

# Práctica 1

---

## Despliegue de aplicaciones web - DAW2

Josep Maria Castell Colom

## Parte 1: Puertos y conexiones

Inicia una sesión en Windows con un usuario con privilegios de administrador.

1. Averigua los puertos TCP a la escucha con el comando `netstat -a -p TCP -n`.

```

josep@josep-Ubuntu:~
→ ~ sudo netstat -atpn
Conexiones activas de Internet (servidores y establecidos)
Proto Recib Enviad Dirección local Dirección remota Estado PID/Program name
tcp 0 0 127.0.0.53:53 0.0.0.0:* ESCUCHAR 652/systemd-resolve
tcp 0 0 127.0.0.1:631 0.0.0.0:* ESCUCHAR 980/cupsd
tcp6 0 0 :::43973 :::* ESCUCHAR 19402/codium
tcp6 0 0 127.0.0.1:64120 :::* ESCUCHAR 19536/java
tcp6 0 0 :::80 :::* ESCUCHAR 1039/apache2
tcp6 0 0 :::1:631 :::* ESCUCHAR 980/cupsd
tcp6 0 0 127.0.0.1:43973 127.0.0.1:51896 ESTABLECIDO 19402/codium
tcp6 0 0 127.0.0.1:51896 127.0.0.1:43973 ESTABLECIDO 19536/java
→ ~ █

```

2. Averigua los puertos UDP a la escucha con el comando `netstat -a -p UDP -n`.

```

josep@josep-Ubuntu:~
→ ~ sudo netstat -aupn
Conexiones activas de Internet (servidores y establecidos)
Proto Recib Enviad Dirección local Dirección remota Estado PID/Program name
udp 0 0 0.0.0.0:52159 0.0.0.0:* 17991/firefox
udp 0 0 127.0.0.53:53 0.0.0.0:* 652/systemd-resolve
udp 0 0 172.16.129.233:68 172.16.128.1:67 ESTABLECIDO 816/NetworkManager
udp 0 0 0.0.0.0:41116 0.0.0.0:* 810/avahi-daemon: r
udp 0 0 0.0.0.0:631 0.0.0.0:* 1689/cups-browsed
udp 0 0 0.0.0.0:5353 0.0.0.0:* 810/avahi-daemon: r
udp6 0 0 :::5353 :::* 810/avahi-daemon: r
udp6 0 0 :::50535 :::* 810/avahi-daemon: r
→ ~ █

```

3. Abre el navegador y accede a una web de internet:

Muestra las conexiones TCP establecidas con el comando `netstat -p TCP -n`.

```

josep@josep-Ubuntu:~
→ ~ sudo netstat -atpn
Conexiones activas de Internet (servidores y establecidos)
Proto Recib Enviad Dirección local Dirección remota Estado PID/Program name
tcp 0 0 127.0.0.53:53 0.0.0.0:* ESCUCHAR 652/systemd-resolve
tcp 0 0 127.0.0.1:631 0.0.0.0:* ESCUCHAR 980/cupsd
tcp 0 0 172.16.129.233:51470 76.76.21.142:443 ESTABLECIDO 19350/VSCodium --st
tcp 0 0 172.16.129.233:57118 34.117.237.239:443 ESTABLECIDO 17991/firefox
tcp 0 0 172.16.129.233:42830 52.41.246.187:443 ESTABLECIDO 17991/firefox
tcp 0 0 172.16.129.233:39046 76.76.21.164:443 ESTABLECIDO 19350/VSCodium --st
tcp6 0 0 :::43973 :::* ESCUCHAR 19402/codium
tcp6 0 0 127.0.0.1:64120 :::* ESCUCHAR 19536/java
tcp6 0 0 :::80 :::* ESCUCHAR 1039/apache2
tcp6 0 0 :::1:631 :::* ESCUCHAR 980/cupsd
tcp6 0 0 127.0.0.1:43973 127.0.0.1:51896 ESTABLECIDO 19402/codium
tcp6 0 0 127.0.0.1:51896 127.0.0.1:43973 ESTABLECIDO 19536/java
→ ~ █

```

3.1. ¿Qué puertos ha signado el sistema operativo al navegador web para establecer las conexiones TCP?

3.2. ¿Qué puertos utilizan los servidores con los que se establecen las conexiones?

4. Comprueba la IP y el nombre del servidor predeterminado de DNS con el comando `nslookup`.

```
nslookup

→ ~ nslookup
> 
```

```
josep@josep-Ubuntu:~
→ ~ resolvectl status
Global
    Protocols: -LLMNR -mDNS -DNSOverTLS DNSSEC=no/unsupported
resolv.conf mode: stub

Link 2 (wlp0s20f3)
    Current Scopes: DNS
    Protocols: +DefaultRoute +LLMNR -mDNS -DNSOverTLS DNSSEC=no/unsupported
Current DNS Server: 8.8.4.4
    DNS Servers: 8.8.8.8 8.8.4.4
→ ~ nslookup 8.8.4.4
4.4.8.8.in-addr.arpa    name = dns.google.

Authoritative answers can be found from:

→ ~ 
```

5. Realiza la resolución inversa de la IP 62.42.63.52, obteniendo el nombre del servidor DNS con el comando `nslookup`.

```
→ ~ nslookup 62.42.63.52
52.63.42.62.in-addr.arpa    name = resolv2.ono.com.

Authoritative answers can be found from:

→ ~ 
```

## Parte 2: Protocolo HTTP

Descarga e instala el programa WIRESHARK.

Abre el navegador.

Inicia una captura con Wireshark en CAPTURE:INTERFACES:START.

Desde el navegador accede a la web <http://www.apache.org>.

Accede a Wireshark y para la captura CAPTURE:STOP.

Busca una trama HTTP en donde la petición sea GET / HTTP/1.1.

Con el botón derecho del ratón selecciona FOLLOW TCP STREAM.

Responde a las siguientes preguntas mostrando capturas de pantalla con las evidencias:

1. ¿Cuál es tu dirección IP? ¿Y tu puerto de origen?
2. ¿Cuál es la dirección IP de destino? ¿Y el puerto de destino?
3. ¿Qué versión de HTTP se utiliza?
4. ¿Qué método de petición se utiliza?
5. ¿Qué ha ocurrido con la respuesta del servidor? (Adquiere o no adquiere lo que solicita)