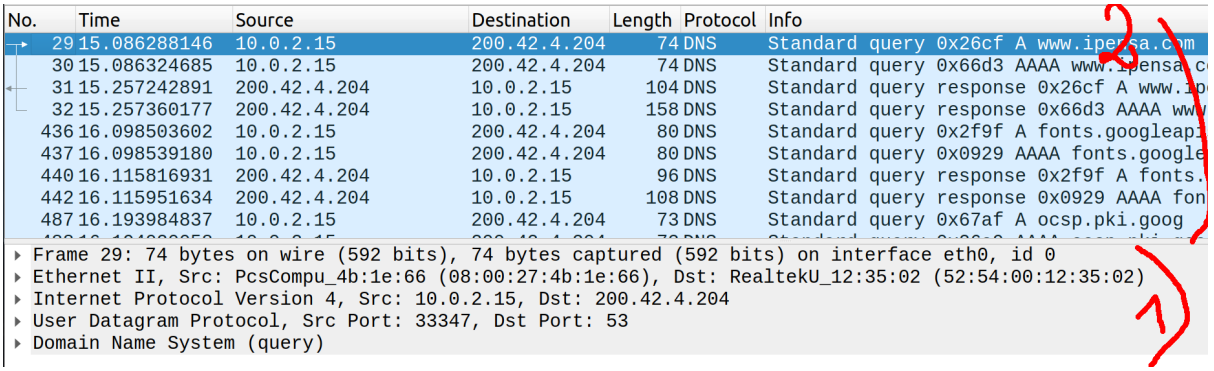
Actividades - Teoría introductoria

En esta actividad veremos una introducción de la funcionalidad de algunos protocolos a través de análisis de captura de tráfico utilizando la herramienta Wireshark.
Descargar e instalar wireshark[1] para realizar las siguientes actividades.

> ⚠ **Sobre los comandos utilizados en las actividades** ⚠
>
> *Se deja en aclaración que, todos los comandos enunciados en este documento tienen la sintaxis para sistemas operativos en **base Debian** (tales como Ubuntu, Debian, Kali, etc). De realizarlos en otras distribuciones recomendamos que busquen la sintaxis correcta para la misma.*
> *También se aclara que, el símbolo pesos al inicio de los comandos es para indicar que debe ejecutarse en una consola, en caso de copiar y pegar los comandos, no incluir el símbolo.*

1. Observemos la imagen de una captura de Wireshark, vamos a analizar la información que vemos:



A partir de la imagen responda las siguientes preguntas:

- ¿Cuántos paquetes se visualizan (cada paquete corresponde a una línea)?
- ¿A qué capa corresponde el protocolo que se ve en la columna “Protocol”?
- Al posicionarse en un paquete(en este caso estamos en la primera línea) en la sección (1) se puede observar la información por capa de dicho paquete, indique cuántas capas ve y cuál es el nombre de cada una.
- En las columnas “Source" y “Destination” podemos observar las direcciones IP de la computadora que envía (origen) y de la que recibe (destino). En los paquetes que se ven,
    - ¿Cuántas direcciones IPs diferentes hay?
    - ¿por qué aparecen en ambas columnas?
    - ¿En qué líneas es emisor y en cuáles es receptor?

[1] Sitio de descarga de Wireshark: https://www.wireshark.org/#download

- ¿Son direcciones IP públicas o privadas?

2. Dada la captura Practica1-act2-captura.pcapng, abrala con el programa Wireshark y realice las siguientes tareas, respondiendo las preguntas de esta sección:
    a. Los siguientes valores son dos filtros distintos. Responda las siguientes preguntas para cada uno de ellos, se deben aplicar en la sección “Filtros” de Wireshark:
        i. `(ip.src == 190.188.234.171 || ip.dst == 190.188.234.171)`
            A. ¿La comunicación está encriptada? En caso de que la respuesta sea no, analizar el flujo TCP. Indicar a qué servicio de capa de aplicación se está accediendo. ¿Qué información puede ver?
            B. ¿Qué protocolos de la capa de aplicación y de transporte están presentes en la comunicación?
            C. ¿A qué servicio corresponde la dirección IP pública interviniente? ¿Puede identificar la web a la que se accede?
            D. ¿Intervienen puertos? ¿Cuáles?
        ii. `(ip.src == 163.10.10.21 || ip.dst == 163.10.10.21)`
            A. ¿La comunicación está encriptada? En caso de que la respuesta sea sí, elegir el número de paquete 1775 para seguir el flujo TCP. Indicar a qué servicio de capa de aplicación se está accediendo. ¿Qué información puede ver?
            B. ¿Qué protocolos de la capa de aplicación y de transporte están presentes en la comunicación?
            C. ¿Puede encontrar algún indicador de la web a la que se accede?
            D. ¿Intervienen puertos? ¿Cuáles?
    b. Utilice el siguiente filtro `(ip.src == 8.8.8.8 || ip.dst == 8.8.8.8)` y responda:
        i. ¿Qué protocolo está presente en la columna “Protocol” ?
        ii. ¿Qué nos permite realizar este protocolo?
        iii. ¿A qué servicio corresponde la dirección IP pública interviniente?
        iv. ¿Identifica números de puertos? ¿Cuáles?
    c. ¿Cuáles son todos los protocolos que hay en la columna “Protocol” en la captura ?
3. Dada la captura Practica1-act3-captura.pcapng, observe:

a. ¿Qué protocolos se encuentran presentes en la columna “Protocol”?

b. Los datos de origen y destino de los paquetes, ¿son direcciones IP?¿la información que se encuentra a qué capa corresponde?

4. Realice una captura de tráfico local de la interfaz cableada y responda:

    a. ¿Qué protocolos se encuentran presentes en la columna “Protocol”?

    b. ¿A qué dispositivos corresponden las IP destino/origen?

5. Realice una captura de tráfico local de la interfaz cableada. Mientras realiza la captura ejecute el comando `ping 8.8.8.8`.

```
$ ping 8.8.8.8
```

    Luego analice:

    a. ¿Aparecen los paquetes en la captura?

    b. ¿Con qué funcionalidad se utiliza la herramienta ‘ping’?.