CyberCheck Suite

CyberCheck Suite is a comprehensive collection of tools to perform cyber forensic data acquisition of digital evidence, analysis and data recovery.

TrueBack

Digital Evidence Seizure and Acquisition Tool

Perform Seize,Acquire or do both seize and acquire together with Trueback which is NIST Compliant. Solutions are available for both Windows and Linux Operating system. The tool creates a report on the seizure acquisition process which has details of the entire process with hash values, exhibit details and the system details as well.

Other Features Includes:

- MD5 hash algorithms.
- Block hash.
- Loseless Compression of acquired image file.
- Generate detailed report on Suspect device Seizure and acquisition.
- Bootable solution in Linux on USB & CD with Disk Preview

CyberCheck

Data Recovery & Analysis Tool

CyberCheck is a forensic data recovery and analysis tool to enable law enforcement officers to quickly and efficiently analyse digital evidence files. The tool has a very simple to use GUI which can be used by a novice user.

Data Analysis

CyberCheck can analyse TrueBack image, Encase image and raw disk dumps.The tool can generate a detailed report on the analysis findings which is very handy for the investigating officers to submit before the court of law. The tool can extract unallocated and disk slack areas, perform data carving on the entire image of slack areas and provides options to do analysis based on file hashes and file's signature.
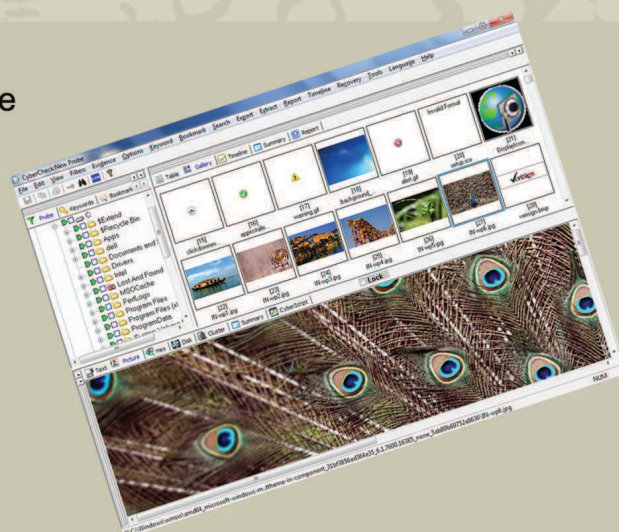
File System Support

File Systems supported by CyberCheck includes FAT12/16/32, NTFS, Linux EXT2/3/4 FS, UFS, CDFS, Sun Solaris, Reiser FS, Unix(Free BSD) and MAC. Also supports dynamic disks and Linux RAID disks

# CyberCheck Suite

Data Recovery

Cybercheck can recover deleted files/folders, deleted partitions and formatted data on a partition. All of these information can be added to the report to record the findings.

Powerful Search Facility

CyberCheck provides a plethora of search options for the investigating officer to ensure that he never misses any data. It has multiple keyword search, GREP search, file search based on hash values, Unicode search to find the data in any language and Index-based search to quickly search through the huge data space.

Other Features Includes:

▶ Preview support for disks and partitions

▶ File Data Carving from ambient space

▶ Picture, Gallery, Timeline and Text/Hex views

▶ Integrated Mailbox, Internet History and Registry viewers

▶ Scripting support for automated analysis

▶ Anti-forensics tools and activities detections

▶ Steganography file detection and extraction of hidden messages.

▶ Unicode & Indian Language support

▶ Report generation

F-RAn
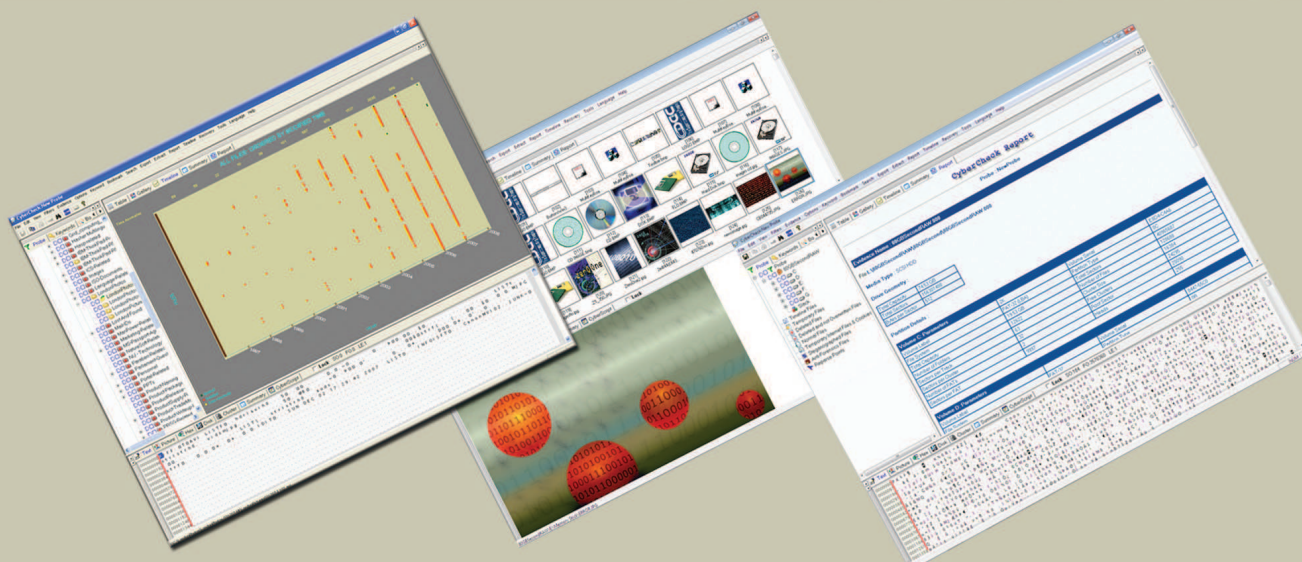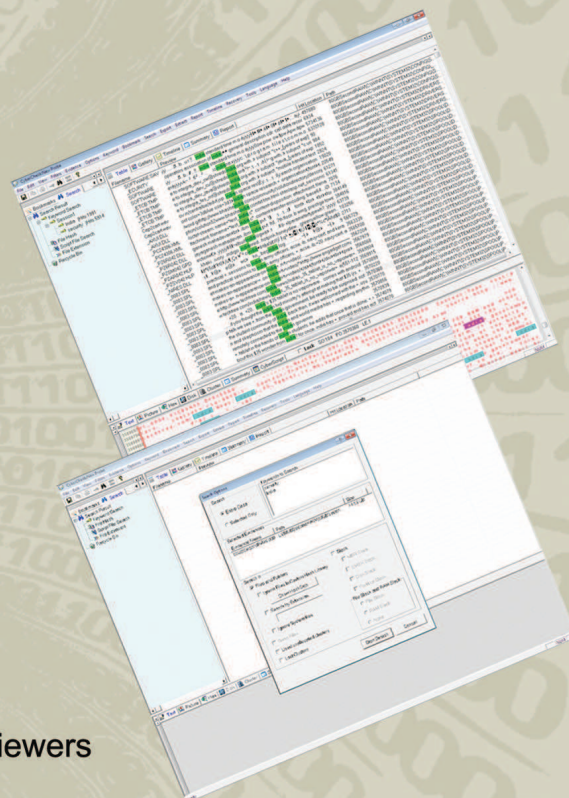
Forensic Registry Analysis Tool

The Forensic registry analysis tool automatically extracts crucial information from the live registry or the raw registry files found in digital evidence image files and displays it in user understandable format. It performs time conversion and translation of binary and other non-ASCII data. The tool can generate a report on extracted information along with hash values which can be printed directly from the tool.

Other Features Includes:

▶ Displays MRU files
▶ Displays Recently accessed applications
▶ List out installed Software & System's Information.
▶ Details of forensically sound information values like shutdown time, auto-complete passwords & removable devices
▶ Hashing registry
▶ MD5 / SHA256 Hashing of raw registry files

F-DaC
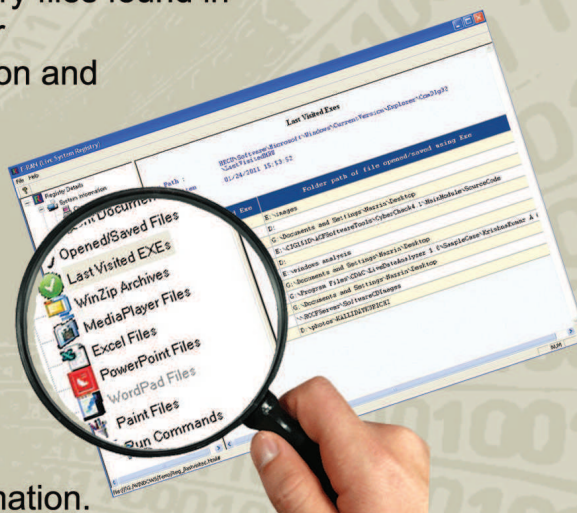
Forensic Data Carving Tool

A forensic data carving tool to carve different files with optimised search engine for identifying files based on headers and footers.The tool can generate report on the carved files which is very handy while producing the evidence before the court of law.

Other Features Includes:

▶ Support for TrueBack image, Encase image and Raw DD images
▶ Carve out Thumbnails from thumbcache
▶ Header/Maximum file size carving
▶ Header Embedded length carving
▶ Support for JPEG, GIF, BMP, PNG, PSD, PDF, ZIP, HTML, MS Office files, Video files(AVI,DAT,MP4, MOV, WMV & 3GP)