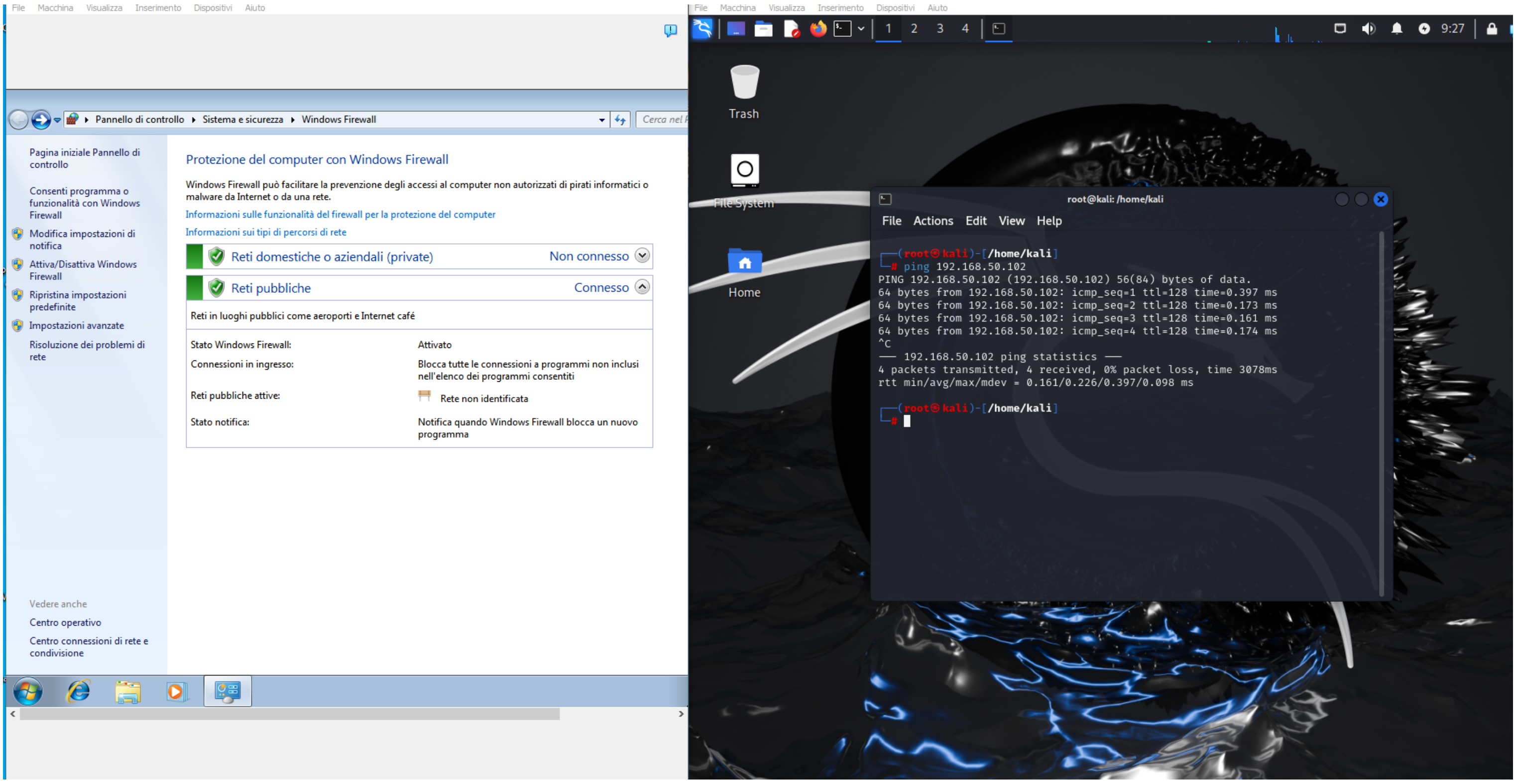
Esercizio Week3 Day 5:

1) Configurare policy per permettere il ping da macchine Linux a Macchina Windows 7 nel nostro laboratorio (Windows firewall)

<u>Procedura in breve: Windows firewall, regole connessioni in entrata, click mouse destro e nuova regola, regola personalizzata avanti, tutti i programmi avanti, selezionare tipo di protocollo "ICMPv4" dal menù a tendina avanti, avanti, avanti, avanti, nome personalizzato e avanti.</u>

Come da screen, Kali riesce a pingare correttamente Windows7 con il Firewall attivo.


File Macchina Visualizza Inserimento Dispositivi Aiuto
Pannello di controllo ▸ Sistema e sicurezza ▸ Windows Firewall
Cerca nel P
Pagina iniziale Pannello di controllo
Consenti programma o funzionalità con Windows Firewall
Modifica impostazioni di notifica
Attiva/Disattiva Windows Firewall
Ripristina impostazioni predefinite
Impostazioni avanzate
Risoluzione dei problemi di rete
Vedere anche
Centro operativo
Centro connessioni di rete e condivisione
Trash
File System
Home
9:27
1 2 3 4
File Actions Edit View Help

Protezione del computer con Windows Firewall

Windows Firewall può facilitare la prevenzione degli accessi al computer non autorizzati di pirati informatici o malware da Internet o da una rete.

Informazioni sulle funzionalità del firewall per la protezione del computer

Informazioni sui tipi di percorsi di rete

Reti domestiche o aziendali (private) — Non connesso

Reti pubbliche — Connesso

Reti in luoghi pubblici come aeroporti e Internet café

Stato Windows Firewall:	Attivato
Connessioni in ingresso:	Blocca tutte le connessioni a programmi non inclusi nell'elenco dei programmi consentiti
Reti pubbliche attive:	Rete non identificata
Stato notifica:	Notifica quando Windows Firewall blocca un nuovo programma

root@kali: /home/kali

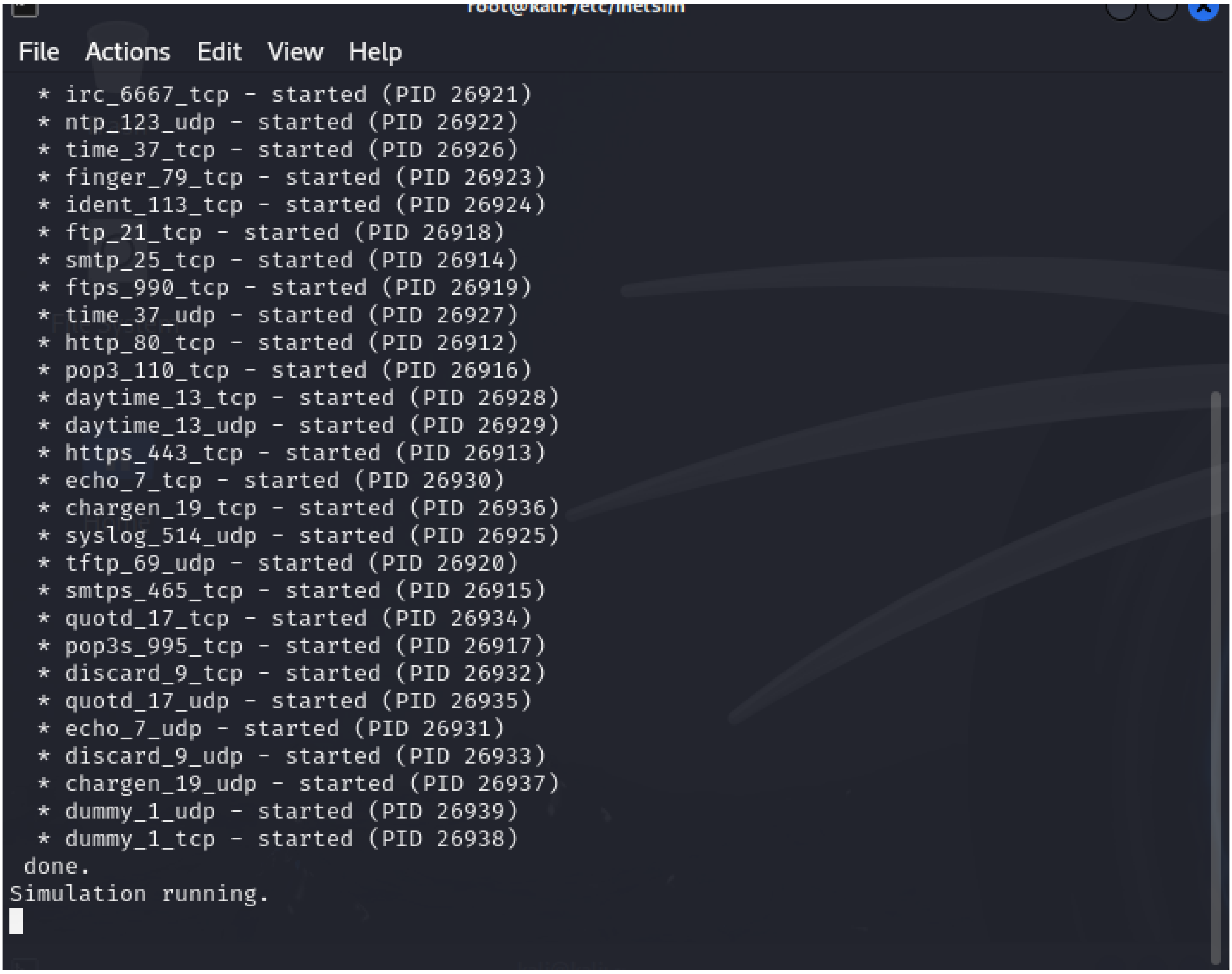
```
┌──(root㉿kali)-[/home/kali]
└─# ping 192.168.50.102
PING 192.168.50.102 (192.168.50.102) 56(84) bytes of data.
64 bytes from 192.168.50.102: icmp_seq=1 ttl=128 time=0.397 ms
64 bytes from 192.168.50.102: icmp_seq=2 ttl=128 time=0.173 ms
64 bytes from 192.168.50.102: icmp_seq=3 ttl=128 time=0.161 ms
64 bytes from 192.168.50.102: icmp_seq=4 ttl=128 time=0.174 ms
^C
── 192.168.50.102 ping statistics ──
4 packets transmitted, 4 received, 0% packet loss, time 3078ms
rtt min/avg/max/mdev = 0.161/0.226/0.397/0.098 ms

┌──(root㉿kali)-[/home/kali]
└─# 
```

2) Utilizzo dell’utility InetSim per l’emulazione di servizi Internet Cattura di pacchetti con Wireshark

Procedura:

Da terminale root (su -, password kali) eseguo il comando *“inetsim --bind-address=127.0.0.1”*

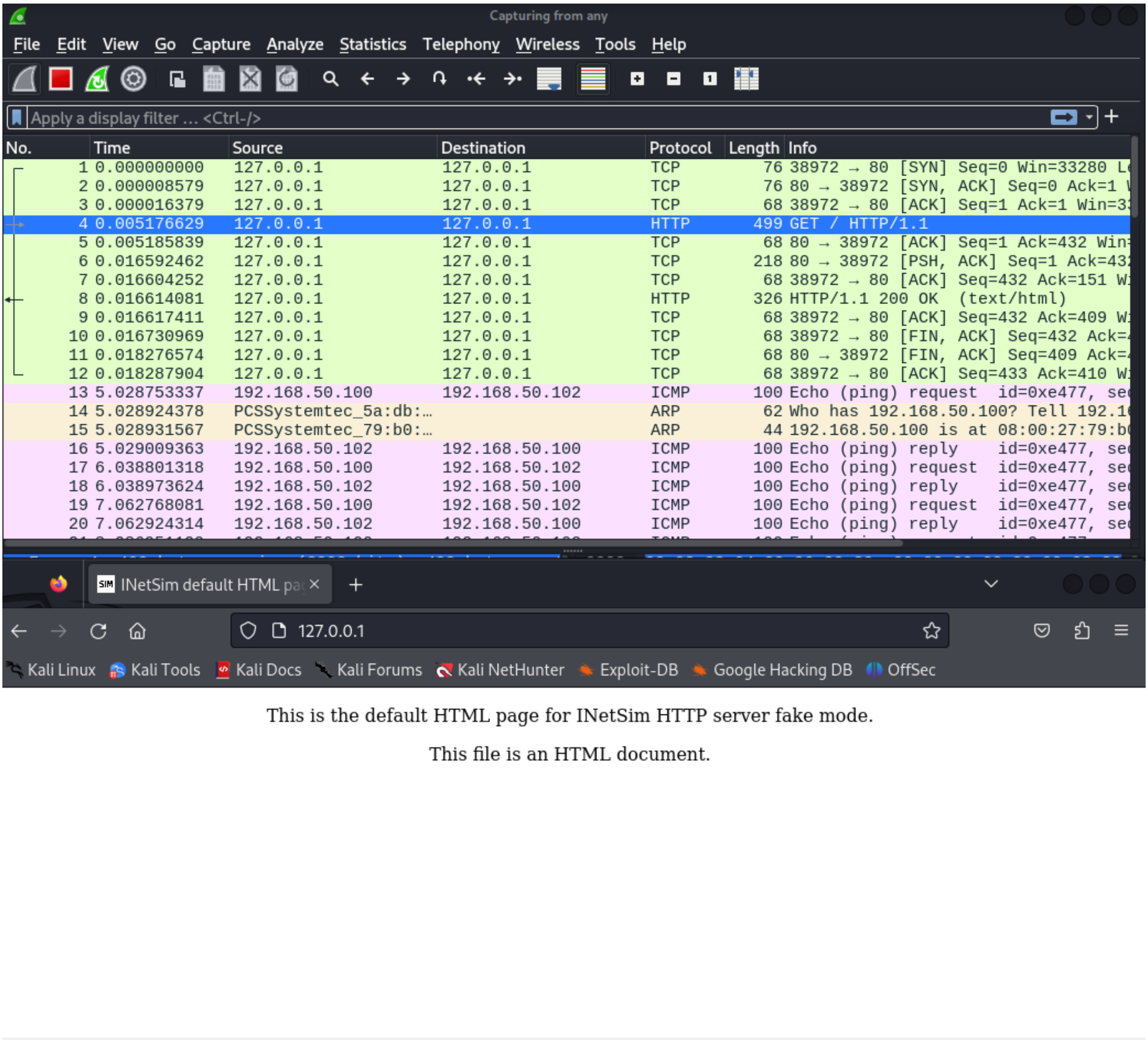
Da terminale root eseguo il comando “*inetsim*”



```
  * irc_6667_tcp - started (PID 26921)
  * ntp_123_udp - started (PID 26922)
  * time_37_tcp - started (PID 26926)
  * finger_79_tcp - started (PID 26923)
  * ident_113_tcp - started (PID 26924)
  * ftp_21_tcp - started (PID 26918)
  * smtp_25_tcp - started (PID 26914)
  * ftps_990_tcp - started (PID 26919)
  * time_37_udp - started (PID 26927)
  * http_80_tcp - started (PID 26912)
  * pop3_110_tcp - started (PID 26916)
  * daytime_13_tcp - started (PID 26928)
  * daytime_13_udp - started (PID 26929)
  * https_443_tcp - started (PID 26913)
  * echo_7_tcp - started (PID 26930)
  * chargen_19_tcp - started (PID 26936)
  * syslog_514_udp - started (PID 26925)
  * tftp_69_udp - started (PID 26920)
  * smtps_465_tcp - started (PID 26915)
  * quotd_17_tcp - started (PID 26934)
  * pop3s_995_tcp - started (PID 26917)
  * discard_9_tcp - started (PID 26932)
  * quotd_17_udp - started (PID 26935)
  * echo_7_udp - started (PID 26931)
  * discard_9_udp - started (PID 26933)
  * chargen_19_udp - started (PID 26937)
  * dummy_1_udp - started (PID 26939)
  * dummy_1_tcp - started (PID 26938)
 done.
Simulation running.
```

Apro Wireshark, seleziono “*Any*” e faccio partire lo sniffing

Apro Firefox e digito 127.0.0.1 mentre inetsim è in esecuzione sul terminale, vedo i movimenti di pacchetti su wireshark, si nota il “SYN / SYN-ACK / ACK” tipico del Three Way Handshake e il GET HTTP.

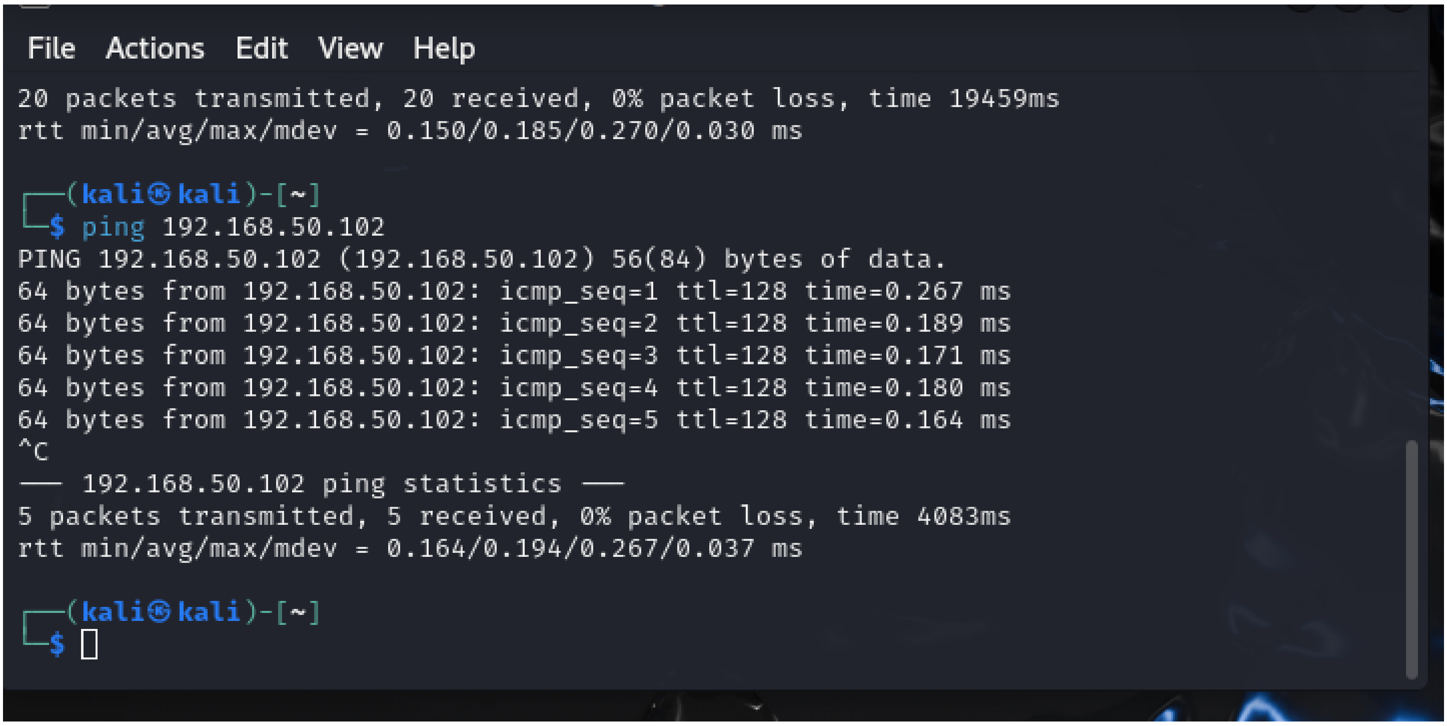


```
No.  Time        Source               Destination      Protocol Length Info
   1 0.000000000 127.0.0.1            127.0.0.1        TCP        76 38972 → 80 [SYN] Seq=0 Win=33280 Le
   2 0.000008579 127.0.0.1            127.0.0.1        TCP        76 80 → 38972 [SYN, ACK] Seq=0 Ack=1 W
   3 0.000016379 127.0.0.1            127.0.0.1        TCP        68 38972 → 80 [ACK] Seq=1 Ack=1 Win=3
   4 0.005176629 127.0.0.1            127.0.0.1        HTTP      499 GET / HTTP/1.1
   5 0.005185839 127.0.0.1            127.0.0.1        TCP        68 80 → 38972 [ACK] Seq=1 Ack=432 Win
   6 0.016592462 127.0.0.1            127.0.0.1        TCP       218 80 → 38972 [PSH, ACK] Seq=1 Ack=43
   7 0.016604252 127.0.0.1            127.0.0.1        TCP        68 38972 → 80 [ACK] Seq=432 Ack=151 Wi
   8 0.016614081 127.0.0.1            127.0.0.1        HTTP      326 HTTP/1.1 200 OK  (text/html)
   9 0.016617411 127.0.0.1            127.0.0.1        TCP        68 38972 → 80 [ACK] Seq=432 Ack=409 Wi
  10 0.016730969 127.0.0.1            127.0.0.1        TCP        68 38972 → 80 [FIN, ACK] Seq=432 Ack=
  11 0.018276574 127.0.0.1            127.0.0.1        TCP        68 80 → 38972 [FIN, ACK] Seq=409 Ack=
  12 0.018287904 127.0.0.1            127.0.0.1        TCP        68 38972 → 80 [ACK] Seq=433 Ack=410 Wi
  13 5.028753337 192.168.50.100       192.168.50.102   ICMP      100 Echo (ping) request  id=0xe477, se
  14 5.028924378 PCSSystemtec_5a:db:…                  ARP        62 Who has 192.168.50.100? Tell 192.1
  15 5.028931567 PCSSystemtec_79:b0:…                  ARP        44 192.168.50.100 is at 08:00:27:79:b
  16 5.029009363 192.168.50.102       192.168.50.100   ICMP      100 Echo (ping) reply    id=0xe477, se
  17 6.038801318 192.168.50.100       192.168.50.102   ICMP      100 Echo (ping) request  id=0xe477, se
  18 6.038973624 192.168.50.102       192.168.50.100   ICMP      100 Echo (ping) reply    id=0xe477, se
  19 7.062768081 192.168.50.100       192.168.50.102   ICMP      100 Echo (ping) request  id=0xe477, se
  20 7.062924314 192.168.50.102       192.168.50.100   ICMP      100 Echo (ping) reply    id=0xe477, se
```

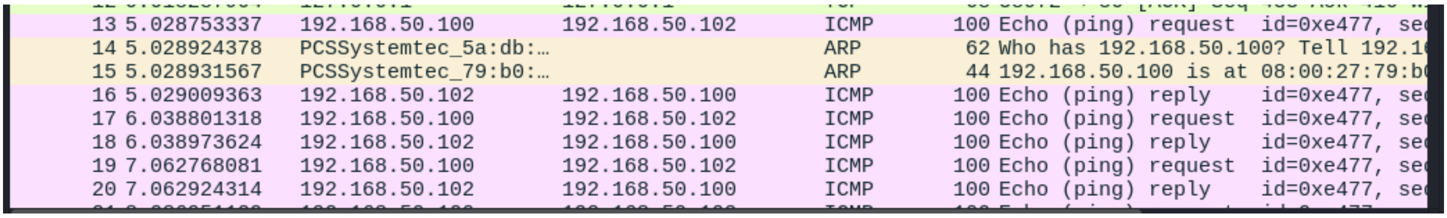
This is the default HTML page for INetSim HTTP server fake mode.

This file is an HTML document.

Per ulteriore prova del funzionamento di Wireshark, pingo la mia WM con Windows7 e noto lo sniffing dei pacchetti di ping (ICMP) in entrata ed uscita



```
20 packets transmitted, 20 received, 0% packet loss, time 19459ms
rtt min/avg/max/mdev = 0.150/0.185/0.270/0.030 ms

┌──(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=0.267 ms
64 bytes from 192.168.50.102: icmp_seq=2 ttl=128 time=0.189 ms
64 bytes from 192.168.50.102: icmp_seq=3 ttl=128 time=0.171 ms
64 bytes from 192.168.50.102: icmp_seq=4 ttl=128 time=0.180 ms
64 bytes from 192.168.50.102: icmp_seq=5 ttl=128 time=0.164 ms
^C
── 192.168.50.102 ping statistics ──
5 packets transmitted, 5 received, 0% packet loss, time 4083ms
rtt min/avg/max/mdev = 0.164/0.194/0.267/0.037 ms

┌──(kali㉿kali)-[~]
└─$ 
```



```
13 5.028753337  192.168.50.100       192.168.50.102   ICMP   100 Echo (ping) request  id=0xe477, se
14 5.028924378  PCSSystemtec_5a:db:…                  ARP     62 Who has 192.168.50.100? Tell 192.1
15 5.028931567  PCSSystemtec_79:b0:…                  ARP     44 192.168.50.100 is at 08:00:27:79:b
16 5.029009363  192.168.50.102       192.168.50.100   ICMP   100 Echo (ping) reply    id=0xe477, se
17 6.038801318  192.168.50.100       192.168.50.102   ICMP   100 Echo (ping) request  id=0xe477, se
18 6.038973624  192.168.50.102       192.168.50.100   ICMP   100 Echo (ping) reply    id=0xe477, se
19 7.062768081  192.168.50.100       192.168.50.102   ICMP   100 Echo (ping) request  id=0xe477, se
20 7.062924314  192.168.50.102       192.168.50.100   ICMP   100 Echo (ping) reply    id=0xe477, se
```