Desactivar cortafuegos: "Iniciar" > "Panel de control" > "Firewall de Windows" > "Desactivar Firewall de Windows"

Desactivar servicios de red: "Conexión de red" > "Abrir Centro de redes y recursos compartidos" > "Conexión de área local" > "Propiedades" en menú contextual. Desactivar "Cliente para redes Microsoft", "Compartir impresoras y archivos para redes Microsoft" y "Programador de paquetes QoS".

Modificar configuración del navegador Mozilla Firefox: escriba "about:config" en la barra de direcciones, acepte el "aviso para manazas" y verá una ventana de configuración avanzada. Use como filtro de búsqueda (debajo de la barra de direcciones) la frase que corresponda; por ejemplo escribir "retry-timeout" si se quiere configurar "network.http.connection-retry-timeout" o "persistent" para "network.http.max-persistent-connections-per-server". Para restaurar el valor de las preferencias modificadas usando la ventana "about:config" hacer "clic" con el botón derecho en cada preferencia y seleccionando "Restablecer".

Limpiar caché del navegador Mozilla Firefox: CTRL+Mayúsculas+Suprimir y clic en el botón "Limpiar ahora".

ipconfig

/all	Visualizar la configuración TCP/IP del host.
/renew	Renovar la configuración TCP/IP v4 del host (vía DHCP).
/release	Liberar la configuración TCP/IPv4 del host.
/displaydns	Visualizar la caché DNS del host.
/flushdns	Borrar la caché DNS del host.
/registerdns	Actualiza todas las concesiones DHCP y vuelve a registrar los nombres DNS.

ping

Realiza prueba de conectividad hasta nivel de Red mediante el protocolo ICMP.
Uso: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS] [-r count] [-s count] [[-j host-list] | [-k host-list]] [-w timeout] [-R] [-S srcaddr] [-c compartment] [-p] [-4] [-6] nombre_destino

-t	Hacer ping al host especificado hasta que se detenga. Para ver estadísticas y continuar, presione Ctrl-Interrumpir; para detener, presione Ctrl+C.
-a	Resolver direcciones en nombres de host.
-n count	Número de solicitudes de eco para enviar.
-l size	Enviar tamaño de búfer.
-f	Establecer marca No fragmentar en paquetes (solo IPv4).
-i TTL	Periodo de vida.
-v TOS	Tipo de servicio (solo IPv4. Esta opción está desusada y no tiene ningún efecto sobre el campo de tipo de servicio del encabezado IP).
-r count	Registrar la ruta de saltos de cuenta (solo IPv4).
-s count	Marca de tiempo de saltos de cuenta (solo IPv4).
-j host-list	Ruta de origen no estricta para lista-host (solo IPv4).
-k host-list	Ruta de origen estricta para lista-host (solo IPv4).
-w timeout	Tiempo de espera en milisegundos para cada respuesta.
-R	Usar encabezado de enrutamiento para probar también la ruta inversa (solo IPv6). Por RFC 5095 el uso de este encabezado de enrutamiento ha quedado en desuso. Es posible que algunos sistemas anulen solicitudes de eco si usa este encabezado.
-S srcaddr	Dirección de origen que se desea usar.
-c compartment	Enrutamiento del identificador del compartimiento.
-p	Hacer ping a la dirección del proveedor de Virtualización de red de Hyper-V.
-4	Forzar el uso de IPv4.
-6	Forzar el uso de IPv6.

tracert

Muestra la ruta de las PDUs ICMP.
Uso: tracert [-d] [-h saltos_máximos] [-j lista_de_hosts] [-w tiempo_de_espera] [-R] [-S srcaddr] [-4] [-6] nombre_dest

-d	No convierte direcciones en nombres de hosts.
-h saltos_max	Máxima cantidad de saltos en la búsqueda del objetivo.
-j lista-host	Enrutamiento relajado de origen a lo largo de la lista de hosts (solo IPv4).
-w tiempo_espera	Tiempo de espera en milisegundos para esperar cada respuesta.
-R	Seguir la ruta de retorno (solo IPv6).
-S srcaddr	Dirección de origen para utilizar (solo IPv6).
-4	Forzar el uso de IPv4.
-6	Forzar el uso de IPv6.

route

Muestra o administra la tabla de enrutamiento del host.

Uso: route [-f] [-p] [-4|-6] comando [destino] [MASK máscara_red] [puerta_enlace] [METRIC métrica] [IF interfaz]

-f	Borra las tablas de enrutamiento de todas las entradas de puerta de enlace. Si se usa junto con uno de los comandos, se borrarán las tablas antes de ejecutarse el comando.
-p	Cuando se usa con el comando ADD, hace una ruta persistente en los arranques del sistema. De manera predeterminada, las rutas no se conservan cuando se reinicia el sistema. Se pasa por alto para todos los demás comandos, que siempre afectan a las rutas persistentes apropiadas.
-4	Forzar el uso de IPv4.
-6	Forzar el uso de IPv6.
comando	Alguno de los siguientes: PRINT Imprime una ruta. Ej: *route PRINT* ADD Agrega una ruta. Ej: *route ADD 157.0.0.0 MASK 255.0.0.0 157.55.80.1 METRIC 3 IF 2* DELETE Elimina una ruta. Ej: *route DELETE 157.0.0.0* CHANGE Modifica una ruta existente. Ej: *route CHANGE 157.0.0.0 MASK 255.0.0.0 157.55.80.5 METRIC 2 IF 2*
destino	Especifica el host.
MASK	Especifica que el siguiente parámetro es el valor de 'máscara_red'. 'máscara_red' especifica un valor de máscara de subred para esta entrada de ruta. Si no se especifica, se usa de forma predeterminada el valor 255.255.255.255.
puerta_enlace	Especifica la puerta de enlace.
IF interfaz	El número de interfaz para la ruta especificada.
METRIC métrica	Especifica la métrica; por ejemplo, costo para el destino.

Nota: Las modificaciones de la tabla de enrutamiento requieren ejecutar el comando en una ventana de Símbolo del sistema abierta en **modo administrador**.

arp

Muestra y modifica las tablas de conversión de direcciones IP en direcciones físicas que utiliza el protocolo de resolución de direcciones (ARP).

ARP -s inet_addr eth_addr [if_addr]

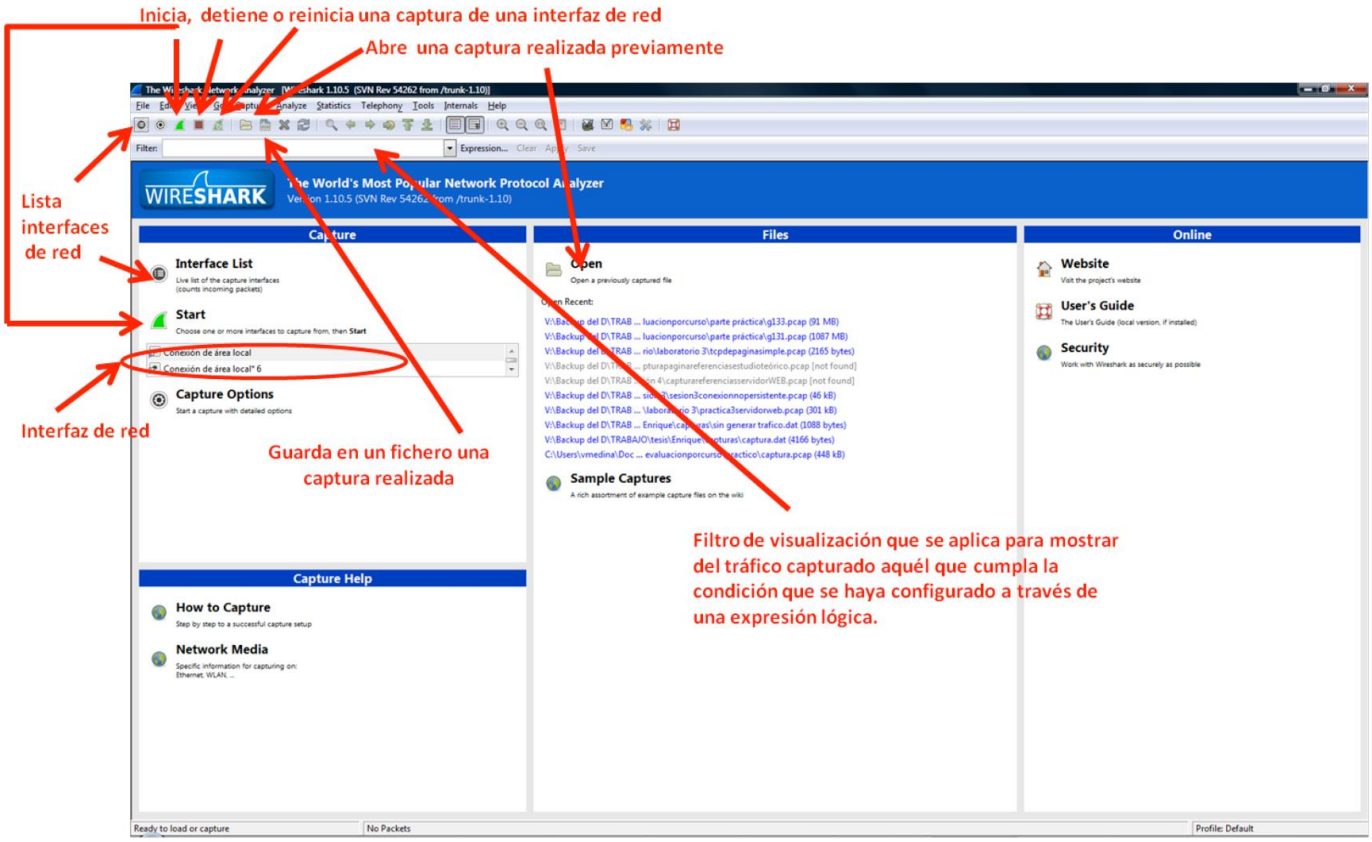
ARP -d inet_addr [if_addr]

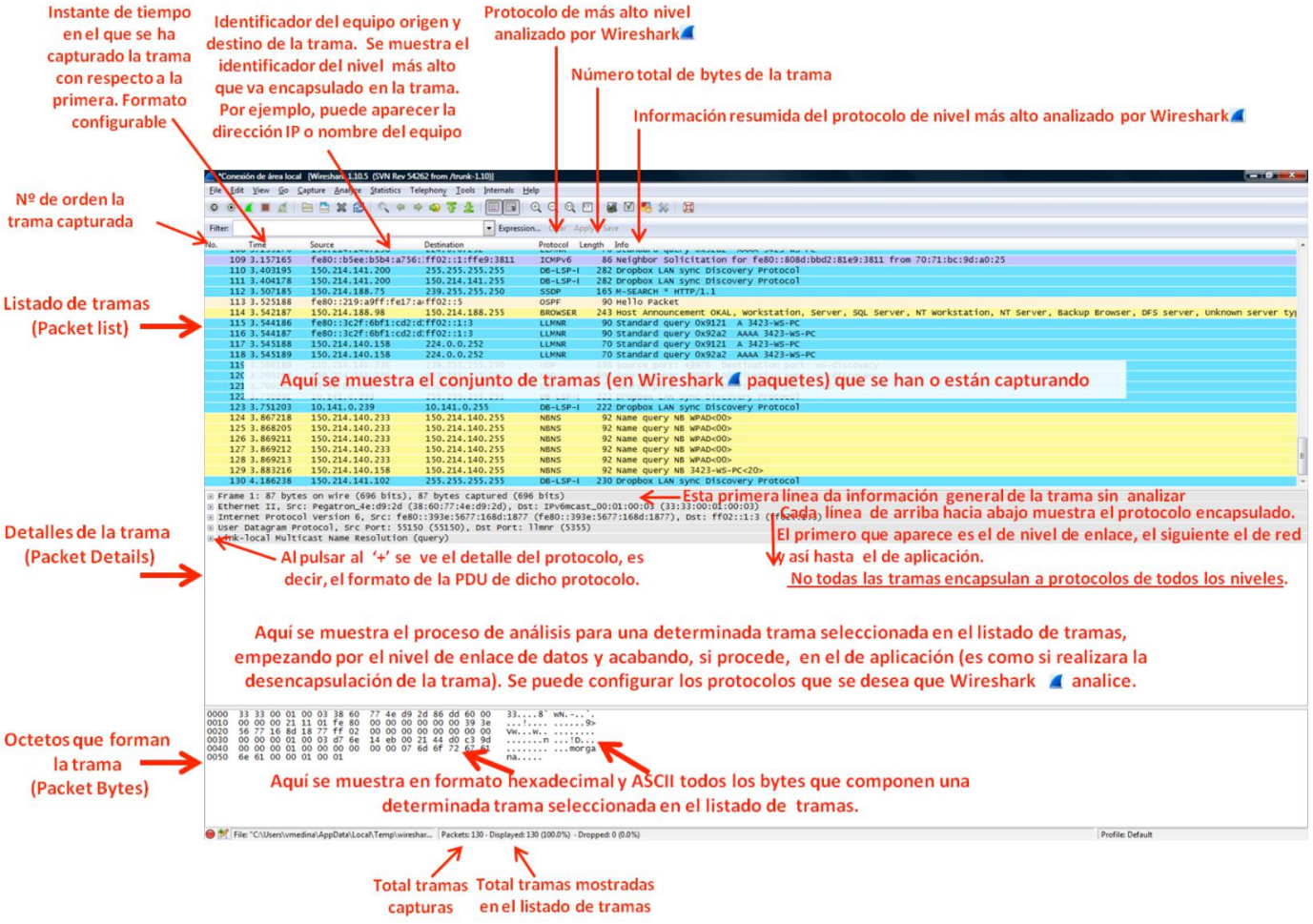
ARP -a [inet_addr] [-N if_addr] [-v]

-a	Pide los datos de protocolo actuales y muestra las entradas ARP actuales. Si se especifica inet_addr, solo se muestran las direcciones IP y física del equipo especificado. Si existe más de una interfaz de red que utilice ARP, se muestran las entradas de cada tabla ARP. Ej: > *arp -a*
-v	Muestra las entradas actuales de ARP en modo detallado. Se mostrarán todas las entradas no válidas y las entradas en la interfaz de bucle invertido.
inet_addr	Especifica una dirección de Internet.
-N if_addr	Muestra las entradas ARP para la interfaz de red especificada por if_addr.
-d	Elimina el host especificado por inet_addr. inet_addr puede incluir el carácter comodín * (asterisco) para eliminar todos los hosts.
-s	Agrega el host y asocia la dirección de Internet inet_addr con la dirección física eth_addr. La dirección física se indica como 6 bytes en formato hexadecimal, separados por guiones. La entrada es permanente. Ej: > *arp -s 157.55.85.212 00-aa-00-62-c6-09*
eth_addr	Especifica una dirección física.
if_addr	Si está presente, especifica la dirección de Internet de la interfaz para la que se debe modificar la tabla de conversión de direcciones. Si no está presente, se utilizará la primera interfaz aplicable.

Nota: Las modificaciones de la caché ARP requieren ejecutar el comando en una ventana de Símbolo del sistema abierta en **modo administrador**.

WIRESHARK


Inicia, detiene o reinicia una captura de una interfaz de red
Abre una captura realizada previamente
Lista interfaces de red
Interfaz de red
Guarda en un fichero una captura realizada
Filtro de visualización que se aplica para mostrar del tráfico capturado aquél que cumpla la condición que se haya configurado a través de una expresión lógica.
Capture
Interface List
Start
Capture Options
Files
Open
Sample Captures
Online
Website
User's Guide
Security
Capture Help
How to Capture
Network Media


Instante de tiempo en el que se ha capturado la trama con respecto a la primera. Formato configurable
Identificador del equipo origen y destino de la trama. Se muestra el identificador del nivel más alto que va encapsulado en la trama. Por ejemplo, puede aparecer la dirección IP o nombre del equipo
Protocolo de más alto nivel analizado por Wireshark
Número total de bytes de la trama
Información resumida del protocolo de nivel más alto analizado por Wireshark
Nº de orden la trama capturada
Listado de tramas (Packet list)
Aquí se muestra el conjunto de tramas (en Wireshark paquetes) que se han o están capturando
Esta primera línea da información general de la trama sin analizar
Cada línea de arriba hacia abajo muestra el protocolo encapsulado. El primero que aparece es el de nivel de enlace, el siguiente el de red y así hasta el de aplicación.
No todas las tramas encapsulan a protocolos de todos los niveles.
Detalles de la trama (Packet Details)
Al pulsar al '+' se ve el detalle del protocolo, es decir, el formato de la PDU de dicho protocolo.
Aquí se muestra el proceso de análisis para una determinada trama seleccionada en el listado de tramas, empezando por el nivel de enlace de datos y acabando, si procede, en el de aplicación (es como si realizara la desencapsulación de la trama). Se puede configurar los protocolos que se desea que Wireshark analice.
Octetos que forman la trama (Packet Bytes)
Aquí se muestra en formato hexadecimal y ASCII todos los bytes que componen una determinada trama seleccionada en el listado de tramas.
Total tramas capturas
Total tramas mostradas en el listado de tramas

Crear una nueva columna: "Edit" → "Preferences" > Clic "Columns" ("User Interface" en panel izquierdo) > Clic "Add" para añadir una nueva columna > Clic "New column" > editar nombre columna + "Intro" en el teclado > Seleccionar en "Field Type" el valor que corresponda.

Poner una PDU como referencia: Seleccionar la PDU a marcar como referencia > Clic derecho > "Set Time Reference (Toggle)".

Seguimiento de un diálogo (TCP o UDP): Seleccionar una PDU del dialógo > Clic derecho > "Follow TCP Stream" o "Follow UDP Stream".

Deshabilitar en Wireshark el análisis de los protocolos TCP y UDP (y los protocolos encapsulados dentro de ellos): MAYÚSCULAS+CTRL+E

Filtros de visualización en Wireshark:
Ejemplos básicos:

- "ip.addr == 193.1.10.1", que muestra tramas que contienen R_PDUs cuya dirección IP origen o destino sea la 193.1.10.1.
- "tcp.port == 80", para mostrar el tráfico con numero de puerto origen o destino el 80.
- "udp.port == 53", que hace lo mismo pero con UDP.
- "ip.src" y "ip.dst" son parecidos a "ip.addr" pero solo se fijan en que la IP especificada este en el origen o en el destino.
- "tcp.dstport" y "tcp.srcport" se fijan solamente en el puerto destino o el origen.
- "http", "dns", "tcp", "udp" y "icmp" son expresiones sencillas que hacen que solo se muestren tramas que encapsulen PDUs de esos protocolos.
- Es posible construir expresiones lógicas complejas combinando expresiones sencillas con los operadores lógicos "and", "or" y "not". Por ejemplo "http or dns" captura tramas que hacen que la expresión lógica "combinada" sea cierta. Es decir, aquellas que hacen que "http" sea cierta y también aquellas que hacen que "dns" sea cierta. También es posible utilizar el operador "contains" que permite buscar cadenas dentro de la PDU de un protocolo, por ejemplo, "http contains GET" permitiría ver todas las tramas que encapsulan PDUs HTTP que contienen la palabra "GET". Otro ejemplo con este operador sería "dns contains www" que nos dejaría ver solo las tramas con PDUs DNS en las que aparezca la cadena "www".
- tcp.len>0, muestra las PDUs que contienen TCP con el campo length mayor de cero.
- tcp.flags.syn==1, muestra las PDUs que contienen TCP y cuya cabecera tiene el bit SYN activo.
- eth.src == DIR_MAC, muestra las PDUs que contienen DIR_MAC en su cabecera Ethernet.
- not (eth.dst == ff:ff:ff:ff:ff:ff), muestra las PDUs cuya dirección MAC destino no sea tráfico broadcast.

Ejemplos avanzados:

- ((dns.qry.type==1 and dns contains lab) or tcp.port==80) and ip.addr==193.1.2.124, muestra tramas que contienen o bien solicitudes DNS preguntando por la una dirección IP versión 4 de aquellos hosts que contengan en su nombre de dominio la palabra “lab” o bien contiene TCP con el puerto 80, y que, al mismo tiempo, contiene la dirección IP 193.1.2.124.
- ((dns.qry.type==1 and dns contains webserver) or (tcp.port==80 and ip.addr==192.10.1.13)) and ip.addr==193.1.2.124, igual que el filtro anterior, pero además especifica la dirección IP del servidor web (192.10.1.13).
- (arp and eth.addr == DIR_MAC_PC_ALUMNO) or (icmp and ip.addr == DIR_IP_PC_ALUMNO), muestra el tráfico ARP con su dirección MAC en el campo MAC origen o MAC destino de las MAC_PDUs y también visualiza el tráfico ICMP con IP origen o destino la de su PC.