



## SECRET AGENT MAN

Ray McGoldrick, Senior Product Manager  
Sofia Fernandez, Technical Writer

Today's USB storage devices come in different shapes and sizes, designed to conveniently store and transport huge amounts of data. They are often worn around one's neck on lanyards, on key chains, inside executive pens, or even concealed in pocketknives. Regardless of how these drives are presented, they all feature the same functions: pluggable, portable, and highly reliable. As the years have gone by, USB devices have become smaller, more affordable, and capable of holding gigabytes of data

- Gartner Dataquest reports the worldwide USB flash drive market for 2006 is expected to reach \$2.3 billion in revenues / 84.6 million in units and is anticipated to grow to \$2.9 billion in revenues / 98.2 million in units by 2008<sup>1</sup>.
- SanDisk reports that USB flash drives address the needs of students: a market of more than 65 million in the U.S. alone. An estimated 6.5 million new college students are expected in the fall of 2006 on U.S. campuses<sup>2</sup>.
- Windows ITPro.com reports on average, 200,000 of the estimated 1 million flash drives sold per week are purchased by corporate customers<sup>3</sup>.

But even with all the advancements in technology, most USB devices are still vulnerable when it comes to data security.

### Common Problems with USB Storage Devices

The two most common problems associated with USB devices are: 1) Unauthorized access to sensitive data during drive sharing; and 2) Lost or stolen drives.

USB flash drives introduce a significant security challenge not only for small and large organizations, but for individual users as well. Their small size and large storage capacity can make it a dangerous tool in the wrong hands.<sup>4</sup>

*Most of these devices have little or no security features and if you happen to lose your flash drive during your morning commute, anyone who picks up the device may be able to access data on it. These devices can also be quickly stolen off a desk, or "borrowed" and later returned to the office once the data has been copied.*

### Access, Transferring & Sharing Files

When considering what tools to use to protect the data on your USB device, it is important to keep several key factors in mind. Can you still easily access and transfer your data without a lot of hassle? Can you still share your data while using the security program on your drive?

---

<sup>1</sup>Gartner Dataquest 2006

<sup>2</sup>www.CampusMag.org 2006

<sup>3</sup>www.Windows ITPro.com 2006

<sup>4</sup><http://labmice.techtarget.com/articles/usbflashdrives.htm>

Currently, a small number of flash drives feature a password protection program that secures the entire drive. Although this solves the problem of unauthorized access or stolen data, it also creates a new problem; you can no longer share data on the device without revealing your password.

Other security programs are known to force users to snake in and out of programs in order to access their data. This often becomes a time consuming task of requiring you to tediously juggle across several steps.

## Solution

The best way to solve these problems is to select a software that enables you to easily access, modify, and share public data while securing important data on a protected private workspace that can easily be accessed by authorized users.

To do this, the software should create two partitions on the device; one that is not protected which can be shared with everyone, and a second protected partition which would require a password to view and access its encrypted data. This would allow you to fully protect your important data from prying eyes.

The software should be straightforward and easy to use. A simple interface that allows you to select the size of each partition by giving you visual feedback as you adjust the size for each partition. The interface should allow for password insertion, confirmation, and as a safeguard a password hint in case you forget your password. (Figure 1.1)

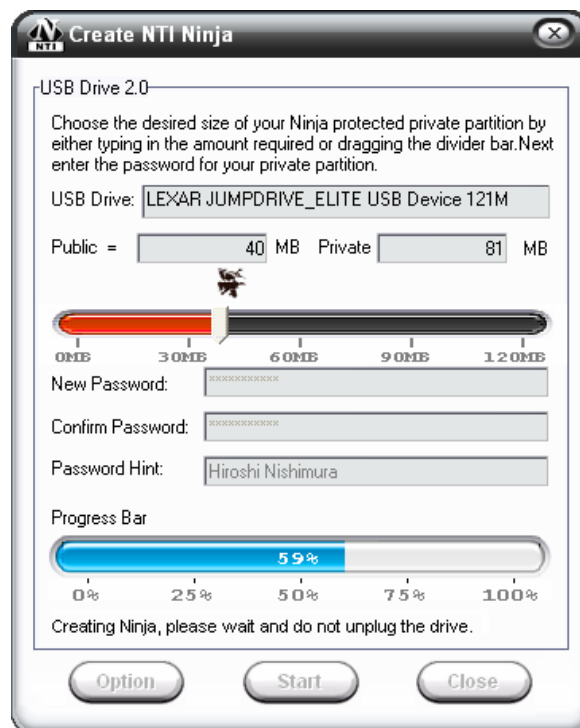


Figure 1.1

Having two partitions would make it easy to transfer data from one workspace to another, just drag and drop. This would eliminate the problem of logging in to one workspace and copying a file then logging out and logging into the other workspace to paste the file.

The software should have an option to select different formats to help enable users to customize their USB storage device according to their particular needs. Additionally, offering a *Quick Format* feature would come in handy to speed up the formatting process. (Figure 1.2)

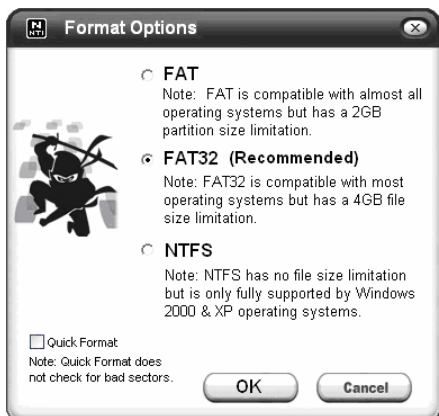


Figure 1.2

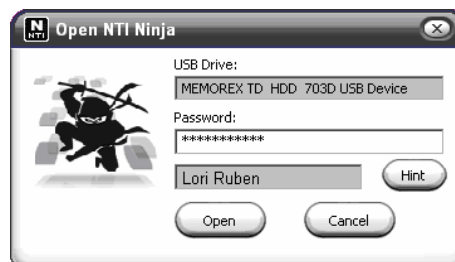


Figure 1.3

When you plug your device into your computer the software should automatically detect it and prompt you for a password to open your private workspace. This simple process would save you time from having to navigate in and out of programs to gain access to your private data. (Figure 1.3)

The application should also hide your private workspace and only make the private area seen when a password has been entered. On computers without the software installed there should not be any trace that a hidden or protected partition even exists.

## Conclusion

The ability to maintain the security of private data without upsetting the file sharing capabilities of public data are some of the features that even a secret agent would appreciate. Users want to be able to access their data as easily as possible and at the same time secure their confidential data. Data security software can meet this demand by implementing public and private partitions that work together in such a way that security is maintained while continuous file sharing remains uninterrupted.

## NTI

NTI is dedicated to providing effective, easy-to-use software solutions. *NTI Ninja<sup>™</sup>* is an exciting software that maximizes data protection by using a driver level encryption technology enabling the creation of private and public partitions on USB storage device. It allows you to easily access and share commonly used files on the public partition, but also restrict and hide access to confidential data on the private partition. To find out how you can benefit from NTI Ninja, or to learn more about other innovative solutions from NTI, please visit: [www.NTIus.com](http://www.NTIus.com).

