**The Sleuth Kit**

1. Basic concept - Framework

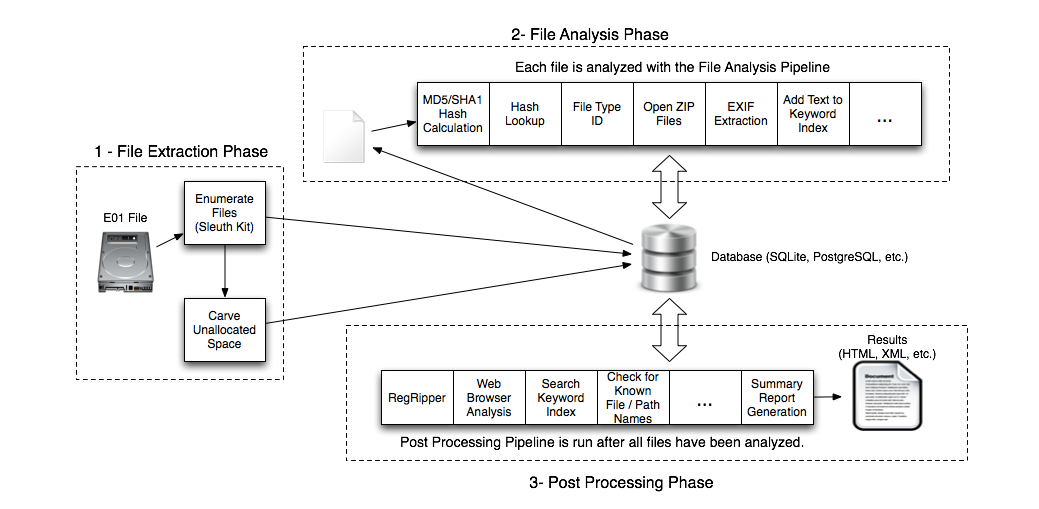
* Image database

Framework TSK menyimpan data dalam sebuah image database. Dapat berupa SQLite atau RDBMS. Detail pemnyimpanan dan retrieving data diatur oleh interface TskImgDB.

* Pipelines & Plug-In Modules

Pipeline agar developer lain bisa menambah modul dengan mudah

* Blackboard  
  Memungkinkan modul untuk berkomunikasi
* Services  
  Core service yang sudah disediakan oleh framework, contohnya logging dan file management
* Three phase analysis process
  + File extraction : file diidentifikasi menggunakan data file sistem, carving, dan metode pemulihan file lainnya
  + File analysis : setiap file dianalisis satu per satu
  + Post-processing : hasil dari analisis tiap file digabungkan dengan hasil analisis image



1. Pipeline & Module

* Pipeline : set of module yang dijalankan dalam urutan tertentu. Setiap modul melakukan specific task. Pipeline dikonfigurasi menggunakan XML file.
* Ada dua pipeline yang sudah didefinisikan oleh framework :
  + File analysis pipeline : perform task on every file in image. Setiap modul pada file analysis pipeline mengirimkan reference ke file object yang bisa digunakan untuk mengakses metadata dan isi filenya. Setiap modul juga dapat mengakses hasil analisis dari modul sebelumnya melalui blackboard. Contoh : hash calculation, hash lookup, archive file extraction, text extraction.
  + Post-processing pipeline : perform task setelah semua file dianalisis satu per satu pada file analysis pipeline. Dapat digunakan untuk dua jenis tugas. Yang pertama untuk menggabungkan hasil dari file analisis pipeline dan membangkitkan laporan. Yang kedua adalah untuk menganalisis sebagian kecil dari kelompok file, misalnya analisis pada Windows registry.
* Ada dua tipe modul yang bisa ada pada setiap jenis pipeline :
  + Plug-in module : deprogram khusus untuk dapat dimasukkan dalam framework. Dapat mengakses seluruh sumber daya dari framework.
  + Executable module : command line tools yang dapat dijalankan dari pipeline. Tidak punya akses ke image database, blackboard dan servis yang disediakan oleh framework. Bisa diakali dengan membuat plug-in module yang spawn proses lain untuk menjalankan executable module.
* Pipeline configuration : file XML yang dapat digunakan untuk mengatur modul apa saja yang akan dijalankan serta urutannya dalam pipeline.

1. Blackboard

* Collection of artifacts, each associated with a file, and each consisting of a name-value pairs called attributes.
* Accessing the blackboard : getting reference to TskBlackboard object from TskServices
* Artifact type : terdiri dari unique type name & human readable display name. Ada yang standard (predefined) dan bisa defined sendiri.
* Attribute type : merupakan name dari pasangan name-value atribut. Sama seperti Artifact type, harus unik, terdiri dari predefined dan bisa define sendiri. Bisa punya context field yg berupa string (contoh penggunaan : tambahkan LastSaved & LastPrinted context value pada artifact DateTime)