***PROCEDIMIENTOS Y HERRAMIENTAS PARA EL PERITAJE INFORMATICO***

**Introducción**

**La informática forense**  es la aplicación de técnicas científicas y analíticas especializadas a infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal.

Dichas técnicas incluyen reconstruir el bien informático, examinar datos residuales, autenticar datos y explicar las características técnicas del uso aplicado a los datos y bienes informáticos.

Como la definición anterior lo indica, esta disciplina hace uso no solo de tecnologías de punta para poder mantener la integridad de los datos y del procesamiento de los mismos, sino que también requiere de una especialización y conocimientos avanzados en materia de informática y sistemas para poder detectar dentro de cualquier dispositivo electrónico lo que ha sucedido. El conocimiento del informático forense abarca el conocimiento no solamente del software sino también de hardware, redes, seguridad, hacking, cracking y recuperación de información.

La informática forense ayuda a detectar pistas sobre ataques informáticos, robo de información, conversaciones o pistas de emails, chats.

La importancia de éstos y el poder mantener su integridad se basa en que la evidencia digital o electrónica es sumamente frágil. El simple hecho de darle doble clic a un archivo modificaría la última fecha de acceso del mismo.

Adicionalmente, un examinador forense digital, dentro del proceso del cómputo forense puede llegar a recuperar información que haya sido borrada desde el sistema operativo.

Es muy importante mencionar que la informática forense o cómputo forense no tiene parte preventiva, es decir, la informática forense no se encarga de prevenir delitos, para ello se encarga la seguridad informática. Es importante tener claro el marco de actuación entre la informática forense, la seguridad informática y la auditoría informática.

**Etapas de una pericia informática**

1. **Adquisición:** significa copiar de una manera especial el contenido en bruto de la información del sistema en observación. Luego se trabajará sobre esta copia dejando intacta la información original. Esta tarea se hará no arrancando la computadora por los medios convencionales sino accediendo a los volúmenes en modo de sólo lectura para que ni un byte sea alterado desde el momento en que empieza nuestra intervención. Hay que tener en cuenta que el simple booteo (arranque) de una computadora altera por lo menos algunos archivos en sus contenidos y fechas, varía la cantidad total de archivos, etc. Lo mismo ocurre cuando abrimos un archivo aunque más no sea para leerlo o imprimirlo. Se puede rastrear todo este tipo de actividad en una computadora. La adquisición puede involucrar desde un disquette o un disco rígido de una computadora hasta un conjunto de discos de un servidor, un juego de cintas, o varias computadoras de una organización.
2. **Validación y preservación de los datos adquiridos:** Por medios matemáticos se debe calcular de manera normalizada un código único correspondiente a esa combinación única de bytes que constituye la totalidad del medio en observación. Este código de validación ha de ser lo suficientemente complejo como para impedir que sea generado en forma reversa con fines dolosos y normalizado como para que cualquier auditor independiente pueda por su cuenta verificar la autenticidad de la imagen tomada y así establecer una cadena de custodia consistente .Desde este momento ya se pueden efectuar copias exactamente iguales de la imagen a los efectos de que diferentes actores puedan conservar una copia de seguridad.

**3) Análisis y descubrimiento de evidencia:** se procede a realizar una batería de pruebas en el laboratorio sobre la copia validada. Es posible analizar y buscar información a muchos diferentes niveles. Partimos de la base de que el usuario sospechoso de una actividad ilícita puede haber borrado la información que lo compromete o pudo haberla ocultado almacenándola por medios no convencionales. Estas búsquedas están orientadas por cada caso en particular y aquí contamos con la información que provee quien solicita el servicio. Se pueden buscar:

* archivos borrados, archivos creados, accedidos o modificados dentro de determinado rango de fechas,
* tipos de archivos con un formato particular que hayan sido alterados, por ejemplo archivos de un sistema de contabilidad renombrados como archivos de un procesador de texto,
* imágenes, mensajes de correo electrónico, actividad desarrollada en internet,
* a diferentes niveles palabras claves tales como un número telefónico, el nombre de una ciudad o una empresa, etc.

En base a este análisis se determina un patrón de comportamiento del usuario en cuanto a la

creación, modificación y borrado de mensajes, actividad de correo electrónico, etc.

**4) Informe:** se presenta un informe escrito en un lenguaje a la vez técnico y claro y un CD donde se hace accesible al usuario no especializado de una forma ordenada la evidencia recuperada y su interpretación.

**Herramientas utilizadas**

**Duplicadores Forenses**

Los duplicadores forense es una tecnología digital destinada para profesionales forenses que necesitan llevar a cabo investigaciones mediante procesos que agilicen la clonación, recopilación de datos de manera rápida y eficiente.

Son herramientas de software y hardware creadas para la copia de discos o particiones enteras, obteniendo una imagen o instantánea de un disco en un momento determinado.

La obtención de imágenes forenses podemos definirla como la copia de la información contenida en dispositivos físicos de almacenamiento, **sin alterar** su contenido.

En particular, no estamos hablando de la copia de archivos individuales, sino de discos o particiones **enteras**, obteniendo una **imagen** o **instantánea** de un disco en un momento determinado. Si bien estas ideas encontraron sus primeras aplicaciones en el área de la **Informática Forense**, para garantizar la preservación y posterior análisis de la **evidencia digital**, en la actualidad puede encontrarse una gran cantidad de herramientas disponibles para el usuario hogareño. Así, el mismo tiene a su merced un abanico de **posibilidades**, desde una pequeña suite forense para adquisición de imágenes, verificación y análisis, hasta la utilización de soluciones menos robustas para tareas específicas, como realizar copias de seguridad o cifrado de los datos, por ejemplo.

En la actualidad hay una gran variedad de duplicadores forenses, por lo que detallaremos los más importantes:

**1. Equipo de Análisis Forense Logicube modelo Forensic Falcon**

* Creación rápida de imagen forense a 20GB/min
* Creación de imagen y verificación desde 4 discos origen a 5 destinos
* Crea imagen hacia o desde una ubicación en red
* Multitarea. Realiza tareas de creación de imagen, borrado y hash simultáneamente
* Interfaz de usuario web. Permite el acceso remoto mediante un navegador de internet.

**2. Duplicadora Logicube modelo Forensic Talon**

* ****Velocidades cercanas a los 4GB/min con UDMA5.
* Cálculo de MD5 o SHA-256 a tiempo real.
* Búsqueda de palabras clave durante el proceso de captura o por separado.
* Captura de datos en formato DD con posibilidad de fraccionar la imagen en trazas de 650MB, 2GB y 4GB
* Tarjeta Compact Flash para almacenamiento de listas de palabras, reportes, actualizaciones de Firmware etc.
* Teclado QWERTY integrado.

**3. Duplicadora Logicube modelo Forensic Dossier**

* Perfecta para trabajo de campo y de laboratorio
* Capaz de ofrecer la captura simultánea de 1 o 2 discos objetivo a 1 o 2 discos de evidencia
* Soporte nativo para dispositivos SATA e IDE y conectividad USB y Firewire
* Velocidades de hasta 7GB/min
* Soporta la adquisición en formato E01 compatible con EnCase y FTK v3.x
* Soporte opcional para dispositivos SCSI y SAS
* Autenticación MD5 y SHA
* Soporte para dispositivos de 2TB y más en formato NTFS
* Posibilidad de captura de un objetivo mayor a 2 dispositivos de menor capacidad
* Búsqueda avanzada de palabras clave
* Compatible con MPFS
* Captura de HPA y DCO
* Teclado QWERTY integrado
* Módulo opcional para el acceso a través de red

**Duplicadora Tableau modelo TD1**

* ****TD1 ofrece funciones necesarias en la
* adquisición de datos de laboratorio y de campo
* Admite los discos duros SATA e IDE
* Proporciona tasas de transferencia de datos de hasta 6 GB/minuto mientras calcula al mismo tiempo los hash MD5 y SHA-1.
* Las funciones estándar incluyen duplicación de disco a disco y de disco a archivo, formateo de disco, borrado de disco, operaciones hash en disco, (MD5 y SHA-1), detección y extracción de HPA/DCO y comprobación de disco en blanco.

**Duplicadora Tableau modelo TD2**

* Construida sobre la fuerza y reputación de la venerada TD1, la duplicadora forense TD2 cuenta con funciones avanzadas
* Rendimiento excepcional en un formato compacto, duradero y de fácil manejo.
* Ha sido diseñado para adquisiciones forenses tanto en campo como en laboratorio, con una interfaz nativa que permite adquirir dispositivos SATA e IDE/PATA con una velocidad de hasta 9 GB/min.
* Utilizando el mismo protocolo que TD1, las investigaciones pueden incluir (opcionalmente) objetivos USB y SAS.
* Capacidades de TD2 se encuentran la duplicación 1:2, duplicación disco a disco o disco a imagen, formateo de unidades, Wipe, Hash (MD5 o SHA-1), detección y eliminación de HPA/DCO, capacidad para realizar imágenes en RAW DD, E01(EnCase comprimido) y EX01.

**Duplicadora Tableau modelo TD3**

* Una herramienta con un núcleo TD3 de alto rendimiento, fiable y fácil de usar.
* Su interfaz de usuario con pantalla táctil de alta resolución hace sencilla la captura forense de datos desde dispositivos SATA, IDE, USB 3.0/2.0/1.1, SAS y FireWire (1394A/B).
* TD3 Forensic Imager soporta el bloqueo de escritura a través de la red, permitiendo la pre visualización o la adquisición de datos desde máquinas remotas utilizando la IP adecuada.

**Duplicadora CRU modelo Ditto**

* Construida completamente en aluminio y llegando a alcanzar velocidades de operación de hasta 6.5GB/min
* Capacidad de navegación y adquisición de datos a través de la red mediante conexión SSL por sus puertos, origen y destino Gigabit Ethernet
* Perfecta para el trabajo de campo al estar equipada con una batería de larga duración
* Sin ruido de ventilación debido a su arquitectura
* Copia simultánea a dos dispositivos en modo RAW DD, clon o mixto
* Interfaz sencilla y amigable
* Capacidad de adquisición desde dispositivos con interfaz SATA/eSATA, PATA, USB 2.0 GbE y PCIe Expansion Module
* Modo silencioso que permite operaciones con baja visibilidad
* Soporte para destino de EXT2/3/4, XFS, HFS+ y FAT32
* Bypass temporal o permanente de HPA/DCO
* Módulos de expansión para permitir la interacción con USB3.0, SAS, FireWire, SCSI, ThunderBolt y PCI/PCI x4

**Duplicadora Voom modelo Hardcopy 3**

* Velocidad de hasta 7.5 Gb por minuto en la transferencia de datos.
* Realiza 2 copias a la vez de un mismo disco duro.
* Verificación SHA256.
* Modos de duplicación (clonación y creación de imágenes).
* Copia DCO y HPA (copia todos los datos incluidos los protegidos).
* Diferentes métodos de borrado.
* Duplicación de otros discos duros (ATA, portátiles...).
* Ingeniería de duplicación de discos.

**Duplicadora Voom modelo Shadow 3**

* Permite investigar discos duros origen en la escena del crimen en cuestión de minutos, antes de crear la imagen
* Permite investigar y analizar discos origen una y otra vez en el laboratorio forense en cuestión de segundos sin necesidad de volver a crear la imagen.
* Permite ver las evidencias en su ambiente nativo.
* Permite presentar las evidencias de una forma comprensible para los no expertos en el propio ordenador investigado.
* Cuando se sospecha una actividad ilícita, como la descarga nocturna de archivos confidenciales, utilice Shadow para verificar la actividad y preservar los metadatos.

**Búsqueda de información**

Esta fase comprende el fuerte del trabajo en donde se analiza el contenido adquirido en busca de vestigios de lo que se quiere hallar. El objetivo final de la fase de análisis en el caso de un proceso judicial o pre-judicial es encontrar la denominada Evidencia Digital, es decir, aquello que relaciona el hecho ocurrido con el “imputado” y la “victima”. Entonces, se piensa en la evidencia digital como en un tipo de evidencia física que está construida de campos magnéticos y pulsos electrónicos que pueden ser

recolectados y analizados con herramientas y técnicas especiales.

La fase de análisis comprende las siguientes etapas:

*1. Extracción lógica*

*2. Extracción física*

*3. Análisis de relaciones*

La **extracción lógica** representa la recuperación de información eliminada a partir del sistema de archivos. Por esa razón se denomina “lógica”, ya que no se accede en forma directa a los bloques, sino a través del Sistema de Archivos, y del Sistema Operativo como intermediario. La mayoría de los sistemas operativos no eliminan la información en el momento en el que un Usuario solicita el borrado de un archivo determinado, sino que , de alguna manera, dejan registrado que el espacio que ocupaba dicho archivo ahora se encuentra disponible. De esta manera, por ejemplo, si fuese posible hallar tal espacio entonces sería posible reconstruir la información original.

Esta etapa de extracción lógica contempla las siguientes tareas:

* Recuperación de archivos eliminados
* Extracción de información a examinar por tipo de archivo
* Extracción de metadatos del archivo presentes en el sistema de archivos
* Extracción de metadatos propios del archivo
* Extracción de archivos protegidos con contraseña
* Extracción de archivos comprimidos
* Extracción de archivos encriptados
* Determinar el tipo de archivo encriptado
* Búsqueda de determinado tipo de archivo oculto. Esta tarea está vinculada a la búsqueda en particular de determinado tipo de archivo, que puede estar oculto en un nombre de archivo con otra extensión
* Búsqueda de información en el área de paginado del Sistema Operativo
* Búsqueda de Información de Configuración. Referida a la información que puede obtenerse del registro de Windows u otros archivos de configuración de las distintos Sistemas Operativos.
* Búsqueda de Información en Procesos en Memoria. Referida a la obtención de información existente en los dump de memoria, en el caso de examinación de equipos que se encontraban en funcionamiento al momento de la adquisición.

La **extracción física** comprende la búsqueda de la información directamente en el espacio de datos omitiendo todo tipo de estructura de sistema de archivos. Con lo cual se da caso omiso a los metadatos y se aplican diferentes técnicas sobre el contenido puro del bloque en el dispositivo de almacenamiento.

En esta etapa podrían estar incluidas, de ser necesario, las siguientes tareas:

* Búsqueda de palabras en el bloque del dispositivo
* Extracción de archivos en espacio desalojado (marcado como libre) y no fragmentado
* Extracción de archivos en espacios desalojados, que puedan estar fragmentados

La etapa de **análisis de relaciones** trata justamente de identificar relaciones entre conjuntos de archivos, con el fin de obtener una conclusión. Esto involucra puntualmente la Identificación de relaciones entre conjunto de archivos vinculados a una actividad en particular (ej.: archivos relacionados a la navegación por internet) y la verificación de aplicaciones instaladas, entre otros.

--------------------------------------------------------------------------------------------------------------------

Dentro de un dispositivo secuestrado existe mucha información que se puede recopilar sencillamente, pero otra gran parte requiere un análisis de mayor profundidad. Para realizar este tipo de análisis es necesario utilizar herramientas que facilitan las tareas de recolección y procesamiento de datos.

Si bien suele pensarse en discos rígidos o pendrives cuando se habla de “dispositivos de almacenamiento”, es importante destacar que también hay que tener en cuenta a las casillas de correo electrónico, los dispositivos móviles, el tráfico de redes, entre otras.

A continuación se muestra un catálogo de herramientas forenses que se utilizan para la búsqueda de información:

- **Forensic ToolKit (FTK):** Forensic ToolKit es una herramienta software desarrollada por AccessData, la cual permite realizar un escaneo completo de un disco duro. De esta forma, se pueden detectar archivos borrados recientemente, cadenas de caracteres tipeados que sirven como entrada a un diccionario de posibles contraseñas, análisis de tráfico de red durante los últimos días, entre otras cosas.

- **Guidance Software EnCase**: la compañía EnCase ofrece una amplia variedad de tecnologías para la informática forense y la ciberseguridad. Con la herramienta EnCase Forensic se puede realizar, de forma similar a FTK, un análisis completo del dispositivo de almacenamiento secuestrado (Tablets, Smartphones, discos duros, dispositivos extraíbles) y generar un reporte en el que figure un listado detallado de la información analizada, dependiendo del propósito y los objetivos de la investigación.

- **Paraben:** ésta organización, además de ofrecer productos para el análisis de discos duros y dispositivos móviles, tiene una fuerte incidencia en lo que respecta al descubrimiento de información vía E-mail. La herramienta E-mail Examiner permite analizar titulares de mensajes, cuerpos, archivos adjuntos, recuperar correos eliminados, búsquedas inteligentes, entre otras cosas.

**Bloqueadores**

Un bloqueador es un dispositivo que se encarga de evitar la escritura sobre un hardware determinado, y que de esta forma se provoque una alteración no deseada en los datos que contiene. Para que los datos en el disco a analizar tengan validez a nivel judicial, es importante que no se produzcan alteraciones una vez que es secuestrado para poder realizar el peritaje correspondiente.

Al igual que en el caso de los Duplicadores forenses, Tableau es una de las empresas líderes en la fabricación de Bloqueadores de escritura de disco. A continuación se detallan algunos ejemplos de estos productos:

**Bloqueador Tableau T35es**

El bloqueador Tableau T35es soporta bloqueo de escritura para dispositivos de almacenamiento tanto con interfaz IDE como SATA, con la velocidad que proporcionan los puertos USB 3.0 con los que cuenta.

Para disponer de mayor seguridad, el modelo T35es introduce un nuevo botón Firmware con el cual se puede setear un modo especial para el bloqueador con la utilidad Tableau Firmware Update (TFU). De esta forma se pueden realizar actualizaciones vía USB, haciendo mucho más fácil mantener actualizada las versiones de los nuevos productos Tableau



**Bloqueador Tableau T35esRW**

El bloqueador Tableau T35es-R2-RW es casi idéntico al que se describió anteriormente. La diferencia radica en que este modelo con carcaza amarilla, cuenta con la funcionalidad de poder bloquear operaciones de Lectura-Escritura, mientras que el anterior (con carcaza negra) solamente bloquea operaciones de Escritura.

Frecuentemente, los kits completos para realizar peritaje informático o forense, contienen tanto un bloqueador de Escritura (negro) como un bloqueador de Lectura-Escritura (amarillo)

****

**Herramientas de uso general**

***ENCASE de guidance software***

Es el paquete profesional más utilizado. Se trata de una herramienta comercial específica. Es una poderosa plataforma de investigación que recolecta datos digitales, realiza análisis, informa sobre descubrimientos y los preserva en un formato válido a efectos legales y validado por los tribunales. Las dos características principales que hacen de EnCase una herramienta software única son la variedad de sistemas operativos y sistemas de archivos que admite para el análisis forense de sistemas informáticos.

Entre otras muchas posibilidades, EnCase permite: escanear discos, crear imágenes de discos para su posterior análisis, recuperar archivos de unidades que hayan sido formateadas, realizar borrado seguro de unidades a bajo nivel, consultas de archivos por tiempos de creación, último acceso y última escritura, identificación de extensiones de archivos, múltiples soporte de archivos. Permite el análisis sobre discos duros, dispositivos USB, tablets, smartphones.

***Forensic Toolkit (FTK) de Accessdata***

Al igual que Encase, es un software de pago orientado a profesionales forenses y analistas e investigadores que asisten a las organizaciones empresariales, la educación, el gobierno y los funcionarios encargados de hacer cumplir la ley de informática.

Forensic Toolkit permite a los usuarios analizar, almacenar, procesar, fabricación e investigación de pruebas electrónicas es en el disco duro de un ordenador. Las características incluyen un análisis del registro, descifrado de contraseñas, descifrar archivos y equipo de recuperación de datos, tales como documentos, e-mail y contraseña alterado o eliminado.

***CAINE***

Caine (Computer Aided Investigative Environment) Es una distribución Live CD basada en Ubuntu. Ofrece un completo entorno forense, de modo que integra herramientas de software existentes, proporcionando una interfaz gráfica amigable. Precisamente éste es el punto clave de CAINE, su interfaz, que permite una integración sencilla y bastante amigable, con respecto a otras distribuciones Live CD.

Entre otras posibilidades, permite clonar y montar unidades, manipular volúmenes de diferentes sistemas operativos (Windows, Unix, Macintosh), recuperar archivos o borrarlos de forma segura, recuperar unidades de disco, auditar los dispositivos conectados a la red (incluso determinando qué puertos tienen abiertos), editores hexadecimales, recuperar archivos de imágenes y de vídeo, recuperar contraseñas, examinar el contenido de los archivos de respaldo que los móviles IPhone dejan en el disco, recuperar datos de DVDs, etc.

***DEFT***

DEFT (Digital Evidence & Forensic Toolkit) es una distribución Live CD basada en Linux Kernel 3 y DART (Digital Advanced Response Toolkit). Se trata de un proyecto italiano de gran éxito, por cierto, y que incluye las mejores herramientas forenses. Además de un número considerable de aplicaciones de Linux y scripts, DEFT también cuenta con la suite de DART que contiene herramientas gratuitas para análisis forense en entornos Windows.

Esta distribución no se centra únicamente en ordenadores, también tenemos aplicaciones para la realización de **análisis forense a dispositivos Android, iPhone y BlackBerry** así como extraer información de las bases de datos SQLite que utilizan los móviles. También tiene herramientas para analizar la red local y la información pasa a través de ella.

***Sleuth Kit y Autopsy***

Sleuth Kit es de Conjunto herramientas de análisis forense de libre distribución. Se ejecuta principalmente sobre plataformas Linux. Su filosofía de funcionamiento se basa en dos tipos de análisis: análisis de sistema muerto (se utiliza la herramienta desde otro sistema operativo y con el sistema a investigar en su soporte sin cargar) o análisis de sistema vivo (cuando se está analizando el sistema sospechoso mientras está funcionando).

Autopsy es Tal vez la mejor herramienta libre que existe para el análisis de evidencia digital. Su interfaz gráfica es un browser que basado en las herramientas en línea de comandos del Sleuth Kit, permite un análisis de diversos tipos de evidencia mediante una captura de una imagen de disco.

***HELIX***

HELIX es otra famosa distribución Linux basada en Ubuntu para respuesta a incidentes y análisis forense. Está desarrollada por e-fense y, aunque sus versiones iniciales eran gratis, desde hace unos años se ofrece como un producto de pago. Dispone de una versión de evaluación por 30 días, ideal para probar el producto. Su principal objetivo es proveer un entorno rápido para análisis forense, recuperación de datos, búsqueda de virus y detección de vulnerabilidades. También incluye algunas herramientas para realizar testeos de penetración. Esta distribución es muy parecida a la distribución CAINE, en cuanto a entorno y funcionalidad.

***X-Ways Forensic: Integrated Computer Forensics Software***

Otro entorno integrado lo ofrece la firma alemana X-Ways (software comercial). Ofrece herramientas forenses, recuperación de datos, seguridad IT. Su buque insignia es WinHex, software para informática forense, recuperación de archivos y editor hexadecimal de archivos, discos y RAM. Sus creadores afirman que no consume gran cantidad de recursos y trabaja de manera muy eficiente.

***SANS investigation Forensic Toolkit – SIFT***

Es un sistema operativo forense de usos múltiples que viene con todas las herramientas necesarias utilizadas en el proceso forense digital. Está construido en Ubuntu con muchas herramientas relacionadas con la informática forense. A principios de éste año, SIFT 3.0 fue lanzado.

***Oxígeno suite Forense***

Oxígeno suite forense es un buen software para reunir pruebas de teléfonos celulares. Esta herramienta ayuda en la recopilación de información del dispositivo (incluyendo fabricante, sistema operativo, número de IMEI, número de serie), los contactos, los mensajes (correos electrónicos, SMS, MMS), recuperar los mensajes borrados, registros de llamadas y la información del calendario. También le permite acceder y analizar datos de dispositivos móviles y documentos. Genera informes fáciles de entender para una mejor comprensión.

***Extractor granel***

Extractor granel es también una herramienta importante y popular forense digital. Analiza las imágenes de disco, archivo o directorio de archivos para extraer información útil. En este proceso, no tiene en cuenta la estructura del sistema de archivos, por lo que es más rápido que otros tipos similares de herramientas disponibles. Básicamente, es utilizado por las agencias de inteligencia y de aplicación de la ley en la resolución de los delitos cibernéticos.

***Informática Online Extractor Evidencia Forense (CAFE)***

Es un conjunto de herramientas desarrollado por expertos en informática forense. Esta herramienta fue desarrollada por Microsoft para reunir pruebas de los sistemas Windows. Se puede instalar en un pen drive USB o disco duro externo. Sólo tiene que conectar el dispositivo USB en el equipo de destino y se inicia un análisis en vivo. Viene con 150 herramientas diferentes con una interfaz gráfica de usuario basada a comandar las herramientas. Es rápido y puede realizar todo el análisis en tan sólo 20 minutos. Para las agencias de aplicación de la ley, Microsoft proporciona soporte técnico gratuito para la herramienta.

***XRY***

Es la herramienta de análisis forense móviles desarrollado por Micro Systemation. Se utiliza para analizar y recuperar información crucial desde dispositivos móviles. Esta herramienta viene con un dispositivo de hardware y software. Hardware conecta teléfonos móviles para PC y software realiza el análisis de los datos del dispositivo y de extracción. Está diseñado para recuperar los datos para el análisis forense.

La última versión de la herramienta puede recuperar datos de todo tipo de teléfonos inteligentes como Android, iPhone y BlackBerry. Reúne datos borrados como los registros de llamadas, imágenes, SMS y mensajes de texto.

**Herramientas para búsqueda de información específica**

**ADQUISICIÓN Y ANÁLISIS DE LA MEMORIA:** Set de utilidades que permite la adquisición de la memoria RAM para posteriormente hacer un análisis con ella.

* [pd](http://www.trapkit.de/research/forensic/pd/) Proccess Dumper - Convierte un proceso de la memoria a fichero.
* [FTK Imager](http://accessdata.com/support/adownloads#FTKImager) - Permite entre otras cosas adquirir la memoria.
* [DumpIt](http://www.moonsols.com/ressources/) - Realiza volcados de memoria a fichero.
* [Responder CE](http://www.hbgary.com/free-tools) - Captura la memoria y permite analizarla.
* [Volatility](https://www.volatilesystems.com/default/volatility) - Analiza procesos y extrae información útil para el analista.
* [RedLine](http://www.mandiant.com/products/free_software/redline/) - Captura la memoria y permite analizarla. Dispone de entrono gráfico.
* [Memorize](https://www.mandiant.com/resources/download/memoryze) - Captura la RAM (Windows y OSX).

**MONTAJE DE DISCOS**: Utilidades para montar imágenes de disco o virtualizar unidades de forma que se tenga acceso al sistema de ficheros para posteriormente analizarla.

* [ImDisk](http://www.ltr-data.se/opencode.html/#ImDisk) - Controlador de disco virtual.
* [OSFMount](http://www.osforensics.com/tools/mount-disk-images.html) - Permite montar imágenes de discos locales en Windows asignando una letra de unidad.
* [raw2vmdk](http://sourceforge.net/projects/raw2vmdk/) - Utilidad en java que permite convertir raw/dd a .vmdk
* [FTK Imager](http://accessdata.com/support/adownloads#FTKImager) - Comentada anteriormente, permite realizar montaje de discos.
* [vhdtool](http://archive.msdn.microsoft.com/vhdtool) - Convertidor de formato raw/dd a .vhd permitiendo el montaje desde el administrador de discos de Windows.
* [LiveView](http://liveview.sourceforge.net/) - Utilidad en java que crea una máquina virtual de VMWare partiendo de una imagen de disco.
* [MountImagePro](http://www.mountimage.com/) - Permite montar imágenes de discos locales en Windows asignando una letra de unidad

**CARVING Y HERRAMIENTAS DE DISCO:** Recuperación de datos perdidos, borrados, búsqueda de patrones y ficheros con contenido determinado como por ejemplo imágenes, vídeos. Recuperación de particiones y tratamiento de estructuras de discos.

* [PhotoRec](http://www.cgsecurity.org/wiki/PhotoRec) - Muy útil, permite la recuperación de imágenes y vídeo.
* [Scalpel](http://www.digitalforensicssolutions.com/Scalpel/) -Independiente del sistema de archivos. Se puede personalizar los ficheros o directorios a recuperar.
* [RecoverRS](http://www.jtmoran.com/tools.html) - Recupera urls de acceso a sitios web y ficheros. Realiza carving directamente desde una imagen de disco.
* [NTFS Recovery](http://www.diskinternals.com/ntfs-recovery/) - Permite recuperar datos y discos aun habiendo formateado el disco.
* [Recuva](http://www.piriform.com/recuva) - Utilidad para la recuperación de ficheros borrados.
* [Raid Reconstructor](http://www.runtime.org/raid.htm) - Recuperar datos de un RAID roto, tanto en raid 5 o raid 0. Incluso si no conocemos los parámetros RAID.
* [CNWrecovery](http://www.cnwrecovery.com/html/data_carving.html) - Recupera sectores corruptos e incorpora utilidades de carving.
* [Restoration](http://www.snapfiles.com/get/restoration.html) - Utilidad para la recuperación de ficheros borrados.
* [Rstudio](http://www.data-recovery-software.net/) - Recuperación de datos de cualquier sistema de disco NTFS, NTFS5, ReFS, FAT12/16/32, exFAT, HFS/HFS+ (Macintosh), Little y Big Endian en sus distintas variaciones UFS1/UFS2 (FreeBSD/OpenBSD/NetBSD/Solaris) y particiones Ext2/Ext3/Ext4 FS.
* [Freerecover](http://sourceforge.net/projects/freerecover/) - Utilidad para la recuperación de ficheros borrados.
* [DMDE](http://dmde.com/) - Admite FAT12/16, FAT32, NTFS, y trabaja bajo Windows 98/ME/2K/XP/Vista/7/8 (GUI y consola), DOS (consola), Linux (Terminal) e incorpora utilidades de carving.  
  [IEF](http://www.magnetforensics.com/software/internet-evidence-finder/ief-standard/) - Internet Evidence Finder Realiza carving sobre una imagen de disco buscando más de 230 aplicaciones como chat de google, Facebook, IOS, memoria RAM, memoria virtual,etc.
* [Bulk\_extractor](https://github.com/simsong/bulk_extractor/wiki/BEViewer) - Permite extraer datos desde una imagen, carpeta o ficheros.

**UTILIDADES PARA EL SISTEMA DE FICHEROS**: Conjunto de herramientas para el análisis de datos y ficheros esenciales en la búsqueda de un incidente.

* [analyzeMFT](http://www.integriography.com/) - David Kovar's utilidad en python que permite extraer la MFT
* [MFT Extractor](http://hexacorn.com/download.php?f=hmft.exe)- Otra utilidad para la extracción de la MFT
* [INDXParse](http://www.williballenthin.com/forensics/indx/index.html) - Herramienta para los índices y fichero $I30.
* [MFT Tools](https://code.google.com/p/mft2csv/downloads/list) (mft2csv, LogFileParser, etc.) Conjunto de utilidades para el acceso a la MFT
* [MFT\_Parser](http://redwolfcomputerforensics.com/downloads/MFT_Parser_08b_Setup.exe) - Extrae y analiza la MFT
* [Prefetch Parser](http://redwolfcomputerforensics.com/downloads/parse_prefetch_info_v1.5.zip) - Extrae y analiza el directorio prefetch
* [Winprefectchview](http://www.nirsoft.net/utils/win_prefetch_view.html) - Extrae y analiza el directorio prefetch
* [Fileassassin](http://www.malwarebytes.org/products/fileassassin) - Desbloquea ficheros bloqueados por los programas

**FRAMEWORKS:** Conjunto estandarizado de conceptos, prácticas y criterios en base a el análisis forense de un caso.

* [PTK](http://ptk.dflabs.com/) - Busca ficheros, genera hash, dispone de rainbow tables. Analiza datos de un disco ya montado.
* [Log2timeline](http://log2timeline.net/) - Es un marco para la creación automática de una línea de tiempo.
* [Plaso](http://plaso.kiddaland.net/) - Evolución de Log2timeline. Framework para la creación automática de una línea de tiempo.
* [OSForensics](http://www.osforensics.com/download.html) - Busca ficheros, genera hash, dispone de rainbow tables. Analiza datos de un disco ya montado.
* [DFF](http://www.digital-forensic.org/) - Framework con entorno gráfico para el análisis.
* [SANS SIFT Workstation](http://computer-forensics.sans.org/community/downloads) - Magnífico Appliance de SANS. Lo utilizo muy a menudo.

**ANÁLISIS DEL REGISTRO DE WINDOWS:** Permite obtener datos del registro como usuarios, permisos, ficheros ejecutados, información del sistema, direcciones IP, información de aplicaciones.

* [RegRipper](https://code.google.com/p/regripper/) - Es una aplicación para la extracción, la correlación, y mostrar la información del registro.
* [WRR](http://www.mitec.cz/wrr.html) - Permite obtener de forma gráfica datos del sistema, usuarios y aplicaciones partiendo del registro.
* [Shellbag Forensics](http://www.williballenthin.com/forensics/shellbags/index.html) Análisis de los shellbag de Windows.
* [Registry Decoder](http://www.digitalforensicssolutions.com/registrydecoder/) - Extrae y realiza correlación aun estando encendida la máquina datos del registro.

**HERRAMIENTAS DE RED:** Todo lo relacionado con el tráfico de red, en busca de patrones anómalos, malware, conexiones sospechosas, identificación de ataques, etc.

* [WireShark](http://www.wireshark.org/) - Herramienta para la captura y análisis de paquetes de red.
* [NetworkMiner](http://www.netresec.com/?page=NetworkMiner) - Herramienta forense para el descubrimiento de información de red.
* Netwitness [Investigator](http://www.netwitness.com/products-services/investigator) - Herramienta forense. La versión 'free edition' está limitado a 1GB de tráfico.
* [Network Appliance Forensic Toolkit](http://blog.didierstevens.com/2012/03/12/naft-release/) - Conjunto de utilidades para la adquisición y análisis de la red.
* [Xplico](http://www.forensicswiki.org/wiki/Xplico) - Extrae todo el contenido de datos de red (archivo pcap o adquisición en tiempo real). Es capaz de extraer todos los correos electrónicos que llevan los protocolos POP y SMTP, y todo el contenido realizado por el protocolo HTTP.
* [Snort](http://www.snort.org/) - Detector de intrusos. Permite la captura de paquetes y su análisis.
* [Splunk](http://www.splunk.com/) - Es el motor para los datos y logs que generan los dispositivos, puestos y servidores. Indexa y aprovecha los datos de las generados por todos los sistemas e infraestructura de IT: ya sea física, virtual o en la nube.
* [AlientVault](http://www.alienvault.com/) - Al igual que Splunk recolecta los datos y logs aplicándoles una capa de inteligencia para la detección de anomalías, intrusiones o fallos en la política de seguridad.

**RECUPERACIÓN DE CONTRASEÑAS:** Todo lo relacionado con la recuperación de contraseñas en Windows, por fuerza bruta, en formularios, en navegadores.

* [Ntpwedit](http://cdslow.webhost.ru/en/ntpwedit/) - Es un editor de contraseña para los sistemas basados ​​en Windows NT (como Windows 2000, XP, Vista, 7 y 8), se puede cambiar o eliminar las contraseñas de cuentas de sistema local. No valido para Active Directory.
* [Ntpasswd](http://www.pogostick.net/%7Epnh/ntpasswd/) - Es un editor de contraseña para los sistemas basados ​​en Windows, permite iniciar la utilidad desde un CD-LIVE
* [pwdump7](http://www.tarasco.org/security/pwdump_7/) - Vuelca los hash. Se ejecuta mediante la extracción de los binarios SAM.
* [SAMInside](http://insidepro.com/eng/saminside.shtml) / [OphCrack](http://ophcrack.sourceforge.net/) / [L0phtcrack](http://www.l0phtcrack.com/)- Hacen un volcado de los hash. Incluyen diccionarios para ataques por fuerza bruta.

**DISPOSITIVOS MÓVILES:** Esta sección dispone de un set de utilidades y herramientas para la recuperación de datos y análisis forense de dispositivos móviles.

***iPhone***

* [iPhoneBrowser](http://code.google.com/p/iphonebrowser/) - Accede al sistema de ficheros del iPhone desde entorno gráfico.
* [iPhone Analyzer](http://sourceforge.net/projects/iphoneanalyzer/) - Explora la estructura de archivos interna del iPhone.
* [iPhoneBackupExtractor](http://www.iphonebackupextractor.com/) - Extrae ficheros de una copia de seguridad realizada anteriormente.
* [iPhone Backup Browser](https://code.google.com/p/iphonebackupbrowser/) - Extrae ficheros de una copia de seguridad realizada anteriormente.
* [iPhone-Dataprotection](https://code.google.com/p/iphone-dataprotection/) - Contiene herramientas para crear un disco RAM forense, realizar fuerza bruta con contraseñas simples (4 dígitos) y descifrar copias de seguridad.
* [iPBA2](http://ipbackupanalyzer.com/) - Accede al sistema de ficheros del iPhone desde entorno gráfico.
* [sPyphone](https://github.com/nst/spyphone) - Explora la estructura de archivos interna.

***BlackBerry***

* [Blackberry Desktop Manager](https://swdownloads.blackberry.com/Downloads/entry.do?code=A8BAA56554F96369AB93E4F3BB068C22) - Software de gestión de datos y backups.
* [Phoneminer](http://www.amraksoftware.com/phoneminer/) - Permite extraer, visualizar y exportar los datos de los archivos de copia de seguridad.
* [Blackberry Backup Extractor](http://www.reincubate.com/res/labs/bbbe/bbbe-latest.exe) - Permite extraer, visualizar y exportar los datos de los archivos de copia de seguridad.
* [MagicBerry](http://menastep.com/pages/magicberry.php)- Puede leer, convertir y extraer la base de datos IPD.

***Android***

* [android-locdump](https://github.com/packetlss/android-locdump). - Permite obtener la geolocalización.
* [androguard](https://code.google.com/p/androguard/#Description) - Permite obtener, modificar y desensamblar formatos EX/ODEX/APK/AXML/ARSC
* [viaforensics](https://github.com/viaforensics/android-forensics) - Framework de utilidades para el análisis forense.
* [Osaf](http://www.osaf-community.org/) - Framework de utilidades para el análisis forense.

**Bloqueadores para protección de la prueba**

Generalmente, los investigadores forenses hacen copias de los dispositivos que se analizan en el peritaje informático (que puede darse en varios formatos) y se deja el original precintado y a buen recaudo, conservando la [cadena de custodia](http://es.wikipedia.org/wiki/Cadena_de_custodia). Cuando no hay tiempo para obtener la copia, o por algún motivo no se puede, se puede trabajar usando un bloqueador de escritura, que garantice que cualquier intento de escritura será frustrado o desviado del disco duro. El objetivo es evitar contaminar la prueba. Para evitar la contaminación del disco duro, normalmente se ocupan bloqueadores de escritura de hardware, los cuales evitan el contacto de lectura con el disco, lo que provocaría una alteración no deseada en los medios.

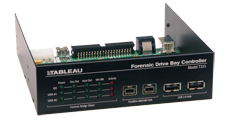
**Herramientas**



***Tableau T35:***

* + El puente forense T35 eSATA ofrece más opciones de conexión nativa del equipo host y del dispositivo que cualquier otro bloqueador de escritura que se encuentra hoy disponible.
  + **Posee** cuatro conexiones diferentes de la interfaz de host (eSATA, FireWire 800, FireWire 400 y USB) y de dos conexiones para dispositivos (SATA e IDE).
  + Es el primer puente de Tableau con una conexión eSATA del host. La interfaz eSATA permite obtener imágenes de las unidades objeto de análisis SATA e IDE a una velocidad superior a FireWire 800.
  + La versión “es” está previamente configurada de fábrica para un funcionamiento de sólo lectura. El color del equipo es negro
  + La versión “es-RW” está previamente configurada de fábrica para un funcionamiento de lectura-escritura. El color del equipo es amarillo (para evitar confusiones con la versión es)
  + La versión “e” es la versión más moderna, con rendimiento y funciones superiores a los modelos anteriores. Se han medido los aumentos de los índices de transferencia de datos SATA de hasta un 60 % (frente a los productos clásicos actuales) con una interfaz de host FireWire 800 y las herramientas de imágenes disponibles de otros fabricantes. T35e reduce los tiempos de adquisición de datos.

***Tableau T335:***

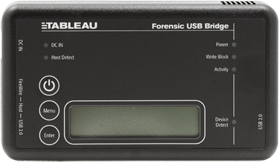
* + Incluye tres puentes independientes, dos SATA y un IDE, cada uno de los cuales puede configurarse para funcionar en modo de sólo lectura o lectura-escritura en el momento de la instalación.
  + El modelo T335 se ha diseñado para su instalación en una bahía de unidad de altura media (5,25 pulgadas) en la parte frontal de una estación de trabajo o torre forense.
  + Este modelo trabaja en conjunto con bandejas de unidad SATA e IDE extraíbles que pueden colocarse cerca del T335 en el equipo host.
  + En un sistema típico, se establecerá un canal SATA y uno IDE en modo de sólo lectura y el canal SATA restante en modo de lectura y escritura. De este modo, el operador puede utilizar una bahía de unidad SATA o IDE bloqueada contra escritura para obtener una imagen de un dispositivo y la bahía de unidad SATA restante para hacer una copia de la imagen.
  + El modelo T335 también incluye un concentrador FireWire800 y USB 2.0 activos, cada uno de ellos con dos conectores en la parte delantera de la unidad, diseñadas para facilitar al usuario un acceso frontal a estos puertos de alta velocidad, con lo que se elimina la necesidad de otro concentrador instalado en la parte frontal.

***Tableau T35i SATA/ID E ( montaje en bahía):***

* El T35i se ha diseñado para instalarse directamente en una estación de trabajo forense. Internamente, el T35i se conecta a la estación de trabajo mediante una conexión FireWire800 de alto rendimiento. Externamente, el T35i puede conectarse a discos duros SATA o IDE (sólo uno a la vez) para la obtención de imágenes forenses con bloqueo de escritura.

***Tableau T345 IDE/SATA/SCSI (montaje en bahía):***

* El modelo T345 se ha diseñado para su instalación en una bahía de unidad de altura media (5,25 pulgadas) en la parte frontal de una estación de trabajo o torre forense. Internamente, el T345 se conecta al equipo host mediante una única conexión FireWire800. Externamente, el T345 dispone de conexiones para IDE, SATA y SCSI, así como una conexión de alimentación y un interruptor de alimentación para la unidad objeto de análisis.
* El T345 está diseñado para su uso con un sólo disco duro objeto de análisis a la vez. T345 reconoce automáticamente el dispositivo conectado, por lo que no hay necesidad de seleccionar IDE, SATA o SCSI de forma manual.
* Explora automáticamente el bus SCSI, por lo que no hay necesidad de establecer los puentes de dirección SCSI en los discos duros SCSI.
* Dado que el T345 utiliza FireWire para conectarse al equipo host, la mayoría de sistemas operativos host (por ejemplo, Microsoft Windows, Mac OS X y algunas variedades de Linux) permitirán el intercambio sin necesidad de reiniciar el equipo host entre dispositivos.

***Tableau T8 US:***

* Permite bloquear de forma segura la escritura basada en hardware en dispositivos USB de almacenamiento masivo.
* El T8 es compatible con dispositivos USB2.0 de alta velocidad (480 mbit/s), USB 1.1 de velocidad máxima (12 mbits/s) y de velocidad baja (1,2 mbit/s) que cumplan la especificación de clase de almacenamiento masivo USB de gran capacidad.
* Funciona con unidades de almacenamiento portátiles USB, unidades de disco USB externas, dispositivos más exóticos como Apple iPod con interfaces USB e incluso cámaras con conexión USB con capacidad de lectura de tarjetas.
* El T8 es compatible con las conexiones USB 2.0 y FireWire400 a un equipo host, lo que posibilita el funcionamiento flexible con una amplia variedad de herramientas forenses de host y de software existentes.
* El usuario dispone de la información del fabricante, modelo, capacidad, número de serie y otros datos técnicos acerca del dispositivo USB conectado a través de una pantalla LCD.

***Tableau T5 IDE:***

* Es el primer bloqueador de escritura de hardware que se puede utilizar con discos duros IDE (ATA paralelo).
* El versátil modelo T5 de Tableau incluye interfaces de host FireWire800 y USB 2.0 que ofrecen la máxima flexibilidad al conectar el T5 al equipo host.
* Está enteramente diseñado para su uso tanto en las configuraciones prácticas como de laboratorio.
* Se puede alternar la unidad entre el bloqueo de escritura y los modos de funcionamiento de lectura-escritura.
* La versión T5-RW está previamente configurado en la fábrica para un funcionamiento de lectura-escritura.

***Tableau T3u SATA:***

* Es un bloqueador de escritura que se utiliza con los discos duros Serie ATA (SATA).
* A diferencia de otras soluciones de bloqueo de escritura SATA, el modelo T3u dispone de compatibilidad nativa con discos duros SATA eliminando la necesidad de un conversor ATA paralelo a serie externo presente en otras soluciones e incrementa la compatibilidad y fiabilidad.
* Incluye interfaces de host FireWire800, FireWire400 y USB 2.0 que ofrecen la máxima flexibilidad al conectar el T3 al equipo host.
* El T3u resulta idóneo tanto para configuraciones de campo como de laboratorio.

***Tableau T4 SCSI:***

* El puente forense T4 SCSI es un bloqueador de escritura para utilizar con discos duros SCSI.
* Rendimiento de 80MB/s
* El modelo T4 es compatible con los dispositivos SCSI y los discos duros más rápidos Ultra 320 que se comercializan actualmente.
* Este modelo escanea automáticamente el bus SCSI para buscar el dispositivo SCSI, por lo que no es necesaria la configuración del Id. de SCSI.
* Incluye interfaces de host FireWire800 y USB 2.
* Si se retira el panel extraíble de plástico se puede alternar el T4 entre el bloqueo de escritura y los modos de funcionamiento de lectura-escritura.

[***Logicube Portable Forensic Lab***](http://www.logicubeforensics.com/products/hd_duplication/pfl.asp)

* Incluye conectividad a dispositivos IDE/UDMA, SCSI, SATA, acceso PCMCIA para dispositivos portátiles y acceso USB
* Dispositivos de 1.8" y 2.5" con adaptadores opcionales, medios Compact Flash y la mayoría de las tarjetas de memoria.
* Permite autenticación MD5 o SHA-256 para asegurar que la integridad de las evidencias.

# *****Bloqueadores de bolsillo*****

Los puentes de bolsillo de Tableau se conectan directamente al dispositivo de almacenamiento, simplifican la configuración y ahorran valioso espacio de almacenamiento en el kit de análisis forense.

Modelos disponibles:

* + **Tableau T15 SATA**
  + **Tableau T15-RW**
  + **Tableau T14 IDE**
  + **Tableau T14-RW**