Innovative solutions in data security

1. Detection of residual traces in free space
   1. Visualization of residual traces of old files remaining in free space
2. Smart clean-up of free space
   1. Clean-up of residual traces in free space areas needing a reset to zero We assure no useless clean-ups.
   2. Areas already reset to zero are not cleaned which can speed up clean-up by 2x to 100x.
   3. Clean-ups will become much faster after the first run.
3. File table clean-up
   1. Clean-up of residual traces in file tables, not only in FAT/MFT
   2. Additional clean-up of INDEX attributes in MFT
4. Smart overwriting
   1. Recognition of type of storage medium of your storage device: magnetic disk, SSD, etc
   2. Adaptation of the erasure algorithms to the storage medium
5. Smart clean-up of jump lists
   1. Clean-up of your jump lists without deleting your pinned items/ websites which are preserved
6. Smart clean-up of Prefetch
   1. Removing of invalid Prefetch entries. Old valid entries are preserved.
7. Deletion of USB history
   1. Deletion of remaining traces of disconnected device (name, date, etc)
8. Scan and clean-up of the content of Pagefile.sys + Hiberfil.sys
   1. Visualization of the content of Pagefile.sys + Hiberfil.sys
   2. Pagefile.sys clean-up options: at each PC shutdown, or at next shutdown only
   3. Control of Hiberfil.sys clean-up: PrivaZer makes sure that the file Hiberfil.sys is reset to zero.
   4. If not, PrivaZer overwrites the content of Hiberfil.sys with zeros.
9. Scan of thumbnails
   1. Full scan of the drive to retrieve remaining thumbs.db files and show their content
   2. Visualization of Thumb Cache files content
10. Scan of residual traces in Indexing service
    1. Scan of remaining traces of deleted files still indexed by Windows ™ (Indexing Service)

Major functionalities

1. Find and display
   1. PrivaZer scans your system and your external storage devices
   2. PrivaZer shows you its findings in easy-to-follow visualizations
2. Clean and protect
   1. Irreversible clean-ups by overwriting techniques
   2. Smart overwriting: PrivaZer automatically recognizes your storage device type and adapts its overwriting algorithms to the storage medium (magnetic disk, SSD, etc)
   3. Your personal documents are preserved
   4. You can control existence of remaining sensitive traces after clean-up
3. Protection against recovery
   1. Your old, deleted files can still be recovered with an expert recovery software.
   2. PrivaZer performs a clean-up of residual traces in the file tables (FAT or MFT) and in the free space to avoid any possibilities of recovery
   3. No recovery possible even with an expert software like:
      1. GetDataback
      2. Testdisk
      3. O&O DiskRecovery
      4. Recuva
      5. Glary Undelete
      6. Easeus Data Recovery
      7. Pandora Recovery
      8. Paragon Backup & Recovery
      9. Ontrack EasyRecovery
      10. Recover My Files
      11. Stellar Phoenix Data Recovery
4. Included visualizer & viewer
   1. Disk usage
   2. Index.dat
   3. Pagefile.sys
   4. Hiberfil.sys
   5. Jump lists
   6. Thumbcache and Thumbs.db
5. Smart clean-up of free space
   1. Optimized clean-up of residual traces remaining in storage free space
   2. Areas already reset to zero are not cleaned which can speed up clean-ups by 2x to 100x.
   3. Efficient clean-up algorithms for fast clean-up
   4. The clean-ups will become much faster after the first run
   5. We assure no useless clean-ups
6. Smart clean-up of cookies
   1. PrivaZer helps you choose cookies to delete
   2. Cookies of your favourite sites are preserved so that you do not need to retype your login/password again and again
7. Smart clean-up of jump lists
   1. Cleans useless histories of opened files, visited websites, etc appearing in jump lists
   2. Your pinned items are preserved
   3. Your pinned websites are preserved
8. Smart clean-up of prefetch
   1. PrivaZer performs a smart clean-up of Windows Prefetch
   2. Prefetch is useful for your system and should not be removed completely
   3. PrivaZer takes care of your Prefetch by removing invalid Prefetch entries
9. Shredder
   1. Definitive and irreversible deletion of files or directories of your choice
10. Other key features
    1. Scheduling of clean-ups
    2. Live measurement of free space gain
    3. PrivaZer priority execution management
    4. Indexing management
    5. Hibernation management
    6. Registry clean-up
    7. Registry restore
    8. System restore

Securely clean more than 100 analysis

* Internet browsers
* Index.dat
* Cookies
* Cookies Tor
* Cookies Flash
* Cookies Silverlight
* DOM Storage
* IndexedDB
* AppCache
* Registry
* RAM
* Pagefile.sys and Hiberfil.sys files
* Use of software
* Messengers
* Histories of visited websites, videos, software, opened docs, etc
* Jumplists
* Recycle bin
* Temp files
* Log files
* Invalid Prefetch entries
* Indexing service
* ThumbCaches, Thumbs.db
* Residual traces of deleted files
* Free space
* File table (MFT or FAT)
* INDEX attributes in MFT
* USN Journal, etc

Definitive deletions of files

* PrivaZer offers you the ability to permanently delete individual files or directories of your choice to prevent full or partial recovery of them.
* Need to delete a specific or directory, but want some assurance that it is truly gone for good?
* PrivaZer permanently and irretrievably erases data that the world doesn’t need to know about.

How to test PrivaZer's performance?

1. Smart clean-up of free space
   * Scan and clean traces in free space with PrivaZer
   * Note elapsed time in the clean-up window
   * Do step 1 again and compare elapsed times
   * You should notice that 2nd clean-up is much faster than 1st one.
   * Comment: smart clean-up of free space is available for all FAT and NTFS formatted drives and for C:\ drives if formatted as NTFS (which is generally the case)
   * Click here to see tutorial & test result no. 1 – PDF link
   * Click here to see tutorial & test result no. 2 – PDF link
2. Detection of residual traces in free space
   * Download free version of sdelete from Microsoft website: here - Link
   * Reset to zero free space with sdelete (use option -z to zero current drive free space)
   * Scan the traces in free space with PrivaZer
   * PrivaZer should detect no trace in the free space.
   * Comment: a minimum level of traces will always be detected on your C:\ drive.
   * Because your system continuously creates files, moves files and deletes temporary files in the background.
   * So, you'd better perform the test on a second internal or external drive.
   * Click here to see tutorial & test result no. 1 – PDF link
   * Click here to see tutorial & test result no. 2 – PDF link
3. Detection of residual traces in free space
   * Clean file table (FAT or MFT) with PrivaZer
   * Download free version of sdelete from Microsoft website: Link
   * Reset to zero free space with sdelete (use option -z to zero current drive free space)
   * Copy a file of about 100 MB or more in size
   * Delete the file
   * Empty recycle bin (to be sure the file is really deleted)
   * Scan traces in free space with PrivaZer
   * PrivaZer should detect residual traces left by the file
     1. in the free space (red colour)
     2. in the file table (FAT or MFT)
   * Click here to see tutorial & test result no. 1 - Link
   * Click here to see tutorial & test result no. 2 - Link
4. File recovery prevention
   * Download free version of recovery software: GetDataback: Link or Recuva: Link
   * If you intend to use GetDataback, be sure to have checked the option: "Recover deleted files"
   * Scan recoverable files with GetDataback
   * Clean traces in free space + traces in FAT/MFT, with PrivaZer
   * Scan again recoverable files with the recovery software
   * The recovery software should no longer detect recoverable files
5. Click here to see tutorial & test result no. 1 – PDF link
6. Click here to see tutorial & test result no. 2 – PDF link