



# Diskeeper® and Disk Encryption

## OVERVIEW

In the early 1990s, Diskeeper Corporation (a Microsoft® Gold Partner) and Microsoft co-wrote Windows® kernel-level code, and exposed an API (Application Programming Interfaces), prior to release of NT4 for third party software providers. This “MoveFile” API as it is called, has allowed defragmentation programs to operate as user-mode applications ever since, through Windows Server™ 2008, Windows 7, etc... The benefit of having integrated defrag-based file movement in Windows is that all file movement in an online defragmentation operation by a product, such as Diskeeper, is entirely handled by the operating system. A defragmenter, such as Diskeeper, is from this viewpoint, logic that instructs the file system, via that API, to put file fragments that it discovers back together again into an available and contiguous free space on a given Windows volume. The process has been 100% safe for data since introduction in NT4.

More recently, the NTFS file system added and fully supports disk/file encryption as evidenced by EFS (Encrypting File System), and Microsoft products such as Windows Bit Locker.

It is fairly well known that Windows also ships with a native defragmenter (a product initially provided by Diskeeper for the Windows 2000 platform). It then stands to reason that Microsoft has a vested interest in maintaining continuing compatibility with defragmentation and, minimally, their own drive/file encryption solutions, and this is certainly the case.

Over the years our vast install base (10 million+) has brought to our attention rare and temporary incompatibilities that other products have had with the Microsoft MoveFile API.

Disk Encryption is becoming an increasingly more popular security measure undertaken in corporate enterprise—and even home use. Limitations in Windows provided tools may drive IT professionals to seek out advanced third party disk encryption solutions (much as they do with disk defragmentation). In past years, as this technology grew from infancy in the Windows arena, a few disk encryption applications had temporary issues with the MoveFile API.

In every case to date, where it has ever even been an issue, *the manufacturer of that encryption software program has recognized this issue and corrected it*, or offered workarounds. Those workarounds may require specific functionality in a third party defragmenter such as Diskeeper’s *File Exclusion feature*, as the native defragmenter that ships with Windows lacks this. In those cases, depending on the technology implemented by the encryption software vendor, a specific file (called a boot loader file) should not be moved.

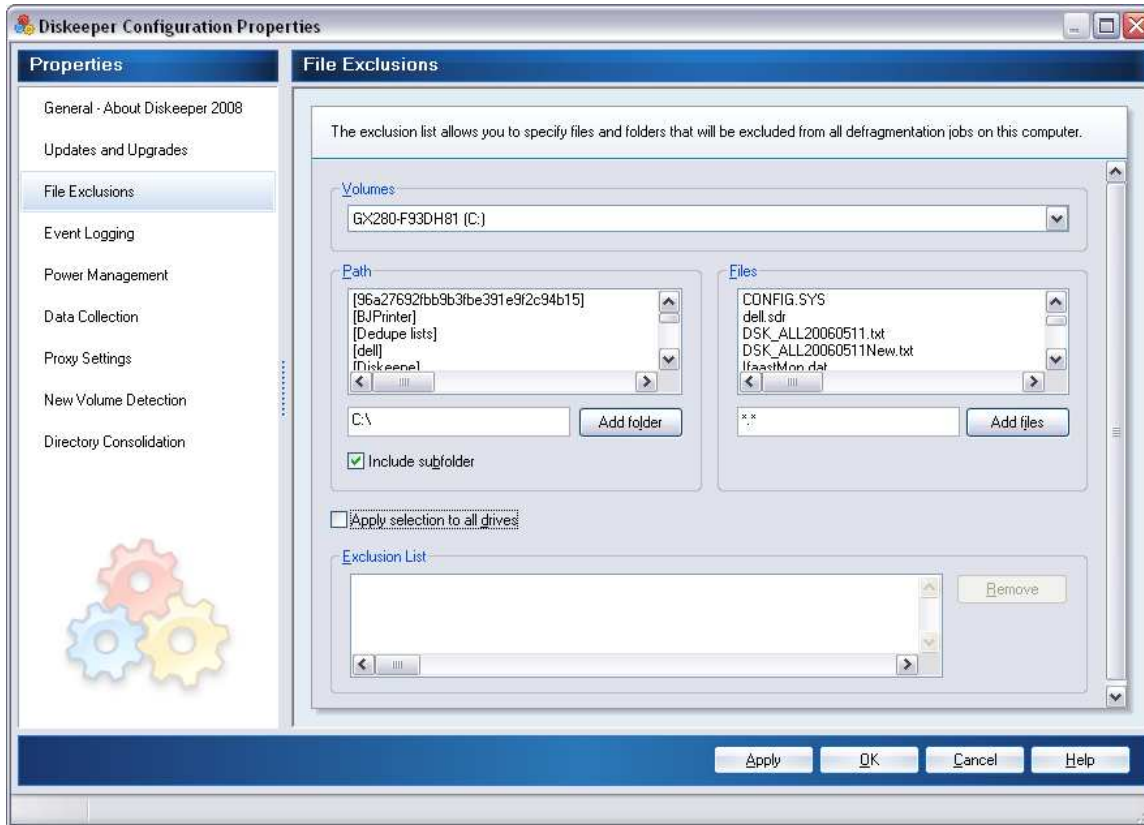


Figure 1.0: Diskeeper's File Exclusion feature used to exclude a file

In fact, with Diskeeper's technology and market leadership, we have worked closely with engineers and support staff from encryption manufactures to ensure their products work perfectly for our common customers. To ensure that Diskeeper is both compatible with file/disk encryption programs and provides a performance benefit, a series of tests were performed.

## METHODOLOGY

### Test Hardware:

|  |   |
|--|---|
| Motherboard: <b>Intel® Desktop Board D945GTP</b> | CPU: <b>Intel Pentium® 4 3.00GHz Processor</b>  |
| Memory: <b>2.00GB DIMM</b>                       | Storage Configuration<br><b>C: ST3250620AS 250GB SATA Drive</b><br><b>D: ST3750640AS 750GB SATA Drive</b> |
| Video: <b>nVidia® GeForce® 7Series 7600GS</b>    |   |

### Test Software:

Operating System: Microsoft Windows Vista® Ultimate SP1  
 Benchmarking Application: PCMark® Vantage  
 Defragmenter: Diskeeper Pro Premier (build 781)  
 Volume Imaging Application: Norton Ghost™  
 File Encryption Programs: EFS, Windows BitLocker™, PGP®  
 Programs to Verify File Integrity: chkdsk, Word, Excel®  
 Diskeeper Corporation "file fragmenter" utility

### Test Procedure:

Two separate baseline environments (test cases) were created to depict varying degrees of fragmentation. A Diskeeper Corporation fragmentation utility was used to create fragmented files (documents, spreadsheets) and folders.

In Test Case 1 (TC1), a very lightly fragmented environment, a 200GB test volume was created on the system volume. The fragmentation / file numbers on the volume were as follows:

- ~50,000 files
  - ~1,300 fragmented files -> ~6000 fragments
- ~10,000 directories
- ~90% free space
- 3 MFT fragments
- 1 Paging file fragment

The volume was then imaged using Norton Ghost for reuse throughout the comparison.

In Test Case 2 (TC2), a heavily fragmented environment, which is also low on available free space, was then created on the same 200GB system volume. The fragmentation / file numbers on this volume were as follows:

- ~100,000 files
  - ~60,000 fragmented files -> ~ 275,000 fragments
- ~10,000 directories
- ~4% free space
- 5 MFT fragments
- 4 Paging file fragments

The volume was then imaged using Norton Ghost for reuse throughout the comparison.

Between all tests, the volume was restored from backup (located on a second physical volume - *ST3750640AS 750GB SATA Drive*) using Norton Ghost, and the system rebooted to flush memory usage. PCMark Vantage was targeted to the system/test volume (*ST3250620AS 250GB SATA Drive*). For the PCMark Vantage benchmark tests, the Hard Disk suite was run to provide the Hard Drive-specific score.

The test volume was encrypted using one of the disk encryption programs, and then benchmarked with PCMark Vantage. Diskeeper then defragmented the volume. After defragmentation completed, chkdsk was used in conjunction with manual investigation of the files to verify continued 100% data access/integrity. It was also verified that the files remained encrypted. The PCMark benchmark was then rerun for a post-defragmentation comparison.

In between each test/test run for the various encryption programs, the volume was restored to repeat the process from the same starting environment.

An additional test was performed that ran encryption with Diskeeper running concurrently to successfully demonstrate simultaneous operating compatibility.

# BENCHMARK TEST RESULTS

## Test Case 1 - Light Fragmentation:

The results of the PCMark Vantage benchmark comparison in the high available free space / low fragmentation environment are in the graphs below:

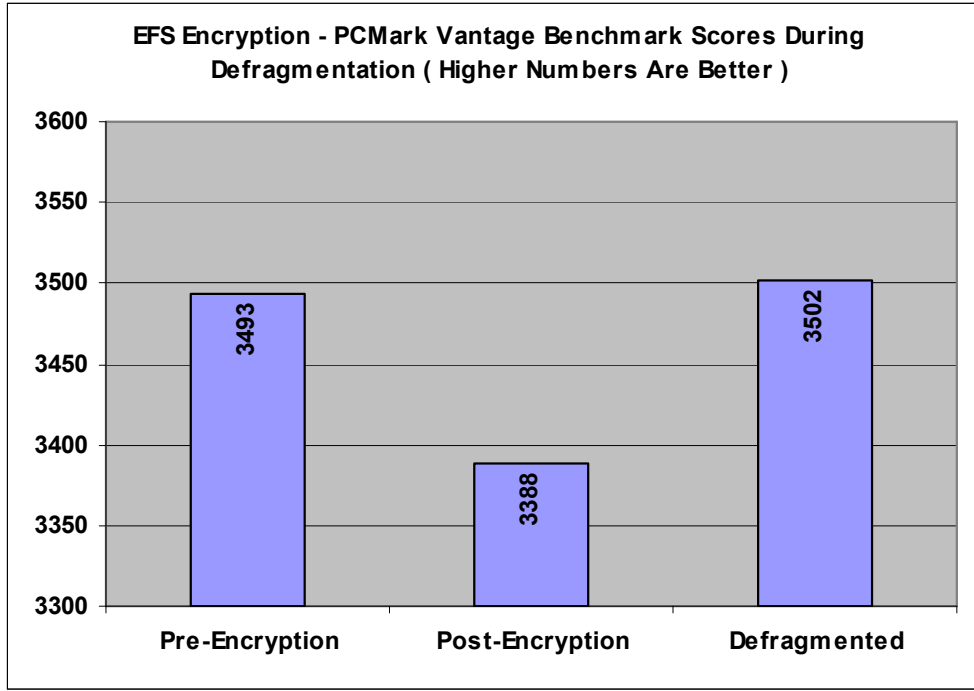


Figure 2.0: EFS Encryption scores (TC1)

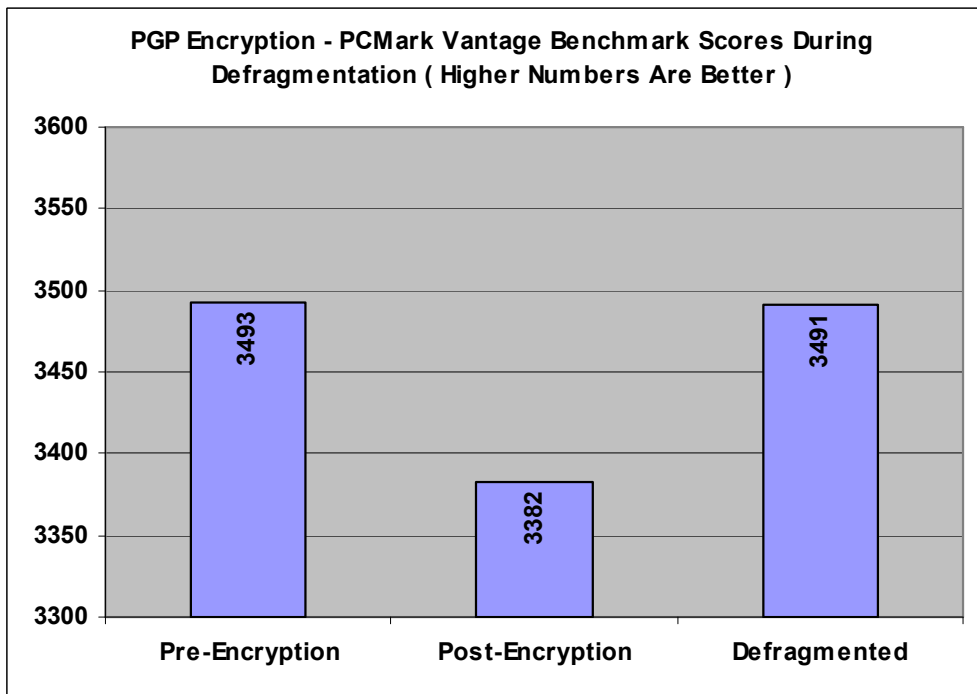


Figure 2.1: PGP Encryption scores (TC1)

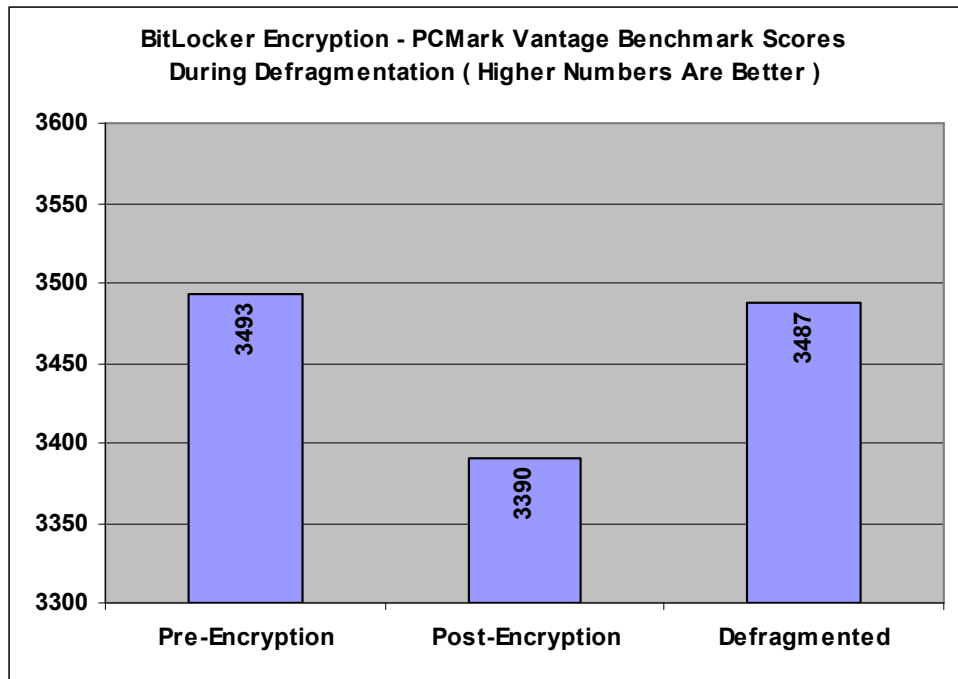


Figure 2.2: Bitlocker Encryption scores (TC1)

Test Case 2 - Heavy Fragmentation:

The results of the PCMark Vantage benchmark comparison in the low free space / high fragmentation environment are in the graphs below:

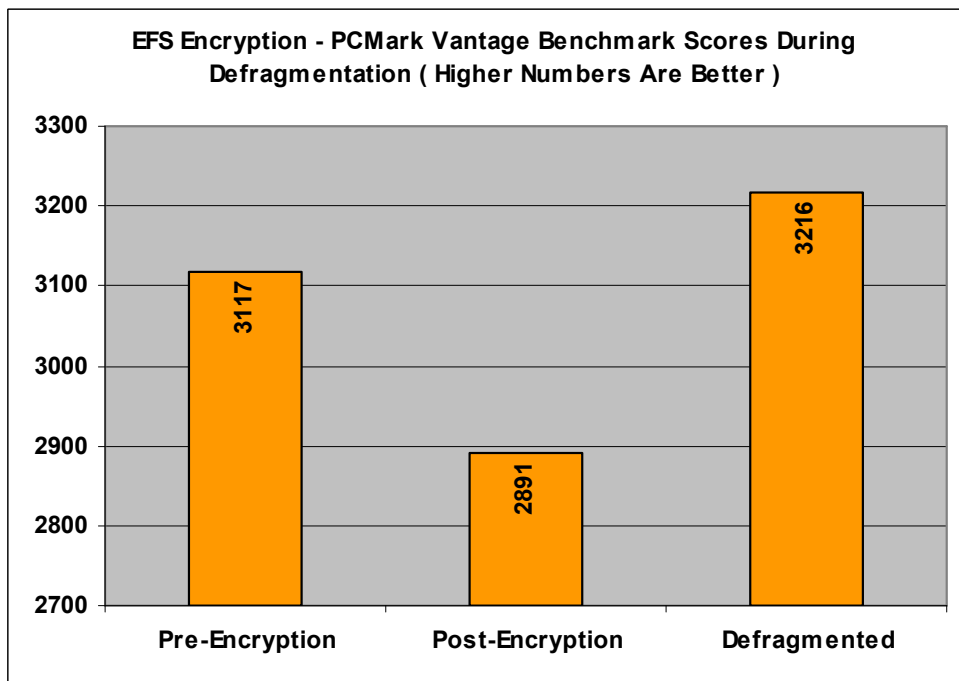


Figure 3.0: EFS Encryption scores (TC2)

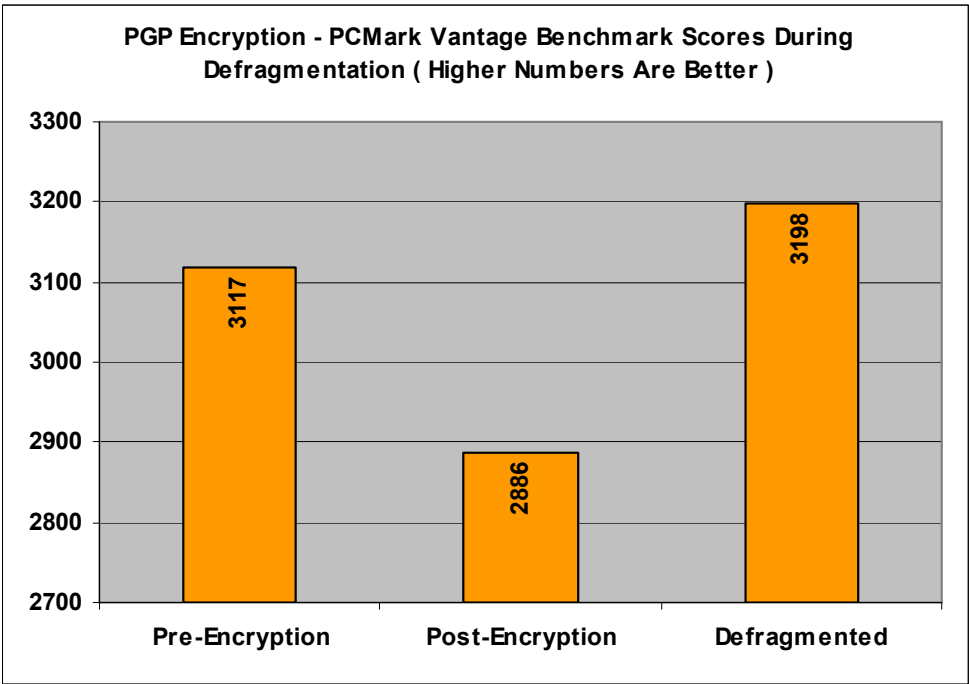


Figure 3.1: PGP Encryption scores (TC2)

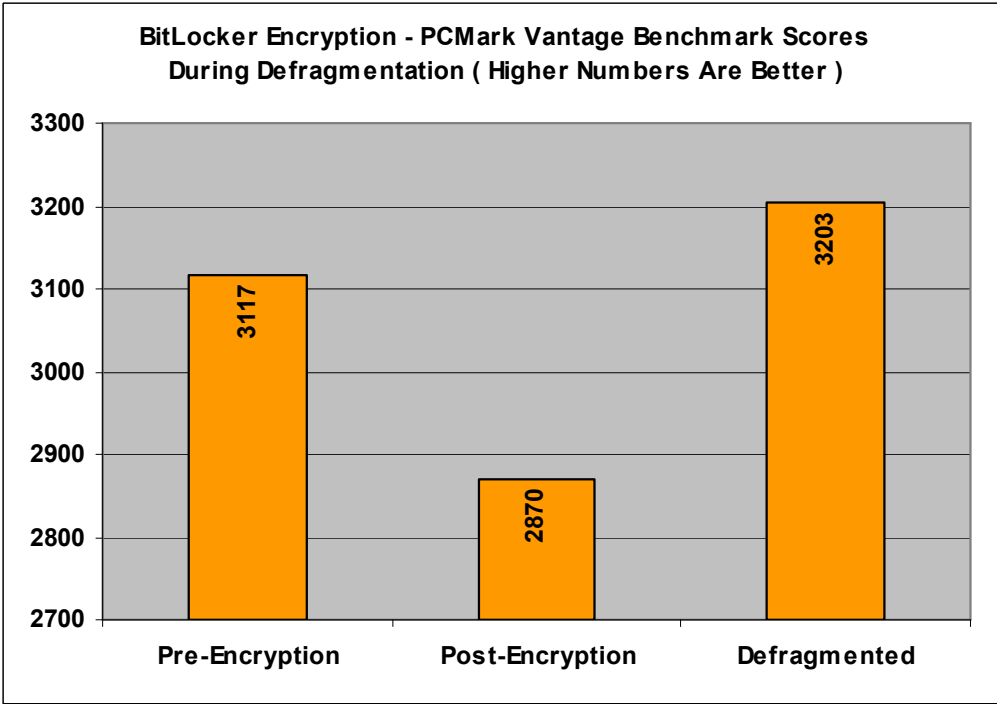


Figure 3.2: Bitlocker Encryption scores (TC2)

## **CONCLUSION**

Testing verified that file defragmentation does not alter encrypted data in any manner. The verification process included post-defragmentation data integrity analysis using chkdsk and manual investigation, by opening encrypted files to ensure full access to the data.

The second component of the tests, measuring performance, clearly demonstrates that disk encryption reduces the benchmark scores of a volume and that disk defragmentation can restore this lost performance. Tests showed that encryption alone reduces file performance from 3% to over 10%. Using Diskeeper improved benchmark scores in every single case, proving that not only is defragmentation technically possible in an encrypted environment, but that it increases performance. This held true in an extreme fragmentation environment with the whole disk encrypted. Using a PC benchmarking utility, average gains of defragmenting an encrypted volume showed over a 10% improvement.

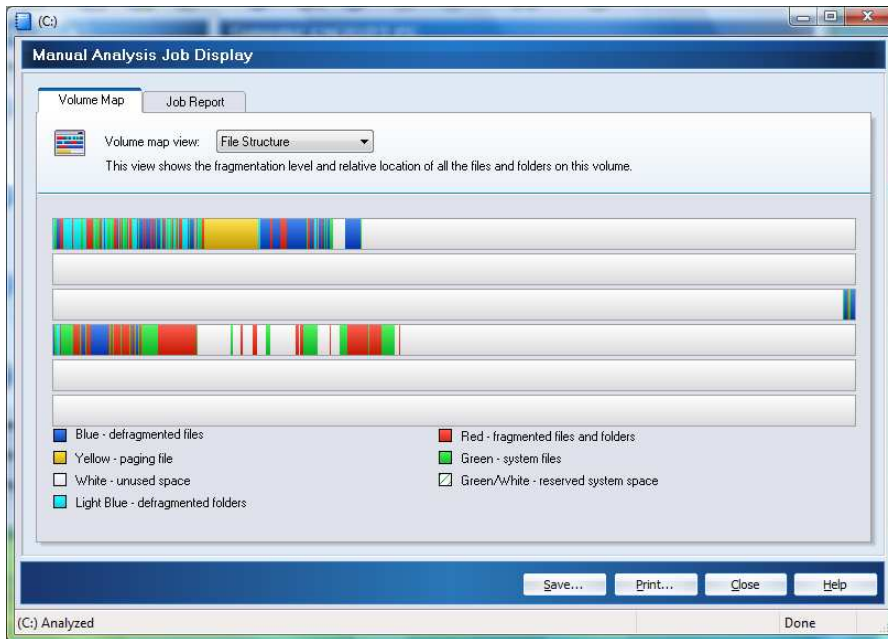
## **RECOMMENDATIONS**

For any current or future Diskeeper Corporation customers looking to employ a disk encryption program, we recommend checking the Encryption ISVs (Independent Software Vendors) Knowledge Base, Help files, or directly contacting the support staff to determine if any special measures are necessary. Based on our experience we also recommend choosing a mature and established vendor in this arena—sound advice for any company looking to deploy a large volume of licenses of any application. As always, you should make sure you are using the most recent version for any encryption solution, such as Guardian Edge EPHD 7.2, Utimaco (SafeGuard Easy) 4.20.x – 4.40.2 with their hotfix SGEflt.sys, or PointSec 6.3.1.

In summary, there are no known issues with using, even simultaneously, disk encryption software and Diskeeper's disk defragmentation software. Combined, your users will have a secure and optimized computing experience.

# APPENDIX

## Test Case 1 – Volume Analysis: Light Fragmentation Environment



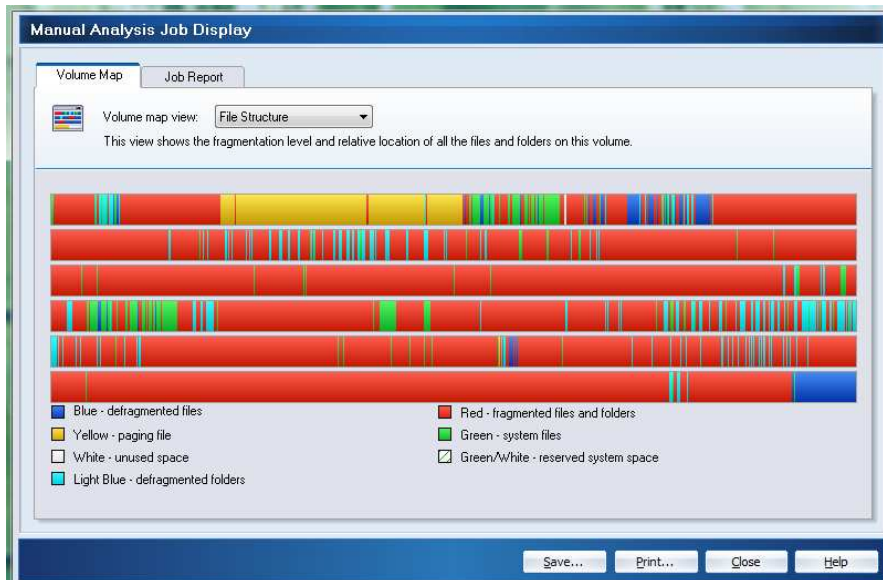
Following is the analysis report taken with the above volume image:

### Statistics

---

|                                       |             |
|---------------------------------------|-------------|
| Volume Files                          |             |
| Volume size                           | = 200 GB    |
| Cluster size                          | = 4 KB      |
| Used space                            | = 21,552 MB |
| Free space                            | = 178 GB    |
| Percent free space                    | = 89 %      |
| Fragmentation percentage              |             |
| Volume fragmentation                  | = 11 %      |
| Data fragmentation                    | = 57 %      |
| Directory fragmentation               |             |
| Total directories                     | = 10,053    |
| Fragmented directories                | = 31        |
| Excess directory fragments            | = 92        |
| File fragmentation                    |             |
| Total files                           | = 47,870    |
| Average file size                     | = 455 KB    |
| Total fragmented files                | = 1,279     |
| Total excess fragments                | = 6,157     |
| Average fragments per file            | = 1.12      |
| Files with performance loss           | = 0         |
| Paging file fragmentation             |             |
| Paging/Swap file size                 | = 2,345 MB  |
| Total fragments                       | = 1         |
| Master File Table (MFT) fragmentation |             |
| Total MFT size                        | = 84,928 KB |
| MFT records In Use                    | = 57,948    |
| Percent MFT in use                    | = 68 %      |
| Total MFT fragments                   | = 3         |

## Test Case 2 – Volume Analysis: Heavy Fragmentation Environment



Following is the analysis report taken with the above volume image:

### Statistics

---

#### Volume Files

Volume size = 200 GB  
Cluster size = 4 KB  
Used space = 192 GB  
Free space = 8,192 MB  
Percent free space = 4 %

#### Fragmentation percentage

Volume fragmentation = 90 %  
Data fragmentation = 93 %

#### Directory fragmentation

Total directories = 9,825  
Fragmented directories = 35  
Excess directory fragments = 423

#### File fragmentation

Total files = 104,707  
Average file size = 1,204 KB  
Total fragmented files = 57,710  
Total excess fragments = 274,336  
Average fragments per file = 3.77  
Files with performance loss = 0

#### Paging file fragmentation

Paging/Swap file size = 2,345 MB  
Total fragments = 4

#### Master File Table (MFT) fragmentation

Total MFT size = 117 MB  
MFT records In Use = 114,823  
Percent MFT in use = 95 %  
Total MFT fragments = 5