Enhancing Desktop and Laptop Security Performance with Disk Defragmentation

OVERVIEW

There are numerous well documented improvements to system performance and reliability when an automated disk defragmentation program is used. Applications load faster, the computer boots to a useable state in less time, backup requires less time to transfer data to an archival storage devices, and many more. This paper pursues a narrowed focus, specifically addressing the tangible benefit that disk defragmentation provides to desktop and laptop client security.

Anti-malware security software has become ubiquitous commodity. Whether used on servers, desktops or laptops, the scanning of files on demand or as a scheduled process, is a significant part of the overall business security equation. This particular research paper will present the results of testing performed on typical desktop/laptop environments.

As a core function, malicious software detection-and-removal applications scan files (including the Windows Registry) for known malware or malware patterns. The general principle is that disk fragmentation will increase the time required to scan for and remove these malicious files. This paper presents data from detailed investigations into the performance improvement in anti-malware scan times when advanced disk defragmentation is applied.

The approach of this report is to display the improvement in antivirus and anti-spyware utility scan times (speed) before and after defragmentation using Diskeeper 2007. Additional measurements were taken *during* the defragmentation process (i.e. before defragmentation had completed) to note immediate returns on scan time improvement.

METHODOLOGY

Software

Defragmentation:
- Diskeeper 2007 Pro Premier (11.0.711)

Antivirus:
- Symantec Norton Antivirus 2007
- Trend Micro Client / Server Edition v7.3
- McAfee Active Virus Scan
- Panda Antivirus 2007

Anti-Spyware
- Ad-Aware SE Personal Edition
- Trend Micro Anti-Spyware for Enterprise[1]
- McAfee Anti-Spyware Enterprise SA 8.5sa

Operating Systems
- *Windows XP Professional with Service Pack (SP) 2*
- *Windows Vista Ultimate*

Hardware

Motherboard: *Intel Desktop Board D945GTP*
CPU: *Intel Pentium 4 3.00GHz Processor with Hyper Threading*
Memory: *1.00GB DIMM in memory slot 1*
Video: *MSI NX7600GS 256MB DDR2*
Storage: *ST380815AS 80GB SATA Drive*
Drive Configuration: *System Volume - C: 80.00GB*

[1] In Windows Vista, Trend Micro Antivirus & Anti-Spyware 2007 was used rather than Trend Micro Anti-Spyware for Enterprise. This was done due to a lack of Vista support for Trend Micro Anti-Spyware for Enterprise at the time of these tests.

Procedure

Purpose: mimic real-world environments

An 80GB SATA drive was fully formatted and installed with Windows XP Professional SP2 with all current Windows updates. Then a battery of software installations were run in order to create an environment which might closely resemble an average user's workstation with *mild* fragmentation. Software products installed included free and trial software from Download.com Top 100 Most Popular list. A standard user's My Documents directory was also filled with an array of different file types which might typically be found there, and the contents fragmented to resemble a My Documents directory on a workstation that has been in use. Finally, Diskeeper 2007 was installed with automatic defragmentation disabled, and the volume backed up to an image. This image was used for all trials in XP Pro SP 2 *pre-defragmentation*.

For each trial, the image was restored, and the antivirus / anti-spyware software currently being run was installed. All auxiliary resource usage in the software was disabled in the available options of the program (automatic scanning, automatic updates, etc) after installation, and the test machine rebooted. One dry run of the scanning software was performed but excluded from timing, as some scanning software builds a file on the scanned drive on their initial run. After reboot, the scan was run and programmatically timed. The machine was then rebooted and scan re-run an additional four times, to achieve the total of five trials (essentially six if the excluded 'dry' run is considered).

Once the above pre-defragmentation trials were completed in Windows XP Professional SP2, the image was restored once more, and Diskeeper 2007's Automatic defragmentation and boot-time defragmentation features were used in order to defragment the volume. Automatic defragmentation was then disabled once more, and the drive newly imaged as a defragmented version.

Then the methodology referenced above was utilized in order to perform timed scan trials with the same software used previously.

Once all trials in Windows XP Pro were complete, the original pre-defragmentation image was restored once more. The OS was then upgraded to Windows Vista Ultimate[2], a number of fragmented files removed (to reduce the fragmentation level) and a new image of a pre-defrag Vista environment was created. The above trial methodology for pre-defrag Windows Vista was then repeated, in this new environment.

Finally, the image was restored once more after the pre-defrag Vista trials were done, and Diskeeper 2007 utilized in order to defragment the volume. After the drive was imaged, the same post-defrag Windows XP Professional trial methodology was used for Windows Vista.

The utilities were all run a total of five times for each test case, with the highest and lowest result from each five-run set removed for purposes of establishing a more accurate median for averaging[3].

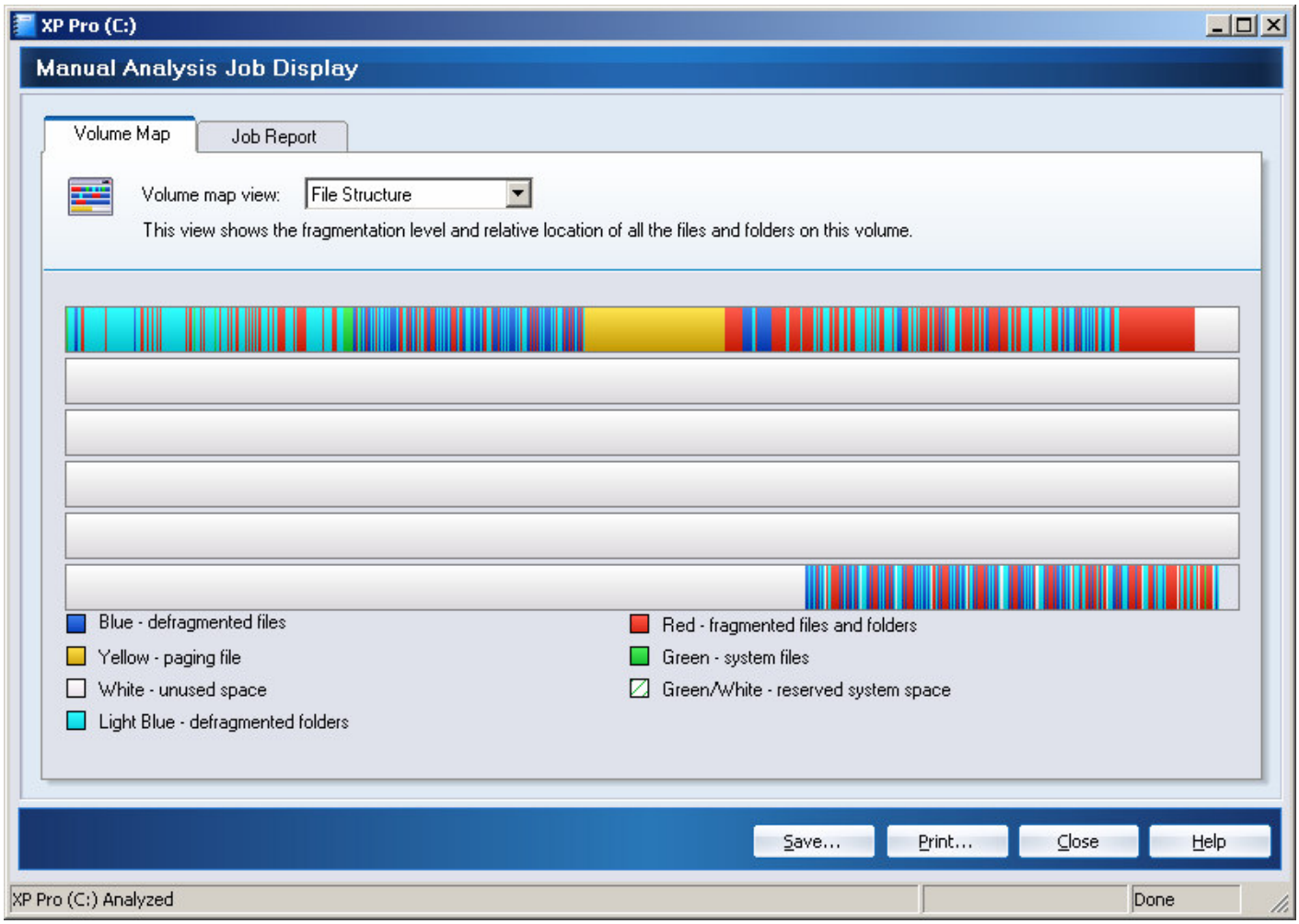
[2] An upgrade to Windows Vista was performed as many of the programs installed to generate real-world fragmentation did not natively support installation onto the Vista operating system, but they did support Windows XP.

[3] The tests performed in this experiment are insufficient to attain a proper judgment of the value of an anti-malware product. All scans executed in these tests were done using standard configurations and are not a comparison of speed of one product versus another. Also note that thoroughness of a scan between products was not evaluated as it is irrelevant for the purposes of this test.

TEST RESULTS

WINDOWS XP PROFESSIONAL TEST

Screen capture of XP Pro prior to defragmentation



Windows XP Volume Statistics – Prior to Defragmentation

Volume Files

Volume size	= 76,317 MB
Cluster size	= 4 KB
Used space	= 16,065 MB
Free space	= 60,253 MB
Percent free space	= 78 %

Fragmentation percentage

Volume fragmentation	= 7 %
Data fragmentation	= 33 %

Directory fragmentation

Total directories	= 5,844
Fragmented directories	= 259
Excess directory fragments	= 1,586

File fragmentation

Total files	= 47,680
Average file size	= 355 KB
Total fragmented files	= 8,196
Total excess fragments	= 47,841
Average fragments per file	= 2.00
Files with performance loss	= 0

Paging file fragmentation

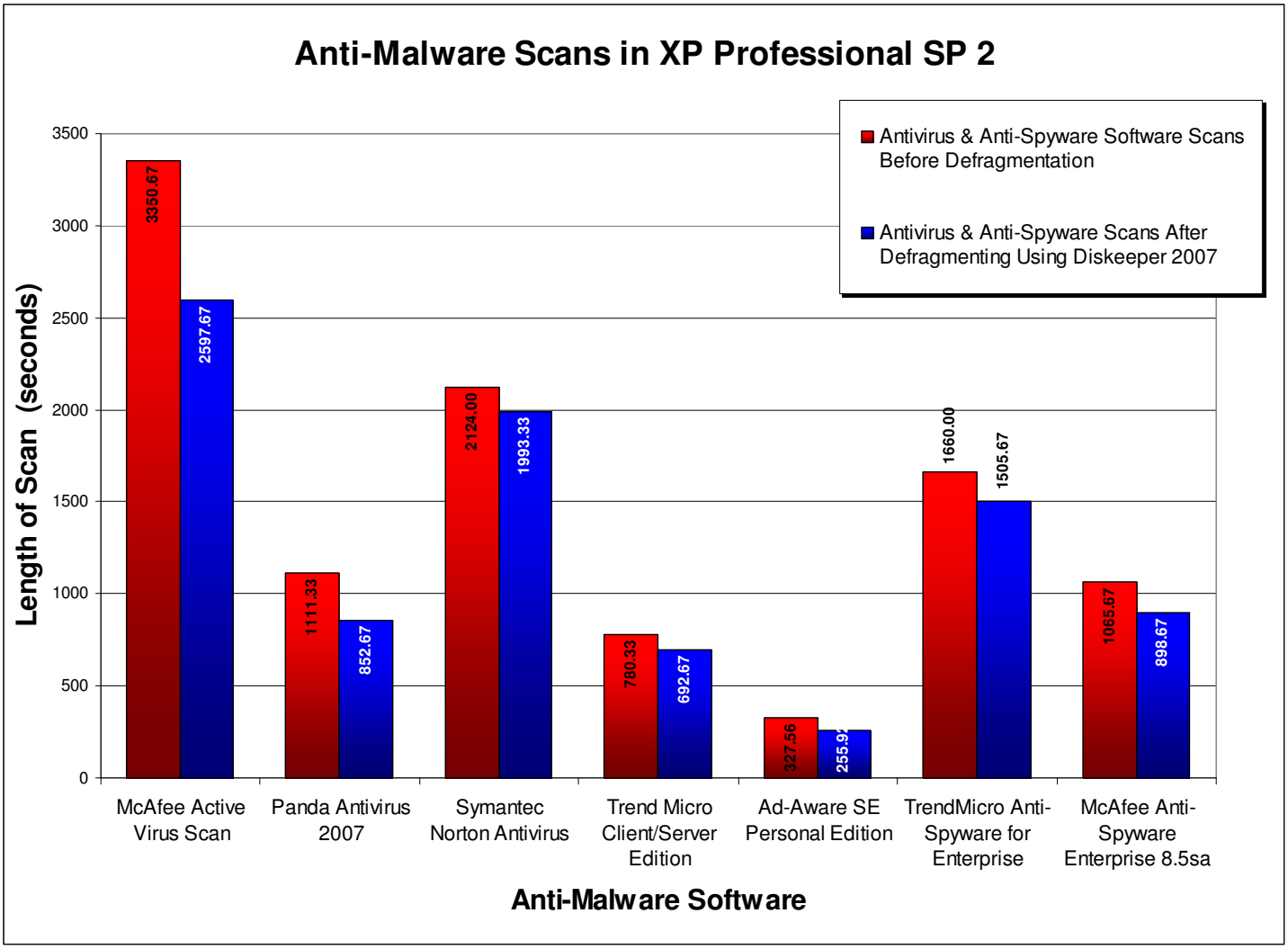
Paging/Swap file size	= 1,524 MB
Total fragments	= 1

Master File Table (MFT) fragmentation

Total MFT size	= 57,008 KB
MFT records In Use	= 53,635
Percent MFT in use	= 94 %
Total MFT fragments	= 16

Graphed Summary Results

In the presented graphs, the numbers are averages based on the median 3 values of the 5 gathered from each trial, in order to produce a more accurate average. (All of the individual results can be found under **Test Results** below)



Detailed Results

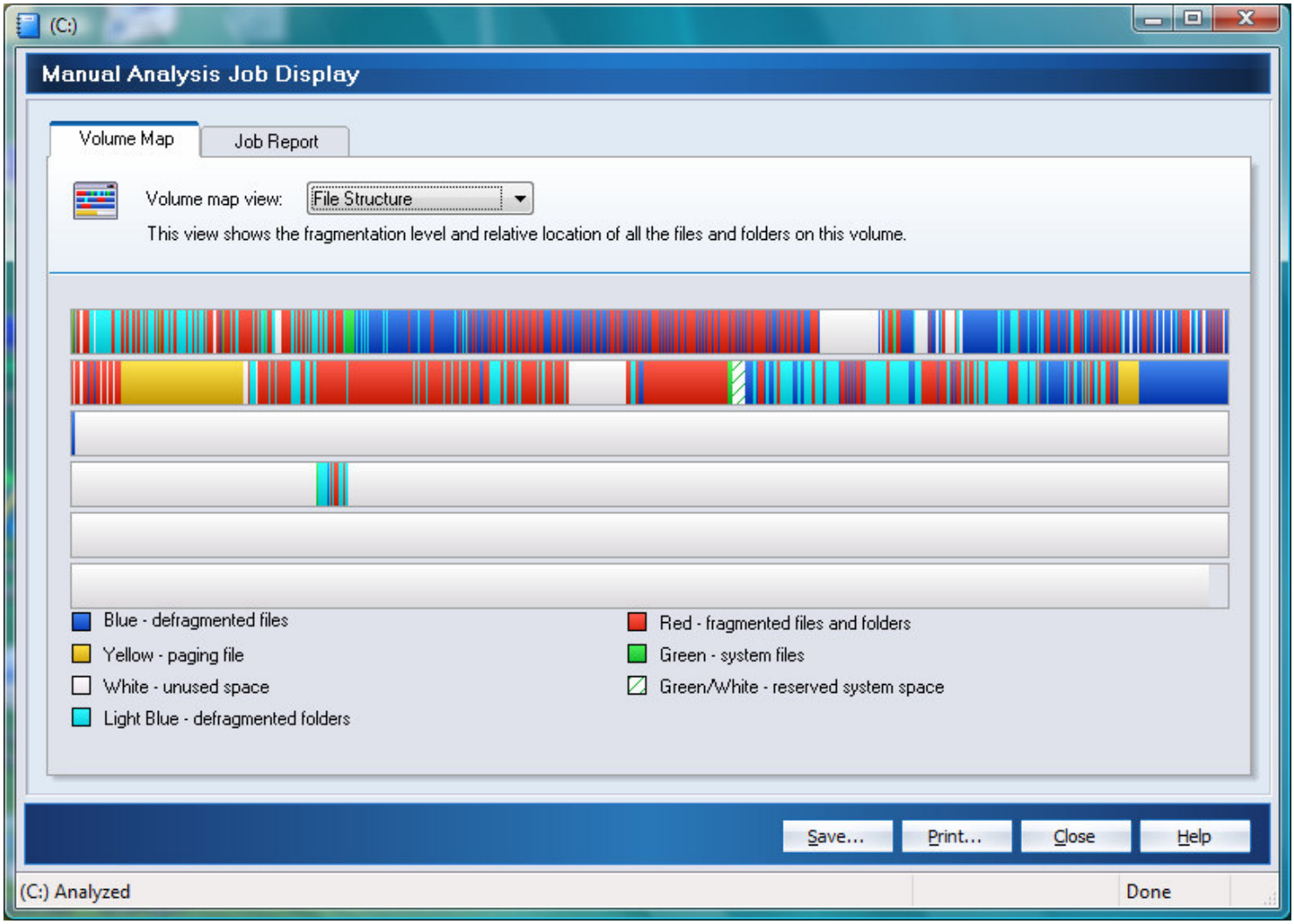
Windows XP Pro SP 2

Antivirus	Scan Times (Seconds)						Improvement After Defragmentation
	1	2	3	4	5	Avg.	
McAfee Active Virus Scan							
Before Defragmenting	3357.00	~~3331.00~~	3344.00	~~3366.00~~	3351.00	3350.67	22.47%
During Defragmentation	3483.00	~~3506.00~~	3012.00	~~2964.00~~	2990.00	3161.67	
After Defragmenting	2595.00	~~2343.00~~	2597.00	2601.00	~~2612.00~~	2597.67	
Panda Antivirus 2007							
Before Defragmenting	1116.00	1108.00	~~1083.00~~	~~1117.00~~	1110.00	1111.33	23.28%
During Defragmentation	~~1120.00~~	1117.00	1101.00	1102.00	~~1100.00~~	1106.67	
After Defragmenting	858.00	843.00	857.00	~~881.00~~	~~828.00~~	852.67	
Symantec Norton Antivirus							
Before Defragmenting	2090.00	2089.00	~~2072.00~~	~~2193.00~~	2105.00	2124.00	6.15%
During Defragmentation	1993.00	~~1990.00~~	1995.00	1988.00	~~2002.00~~	1992.00	
After Defragmenting	~~2002.00~~	1994.00	~~1990.00~~	1990.00	1996.00	1993.33	
Trend Micro Client/Server Edition							
Before Defragmenting	780.00	~~783.00~~	~~780.00~~	781.00	780.00	780.33	11.23%
During Defragmentation	692.00	~~681.00~~	695.00	699.00	~~702.00~~	695.33	
After Defragmenting	~~700.00~~	690.00	698.00	690.00	~~686.00~~	692.67	

Anti-Spyware	Scan Times (Seconds)						Improvement After Defragmentation
	1	2	3	4	5	Avg.	
Ad-Aware SE Personal Edition							
Before Defragmenting	332.20	327.83	~~317.39~~	322.66	~~335.96~~	327.56	21.87%
During Defragmentation	~~262.14~~	270.39	272.72	~~272.90~~	271.27	271.46	
After Defragmenting	255.74	~~261.55~~	258.33	253.69	~~241.01~~	255.92	
Trend Micro Anti-Spyware for Enterprise							
Before Defragmenting	1668.00	1661.00	~~1624.00~~	1651.00	~~1672.00~~	1660.00	9.30%
During Defragmentation	~~1522.00~~	~~1541.00~~	1526.00	1524.00	1534.00	1528.00	
After Defragmenting	1500.00	~~1518.00~~	1506.00	~~1498.00~~	1511.00	1505.67	
McAfee Anti-Spyware Enterprise 8.5sa							
Before Defragmenting	1061.00	1065.00	~~946.00~~	~~1076.00~~	1071.00	1065.67	15.67%
During Defragmentation	899.00	902.00	906.00	~~881.00~~	~~912.00~~	902.33	
After Defragmenting	897.00	899.00	~~892.00~~	~~906.00~~	900.00	898.67	

WINDOWS VISTA ULTIMATE TEST

Screen capture of Windows Vista prior to defragmentation



Windows Vista Volume Statistics – Prior to Defragmentation

Volume Files

Volume size	= 76,317 MB
Cluster size	= 4 KB
Used space	= 21,160 MB
Free space	= 55,157 MB
Percent free space	= 72 %

Fragmentation percentage

Volume fragmentation	= 9 %
Data fragmentation	= 32 %

Directory fragmentation

Total directories	= 12,289
Fragmented directories	= 301
Excess directory fragments	= 3,181

File fragmentation

Total files	= 65,065
Average file size	= 336 KB
Total fragmented files	= 5,426
Total excess fragments	= 21,979
Average fragments per file	= 1.33
Files with performance loss	= 0

Paging file fragmentation

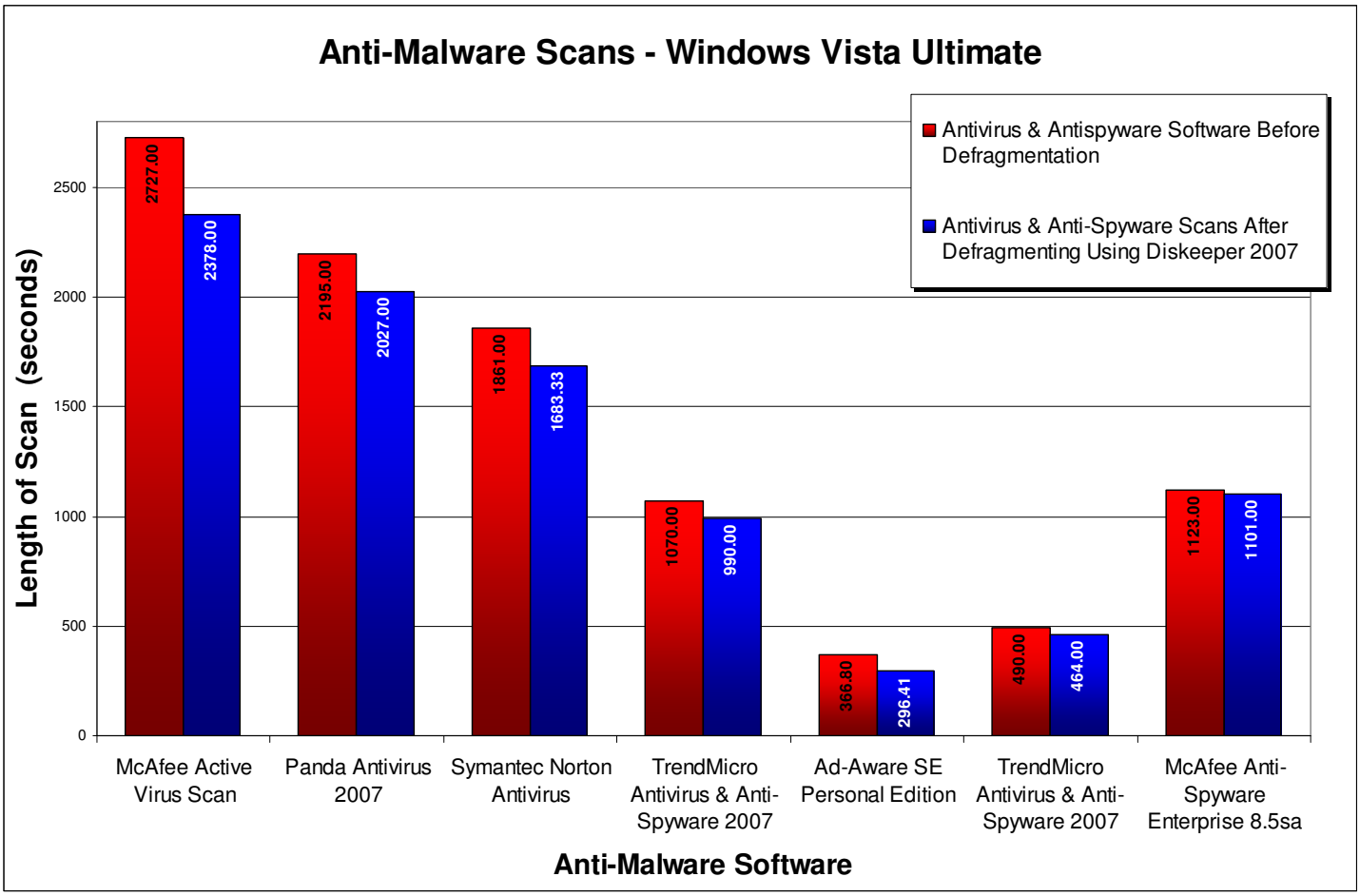
Paging/Swap file size	= 1,537 MB
Total fragments	= 2

Master File Table (MFT) fragmentation

Total MFT size	= 100 MB
MFT records In Use	= 77,461
Percent MFT in use	= 74 %
Total MFT fragments	= 21

Graphed Summary Results

In the presented graphs, the numbers are averages based on the median 3 values of the 5 gathered from each trial, in order to produce a more accurate average. (All of the individual results can be found under **Test Results** below)



Detailed Results

Windows Vista Ultimate

Antivirus	Scan Times (Seconds)						Improvement After Defragmentation
	1	2	3	4	5	Avg.	
McAfee Active Virus Scan							
Before Defragmenting	~~2750.00~~	2728.00	2721.00	~~2710.00~~	2732.00	2727.00	12.80%
During Defragmentation	2486.00	2450.00	~~2491.00~~	~~2400.00~~	2457.00	2464.33	
After Defragmenting	2368.00	2391.00	~~2393.00~~	2375.00	~~2343.00~~	2378.00	
Panda Antivirus 2007							
Before Defragmenting	~~2208.00~~	2205.00	2187.00	2193.00	~~2180.00~~	2195.00	7.65%
During Defragmentation	2080.00	~~2040.00~~	2066.00	~~2081.00~~	2055.00	2067.00	
After Defragmenting	2024.00	2019.00	~~2000.00~~	~~2049.00~~	2038.00	2027.00	
Symantec Norton Antivirus							
Before Defragmenting	1865.00	~~1850.00~~	1854.00	1864.00	~~1892.00~~	1861.00	9.55%
During Defragmentation	1683.00	~~1661.00~~	1679.00	1689.00	~~1701.00~~	1683.67	
After Defragmenting	~~1668.00~~	1683.00	1679.00	~~1694.00~~	1688.00	1683.33	
Trend Micro Antivirus & Anti-Spyware 2007							
Before Defragmenting	1074.00	1061.00	1075.00	~~1059.00~~	~~1080.00~~	1070.00	7.48%
During Defragmentation	990.00	~~1012.00~~	~~969.00~~	989.00	990.00	989.67	
After Defragmenting	~~1006.00~~	985.00	~~972.00~~	996.00	989.00	990.00	

Anti-Spyware	Scan Times (Seconds)						Improvement After Defragmentation
	1	2	3	4	5	Avg.	
Ad-Aware SE Personal Edition							
Before Defragmenting	400.89	356.28	343.22	~~341.17~~	~~407.09~~	366.80	19.19%
During Defragmentation	~~347.11~~	303.98	302.83	~~294.68~~	311.02	305.94	
After Defragmenting	~~329.45~~	285.33	304.06	299.84	~~281.12~~	296.41	
Trend Micro Antivirus & Anti-Spyware 2007							
Before Defragmenting	495.00	~~473.00~~	489.00	486.00	~~502.00~~	490.00	5.31%
During Defragmentation	472.00	~~482.00~~	470.00	~~465.00~~	473.00	471.67	
After Defragmenting	~~479.00~~	459.00	~~453.00~~	461.00	472.00	464.00	
McAfee Anti-Spyware Enterprise 8.5sa							
Before Defragmenting	1113.00	1132.00	~~1111.00~~	~~1140.00~~	1124.00	1123.00	1.96%
During Defragmentation	1120.00	1114.00	~~1112.00~~	1108.00	~~1133.00~~	1114.00	
After Defragmenting	~~1124.00~~	~~1090.00~~	1100.00	1107.00	1096.00	1101.00	

CONCLUSION

In every comparison trial, scan times were improved after Diskeeper defragmented the target volume. The basic principle is that the greater the degree of fragmentation, the worse a computer will perform. This holds true for anti-malware applications just as it would for any user interaction with a fragmented computer.

In Windows Vista, Ad-Aware SE Personal Edition exhibited the greatest improvement with 19.19%. The improvement in scan times across the 7 software products tested averaged out at 9.13%.

In Windows XP Professional, the greatest improvement in scan time after defragmentation was displayed by Panda Antivirus 2007, which exhibited a 23.28% faster scan time. The average improvement in scan times over all of the software products was 15.7%.

Similarly, improvements *during* automated defragmentation, are readily evident over that of a fragmented state. In a number of the antivirus trials, evidence presented annotates gradual improvement in scan times between the initial 'fragmented' state and a fully completed 'defragmented' state. Over a majority of trials, the 'during defragmentation' scan times nearly mirrored those of the 'post defragmentation' numbers. In other words, a significant percentage of the performance gain is realized immediately as the fragmentation state improves.

The fragmentation levels in the trials are based on Diskeeper Corporation's research into what is defined as *very mild* fragmentation on a real-world computer. This translates into slightly over 20,000 excess fragments on Windows Vista and just over 47,000 in Windows XP, achieved by natural means. Windows XP tests were performed with greater levels of fragmentation as this operating system does not include a natively scheduled bare bones defragmenter. Windows Vista fragmentation levels are depictive of file fragment accumulation in-between default schedules and based on the relative limited effectiveness of that operating system's native solution. Desktops and Laptops in use for more than 6 months are very likely to have fragmentation in significantly higher ranges. Fragmentation exceeding 100,000 excess extents is routine, and to be expected, on roaming laptops and power-user desktops where local activity is greater. Free software utilities such as Disk Performance Analyzer for Networks (available at most share/freeware download sites and Diskeeper.com) offer easy network wide and system-by-system fragmentation analysis.

In summary, the use of an automated defragmentation tool provides an excellent compliment to security software. Advanced technology such as the ability to run invisibly on a computer, and solving disk fragmentation in real-time are vital. This is especially true in corporate environments where the technology eliminates the need to manage potential scheduling conflicts from disparate applications (e.g. defragmenter and anti-virus, anti-spyware, etc), affords application compatibility, and guarantees optimized disks for security processing.

Diskeeper corporation
7590 N. Glenoaks Blvd.
Burbank, CA 91504
800-829-6468
www.diskeeper.com