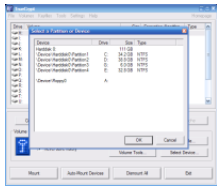


25 January 2007

By: Ionut Ilascu, Editor, Software Reviews



## The Last Stand

### *Encrypt the files and volumes*

Usually in a multi-user environment, privacy is hard to achieve. There is not much to do for a regular computer user in order to protect certain sensitive data. A neophyte user will limit to applying passwords to the accounts, but that can be easily undone. So archiving the sensitive files and applying a password would seem a logical choice. However secure this process may be, it will take a lot of time to open the archive and be able to write files back in it. A viable solution, less painful and faster, would be creating virtual volumes. Their size can be defined by the user and mounting and unmounting them is done very fast. They act as real volumes, and depending on the encryption method you are using they can be extremely reliable. TrueCrypt is a free utility that can encrypt volumes and create virtual ones. The virtual drives are encrypted with one of the eleven encryption algorithms available in the application: AES-256, Blowfish, CAST5, Serpent, Triple DES, Twofish, AES-Twofish, AES-Twofish-Serpent, Serpent-AES, Serpent-Twofish-AES and Twofish-Serpent. The hash algorithm also depends on user's choice and can be RIPEMD-160, SHA-1 or Whirlpool. Hash value practically provides a small digital fingerprint from any kind of data on your computer. This way, the files can be recognized by the machine and handled accordingly. The interface of the application is as simple as can be and the regular user can handle it quite easy. However, a little work can be done here in order to make it more appealing. After all, Vista is coming with all those pretty pictures. Taking a look at the graphics included in the package one can clearly see that the emphasis of the developer was on functionality and the aesthetics came second. Regarding the functionality, the application boasts with capabilities of encrypting both entire drives and even disks as well as creating virtual volumes protected by a password or a key stored on the computer. If the user encounters any problems while working with the TrueCrypt, a User's Guide is included in the installation of the application. The 105 PDF file will thoroughly explain all the abilities TrueCrypt has and will also answer questions about technical terms and operations. The volume encrypting possibilities provided by TrueCrypt are extensive enough to go as far as protecting CDs, DVDs or USB memory sticks. For the removable storage device to be automatically mounted when inserted, a special script file needs to be created ("autorun.inf"). This can be created using the Traveller Disk Setup function in the Tools menu. The best feature TrueCrypt provides for the user is the possibility of creating a virtual volume inside a virtual volume. This drive is called "hidden drive" and supports a different password than the outer volume that shelters it. Its purpose is to create a better protected environment for your sensitive data. It is totally invisible, but the only alleged drawback is that the virtual partition will have to be FAT type. Considering that nowadays very few computers still use this file system (NTFS works better, is more reliable and the security is higher on Windows XP) this may sound as a downside. But due to its more feeble protection, TrueCrypt can make these drives totally invisible and cannot be detected by checking the free space on the outer drive (the free space on any TrueCrypt volume is always filled with random data; the condition for this to happen is to have Quick Format function disabled). The entire process and the works are extensively explained in the User's Guide. Keyfiles for locking the virtual volumes can be randomly generated by TrueCrypt and stored on the computer's HDD. The downside of the keyfiles is that they cannot be saved directly on a USB memory stick and the "tiresome" process of moving/copying it from the HDD to the removable storage device is mandatory. The best thing is that the user can create a virtual drive out of any file there is on the computer. This way, you will take an extra protection measure as the extension is preserved and mounting

it is done with no problems. Your virtual drive file can be stored anywhere on your computer and not be recognized by prying eyes as it is masked by the extension and the icon of the software it is associated with. The only issue you should pay attention to in this case is the size and type of file you choose (an image file of 4BG will definitely draw your attention). **The Good** Similar applications cost enough to make you avoid them. TrueCrypt is open-source. You can create virtual volumes inside virtual volumes (create hidden partitions). User's Guide provides far-reaching information on how to use the software and what to use it for. The ease of use can make even neophytes look like experts in virtual drive creating. CDs, DVDs and USB memory sticks can be encrypted with no difficulty. **The Bad** The container of the virtual drive can be moved, copied and, most of all, deleted just like any other regular file. **The Truth** Try it, it is free and easy to use. The options provided and the explanations in the User's Guide will help you get through the possible intricacies. *Here are some snapshots of the application in action:*