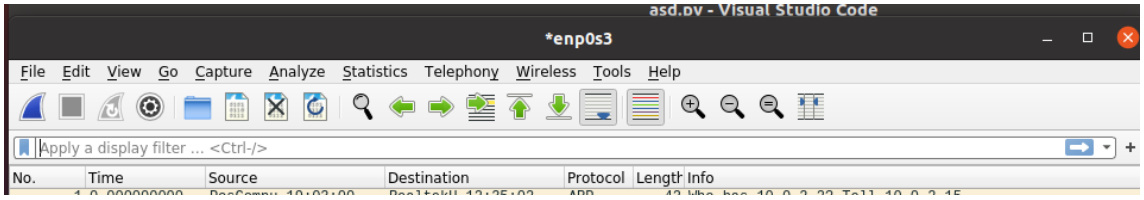
1 Ponemos el código en Python que necesitamos.

```
home > a > asd.py > ...
  1  import socket
  2
  3  s = socket.socket(socket.AF_INET, socket.SOCK_RAW, socket.IPPROTO_TCP)
  4  s.setsockopt(socket.IPPROTO_IP, socket.IP_HDRINCL, 1)
  5
  6  ip_header = b'\x45\x00\x00\x1c' # Version, IHL, Type of Service | Total Length
  7  ip_header += b'\xab\xcd\x00\x00' # Identification | Flags, Fragment Offset
  8  ip_header += b'\x40\x01\x6b\xd8' # TTL, Protocol | Header Checksum
  9  ip_header += b'\x0A\x00\x02\x0F' # Source Address (10.0.2.15 0A.00.02.0F)
 10  ip_header += b'\x5B\x8E\xD6\xB5' # Destination Address (91.142.214.181 5B.8E.D6.B5)
 11
 12  icmp_header = b'\x08\x00\xe5\xca' # Type of message, Code | Checksum
 13  icmp_header += b'\x12\x34\x00\x01' # Identifier | Sequence Number
 14
 15  packet = ip_header + icmp_header
 16  s.sendto(packet, ('91.142.214.181', 0))
```

Con nuestras IPs de origen y destino.

2 Ponemos a capturar el wireshark y enviamos el paquete con el comando de a continuación

```
sudo: /home/a/asd.py: orden no encontrada
a@a:~$ sudo /bin/python3 /home/a/asd.py
```




3. Filtramos por ICMP y vemos las request y los reply