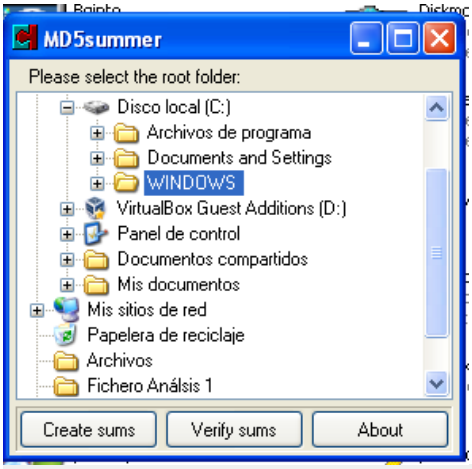
Asignatura	Datos del alumno	Fecha
Seguridad en el *Software*	Apellidos: Paz López	27/01/2022
	Nombre: Angel Ramon	

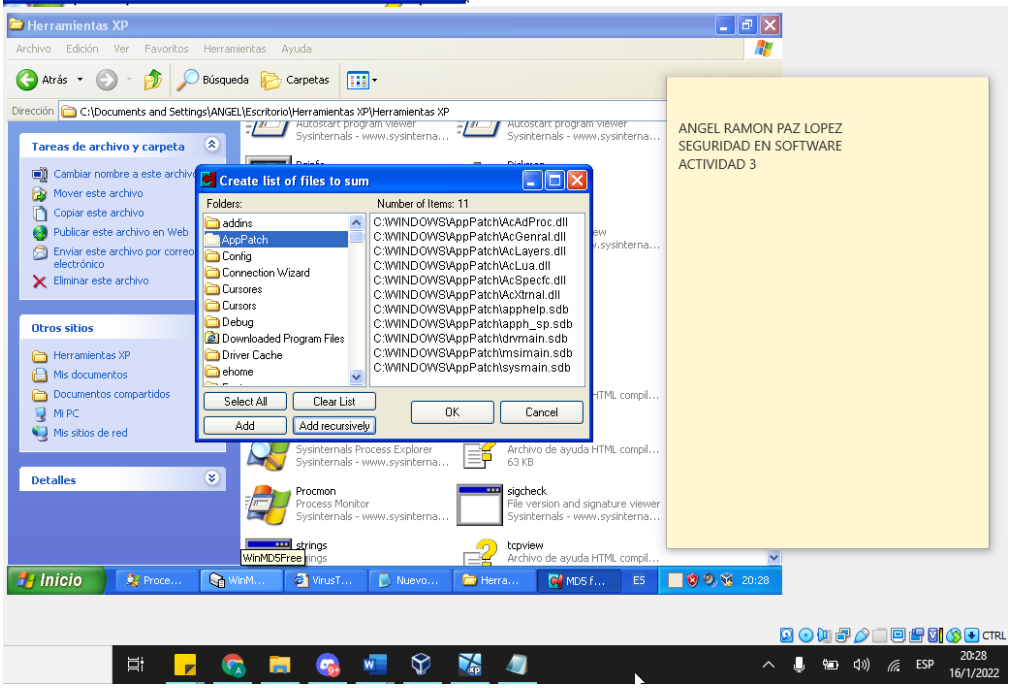
ACCIONES INICIALES

Verificar la integridad del fichero de línea base de referencia mediante la utilidad MD5summer.

Elegimos la ruta C:\WINDOWS



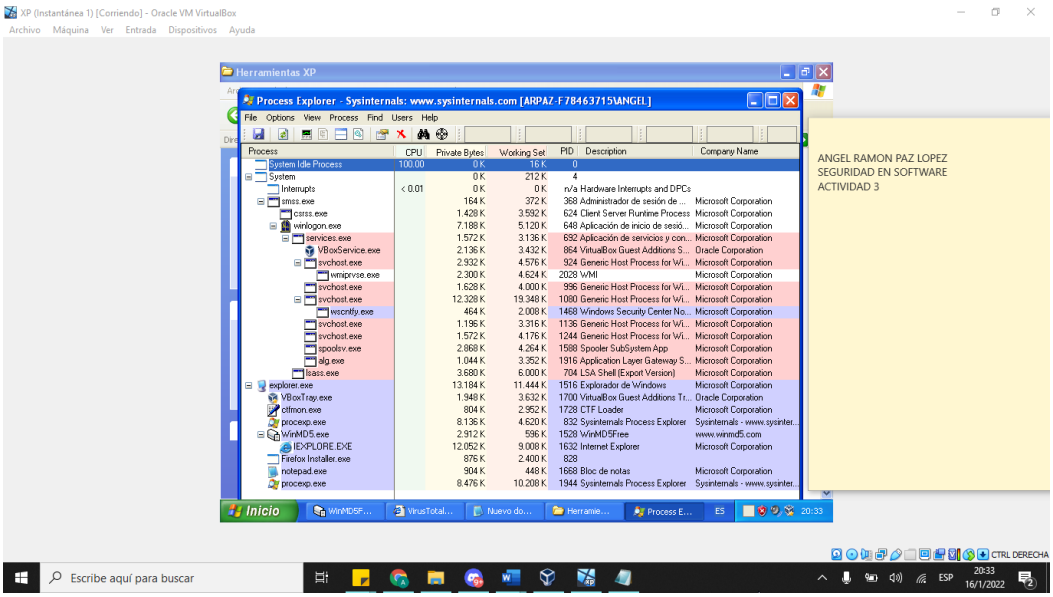
Damos clic en **Create sums**



Elegimos la carpeta AppPatch y damos **Add secursively** para crear el hash md5 de todos los ficheros

Inicio Process Explorer

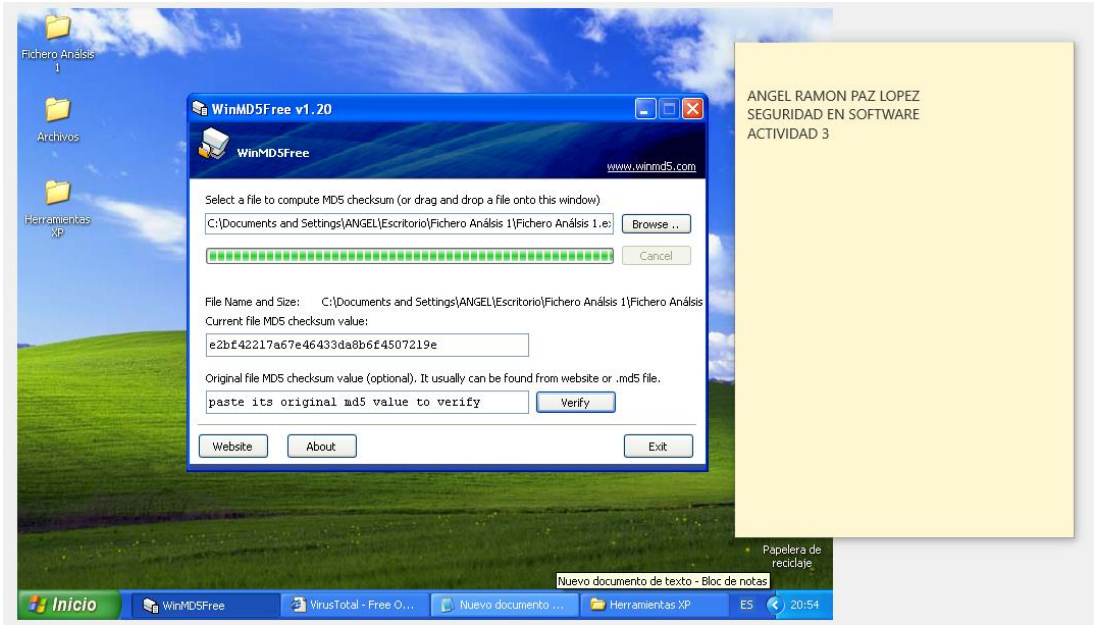
Observamos los procesos



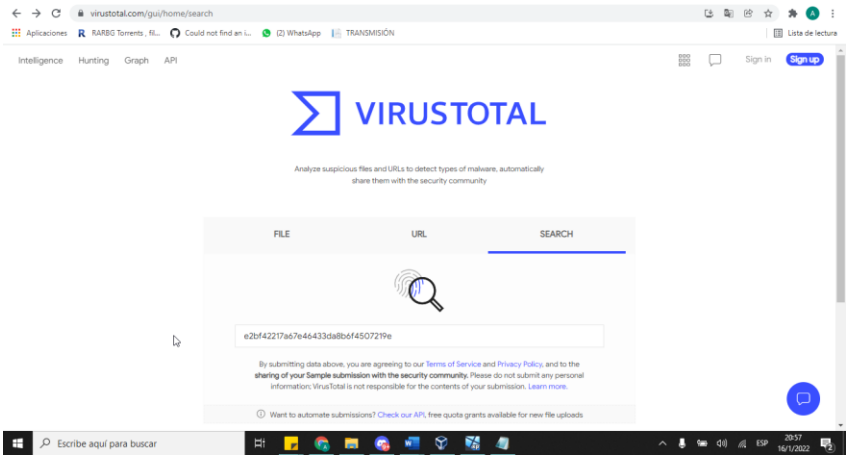
CLASIFICACIÓN

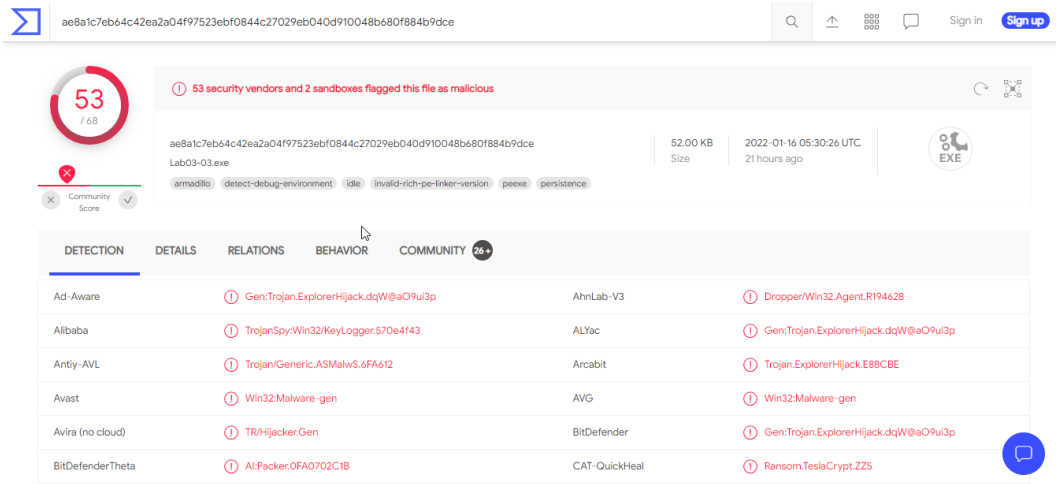
Examinamos el archivo ejecutable del malware sin acceder al código malicioso, para identificarlo y obtener información inicial.

Usamos la Herramienta **WinMD5** para obtener el hash del archivo malicioso

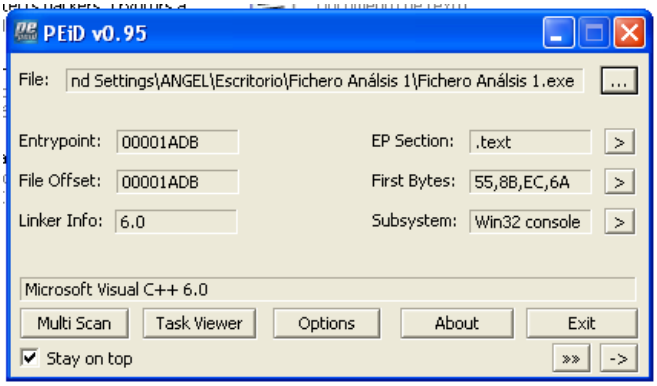


Comprobamos el tipo de malware subiendo el hash del malware a VirusTotal en el botón Search

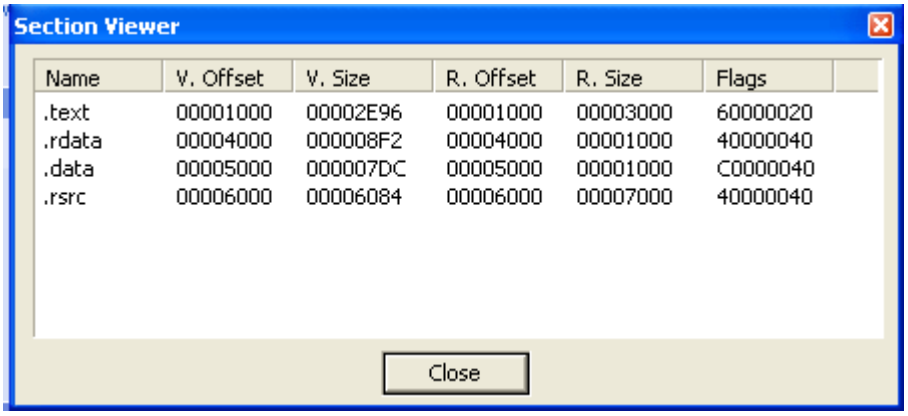




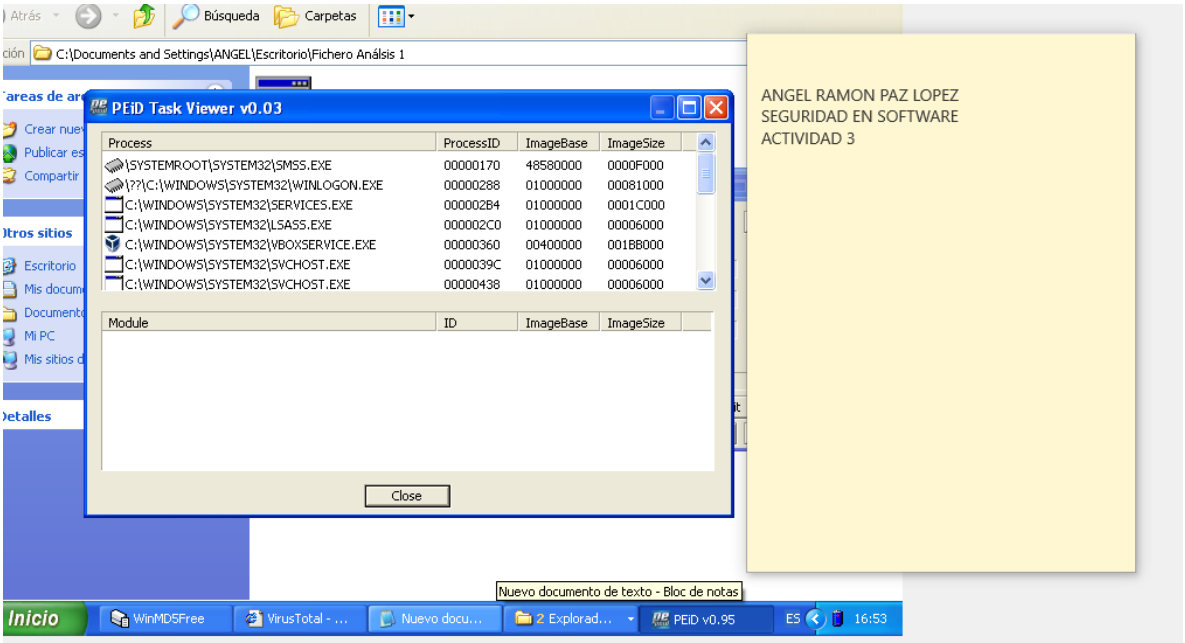
Identificación de técnicas de ofuscación y empaquetamiento usando la herramienta PEiD



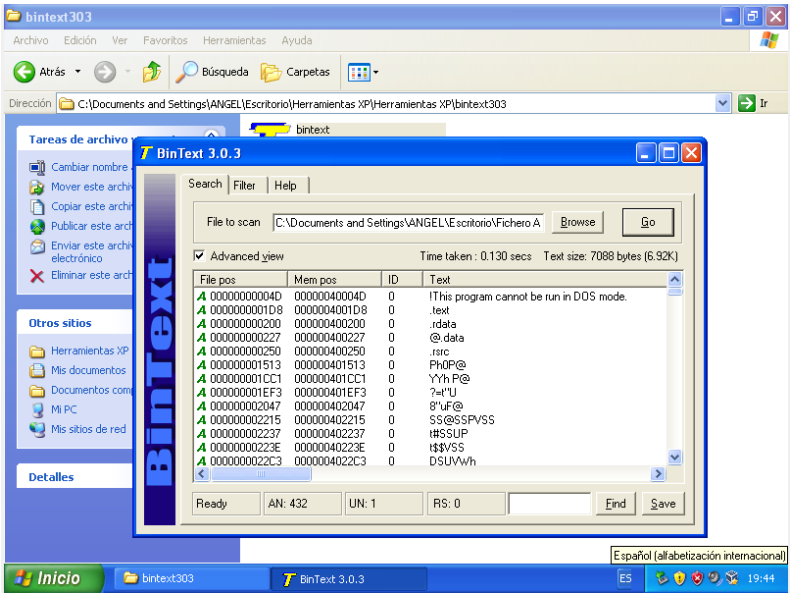
En la cual podemos ver varias secciones, donde podemos ver nuestros datos, la reubicación, el texto del punto, sus compensaciones, banderas, tamaño, punto de entrada



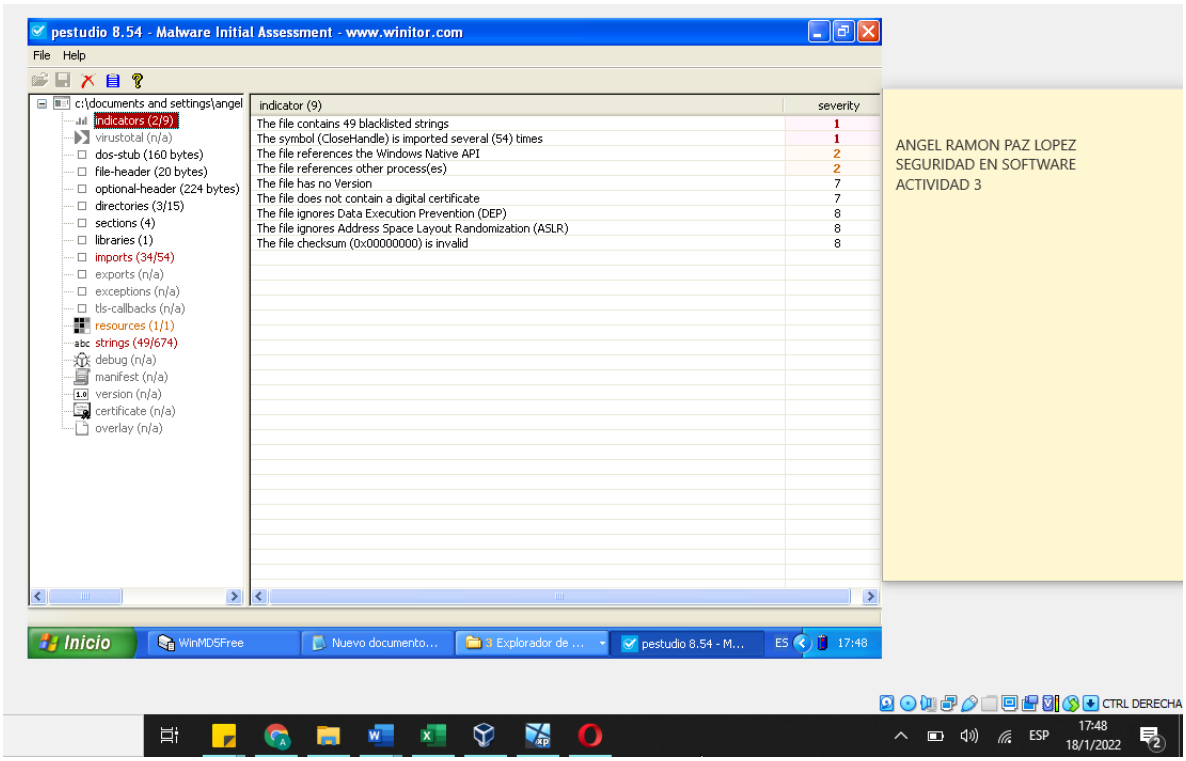
También podemos ver la vista de tareas para ver que otros elementos podrían usarlo



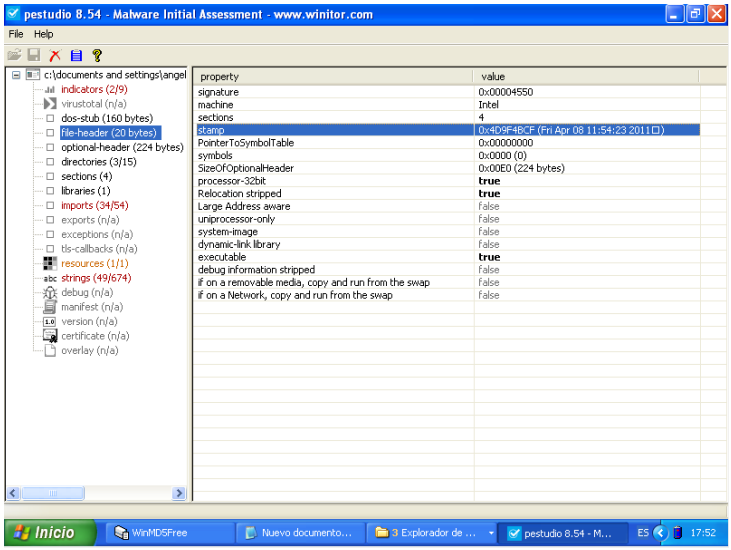
Búsqueda de cadenas de texto en el archivo ejecutable con la Herramienta **BinText**



Formato y estructura del fichero. Usaremos la Herramienta **PEStudio**

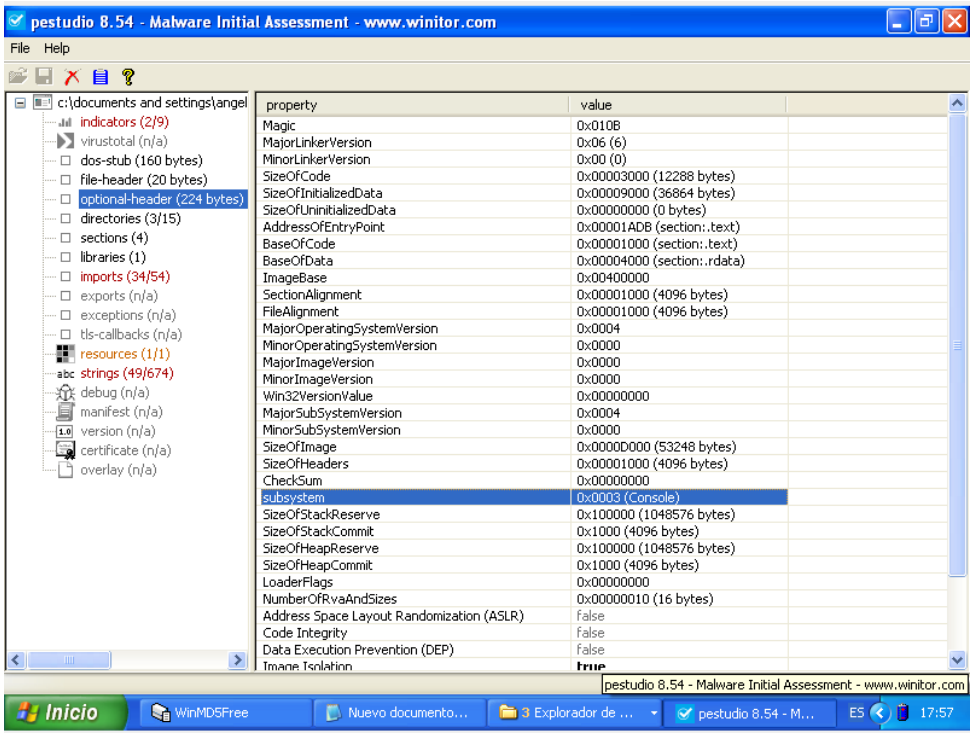


En la cual podemos observar los indicadores con su respectiva severidad, también podemos observar el encabezado del archivo (file-header)



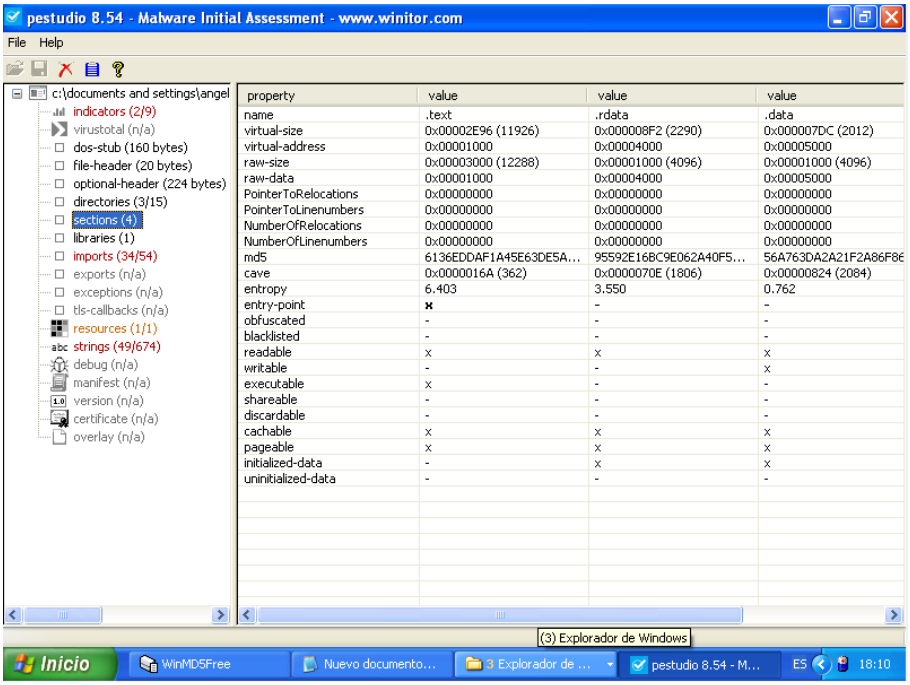
Donde podemos encontrar el sello de compilador con información importante como la fecha de compilación del archivo.

En el encabezado opcional (optional-header) podemos encontrar información importante como a que subsistema pueda afectar el archivo malicioso

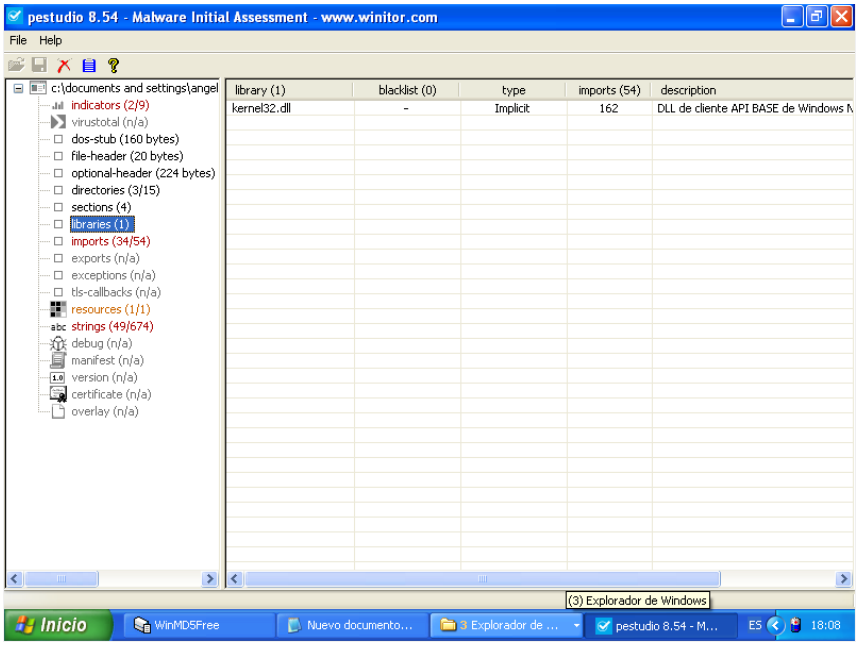


En el caso podemos ver que el subsistema que afecta es a la consola

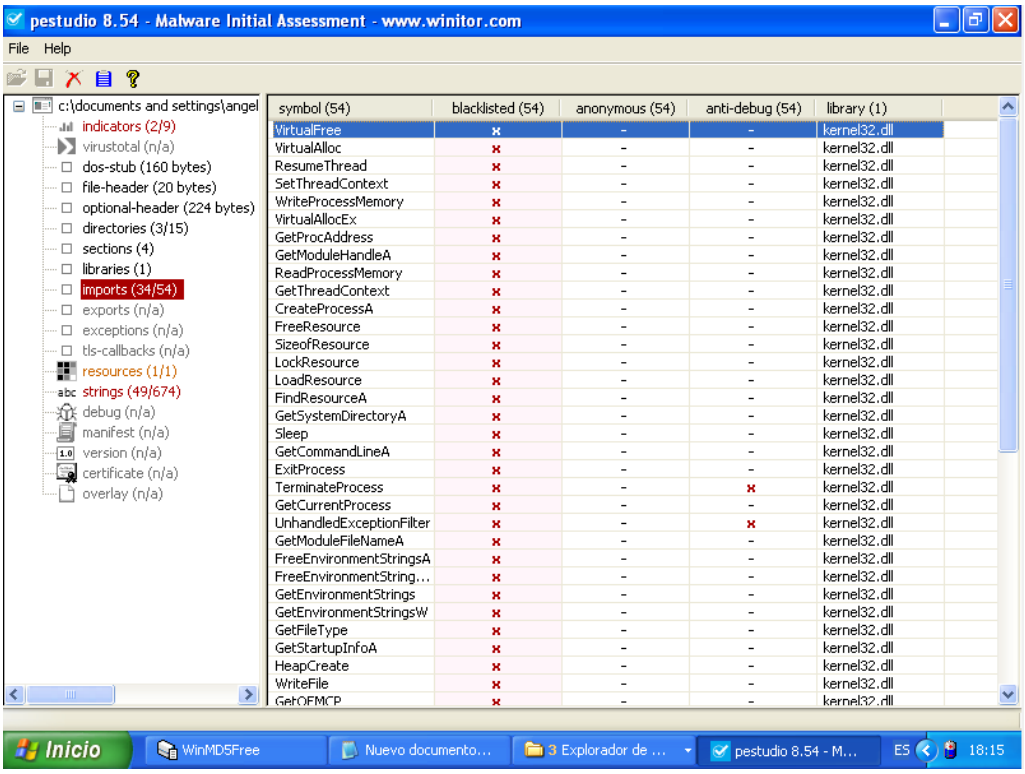
En sections podemos ver la información como ser que el archivo es un ejecutable además podemos ver los permisos que se indican con una **x**



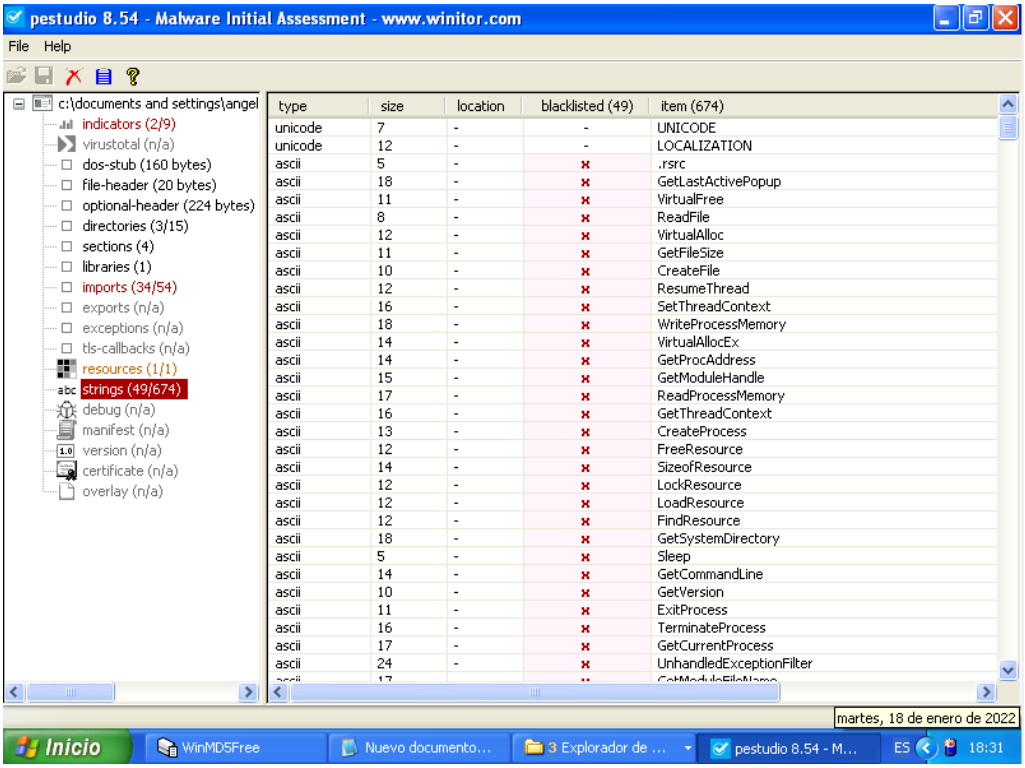
Podemos ver también las librerías



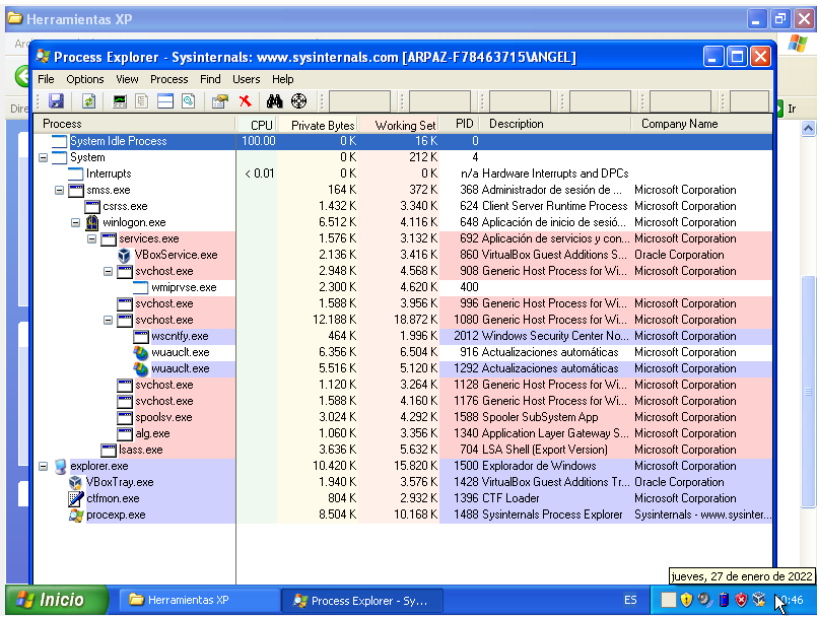
En Imports encontramos funciones importantes donde podemos observar que la mayoría de symbol o procesos se encuentran en la lista negra lo cual el programa los considera maliciosos, y además nos muestra la librería al cual corresponden.



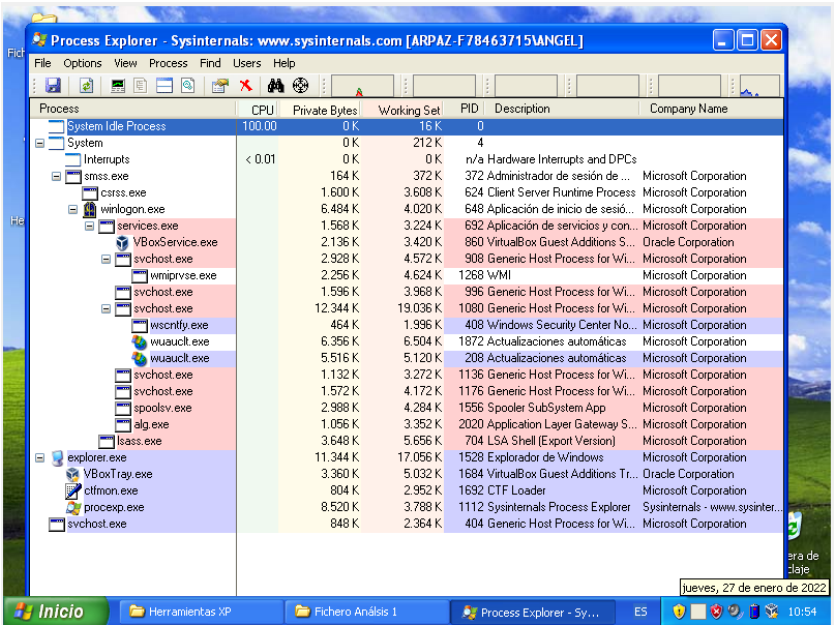
En los strings encontramos la siguiente informacion



Ejecución del Fichero Malicioso



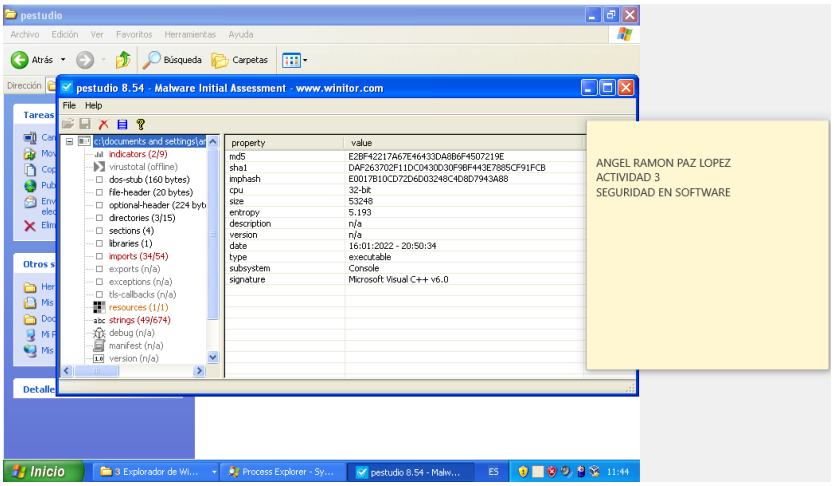
Antes de ejecutar



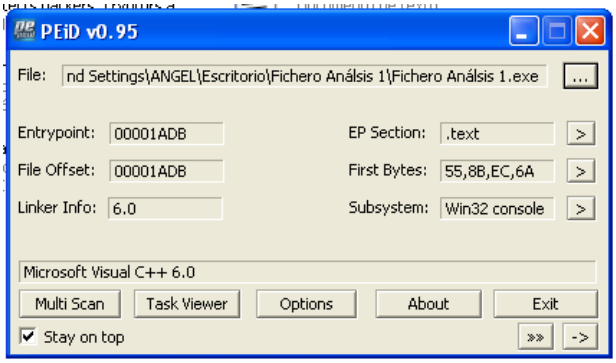
Después de Ejecutar el archivo Fichero Análisis 1.exe

Podemos observar que una vez que se ejecutó el malware se creó un proceso llamado svchost.exe el cual no tiene ningun proceso padre ni subprocesos es decir no tiene ninguna estructura lo cual es sospechoso.

1. **Hash MD5 de archivo malicioso.**

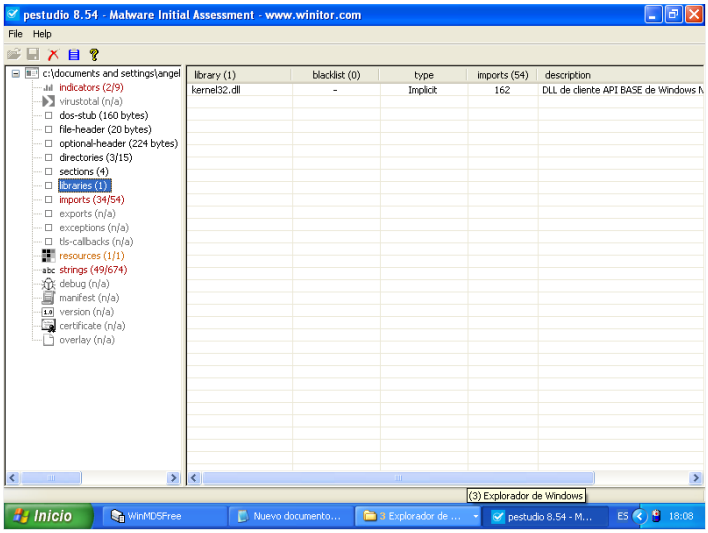


2. **¿Cuál es el punto original de entrada del ejecutable (OEP)?**



Con PEiD podemos ver que el punto de entrada del archivo malicioso es 00001ADB

3. **¿A qué DLL hace referencia el fichero?**



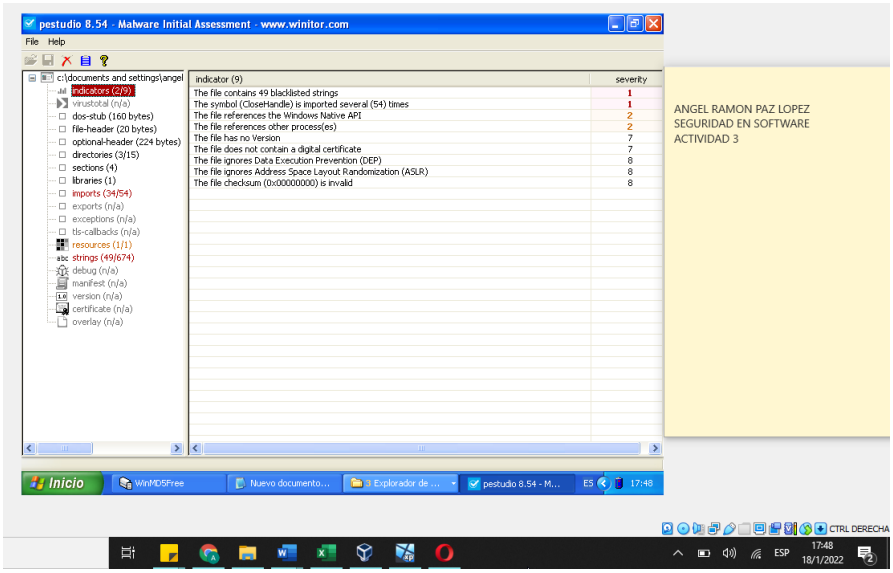
Con pestudio podemos ver con que librerías hace referencia el archivo malicioso en este caso podemos observar que es con kernel32.dll

4. **¿Esta comprimido el fichero? En caso afirmativo indique cual es el compresor.**

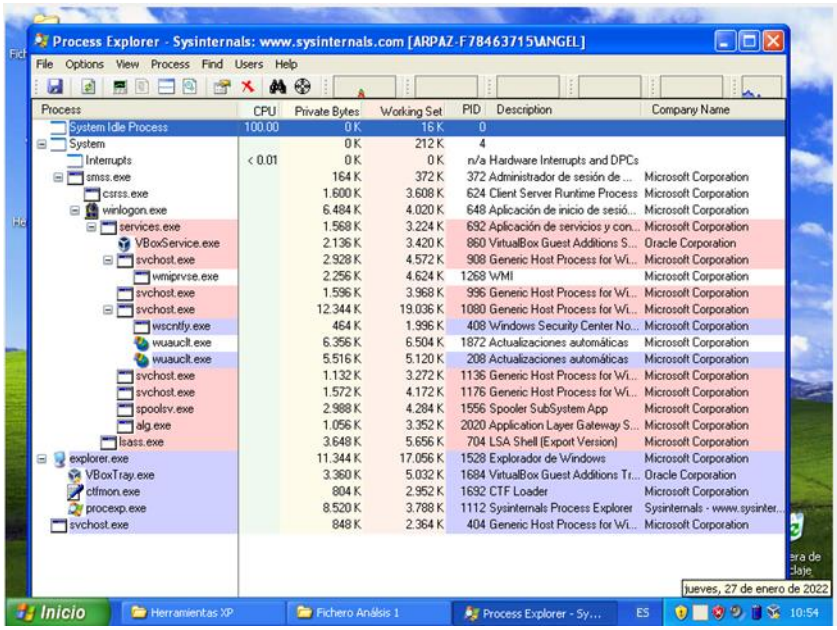
   No

5. **¿Qué indicadores sospechosos presenta el archivo?**

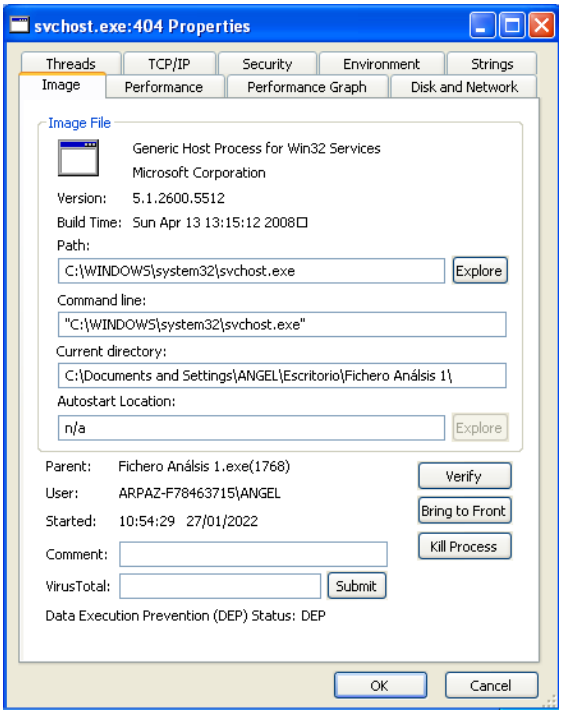
   Con la herramienta pestudio analizamos el archivo y nos muestra 9 indicadores



6. **¿Qué observas al supervisar este malware con Process Explorer?**



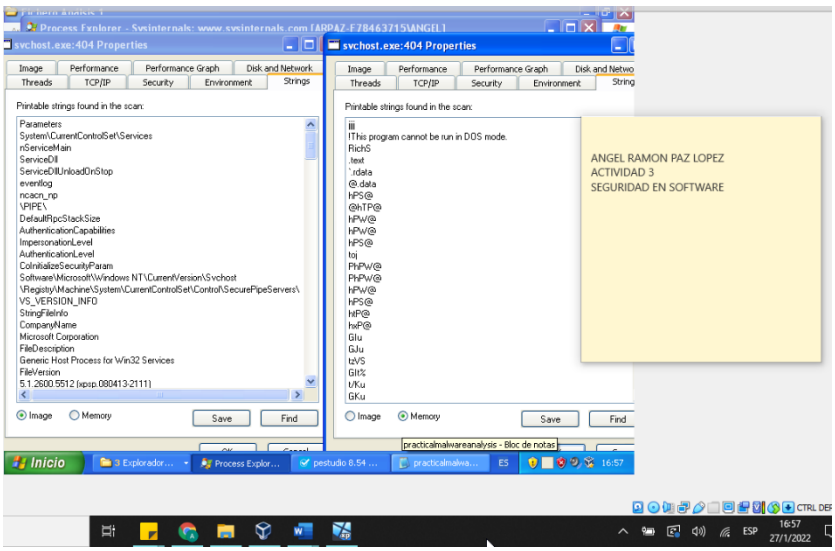
La creación de un proceso svchost.exe sin estructura y cuyas propiedades son sospechosas ya que tiene como padre el archivo de Fichero Análisis 1



7. **¿Puedes identificar modificaciones de las cadenas del proceso en memoria con respecto al disco?**

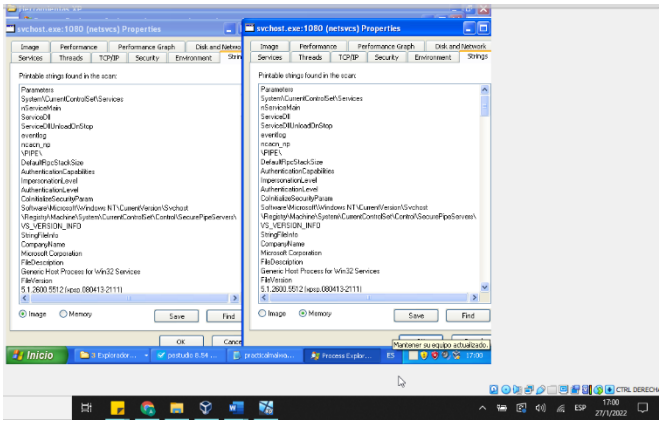
   Si, para ello con la misma herramienta de Process Explorer vemos el proceso huérfano svchost.exe por lo cual compararemos la imagen del proceso en disco con la imagen del proceso en memoria, también compararemos si contienen las mismas cadenas (strings) o son diferentes. Daremos clic derecho svchost.exe y clic en propiedades.

   Primero vemos el svchost.exe huerfano



Podemos observar que hay diferencias entre la imagen y lo que hay en memoria, y con ellos podemos sacar la conclusión de que es un archivo malicioso.

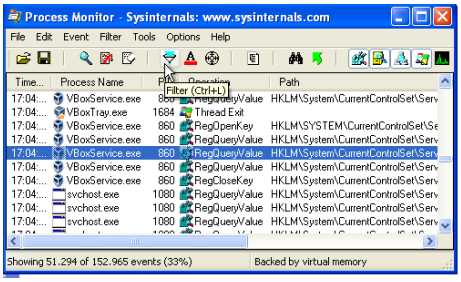
Ahora verificamos el otro archivo svchost.exe



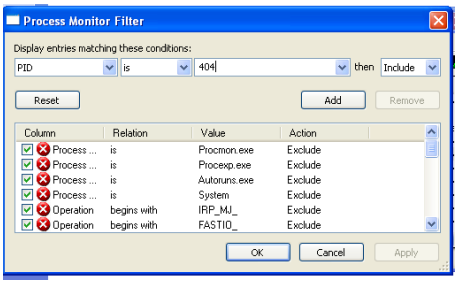
Comprobamos que en este caso no hay problemas ya que este archivo no es un malware

8. ¿Qué archivos crea?

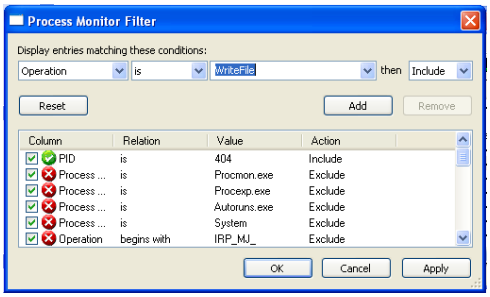
Ahora con Process Monitor averiguamos si crea con un archivo para ello configuraremos los filtros

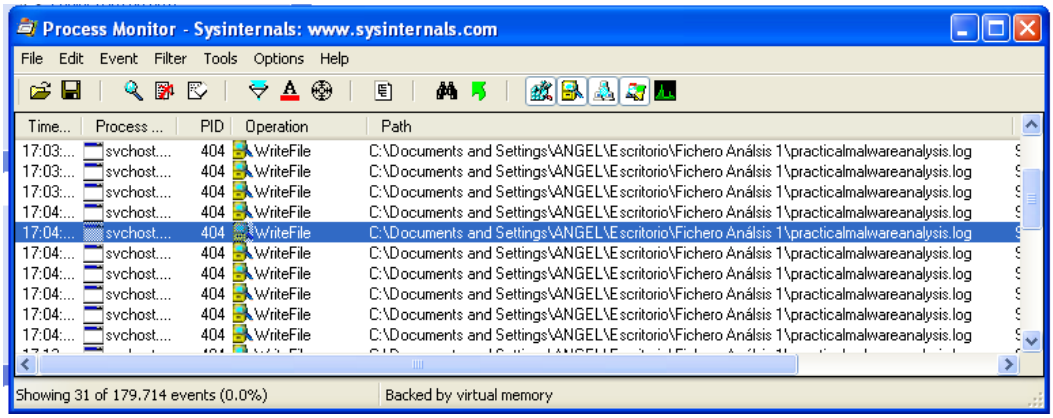


En el proceso anterior podemos ver que el PiD del archivo malicioso es 404 damos en Add

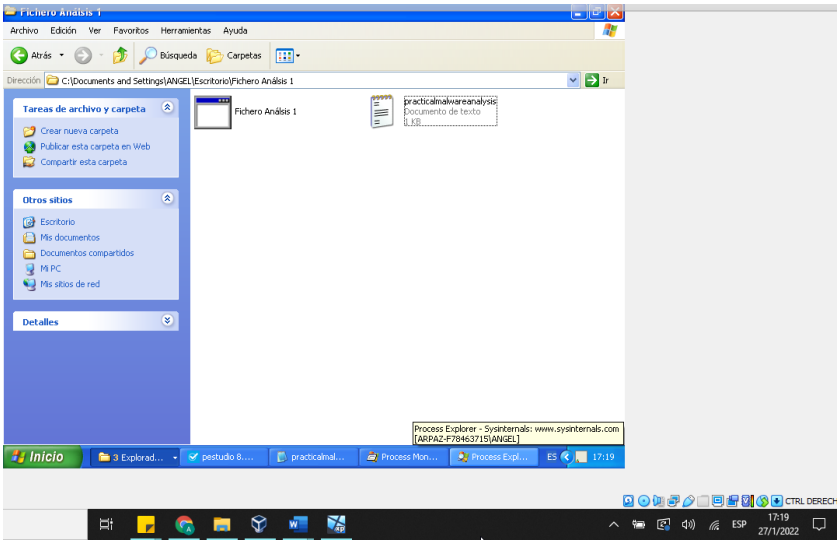


Despues colocamos otro filtro de Operación y colocamos WriteFile para ver si el malware crea o escribe en un archivo

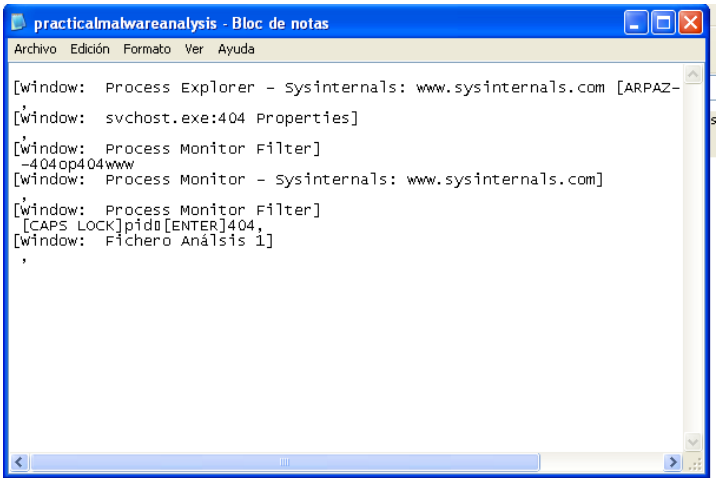




Podemos observar que este proceso malicioso esta escribiendo en un archivo llamado practicalmalwareanalysis.log lo cual lo podemos encontrar en el Path.

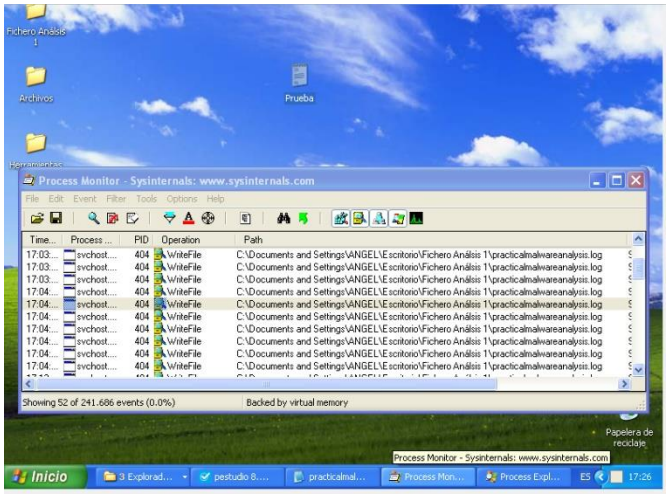


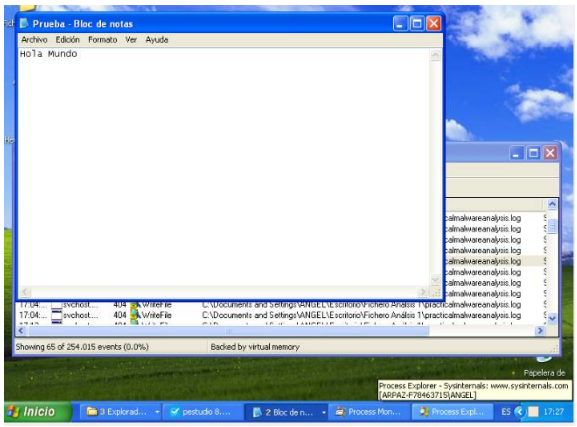
Y este es el contenido del archivo.



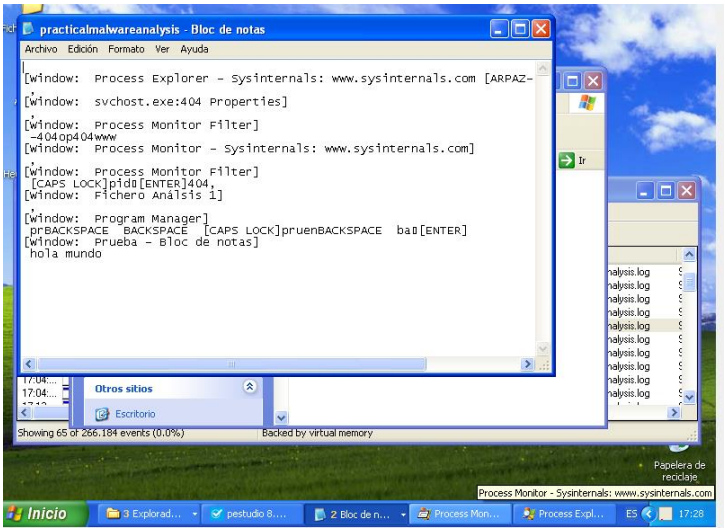
9. ¿Cuál es el propósito de este?

Con todos los procedimientos que hemos realizado en las anteriores preguntas podemos llegar a la conclusión de que el malware es un Keylogger ya que se han guardado las pulsaciones de tecla que habíamos hecho. Para confirmar nuestra conclusión crearemos un bloc de notas con el nombre de “Prueba” con la frase “Hola Mundo” y si en el archivo de Keylogger sale registrados damos por confirmado.





Ahora confirmamos en el archivo practicalmalwareanalysis.log



Y podemos verificar que se registró la creación del archivo de bloc de notas y la frase que escribimos.