*SNIFFER*

# **Objetivo**

Utilizar el lenguaje Python para capturar paquetes de los protocolos más usados en redes de computadores:

* Cabecera IP
  + Cabecera ICMP.
  + Cabecera UDP
    - Cabecera DNS
  + Cabecera TCP

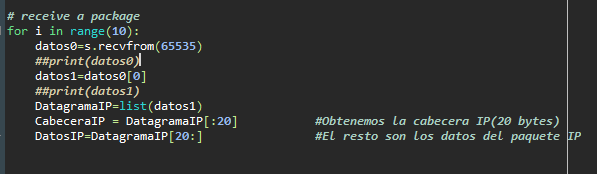
Como guión introductorio vamos a emplear el siguiente sniffer básico:



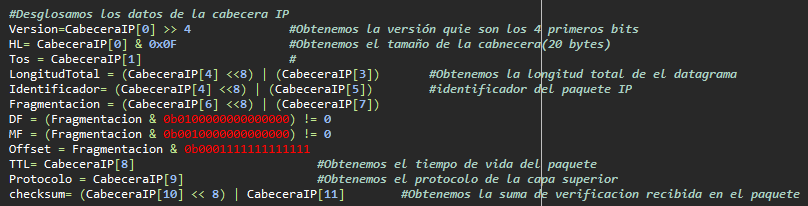
# **Sniffer**

## Obtención de la cabecera ip

Inicialmente capturamos paquetes con el sniffer básico anterior y después desglosamos la información obtenida en cada paquete, los 20 primeros paquetes son los correspondientes a la cabecera IP y el resto a los datos del datagrama.



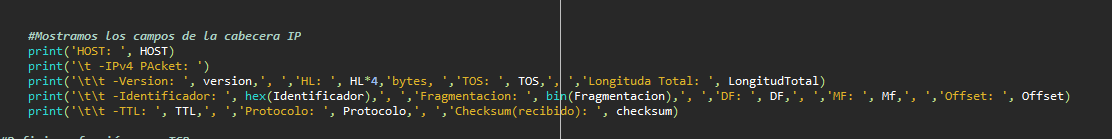
A continuación desglosamos la información obtenida en la cabecera IP:



Para diferenciar las distintas partes de la cabecera, contamos los tamaños en bytes.

Para el campo *versión* el cual ocupa los 4 primeros bits, cogemos *CabeceraIP[0]* y avanzamos 4 bits con *>>4*

Por último mostramos los campos del datagrama IP:



## Obtención de la cabecera TCP

La cabecera TCP se encontrará en los datos IP, si en el campo protocolo de la cabecera IP el valor es 6.

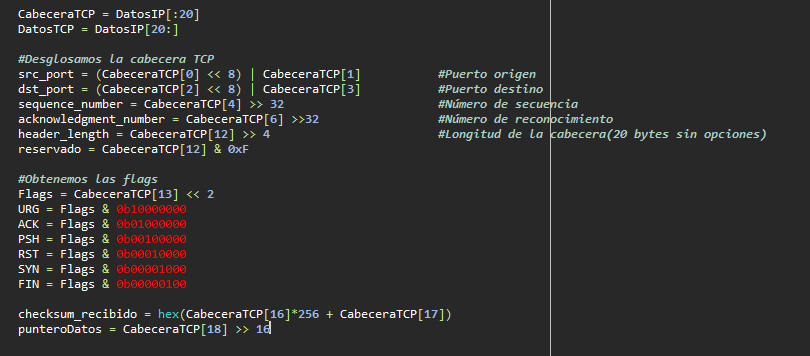
Como la cabecera TCP ocupa 20 bytes, cogemos los primeros 20 bytes de los datos IP:



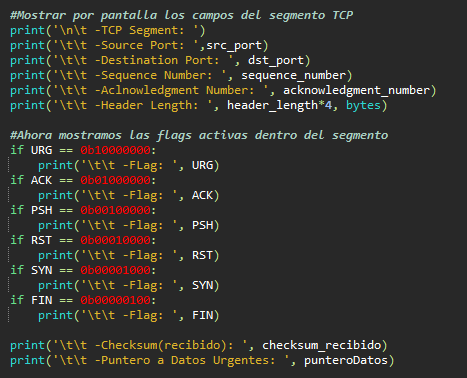
Para los datos TCP cogemos el resto de bytes de datos IP después de los 20 correspondientes a la cabecera TCP:



A continuación desglosamos los campos de la cabecera TCP al igual que hemos hecho antes con la IP.



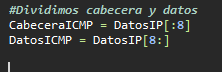
Una vez obtenidos los campos de la cabecera TCP toca mostrarlos por pantalla.



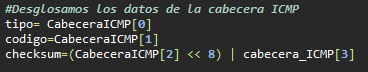
## Obtención de la cabecera ICMP

El mensaje ICMP aparece cuando en el campo protocolo de la cabecera IP hay como valor un 1, la cabecera ICMP ocupa 8 bytes.

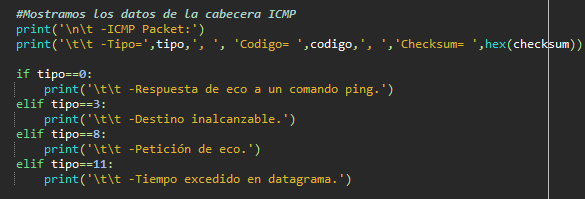
Para coger la cabecera haremos igual que con TCP, pero en este caso con 8 bytes:



A continuación desglosamos la cabecera ICMP:

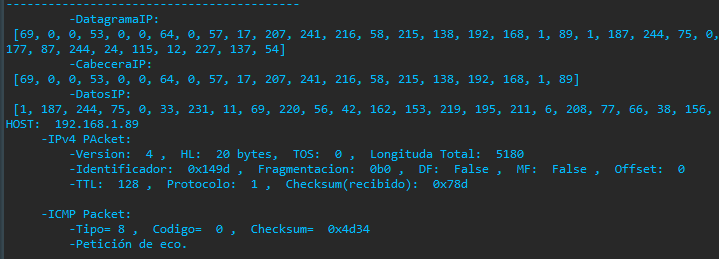


Por último mostramos por pantalla los datos de la cabecera ICMP:

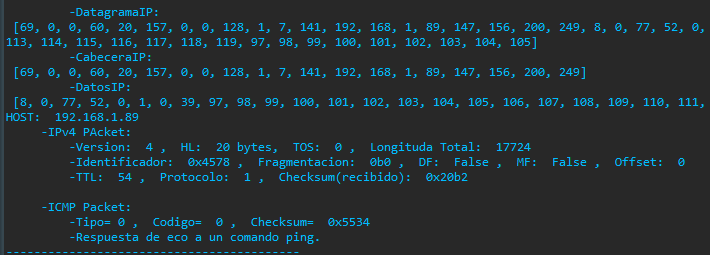


Sacar los datos de la cabecera resulta sencillo, sin embargo, esa información hay que tratarla como es el caso del campo tipo dentro de la cabecera ICMP, está representa el tipo de mensaje ICMP, si es 0 indica una respuesta de eco a un comando ping, si es 3 representa un error destino inalcanzable seguramente porque se ha acabado el tiempo de vida del mensaje, si es un 8 es un mensaje de petición de eco y por último si el campo tipo es un 11 error tiempo excedido en datagrama.

Captura de un paquete ICMP:



En este caso hemos capturado una petición de eco a [www.uv.es](http://www.uv.es) ya que si nos fijamos el campo tipo es 8.



Aquí está la respuesta al comando ping que hemos enviado a [www.uv.es](http://www.uv.es), vemos que campo tipo 0.

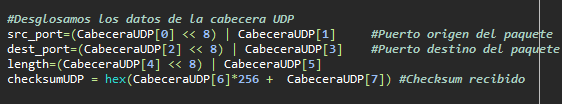
## Obtención de la cabecera UDP

La cabecera UDP ocupa 8 bytes de datos, entonces necesitamos los 8 primeros bytes de los datos IP:



Para los datos UDP cogemos a partir de los 8 bytes que ocupa la cabecera dentro de los datos IP hasta el final.

Después desglosamos la cabecera UDP:



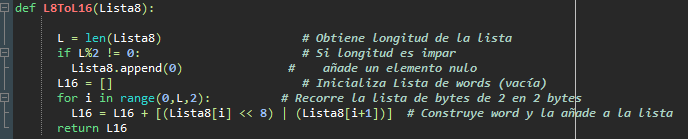
Para mensajes UDP comprobamos si el checksum recibido es correcto, primero construimos la pseudocabecera para el cálculo del checksum:



Luego borramos el checksum para que no forme parte del cálculo:

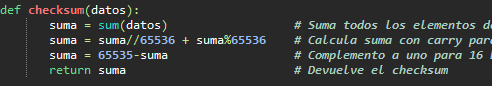


Ahora necesitamos pasar la lista de bytes a words, para ello utilizamos la siguiente función:

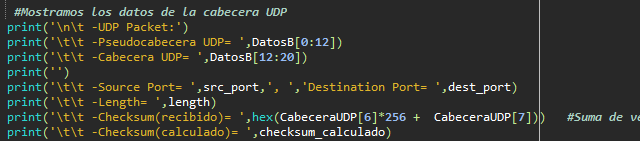


****

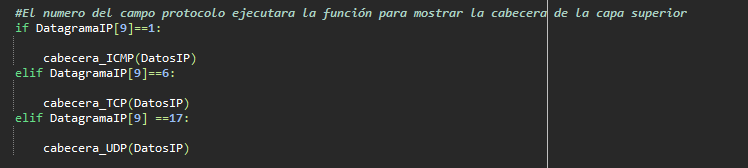
Por último solo queda el cálculo del checksum, usamos la siguiente función:



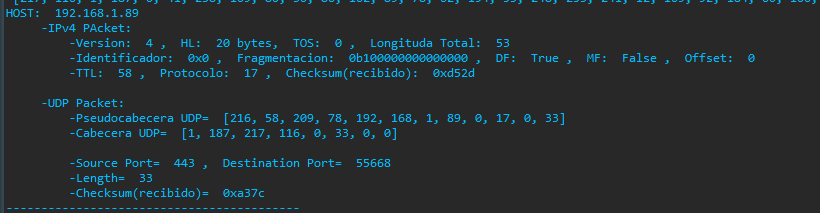
Después de desglosar la cabecera falta mostrarla por pantalla:



Para que el mensaje sea UDP el campo protocolo en la cabecera IP tiene que tener el valor 17, podemos deducir que de esta manera ejecutamos la función que trata la cabecera UDP:

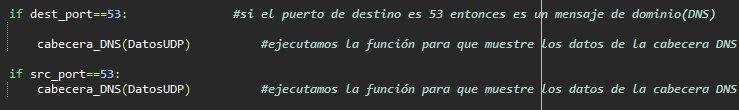


Paquetes UDP capturados:



## Obtención de la cabecera DNS

Los mensajes DNS o mensajes de dominio tienen una cabecera de 12 bytes y aparecen junto a los mensajes UDP, es fácil detectarlos ya que utilizan como puerto el número 53. Por lo tanto añadiremos el siguiente código dentro de la función UDP para detectar si es o no un mensaje dns:

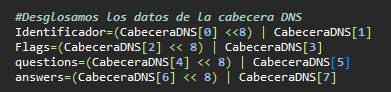


Como hemos hecho en todos los tipos de datagramas IP, lo primero desglosamos la cabecera:

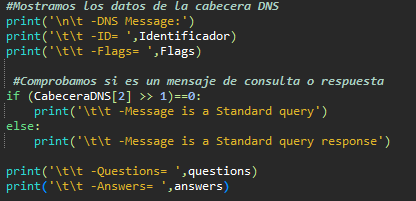


Diferenciamos entre la cabecera y los datos para mensajes DNS.

Después estructuramos los campos de la cabecera:

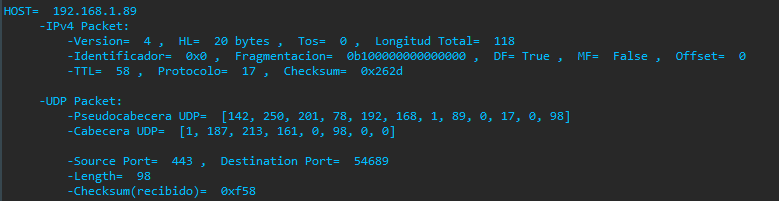


Mostramos los campos DNS por pantalla:

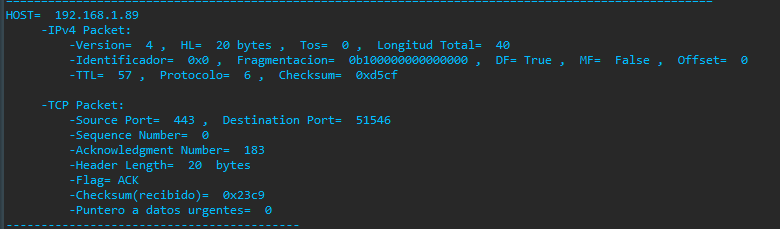


Para comprobar si es un mensaje de consulta o de respuesta nos fijamos en las flags que lleva dicho mensaje dns, si el campo QR está a 0 es un mensaje de consulta, en caso contrario indicamos que es un mensaje de respuesta.

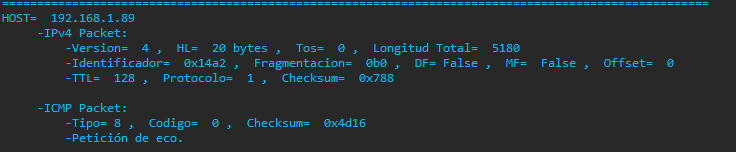
# **Memoria de pruebas**



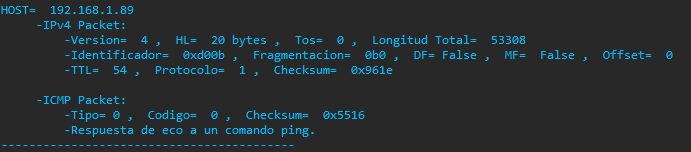
Datagrama IPv4 con mensaje UDP.



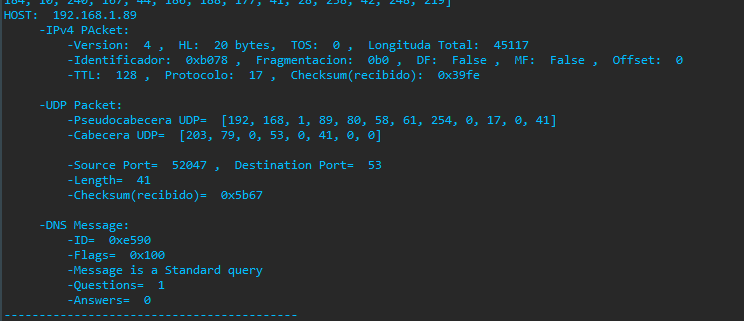
Segmento TCP.



Mensaje ICMP, petición de eco.



Mensaje ICMP, respuesta de eco a un comando ping.



Mensaje DNS de consulta.