EJERCICIO DE REDES
-DNS-

Alejandro Rodríguez Rojas

Sumario

1 Introducción

Vamos a utilizar el comando “dig” para verificar que las IP de www.marca.com y www.elmundo.es son iguales.

Para utilizar el comando dig deberemos instalar “dnsutils”:

#:apt-get install dnsutils

Acto seguido utilizaremos wireshark para verificar el dns de la red www.elmundo.es , para ello debemos instalar el paquete wireshark

#:apt-get install wireshark

Para ejecutar wireshark tendremos que entrar como root y escribir en la terminal:

#:wireshark

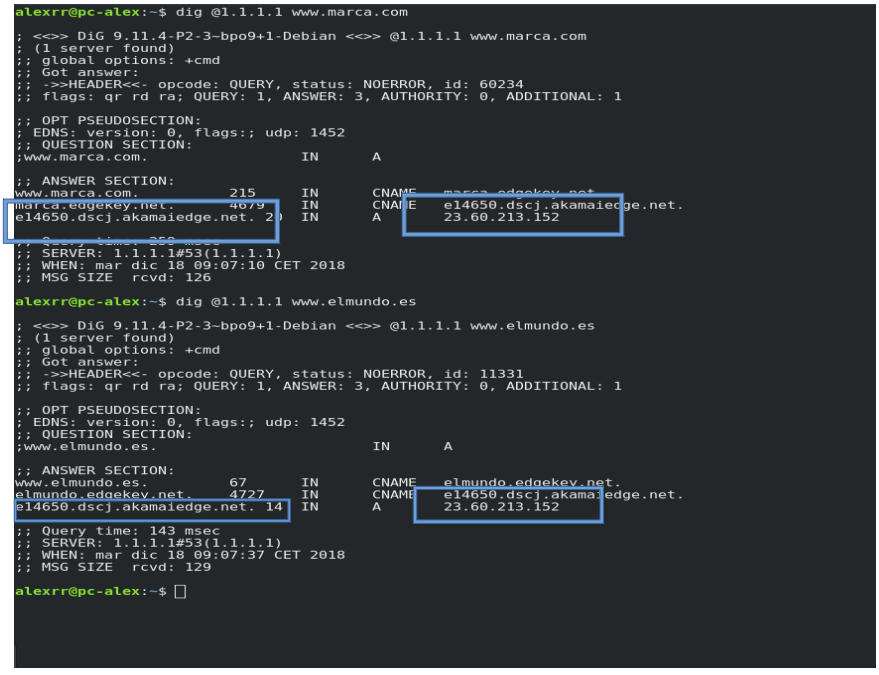
2 Comando Dig

Para verificar que ambas paginas se alojan en un mismo servidor debemos utilizar el comando dig:

dig www.marca.com

dig www.elmundo.es

Utilizaremos dig @1.1.1.1 {Nombre de web}, ya que marca es inutilizable



Como podemos observar, ambos tienen un mismo servidor conjunto, que es la IP:

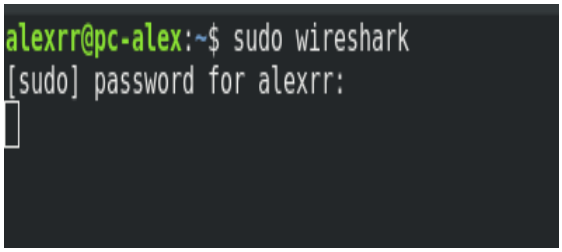
23.60.213.152

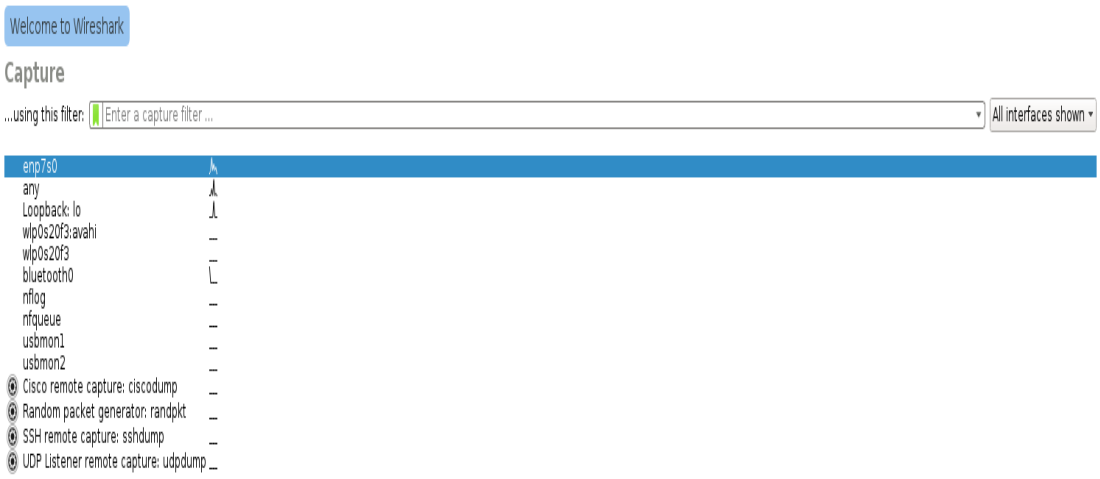
3 Wireshark

Para utilizar Wireshark primero debemos instalarlo, para ello ejecutamos una terminal en nuestro sistema Linux y escribimos el siguiente comando:

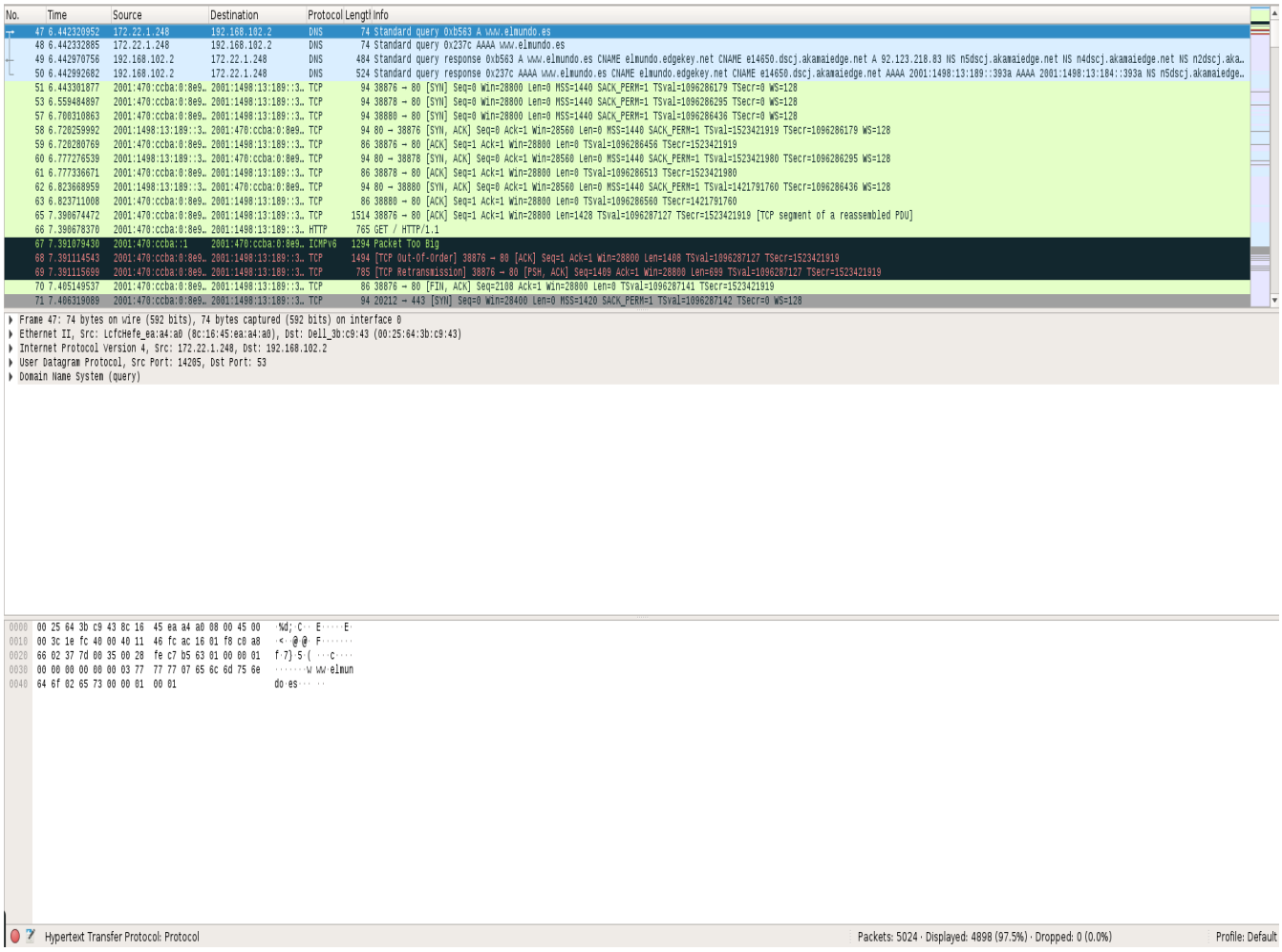
#:apt-get install wireshark

Al instalarlo deberemos ejecutarlo como root escribiendo wireshark en la terminal o accediendo mediante superusuario al programa(Si no estas en superusuario no te detectará la tarjeta de red).

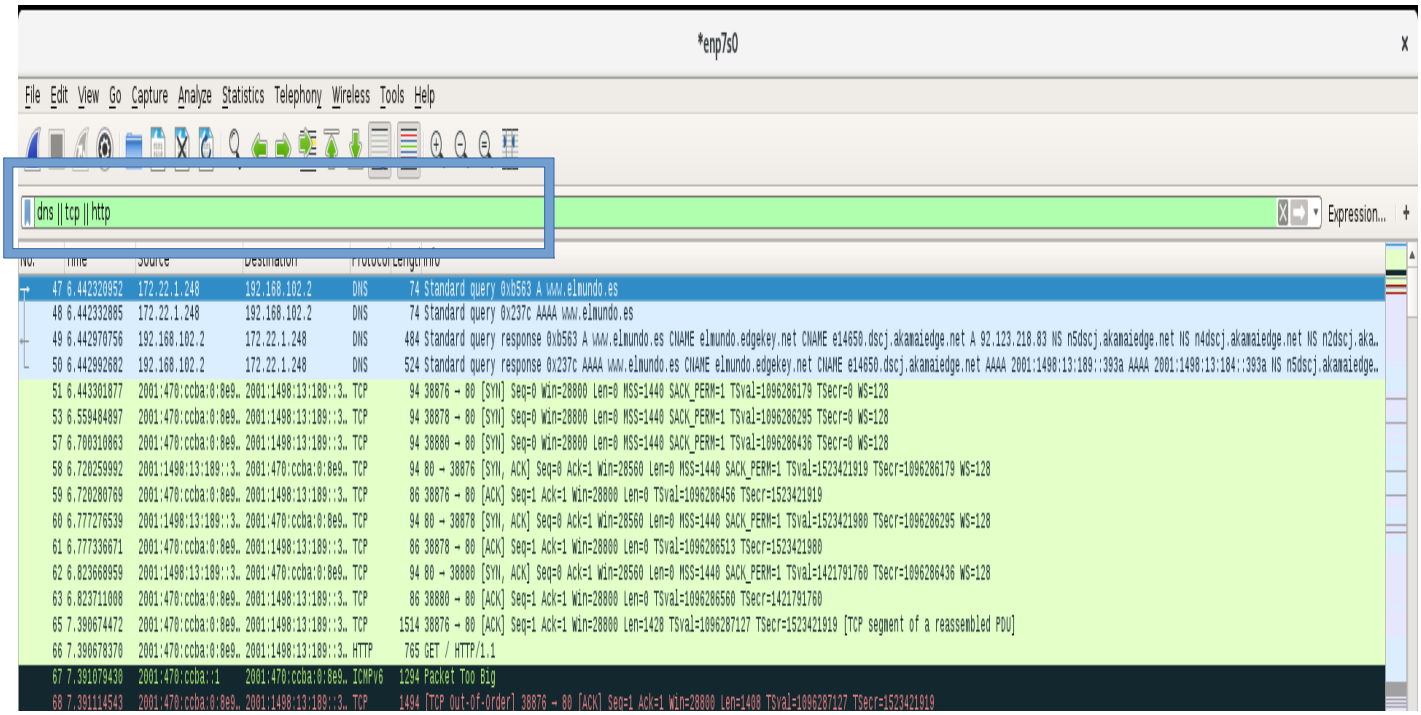




Seleccionamos la tarjeta de red y ya estará wireshark escuchando.



Filtramos por dns, tcp y http y ya tendrémos la captura lista.



El ejercicio se resolvería así:

El cuadrado azul representa el DNS hacia el servidor, el cuadrado amarillo representa la resolucion TCP, (SYN_ACK y ACK) y la verde representa la resolucion HTTP

4 Conclusión

Con esto hemos aprendido a utilizar wireshark y verificar que los servidores de marca y elmundo son los mismos.