IFCT0109. SEGURIDAD INFORMÁTICA

MF0487_3 AUDITORÍA DE SEGURIDAD INFORMÁTICA

UD04

ANEXO. HERRAMIENTA WIRESHARK

DOCENTE: BENITO MANUEL GONZÁLEZ RODRÍGUEZ

WIRESHARK

¿QUE ES WIRESHARK?

WIRESHARK ES UN ANALIZADOR DE PROTOCOLOS OPEN-SOURCE QUE ACTUALMENTE ESTÁ DISPONIBLE PARA PLATAFORMAS WINDOWS Y UNIX.

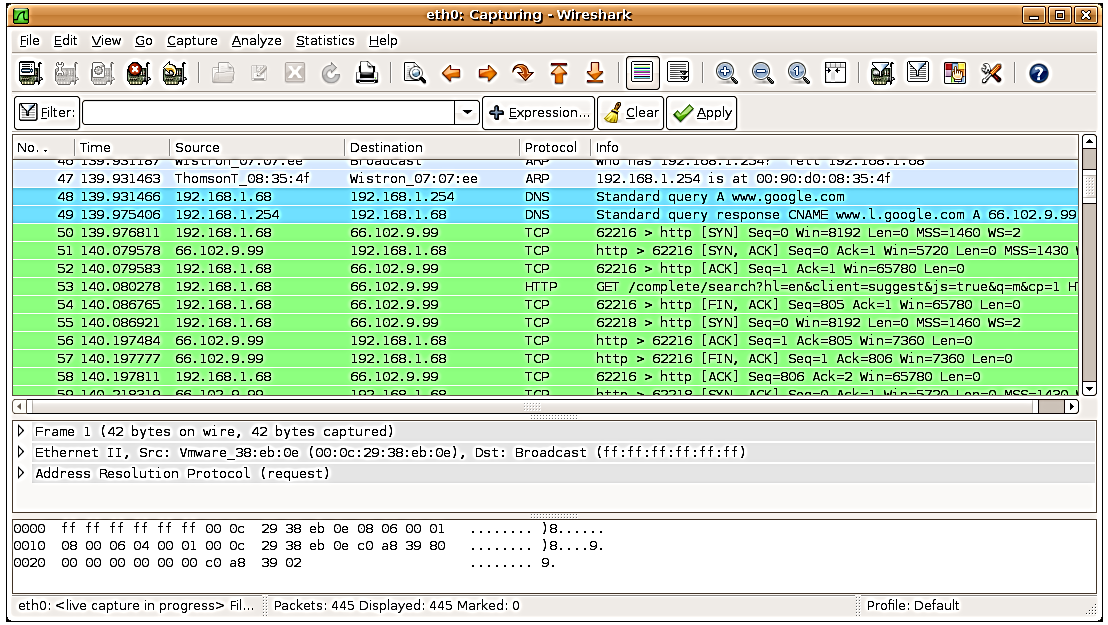
SU PRINCIPAL **OBJETIVO** ES EL ANÁLISIS DE TRÁFICO, PERO ADEMÁS ES UNA EXCELENTE APLICACIÓN DIDÁCTICA PARA EL ESTUDIO DE LAS COMUNICACIONES Y PARA LA RESOLUCIÓN DE PROBLEMAS DE RED.

NO TIENE LA CAPACIDAD DE CAPTURAR PAQUETES DE LA RED, SINO QUE SE APOYA EN MOTORES DE CAPTURA COMO **LIBPCAP** EN UNIX/LINUS Y NPCAP EN WINDOWS

WIRESHARK

¿QUE ES WIRESHARK?

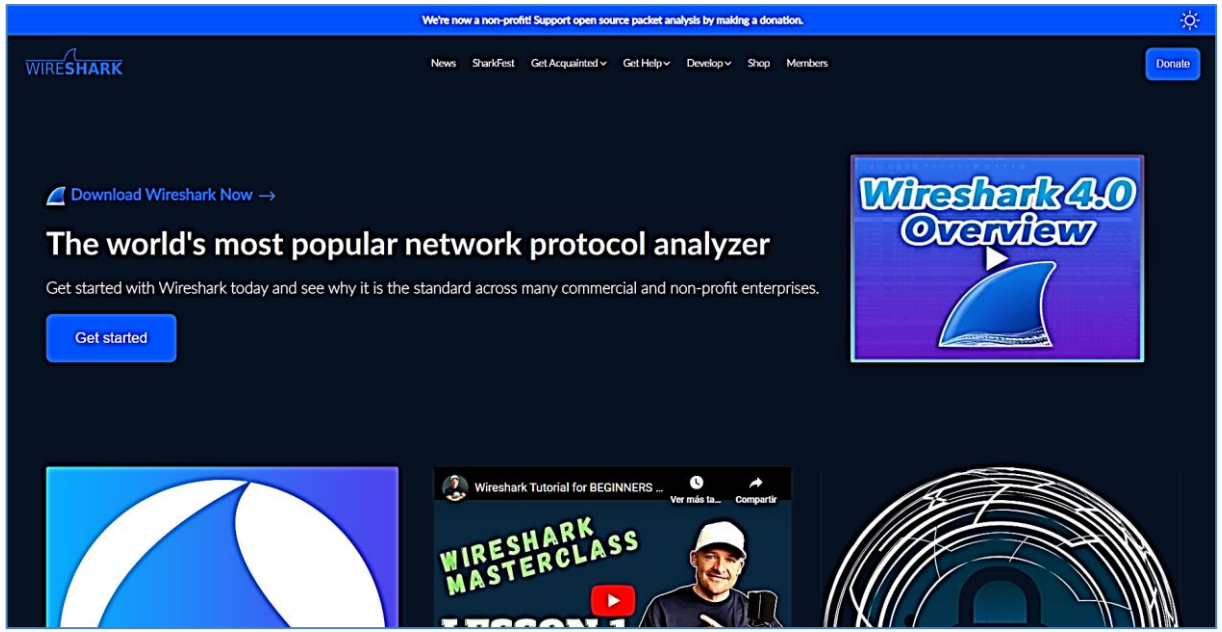
IMPLEMENTA UNA AMPLIA GAMA DE **FILTROS** QUE FACILITAN LA DEFINICIÓN DE CRITERIOS DE BÚSQUEDA PARA LOS MÁS DE 1100 PROTOCOLOS SOPORTADOS ACTUALMENTE Y TODO ELLO POR MEDIO DE UNA INTERFAZ SENCILLA E INTUITIVA QUE PERMITE DESGLOSAR POR CAPAS CADA UNO DE LOS PAQUETES CAPTURADOS.

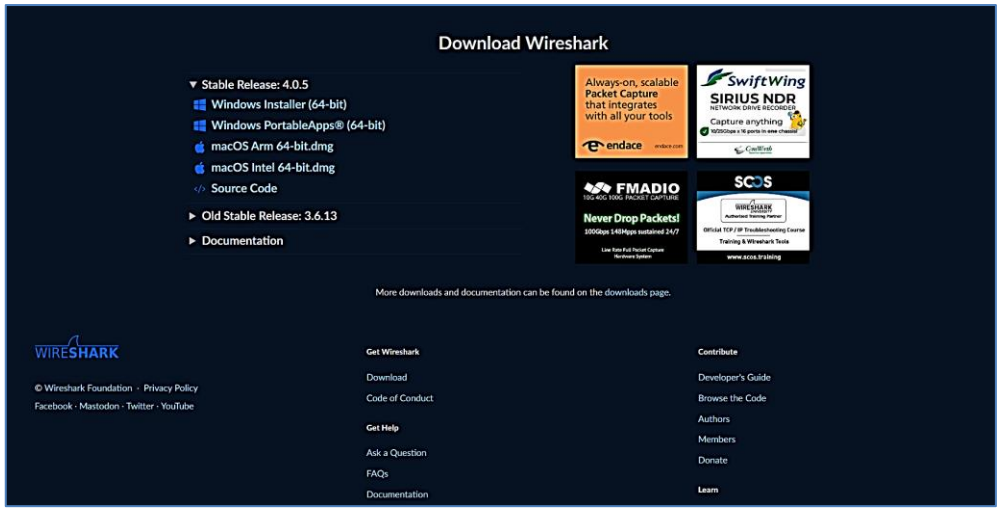


WIRESHARK

DESCARGA E INSTALACIÓN:

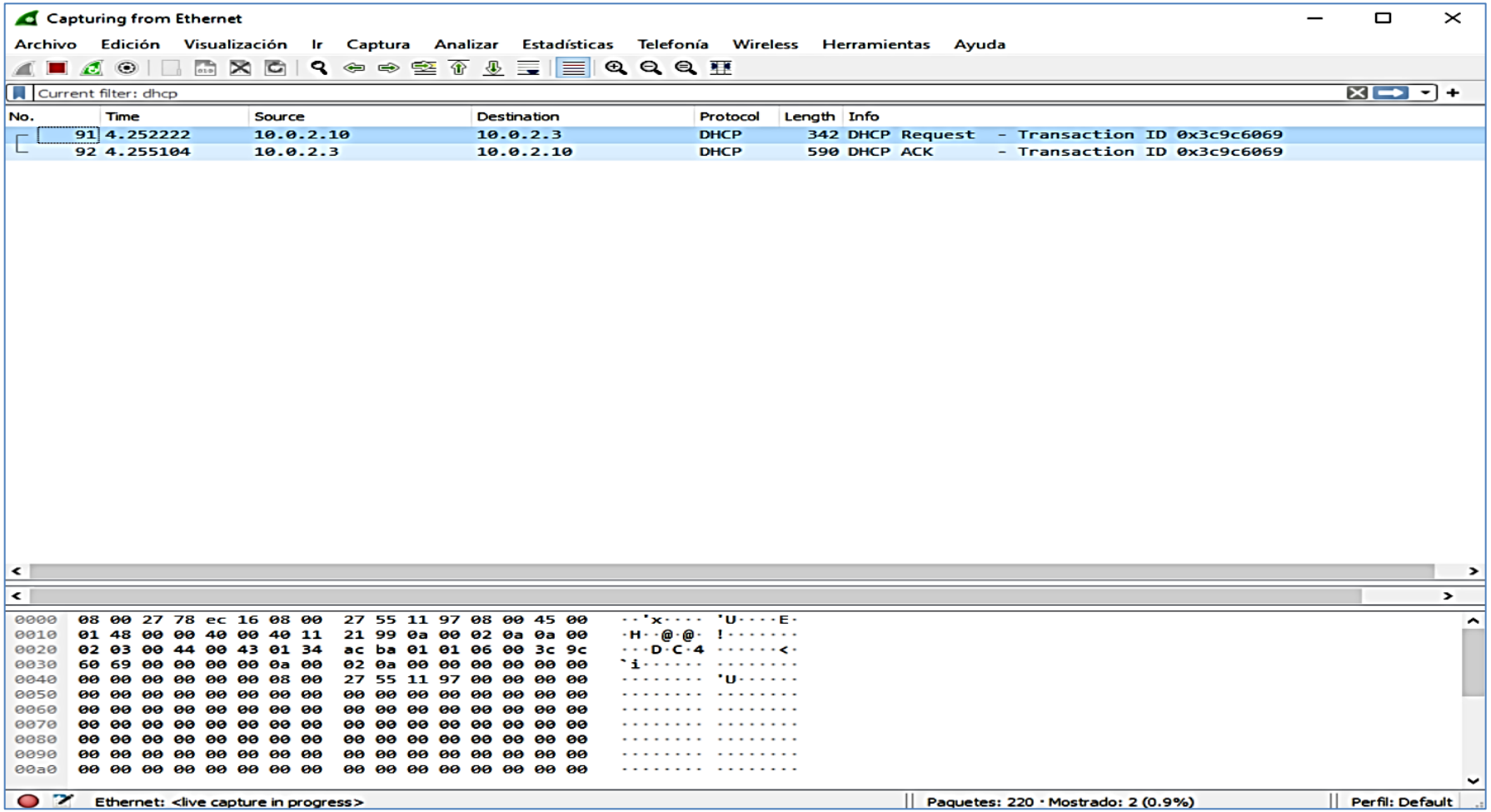
HTTPS://WWW.WIRESHARK.ORG/





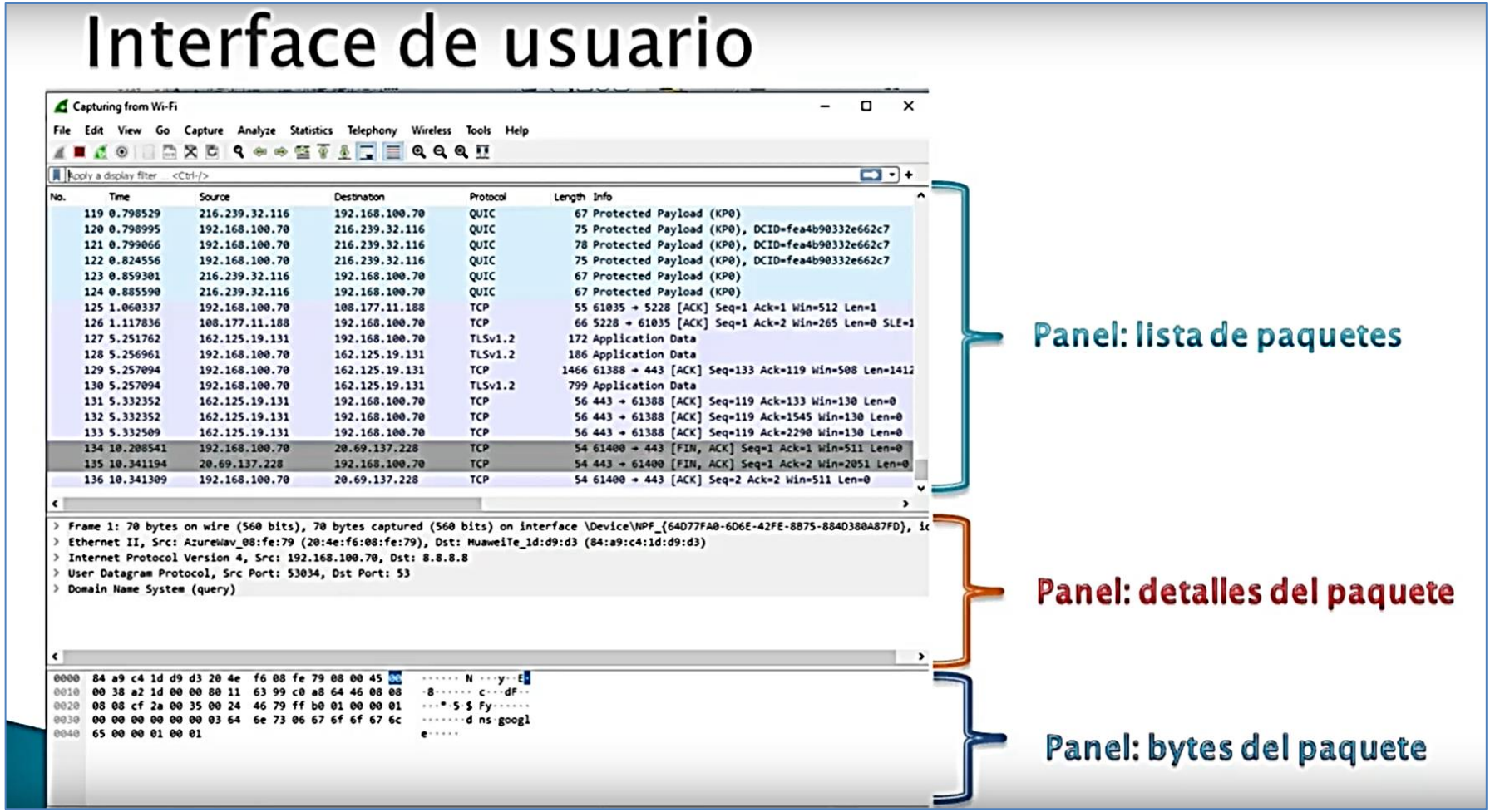
WIRESHARK

CAPTURA DE PAQUETES



WIRESHARK

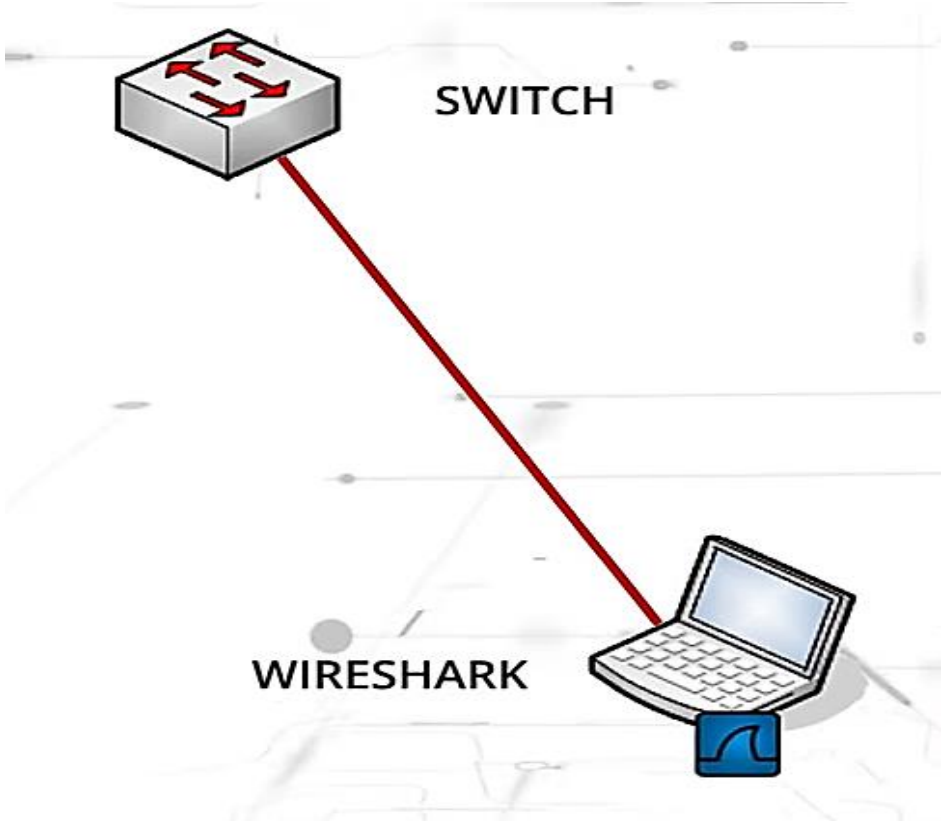
CAPTURA DE PAQUETES



WIRESHARK

CAPTURA DE PAQUETES

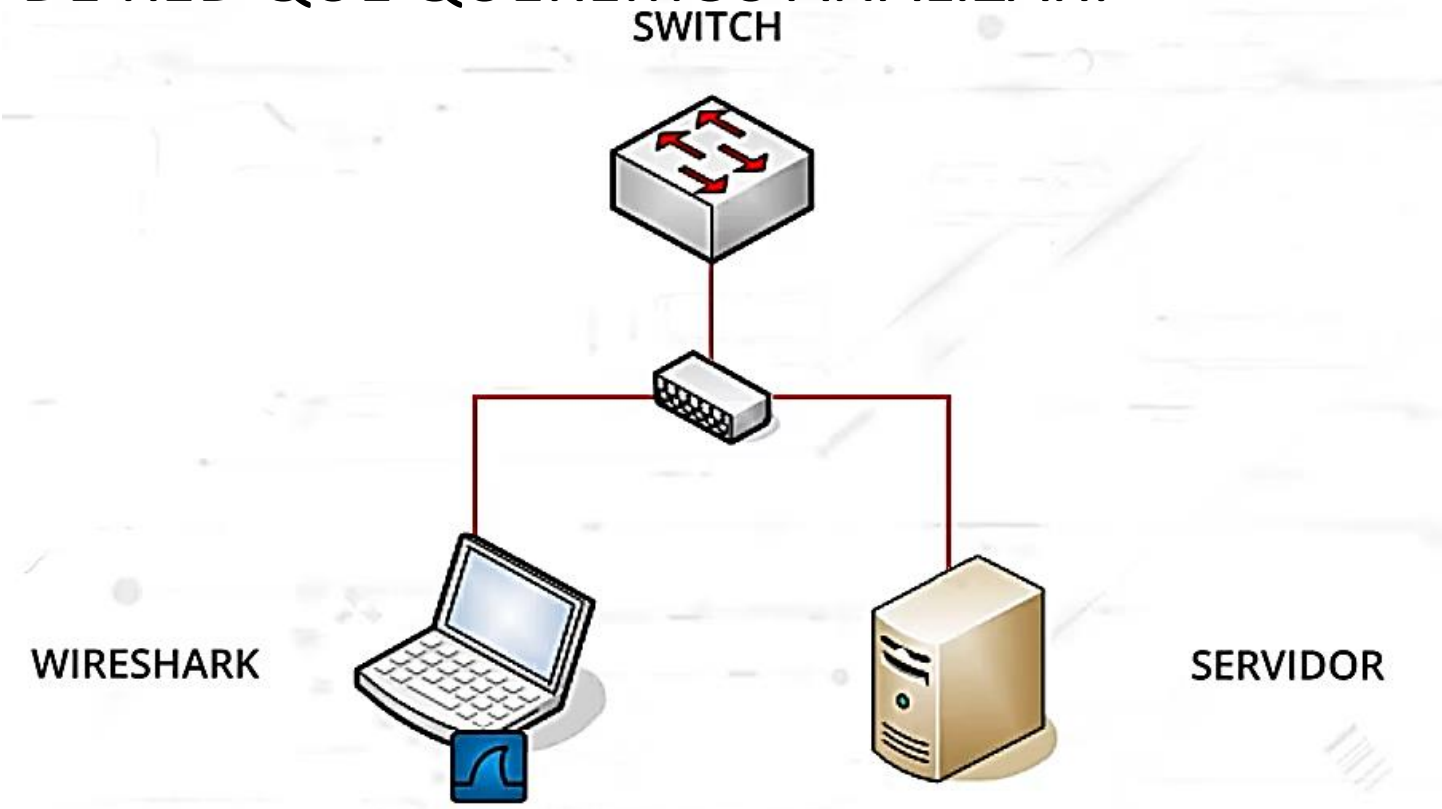
UN SWITCH VA A MOSTRAR SOLAMENTE EL TRÁFICO DIRIGIDO A NUESTRA MÁQUINA:



WIRESHARK

CAPTURA DE PAQUETES

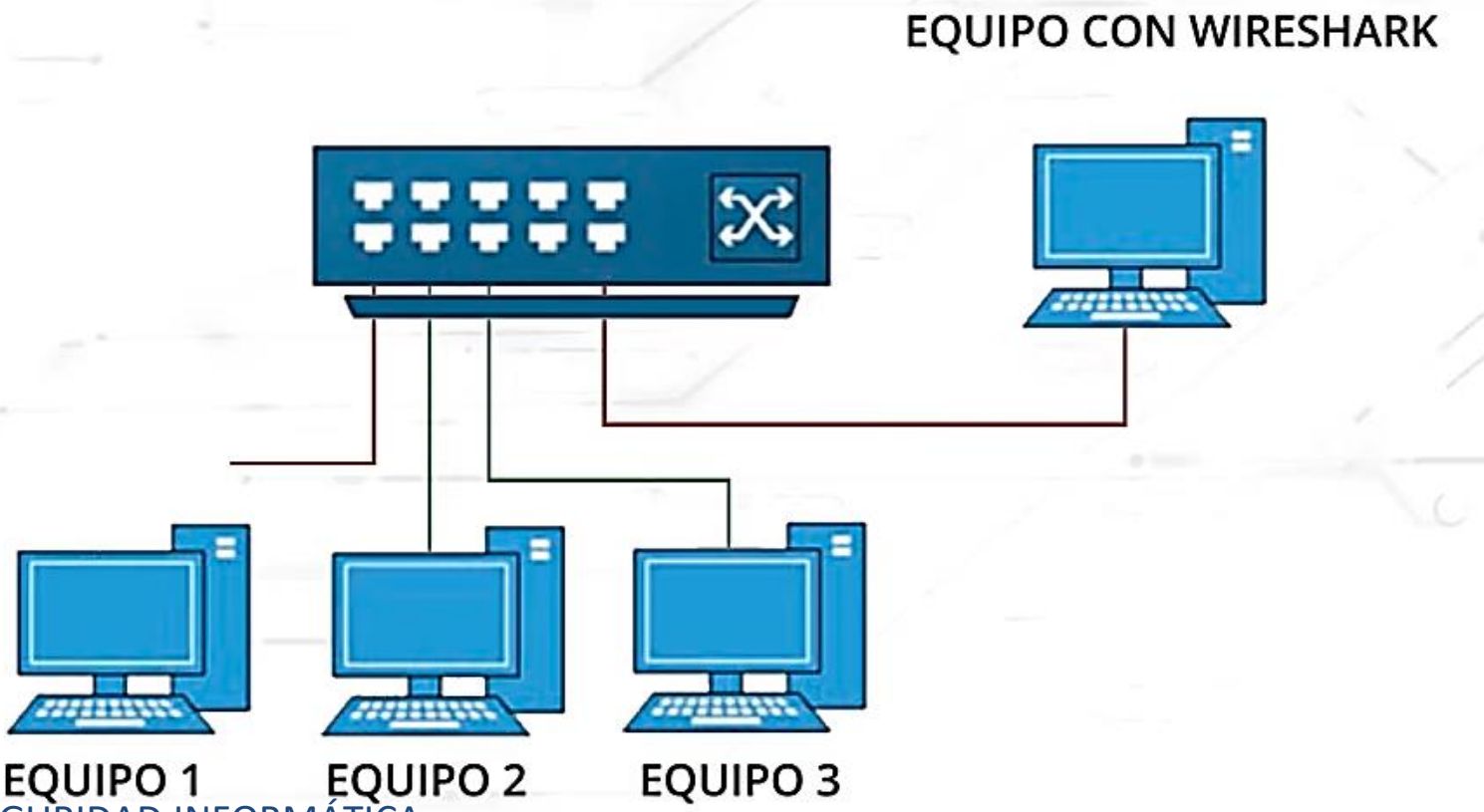
SE PUEDE UTILIZAR UN HUB PARA CAPTURAR TODO EL TRÁFICO DIRIGIDO AL SEGMENTO DE RED QUE QUEREMOS ANALIZAR:



WIRESHARK

CAPTURA DE PAQUETES

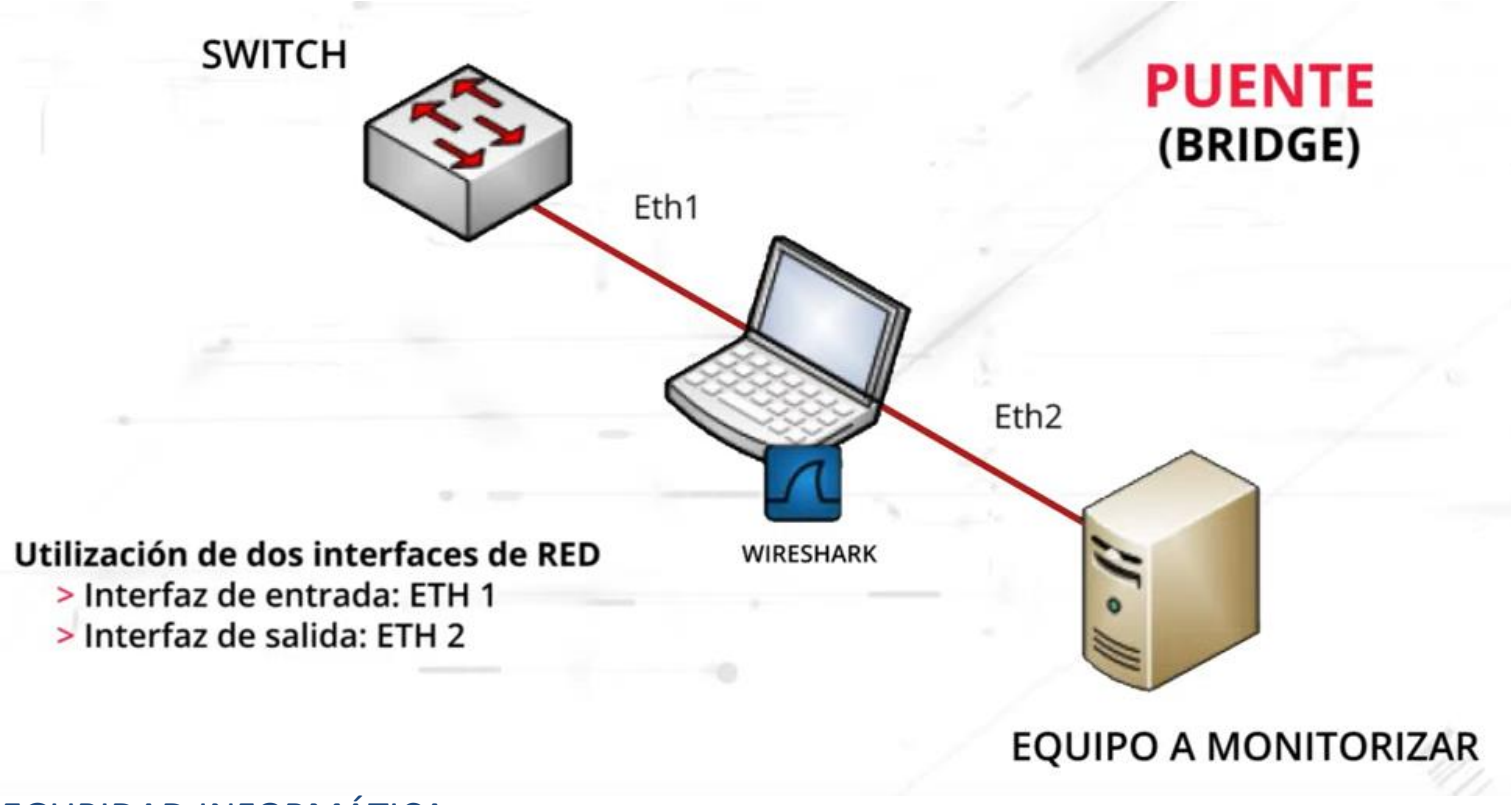
SE PUEDE UTILIZAR LA FUNCIONALIDAD **PORT MIRRORING** O **ESPEJO DE PUERTOS** QUE PROPORCIONAN ALGUNOS SWITCHES:



WIRESHARK

CAPTURA DE PAQUETES

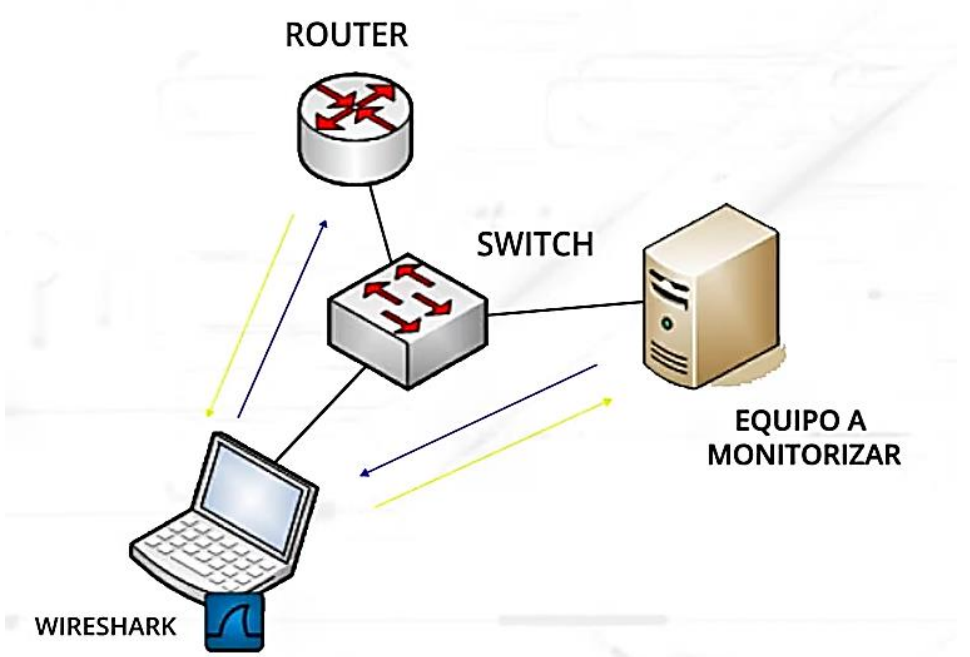
SE PUEDE UTILIZAR EL MODO PUENTE (**BRIDGE**) UTILIZANDO UN EQUIPOS CON DOS TARJETAS DE RED



WIRESHARK

CAPTURA DE PAQUETES

SE PUEDE UTILIZAR **ARP SPOOFING**,O ENVENENAMIENTO DE TABLAS ARP. CON ESTA TÉCNICA CONSEGUIMOS QUE EL EQUIPO A MONITORIZAR ENVÍE TODAS LAS TRAMAS A TRAVÉS DE NUESTRO PC



WIRESHARK

REDES WIFI (WIRELESS 802.1)

EN EL MODO PROMISCUO SOLO REALIZA CAPTURAS A PAQUETES DIRIGIDOS SOLAMENTE AL SSID ASOCIADO AL EQUIPO

LOS PAQUETES DE OTROS SSID NO FORMAN PATE DE LA CAPTURA

EL ENCABEZADO 802.11 SE ELIMINA Y ES REEMPLAZADO POR UN ENCABEZADO ETHERNET “FALSO”

PARA PODER REALIZAR CAPTURAS DE OTROS SSID HAY QUE TENER UNA NIC EN MODO MONITOR, DE ESTA MANERA SI CAPTURARÁ LOS PAQUETES DE TODOS LOS SSID DEL CANAL DE RADIO SELECCIONADO.

EL MODO MONITOR NO ESTÁ SOPORTADO EN WINDOWS


ESTO ES
TODO