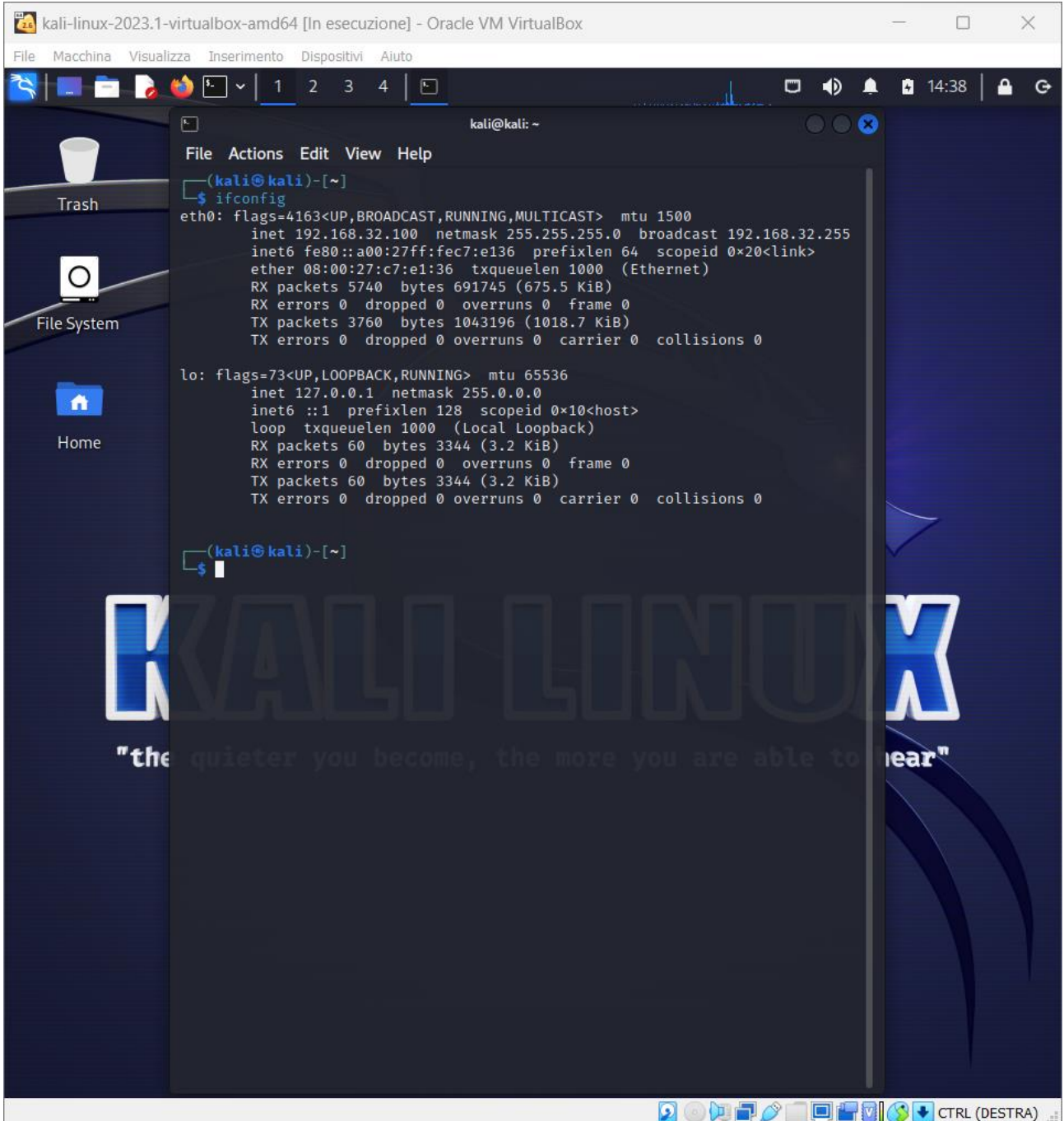


REPORT

1)

Per prima cosa abbiamo configurato le due macchine in modo tale che fossero in grado di comunicare tra di loro, impostando un IP statico 192.168.32.100 kali e 192.168.32.101 W7 verificando attraverso il ping



```
kali-linux-2023.1-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
1 2 3 4
kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.32.100 netmask 255.255.255.0 broadcast 192.168.32.255
    inet6 fe80::a00:27ff:fec7:e136 prefixlen 64 scopeid 0<20<link>
    ether 08:00:27:c7:e1:36 txqueuelen 1000 (Ethernet)
    RX packets 5740 bytes 691745 (675.5 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 3760 bytes 1043196 (1018.7 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 60 bytes 3344 (3.2 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 60 bytes 3344 (3.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali@kali)-[~]
$
```



```
C:\Windows\system32\cmd.exe

Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\ vboxuser>ping 192.168.32.100

Pinging 192.168.32.100 with 32 bytes of data:
Reply from 192.168.32.100: bytes=32 time<1ms TTL=64
Reply from 192.168.32.100: bytes=32 time<1ms TTL=64
Reply from 192.168.32.100: bytes=32 time<1ms TTL=64
Reply from 192.168.32.100: bytes=32 time<1ms TTL=64

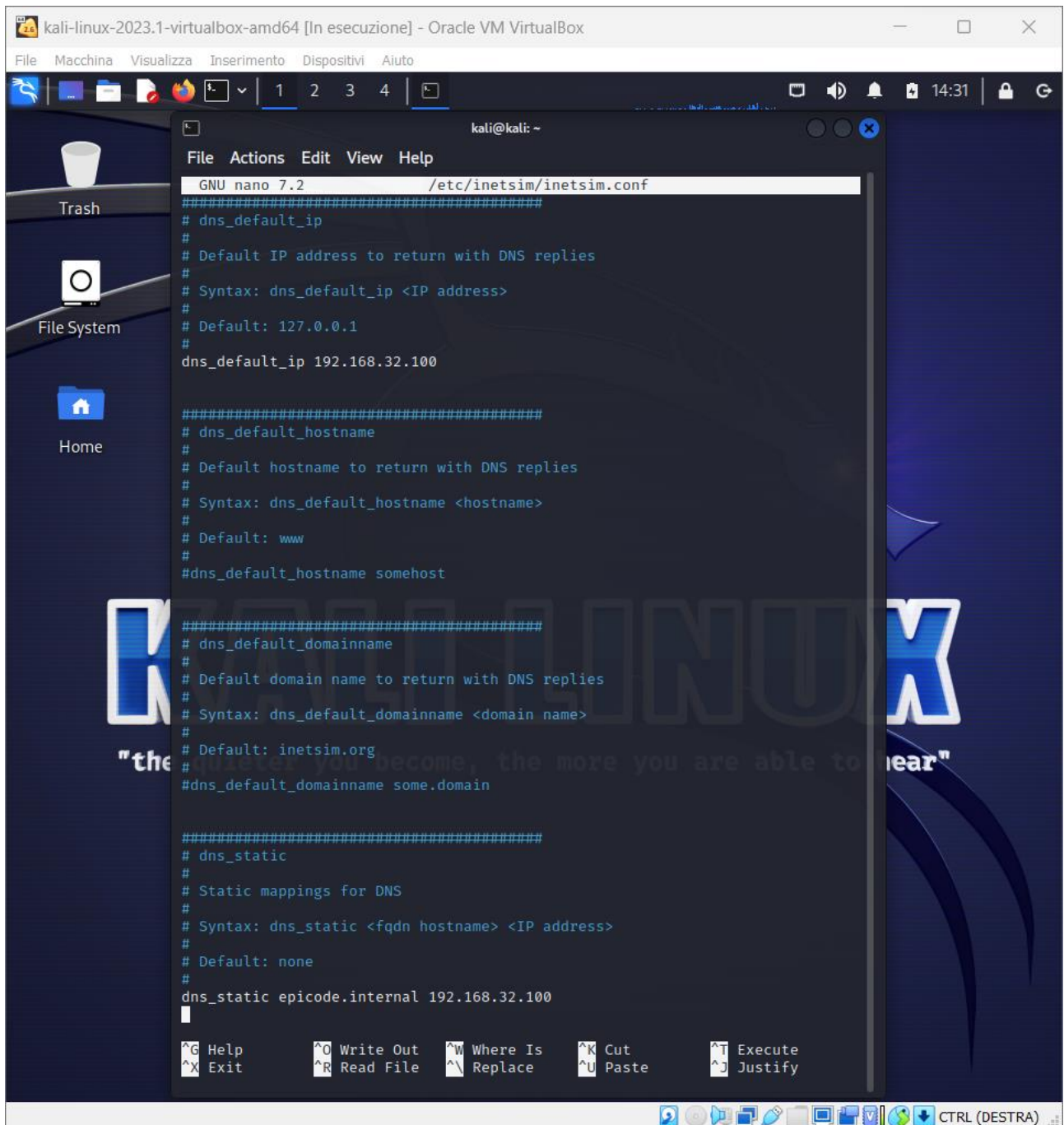
Ping statistics for 192.168.32.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\ vboxuser>

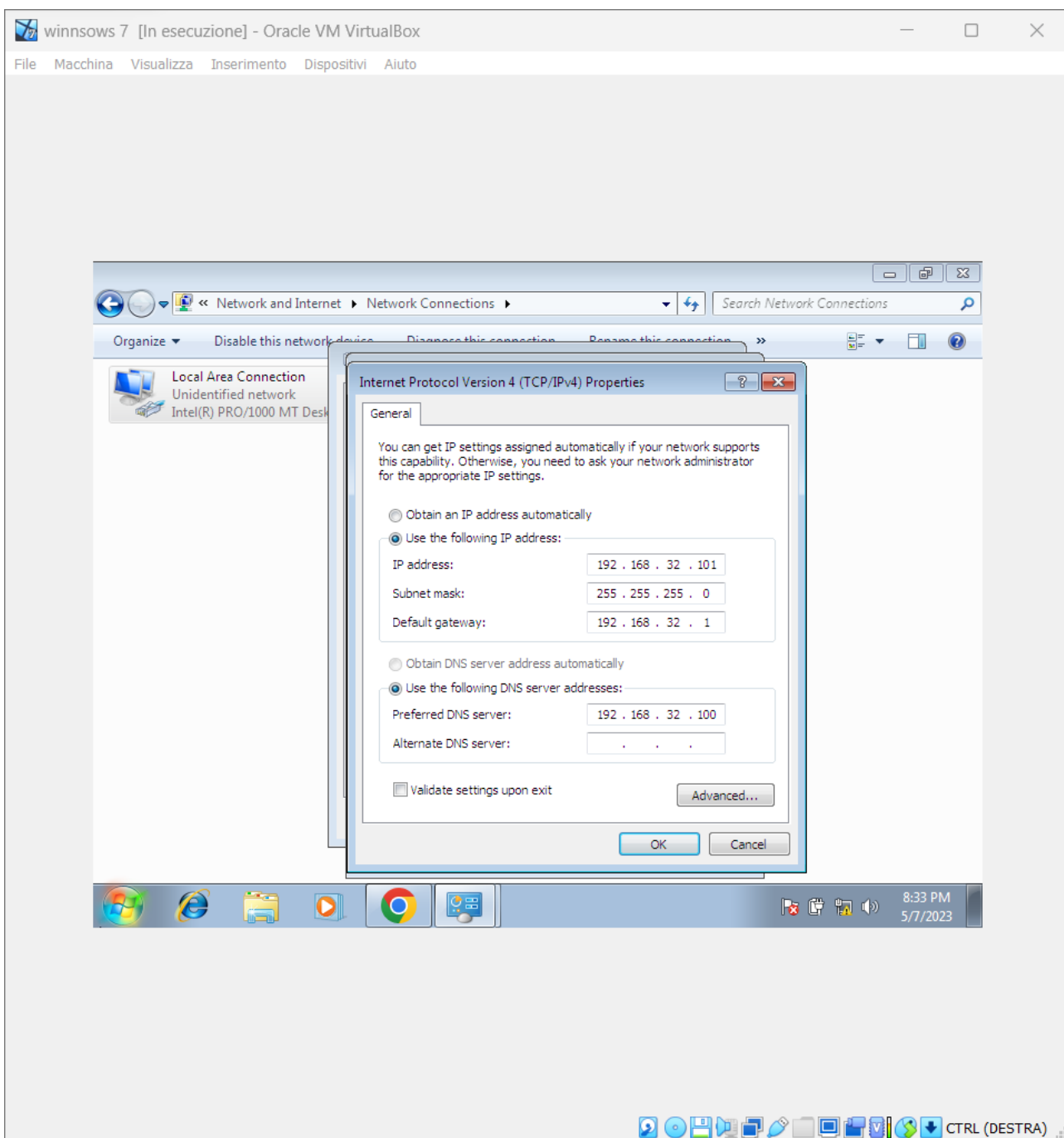
C:\Users\ vboxuser>
```

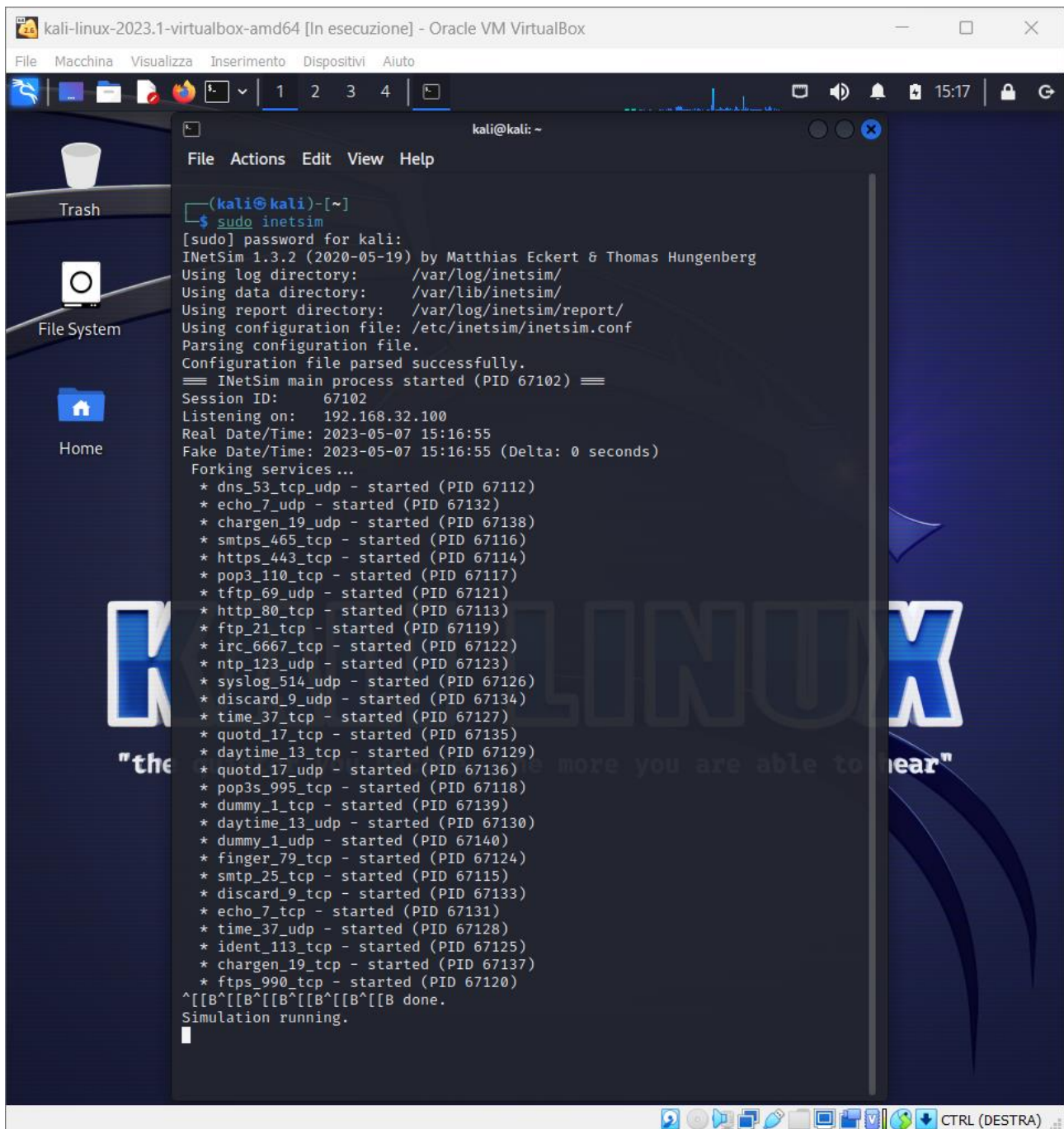
2)

Su kali abbiamo impostato il dns in modo che risponda a epicode.internal e contestualmente facciamo partire la simulazione e in fine si imposta il DNS anche su windows 7



```
kali@kali: ~  
File Actions Edit View Help  
GNU nano 7.2 /etc/inetsim/inetsim.conf  
#####  
# 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_hostname  
#  
# Default hostname to return with DNS replies  
#  
# Syntax: dns_default_hostname <hostname>  
#  
# Default: www  
#  
#dns_default_hostname somehost  
  
#####  
# dns_default_domainname  
#  
# Default domain name to return with DNS replies  
#  
# Syntax: dns_default_domainname <domain name>  
#  
# Default: inetsim.org  
#  
#dns_default_domainname some.domain  
  
#####  
# dns_static  
#  
# Static mappings for DNS  
#  
# Syntax: dns_static <fqdn hostname> <IP address>  
#  
# Default: none  
#  
dns_static epicode.internal 192.168.32.100  
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute  
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify  
CTRL (DESTRA)
```





```
kali-linux-2023.1-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto

kali@kali: ~
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 67102) ==
Session ID: 67102
Listening on: 192.168.32.100
Real Date/Time: 2023-05-07 15:16:55
Fake Date/Time: 2023-05-07 15:16:55 (Delta: 0 seconds)
Forking services ...
* dns_53_tcp_udp - started (PID 67112)
* echo_7_udp - started (PID 67132)
* chargen_19_udp - started (PID 67138)
* smtps_465_tcp - started (PID 67116)
* https_443_tcp - started (PID 67114)
* pop3_110_tcp - started (PID 67117)
* tftp_69_udp - started (PID 67121)
* http_80_tcp - started (PID 67113)
* ftp_21_tcp - started (PID 67119)
* irc_6667_tcp - started (PID 67122)
* ntp_123_udp - started (PID 67123)
* syslog_514_udp - started (PID 67126)
* discard_9_udp - started (PID 67134)
* time_37_tcp - started (PID 67127)
* quotd_17_tcp - started (PID 67135)
* daytime_13_tcp - started (PID 67129)
* quotd_17_udp - started (PID 67136)
* pop3s_995_tcp - started (PID 67118)
* dummy_1_tcp - started (PID 67139)
* daytime_13_udp - started (PID 67130)
* dummy_1_udp - started (PID 67140)
* finger_79_tcp - started (PID 67124)
* smtp_25_tcp - started (PID 67115)
* discard_9_tcp - started (PID 67133)
* echo_7_tcp - started (PID 67131)
* time_37_udp - started (PID 67128)
* ident_113_tcp - started (PID 67125)
* chargen_19_tcp - started (PID 67137)
* ftps_990_tcp - started (PID 67120)
^[[B^[[B^[[B^[[B^[[B done.
Simulation running.
```

3) Ora intercettiamo la comunicazione tra client e host con wireshark con il quale possiamo osservare il MAC address della sorgente e della destinazione nella prima foto osserviamo HTTPS e la porta la 443 invece nella seconda foto possiamo osservare l'HTTP che utilizzerà la porta 80. La differenza tra i 2 protocolli sta nella sicurezza, HTTP è una trasmissione in chiaro quindi chiunque può intercettare il flusso di dati e averne accesso cosa non fattibile con HTTPS in quanto criptata dai TLS.

The screenshot displays the Wireshark network protocol analyzer interface. The top menu bar includes File, Machine, Visualizza, Inserimento, Dispositivi, and Aiuto. The main window is titled 'kali-linux-2023.1-virtualbox-amd64 [in esecuzione] - Oracle VM VirtualBox' and shows a packet capture of an SSH session on the 'https.pcapng' file.

The packet list on the left shows a sequence of packets. The selected packet is No. 11, which is an Ethernet II packet from 'PcsCompu_39:ec:20' to 'PcsCompu_c7:e1:36'. The packet details pane on the right shows the structure of the selected packet, including Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. The packet bytes pane on the right shows the raw data in hexadecimal and ASCII.

The packet details pane for the selected packet (No. 11) shows the following structure:

- Ethernet II, Src: PcsCompu_39:ec:20 (08:00:27:39:ec:20), Dst: PcsCompu_c7:e1:36 (08:00:27:c7:e1:36)
 - Destination: PcsCompu_c7:e1:36 (08:00:27:c7:e1:36)
 - Address: PcsCompu_c7:e1:36 (08:00:27:c7:e1:36)
 -0 = LG bit: Globally unique address (factory default)
 -0 = IG bit: Individual address (unicast)
 - Source: PcsCompu_39:ec:20 (08:00:27:39:ec:20)
 - Address: PcsCompu_39:ec:20 (08:00:27:39:ec:20)
 -0 = LG bit: Globally unique address (factory default)
 -0 = IG bit: Individual address (unicast)
 - Type: IPv4 (0x0800)
 - Internet Protocol Version 4, Src: 192.168.32.101, Dst: 192.168.32.100
 - Transmission Control Protocol, Src Port: 49892, Dst Port: 443, Seq: 0, Len: 0

The packet bytes pane on the right shows the raw data in hexadecimal and ASCII. The data is displayed in a hex dump format, with the first line showing the Ethernet II header (0800 0800 27c7 e136 0800 2739 ec20 0800 27c7 e136).

HTTP

kali-linux-2023.1-virtualbox-amd64 [in esecuzione] - Oracle VM VirtualBox

File Macchine Visualizza Inserimento Dispositivi Aiuto

*eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Firewall ACL Rules

Credentials

Apply a display filter ... <Ctrl-F>

Lua

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.32.101	192.168.32.100	TCP	66	49691 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
2	0.000055010	192.168.32.100	192.168.32.101	TCP	66	80 → 49691 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
3	0.000230140	192.168.32.101	192.168.32.100	TCP	60	49691 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
4	0.002362140	192.168.32.101	192.168.32.100	HTTP	532	GET / HTTP/1.1
5	0.002396040	192.168.32.100	192.168.32.101	TCP	54	80 → 49690 [ACK] Seq=1 Ack=479 Win=501 Len=0
6	0.015839750	192.168.32.100	192.168.32.101	TCP	204	80 → 49690 [PSH, ACK] Seq=1 Ack=479 Win=501 Len=150 [TCP segment of a reassembled PDU]
7	0.018497830	192.168.32.100	192.168.32.101	HTTP	312	HTTP/1.1 200 OK (text/html)
8	0.018819737	192.168.32.101	192.168.32.100	TCP	60	49690 → 80 [ACK] Seq=479 Ack=410 Win=255 Len=0
9	0.048630540	192.168.32.101	192.168.32.100	TCP	60	49690 → 80 [FIN, ACK] Seq=479 Ack=410 Win=255 Len=0
10	0.048666700	192.168.32.101	192.168.32.101	TCP	54	80 → 49690 [ACK] Seq=410 Ack=480 Win=501 Len=0
11	0.067973919	192.168.32.101	192.168.32.100	HTTP	451	GET /favicon.ico HTTP/1.1
12	0.068014997	192.168.32.100	192.168.32.101	TCP	54	80 → 49691 [ACK] Seq=1 Ack=398 Win=64128 Len=0
13	0.083347994	192.168.32.100	192.168.32.101	TCP	207	80 → 49691 [PSH, ACK] Seq=1 Ack=398 Win=64128 Len=153 [TCP segment of a reassembled PDU]
14	0.087165298	192.168.32.100	192.168.32.101	HTTP	252	HTTP/1.1 200 OK (image/x-icon)
15	0.087505776	192.168.32.101	192.168.32.100	TCP	60	49691 → 80 [ACK] Seq=398 Ack=353 Win=65280 Len=0
16	0.092658481	192.168.32.101	192.168.32.100	TCP	60	49691 → 80 [FIN, ACK] Seq=398 Ack=353 Win=65280 Len=0
17	0.092690727	192.168.32.101	192.168.32.101	TCP	54	80 → 49691 [ACK] Seq=353 Ack=399 Win=64128 Len=0
18	0.766525836	192.168.32.101	192.168.32.100	TCP	66	49692 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM

[Time delta from previous displayed frame: 0.000000000 seconds]
[Time since reference or first frame: 0.000000000 seconds]
Frame Number: 1
Frame Length: 66 bytes (528 bits)
Capture Length: 66 bytes (528 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:tcp]
[Coloring Rule Name: HTTP]
[Coloring Rule String: http || tcp.port == 80 || http2]

Ethernet II, Src: PcsCompu_39:ec:20 (08:00:27:39:ec:20), Dst: PcsCompu_c7:e1:36 (08:00:27:c7:e1:36)

- Destination: PcsCompu_c7:e1:36 (08:00:27:c7:e1:36)
Address: PcsCompu_c7:e1:36 (08:00:27:c7:e1:36)
... .. = LG bit: Globally unique address (factory default)
... .. = IG bit: Individual address (unicast)
- Source: PcsCompu_39:ec:20 (08:00:27:39:ec:20)
Address: PcsCompu_39:ec:20 (08:00:27:39:ec:20)
... .. = LG bit: Globally unique address (factory default)
... .. = IG bit: Individual address (unicast)

Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 192.168.32.101, Dst: 192.168.32.100

Transmission Control Protocol, Src Port: 49691, Dst Port: 80, Seq: 0, Len: 0

wireshark_eth0Z4XE41.pcapng

Packets: 30 - Displayed: 30 (100.0%)

Profile: Default

CTRL (DESTRA)