

IP kali

```
(alessio@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:fe4:4ff0 prefixlen 64 scopeid 0x20<link>
            ether 08:00:27:c4:4f:f0 txqueuelen 1000 (Ethernet)
                RX packets 10 bytes 904 (904.0 B)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 32 bytes 3748 (3.6 KiB)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

IP Win 7

```
Windows IP Configuration

Ethernet adapter Local Area Connection:
  Connection-specific DNS Suffix . .
  Link-local IPv6 Address . . . . . fe80::1060:e1b4:6e97:c82ax11
  IPv4 Address . . . . . 192.168.32.101
  Subnet Mask . . . . . 255.255.255.0
  Default Gateway . . . . . 192.168.32.1

Tunnel adapter isatap.<51CEDC76-E031-447A-A7BA-7220996385B6>:
  Media State . . . . . Media disconnected
  Connection-specific DNS Suffix . .

C:\Users\vboxuser>_
```

Kali

```

Kali Linux [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
alessio@kali: ~
File Actions Edit View Help
Forking services...
* dns_53_tcp_udp - started (PID 27761)
* https_443_tcp - started (PID 27762)
done.
Simulation running.
^C * https_443_tcp - stopped (PID 27762)
* dns_53_tcp_udp - stopped (PID 27761)
Simulation stopped.
== INetSim main process stopped (PID 27759) ==
File system

(alessio@kali)-[~]
$ sudo nano /etc/inetsim/inetsim.conf

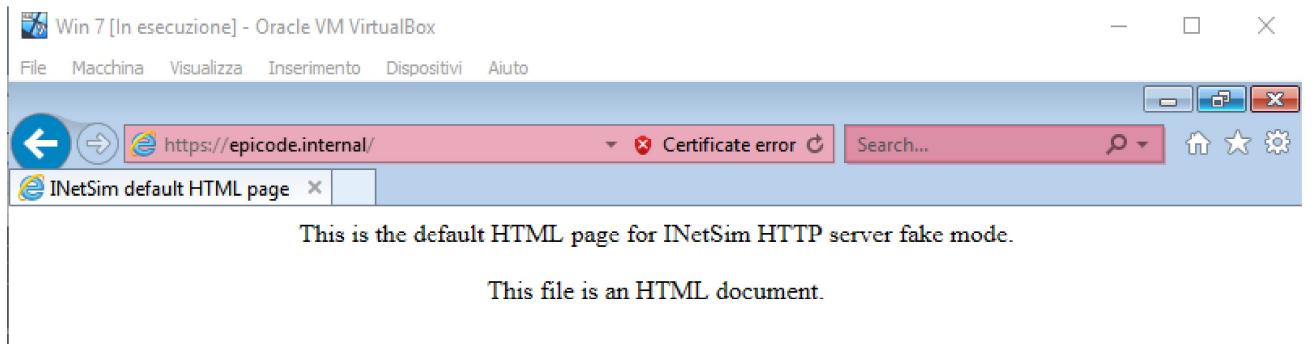
(alessio@kali)-[~]
$ sudo inetsim
INetSim 1.3.2 (2020-05-19) by Matthias Eckert & Thomas Hungenberg
Using log directory:      /var/log/inetsim/
Using data directory:     /var/lib/inetsim/
Using report directory:   /var/log/inetsim/report/
Using configuration file: /etc/inetsim/inetsim.conf
Parsing configuration file.
Configuration file parsed successfully.
== INetSim main process started (PID 29035) ==
Session ID: 29035
Listening on: 192.168.32.100
Real Date/Time: 2023-01-27 05:23:30
Fake Date/Time: 2023-01-27 05:23:30 (Delta: 0 seconds)
Forking services...
* dns_53_tcp_udp - started (PID 29041)
* https_443_tcp - started (PID 29042)
done.
Simulation running.

alessio@kali: ~
File Actions Edit View Help
[sudo] password for alessio:
(alessio@kali)-[~]
$ sudo nano /etc/network/interfaces
[sudo] password for alessio:
(alessio@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:fe00:1000 prefixlen 64 scopeid 0x20<link>
                  ether 08:00:27:c4:4f:f0 txqueuelen 1000 (Ethernet)
                  RX packets 203 bytes 16132 (15.7 KiB)
                  RX errors 0 dropped 0 overruns 0 frame 0
                  TX packets 34 bytes 3888 (3.7 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 0x10<host>
          loop txqueuelen 1000 (Local Loopback)
          RX packets 4 bytes 240 (240.0 B)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 4 bytes 240 (240.0 B)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

## HTTPS da Win7



## Wireshark su Https, con MAC sorgente di Windows

Capturing from any

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Protocol	Length	Info
242	118.814464845	192.168.32.100	192.168.32.101	TLSv1.2	87	Encrypted Alert
243	118.815276821	192.168.32.101	192.168.32.100	TCP	62	49211 → 443 [RST, ACK] Seq=87 Ack=231
244	118.816266032	192.168.32.101	192.168.32.100	TCP	64	49214 → 443 [SYN] Seq=0 Win=1
245	118.816281787	192.168.32.100	192.168.32.101	TCP	64	443 → 49214 [SYN, ACK] Seq=1 Win=1
246	118.816787873	192.168.32.101	192.168.32.100	TCP	62	49214 → 443 [ACK] Seq=1 Win=1
247	118.817047223	192.168.32.101	192.168.32.100	TLSv1.2	273	Client Hello
248	118.817053226	192.168.32.100	192.168.32.101	TCP	56	443 → 49214 [ACK] Seq=1 Win=1
249	118.844065009	192.168.32.100	192.168.32.101	TLSv1.2	1823	Server Hello, Certificate
250	118.844530980	192.168.32.101	192.168.32.100	TCP	62	49214 → 443 [ACK] Seq=218
251	118.862010797	192.168.32.101	192.168.32.100	TLSv1.2	374	Client Key Exchange, Change Cipher Spec, Encry
252	118.864475927	192.168.32.100	192.168.32.101	TLSv1.2	107	Change Cipher Spec, Encry
253	118.865295048	192.168.32.101	192.168.32.100	TCP	62	49214 → 443 [ACK] Seq=536
254	118.868927284	192.168.32.101	192.168.32.100	TLSv1.2	336	Application Data
255	118.875704974	192.168.32.100	192.168.32.101	TLSv1.2	236	Application Data
256	118.877122441	192.168.32.101	192.168.32.100	TCP	62	49214 → 443 [ACK] Seq=816
257	118.877131863	192.168.32.100	192.168.32.101	TLSv1.2	343	Application Data
258	118.877285866	192.168.32.100	192.168.32.101	TLSv1.2	87	Encrypted Alert
259	118.877531358	192.168.32.101	192.168.32.100	TCP	62	49214 → 443 [ACK] Seq=816
260	118.877719738	192.168.32.101	192.168.32.100	TCP	62	49214 → 443 [ACK] Seq=816
261	118.878159681	192.168.32.101	192.168.32.100	TCP	62	49214 → 443 [FIN, ACK] Seq=816 Win=1
262	118.878168976	192.168.32.100	192.168.32.101	TCP	56	443 → 49214 [ACK] Seq=231

Frame 256: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface eth0, Intel PRO/100 MT Desktop, IEEE 802.3 (Ethernet), Src: PcsCompu\_a1:50:9e (08:00:27:a1:50:9e), Dst: 192.168.32.100 (192.168.32.100)

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

Transmission Control Protocol, Src Port: 49214, Dst Port: 443

Source Port: 49214  
 Destination Port: 443  
 [Stream index: 19]  
 [Conversation completeness: Complete, WITH\_DATA (31)]  
 [TCP Segment Len: 0]  
 Sequence Number: 816 (relative sequence number)  
 Sequence Number (raw): 1822348409  
 Acknowledgment Number: 816 (relative sequence number)  
 Acknowledgment Number (raw): 1822348409

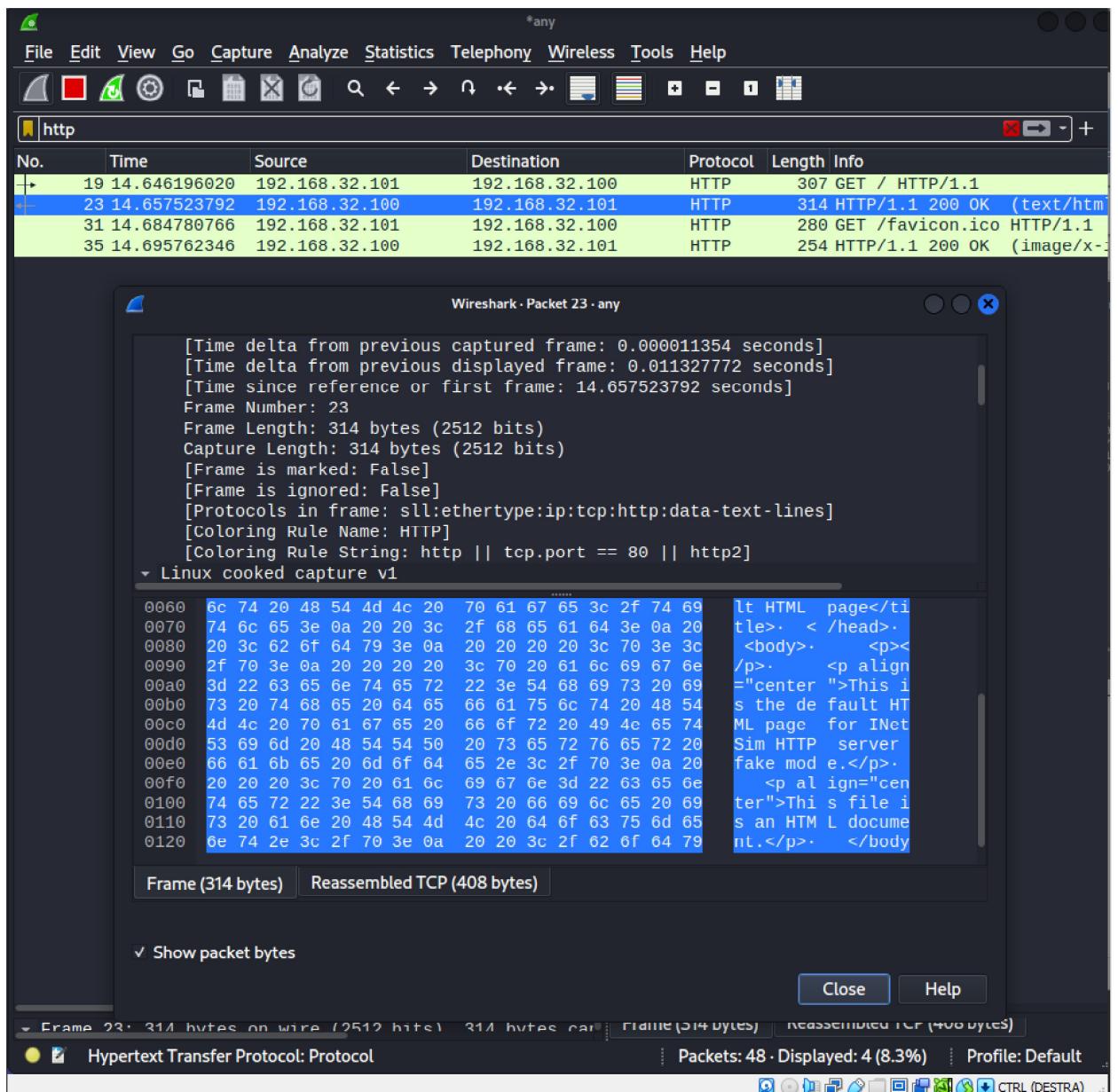
Source link-layer address (Sll.src.eth), 6 bytes

Packets: 262 · Displayed: 262 (100.0%) · Profile: Default

HTTP da Win 7

The browser window title bar says "SIM http://epicode.internal/" and the address bar says "SIM INetSim default HTML page". The main content area displays the text: "This is the default HTML page for INetSim HTTP server fake mode." and "This file is an HTML document."

Wireshark su Http



MAC Kali

→	25	49.137277245	192.168.32.101	192.168.32.100
←	29	49.147558039	192.168.32.100	192.168.32.101

```
Frame 25: 307 bytes on wire (2456 bits), 307 bytes captured
Linux cooked capture v1
    Packet type: Unicast to us (0)
    Link-layer address type: Ethernet (1)
    Link-layer address length: 6
    Source: PcsCompu_a1:50:9e (08:00:27:a1:50:9e)
    Unused: 0000
```