

Continuamos ofreciendo la descarga gratuita del software "INVESTIGADOR": una aplicación forense de especial utilidad para inspección y recolección automática de evidencia digital. Este script utiliza aplicaciones gratuitas para realizar una recolección de información digital asociada a un equipo informático. Este release presenta una depurada interfaz de usuario.

Investigador. Inspección y recolección automática de evidencia digital.
Live forensics y user profiling in Lab.
Desarrollado en el Laboratorio Pericial Informatico - Neuquen - Argentina.
<http://www.informaticapericial.com.ar>

Versión: 2.0

Fecha de lanzamiento: 23-05-2012

Este software utiliza aplicaciones gratuitas para realizar una recolección de información digital asociada a un equipo informático.

Normalmente los archivos y carpetas que conforman "Investigador" deben ser copiados a un dispositivo removible, por ejemplo en un pendrive. Posteriormente, este dispositivo se irá conectando en los equipos informáticos en el lugar del hecho para recolectar información digital, o bien ejecutado en el laboratorio sobre máquinas virtuales creadas a partir de imagenes forenses de los equipos informaticos.

Este proceso puede demorar varios minutos. No lo cancele ni cierre las ventanas emergentes que la aplicación vaya desplegando.

Los resultados del triage son guardados en una carpeta en el mismo dispositivo desde el que se ejecuta el software.

Asimismo, el software Investigador crea una carpeta comprimida con todos los archivos resultantes de la inspección digital automatizada.

El software se ejecuta con el comando: `investigador.exe`

Pueden seleccionarse opciones de inspección desde menús y pulsar el botón "Ejecutar" para iniciar el proceso de recolección automática de evidencia digital sobre un equipo informático.

El software Investigador crea una carpeta que contiene un archivo index.html desde el cual podrá accederse a toda la información digital recolectada.

La aplicación contiene dos herramientas muy útiles durante las inspecciones digitales en el lugar del hecho, a saber: Búsqueda de Archivos y Hashing.

Utilizado en una inspección preliminar en el lugar del hecho, el software permite obtener información volátil. Investigador es valioso como ayuda para determinar si un equipo informático puede ser fuente potencial de evidencia digital, y si es procedente el secuestro del material probatorio o la generación de una imagen forense para un posterior análisis forense exhaustivo de los contenidos digitales (pericia informática).

En el laboratorio pericial informático, esta herramienta se introduce y ejecuta en una máquina virtual generada a partir de la imagen forense de un equipo informático y permite obtener un perfil general con datos del sistema operativo, actividades realizadas por el usuario del equipo informático y algunas contraseñas guardadas voluntariamente al utilizar navegadores de Internet. Estos elementos son de utilidad para trazar lineamientos forenses y profundizar la investigación digital.

[Descargue la aplicación INVESTIGADOR](#)

SE AGRADECEN comentarios sobre el funcionamiento del software mediante el formulario al pie del artículo.

Cordiales saludos a la comunidad forense argentina.

Sebastian Gomez

<http://sebastiangomez.sytes.net>