Práctica 4. Primeros pasos SNORT

1. Instala el Snort para Windows (Snort\_2\_9\_7\_2\_Installer.exe). Elige las opciones por defecto:
   1. Componentes (Snort, Dynamic Rules, Documentation)
   2. Ubicación (C:\Snort)
   3. ¿Qué pantallazo aparece al terminar la ejecución?
2. Carpetas en el Snort
   1. Haz un pantallazo del directorio de archivos del Snort y describe que hay en cada una de las carpetas
   2. ¿Cómo lo desinstalarías?
3. Ejecución del Snort
   1. Entra por el cmd a la carpeta bin para ejecutar el Snort, para ello utiliza las instrucciones
      1. cd (cambiar directorio)
      2. snort (dentro de la carpeta bin)
   2. Una vez ejecutado, espera para recibir paquetes, y después pulsa CTRL + C para ver el informe que genera
   3. Ejecuta: snort -?
   4. Muestra las interfaces (conexiones de red) que disponemos para gestionar
      1. ¿Cuál es el número de interfaz asociado a tu conexión de red?
      2. Realiza una prueba con todas las interfaces (snort –i 1, snort –i 2…) y comprueba resultados
   5. Muestra la versión del snort
   6. Prueba las siguientes instrucciones con la interfaz correcta
      1. Snort –i 2 –v
      2. Snort –i 2 -vd
      3. Snort –i 2 –vde
4. Almacenar la salida en la carpeta log
   1. Snort –i 2 ../log
   2. Para el proceso
   3. Abre el fichero que se ha creado en .log con el Wireshark (no con el notepad)