Práctica 1: Analizadores

Titulación:	Grado en Ingeniería Informática
Asignatura:	Redes de Computadores II
Alumnos:	Nombre y DNI
	Nombre y DNI

Introducción a los analizadores de red

1. **`Icmp`**. Utilizando *tcpdump* guarda una captura con nombre *ping.cap* con el tráfico que se genera al enviar un sólo *ping* desde tu equipo a informatica.usal.es.
    - Incluye en el informe la orden *ping* y *tcpdump* tecleadas y explica todo el tráfico implicado apoyándote en las imágenes de la captura del tráfico (utiliza *wireshark* para visualizarla) que consideres necesarias.
2. **`Arp.`** Usa *tcpdump* para guardar una captura con nombre *arp.cap* con el tráfico ARP (solo las preguntas).
    - Incluye en el informe la(s) orden(es) utilizadas para generar tráfico y la orden *tcpdump* tecleada e interpreta (apoyándote de las capturas de pantalla necesarias) porqué se produce el tráfico ARP observado (utiliza *wireshark* para visualizarla la captura realizada).
3. **`Dns.`** Usa tcpdump para guardar una captura con nombre *dns.cap* con el tráfico que se genera al resolver el nombre de dominio informatica.usal.es con la orden nslookup.
    - Incluye en el informe la orden nslookup y tcpdump tecleadas y explica todo el tráfico implicado apoyándote en las imágenes de la captura del tráfico (utiliza *wireshark* para visualizarla) que consideres necesarias.
4. **`Http, https, ftp.`** Usa *wireshark* para guardar una captura con nombre http.*cap* con el tráfico que se genera al visitar desde el navegador web las siguientes direcciones: http://informatica.usal.es, http://bddoc.csic.es:8080, https://moodle.usal.es, ftp://ftp.rediris.es.
    - Explica para cada una de las direcciones visitadas el tráfico implicado apoyándote en las imágenes de la captura del tráfico que consideres necesarias.
    - Especifica los filtros que podrías sobre la captura y muestra su correcto funcionamiento (capturas de pantalla y texto que las explique) para:
        - Ver el tráfico de DNS sabiendo que opera por el puerto 53
        - Ver todo el tráfico de la subred de los equipos del aula
        - Ver el tráfico de *broadcast* de la subred del aula
        - Suprimir el tráfico NetBIOS sabiendo que opera por los puertos 137, 138 y 139 pero desconocemos si UDP ó TCP