



NIJ

Special

REPORT

ACES Software Write Block Tool Test Report: Writeblocker Windows XP V6.10.0

NIJ Website

**U.S. Department of Justice
Office of Justice Programs**

810 Seventh Street N.W.
Washington, DC 20531

Michael B. Mukasey
Attorney General

Jeffrey L. Sedgwick
Acting Assistant Attorney General

David W. Hagy
Acting Principal Deputy Director, National Institute of Justice

This and other publications and products of the National Institute of Justice can be found at:

National Institute of Justice
NIJ Website

Office of Justice Programs
Innovation • Partnerships • Safer Neighborhoods
OOJ Website



JAN. 08

**ACES Software Write Block Tool
Test Report: Writeblocker Windows
XP V6.10.0**

NCJ 220222



David W. Hagy

Acting Principal Deputy Director, National Institute of Justice

This report was prepared for the National Institute of Justice, U.S. Department of Justice, by the Office of Law Enforcement Standards of the National Institute of Standards and Technology under Interagency Agreement 2003-IJ-R-029.

The National Institute of Justice is a component of the Office of Justice Programs, which also includes the Bureau of Justice Assistance, the Bureau of Justice Statistics, the Office of Juvenile Justice and Delinquency Prevention, and the Office for Victims of Crime.

**ACES Software Write Block Tool Test Report:
Writeblocker XP V6.10.0**

January 2008



National Institute of Standards and Technology
Technology Administration, U.S. Department of Commerce

Contents

Introduction	7
1. Results Summary by Base Requirements	8
2. Anomalies	9
3. Observations	10
4. Test Case Selection	11
5. Test Results by Assertion	12
5.1 MANDATORY ASSERTIONS	12
5.2 OPTIONAL ASSERTIONS	13
6. Testing Environment	14
6.1 TEST COMPUTER	14
6.2 HARD DISK DRIVES	14
6.3 TEST SOFTWARE	15
6.4 RUN PROTOCOL SELECTION	16
7. Interpretation of Test Results	17
7.1 TEST ASSERTION VERIFICATION	17
7.2 OPTIONAL ASSERTIONS	18
8. Key to reading test results	20
8.1 HARD DISK CONFIGURATION	20
8.2 WRITE BLOCKER CONFIGURATION	21
8.3 TEST OUTPUT SUMMARY	22
9. Test Result Summaries	23
9.1 TEST CASE SWB-01	23
9.1.1. Hard disk configuration	23
9.1.2. Write blocker configuration	24
9.1.3. Test output summary	25
9.1.4. Hard disk hash results	25
9.1.5. Test result analysis	25
9.2 TEST CASE SWB-02	26
9.2.1. Hard disk configuration	26
9.2.2. Write blocker configuration	27
9.2.3. Test output summary	28
9.2.4. Hard disk hash results	28
9.2.5. Test result analysis	29
9.3 TEST CASE SWB-03	30
9.3.1. Hard disk configuration	30
9.3.2. Write blocker configuration	31
9.3.3. Test output summary	32
9.3.4. Hard disk hash results	32
9.3.5. Test result analysis	33
9.4 TEST CASE SWB-04	34
9.4.1. Hard disk configuration	34
9.4.2. Write blocker configuration	35
9.4.3. Test output summary	36

9.4.4.	Hard disk hash results	36
9.4.5.	Test results analysis	37
9.5	TEST CASE SWB-05	38
9.5.1.	Hard disk configuration	38
9.5.2.	Write blocker configuration	39
9.5.3.	Test output summary	40
9.5.4.	Hard disk hash results	40
9.5.5.	Test results analysis	41
9.6	TEST CASE SWB-06	42
9.6.1.	Hard disk configuration	42
9.6.2.	Write blocker configuration	43
9.6.3.	Test output summary	44
9.6.4.	Hard disk hash results	44
9.6.5.	Test results analysis	45
9.7	TEST CASE SWB-07	46
9.7.1.	Hard disk configuration	46
9.7.2.	Write blocker configuration	47
9.7.3.	Test output summary	48
9.7.4.	Hard disk hash results	49
9.7.5.	Test results analysis	49
9.8	TEST CASE SWB-08	50
9.8.1.	Hard disk configuration	50
9.8.2.	Write blocker configuration	51
9.8.3.	Test output summary	51
9.8.4.	Hard disk hash results	52
9.8.5.	Test results analysis	53
9.9	TEST CASE SWB-09	54
9.9.1.	Hard disk configuration	54
9.9.2.	Write blocker configuration	55
9.9.3.	Test output summary	55
9.9.4.	Hard disk hash results	56
9.9.5.	Test results analysis	57
9.10	TEST CASE SWB-10	58
9.10.1.	Hard disk configuration	58
9.10.2.	Write blocker configuration	59
9.10.3.	Test output summary	60
9.10.4.	Hard disk hash results	61
9.10.5.	Test results analysis	61
9.11	TEST CASE SWB-11	62
9.11.1.	Hard disk configuration	62
9.11.2.	Write blocker configuration	63
9.11.3.	Test output summary	63
9.11.4.	Hard disk hash results	64
9.11.5.	Test results analysis	65
9.12	TEST CASE SWB-12	66
9.12.1.	Hard disk configuration	66

9.12.2.	Write blocker configuration	67
9.12.3.	Test output summary	68
9.12.4.	Hard disk hash results	69
9.12.5.	Test results analysis	69
9.13	TEST CASE SWB-13	70
9.13.1.	Hard disk configuration	70
9.13.2.	Write blocker configuration	71
9.13.3.	Test output summary	72
9.13.4.	Hard disk hash results	73
9.13.5.	Test results analysis	73
9.14	TEST CASE SWB-14	74
9.14.1.	Hard disk configuration	74
9.14.2.	Write blocker configuration	75
9.14.3.	Test output summary	76
9.14.4.	Hard disk hash results	77
9.14.5.	Test results analysis	77
9.15	TEST CASE SWB-15	78
9.15.1.	Hard disk configuration	78
9.15.2.	Write Blocker Configuration	79
9.15.3.	Test output summary	80
9.15.4.	Hard disk hash results	81
9.15.5.	Test results analysis	81
9.16	TEST CASE SWB-16	82
9.16.1.	Hard disk configuration	82
9.16.2.	Write blocker configuration	83
9.16.3.	Test output summary	84
9.16.4.	Hard disk hash results	85
9.16.5.	Test results analysis	85
9.17	TEST CASE SWB-17	86
9.17.1.	Hard disk configuration	86
9.17.2.	Write blocker configuration	87
9.17.3.	Test output summary	88
9.17.4.	Hard disk hash results	89
9.17.5.	Test results analysis	89
9.18	TEST CASE SWB-18	90
9.18.1.	Hard disk configuration	90
9.18.2.	Write blocker configuration	91
9.18.3.	Test output summary	92
9.18.4.	Hard disk hash results	93
9.18.5.	Test results analysis	93
9.19	TEST CASE SWB-19	94
9.19.1.	Hard disk configuration	94
9.19.2.	Write blocker configuration	95
9.19.3.	Test output summary	96
9.19.4.	Hard disk hash results	97
9.19.5.	Test results analysis	97

9.20	TEST CASE SWB-20	98
9.20.1.	Hard disk configuration	98
9.20.2.	Write blocker configuration	99
9.20.3.	Test output summary	100
9.20.4.	Hard disk hash results	101
9.20.5.	Test results analysis	101
9.21	TEST CASE SWB-21	102
9.21.1.	Hard disk configuration	102
9.21.2.	Write blocker configuration	103
9.21.3.	Test output summary	104
9.21.4.	Hard disk hash results	105
9.21.5.	Test results analysis	105
9.22	TEST CASE SWB-22	106
9.22.1.	Hard disk configuration	106
9.22.2.	Write blocker configuration	107
9.22.3.	Test output summary	108
9.22.4.	Hard disk hash results	109
9.22.5.	Test results analysis	109
9.23	TEST CASE SWB-23	110
9.23.1.	Hard disk configuration	110
9.23.2.	Write blocker configuration	111
9.23.3.	Test output summary	112
9.23.4.	Hard disk hash results	113
9.23.5.	Test results analysis	113
9.24	TEST CASE SWB-24	114
9.24.1.	Hard disk configuration	114
9.24.2.	Write blocker configuration	115
9.24.3.	Test output summary	115
9.24.4.	Hard disk hash results	116
9.24.5.	Test results analysis	116
9.25	TEST CASE SWB-25	117
9.25.1.	Hard disk configuration	117
9.25.2.	Write blocker configuration	118
9.25.3.	Test output summary	119
9.25.4.	Hard disk hash results	120
9.25.5.	Test results analysis	120
9.26	TEST CASE SWB-26	121
9.26.1.	Hard disk configuration	121
9.26.2.	Write blocker configuration	122
9.26.3.	Test output summary	123
9.26.4.	Hard disk hash results	123
9.26.5.	Test results analysis	123
9.27	TEST CASE SWB-27	124
9.27.1.	Hard disk configuration	124
9.27.2.	Write blocker configuration	125
9.27.3.	Test output summary	126

9.27.4.	Hard disk hash results	127
9.27.5.	Test results analysis	127
9.28	TEST CASE SWB-28	128
9.28.1.	Hard disk configuration	128
9.28.2.	Write blocker configuration	129
9.28.3.	Test output summary	130
9.28.4.	Hard disk hash results	130
9.28.5.	Test results analysis	131
9.29	TEST CASE SWB-29	132
9.29.1.	Hard disk configuration	132
9.29.2.	Write blocker configuration	133
9.29.3.	Test output summary	134
9.29.4.	Hard disk hash results	135
9.29.5.	Test results analysis	135
9.30	TEST CASE SWB-30	136
9.30.1.	Hard disk configuration	136
9.30.2.	Write blocker configuration	137
9.30.3.	Test output summary	138
9.30.4.	Hard disk hash results	139
9.30.5.	Test results analysis	139
Appendix A		140
Appendix B		150

Introduction

The Computer Forensics Tool Testing (CFTT) program is a joint project of the National Institute of Justice (NIJ), the research and development organization of the U.S. Department of Justice, and the National Institute of Standards and Technology's (NIST's) Office of Law Enforcement Standards and Information Technology Laboratory. CFTT is supported by other organizations, including the Federal Bureau of Investigation, the Department of Defense Cyber Crime Center, and the Department of Homeland Security's Bureau of Immigration and Customs Enforcement and U.S. Secret Service. The objective of the CFTT project is to provide measurable assurance to practitioners, researchers, and other applicable users that the tools used in computer forensics investigations provide accurate results. Accomplishing this requires the development of specifications and test methods for computer forensics tools and subsequent testing of specific tools against those specifications.

Test results provide the information necessary for developers to improve tools, users to make informed choices, and the legal community and others to understand the tools' capabilities. The approach for testing computer forensic tools is based on well-recognized methodologies for conformance and quality testing. The specifications and test methods are posted on the [CFTT web site](#) for both comment and review by the computer forensics community.

This document reports test results for **Writeblocker XP, Version 6.10.0**. All testing was conducted in accordance with the *ACES Software Write Block Tool Specification & Test Plan Version 1.0* that may be found on the CFTT web site.

1. Results Summary by Base Requirements

Product ID: Writeblocker XP V6.10.0
Producer: Booz, Allen, Hamilton, Inc.
Operating Environment: Microsoft Windows XP, Intel x86

The tool shall not allow a protected drive to be changed.

The tool failed to block some test commands from the protected categories that were sent to protected drives but no changes to the protected drives were observed.

The tool shall not prevent obtaining any information from or about any drive.

The tool did not alter or block test commands from any non-protected category that were sent to protected or unprotected drives.

The tool shall not prevent any operations to a drive that is not protected.

The tool did not alter or block any test commands sent to unprotected drives.

2. Anomalies

The tool blocked all SCSI-2 commands from the WRITE category but failed to block most of the SCSI-3 commands in that category. The tool also failed to block four internal IRP functions from the WRITE category. The tool did not block any of the commands from the VENDOR_SPECIFIC and UNDEFINED categories. See Sections 9.3.5, 9.4.5, and 9.5.5 for a complete list of the commands allowed.

Test cases: SWB-03, SWB-05, SWB-06 through SWB-23

3. Observations

The tested tool, Writeblocker XP V6.10.0, consists of two kernel mode device drivers, NTWBFS and NTWBPM, and a user mode GUI control application. The NTWBFS driver is a file system filter driver that filters file system calls and the NTWBPM driver is a physical device filter that filters hardware I/O requests. Of the two kernel mode drivers, the NTWBPM driver was tested directly by test cases SWB-01 through SWB-24. Test cases SWB-25 through SWB-30 tested the ability of both components, working together, to protect a hard drive. The decision to test the physical device driver directly is predicated on the assumption that all file system functions are ultimately manifested as physical I/O requests. Filtering at the file system level is often necessary to simulate successful completion of logical file system I/O activity that would cause the operating system to crash or hang should the physical I/O operation return a failure status.

Test cases SWB-25 through SWB-30 demonstrate that Writeblocker XP blocked all attempts to write to a protected drive by commands issued from common operating system tools and from the widely used forensic tools FTK™ and EnCase®. While for test cases SWB-01 through SWB-24, some commands that could write to a drive are not blocked by the NTWBPM component, these commands are not likely to reach the NTWBPM component because the commands not blocked by NTWBPM are either blocked by the file system component (NTWBFS) or the commands are not issued by software typically used for acquiring or previewing digital data as part of a sound forensic examination.

4. Test Case Selection

The test cases were selected from *ACES Software Write Block Tool Specification and Test Plan Version 1.0*. All 30 test cases from that specification were run.

5. Test Results by Assertion

Product ID: Writeblocker XP V6.10.0
Producer: Booz, Allen, Hamilton, Inc.
Product Checksum: SHA1:
Operating Environment: Microsoft Windows XP, Intel x86

5.1 Mandatory Assertions

SWB-AM-01 If a drive is unprotected then the tool shall not block any command.

The tool did not alter or block any test commands sent to unprotected drives.

SWB-AM-02 If a drive is protected and a command from the READ category is issued then the tool shall not block the command.

The tool did not block or alter any test command from the READ category sent to a protected drive.

SWB-AM-03 If a drive is protected and a command from the WRITE category is issued then the tool shall block the command.

The tool failed to block 12 of the 34 test commands from the WRITE category issued to protected drives.

SWB-AM-04 If a drive is protected and a command from the VENDOR_SPECIFIC category is issued then the tool shall block the command.

The tool failed to block any of the 34 test commands from the VENDOR_SPECIFIC category issued to protected drives.

SWB-AM-05 If a drive is protected and a command from the UNDEFINED category is issued then the tool shall block the command.

The tool failed to block any of the of the 80 test commands from the UNDEFINED category issued to protected drives.

SWB-AM-06 If a drive is protected and a command from the OTHER category is issued then the tool shall not block the command.

The tool did not block or alter any test command from the OTHER category sent to a protected drive.

SWB-AM-07 If the tool is executed then the tool shall issue a message indicating the tool is active.

Not applicable. This tool cannot be executed by user command.

SWB-AM-08 If the tool is executed the tool shall issue a message indicating all drives accessible by the covered interfaces.

The management GUI application displays a list of all drives connected to covered interfaces.

SWB-AM-09 **If the tool is executed then the tool shall issue a message indicating the protection status of each drive connected to a covered interface.**

The management GUI application displays the protection status of all drives connected to covered interfaces.

5.2 Optional assertions

SWB-AO-01 **If a subset of all covered drives is specified for protection, then commands from the write category shall be blocked for drives in the selected subset.**

The tool failed to block 12 of the 34 test commands from the WRITE category issued to protected drives.

SWB-AO-02 **If a subset of all drives is specified for protection, then commands from the VENDOR_SPECIFIC category shall be blocked for drives in the selected set.**

The tool failed to block all of the 80 test commands from the VENDOR_SPECIFIC category issued to protected drives.

SWB-AO-03 **If a subset of covered drives is selected for protection, then commands from the UNDEFINED category shall be blocked for drives in the selected set.**

The tool failed to block all of the 53 test commands from the UNDEFINED category sent to protected drives.

SWB-AO-04 **If a subset of covered drives is selected for protection, then commands from the READ category shall be not blocked for drives in the selected set.**

The tool did not block any test commands from the READ category sent to the drives.

SWB-AO-05 **If a subset of covered drives is selected for protection, then commands from the OTHER category shall be not blocked for drives in the selected set.**

The tool did not block any test commands from the OTHER category sent to the drives.

SWB-AO-06 **If a subset of covered drives is selected for protection, then no commands from the any category shall be blocked for drives not in the selected set.**

The tool did not block any commands sent to unprotected drives.

SWB-AO-07 **If the tool is active and the tool is deactivated then no commands to any drive shall be blocked.**

No commands to any drive were blocked after the tool was deinstalled.

SWB-AO-08 **If the tool blocks a command then the tool shall issue either an audio or visual signal.**

The tool displays a visual indication of blocked commands in the event log window of the control program.

6. Testing Environment

The tests were run in the NIST CFTT laboratory. This section describes the hardware (host computer and hard drives) and software used for the tests.

6.1 Test Computer

The hardware configuration of test computer FRANK is:

Intel® D865GBF Motherboard
BIOS: Intel/AMI BF86510A.86A.0053.P13
Intel Dual Pentium® 4 CPU 3.4Ghz
3072M Memory
Adaptec® 29160 SCSI Adapter card Ultra 160
Sony DVD RW DRU-530A
Two slots for removable IDE hard disk drives
Two slots for removable SCSI hard disk drives
Two slots for removable SATA hard disk drives

6.2 Hard Disk Drives

The hard disk drives that were used in the testing are shown in the table below. These hard drives were mounted in removable storage modules and installed/deinstalled as needed for the individual test being run. The label column indicates an external identification label affixed to the housing in which the drive was installed. Each drive was formatted with an NTFS or FAT partition and a Windows volume was created on that partition. The volumes were assigned volume labels that correspond to the external label on the physical device. The volume labels allow easy identification of which physical drives are associated with which physical device objects while the Windows operating system is running.

Label	Model	Interface	Usable Sectors	Size
25	Seagate ST373405LC	SCSI	143374741	73408 MB
27	Quantum ATLAS-10K3-18-SCA_	SCSI	35916548	18389 MB
70	IC35L040AVER07-0	IDE	80418240	41174 MB
119	WDC WD1200JD-00GBB0	SATA	234441648	120034 MB

6.3 Test Software

The following table describes the software packages installed on the test system.

Package	Description
Writeblocker XP V6.10.0	Writeblocker XP Version 6.10.0 <ul style="list-style-type: none">NTWBPM—a kernel mode device filter driver that implements write blocking at the physical device level.NTWBFS—a kernel mode file system filter driver that implements write blocking at the file system level.Writeblocker.exe—a user mode GUI for configuring and monitoring the kernel mode filters
SWBTS V1.2	The NIST Software Writeblocker Test Suite V1.2 <ul style="list-style-type: none">PITCHER—a kernel filter driver that implements a custom IOCTL interface for generating kernel mode IRPs.CATCHER—a kernel filter driver that monitors IRP traffic on a device driver stack and catches and completes test generated IRPs.DEVCTL—a user mode console application for controlling the tests. It generates test IRPs and logs the results.
BusTrace 2003	A third party kernel mode software package for monitoring IRP traffic within the Windows device driver stacks

The NIST Software Write Blocker Test Suite V1.2 software was used to conduct the testing. This software consists of two kernel mode device drivers and a user mode control program. The kernel mode drivers monitor the flow of I/O requests within the device driver stacks being tested. The user mode application initiates test I/O requests and tallies the outcome of the tests.

Writeblocker XP V6.10.0 was the software write block tool tested. This package consists of two kernel mode device drivers: NTWBFS and NTWBPM, and a user mode GUI control application. The NTWBFS driver is a file system filter driver that filters file system calls and the NTWBPM driver is a physical device filter that filters hardware I/O requests. Of the two kernel mode drivers, only the NTWBPM driver was tested. The decision to test only the physical device driver is predicated on the assumption that all file system functions are ultimately manifested as physical I/O requests. Filtering at the file system level is often necessary to simulate successful completion of logical file system I/O activity that would cause the operating system to crash or hang should the physical I/O operation return a failure status. The behavior of this component of the tool is not however a determining factor on the overall requirements of the test assertions for software write blocking tools.

The BusTrace 2003 package is a commercial software package for monitoring the movement of IRP traffic on Windows device driver stacks. The Filter Load Order utility from this package was used to confirm the test suite and write blocker kernel drivers were properly installed prior to running the tests. Appendix B contains screen captures from that utility showing the load order of the driver modules.

6.4 Run Protocol Selection

The run protocols define the actual procedures to follow for running the test cases. They are described in the test plan document.

- Test cases SWB-01 through SWB-22 and SWB-26 through SWB-30 were conducted using the RUN protocol.
- Test case SWB-23 was conducted using the BOOT protocol.
- Test case SWB-24 was conducted using the UNINSTALL protocol.

7. Interpretation of Test Results

The primary item of interest when interpreting the test results is a determination of the conformance of the tool to the test assertions. This section lists each assertion and identifies the information in the test output files relevant to evaluating the tool's conformance to the assertions. Conformance to each assertion tested by a test case is evaluated by examination of the commands issued by the test application and the command results returned by the test application. This document contains only a representative subset of the total output file information collected and is sufficient to illustrate the basis for the test interpretations. The information omitted contains basically redundant results and is omitted for the sake of limiting the size of this document. A complete archive of all test result data may be downloaded from the [website](#).

7.1 Test Assertion Verification

The protection status of each drive tested is identified in the output summary immediately prior to the start of each test. The status shown is either "software WRITE PROTECTED" or "software WRITE ENABLED". The summary also contains a tally of the commands in each category sent to the drive. For each command category the tally contains the TOTAL number of commands in the category issued and subtotals for the number of commands in that category that were ALLOWED and the number BLOCKED. These tallies indicate test assertion conformance as follows:

SWB-AM-01 If a drive is unprotected then the tool shall not block any command.

The tool conforms to this assertion if all tallies of BLOCKED commands from all categories sent to a "software WRITE ENABLED" drive are 0.

SWB-AM-02 If a drive is protected and a command from the READ category is issued to the protected drive then the tool shall not block the command.

The tool conforms to this assertion if the tally of BLOCKED commands from the READ category sent to a "software WRITE PROTECTED" drive is 0.

SWB-AM-03 If a drive is protected and a command from the VENDOR_SPECIFIC category is issued to the protected drive then the tool shall block the command.

The tool conforms to this assertion if the tally of ALLOWED commands from the VENDOR_SPECIFIC category sent to a "software WRITE PROTECTED" drive is 0.

SWB-AM-04 If a drive is protected and a command from the UNDEFINED category is issued to the protected drive then the tool shall block the command.

The tool conforms to this assertion if the tally of ALLOWED commands from the UNDEFINED category sent to a "software WRITE PROTECTED" drive is 0.

SWB-AM-05 If a drive is protected and a command from the READ category is issued to the protected drive then the tool shall not block the command.

The tool conforms to this assertion if the tally of BLOCKED commands from the READ category sent to a "software WRITE PROTECTED" drive is 0.

SWB-AM-06 If a drive is protected and a command from the OTHER category is issued to the drive then the tool shall not block the command.

The tool conforms to this assertion if the tally of BLOCKED commands from the OTHER category sent to a “software WRITE PROTECTED” drive is 0.

SWB-AM-07 If the tool is executed then the tool shall issue a message indicating the tool is active.

Not applicable – the tool is activated by the operating system boot process.

SWB-AM-08 If the tool is executed then the tool shall issue a message indicating all drives accessible by the covered interfaces.

The tool tested provides a management GUI used to control the configuration of protected drives. Captured images of the management screen used to setup the tool prior to running each test case are included in the test output of each test run. The tool conforms to this assertion if all drives configured for a test are shown in the captured image.

SWB-AM-09 If the tool is executed then the tool shall issue a message indicating the protection status of all drives accessible by the covered interface.

The tool tested provides a management GUI used to control the configuration of protected drives. Captured images of the management screen used to setup the tool prior to running each test case are included in test output of each test run. The tool conforms to this assertion if the protection status of all drives configured for each test is shown in the captured image.

SWB-AM-10 If a drive is protected and a command from the BASIC operation category is issued then the command shall fail with an error status and the drive shall not be altered in any way.

7.2 Optional Assertions

SWB-AO-01 If a subset of all covered drives is specified for protection, then commands from the WRITE category shall be blocked for drives in the selected subset.

The tool conforms to this assertion if the ALLOWED tally for commands in the WRITE category is 0 for all “software WRITE PROTECTED” drives tested.

SWB-AO-02 If a subset of all covered drives is specified for protection, then commands from the VENDOR_SPECIFIC category shall be blocked for drives in the selected subset.

The tool conforms to this assertion if the ALLOWED tally for commands in the VENDOR_SPECIFIC category is 0 for all “software WRITE PROTECTED” drives tested.

SWB-AO-03 If a subset of all covered drives is specified for protection, then commands from the UNDEFINED category shall be blocked for drives in the selected subset.

The tool conforms to this assertion if the ALLOWED tally for commands in the UNDEFINED category is 0 for all “software WRITE PROTECTED” drives tested.

SWB-AO-04 If a subset of all covered drives is specified for protection, then commands from the READ category shall not be blocked for drives in the selected subset.

The tool conforms to this assertion if the BLOCKED tally for commands in the READ category is 0 for all “software WRITE PROTECTED” drives tested.

SWB-AO-05 If a subset of all covered drives is specified for protection, then commands from the OTHER category shall not be blocked for drives in the selected subset.

The tool conforms to this assertion if the BLOCKED tally for commands in the OTHER category is 0 for all “software WRITE PROTECTED” drives tested.

SWB-AO-06 If a subset of all covered drives is specified for protection, then no commands from any category shall be blocked for drives not in the selected subset.

The tool conforms to this assertion if the BLOCKED tally for all commands in all categories is 0 for all “software WRITE ENABLED” drives tested.

SWB-AO-07 If the tool is active and the tool is deactivated then no commands to any drive shall be blocked.

Not applicable – tool is activated by the operating system boot process and cannot be deactivated by user command.

SWB-AO-08 If the tool blocks a command then the tool shall issue either an audio or visual signal.

The management GUI includes an event log window. The tool conforms to this assertion if an event log entry is displayed in that window when a command is blocked.

SWB-AO-09 If the tool is configured to be active during the operating system boot process then no changes shall be made to protected drives.

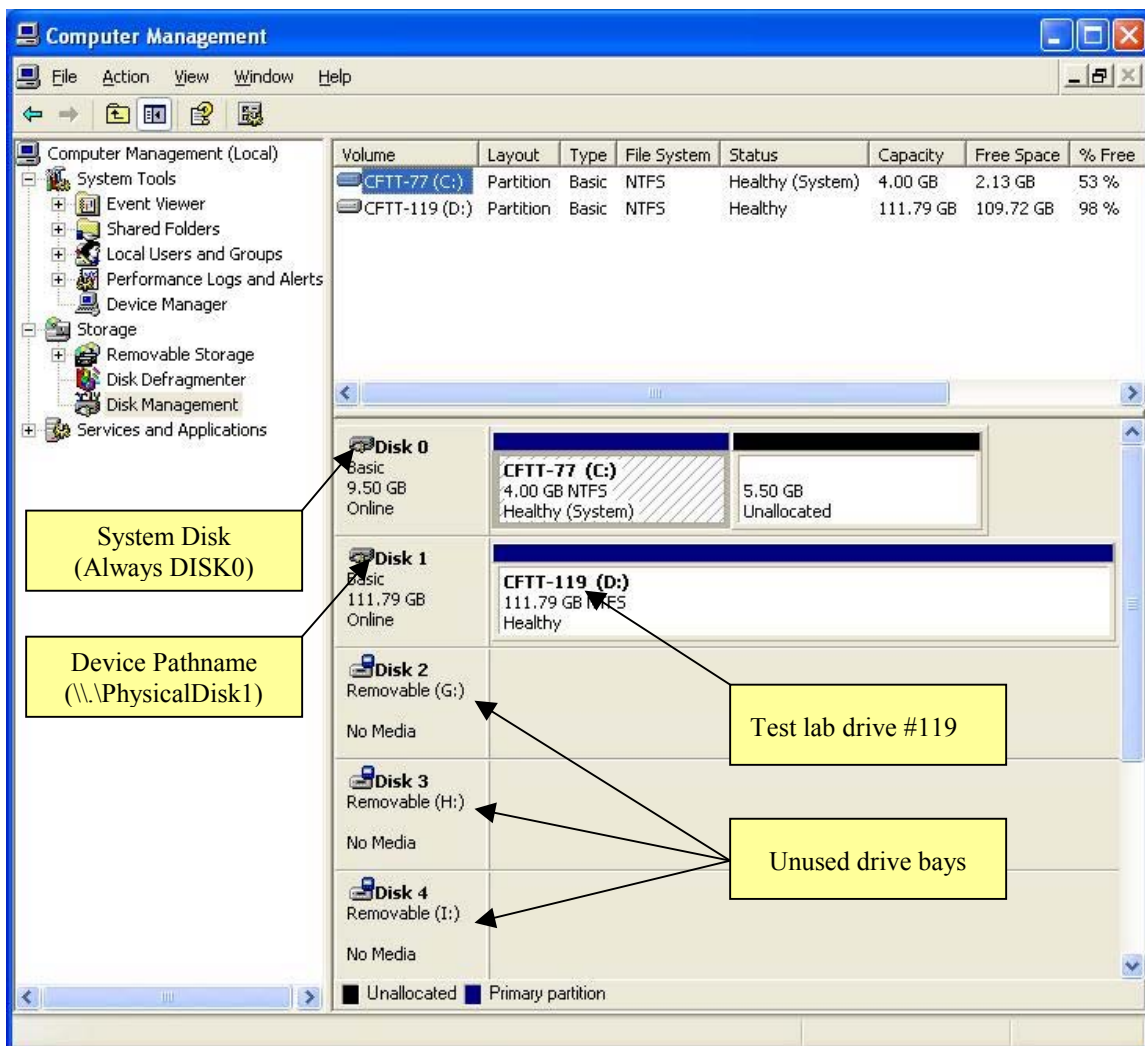
The tool conforms to this assertion if the SHA1 hashes of all protected drives are unchanged across an operating system boot.

8. Key to reading test results

The test summary sections each contain the following subsections.

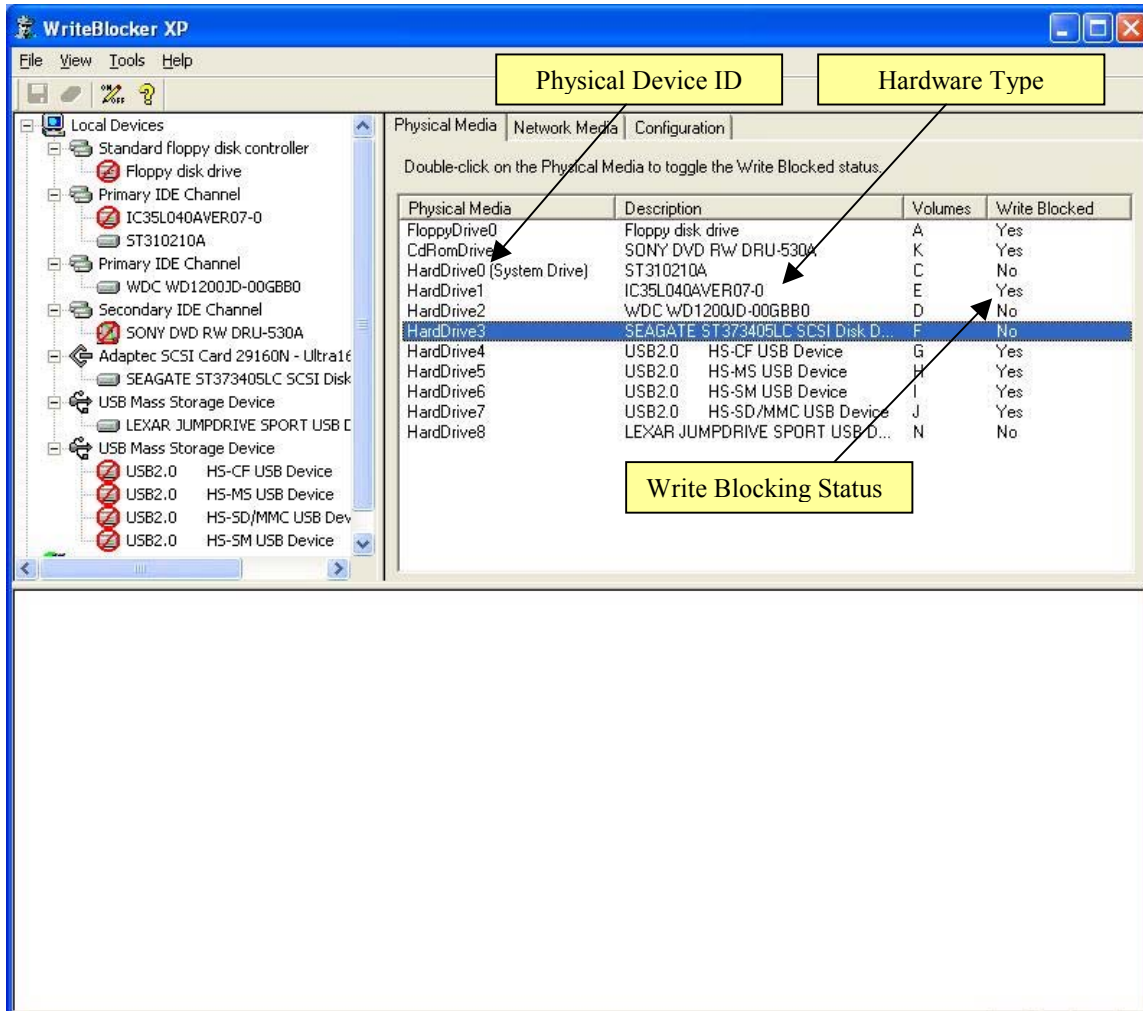
8.1 Hard disk configuration

This section contains a screen capture of the Disk Manager window on the test system similar to the ones shown in the test summary sections. The fields in this window of primary interest with regard to the test cases are highlighted in the example. To assist in identifying which Window's device corresponds to which physical drive installed into the machine, the software volume label written on each drive is of the form CFTT-nnn where nnn represents the external physical label affixed to drives used in the CFTT test laboratory.



8.2 Write blocker configuration

This section contains a screen capture of the Writeblocker GUI configuration window. The fields relevant to interpretation of the test results are highlighted in the example below.



8.3 Test output summary

The test application prints a summary of the test results to the console output device from which the test was run. The Test Output Summary section contains a listing of this information as shown below.

```
1  NIST Software Write Blocker Test Suite V1.2
2  Thu Aug 25 10:06:24 2005
3
4  Test case:          SWB-01
5  Command set:       RWOVU
6  Number of drives:   1
7  Protection pattern: U
8  Test administered by: DPA
9  Details logged to file: SWB-01.log
10
11 **** Test results summary (see logfile for details) ****
12
13 Testing device \\.\PhysicalDrive1
14 Device is software WRITE ENABLED
15
16 Test Category          Allowed    Blocked    Total
17 -----
18 Read IRP's .....         4          0         4
19 Write IRP's .....         8          0         8
20 Other IRP's .....        15          0        15
21
22 Read CDB's .....        27          0        27
23 Write CDB's .....        34          0        34
24 Other CDB's .....        62          0        62
25 Vendor Specific CDB's ..... 80          0        80
26 Undefined CDB's .....        53          0        53
```

Line 1 - test suite identification

Line 2 - date and time of test

Line 4 - test case run

Line 5 - command set to be tested

Line 6 - number of hard drives to be tested

Line 7 - protection pattern of hard drives

Line 8 - individual conducting the test

Line 9 - file name of detailed output file

Line 13 - full pathname of hard drive under test

Line 14 - write protection status of hard drive under test

Line 18 - count of kernel IRPs from the READ command category that were issued

Line 19 - count of kernel IRPs from the WRITE command category that were issued

Line 20 - count of kernel IRPs from the OTHER command category that were issued

Line 22 - count of SCSI CDBs from the READ command category that were issued

Line 23 - count of SCSI CDBs from the WRITE command category that were issued

Line 24 - count of SCSI CDBs from the OTHER command category that were issued

Line 25 - count of SCSI CDBs from the VENDOR_SPECIFIC command category that were issued

Line 26 - count of SCSI CDBs from the UNDEFINED command category that were issued

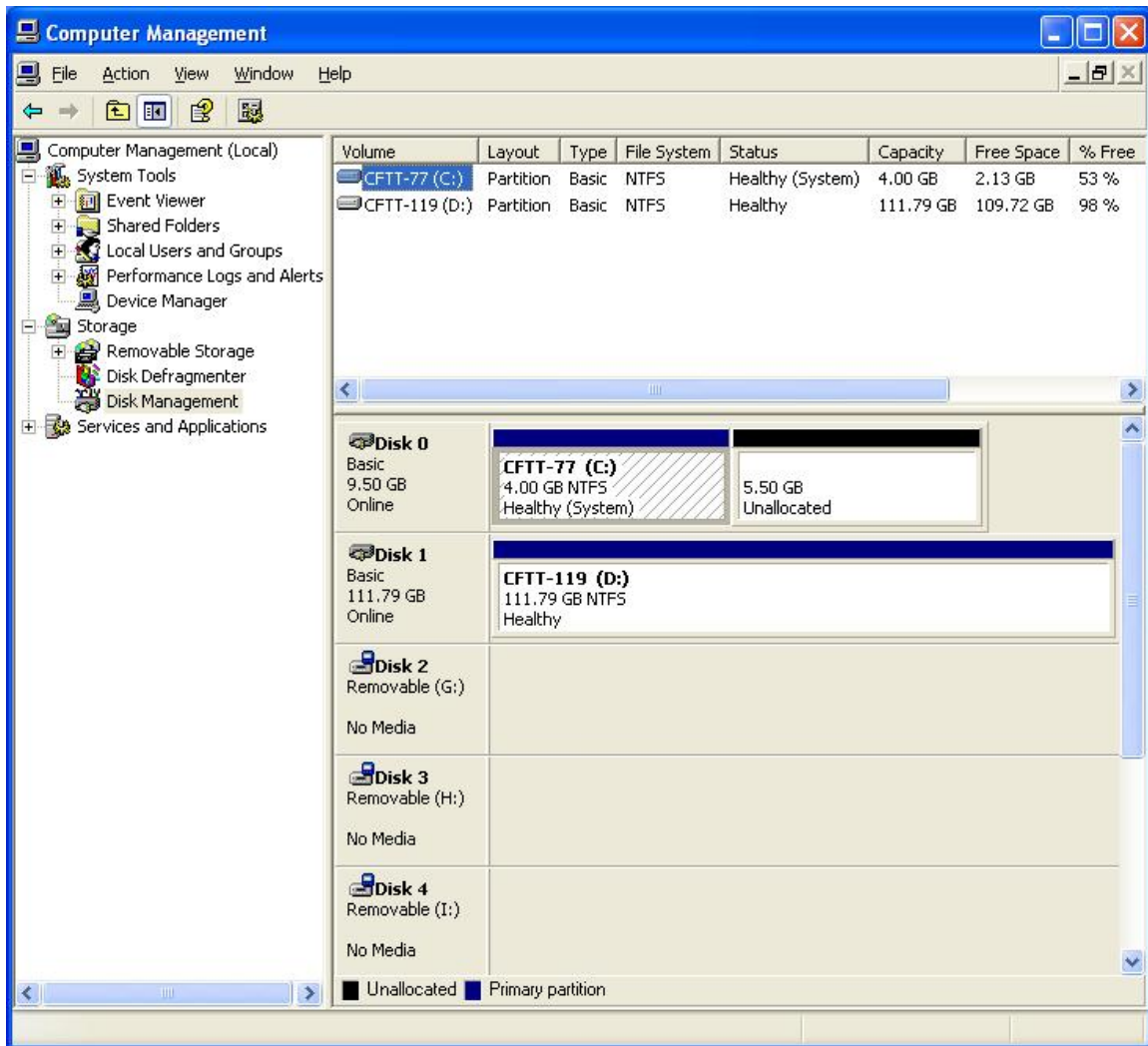
9. Test Result Summaries

9.1 Test Case SWB-01

This test case's primary purpose is to test the tool's compliance with SWB-AM-01. It issues all possible I/O commands to a single unprotected disk drive.

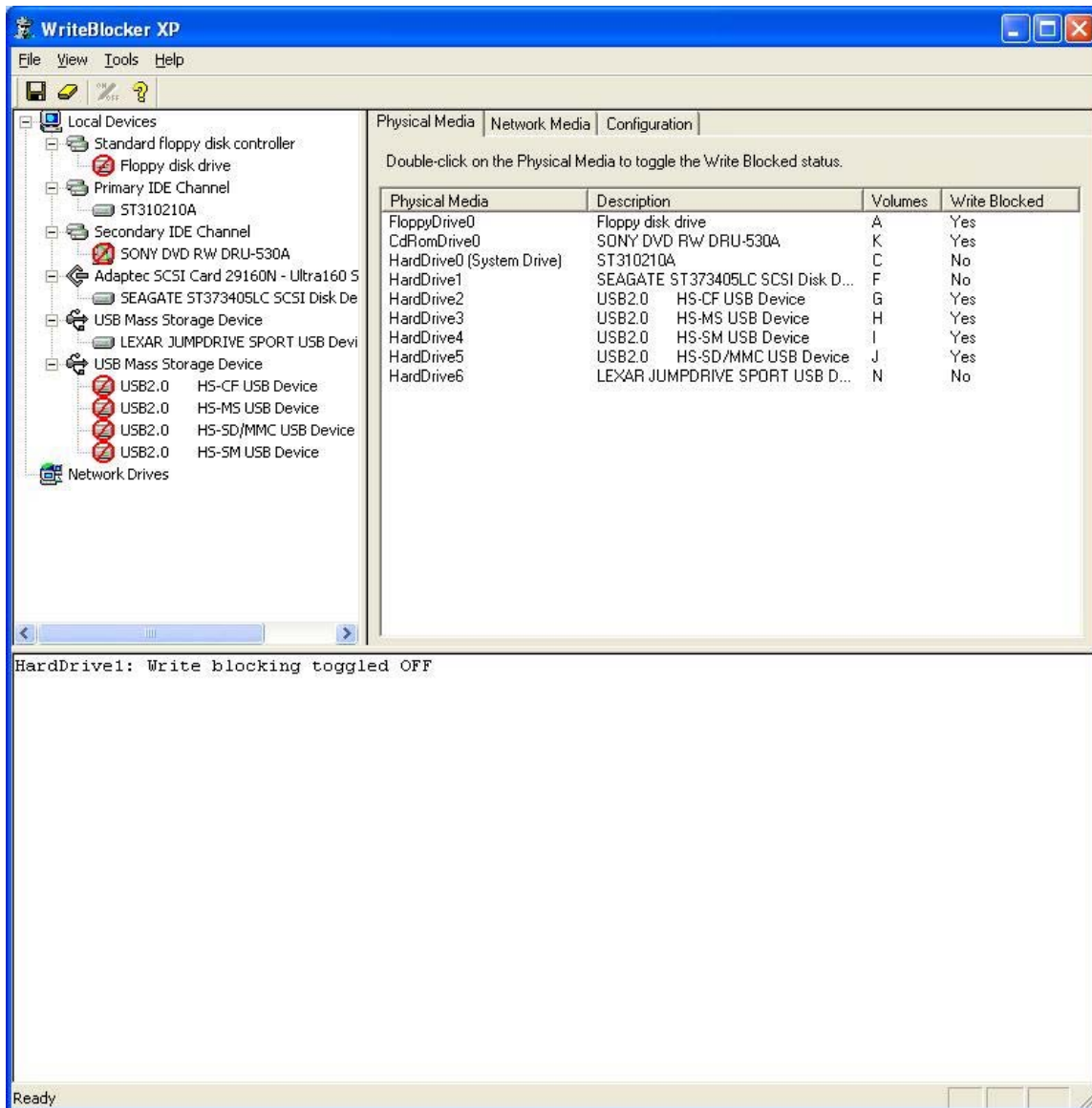
9.1.1. Hard disk configuration

The hard disk configuration used for this test is shown below.



9.1.2. Write blocker configuration

The Writeblocker XP configuration used in this test is shown below.



9.1.3. Test output summary

NIST Software Write Blocker Test Suite V1.2
Thu Aug 25 10:06:24 2005

Test case: SWB-01
Command set: RWOVU
Number of drives: 1
Protection pattern: U
Test administered by: DPA
Details logged to file: SWB-01.log

**** Test results summary (see logfile for details) ****

Testing device \\.\PhysicalDrive1
Device is software WRITE ENABLED

Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	8	0	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	34	0	34
Other CDB's	62	0	62
Vendor Specific CDB's	80	0	80
Undefined CDB's	53	0	53

9.1.4. Hard disk hash results

Drive Identification	Computed	SHA1 Value
\\.\PhysicalDrive1 (CFTT-119)	Before	FBA020AEEC67FF23C40C8BFB5F55DEDBB76385D5
	After	FBA020AEEC67FF23C40C8BFB5F55DEDBB76385D5

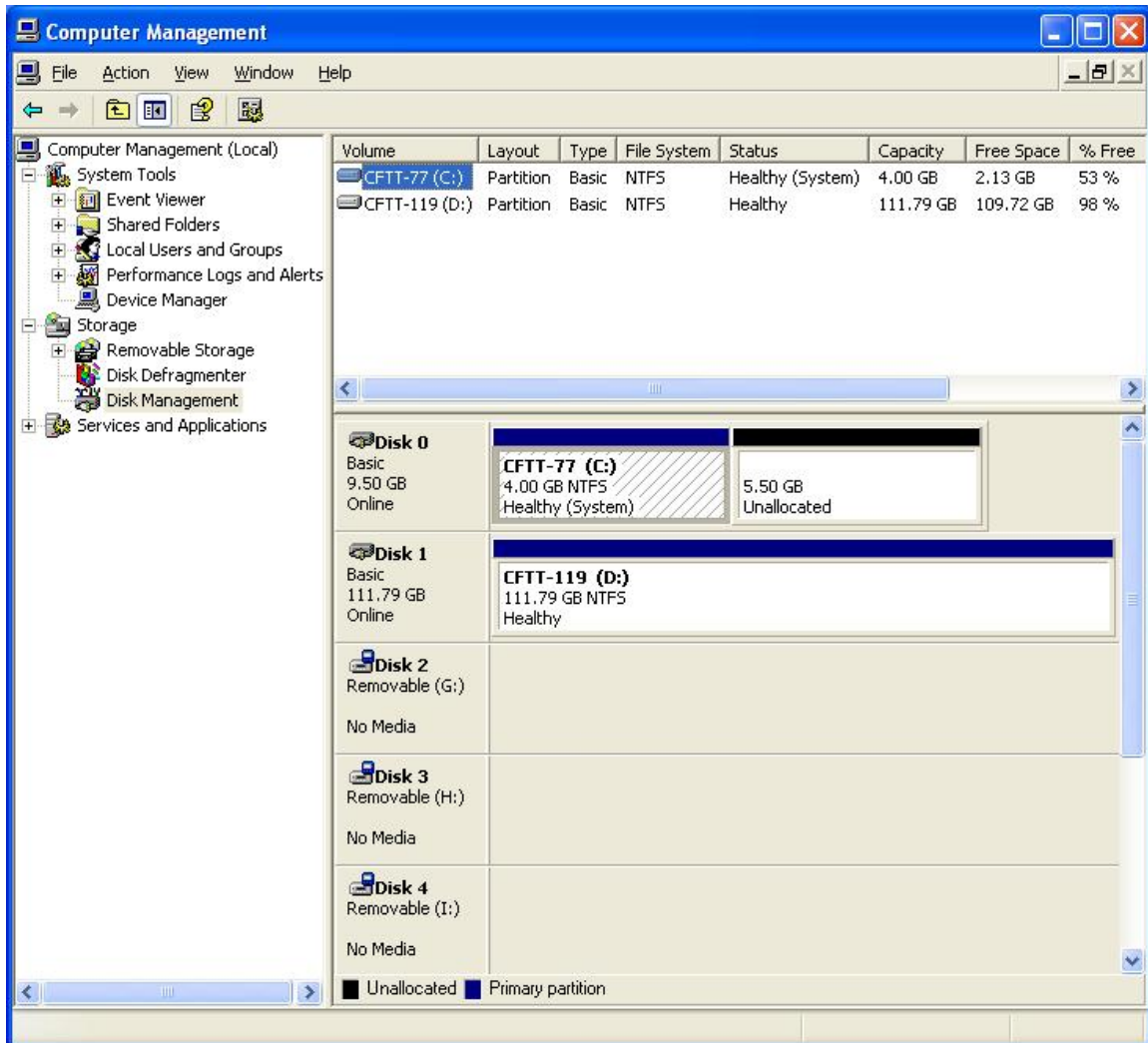
9.1.5. Test result analysis

The expected result for this test was that all command functions issued would be passed by the tool.
That result was observed.

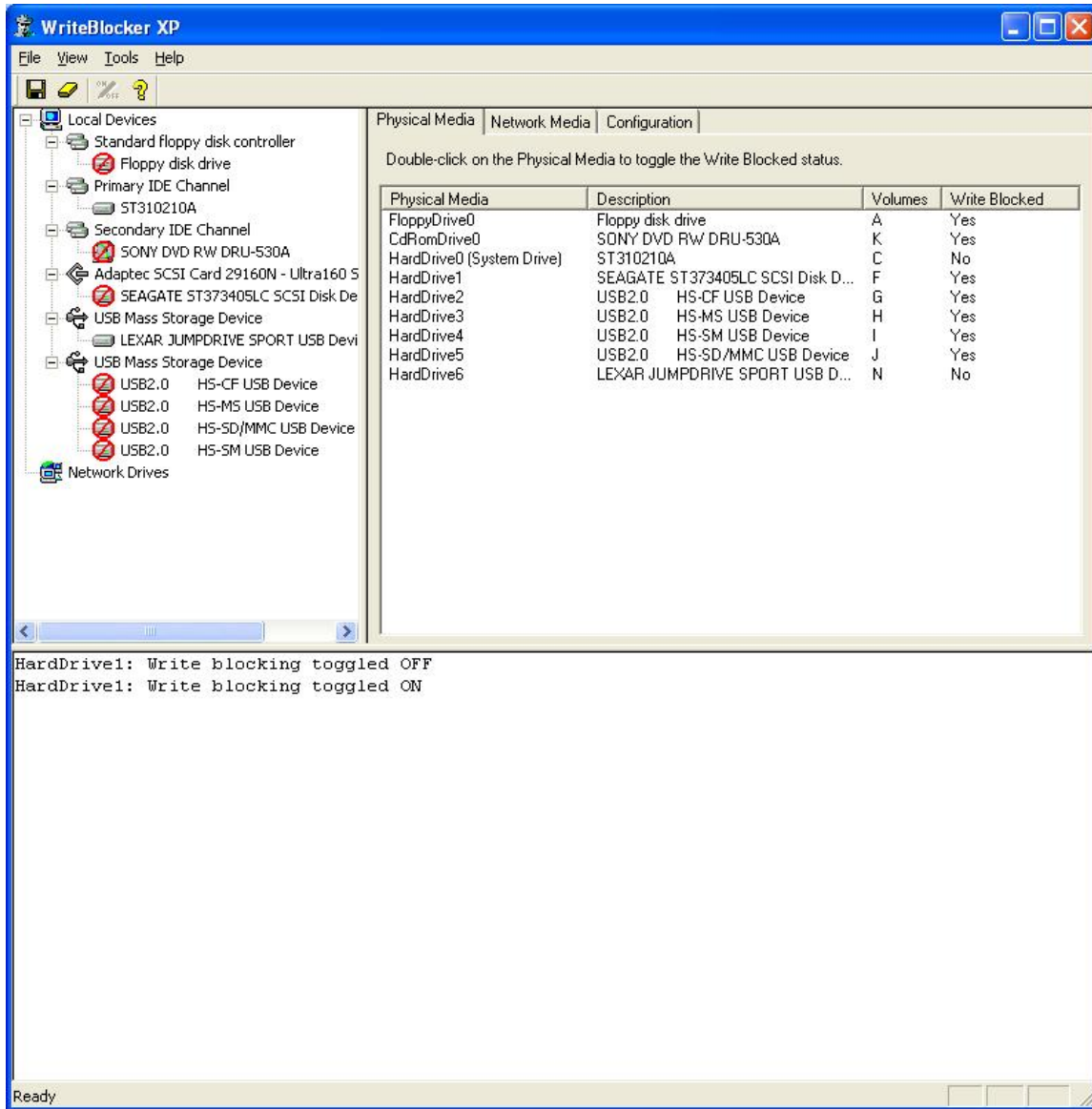
9.2 Test case SWB-02

This test case tests the tool's compliance with SWB-AM-02. It issues all possible READ commands to a single protected disk drive. The expected result is that the tool will not block any READ command issued by the test application

9.2.1. Hard disk configuration



9.2.2. Write blocker configuration



9.2.3. Test output summary

```

NIST Software Write Blocker Test Suite V1.2
Thu Aug 18 11:14:11 2005

Test case:                SWB-02
Command set:              R
Number of drives:         1
Protection pattern:       P
Test administered by:     DPA
Details logged to file:   SWB-02.log

**** Test results summary (see logfile for details) ****

Testing device \\.\PhysicalDrive1
Device is software WRITE PROTECTED

```

Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	0	0	0
Other IRP's	0	0	0
Read CDB's	27	0	27
Write CDB's	0	0	0
Other CDB's	0	0	0
Vendor Specific CDB's	0	0	0
Undefined CDB's	0	0	0

9.2.4. Hard disk hash results

Drive Identification	Computed	SHA1 Value
\\.\PhysicalDrive1 (CFTT-119)	Before	FBA020AEEC67FF23C40C8BFB5F55DEDBB76385D5
	After	FBA020AEEC67FF23C40C8BFB5F55DEDBB76385D5

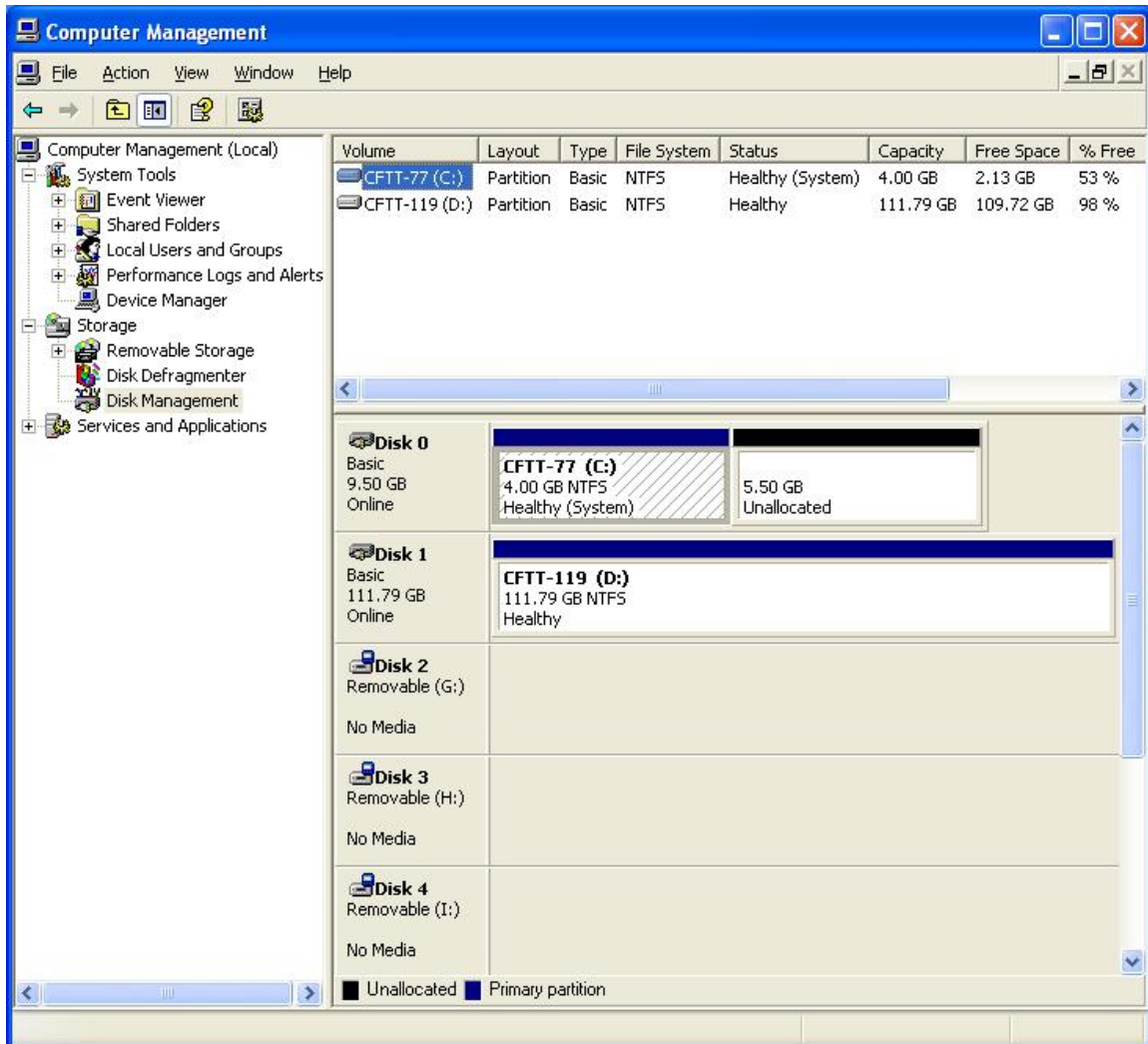
9.2.5. Test result analysis

The expected result for this test was that all READ functions issued would be passed by the tool. That result was observed.

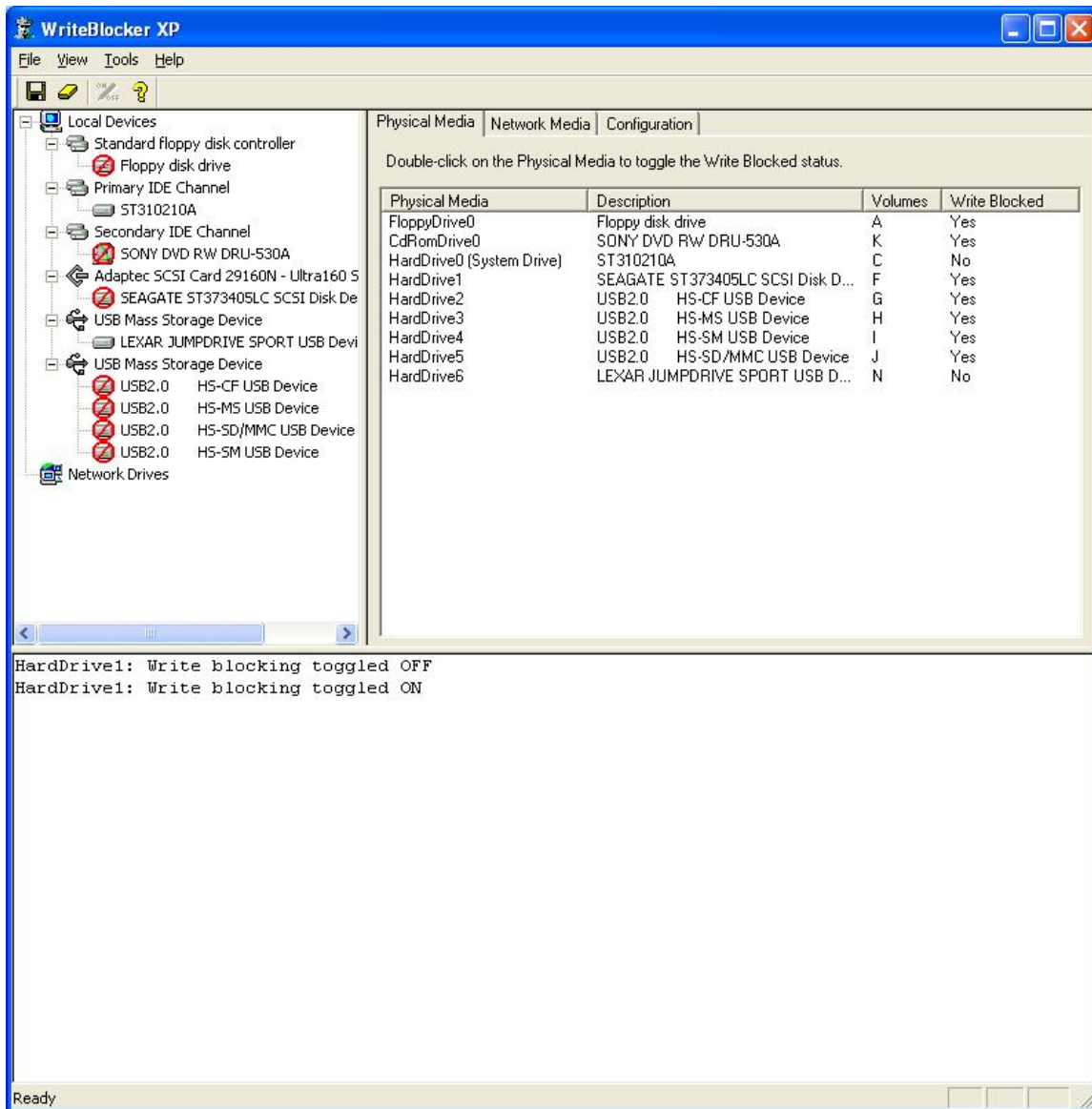
9.3 Test case SWB-03

This test case tests the tool's compliance with SWB-AM-03. It issues all possible commands from the WRITE category to a single protected disk drive. The expected result of this test is that the tool will block all commands issued by the test application.

9.3.1. Hard disk configuration



9.3.2. Write blocker configuration



9.3.3. Test output summary

NIST Software Write Blocker Test Suite V1.2

Thu Aug 25 10:09:52 2005

Test case: SWB-03
Command set: W
Number of drives: 1
Protection pattern: P
Test administered by: DPA
Details logged to file: SWB-03.log

**** Test results summary (see logfile for details) ****

Testing device \\.\PhysicalDrive1
Device is software WRITE PROTECTED

Test Category	Allowed	Blocked	Total
Read IRP's	0	0	0
Write IRP's	4	4	8
Other IRP's	0	0	0
Read CDB's	0	0	0
Write CDB's	22	12	34
Other CDB's	0	0	0
Vendor Specific CDB's	0	0	0
Undefined CDB's	0	0	0

9.3.4. Hard disk hash results

Drive Identification	Computed	SHA1 Value
\\.\PhysicalDrive1 (CFTT-119)	Before	FBA020AEEC67FF23C40C8BFB5F55DEDBB76385D5
	After	FBA020AEEC67FF23C40C8BFB5F55DEDBB76385D5

9.3.5. Test result analysis

- The tool failed to produce the expected result
- The hard disk was not modified
- The tool failed to block four of the eight IRP major functions from the WRITE category that were issued. These IRP functions are:

IRP Major Function Name	Opcode	Comment
IRP_MJ_CREATE	0x00	Appears to be blocked at file system level.
IRP_MJ_FLUSH_BUFFERS	0x09	Appears to be blocked at file system level
IRP_MJ_SET_SECURITY	0x15	Appears to be blocked at file system level
IRP_MJ_SET_QUOTA	0x1A	Appears to be blocked at file system level

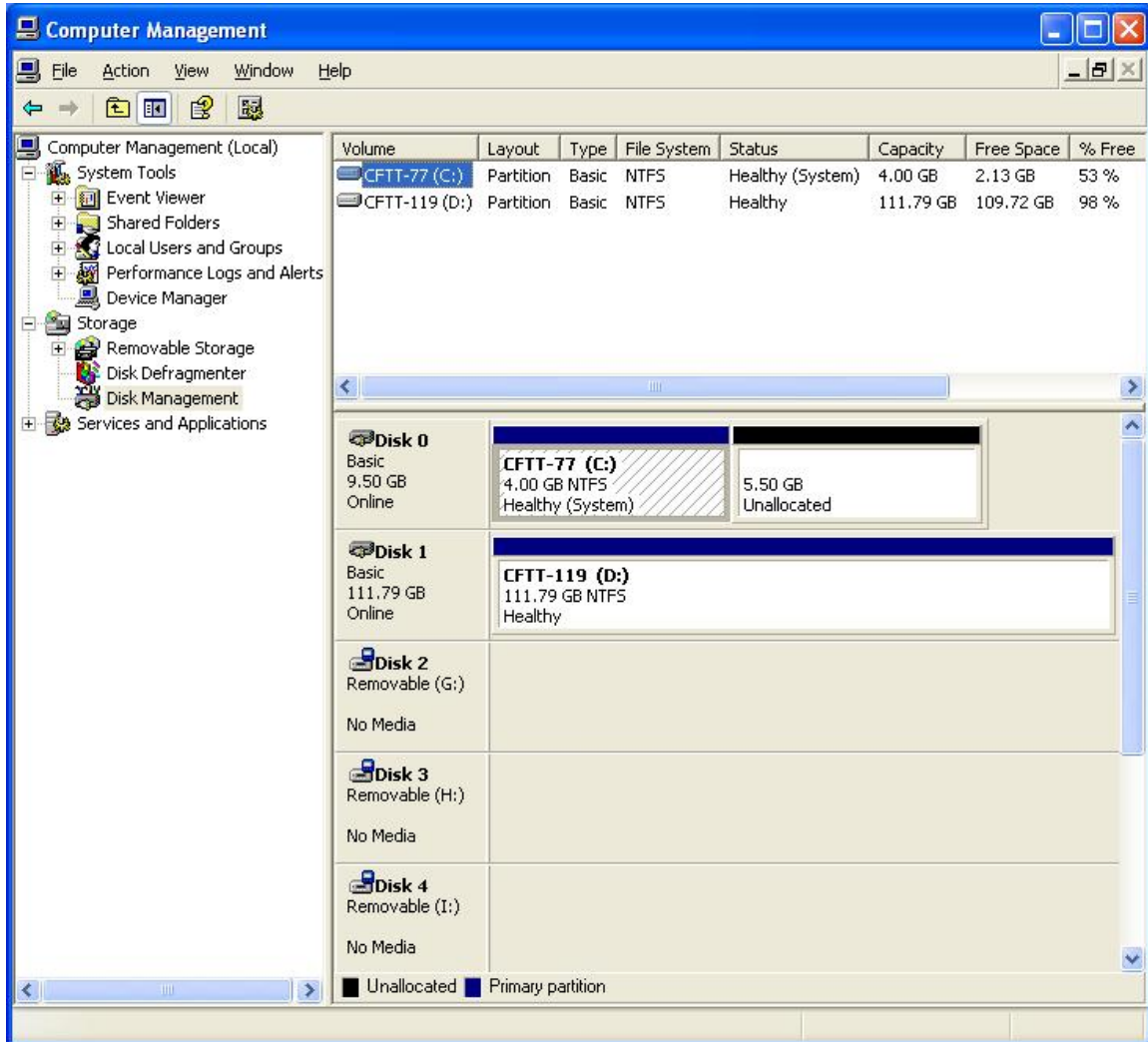
- The tool also failed to block 22 of the 34 SCSI CDB's in the WRITE category issued by the test application. The 22 SCSI commands that were not blocked by the tool are:

SCSI Command Name	Opcode	Comment
REASSIGN_BLOCKS	0x07	Optional for hard drives
WRITE_FILEMARKS	0x10	Vendor specific implementation for hard drives
COPY	0x18	Obsolete command
ERASE	0x19	Vendor specific implementation for hard drives
COPY_COMPARE	0x3A	Optional per SPC3
WRITE_LONG10	0x3F	Optional per SPC3
WRITE_SAME10	0x41	Optional per SPC3
XDWRITE10	0x50	Optional per SPC3
XPWRITE10	0x51	Optional per SPC3
SEND_CUE_SHEET	0x5D	CDROM drives
VARIABLE_LENGTH_CDB	0x7F	Encapsulates multiple variable length CDB's
XDWRITE_EXTENDED	0x80	
REBUILD	0x81	
REGENERATE	0x82	
EXTENDED_COPY	0x83	
ATA_PASSTHROUGH16	0x85	SCSI wrapper for any raw ATA command
WRITE16	0x8A	
WRITE_AND_VERIFY16	0x8E	
SYNCHRONIZE_CACHE	0x91	
WRITE_SAME16	0x93	
ATA_PASSTHROUGH12	0xA1	SCSI wrapper for any raw ATA command
ERASE12	0xAC	Vendor specific implementation for hard drives
WRITE_AND_VERIFY12	0xAE	Optional per SPC3

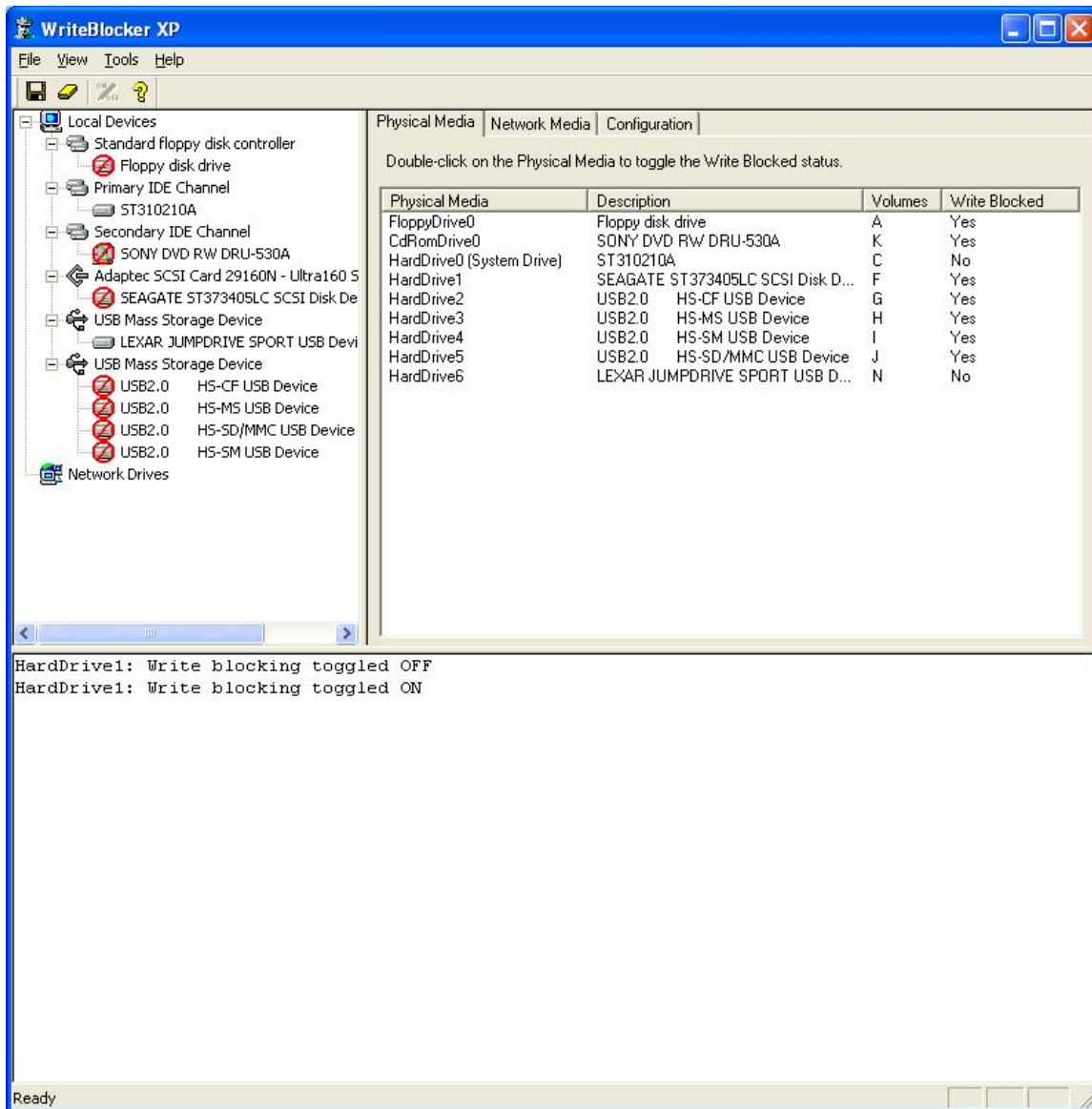
9.4 Test case SWB-04

This test case tests the tool's compliance with SWB-AM-04. It issues all possible commands from the `VENDOR_SPECIFIC` command set to a single protected disk drive. It uses the same hard drive setup as SWB-03. The expected result of this test is that the tool will block all commands issued by the test application.

9.4.1. Hard disk configuration



9.4.2. Write blocker configuration



9.4.3. Test output summary

```

NIST Software Write Blocker Test Suite V1.2
Fri Aug 26 20:47:01 2005

Test case:                SWB-04
Command set:              V
Number of drives:         1
Protection pattern:       P
Test administered by:     DPA
Details logged to file:   SWB-04.log

**** Test results summary (see logfile for details) ****

Testing device \\.\PhysicalDrive1
Device is software WRITE PROTECTED


```

Test Category	Allowed	Blocked	Total
Read IRP's	0	0	0
Write IRP's	0	0	0
Other IRP's	0	0	0
Read CDB's	0	0	0
Write CDB's	0	0	0
Other CDB's	0	0	0
Vendor SPeci fi c CDB's	80	0	80
Undefined CDB's	0	0	0

9.4.4. Hard disk hash results

Drive Identification	Computed	SHA1 Value
\\.\PhysicalDrive1 (CFTT-119)	Before	FBA020AEEC67FF23C40C8BFB5F55DEDBB76385D5
	After	FBA020AEEC67FF23C40C8BFB5F55DEDBB76385D5

9.4.5. Test results analysis

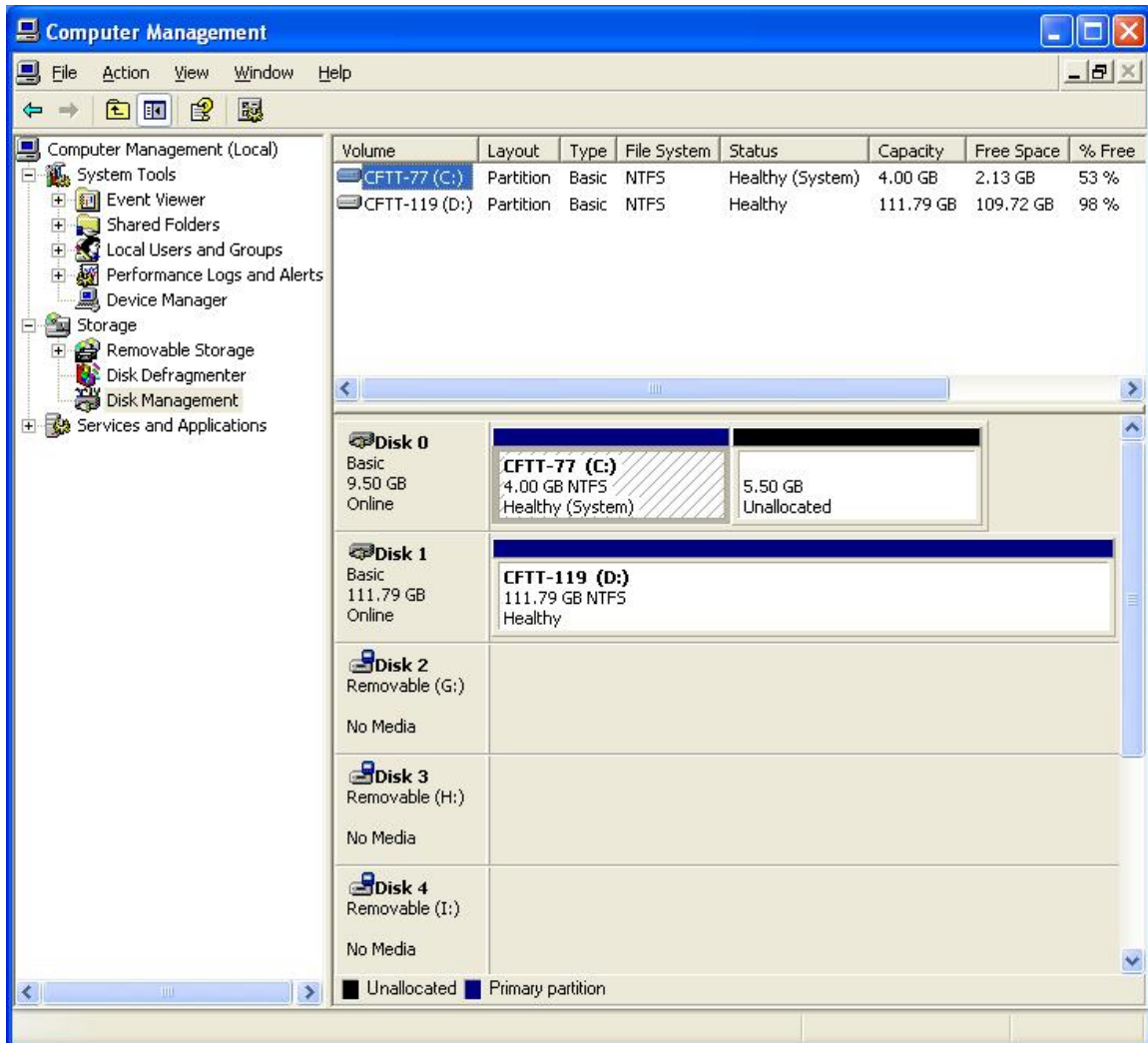
- The tool failed to produce the expected result
- The hard disk was not modified
- The tool failed to block any of the commands issued. The commands passed by the tool are shown below

SCSI Command	OPCODE	Comments
Vendor Specific	0x02	
Vendor Specific	0x06	
Vendor Specific	0x09	
Vendor Specific	0x0C	
Vendor Specific	0x0D	
Vendor Specific	0x0E	
Vendor Specific	0x0F	
Vendor Specific	0x11	
Vendor Specific	0x14	
Vendor Specific	0x20	
Vendor Specific	0x21	
Vendor Specific	0x22	
Vendor Specific	0x23	
Vendor Specific	0x26	
Vendor Specific	0x27	
Vendor Specific	0x2D	
Vendor Specific	0xC0-0xFF	All opcodes (inclusive) in this range

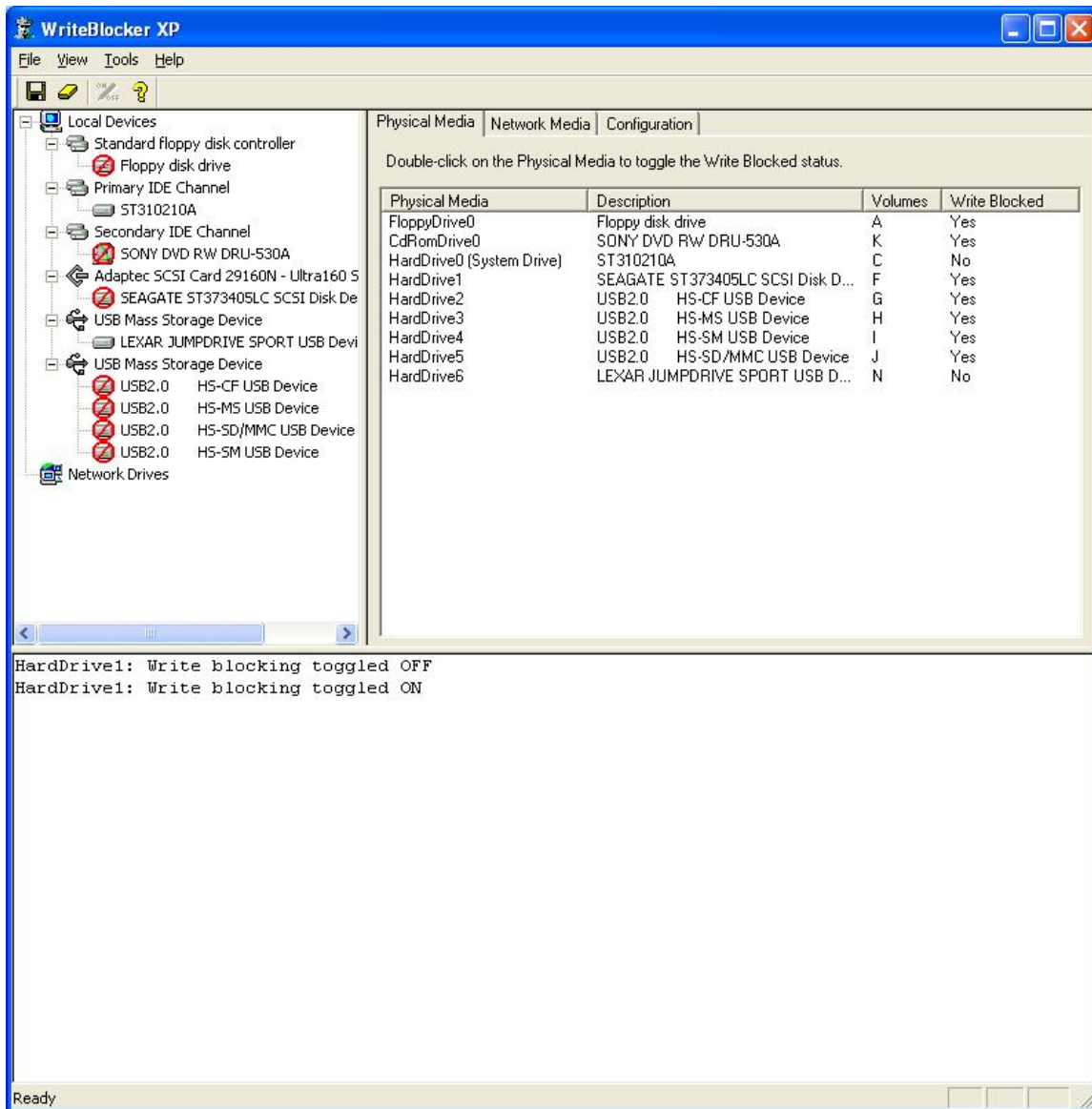
9.5 Test case SWB-05

This test case tests the tool's compliance with SWB-AM-05. It issues all possible commands from the UNDEFINED command set to a single protected disk drive. It uses the same hard drive setup as SWB-04. The expected result of this test is that the tool will block all commands issued by the test application.

9.5.1. Hard disk configuration



9.5.2. Write blocker configuration



9.5.3. Test output summary

```

NIST Software Write Blocker Test Suite V1.2
Fri Aug 26 20:47:28 2005

Test case:                SWB-05
Command set:              U
Number of drives:         1
Protection pattern:       P
Test administered by:     DPA
Details logged to file:   SWB-05.log

**** Test results summary (see logfile for details) ****

Testing device \\.\PhysicalDrive1
Device is software WRITE PROTECTED

```

Test Category	Allowed	Blocked	Total
Read IRP's	0	0	0
Write IRP's	0	0	0
Other IRP's	0	0	0
Read CDB's	0	0	0
Write CDB's	0	0	0
Other CDB's	0	0	0
Vendor Specific CDB's	0	0	0
Undefined CDB's	53	0	53

9.5.4. Hard disk hash results

Drive Identification	Computed	SHA1 Value
\\.\PhysicalDrive1 (CFTT-119)	Before	FBA020AEEC67FF23C40C8BFB5F55DEDBB76385D5
	After	FBA020AEEC67FF23C40C8BFB5F55DEDBB76385D5

9.5.5. Test results analysis

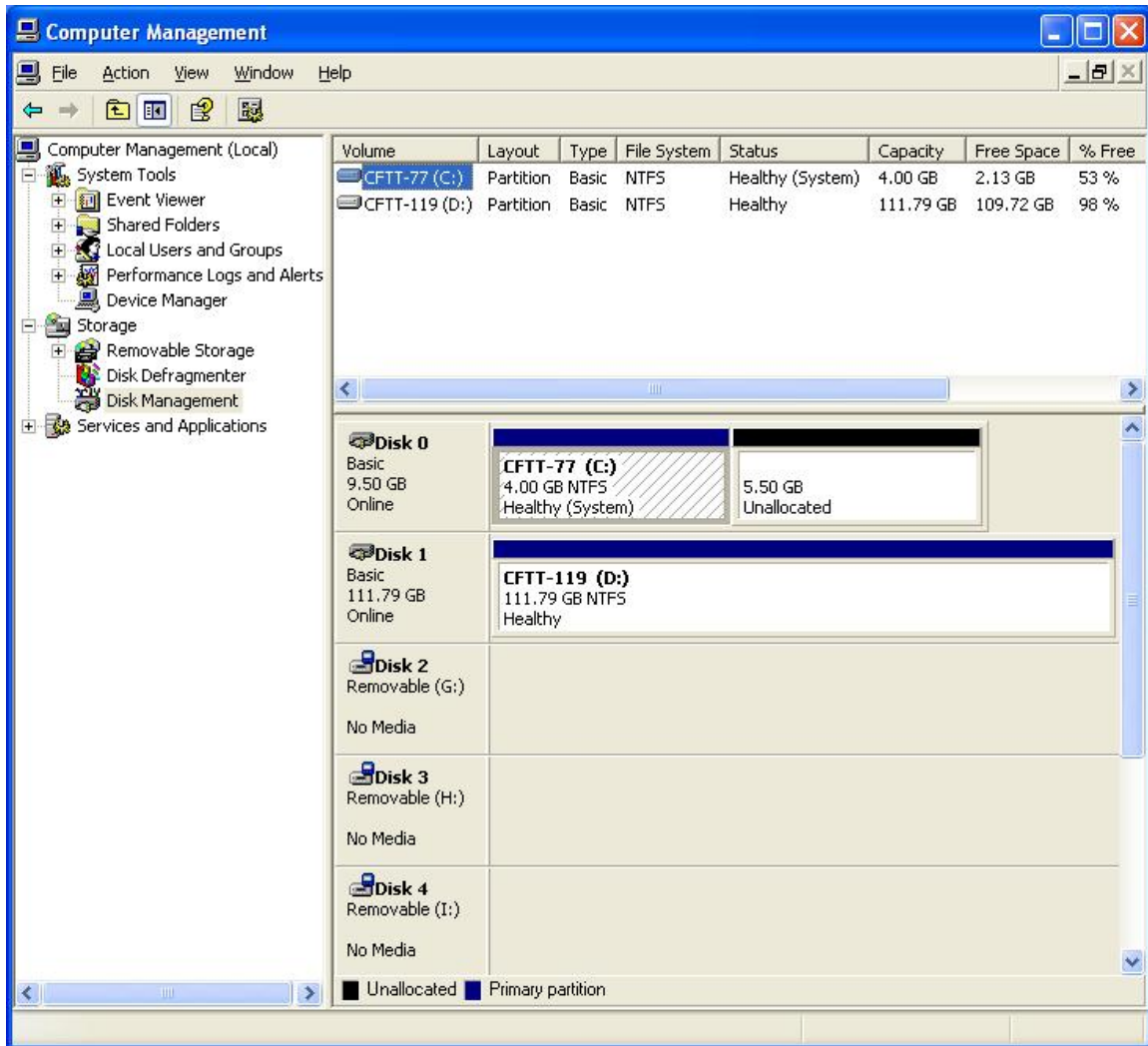
- The tool failed to produce the expected result
- The hard disk was not modified
- The tool did not block any of the commands in the UNDEFINED category. The UNDEFINED commands allowed by the tool are shown below

SCSI Command	OPCODE	Comments
Undefined	0x1F	
Undefined	0x3D	
Undefined	0x59	
Undefined	0x60-0x7E	All opcodes inclusive in this range
Undefined	0x89	
Undefined	0x8B	
Undefined	0x94	
Undefined	0x95	
Undefined	0x96	
Undefined	0x97	
Undefined	0x98	
Undefined	0x99	
Undefined	0x9A	
Undefined	0x9B	
Undefined	0x9C	
Undefined	0x9D	
Undefined	0x9E	
Undefined	0x9F	
Undefined	0xA2	
Undefined	0xA9	
Undefined	0xAB	
Undefined	0xB5	

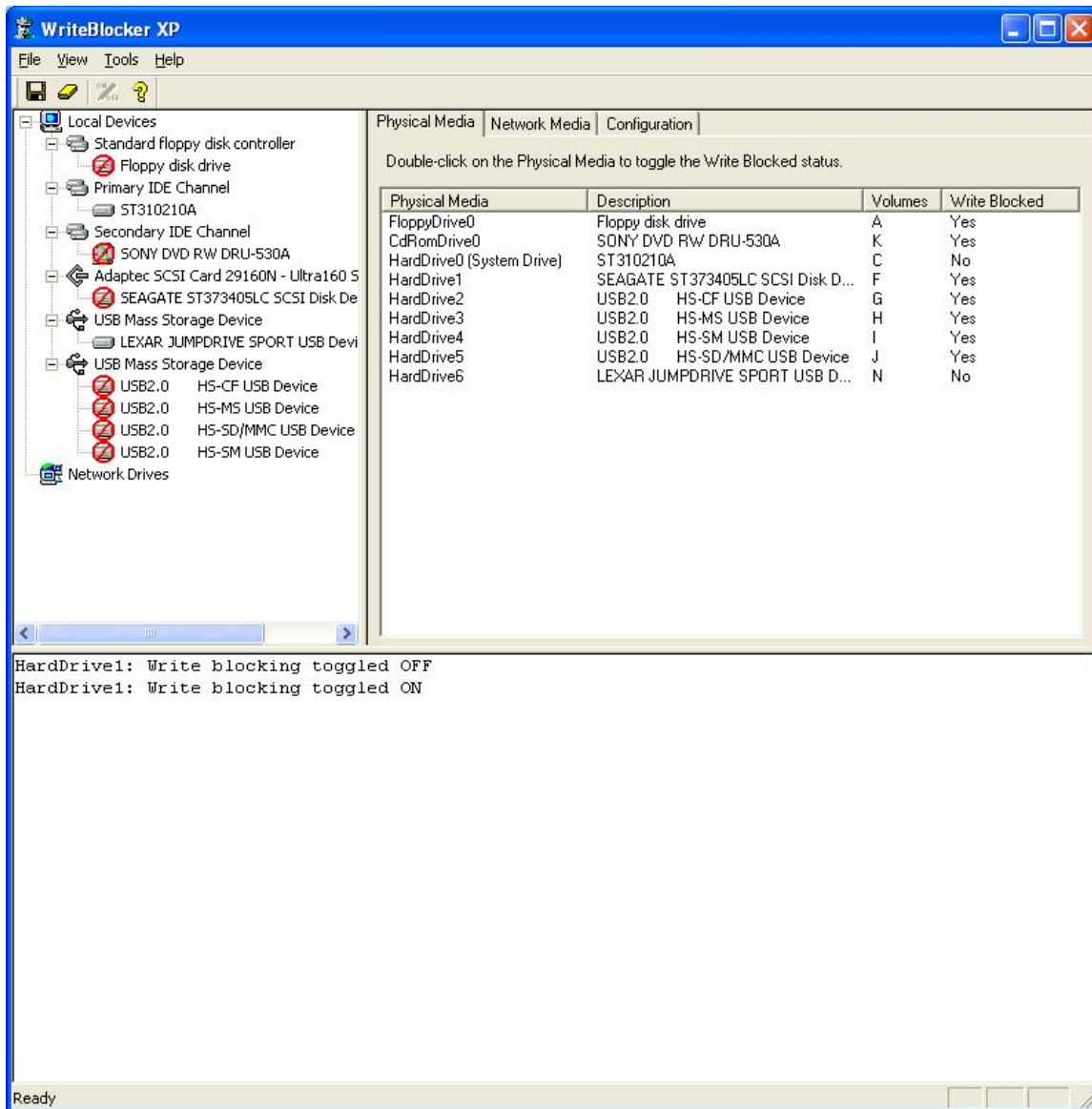
9.6 Test case SWB-06

This test case tests the tool's compliance with SWB-AM-06. It issues all possible commands from the OTHER command set to a single protected disk drive. It uses the same hard drive setup as SWB-05. The expected result of this test is that the tool will allow all commands issued by the test application.

9.6.1. Hard disk configuration



9.6.2. Write blocker configuration



9.6.3. Test output summary

NIST Software Write Blocker Test Suite V1.2

Fri Aug 26 20:48:11 2005

Test case: SWB-06
Command set: 0
Number of drives: 1
Protection pattern: P
Test administered by: DPA
Details logged to file: SWB-06.log

**** Test results summary (see logfile for details) ****

Testing device \\.\PhysicalDrive1
Device is software WRITE PROTECTED

Test Category	Allowed	Blocked	Total
Read IRP's	0	0	0
Write IRP's	0	0	0
Other IRP's	15	0	15
Read CDB's	0	0	0
Write CDB's	0	0	0
Other CDB's	62	0	62
Vendor Specific CDB's	0	0	0
Undefined CDB's	0	0	0

9.6.4. Hard disk hash results

Drive Identification	Computed	SHA1 Value
\\.\PhysicalDrive1 (CFTT-119)	Before	FBA020AEEC67FF23C40C8BFB5F55DEDBB76385D5
	After	FBA020AEEC67FF23C40C8BFB5F55DEDBB76385D5

9.6.5. Test results analysis

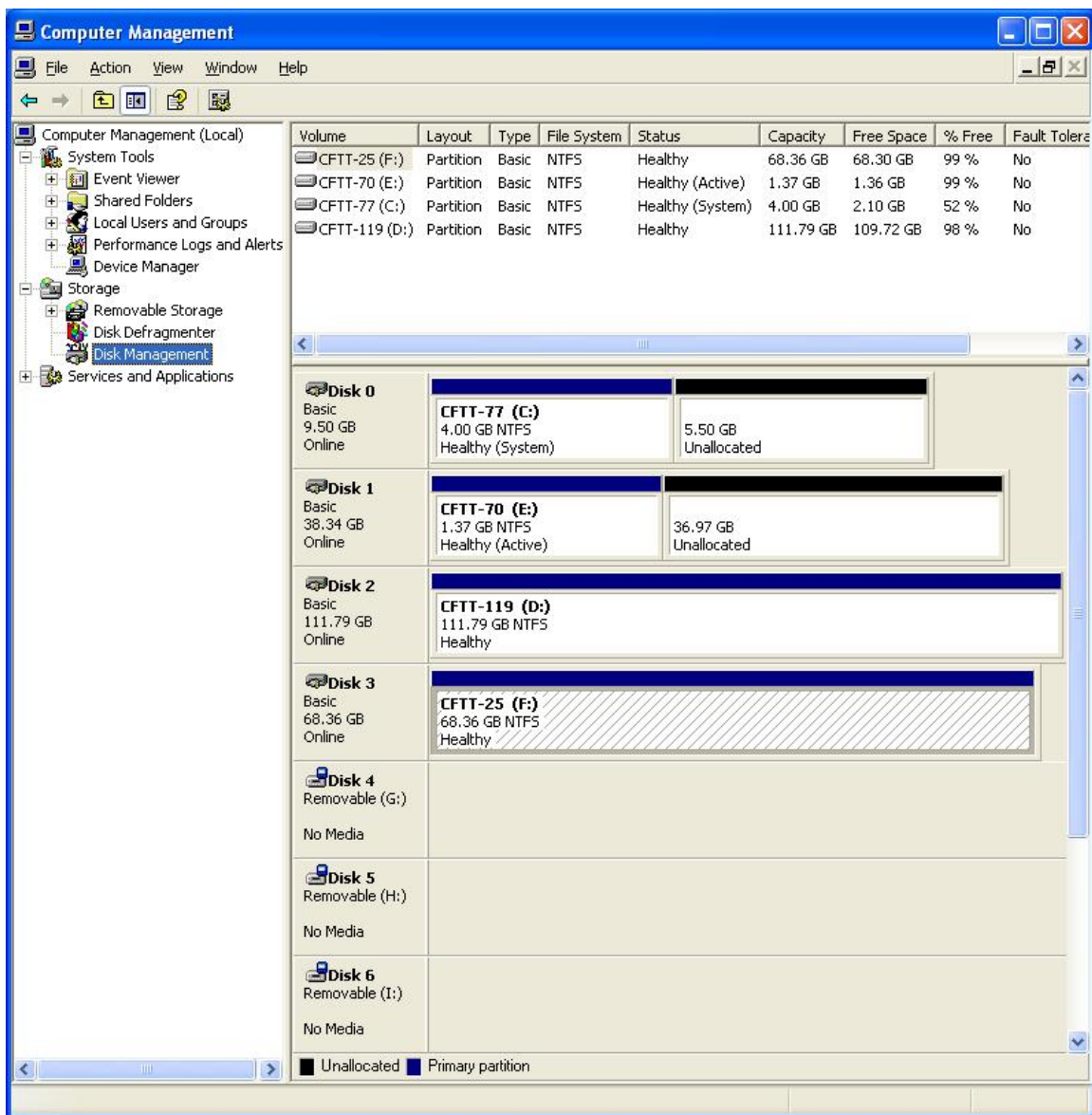
The tool produced the expected result. The tool did not block any of the commands in the OTHER category.

9.7 Test case SWB-07

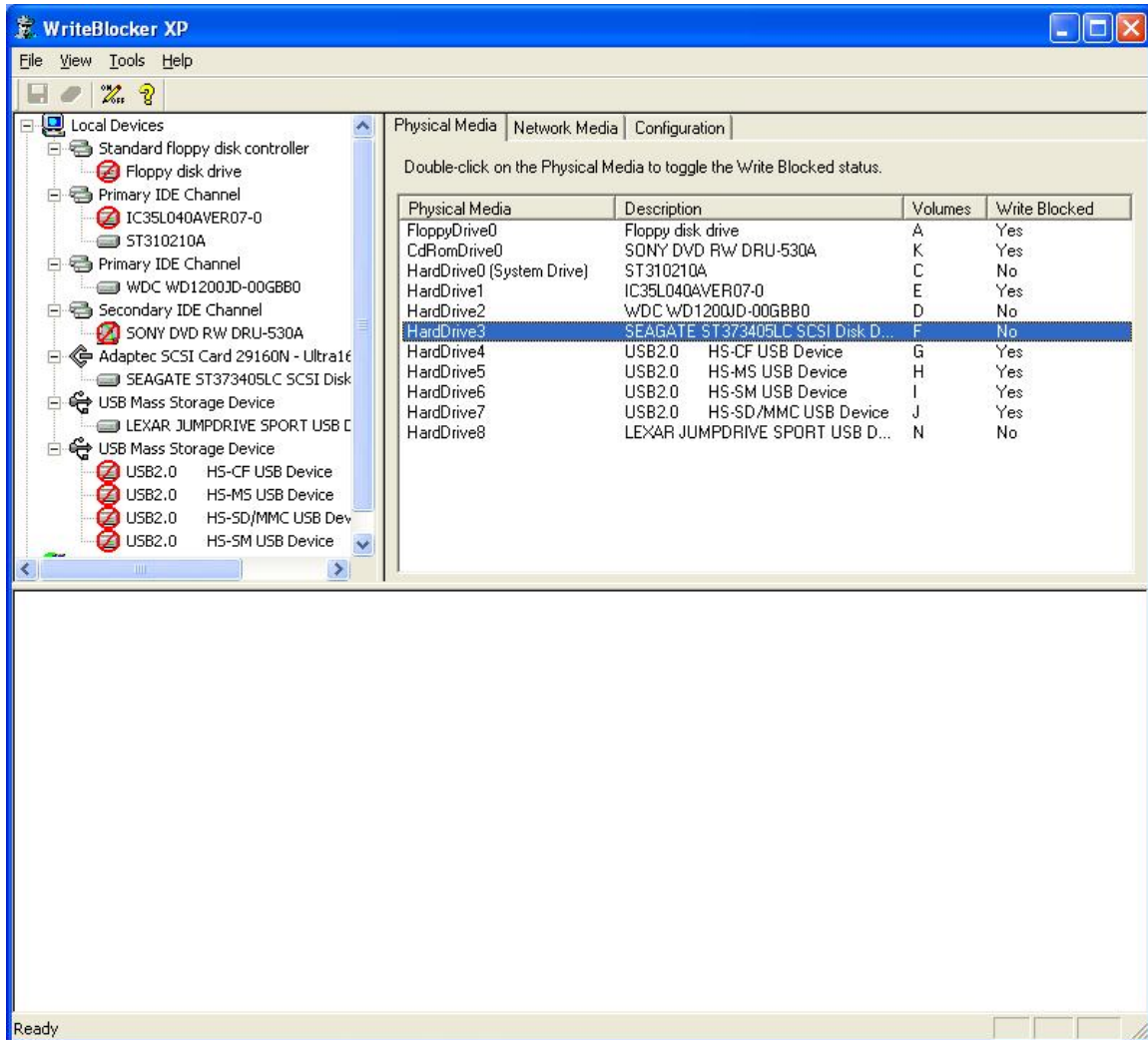
This case tests the tool's compliance with optional assertions SWB-AO-01 through SWB-AO-06. It issues all possible commands to a set of three drives protected with the pattern PUU. The expected result of this test is the tool will:

- Block all commands from the WRITE, VENDOR_SPECIFIC, and UNDEFINED categories issued to protected drives
- Pass all commands from the READ and OTHER categories issued to protected drives
- Pass all commands from all categories issued to unprotected drives

9.7.1. Hard disk configuration



9.7.2. Write blocker configuration



9.7.3. Test output summary

NIST Software Write Blocker Test Suite V1.2
Sat Aug 27 11:04:49 2005

Test case: SWB-07
Command set: RWOVU
Number of drives: 3
Protection pattern: PUU
Test administered by: DPA
Details logged to file: SWB-07.log

**** Test results summary (see logfile for details) ****

Testing device \\.\Physical Drive1
Device is software WRITE PROTECTED

Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	4	4	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	22	12	34
Other CDB's	62	0	62
Vendor SPeci fic CDB's	80	0	80
Undefined CDB's	53	0	53

Testing device \\.\Physical Drive2
Device is software WRITE ENABLED

Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	8	0	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	34	0	34
Other CDB's	62	0	62
Vendor SPeci fic CDB's	80	0	80
Undefined CDB's	53	0	53

Testing device \\.\Physical Drive3
Device is software WRITE ENABLED

Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	8	0	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	34	0	34
Other CDB's	62	0	62
Vendor SPeci fic CDB's	80	0	80
Undefined CDB's	53	0	53

9.7.4. Hard disk hash results

Drive Identification		Computed	SHA1 Value
\\.\PhysicalDrive1 (CFTT-70)	P	Before	ECD7751DB6688D7DCD72A19CC3971A73252D5588
		After	ECD7751DB6688D7DCD72A19CC3971A73252D5588
\\.\PhysicalDrive2 (CFTT-119)	U	Before	79E3AD4068FED4BB73D1E85A397B8DD0F274FF86
		After	F55DBB07965E5AB748A1D7CFD60C595794C4678C
\\.\PhysicalDrive3 (CFTT-25)	U	Before	FBA020AEEC67FF23C40C8BFB5F55DEDBB76385D5
		After	968945BA353E565D9DD53B6CAB9F8CC74563087D

9.7.5. Test results analysis

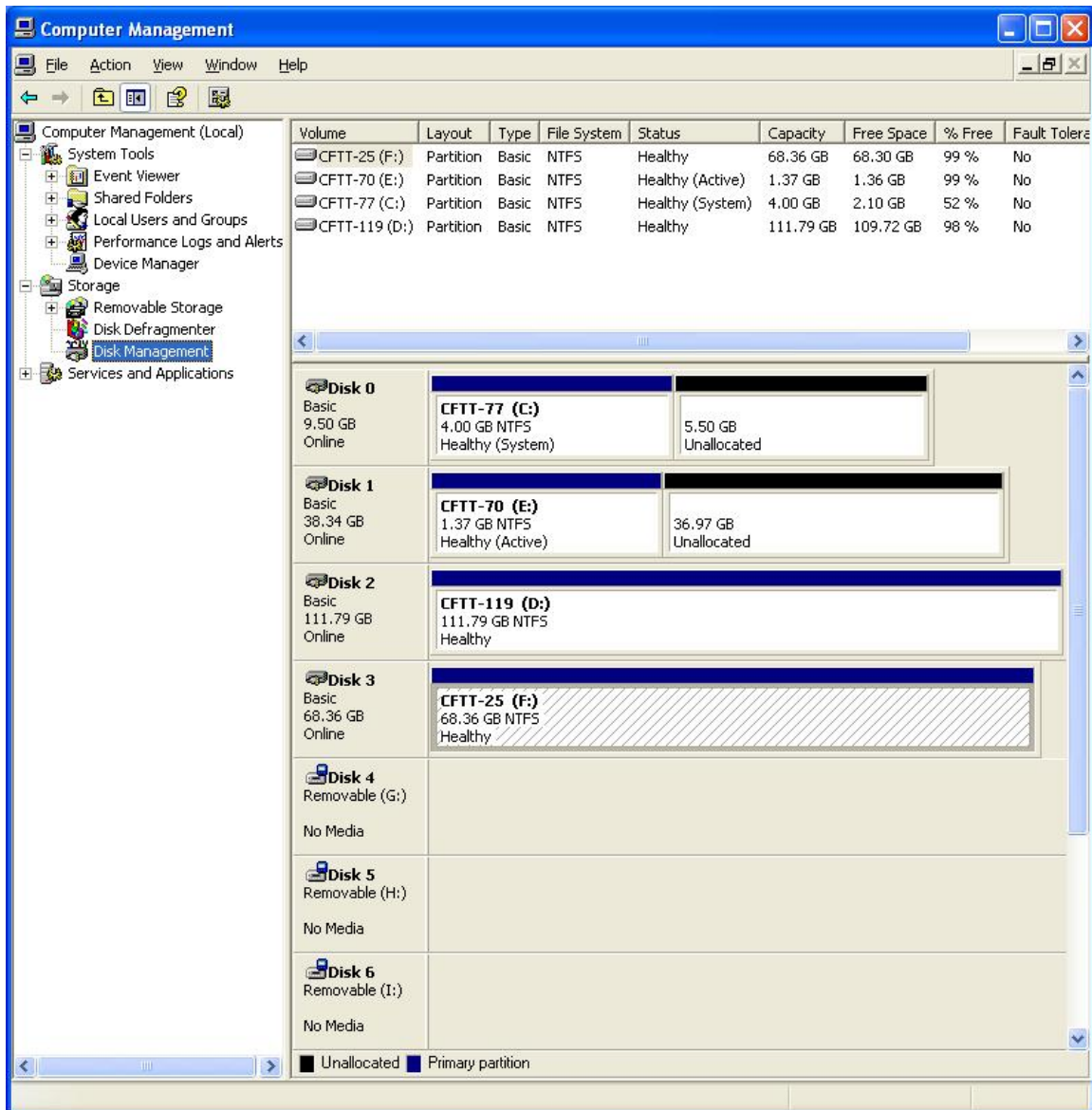
The tool failed to produce the expected result. The number of drives configured and the pattern of protection applied did not alter the ability of the tool to protect designated drives. However, the tool failed to block all commands in the protected categories. The protection failures observed were identical to those of tests SWB-03, SWB-04, and SWB-06.

9.8 Test case SWB-08

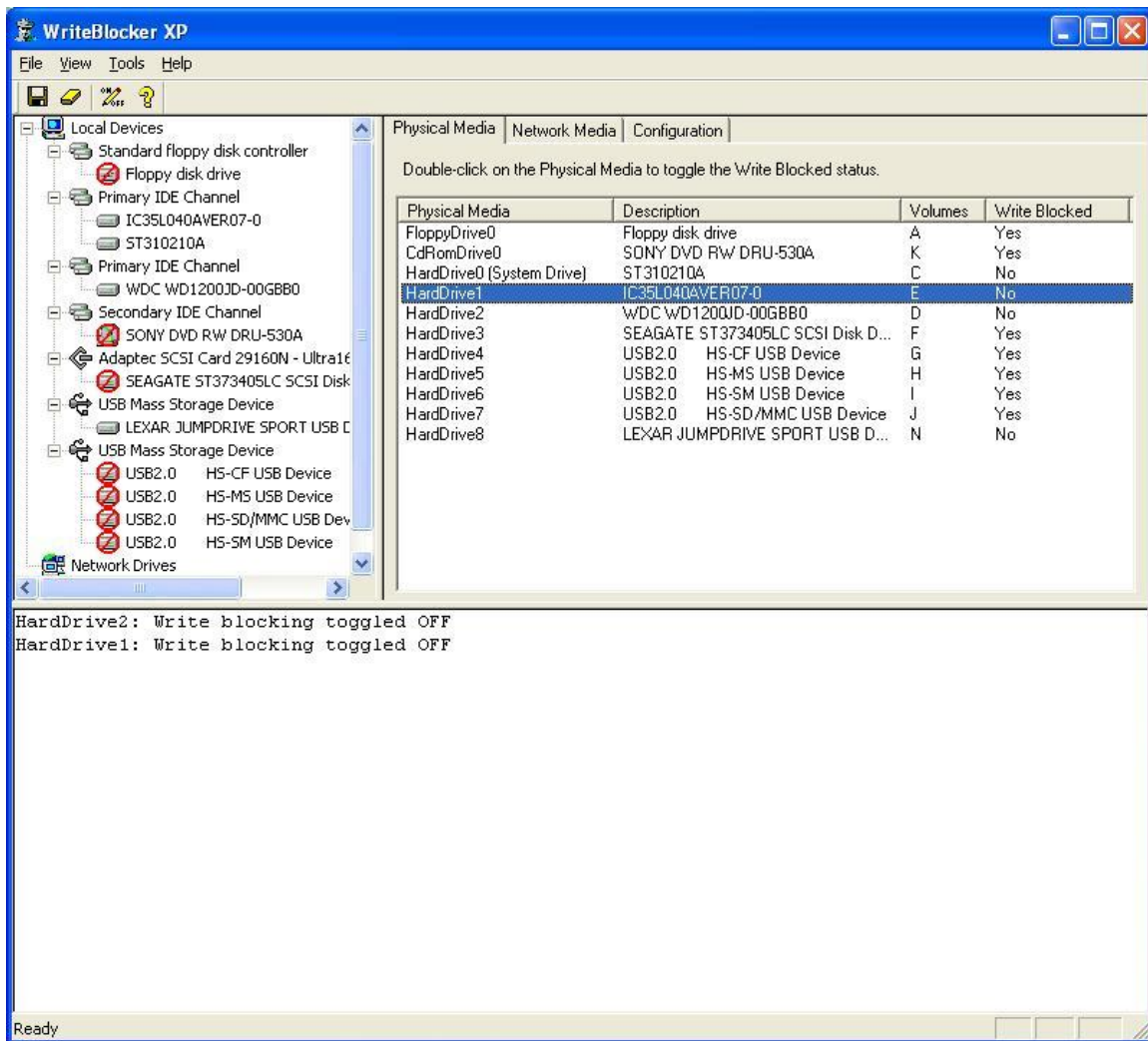
This case tests the tool's compliance with optional assertions SWB-AO-01 through SWB-AO-06. It issues all possible commands to a set of three drives protected with the pattern UPU. The expected result of this test is the tool will:

- Block all commands from the WRITE, VENDOR_SPECIFIC, and UNDEFINED categories issued to protected drives
- Pass all commands from the READ and OTHER categories issued to protected drives
- Pass all commands from all categories issued to unprotected drives

9.8.1. Hard disk configuration



9.8.2. Write blocker configuration



9.8.3. Test output summary

NIST Software Write Blocker Test Suite V1.2
Sun Aug 28 09:58:45 2005

Test case: SWB-08
Command set: RWOVU
Number of drives: 3
Protection pattern: UPU
Test administered by: DPA
Details logged to file: SWB-08.log

**** Test results summary (see logfile for details) ****

Testing device \\.\Physical Drive1
Device is software WRITE ENABLED

Test Category	Allowed	Blocked	Total
---------------	---------	---------	-------

Read IRP's	4	0	4
Write IRP's	8	0	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	34	0	34
Other CDB's	62	0	62
Vendor SPeci fi c CDB's	80	0	80
Unde fi ned CDB's	53	0	53
Testing device \\.\Physical Drive2 Device is software WRITE PROTECTED			
Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	4	4	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	22	12	34
Other CDB's	62	0	62
Vendor SPeci fi c CDB's	80	0	80
Unde fi ned CDB's	53	0	53
Testing device \\.\Physical Drive3 Device is software WRITE ENABLED			
Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	8	0	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	34	0	34
Other CDB's	62	0	62
Vendor SPeci fi c CDB's	80	0	80
Unde fi ned CDB's	53	0	53

9.8.4. Hard disk hash results

Drive Identification		Computed	SHA1 Value
\\.\PhysicalDrive1 (CFTT-70)	U	Before	ECD7751DB6688D7DCD72A19CC3971A73252D5588
		After	6C557AF418DDC0110D55DA3D5F5C33A1BB9164E4
\\.\PhysicalDrive2 (CFTT-119)	P	Before	F55DBB07965E5AB748A1D7CFD60C595794C4678C
		After	F55DBB07965E5AB748A1D7CFD60C595794C4678C
\\.\PhysicalDrive3 (CFTT-25)	U	Before	968945BA353E565D9DD53B6CAB9F8CC74563087D
		After	F55DBB07965E5AB748A1D7CFD60C595794C4678C

9.8.5. Test results analysis

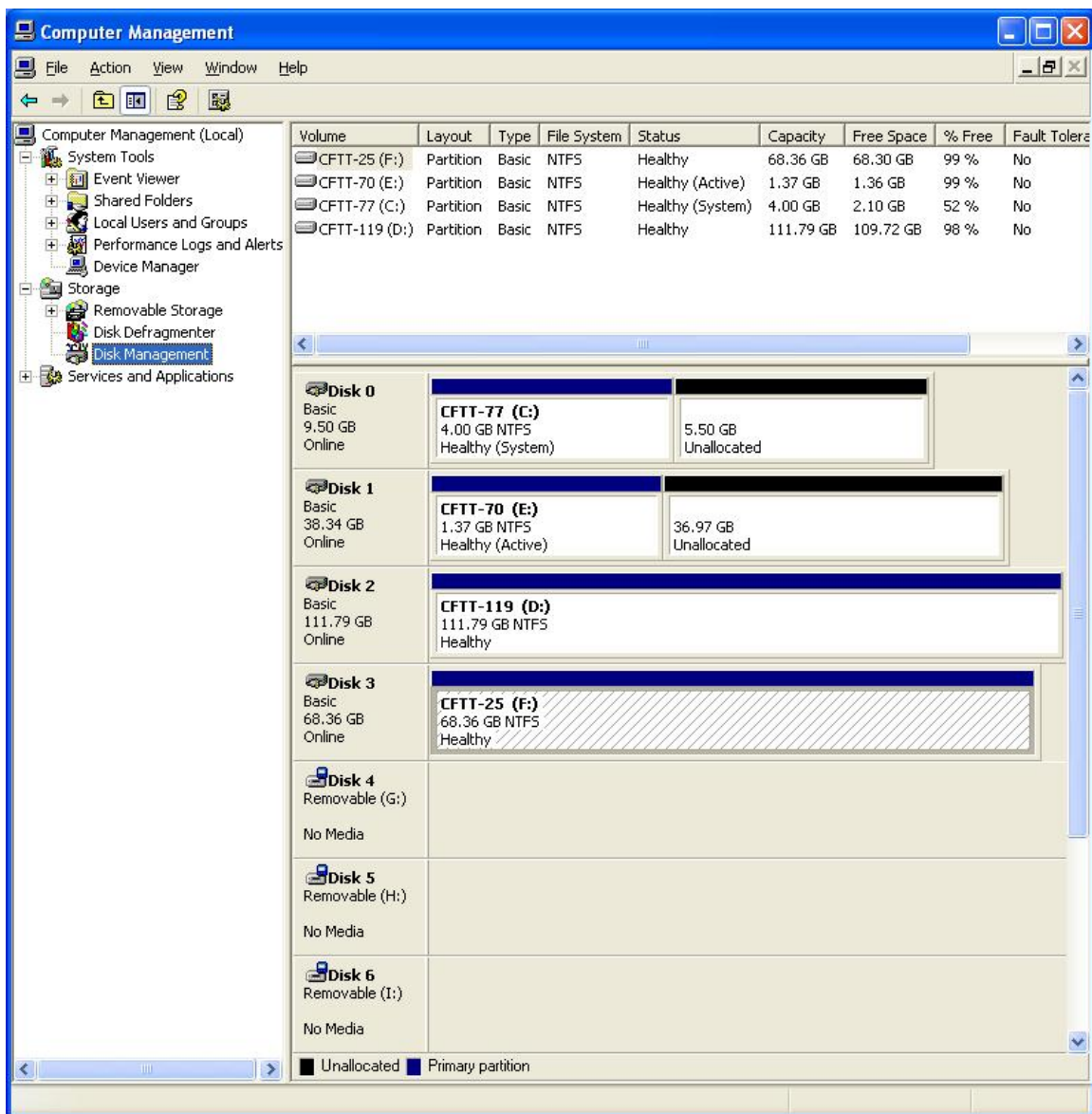
The tool failed to produce the expected result. The number of drives configured and the pattern of protection applied did not alter the ability of the tool to protect designated drives. However, the tool failed to block all commands in the protected categories. The protection failures observed were identical to those of tests SWB-03, SWB-04, and SWB-06.

9.9 Test case SWB-09

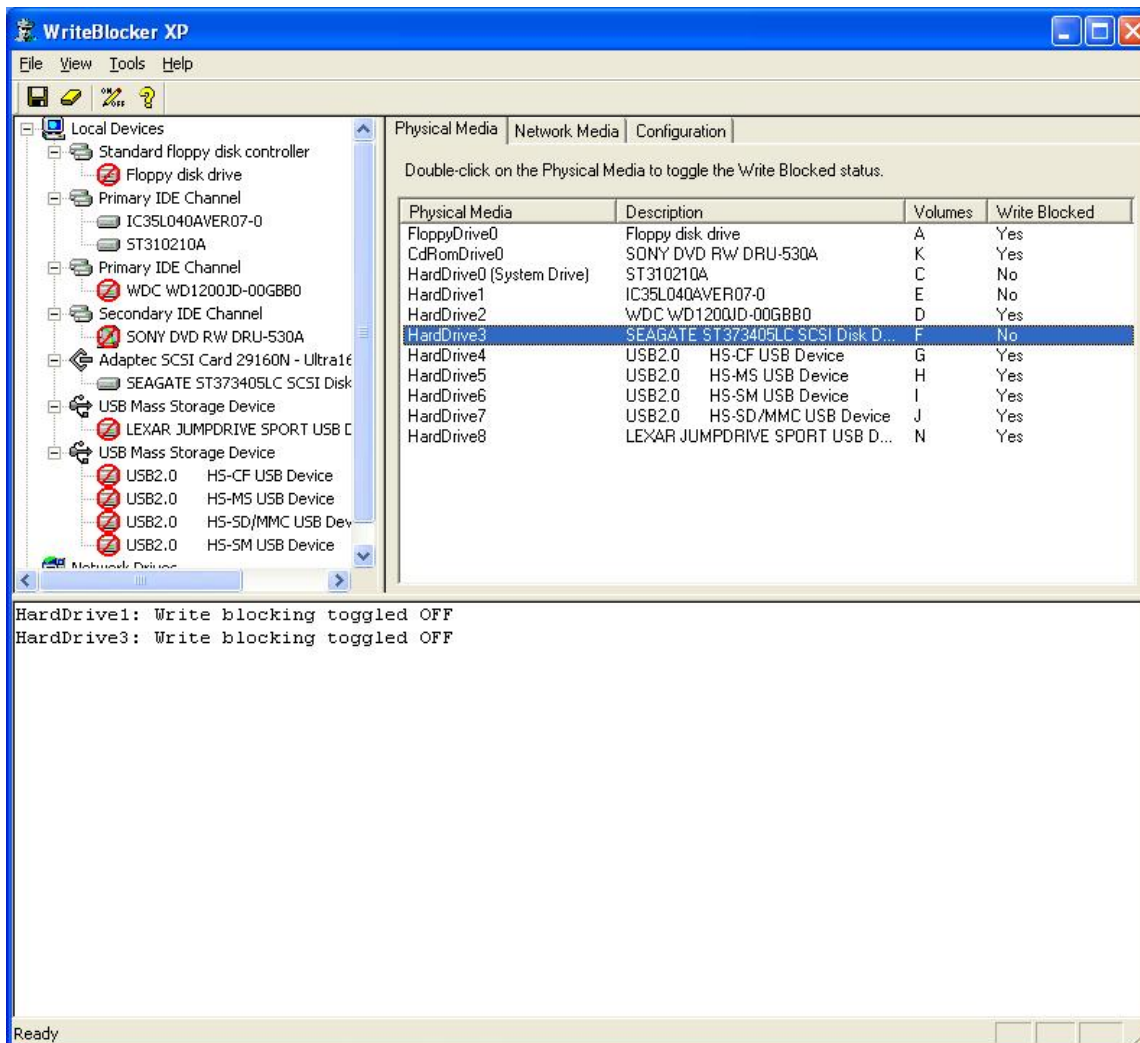
This case tests the tool's compliance with optional assertions SWB-AO-01 through SWB-AO-06. It issues all possible commands to a set of three drives protected with the pattern UUP. The expected result of this test is the tool will:

- Block all commands from the WRITE, VENDOR_SPECIFIC, and UNDEFINED categories issued to protected drives
- Pass all commands from the READ and OTHER categories issued to protected drives
- Pass all commands from all categories issued to unprotected drives

9.9.1. Hard disk configuration



9.9.2. Write blocker configuration



9.9.3. Test output summary

NIST Software Write Blocker Test Suite V1.2
Sun Aug 28 11:27:37 2005

Test case: SWB-09
Command set: RWOVU
Number of drives: 3
Protection pattern: UUP
Test administered by: DPA
Details logged to file: SWB-09.log

**** Test results summary (see logfile for details) ****

Testing device \\.\Physical Drive1
Device is software WRITE ENABLED

Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	8	0	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	34	0	34
Other CDB's	62	0	62
Vendor Specific CDB's	80	0	80
Undefined CDB's	53	0	53
Testing device \\.\PhysicalDrive2 Device is software WRITE ENABLED			
Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	8	0	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	34	0	34
Other CDB's	62	0	62
Vendor Specific CDB's	80	0	80
Undefined CDB's	53	0	53
Testing device \\.\PhysicalDrive3 Device is software WRITE PROTECTED			
Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	4	4	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	22	12	34
Other CDB's	62	0	62
Vendor Specific CDB's	80	0	80
Undefined CDB's	53	0	53

9.9.4. Hard disk hash results

Drive Identification		Computed	SHA1 Value
\\.\PhysicalDrive1 (CFTT-70)	U	Before	6C557AF418DDC0110D55DA3D5F5C33A1BB9164E4
		After	297878E0CDBDDAA955896F791157A3A3330182B5
\\.\PhysicalDrive2 (CFTT-119)	U	Before	F55DBB07965E5AB748A1D7CFD60C595794C4678C
		After	04CBBEED33C996296E6EAE2568D7B0C1140F4AF2
\\.\PhysicalDrive3 (CFTT-25)	P	Before	C2858F133AA1241976AFA91BE124B9E58138533B
		After	C2858F133AA1241976AFA91BE124B9E58138533B

9.9.5. Test results analysis

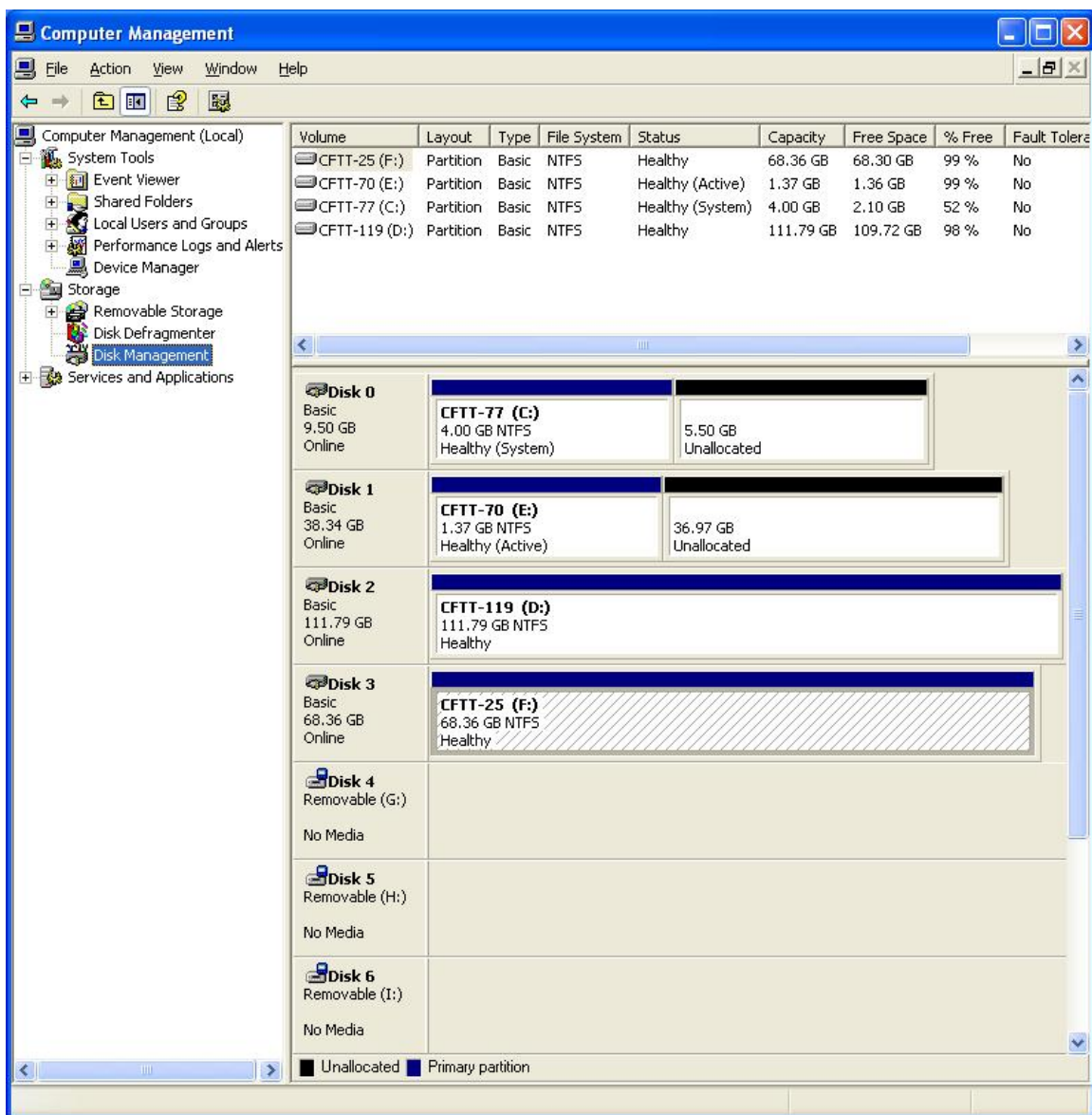
The tool failed to produce the expected result. The number of drives configured and the pattern of protection applied did not alter the ability of the tool to protect designated drives. However, the tool failed to block all commands in the protected categories. The protection failures observed were identical to those of tests SWB-03, SWB-04, and SWB-06.

9.10 Test case SWB-10

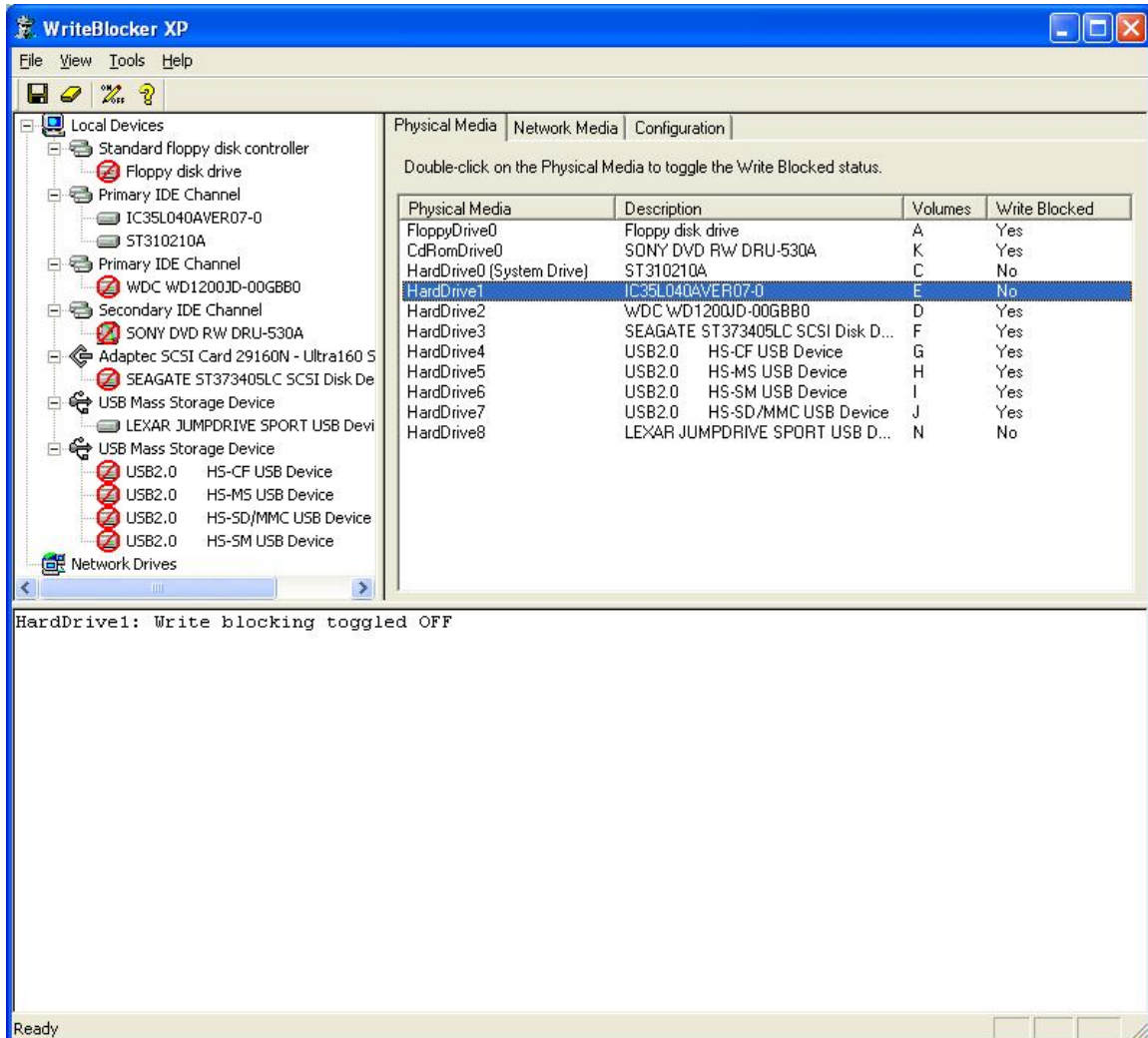
This case tests the tool's compliance with optional assertions SWB-AO-01 through SWB-AO-06. It issues all possible commands to a set of three drives protected with the pattern UPP. The expected result of this test is the tool will:

- Block all commands from the WRITE, VENDOR_SPECIFIC, and UNDEFINED categories issued to protected drives
- Pass all commands from the READ and OTHER categories issued to protected drives
- Pass all commands from all categories issued to unprotected drives

9.10.1. Hard disk configuration



9.10.2. Write blocker configuration



9.10.3. Test output summary

NIST Software Write Blocker Test Suite V1.2

Sun Aug 28 12:38:03 2005

Test case: SWB-10
Command set: RWOVU
Number of drives: 3
Protection pattern: UPP
Test administered by: DPA
Details logged to file: SWB-10.log

**** Test results summary (see logfile for details) ****

Testing device \\.\PhysicalDrive1

Device is software WRITE ENABLED

Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	8	0	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	34	0	34
Other CDB's	62	0	62
Vendor Specific CDB's	80	0	80
Undefined CDB's	53	0	53

Testing device \\.\PhysicalDrive2

Device is software WRITE PROTECTED

Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	4	4	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	22	12	34
Other CDB's	62	0	62
Vendor Specific CDB's	80	0	80
Undefined CDB's	53	0	53

Testing device \\.\PhysicalDrive3

Device is software WRITE PROTECTED

Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	4	4	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	22	12	34
Other CDB's	62	0	62
Vendor Specific CDB's	80	0	80
Undefined CDB's	53	0	53

9.10.4. Hard disk hash results

Drive Identification		Computed	SHA1 Value
\\.\PhysicalDrive1 (CFTT-70)	U	Before	297878E0CDBDDAA955896F791157A3A3330182B5
		After	6B60F2CF1391DE31D795318E2074670FF6646EE0
\\.\PhysicalDrive2 (CFTT-119)	P	Before	04CBBEED33C996296E6EAE2568D7B0C1140F4AF2
		After	04CBBEED33C996296E6EAE2568D7B0C1140F4AF2
\\.\PhysicalDrive3 (CFTT-25)	P	Before	C2858F133AA1241976AFA91BE124B9E58138533B
		After	C2858F133AA1241976AFA91BE124B9E58138533B

9.10.5. Test results analysis

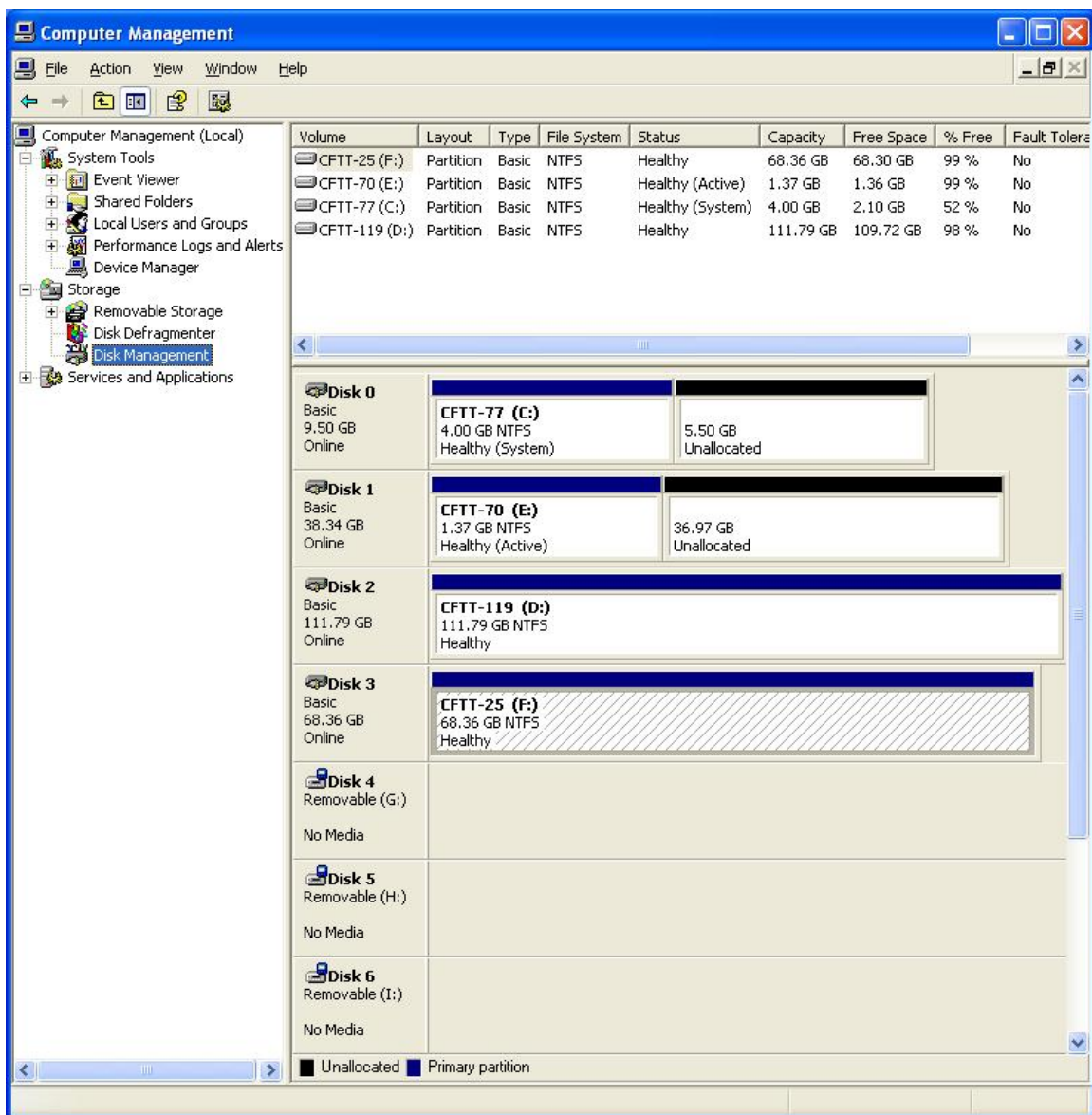
The tool failed to produce the expected result. The number of drives configured and the pattern of protection applied did not alter the ability of the tool to protect designated drives. However, the tool failed to block all commands in the protected categories. The protection failures observed were identical to those of tests SWB-03, SWB-04, and SWB-06.

9.11 Test case SWB-11

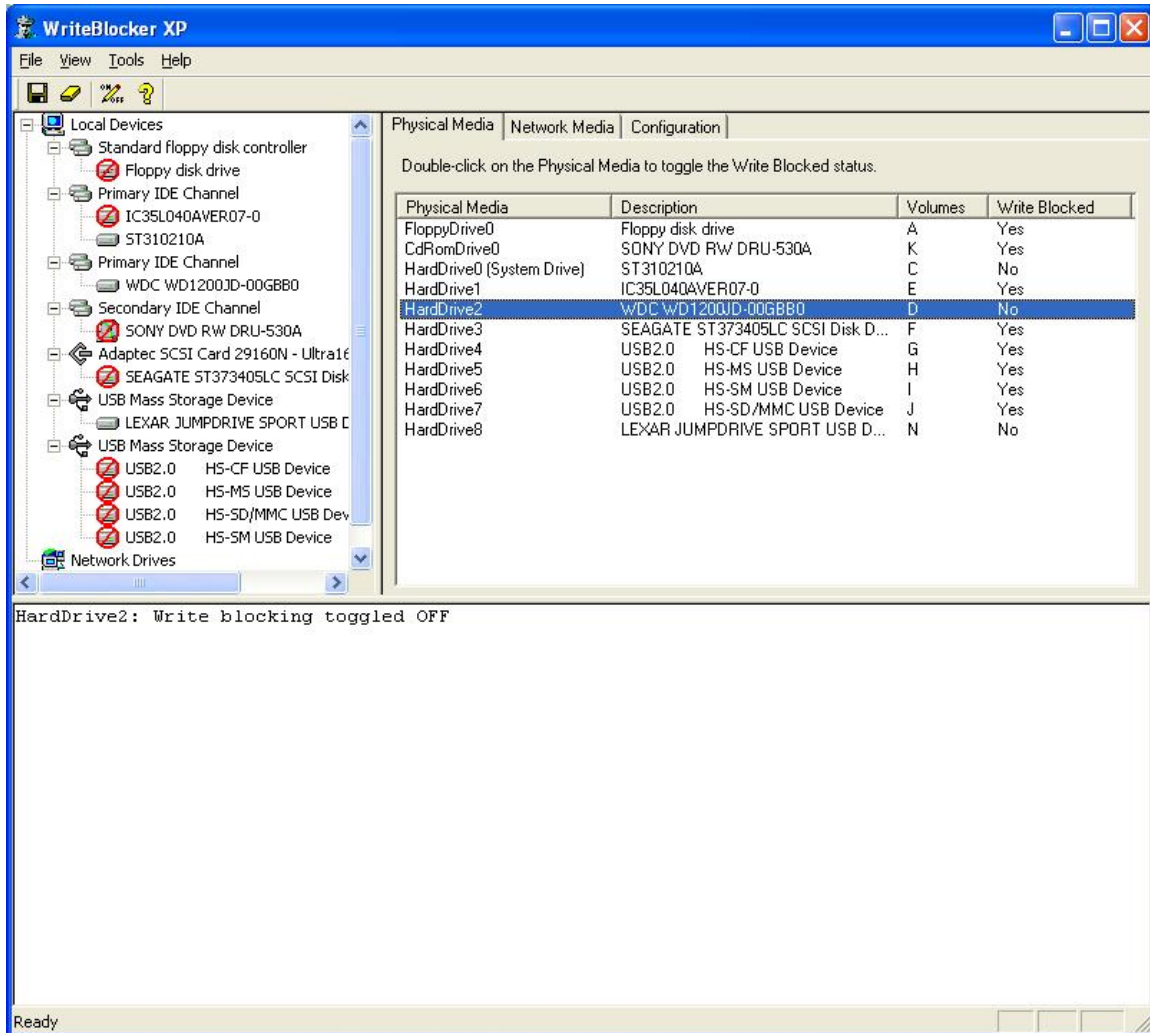
This case tests the tool's compliance with optional assertions SWB-AO-01 through SWB-AO-06. It issues all possible commands to a set of three drives protected with the pattern PUP. The expected result of this test is the tool will:

- Block all commands from the WRITE, VENDOR_SPECIFIC, and UNDEFINED categories issued to protected drives
- Pass all commands from the READ and OTHER categories issued to protected drives
- Pass all commands from all categories issued to unprotected drives

9.11.1. Hard disk configuration



9.11.2. Write blocker configuration



9.11.3. Test output summary

NI ST Software Write Blocker Test Suite V1.2
Sun Aug 28 14:04:40 2005

Test case: SWB-11
Command set: RWOVU
Number of drives: 3
Protection pattern: PUP
Test administered by: DPA
Details logged to file: SWB-11.log

**** Test results summary (see logfile for details) ****

Testing device \\.\Physical Drive1
Device is software WRITE PROTECTED

Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	4	4	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	22	12	34
Other CDB's	62	0	62
Vendor Specific CDB's	80	0	80
Undefined CDB's	53	0	53
Testing device \\.\PhysicalDrive2 Device is software WRITE ENABLED			
Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	8	0	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	34	0	34
Other CDB's	62	0	62
Vendor Specific CDB's	80	0	80
Undefined CDB's	53	0	53
Testing device \\.\PhysicalDrive3 Device is software WRITE PROTECTED			
Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	4	4	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	22	12	34
Other CDB's	62	0	62
Vendor Specific CDB's	80	0	80
Undefined CDB's	53	0	53

9.11.4. Hard disk hash results

Drive Identification		Computed	SHA1 Value
\\.\PhysicalDrive1 (CFTT-70)	P	Before	6B60F2CF1391DE31D795318E2074670FF6646EE0
		After	6B60F2CF1391DE31D795318E2074670FF6646EE0
\\.\PhysicalDrive2 (CFTT-119)	U	Before	04CBBEED33C996296E6EAE2568D7B0C1140F4AF2
		After	98CB37515F44BF652BF620B1869EADE0C9D7A8ED
\\.\PhysicalDrive3 (CFTT-25)	P	Before	C2858F133AA1241976AFA91BE124B9E58138533B
		After	C2858F133AA1241976AFA91BE124B9E58138533B

9.11.5. Test results analysis

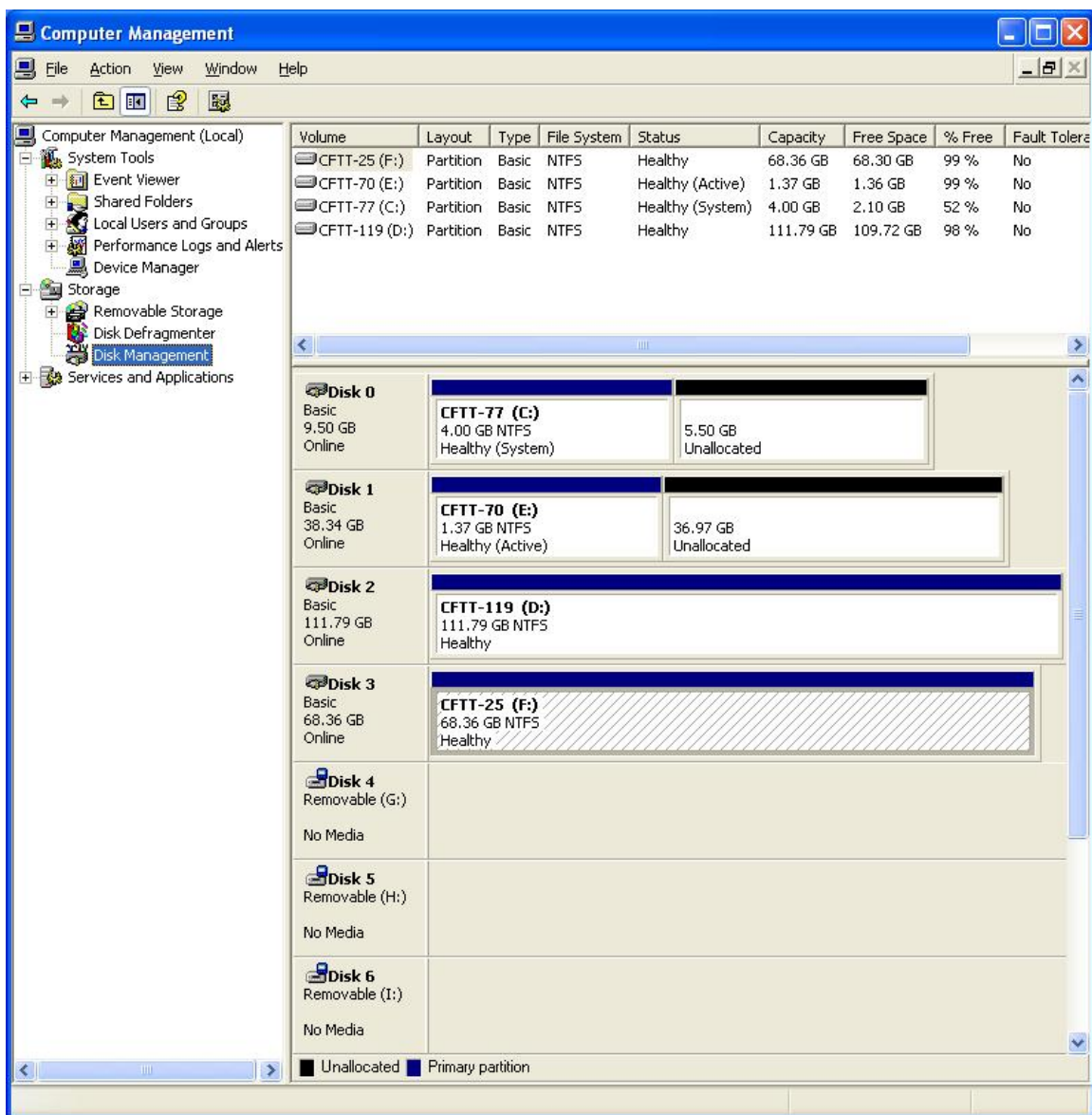
The tool failed to produce the expected result. The number of drives configured and the pattern of protection applied did not alter the ability of the tool to protect designated drives. However, the tool failed to block all commands in the protected categories. The protection failures observed were identical to those of tests SWB-03, SWB-04, and SWB-06.

9.12 Test case SWB-12

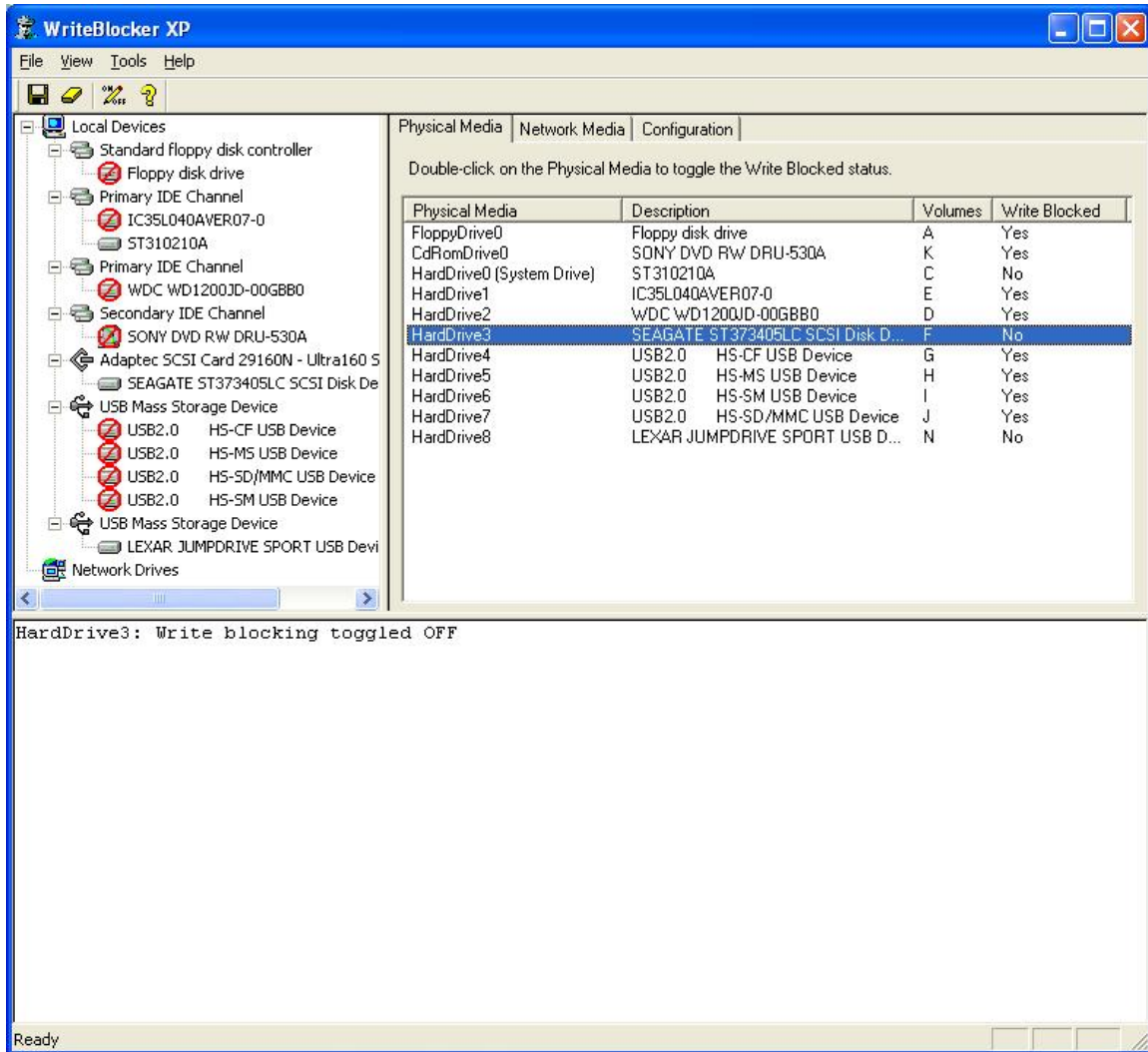
This case tests the tool's compliance with optional assertions SWB-AO-01 through SWB-AO-06. It issues all possible commands to a set of three drives protected with the pattern PPU. The expected result of this test is the tool will:

- Block all commands from the WRITE, VENDOR_SPECIFIC, and UNDEFINED categories issued to protected drives
- Pass all commands from the READ and OTHER categories issued to protected drives
- Pass all commands from all categories issued to unprotected drives

9.12.1. Hard disk configuration



9.12.2. Write blocker configuration



9.12.3. Test output summary

NIST Software Write Blocker Test Suite V1.2
Mon Aug 29 09:24:01 2005

Test case: SWB-12
Command set: RWOVU
Number of drives: 3
Protection pattern: PPU
Test administered by: DPA
Details logged to file: SWB-12.log

**** Test results summary (see logfile for details) ****

Testing device \\.\Physical Drive1
Device is software WRITE PROTECTED

Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	4	4	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	22	12	34
Other CDB's	62	0	62
Vendor SPeci fi c CDB's	80	0	80
Undefined CDB's	53	0	53

Testing device \\.\Physical Drive2
Device is software WRITE PROTECTED

Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	4	4	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	22	12	34
Other CDB's	62	0	62
Vendor SPeci fi c CDB's	80	0	80
Undefined CDB's	53	0	53

Testing device \\.\Physical Drive3
Device is software WRITE ENABLED

Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	8	0	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	34	0	34
Other CDB's	62	0	62
Vendor SPeci fi c CDB's	80	0	80
Undefined CDB's	53	0	53

9.12.4. Hard disk hash results

Drive Identification		Computed	SHA1 Value
\\.\PhysicalDrive1 (CFTT-70)	P	Before	6B60F2CF1391DE31D795318E2074670FF6646EE0
		After	6B60F2CF1391DE31D795318E2074670FF6646EE0
\\.\PhysicalDrive2 (CFTT-119)	P	Before	98CB37515F44BF652BF620B1869EADE0C9D7A8ED
		After	98CB37515F44BF652BF620B1869EADE0C9D7A8ED
\\.\PhysicalDrive3 (CFTT-25)	U	Before	C2858F133AA1241976AFA91BE124B9E58138533B
		After	44B1872214D834D0B180FF7F9F0F83EBD558553A

9.12.5. Test results analysis

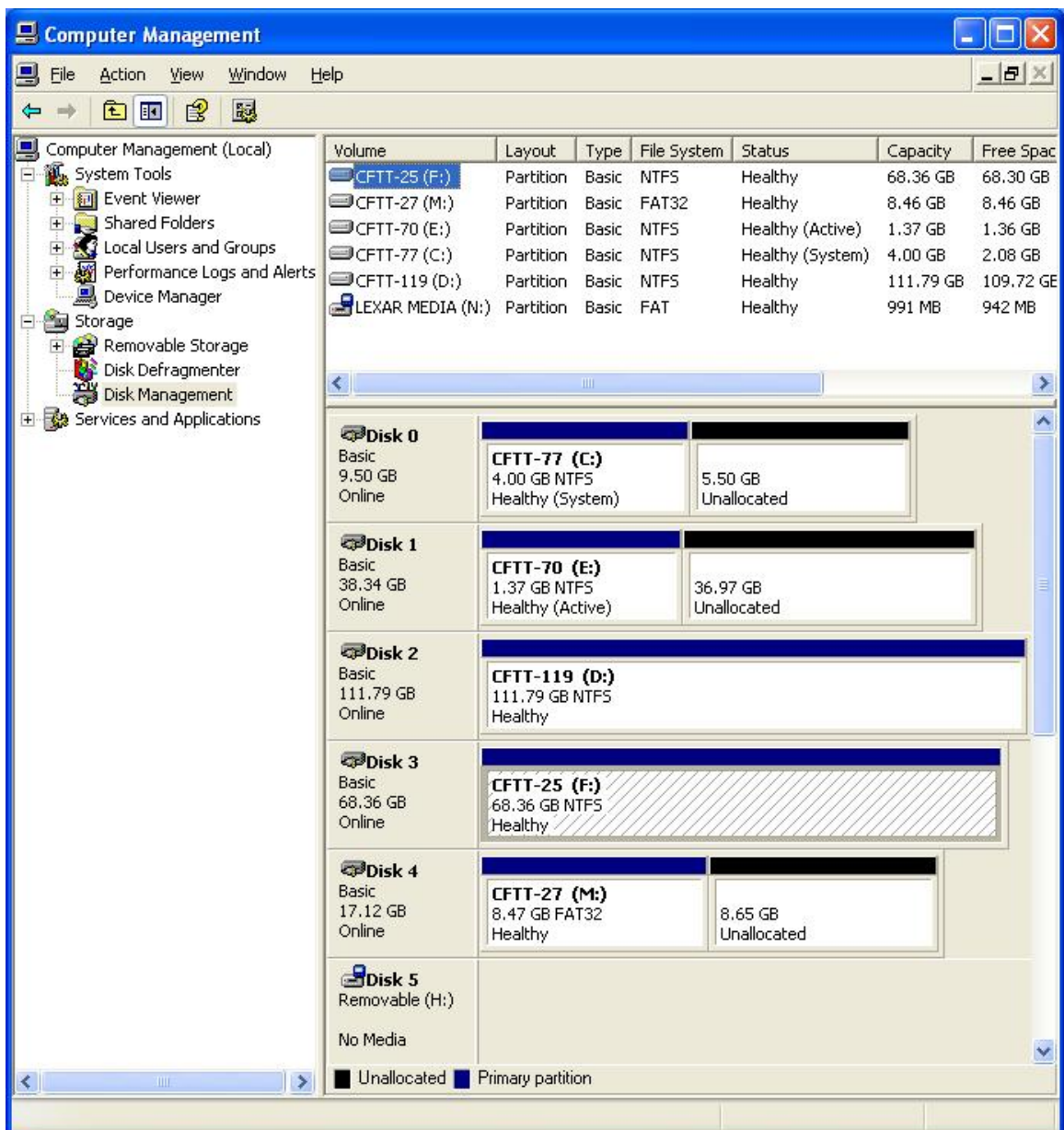
The tool failed to produce the expected result. The number of drives configured and the pattern of protection applied did not alter the ability of the tool to protect designated drives. However, the tool failed to block all commands in the protected categories. The protection failures observed were identical to those of tests SWB-03, SWB-04, and SWB-06.

9.13 Test case SWB-13

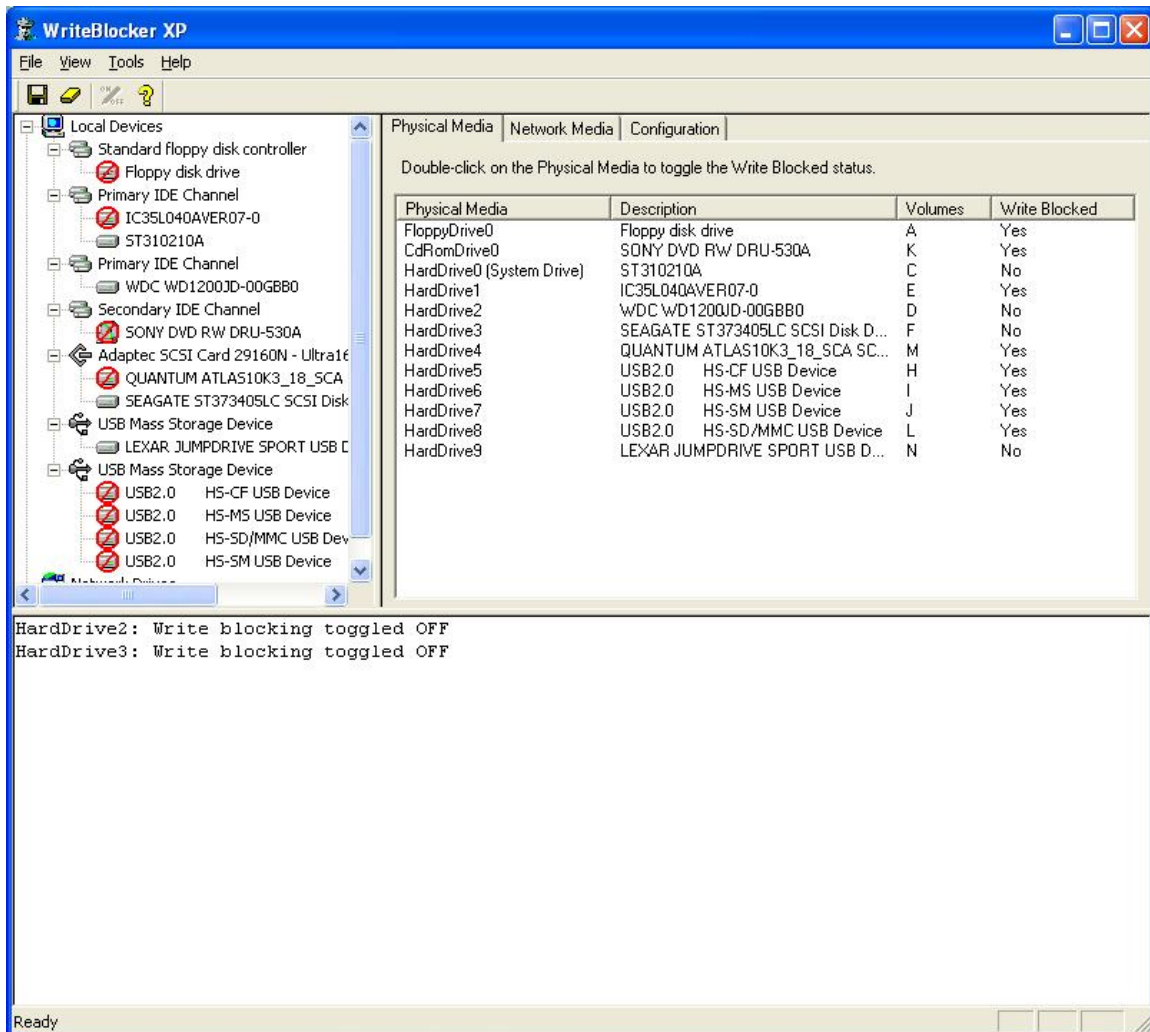
This case tests the tool's compliance with optional assertions SWB-AO-01 through SWB-AO-06. It issues all possible commands to a set of four drives protected with the pattern NOT_MIDDLE. The expected result of this test is the tool will:

- Block all commands from the WRITE, VENDOR_SPECIFIC, and UNDEFINED categories issued to protected drives
- Pass all commands from the READ and OTHER categories issued to protected drives
- Pass all commands from all categories issued to unprotected drives

9.13.1. Hard disk configuration



9.13.2. Write blocker configuration



9.13.3. Test output summary

NIST Software Write Blocker Test Suite V1.2
Tue Sep 06 15:29:32 2005

Test case: SWB-13
Command set: RWOVU
Number of drives: 4
Protection pattern: PUUP
Test administered by: DPA
Details logged to file: SWB-13.log

**** Test results summary (see logfile for details) ****

Testing device \\.\Physical Drive1
Device is software WRITE PROTECTED

Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	4	4	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	22	12	34
Other CDB's	62	0	62
Vendor SPeci fic CDB's	80	0	80
Undefined CDB's	53	0	53

Testing device \\.\Physical Drive2
Device is software WRITE ENABLED

Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	8	0	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	34	0	34
Other CDB's	62	0	62
Vendor SPeci fic CDB's	80	0	80
Undefined CDB's	53	0	53

Testing device \\.\Physical Drive3
Device is software WRITE ENABLED

Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	8	0	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	34	0	34
Other CDB's	62	0	62
Vendor SPeci fic CDB's	80	0	80
Undefined CDB's	53	0	53

Testing device \\.\PhysicalDrive4 Device is software WRITE PROTECTED			
Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	4	4	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	22	12	34
Other CDB's	62	0	62
Vendor Specific CDB's	80	0	80
Undefined CDB's	53	0	53

9.13.4. Hard disk hash results

Drive Identification		Computed	SHA1 Value
\\.\PhysicalDrive1 (CFTT-70)	P	Before	6B60F2CF1391DE31D795318E2074670FF6646EE0
		After	6B60F2CF1391DE31D795318E2074670FF6646EE0
\\.\PhysicalDrive2 (CFTT-119)	U	Before	98CB37515F44BF652BF620B1869EADE0C9D7A8ED
		After	2A45F3A7932AD6BF5700D3EE00690E06C8E07EEA
\\.\PhysicalDrive3 (CFTT-25)	U	Before	47053F56C76CA4A10100232AFDDB93AD4FEF7FE9
		After	44B1872214D834D0B180FF7F9F0F83EBD558553A
\\.\PhysicalDrive4 (CFTT-27)	P	Before	C4848A0D8BB04D5D684A51F966BE009C7E47EFAA
		After	C4848A0D8BB04D5D684A51F966BE009C7E47EFAA

9.13.5. Test results analysis

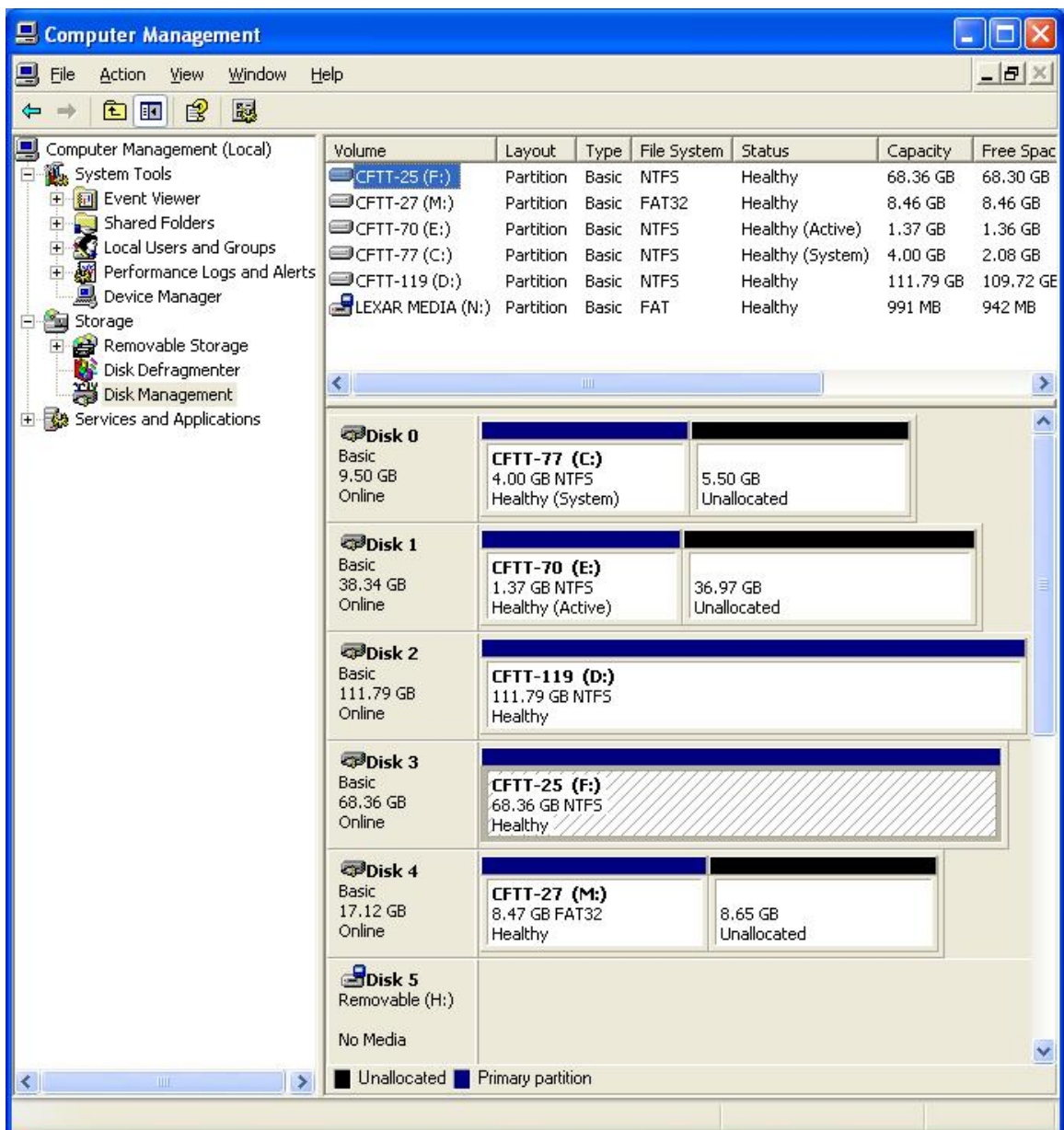
The tool failed to produce the expected result. The number of drives configured and the pattern of protection applied did not alter the ability of the tool to protect designated drives. However, the tool failed to block all commands in the protected categories. The protection failures observed were identical to those of tests SWB-03, SWB-04, and SWB-06.

9.14 Test case SWB-14

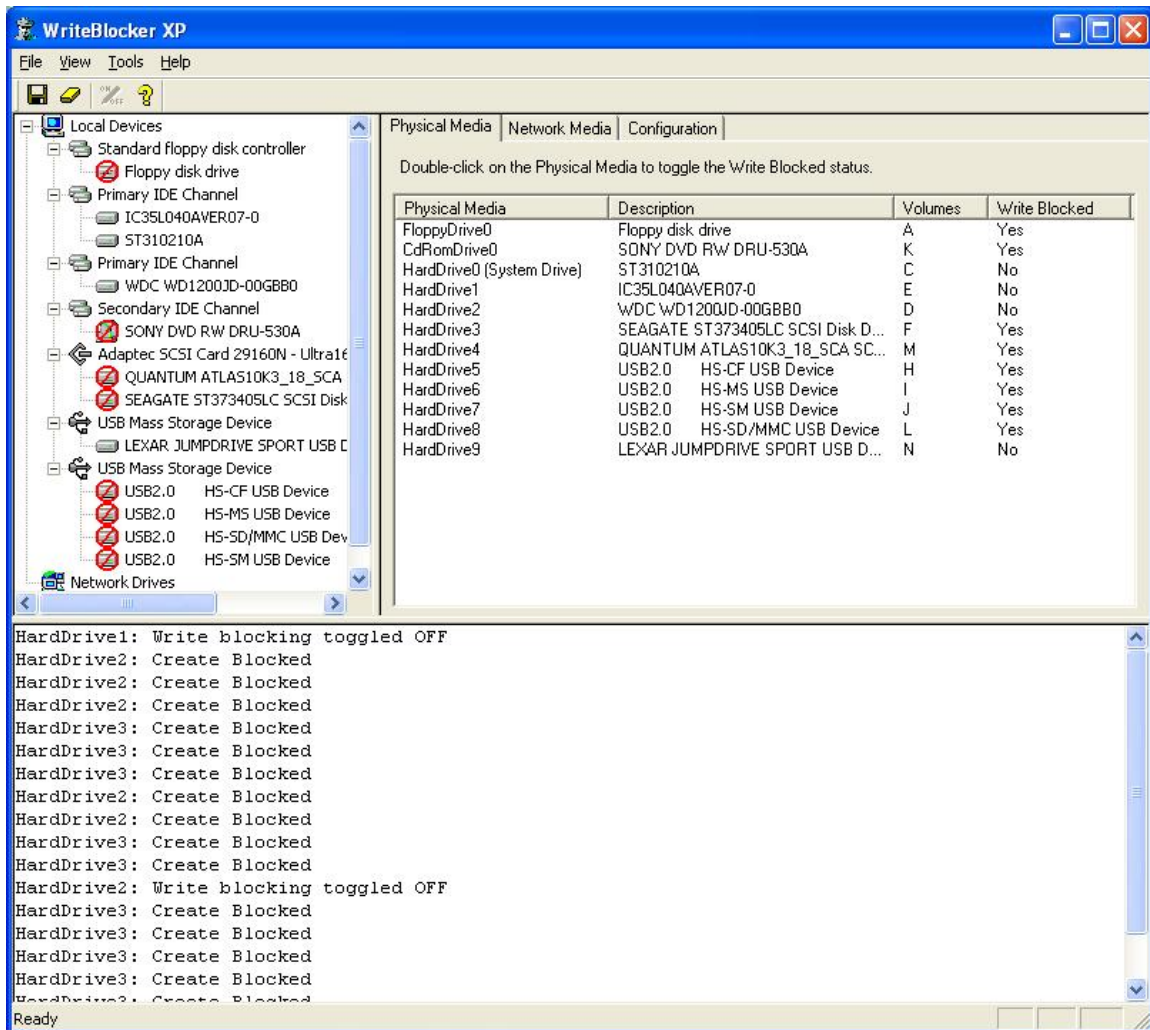
This case tests the tool's compliance with optional assertions SWB-AO-01 through SWB-AO-06. It issues all possible commands to a set of four drives protected with the pattern HIGH. The expected result of this test is the tool will:

- Block all commands from the WRITE, VENDOR_SPECIFIC, and UNDEFINED categories issued to protected drives
- Pass all commands from the READ and OTHER categories issued to protected drives
- Pass all commands from all categories issued to unprotected drives

9.14.1. Hard disk configuration



9.14.2. Write blocker configuration



9.14.3. Test output summary

NIST Software Write Blocker Test Suite V1.2
Wed Sep 07 09:25:45 2005

Test case: SWB-14
Command set: RWOVU
Number of drives: 4
Protection pattern: UUPP
Test administered by: DPA
Details logged to file: SWB-14.log

**** Test results summary (see logfile for details) ****

Testing device \\.\Physical Drive1
Device is software WRITE ENABLED

Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	8	0	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	34	0	34
Other CDB's	62	0	62
Vendor SPECIFIC CDB's	80	0	80
Undefined CDB's	53	0	53

Testing device \\.\Physical Drive2
Device is software WRITE ENABLED

Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	8	0	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	34	0	34
Other CDB's	62	0	62
Vendor SPECIFIC CDB's	80	0	80
Undefined CDB's	53	0	53

Testing device \\.\Physical Drive3
Device is software WRITE PROTECTED

Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	4	4	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	22	12	34
Other CDB's	62	0	62
Vendor SPECIFIC CDB's	80	0	80
Undefined CDB's	53	0	53

Testing device \\.\PhysicalDrive4
Device is software WRITE PROTECTED

Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	4	4	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	22	12	34
Other CDB's	62	0	62
Vendor SPeci fic CDB's	80	0	80
Undefined CDB's	53	0	53

9.14.4. Hard disk hash results

Drive Identification		Computed	SHA1 Value
\\.\PhysicalDrive1 (CFTT-70)	U	Before	B60F2CF1391DE31D795318E2074670FF6646EE0
		After	DD28B6EB3F83631A6B917A07EE73A7AD123EEAD
\\.\PhysicalDrive2 (CFTT-119)	U	Before	2A45F3A7932AD6BF5700D3EE00690E06C8E07EEA
		After	9C448EB3FA0DF5093EE28B7AF0835F53940E91A8
\\.\PhysicalDrive3 (CFTT-25)	P	Before	44B1872214D834D0B180FF7F9F0F83EBD558553A
		After	44B1872214D834D0B180FF7F9F0F83EBD558553A
\\.\PhysicalDrive4 (CFTT-27)	P	Before	C4848A0D8BB04D5D684A51F966BE009C7E47EFAA
		After	C4848A0D8BB04D5D684A51F966BE009C7E47EFAA

9.14.5. Test results analysis

The tool failed to produce the expected result. The number of drives configured and the pattern of protection applied did not alter the ability of the tool to protect designated drives. However, the tool failed to block all commands in the protected categories. The protection failures observed were identical to those of tests SWB-03, SWB-04, and SWB-06.

9.15 Test case SWB-15

This case tests the tool's compliance with optional assertions SWB-AO-01 through SWB-AO-06. It issues all possible commands to a set of four drives protected with the pattern NOT_FIRST. The expected result of this test is the tool will:

- Block all commands from the WRITE, VENDOR_SPECIFIC, and UNDEFINED categories issued to protected drives
- Pass all commands from the READ and OTHER categories issued to protected drives
- Pass all commands from all categories issued to unprotected drives

9.15.1. Hard disk configuration

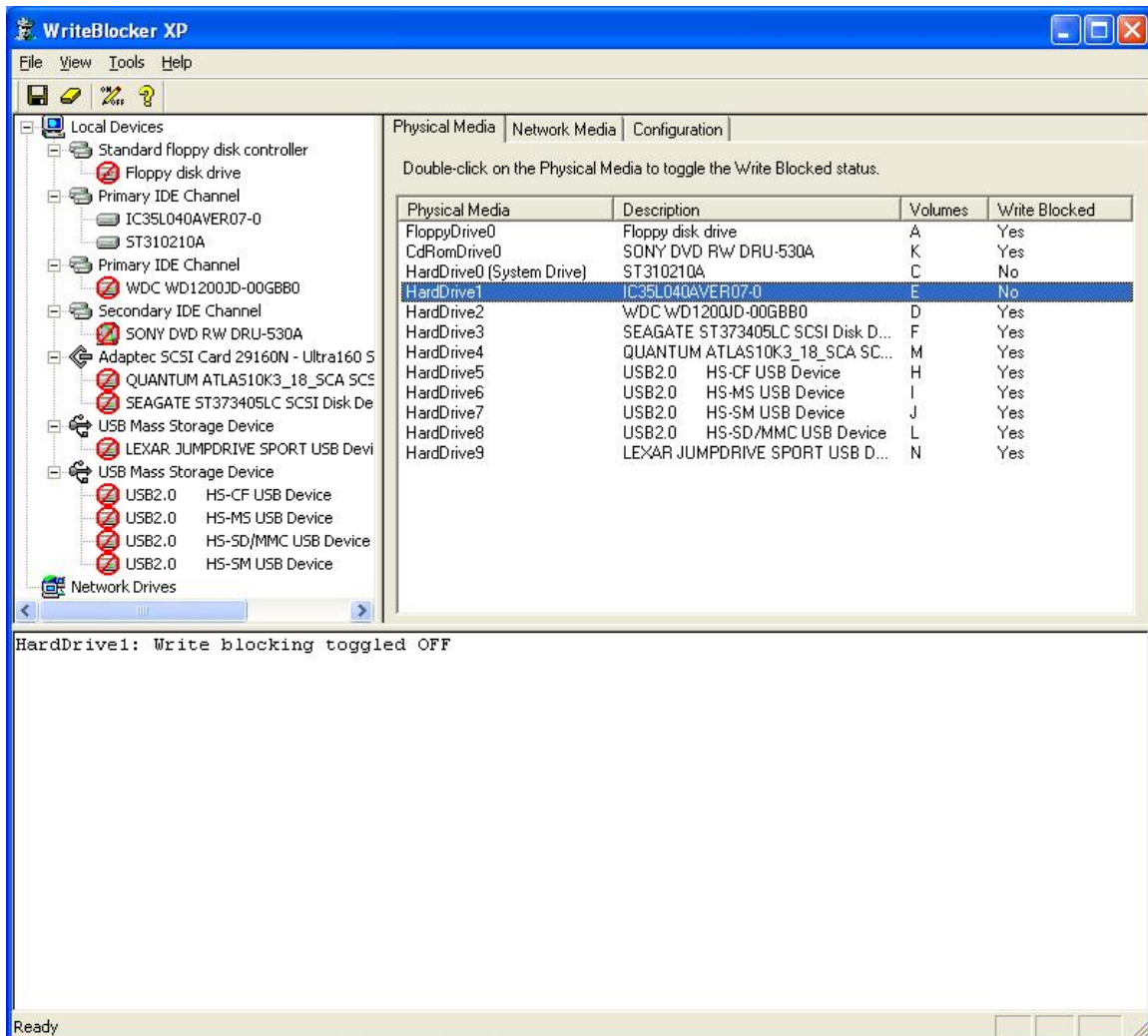
The screenshot displays the Windows Computer Management console. The left pane shows the tree view with 'Storage' expanded, showing 'Removable Storage', 'Disk Defragmenter', 'Disk Management', and 'Services and Applications'. The right pane shows a table of volumes and a detailed view of the disks.

Volume	Layout	Type	File System	Status	Capacity	Free Space
CFTT-25 (F:)	Partition	Basic	NTFS	Healthy	68.36 GB	68.30 GB
CFTT-27 (M:)	Partition	Basic	FAT32	Healthy	8.46 GB	8.46 GB
CFTT-70 (E:)	Partition	Basic	NTFS	Healthy (Active)	1.37 GB	1.36 GB
CFTT-77 (C:)	Partition	Basic	NTFS	Healthy (System)	4.00 GB	2.08 GB
CFTT-119 (D:)	Partition	Basic	NTFS	Healthy	111.79 GB	109.72 GB
LEXAR MEDIA (N:)	Partition	Basic	FAT	Healthy	991 MB	942 MB

Disk	Layout	Type	File System	Status	Capacity	Free Space
Disk 0	Basic	9.50 GB	Online	CFTT-77 (C:)	4.00 GB NTFS	5.50 GB Unallocated
Disk 1	Basic	38.34 GB	Online	CFTT-70 (E:)	1.37 GB NTFS	36.97 GB Unallocated
Disk 2	Basic	111.79 GB	Online	CFTT-119 (D:)	111.79 GB NTFS	Healthy
Disk 3	Basic	68.36 GB	Online	CFTT-25 (F:)	68.36 GB NTFS	Healthy
Disk 4	Basic	17.12 GB	Online	CFTT-27 (M:)	8.47 GB FAT32	8.65 GB Unallocated
Disk 5	Removable (H:)	No Media				

Legend: ■ Unallocated ■ Primary partition

9.15.2. Write Blocker Configuration



9.15.3. Test output summary

NIST Software Write Blocker Test Suite V1.2

Wed Sep 07 11:48:50 2005

Test case: SWB-15
Command set: RWOVU
Number of drives: 4
Protection pattern: UPPP
Test administered by: DPA
Details logged to file: SWB-15.log

**** Test results summary (see logfile for details) ****

Testing device \\.\Physical Drive1
Device is software WRITE ENABLED

Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	8	0	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	34	0	34
Other CDB's	62	0	62
Vendor Specific CDB's	80	0	80
Undefined CDB's	53	0	53

Testing device \\.\Physical Drive2
Device is software WRITE PROTECTED

Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	4	4	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	22	12	34
Other CDB's	62	0	62
Vendor Specific CDB's	80	0	80
Undefined CDB's	53	0	53

Testing device \\.\Physical Drive3
Device is software WRITE PROTECTED

Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	4	4	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	22	12	34
Other CDB's	62	0	62
Vendor Specific CDB's	80	0	80
Undefined CDB's	53	0	53

Testing device \\.\PhysicalDrive4 Device is software WRITE PROTECTED			
Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	4	4	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	22	12	34
Other CDB's	62	0	62
Vendor Specific CDB's	80	0	80
Undefined CDB's	53	0	53

9.15.4. Hard disk hash results

Drive Identification		Computed	SHA1 Value
\\.\PhysicalDrive1 (CFTT-70)	U	Before	DD28B6EB3F83631A6B917A07EE73A7AD123EEEAD
		After	E66350590512EC41048B73E8C2E69283AE313248
\\.\PhysicalDrive2 (CFTT-119)	P	Before	9C448EB3FA0DF5093EE28B7AF0835F53940E91A8
		After	9C448EB3FA0DF5093EE28B7AF0835F53940E91A8
\\.\PhysicalDrive3 (CFTT-25)	P	Before	44B1872214D834D0B180FF7F9F0F83EBD558553A
		After	44B1872214D834D0B180FF7F9F0F83EBD558553A
\\.\PhysicalDrive4 (CFTT-27)	P	Before	C4848A0D8BB04D5D684A51F966BE009C7E47EFAA
		After	C4848A0D8BB04D5D684A51F966BE009C7E47EFAA

9.15.5. Test results analysis

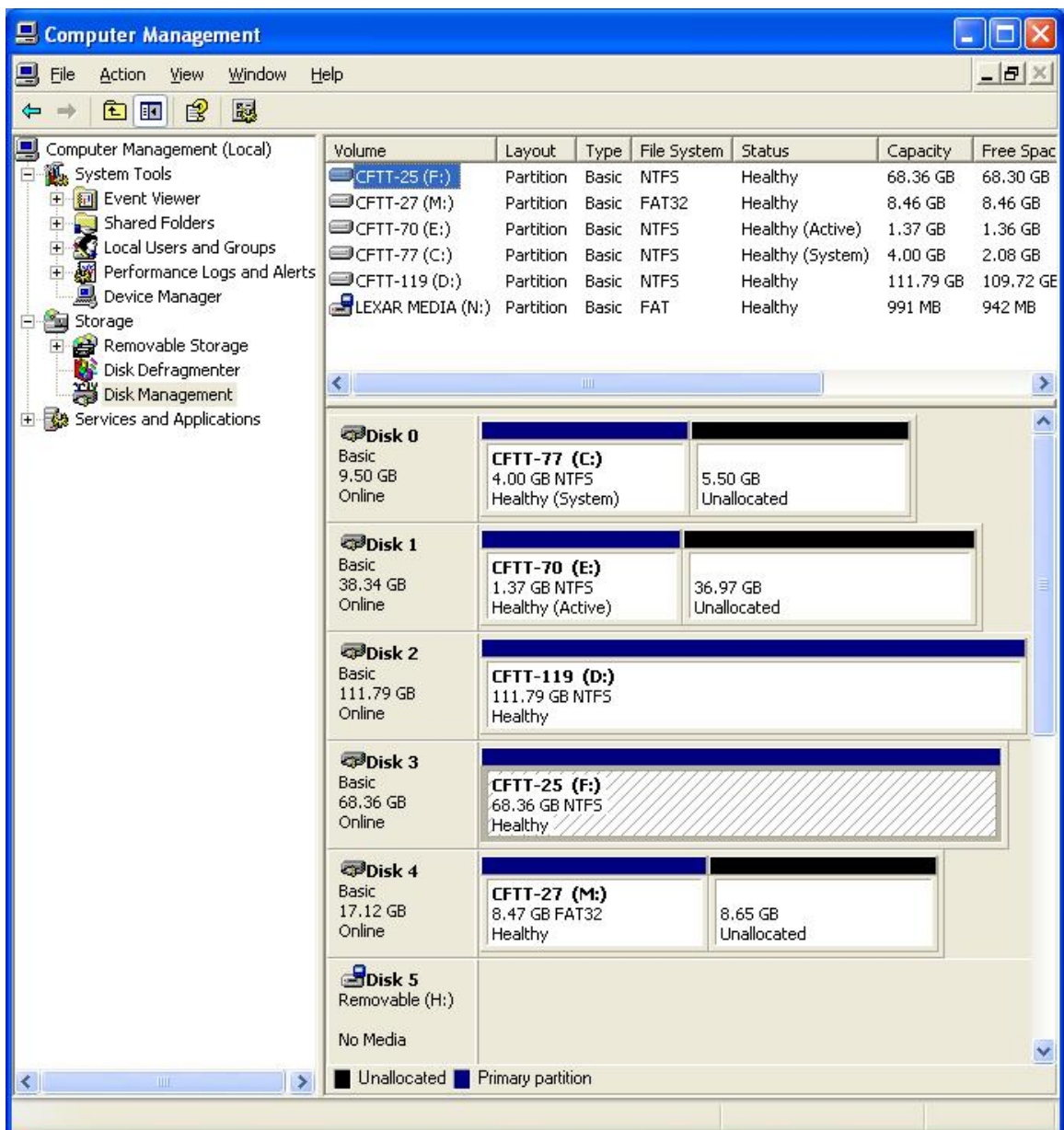
The tool failed to produce the expected result. The pattern of protection did not affect the ability of the tool to protect designated drives but the protection applied failed to block all commands in the protected categories. The protection applied for protected drives was identical to tests SWB-03, SWB-04, and SWB-06.

9.16 Test case SWB-16

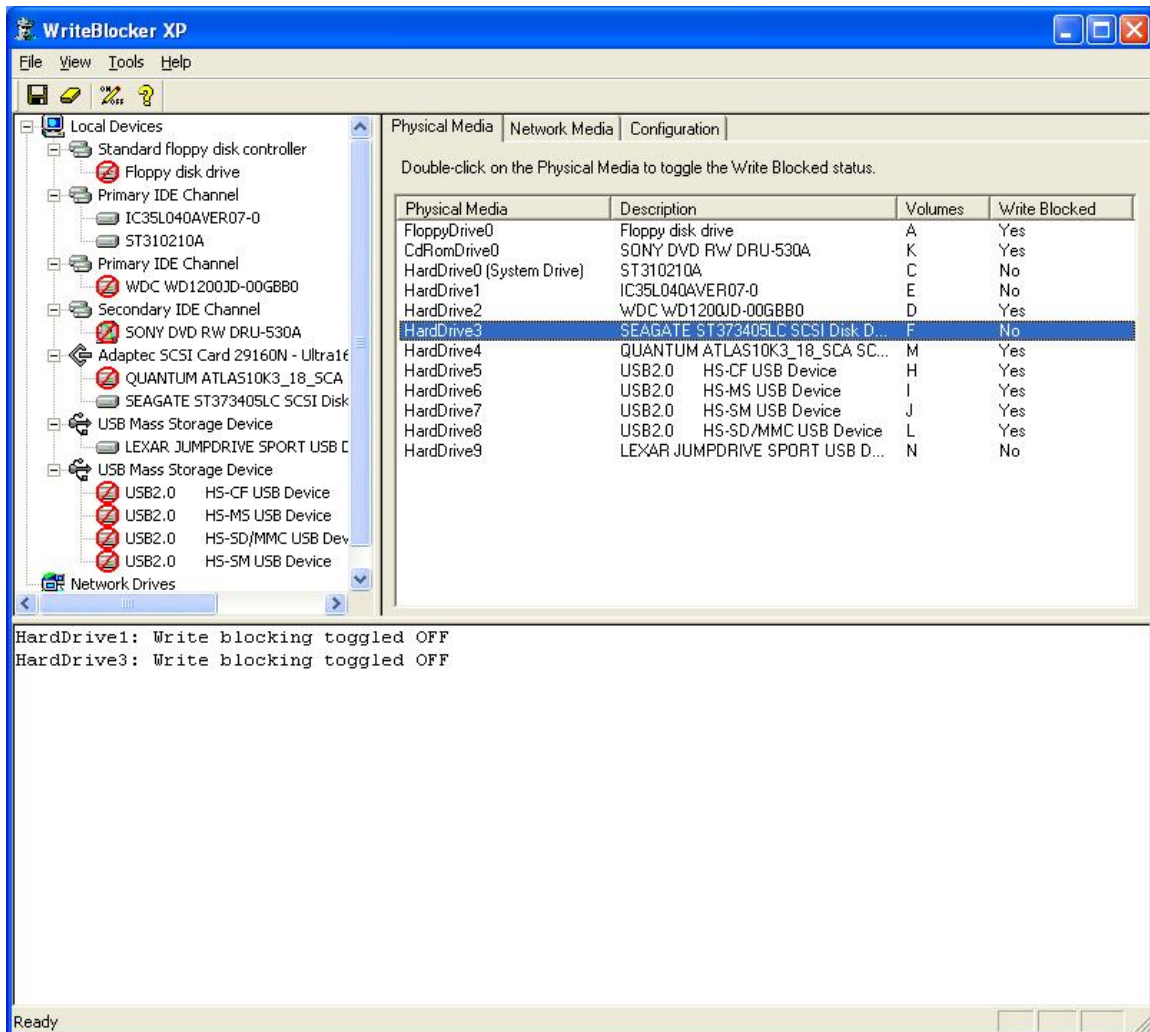
This case tests the tool's compliance with optional assertions SWB-AO-01 through SWB-AO-06. It issues all possible commands to a set of four drives protected with the pattern EVEN. The expected result of this test is the tool will:

- Block all commands from the WRITE, VENDOR_SPECIFIC, and UNDEFINED categories issued to protected drives
- Pass all commands from the READ and OTHER categories issued to protected drives
- Pass all commands from all categories issued to unprotected drives

9.16.1. Hard disk configuration



9.16.2. Write blocker configuration



9.16.3. Test output summary

NIST Software Write Blocker Test Suite V1.2

Wed Sep 07 13:55:33 2005

Test case: SWB-16
Command set: RWOVU
Number of drives: 4
Protection pattern: UPUP
Test administered by: DPA
Details logged to file: SWB-16.log

**** Test results summary (see logfile for details) ****

Testing device \\.\Physical Drive1
Device is software WRITE ENABLED

Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	8	0	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	34	0	34
Other CDB's	62	0	62
Vendor Specific CDB's	80	0	80
Undefined CDB's	53	0	53

Testing device \\.\Physical Drive2
Device is software WRITE PROTECTED

Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	4	4	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	22	12	34
Other CDB's	62	0	62
Vendor Specific CDB's	80	0	80
Undefined CDB's	53	0	53

Testing device \\.\Physical Drive3
Device is software WRITE ENABLED

Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	8	0	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	34	0	34
Other CDB's	62	0	62
Vendor Specific CDB's	80	0	80
Undefined CDB's	53	0	53

Testing device \\.\PhysicalDrive4 Device is software WRITE PROTECTED			
Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	4	4	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	22	12	34
Other CDB's	62	0	62
Vendor Specific CDB's	80	0	80
Undefined CDB's	53	0	53

9.16.4. Hard disk hash results

Drive Identification		Computed	SHA1 Value
\\.\PhysicalDrive1 (CFTT-70)	U	Before	E66350590512EC41048B73E8C2E69283AE313248
		After	7CA790CE7D88AE88DB474EA036D2FBA0CBE46609
\\.\PhysicalDrive2 (CFTT-119)	P	Before	9C448EB3FA0DF5093EE28B7AF0835F53940E91A8
		After	9C448EB3FA0DF5093EE28B7AF0835F53940E91A8
\\.\PhysicalDrive3 (CFTT-25)	U	Before	44B1872214D834D0B180FF7F9F0F83EBD558553A
		After	D9AFB629767E4337B52DCCE75A99A8263BBDBB0A
\\.\PhysicalDrive4 (CFTT-27)	P	Before	C4848A0D8BB04D5D684A51F966BE009C7E47EFAA
		After	C4848A0D8BB04D5D684A51F966BE009C7E47EFAA

9.16.5. Test results analysis

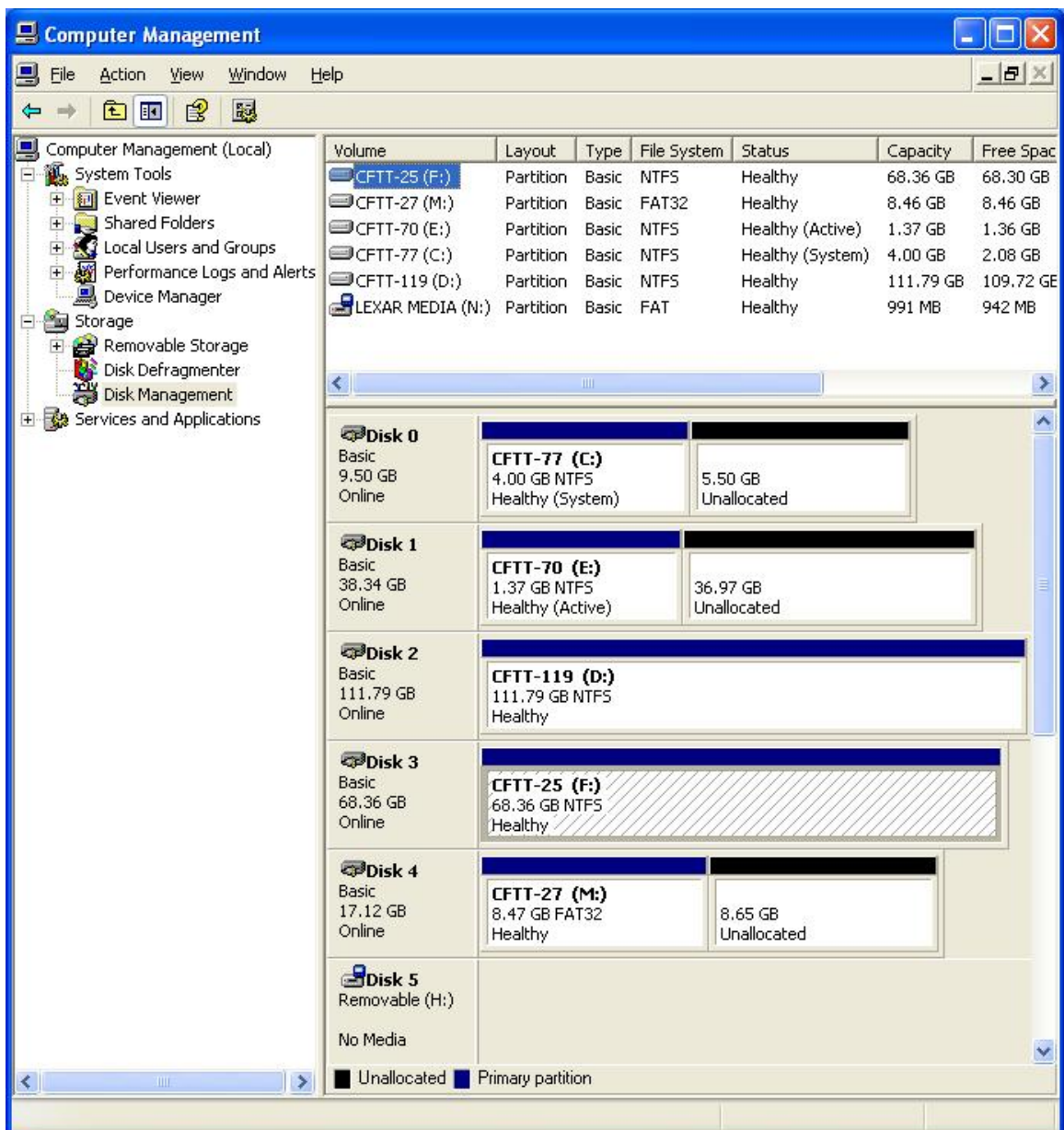
The tool failed to produce the expected result. The pattern of protection did not affect the ability of the tool to protect designated drives but the protection applied failed to block all commands in the protected categories. The protection applied for protected drives was identical to tests SWB-03, SWB-04, and SWB-06.

9.17 Test case SWB-17

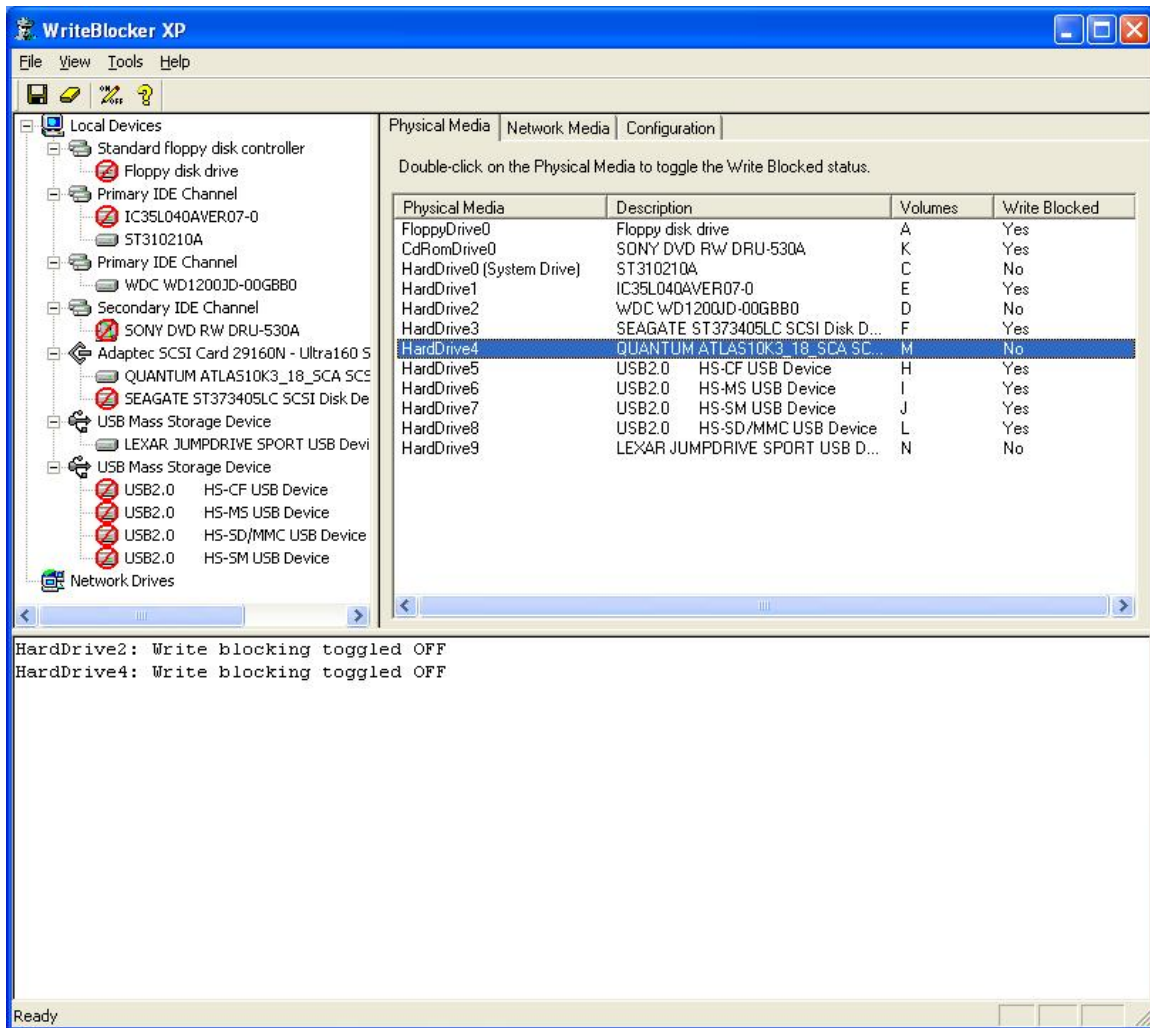
This case tests the tool's compliance with optional assertions SWB-AO-01 through SWB-AO-06. It issues all possible commands to a set of four drives protected with the pattern ODD. The expected result of this test is the tool will:

- Block all commands from the WRITE, VENDOR_SPECIFIC, and UNDEFINED categories issued to protected drives
- Pass all commands from the READ and OTHER categories issued to protected drives
- Pass all commands from all categories issued to unprotected drives

9.17.1. Hard disk configuration



9.17.2. Write blocker configuration



9.17.3. Test output summary

NIST Software Write Blocker Test Suite V1.2
Wed Sep 07 15:08:26 2005

Test case: SWB-17
Command set: RWOVU
Number of drives: 4
Protection pattern: PUPU
Test administered by: DPA
Details logged to file: SWB-17.log

**** Test results summary (see logfile for details) ****

Testing device \\.\Physical Drive1
Device is software WRITE PROTECTED

Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	4	4	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	22	12	34
Other CDB's	62	0	62
Vendor SPeci fic CDB's	80	0	80
Undefined CDB's	53	0	53

Testing device \\.\Physical Drive2
Device is software WRITE ENABLED

Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	8	0	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	34	0	34
Other CDB's	62	0	62
Vendor SPeci fic CDB's	80	0	80
Undefined CDB's	53	0	53

Testing device \\.\Physical Drive3
Device is software WRITE PROTECTED

Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	4	4	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	22	12	34
Other CDB's	62	0	62
Vendor SPeci fic CDB's	80	0	80

Undefined CDB's	53	0	53
Testing device \\.\PhysicalDrive4 Device is software WRITE ENABLED			
Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	8	0	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	34	0	34
Other CDB's	62	0	62
Vendor Specific CDB's	80	0	80
Undefined CDB's	53	0	53

9.17.4. Hard disk hash results

Drive Identification		Computed	SHA1 Value
\\.\PhysicalDrive1 (CFTT-70)	P	Before	7CA790CE7D88AE88DB474EA036D2FBA0CBE46609
		After	7CA790CE7D88AE88DB474EA036D2FBA0CBE46609
\\.\PhysicalDrive2 (CFTT-119)	U	Before	9C448EB3FA0DF5093EE28B7AF0835F53940E91A8
		After	336468E49C86BCF47D6B6EC157C83F6546F680E7
\\.\PhysicalDrive3 (CFTT-25)	P	Before	D9AFB629767E4337B52DCCE75A99A8263BBDBB0A
		After	D9AFB629767E4337B52DCCE75A99A8263BBDBB0A
\\.\PhysicalDrive4 (CFTT-27)	U	Before	C4848A0D8BB04D5D684A51F966BE009C7E47EFAA
		After	C4848A0D8BB04D5D684A51F966BE009C7E47EFAA

9.17.5. Test results analysis

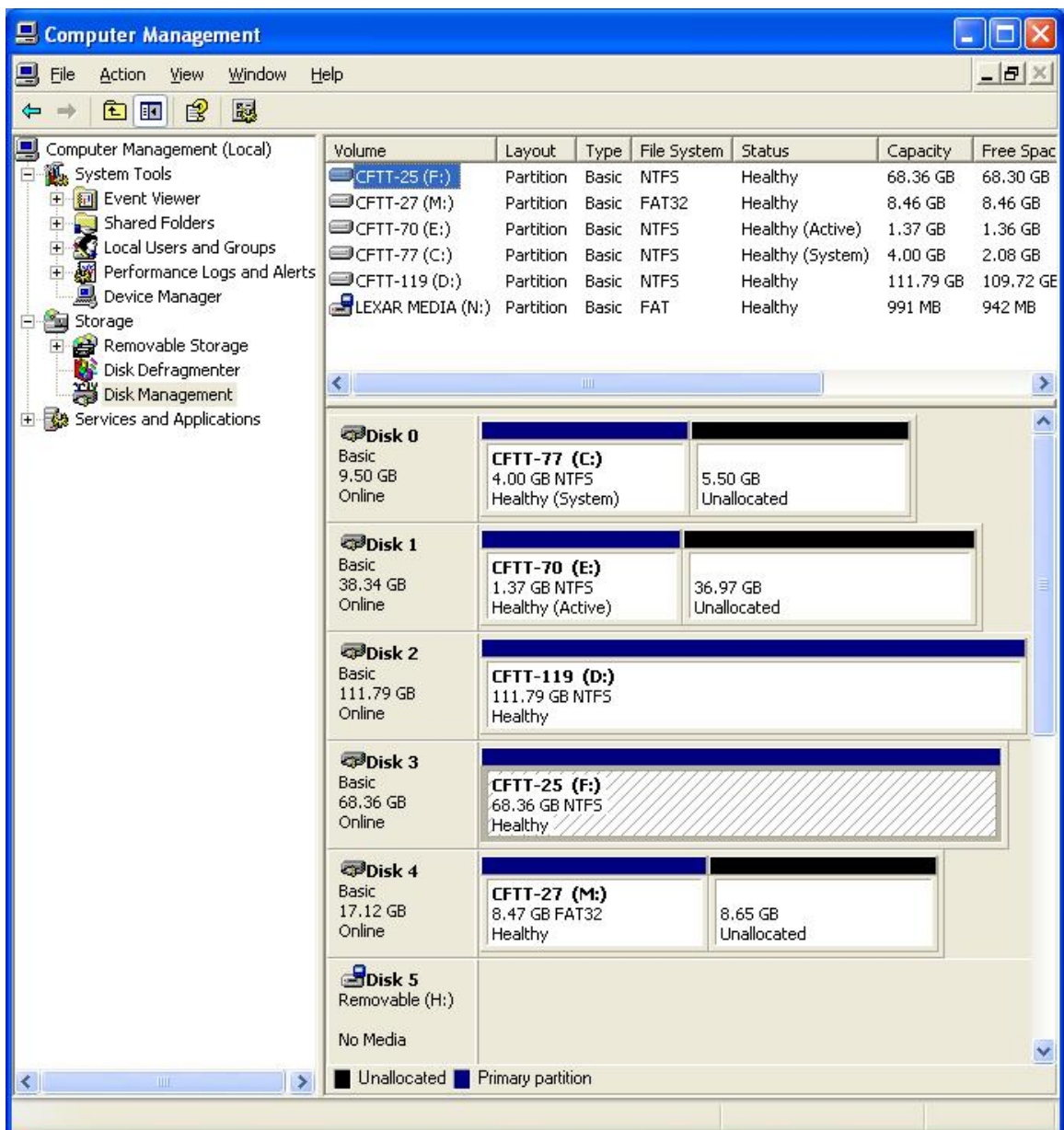
The tool failed to produce the expected result. The pattern of protection did not affect the ability of the tool to protect designated drives but the protection applied failed to block all commands in the protected categories. The protection applied for protected drives was identical to tests SWB-03, SWB-04, and SWB-06.

9.18 Test case SWB-18

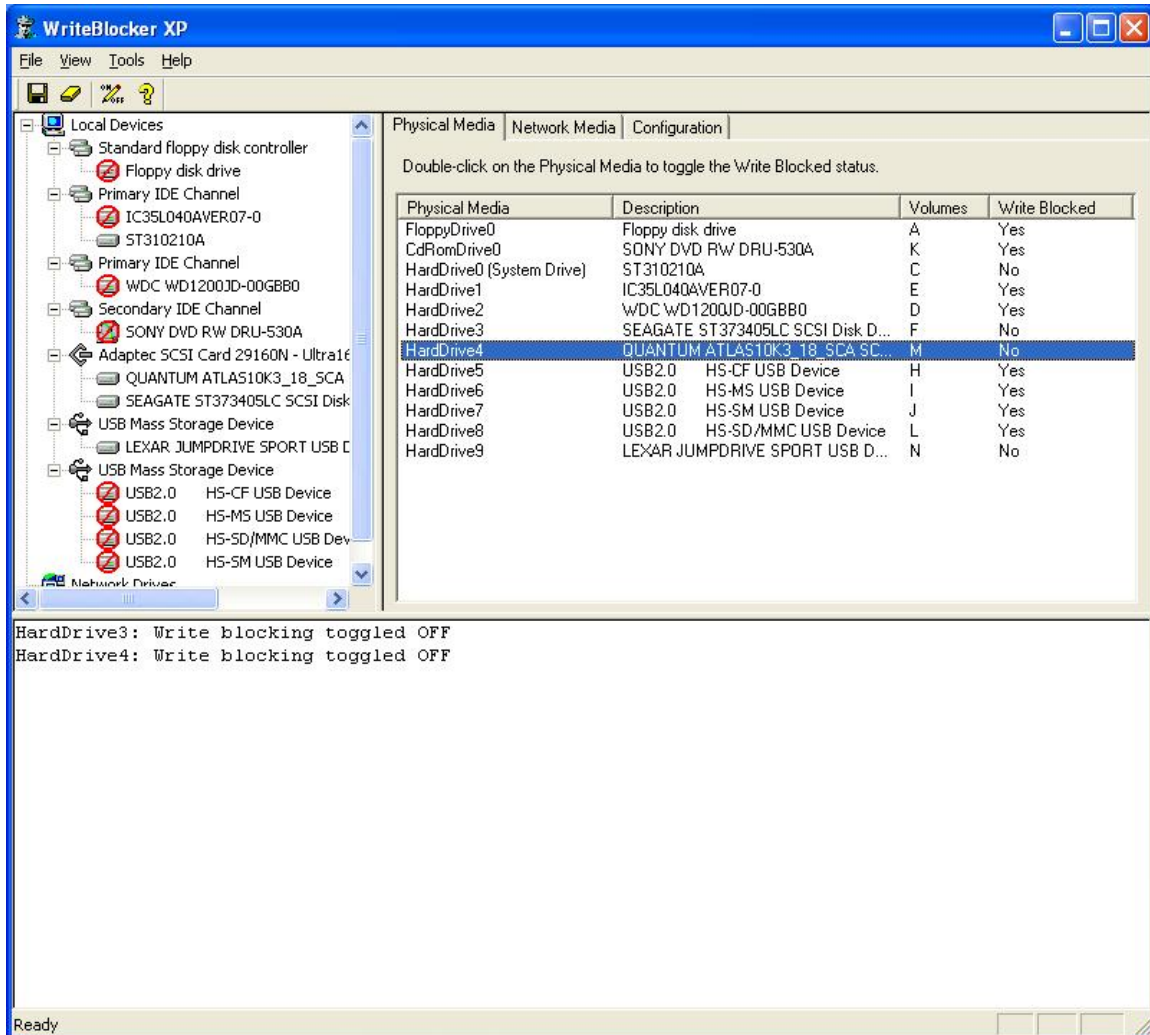
This case tests the tool's compliance with optional assertions SWB-AO-01 through SWB-AO-06. It issues all possible commands to a set of four drives protected with the pattern FIRST. The expected result of this test is the tool will:

- Block all commands from the WRITE, VENDOR_SPECIFIC, and UNDEFINED categories issued to protected drives
- Pass all commands from the READ and OTHER categories issued to protected drives
- Pass all commands from all categories issued to unprotected drives

9.18.1. Hard disk configuration



9.18.2. Write blocker configuration



9.18.3. Test output summary

NIST Software Write Blocker Test Suite V1.2
Wed Sep 07 16:22:57 2005

Test case: SWB-18
Command set: RWOVU
Number of drives: 4
Protection pattern: PPUU
Test administered by: DPA
Details logged to file: SWB-18.log

**** Test results summary (see logfile for details) ****

Testing device \\.\Physical Drive1
Device is software WRITE PROTECTED

Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	4	4	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	22	12	34
Other CDB's	62	0	62
Vendor SPeci fic CDB's	80	0	80
Undefined CDB's	53	0	53

Testing device \\.\Physical Drive2
Device is software WRITE PROTECTED

Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	4	4	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	22	12	34
Other CDB's	62	0	62
Vendor SPeci fic CDB's	80	0	80
Undefined CDB's	53	0	53

Testing device \\.\Physical Drive3
Device is software WRITE ENABLED

Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	8	0	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	34	0	34
Other CDB's	62	0	62
Vendor SPeci fic CDB's	80	0	80

Undefined CDB's	53	0	53
Testing device \\.\PhysicalDrive4 Device is software WRITE ENABLED			
Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	8	0	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	34	0	34
Other CDB's	62	0	62
Vendor Specific CDB's	80	0	80
Undefined CDB's	53	0	53

9.18.4. Hard disk hash results

Drive Identification		Computed	SHA1 Value
\\.\PhysicalDrive1 (CFTT-70)	P	Before	7CA790CE7D88AE88DB474EA036D2FBA0CBE46609
		After	7CA790CE7D88AE88DB474EA036D2FBA0CBE46609
\\.\PhysicalDrive2 (CFTT-119)	P	Before	336468E49C86BCF47D6B6EC157C83F6546F680E7
		After	336468E49C86BCF47D6B6EC157C83F6546F680E7
\\.\PhysicalDrive3 (CFTT-25)	U	Before	D9AFB629767E4337B52DCCE75A99A8263BBDBB0A
		After	1855E34326E0786F34737DDC72197977980BBB77
\\.\PhysicalDrive4 (CFTT-27)	U	Before	C4848A0D8BB04D5D684A51F966BE009C7E47EFAA
		After	C4848A0D8BB04D5D684A51F966BE009C7E47EFAA

9.18.5. Test results analysis

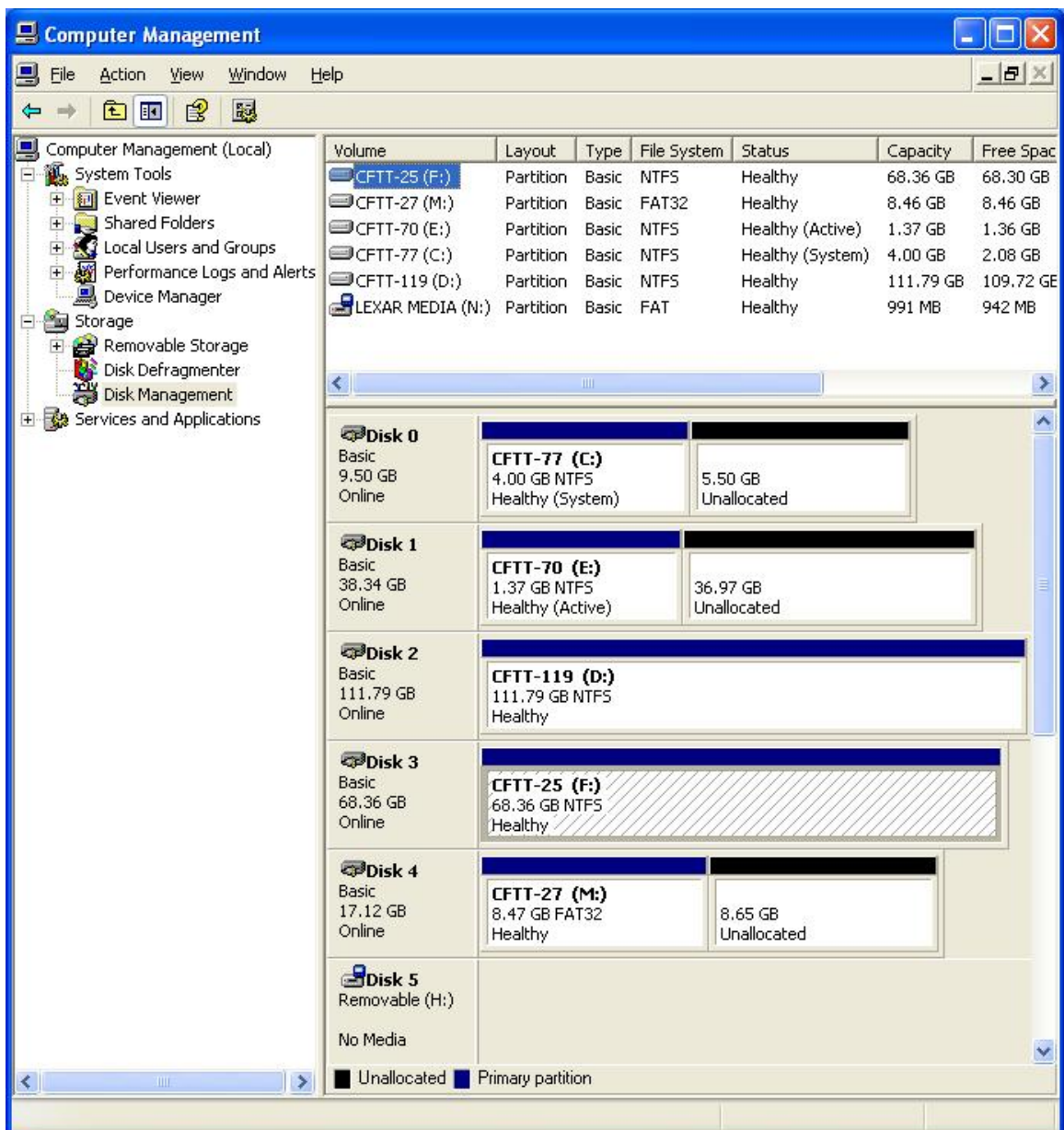
The tool failed to produce the expected result. The pattern of protection did not affect the ability of the tool to protect designated drives but the protection applied failed to block all commands in the protected categories. The protection applied for protected drives was identical to tests SWB-03, SWB-04, and SWB-06.

9.19 Test case SWB-19

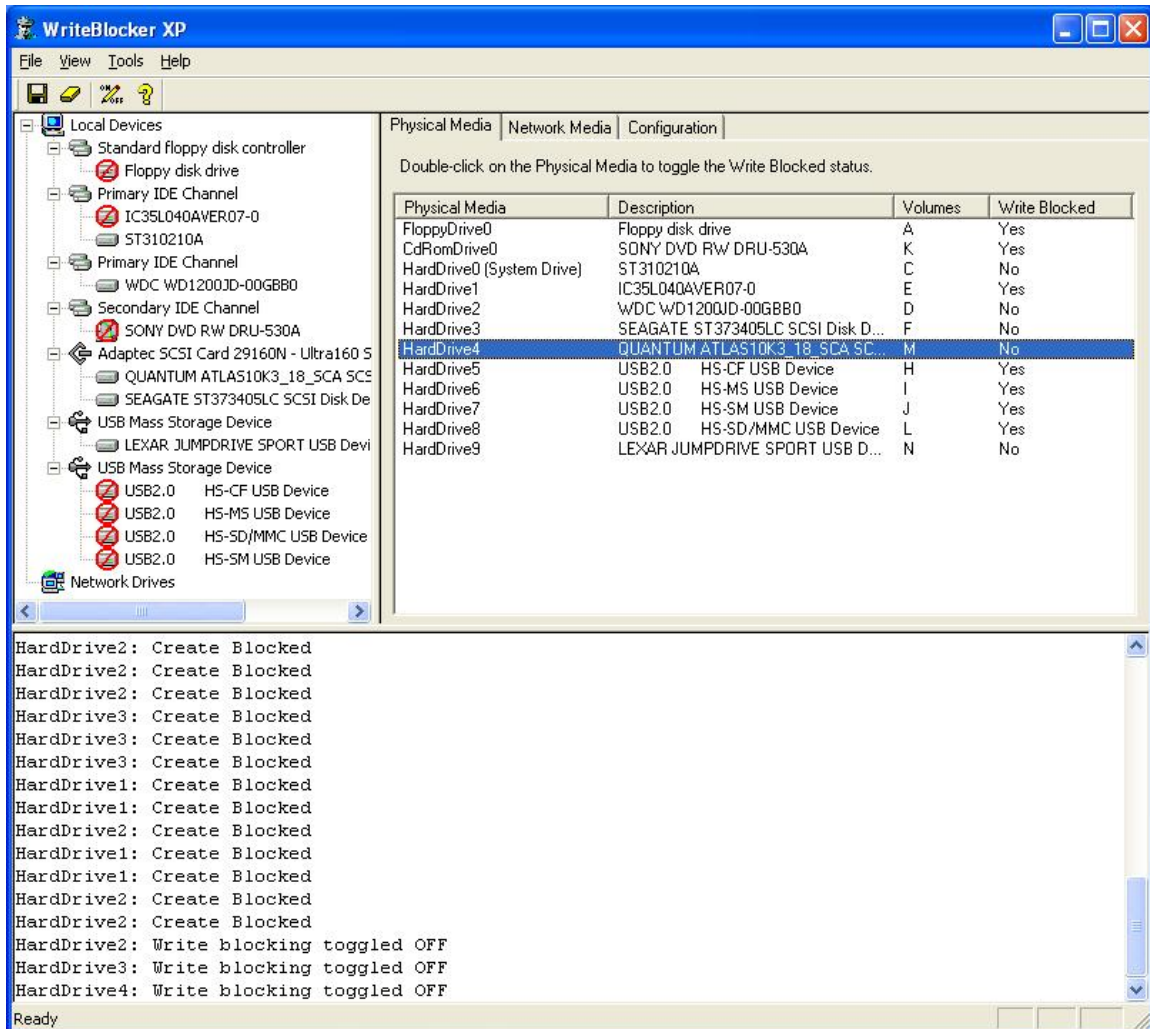
This case tests the tool's compliance with optional assertions SWB-AO-01 through SWB-AO-06. It issues all possible commands to a set of four drives protected with the pattern FIRST. The expected result of this test is the tool will:

- Block all commands from the WRITE, VENDOR_SPECIFIC, and UNDEFINED categories issued to protected drives
- Pass all commands from the READ and OTHER categories issued to protected drives
- Pass all commands from all categories issued to unprotected drives

9.19.1. Hard disk configuration



9.19.2. Write blocker configuration



9.19.3. Test output summary

NIST Software Write Blocker Test Suite V1.2
Thu Sep 08 08:31:10 2005

Test case: SWB-19
Command set: RWOVU
Number of drives: 4
Protection pattern: PUUU
Test administered by: DPA
Details logged to file: SWB-19.log

**** Test results summary (see logfile for details) ****

Testing device \\.\Physical Drive1
Device is software WRITE PROTECTED

Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	4	4	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	22	12	34
Other CDB's	62	0	62
Vendor Specific CDB's	80	0	80
Undefined CDB's	53	0	53

Testing device \\.\Physical Drive2
Device is software WRITE ENABLED

Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	8	0	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	34	0	34
Other CDB's	62	0	62
Vendor Specific CDB's	80	0	80
Undefined CDB's	53	0	53

Testing device \\.\Physical Drive3
Device is software WRITE ENABLED

Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	8	0	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	34	0	34
Other CDB's	62	0	62
Vendor Specific CDB's	80	0	80
Undefined CDB's	53	0	53

Testing device \\.\PhysicalDrive4 Device is software WRITE ENABLED			
Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	8	0	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	34	0	34
Other CDB's	62	0	62
Vendor SPeci fic CDB's	80	0	80
Undefined CDB's	53	0	53

9.19.4. Hard disk hash results

Drive Identification		Computed	SHA1 Value
\\.\PhysicalDrive1 (CFTT-70)	P	Before	7CA790CE7D88AE88DB474EA036D2FBA0CBE46609
		After	7CA790CE7D88AE88DB474EA036D2FBA0CBE46609
\\.\PhysicalDrive2 (CFTT-119)	U	Before	336468E49C86BCF47D6B6EC157C83F6546F680E7
		After	0D65AB595B26DAB353A9DA4B9D41AF8894912510
\\.\PhysicalDrive3 (CFTT-25)	U	Before	1855E34326E0786F34737DDC72197977980BBB77
		After	E465187EE396FFA8AEEB2F6E8FA0957A02AC1FBD
\\.\PhysicalDrive4 (CFTT-27)	U	Before	C4848A0D8BB04D5D684A51F966BE009C7E47EFAA
		After	C4848A0D8BB04D5D684A51F966BE009C7E47EFAA

9.19.5. Test results analysis

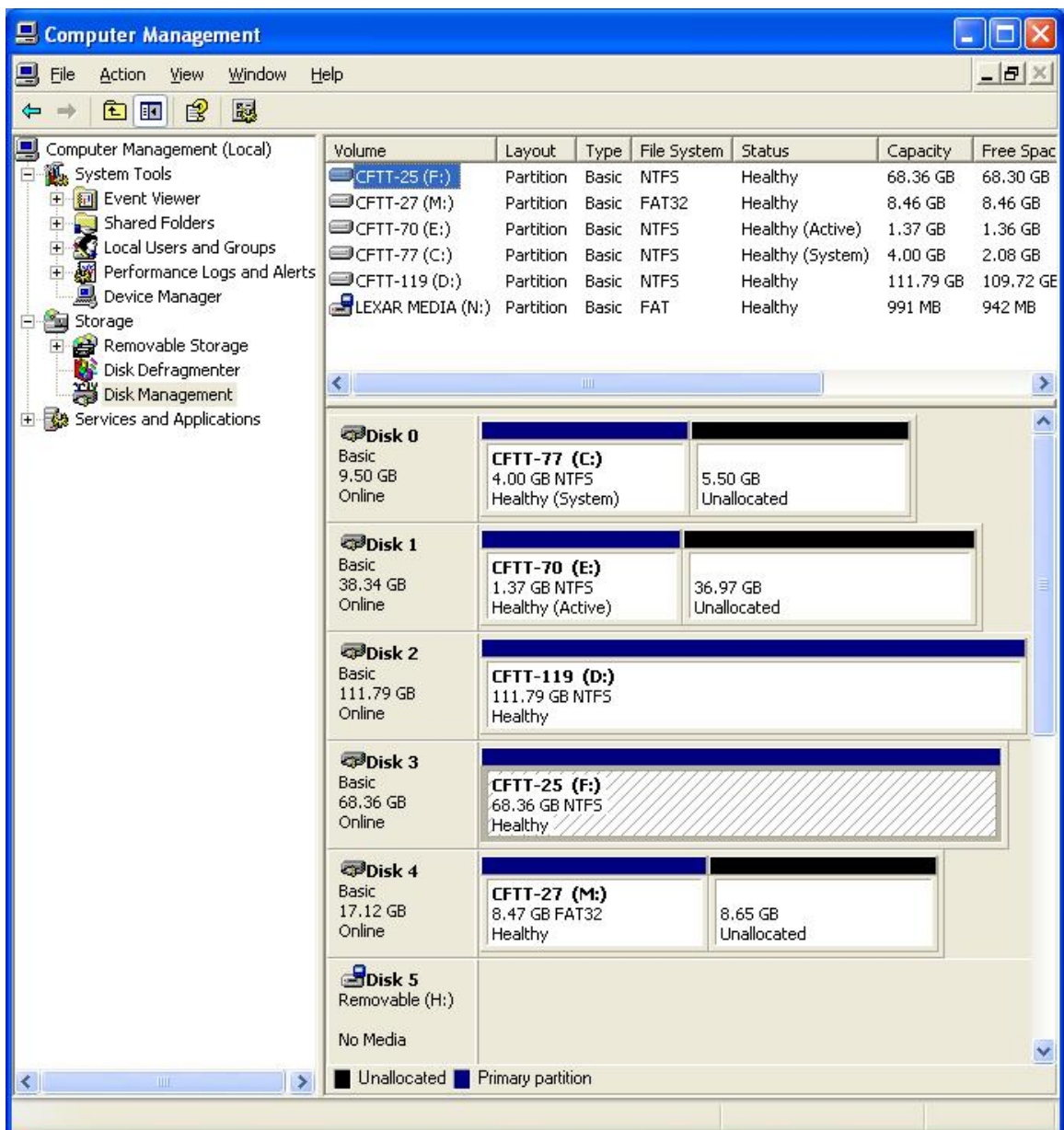
The tool failed to produce the expected result. The pattern of protection did not affect the ability of the tool to protect designated drives but the protection applied failed to block all commands in the protected categories. The protection applied for protected drives was identical to tests SWB-03, SWB-04, and SWB-06.

9.20 Test case SWB-20

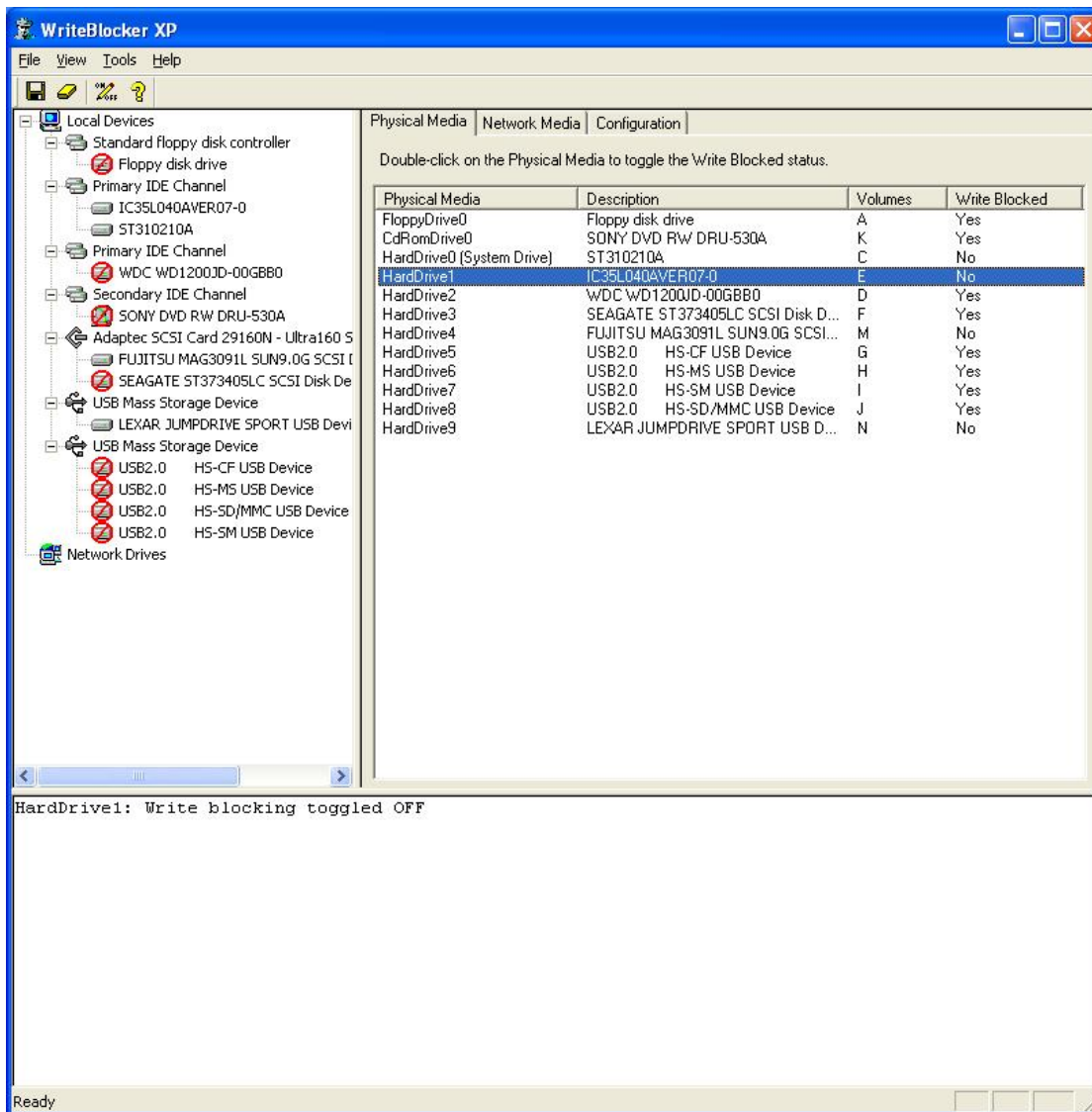
This case tests the tool's compliance with optional assertions SWB-AO-01 through SWB-AO-06. It issues all possible commands to a set of four drives protected with the pattern MIDDLE. The expected result of this test is the tool will:

- Block all commands from the WRITE, VENDOR_SPECIFIC, and UNDEFINED categories issued to protected drives
- Pass all commands from the READ and OTHER categories issued to protected drives
- Pass all commands from all categories issued to unprotected drives

9.20.1. Hard disk configuration



9.20.2. Write blocker configuration



9.20.3. Test output summary

NIST Software Write Blocker Test Suite V1.2

Thu Nov 17 10:50:44 2005

Test case: SWB-20

Command set: RWOVU

Number of drives: 4

Protection pattern: UPPU

**** Test results summary (see DETAILS.log for details) ****

Testing device \\.\Physical Drive1

Device is software WRITE ENABLED

Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	8	0	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	34	0	34
Other CDB's	62	0	62
Vendor Specific CDB's	80	0	80
Undefined CDB's	53	0	53

Testing device \\.\Physical Drive2

Device is software WRITE PROTECTED

Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	4	4	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	22	12	34
Other CDB's	62	0	62
Vendor Specific CDB's	80	0	80
Undefined CDB's	53	0	53

Testing device \\.\Physical Drive3

Device is software WRITE PROTECTED

Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	4	4	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	22	12	34
Other CDB's	62	0	62
Vendor Specific CDB's	80	0	80
Undefined CDB's	53	0	53

Testing device \\.\Physical Drive4

Device is software WRITE ENABLED

Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	8	0	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	34	0	34
Other CDB's	62	0	62
Vendor Specific CDB's	80	0	80
Undefined CDB's	53	0	53

9.20.4. Hard disk hash results

Drive Identification		Computed	SHA1 Value
\\.\PhysicalDrive1 (CFTT-70)	U	Before	7CA790CE7D88AE88DB474EA036D2FBA0CBE46609
		After	312276340EC7213BB421A0E8FC8A740E134952F4
\\.\PhysicalDrive2 (CFTT-119)	P	Before	0D65AB595B26DAB353A9DA4B9D41AF8894912510
		After	0D65AB595B26DAB353A9DA4B9D41AF8894912510
\\.\PhysicalDrive3 (CFTT-25)	P	Before	E465187EE396FFA8AEEB2F6E8FA0957A02AC1FBD
		After	E465187EE396FFA8AEEB2F6E8FA0957A02AC1FBD
\\.\PhysicalDrive4 (CFTT-27)	U	Before	C4848A0D8BB04D5D684A51F966BE009C7E47EFAA
		After	C4848A0D8BB04D5D684A51F966BE009C7E47EFAA

9.20.5. Test results analysis

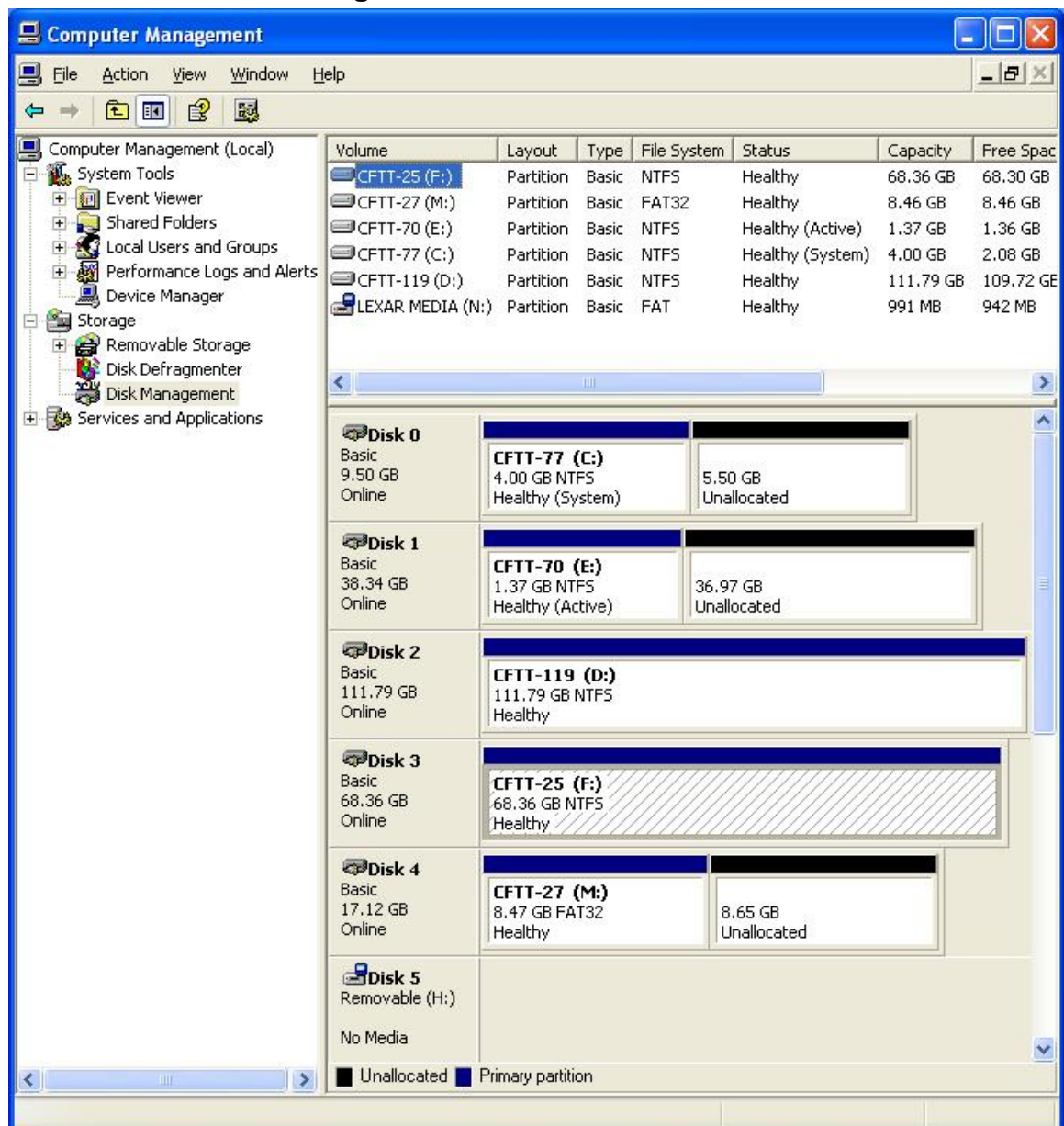
The tool failed to produce the expected result. The pattern of protection did not affect the ability of the tool to protect designated drives but the protection applied failed to block all commands in the protected categories. The protection applied for protected drives was identical to tests SWB-03, SWB-04, and SWB-06.

9.21 Test case SWB-21

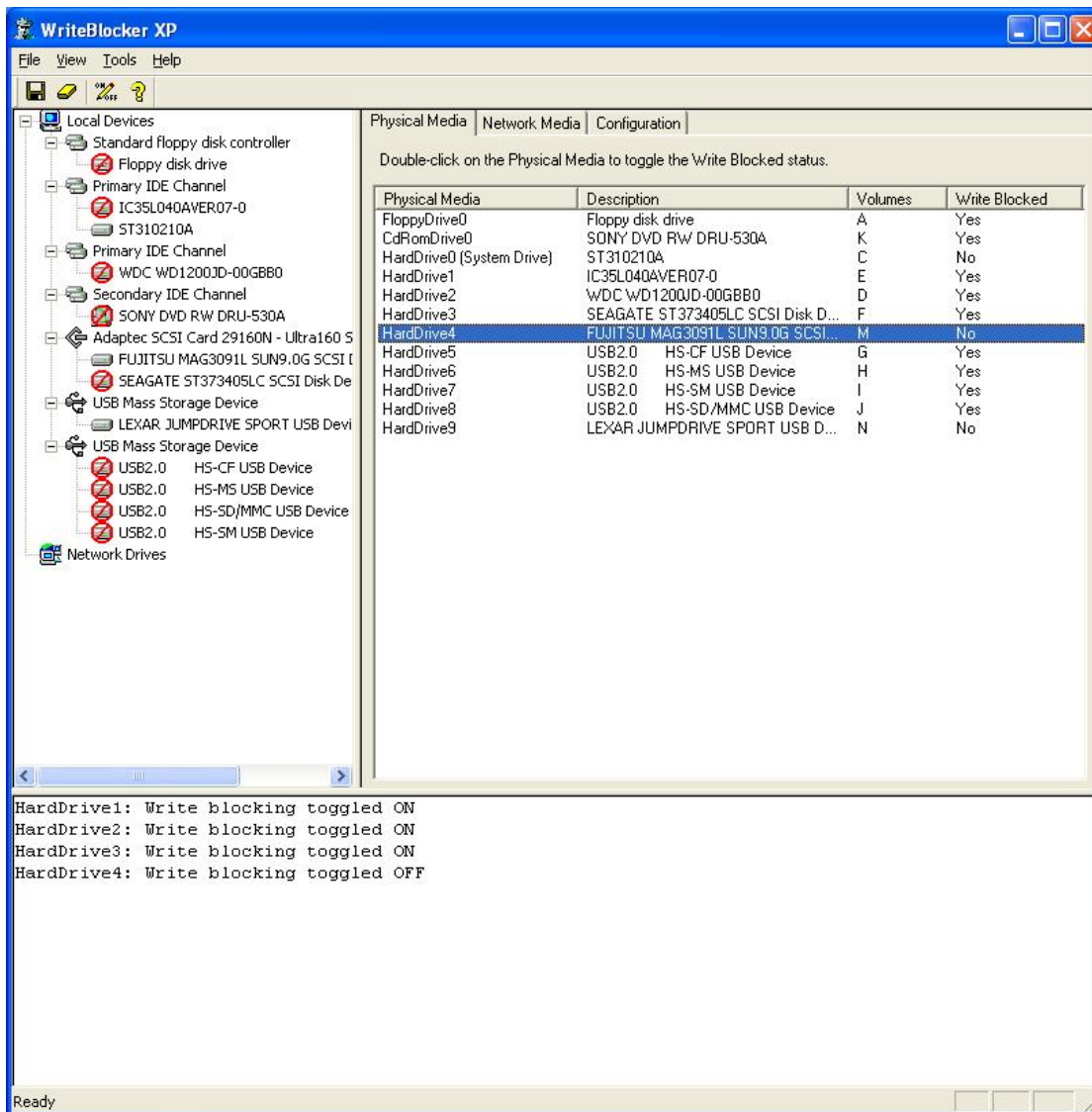
This case tests the tool's compliance with optional assertions SWB-AO-01 through SWB-AO-06. It issues all possible commands to a set of four drives protected with the pattern NOT_LAST. The expected result of this test is the tool will:

- Block all commands from the WRITE, VENDOR_SPECIFIC, and UNDEFINED categories issued to protected drives
- Pass all commands from the READ and OTHER categories issued to protected drives
- Pass all commands from all categories issued to unprotected drives

9.21.1. Hard disk configuration



9.21.2. Write blocker configuration



9.21.3. Test output summary

NIST Software Write Blocker Test Suite V1.2

Wed Dec 07 10:36:05 2005

Test case: SWB-21

Command set: RWOVU

Number of drives: 4

Protection pattern: PPPU

**** Test results summary (see DETAILS.log for details) ****

Testing device \\.\Physical Drive1

Device is software WRITE PROTECTED

Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	4	4	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	22	12	34
Other CDB's	62	0	62
Vendor Specific CDB's	80	0	80
Undefined CDB's	53	0	53

Testing device \\.\Physical Drive2

Device is software WRITE PROTECTED

Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	4	4	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	22	12	34
Other CDB's	62	0	62
Vendor Specific CDB's	80	0	80
Undefined CDB's	53	0	53

Testing device \\.\Physical Drive3

Device is software WRITE PROTECTED

Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	4	4	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	22	12	34
Other CDB's	62	0	62
Vendor Specific CDB's	80	0	80
Undefined CDB's	53	0	53

Testing device \\.\Physical Drive4

Device is software WRITE ENABLED

Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	8	0	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	34	0	34
Other CDB's	62	0	62
Vendor Specific CDB's	80	0	80
Undefined CDB's	53	0	53

9.21.4. Hard disk hash results

Drive Identification		Computed	SHA1 Value
\\.\PhysicalDrive1 (CFTT-70)	P	Before	312276340EC7213BB421A0E8FC8A740E134952F4
		After	312276340EC7213BB421A0E8FC8A740E134952F4
\\.\PhysicalDrive2 (CFTT-119)	P	Before	0D65AB595B26DAB353A9DA4B9D41AF8894912510
		After	0D65AB595B26DAB353A9DA4B9D41AF8894912510
\\.\PhysicalDrive3 (CFTT-25)	P	Before	9209D850F541DBC1DC68B68255112FBCAF316FB3
		After	9209D850F541DBC1DC68B68255112FBCAF316FB3
\\.\PhysicalDrive4 (CFTT-27)	U	Before	C4848A0D8BB04D5D684A51F966BE009C7E47EFAA
		After	C4848A0D8BB04D5D684A51F966BE009C7E47EFAA

9.21.5. Test results analysis

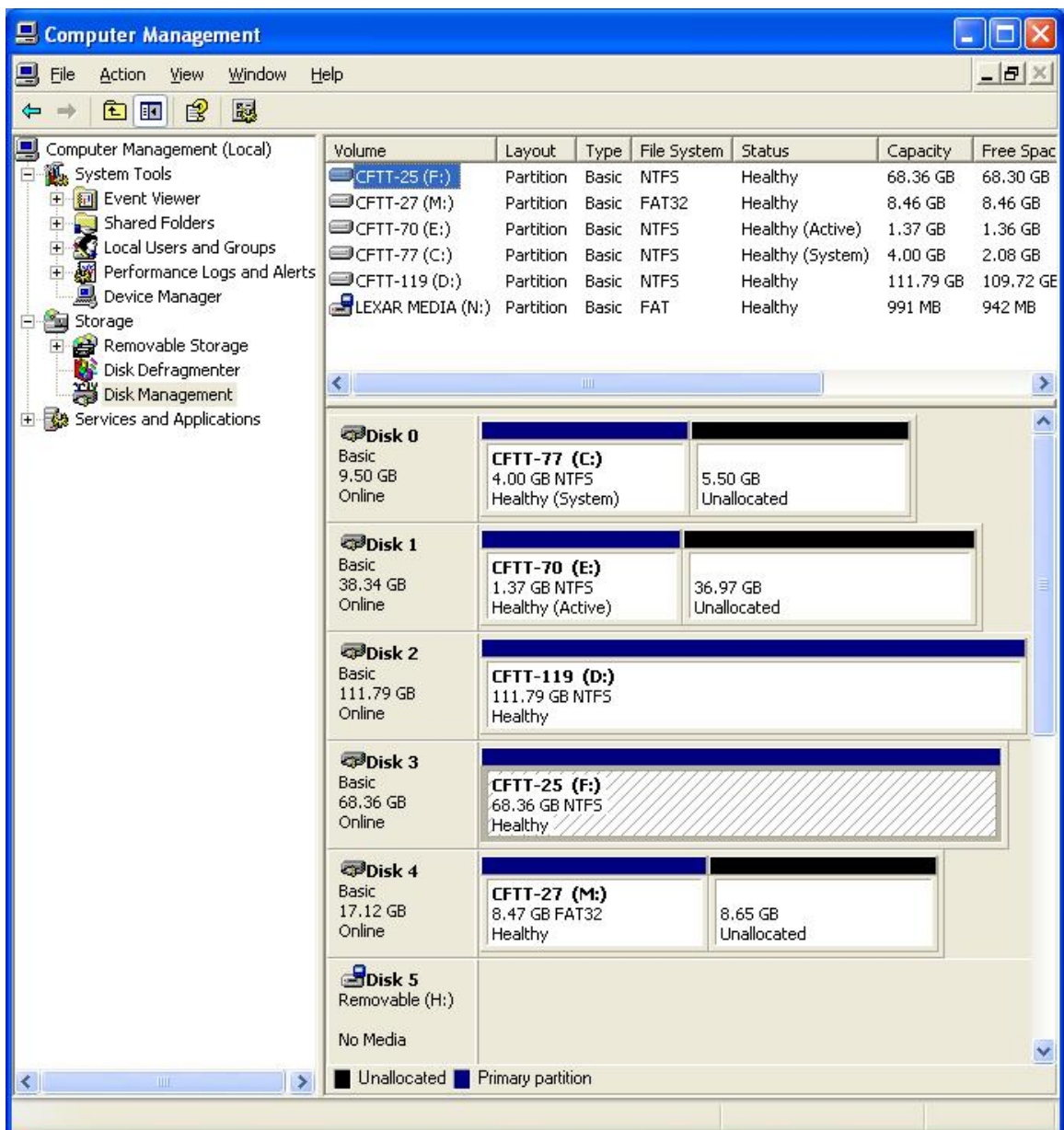
The tool failed to produce the expected result. The pattern of protection did not affect the ability of the tool to protect designated drives but the protection applied failed to block all commands in the protected categories. The protection applied for protected drives was identical to tests SWB-03, SWB-04, and SWB-06.

9.22 Test case SWB-22

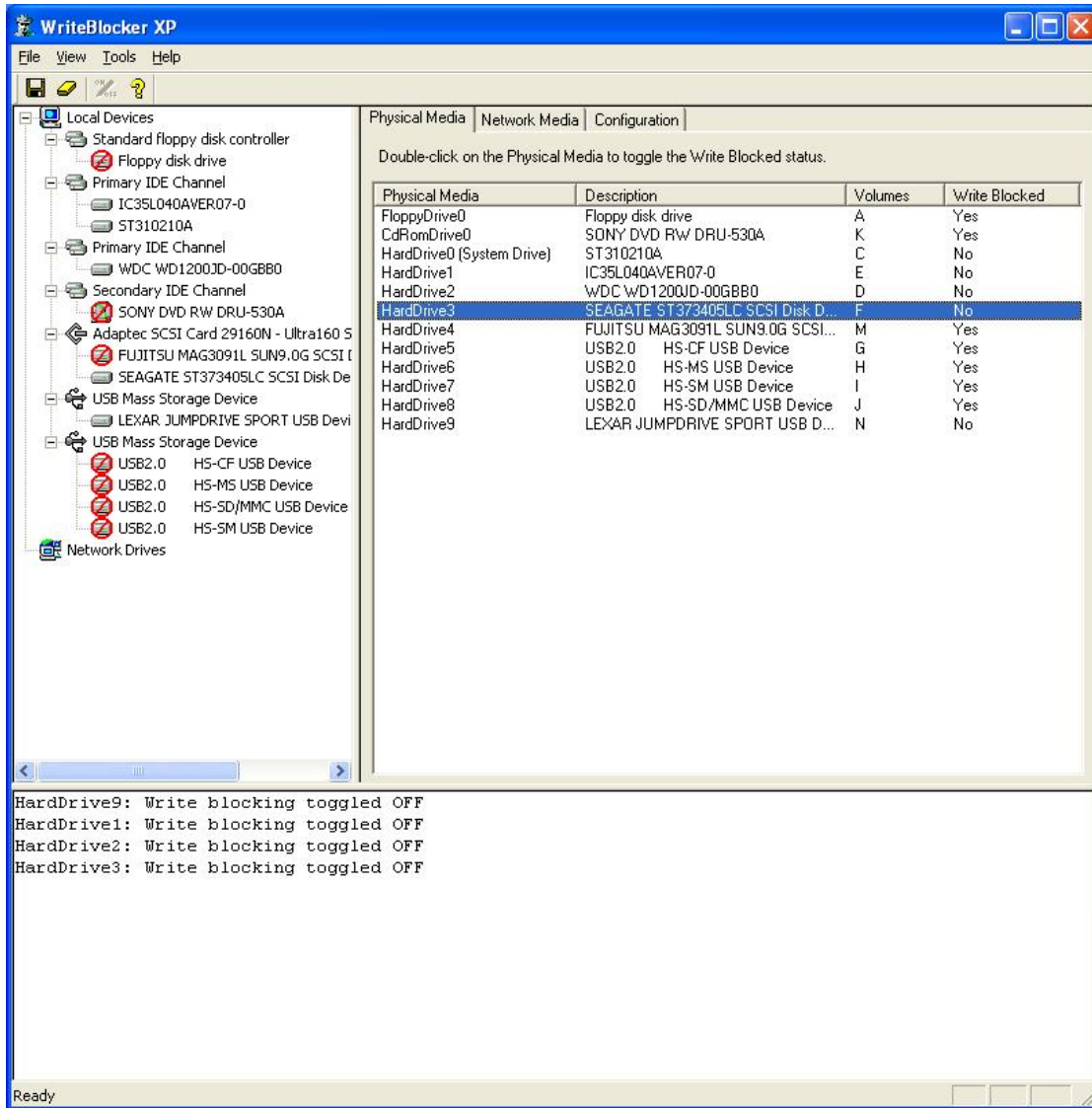
This case tests the tool's compliance with optional assertions SWB-AO-01 through SWB-AO-06. It issues all possible commands to a set of four drives protected with the pattern LAST. The expected result of this test is the tool will:

- Block all commands from the WRITE, VENDOR_SPECIFIC, and UNDEFINED categories issued to protected drives
- Pass all commands from the READ and OTHER categories issued to protected drives
- Pass all commands from all categories issued to unprotected drives

9.22.1. Hard disk configuration



9.22.2. Write blocker configuration



9.22.3. Test output summary

NIST Software Write Blocker Test Suite V1.2
Thu Dec 08 11:08:37 2005

Test case: SWB-22
Command set: RWOUV
Number of drives: 4
Protection pattern: UUUP

**** Test results summary (see DETAILS.log for details) ****

Testing device \\.\Physical Drive1
Device is software WRITE ENABLED

Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	8	0	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	34	0	34
Other CDB's	62	0	62
Vendor SPeci fic CDB's	80	0	80
Undefined CDB's	53	0	53

Testing device \\.\Physical Drive2
Device is software WRITE ENABLED

Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	8	0	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	34	0	34
Other CDB's	62	0	62
Vendor SPeci fic CDB's	80	0	80
Undefined CDB's	53	0	53

Testing device \\.\Physical Drive3
Device is software WRITE ENABLED

Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	8	0	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	34	0	34
Other CDB's	62	0	62
Vendor SPeci fic CDB's	80	0	80
Undefined CDB's	53	0	53

Testing device \\.\Physical Drive4

Device is software WRITE PROTECTED			
Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	4	4	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	22	12	34
Other CDB's	62	0	62
Vendor Specific CDB's	80	0	80
Undefined CDB's	53	0	53

9.22.4. Hard disk hash results

Drive Identification		Computed	SHA1 Value
\\.\PhysicalDrive1 (CFTT-70)	U	Before	3AF5776C4DA23E4D139360428C33B6BC6C29F126
		After	A839904C750EEE543EDFB8ABF61E907D877D1EC1
\\.\PhysicalDrive2 (CFTT-119)	U	Before	28BA3B10D66DD4CED4F84C680C6E04F4227EC6F
		After	14D483C72DBC4C438C625170A3CCD08A60C65897
\\.\PhysicalDrive3 (CFTT-25)	U	Before	9209D850F541DBC1DC68B68255112FBCAF316FB3
		After	F34C6C4F96A2D9C41F3B962B5546B2BDB597A4F4
\\.\PhysicalDrive4 (CFTT-27)	P	Before	C4848A0D8BB04D5D684A51F966BE009C7E47EFAA
		After	C4848A0D8BB04D5D684A51F966BE009C7E47EFAA

9.22.5. Test results analysis

The tool failed to produce the expected result. The number of drives configured and the pattern of protection applied did not alter the ability of the tool to protect designated drives. However, the tool failed to block all commands in the protected categories. The protection failures observed were identical to those of tests SWB-03, SWB-04, and SWB-06.

9.23 Test case SWB-23

This case tests the tool's compliance with optional assertions SWB-AO-01 through SWB-AO-08. It is run using the BOOT protocol, in which all configured drives are protected, the system is rebooted and all possible commands issued to all drives. The expected result of this test is the tool will:

- Block all commands from the WRITE, VENDOR_SPECIFIC, and UNDEFINED categories issued to protected drives
- Pass all commands from the READ and OTHER categories issued to protected drives
- Pass all commands from all categories issued to unprotected drives
- Display a message indicating each command blocked

9.23.1. Hard disk configuration

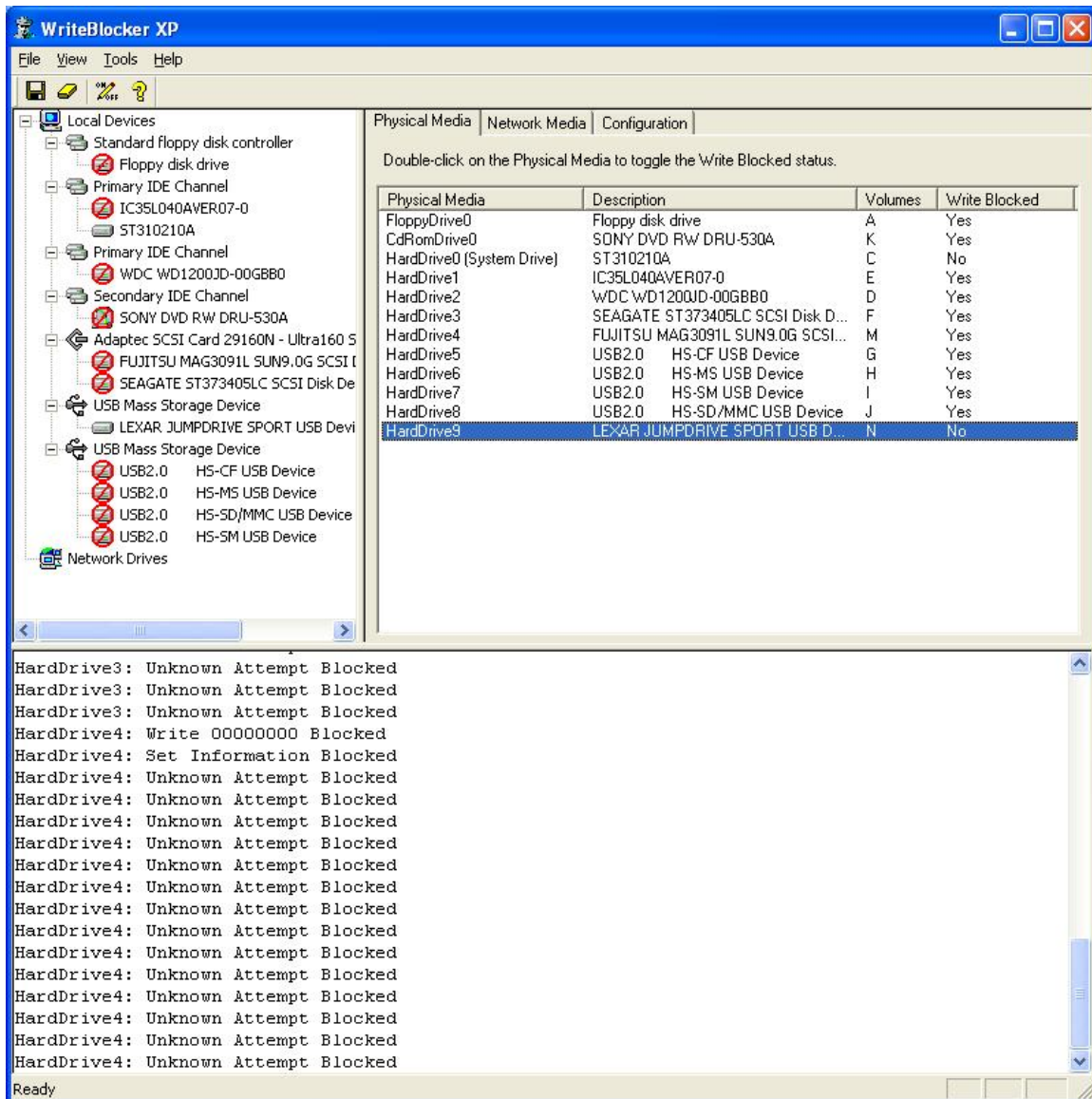
The screenshot displays the Windows 'Computer Management' console. The left pane shows the 'Storage' tree with 'Disk Management' selected. The main pane shows a table of volumes and a detailed view of disks below.

Volume	Layout	Type	File System	Status	Capacity	Free Space
CFTT-25 (F:)	Partition	Basic	NTFS	Healthy	68.36 GB	68.30 GB
CFTT-27 (M:)	Partition	Basic	FAT32	Healthy	8.46 GB	8.46 GB
CFTT-70 (E:)	Partition	Basic	NTFS	Healthy (Active)	1.37 GB	1.36 GB
CFTT-77 (C:)	Partition	Basic	NTFS	Healthy (System)	4.00 GB	2.08 GB
CFTT-119 (D:)	Partition	Basic	NTFS	Healthy	111.79 GB	109.72 GB
LEXAR MEDIA (N:)	Partition	Basic	FAT	Healthy	991 MB	942 MB

Disk	Type	Capacity	Online	Volume	File System	Status	Free Space
Disk 0	Basic	9.50 GB	Online	CFTT-77 (C:)	4.00 GB NTFS	Healthy (System)	5.50 GB Unallocated
Disk 1	Basic	38.34 GB	Online	CFTT-70 (E:)	1.37 GB NTFS	Healthy (Active)	36.97 GB Unallocated
Disk 2	Basic	111.79 GB	Online	CFTT-119 (D:)	111.79 GB NTFS	Healthy	
Disk 3	Basic	68.36 GB	Online	CFTT-25 (F:)	68.36 GB NTFS	Healthy	
Disk 4	Basic	17.12 GB	Online	CFTT-27 (M:)	8.47 GB FAT32	Healthy	8.65 GB Unallocated
Disk 5	Removable (H:)			No Media			

Legend: ■ Unallocated ■ Primary partition

9.23.2. Write blocker configuration



9.23.3. Test output summary

NIST Software Write Blocker Test Suite V1.2

Wed Dec 07 13:43:35 2005

Test case: SWB-23

Command set: RWOVU

Number of drives: 4

Protection pattern: PPPP

**** Test results summary (see DETAILS.log for details) ****

Testing device \\.\Physical Drive1

Device is software WRITE PROTECTED

Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	4	4	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	22	12	34
Other CDB's	62	0	62
Vendor Specific CDB's	80	0	80
Undefined CDB's	53	0	53

Testing device \\.\Physical Drive2

Device is software WRITE PROTECTED

Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	4	4	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	22	12	34
Other CDB's	62	0	62
Vendor Specific CDB's	80	0	80
Undefined CDB's	53	0	53

Testing device \\.\Physical Drive3

Device is software WRITE PROTECTED

Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	4	4	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	22	12	34
Other CDB's	62	0	62
Vendor Specific CDB's	80	0	80
Undefined CDB's	53	0	53

Testing device \\.\Physical Drive4

Device is software WRITE PROTECTED

Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	4	4	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	22	12	34
Other CDB's	62	0	62
Vendor Specific CDB's	80	0	80
Undefined CDB's	53	0	53

9.23.4. Hard disk hash results

Drive Identification		Computed	SHA1 Value
\\.\PhysicalDrive1 (CFTT-70)	P	Before	3AF5776C4DA23E4D139360428C33B6BC6C29F126
		After	3AF5776C4DA23E4D139360428C33B6BC6C29F126
\\.\PhysicalDrive2 (CFTT-119)	P	Before	828BA3B10D66DD4CED4F84C680C6E04F4227EC6F
		After	828BA3B10D66DD4CED4F84C680C6E04F4227EC6F
\\.\PhysicalDrive3 (CFTT-25)	P	Before	9209D850F541DBC1DC68B68255112FBCAF316FB3
		After	9209D850F541DBC1DC68B68255112FBCAF316FB3
\\.\PhysicalDrive4 (CFTT-27)	P	Before	C4848A0D8BB04D5D684A51F966BE009C7E47EFAA
		After	C4848A0D8BB04D5D684A51F966BE009C7E47EFAA

9.23.5. Test results analysis

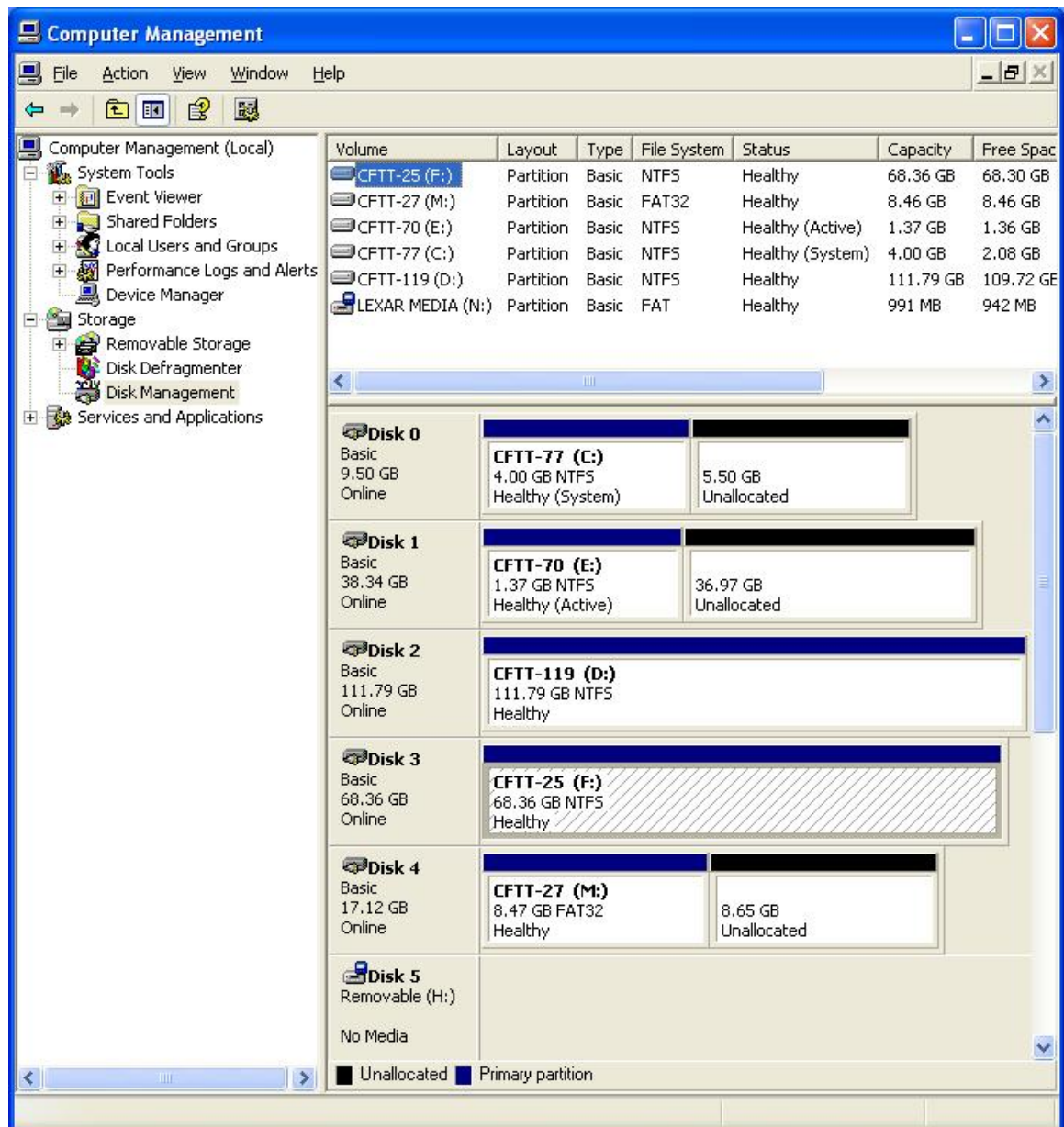
The tool failed to produce the expected result. The pattern of protection did not affect the ability of the tool to protect designated drives but the protection applied failed to block all commands in the protected categories. The protection applied for protected drives was identical to tests SWB-03, SWB-04, and SWB-06.

9.24 Test case SWB-24

This case tests the tool's compliance with mandatory assertions SWB-MO-03 through SWB-MO-09 and optional assertion SWB-AO-07. It is run using the UNINSTALL protocol, in which the tool is de-installed, the system is rebooted and all possible commands issued to all drives. The expected result of this test is:

- No command from any category will be blocked for any drive

9.24.1. Hard disk configuration



9.24.2. Write blocker configuration

None

9.24.3. Test output summary

```
NIST Software Write Blocker Test Suite V1.2
Thu Aug 25 10:35:33 2005

Test case:          SWB-24
Command set:        RWOVU
Number of drives:    4
Protection pattern: UUUU
Test administered by: DPA
Details logged to file: SWB-24.log

**** Test results summary (see logfile for details) ****

Testing device \\.\Physical Drive1
Device is software WRITE ENABLED

      Test Category          Allowed    Blocked    Total
-----
Read IRP's .....           4           0         4
Write IRP's .....           8           0         8
Other IRP's .....          15           0        15

Read CDB's .....           27           0        27
Write CDB's .....          34           0        34
Other CDB's .....          62           0        62
Vendor Specific CDB's ..... 80           0        80
Undefined CDB's .....       53           0        53

Testing device \\.\Physical Drive2
Device is software WRITE ENABLED

      Test Category          Allowed    Blocked    Total
-----
Read IRP's .....           4           0         4
Write IRP's .....           8           0         8
Other IRP's .....          15           0        15

Read CDB's .....           27           0        27
Write CDB's .....          34           0        34
Other CDB's .....          62           0        62
Vendor Specific CDB's ..... 80           0        80
Undefined CDB's .....       53           0        53

Testing device \\.\Physical Drive3
Device is software WRITE ENABLED

      Test Category          Allowed    Blocked    Total
-----
Read IRP's .....           4           0         4
Write IRP's .....           8           0         8
Other IRP's .....          15           0        15

Read CDB's .....           27           0        27
Write CDB's .....          34           0        34
```

Other CDB's	62	0	62
Vendor SPeci fi c CDB's	80	0	80
Unde fi ned CDB's	53	0	53
Testing device \\.\PhysicalDrive4 Device is software WRITE ENABLED			
Test Category	Al l owed	Bl ocked	Total
Read IRP's	4	0	4
Write IRP's	8	0	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	34	0	34
Other CDB's	62	0	62
Vendor SPeci fi c CDB's	80	0	80
Unde fi ned CDB's	53	0	53

9.24.4. Hard disk hash results

Drive Identification		Computed	SHA1 Value
\\.\PhysicalDrive1 (CFTT-70)	U	Before	N/A
		After	N/A
\\.\PhysicalDrive2 (CFTT-119)	U	Before	N/A
		After	N/A
\\.\PhysicalDrive3 (CFTT-25)	U	Before	N/A
		After	N/A
\\.\PhysicalDrive4 (CFTT-27)	U	Before	N/A
		After	N/A

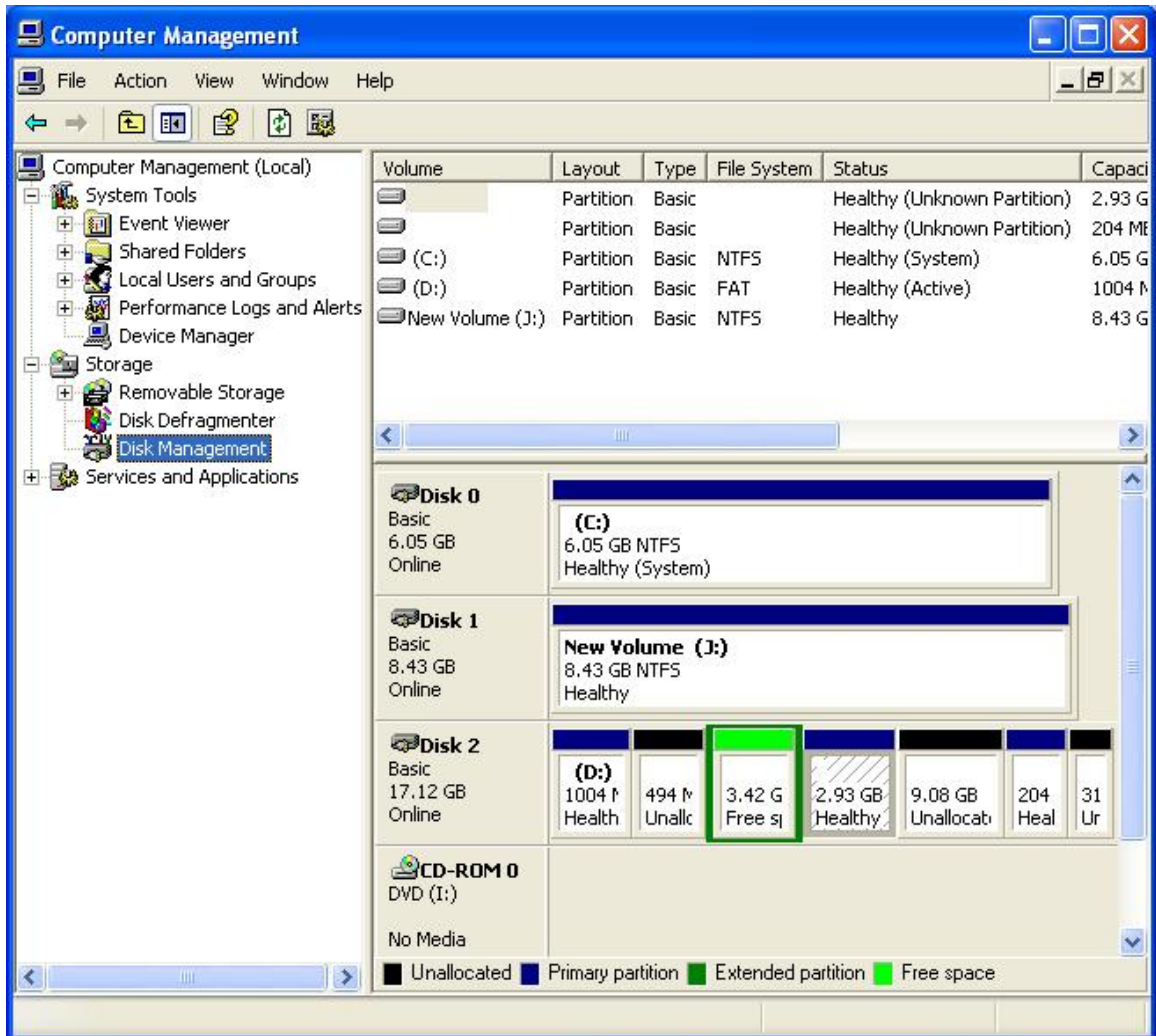
9.24.5. Test results analysis

The tool produced the expected result. No commands were blocked after the de-installation procedure was run and the system was rebooted.

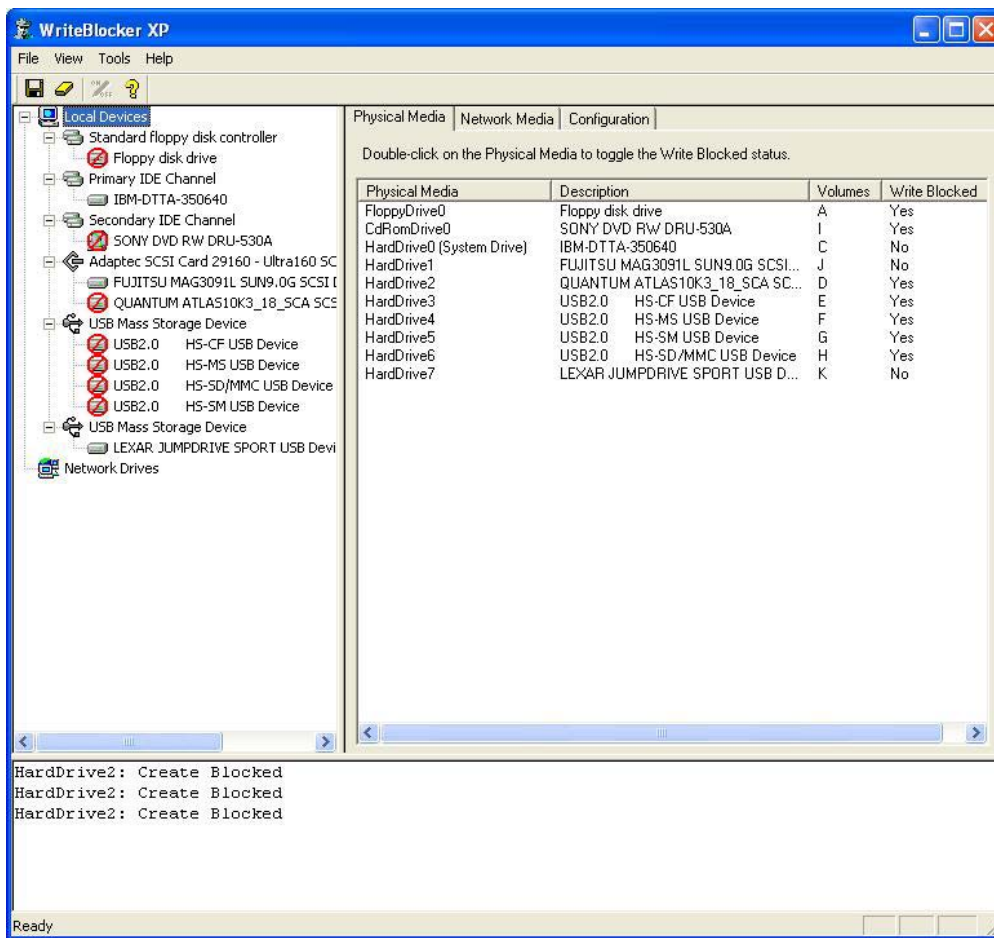
9.25 Test case SWB-25

This case tests the tool's compliance with mandatory assertion SWB-AM-10. The expected result of this test is that the IMAGE operation will fail with an I/O error and the disk hash of the test disk will be unchanged by the test.

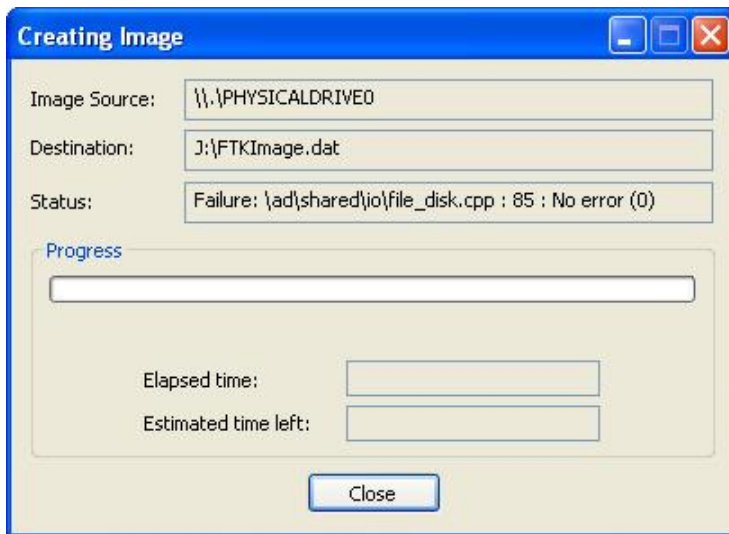
9.25.1. Hard disk configuration

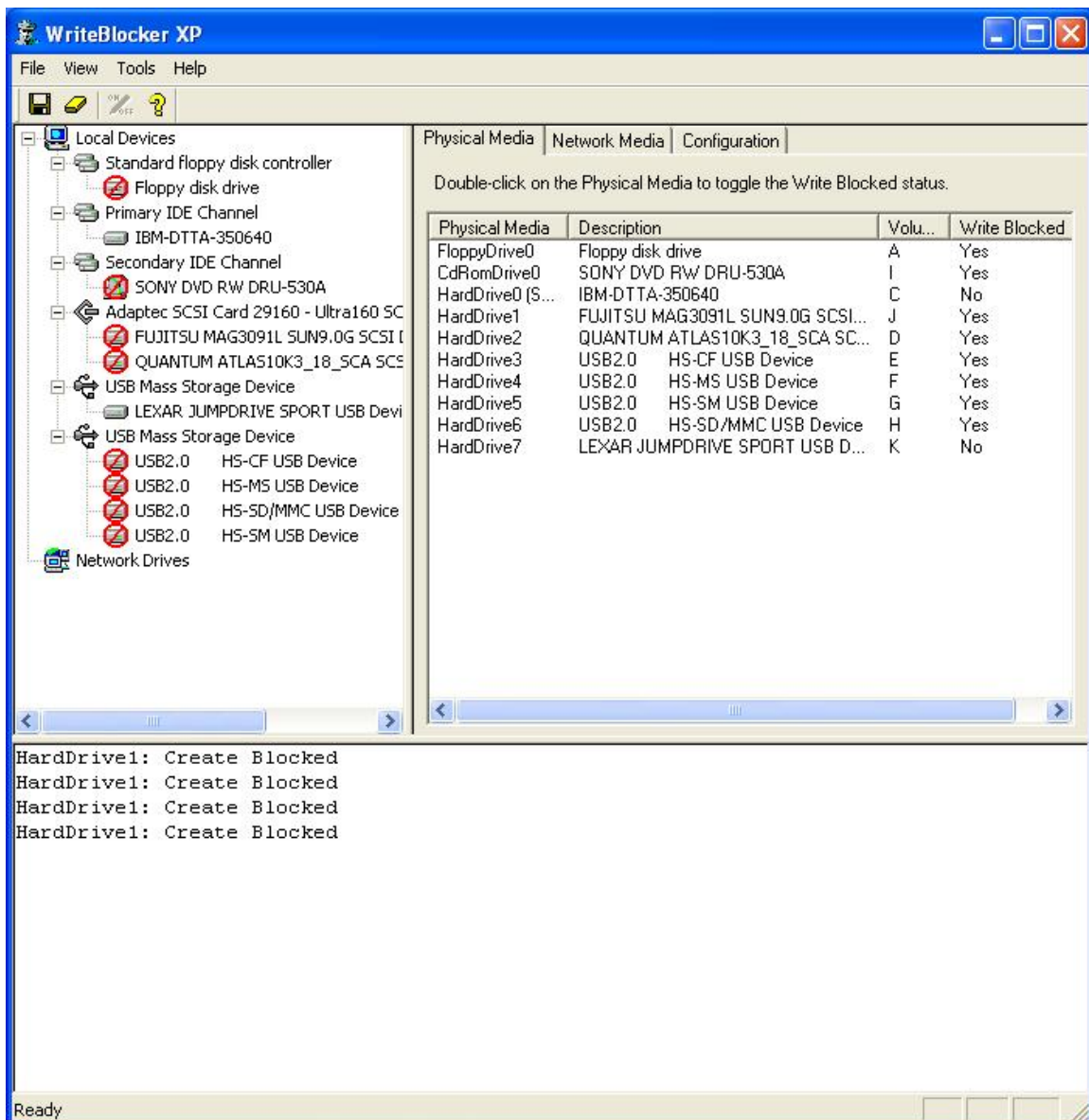


9.25.2. Write blocker configuration



9.25.3. Test output summary





9.25.4. Hard disk hash results

Drive Identification		Computed	SHA1 Value
\\.\PhysicalDrive1 (CFTT-26)	P	Before	233283A966083375DE84FOCF2B4A2BCEC73BC974
		After	233283A966083375DE84FOCF2B4A2BCEC73BC974

9.25.5. Test results analysis

The tool produced the expected result. The IMAGE operation failed with error number 85, 4 blocked commands (CREATE) were logged by the write blocker tool, and the hash value of the target disk was unchanged after the test.

This case test's the tools compliance with mandatory assertion SWB-AM-10 and optional assertion SWB-AO-08. The expected result of this test is that the ACQUIRE operation will fail with an I/O error, one or more blocked commands will be logged by the write blocker, and the disk hash of the test disk will be unchanged by the test.

Computer Management

File Action View Window Help

Computer Management (Local)

- System Tools
 - Event Viewer
 - Shared Folders
 - Local Users and Groups
 - Performance Logs and Alerts
 - Device Manager
- Storage
 - Removable Storage
 - Disk Defragmenter
 - Disk Management**
- Services and Applications

Volume	Layout	Type	File System	Status	Capacity
	Partition	Basic		Healthy (Unknown Partition)	2.93 GB
	Partition	Basic		Healthy (Unknown Partition)	204 MB
(C:)	Partition	Basic	NTFS	Healthy (System)	6.05 GB
(D:)	Partition	Basic	FAT	Healthy (Active)	1004 MB
New Volume (J:)	Partition	Basic	NTFS	Healthy	8.43 GB

Disk 0
Basic
6.05 GB
Online

(C:)
6.05 GB NTFS
Healthy (System)

Disk 1
Basic
8.43 GB
Online

New Volume (J:)
8.43 GB NTFS
Healthy

Disk 2
Basic
17.12 GB
Online

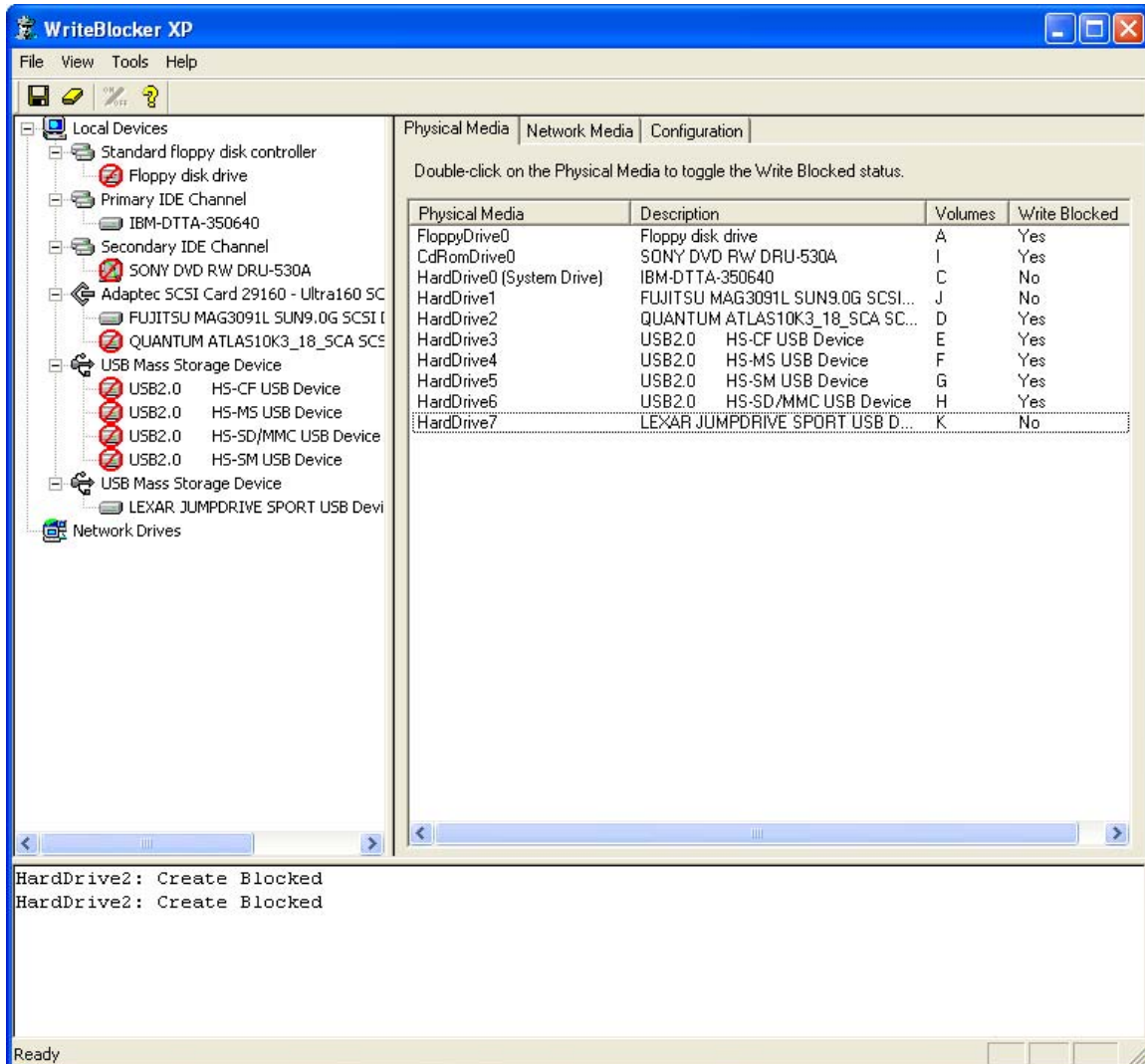
Volume	Layout	Type	File System	Status	Capacity	Free Space
(D:)	Partition	Basic	FAT	Healthy	1004 MB	3.42 GB

CD-ROM 0
DVD (I:)

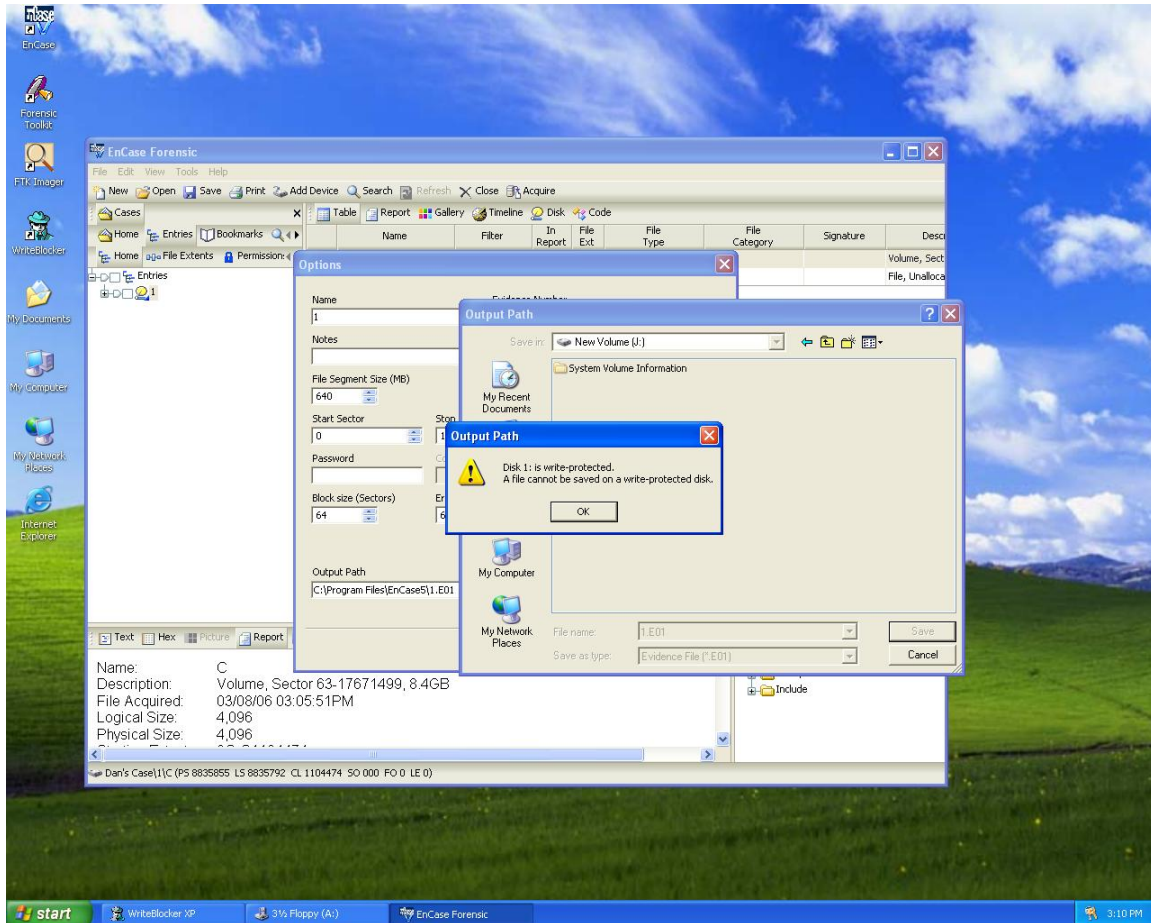
No Media

Unallocated Primary partition Extended partition Free space

9.26.2. Write blocker configuration



9.26.3. Test output summary



9.26.4. Hard disk hash results

Drive Identification		Computed	SHA1 Value
\\.\PhysicalDrive2	P	Before	233283A966083375DE84FOCF2B4A2BCEC73BC974
		After	233283A966083375DE84FOCF2B4A2BCEC73BC974

9.26.5. Test results analysis

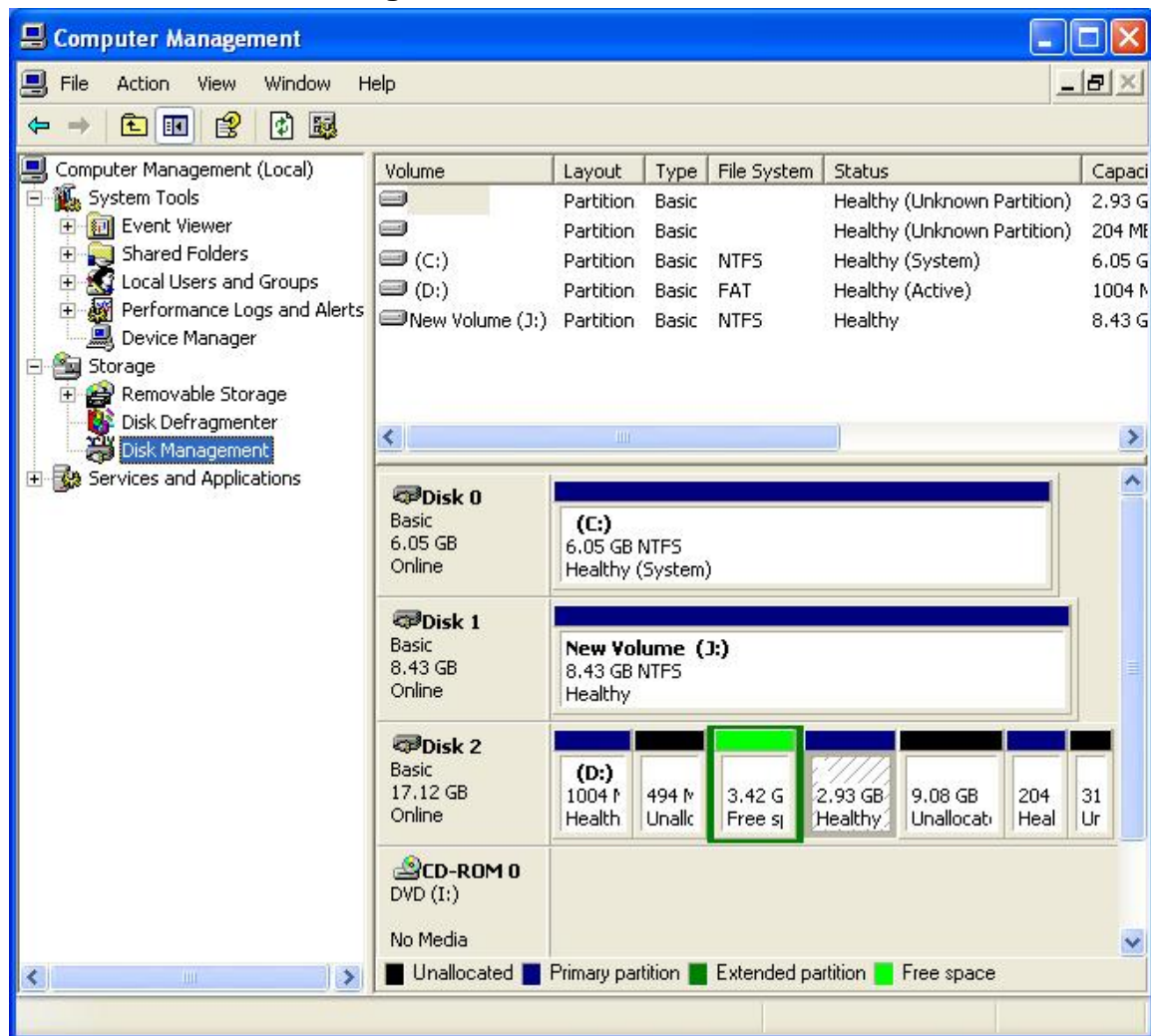
The test produced the expected result. The command failed with a write protection error on the output device, the write block tool logged 2 blocked commands (CREATE), and the hash value of the protected drive was unchanged after the test.

9.27 Test case SWB-27

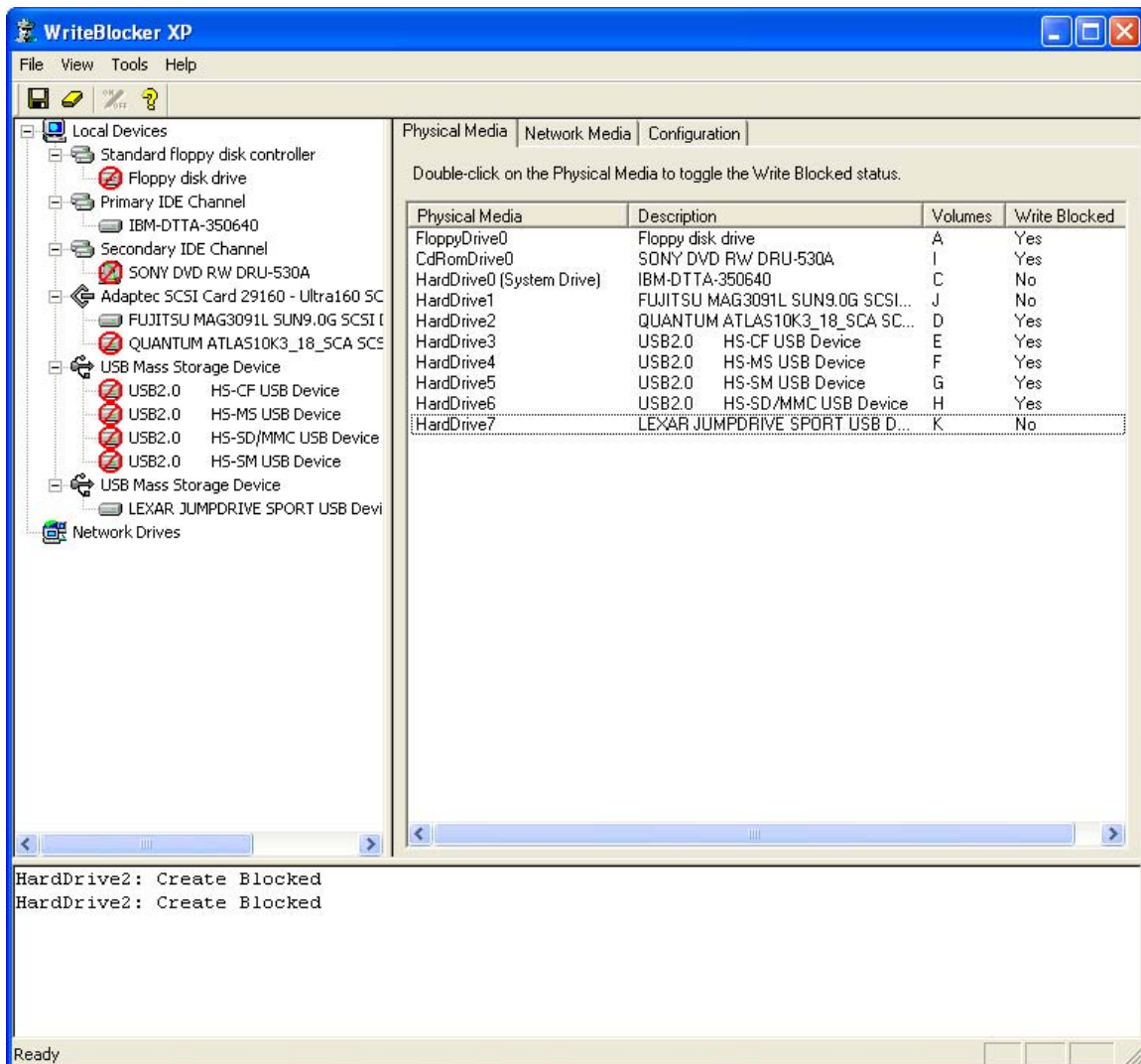
This case tests the tool's compliance with assertion SWB-AM-10. It is run using the Typical protocol. The expected result of this test is:

- The COPY command will fail with an error message
- The tool will display a message indicating each command blocked
- The hash value of the target disk will be unchanged after the test

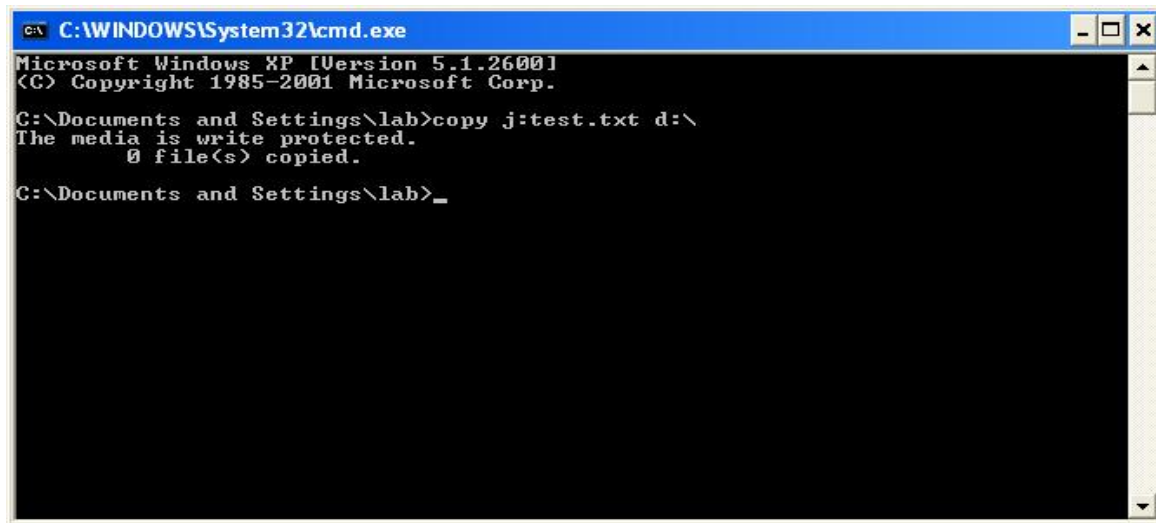
9.27.1. Hard disk configuration



9.27.2. Write blocker configuration



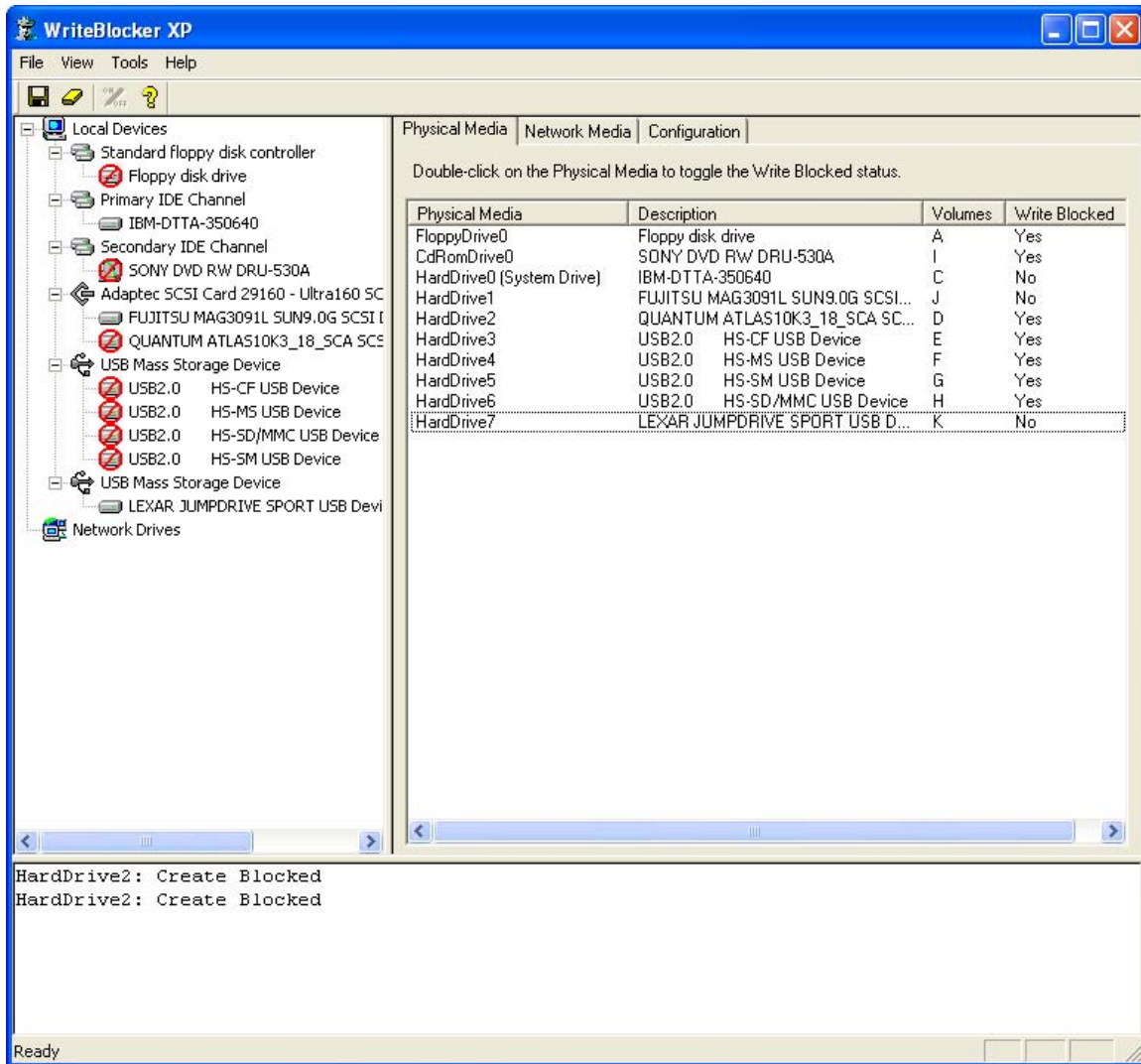
9.27.3. Test output summary



```
C:\WINDOWS\System32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\lab>copy j:test.txt d:\
The media is write protected.
    0 file(s) copied.

C:\Documents and Settings\lab>_
```



9.27.4. Hard disk hash results

Drive Identification		Computed	SHA1 Value
\\.\PhysicalDrive2	P	Before	233283A966083375DE84FOCF2B4A2BCEC73BC974
		After	233283A966083375DE84FOCF2B4A2BCEC73BC974

9.27.5. Test results analysis

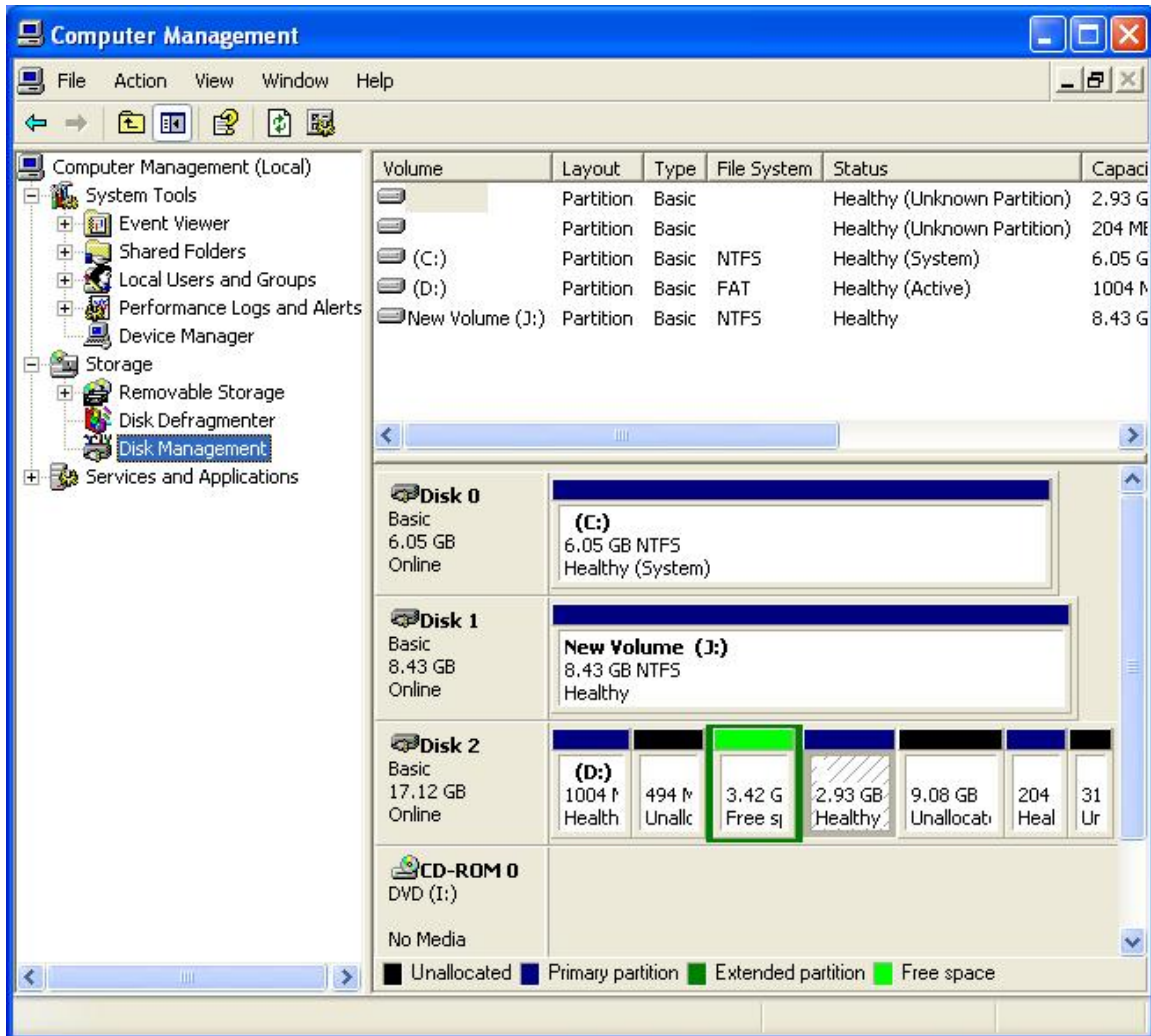
The tool produced the expected result. The COPY operation failed with a write protection error message, two blocked commands (CREATE) were logged by the write blocker tool, and the hash value of the target disk was unchanged after the test.

9.28 Test case SWB-28

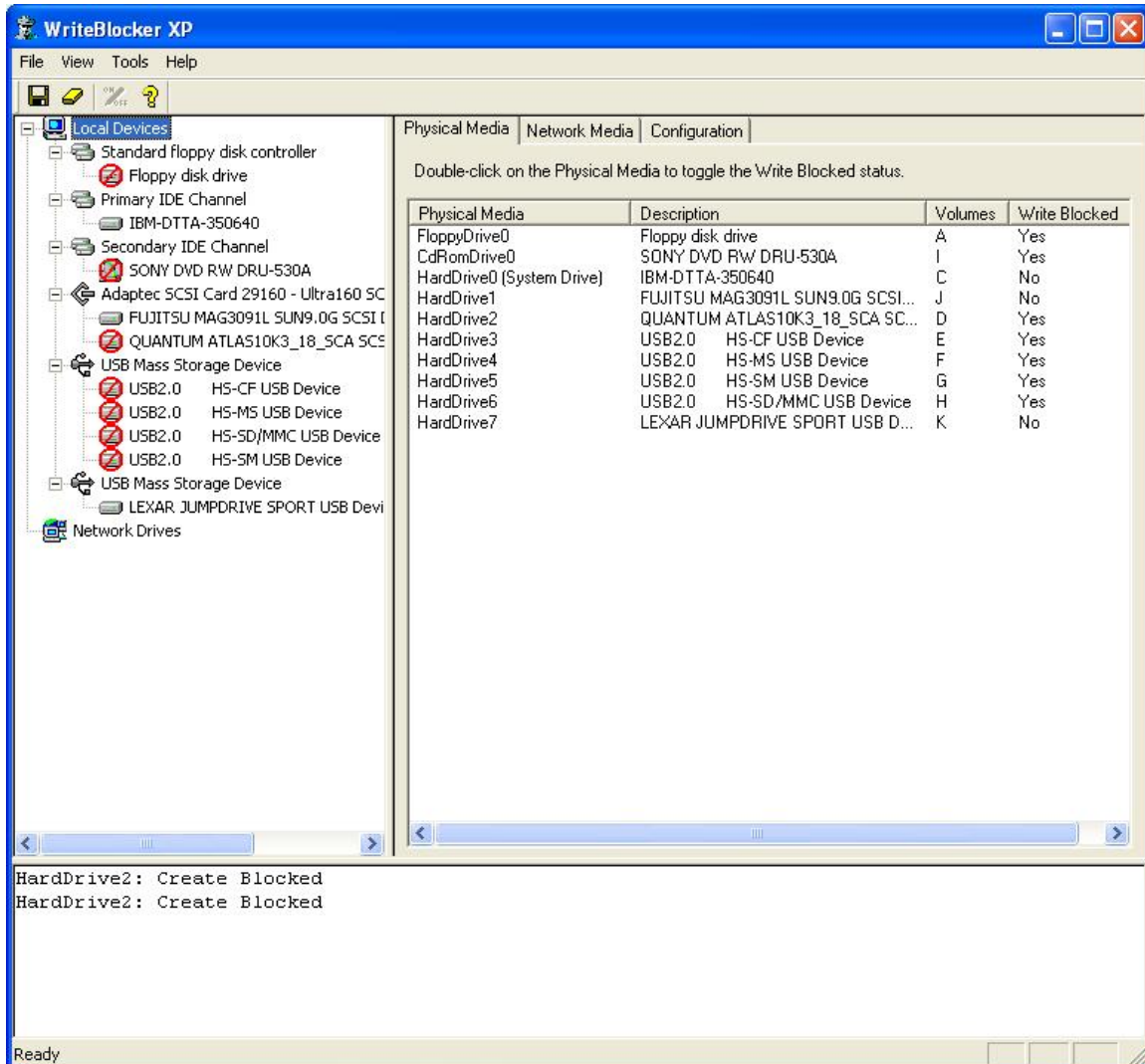
This case tests the tool's compliance with assertion SWB-AM-10. It is run using the Typical protocol. The expected result of this test is:

- The DROP operation will fail with an error message
- The tool will display a message indicating each command blocked
- The hash value of the target disk will be unchanged after the test

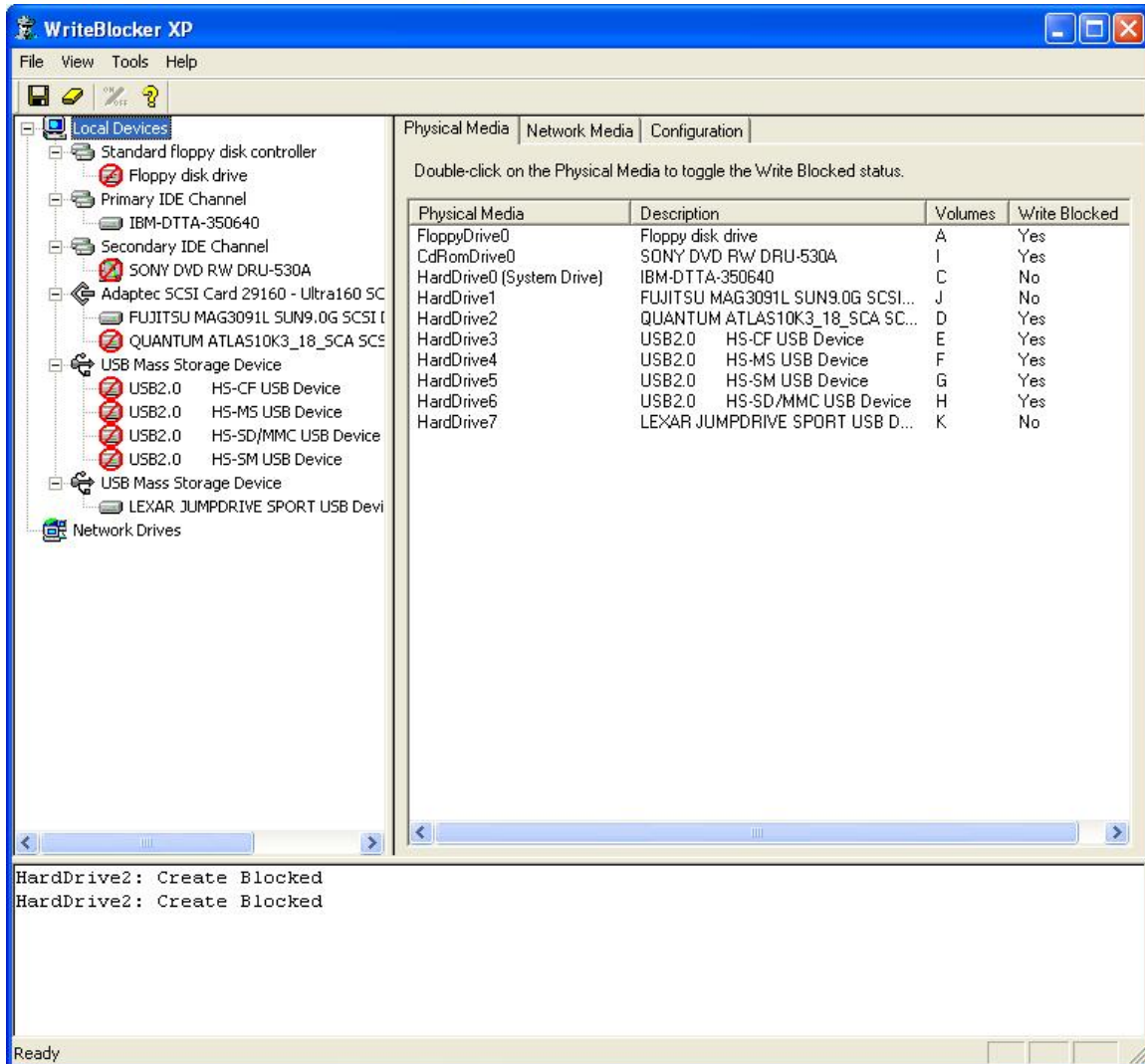
9.28.1. Hard disk configuration



9.28.2. Write blocker configuration



9.28.3. Test output summary



9.28.4. Hard disk hash results

Drive Identification		Computed	SHA1 Value
\\.\PhysicalDrive1	P	Before	233283A966083375DE84FOCF2B4A2BCEC73BC974
		After	233283A966083375DE84FOCF2B4A2BCEC73BC974

9.28.5. Test results analysis

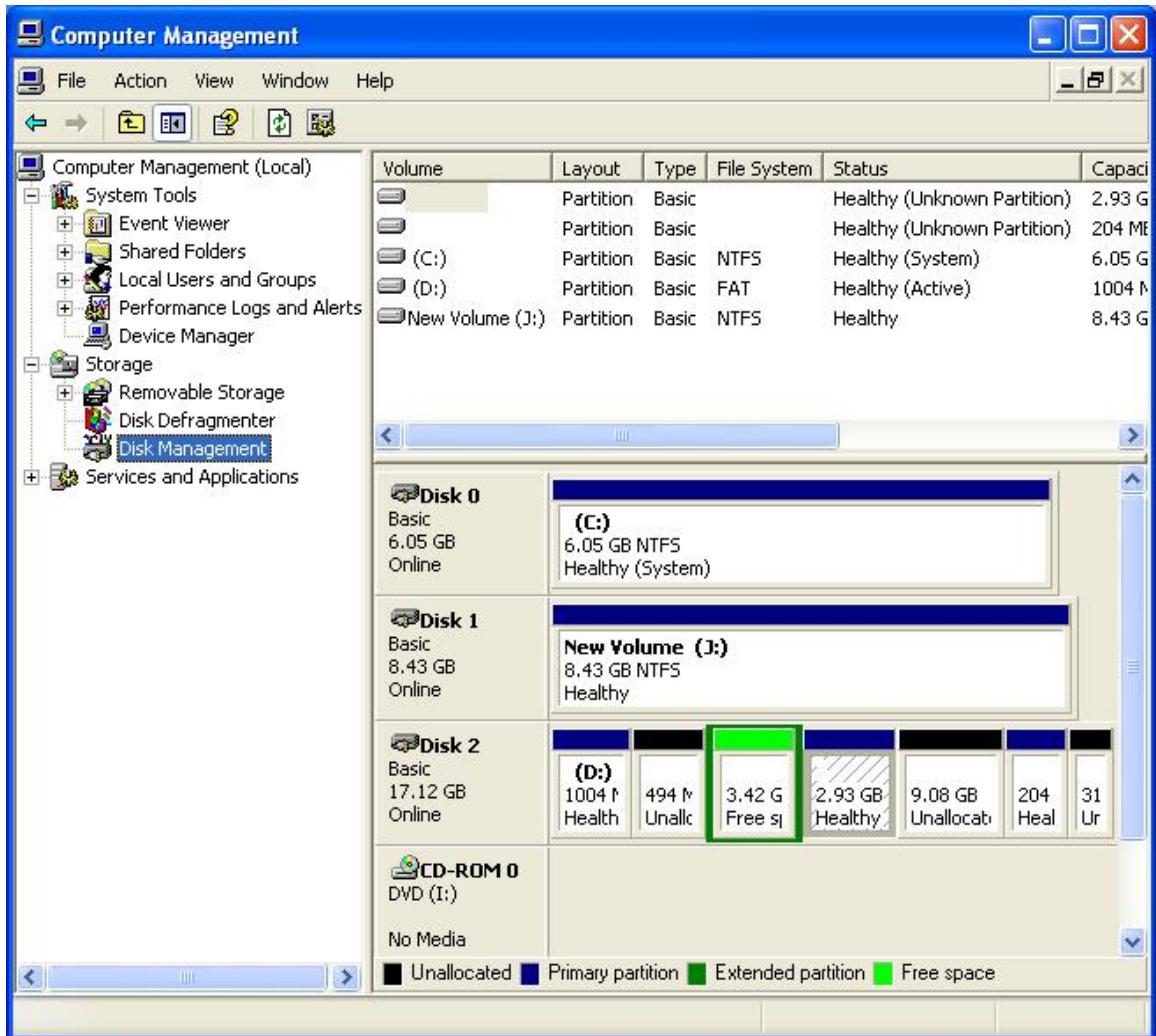
The tool produced the expected result. The DROP operation failed with a write protection error message, 2 blocked commands (CREATE) were logged by the write blocker tool, and the hash value of the target disk wsa unchanged after the test.

9.29 Test Case SWB-29

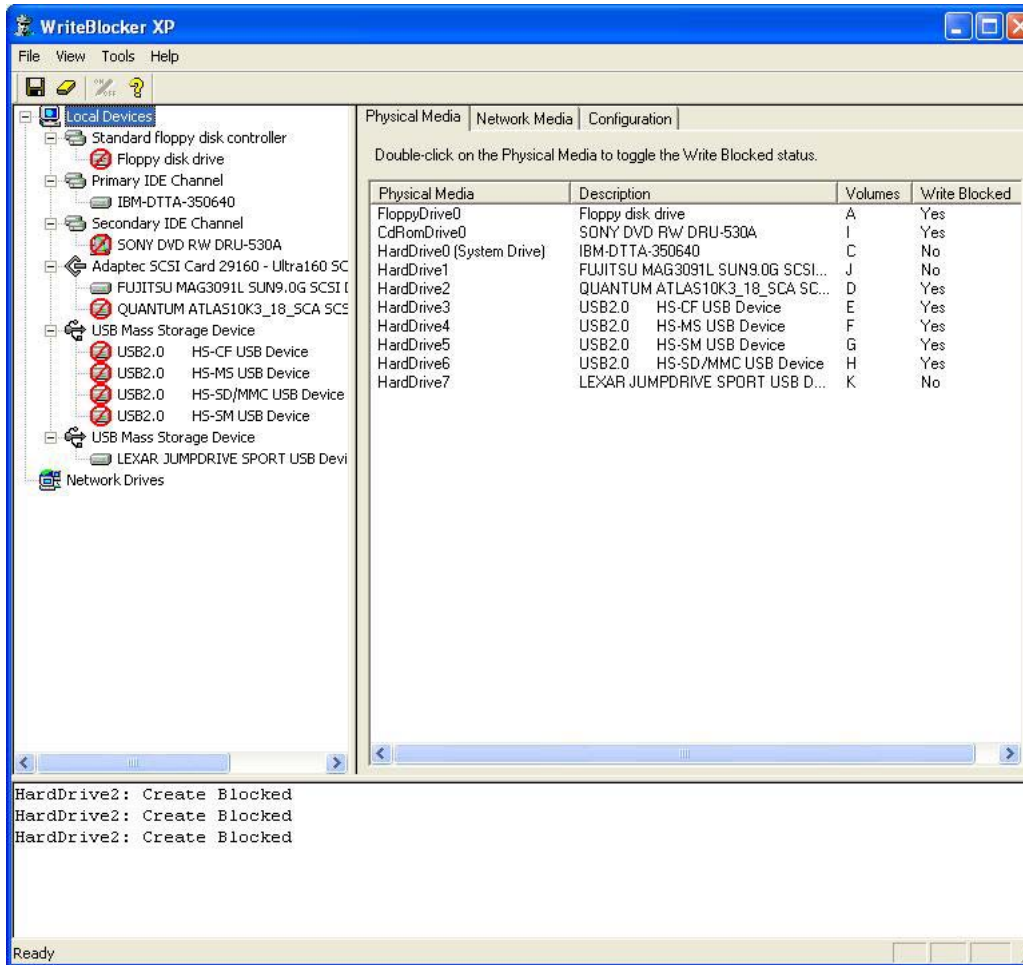
This case tests the tool's compliance with assertions SWB-AM-10 and SWB-AO-08. It is run using the Typical protocol. The expected result of this test is:

- The PASTE operation will fail with an error message
- The tool will display a message indicating each command blocked
- The hash value of the target disk will be unchanged after the test

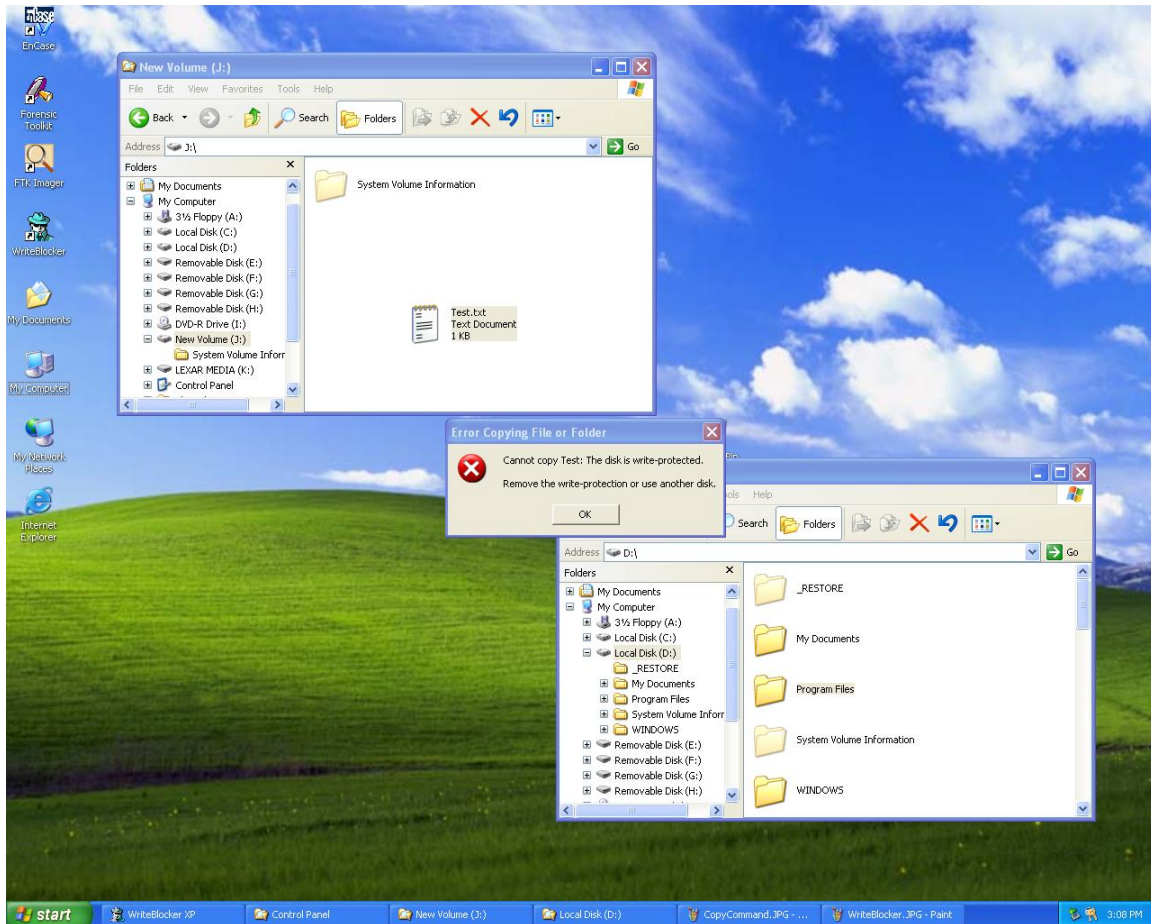
9.29.1. Hard disk configuration

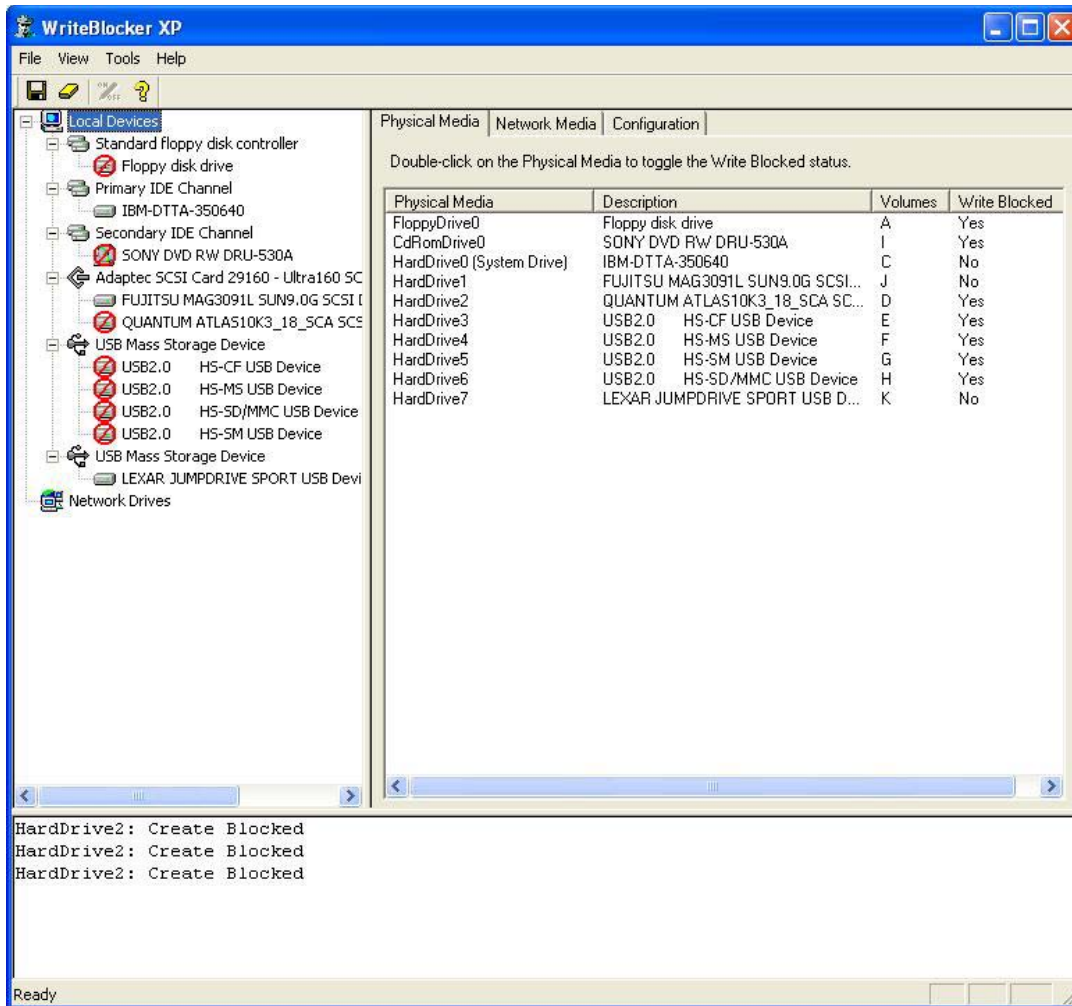


9.29.2. Write blocker configuration



9.29.3. Test output summary





9.29.4. Hard disk hash results

Drive Identification		Computed	SHA1 Value
\\.\PhysicalDrive2	P	Before	233283A966083375DE84FOCF2B4A2BCEC73BC974
		After	233283A966083375DE84FOCF2B4A2BCEC73BC974

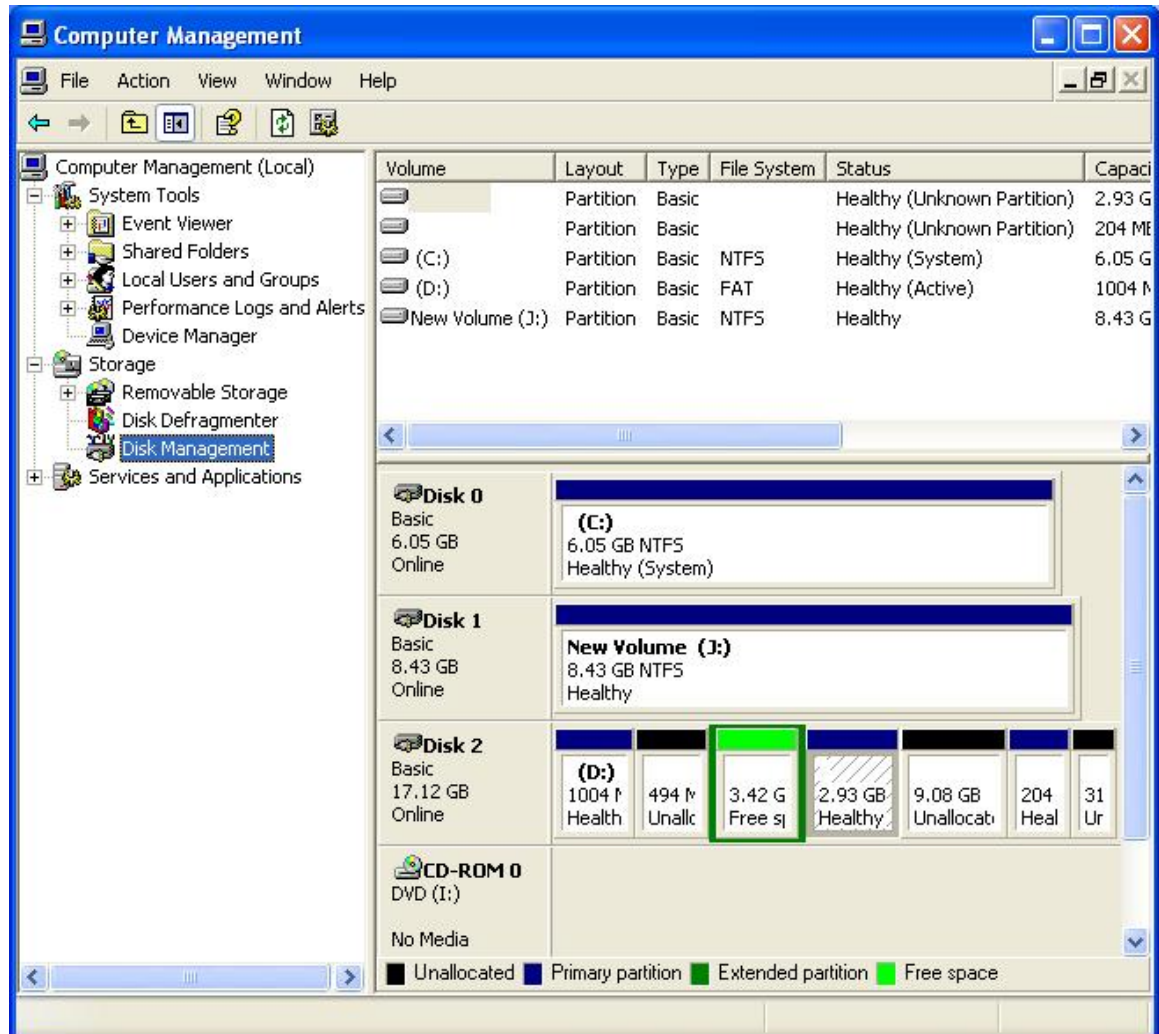
9.29.5. Test results analysis

The tool produced the expected result. The DROP operation failed with a write protection error message, 3 blocked commands (CREATE) were logged by the write blocker tool, and the hash value of the target disk was unchanged after the test.

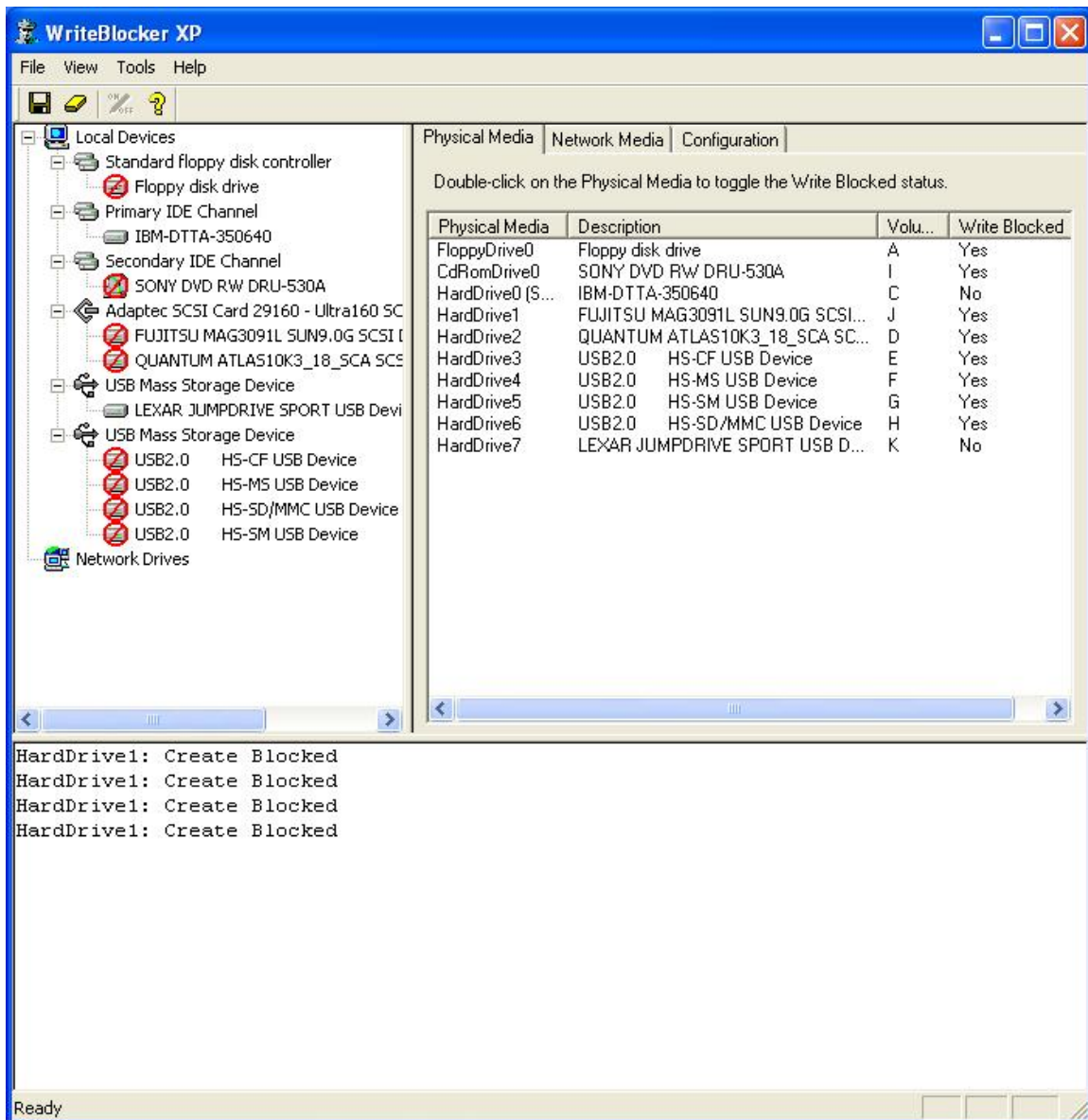
9.30 Test case SWB-30

This case tests the tool's compliance with mandatory assertion SWB-AM-10 and optional assertion SWB-AO-08. The expected result of this test is that the SAVE AS operation will fail with an I/O error, one or more blocked commands will be logged by the write blocker, and the disk hash of the test disk will be unchanged by the test.

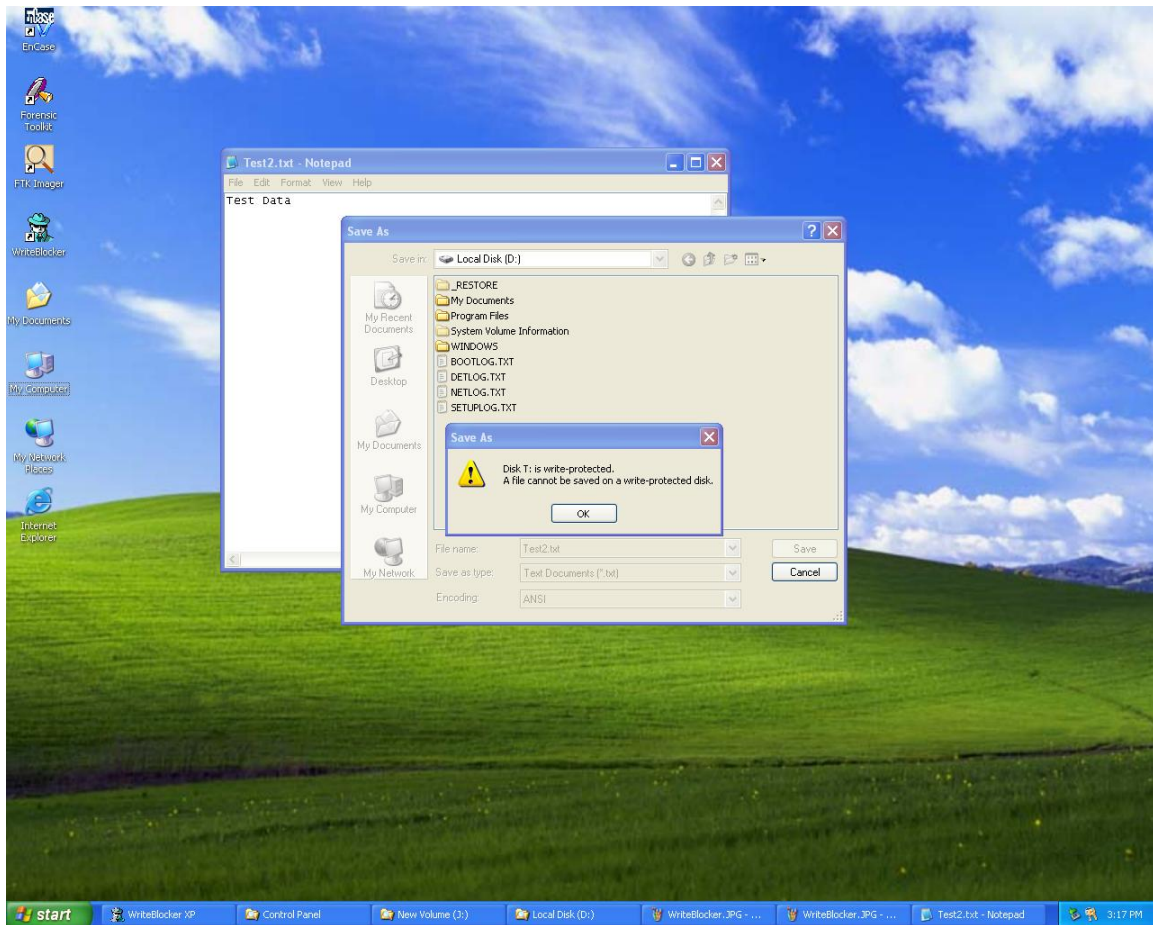
9.30.1. Hard disk configuration

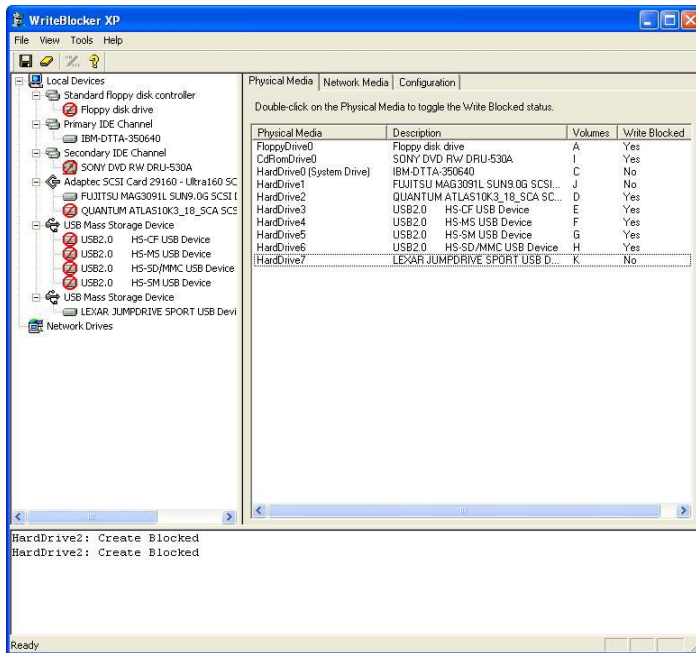


9.30.2. Write blocker configuration



9.30.3. Test output summary





9.30.4. Hard disk hash results

Drive Identification		Computed	SHA1 Value
\\.\PhysicalDrive2	P	Before	233283A966083375DE84FOCF2B4A2BCEC73BC974
		After	233283A966083375DE84FOCF2B4A2BCEC73BC974

9.30.5. Test results analysis

The tool produced the expected result. The drag and drop operation failed with a write protection error, the tool logged two blocked commands (CREATE) and the protected drive was not altered.

Appendix A – Sample Logfile Listings

Figure A-1 – Logfile output listing for test SWB-01

NIST Software Write Blocker Test Suite V1.2		
Wed Aug 17 11:01:27 2005		
Test case: SWB-01		
Command set: RWOVU		
Number of drives: 1		
Protection pattern: U		
Test administered by: DPA		
Testing device \\.\Physical Drive1		
Device is software WRITE ENABLED		
IRP Function	Code	Result
IRP_MJ_CREATE	(0x00)	ALLOWED
IRP_MJ_CREATE_NAMED_PIPE	(0x01)	ALLOWED
IRP_MJ_CLOSE	(0x02)	ALLOWED
IRP_MJ_READ	(0x03)	ALLOWED
IRP_MJ_WRITE	(0x04)	ALLOWED
IRP_MJ_QUERY_INFORMATION	(0x05)	ALLOWED
IRP_MJ_SET_INFORMATION	(0x06)	ALLOWED
IRP_MJ_QUERY_EA	(0x07)	ALLOWED
IRP_MJ_SET_EA	(0x08)	ALLOWED
IRP_MJ_FLUSH_BUFFERS	(0x09)	ALLOWED
IRP_MJ_QUERY_VOLUME_INFORMATION	(0x0A)	ALLOWED
IRP_MJ_SET_VOLUME_INFORMATION	(0x0B)	ALLOWED
IRP_MJ_DIRECTORY_CONTROL	(0x0C)	ALLOWED
IRP_MJ_FILE_SYSTEM_CONTROL	(0x0D)	ALLOWED
IRP_MJ_DEVICE_CONTROL	(0x0E)	ALLOWED
IRP_MJ SCSI	(0x0F)	
SCSI Operation	Opcode	
TEST_UNIT_READY	(0x00)	ALLOWED
REWIND	(0x01)	ALLOWED
VENDOR_SPECIFIC_CDB	(0x02)	ALLOWED
REQUEST_SENSE	(0x03)	ALLOWED
FORMAT_UNIT	(0x04)	ALLOWED
READ_BLOCK_LIMITS	(0x05)	ALLOWED
VENDOR_SPECIFIC_CDB	(0x06)	ALLOWED
REASSIGN_BLOCKS	(0x07)	ALLOWED
READ6	(0x08)	ALLOWED
VENDOR_SPECIFIC_CDB	(0x09)	ALLOWED
WRITE6	(0x0A)	ALLOWED
SEEK6	(0x0B)	ALLOWED
VENDOR_SPECIFIC_CDB	(0x0C)	ALLOWED
VENDOR_SPECIFIC_CDB	(0x0D)	ALLOWED
VENDOR_SPECIFIC_CDB	(0x0E)	ALLOWED
READ_REVERSE6	(0x0F)	ALLOWED
WRITE_FILEMARKS	(0x10)	ALLOWED
SPACE	(0x11)	ALLOWED
INQUIRY	(0x12)	ALLOWED
VERIFY6	(0x13)	ALLOWED
RECOVER_BUF_DATA	(0x14)	ALLOWED
MODE_SELECT	(0x15)	ALLOWED
RESERVE_UNIT	(0x16)	ALLOWED
RELEASE_UNIT	(0x17)	ALLOWED
COPY	(0x18)	ALLOWED
ERASE	(0x19)	ALLOWED
MODE_SENSE	(0x1A)	ALLOWED
START_STOP_UNIT	(0x1B)	ALLOWED
RECEIVE_DIAGNOSTIC	(0x1C)	ALLOWED
SEND_DIAGNOSTIC	(0x1D)	ALLOWED
MEDIUM_REMOVAL	(0x1E)	ALLOWED
UNDEFINED_CDB	(0x1F)	ALLOWED
VENDOR_SPECIFIC_CDB	(0x20)	ALLOWED
VENDOR_SPECIFIC_CDB	(0x21)	ALLOWED
VENDOR_SPECIFIC_CDB	(0x22)	ALLOWED
VENDOR_SPECIFIC_CDB	(0x23)	ALLOWED
SET_WINDOW	(0x24)	ALLOWED
READ_CAPACITY	(0x25)	ALLOWED
VENDOR_SPECIFIC_CDB	(0x26)	ALLOWED
VENDOR_SPECIFIC_CDB	(0x27)	ALLOWED

Figure A-1 – Logfile output listing for test SWB-01

READ10	(0x28)	ALLOWED
READ_GENERATION	(0x29)	ALLOWED
WRITE10	(0x2A)	ALLOWED
SEEK10	(0x2B)	ALLOWED
ERASE10	(0x2C)	ALLOWED
VENDOR_SPECIFIC_CDB	(0x2D)	ALLOWED
WRITE_AND_VERIFY10	(0x2E)	ALLOWED
VERIFY	(0x2F)	ALLOWED
SEARCH_DATA_HIGH	(0x30)	ALLOWED
SEARCH_DATA_EQUAL	(0x31)	ALLOWED
SEARCH_DATA_LOW	(0x32)	ALLOWED
SET_LIMITS	(0x33)	ALLOWED
READ_POSITION	(0x34)	ALLOWED
SYNCHRONIZE_CACHE	(0x35)	ALLOWED
LOCK_UNLOCK_CACHE	(0x36)	ALLOWED
READ_DEFECT_DATA	(0x37)	ALLOWED
MEDIUM_SCAN	(0x38)	ALLOWED
COMPARE	(0x39)	ALLOWED
COPY_COMPARE	(0x3A)	ALLOWED
WRITE_DATA_BUFFER	(0x3B)	ALLOWED
READ_DATA_BUFFER	(0x3C)	ALLOWED
UNDEFINED_CDB	(0x3D)	ALLOWED
READ_LONG10	(0x3E)	ALLOWED
WRITE_LONG10	(0x3F)	ALLOWED
CHANGE_DEFINITION	(0x40)	ALLOWED
WRITE_SAME10	(0x41)	ALLOWED
READ_SUB_CHANNEL	(0x42)	ALLOWED
READ_TOC	(0x43)	ALLOWED
READ_HEADER	(0x44)	ALLOWED
PLAY_AUDIO	(0x45)	ALLOWED
GET_CONFIGURATION	(0x46)	ALLOWED
PLAY_AUDIO_MSF	(0x47)	ALLOWED
PLAY_TRACK_INDEX	(0x48)	ALLOWED
PLAY_TRACK_RELATIVE	(0x49)	ALLOWED
GET_EVENT_STATUS	(0x4A)	ALLOWED
PAUSE_RESUME	(0x4B)	ALLOWED
LOG_SELECT	(0x4C)	ALLOWED
LOG_SENSE	(0x4D)	ALLOWED
STOP_PLAY_SCAN	(0x4E)	ALLOWED
UNDEFINED_CDB	(0x4F)	ALLOWED
XDWRITE10	(0x50)	ALLOWED
XPWRITE10	(0x51)	ALLOWED
XDREAD10	(0x52)	ALLOWED
XDWRTucRead10	(0x53)	ALLOWED
SEND_OPCODE_INFORMATION	(0x54)	ALLOWED
MODE_SELECT10	(0x55)	ALLOWED
RESERVE_UNIT10	(0x56)	ALLOWED
RELEASE_UNIT10	(0x57)	ALLOWED
REPAIR_TRACK	(0x58)	ALLOWED
UNDEFINED_CDB	(0x59)	ALLOWED
MODE_SENSE10	(0x5A)	ALLOWED
CLOSE_TRACK_SESSION	(0x5B)	ALLOWED
READ_BUFFER_CAPACITY	(0x5C)	ALLOWED
SEND_CUE_SHEET	(0x5D)	ALLOWED
PERSISTENT_RESERVE_IN	(0x5E)	ALLOWED
PERSISTENT_RESERVE_OUT	(0x5F)	ALLOWED
UNDEFINED_CDB	(0x60)	ALLOWED
UNDEFINED_CDB	(0x61)	ALLOWED
UNDEFINED_CDB	(0x62)	ALLOWED
UNDEFINED_CDB	(0x63)	ALLOWED
UNDEFINED_CDB	(0x64)	ALLOWED
UNDEFINED_CDB	(0x65)	ALLOWED
UNDEFINED_CDB	(0x66)	ALLOWED
UNDEFINED_CDB	(0x67)	ALLOWED
UNDEFINED_CDB	(0x68)	ALLOWED
UNDEFINED_CDB	(0x69)	ALLOWED
UNDEFINED_CDB	(0x6A)	ALLOWED
UNDEFINED_CDB	(0x6B)	ALLOWED
UNDEFINED_CDB	(0x6C)	ALLOWED
UNDEFINED_CDB	(0x6D)	ALLOWED
UNDEFINED_CDB	(0x6E)	ALLOWED
UNDEFINED_CDB	(0x6F)	ALLOWED
UNDEFINED_CDB	(0x70)	ALLOWED
UNDEFINED_CDB	(0x71)	ALLOWED
UNDEFINED_CDB	(0x72)	ALLOWED
UNDEFINED_CDB	(0x73)	ALLOWED

Figure A-1 – Logfile output listing for test SWB-01

UNDEFINED_CDB	(0x74)	ALLOWED
UNDEFINED_CDB	(0x75)	ALLOWED
UNDEFINED_CDB	(0x76)	ALLOWED
UNDEFINED_CDB	(0x77)	ALLOWED
UNDEFINED_CDB	(0x78)	ALLOWED
UNDEFINED_CDB	(0x79)	ALLOWED
UNDEFINED_CDB	(0x7A)	ALLOWED
UNDEFINED_CDB	(0x7B)	ALLOWED
UNDEFINED_CDB	(0x7C)	ALLOWED
UNDEFINED_CDB	(0x7D)	ALLOWED
UNDEFINED_CDB	(0x7E)	ALLOWED
UNDEFINED_CDB	(0x7F)	ALLOWED
XDWRITE_EXTENDED	(0x80)	ALLOWED
REBUILD	(0x81)	ALLOWED
REGENERATE	(0x82)	ALLOWED
EXTENDED_COPY	(0x83)	ALLOWED
RECEIVE_COPY_RESULTS	(0x84)	ALLOWED
ATA_PASSTHROUGH16	(0x85)	ALLOWED
ACCESS_CONTROL_IN	(0x86)	ALLOWED
ACCESS_CONTROL_OUT	(0x87)	ALLOWED
READ16	(0x88)	ALLOWED
UNDEFINED_CDB	(0x89)	ALLOWED
WRITE16	(0x8A)	ALLOWED
UNDEFINED_CDB	(0x8B)	ALLOWED
READ_ATTRIBUTE	(0x8C)	ALLOWED
WRITE_ATTRIBUTE	(0x8D)	ALLOWED
WRITE_AND_VERIFY16	(0x8E)	ALLOWED
VERIFY16	(0x8F)	ALLOWED
PRE-FETCH16	(0x90)	ALLOWED
SYNCHRONIZE_CACHE16	(0x91)	ALLOWED
LOCK-UNLOCK_CACHE	(0x92)	ALLOWED
WRITE_SAME16	(0x93)	ALLOWED
UNDEFINED_CDB	(0x94)	ALLOWED
UNDEFINED_CDB	(0x95)	ALLOWED
UNDEFINED_CDB	(0x96)	ALLOWED
UNDEFINED_CDB	(0x97)	ALLOWED
UNDEFINED_CDB	(0x98)	ALLOWED
UNDEFINED_CDB	(0x99)	ALLOWED
UNDEFINED_CDB	(0x9A)	ALLOWED
UNDEFINED_CDB	(0x9B)	ALLOWED
UNDEFINED_CDB	(0x9C)	ALLOWED
UNDEFINED_CDB	(0x9D)	ALLOWED
UNDEFINED_CDB	(0x9E)	ALLOWED
UNDEFINED_CDB	(0x9F)	ALLOWED
REPORT_LUNS	(0xA0)	ALLOWED
ATA_PASSTHROUGH12	(0xA1)	ALLOWED
SEND_EVENT	(0xA2)	ALLOWED
SEND_KEY	(0xA3)	ALLOWED
REPORT_KEY	(0xA4)	ALLOWED
MOVE_MEDIUM	(0xA5)	ALLOWED
LOAD_UNLOAD_SLOT	(0xA6)	ALLOWED
SET_READ_AHEAD	(0xA7)	ALLOWED
READ12	(0xA8)	ALLOWED
UNDEFINED_CDB	(0xA9)	ALLOWED
WRITE12	(0xAA)	ALLOWED
UNDEFINED_CDB	(0xAB)	ALLOWED
ERASE12	(0xAC)	ALLOWED
READ_DVD_STRUCTURE	(0xAD)	ALLOWED
WRITE_AND_VERIFY12	(0xAE)	ALLOWED
VERIFY12	(0xAF)	ALLOWED
SEARCH_DATA_HIGH12	(0xB0)	ALLOWED
SEARCH_DATA_EQUAL12	(0xB1)	ALLOWED
SEARCH_DATA_LOW12	(0xB2)	ALLOWED
SET_LIMITS12	(0xB3)	ALLOWED
READ_ELEMENT_STATUS_AT	(0xB4)	ALLOWED
REQUEST_VOL_ELEMENT	(0xB5)	ALLOWED
SEND_VOLUME_TAG	(0xB6)	ALLOWED
READ_DEFECT_DATA12	(0xB7)	ALLOWED
READ_ELEMENT_STATUS	(0xB8)	ALLOWED
READ_CD_MSF12	(0xB9)	ALLOWED
SCANT12	(0xBA)	ALLOWED
SET_CDROM_SPEED12	(0xBB)	ALLOWED
PLAY_CD12	(0xBC)	ALLOWED
MECHANISM_STATUS	(0xBD)	ALLOWED
READ_CD12	(0xBE)	ALLOWED
SEND_DVD_STRUCTURE	(0xBF)	ALLOWED

Figure A-1 – Logfile output listing for test SWB-01

VENDOR_SPECIFIC_CDB	(0xC0)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xC1)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xC2)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xC3)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xC4)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xC5)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xC6)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xC7)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xC8)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xC9)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xCA)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xCB)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xCC)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xCD)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xCE)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xCF)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xD0)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xD1)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xD2)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xD3)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xD4)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xD5)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xD6)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xD7)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xD8)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xD9)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xDA)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xDB)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xDC)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xDD)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xDE)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xDF)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xE0)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xE1)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xE2)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xE3)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xE4)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xE5)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xE6)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xE7)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xE8)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xE9)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xEA)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xEB)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xEC)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xED)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xEE)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xEF)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xF0)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xF1)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xF2)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xF3)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xF4)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xF5)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xF6)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xF7)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xF8)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xF9)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xFA)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xFB)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xFC)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xFD)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xFE)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xFF)	ALLOWED
IRP_MJ_SHUTDOWN	(0x10)	ALLOWED
IRP_MJ_LOCK_CONTROL	(0x11)	ALLOWED
IRP_MJ_CLEANUP	(0x12)	ALLOWED
IRP_MJ_CREATE_MAILSLOT	(0x13)	ALLOWED
IRP_MJ_QUERY_SECURITY	(0x14)	ALLOWED
IRP_MJ_SET_SECURITY	(0x15)	ALLOWED
IRP_MJ_POWER	(0x16)	ALLOWED
IRP_MJ_SYSTEM_CONTROL	(0x17)	ALLOWED
IRP_MJ_DEVICE_CHANGE	(0x18)	ALLOWED
IRP_MJ_QUERY_QUOTA	(0x19)	ALLOWED
IRP_MJ_SET_QUOTA	(0x1A)	ALLOWED

Figure A-1 – Logfile output listing for test SWB-01

IRP_MJ_PNP (0x1B) ALLOWED			
***** TEST RESULTS SUMMARY *****			
Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	8	0	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	34	0	34
Other CDB's	62	0	62
Vendor SPeci fic CDB's	80	0	80
Undefined CDB's	53	0	53

Figure A-2 – Logfile output listing for test SWB-02

NIST Software Write Blocker Test Suite V1.2		
Wed Aug 17 11:01:27 2005		
Test case: SWB-01		
Command set: RWOVU		
Number of drives: 1		
Protection pattern: U		
Test administered by: DPA		
Testing device \\.\Physical Drive1		
Device is software WRITE ENABLED		
IRP Function	Code	Result
IRP_MJ_CREATE	(0x00)	ALLOWED
IRP_MJ_CREATE_NAMED_PIPE	(0x01)	ALLOWED
IRP_MJ_CLOSE	(0x02)	ALLOWED
IRP_MJ_READ	(0x03)	ALLOWED
IRP_MJ_WRITE	(0x04)	ALLOWED
IRP_MJ_QUERY_INFORMATION	(0x05)	ALLOWED
IRP_MJ_SET_INFORMATION	(0x06)	ALLOWED
IRP_MJ_QUERY_EA	(0x07)	ALLOWED
IRP_MJ_SET_EA	(0x08)	ALLOWED
IRP_MJ_FLUSH_BUFFERS	(0x09)	ALLOWED
IRP_MJ_QUERY_VOLUME_INFORMATION	(0x0A)	ALLOWED
IRP_MJ_SET_VOLUME_INFORMATION	(0x0B)	ALLOWED
IRP_MJ_DIRECTORY_CONTROL	(0x0C)	ALLOWED
IRP_MJ_FILE_SYSTEM_CONTROL	(0x0D)	ALLOWED
IRP_MJ_DEVICE_CONTROL	(0x0E)	ALLOWED
IRP_MJ SCSI	(0x0F)	
SCSI Operation	Opcode	
TEST_UNIT_READY	(0x00)	ALLOWED
REWIND	(0x01)	ALLOWED
VENDOR_SPECIFIC_CDB	(0x02)	ALLOWED
REQUEST_SENSE	(0x03)	ALLOWED
FORMAT_UNIT	(0x04)	ALLOWED
READ_BLOCK_LIMITS	(0x05)	ALLOWED
VENDOR_SPECIFIC_CDB	(0x06)	ALLOWED
REASSIGN_BLOCKS	(0x07)	ALLOWED
READ6	(0x08)	ALLOWED
VENDOR_SPECIFIC_CDB	(0x09)	ALLOWED
WRITE6	(0x0A)	ALLOWED
SEEK6	(0x0B)	ALLOWED
VENDOR_SPECIFIC_CDB	(0x0C)	ALLOWED
VENDOR_SPECIFIC_CDB	(0x0D)	ALLOWED
VENDOR_SPECIFIC_CDB	(0x0E)	ALLOWED
READ_REVERSE6	(0x0F)	ALLOWED
WRITE_FILEMARKS	(0x10)	ALLOWED
SPACE	(0x11)	ALLOWED
INQUIRY	(0x12)	ALLOWED
VERIFY6	(0x13)	ALLOWED
RECOVER_BUF_DATA	(0x14)	ALLOWED
MODE_SELECT	(0x15)	ALLOWED
RESERVE_UNIT	(0x16)	ALLOWED
RELEASE_UNIT	(0x17)	ALLOWED
COPY	(0x18)	ALLOWED
ERASE	(0x19)	ALLOWED
MODE_SENSE	(0x1A)	ALLOWED
START_STOP_UNIT	(0x1B)	ALLOWED
RECEIVE_DIAGNOSTIC	(0x1C)	ALLOWED
SEND_DIAGNOSTIC	(0x1D)	ALLOWED
MEDIUM_REMOVAL	(0x1E)	ALLOWED
UNDEFINED_CDB	(0x1F)	ALLOWED
VENDOR_SPECIFIC_CDB	(0x20)	ALLOWED
VENDOR_SPECIFIC_CDB	(0x21)	ALLOWED
VENDOR_SPECIFIC_CDB	(0x22)	ALLOWED
VENDOR_SPECIFIC_CDB	(0x23)	ALLOWED
SET_WINDOW	(0x24)	ALLOWED
READ_CAPACITY	(0x25)	ALLOWED
VENDOR_SPECIFIC_CDB	(0x26)	ALLOWED
VENDOR_SPECIFIC_CDB	(0x27)	ALLOWED
READ10	(0x28)	ALLOWED
READ_GENERATION	(0x29)	ALLOWED

Figure A-2 – Logfile output listing for test SWB-02

WRITE10	(0x2A)	ALLOWED
SEEK10	(0x2B)	ALLOWED
ERASE10	(0x2C)	ALLOWED
VENDOR_SPECIFIC_CDB	(0x2D)	ALLOWED
WRITE_AND_VERIFY10	(0x2E)	ALLOWED
VERIFY	(0x2F)	ALLOWED
SEARCH_DATA_HIGH	(0x30)	ALLOWED
SEARCH_DATA_EQUAL	(0x31)	ALLOWED
SEARCH_DATA_LOW	(0x32)	ALLOWED
SET_LIMITS	(0x33)	ALLOWED
READ_POSITION	(0x34)	ALLOWED
SYNCHRONIZE_CACHE	(0x35)	ALLOWED
LOCK_UNLOCK_CACHE	(0x36)	ALLOWED
READ_DEFECT_DATA	(0x37)	ALLOWED
MEDIUM_SCAN	(0x38)	ALLOWED
COMPARE	(0x39)	ALLOWED
COPY_COMPARE	(0x3A)	ALLOWED
WRITE_DATA_BUFFER	(0x3B)	ALLOWED
READ_DATA_BUFFER	(0x3C)	ALLOWED
UNDEFINED_CDB	(0x3D)	ALLOWED
READ_LONG10	(0x3E)	ALLOWED
WRITE_LONG10	(0x3F)	ALLOWED
CHANGE_DEFINITION	(0x40)	ALLOWED
WRITE_SAME10	(0x41)	ALLOWED
READ_SUB_CHANNEL	(0x42)	ALLOWED
READ_TOC	(0x43)	ALLOWED
READ_HEADER	(0x44)	ALLOWED
PLAY_AUDIO	(0x45)	ALLOWED
GET_CONFIGURATION	(0x46)	ALLOWED
PLAY_AUDIO_MSF	(0x47)	ALLOWED
PLAY_TRACK_INDEX	(0x48)	ALLOWED
PLAY_TRACK_RELATIVE	(0x49)	ALLOWED
GET_EVENT_STATUS	(0x4A)	ALLOWED
PAUSE_RESUME	(0x4B)	ALLOWED
LOG_SELECT	(0x4C)	ALLOWED
LOG_SENSE	(0x4D)	ALLOWED
STOP_PLAY_SCAN	(0x4E)	ALLOWED
UNDEFINED_CDB	(0x4F)	ALLOWED
XDWRITE10	(0x50)	ALLOWED
XPWRITE10	(0x51)	ALLOWED
XDREAD10	(0x52)	ALLOWED
XDWRI TucRead10	(0x53)	ALLOWED
SEND_OPC_INFORMATION	(0x54)	ALLOWED
MODE_SELECT10	(0x55)	ALLOWED
RESERVE_UNIT10	(0x56)	ALLOWED
RELEASE_UNIT10	(0x57)	ALLOWED
REPAIR_TRACK	(0x58)	ALLOWED
UNDEFINED_CDB	(0x59)	ALLOWED
MODE_SENSE10	(0x5A)	ALLOWED
CLOSE_TRACK_SESSION	(0x5B)	ALLOWED
READ_BUFFER_CAPACITY	(0x5C)	ALLOWED
SEND_CUE_SHEET	(0x5D)	ALLOWED
PERSISTENT_RESERVE_IN	(0x5E)	ALLOWED
PERSISTENT_RESERVE_OUT	(0x5F)	ALLOWED
UNDEFINED_CDB	(0x60)	ALLOWED
UNDEFINED_CDB	(0x61)	ALLOWED
UNDEFINED_CDB	(0x62)	ALLOWED
UNDEFINED_CDB	(0x63)	ALLOWED
UNDEFINED_CDB	(0x64)	ALLOWED
UNDEFINED_CDB	(0x65)	ALLOWED
UNDEFINED_CDB	(0x66)	ALLOWED
UNDEFINED_CDB	(0x67)	ALLOWED
UNDEFINED_CDB	(0x68)	ALLOWED
UNDEFINED_CDB	(0x69)	ALLOWED
UNDEFINED_CDB	(0x6A)	ALLOWED
UNDEFINED_CDB	(0x6B)	ALLOWED
UNDEFINED_CDB	(0x6C)	ALLOWED
UNDEFINED_CDB	(0x6D)	ALLOWED
UNDEFINED_CDB	(0x6E)	ALLOWED
UNDEFINED_CDB	(0x6F)	ALLOWED
UNDEFINED_CDB	(0x70)	ALLOWED
UNDEFINED_CDB	(0x71)	ALLOWED
UNDEFINED_CDB	(0x72)	ALLOWED
UNDEFINED_CDB	(0x73)	ALLOWED
UNDEFINED_CDB	(0x74)	ALLOWED
UNDEFINED_CDB	(0x75)	ALLOWED

Figure A-2 – Logfile output listing for test SWB-02

UNDEFINED_CDB	(0x76)	ALLOWED
UNDEFINED_CDB	(0x77)	ALLOWED
UNDEFINED_CDB	(0x78)	ALLOWED
UNDEFINED_CDB	(0x79)	ALLOWED
UNDEFINED_CDB	(0x7A)	ALLOWED
UNDEFINED_CDB	(0x7B)	ALLOWED
UNDEFINED_CDB	(0x7C)	ALLOWED
UNDEFINED_CDB	(0x7D)	ALLOWED
UNDEFINED_CDB	(0x7E)	ALLOWED
UNDEFINED_CDB	(0x7F)	ALLOWED
XDWRITE_EXTENDED	(0x80)	ALLOWED
REBUILD	(0x81)	ALLOWED
REGENERATE	(0x82)	ALLOWED
EXTENDED_COPY	(0x83)	ALLOWED
RECEIVE_COPY_RESULTS	(0x84)	ALLOWED
ATA_PASSTHROUGH16	(0x85)	ALLOWED
ACCESS_CONTROL_IN	(0x86)	ALLOWED
ACCESS_CONTROL_OUT	(0x87)	ALLOWED
READ16	(0x88)	ALLOWED
UNDEFINED_CDB	(0x89)	ALLOWED
WRITE16	(0x8A)	ALLOWED
UNDEFINED_CDB	(0x8B)	ALLOWED
READ_ATTRIBUTE	(0x8C)	ALLOWED
WRITE_ATTRIBUTE	(0x8D)	ALLOWED
WRITE_AND_VERIFY16	(0x8E)	ALLOWED
VERIFY16	(0x8F)	ALLOWED
PRE-FETCH16	(0x90)	ALLOWED
SYNCHRONIZE_CACHE16	(0x91)	ALLOWED
LOCK-UNLOCK_CACHE	(0x92)	ALLOWED
WRITE_SAME16	(0x93)	ALLOWED
UNDEFINED_CDB	(0x94)	ALLOWED
UNDEFINED_CDB	(0x95)	ALLOWED
UNDEFINED_CDB	(0x96)	ALLOWED
UNDEFINED_CDB	(0x97)	ALLOWED
UNDEFINED_CDB	(0x98)	ALLOWED
UNDEFINED_CDB	(0x99)	ALLOWED
UNDEFINED_CDB	(0x9A)	ALLOWED
UNDEFINED_CDB	(0x9B)	ALLOWED
UNDEFINED_CDB	(0x9C)	ALLOWED
UNDEFINED_CDB	(0x9D)	ALLOWED
UNDEFINED_CDB	(0x9E)	ALLOWED
UNDEFINED_CDB	(0x9F)	ALLOWED
REPORT_LUNS	(0xA0)	ALLOWED
ATA_PASSTHROUGH12	(0xA1)	ALLOWED
SEND_EVENT	(0xA2)	ALLOWED
SEND_KEY	(0xA3)	ALLOWED
REPORT_KEY	(0xA4)	ALLOWED
MOVE_MEDIUM	(0xA5)	ALLOWED
LOAD_UNLOAD_SLOT	(0xA6)	ALLOWED
SET_READ_AHEAD	(0xA7)	ALLOWED
READ12	(0xA8)	ALLOWED
UNDEFINED_CDB	(0xA9)	ALLOWED
WRITE12	(0xAA)	ALLOWED
UNDEFINED_CDB	(0xAB)	ALLOWED
ERASE12	(0xAC)	ALLOWED
READ_DVD_STRUCTURE	(0xAD)	ALLOWED
WRITE_AND_VERIFY12	(0xAE)	ALLOWED
VERIFY12	(0xAF)	ALLOWED
SEARCH_DATA_HIGH12	(0xB0)	ALLOWED
SEARCH_DATA_EQUAL12	(0xB1)	ALLOWED
SEARCH_DATA_LOW12	(0xB2)	ALLOWED
SET_LIMITS12	(0xB3)	ALLOWED
READ_ELEMENT_STATUS_AT	(0xB4)	ALLOWED
REQUEST_VOL_ELEMENT	(0xB5)	ALLOWED
SEND_VOLUME_TAG	(0xB6)	ALLOWED
READ_DEFECT_DATA12	(0xB7)	ALLOWED
READ_ELEMENT_STATUS	(0xB8)	ALLOWED
READ_CD_MSF12	(0xB9)	ALLOWED
SCAN12	(0xBA)	ALLOWED
SET_CDROM_SPEED12	(0xBB)	ALLOWED
PLAY_CD12	(0xBC)	ALLOWED
MECHANISM_STATUS	(0xBD)	ALLOWED
READ_CD12	(0xBE)	ALLOWED
SEND_DVD_STRUCTURE	(0xBF)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xC0)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xC1)	ALLOWED

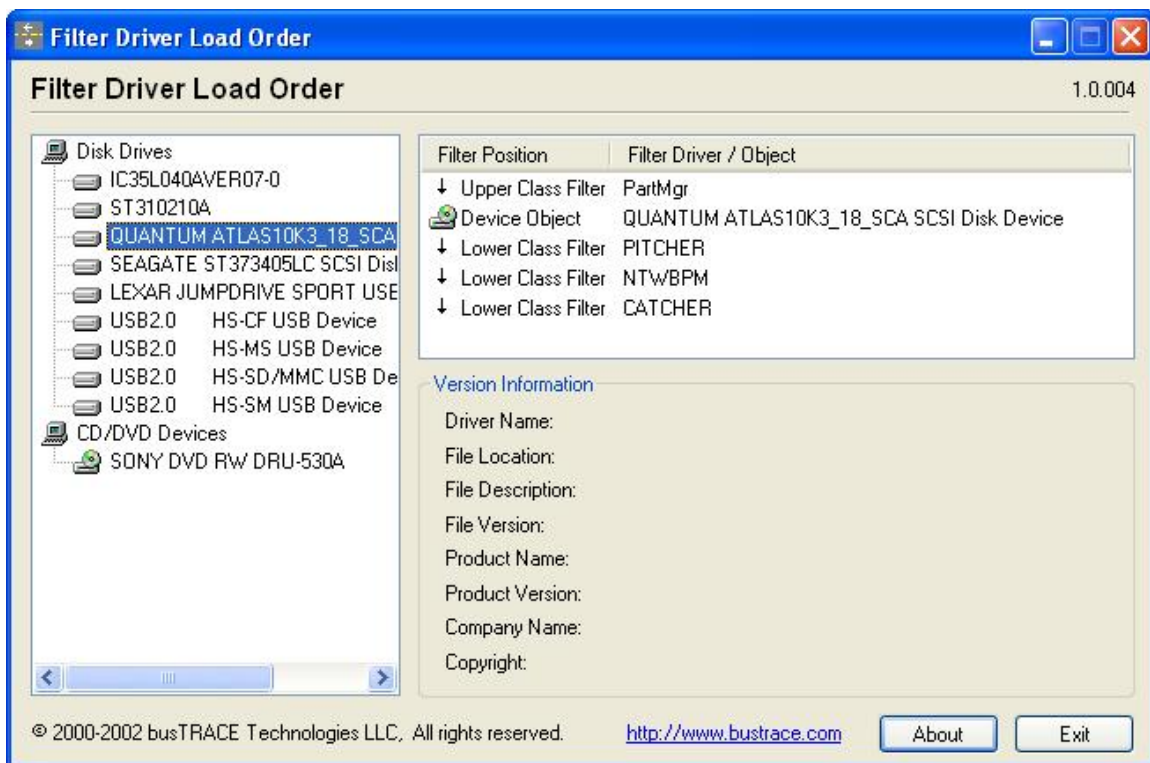
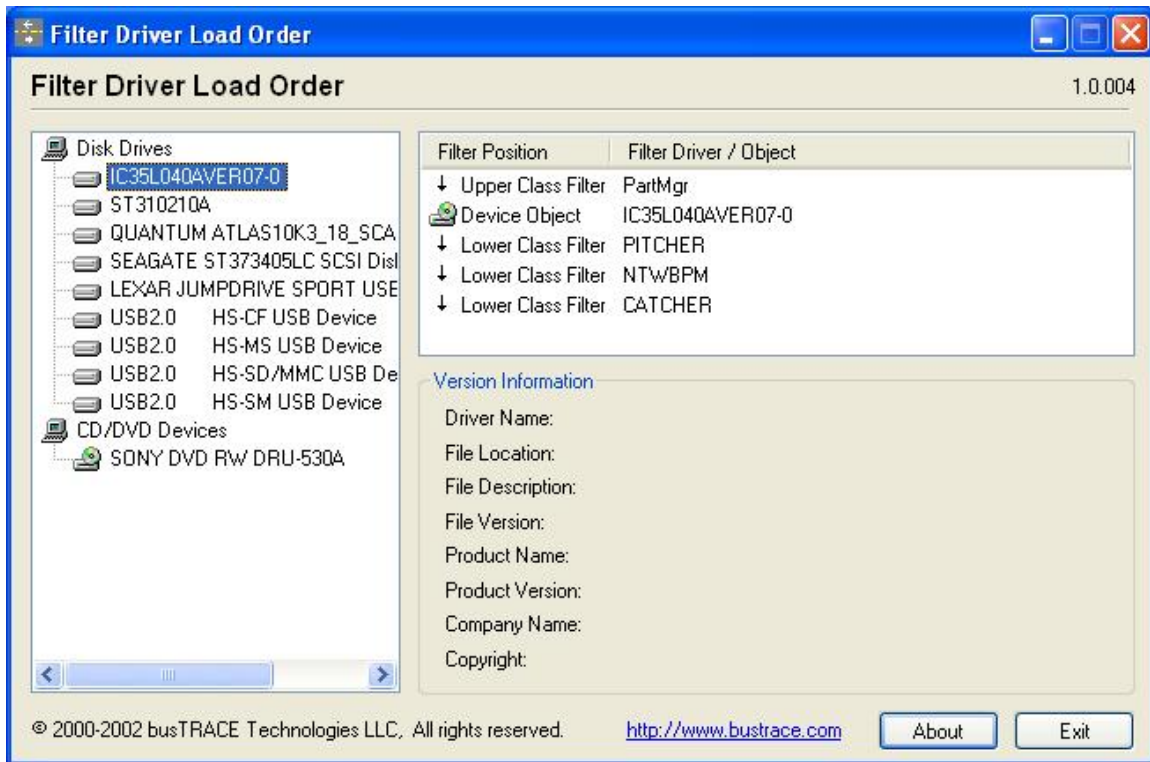
Figure A-2 – Logfile output listing for test SWB-02

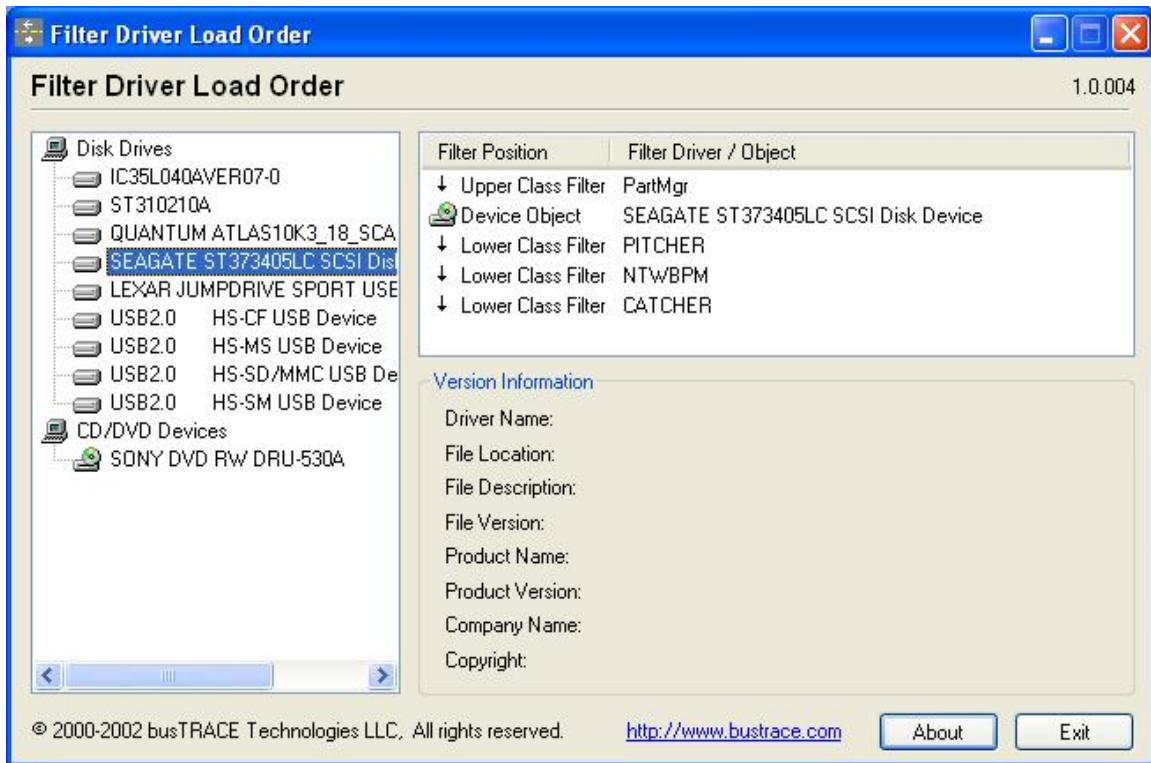
VENDOR_SPECIFIC_CDB	(0xC2)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xC3)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xC4)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xC5)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xC6)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xC7)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xC8)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xC9)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xCA)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xCB)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xCC)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xCD)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xCE)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xCF)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xD0)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xD1)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xD2)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xD3)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xD4)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xD5)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xD6)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xD7)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xD8)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xD9)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xDA)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xDB)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xDC)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xDD)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xDE)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xDF)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xE0)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xE1)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xE2)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xE3)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xE4)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xE5)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xE6)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xE7)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xE8)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xE9)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xEA)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xEB)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xEC)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xED)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xEE)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xEF)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xF0)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xF1)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xF2)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xF3)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xF4)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xF5)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xF6)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xF7)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xF8)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xF9)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xFA)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xFB)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xFC)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xFD)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xFE)	ALLOWED
VENDOR_SPECIFIC_CDB	(0xFF)	ALLOWED
IRP_MJ_SHUTDOWN	(0x10)	ALLOWED
IRP_MJ_LOCK_CONTROL	(0x11)	ALLOWED
IRP_MJ_CLEANUP	(0x12)	ALLOWED
IRP_MJ_CREATE_MAILSLOT	(0x13)	ALLOWED
IRP_MJ_QUERY_SECURITY	(0x14)	ALLOWED
IRP_MJ_SET_SECURITY	(0x15)	ALLOWED
IRP_MJ_POWER	(0x16)	ALLOWED
IRP_MJ_SYSTEM_CONTROL	(0x17)	ALLOWED
IRP_MJ_DEVICE_CHANGE	(0x18)	ALLOWED
IRP_MJ_QUERY_QUOTA	(0x19)	ALLOWED
IRP_MJ_SET_QUOTA	(0x1A)	ALLOWED
IRP_MJ_PNP	(0x1B)	ALLOWED

Figure A-2 – Logfile output listing for test SWB-02

***** TEST RESULTS SUMMARY *****			
Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	8	0	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	34	0	34
Other CDB's	62	0	62
Vendor SPeci fic CDB's	80	0	80
Undefi ned CDB's	53	0	53

Appendix B – Filter Driver Load Orders





About the National Institute of Justice

NIJ is the research, development, and evaluation agency of the U.S. Department of Justice. NIJ's mission is to advance scientific research, development, and evaluation to enhance the administration of justice and public safety. NIJ's principal authorities are derived from the Omnibus Crime Control and Safe Streets Act of 1968, as amended (see 42 U.S.C. §§ 3721–3723).

The NIJ Director is appointed by the President and confirmed by the Senate. The Director establishes the Institute's objectives, guided by the priorities of the Office of Justice Programs, the U.S. Department of Justice, and the needs of the field. The Institute actively solicits the views of criminal justice and other professionals and researchers to inform its search for the knowledge and tools to guide policy and practice.

Strategic Goals

NIJ has seven strategic goals grouped into three categories:

Creating relevant knowledge and tools

1. Partner with State and local practitioners and policymakers to identify social science research and technology needs.
2. Create scientific, relevant, and reliable knowledge—with a particular emphasis on terrorism, violent crime, drugs and crime, cost-effectiveness, and community-based efforts—to enhance the administration of justice and public safety.
3. Develop affordable and effective tools and technologies to enhance the administration of justice and public safety.

Dissemination

4. Disseminate relevant knowledge and information to practitioners and policymakers in an understandable, timely, and concise manner.
5. Act as an honest broker to identify the information, tools, and technologies that respond to the needs of stakeholders.

Agency management

6. Practice fairness and openness in the research and development process.
7. Ensure professionalism, excellence, accountability, cost-effectiveness, and integrity in the management and conduct of NIJ activities and programs.

Program Areas

In addressing these strategic challenges, the Institute is involved in the following program areas: crime control and prevention, including policing; drugs and crime; justice systems and offender behavior, including corrections; violence and victimization; communications and information technologies; critical incident response; investigative and forensic sciences, including DNA; less-than-lethal technologies; officer protection; education and training technologies; testing and standards; technology assistance to law enforcement and corrections agencies; field testing of promising programs; and international crime control.

In addition to sponsoring research and development and technology assistance, NIJ evaluates programs, policies, and technologies. NIJ communicates its research and evaluation findings through conferences and print and electronic media.

To find out more about the National Institute of Justice, please visit:

<http://www.ojp.usdoj.gov/nij>

or contact:

National Criminal Justice
Reference Service
P.O. Box 6000
Rockville, MD 20849–6000
800–851–3420
e-mail: askncjrs@ncjrs.org