

Hachetetepé dos puntos SLAAC SLACC

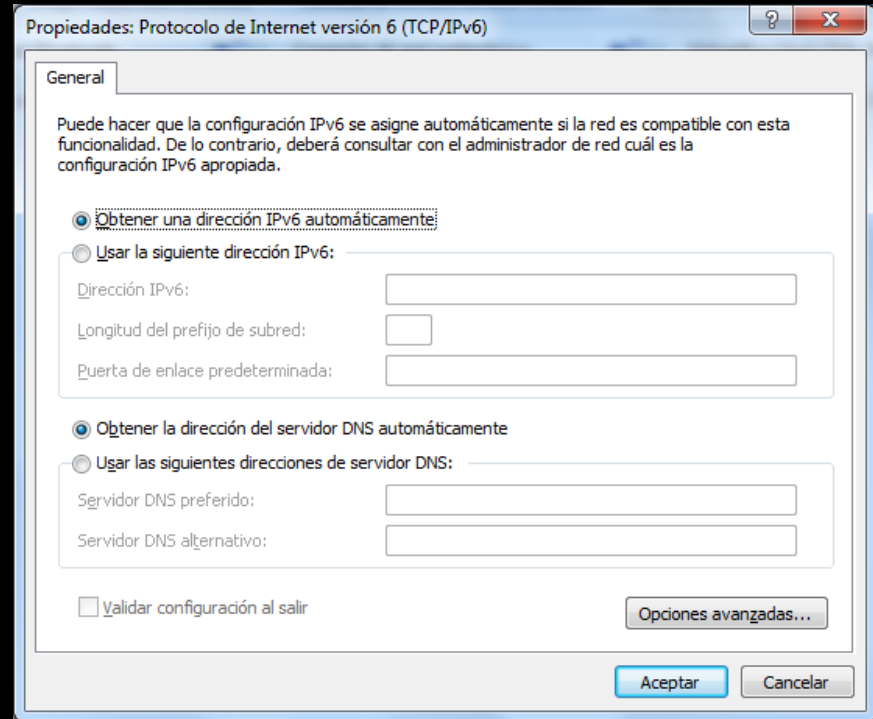
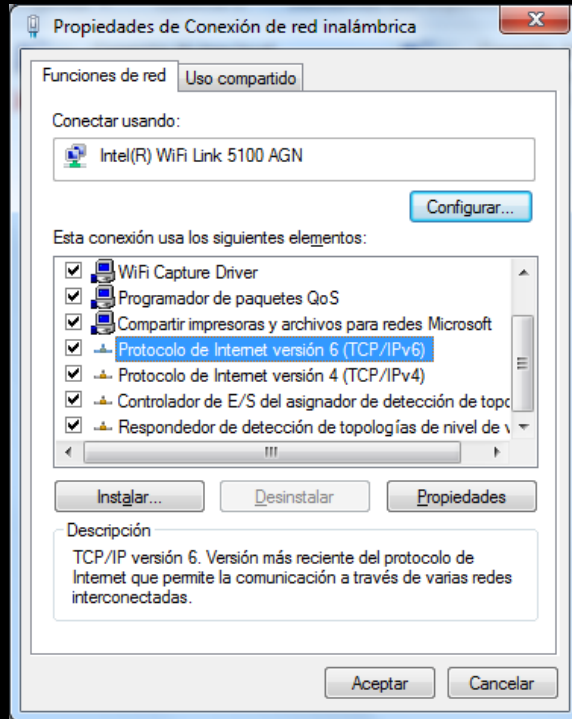
Chema Alonso

chema@informatica64.com

TROOPERS 20013

Informática 64

IPv6 is on your box!



And it works!: 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
```

And it works!: route print

```
IPv6 Tabla de enrutamiento
```

```
=====
```

```
Rutas activas:
```

	Quando 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

And it works!: Neighbors

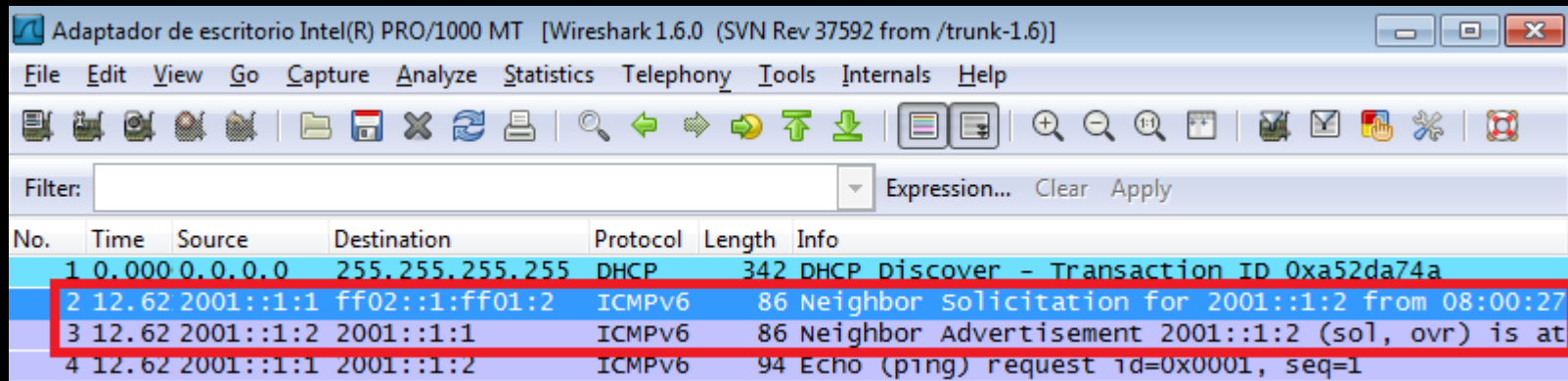
```
C:\Users\user>netsh interface ipv6 show neighbors
```

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 (Enrutador)
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

ICMPv6

- **No ARP**
 - No ARP Spoofing
 - Tools anti-ARP Spoofing are useless
- **Neighbor Discover uses ICMPv6**
 - NS: Neighbor Solicitation
 - NA: Neighbor Advertisement

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

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: 0x00000000
 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	85	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)
```

Evil FOCA

The screenshot displays the Evil FOCA application window, version 0.1.2.0. The interface is divided into several sections:

- Network:** A tree view on the left shows a list of neighbors with their IP and MAC addresses. The selected neighbor is F4CE46BFA284 (Area54) with IP 192.168.0.54 and MAC 00E04CE0E10F.
- Configuration:** The main area shows settings for MITM IPv4, DoS IPv4, and DNS Hijacking. Under MITM IPv4, the "DHCP ACK Injection" tab is active. It includes fields for "Fake DNS" (8.8.8.8), "Fake gateway", and "MAC". There are radio buttons for "Attack all computers" and "Attack computer with this MAC" (selected), and a checkbox for "Use this computer as gateway". A "Start" button is present.
- DHCP ACK Injection:** A text box on the right explains: "- This computer acts as a rogue DHCP server, configuring the clients to connect to your IP address as gateway."
- Attack Log:** A table below the configuration shows active attacks. The first entry is "SlaacMitm" with target 1: "/Attacker default gateway" and target 2: "fe80::6d59:1c72:8952:f786". The "Active" column has a checked box.
- Log Window:** At the bottom, a log window shows messages from the "NeighborSpoofing" module, such as "New neighbor detected with 00155D008F05 as physical address".

Demo 1: Mitm using NA Spoofing

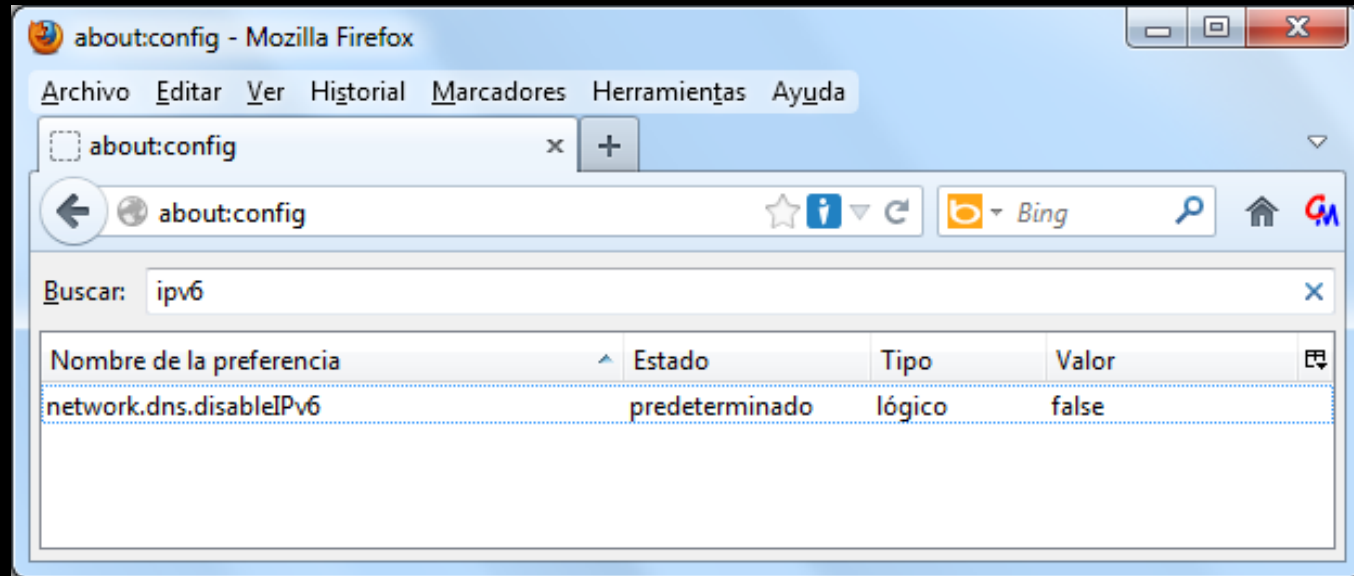
ICMPv6: SLAAC

- 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

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

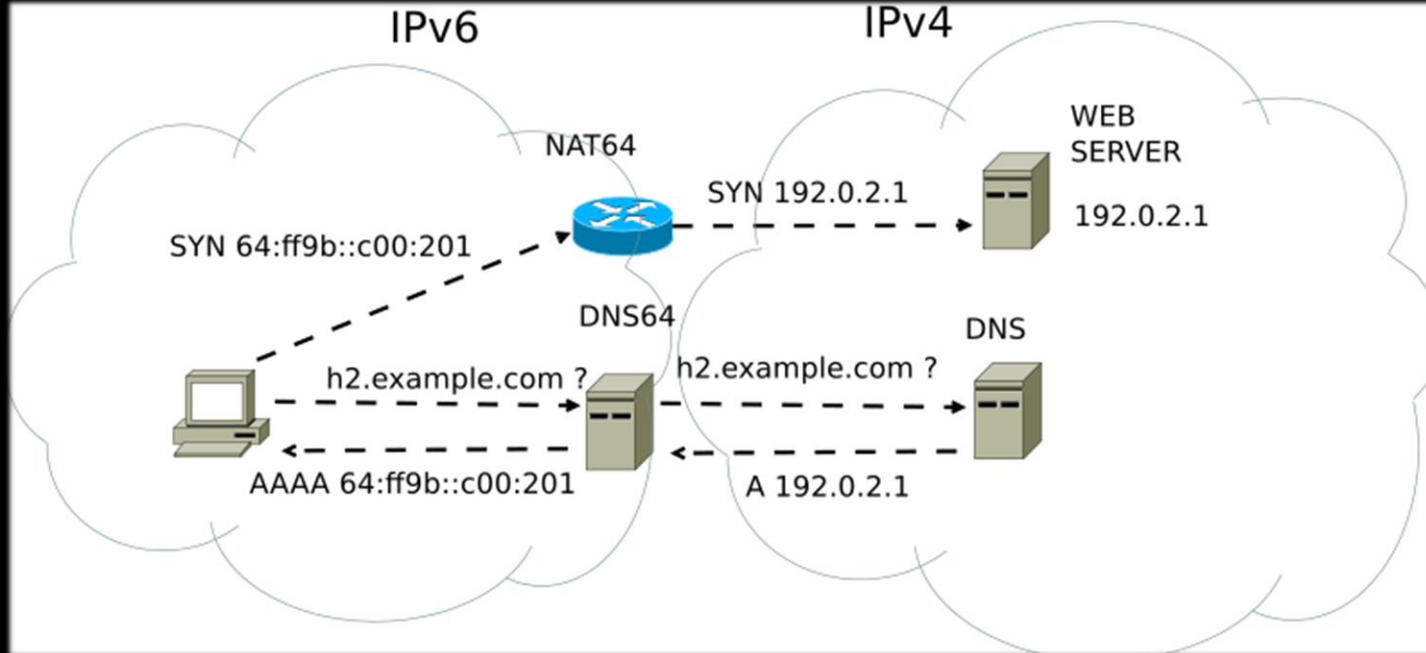
And it works!: Web Browser



Windows Behavior

- IPv4 & IPv6
 - DNSv4 queries A & AAAA
- IPv6 Only
 - DNSv6 queries A
- IPv6 & IPv4 Local Link
 - DNSv6 queries AAAA

DNS64 & NAT64



HTTP-s Connections

- **SSL Strip**
 - Remove “S” from HTTP-s links
- **SSL Sniff**
 - Use a Fake CA to create dynamicly Fake CA
- **Evil FOCA does SSL Strip (so far)**

Demo 2: Windows behavior

Demo 2: hachetetepe dos puntos SLAAC SLACC

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

Conclusions

FEAR (the EVIL) FOCA!

Thanks to

- **THC (The Hacking Choice)**
 - Included in Back Track
 - 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;
    }
};
```

Questions?

chema@informatica64.com

TROOPERS 20013

Informática 64