

6 March 2008

By: Ionut Ilascu, Editor, Software Reviews



NTI Ninja

## [Ninja USB Protection](#)

### *Invisibility mode for file protection*

Memory sticks have become part of our storing device arsenal and some of the users are 100% dependent on the little fellows. Some think that its portability is sufficient protection for the data stored on it because, as long as you have it in your pocket or stuck in the computer you are working on, there is no way a perpetrator could get the hands on your important files. And yet you are familiar to those situations when you lose track of it and have hard times remembering where you left it. In other words, you lost it and although you won't admit it, all the data on the memory stick is no longer safe. U3 is one way to protect your data, thanks to its security feature that allows locking it with a password. But, in lack of this kind of device, software solutions are a good resort. NTI Ninja is one of the alternatives available and it comes with a 30 days trial. As the name suggests, it attempts to become the invisible bodyguard of your flash pen. It works by splitting your flash drive into two partitions, a public one that can be accessed by any user with absolutely no effort, and a hidden one that can be used only if the right password is entered. The interface is way too easy to use as the three buttons available are self explanatory with regards to their purpose. However, in order to use them, you have to plug in the portable device first. In case there are multiple USB drives plugged in, choose the one you want to store protected data on and create your ninja. Next, you have to set the size of the public partition, the one that everybody has access to. The moment you type in a value the application will automatically calculate the amount of space left for the private one. Applying a protection password (nothing less than 8 characters is accepted) and hitting the Start button will initiate the process of dividing the drive. Make sure you have nothing deposited on the drive as the process of splitting the flash pen involves formatting of the drive (FAT, FAT32 and NTFS are supported). You will however receive the appropriate warnings beforehand. Believe it or not, this is the entire process of making a private drive on your flash pen. Once all operations have completed (do not hurry up to plug the portable device out and follow the on screen instructions), your device should be able to run on absolutely any computer you plug it in and, according to my experience, it should provide a way to access the private partition. If public partition loads and it appears to be empty, try switching the view of hidden files and folders on for a change and you'll definitely bump into a hidden "Setup" folder. From there, launch "Open.exe". After this action was carried out, we did not receive the same feedback on all test systems we tried NTI Ninja. Out of two Vista Business, the app worked only with the one the software was installed on; with Vista Business happened the same, but when testing it on Windows, it worked like a charm and we gained access to the private partition easily. Additional testing carried out on a squeaky clean Vista Home Premium edition resulted in the same outcome, namely the password could not be entered in the NTI Ninja Open dialog. However, the only inconvenient we encountered when getting to make visible the private partition on the systems the software worked was that the setup files were stored with hidden attributes and, unless you unveiled them, there was really no way to benefit from the data. On the systems it did not work, the problem consisted in the fact that the Open dialog would remain unaffected by the introduction of the password and no matter how many times "Open" button is pressed the app simply does not process it. If you want to remove the hidden partition on the flash drive, suffice to start the software and click Remove Ninja button. Care should be taken when proceeding to this operation because all files and folders on the hidden partition will automatically be deleted. NTI Ninja is extremely handy for users that need to carry sensitive data on portable devices and keep it as safe as possible (there can't be any safer than invisible), but it fails to deliver the means of accessing the

private partition regardless of the computer used, as the application proved to be quite picky. But it seems it works better on XP systems than on Vista and, if you are worried about checking the drive in a non-Windows environment, you've got nothing to worry as during our testing on Mac and Linux the private partition remained hidden and only the public part was visible. The application does a great job protecting the data by creating a hidden partition, but we encountered problems with the setup files on the portable drive as they were quite picky and did not work on all stations we tested the app on. Besides the fact that password menu did not automatically prompt the user for typing it, the entire portable application is stored with hidden attributes on the public partition. So, if your system is not set up to hidden files and folders, the Setup folder of the application is going to slip your eyes. **The Good** NTI Ninja is extremely easy to use and handling the pen drive with protected partition is a breeze due to the portable instance of the app. There are three different file system formatting methods, FAT, FAT 32 and NTFS and for each of them there is a brief description for a better understanding of the alternative. You get to define the amount of space dedicated for public folders that can be accessed by anyone getting their hands on the memory stick and the difference is reserved for the private storage. **The Bad** We faced quite some trouble while trying to access the private partition with the right password, as the app would not process the countersign. The greatest failure percentage was on Vista systems, while with XP the rate of success was slightly higher. **The Truth** The fact that Setup folder is not visible could be to users' advantage, and if so, it should also be mentioned somewhere in the software or its help file. Sadly, our tests were not too successful as the software refused to process the password we provided and act accordingly. But, on the upside, the protection is quite heavy as even viewing the content of the private partition from another operating system was impossible and it seems that this can be done only in Windows environment via password screen. Setting it up and working with the software is the exact opposite of rocket science and regardless of your skill level there will be no problem handling its options. Hopefully, future versions will fix the glitch because it would be a shame to lose such protection. *Here are some snapshots of the application in action:*