DataTraveler Elite and DataTraveler Elite – Privacy Edition

Advanced Security and High Performance White Paper

A leading-edge solution for business and corporate IT users that combines advanced data security with outstanding performance.

Introduction

Conveniently small, portable, and easy to use, USB Flash drives have become one of the fastest-growing Flash memory products. Many business customers and advanced consumers require key features to enhance their use of USB Flash drives, including advanced security, high performance and file synchronization.

Customers require advanced security to guard against sensitive data loss should the drives get lost, misplaced, or borrowed without permission. They want high-performance drives to speed up data transfers and increase productivity, with file synchronization between a computer and the drive to allow key data to be backed up and available for use on the road or on other PCs.

Kingston's DataTraveler® Elite ("DT Elite" or simply "DTE") and DataTraveler Elite – Privacy Edition ("DT Elite – Privacy" or simply "DTEP") USB Flash drives meet these needs. With the industry's highest performance and two-layer security incorporating hardware-based 128-bit AES encryption, DTE and DTEP drives are among the most secure USB Flash drives for Windows® -based systems in the world. In addition, DT Elite drives incorporate file management and folder synchronization through an easy-to-use TravelerSafe+ file management console.

This white paper will provide more details on the advanced security and high-performance features of the DTE and DTEP ultra-secure USB storage drives.

1.0 DT Elite and DT Elite – Privacy Edition Security Features

Robust security is the primary feature that was engineered into the DTE and DTEP drives. A two-layer security mechanism that features user authentication and hardware-based, real-time data encryption guards sensitive data stored in the privacy zone.

Both drives incorporate a built-in encryption/decryption co-processor for advanced security. They feature an industry-leading, high-performance Flash memory controller that offers one of the highest levels of USB 2.0 performance available on the market today.

The major difference between the DTE and DTEP drives is that the DTE drive allows for a public zone where files are always visible and accessible. The DTE – Privacy Edition drive does not allow a public zone; all data is invisible and encrypted until the user has successfully entered a valid password to access the privacy zone and its files. In addition, DTEP drives require a strong password, with a minimum length of 6 characters and requiring a mix of two of the following: Alphabetic, numeric, and special characters. Strong passwords, coupled with limited password retry capabilities (explained in section 1.3), make DTEP drives ultra-secure for enterprise-grade data protection.

1.1 User Authentication

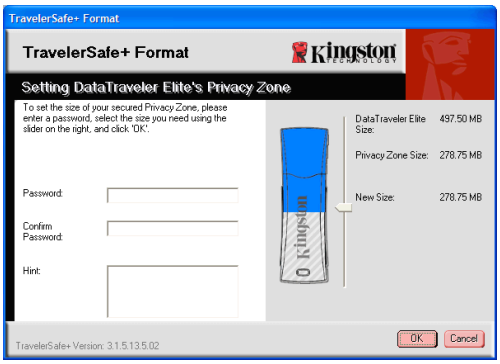
To activate the security features of the DataTraveler Elite, the user must create a privacy zone. As shipped from the factory, the DT Elite drive is set up as a single, public zone. All data stored in the public zone can be read by any host computer.

DTEP drives do not allow a public zone and are set up with a 100 percent privacy zone. There is no way to set up a public zone for data security reasons. In addition, DTEP drives do not provide a TravelerSafe+ program – they auto-launch their built-in login program to enter a password and access the drive.

1.2 Public and Privacy Zones on the DT Elite Drives

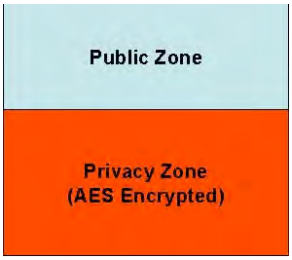
The owner of the DT Elite creates a privacy zone for the storage of secure data using TravelerSafe+, the DT Elite's access protection software for Windows-based systems. He or she defines a password to control access to the privacy zone, which is an area on the drive in which all sensitive data is kept. This password is stored in the DT Elite in an encrypted mode that makes it very difficult to decrypt.

The public and private zones are set when the DT Elite drive is first used, or when the owner wants to update the relative sizes, through the TravelerSafe+ program as shown below:



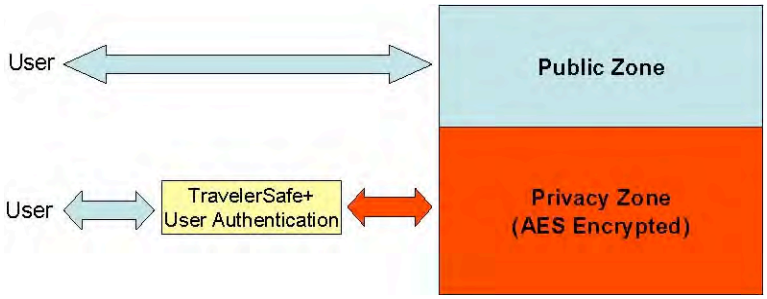
DTE drives feature a TravelerSafe+ Console to set zone sizes

Once a privacy zone is created using the TravelerSafe+ console, data stored there will be encrypted using the Advanced Encryption Standard (AES-128):



DT Elite with public and encrypted, password-protected privacy zone (shown in red)

Without a valid password, unauthorized access to the privacy zone is blocked, and the data remains encrypted and protected. Whenever the DT Elite is connected to a host computer, the TravelerSafe+ console needs to be used to log into and access the privacy zone:

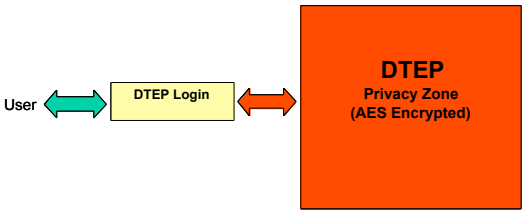


The privacy zone can only be accessed after valid password logon

Unlike other software consoles that allow unlimited numbers of incorrect passwords, DT Elite has a factory-set limit that locks the privacy zone after 25 *consecutive* failed attempts to log in. This limit blocks "Brute Force Attacks," in which programs are used to test millions of password combinations to find the correct password. After 25 consecutive invalid attempts, the DT Elite will lock out the privacy zone; the only option left at this point is to reformat the drive, thus losing all the encrypted data stored in the privacy zone.

1.3 Privacy Zone in DT Elite – Privacy Edition

DTEP drives only allow a privacy zone so there is no option to create a public zone. When a user successfully enters a valid password, the privacy zone allows access to all the files stored there.



DT Elite – Privacy Edition drive with only an encrypted, password-protected privacy zone

Like DTE drives, the DT Elite – Privacy Edition drives also lock the privacy zone after 25 consecutive failed attempts to log in. This limit blocks "Brute Force Attacks," in which programs are used to test millions of password combinations to find the correct password. After 25 consecutive invalid attempts, the DTEP drive will lock out; the only option left at this point is to reformat the drive, thus losing all the encrypted data.

2.0 Hardware-Based, Real-Time Data Encryption

Cryptography is the science of encrypting and decrypting data using a special "key" to encode and decode the data. Unencrypted data (or files) are processed through an encryption engine (either in software or in hardware) to produce an encrypted file; without the exact key, the data is unusable.

Kingston DT Elite and DT Elite – Privacy Edition drives feature one of the industry's best, most robust data encryption capabilities. Their encryption technology is based upon the same standard

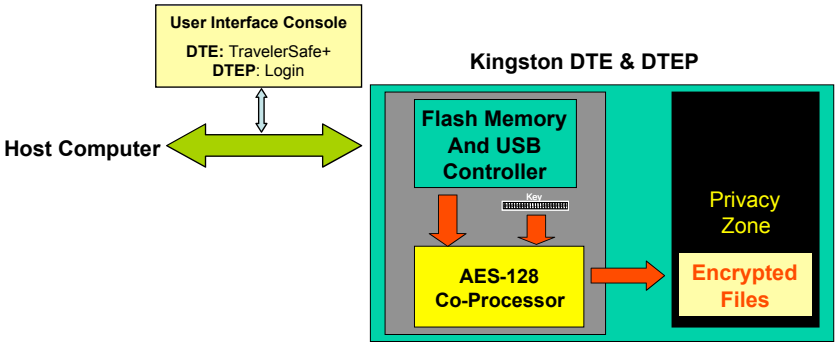
used in high-security applications – the Advanced Encryption Standard (AES). Keys are sequences of bits (128 in the case of AES-128) which are used by the encryption/decryption engine to uniquely process the data.

2.1 Advanced Encryption Standard (AES-128)

The Advanced Encryption Standard was defined by the National Institute of Standards and Technology (NIST) in 1997. Kingston has adopted the AES-128 standard for 128-bit encryption/decryption. With this standard, if a key is used to encrypt data, the exact same key must be used to decrypt the data. Without the same key, data would be a useless string of data.

2.2 DT Elite and DT Elite – Privacy Edition's Real-Time, Hardware-Based Encryption

The AES encryption/decryption functions are performed directly in the DTE's or DTEP's Flash memory controller.



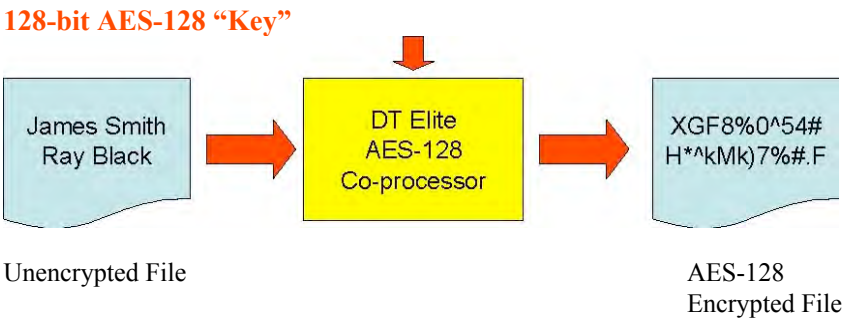
DTE/DTEP Security Architecture

When a DTE or DTEP drive is connected to a host computer, data and file management commands are exchanged between the host computer and the DTE/DTEP Flash memory and USB controller.

With DT Elite drives, when data is written to a public zone, the data is written to the Flash memory storage without any encryption. This data can be read on any host computer or other device. To access the privacy zone, the user is required to use the TravelerSafe+ console and enter a valid password. Once logged in, the host computer will be able to write and read data from the privacy zone. This is illustrated in the chart above.

With DT Elite – Privacy Edition drives, a Login program is automatically launched to allow for the entry of a valid password. Once the password is successfully entered, the data content of the drive is visible and accessible.

When data is written to a privacy zone of either the DT Elite or the DT Elite – Privacy Edition, it is encrypted by the AES Encryption and Decryption Co-Processor in real-time, and then written to the Flash memory storage. Similarly for reads, the data is decrypted real-time on the DT Elite drive and then sent to the host computer.

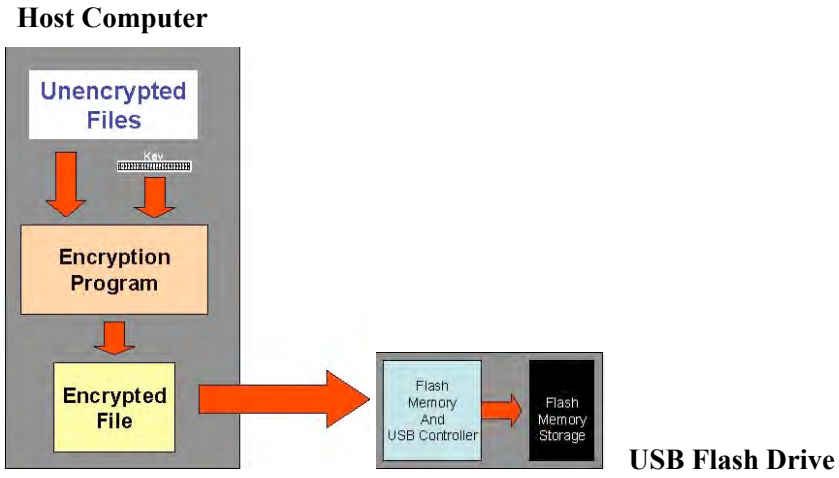


The DT Elite Encryption Process

Without the unique 128-bit key, which is uniquely generated for the DT Elite utilizing a true random number generator, encrypted data is nearly impossible to decode.

3.0 Software-Based Encryption vs. DT Elite's Hardware-Based AES Encryption

3.1 Software-Based Encryption



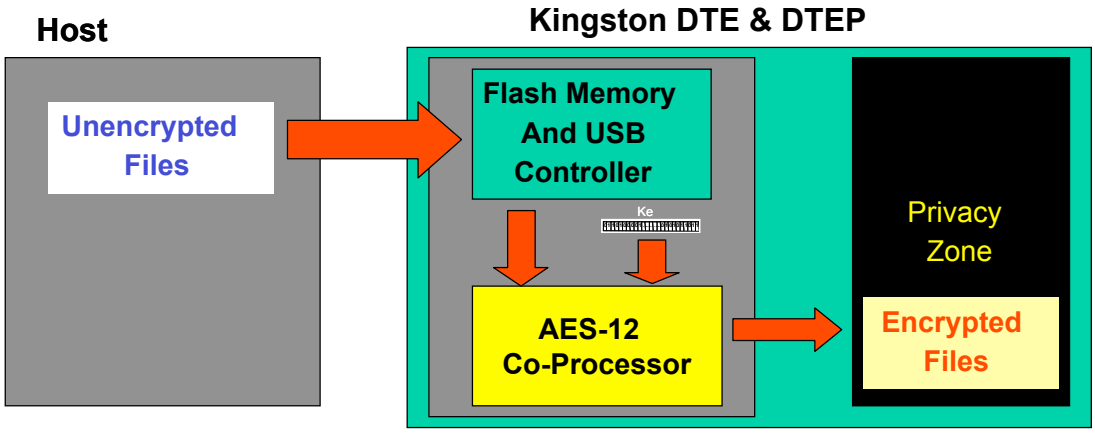
Software-Based Encryption

In this case, the user has to explicitly run a program to encrypt a file. When the file is encrypted, the file can then be copied to the USB Flash drive.

When run on host computers, encryption and decryption programs take up a lot of processor resources and reduce overall system performance.

3.2 DT Elite & DT Elite – Privacy Edition Hardware-Based Encryption

Because the processor-intense AES encryption/decryption is done through a DTE's or DTEP's dedicated co-processor, both drives offer an industry-leading performance level over software encryption programs.



DTE/DTEP drives have Built-in Hardware AES-128 Encryption Co-Processors

In addition, utilizing hardware encryption on both drives does not expose the AES "key" to host computers or networks, further increasing security. The encrypted user password and the key are never shared outside of the DT Elite or DT Elite – Privacy Edition drives. With software-based encryption approaches, the key or keys are exposed to the host computer and network.

As can be seen in the Benchmarking section, there is no performance penalty when storing files on the public and privacy zones in a DT Elite or DT Elite – Privacy Edition (see **section 3.2.3**).

	DT Elite & DT Elite – Privacy Edition with built-in, hardware-based encryption/decryption	**Other USB Drives with Software-based Encryption**
Invalid Password Retry limit	Yes	Rare
Advanced hashing (encoding) of user password to secure it	Yes	Varies
Dedicated AES co-processor on USB drive	Yes	No
Data encrypted/decrypted on host computer	No	Yes
AES key exposed to host computer or network	No	Yes
Performance penalty	No	Yes (40-50% slower)

Benefits of DTE/DTEP Hardware-Based Encryption vs. Software Approaches

4.0 Certifications and Operating System Support:

The Kingston DT Elite and DT Elite — Privacy Edition are certified as Hi-Speed USB 2.0 drives. OS support, especially of encryption features, is shown below:

Operating System	File Transfer	Password Protection/ Data Encryption
Win 2000†, Win XP	Yes	Yes
Mac OS10.x and above	Yes	No
Linux Kernel 2.4 and above	Yes	No
Win NT, Win 95, Win 98, Win98SE, Win ME	Not Supported	Not Supported

† For Windows 2000 users without administrative privileges, USB 2.0 is required.

The DT Elite and DT Elite – Privacy Edition drives also meet the provisions of the Cryptography Note (Note 3) in Category 5, Part 2, of the Commerce Control List (United States Department of Commerce – Bureau of Industry and Security – Encryption regulatory).

5.0 DataTraveler Elite & DataTraveler Elite - Privacy Edition Performance*

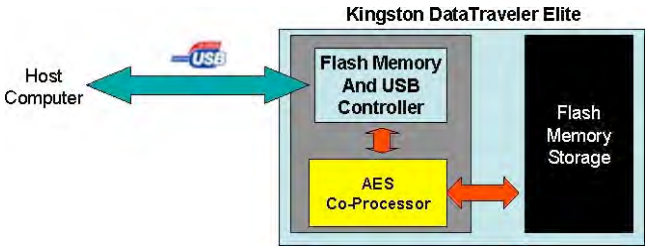
Kingston's DTE and DTEP USB Flash drives are engineered with a state-of-the-art, Hi-Speed USB 2.0 controller that delivers outstanding performance. Even when AES-128 encryption/decryption security is used, their performance is not reduced due to the built-in AES-128 co-processor. DT Elite and DT Elite – Privacy Edition drives makes no performance compromises while delivering an advanced level of security.

	Read Data Transfer Rate (Peak)	Write Data Transfer Rate (Peak)	Public/Privacy Zone Support	Advanced Security
DataTraveler Elite	24 MB/sec.	14 MB/sec.	Yes	Yes (Hardware AES-128)
DataTraveler Elite – Privacy Edition	24 MB/sec.	14 MB/sec.	No – Only Privacy Zone	Yes (Hardware AES-128)
DataTraveler II Plus – Migo Edition	19 MB/sec.	13 MB/sec.	Yes	No
DataTraveler II	11 MB/sec.	7 MB/sec.	Yes	No
DataTraveler	6 MB/sec	3 MB/sec.	No	No

Kingston DataTraveler Transfer Rates and Security Features

*Speed may vary due to host hardware, software and usage.

5.1 Hi-Speed USB 2.0 Interface



The DTE/DTEP Drives Feature a Certified, Hi-Speed USB Interface

Because the USB Hi-Speed standard is a range (for more information, please see Kingston's Flash Memory Guide at kingston.com/Digital_Media_Guide), products can offer different performance levels despite having the same Hi-Speed USB logo. Kingston's DataTraveler USB Flash drives all feature advanced Flash controllers and deliver outstanding performance.

The DT Elite and DT Elite – Privacy Edition drives offer data transfer rates of up to 24 MB/sec. read and 14 MB/sec. write (Speed may vary due to host hardware, software and usage.) Even with encryption, their performance levels are not significantly impacted due to the real-time, hardware-based encryption/decryption technology built into the drives.

5.2 "Common User" Benchmarks

The following benchmarks were conducted on an Intel D875PBZ motherboard (Intel 875P chipset, 2.4-GHz Pentium® 4 processor, Windows XP Pro + Support Pack 1 installed, 1-GB Kingston HyperX PC3200 memory, and 7200-RPM hard drive). All DataTraveler Flash drives were in new condition and were formatted as FAT32. The benchmark's goal was to measure performance based on typical user scenarios — transferring different kinds and sizes of files from a computer to the DataTraveler Flash drives (utilizing public zones in the DT II, DT II Plus – Migo Edition, and DT Elite Flash drives, and the privacy zone in the DT Elite – Privacy Edition), reading them back, and then deleting the files. The stopwatch approach was used to measure the elapsed time, which was rounded to the closest second.

Note: These benchmarks should be used only as a guide to performance. Many factors, such as the performance level and configuration of the host computer hardware, the Operating System of the host computer and how it's configured, the USB connection speed, and the actual number of files and their sizes may affect benchmark results. In addition, ongoing product improvements may also improve DataTraveler performance.

The DataTraveler drives tested are abbreviated as:

DT	= DataTraveler
DT II	= DataTraveler II
DT II Plus – Migo Edition	= DataTraveler II Plus – Migo Edition
DT Elite	= DataTraveler Elite & DataTraveler Elite – Privacy Edition

DT Elite – Privacy Edition drives offer the same performance as DT Elite drives, with the main difference being that DTEP drives feature a 100% privacy zone for maximum security. The results are combined in the tables below under "DT Elite."

5.2.1 Large Directory/Large Number of Files Benchmarks

The following three benchmarks utilize large-sized directories with many files to show the performance scalability of DataTraveler Flash drives.

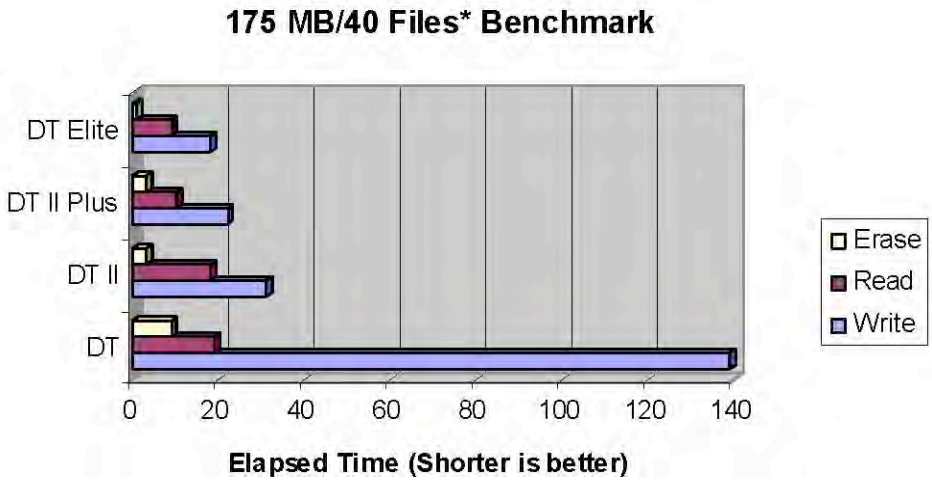
5.2.1.1 175-MB/ 40 Files Benchmark

A 175-MB directory containing 40 files was written to, read from, and erased from the DataTravelers:

175-MB, 40 Files Benchmark

Benchmark	Write	Read	Erase
DT	139	19	9
DT II	31	18	3
DT II Plus	22	10	3
DT Elite	18	9	1

Elapsed time (measured in seconds)



* Files used are PowerPoint files varying in size from 15 KB to almost 21 MB.

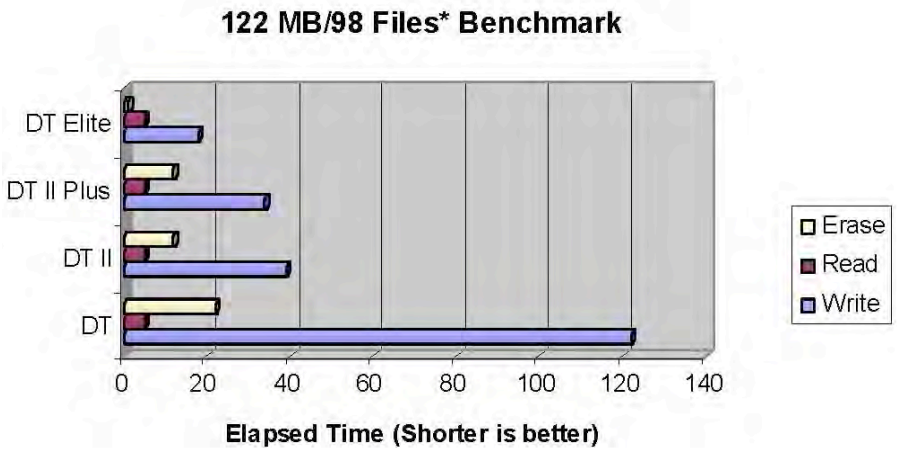
5.2.1.2 122-MB/98 Files Benchmark

In this benchmark, a 122-MB directory containing 98 files was written to, read from, and erased from the DataTravelers:

122-MB, 98 Files Benchmark

Benchmark	Write	Read	Erase
DT	122	5	22
DT II	39	5	12
DT II Plus	34	5	12
DT Elite	18	5	1

Elapsed time (measured in seconds)



* Files used are JPEG picture files from a 3.3 mega pixel digital camera. File sizes vary from 475 KB to 2.6 MB.

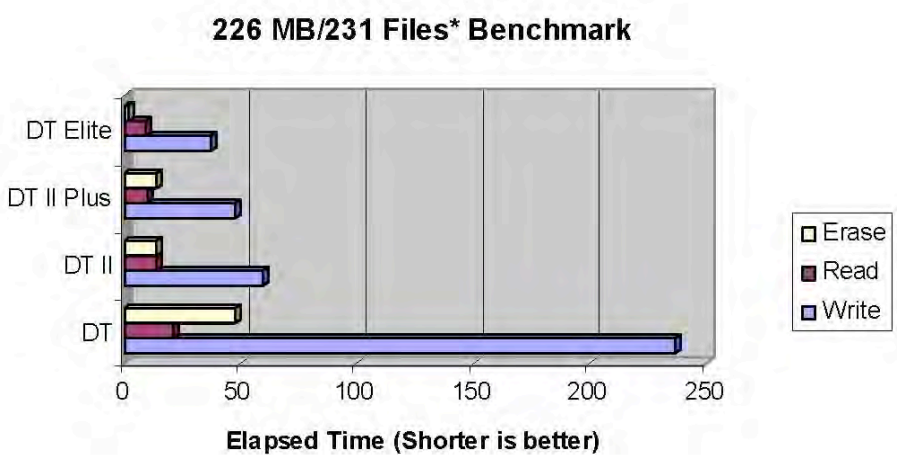
5.2.1.3 226-MB/231 Files Benchmark

In this benchmark, a 226-MB directory containing 231 files was written to, read from, and erased from the DataTravelers:

226-MB, 231 Files Benchmark

Benchmark	Write	Read	Erase
DT	237	21	48
DT II	60	14	14
DT II Plus	48	10	14
DT Elite	37	9	2

Elapsed time (measured in seconds)



* Files used are JPEG picture files from a 3.3 mega pixel digital camera. File sizes vary from 475 KB to 2.6 MB.

For this benchmark, a single 116-MB file was written to, read from, and erased from the DataTravelers:

116-MB File Benchmark

Benchmark	Write	Read	Erase
DT	74	17	1
DT II	17	10	1
DT II Plus	11	7	1
DT Elite	11	4	1

Elapsed time (measured in seconds)

* File used is a 116-MB audio/video VOB file.

5.3 DTE/DTEP Encryption/Decryption Performance Benchmark

The175-MB/ 40-files benchmark was used to test the DT Elite/DT Elite – Privacy Edition's AES-128 encryption/decryption performance.

AES-128 Benchmark	Write	Read	Erase
DTE: Public Zone (no encryption)	18	7	1
DTE/DTEP: Privacy Zone (with AES-128 encryption)	18	7	1

As expected, there are *absolutely* no performance compromises resulting from the DT Elite's hardware-based AES-128 encryption/decryption. DT Elite – Privacy Edition

drives perform identically as DT Elite drives; the only difference is that the DTEP features a 100 percent privacy zone (no public zone).

6.0 Conclusion

Kingston's DataTraveler Elite and DataTraveler Elite – Privacy Edition drives are state-of-the-art, advanced security, high-performance Flash drives. They are ideally suited for business organizations as well as advanced consumers seeking the advanced security of hardware AES encryption and high-performance USB 2.0 interface.

Printed in the USA MKF-747.1