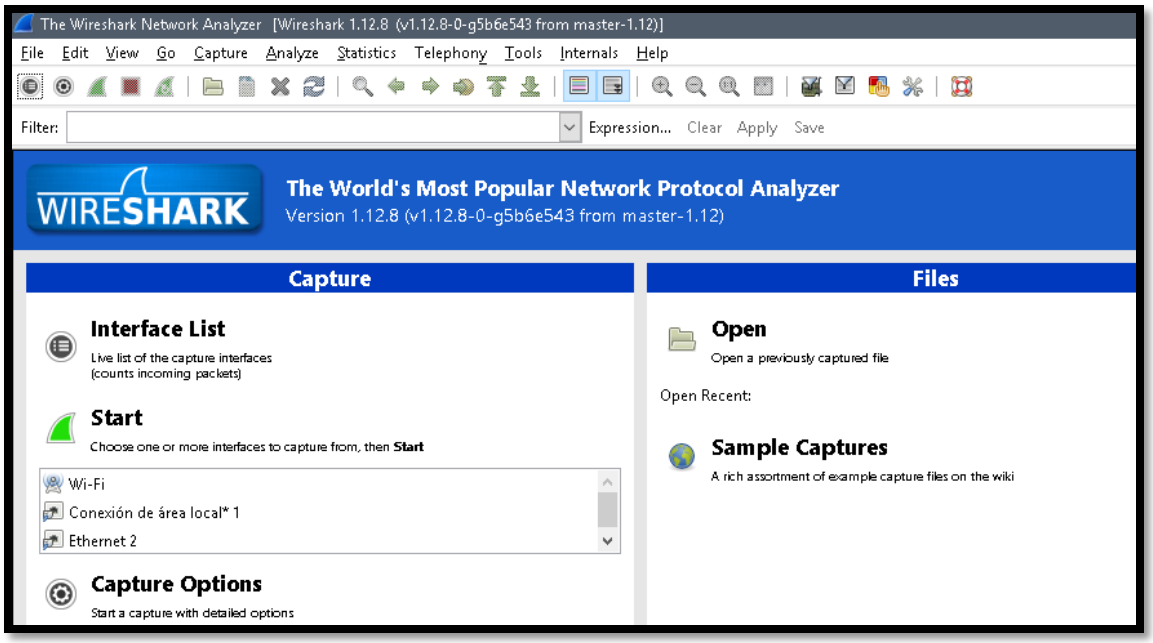
MONITOREO DE PAQUETES CON WIRESHARK

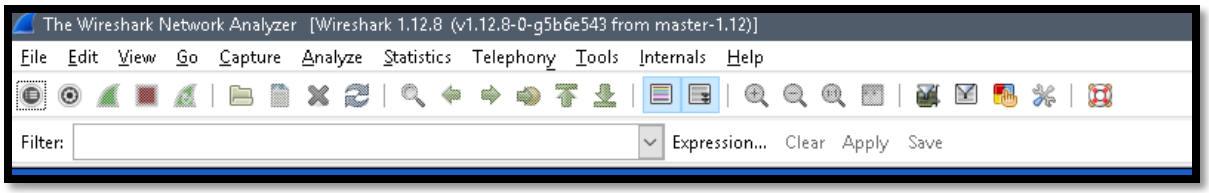
Elaborado por: Yersson Stiven Malaver Barreto

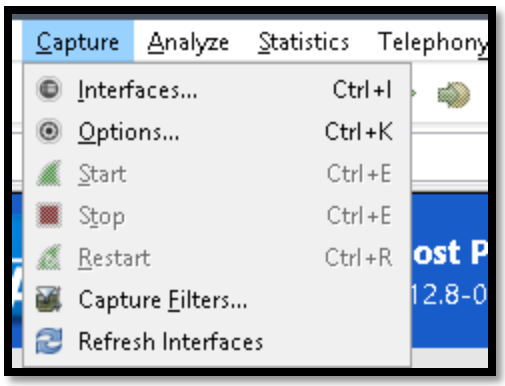
Elementos a tener en cuenta de Wireshark:

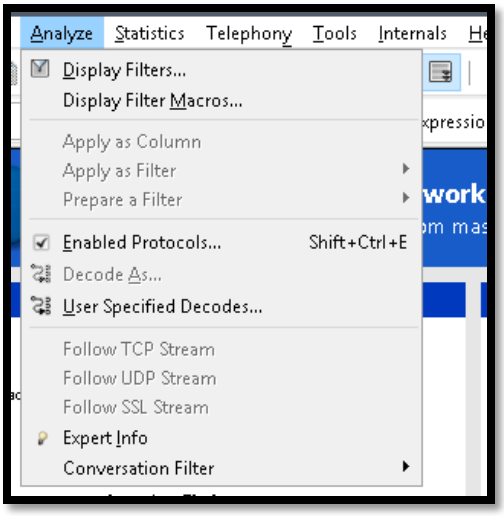
1) Desde un usuario privilegiado (Administrador) abrimos nuestra herramienta de monitoreo Wireshark, esto es debido a que para poder trabajar e inicializar de manera efectiva las interfaces de red se deben poseer ciertos privilegios.



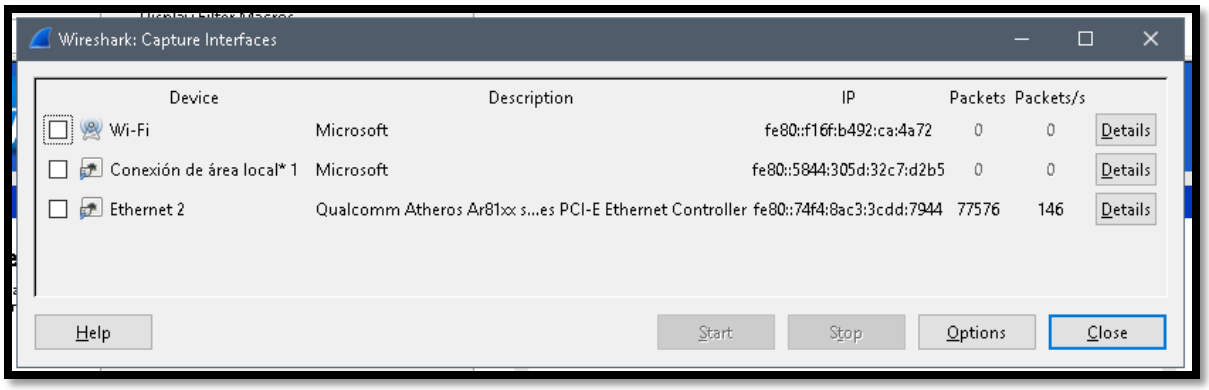
2) Una vez tenemos la aplicación abierta, pasamos a conocer las funcionalidades de los botones de la interfaz principal y en seguida pasamos a los sub-menús que nos serán útiles para el manejo del software, es importante que este paso lo realice con su tutor, previa consulta por parte suya de los componentes del programa.



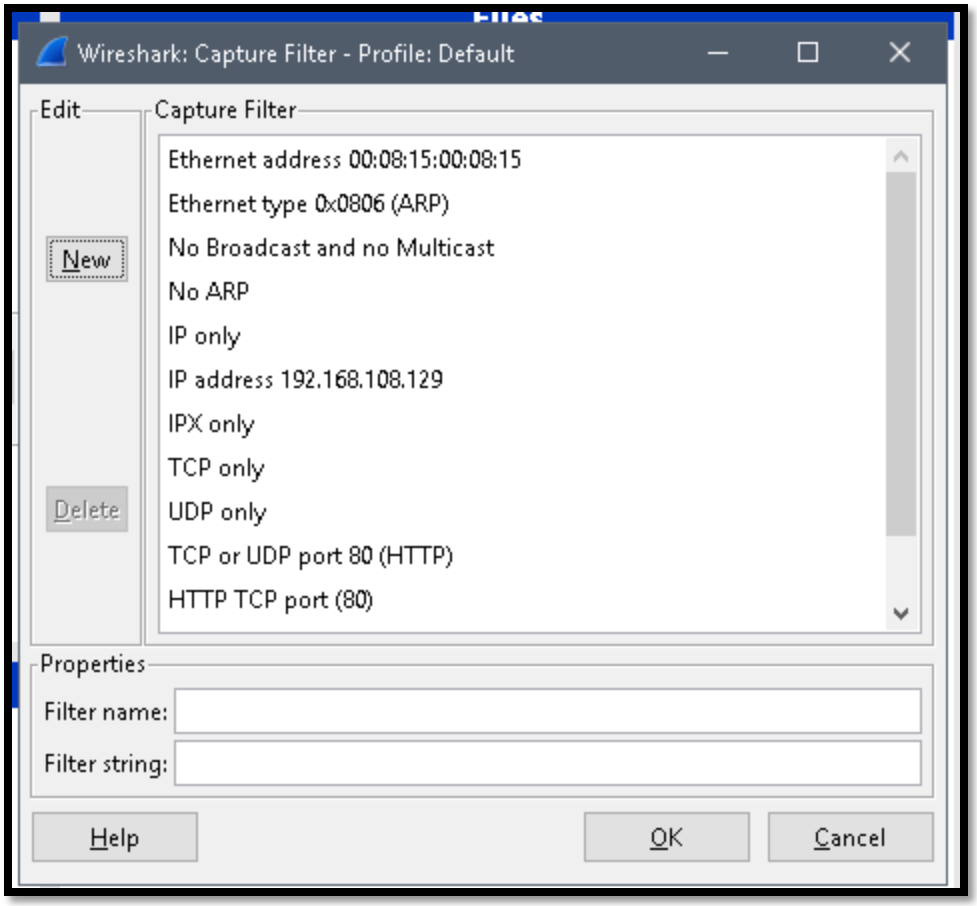




3) Luego del reconocimiento de los botones, menús y sub-menús del programa es importante reconocer por donde haremos la captura, para ello nos dirigimos al menú “capture” y seleccionamos la opción “interfaces”, allí podremos ver por cuál de las interfaces capturaremos tráfico.

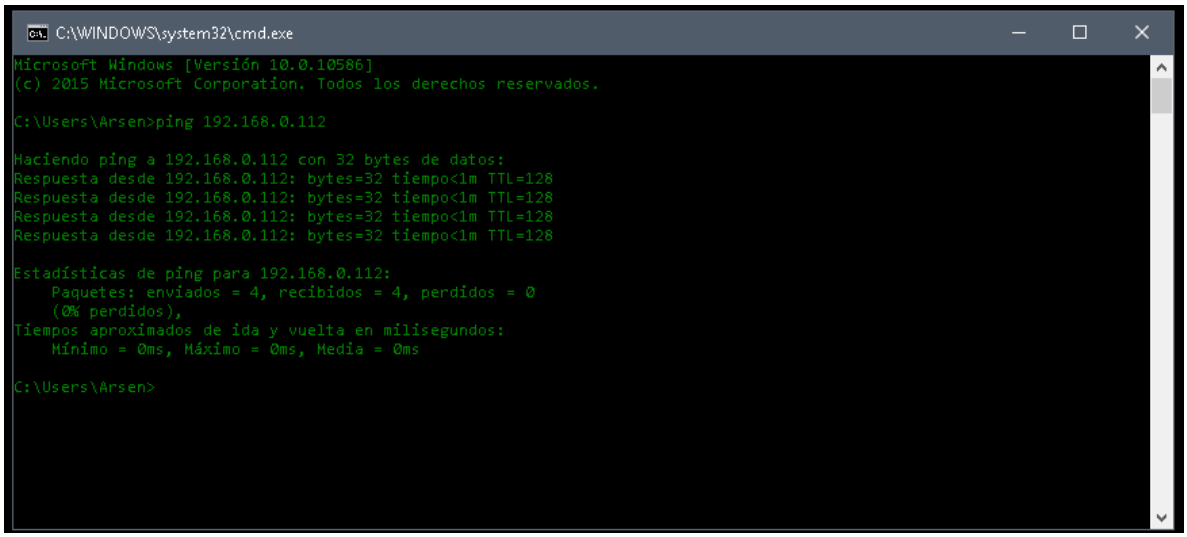


4) Mediante el botón “Capture filter”, podemos seleccionar el filtro a utilizar para la captura de los datos, aquí se pude elegir o crear uno personalizado.



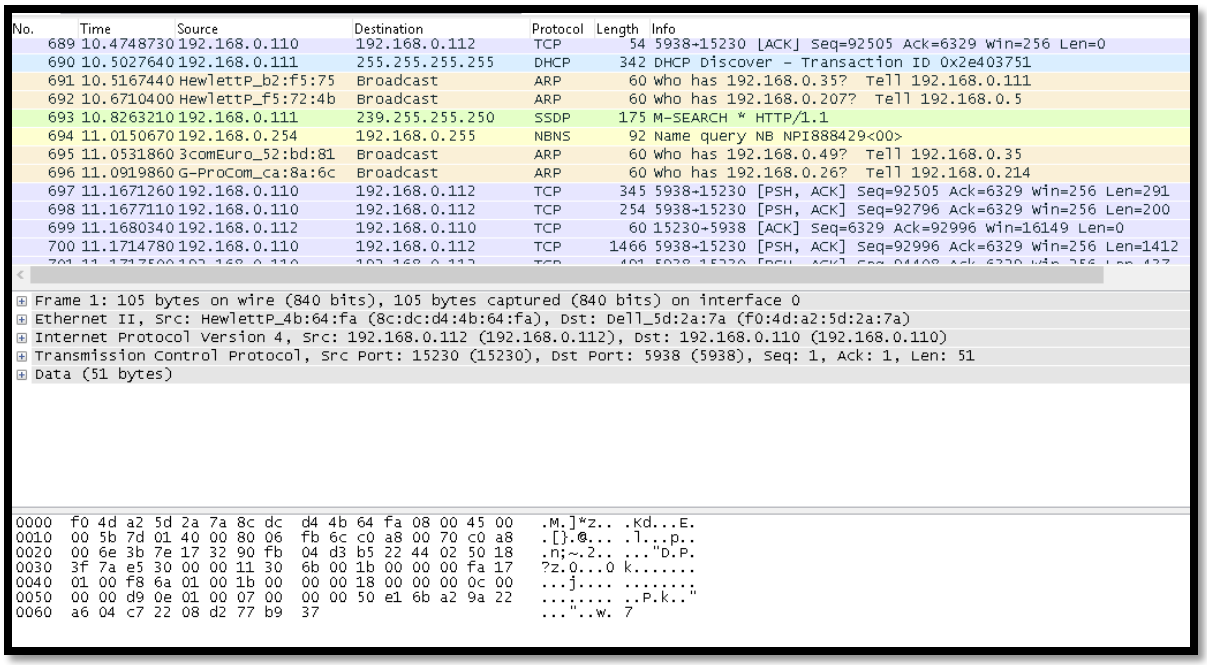
PARTE II - La práctica:

1) Desde la maquina atacante capturemos tráfico de red con Wireshark, es importante establecer comunicación con la maquina víctima, para ello podríamos hacer ping, o utilizar la maquina servidor que configuramos en la práctica 1.



2) Luego de capturado el tráfico de red, paramos la captura y guardamos el archivo generado. Respondemos las siguientes preguntas:

¿Qué información nos da la herramienta del tráfico capturado?
¿Cómo podemos interpretar lo capturado?

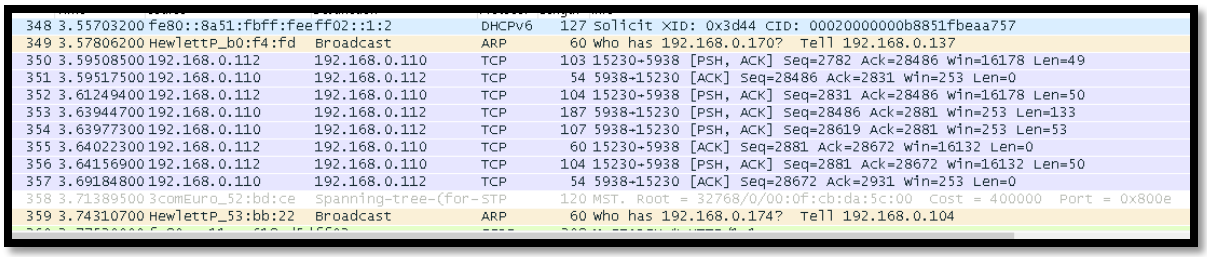


Tráfico capturado.

Respuesta: La herramienta nos muestras el tráfico capturado a manera de registros. Con datos como Host fuente, el host de destino, protocolo utilizado, longitud del paquete.

La herramienta permite mostrar el contenido de cada registro en la parte inferior de la ventana. Allí se listan los componentes del paquete. Si seleccionamos un componente, Wireshark no muestra el contenido de ese elemento.

3) Ahora iniciamos una nueva captura y con un navegador web desde nuestra victima (máquina virtual que se sugirió) abrimos una página cualquiera de internet.
Con lo anterior respondemos:
¿Qué paquetes distintos a la anterior captura se pueden identificar?

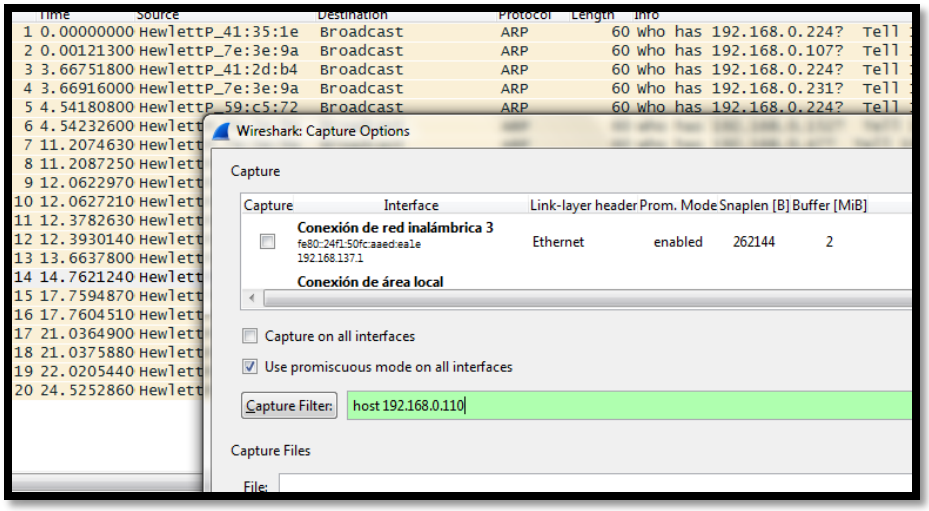


348	3.55703200	fe80::8a51:fbff:fee	ff02::1:2	DHCPv6	127	Solicit XID: 0x3d44 CID: 000200000000b8851fbeaa757
349	3.57806200	HewlettP_b0:f4:fd	Broadcast	ARP	60	Who has 192.168.0.170? Tell 192.168.0.137
350	3.59508500	192.168.0.112	192.168.0.110	TCP	103	15230→5938 [PSH, ACK] Seq=2782 Ack=28486 Win=16178 Len=49
351	3.59517500	192.168.0.110	192.168.0.112	TCP	54	5938→15230 [ACK] Seq=28486 Ack=2831 Win=253 Len=0
352	3.61249400	192.168.0.112	192.168.0.110	TCP	104	15230→5938 [PSH, ACK] Seq=2831 Ack=28486 Win=16178 Len=50
353	3.63944700	192.168.0.110	192.168.0.112	TCP	187	5938→15230 [PSH, ACK] Seq=28486 Ack=2881 Win=253 Len=133
354	3.63977300	192.168.0.110	192.168.0.112	TCP	107	5938→15230 [PSH, ACK] Seq=28619 Ack=2881 Win=253 Len=53
355	3.64022300	192.168.0.112	192.168.0.110	TCP	60	15230→5938 [ACK] Seq=2881 Ack=28672 Win=16132 Len=0
356	3.64156900	192.168.0.112	192.168.0.110	TCP	104	15230→5938 [PSH, ACK] Seq=2881 Ack=28672 Win=16132 Len=50
357	3.69184800	192.168.0.110	192.168.0.112	TCP	54	5938→15230 [ACK] Seq=28672 Ack=2931 Win=253 Len=0
358	3.71389500	3comEuro_52:bd:ce	Spanning-tree-(for-STP	STP	120	MST. Root = 32768/0/00:0f:cb:da:5c:00 Cost = 400000 Port = 0x800e
359	3.74310700	HewlettP_53:bb:22	Broadcast	ARP	60	Who has 192.168.0.174? Tell 192.168.0.104

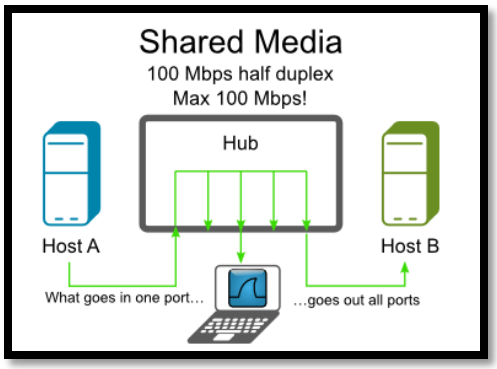
¿Cómo se puede interpretar la captura en términos de TCP/IP?

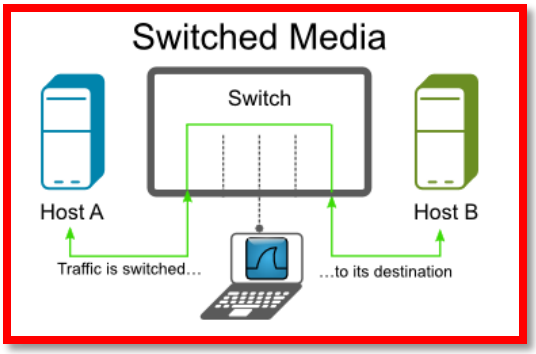
Este protocolo utiliza varias propiedades para operar, Wireshark nos muestra los detalles como por ejemplo la longitud del paquete, los datos de las cabeceras. Además nos muestra los datos del paquete en caracteres legibles al usuario.

Ahora vamos a usar un filtro predeterminado en las capturas, esto con el fin de disminuir capturas que en el momento no nos interesan. Teniendo clara la IP del equipo que deseamos monitorear vamos a usar el filtro de direcciones IP, en opciones de captura en el campo de filtro de captura escribimos lo siguiente:
host
Ip_target

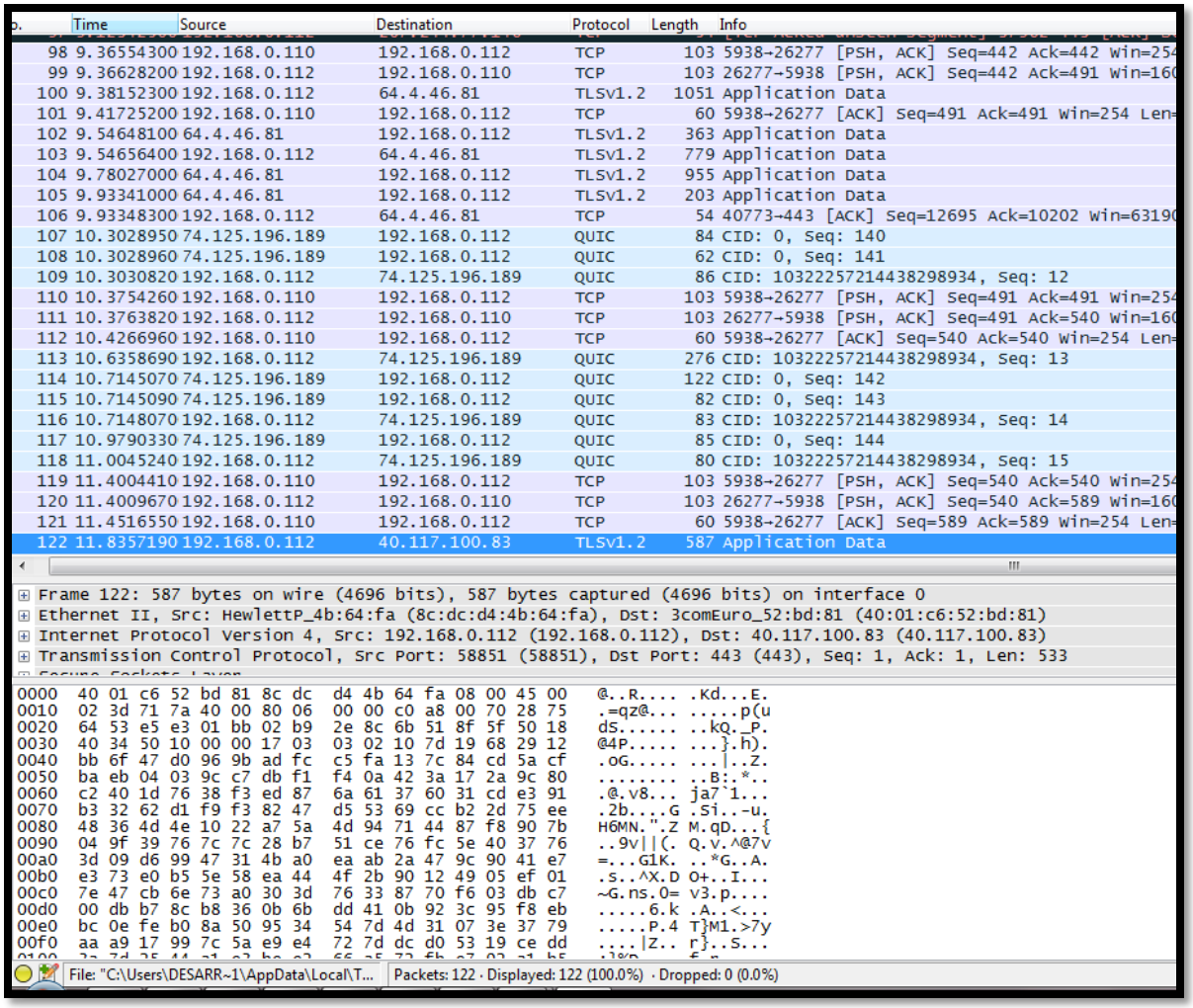


En las redes modernas ya no están fácil capturar los paquetes de un Ip distinta la nuestra. Los Switches tienen un sistema que impide la captura de los paquetes del objetivo. Como se menciona en esta página: https://wiki.wireshark.org/CaptureSetup/Ethernet



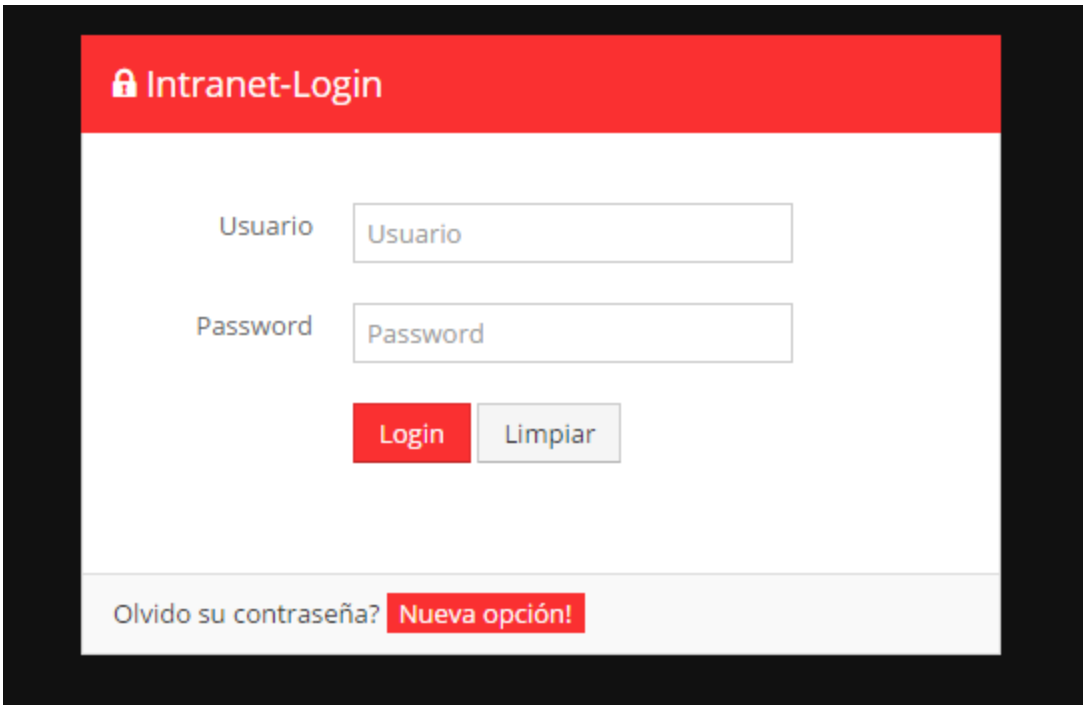


La solucion que proponen es utilizar un Ethernet Hub o situarse directamente en la Ip que deseamos escanear.

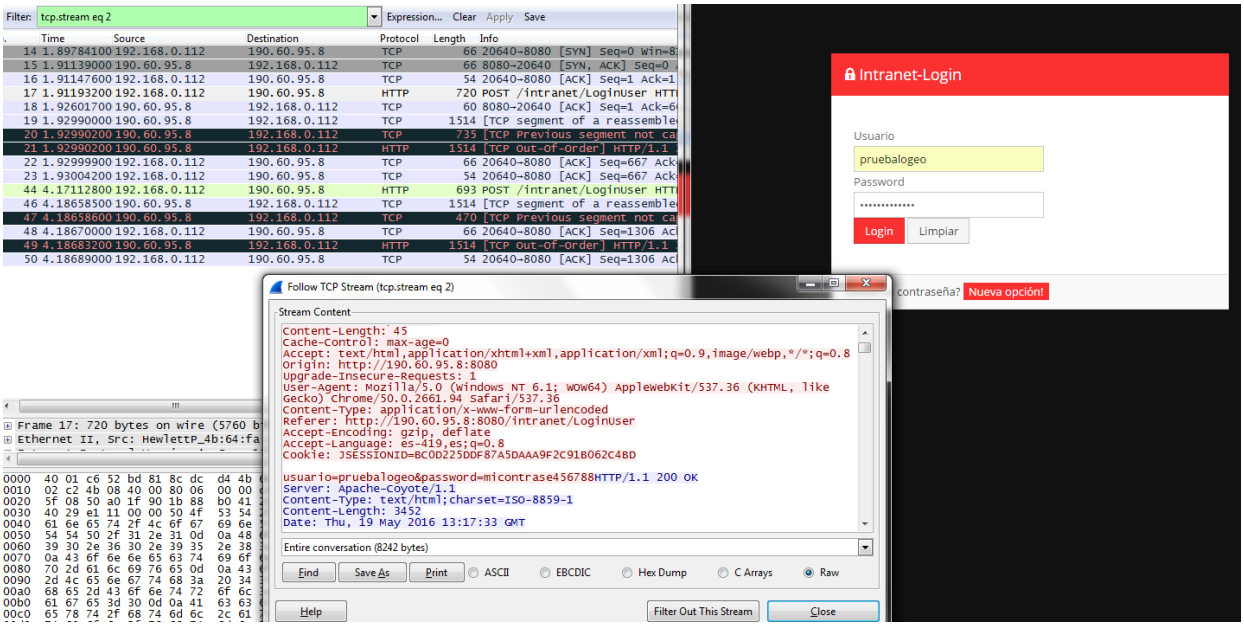


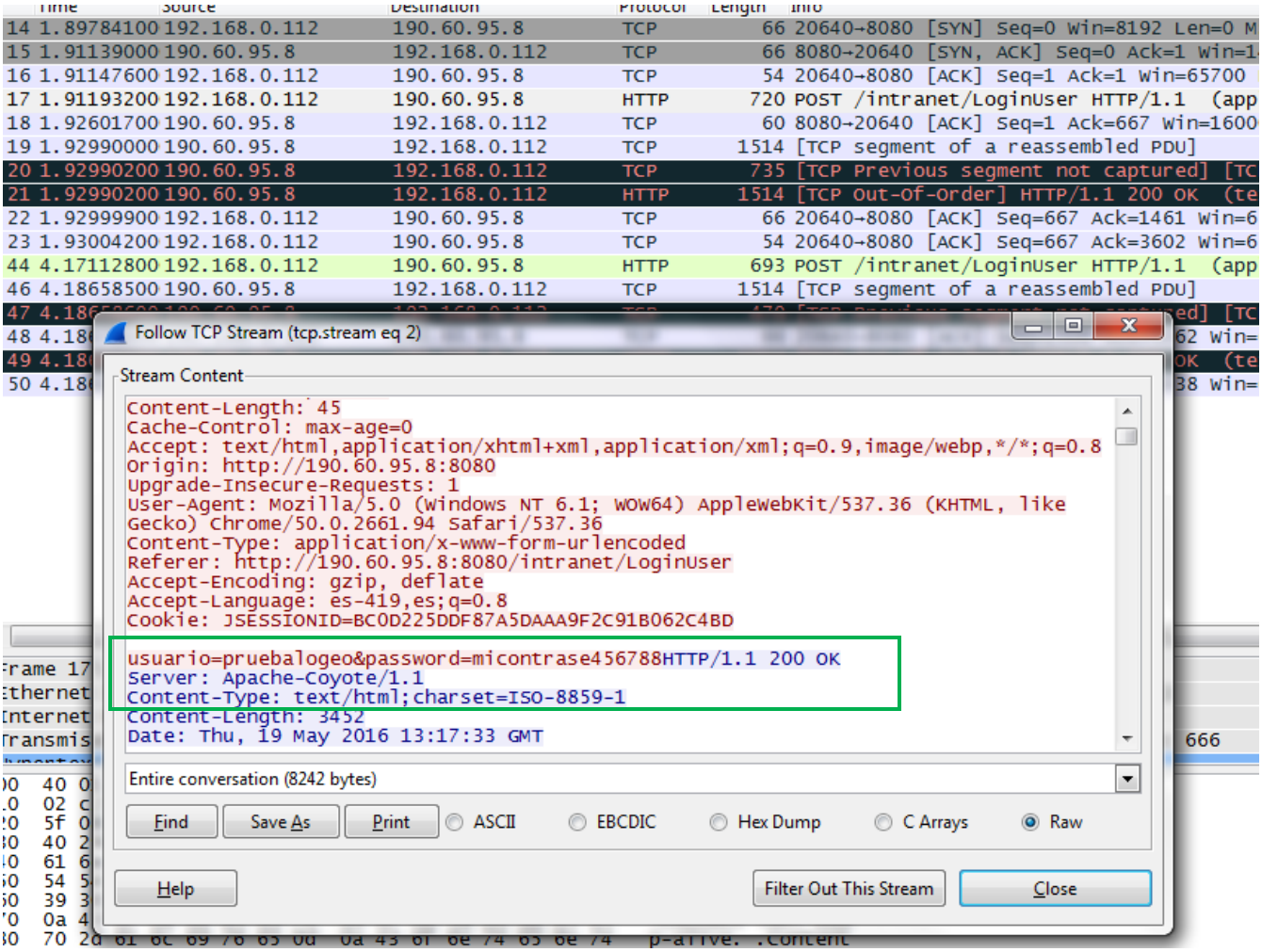
En vista del problema de captura mencionado anteriormente, se hará una prueba con la maquina local, y ver si podemos capturar los datos de navegación:

Sito web objetivo: http://190.60.95.8:8080/intranet/



Capturamos los paquetes y obtenemos los datos de acceso al sitio:





Con esta herramienta se ha comprendido un poco mejor como viaja la información en las redes informáticas. Y también como hay herramientas que permiten hacer seguimiento a los paquetes de nuestros usuarios. Muestran la importancia de implementar buena seguridad en nuestros sistemas de información.

REFERENCIAS BIBLIOGRÁFICAS

- ✓ Cambero, L. (2015). Análisis de Tráfico con Wireshark (Parte1) [Video]. Disponible en: https://youtu.be/lxCENEGhztU

- ✓ Gómez, R. (2014). Tutorial como Instalar y Configurar Wireshark [Video]. Disponible en: https://youtu.be/l0AMIh59955U

- ✓ iTutosPc (2013). Como Descargar e Instalar VirtualBox 4.3.2 en Windows 8 32 y 64 BITS 2016 [Video]. Disponible en: https://youtu.be/H_GgZmT1u7s
- ✓
- ✓ Samboni Núñez, D. M. (2012). Diapositivas online tituladas "Manual Básico de WireShark". Publicadas en el sitio web 2.0 de alojamiento de diapositivas denominado "Slideshare", el 26 de Febrero de 2012. Extraídas el 18 de Mayo de 2016, http://es.slideshare.net/DIANYSS2012/manual-bsico-de-wireshark
- ✓
- ✓ windowscracker1 (2015). Descargar e Instalar VMWare Workstation 11 Full - Virtualiza varios sistemas operativos [2016] [Video]. Disponible en: https://youtu.be/3ajD6m_gyHE