Forensic Toolkit

Forensic Toolkit is computer software developed by "AccessData" company and was released in May 2017. This tool objective is to scan hard drives while gathering various information.

The Forensic Toolkit scan to locate deleted emails and scan a disk for text strings to use them as a password dictionary to crack encryption.

The toolkit also includes another standalone program called "disk imaging".   
The imager is a simple tool that saves an image of a hard disk in one file/segment that may be reconstructed later.   
FTK Imager calculates MD5 hash values and confirms the integrity of the files before closing it.

FTK is a very fast and stable and due to his use of distributed processing he uses 100 percent of its hardware resources.  
Since indexing is done up front FTK is a very fast searching tool and he is also DataBase driven and All his data is stored securely and centrally.

Some of the tools that FTK contains are:  
**Email** **Analysis** - provides an intuitive interface for email analysis for forensic professionals. This includes having the ability to parse emails for certain words, header analysis for a source IP address, etc.  
**File Decryption** - A central feature of FTK, file decryption is arguably the most common use of the software. Whether you want to crack passwords or decrypt entire files, FTK has an answer for it. You can retrieve passwords for over 100 applications with FTK.  
**Data Carving** - includes a robust data carving engine. Investigators have the option to search files based on size, data type, and even pixel size.

**Data Visualization** - Evidence visualization is an up-and-coming paradigm in computer forensics. Rather than analyzing textual data, forensic experts can now use various data visualization techniques to generate a more intuitive picture of a case. FTK empowers such users, with timeline construction, cluster graphs, and geolocation.

**Web Viewer** - One of the more recent additions to the suite, the FTK Web Viewer is a tool that accelerates case assessments by granting access of case files to attorneys in real time, while evidence is still being processed by FTK. It also allows for multi-case searching, which means that you don’t have to manually cross-reference evidence from different cases.

**Cerberus** - Embracing the shift towards analytics, FTK has included a powerful automated malware detection feature called Cerberus. It uses machine intelligence to sniff malware on a computer, subsequently suggesting actions to deal with it if found.

**OCR** - Another feature that borrows heavily from AI and computer vision, FTK’s Optical Character Recognition engine allows for fast conversion of images to readable text. Multi-language support is also included.