1. Abre con Wireshark el archivo lab_-01.pcap:
   a. Ve a *Edit → Configuration profiles* y crea un nuevo perfil llamado Boletin_n1.
   b. Verifica en la parte derecha de la barra de Estado que el perfil activo es Boletin_n1 y procede a borrar todos los Display filters y Coloring rules.
   c. ESTADÍSTICAS: Analiza la captura y responde:
      - Nº de equipos que a nivel de enlace intervienen en la captura.
      - Qué equipo a nivel de enlace es el más activo (indica nº total de paquetes, paquetes enviados y recibidos, total de Bytes, total de Bytes enviados y total de Bytes recibidos).
      - Repite el apartado anterior para el nivel de red, TCP y UDP.
      - Indica los elementos participantes de nivel de enlace, ip, tcp y udp, de la conversación más activa en cada nivel del TCP/IP.
      - Teniendo en cuenta la jerarquía de protocolos haz un dibujo del modelo TCP/IP usando los protocolos presentes en la captura.
   d. Haz los siguientes DISPLAY FILTERS:

Nombre	**Acción**
Broadcast	Ver únicamente tramas ethernet broadcast
Eth. origen PC1	Ver únicamente tramas ethernet enviadas por 00:11:d8:12:56:c4
Eth. destino PC2	Ver únicamente tramas ethernet destinadas a 00:30:da:ed:43:ad
Eth. PC3	Ver todas las tramas enviadas y recibidas por el equipo 01:00:5e:00:00:fb
Eth. PC2 ↔ PC3	Ver todas las tramas Ethernet intercambiadas entre 00:11:d8:12:56:c4 y 01:00:5e:00:00:fb
ARP	Ver todas las tramas ethernet que transportan paquetes ARP
ARP Request	Ver todos lo ARP Request
Eth. NO PC1	Ver todas las tramas ethernet donde no intervenga 00:11:d8:12:56:c4
IP origen 50.57.203.250	Ver los datagramas IP enviados por el equipo 50.57.203.250
IP destino 192.16.192.166	Ver los datagramas IP destinados al equipo 192.16.192.166
IP_101 ↔ IP_80.58.32.97	Ver los datagramas IP intercambiadas entre 192.168.0.101 y 80.58.32.97
IP_80.58.32.97	Ver los datagramas IP enviados y recibidos por 80.58.32.97
NO IP_80.58.32.97	Ver los datagramas IP donde no intervenga 80.58.32.97
ICMP	Ver todos los datagramas IP que transportan en el campo de datos mensajes ICMP
ICMP Echo Request	Ver todos los mensajes ICMP de tipo Echo Request
ICMP Tiempo Excedido	Ver todos los mensajes ICMP de tipo Tiempo Excedido
TTL 1	Ver todos los datagramas IP con TTL=1
TTL 6	Ver todos los datagramas IP con TTL<=6
ICMP IP_74 ↔ IP_1	Mensajes ICMP Echo Request y Reply intercambiados entre 74.125.230.210 y 192.168.0.1
DNS	Mensajes con origen el puerto por defecto asociado al servicio DNS
www.atareao.es	Mensajes destinados al puerto tcp 80 de la máquina 92.43.17.150
Atareao.es	Mensaje que contengan la palabra atareao.es
Atareao.es_js	Peticiones de archivos javascript (que acaben en .js)
FTP-Control	Mensajes FTP de control intercambiados entre 192.168.0.1 y 130.206.1.5

FTP-Data	Mensajes FTP de datos intercambiados entre 192.168.0.1 y 130.206.1.5

e. Crea, siguiendo el orden indicado, las siguientes reglas de coloreado:

Nombre	**Acción**
ARP	Colorear todas las tramas ethernet que transportan paquetes ARP
Errores ICMP	Colorear todos los mensajes ICMP de error (destino inalcanzable, tiempo excedido, redirect y source quench)
ICMP	Colorear todos los mensajes ICMP
TTL	Colorear los paquetes con un tiempo de vida inferior a 10

f. GRÁFICOS: Haz un gráfico donde se vea a la vez la evolución temporal del tráfico de los protocolo http, ftp y dns de la captura .

g. GeoIP: Instala y activa las librerías necesarias para tener Geolocalización en Wireshark e indica el filter string para ver únicamente los paquetes enviados desde España

Trama Ethernet II

8 bytes	6 bytes	6 bytes	2 bytes	0-1500 bytes	0-46 bytes	4 bytes
Preámbulo	Dirección MAC destino	Dirección MAC origen	Ethertype	Datos	Relleno	FCS

Trama IEEE 802.3

7 bytes	1 byte	2 ó 6 bytes	2 ó 6 bytes	2 bytes	0-1500 bytes	0-46 bytes	4 bytes
Preámbulo	Delimitador Inicio	MAC destino	MAC origen	Longitud	Datos	Relleno	FCS