

Proposal Proyek Akhir
EC-5010 Keamanan Sistem Informasi

Forensik Komputer : Evaluasi Autopsy dan Sleuthkit

Oleh:

Daniel Widyanto

13200021

Abstrak

Autopsy dan sleuthkit adalah *open source* forensik *toolkit* berlisensi GPL. Keduanya merupakan pengganti TCT (*The Coroner Toolkit*) dan TCTUTILS. TCT dan TCTUTILS saat ini tidak lagi dikembangkan publik open source. Dibandingkan TCT / TCTUTILS, sleuthkit / autopsy mempunyai banyak kelebihan. Diantaranya adalah kemampuan untuk menganalisis data di berbagai filesistem yang berbeda. Hal ini memungkinkan ahli forensik untuk menganalisis data di NTFS dengan UNIX/Linux. Selain itu, autopsy juga dilengkapi dengan fasilitas manajemen data. Secara otomatis, autopsy akan menghasilkan file log mengenai langkah-langkah yang telah diambil saat melakukan forensik. Berbagai kelebihan ini menjadikan sleuthkit / autopsy sebagai toolkit forensik terbaik di dunia open source.

Makalah ini menyajikan hasil evaluasi penggunaan autopsy dan sleuthkit. Isi makalah meliputi instalasi, pembahasan fasilitas autopsy dan sleuthkit (beserta cara penggunaan), file-file konfigurasi, dan trik-trik yang dipakai untuk menggali informasi. Penulis berharap makalah ini dapat menjadi referensi utama bagi pendesain forensik toolkit serupa.