

CAINE, LiveCD GNU/Linux para Informática Forense

CAINE (Computer Aided INvestigative Environment), es una distribución GNU/Linux en modo LiveCD creada por Giancarlo Giustini como un proyecto de Informática Forense (Forense Digital) para el Centro de Investigación en Seguridad (CRIS), con el apoyo de la Universidad de Modena y Reggio Emilia.

El proyecto CAINE (Computer Aided INvestigative Environment) no pretende ser una nueva herramienta forense o framework de recopilación de ellas, pues este tipo de distribuciones ya existen (ej. Felix FCCU, Deft, entre otras). CAINE propone como novedad un nuevo entorno de fácil uso para todo este tipo de herramientas. Además introduce nuevas características importantes, que aspiran a llenar el vacío de interoperabilidad a través de diferentes herramientas forenses, ya que proporciona una interfaz gráfica homogénea que guía a los investigadores digitales durante la adquisición y el análisis de las pruebas electrónicas, y ofrece un proceso semi-automático durante la documentación y generación de informes y resultados.

El proyecto CAINE proporciona al usuario las siguientes principales novedades:

- Fácil interoperabilidad durante todo el análisis (Preservación, Recolección, Análisis, Reportes).
- Amigable entorno gráfico.
- Ubuntu como sistema base, ello implica un fácil uso y fácil instalación o adaptación sobre nuestro entorno de trabajo.
- Generación semi-automática de reportes.
- Algunas herramientas incluidas:
 - Grissom Analyzer
 - Automated Image & Restore (AIR)
 - Guymager
 - Foremost and Scalpel
 - Autopsy 2.20 and TSK 3.0
 - SFDumper
 - Fundl
 - Stegdetect
 - Ophcrack

- Más información sobre CAINE (Página Oficial del Proyecto)
- Descargar CAINE (ISO, +/- 670Mb)
- Descargar máquina virtual desarrollada para VMware WorkStation o VMware Player (Desarrollada por el equipo Bagside)

Fuente: <http://seguridad-informacion.blogspot.com/2008/11/caine-livecd-gnulinix-para-informtica.html>