SEGURIDAD INFORMÁTICA

JOSÉ PABLO HERNÁNDEZ

SEGURIDAD INFORMÁTICA

3.3.1.MF0488_3. Capítulo 3
Parte 2
Análisis forense informático

JOSÉ PABLO HERNÁNDEZ

4. GUÍA PARA LA RECOGIDA DE EVIDENCIAS ELECTRÓNICAS

Conceptos imprescindibles:

- **Evidencias volátiles y no volátiles.**
- **Etiquetado de evidencias.**
- **Cadena de custodia.**
- **Ficheros y directorios ocultos.**
- **Recuperación de ficheros borrados.**

4.1. EVIDENCIAS VOLÁTILES Y NO VOLÁTILES

Las evidencias digitales se clasifican en evidencias volátiles y no volátiles:

- **Las evidencias volátiles** son aquellas que se pierden cuando se apaga el equipo (estado de la memoria, procesos en ejecución, etc.).
- **Las evidencias no volátiles**, sin embargo, se almacenan en el sistema de ficheros y no se pierden al apagar el equipo (aplicaciones, configuraciones, etc.).

4.1. EVIDENCIAS VOLÁTILES Y NO VOLÁTILES

Orden de preservación de las evidencias digitales:

- Registros, memoria caché, memoria de periféricos
- Memoria física
- Estado de las conexiones de red
- Ficheros temporales del sistema
- Procesos que se están ejecutando en ese momento
- Discos duros, rígidos
- Archivos de backups
- Registros y datos de monitorización remotos relevantes
- Configuración física y topología de la red
- CD-ROM, impresiones

4.2. ETIQUETADO DE EVIDENCIAS

Para que las evidencias se puedan admitir como tal deben cumplir con una serie de requisitos:

- Deben conservarse en un estado lo más parecido posible al estado en el que se encontraron.
- En la medida de lo posible, debe realizarse una copia exacta de la evidencia original para realizar los trabajos de investigación sobre la misma y no dañar los datos originales.
- Las copias realizadas deberán realizarse en medios estériles, es decir, en medios que no hayan contenido ningún dato anteriormente.
- Las evidencias deberán etiquetarse y documentarse debidamente en la cadena de custodia. Además, cada acción realizada sobre la evidencia o sobre su copia deberá ser también documentada con detalle.
- Las evidencias digitales deberán documentarse con firmas digitales del investigador para garantizar que nadie más realiza ninguna acción sobre ellas.

4.2. ETIQUETADO DE EVIDENCIAS

En el momento de etiquetar las evidencias digitales hay que tener en cuenta que se clasifican en varias categorías:

- Registros generados por ordenador.
- Registros almacenados por ordenadores.
- Registros híbridos.
- Registros de cada servidor.
- Registros de tráfico de red.
- Registros de aplicación.

4.2. ETIQUETADO DE EVIDENCIAS

Criterios de admisibilidad de evidencias electrónicas	
Autenticidad	La evidencia debe haber sido generada y registrada en la escena del crimen y debe mostrar que los medios utilizados no se han modificado.
Confiabilidad	Las evidencias serán confiables si el sistema que las produjo no ha sido violado y estaba funcionando correctamente cuando se recibió, almacenó o generó la prueba.
Completitud o suficiencia	La evidencia debe estar completa, tiene que haberse mantenido su integridad.
Respeto por las leyes	Las técnicas de recolección y tratamiento de la evidencia deben cumplir las normativas legales vigentes en el ordenamiento jurídico.

4.3. CADENA DE CUSTODIA

La cadena de custodia debe:

- Reducir todo lo posible la cantidad de agentes que traten las evidencias.
- Mantener la identidad de las personas implicadas en todo el proceso de gestión de la evidencia.
- Asegurar la firmeza de las evidencias cuando estén almacenadas para asegurar su protección.
- Registrar los tiempos firmados por cada agente en los intercambios de evidencias entre ellos para detectar al responsable de su tratamiento en cada momento.

4.4. FICHEROS Y DIRECTORIOS OCULTOS

En el momento de realizar la recolección de evidencias hay que tener en cuenta que puede haber evidencias escondidas en ficheros o directorios ocultos.

Es más, los atacantes suelen esconderse en archivos ocultos, por lo que es fundamental averiguar su localización y de qué tipo son para considerar si pueden ser evidencias ocultas o si deben descartarse por ser archivos inofensivos.

4.5. INFORMACIÓN OCULTA DEL SISTEMA

También deben encontrarse los distintos parámetros e informaciones del sistema que se han mantenido ocultos para protegerlos de atacantes para comprobar si han sido alterados.

4.6. RECUPERACIÓN DE FICHEROS BORRADOS

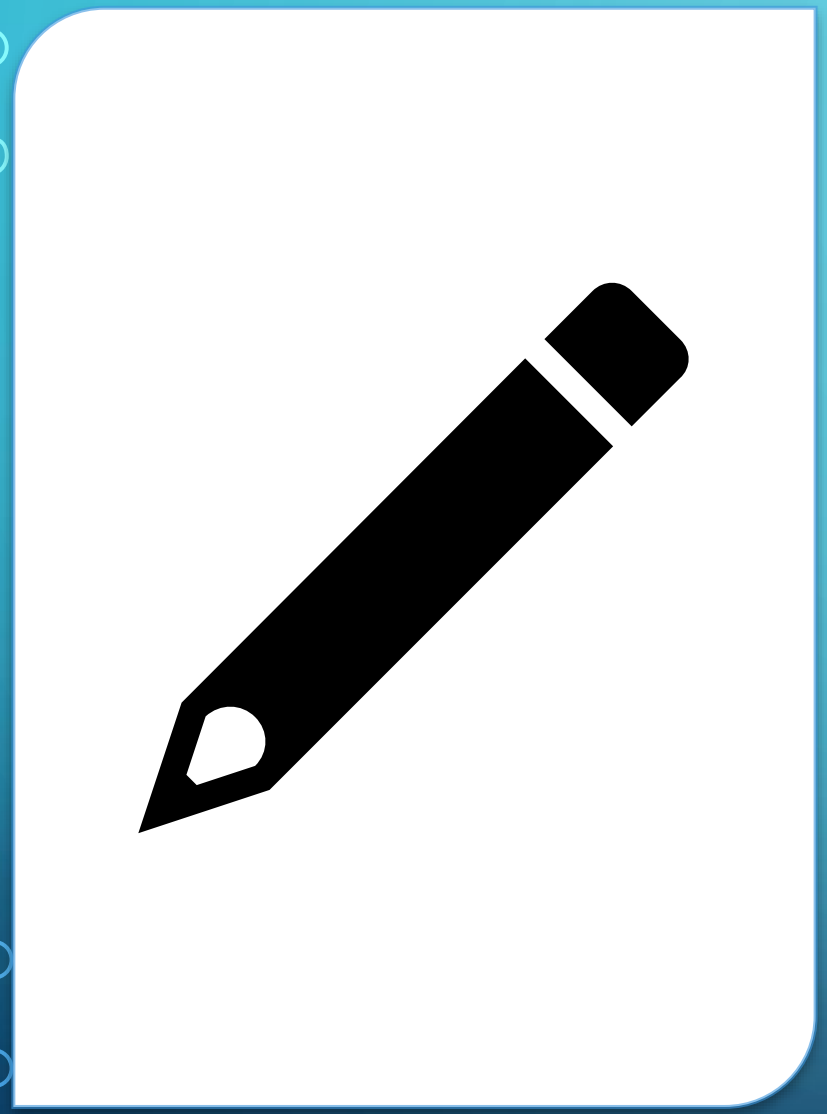
En general, cuando un archivo se elimina no es borrado definitivamente, sino que se mantiene en la papelera de reciclaje durante un período determinado. Es más, cuando este archivo se borra de la papelera de reciclaje queda marcado como borrado pero sigue físicamente en el disco duro a pesar de estar oculto para los usuarios.

En cuanto al análisis forense se recomienda localizar estos archivos eliminados que no han desaparecido definitivamente del equipo para intentar descubrir archivos sospechosos y, por lo tanto, posibles evidencias digitales.

4.6. RECUPERACIÓN DE FICHEROS BORRADOS

En general, cuando un archivo se elimina no es borrado definitivamente, sino que se mantiene en la papelera de reciclaje durante un período determinado. Es más, cuando este archivo se borra de la papelera de reciclaje queda marcado como borrado pero sigue físicamente en el disco duro a pesar de estar oculto para los usuarios.

En cuanto al análisis forense se recomienda localizar estos archivos eliminados que no han desaparecido definitivamente del equipo para intentar descubrir archivos sospechosos y, por lo tanto, posibles evidencias digitales.



Ejemplo.

REALIZANDO UNAS TAREAS DE SU TRABAJO HABITUAL HA SALTADO UNA ALARMA EN EL EQUIPO DE UN INTENTO DE ATAQUE. A CONSECUENCIA DE LA ALARMA SE HA ASUSTADO Y HA APAGADO EL EQUIPO DIRECTAMENTE SIN GUARDAR NADA. ¿HA HECHO BIEN? ¿QUÉ EFECTOS PUEDE CONLLEVAR APAGAR EL ORDENADOR JUSTO EN EL MOMENTO DE PRODUCIRSE UN ATAQUE? ¿CUÁL SERÍA EL PROCEDIMIENTO CORRECTO?

Ejemplo. Solución

CUANDO APARECE UN ATAQUE EN EL EQUIPO NO SE DEBE APAGAR EL SISTEMA DE INMEDIATO PORQUE SE PUEDEN PERDER TODOS LOS DATOS DE LAS EVIDENCIAS VOLÁTILES QUE PERMITAN IDENTIFICAR AL ATACANTE Y TODOS LOS HECHOS SUCEDIDOS.

ANTES DE APAGAR EL EQUIPO DEBE REALIZARSE UNA COPIA DE LAS EVIDENCIAS VOLÁTILES (ACTUANDO POR ORDEN DE VOLATILIDAD) QUE PERMITA ANALIZARLAS UNA VEZ HAYAN DESAPARECIDO DEL EQUIPO.

Ejemplo.

ESTÁ EN PROCESO DE RECOLECCIÓN Y ANÁLISIS DE EVIDENCIAS, HA HECHO UNA COPIA DE LAS EVIDENCIAS ELECTRÓNICAS EN UN DISCO DURO EXTERNO Y, POSTERIORMENTE, HA ALMACENADO OTROS ARCHIVOS EN EL MISMO DISCO DURO. ¿LAS EVIDENCIAS RECOGIDAS EN ESE DISCO DURO SERÍAN ADMISIBLES? ¿SE INCUMPLE ALGÚN CRITERIO DE ADMISIBILIDAD? ¿CUÁL? ¿QUÉ SERÍA LO MÁS RECOMENDABLE PARA ALMACENAR COPIAS DE EVIDENCIAS?

Ejemplo. Solución

PARA QUE LAS EVIDENCIAS RECOGIDAS EN UN SOPORTE O MEDIO INFORMÁTICO SEAN ADMISIBLES ES INDISPENSABLE QUE ESE MEDIO NO RECIBA NINGUNA MODIFICACIÓN POSTERIOR, POR LO QUE EN ESTE CASO LAS EVIDENCIAS DEL DISCO DURO NO SE PODRÍAN ADMITIR AL HABER GUARDADO OTROS ARCHIVOS EN ÉL.

EN ESTE CASO SE INCUMPLE EL PRINCIPIO DE AUTENTICIDAD DE LA EVIDENCIA ELECTRÓNICA EN EL QUE SE INDICA QUE: “LA EVIDENCIA DEBE HABER SIDO GENERADA Y REGISTRADA EN LA ESCENA DEL CRIMEN Y DEBE MOSTRAR QUE LOS MEDIOS UTILIZADOS NO SE HAN ALTERADO”.

PARA QUE LAS EVIDENCIAS ELECTRÓNICAS SEAN ADMISIBLES EN CUANTO A AUTENTICIDAD SE RECOMIENDA QUE LOS MEDIOS QUE ALMACENAN LAS EVIDENCIAS NO SEAN MODIFICADOS PARA EVITAR INFORMACIÓN ERRÓNEA QUE PUEDA ALTERAR LOS RESULTADOS DEL ANÁLISIS.

5. GUÍA PARA EL ANÁLISIS DE LAS EVIDENCIAS ELECTRÓNICAS RECOGIDAS

Una vez recopiladas las evidencias digitales y almacenadas adecuadamente, el análisis forense digital debe encargarse de la reconstrucción y temporalización de los hechos ocurridos con los datos recopilados.

Con este análisis deberán recopilarse los hechos desde el momento inicial del incidente hasta su descubrimiento y se dará por finalizado cuando se detecte quién realizó el ataque, cómo se produjo, cuál fue su objetivo y bajo qué circunstancias se cometió.

5.1. PREPARACIÓN DEL ENTORNO DE TRABAJO PARA EL ANÁLISIS

Se aconseja preparar dos estaciones de trabajo:

- Una de ellas deberá contener dos discos duros: en uno se instalará el sistema operativo que servirá de anfitrión y con el que se realizará el análisis de las evidencias y en otro se volcará la imagen del disco duro del equipo atacado.
- En la otra estación de trabajo se instalará un sistema operativo configurado exactamente igual que el equipo atacado.

5.2. RECONSTRUCCIÓN DE LA SECUENCIA TEMPORAL DEL ATAQUE

Se deberá recopilar y analizar la siguiente información de los ficheros:

- Tamaño y tipo de fichero.
- Usuarios y grupos a los que pertenece el fichero.
- Permisos de acceso.
- Detección sobre si el fichero fue borrado o no.
- Trazado de ruta completo.
- Marcas de tiempo: fecha y hora de su creación, modificación, borrado y acceso.

5.3. DETERMINACIÓN DE CÓMO SE REALIZÓ EL ATAQUE

Cuando ya se ha determinado el orden de los acontecimientos producidos en el ataque deberá realizarse un análisis para detectar cómo se accedió al sistema, investigando las vulnerabilidades de las que se haya podido aprovechar el atacante para acceder a este.

También se deberá investigar cuáles fueron las herramientas utilizadas por el atacante que le permitieron aprovecharse de la vulnerabilidad o fallo de administración y acceder al sistema.

5.4. IDENTIFICACIÓN DEL ATACANTE O ATACANTES

La identificación del atacante o atacantes es fundamental sobre todo cuando la organización quiere tomar acciones legales contra los responsables.

En el proceso de identificación deberá intentar averiguarse inicialmente la dirección IP del atacante mediante la revisión de los registros de las conexiones de red.

5.5. EVALUACIÓN DEL IMPACTO CAUSADO

Tipos de ataques

Activos: Ataques en los que se altera la información del sistema, poniendo en compromiso su funcionamiento habitual.

Pasivos: Ataques limitados a observar y escuchar los equipos sin alterar sus datos.

5.6. DOCUMENTACIÓN DEL ATAQUE

Deberían elaborarse formularios como mínimo de los siguientes aspectos:

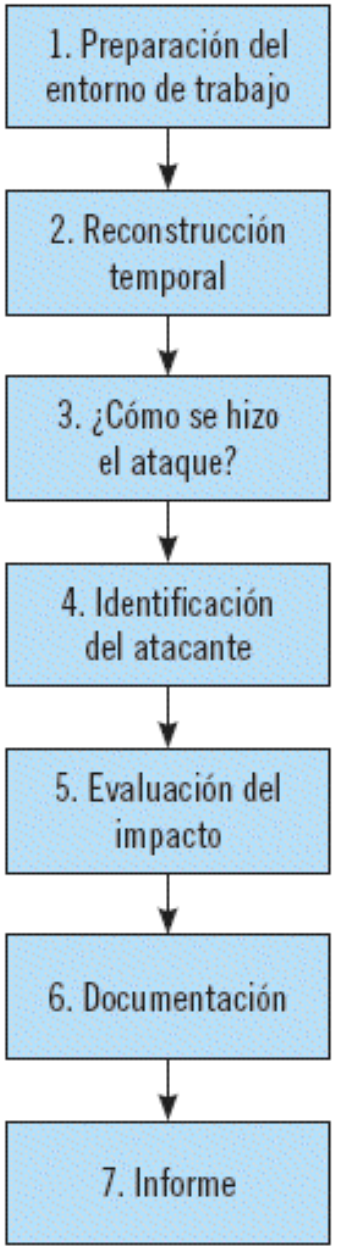
- Cadena de custodia de la evidencia.
- Identificación de los equipos, componentes y dispositivos.
- Ataques tipificados.
- Recolección y almacenamiento de las evidencias.
- Discos duros de la organización.

5.7. ELABORACIÓN DEL INFORME

En general, este informe deberá contener los aspectos siguientes:

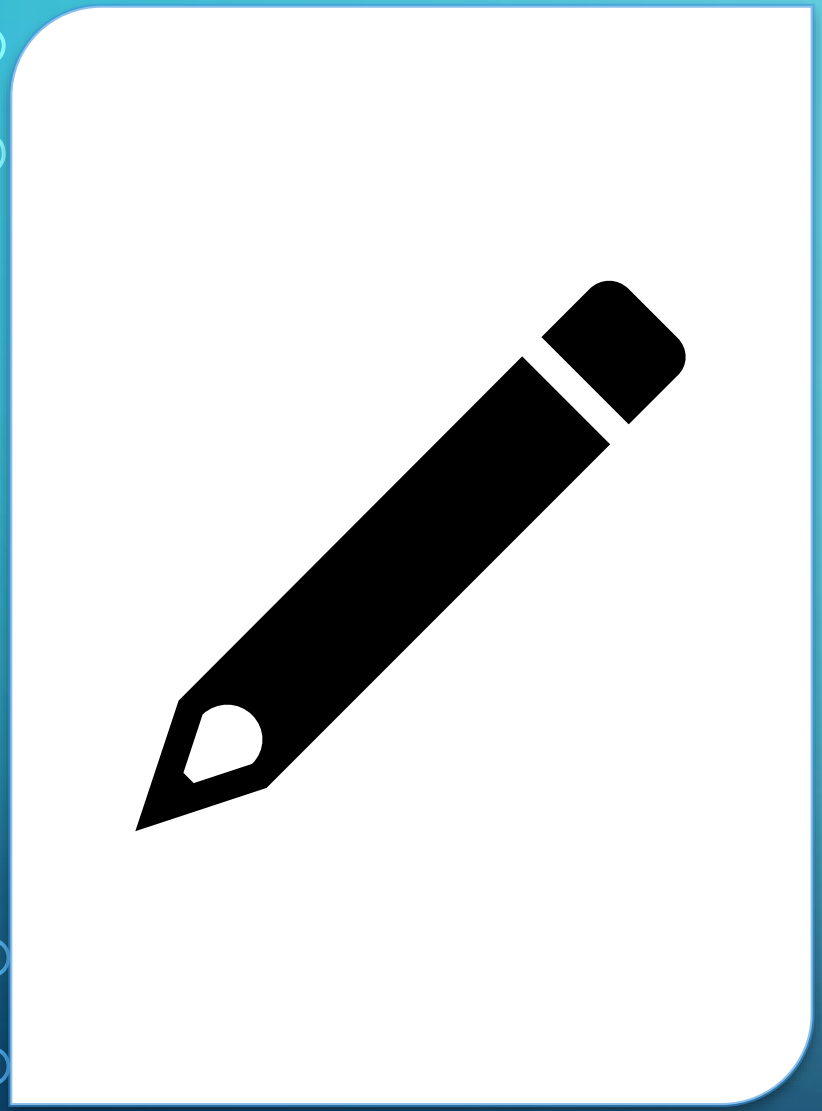
- Antecedentes del ataque.
- Recolección previa de datos y evidencias.
- Descripción de la evidencia.
- Herramientas utilizadas en el análisis.
- Análisis de la evidencia (incluyendo toda la información de los equipos y dispositivos analizados).
- Descripción de los hallazgos encontrados (huellas del ataque, vulnerabilidades aprovechadas, origen del ataque, alcance, etc.).
- Cronología del ataque.
- Conclusiones.
- Recomendaciones.

5.8. RESUMEN


1. Preparación del entorno de trabajo
2. Reconstrucción temporal
3. ¿Cómo se hizo el ataque?
4. Identificación del atacante
5. Evaluación del impacto
6. Documentación
7. Informe

Ejemplo.

USTED, COMO RESPONSABLE DE SEGURIDAD, HA DETECTADO QUE SE HA PRODUCIDO UNA INTRUSIÓN EN UNO DE LOS EQUIPOS DE LA ORGANIZACIÓN. LA INTRUSIÓN HA PROVOCADO EL BORRADO DE VARIOS ARCHIVOS IMPORTANTES Y, POR ELLO, TIENE PREVISTO REALIZAR UN ANÁLISIS FORENSE PARA LOCALIZAR AL ATACANTE Y TOMAR MEDIDAS JUDICIALES CONTRA ÉL. ¿QUÉ TIPO DE ATAQUE SE HA PRODUCIDO Y QUÉ INFORMACIÓN DEBERÁ RECOPILAR PARA RECONSTRUIR SU SECUENCIA TEMPORAL?



Ejemplo. Solución

AL HABERSE PRODUCIDO BORRADO DE INFORMACIÓN DEBIDO AL ATAQUE SE DEDUCE QUE SE TRATA DE UN ATAQUE ACTIVO (LOS ATAQUES PASIVOS NO MODIFICAN LA INFORMACIÓN DEL EQUIPO AFECTADO, SIMPLEMENTE LA "ESPÍAN"). PARA RECONSTRUIR SU SECUENCIA TEMPORAL Y CONOCER EL ORIGEN DEL ATAQUE DEBERÍA RECOPILARSE LA INFORMACIÓN SIGUIENTE DE LOS FICHEROS ELIMINADOS Y DE LOS SOSPECHOSOS:

TAMAÑO Y TIPO DE LOS FICHEROS.

USUARIOS Y GRUPOS A LOS QUE PERTENECEN LOS FICHEROS.

PERMISOS DE ACCESO.

DETECCIÓN DE LOS FICHEROS ELIMINADOS.

TRAZADO DE RUTA COMPLETO.

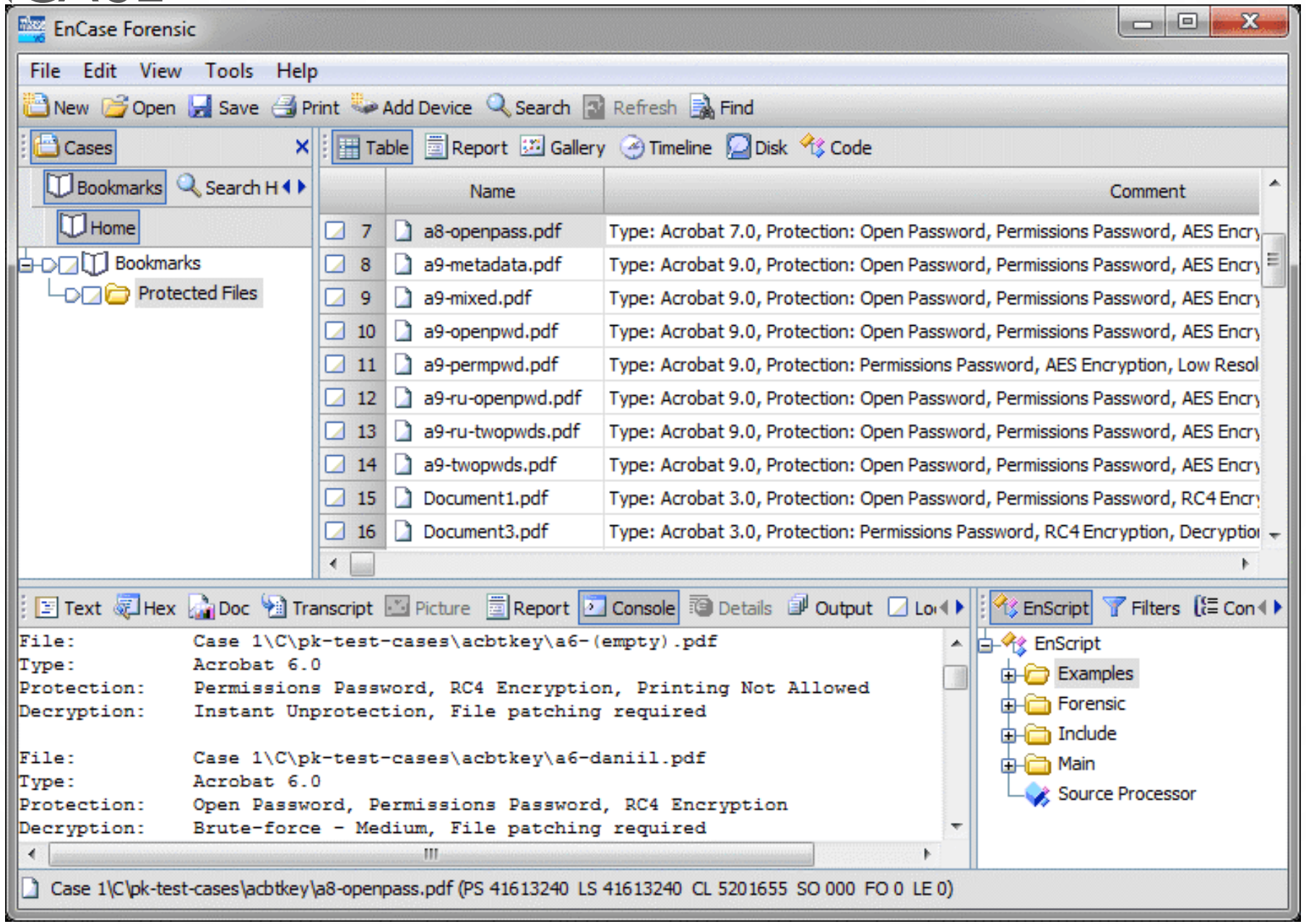
MARCAS DE TIEMPO.

6. GUÍA PARA LA SELECCIÓN DE LAS HERRAMIENTAS DE ANÁLISIS FORENSE

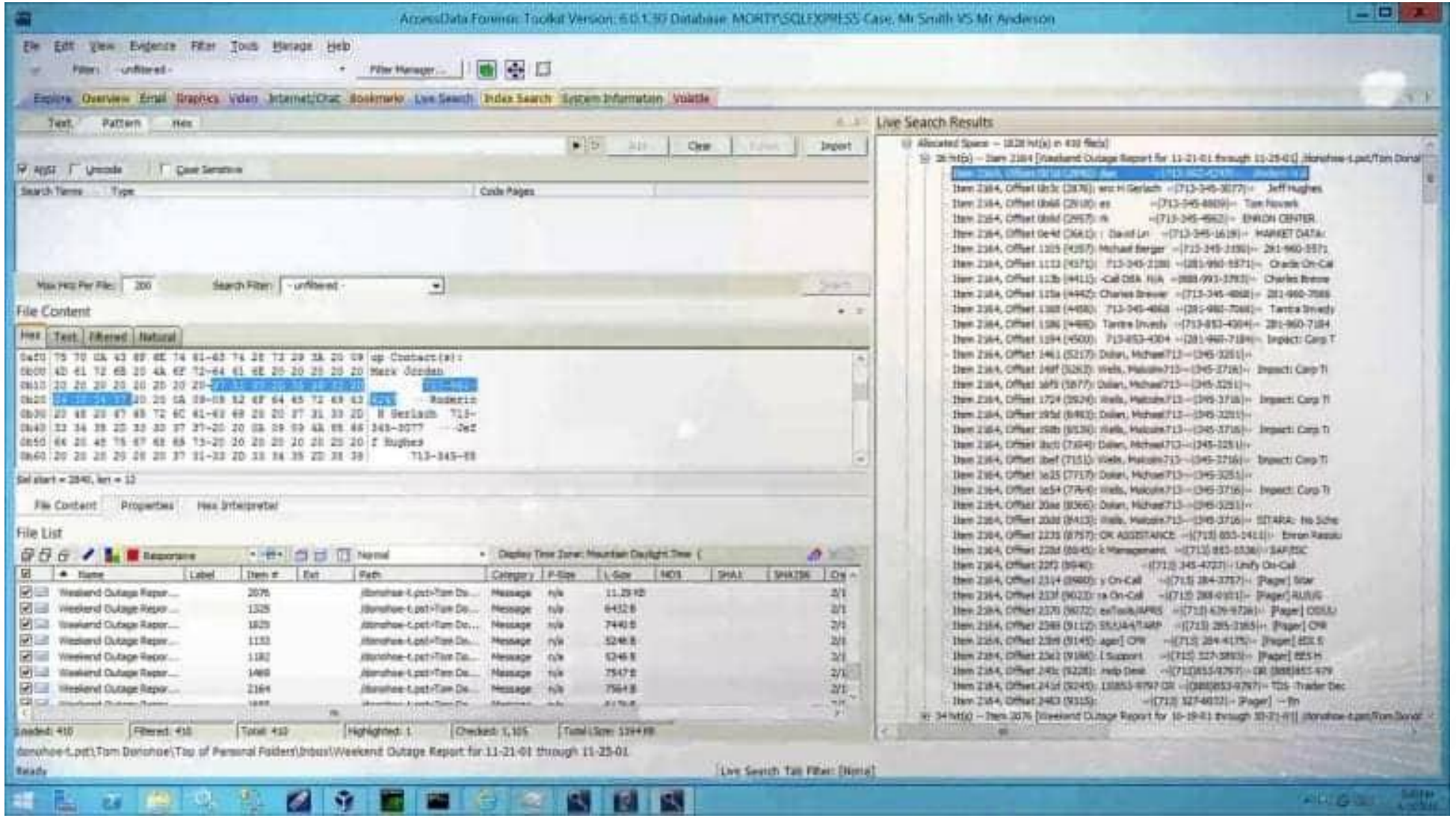
La detección de evidencias y el posterior análisis de las mismas puede ser una tarea bastante tediosa para los investigadores si no utilizan herramientas específicas que completen y añadan eficacia a la investigación.

La elección de la herramienta adecuada dependerá del sistema operativo utilizado y de la preferencia entre software comercial y software libre.

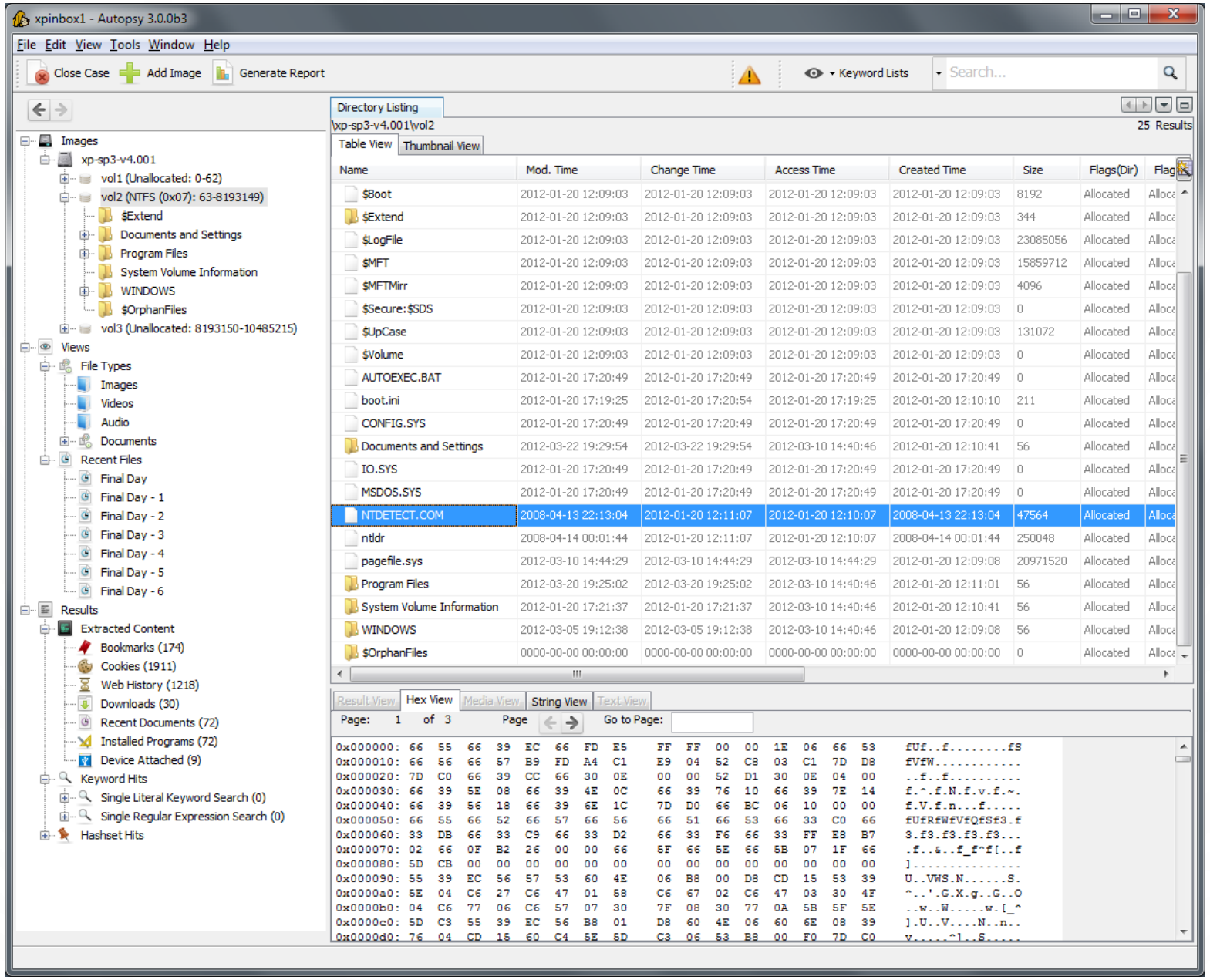
6.1. ENCASE


EnCase Forensic
File Edit View Tools Help
New Open Save Print Add Device Search Refresh Find
Cases
Bookmarks Search H
Home
Bookmarks
Protected Files
Table Report Gallery Timeline Disk Code
Name Comment
7 a8-openpass.pdf Type: Acrobat 7.0, Protection: Open Password, Permissions Password, AES Encry
8 a9-metadata.pdf Type: Acrobat 9.0, Protection: Open Password, Permissions Password, AES Encry
9 a9-mixed.pdf Type: Acrobat 9.0, Protection: Open Password, Permissions Password, AES Encry
10 a9-openpwd.pdf Type: Acrobat 9.0, Protection: Open Password, Permissions Password, AES Encry
11 a9-permpwd.pdf Type: Acrobat 9.0, Protection: Permissions Password, AES Encryption, Low Resol
12 a9-ru-openpwd.pdf Type: Acrobat 9.0, Protection: Open Password, Permissions Password, AES Encry
13 a9-ru-twopwds.pdf Type: Acrobat 9.0, Protection: Open Password, Permissions Password, AES Encry
14 a9-twopwds.pdf Type: Acrobat 9.0, Protection: Open Password, Permissions Password, AES Encry
15 Document1.pdf Type: Acrobat 3.0, Protection: Open Password, Permissions Password, RC4 Encry
16 Document3.pdf Type: Acrobat 3.0, Protection: Permissions Password, RC4 Encryption, Decryptio
Text Hex Doc Transcript Picture Report Console Details Output Lo
File: Case 1\C\pk-test-cases\acbtkey\a6-(empty).pdf
Type: Acrobat 6.0
Protection: Permissions Password, RC4 Encryption, Printing Not Allowed
Decryption: Instant Unprotection, File patching required
File: Case 1\C\pk-test-cases\acbtkey\a6-daniil.pdf
Type: Acrobat 6.0
Protection: Open Password, Permissions Password, RC4 Encryption
Decryption: Brute-force - Medium, File patching required
EnScript Filters Con
EnScript
Examples
Forensic
Include
Main
Source Processor
Case 1\C\pk-test-cases\acbtkey\a8-openpass.pdf (PS 41613240 LS 41613240 CL 5201655 SO 000 FO 0 LE 0)

6.2. THE FORENSIC TOOLKIT



6.3. THE SLEUTH KIT Y AUTOPSY

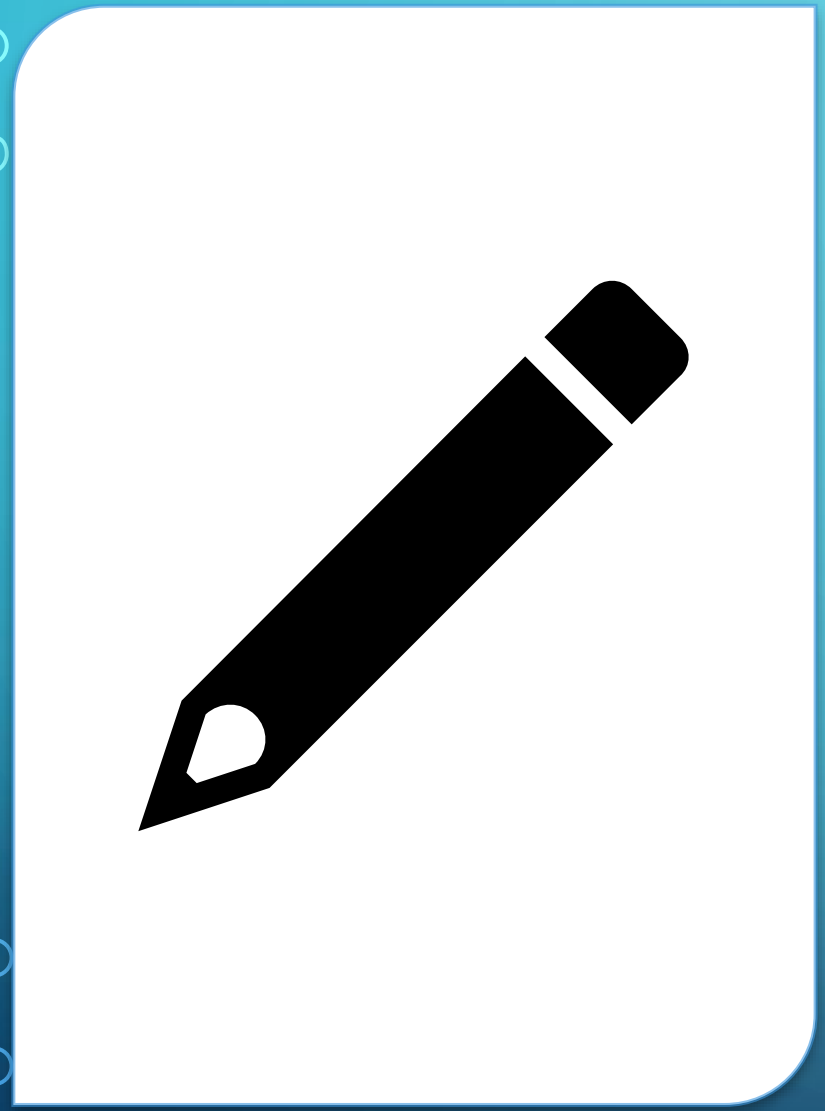


6.3. KIT DE CAMPO CRU

Forensic Field Kit A6

6.4. DUPLICADORA DE DISCO DURO

Ejercicios



3.3.100.1.MF0488_3_EJERCICIOSCAPITULO_3.DOCX