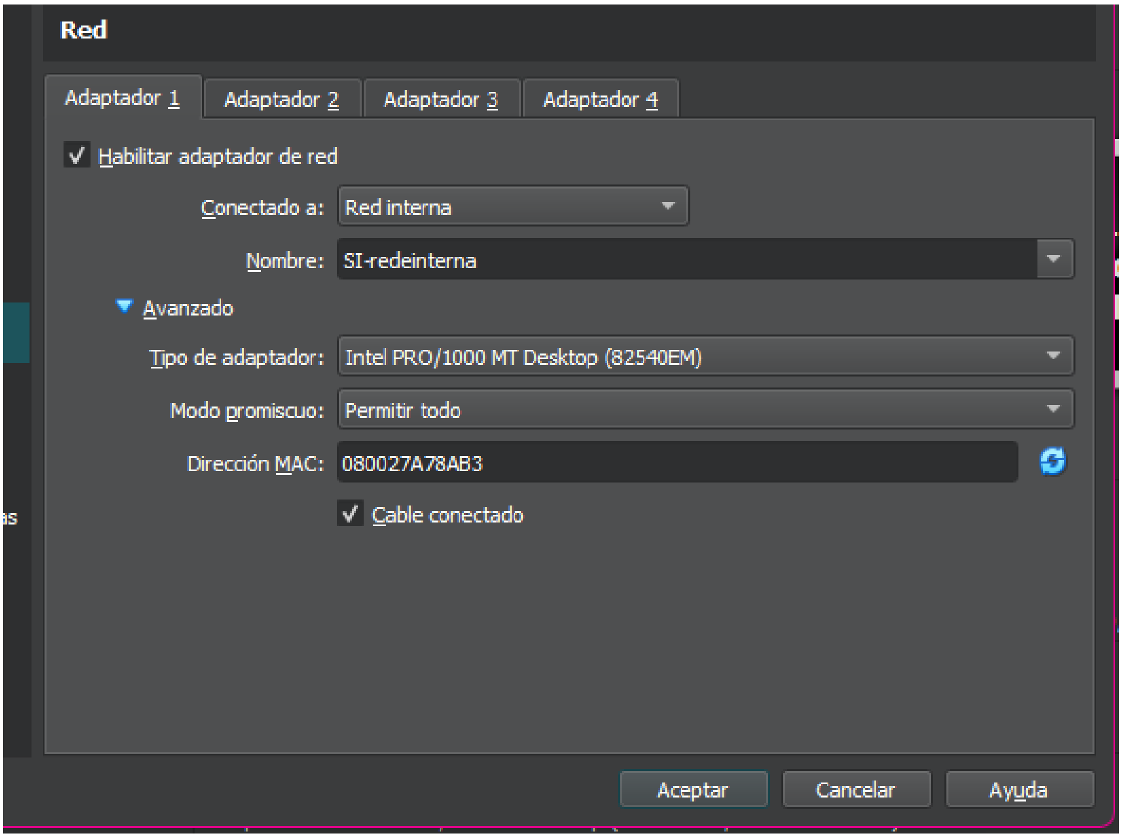
Wireshark

- Instala Wireshark na máquina de W10: https://www.wireshark.org/#download
- Configura o interfaz de rede en modo promíscuo e arráncao.



☑ Habilitar adaptador de red

Conectado a: Red interna

Nombre: SI-redeinterna

Avanzado

Tipo de adaptador: Intel PRO/1000 MT Desktop (82540EM)

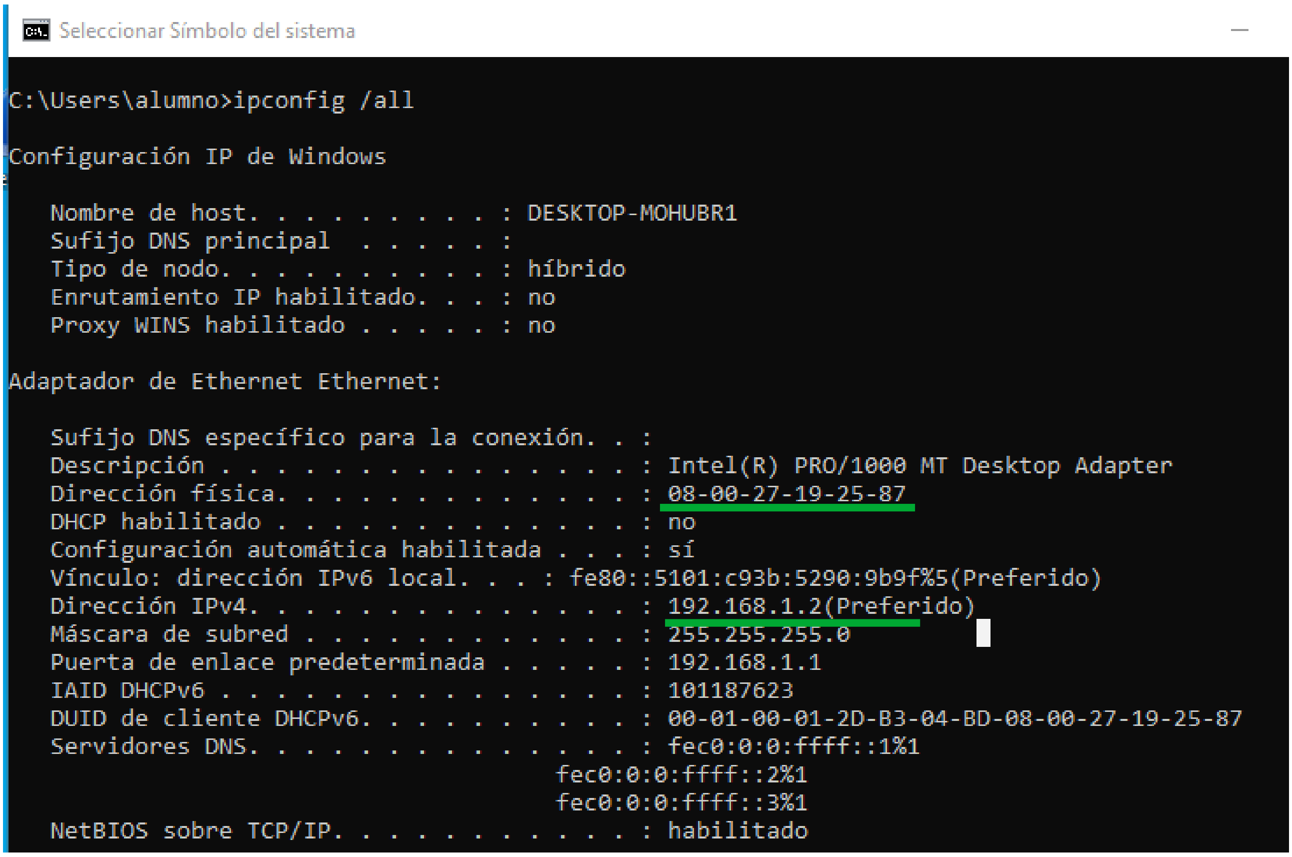
Modo promiscuo: Permitir todo

Dirección MAC: 080027A78AB3

☑ Cable conectado

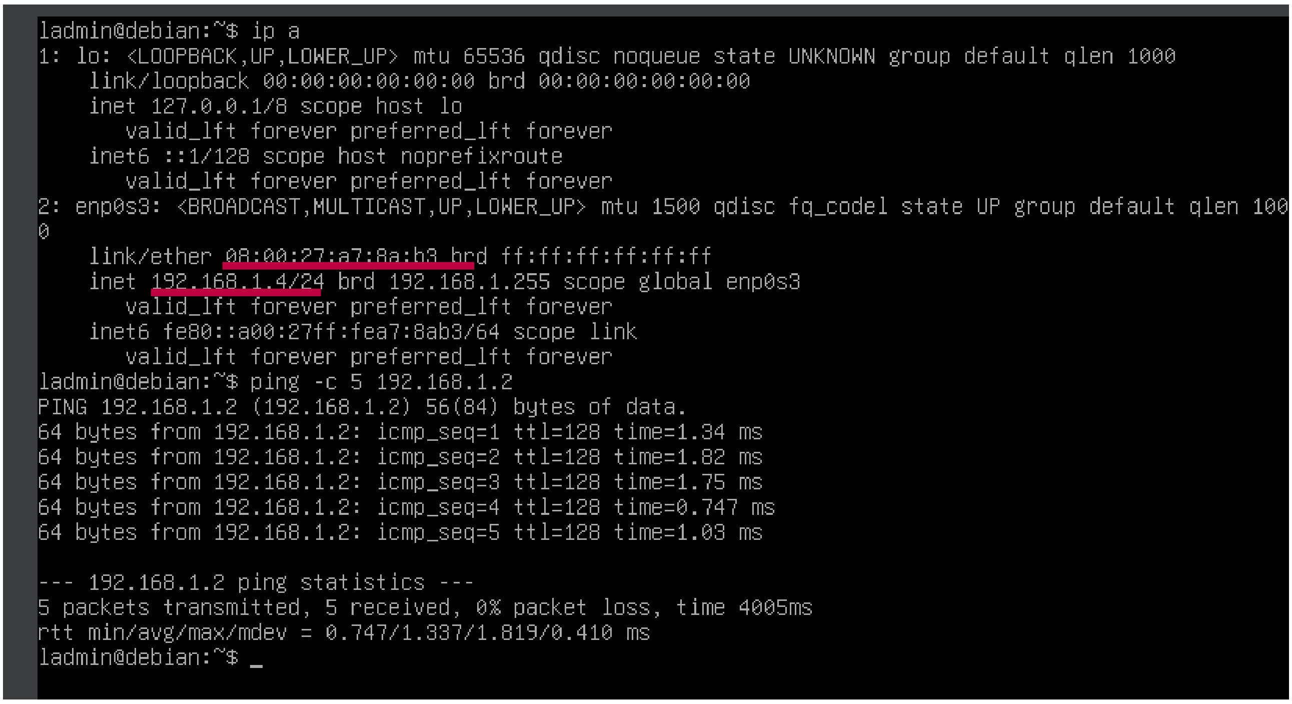
- Executa un ping único dende debian server con destino ao W10. Analiza as peticións ICMP e comproba, mediante capturas, que tanto as MAC como as IP de orixe e destino son correctas.

Windows:

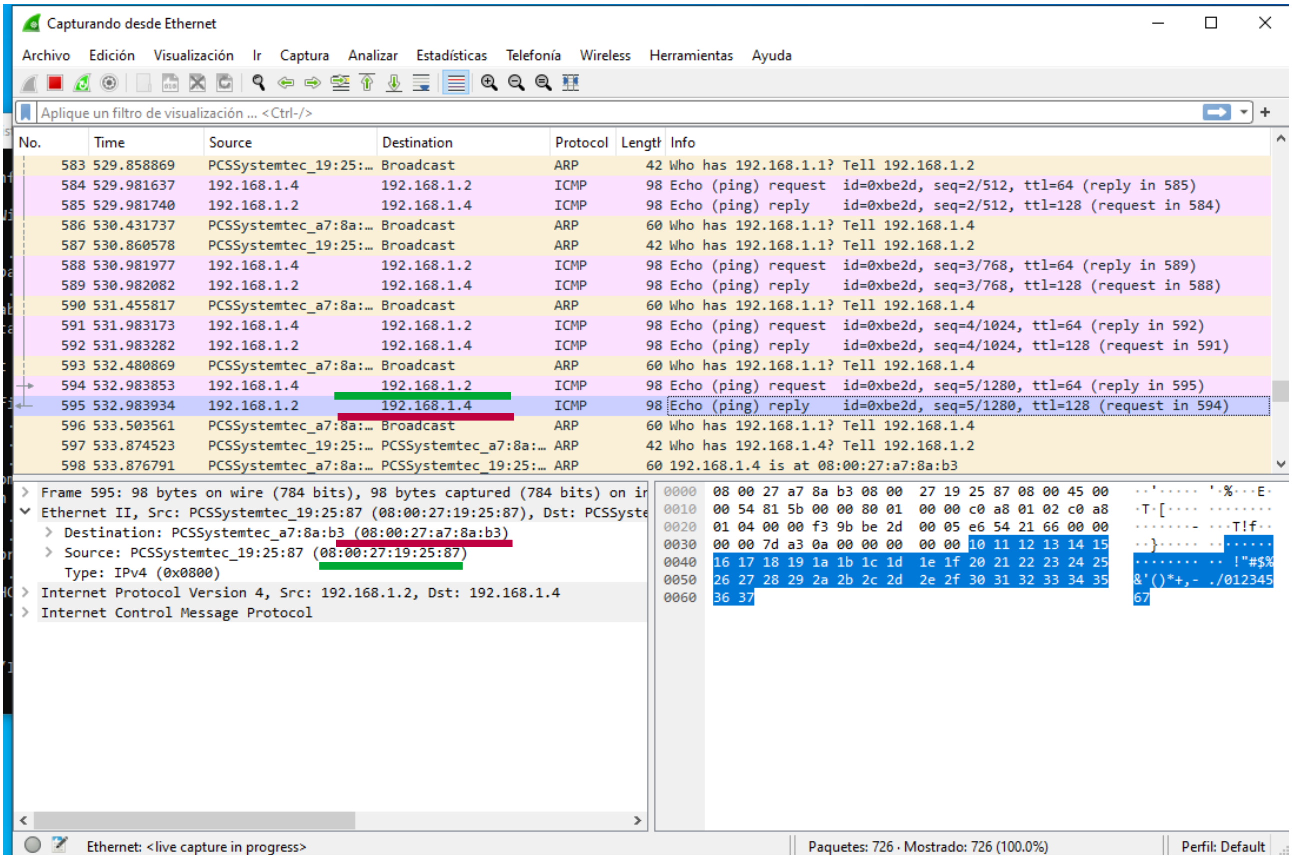


```
C:\Users\alumno>ipconfig /all

Configuración IP de Windows

   Nombre de host. . . . . . . . . : DESKTOP-MOHUBR1
   Sufijo DNS principal  . . . . . :
   Tipo de nodo. . . . . . . . . . : híbrido
   Enrutamiento IP habilitado. . . : no
   Proxy WINS habilitado . . . . . : no

Adaptador de Ethernet Ethernet:

   Sufijo DNS específico para la conexión. . :
   Descripción . . . . . . . . . . . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
   Dirección física. . . . . . . . . . . . . : 08-00-27-19-25-87
   DHCP habilitado . . . . . . . . . . . . . : no
   Configuración automática habilitada . . . : sí
   Vínculo: dirección IPv6 local. . . : fe80::5101:c93b:5290:9b9f%5(Preferido)
   Dirección IPv4. . . . . . . . . . . . . . : 192.168.1.2(Preferido)
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . : 192.168.1.1
   IAID DHCPv6 . . . . . . . . . . . . . . . : 101187623
   DUID de cliente DHCPv6. . . . . . . . . . : 00-01-00-01-2D-B3-04-BD-08-00-27-19-25-87
   Servidores DNS. . . . . . . . . . . . . . : fec0:0:0:ffff::1%1
                                       fec0:0:0:ffff::2%1
                                       fec0:0:0:ffff::3%1
   NetBIOS sobre TCP/IP. . . . . . . . . . . : habilitado
```

Debian:



```
ladmin@debian:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 100
0
    link/ether 08:00:27:a7:8a:b3 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.4/24 brd 192.168.1.255 scope global enp0s3
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fea7:8ab3/64 scope link
       valid_lft forever preferred_lft forever
ladmin@debian:~$ ping -c 5 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
64 bytes from 192.168.1.2: icmp_seq=1 ttl=128 time=1.34 ms
64 bytes from 192.168.1.2: icmp_seq=2 ttl=128 time=1.82 ms
64 bytes from 192.168.1.2: icmp_seq=3 ttl=128 time=1.75 ms
64 bytes from 192.168.1.2: icmp_seq=4 ttl=128 time=0.747 ms
64 bytes from 192.168.1.2: icmp_seq=5 ttl=128 time=1.03 ms

--- 192.168.1.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 0.747/1.337/1.819/0.410 ms
ladmin@debian:~$ _
```



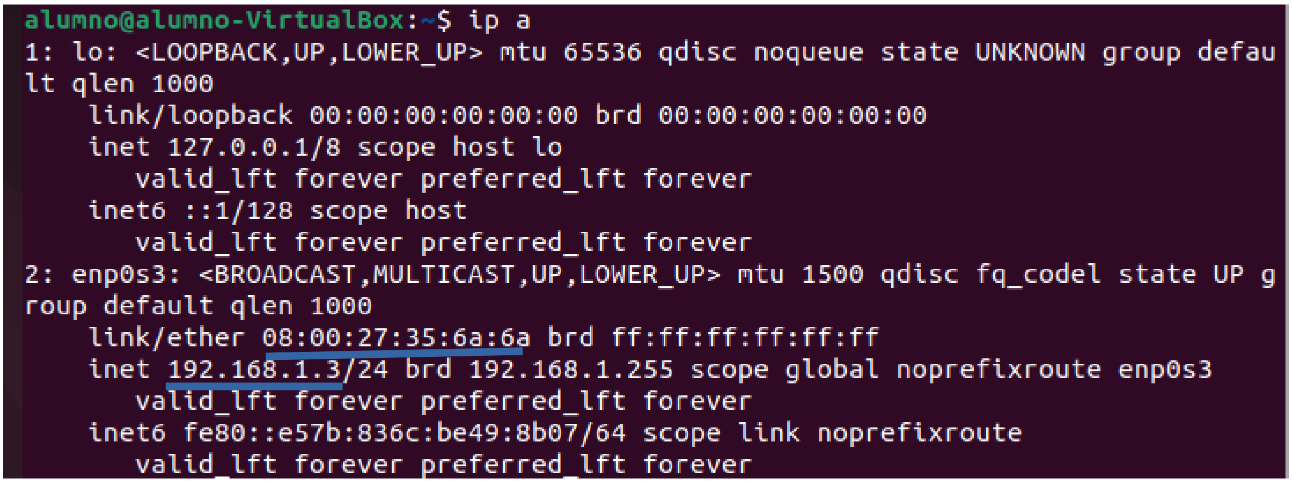
```
No.  Time        Source                Destination           Protocol Length Info
 583 529.858869  PCSSystemtec_19:25:… Broadcast             ARP      42 Who has 192.168.1.1? Tell 192.168.1.2
 584 529.981637  192.168.1.4           192.168.1.2           ICMP     98 Echo (ping) request  id=0xbe2d, seq=2/512, ttl=64 (reply in 585)
 585 529.981740  192.168.1.2           192.168.1.4           ICMP     98 Echo (ping) reply    id=0xbe2d, seq=2/512, ttl=128 (request in 584)
 586 530.431737  PCSSystemtec_a7:8a:… Broadcast             ARP      60 Who has 192.168.1.1? Tell 192.168.1.4
 587 530.860578  PCSSystemtec_19:25:… Broadcast             ARP      42 Who has 192.168.1.1? Tell 192.168.1.2
 588 530.981977  192.168.1.4           192.168.1.2           ICMP     98 Echo (ping) request  id=0xbe2d, seq=3/768, ttl=64 (reply in 589)
 589 530.982082  192.168.1.2           192.168.1.4           ICMP     98 Echo (ping) reply    id=0xbe2d, seq=3/768, ttl=128 (request in 588)
 590 531.455817  PCSSystemtec_a7:8a:… Broadcast             ARP      60 Who has 192.168.1.1? Tell 192.168.1.4
 591 531.983173  192.168.1.4           192.168.1.2           ICMP     98 Echo (ping) request  id=0xbe2d, seq=4/1024, ttl=64 (reply in 592)
 592 531.983282  192.168.1.2           192.168.1.4           ICMP     98 Echo (ping) reply    id=0xbe2d, seq=4/1024, ttl=128 (request in 591)
 593 532.480869  PCSSystemtec_a7:8a:… Broadcast             ARP      60 Who has 192.168.1.1? Tell 192.168.1.4
 594 532.983853  192.168.1.4           192.168.1.2           ICMP     98 Echo (ping) request  id=0xbe2d, seq=5/1280, ttl=64 (reply in 595)
 595 532.983934  192.168.1.2           192.168.1.4           ICMP     98 Echo (ping) reply    id=0xbe2d, seq=5/1280, ttl=128 (request in 594)
 596 533.503561  PCSSystemtec_a7:8a:… Broadcast             ARP      60 Who has 192.168.1.1? Tell 192.168.1.4
 597 533.874523  PCSSystemtec_19:25:… PCSSystemtec_a7:8a:… ARP      42 Who has 192.168.1.4? Tell 192.168.1.2
 598 533.876791  PCSSystemtec_a7:8a:… PCSSystemtec_19:25:… ARP      60 192.168.1.4 is at 08:00:27:a7:8a:b3
```

```
> Frame 595: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on ir
v Ethernet II, Src: PCSSystemtec_19:25:87 (08:00:27:19:25:87), Dst: PCSSyste
  > Destination: PCSSystemtec_a7:8a:b3 (08:00:27:a7:8a:b3)
  > Source: PCSSystemtec_19:25:87 (08:00:27:19:25:87)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 192.168.1.2, Dst: 192.168.1.4
> Internet Control Message Protocol
```

```
0000  08 00 27 a7 8a b3 08 00  27 19 25 87 08 00 45 00   ··'·····'·%···E·
0010  00 54 81 5b 00 00 80 01  00 00 c0 a8 01 02 c0 a8   ·T·[············
0020  01 04 00 00 f3 9b be 2d  00 05 e6 54 21 66 00 00   ·······-···T!f··
0030  00 00 7d a3 0a 00 00 00  00 00 10 11 12 13 14 15   ··}·············
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ·········· !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,-./012345
0060  36 37                                              67
```

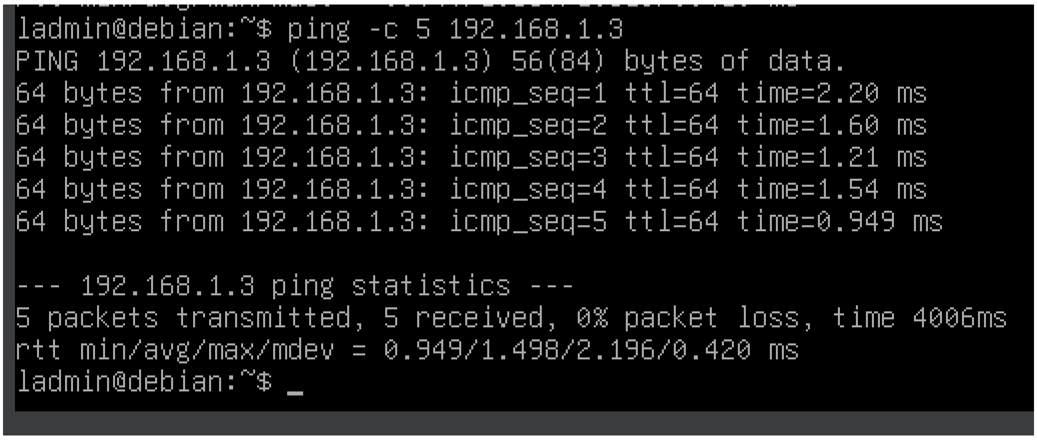
Ethernet: <live capture in progress> Paquetes: 726 · Mostrado: 726 (100.0%) Perfil: Default

- Se fas un ping entre os dous linux, tamén o captura? Sí.

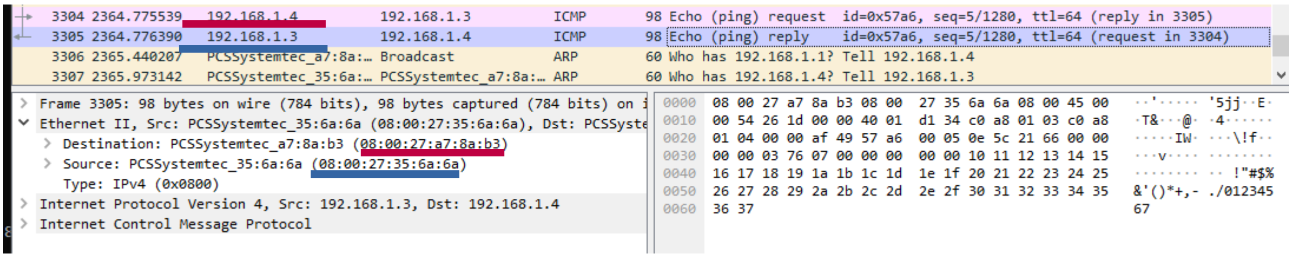


```
alumno@alumno-VirtualBox:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defau
lt qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g
roup default qlen 1000
    link/ether 08:00:27:35:6a:6a brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.3/24 brd 192.168.1.255 scope global noprefixroute enp0s3
       valid_lft forever preferred_lft forever
    inet6 fe80::e57b:836c:be49:8b07/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

Ping de Debian a Ubuntu:



```
ladmin@debian:~$ ping -c 5 192.168.1.3
PING 192.168.1.3 (192.168.1.3) 56(84) bytes of data.
64 bytes from 192.168.1.3: icmp_seq=1 ttl=64 time=2.20 ms
64 bytes from 192.168.1.3: icmp_seq=2 ttl=64 time=1.60 ms
64 bytes from 192.168.1.3: icmp_seq=3 ttl=64 time=1.21 ms
64 bytes from 192.168.1.3: icmp_seq=4 ttl=64 time=1.54 ms
64 bytes from 192.168.1.3: icmp_seq=5 ttl=64 time=0.949 ms

--- 192.168.1.3 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 0.949/1.498/2.196/0.420 ms
ladmin@debian:~$ _
```



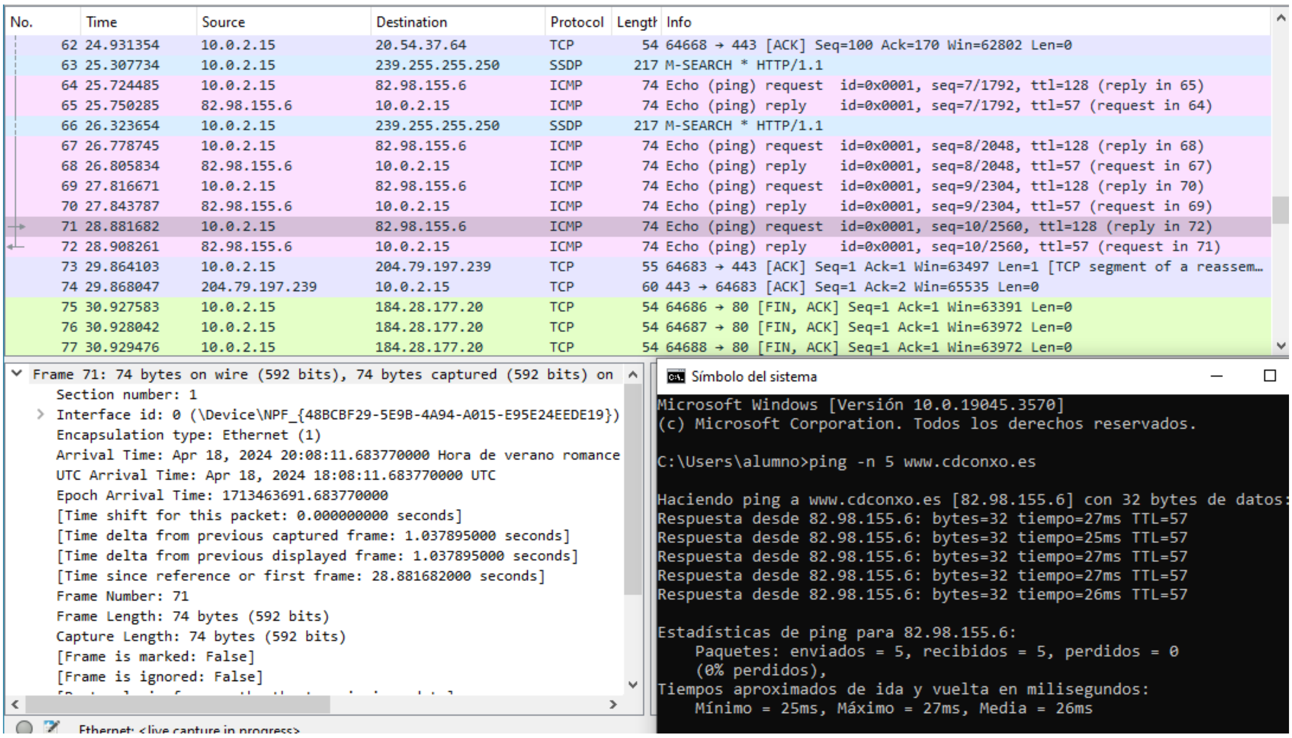
```
3304 2364.775539  192.168.1.4        192.168.1.3        ICMP   98 Echo (ping) request  id=0x57a6, seq=5/1280, ttl=64 (reply in 3305)
3305 2364.776390  192.168.1.3        192.168.1.4        ICMP   98 Echo (ping) reply    id=0x57a6, seq=5/1280, ttl=64 (request in 3304)
3306 2365.440207  PCSSystemtec_a7:8a:… Broadcast          ARP    60 Who has 192.168.1.1? Tell 192.168.1.4
3307 2365.973142  PCSSystemtec_35:6a:… PCSSystemtec_a7:8a:… ARP    60 Who has 192.168.1.4? Tell 192.168.1.3
```

```
> Frame 3305: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on i
v Ethernet II, Src: PCSSystemtec_35:6a:6a (08:00:27:35:6a:6a), Dst: PCSSyste
  > Destination: PCSSystemtec_a7:8a:b3 (08:00:27:a7:8a:b3)
  > Source: PCSSystemtec_35:6a:6a (08:00:27:35:6a:6a)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 192.168.1.3, Dst: 192.168.1.4
> Internet Control Message Protocol
```

```
0000  08 00 27 a7 8a b3 08 00  27 35 6a 6a 08 00 45 00   ··'·····'5jj··E·
0010  00 54 26 1d 00 00 40 01  d1 34 c0 a8 01 03 c0 a8   ·T&···@··4······
0020  01 04 00 00 af 49 57 a6  00 05 0e 5c 21 66 00 00   ·····IW····\!f··
0030  00 00 03 76 07 00 00 00  00 00 10 11 12 13 14 15   ···v············
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ·········· !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,-./012345
0060  36 37                                              67
```

- [Opcional] Podes tentar de conectarte a unha páxina que non sexa HTTPS e ver se os datos van en claro. Se atopas unha con contrasinais sería perfecto. Podes facer a proba con HTTPS tamén para ver as diferencias.

Ping a http://www.cdconxo.es

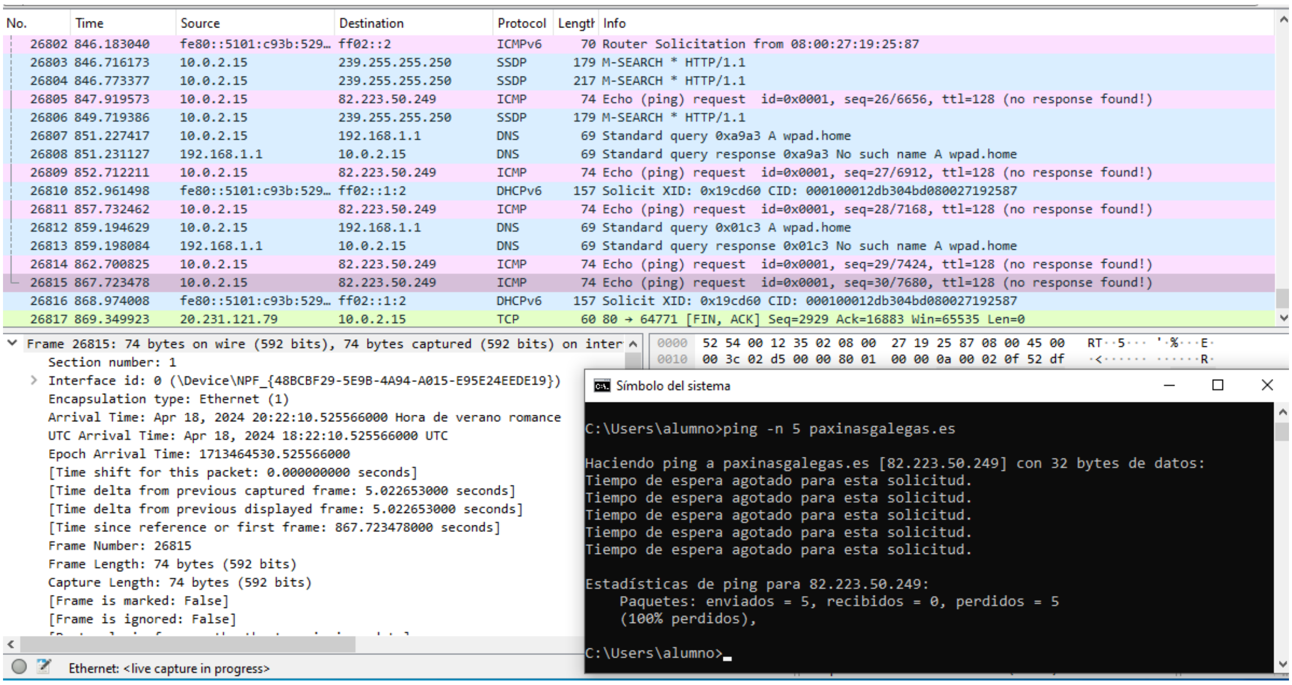


No.	Time	Source	Destination	Protocol	Length	Info
62	24.931354	10.0.2.15	20.54.37.64	TCP	54	64668 → 443 [ACK] Seq=100 Ack=170 Win=62802 Len=0
63	25.307734	10.0.2.15	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
64	25.724485	10.0.2.15	82.98.155.6	ICMP	74	Echo (ping) request id=0x0001, seq=7/1792, ttl=128 (reply in 65)
65	25.750285	82.98.155.6	10.0.2.15	ICMP	74	Echo (ping) reply id=0x0001, seq=7/1792, ttl=57 (request in 64)
66	26.323654	10.0.2.15	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
67	26.778745	10.0.2.15	82.98.155.6	ICMP	74	Echo (ping) request id=0x0001, seq=8/2048, ttl=128 (reply in 68)
68	26.805834	82.98.155.6	10.0.2.15	ICMP	74	Echo (ping) reply id=0x0001, seq=8/2048, ttl=57 (request in 67)
69	27.816671	10.0.2.15	82.98.155.6	ICMP	74	Echo (ping) request id=0x0001, seq=9/2304, ttl=128 (reply in 70)
70	27.843787	82.98.155.6	10.0.2.15	ICMP	74	Echo (ping) reply id=0x0001, seq=9/2304, ttl=57 (request in 69)
71	28.881682	10.0.2.15	82.98.155.6	ICMP	74	Echo (ping) request id=0x0001, seq=10/2560, ttl=128 (reply in 72)
72	28.908261	82.98.155.6	10.0.2.15	ICMP	74	Echo (ping) reply id=0x0001, seq=10/2560, ttl=57 (request in 71)
73	29.864103	10.0.2.15	204.79.197.239	TCP	55	64683 → 443 [ACK] Seq=1 Ack=1 Win=63497 Len=1 [TCP segment of a reassem…
74	29.868047	204.79.197.239	10.0.2.15	TCP	60	443 → 64683 [ACK] Seq=1 Ack=2 Win=65535 Len=0
75	30.927583	10.0.2.15	184.28.177.20	TCP	54	64686 → 80 [FIN, ACK] Seq=1 Ack=1 Win=63391 Len=0
76	30.928042	10.0.2.15	184.28.177.20	TCP	54	64687 → 80 [FIN, ACK] Seq=1 Ack=1 Win=63972 Len=0
77	30.929476	10.0.2.15	184.28.177.20	TCP	54	64688 → 80 [FIN, ACK] Seq=1 Ack=1 Win=63972 Len=0

```
Frame 71: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on
    Section number: 1
  > Interface id: 0 (\Device\NPF_{48BCBF29-5E9B-4A94-A015-E95E24EEDE19})
    Encapsulation type: Ethernet (1)
    Arrival Time: Apr 18, 2024 20:08:11.683770000 Hora de verano romance
    UTC Arrival Time: Apr 18, 2024 18:08:11.683770000 UTC
    Epoch Arrival Time: 1713463691.683770000
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 1.037895000 seconds]
    [Time delta from previous displayed frame: 1.037895000 seconds]
    [Time since reference or first frame: 28.881682000 seconds]
    Frame Number: 71
    Frame Length: 74 bytes (592 bits)
    Capture Length: 74 bytes (592 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
```

```
Microsoft Windows [Versión 10.0.19045.3570]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\alumno>ping -n 5 www.cdconxo.es

Haciendo ping a www.cdconxo.es [82.98.155.6] con 32 bytes de datos:
Respuesta desde 82.98.155.6: bytes=32 tiempo=27ms TTL=57
Respuesta desde 82.98.155.6: bytes=32 tiempo=25ms TTL=57
Respuesta desde 82.98.155.6: bytes=32 tiempo=27ms TTL=57
Respuesta desde 82.98.155.6: bytes=32 tiempo=27ms TTL=57
Respuesta desde 82.98.155.6: bytes=32 tiempo=26ms TTL=57

Estadísticas de ping para 82.98.155.6:
    Paquetes: enviados = 5, recibidos = 5, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 25ms, Máximo = 27ms, Media = 26ms
```

Ping a https://www.paxinasgalegas.es



No.	Time	Source	Destination	Protocol	Length	Info
26802	846.183040	fe80::5101:c93b:529…	ff02::2	ICMPv6	70	Router Solicitation from 08:00:27:19:25:87
26803	846.716173	10.0.2.15	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
26804	846.773377	10.0.2.15	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
26805	847.919573	10.0.2.15	82.223.50.249	ICMP	74	Echo (ping) request id=0x0001, seq=26/6656, ttl=128 (no response found!)
26806	849.719386	10.0.2.15	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
26807	851.227417	10.0.2.15	192.168.1.1	DNS	69	Standard query 0xa9a3 A wpad.home
26808	851.231127	192.168.1.1	10.0.2.15	DNS	69	Standard query response 0xa9a3 No such name A wpad.home
26809	852.712211	10.0.2.15	82.223.50.249	ICMP	74	Echo (ping) request id=0x0001, seq=27/6912, ttl=128 (no response found!)
26810	852.961498	fe80::5101:c93b:529…	ff02::1:2	DHCPv6	157	Solicit XID: 0x19cd60 CID: 000100012db304bd080027192587
26811	857.732462	10.0.2.15	82.223.50.249	ICMP	74	Echo (ping) request id=0x0001, seq=28/7168, ttl=128 (no response found!)
26812	859.194629	10.0.2.15	192.168.1.1	DNS	69	Standard query 0x01c3 A wpad.home
26813	859.198084	192.168.1.1	10.0.2.15	DNS	69	Standard query response 0x01c3 No such name A wpad.home
26814	862.700825	10.0.2.15	82.223.50.249	ICMP	74	Echo (ping) request id=0x0001, seq=29/7424, ttl=128 (no response found!)
26815	867.723478	10.0.2.15	82.223.50.249	ICMP	74	Echo (ping) request id=0x0001, seq=30/7680, ttl=128 (no response found!)
26816	868.974008	fe80::5101:c93b:529…	ff02::1:2	DHCPv6	157	Solicit XID: 0x19cd60 CID: 000100012db304bd080027192587
26817	869.349923	20.231.121.79	10.0.2.15	TCP	60	80 → 64771 [FIN, ACK] Seq=2929 Ack=16883 Win=65535 Len=0

```
Frame 26815: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on inter
    Section number: 1
  > Interface id: 0 (\Device\NPF_{48BCBF29-5E9B-4A94-A015-E95E24EEDE19})
    Encapsulation type: Ethernet (1)
    Arrival Time: Apr 18, 2024 20:22:10.525566000 Hora de verano romance
    UTC Arrival Time: Apr 18, 2024 18:22:10.525566000 UTC
    Epoch Arrival Time: 1713464530.525566000
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 5.022653000 seconds]
    [Time delta from previous displayed frame: 5.022653000 seconds]
    [Time since reference or first frame: 867.723478000 seconds]
    Frame Number: 26815
    Frame Length: 74 bytes (592 bits)
    Capture Length: 74 bytes (592 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
```

```
0000  52 54 00 12 35 02 08 00  27 19 25 87 08 00 45 00   RT··5··· '·%···E·
0010  00 3c 02 d5 00 00 80 01  00 00 0a 00 02 0f 52 df   ·<······ ······R·
```

```
C:\Users\alumno>ping -n 5 paxinasgalegas.es

Haciendo ping a paxinasgalegas.es [82.223.50.249] con 32 bytes de datos:
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.

Estadísticas de ping para 82.223.50.249:
    Paquetes: enviados = 5, recibidos = 0, perdidos = 5
    (100% perdidos),

C:\Users\alumno>
```