CHFI Tool Notes by Ken Underhill

Recover My Files (Windows): recovers deleted files emptied from the recycle bin, or lost because of the format or corruption of a hard drive, virus or Trojan infection, and unexpected system shutdown or software failure. Recovers even if you have reinstalled Windows. Gets data from RAW hard drives, partition errors, and after hard disk crash. Preview “data-on-the-fly” while searching.

Recuva: recovers pictures, music, documents, videos, emails, or any other file type that are lost. Can also recover from rewritable media like memory cards, external hard drives, USB, etc… Offers superior file recovery and can recover files from damaged or newly formatted drives and the chances of recovery are higher. Offers Advanced Deep Scan mode that scours a drive to find any traces of files that have been deleted. Securely deletes files with secure overwrite feature that meets military standards.

EASEUS Data Recovery Wizard: a hard drive data recovery software to recover data lost from PCs, laptops, or other storage media because of deleting, formatting, partition loss, OS crash, virus attack, etc…Supports large hard disk, can specify recovery file types for precise search results, allows you to preview files before recovering.

Advanced Disk Recovery: scans the entire system for deleted files and folders and provides an opportunity to recover them. Hard drives, partitions, external devices, CDs, DVDs can be scanned for recoverable files with Advanced Disk Recovery. Offers two types of scans-- Quick Scan uses the Master File Table to find all files with the same file name. Deep Scan uses file signatures to search for deleted files and folders. After either type of scan, you are able to preview deleted files and folders, and restore any or all of them to the location of your choice. With a few clicks, you can locate and restore the majority of the files.

OnTrack Easy Recovery: data recovery software ready to retrieve missing files. It recovers data and also protects it.

Undelete Plus: recovers documents, photos, email, video, music. Recovers files emptied from the recycle bin, after accidental formatting, recovers even if Windows reinstalled. Recovers from storage devices.

Active@ File Recovery: contains CD/DVD ISO image that allows you to burn a bootable CD or DVD with a lightweight version of Windows 7. Can recover from a system that is not bootable.

Pandora Recovery: allows you to locate and recover files deleted from FAT and NTFS-formatted volumes. Scans and builds an index of existing and deleted files and directories.

Disk Drill (Windows or Mac): Recovers data from internal and external hard drives, USB, iPod, memory cards. Recovers files from partition loss, hard drive reformatting, failed bootup, accidental deletion, Recycle Bin cleanup, and memory card corruption.

R-Studio (Mac, Windows, Linux): raw file can be used for heavily damaged or unknown file systems, recovers data on disks even if partitions are formatted, damaged, or deleted.

Data Rescue 4 for Mac (also Windows version): recovers files from crashed or virus-corrupted hard drive, non-mounting hard drive, reinstalled OS, or accidently reformatted hard drive, or damaged, missing, or previously deleted files. Recovers all file types from any HFS/HFS+ formatted drive.

Stellar Phoenix (Mac or Windows): recovers deleted files with their original file name. Supports RAW recovery on lost volumes.

File Salvage (Mac): recovers lost files, iTunes libraries, iPhoto collections, lost data. Recovers from Mac OS hard drive, USB, PC disk, Linux disk, FAT32 disk, FLASH card, scratched CD, digital camera, iPod, and any other file system recognized by Mac OS.

DiskDigger (Windows 10, 8, 7, Vista, XP): undeletes and recovers lost files from hard drives, memory cards, USB drives. Recovers documents or photos accidently deleted or from a reformatted camera memory card, or can be used to check files on an old USB drive. Shows recoverable files as a **thumbnail preview**,

Total Recall: recovers lost data from hard drives, **RAID**, photos, deleted files, iPods, FireWire, and USB.

Quick Recovery: recovers files that have been lost, deleted, corrupted, or deteriorated. Searches, scans, and recovers files that are **encrypted and password protected** and restores them. Repairs and recovers **disk bad sectors**, recovers virus-prone files, hidden and password protected files.

Data Recovery Pro: restores **deleted emails and email attachments**. Deeply scans hard drives, external drives, iPod Shuffle, iPod NANO, and iPod Classic to recover a wide variety of files.

SysAnalyzer (for dynamic malware analysis): helps you monitor the installation of executables, shows information like process ID, the new file path, open ports, process DLLs, loaded drivers, and tasks.

Dependency Walker (for dynamic malware analysis): lists all dependent modules, builds hierarchical tree diagram, records all the functions each module exports and calls, can detect application problems like missing/invalid modules, import/export mismatch, circular dependency errors, mismatched machine modules, and module initialization failure.

Xplico: Open Source network forensic analysis tool (NFAT) that extracts applications data contained from an internet traffic capture. Example--- from a pcap file it would extract all email, HTTP contents, VOIP calls, FTP, etc…

Comodo Programs Manager: dynamic malware analysis tool that helps investigators detect hidden and background installations which the malware performs.

Install Watch: dynamic malware analysis tool that helps investigators detect hidden and background installations which the malware performs.

Jv16 (jv16 Power Tools): this is used to analysis registry changes in malware analysis. Registry Cleaner is a part of this set of tools that detects errors that can have a measurable impact against system performance.

Cain & Abel: password recovery tool for Microsoft OS, offers cracking, password sniffing, VoIP recording, recover wireless network keys, reveals password boxes, uncovers cached passwords, analyzes routing protocols.

Capsa (network analyzer): supports over 300 network protocols, monitors network traffic, email monitoring, **can be used to detect Trojans**.

FileMerlin (document conversion): converts word processing, xls, ppt, and database files between wide range of file formats. Regarding as the premiere document conversion product.

AccessData FTK: can read dd image files (Ilook can also read dd image files), can calculate MD5 hash values and ensure data integrity, court-cited digital investigations platform that provides processing and indexing up front so filtering and searching is fast, can be setup for distributed processing and incorporate web-based case management and collaborative analysis, can create an image of a phone memory card.

Nuix Corporate Investigation Suite: used to collect, process, analyze, review, and report evidence

The Sleuth Kit (TSK): collection of command line tools and a C library to analyze disk images and recover files from them.

Remo Recover Pro (Mac): binary application that makes Mac data recovery easy on PowerPC and Intel based machines, recovers files lost emptied from the Trash or lost due to inaccessible Mac volumes, able to recover data even if the Disk Verify and Repair tool fails to retrieve the lost data.

Cisdem Data Recovery (DR) 3 (Mac OS): designed to help you recover and restore your lost data like videos, music, documents, archives, photos, and more. Offers a Quick scan and Deep scan. Link: https://www.cisdem.com/manual/datarecovery.pdf

Registry Editor (regedit) (Windows): used to load (open) or unload registry hives (hives begin with HKEY)

Proc Heap Viewer: enumerates process heaps in Windows. Uses a better process than Windows heap functions, which makes it fast and highly efficient. Can be used to discover heap related vulnerabilities.

Memory Viewer: view system memory configuration. Gives you information about the memory cards installed on the computer and the current memory allocation.