

```
File Macchina Visualizza Inserimento Dispositivi Aiuto
kali@kali: ~
File Actions Edit View Help
Fake Date/Time: 2023-01-27 08:23:00 (Delta: 0 seconds)
Forking services ...
* dns_53_tcp_udp - started (PID 49156)
* http_80_tcp - started (PID 49157)
done.
Simulation running.
^C * http_80_tcp - stopped (PID 49157)
* dns_53_tcp_udp - stopped (PID 49156)
Simulation stopped.
Report written to '/var/log/inetsim/report/report.49154.txt' (17 lines)
== INetSim main process stopped (PID 49154) ==
.
(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:fe1d:2b27 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:1d:2b:27 txqueuelen 1000 (Ethernet)
    RX packets 2534 bytes 231109 (225.6 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1177 bytes 244857 (239.1 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 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
```

Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

☐ Obtain an IP address automatically

☒ Use the following IP address:

IP address: 192 . 168 . 32 . 101

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 32 . 1

☐ Obtain DNS server address automatically

☒ Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 32 . 100

Alternate DNS server: . . .

☐ Validate settings upon exit

Advanced...

OK Cancel

```
Pinging epicode.internal [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
```

Modifica indirizzi IP e aggiunta server DNS su Windows (IP Kali)

Test di comunicazione con un ping

```

File Actions Edit View Help
GNU nano 6.4 /etc/inetsim/inetsim.conf *
#####
#
# INetSim configuration file
#
#####
# Main configuration
#####
#####
# start_service
#
# The services to start
#
# Syntax: start_service <service name>
#
# Default: none
#
# Available service names are:
# dns, http, smtp, pop3, tftp, ftp, ntp, time_tcp,
# time_udp, daytime_tcp, daytime_udp, echo_tcp,
# echo_udp, discard_tcp, discard_udp, quotd_tcp,
# quotd_udp, chargen_tcp, chargen_udp, finger,
# ident, syslog, dummy_tcp, dummy_udp, smtps, pop3s,
# ftps, irc, https
#
start_service dns
start_service http
start_service https
start_service smtp

```

```

#####
# service_bind_address
#
# IP address to bind services to
#
# Syntax: service_bind_address <IP address>
#
# Default: 127.0.0.1
#
service_bind_address 192.168.32.100
#####

```

```

#####
# dns_default_ip
#
# Default IP address to return with DNS replies
#
# Syntax: dns_default_ip <IP address>
#
# Default: inetsim.org
#
dns_default_ip 192.168.32.100

#####
# dns_default_hostname
#
# Default hostname to return with DNS replies
#
# Syntax: dns_default_hostname <hostname>
#
Default: www.epicode.internal
#
#dns_default_hostname somehost

```

```

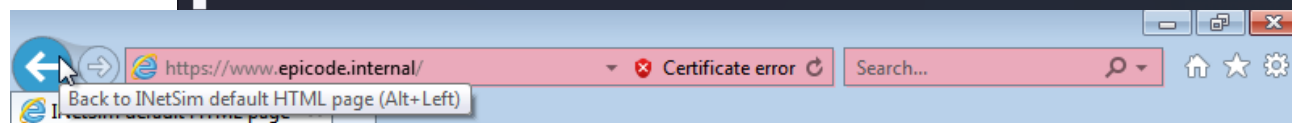
#####
# dns_static
#
# Static mappings for DNS
#
# Syntax: dns_static <fqdn hostname> <IP address>
#
# Default: none
#
dns_static epicode.internal 192.168.32.100
#dns_static ns1.foo.com 10.70.50.30
#dns_static ftp.bar.net 10.10.20.30

```

```

(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.
Warning: Unknown option 'Default:' in configuration file '/etc/inetsim/inetsim.conf' line 217
Configuration file parsed successfully.
== INetSim main process started (PID 54791) ==
Session ID: 54791
Listening on: 192.168.32.100
Real Date/Time: 2023-01-27 08:45:43
Fake Date/Time: 2023-01-27 08:45:43 (Delta: 0 seconds)
Forking services ...
* dns_53_tcp_udp - started (PID 54793)
* https_443_tcp - started (PID 54794)
done.
Simulation running.

```



Modifica di inetsim in voci DNS e abilitazione servizi https e DNS.

Attivazione simulazione

Ricerca di epicode.internal su browser di Windows

*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	PcsCompu_e8:14:fd		ARP	62	Who has 192.168.32.100? Tell 192.168.32.101
2	0.000012161	PcsCompu_1d:2b:27		ARP	44	192.168.32.100 is at 08:00:27:1d:2b:27
3	0.000153324	192.168.32.101	192.168.32.100	TCP	68	59552 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
4	0.000174050	192.168.32.100	192.168.32.101	TCP	68	443 → 59552 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
5	0.000292960	192.168.32.101	192.168.32.100	TCP	62	59552 → 443 [ACK] Seq=1 Ack=1 Win=65536 Len=0
6	0.000461919	192.168.32.101	192.168.32.100	TLSv1.2	277	Client Hello
7	0.000469409	192.168.32.100	192.168.32.101	TCP	56	443 → 59552 [ACK] Seq=1 Ack=222 Win=64128 Len=0
8	0.035092136	192.168.32.100	192.168.32.101	TLSv1.2	1823	Server Hello, Certificate, Server Key Exchange, Server Hello Done
9	0.035365279	192.168.32.101	192.168.32.100	TCP	62	59552 → 443 [ACK] Seq=222 Ack=1768 Win=65536 Len=0
10	0.056686115	192.168.32.101	192.168.32.100	TLSv1.2	374	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
11	0.059602129	192.168.32.100	192.168.32.101	TLSv1.2	107	Change Cipher Spec, Encrypted Handshake Message
12	0.060001320	192.168.32.101	192.168.32.100	TCP	62	59552 → 443 [ACK] Seq=540 Ack=1819 Win=65536 Len=0
13	0.065188769	192.168.32.101	192.168.32.100	TLSv1.2	340	Application Data
14	0.074346115	192.168.32.100	192.168.32.101	TLSv1.2	236	Application Data
15	0.074653654	192.168.32.101	192.168.32.100	TCP	62	59552 → 443 [ACK] Seq=824 Ack=1999 Win=65280 Len=0
16	0.074669648	192.168.32.100	192.168.32.101	TLSv1.2	343	Application Data
17	0.074884077	192.168.32.101	192.168.32.100	TCP	62	59552 → 443 [ACK] Seq=824 Ack=2286 Win=65024 Len=0
18	0.076188053	192.168.32.100	192.168.32.101	TLSv1.2	87	Encrypted Alert
19	0.076317578	192.168.32.101	192.168.32.100	TCP	62	59552 → 443 [ACK] Seq=824 Ack=2317 Win=65024 Len=0
20	0.076321680	192.168.32.100	192.168.32.101	TCP	56	443 → 59552 [FIN, ACK] Seq=2317 Ack=824 Win=64128 Len=0
21	0.076435515	192.168.32.101	192.168.32.100	TCP	62	59552 → 443 [ACK] Seq=824 Ack=2318 Win=65024 Len=0
22	0.076507886	192.168.32.101	192.168.32.100	TCP	62	59552 → 443 [FIN, ACK] Seq=824 Ack=2318 Win=65024 Len=0
23	0.076517999	192.168.32.100	192.168.32.101	TCP	56	443 → 59552 [ACK] Seq=2318 Ack=825 Win=64128 Len=0
24	0.083884085	192.168.32.101	192.168.32.100	TCP	68	59553 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
25	0.083905319	192.168.32.100	192.168.32.101	TCP	68	443 → 59553 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
26	0.084084273	192.168.32.101	192.168.32.100	TCP	62	59553 → 443 [ACK] Seq=1 Ack=1 Win=65536 Len=0
27	0.084398283	192.168.32.101	192.168.32.100	TLSv1.2	277	Client Hello
28	0.084405798	192.168.32.100	192.168.32.101	TCP	56	443 → 59553 [ACK] Seq=1 Ack=222 Win=64128 Len=0
29	0.116581940	192.168.32.100	192.168.32.101	TLSv1.2	1823	Server Hello, Certificate, Server Key Exchange, Server Hello Done
30	0.116946640	192.168.32.101	192.168.32.100	TCP	62	59553 → 443 [ACK] Seq=222 Ack=1768 Win=65536 Len=0
31	0.137849925	192.168.32.101	192.168.32.100	TLSv1.2	374	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
32	0.140893903	192.168.32.100	192.168.32.101	TLSv1.2	107	Change Cipher Spec, Encrypted Handshake Message
33	0.141220536	192.168.32.101	192.168.32.100	TCP	62	59553 → 443 [ACK] Seq=540 Ack=1819 Win=65536 Len=0
34	0.145044521	PcsCompu_e8:14:fd		ARP	62	Who has 192.168.32.1? Tell 192.168.32.101
35	0.731614894	PcsCompu_e8:14:fd		ARP	62	Who has 192.168.32.1? Tell 192.168.32.101
36	1.731603558	PcsCompu_e8:14:fd		ARP	62	Who has 192.168.32.1? Tell 192.168.32.101
37	3.284916582	PcsCompu_e8:14:fd		ARP	62	Who has 192.168.32.1? Tell 192.168.32.101

Cattura dei pacchetti su Kali con Whireshark

Con servizio https attivo su InetSim

*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	PcsCompu_e8:14:fd		ARP	62	Who has 192.168.32.100? Tell 192.168.32.101
2	0.000012603	PcsCompu_1d:2b:27		ARP	44	192.168.32.100 is at 08:00:27:1d:2b:27
3	0.000205415	192.168.32.101	192.168.32.100	TCP	68	59536 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
4	0.000225457	192.168.32.100	192.168.32.101	TCP	68	80 → 59536 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
5	0.000376989	192.168.32.101	192.168.32.100	TCP	62	59536 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
6	0.000584035	192.168.32.101	192.168.32.100	HTTP	311	GET / HTTP/1.1
7	0.000591024	192.168.32.100	192.168.32.101	TCP	56	80 → 59536 [ACK] Seq=1 Ack=256 Win=64128 Len=0
8	0.012616724	192.168.32.100	192.168.32.101	TCP	206	80 → 59536 [PSH, ACK] Seq=1 Ack=256 Win=64128 Len=150 [TCP segment of data
9	0.012844494	192.168.32.101	192.168.32.100	TCP	62	59536 → 80 [ACK] Seq=256 Ack=151 Win=65536 Len=0
10	0.012857837	192.168.32.100	192.168.32.101	HTTP	314	HTTP/1.1 200 OK (text/html)
11	0.012968439	192.168.32.101	192.168.32.100	TCP	62	59536 → 80 [ACK] Seq=256 Ack=409 Win=65280 Len=0
12	0.014168097	192.168.32.100	192.168.32.101	TCP	56	80 → 59536 [FIN, ACK] Seq=409 Ack=256 Win=64128 Len=0
13	0.014248007	192.168.32.101	192.168.32.100	TCP	62	59536 → 80 [FIN, ACK] Seq=256 Ack=409 Win=65280 Len=0
14	0.014257914	192.168.32.100	192.168.32.101	TCP	56	80 → 59536 [ACK] Seq=410 Ack=257 Win=64128 Len=0
15	0.014303218	192.168.32.101	192.168.32.100	TCP	62	59536 → 80 [ACK] Seq=257 Ack=410 Win=65280 Len=0
16	5.229065395	PcsCompu_1d:2b:27		ARP	44	Who has 192.168.32.101? Tell 192.168.32.100
17	5.229387658	PcsCompu_e8:14:fd		ARP	62	192.168.32.101 is at 08:00:27:e8:14:fd

Cattura dei pacchetti su Kali con Whireshark

Con servizio http attivo su InetSim

(dopo aver modificato InetSim e riavviato la simulazione)

Wireshark · Packet 3 · any

- ▶ Frame 3: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface
- ▼ Linux cooked capture v1
 - Packet type: Unicast to us (0)
 - Link-layer address type: Ethernet (1)
 - Link-layer address length: 6
 - Source: PcsCompu_e8:14:fd (08:00:27:e8:14:fd)
 - Unused: 0000
 - Protocol: IPv4 (0x0800)
- ▼ Internet Protocol Version 4, Src: 192.168.32.101, Dst: 192.168.32.100
 - 0100 = Version: 4
 - 0101 = Header Length: 20 bytes (5)
 - ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

0000	00 00 00 01 00 06	08 00 27 e8 14 fd	00 00 08 00 '...' ..
0010	45 00 00 34 06 ec	40 00 80 06 31 be	c0 a8 20 65	E..4..@..1.. e
0020	c0 a8 20 64 e8 a0	01 bb ff 38 07 53	00 00 00 00	.. d.... 8.S...
0030	80 02 20 00 9c 0e	00 00 02 04 05 b4	01 03 03 08
0040	01 01 04 02		

✓ Show packet bytes

MAC Windows 7

Wireshark · Packet 4 · any

- ▶ Frame 4: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface
- ▼ Linux cooked capture v1
 - Packet type: Sent by us (4)
 - Link-layer address type: Ethernet (1)
 - Link-layer address length: 6
 - Source: PcsCompu_1d:2b:27 (08:00:27:1d:2b:27)
 - Unused: 0000
 - Protocol: IPv4 (0x0800)
- ▼ Internet Protocol Version 4, Src: 192.168.32.100, Dst: 192.168.32.101
 - 0100 = Version: 4
 - 0101 = Header Length: 20 bytes (5)
 - ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

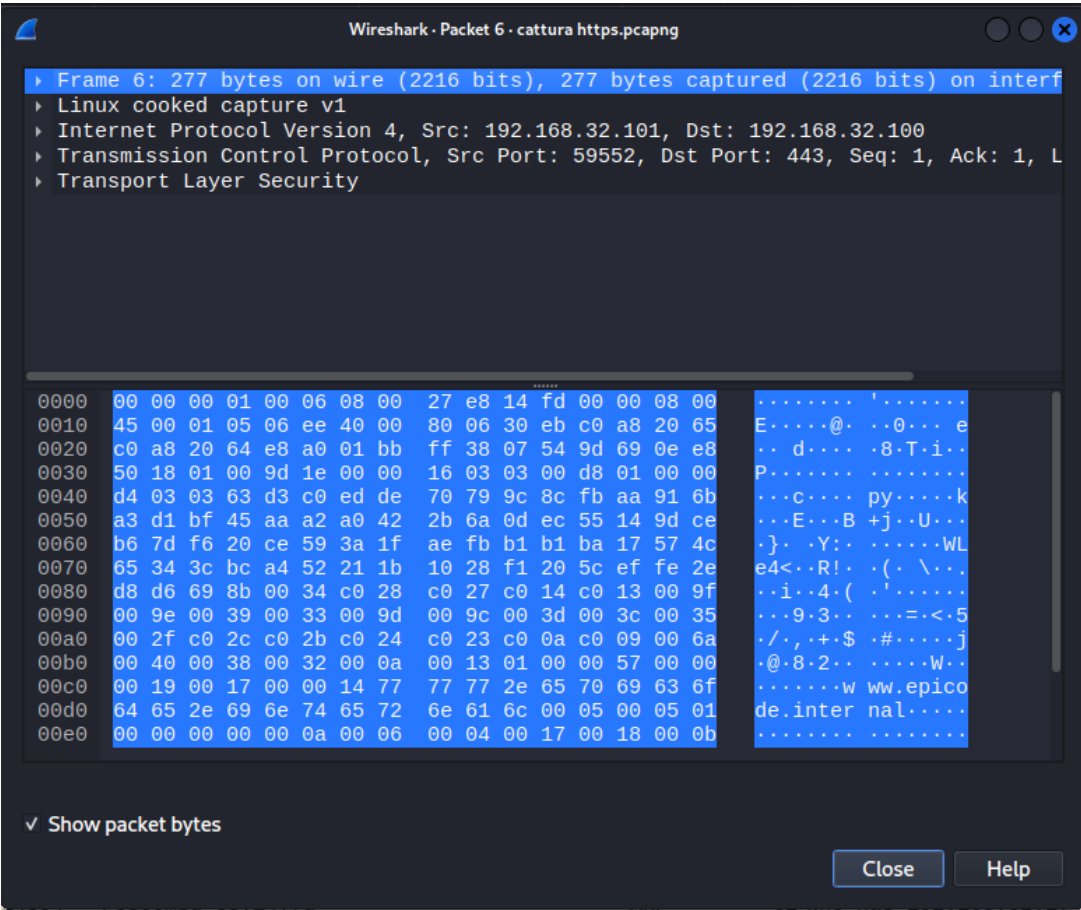
0000	00 04 00 01 00 06	08 00 27 1d 2b 27	00 00 08 00 '++' ..
0010	45 00 00 34 00 00	40 00 40 06 78 aa	c0 a8 20 64	E..4..@..@.x.. d
0020	c0 a8 20 65 01 bb	e8 a0 9d 69 0e e7	ff 38 07 54	.. e.... i...8.T
0030	80 12 fa f0 c2 40	00 00 02 04 05 b4	01 01 04 02@..
0040	01 03 03 07		

No.: 4 · Time: 0.000174050 · Source: 192.168.32.100 · Destin..., ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128

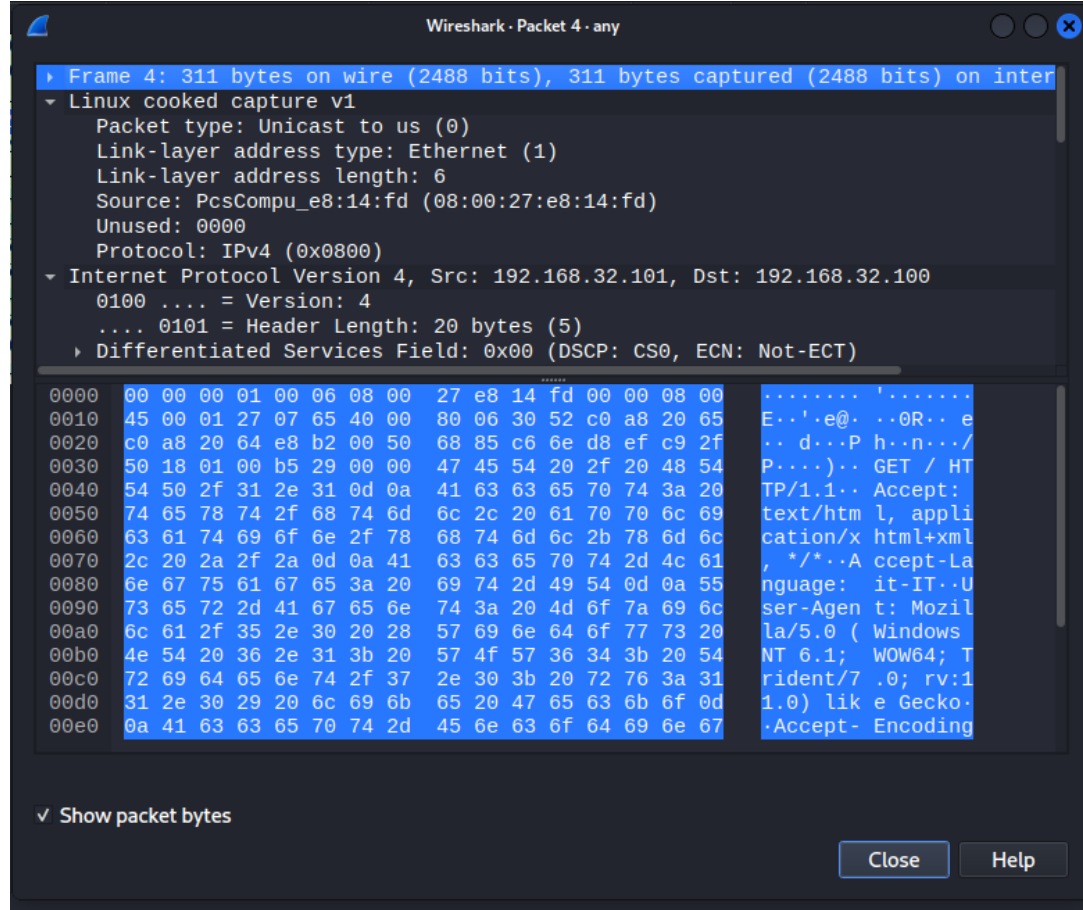
✓ Show packet bytes

Close Help

MAC Kali Linux



Pacchetto cifratura dal protocollo di sicurezza di https



Pacchetto protocollo http

Pacchetto cifrato dal protocollo di sicurezza di https

Col protocollo http il contenuto del pacchetto rimane in chiaro, leggibile da Whireshark.

Questa oltre alla differenza di porte dedicate (443 per https e 80 per http), è la differenza più grande tra i due.