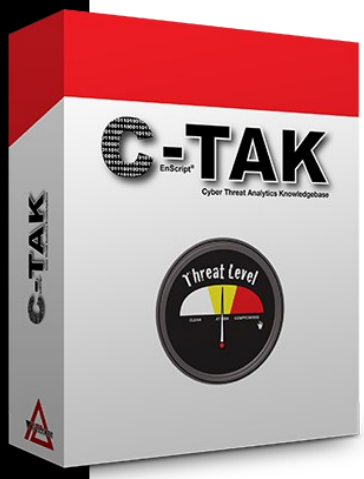
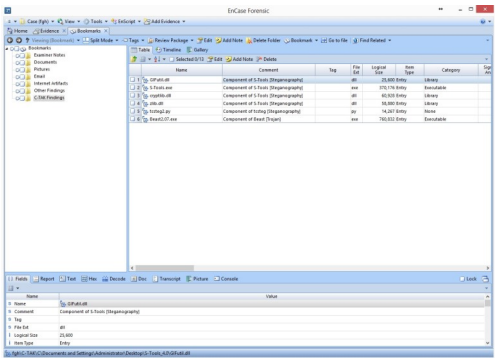
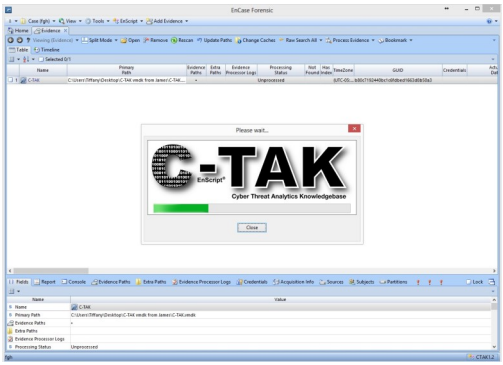
C-TAK™

HOJA INFORMATIVA



Amplié su búsqueda de evidencia de EnCase® con Cyber-Threat Analytics Knowledgebase (C-TAK). Esta tecnología proporciona examinadores con alto rendimiento y la identificación precisa de las amenazas cibernéticas como Troyanos, Esteganografía, Rootkits y Anti-forenses que puede afectar directamente las investigaciones. No sólo la presencia y la clasificación de estos programas permiten a los examinadores de ver a sospechosos desde una nueva perspectiva, sino a un nivel de paranoia, sofisticación del sospechoso y conductas encubiertas también se pueden derivar en la búsqueda de aplicaciones con un tema común. Estos comportamientos pueden ayudar a determinar la capacidad sospechosa, actividades, intención, amenaza o "conciencia de culpa".





PRUEBA GRATIS C-TAK:

Nuestra versión de prueba gratuita de 30 días de C-TAK ofrece la identificación rápida de una amplia gama de amenazas cibernéticas incluyendo: Troyanos, Keyloggers (capturadores de teclado) y Rootkits.

C-TAK VERSIÓN 2.0:

C-TAK ofrece la rápida identificación de una amplia gama de amenazas cibernéticas. La versión completa incluye los siguientes conjuntos de datos: Anti-forenses, Botnet (las Redes de Bots), Herramienta de Fraude, Denegación de Servicio, Criptografía, Escner de Exploits, Keylogger (Capturador de Teclado), Descifrado de Contraseñas, Peer to Peer, Piratería, Acceso Remoto, Rootkit, Scareware, Sniffer (Rastreador de Red), Programa Espía, Esteganografía, Juego de Herramientas, Troyano, Amenaza de la Web, Hacking en Redes Inalámbricas y Ransomware.

C-TAK es una aplicación EnCase desarrollada específicamente por EnCase AppCentral. C-TAK Versión 2.0 ha sido probado con EnCase Forensic versión 7.1.

Para adquirir u obtener información adicional, póngase en contacto con sales@wetstonetech.com

WetStone