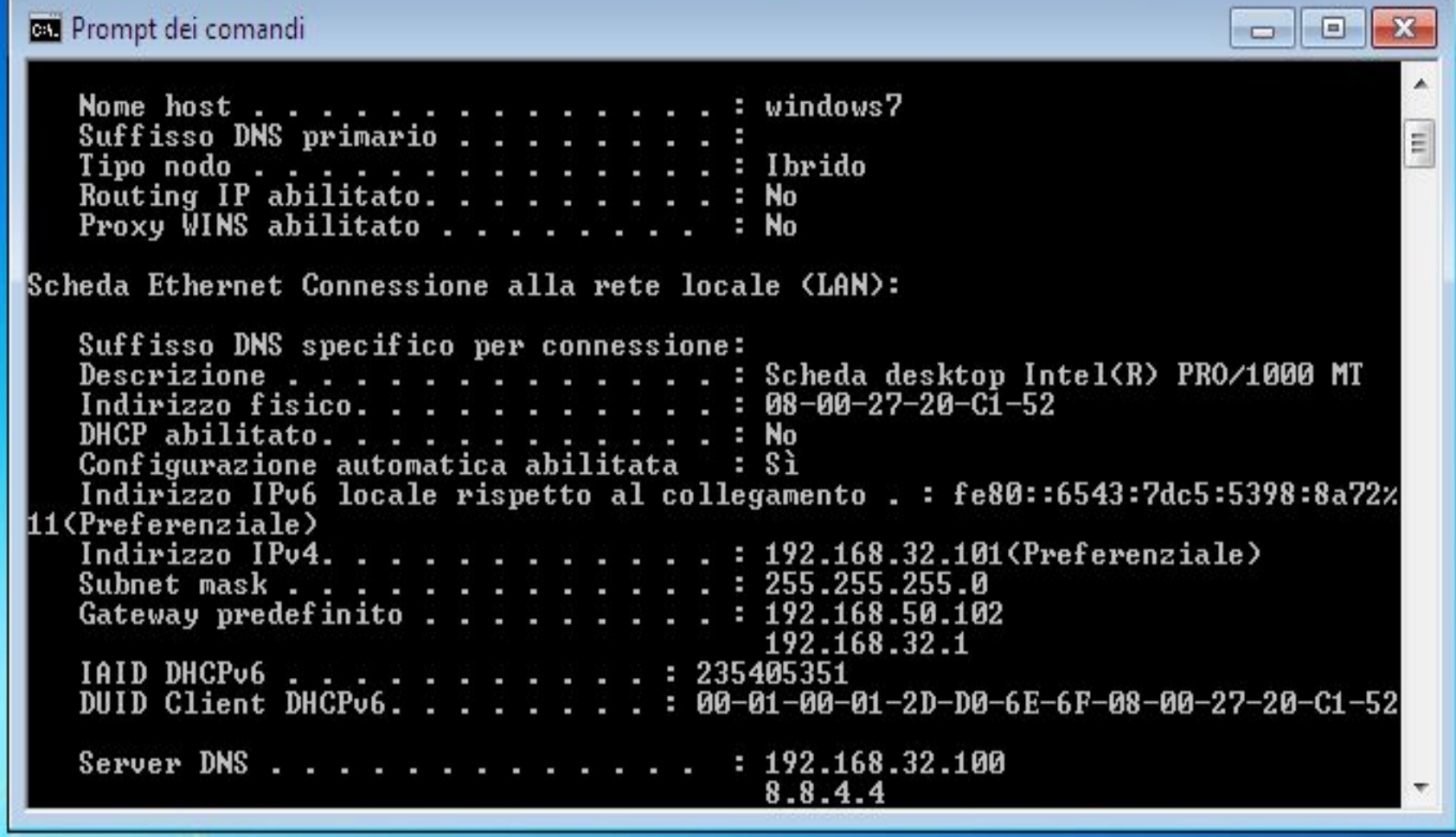
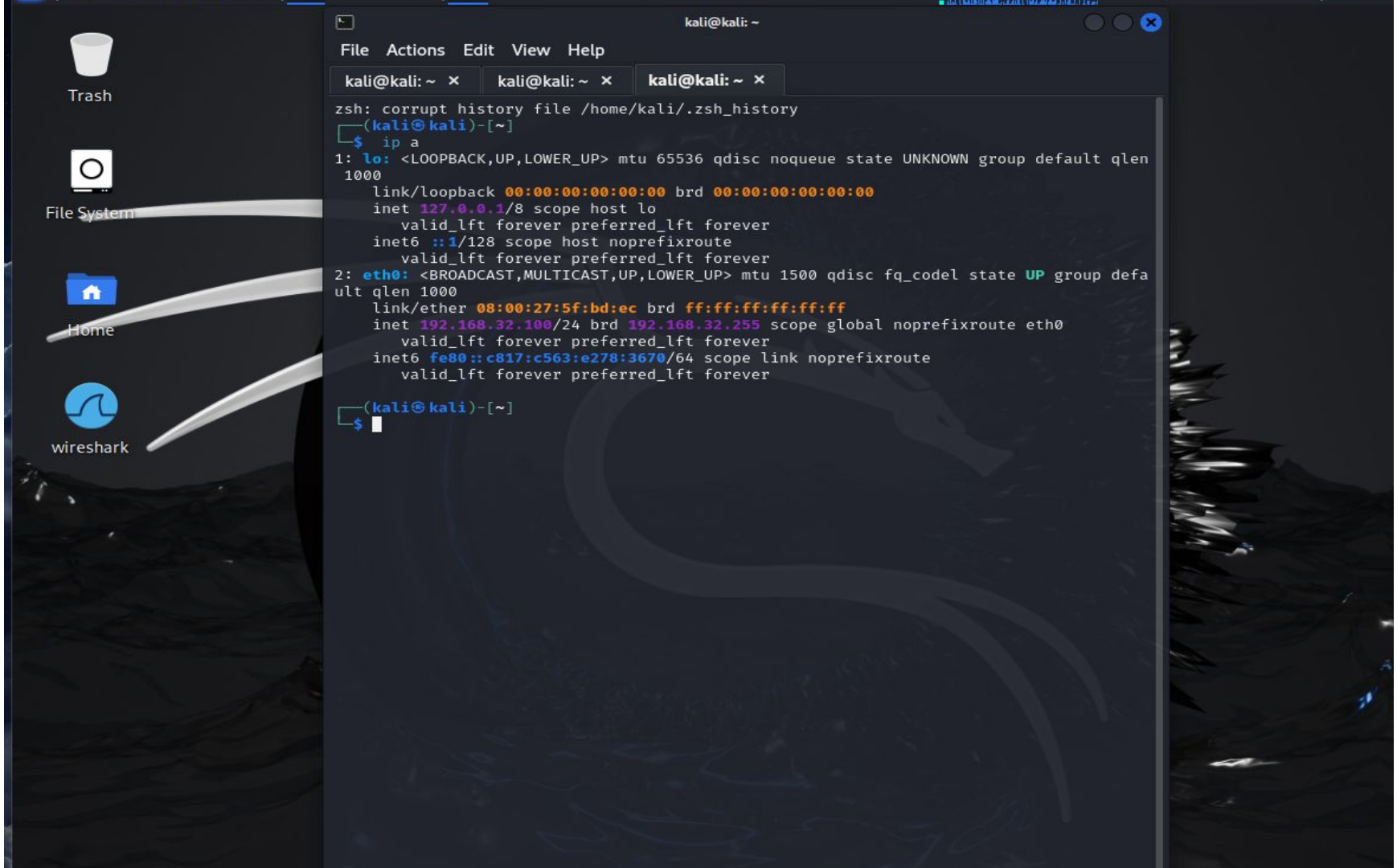
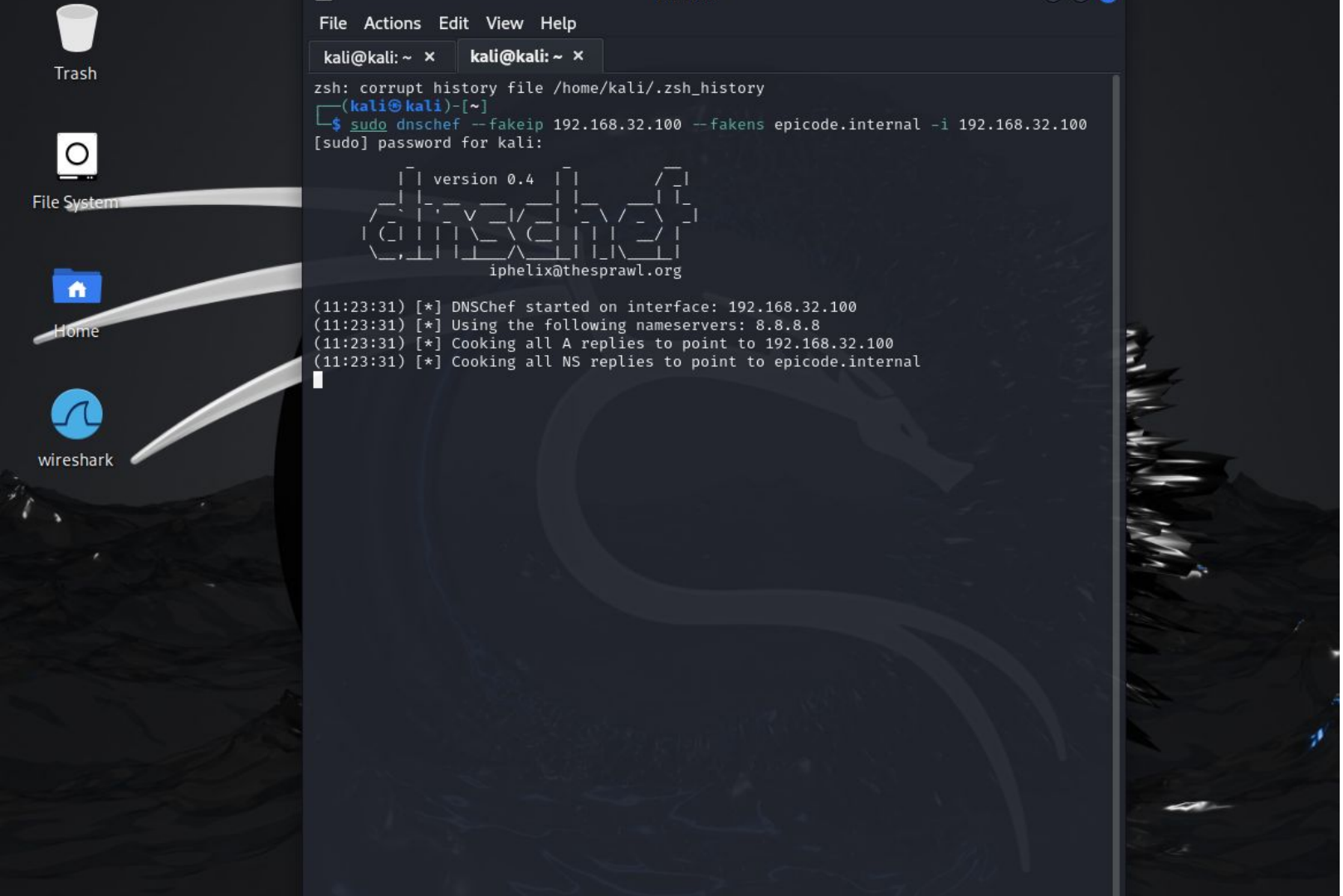
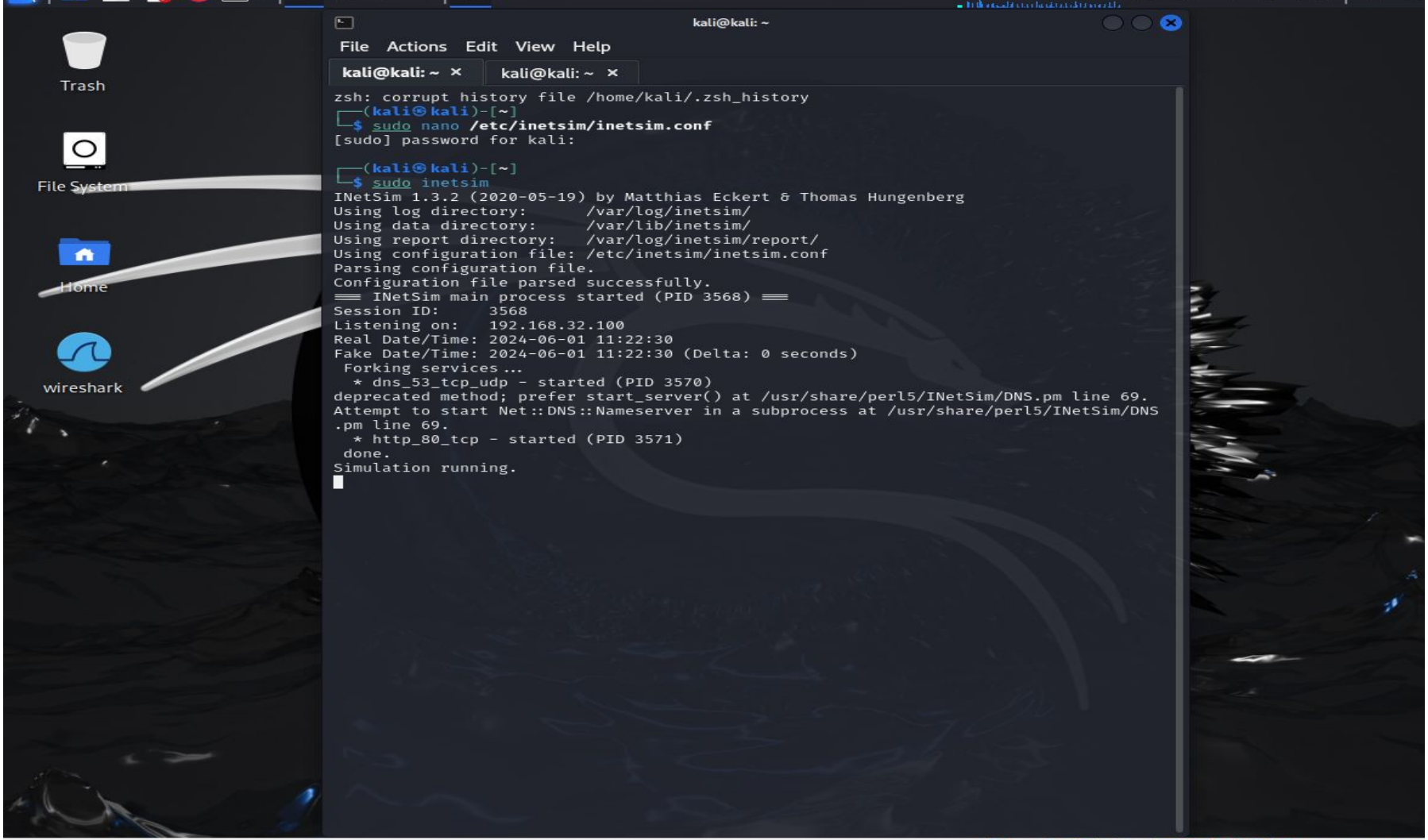
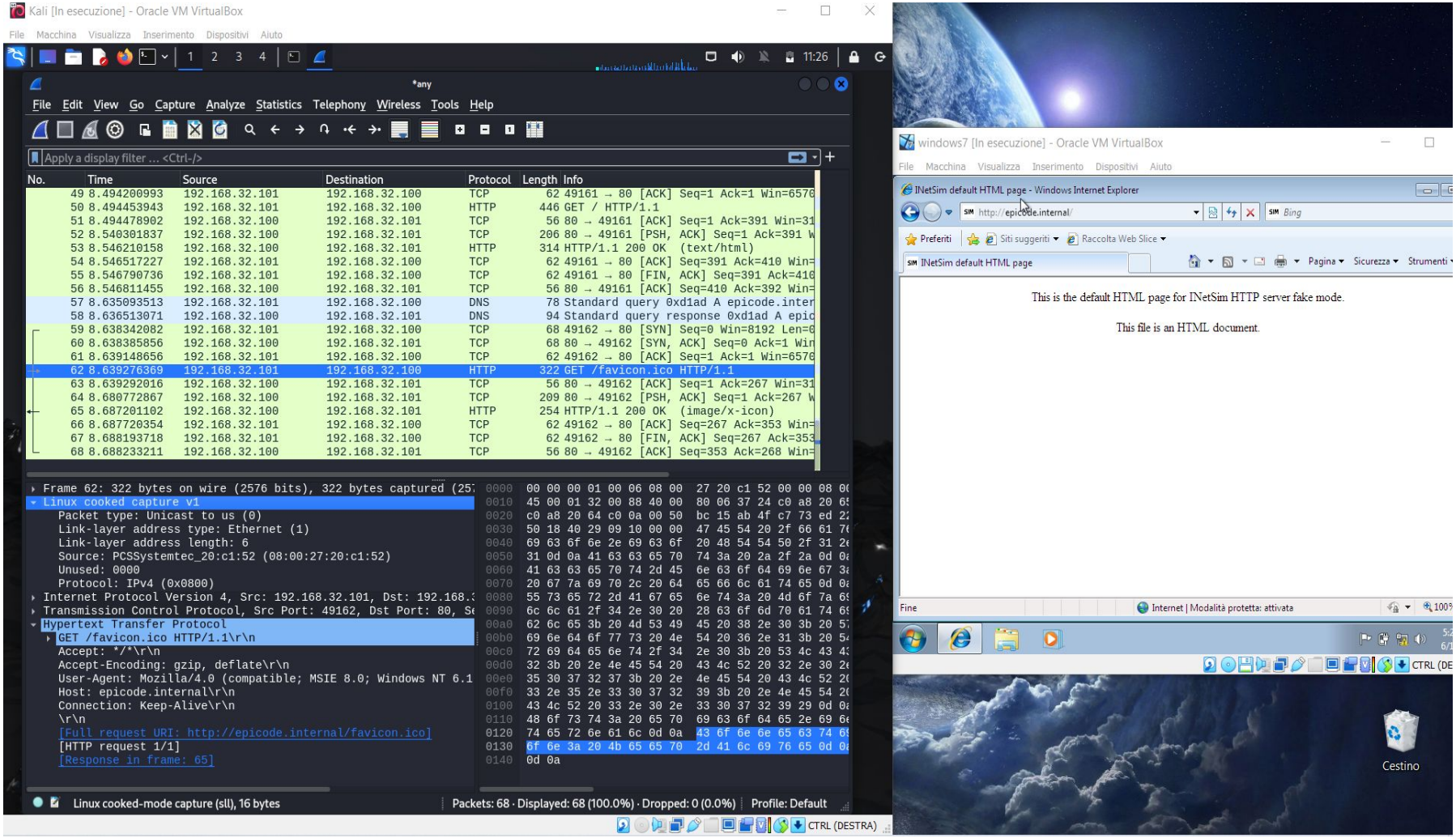
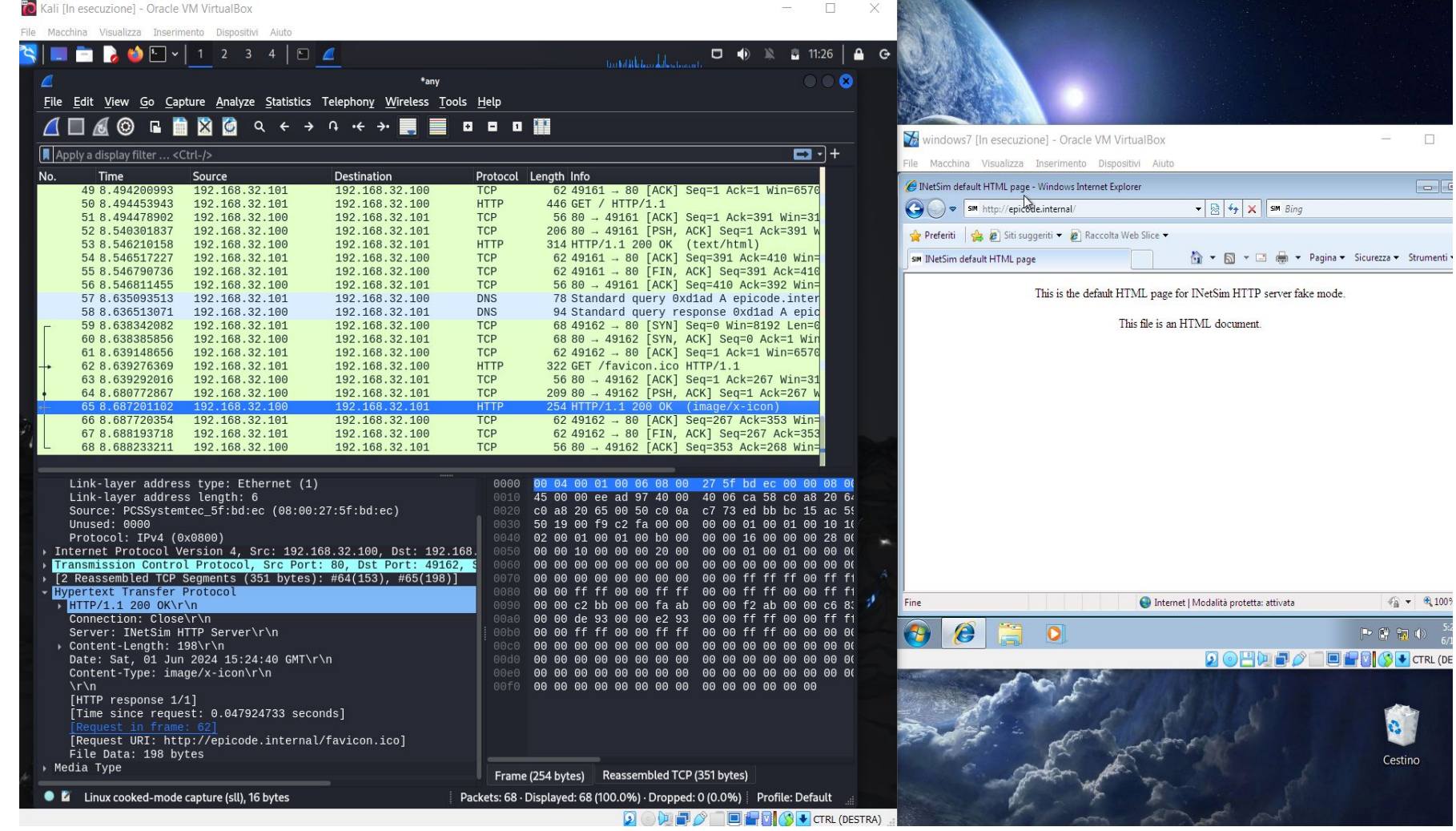

Prompt dei comandi
Nome host . . . . . : windows7
Suffisso DNS primario . . . . . :
Tipo nodo . . . . . : Ibrido
Routing IP abilitato. . . . . : No
Proxy WINS abilitato . . . . . : No
Scheda Ethernet Connessione alla rete locale (LAN):
Suffisso DNS specifico per connessione:
Descrizione . . . . . : Scheda desktop Intel(R) PRO/1000 MT
Indirizzo fisico. . . . . : 08-00-27-20-C1-52
DHCP abilitato. . . . . : No
Configurazione automatica abilitata : Sì
Indirizzo IPv6 locale rispetto al collegamento . : fe80::6543:7dc5:5398:8a72%
11(Preferenziale)
Indirizzo IPv4. . . . . : 192.168.32.101(Preferenziale)
Subnet mask . . . . . : 255.255.255.0
Gateway predefinito . . . . . : 192.168.50.102
192.168.32.1
IAID DHCPv6 . . . . . : 235405351
DUID Client DHCPv6. . . . . : 00-01-00-01-2D-D0-6E-6F-08-00-27-20-C1-52
Server DNS . . . . . : 192.168.32.100
8.8.4.4

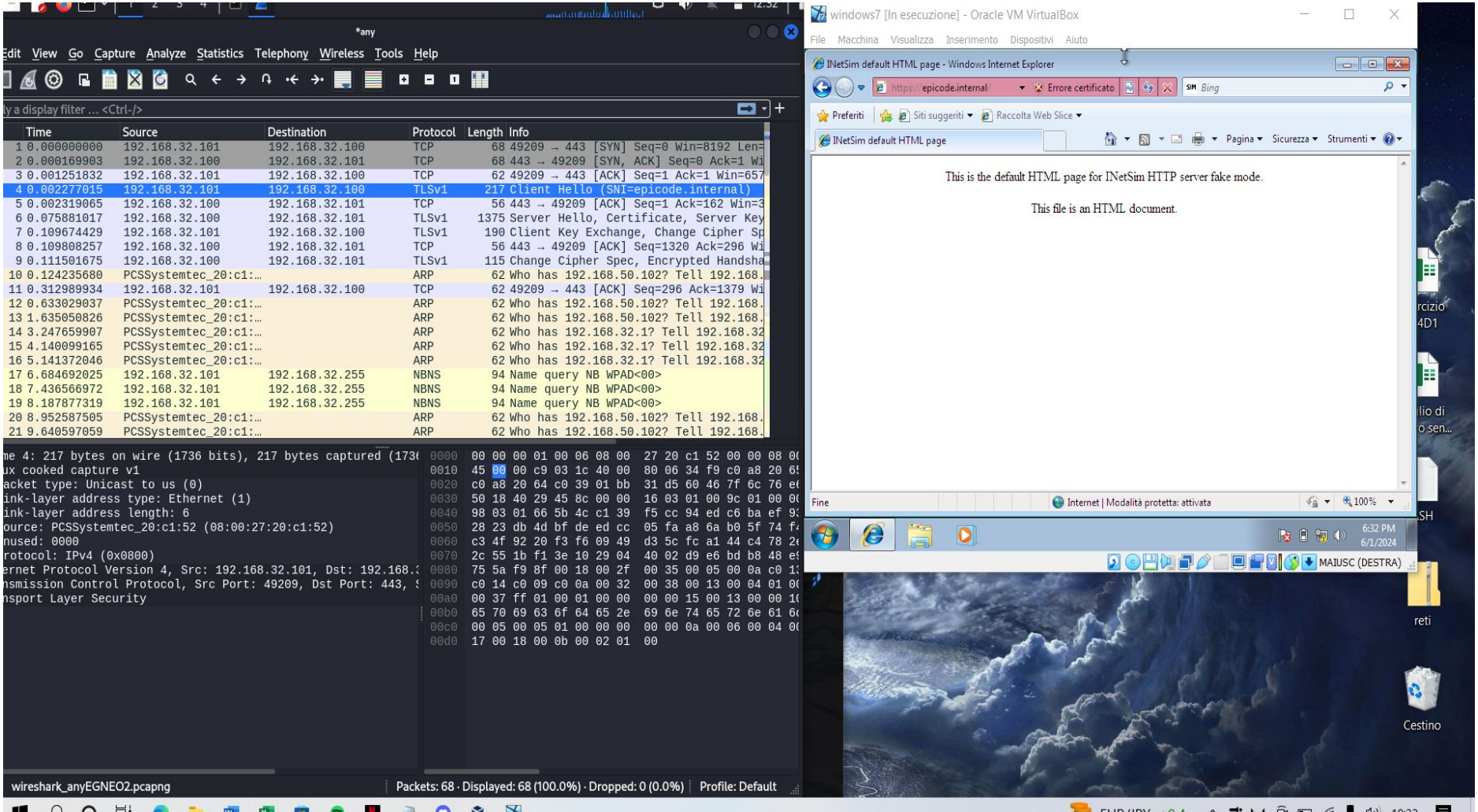

Trash
File System
Home
wireshark
kali@kali: ~
File Actions Edit View Help
kali@kali: ~ ×
kali@kali: ~ ×
kali@kali: ~ ×
zsh: corrupt history file /home/kali/.zsh_history
(kali㉿kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host noprefixroute
valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
link/ether 08:00:27:5f:bd:ec brd ff:ff:ff:ff:ff:ff
inet 192.168.32.100/24 brd 192.168.32.255 scope global noprefixroute eth0
valid_lft forever preferred_lft forever
inet6 fe80::c817:c563:e278:3670/64 scope link noprefixroute
valid_lft forever preferred_lft forever
(kali㉿kali)-[~]
$

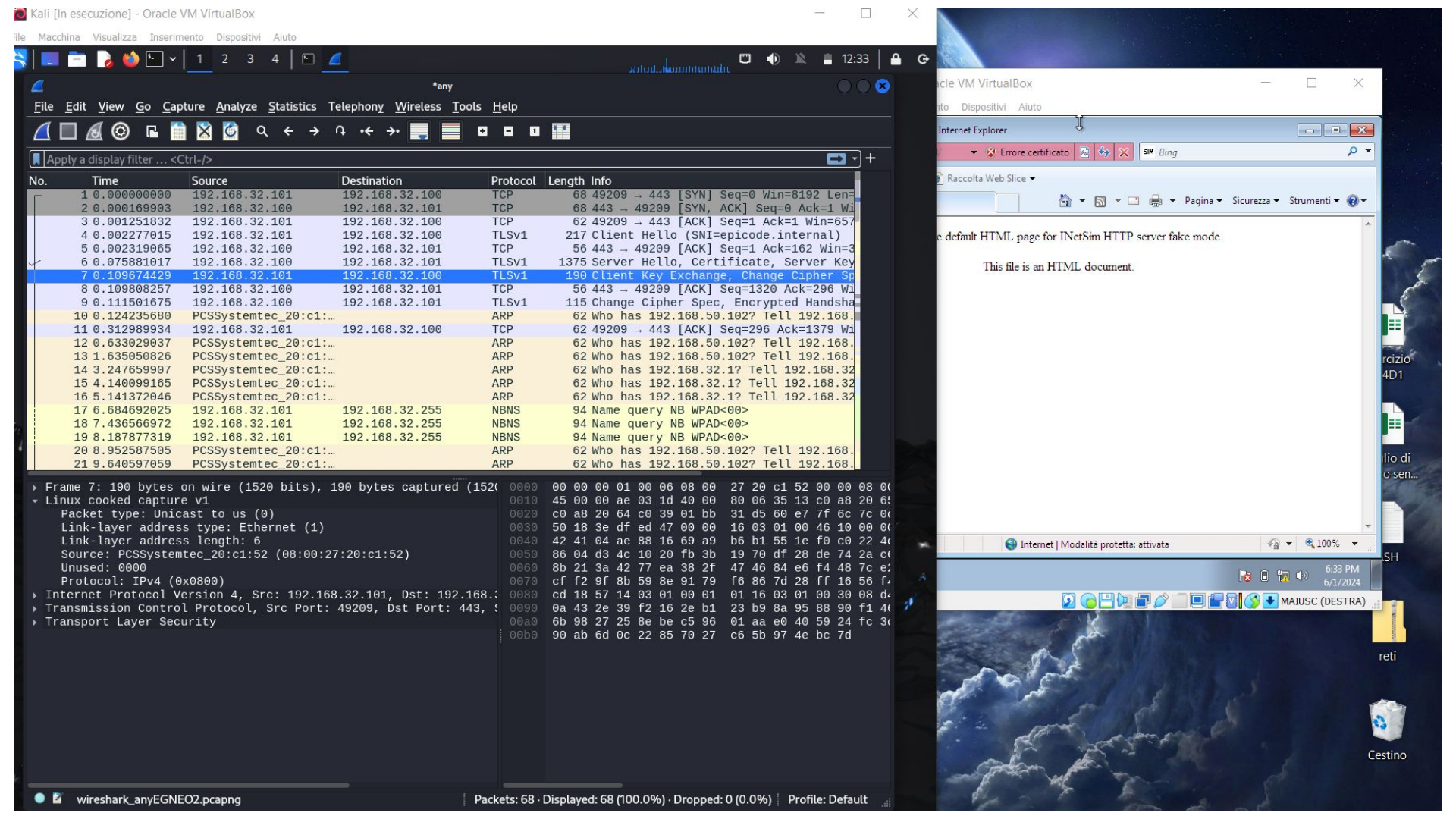

Trash
File System
Home
wireshark
File Actions Edit View Help
kali@kali: ~ ×
kali@kali: ~ ×
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ sudo dnschef --fakeip 192.168.32.100 --fakens epicode.internal -i 192.168.32.100
[sudo] password for kali:
version 0.4
iphelix@thesprawl.org
(11:23:31) [*] DNSChef started on interface: 192.168.32.100
(11:23:31) [*] Using the following nameservers: 8.8.8.8
(11:23:31) [*] Cooking all A replies to point to 192.168.32.100
(11:23:31) [*] Cooking all NS replies to point to epicode.internal

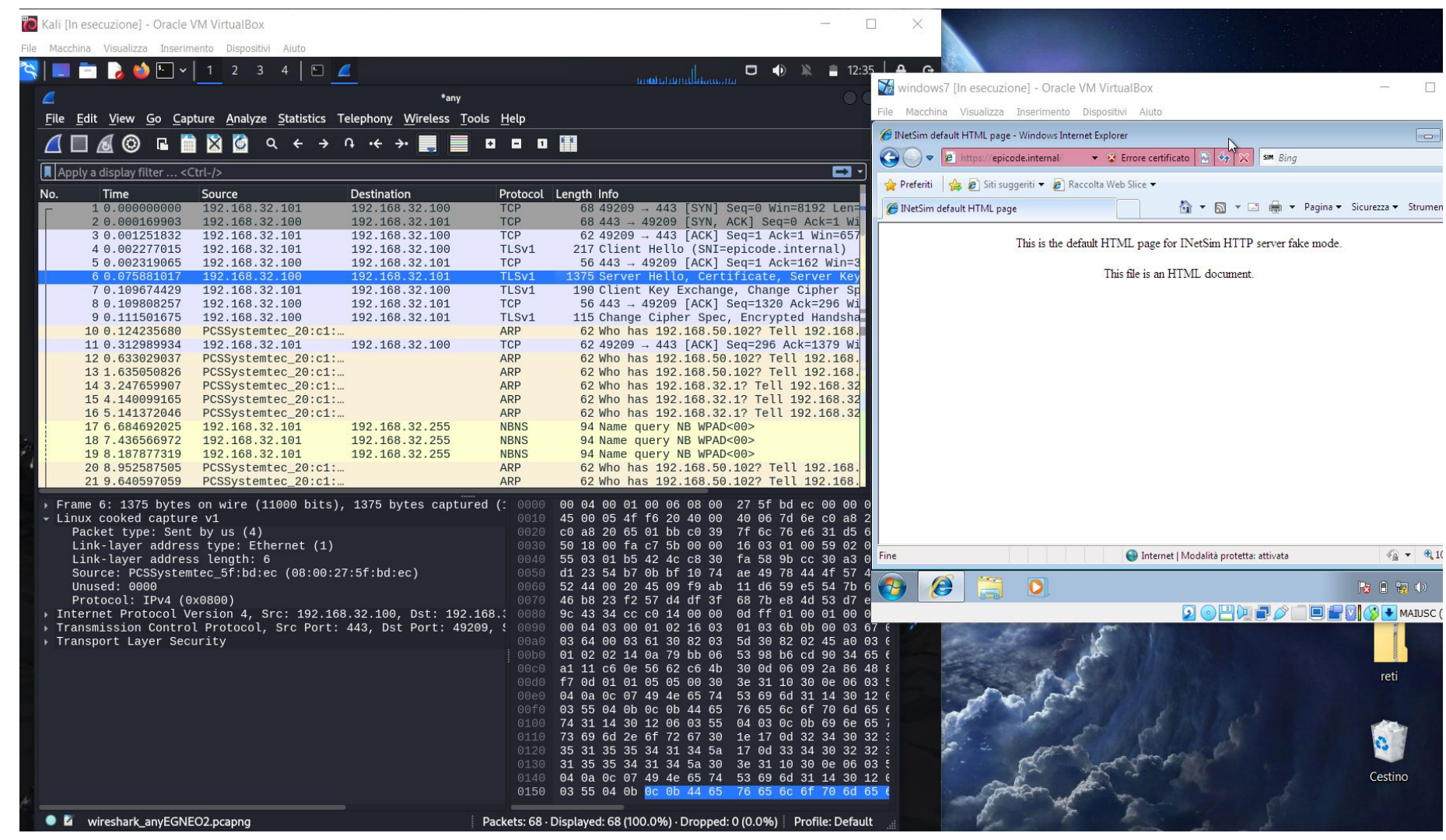

Trash
File System
Home
wireshark
kali@kali: ~
File Actions Edit View Help
kali@kali: ~ ×
kali@kali: ~ ×
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ sudo nano /etc/inetsim/inetsim.conf
[sudo] password for kali:
┌──(kali㉿kali)-[~]
└─$ sudo inetsim
INetSim 1.3.2 (2020-05-19) 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 3568) ===
Session ID: 3568
Listening on: 192.168.32.100
Real Date/Time: 2024-06-01 11:22:30
Fake Date/Time: 2024-06-01 11:22:30 (Delta: 0 seconds)
Forking services...
* dns_53_tcp_udp - started (PID 3570)
deprecated method; prefer start_server() at /usr/share/perl5/INetSim/DNS.pm line 69.
Attempt to start Net::DNS::Nameserver in a subprocess at /usr/share/perl5/INetSim/DNS
.pm line 69.
* http_80_tcp - started (PID 3571)
done.
Simulation running.
CTRL (DESTRA)


Kali [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
*any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
49 8.494200993 192.168.32.101 192.168.32.100 TCP 62 49161 → 80 [ACK] Seq=1 Ack=1 Win=6576
50 8.494453943 192.168.32.101 192.168.32.100 HTTP 446 GET / HTTP/1.1
51 8.494478902 192.168.32.100 192.168.32.101 TCP 56 80 → 49161 [ACK] Seq=1 Ack=391 Win=31
52 8.540301837 192.168.32.100 192.168.32.101 TCP 206 80 → 49161 [PSH, ACK] Seq=1 Ack=391 W
53 8.546210158 192.168.32.100 192.168.32.101 HTTP 314 HTTP/1.1 200 OK (text/html)
54 8.546517227 192.168.32.101 192.168.32.100 TCP 62 49161 → 80 [ACK] Seq=391 Ack=410 Win=
55 8.546790736 192.168.32.101 192.168.32.100 TCP 62 49161 → 80 [FIN, ACK] Seq=391 Ack=410
56 8.546811455 192.168.32.100 192.168.32.101 TCP 56 80 → 49161 [ACK] Seq=410 Ack=392 Win=
57 8.635093513 192.168.32.101 192.168.32.100 DNS 78 Standard query 0xd1ad A epicode.inter
58 8.636513071 192.168.32.100 192.168.32.101 DNS 94 Standard query response 0xd1ad A epic
59 8.638342082 192.168.32.101 192.168.32.100 TCP 68 49162 → 80 [SYN] Seq=0 Win=8192 Len=0
60 8.638385856 192.168.32.100 192.168.32.101 TCP 68 80 → 49162 [SYN, ACK] Seq=0 Ack=1 Win
61 8.639148656 192.168.32.101 192.168.32.100 TCP 62 49162 → 80 [ACK] Seq=1 Ack=1 Win=6576
62 8.639276369 192.168.32.101 192.168.32.100 HTTP 322 GET /favicon.ico HTTP/1.1
63 8.639292016 192.168.32.100 192.168.32.101 TCP 56 80 → 49162 [ACK] Seq=1 Ack=267 Win=31
64 8.680772867 192.168.32.100 192.168.32.101 TCP 209 80 → 49162 [PSH, ACK] Seq=1 Ack=267 W
65 8.687201102 192.168.32.100 192.168.32.101 HTTP 254 HTTP/1.1 200 OK (image/x-icon)
66 8.687720354 192.168.32.101 192.168.32.100 TCP 62 49162 → 80 [ACK] Seq=267 Ack=353 Win=
67 8.688193718 192.168.32.101 192.168.32.100 TCP 62 49162 → 80 [FIN, ACK] Seq=267 Ack=353
68 8.688233211 192.168.32.100 192.168.32.101 TCP 56 80 → 49162 [ACK] Seq=353 Ack=268 Win=
Frame 62: 322 bytes on wire (2576 bits), 322 bytes captured (257
Linux cooked capture v1
Packet type: Unicast to us (0)
Link-layer address type: Ethernet (1)
Link-layer address length: 6
Source: PCSSystemtec_20:c1:52 (08:00:27:20:c1:52)
Unused: 0000
Protocol: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.32.101, Dst: 192.168.3
Transmission Control Protocol, Src Port: 49162, Dst Port: 80, Se
Hypertext Transfer Protocol
GET /favicon.ico HTTP/1.1\r\n
Accept: */*\r\n
Accept-Encoding: gzip, deflate\r\n
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1
Host: epicode.internal\r\n
Connection: Keep-Alive\r\n
\r\n
[Full request URI: http://epicode.internal/favicon.ico]
[HTTP request 1/1]
[Response in frame: 65]
0000 00 00 00 01 00 06 08 00 27 20 c1 52 00 00 08 0
0010 45 00 01 32 00 88 40 00 80 06 37 24 c0 a8 20 6
0020 c0 a8 20 64 c0 0a 00 50 bc 15 ab 4f c7 73 ed 2
0030 50 18 40 29 09 10 00 00 47 45 54 20 2f 66 61 7
0040 69 63 6f 6e 2e 69 63 6f 20 48 54 54 50 2f 31 2
0050 31 0d 0a 41 63 63 65 70 74 3a 20 2a 2f 2a 0d 0
0060 41 63 63 65 70 74 2d 45 6e 63 6f 64 69 6e 67 3
0070 20 67 7a 69 70 2c 20 64 65 66 6c 61 74 65 0d 0
0080 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 6
0090 6c 6c 61 2f 34 2e 30 20 28 63 6f 6d 70 61 74 6
00a0 62 6c 65 3b 20 4d 53 49 45 20 38 2e 30 3b 20 5
00b0 69 6e 64 6f 77 73 20 4e 54 20 36 2e 31 3b 20 5
00c0 72 69 64 65 6e 74 2f 34 2e 30 3b 20 53 4c 43 4
00d0 32 3b 20 2e 4e 45 54 20 43 4c 52 20 32 2e 30 2
00e0 35 30 37 32 37 3b 20 2e 4e 45 54 20 43 4c 52 2
00f0 33 2e 35 2e 33 30 37 32 39 3b 20 2e 4e 45 54 2
0100 43 4c 52 20 33 2e 30 2e 33 30 37 32 39 29 0d 0
0110 48 6f 73 74 3a 20 65 70 69 63 6f 64 65 2e 69 6
0120 74 65 72 6e 61 6c 0d 0a 43 6f 6e 6e 65 63 74 6
0130 6f 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d 0
0140 0d 0a
Linux cooked-mode capture (sll), 16 bytes
Packets: 68 · Displayed: 68 (100.0%) · Dropped: 0 (0.0%)
Profile: Default
CTRL (DESTRA)
windows7 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
INetSim default HTML page - Windows Internet Explorer
http://epicode.internal/
Preferiti
INetSim default HTML page
This is the default HTML page for INetSim HTTP server fake mode.
This file is an HTML document.
Fine
Internet | Modalità protetta: attivata
Cestino


Kali [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
11:26
*any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
49 8.494200993 192.168.32.101 192.168.32.100 TCP 62 49161 → 80 [ACK] Seq=1 Ack=1 Win=6570
50 8.494453943 192.168.32.101 192.168.32.100 HTTP 446 GET / HTTP/1.1
51 8.494478902 192.168.32.100 192.168.32.101 TCP 56 80 → 49161 [ACK] Seq=1 Ack=391 Win=31
52 8.540301837 192.168.32.100 192.168.32.101 TCP 206 80 → 49161 [PSH, ACK] Seq=1 Ack=391 W
53 8.546210158 192.168.32.100 192.168.32.101 HTTP 314 HTTP/1.1 200 OK (text/html)
54 8.546517227 192.168.32.101 192.168.32.100 TCP 62 49161 → 80 [ACK] Seq=391 Ack=410 Win=
55 8.546790736 192.168.32.101 192.168.32.100 TCP 62 49161 → 80 [FIN, ACK] Seq=391 Ack=410
56 8.546811455 192.168.32.100 192.168.32.101 TCP 56 80 → 49161 [ACK] Seq=410 Ack=392 Win=
57 8.635093513 192.168.32.101 192.168.32.100 DNS 78 Standard query 0xd1ad A epicode.inter
58 8.636513071 192.168.32.100 192.168.32.101 DNS 94 Standard query response 0xd1ad A epic
59 8.638342082 192.168.32.101 192.168.32.100 TCP 68 49162 → 80 [SYN] Seq=0 Win=8192 Len=0
60 8.638385856 192.168.32.100 192.168.32.101 TCP 68 80 → 49162 [SYN, ACK] Seq=0 Ack=1 Win
61 8.639148656 192.168.32.101 192.168.32.100 TCP 62 49162 → 80 [ACK] Seq=1 Ack=1 Win=6570
62 8.639276369 192.168.32.101 192.168.32.100 HTTP 322 GET /favicon.ico HTTP/1.1
63 8.639292016 192.168.32.100 192.168.32.101 TCP 56 80 → 49162 [ACK] Seq=1 Ack=267 Win=31
64 8.680772867 192.168.32.100 192.168.32.101 TCP 209 80 → 49162 [PSH, ACK] Seq=1 Ack=267 W
65 8.687201102 192.168.32.100 192.168.32.101 HTTP 254 HTTP/1.1 200 OK (image/x-icon)
66 8.687720354 192.168.32.101 192.168.32.100 TCP 62 49162 → 80 [ACK] Seq=267 Ack=353 Win=
67 8.688193718 192.168.32.101 192.168.32.100 TCP 62 49162 → 80 [FIN, ACK] Seq=267 Ack=353
68 8.688233211 192.168.32.100 192.168.32.101 TCP 56 80 → 49162 [ACK] Seq=353 Ack=268 Win=
Link-layer address type: Ethernet (1)
Link-layer address length: 6
Source: PCSSystemtec_5f:bd:ec (08:00:27:5f:bd:ec)
Unused: 0000
Protocol: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.32.100, Dst: 192.168.
Transmission Control Protocol, Src Port: 80, Dst Port: 49162, S
[2 Reassembled TCP Segments (351 bytes): #64(153), #65(198)]
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
Connection: Close\r\n
Server: INetSim HTTP Server\r\n
Content-Length: 198\r\n
Date: Sat, 01 Jun 2024 15:24:40 GMT\r\n
Content-Type: image/x-icon\r\n
\r\n
[HTTP response 1/1]
[Time since request: 0.047924733 seconds]
[Request in frame: 62]
[Request URI: http://epicode.internal/favicon.ico]
File Data: 198 bytes
Media Type
0000 00 04 00 01 00 06 08 00 27 5f bd ec 00 00 08 0
0010 45 00 00 ee ad 97 40 00 40 06 ca 58 c0 a8 20 6
0020 c0 a8 20 65 00 50 c0 0a c7 73 ed bb bc 15 ac 5
0030 50 19 00 f9 c2 fa 00 00 00 00 01 00 01 00 10 1
0040 02 00 01 00 01 00 b0 00 00 00 16 00 00 00 28 0
0050 00 00 10 00 00 00 20 00 00 00 01 00 01 00 00 0
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0
0070 00 00 00 00 00 00 00 00 00 00 ff ff ff 00 ff f
0080 00 00 ff ff 00 00 ff ff 00 00 ff ff 00 00 ff f
0090 00 00 c2 bb 00 00 fa ab 00 00 f2 ab 00 00 c6 8
00a0 00 00 de 93 00 00 e2 93 00 00 ff ff 00 00 ff f
00b0 00 00 ff ff 00 00 ff ff 00 00 ff ff 00 00 00 0
00c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0
00d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0
00e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0
00f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Frame (254 bytes)
Reassembled TCP (351 bytes)
Linux cooked-mode capture (sll), 16 bytes
Packets: 68 · Displayed: 68 (100.0%) · Dropped: 0 (0.0%)
Profile: Default
CTRL (DESTRA)
windows7 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
INetSim default HTML page - Windows Internet Explorer
http://epicode.internal/
Bing
Preferiti
Siti suggeriti
Raccolta Web Slice
INetSim default HTML page
Pagina
Sicurezza
Strumenti
This is the default HTML page for INetSim HTTP server fake mode.
This file is an HTML document.
Fine
Internet | Modalità protetta: attivata
100%
CTRL (DE
Cestino


*any
Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000000 192.168.32.101 192.168.32.100 TCP 68 49209 → 443 [SYN] Seq=0 Win=8192 Len=
2 0.000169903 192.168.32.100 192.168.32.101 TCP 68 443 → 49209 [SYN, ACK] Seq=0 Ack=1 Wi
3 0.001251832 192.168.32.101 192.168.32.100 TCP 62 49209 → 443 [ACK] Seq=1 Ack=1 Win=657
4 0.002277015 192.168.32.101 192.168.32.100 TLSv1 217 Client Hello (SNI=epicode.internal)
5 0.002319065 192.168.32.100 192.168.32.101 TCP 56 443 → 49209 [ACK] Seq=1 Ack=162 Win=3
6 0.075881017 192.168.32.100 192.168.32.101 TLSv1 1375 Server Hello, Certificate, Server Key
7 0.109674429 192.168.32.101 192.168.32.100 TLSv1 190 Client Key Exchange, Change Cipher Sp
8 0.109808257 192.168.32.100 192.168.32.101 TCP 56 443 → 49209 [ACK] Seq=1320 Ack=296 Wi
9 0.111501675 192.168.32.100 192.168.32.101 TLSv1 115 Change Cipher Spec, Encrypted Handsha
10 0.124235680 PCSSystemtec_20:c1:... ARP 62 Who has 192.168.50.102? Tell 192.168.
11 0.312989934 192.168.32.101 192.168.32.100 TCP 62 49209 → 443 [ACK] Seq=296 Ack=1379 Wi
12 0.633029037 PCSSystemtec_20:c1:... ARP 62 Who has 192.168.50.102? Tell 192.168.
13 1.635050826 PCSSystemtec_20:c1:... ARP 62 Who has 192.168.50.102? Tell 192.168.
14 3.247659907 PCSSystemtec_20:c1:... ARP 62 Who has 192.168.32.1? Tell 192.168.32
15 4.140099165 PCSSystemtec_20:c1:... ARP 62 Who has 192.168.32.1? Tell 192.168.32
16 5.141372046 PCSSystemtec_20:c1:... ARP 62 Who has 192.168.32.1? Tell 192.168.32
17 6.684692025 192.168.32.101 192.168.32.255 NBNS 94 Name query NB WPAD<00>
18 7.436566972 192.168.32.101 192.168.32.255 NBNS 94 Name query NB WPAD<00>
19 8.187877319 192.168.32.101 192.168.32.255 NBNS 94 Name query NB WPAD<00>
20 8.952587505 PCSSystemtec_20:c1:... ARP 62 Who has 192.168.50.102? Tell 192.168.
21 9.640597059 PCSSystemtec_20:c1:... ARP 62 Who has 192.168.50.102? Tell 192.168.
Frame 4: 217 bytes on wire (1736 bits), 217 bytes captured (173(
Linux cooked capture v1
Packet type: Unicast to us (0)
Link-layer address type: Ethernet (1)
Link-layer address length: 6
Source: PCSSystemtec_20:c1:52 (08:00:27:20:c1:52)
Unused: 0000
Protocol: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.32.101, Dst: 192.168.3
Transmission Control Protocol, Src Port: 49209, Dst Port: 443, S
Transport Layer Security
0000 00 00 00 01 00 06 08 00 27 20 c1 52 00 00 08 0(
0010 45 00 00 c9 03 1c 40 00 80 06 34 f9 c0 a8 20 6(
0020 c0 a8 20 64 c0 39 01 bb 31 d5 60 46 7f 6c 76 e(
0030 50 18 40 29 45 8c 00 00 16 03 01 00 9c 01 00 0(
0040 98 03 01 66 5b 4c c1 39 f5 cc 94 ed c6 ba ef 9(
0050 28 23 db 4d bf de ed cc 05 fa a8 6a b0 5f 74 f(
0060 c3 4f 92 20 f3 f6 09 49 d3 5c fc a1 44 c4 78 2(
0070 2c 55 1b f1 3e 10 29 04 40 02 d9 e6 bd b8 48 e(
0080 75 5a f9 8f 00 18 00 2f 00 35 00 05 00 0a c0 1(
0090 c0 14 c0 09 c0 0a 00 32 00 38 00 13 00 04 01 0(
00a0 00 37 ff 01 00 01 00 00 00 00 15 00 13 00 00 1(
00b0 65 70 69 63 6f 64 65 2e 69 6e 74 65 72 6e 61 6(
00c0 00 05 00 05 01 00 00 00 00 00 0a 00 06 00 04 0(
00d0 17 00 18 00 0b 00 02 01 00
wireshark_anyEGNEO2.pcapng
Packets: 68 · Displayed: 68 (100.0%) · Dropped: 0 (0.0%)
Profile: Default
windows7 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
INetSim default HTML page - Windows Internet Explorer
https://epicode.internal/
Errore certificato
Bing
Preferiti
Siti suggeriti
Raccolta Web Slice
INetSim default HTML page
Pagina
Sicurezza
Strumenti
This is the default HTML page for INetSim HTTP server fake mode.
This file is an HTML document.
Fine
Internet | Modalità protetta: attivata
100%
6:32 PM
6/1/2024
MAIUSC (DESTRA)
reti
Cestino
EUR/JPY +0,4...
18:32


Kali [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
1 2 3 4
12:33
*any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000000 192.168.32.101 192.168.32.100 TCP 68 49209 → 443 [SYN] Seq=0 Win=8192 Len=
2 0.000169903 192.168.32.100 192.168.32.101 TCP 68 443 → 49209 [SYN, ACK] Seq=0 Ack=1 Wi
3 0.001251832 192.168.32.101 192.168.32.100 TCP 62 49209 → 443 [ACK] Seq=1 Ack=1 Win=657
4 0.002277015 192.168.32.101 192.168.32.100 TLSv1 217 Client Hello (SNI=epicode.internal)
5 0.002319065 192.168.32.100 192.168.32.101 TCP 56 443 → 49209 [ACK] Seq=1 Ack=162 Win=3
6 0.075881017 192.168.32.100 192.168.32.101 TLSv1 1375 Server Hello, Certificate, Server Key
7 0.109674429 192.168.32.101 192.168.32.100 TLSv1 190 Client Key Exchange, Change Cipher Sp
8 0.109808257 192.168.32.100 192.168.32.101 TCP 56 443 → 49209 [ACK] Seq=1320 Ack=296 Wi
9 0.111501675 192.168.32.100 192.168.32.101 TLSv1 115 Change Cipher Spec, Encrypted Handsha
10 0.124235680 PCSSystemtec_20:c1:… ARP 62 Who has 192.168.50.102? Tell 192.168.
11 0.312989934 192.168.32.101 192.168.32.100 TCP 62 49209 → 443 [ACK] Seq=296 Ack=1379 Wi
12 0.633029037 PCSSystemtec_20:c1:… ARP 62 Who has 192.168.50.102? Tell 192.168.
13 1.635050826 PCSSystemtec_20:c1:… ARP 62 Who has 192.168.50.102? Tell 192.168.
14 3.247659907 PCSSystemtec_20:c1:… ARP 62 Who has 192.168.32.1? Tell 192.168.32
15 4.140099165 PCSSystemtec_20:c1:… ARP 62 Who has 192.168.32.1? Tell 192.168.32
16 5.141372046 PCSSystemtec_20:c1:… ARP 62 Who has 192.168.32.1? Tell 192.168.32
17 6.684692025 192.168.32.101 192.168.32.255 NBNS 94 Name query NB WPAD<00>
18 7.436566972 192.168.32.101 192.168.32.255 NBNS 94 Name query NB WPAD<00>
19 8.187877319 192.168.32.101 192.168.32.255 NBNS 94 Name query NB WPAD<00>
20 8.952587505 PCSSystemtec_20:c1:… ARP 62 Who has 192.168.50.102? Tell 192.168.
21 9.640597059 PCSSystemtec_20:c1:… ARP 62 Who has 192.168.50.102? Tell 192.168.
Frame 7: 190 bytes on wire (1520 bits), 190 bytes captured (152
Linux cooked capture v1
Packet type: Unicast to us (0)
Link-layer address type: Ethernet (1)
Link-layer address length: 6
Source: PCSSystemtec_20:c1:52 (08:00:27:20:c1:52)
Unused: 0000
Protocol: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.32.101, Dst: 192.168.3
Transmission Control Protocol, Src Port: 49209, Dst Port: 443, S
Transport Layer Security
0000 00 00 00 01 00 06 08 00 27 20 c1 52 00 00 08 0
0010 45 00 00 ae 03 1d 40 00 80 06 35 13 c0 a8 20 6
0020 c0 a8 20 64 c0 39 01 bb 31 d5 60 e7 7f 6c 7c 0
0030 50 18 3e df ed 47 00 00 16 03 01 00 46 10 00 0
0040 42 41 04 ae 88 16 69 a9 b6 b1 55 1e f0 c0 22 4
0050 86 04 d3 4c 10 20 fb 3b 19 70 df 28 de 74 2a c
0060 8b 21 3a 42 77 ea 38 2f 47 46 84 e6 f4 48 7c e
0070 cf f2 9f 8b 59 8e 91 79 f6 86 7d 28 ff 16 56 f
0080 cd 18 57 14 03 01 00 01 01 16 03 01 00 30 08 d
0090 0a 43 2e 39 f2 16 2e b1 23 b9 8a 95 88 90 f1 4
00a0 6b 98 27 25 8e be c5 96 01 aa e0 40 59 24 fc 3
00b0 90 ab 6d 0c 22 85 70 27 c6 5b 97 4e bc 7d
wireshark_anyEGNEO2.pcapng
Packets: 68 · Displayed: 68 (100.0%) · Dropped: 0 (0.0%)
Profile: Default
Internet Explorer
Errore certificato
Bing
Raccolta Web Slice
Pagina Sicurezza Strumenti
e default HTML page for INetSim HTTP server fake mode.
This file is an HTML document.
Internet | Modalità protetta: attivata
100%
6:33 PM
6/1/2024
MAIUSC (DESTRA)
reti
Cestino


Kali [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
*any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000000 192.168.32.101 192.168.32.100 TCP 68 49209 → 443 [SYN] Seq=0 Win=8192 Len=
2 0.000169903 192.168.32.100 192.168.32.101 TCP 68 443 → 49209 [SYN, ACK] Seq=0 Ack=1 Wi
3 0.001251832 192.168.32.101 192.168.32.100 TCP 62 49209 → 443 [ACK] Seq=1 Ack=1 Win=657
4 0.002277015 192.168.32.101 192.168.32.100 TLSv1 217 Client Hello (SNI=epicode.internal)
5 0.002319065 192.168.32.100 192.168.32.101 TCP 56 443 → 49209 [ACK] Seq=1 Ack=162 Win=3
6 0.075881017 192.168.32.100 192.168.32.101 TLSv1 1375 Server Hello, Certificate, Server Key
7 0.109674429 192.168.32.101 192.168.32.100 TLSv1 190 Client Key Exchange, Change Cipher Sp
8 0.109808257 192.168.32.100 192.168.32.101 TCP 56 443 → 49209 [ACK] Seq=1320 Ack=296 Wi
9 0.111501675 192.168.32.100 192.168.32.101 TLSv1 115 Change Cipher Spec, Encrypted Handsha
10 0.124235680 PCSSystemtec_20:c1:… ARP 62 Who has 192.168.50.102? Tell 192.168.
11 0.312989934 192.168.32.101 192.168.32.100 TCP 62 49209 → 443 [ACK] Seq=296 Ack=1379 Wi
12 0.633029037 PCSSystemtec_20:c1:… ARP 62 Who has 192.168.50.102? Tell 192.168.
13 1.635050826 PCSSystemtec_20:c1:… ARP 62 Who has 192.168.50.102? Tell 192.168.
14 3.247659907 PCSSystemtec_20:c1:… ARP 62 Who has 192.168.32.1? Tell 192.168.32
15 4.140099165 PCSSystemtec_20:c1:… ARP 62 Who has 192.168.32.1? Tell 192.168.32
16 5.141372046 PCSSystemtec_20:c1:… ARP 62 Who has 192.168.32.1? Tell 192.168.32
17 6.684692025 192.168.32.101 192.168.32.255 NBNS 94 Name query NB WPAD<00>
18 7.436566972 192.168.32.101 192.168.32.255 NBNS 94 Name query NB WPAD<00>
19 8.187877319 192.168.32.101 192.168.32.255 NBNS 94 Name query NB WPAD<00>
20 8.952587505 PCSSystemtec_20:c1:… ARP 62 Who has 192.168.50.102? Tell 192.168.
21 9.640597059 PCSSystemtec_20:c1:… ARP 62 Who has 192.168.50.102? Tell 192.168.
Frame 6: 1375 bytes on wire (11000 bits), 1375 bytes captured (
Linux cooked capture v1
Packet type: Sent by us (4)
Link-layer address type: Ethernet (1)
Link-layer address length: 6
Source: PCSSystemtec_5f:bd:ec (08:00:27:5f:bd:ec)
Unused: 0000
Protocol: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.32.100, Dst: 192.168.
Transmission Control Protocol, Src Port: 443, Dst Port: 49209,
Transport Layer Security
0000 00 04 00 01 00 06 08 00 27 5f bd ec 00 00
0010 45 00 05 4f f6 20 40 00 40 06 7d 6e c0 a8
0020 c0 a8 20 65 01 bb c0 39 7f 6c 76 e6 31 d5
0030 50 18 00 fa c7 5b 00 00 16 03 01 00 59 02
0040 55 03 01 b5 42 4c c8 30 fa 58 9b cc 30 a3
0050 d1 23 54 b7 0b bf 10 74 ae 49 78 44 4f 57
0060 52 44 00 20 45 09 f9 ab 11 d6 59 e5 54 7b
0070 46 b8 23 f2 57 d4 df 3f 68 7b e8 4d 53 d7
0080 9c 43 34 cc c0 14 00 00 0d ff 01 00 01 00
0090 00 04 03 00 01 02 16 03 01 03 6b 0b 00 03
00a0 03 64 00 03 61 30 82 03 5d 30 82 02 45 a0
00b0 01 02 02 14 0a 79 bb 06 53 98 b6 cd 90 34
00c0 a1 11 c6 0e 56 62 c6 4b 30 0d 06 09 2a 86
00d0 f7 0d 01 01 05 05 00 30 3e 31 10 30 0e 06
00e0 04 0a 0c 07 49 4e 65 74 53 69 6d 31 14 30
00f0 03 55 04 0b 0c 0b 44 65 76 65 6c 6f 70 6d
0100 74 31 14 30 12 06 03 55 04 03 0c 0b 69 6e
0110 73 69 6d 2e 6f 72 67 30 1e 17 0d 32 34 30
0120 35 31 35 35 34 31 34 5a 17 0d 33 34 30 32
0130 31 35 35 34 31 34 5a 30 3e 31 10 30 0e 06
0140 04 0a 0c 07 49 4e 65 74 53 69 6d 31 14 30
0150 03 55 04 0b 0c 0b 44 65 76 65 6c 6f 70 6d
wireshark_anyEGNEO2.pcapng
Packets: 68 · Displayed: 68 (100.0%) · Dropped: 0 (0.0%)
Profile: Default
windows7 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
INetSim default HTML page - Windows Internet Explorer
https://epicode.internal/
Errore certificato
Preferiti
Siti suggeriti
Raccolta Web Slice
INetSim default HTML page
This is the default HTML page for INetSim HTTP server fake mode.
This file is an HTML document.
Fine
Internet | Modalità protetta: attivata
reti
Cestino

COMMENTO ESERCIZIO

Le principali differenze osservate tra HTTP e HTTPS è stata la sicurezza offerta da HTTPS grazie alla crittografia SSL/TLS, che garantisce la protezione dei dati e l’autenticità del server. Questo esercizio ha sottolineato l’importanza di utilizzare HTTPS per proteggere le informazioni sensibili, soprattutto in un contesto in cui la sicurezza dei dati è fondamentale.