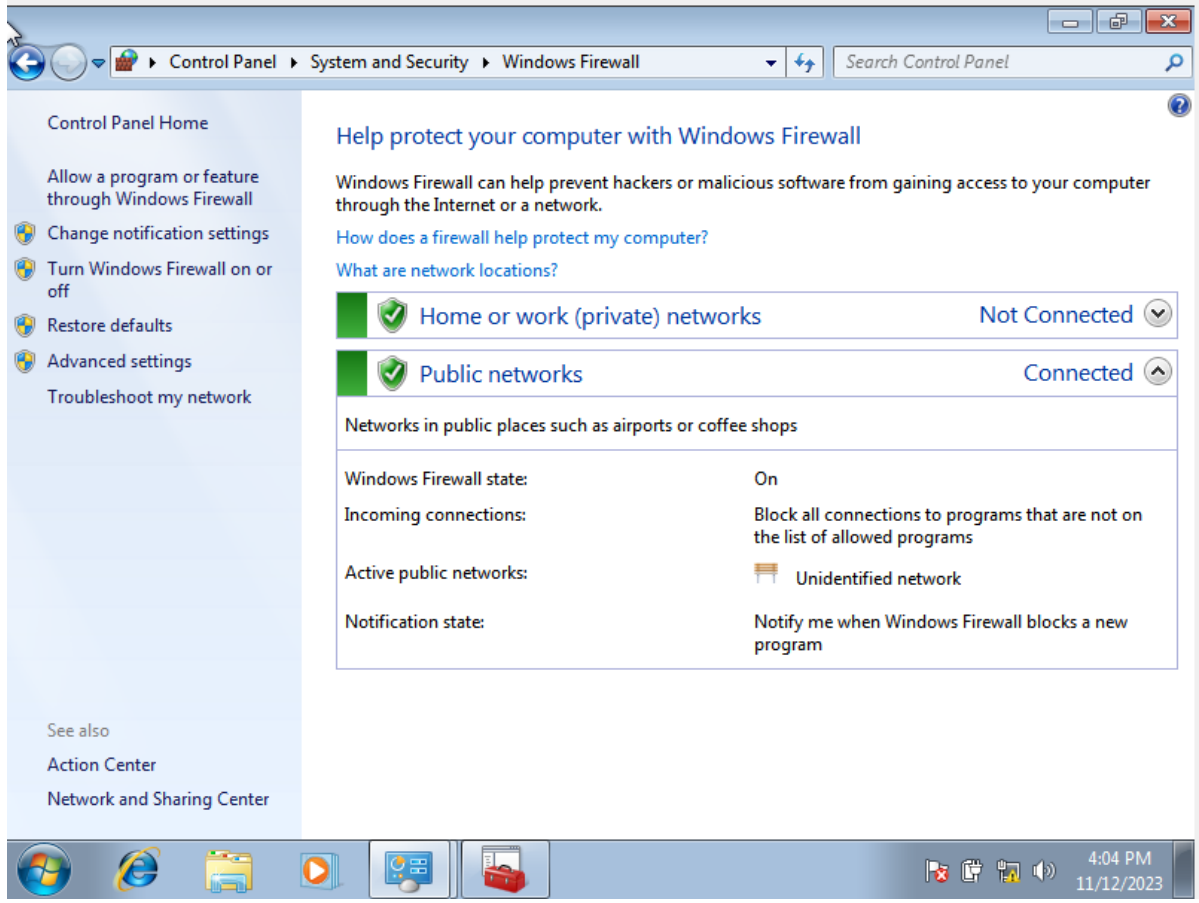
# W3D4

PING VERSO WINDOWS7 , INET E WIRESHARK

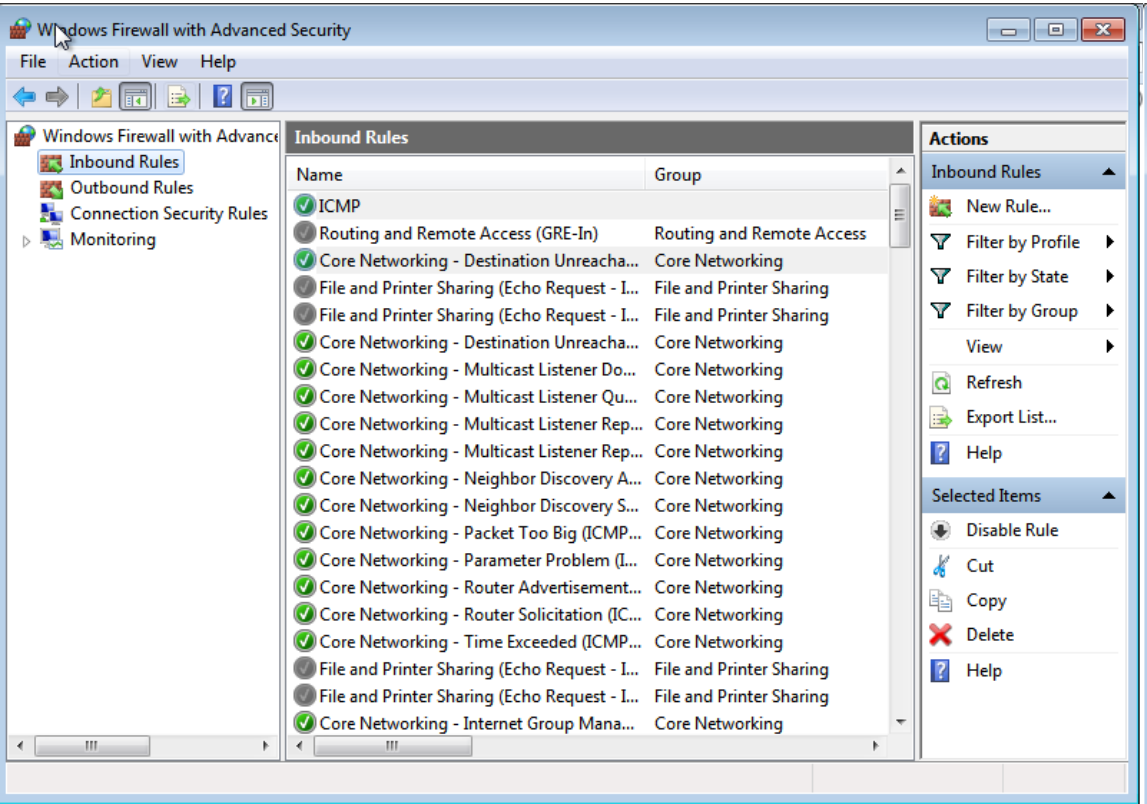
# Ping da VM Linux a Windows 7

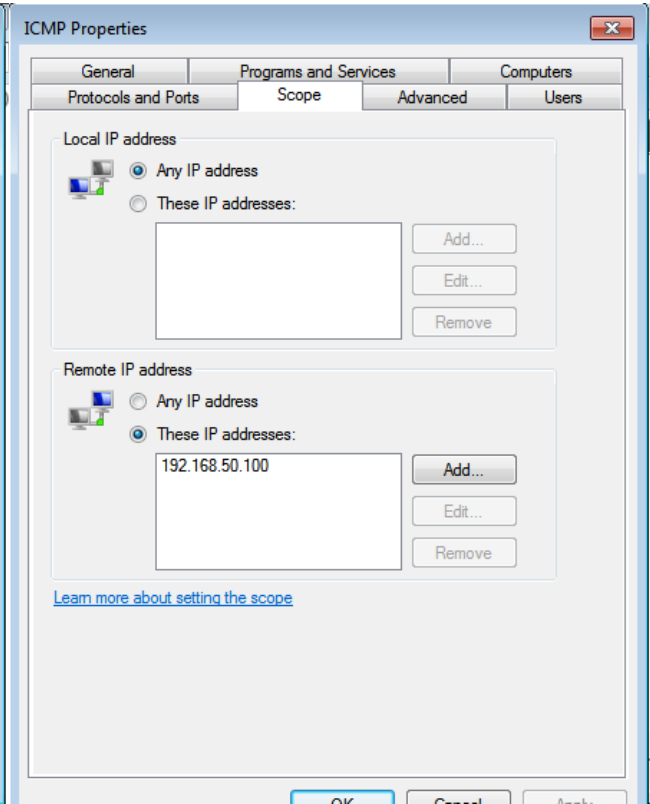
Innanzitutto per effettuare il ping su windows 7 bisogna modificare le policy del firewall che al momento non permettono di ricevere pacchetti col protocollo ICMP (che permette di realizzare l'operazione di ping), per cui andremo a creare una nuova regola in «advanced settings»

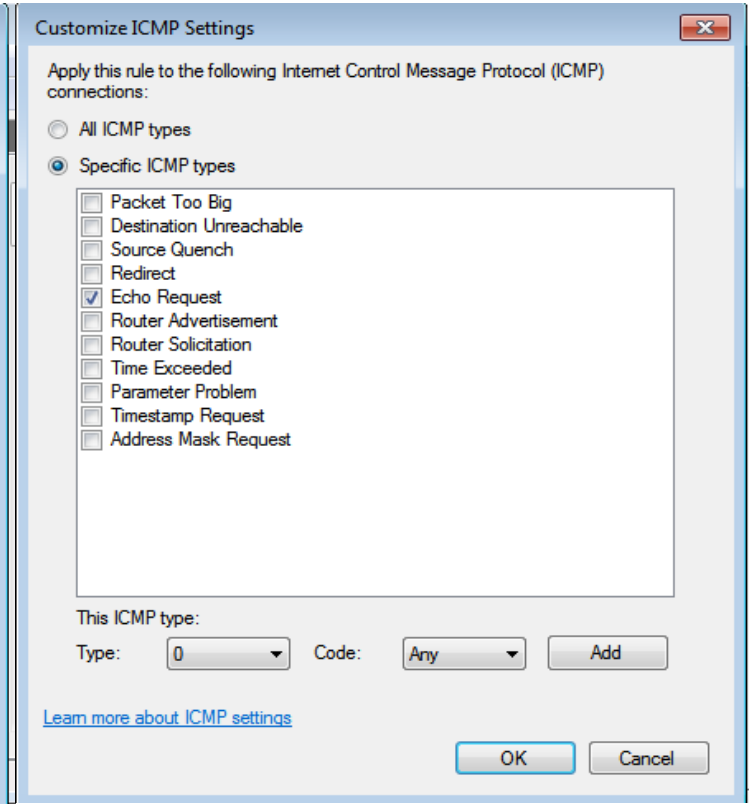


# Ping da VM Linux a Windows 7

La nuova regola è stata creata per poter ricevere il traffico entrante tramite un ping, specificando l'indirizzo da cui proviene.



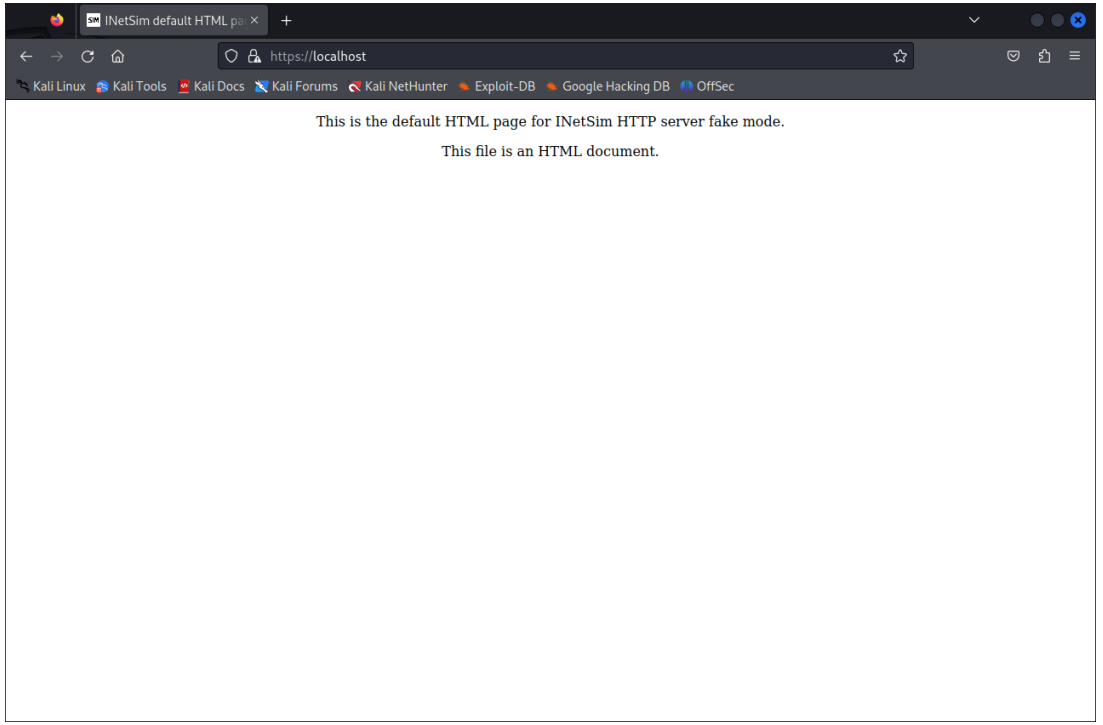



# Utilizzo InetSim ed emulazione servizi internet

Dopo aver abilitato sul file di configurazione di Inet i soli servizi che funzionano tramite protocolli http e https e dopo aver impostato il bind tra il con l'indirizzo di loopback…

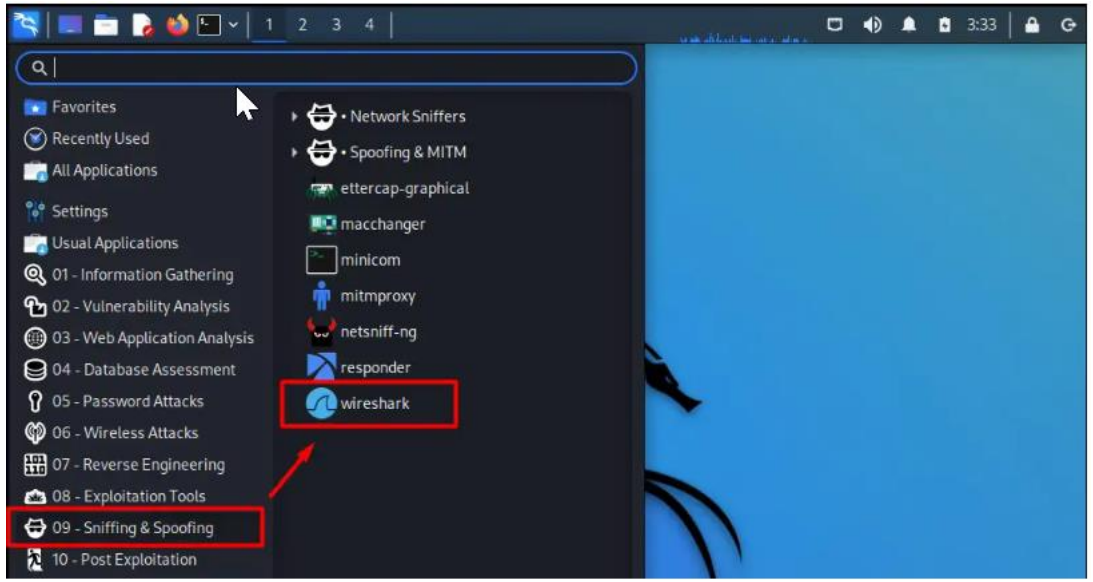
```
┌──(kali㉿kali)-[~]
└─$ sudo inetsim
[sudo] password for kali:
INetSim 1.3.2 (2020-05-19) by Matthias Eckert & Thomas Hungenberg
Using log directory:      /var/log/inetsim/
Using data directory:     /var/lib/inetsim/
Using report directory:   /var/log/inetsim/report/
Using configuration file: /etc/inetsim/inetsim.conf
Parsing configuration file.
Configuration file parsed successfully.
=== INetSim main process started (PID 114758) ===
Session ID:     114758
Listening on:   127.0.0.1
Real Date/Time: 2023-11-12 15:08:42
Fake Date/Time: 2023-11-12 15:08:42 (Delta: 0 seconds)
 Forking services...
  * https_443_tcp - started (PID 114761)
  * http_80_tcp - started (PID 114760)
 done.
Simulation running.
```

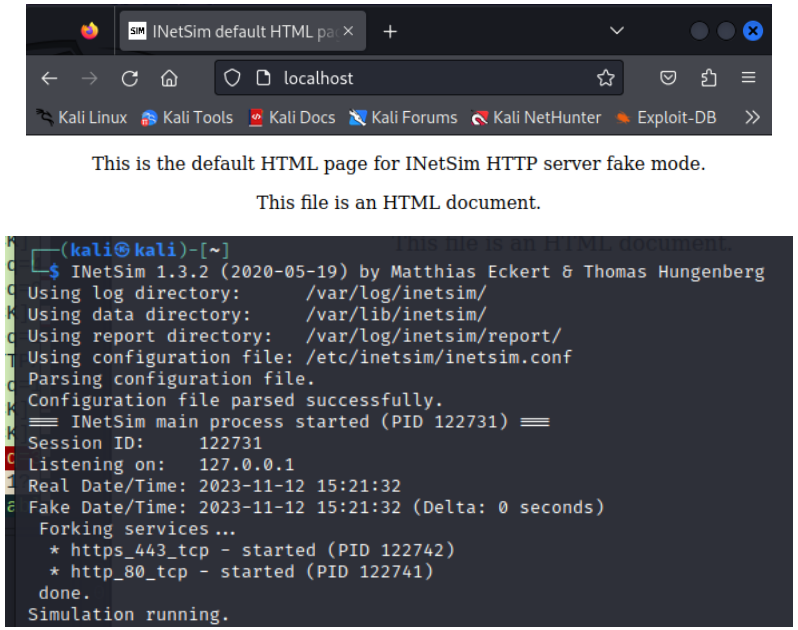


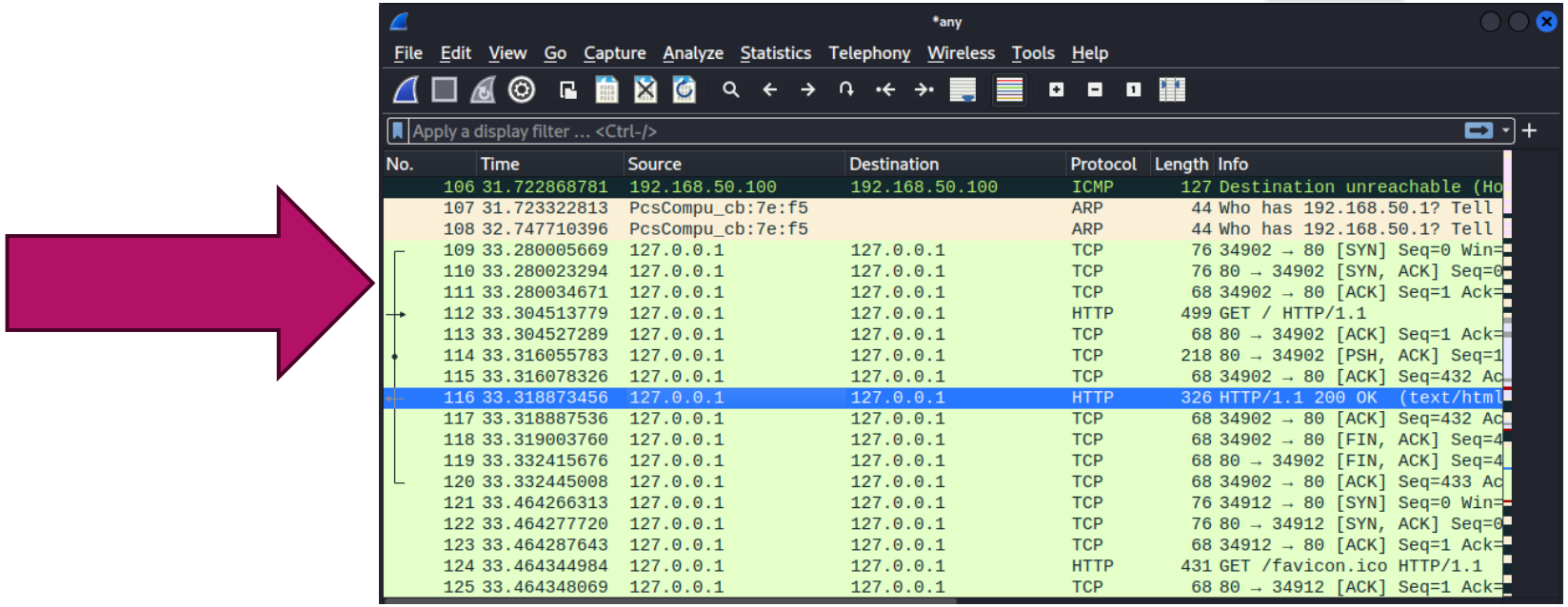

…verifico se effettuando da browser una richiesta HTTPS sul localhost e se mi restituisce il file di impostato di default.

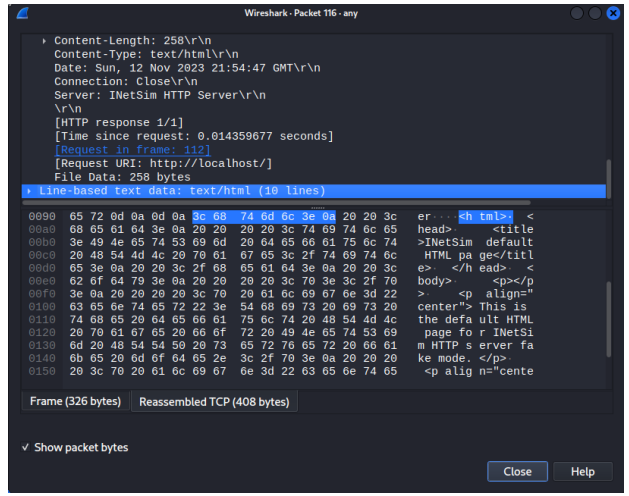
# Cattura pacchetti con wireshark

**Con wireshark posso vedere il traffico di pacchetti che passano per una scheda di rete o un'intera rete se sono in modalità promiscua. Qui di seguito le sezioni di traffico relative alle richieste di file tramite protocollo http e https(fatte come nell'esempio precedente col browser), e quelle invece dedicate al Ping verso la macchina di windows 7.**



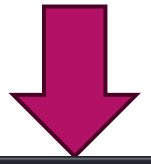



In questo caso essendo il protocollo http non criptato ho anche la possibilità di vedere il contenuto del pacchetto.
Da notare che prima di ottenere la pagina c'è la parte relativa al three-way-handshake che funziona tramite il protocollo TCP.

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.50.102
PING 192.168.50.102 (192.168.50.102) 56(84) bytes of data.
64 bytes from 192.168.50.102: icmp_seq=1 ttl=128 time=1.45 ms
64 bytes from 192.168.50.102: icmp_seq=2 ttl=128 time=1.20 ms
64 bytes from 192.168.50.102: icmp_seq=3 ttl=128 time=0.889 ms
64 bytes from 192.168.50.102: icmp_seq=4 ttl=128 time=1.15 ms
64 bytes from 192.168.50.102: icmp_seq=5 ttl=128 time=1.17 ms
64 bytes from 192.168.50.102: icmp_seq=6 ttl=128 time=0.694 ms
64 bytes from 192.168.50.102: icmp_seq=7 ttl=128 time=1.78 ms
64 bytes from 192.168.50.102: icmp_seq=8 ttl=128 time=1.38 ms
64 bytes from 192.168.50.102: icmp_seq=9 ttl=128 time=1.30 ms
64 bytes from 192.168.50.102: icmp_seq=10 ttl=128 time=0.606 ms
^C
── 192.168.50.102 ping statistics ──
10 packets transmitted, 10 received, 0% packet loss, time 9026ms
rtt min/avg/max/mdev = 0.606/1.161/1.780/0.337 ms
```



Apply a display filter … <Ctrl-/>

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 1 | 0.000000000 | 192.168.50.100 | 192.168.50.102 | ICMP | 100 | Echo (ping) request id=0x69e4, seq=1/256, ttl=64 (reply in 4) |
| 2 | 0.000889907 | PcsCompu_72:3d:a5 | | ARP | 62 | Who has 192.168.50.100? Tell 192.168.50.102 |
| 3 | 0.000910576 | PcsCompu_cb:7e:f5 | | ARP | 44 | 192.168.50.100 is at 08:00:27:cb:7e:f5 |
| 4 | 0.001424796 | 192.168.50.102 | 192.168.50.100 | ICMP | 100 | Echo (ping) reply id=0x69e4, seq=1/256, ttl=128 (request in 1) |
| 5 | 1.002737199 | 192.168.50.100 | 192.168.50.102 | ICMP | 100 | Echo (ping) request id=0x69e4, seq=2/512, ttl=64 (reply in 6) |
| 6 | 1.003909927 | 192.168.50.102 | 192.168.50.100 | ICMP | 100 | Echo (ping) reply id=0x69e4, seq=2/512, ttl=128 (request in 5) |
| 7 | 2.007616988 | 192.168.50.100 | 192.168.50.102 | ICMP | 100 | Echo (ping) request id=0x69e4, seq=3/768, ttl=64 (reply in 8) |

Questo invece è il traffico generato dal ping, su wireshark constatiamo che ciò viene realizzato tramite il protocollo ICMP , protocollo per cui in precedenza abbiamo creato l'eccezione sul firewall di windows 7.