



BlackBag Technologies, Inc. Software forense para Macintosh

BlackBag Technologies es uno de los principales proveedores de soluciones forenses. El Macintosh Forensic Software de BlackBag (BlackBag MFS) es un conjunto de herramientas independientes que le brindan al examinador el nivel de flexibilidad disponible más alto en el campo forense. Los examinadores pueden ejecutar una o más aplicaciones durante una investigación para obtener la mayor cantidad de evidencia, mientras lleva a cabo revisiones eficientes y seguras de los sistemas de archivos de Macintosh (HFS o HFS+), haciendo de la suite de BlackBag un elemento clave dentro del conjunto de herramientas de cualquier examinador forense.

Hacer imágenes

El proceso de hacer una imagen es uno de los aspectos más importantes del cómputo forense. En BlackBag creemos que los examinadores deben tener la flexibilidad de hacer imágenes con una herramienta estándar para que puedan elegir la mejor herramienta para realizar el análisis. Por esta razón, BlackBag MFS cuenta con varios métodos para hacer una imagen. Aunque nosotros recomendamos que utilice dd por su flexibilidad y confiabilidad, BlackBag MFS está diseñado para trabajar con cualquier estándar abierto de imágenes: dd, i-Look, Disk Copy, y SafeBack. No todas las herramientas de análisis forense ofrecen esta flexibilidad, de hecho algunas imágenes hechas con herramientas propietarias no pueden ser analizadas en programas diferentes, lo que limita a los examinadores a la funcionalidad de esa herramienta, lo que puede provocar que pase por alto evidencia valiosa. Por lo tanto, BlackBag le recomienda hacer imágenes utilizando el sistema Mac OS X para aprovechar las herramientas que incluye, como dd, para poder hacer el proceso más simple, rápido y flexible.

Analizando las imágenes

El análisis de evidencias digitales se realiza mejor utilizando la misma plataforma en la cual estaba la evidencia original. Por ejemplo, los sistemas de archivos de Mac, HFS y HFS+, incluyen información que no pueden interpretar otros sistemas operativos. Al realizar el análisis en un sistema operativo Macintosh, un examinador puede usar sus características de seguridad, como deshabilitar autodiskmounting, bloquear el dispositivo, etc. las cuales le ayudarán a preservar la integridad de la evidencia durante el análisis. Sin embargo, cuando haga la imagen de un disco, le recomendamos utilizar el BlackBag Firebox para mantener la integridad de la evidencia digital.

Software para análisis forense BlackBag Macintosh

La siguiente lista muestra las características principales de la suite BlackBag MFS

Active File Searcher permite especificar archivos activos en un sistema para poder realizar búsquedas utilizando palabras clave.



