PRÁCTICA : E3 - Asegurar la INTEGRIDAD de los datos en Windows / Linux **MF0486_3 : Seguridad en Equipos Informáticos**		**Fecha**	09 / 03 / 2022
		Página 1 de 3	
Curso	**7.1. MF0486_3 Seguridad en equipos informáticos**	**Plan de Formación**	FC-2021.1/II.000/1914256

Nombre y Apellidos:	**JAVIER PRUNELL ACOSTA**	**Firma del Alumno:**	
DNI:	54056005W	**Firma del Profesor:**	

Apto: ☐ **No Apto:** ☐ **Calificación:** ☐

Instrucciones Generales

La puntuación máxima será de 10 puntos.
Esta prueba tendrá una duración máxima de 420 minutos
(Temporalizados durante la Unidad de Aprendizaje)

El alumno/a deberá acatar las siguientes normas durante la duración de la práctica :

- Rellene el encabezado con su nombre, apellidos y D.N.I.
- Firme en todas y cada una de las hojas entregadas, incluidas las que estén en blanco.
- Usar exclusivamente bolígrafo azul o negro
- Guardar los ficheros generados en una carpeta con nombre **MF0486_E3**
- El docente le indicará al final como entregar el contenido de dicha carpeta
- Al finalizar el ejercicio y antes de entregarlo **comprueba tus respuestas**, en caso de duda consulta al docente.

Equipo y material

- Bolígrafo azul.
- Folios.
- Ordenadores.
- Conexión a Internet. (Para buscar información a modo de ayuda)
- **SFC :** Sistema operativo Windows (Virtualizado)
- **Rootkit Hunter :** Sistema operativo Linux (virtualizado)
- Pendrive.

Instrucciones específicas

El objetivo de esta práctica guiada será como se puede asegurar la **integridad** de los datos en sistemas Windows y Linux.

Condiciones de realización:

La actividad se llevará a cabo en el aula y el alumnado contará en todo momento supervisión del docente.

El alumnado contará con una duración de 420 minutos para realizar la práctica.
Se podrá realizar en varias partes con una duración cada una de 60 minutos.

El alumno podrá hacer uso de internet para su realización, y se detallan a continuación algunas webs de ayuda.

Páginas webs :

SFC (System File Check)

https://en.wikipedia.org/wiki/System_File_Checker
https://neosmart.net/wiki/sfc/
https://support.microsoft.com/es-es/kb/929833

rootkit

https://es.wikipedia.org/wiki/Rootkit
https://es.wikipedia.org/wiki/Rkhunter
https://rootkit.nl/projects/rootkit_hunter.html

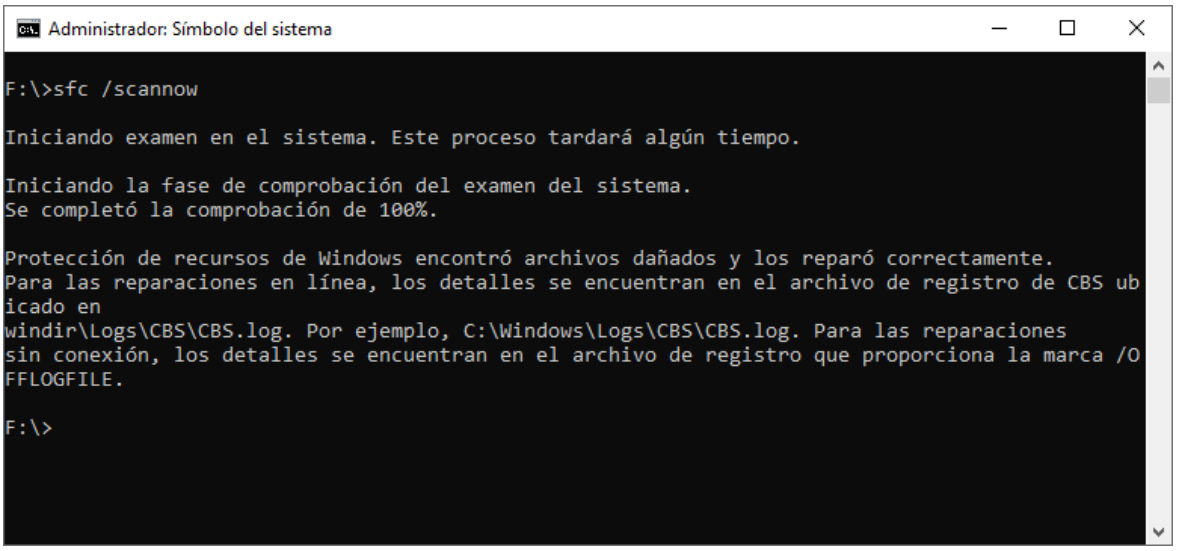
En ella se valorará la utilización de herramientas para la gestión del tiempo y secuenciación del uso de las aplicaciones necesarias. Y se observará especialmente la autonomía del alumnado a la hora de ejecutar y tomar decisiones. Como también la estructuración del ejercicio en donde se solicitará, orden, coherencia y limpieza.

Una vez terminado la práctica se le notificará al docente y pasará a su evaluación.

Descripción de la práctica

El SFC en Windows 10 es una utilidad en Microsoft Windows que permite a los usuarios buscar y restaurar archivos de sistema de Windows corruptos. En este caso, vamos a utilizar un pendrive para localizar y reparar archivos corruptos del mismo.

Abrimos el CMD con privilegios de administrador. Posteriormente accedemos a la unidad, en este caso el pendrive se encuentra en la unidad **F:** y ejecutamos el comando: **sfc /scannow**

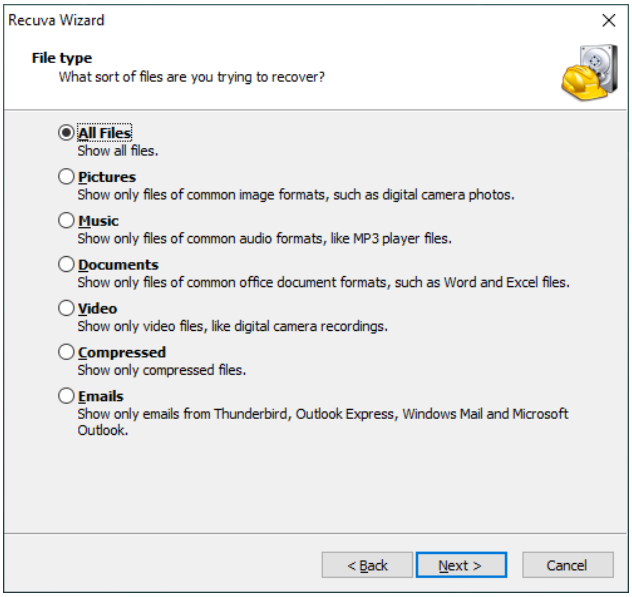


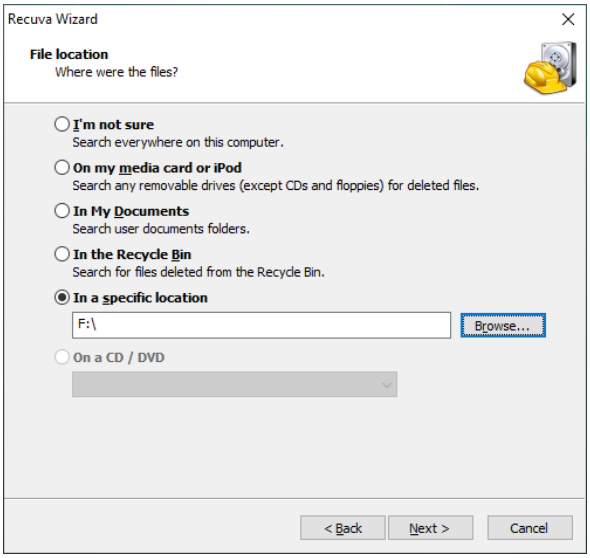
Para especificar más el comando SFC, tendremos que saber que:

```
/SCANNOW        Examina la integridad de todos los archivos protegidos del sistema y repara los archivos con
                problemas si es posible.
/VERIFYONLY     Examina la integridad de todos los archivos protegidos del sistema, pero no realiza
                ninguna reparación.
/SCANFILE       Examina la integridad del archivo al que se hace referencia y lo
                repara si se detectan problemas. Debe especificarse la ruta de acceso completa de <archivo>.
/VERIFYFILE     Comprueba la integridad del archivo con la ruta de acceso completa de <archivo>, pero no realiza ninguna
                reparación.
/OFFBOOTDIR     Para la reparación sin conexión, indica la ubicación del directorio de arranque sin conexión.
/OFFWINDIR      Para la reparación sin conexión, indica la ubicación del directorio de Windows sin conexión.
/OFFLOGFILE     Para la reparación sin conexión, puedes activar el registro si especificas la ruta del archivo de registro.
```

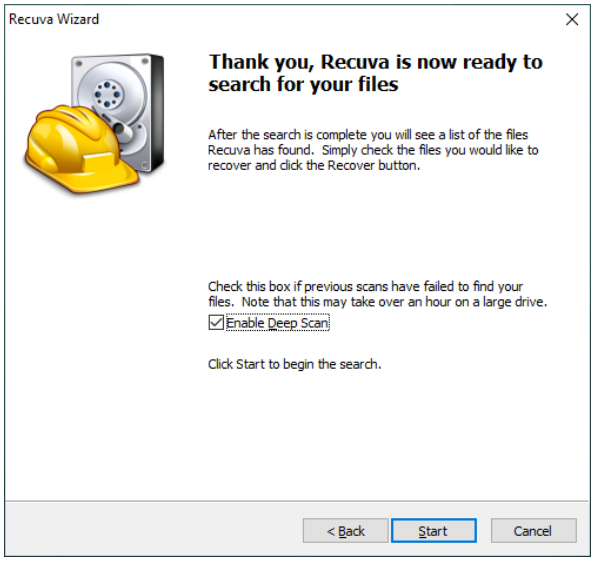
En este caso, tenemos la herramienta que Windows nos ha proporcionado. Por ello existen varios programas al respecto para verificar los discos duros. Uno de los más importantes es el Recuva.

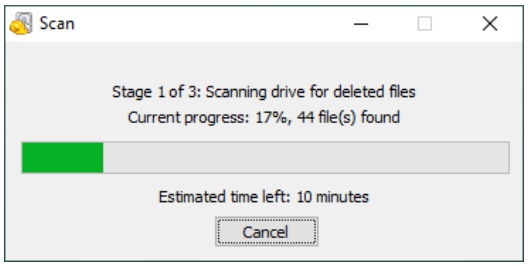
Vamos a verificar una unidad de disco con el programa Recuva. Después de la instalación, nos aparecerá un asistente donde le indicaremos que archivos pueden estar dañados o eliminados. De esta forma, seleccionamos todos los archivos y los ubicamos en el pendrive de la unidad **F:**



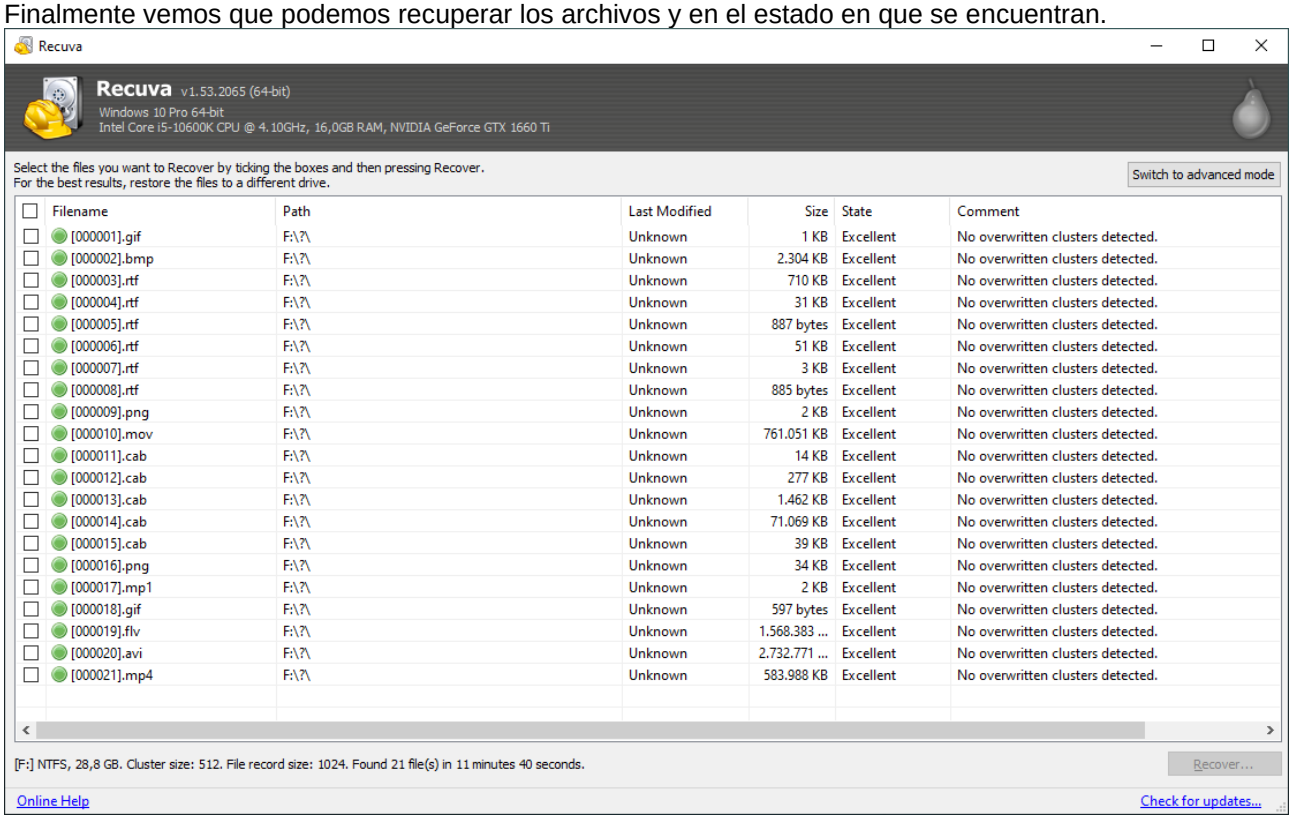


En la siguiente pantalla, podemos visualizar que podemos hacer un escaneo profundo. Recordar que este tipo de escaneo estará unido al tiempo. Cuando más grande es el disco duro, y a través de un escaneo profundo, pues más cantidad de tiempo.

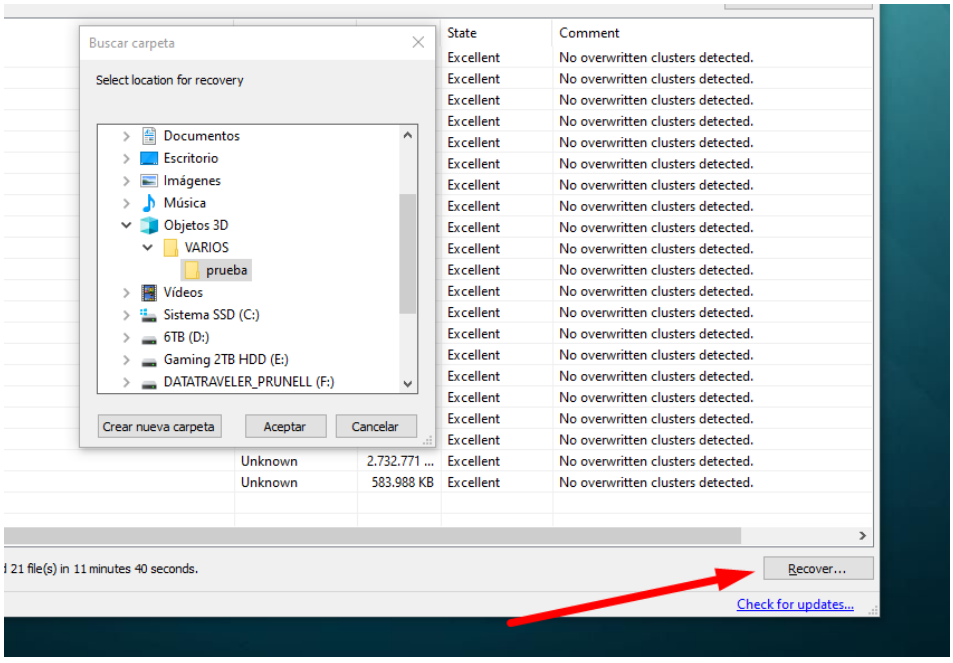




Finalmente vemos que podemos recuperar los archivos y en el estado en que se encuentran.



Al seleccionar los archivos, le damos a recuperar y seleccionamos el lugar de recuperacion.



Rootkit hunter

Rkhunter es una aplicación para la terminal de Linux que se encarga automáticamente a analizar nuestro sistema en busca de malware de forma masiva. Es importante destacara que es una herramienta gratuita.

Para su **instalación** debemos primeramente ir a cualquier distribución de Linux y ejecutar el comando:

sudo su install rkhunter -y

Después de la instalación es recomendable actualizar la base de datos de todo el malware que existe en el momento del análisis. Es importante aclarar que, dentro de la configuración de la actualización, tenemos que modificar un archivo para comentar una línea. Esta línea es de vital importancia para lograr que la actualización se realice.

Sudo rkhunter - -update

```
┌──(root㉿kali)-[/home/javier]
└─# sudo rkhunter --update
[ Rootkit Hunter version 1.4.6 ]

Checking rkhunter data files...
  Checking file mirrors.dat                                  [ Skipped ]
  Checking file programs_bad.dat                             [ Update failed ]
  Checking file backdoorports.dat                            [ Update failed ]
  Checking file suspscan.dat                                 [ Update failed ]
  Checking file i18n versions                                [ Update failed ]

Please check the log file (/var/log/rkhunter.log)
```

Después de su instalación, procedemos a la configuración y ejecución del mismo, ya que es un programa que no se ejecuta automáticamente, no nos encontramos antes un **Daemon** de Linux. Para ello, tenemos que ejecutarlo con:

Sudo rkhunter - -ckeck

De esta forma, el programa analiza todo el sistema y se genera una base de datos para que se analice cuando se le pida.

Finalmente, el programa nos genera un archivo log con la información del sistema.

```
System checks summary
=====================

File properties checks...
    Required commands check failed
    Files checked: 146
    Suspect files: 1

Rootkit checks...
    Rootkits checked : 497
    Possible rootkits: 3

Applications checks...
    All checks skipped

The system checks took: 1 minute and 58 seconds

All results have been written to the log file: /var/log/rkhunter.log

One or more warnings have been found while checking the system.
Please check the log file (/var/log/rkhunter.log)
```

CHKROOTKIT

Para reconocer, eliminar y escanear el sistema a través de Linux, tendremos otro malware llamado CHKROOTKIT. Inicialmente vamos a instalarlo para comprobar cómo funciona.

Apt install chkrootkit

Comprobamos que ante este malware, también debemos modificar algunos archivos del programa, en este caso, /etc/chkrootkit.conf, buscamos la primera línea con: **RUN_DAILY=<<verdadero>>**

A continuación, podemos ejecutar el programa fácilmente introduciendo: **chkrootkit**