Práctica del Tema 1

En esta práctica se pretende familiarizarse con el uso de una de las herramientas más empleadas y específicas para el análisis de tráfico de red (Wireshark). Esta herramienta se puede usar directamente con ficheros que contienen la captura completa de los paquetes de red en formato PCAP (Packet Capture) o bien sobre tráfico en tiempo real (se puede configurar para leer directamente de las tarjetas de red del equipo donde se este ejecutando). Para más información del funcionamiento sobre PCAP, se pueden consultar los dos siguientes enlaces:

http://www.tech-faq.com/pcap.html

https://resources.infosecinstitute.com/pcap-analysis-basics-with-wireshark/

Wireshark (https://www.wireshark.org/) es una herramienta sencilla de emplear y que automatiza la búsqueda de información dentro de los archivos de captura (mediante el uso de filtros), asi como añade la posibilidad de extraer información (objetos) de los propios paquetes capturados (por ejemplo, ficheros o adjuntos que pueden corresponderse con malware). En concreto, Wireshark se usa fundamentalmente para:

- Capturar paquetes de datos de la red
- Identificar y analizar protocolos
- Aislar e identificar tráfico de/hacia fuentes/destinos (IP/Mac Address)
- Inspeccionar el contenido de los paquetes de datos

La práctica está compuesta por tres partes, cuyos entregables se añadirán a un fichero zip completo. Cada parte tendrá un directorio denominado parteX (X en el rango [1:3]), que deberá contener los entregables que se piden para cada parte/apartado.

Parte 1. Instalación de Wireshark (1.5 puntos)

Este apartado consiste en la instalación de Wireshark de manera local, de forma que se pueda usar para el resto de aparatados de la práctica. Se debe descargar el instalable desde la página web de Wireshak:

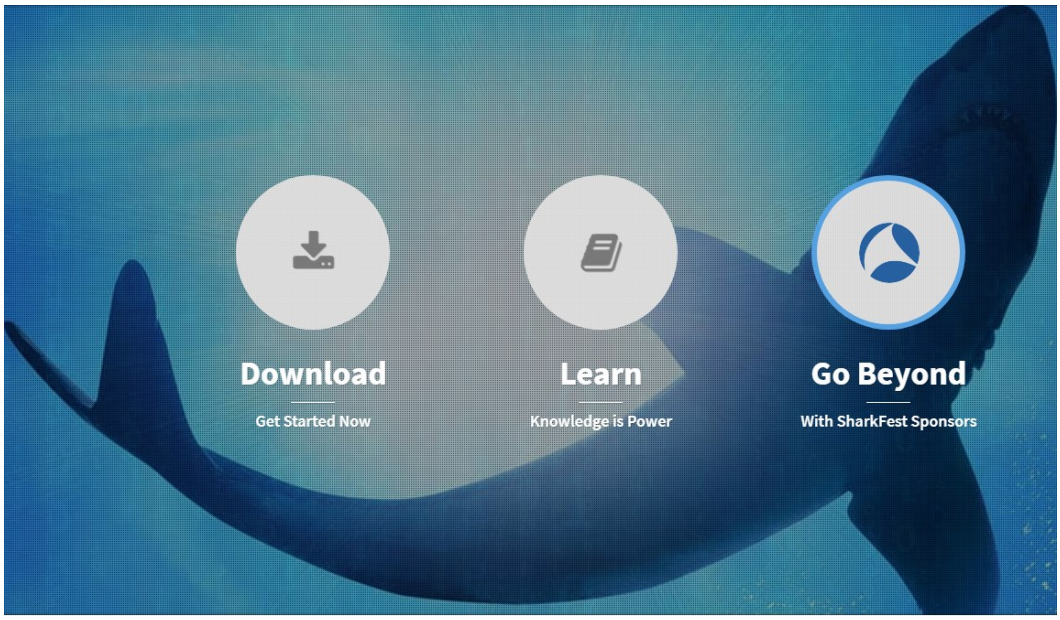

Fig.1.- Página web de Wireshark

Se recomienda instalar Wireshark en algún entorno con capacidades gráficas (Windows; Mac, Ubuntu/Debian Desktop) porque facilita la inspección y uso de la herramienta. Se puede emplear la línea de comandos pero la visualización no es la más adecuada para este tipo de tares.

En la instalación puede ocurrir que se le pida instalar el controlador de acceso local a las interfaces de red. Puesto que no se va a usar Wireshark para monitorizar/analizar el tráfico en tiempo real (Live Network), no es necesario instalar el Npcap Lookback Adapter.

Pruebas

Se debe comprobar que se pueden cargar ficheros en formato Pcap. Para ello, se debe emplear el fichero PCAP denominado "`traffic-for-wireshark-column-setup.pcap`" y que está disponible en el curso virtual.

Comprobar que el paquete ubicado en sexto lugar contiene una petición GET a un sitio Web, tal y como se muestra en la Figura 2

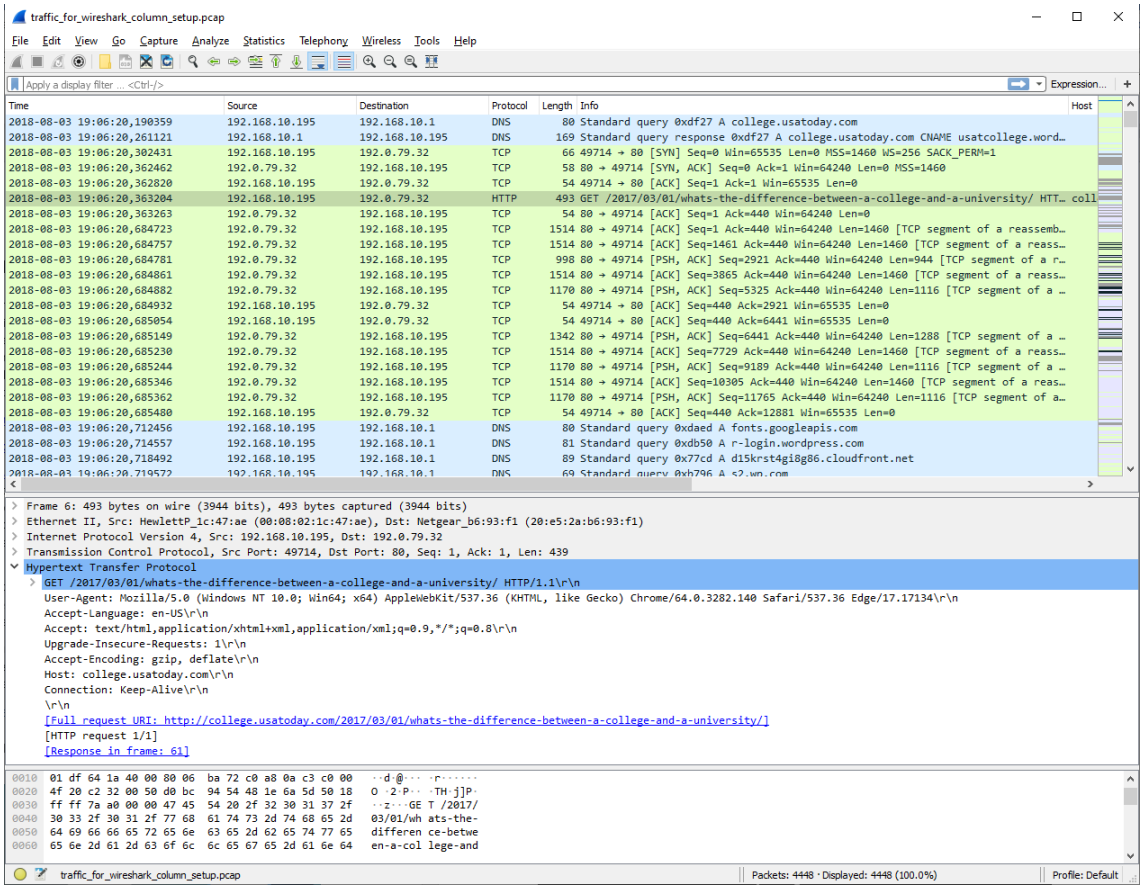

Fig.2.- Interface de Wireshark

Entregables del apartado

Se debe incluir en el subdirectorio "parte1" del fichero zip con la solución completa, los siguientes apartados:

- Subdirectorio **doc** (dentro del directorio parte1). Indicar en un informe de no más de dos páginas los problemas encontrados en la instalación
- Subdirectorio **pruebas** (dentro del directorio parte1). Rellenar la siguiente tabla, respecto de los datos asociados al paquete de datos usado para comprobar la instalación de Wireshark. La tabla debe estar incluida en un fichero de tipo doc/docx/pdf.

Clave	Valor
Dirección URL de la petición HTTP (GET)	
Dirección IP destino	
Puerto destino	
Mac Address Origen	
IP equipo origen	

Parte 2. Familiarización con Wireshark (2.5 puntos)

En esta parte se pretende que el estudiante conozca los procedimientos básicos con la herramienta Wireshark. Para ello, el estudiante debe realizar los siguientes tutoriales que se pueden encontrar en el siguiente enlace:

https://www.malware-traffic-analysis.net/tutorials/index.html

Los tutoriales concretos a realizar son los siguientes (los enunciados y los ficheros pcap a emplear se pueden descargar desde el propio tutorial o en el propio curso virtual)

Customizing Wireshark – Changing Your Column Display

URL directo: https://unit42.paloaltonetworks.com/unit42-customizing-wireshark-changing-column-display/

Using Wireshark: Identifying Hosts and Users

URL directo: https://unit42.paloaltonetworks.com/using-wireshark-identifying-hosts-and-users/

Using Wireshark – Display Filter Expressions

URL directo: https://unit42.paloaltonetworks.com/using-wireshark-display-filter-expressions/

Using Wireshark: Exporting Objects from a Pcap

URL directo: https://unit42.paloaltonetworks.com/using-wireshark-exporting-objects-from-a-pcap/

Pruebas

La realización del cada tutorial es la propia prueba de ejecución del apartado.

Entregables del apartado

Se debe incluir en el subdirectorio "parte2" del fichero zip con la solución completa, los siguientes apartados:

- Subdirectorio **doc** (dentro del directorio parte2). Indicar en un informe de no más de ocho páginas (dos por cada tutorial como máximo):
    - Problemas encontrados en la realización
    - Lecciones aprendidas del tutorial. No solo a nivel de uso de la herramienta Wireshark, sino conceptos adicionales que no se conocían (los tutoriales son muy completos y tratan muchos temas diversos)

Parte 3. Ejercicios prácticos (6 puntos)

Una vez vistos los tutoriales, que permiten hacer una sesión dirigida, se deben realizar los siguientes dos ejercicios libres (sin guión).

2019-01-28 - TRAFFIC ANALYSIS EXERCISE - TIMBERSHADE

URL directo: https://www.malware-traffic-analysis.net/2019/01/28/index.html

2019-05-02 - TRAFFIC ANALYSIS EXERCISE - BEGUILESOFT

URL directo: https://www.malware-traffic-analysis.net/2019/05/02/index.html

Todos los ejercicios tienen sus respuestas asociadas, por lo que se pide que se intente primero antes de ver las soluciones. En los entregables, indicar si se han podido obtener todas las respuestas a las preguntas y en caso contrario, desde que punto no ha sido posible continuar. Para cada tarea/ejercicio hay una serie de preguntas que se deben responder y añadir como parte de los entregables.

Como recomendación, se le indica al estudiante que defina un procedimiento de trabajo/búsqueda sobre el contenido de los paquetes para obtener las respuestas pedidas por el ejercicio.

Pruebas

La realización de cada ejercicio es la propia prueba de ejecución del apartado.

Entregables del apartado

Se debe incluir en el subdirectorio “parte3” del fichero zip con la solución completa, los siguientes apartados:

- Subdirectorio **doc** (dentro del directorio parte3). Indicar en un informe de no más de dos páginas los problemas encontrados en la solución de los ejercicios y si ha sido posible finalizar el ejercicio.
- Subdirectorio **pruebas** (dentro del directorio parte3). Rellenar en una tabla las preguntas que se realizan para cada ejercicio. Las dos tablas deben estar incluidas en un fichero de tipo doc/docx/pdf.
- Subdirectorio **proc** (dentro del directorio parte3). Indicar en un informe la metodología diseñada para cada ejercicio, asi como los resultados intermedios más relevantes asociados a cada paso de la metodología diseñada. Este punto se valorará específicamente como parte muy importante de la puntuación final de cada ejercicio.