack=1 W
139	32.574497440	192.168.32.101	192.168.32.100	HTTP	525	GET / HTTP/1.1
140	32.574559802	192.168.32.100	192.168.32.101	TCP	54	80 → 54614 [ACK] Seq=1 Ack=472
146	32.585091583	192.168.32.100	192.168.32.101	TCP	204	80 → 54614 [PSH, ACK] Seq=1 Ac
147	32.586500862	192.168.32.100	192.168.32.101	HTTP	312	HTTP/1.1 200 OK (text/html)
148	32.587730544	192.168.32.101	192.168.32.100	TCP	60	54614 → 80 [ACK] Seq=472 Ack=4
149	32.654825596	192.168.32.101	192.168.32.100	TCP	60	54614 → 80 [FIN, ACK] Seq=472
150	32.654843235	192.168.32.100	192.168.32.101	TCP	54	80 → 54614 [ACK] Seq=410 Ack=4

Rule Name: HTTP
Rule String: http || tcp.port == 80 || http2]
, Src: PCSSystemtec_39:d5:b5 (08:00:27:39:d5:b5), Dst:
on: PCSSystemtec_63:b0:05 (08:00:27:39:d5:b5)
0. = LG bit: Globally unique addre
.0 = IG bit: Individual address (u
CSSystemtec_39:d5:b5 (08:00:27:39:d5:b5)
4 (0x0800)
ndex: 1]
otocol Version 4, Src: 192.168.32.101, Dst: 192.168.32.
Control Protocol, Src Port: 57171, Dst Port: 80, Seq:
rt: 57171
on Port: 80
ndex: 0]

Specifies if this is an individual (unicast)...dcast/multicast) address (eth.dst.ig), 1 bit Packets: 232 · Displayed: 23 (9.9%) Profile: Default

E così' via per i mac de

Text Editor
Simple Text Editor File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Capturing from eth0

tcp.port == 80 || udp.port == 80

No.	Time	Source	Destination	Protocol	Length	Info
133	32.546090016	192.168.32.101	192.168.32.100	TCP	66	57171 → 80 [SYN] Seq=0 Win=642
134	32.546111827	192.168.32.100	192.168.32.101	TCP	66	80 → 57171 [SYN, ACK] Seq=0 Ac
135	32.546795141	192.168.32.101	192.168.32.100	TCP	60	57171 → 80 [ACK] Seq=1 Ack=1 W
136	32.547177429	192.168.32.101	192.168.32.100	TCP	66	54614 → 80 [SYN] Seq=0 Win=642
137	32.547187924	192.168.32.100	192.168.32.101	TCP	66	80 → 54614 [SYN, ACK] Seq=0 Ac
138	32.547530152	192.168.32.101	192.168.32.100	TCP	60	54614 → 80 [ACK] Seq=1 Ack=1 W
139	32.574497440	192.168.32.101	192.168.32.100	HTTP	525	GET / HTTP/1.1
140	32.574559802	192.168.32.100	192.168.32.101	TCP	54	80 → 54614 [ACK] Seq=1 Ack=472
146	32.585091583	192.168.32.100	192.168.32.101	TCP	204	80 → 54614 [PSH, ACK] Seq=1 Ac
147	32.586500862	192.168.32.100	192.168.32.101	HTTP	312	HTTP/1.1 200 OK (text/html)
148	32.587730544	192.168.32.101	192.168.32.100	TCP	60	54614 → 80 [ACK] Seq=472 Ack=4
149	32.654825596	192.168.32.101	192.168.32.100	TCP	60	54614 → 80 [FIN, ACK] Seq=472
150	32.654843235	192.168.32.100	192.168.32.101	TCP	54	80 → 54614 [ACK] Seq=472 Ack=4

..., Dst: PCSSystemtec_63:b0:05 (08:00:27:63:b0:05)
e address (factory default)
ress (unicast)

168.32.100
0, Seq: 0, Len: 0

This shows the raw value of the acknowledgment number (tcp.ack_raw), 4 bytes Packets: 232 - Displayed: 23 (9.9%) Profile: Default

stinatari

kali@kali: ~ Capturing from eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.port == 443 || udp.port == 443

No.	Time	Source	Destination	Protocol	Length	Info
111	15.856174480	192.168.32.101	192.168.32.100	TCP	66	60733 → 443 [SYN] Seq=0 Win=64
112	15.856199603	192.168.32.100	192.168.32.101	TCP	66	443 → 60733 [SYN, ACK] Seq=0 A
113	15.856848499	192.168.32.101	192.168.32.100	TCP	60	60733 → 443 [ACK] Seq=1 Ack=1
114	15.857139760	192.168.32.101	192.168.32.100	TCP	66	58900 → 443 [SYN] Seq=0 Win=64
115	15.857149615	192.168.32.100	192.168.32.101	TCP	66	443 → 58900 [SYN, ACK] Seq=0 A
116	15.857673917	192.168.32.101	192.168.32.100	TCP	60	58900 → 443 [ACK] Seq=1 Ack=1
117	15.904548896	192.168.32.101	192.168.32.100	TLSv1.3	571	Client Hello
118	15.904565224	192.168.32.100	192.168.32.101	TCP	54	443 → 58900 [ACK] Seq=1 Ack=51
119	15.905802165	192.168.32.101	192.168.32.100	TLSv1.3	571	Client Hello
120	15.905847859	192.168.32.100	192.168.32.101	TCP	54	443 → 60733 [ACK] Seq=1 Ack=51
121	15.907497569	192.168.32.100	192.168.32.101	TLSv1.3	1497	Server Hello, Change Cipher Sp
122	15.907950588	192.168.32.100	192.168.32.101	TLSv1.3	1497	Server Hello, Change Cipher Sp
125	15.960472530	192.168.32.101	192.168.32.100	TCP	60	60733 → 443 [ACK] Seq=518 Ack=

ured (528 bits) on interface eth0, id 0
Dst: PCSSystemtec_63:b0:05 (08:00:27:63:b0:05)
address (factory default)
is (unicast)
address (factory default)
is (unicast)

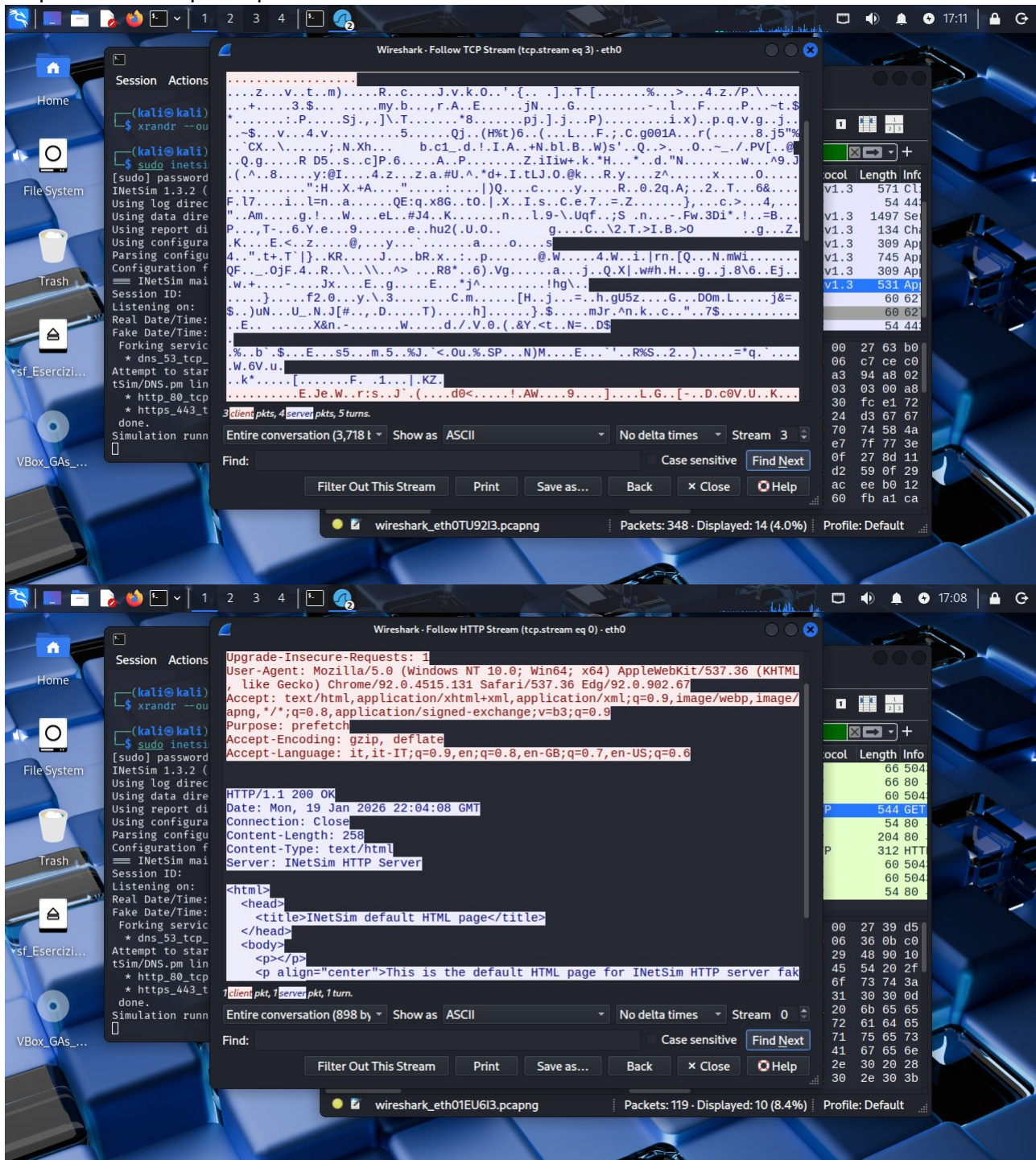
8.32.100
0, Seq: 0, Len: 0

This shows the raw value of the acknowledgment number (tcp.ack_raw), 4 bytes Packets: 192 - Displayed: 36 (18.8%) Profile: Default

Ripetere l'esercizio, sostituendo il server HTTPS, con un server HTTP. Si intercetti nuovamente il traffico, evidenziando le eventuali differenze tra il traffico appena catturato in HTTP ed il traffico precedente in HTTPS. Spiegare, motivandole, le principali differenze se presenti.

Qui ho analizzato i pacchetti http per http appunto

E i pacchetti TLS per https



Come possiamo notare una delle differenza tra http e https. Principalmente è che in http riusciamo a leggere il contenuto del pacchetto chiaramente, mentre in https è criptato.