

Prima consegna

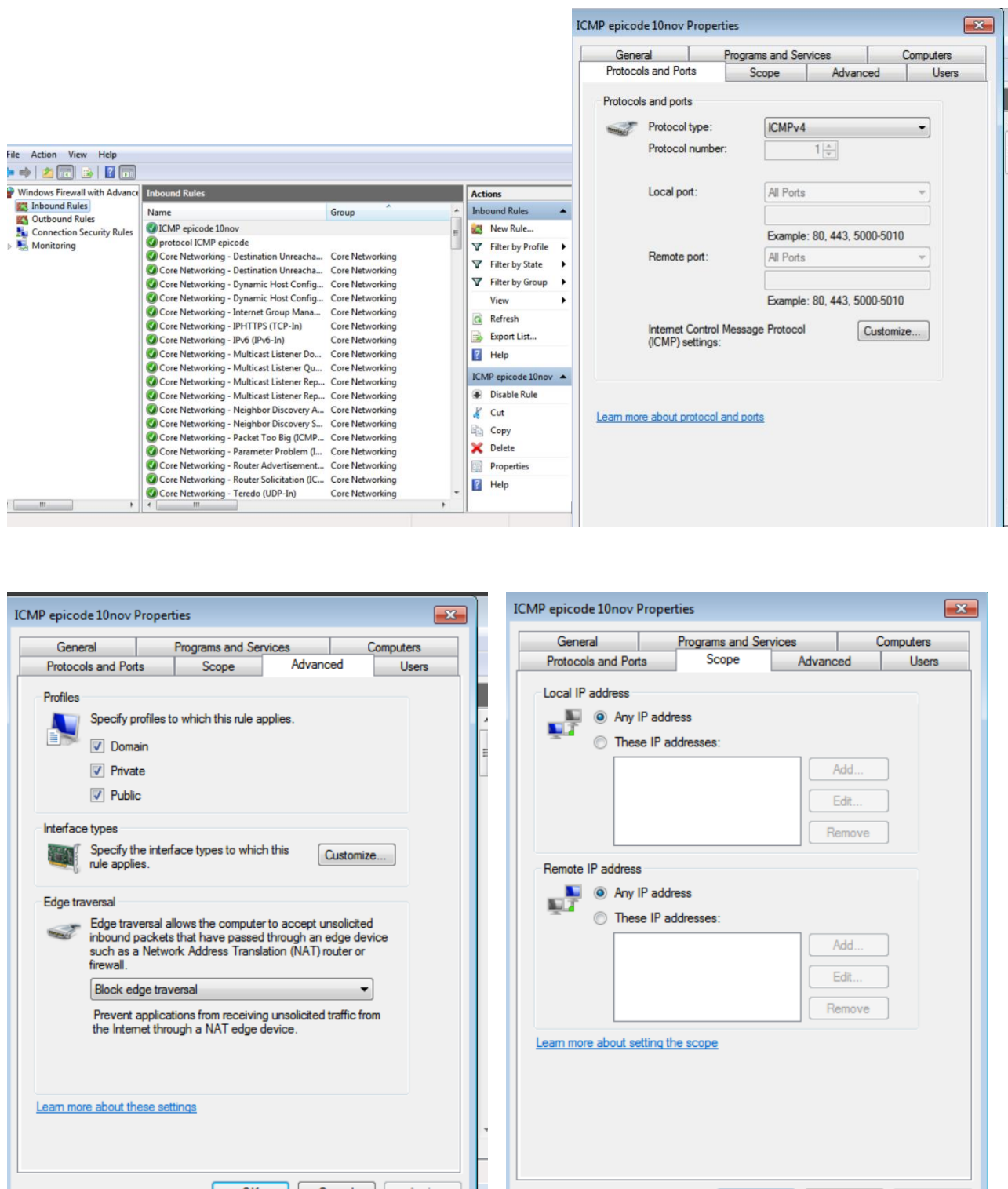
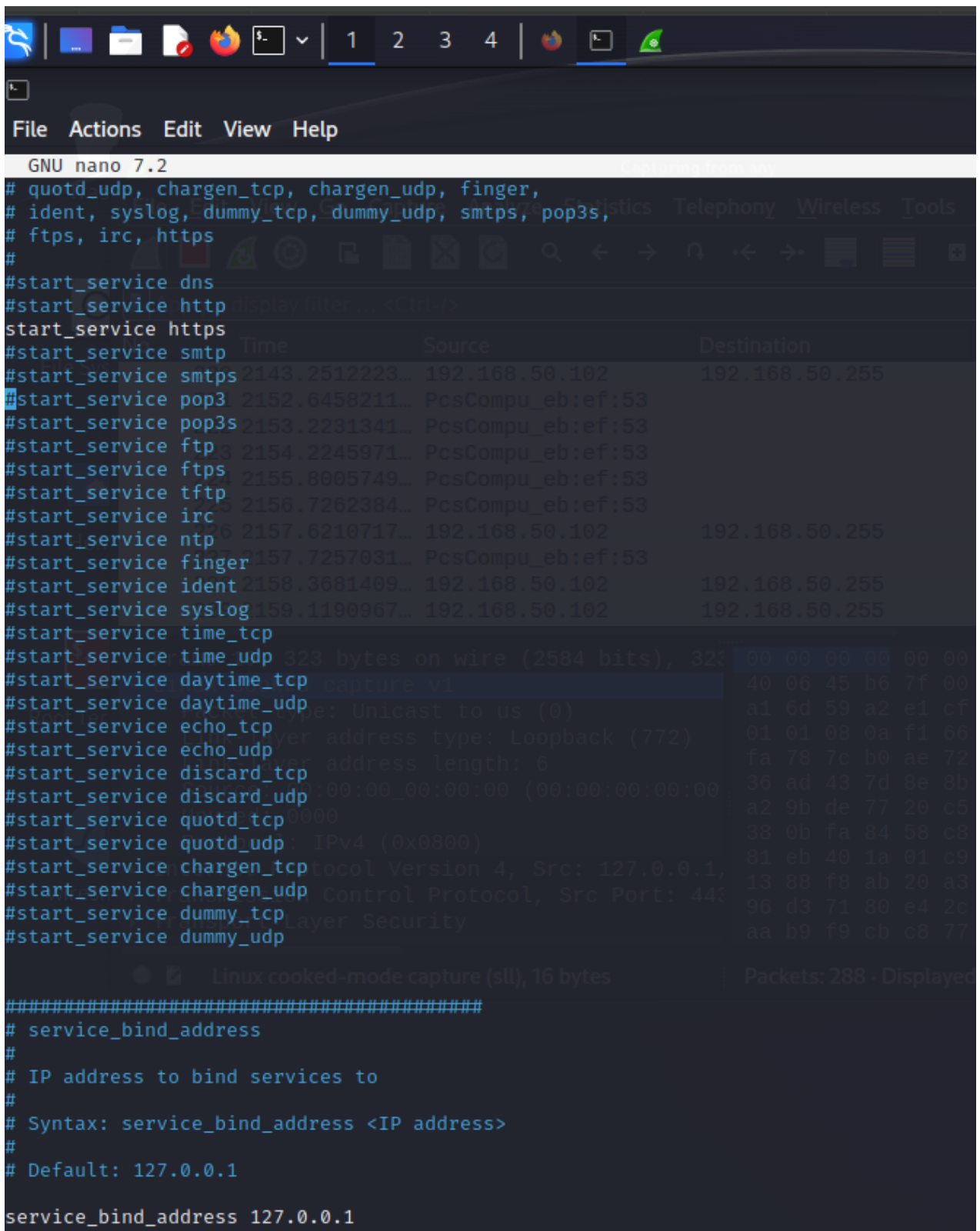


Figura 1: configurazione policy ICMP nel firewall di Windows 7.

Seconda consegna



```
File Actions Edit View Help
GNU nano 7.2
# 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
#start_service smtps
#start_service pop3
#start_service pop3s
#start_service ftp
#start_service ftps
#start_service tftp
#start_service irc
#start_service ntp
#start_service finger
#start_service ident
#start_service syslog
#start_service time_tcp
#start_service time_udp
#start_service daytime_tcp
#start_service daytime_udp
#start_service echo_tcp
#start_service echo_udp
#start_service discard_tcp
#start_service discard_udp
#start_service quotd_tcp
#start_service quotd_udp
#start_service chargen_tcp
#start_service chargen_udp
#start_service dummy_tcp
#start_service dummy_udp

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

service_bind_address 127.0.0.1
```

Figura 2: configurazione INetSim su Kali Linux.

```

File Actions Edit View Help
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 11060) ==
Session ID: 11060
Listening on: 127.0.0.1
Real Date/Time: 2023-11-11 02:36:31
Fake Date/Time: 2023-11-11 02:36:31 (Delta: 0 seconds)
Forking services...
* https_443_tcp - started (PID 11062)
done.
Simulation running.
^C * https_443_tcp - stopped (PID 11062)
* https_443_tcp - stopped (PID 11062)
Simulation stopped.
Report written to '/var/log/inetsim/report/report.11060.txt' (30 lines)
== INetSim main process stopped (PID 11060) ==

(kali@kali)-[/etc/inetsim]
$ sudo nano inetsim.conf
[sudo] password for kali:
(kali@kali)-[/etc/inetsim]
$ 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 47893) ==
Session ID: 47893
Listening on: 127.0.0.1
Real Date/Time: 2023-11-11 03:54:58
Fake Date/Time: 2023-11-11 03:54:58 (Delta: 0 seconds)
Forking services...
* https_443_tcp - started (PID 47903)
done.
Simulation running.

```

Figura 3: avvio simulazione INetSim su Kali Linux.

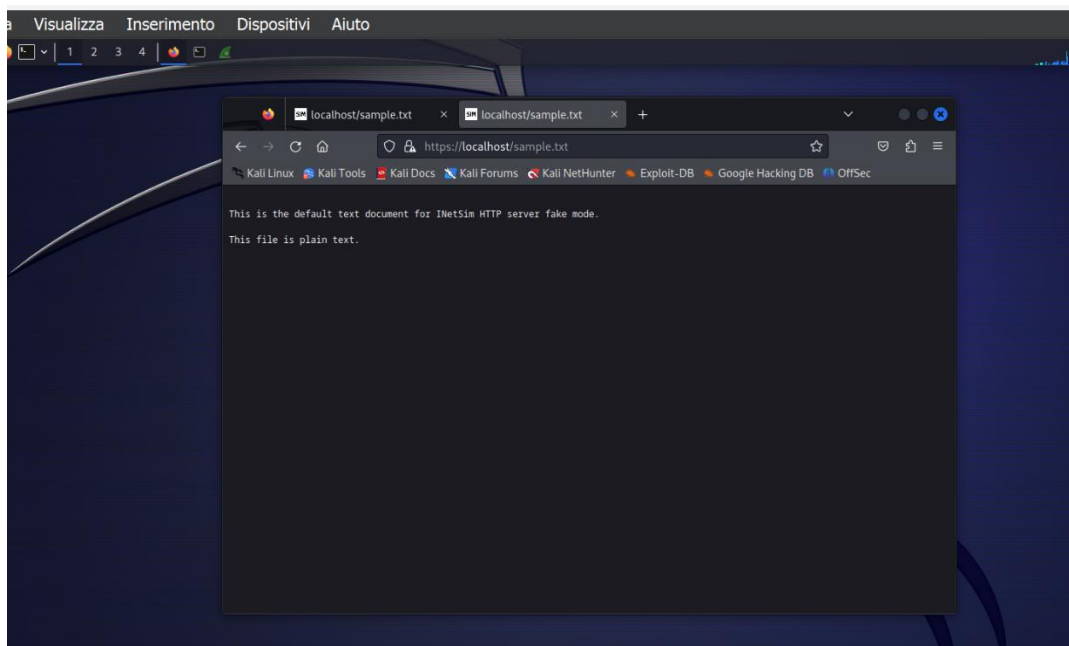


Figura 4: emulazione servizi internet su Kali Linux.

Terza consegna

Protocolli https

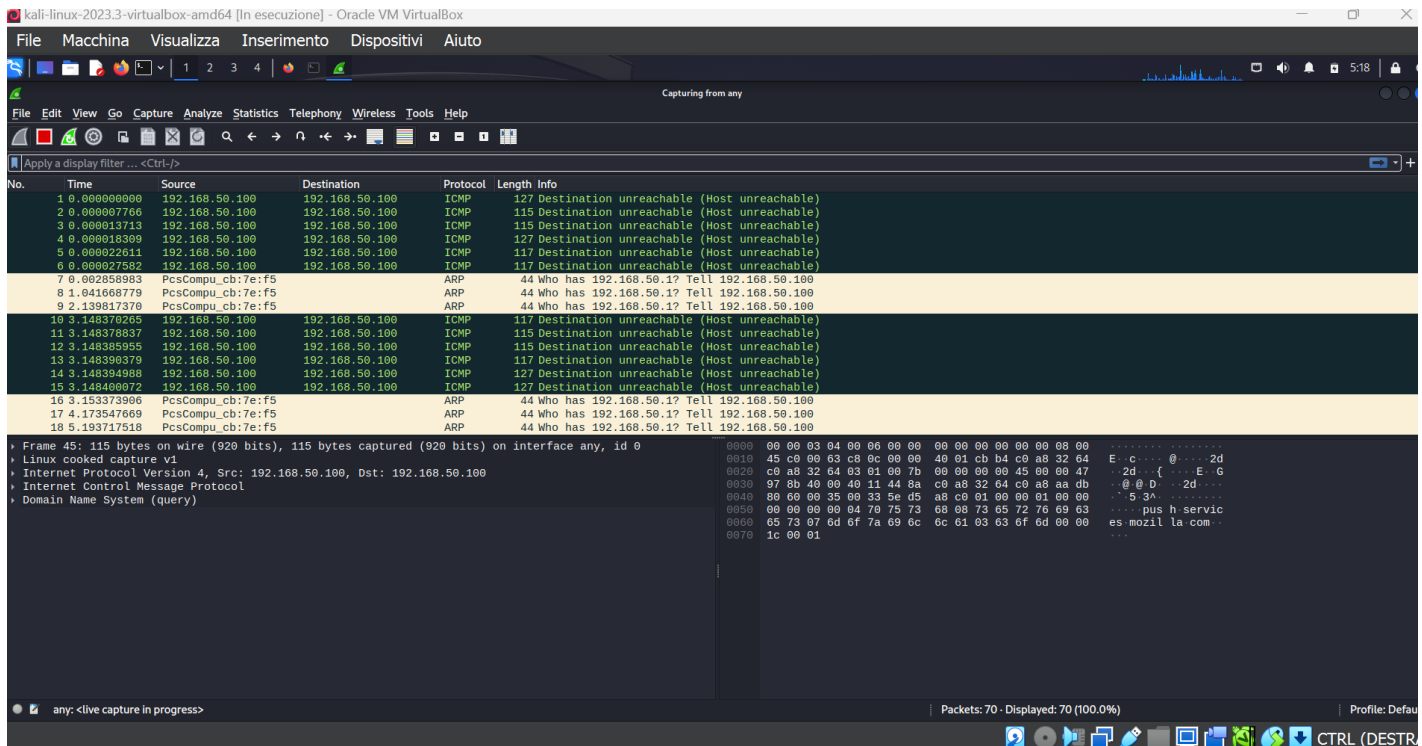


Figura 5: Cattura pacchetti su Wireshark in https, utilizzando la porta "Any".

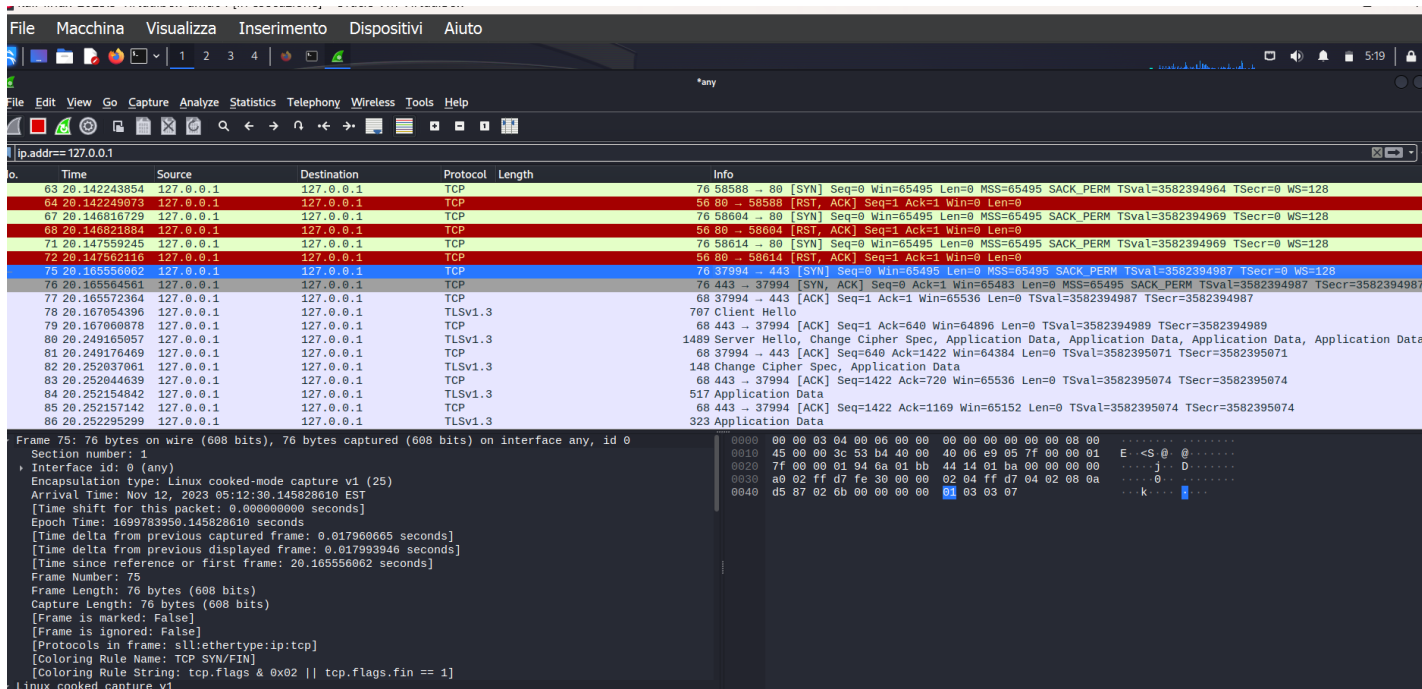


Figura 6: scambio di pacchetti con three-hand-shake in https dopo aver applicato il filtro "ip.addr == 127.0.0.1".

Protocolli http

The image shows a Wireshark packet capture of an HTTP connection. The filter applied is `ip.addr == 127.0.0.1`. The packet list shows several ICMP 'Destination unreachable' messages and a successful TCP SYN exchange. The selected packet (No. 343) is a TCP segment from 127.0.0.1:45568 to 127.0.0.1:80, Seq=0, Win=0, Len=0. The packet details pane shows the following information:

- [Header checksum status: Unverified]
- Source Address: 127.0.0.1
- Destination Address: 127.0.0.1
- Transmission Control Protocol, Src Port: 45568, Dst Port: 80, Seq: 0, Len: 0
- Source Port: 45568
- Destination Port: 80
- [Stream index: 2]
- [Conversation completeness: Incomplete (37)]
- [TCP Segment Len: 0]
- Sequence Number: 0 (relative sequence number)
- Sequence Number (raw): 320710256
- [Next Sequence Number: 1 (relative sequence number)]
- Acknowledgment Number: 0
- Acknowledgment number (raw): 0
- 1010 = Header Length: 40 bytes (10)
- Flags: 0x002 (SYN)
- Window: 65495
- [calculated window size: 65495]
- Checksum: 0xfe30 [unverified]

The packet bytes pane shows the raw data of the SYN packet, with the flag byte highlighted in blue.

Figura 7: scambio di pacchetti in http dopo aver applicato il filtro "ip.addr == 127.0.0.1".