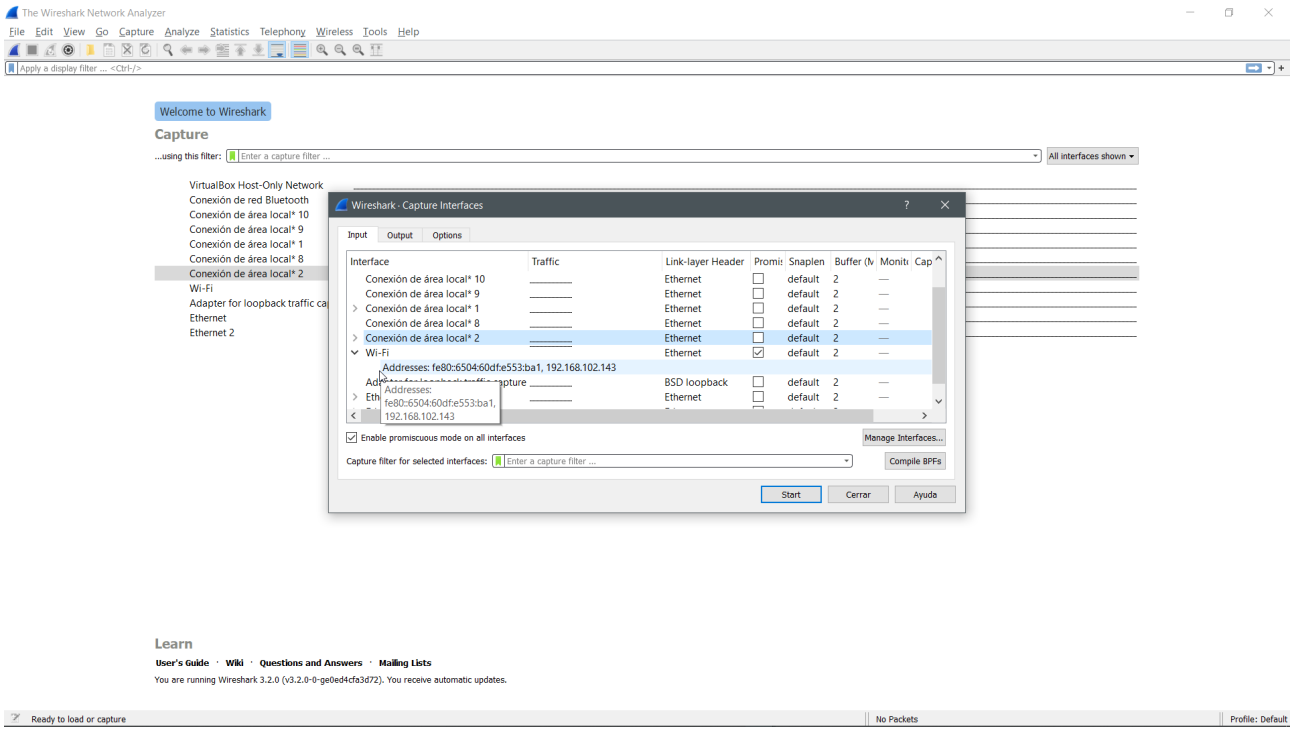
Yago Fernández Blanco
2º ASIR
Seguridad y alta disponibilidad
09/01/2020

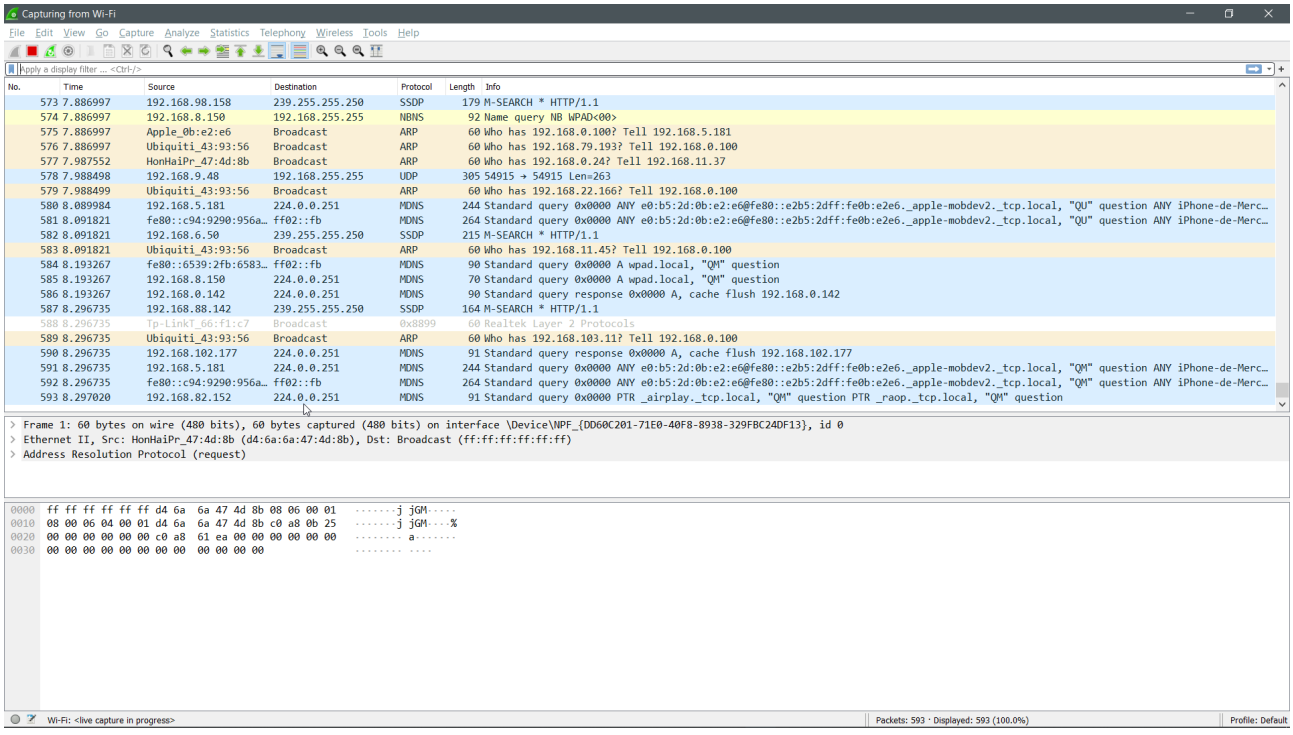
PRÁCTICA WIRESHARK

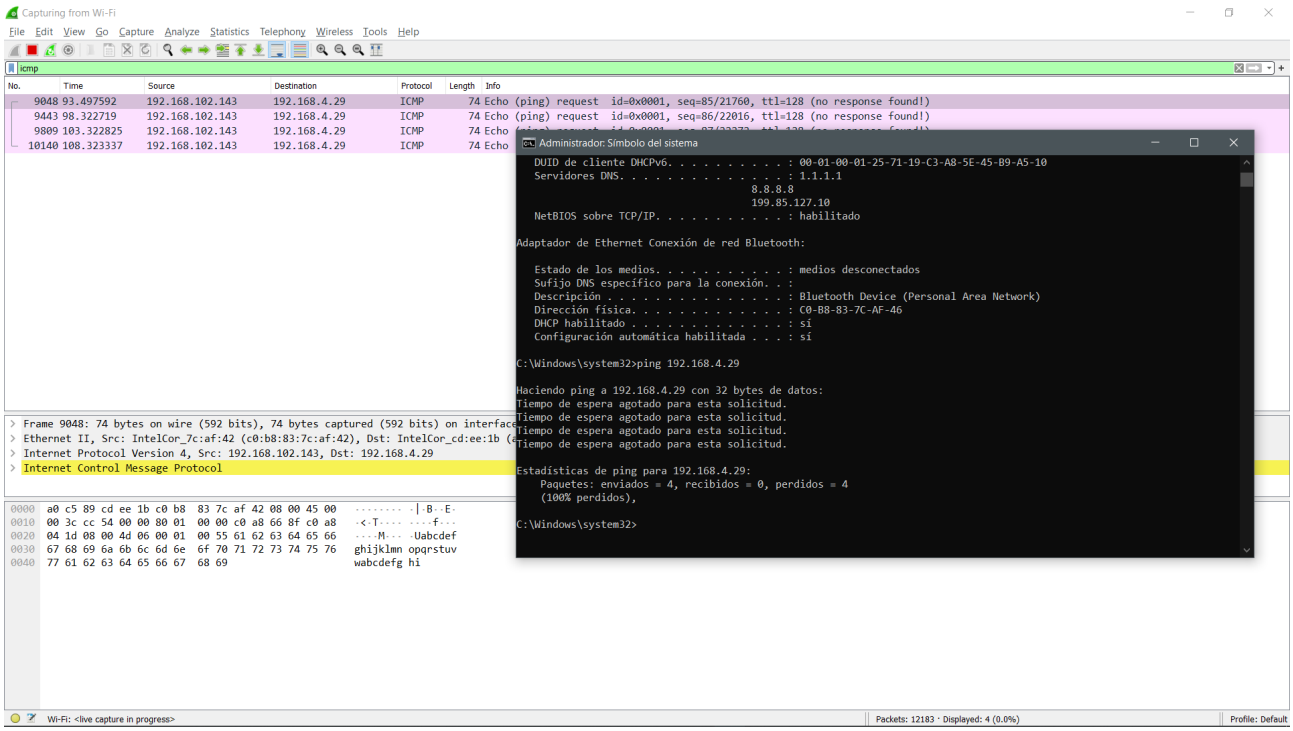
ANALISIS DATOS ICMP

1. Recuperación de las direcciones de interfaz de la PC.

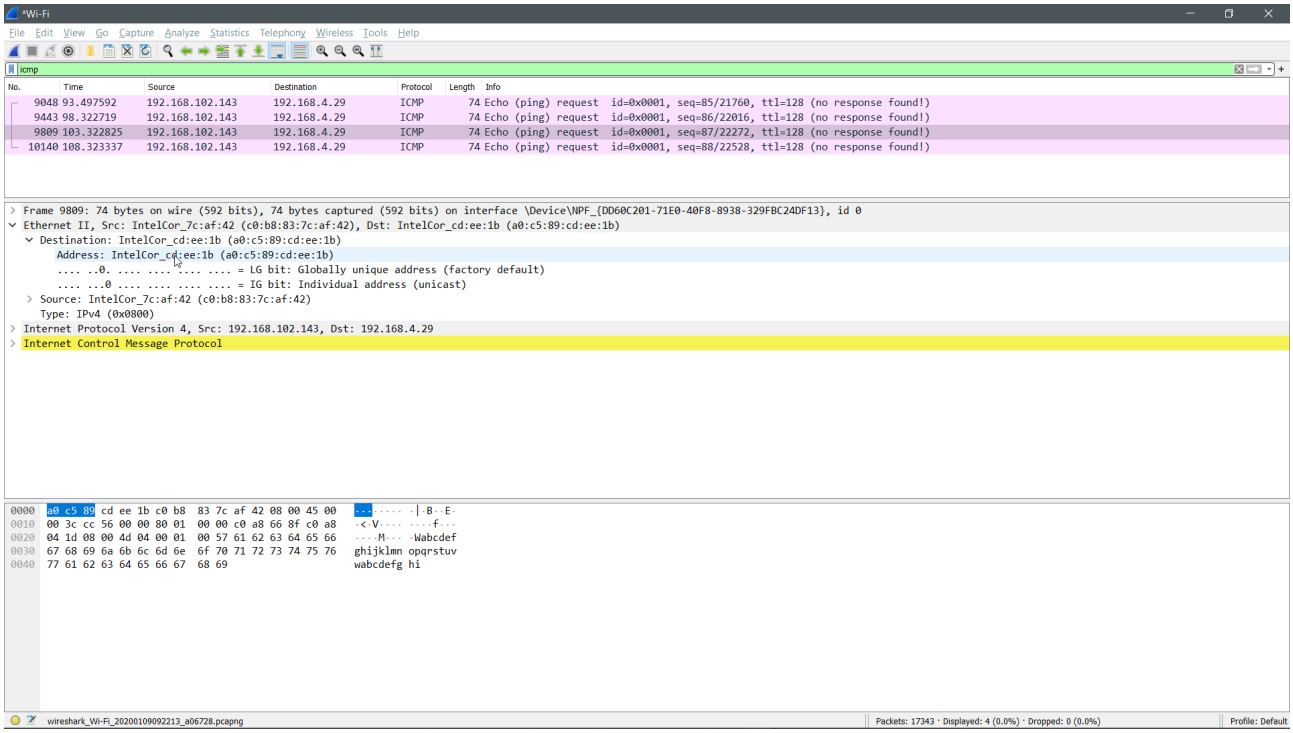
```
Administrador: Símbolo del sistema

Adaptador de Ethernet Ethernet 2:

   Estado de los medios. . . . . . . . . . . : medios desconectados
   Sufijo DNS específico para la conexión. . :
   Descripción . . . . . . . . . . . . . . . : Windscribe VPN
   Dirección física. . . . . . . . . . . . . : 00-FF-9F-35-20-76
   DHCP habilitado . . . . . . . . . . . . . : sí
   Configuración automática habilitada . . . : sí

Adaptador de LAN inalámbrica Wi-Fi:

   Sufijo DNS específico para la conexión. . :
   Descripción . . . . . . . . . . . . . . . : Intel(R) Wireless-AC 9560 160MHz
   Dirección física. . . . . . . . . . . . . : C0-B8-83-7C-AF-42
   DHCP habilitado . . . . . . . . . . . . . : sí
   Configuración automática habilitada . . . : sí
   Vínculo: dirección IPv6 local. . . : fe80::6504:60df:e553:ba1%18(Preferido)
   Dirección IPv4. . . . . . . . . . . . . . : 192.168.102.143(Preferido)
   Máscara de subred . . . . . . . . . . . . : 255.255.0.0
   Concesión obtenida. . . . . . . . . . . . : jueves, 9 de enero de 2020 8:47:53
   La concesión expira . . . . . . . . . . . : viernes, 10 de enero de 2020 8:47:52
   Puerta de enlace predeterminada . . . . . : 192.168.0.100
   Servidor DHCP . . . . . . . . . . . . . . : 192.168.0.100
   IAID DHCPv6 . . . . . . . . . . . . . . . : 146847875
   DUID de cliente DHCPv6. . . . . . . . . . : 00-01-00-01-25-71-19-C3-A8-5E-45-B9-A5-10
   Servidores DNS. . . . . . . . . . . . . . : 1.1.1.1
                                   8.8.8.8
                                   199.85.127.10
   NetBIOS sobre TCP/IP. . . . . . . . . . . : habilitado

Adaptador de Ethernet Conexión de red Bluetooth:

   Estado de los medios. . . . . . . . . . . : medios desconectados
   Sufijo DNS específico para la conexión. . :
   Descripción . . . . . . . . . . . . . . . : Bluetooth Device (Personal Area Network)
   Dirección física. . . . . . . . . . . . . : C0-B8-83-7C-AF-46
   DHCP habilitado . . . . . . . . . . . . . : sí
   Configuración automática habilitada . . . : sí

C:\Windows\system32>
```


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Capture
...using this filter: Enter a capture filter ...
All interfaces shown
VirtualBox Host-Only Network
Conexión de red Bluetooth
Conexión de área local* 10
Conexión de área local* 9
Conexión de área local* 1
Conexión de área local* 8
Conexión de área local* 2
Wi-Fi
Adapter for loopback traffic ca
Ethernet
Ethernet 2
Wireshark · Capture Interfaces
Input
Output
Options
Interface
Traffic
Link-layer Header
Promis
Snaplen
Buffer (M
Monit
Cap
Conexión de área local* 10 Ethernet default 2
Conexión de área local* 9 Ethernet default 2
Conexión de área local* 1 Ethernet default 2
Conexión de área local* 8 Ethernet default 2
Conexión de área local* 2 Ethernet default 2
Wi-Fi Ethernet default 2
Addresses: fe80:6504:60df:e553:ba1, 192.168.102.143
BSD loopback default 2
Ethernet default 2
Addresses:
fe80:6504:60df:e553:ba1,
192.168.102.143
Enable promiscuous mode on all interfaces
Manage Interfaces...
Capture filter for selected interfaces: Enter a capture filter ...
Compile BPFs
Start
Cerrar
Ayuda
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
You are running Wireshark 3.2.0 (v3.2.0-0-ge0ed4cfa3d72). You receive automatic updates.
Ready to load or capture
No Packets
Profile: Default

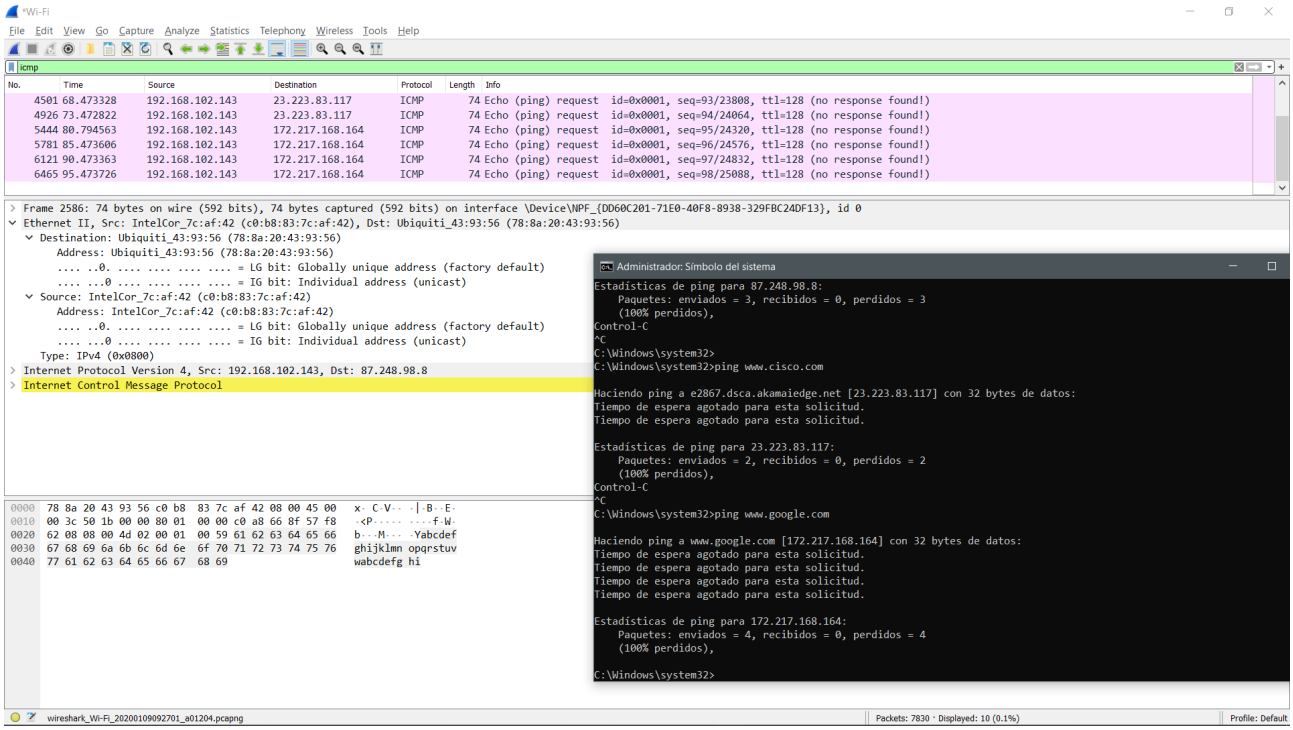

Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
573 7.886997 192.168.98.158 239.255.255.250 SSDP 179 M-SEARCH * HTTP/1.1
574 7.886997 192.168.8.150 192.168.255.255 NBNS 92 Name query NB WPAD<00>
575 7.886997 Apple_0b:e2:e6 Broadcast ARP 60 Who has 192.168.0.100? Tell 192.168.5.181
576 7.886997 Ubiquiti_43:93:56 Broadcast ARP 60 Who has 192.168.79.193? Tell 192.168.0.100
577 7.987552 HonHaiPr_47:4d:8b Broadcast ARP 60 Who has 192.168.0.24? Tell 192.168.11.37
578 7.988498 192.168.9.48 192.168.255.255 UDP 305 54915 → 54915 Len=263
579 7.988499 Ubiquiti_43:93:56 Broadcast ARP 60 Who has 192.168.22.166? Tell 192.168.0.100
580 8.089984 192.168.5.181 224.0.0.251 MDNS 244 Standard query 0x0000 ANY e0:b5:2d:0b:e2:e6@fe80::e2b5:2dff:fe0b:e2e6._apple-mobdev2._tcp.local, "QU" question ANY iPhone-de-Merc…
581 8.091821 fe80::c94:9290:956a… ff02::fb MDNS 264 Standard query 0x0000 ANY e0:b5:2d:0b:e2:e6@fe80::e2b5:2dff:fe0b:e2e6._apple-mobdev2._tcp.local, "QU" question ANY iPhone-de-Merc…
582 8.091821 192.168.6.50 239.255.255.250 SSDP 215 M-SEARCH * HTTP/1.1
583 8.091821 Ubiquiti_43:93:56 Broadcast ARP 60 Who has 192.168.11.45? Tell 192.168.0.100
584 8.193267 fe80::6539:2fb:6583… ff02::fb MDNS 90 Standard query 0x0000 A wpad.local, "QM" question
585 8.193267 192.168.8.150 224.0.0.251 MDNS 70 Standard query 0x0000 A wpad.local, "QM" question
586 8.193267 192.168.0.142 224.0.0.251 MDNS 90 Standard query response 0x0000 A, cache flush 192.168.0.142
587 8.296735 192.168.88.142 239.255.255.250 SSDP 164 M-SEARCH * HTTP/1.1
588 8.296735 Tp-LinkT_66:f1:c7 Broadcast 0x8899 60 Realtek Layer 2 Protocols
589 8.296735 Ubiquiti_43:93:56 Broadcast ARP 60 Who has 192.168.103.11? Tell 192.168.0.100
590 8.296735 192.168.102.177 224.0.0.251 MDNS 91 Standard query response 0x0000 A, cache flush 192.168.102.177
591 8.296735 192.168.5.181 224.0.0.251 MDNS 244 Standard query 0x0000 ANY e0:b5:2d:0b:e2:e6@fe80::e2b5:2dff:fe0b:e2e6._apple-mobdev2._tcp.local, "QM" question ANY iPhone-de-Merc…
592 8.296735 fe80::c94:9290:956a… ff02::fb MDNS 264 Standard query 0x0000 ANY e0:b5:2d:0b:e2:e6@fe80::e2b5:2dff:fe0b:e2e6._apple-mobdev2._tcp.local, "QM" question ANY iPhone-de-Merc…
593 8.297020 192.168.82.152 224.0.0.251 MDNS 91 Standard query 0x0000 PTR _airplay._tcp.local, "QM" question PTR _raop._tcp.local, "QM" question
Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{DD60C201-71E0-40F8-8938-329FBC24DF13}, id 0
Ethernet II, Src: HonHaiPr_47:4d:8b (d4:6a:6a:47:4d:8b), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)
0000 ff ff ff ff ff ff d4 6a 6a 47 4d 8b 08 06 00 01 ·····j jGM·····
0010 08 00 06 04 00 01 d4 6a 6a 47 4d 8b c0 a8 0b 25 ·····j jGM····%
0020 00 00 00 00 00 00 c0 a8 61 ea 00 00 00 00 00 00 ·····a·····
0030 00 00 00 00 00 00 00 00 00 00 00 00 ·····
Wi-Fi: <live capture in progress>
Packets: 593 · Displayed: 593 (100.0%)
Profile: Default



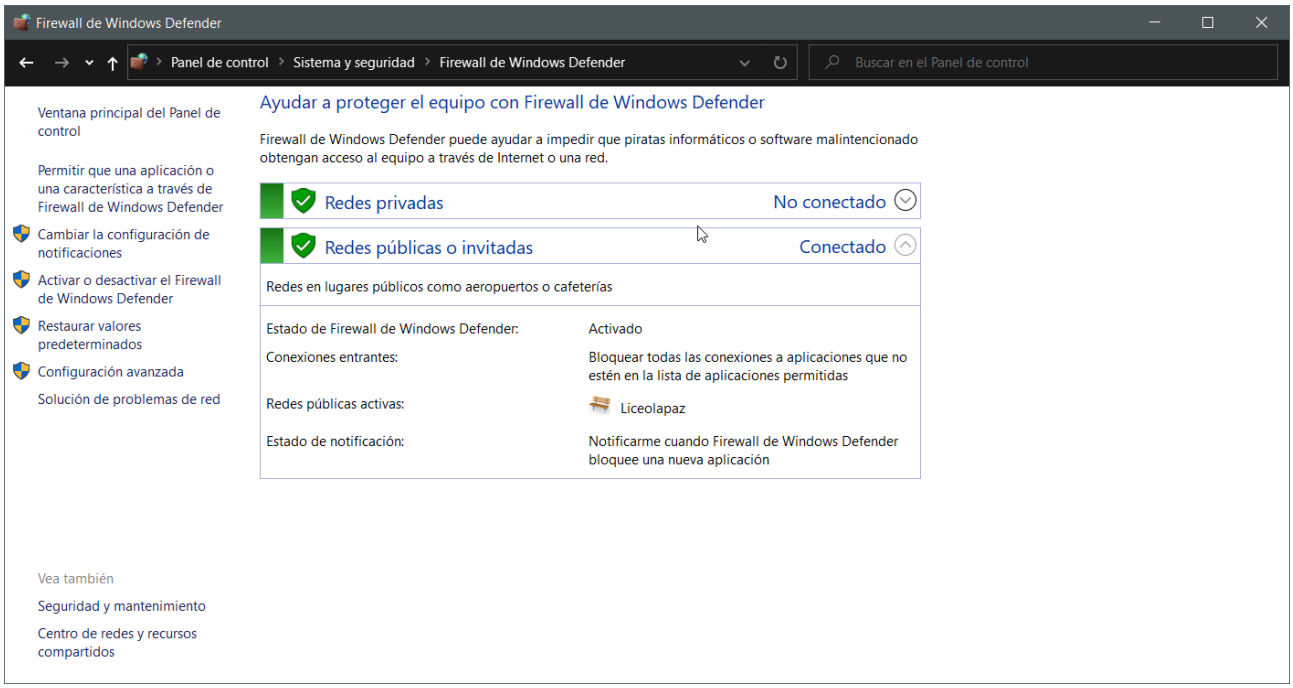
SERGIO TIENE BLOQUEADO LOS PINGs EN LA RED

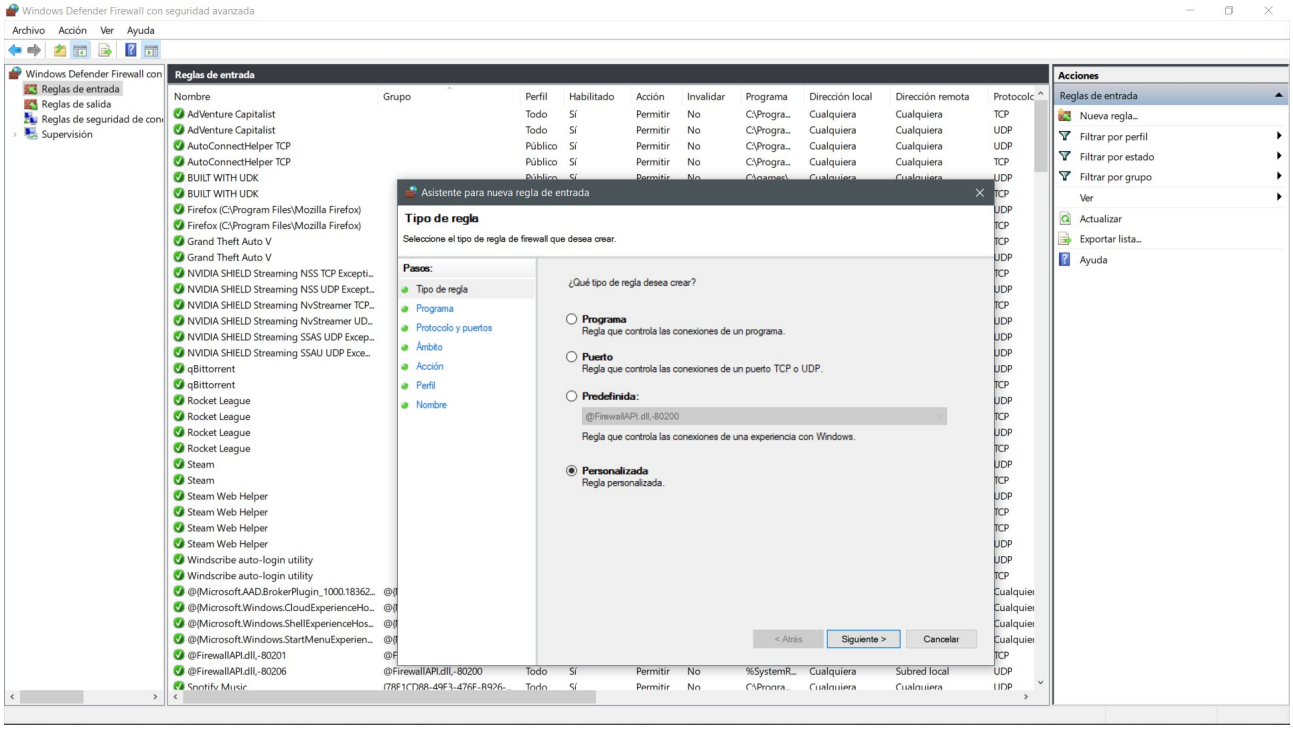


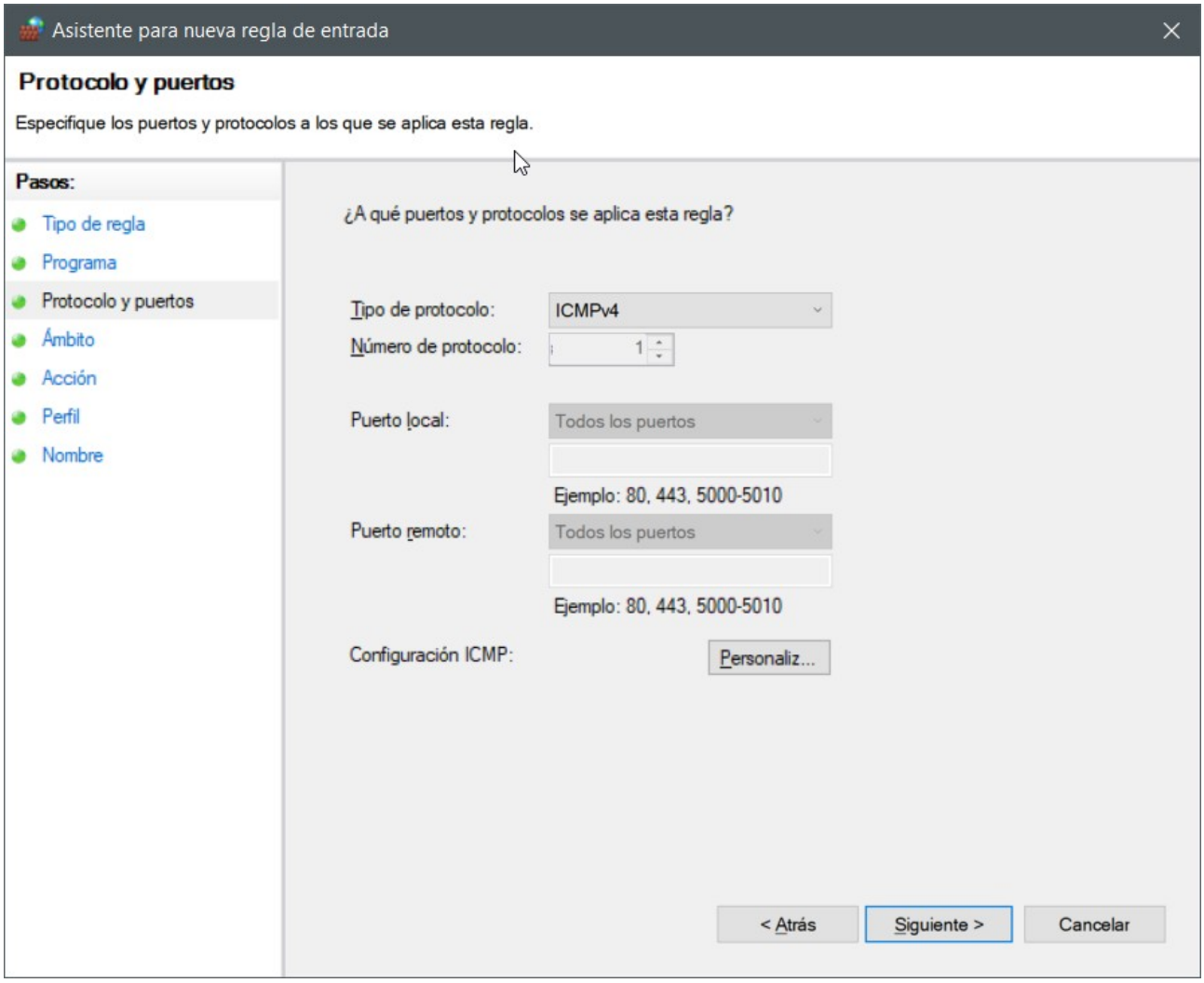
2. Análisis datos remotos.

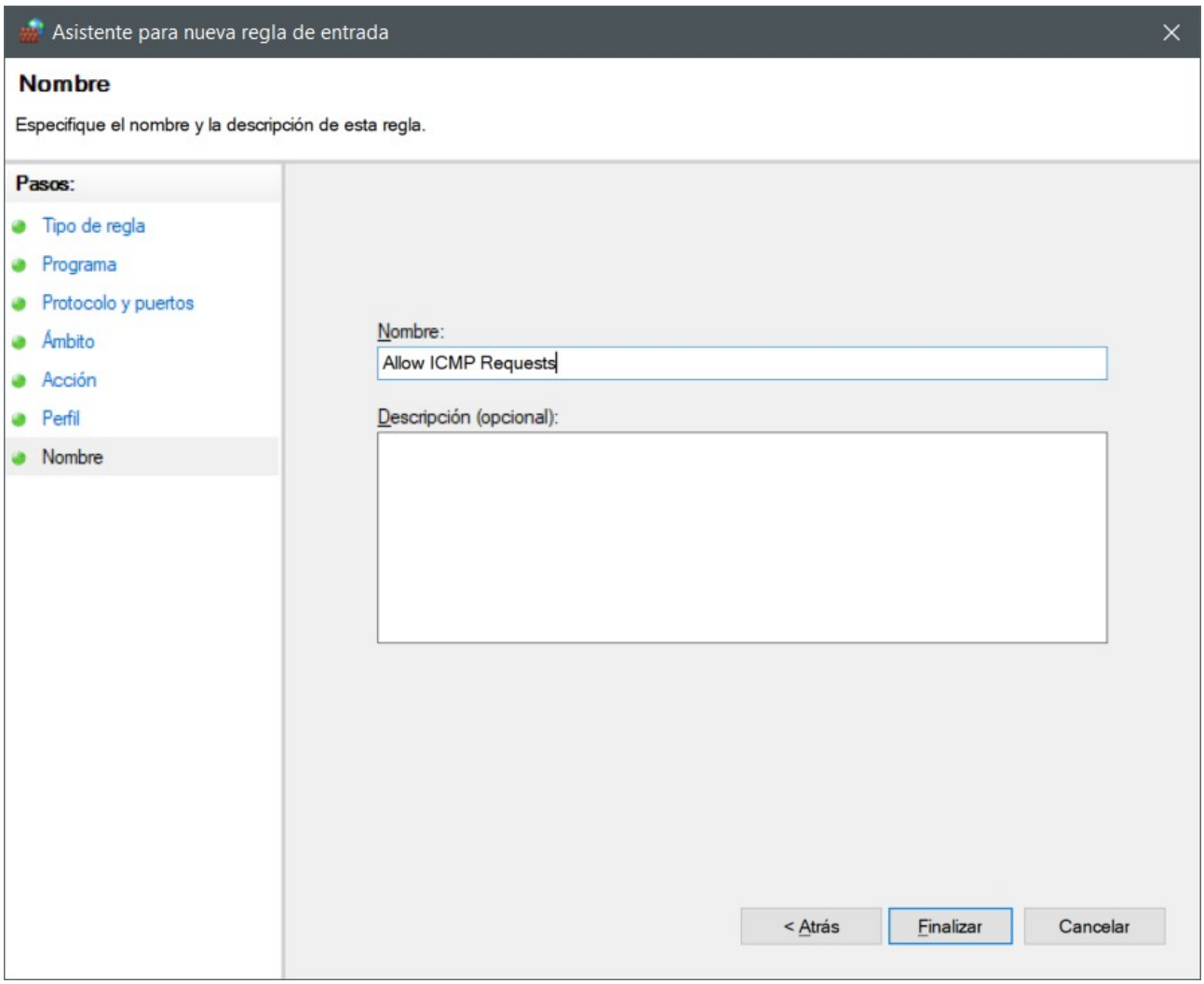


3. Permitir tráfico ICMP.




Windows Defender Firewall con seguridad avanzada
Archivo Acción Ver Ayuda
Windows Defender Firewall con
Reglas de entrada
Reglas de salida
Supervisión
Reglas de entrada
Nombre Grupo Perfil Habilitado Acción Invalidar Programa Dirección local Dirección remota Protocolo
Acciones
Reglas de entrada
Nueva regla...
Filtrar por perfil
Filtrar por estado
Filtrar por grupo
Ver
Actualizar
Exportar lista...
Ayuda
Asistente para nueva regla de entrada
Tipo de regla
Seleccione el tipo de regla de firewall que desea crear.
Pasos:
Tipo de regla
Programa
Protocolo y puertos
Ámbito
Acción
Perfil
Nombre
¿Qué tipo de regla desea crear?
Programa
Regla que controla las conexiones de un programa.
Puerto
Regla que controla las conexiones de un puerto TCP o UDP.
Predefinida:
@FirewallAPI.dll,-80200
Regla que controla las conexiones de una experiencia con Windows.
Personalizada
Regla personalizada.
< Atrás
Siguiente >
Cancelar

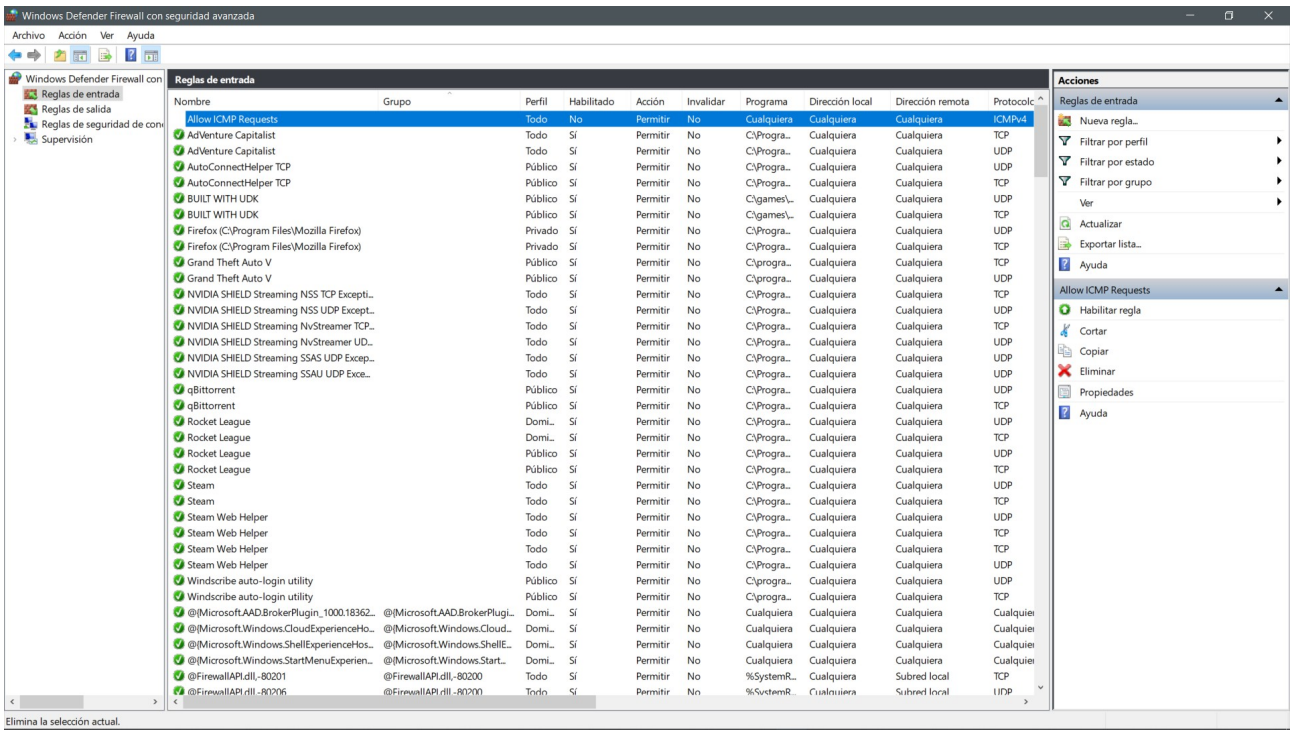

Asistente para nueva regla de entrada
Protocolo y puertos
Especifique los puertos y protocolos a los que se aplica esta regla.
Pasos:
Tipo de regla
Programa
Protocolo y puertos
Ámbito
Acción
Perfil
Nombre
¿A qué puertos y protocolos se aplica esta regla?
Tipo de protocolo:
ICMPv4
Número de protocolo:
1
Puerto local:
Todos los puertos
Ejemplo: 80, 443, 5000-5010
Puerto remoto:
Todos los puertos
Ejemplo: 80, 443, 5000-5010
Configuración ICMP:
Personaliz...
< Atrás
Siguiente >
Cancelar



eguridad avanzada

Reglas de entrada

Nombre	Grupo	Perfil	Habilitado	Acción	Invalidar	Programa	Dirección local	Dirección remota	Protocolo
Allow ICMP Requests		Todo	Sí	Permitir	No	Cualquiera	Cualquiera	Cualquiera	ICMPv4
AdVenture Capitalist		Todo	Sí	Permitir	No	C:\Progra...	Cualquiera	Cualquiera	TCP
AdVenture Capitalist		Todo	Sí	Permitir	No	C:\Progra...	Cualquiera	Cualquiera	UDP
AutoConnectHelper TCP		Público	Sí	Permitir	No	C:\Progra...	Cualquiera	Cualquiera	UDP
AutoConnectHelper TCP		Público	Sí	Permitir	No	C:\Progra...	Cualquiera	Cualquiera	TCP
BUILT WITH UDK		Público	Sí	Permitir	No	C:\games\...	Cualquiera	Cualquiera	UDP
BUILT WITH UDK		Público	Sí	Permitir	No	C:\games\...	Cualquiera	Cualquiera	TCP
Firefox (C:\Program Files\Mozilla Firefox)		Privado	Sí	Permitir	No	C:\Progra...	Cualquiera	Cualquiera	UDP
Firefox (C:\Program Files\Mozilla Firefox)		Privado	Sí	Permitir	No	C:\Progra...	Cualquiera	Cualquiera	TCP
Grand Theft Auto V		Público	Sí	Permitir	No	C:\progra...	Cualquiera	Cualquiera	TCP
Grand Theft Auto V		Público	Sí	Permitir	No	C:\progra...	Cualquiera	Cualquiera	UDP



Deshabilitamos y eliminamos