Turbo_Resumen_Express.txt

la informatica forense es el proceso de identificar, preservar, analizar y presentar evidencias de una forma legar y aceptable aplicando técnicas científicas y analíticas especializadas a la infraestructura tecnológica.
Principio de locardx: siempre que dos objetos entran en contacto transfieren parte del material que incorporan al otro objeto

Funciones o ambito de actuacion
recopilación y preservacion de pruebas digitales
Analissi de pruiebas
Recuperacion de datos
investigacion de incidentes de seguridad
analisis de redes y cominicaciones
creacion de informes y testimonio en tribunales
asesoria y capacitacion
investigacion y desarrollo

Guias para el proceso de investifgdacion forense

Estandares:
AENOR e IOS/IEC

Familia 71505:
-1 Vocabulario y principios generales
-2 Buenas prácticas
-3 Formatos y mecanismos técnicos

UNE 71506: Metodología para el análisis forense de las evidencias
- Preservación
- Adquisición
- Docimentación
- Anbalisis
- Presentacion

UNE 1927010: Criterios generales para elaboración de informes

ISO 27037 Guias para identificación, recolección, adquisición y preservacion de evidencias digitales
ISO 27042: Guias para el analisis e interpretación de evidencias

Proceso de investigación forense (Preparación, identificacion, adquisición, preservacion, analissi y presentacion PIAPAP)
1. Preparación del caso
Es importante hacer una preparación previa para poder adquirir las evidencias correctamente y que todo sea correcto legalmente: contar con los permisos, autorización y contrato

Aseguirar la escena para evitar modificación o destrucción de las evidencias digitales

2. Identificación
Consiste en detectar y localziar fuentes de evidencia digital
Se debe determinar la fuente de los datos, ubnicación y relación con el incidente investigado
Incluye la evaluación preliminar de los dispositivos y mdedios de almacenamiento apra evitar alteraciones
Revisar entorno legal que protege el bien
INICIO de cadena de custodia

2.1 Revisión de enterono legarl que protege el bien
Analizar normativas y regulaciones aplicables a la evidencia digital y al bien protegido, asegurando que la recolección, adquisición y análisis de los datos se realicend e manera legarl y sean adminisibles en un proceso judicial

2.2 Cadena de custodia
Procedimiento mediante el cual se garantiza la autenticidad de la prueba digital desde su obtención hasta que se aporta como hecho porbatorio a un procedimiento judicial.

Es fundamental mantener la cadenad e custodia para garantizar que la evedencia digital sea adminisble en un tribunal.
Para garantizar la cadena de custiodia se debe documentar detalles de:
- descubrimiento y recolección de la evidencia
- Manejo de la evidencia
- Quien custodió la evidencia
- Cambios de custodia

3. Adquisición

Recopilación de pruebas digitales de dispositivos electrónicos usando técnicas y herramientas especializadas para garantizar la integridad y autenticidad de los datos
Debe documentarse para garantizar la cadena de custodia.
La adquisición se debe hacer por orden de volatilidad, comenzando por registros y cache, pasando a ram, archivos temporales, disco....

Hay 2 modos de adquisición:
- Live: compleja, se hace volcado de RAM y se tira del cable
- DEAD: más siple, se tira del cable a machete

Clonado: consiste en realizar una copia exacta bit a bit de un disco, incluyendo errores osectores defectuosos.
Objetivos: Disponer de una copia sobre la que realizar el analisis sin alterar la prueba.
HHerramientas: dd, dcfldd, dc3dd, FTK Imager
OJO: NO SE DEBE MONTAR NUNCA EL DISCO

clonado dd: DD if=/dev/sda of=/dev/sdb bs=1M

Integridad: es preciso asegurar que los datos clonados son una copia original, para ello se usan funciones hash SHA-2 o SHA-3, aunque en caso de no disponer de estas se pueden combinar MD5 y SHA-1
Si se hace clonado con dc3dd se puede comprobar al vuelo: dc3dd if=/dev/sdb of/imagen5.img hash=md5,sha256

4. Preservación

Adecuado tratamiento y documentación de las evidencias garantizando la cadena de custodia. se deben documentar los procedimientos

5. Analisis+
Examinar los datos recopilados
Autopsy, creado por brian portaaviones, open source,, permite trabajo en equipo y es multiplataforma

Volatility: Analisis forense de memoria, tiene 2 versiones

6. Presentación de los resultados
recopilar y documentar toda la onfo obtenida para genrar un informe pericial.

El perito informatico es un experto en tecnologías de la información y sistremas informáticos
El perito forense es un experto en ciencias forenses
El perito informatico forense es un experto en informatica forense especializado en la identificación, preservación, análisis y presentación de pruebas digitales en investigaciones y casos legales.

El perito judicial es unn profesional adotado de conocimientos especializados y reconocidos a través de sus estudios superiores que suministra información u opinión fundada a los tribunales de justicia sobre los puntos litigiosos que son materia de siu dicatamen

Perito de oficio: elegido por juez o tribunal
Perito de parte: Elegido por una de las partes y luego aceptado por juez o fiscal

código deontológico
Es un código de ética profesional que recoge un concepto de criterios, normas y valores que redacta y aceptan los profesionales de una actividad

Responsabilidades: Civilm penal, disciplinaria y provesional

Cuerpo oficial de Peritos colegiados (COP, conjunto de peritos colegiados.

Normativas en españa
LOPDGDD
Codigo Pejal
Ley de enjuiciamiento civil
Ley de enjuiciamiento Criminal
Ley de Servicios de la Sociedad de la informacióny comercio electrónico
Ley orgánica de protección de la seguridad ciudadana
Ley de conservación de datos

LOPDGDD: Regula la protección de datos personales en españay garantiza los derechos diitales de los ciudadanos. Está en consonancia con el GDPR que establece los requisitos estruicvtos en relaci

El codigo penal español contiene disposiciones para delitos informaticos

La ley de enjuiciamiento civil regula los procedimientos y procesos en casos civiles en españa

---

Analisis forense en windows

Un artefacto se refiere a cualquier objeto, dato o elemento almacenado en un sistema informático que pueda proporcionar información valiosa para una investigación. Hay 2 tipos:
- de aplicación
- de sistema operativo

Archivos de registro o logs
son artefactos interesantes en cualquier OS
Contienen información de eventos específicos, apps y servicios

Event logs: registros que se pueden encontrar en el event viewer o eventvwr.msc y están organizados en diferentes categorías como aplicación,

seguridad configuración y sistema. Aqui se peuden ver inicios de sesión, cambios de configuracion, fechas de acceso, permisos....
Los event losgs se pueden encontrar en %systemRoot%/System32/config o %SystemRoot%/system32/winevt/Logs dependiendo de si es previo o posterior a vista

Registros de aplicaciones
Muchas apps generan sus propios registros, se pueden encontrar en %APPData% para ususarios específicos o en %ProgramData% para todo el equipo

Registros sobre la instalación

Mirando en la raiz del sistema pueden ser:
- setupact.log: acciones de instalación
- setuperr.log errores de instalación
- WindowsUpdate.log: Actualizaciones del sistema y apolicaciones
- Debug/mrt.log Resultados de la erramienta de eliminación de malware de windows.
- Security/logs/scecomp.old: Componentes de windows que no se pudieron instalar
- /softwareDistribution/reportingEvents.log: Contiene eventos relacionados con la actualización
- /Logs/CBS/CBS.log: Almacena info relacionadas con el component based servicing, que se usa para administrar actualizaciones del sistema
- /inf/setupapi.dev.log: detecciones de nuevo dispositivo o actualización de driver existente
- /inf/setupapi.app.log: Instalación de componentes o aplicaciones
- /inf/setupapi.setup.log: Operaciones de instalación o config de windows
- /inf/setupapi.offline.log: Procesos o reparaciones realizados en modo fuera de linea
- /PANTHER*.log,xml: Información de acciones, errores cuando se actualiza desde una versión anterior de windows.
- /Performance/Winsat/winsat.log: Trazas de utilización de Windows System Assessment tool (WINSAT)

Papelera de reciclaje

Puede contener archivos borrados así como la fecha, hora y ubicación de la que fueron borrados
- En Windows 95 se encuentra en C:/RECYCLED
- En Sistemas NT pre VISTA en C:/RECYCLER
- en sistemas Post Vista en C:/$Recycle.Bin

En el interior de la carpeta de cada usuario hay 2 tipos de archivos:
- $I: Contienen el nombre,ruta y algunos datos del archivo
- $R: Contienen el contenido del arcivo original

Registro de Windows (Windows Registry)

Base de datos jerárquica que contiene info y conffig del SO y el HW, además de apps instaladas y preferencias de usuarios.
- Frecuencia y tiempo de uso de apps: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist, Se peude visualizar con USERAssistView
- Dispositivos USB conectados: HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Enum/USBStor
- Asociaciones de tipos de archivos y programas predeterminados: HKEY_CLASSES_ROOT/.<extension>

HKEYs

El registro de Windows se divide en varias secciones principales llamadas HKEYs (Handle to Registry Key)_
- HKEY_CLASSES_ROOT (HKCR): Info sobre tipos de archivos, extensines, asociaciones....
- HKEY_CURRENT_USER (HKCU): Info sobre configuraciones y preferencias de un usuario en la sesión actual.
- HKEY_LOCAL_MACHINE (HKLM): Guarda configuraciones y datos relacionados con Hardware, software y controladores del sistema
- HKEY_USERS (HKU): Almacena configuraciones y preferencias de todos los usuarios del sistema
- HKEY_CURRENT_CONFIG (HKCC): Contiene info sobre el perfil de hardware activo

Hives

El registro se agrupa en secciones lógicas conocidas como Hives, que son un grupo de claves, subclaves y valores relacionados con una parte específica del SO o las configs del usuario
Permiten organizar y estructurar la infod el registro, facilitando su administración y mantenimiento. Cada Hive se respalda en Hive Files que contienen copias de seguridad de sus datos.
- Los hives de respaldo para todos los hives (Salvo HKEY_CURRENT_USER) están en %SystemRoot%/System32/config.
- Los hives de respaldo para HKEY_CURRENT_USER estan en %UserProfile%

Algunos Hive files importantes son los siguientes:
- %SystemRoot%/System32/config/SAM: HKEY_LOCAL_MACHINE/SAM, archivos de Security Accounts Manager, contiene info de cuentas de usuario y sus contraselas hasheadas
- %SystemRoot%/System32/config/SECURITY: HKEY_LOCAL_MACHINE/SECURITY: Configuraciones de políticas de contraseña, bloqueo de cuentas, privilegios y control de acceso
- %SystemRoot%/System32/config/SOFTWARE: HKEY_LOCAL_MACHINE/SOFTWARE:

```
Detalles sobre las aplicaciones instaladas
- %SystemRoot%/System32/config/SYSTEM: HKEY_LOCAL_MACHINE/SYSTEM: Detalles
sobre el hardware de sistema, contiene también la clave de cifrado de las
contraseñas almacenadas en SAM
- %SystemRoot%/System32/config/DEFAULT: HKEY_USERS/DEFAULT: Contiene la
configuracion de usuario predeterminada
- %UserProfile%/NTUSER.DAT: HKEY_USERS/<USER_ID>: Preferencias específicas
del usuario.
- %UserProfile%/AppData/Local/Microsoft/Windows/UsrClass.dat:
HKEY_CURRENT_USER\Software\Classes: Contiene información de las preferencias
específicas del usuario
```