



NIJ

Special

REPORT

**ACES Software Write Block Tool Test
Report: Writeblocker Windows 2000 V5.02.00**

[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
[OJP Website](#)



JAN. 08

**ACES Software Write Block Tool
Test Report: Writeblocker Windows
2000 V5.02.00**

NCJ 220221



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 Windows 2000 V5.02.00**

January 2008

NIST

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.....	15
6.1 TEST COMPUTER.....	15
6.2 HARD DISK DRIVES	15
6.3 TEST SOFTWARE	16
6.4 RUN PROTOCOL SELECTION.....	17
7. Interpretation of Test Results.....	18
7.1 TEST ASSERTION VERIFICATION	18
7.2 OPTIONAL ASSERTIONS	19
8. Key to reading test results.....	21
8.1 HARD DISK CONFIGURATION	21
8.2 WRITE BLOCKER CONFIGURATION	22
8.3 TEST OUTPUT SUMMARY	23
9. Test Result Summaries	24
9.1 TEST CASE SWB-01.....	24
9.1.1 Hard disk configuration	24
9.1.2 Write blocker configuration.....	25
9.1.3 Test output summary.....	26
9.1.4 Hard disk hash results	26
9.1.5 Test result analysis.....	26
9.2 TEST CASE SWB-02.....	27
9.2.1 Hard disk configuration	27
9.2.2 Write blocker configuration.....	28
9.2.3 Test output summary.....	29
9.2.4 Hard disk hash results	29
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.....	52
9.8.4	Hard disk hash results	53
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.....	56
9.9.4	Hard disk hash results	57
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.....	64
9.11.4	Hard disk hash results	65
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	126
9.27.5	Test results analysis	126
9.28	TEST CASE SWB-28.....	127
9.28.1	Hard disk configuration	127
9.28.2	Write blocker configuration.....	128
9.28.3	Test output summary.....	129
9.28.4	Hard disk hash results	130
9.28.5	Test results analysis	130
9.29	TEST CASE SWB-29.....	131
9.29.1	Hard disk configuration	131
9.29.2	Write blocker configuration.....	132
9.29.3	Test output summary.....	133
9.29.4	Hard disk hash results	134
9.29.5	Test results analysis	134
9.30	TEST CASE SWB-30.....	135
9.30.1	Hard disk configuration	135
9.30.2	Write blocker configuration.....	136
9.30.3	Test output summary.....	137
9.30.4	Hard disk hash results	138
9.30.5	Test results analysis	138
Appendix A		139
Appendix B		145

Introduction

The Computer Forensics Tool Testing (CFTT) program is a joint project of the National Institute of Justice, 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 Windows 2000, Version 5.02.00**. 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 Windows 2000 V5.02.00
Producer: Booz, Allen, Hamilton, Inc.
Operating Environment: Microsoft Windows 2000, 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 nonprotected 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 Windows 2000 V5.02.00, 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 W2K 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 W2K V5.02.00
Producer: Booze, Allen, Hamilton, Inc.
Product Checksum: SHA1:
Operating Environment: Microsoft Windows W2K, 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 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.

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.

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.**

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 3.4hz 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 Windows 2000 V5.02.00	<p>Writeblocker Windows 2000 V5.02.00</p> <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 node 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	<p>The NIST Software Writeblocker Test Suite V1.2</p> <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	<p>A third party kernel mode software package for monitoring IRP traffic within the Windows device driver stacks.</p>

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.

The tested tool, Writeblocker Windows 2000 V5.02.00, 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.

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 tools 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 are omitted for the sake of limiting the size of this document. A complete archive of all test result data may be downloaded from the [CFTT 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 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 all drives configured for each test is shown in the captured image.

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 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-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—this 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.**

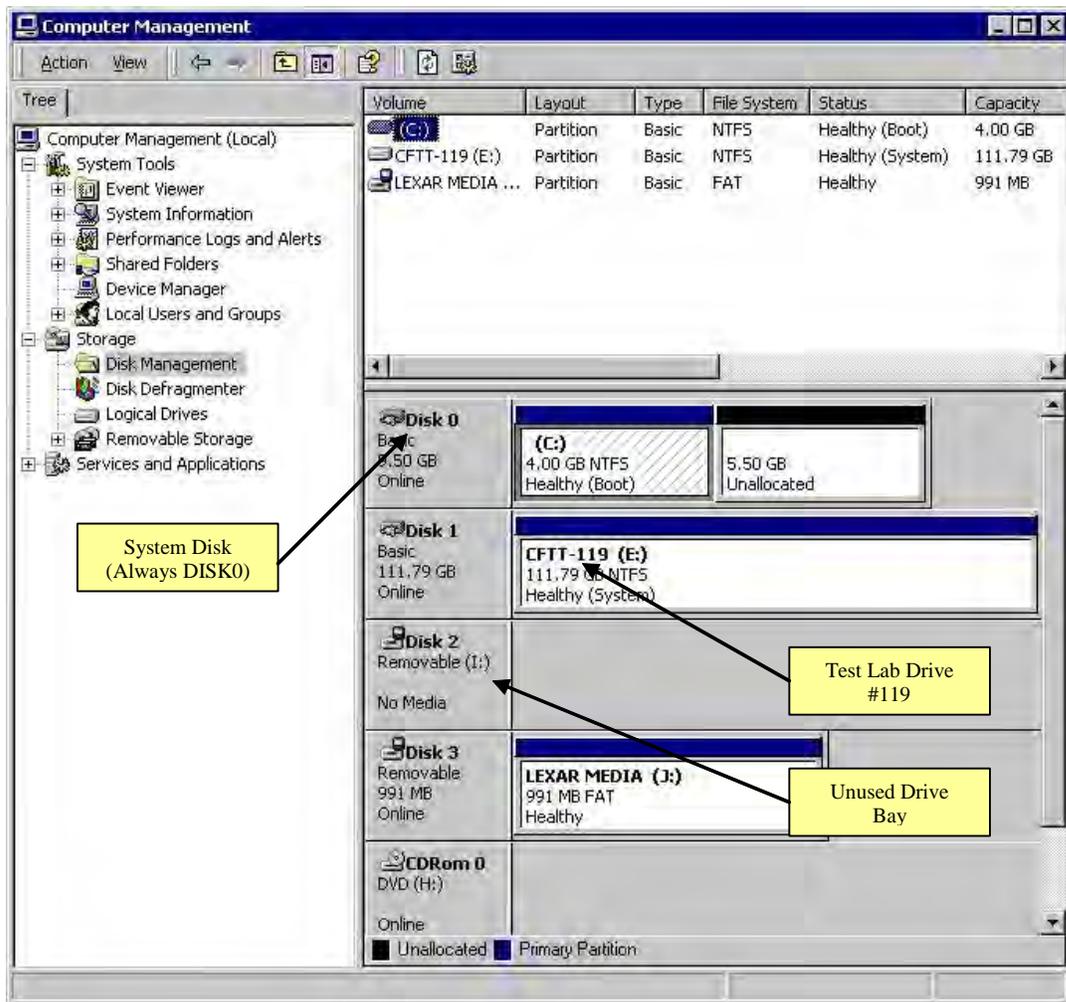
The tool conforms to this assertion if the SHA1 hashes of all protected drives are unchanged across an operating system boot.

8. Key to reading test results

The test summary sections each contain the following subsections.

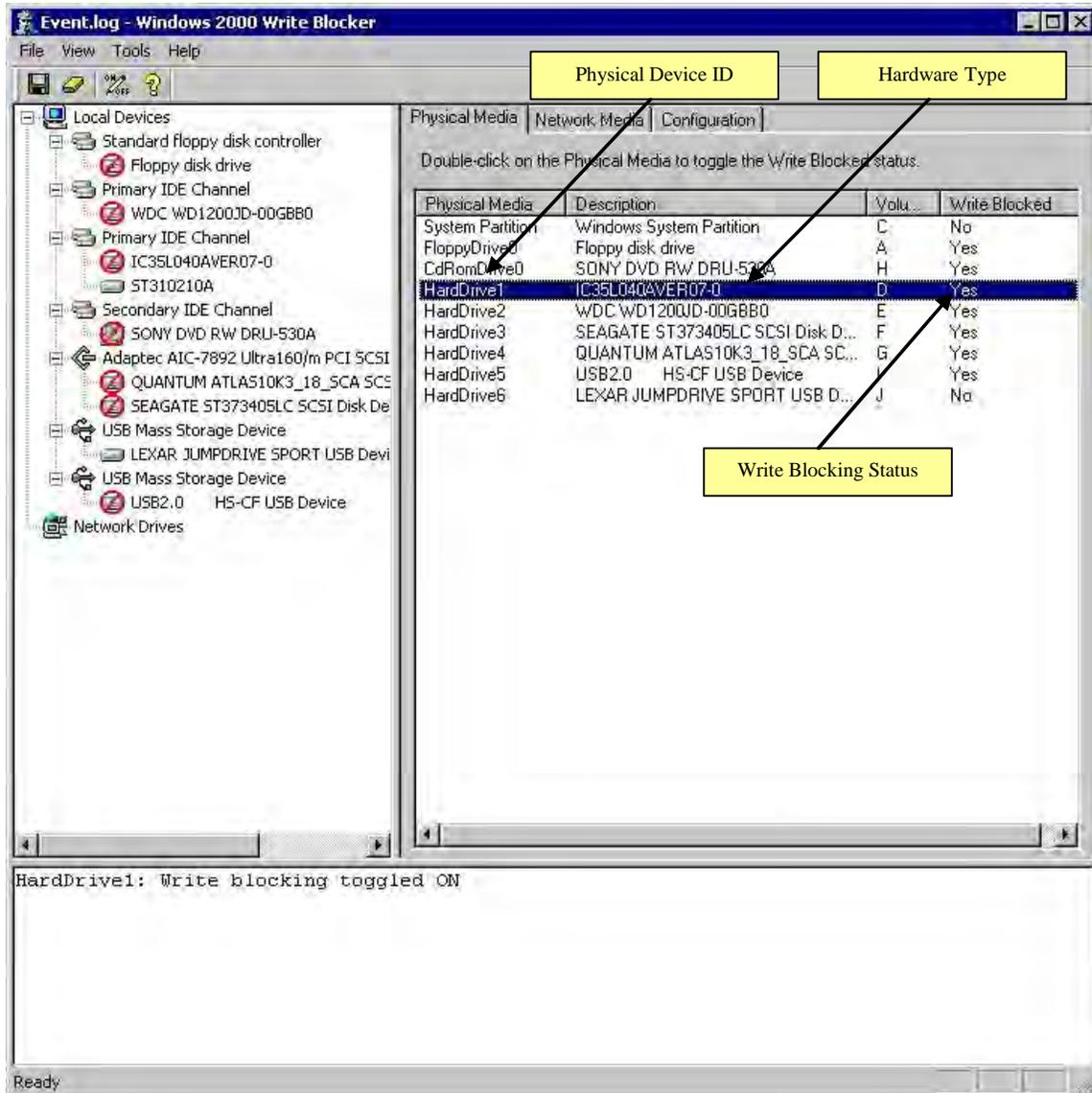
8.1 Hard disk configuration

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

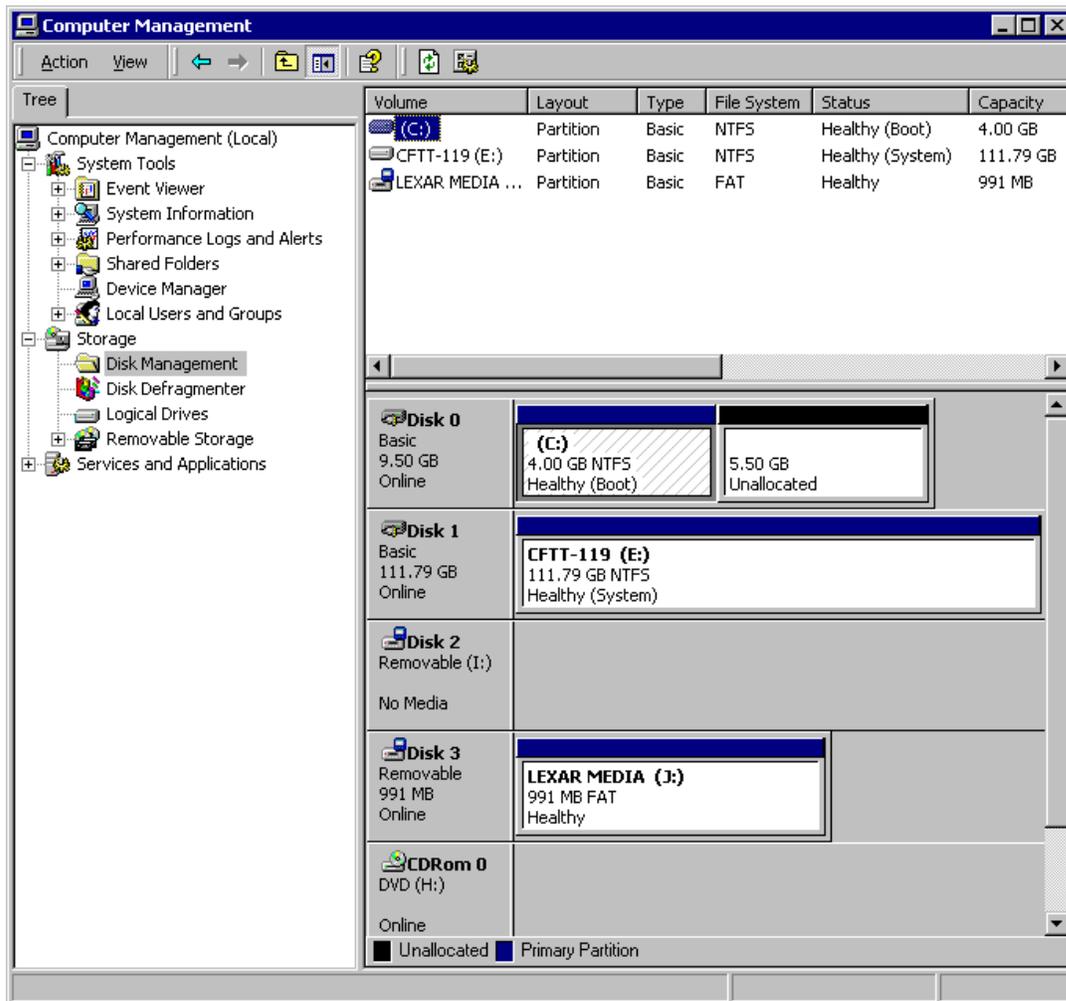
9. Test Result Summaries

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.

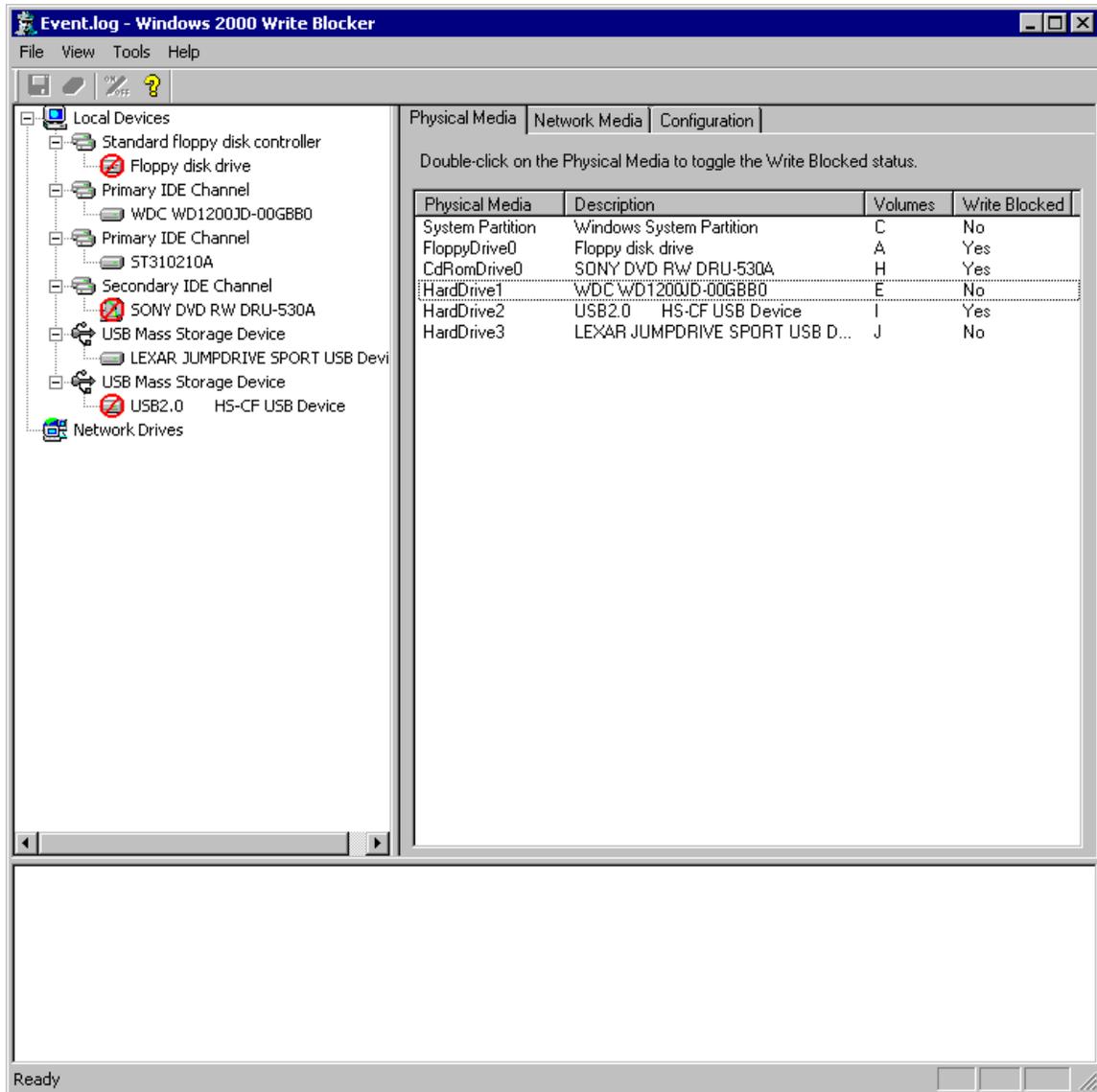
9.1.1 Hard disk configuration

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



9.1.2 Write blocker configuration

The Writeblocker W2K configuration used in this test is shown below.



9.1.3 Test output summary

```
NIST Software Write Blocker Test Suite V1.2
Tue Mar 28 15:32:28 2006

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	0EA083FC760A011547BE6817A6238401FF76AEF1
	After	9381A9693638EF9BDD2B83ACC7E6B2F94157C83A

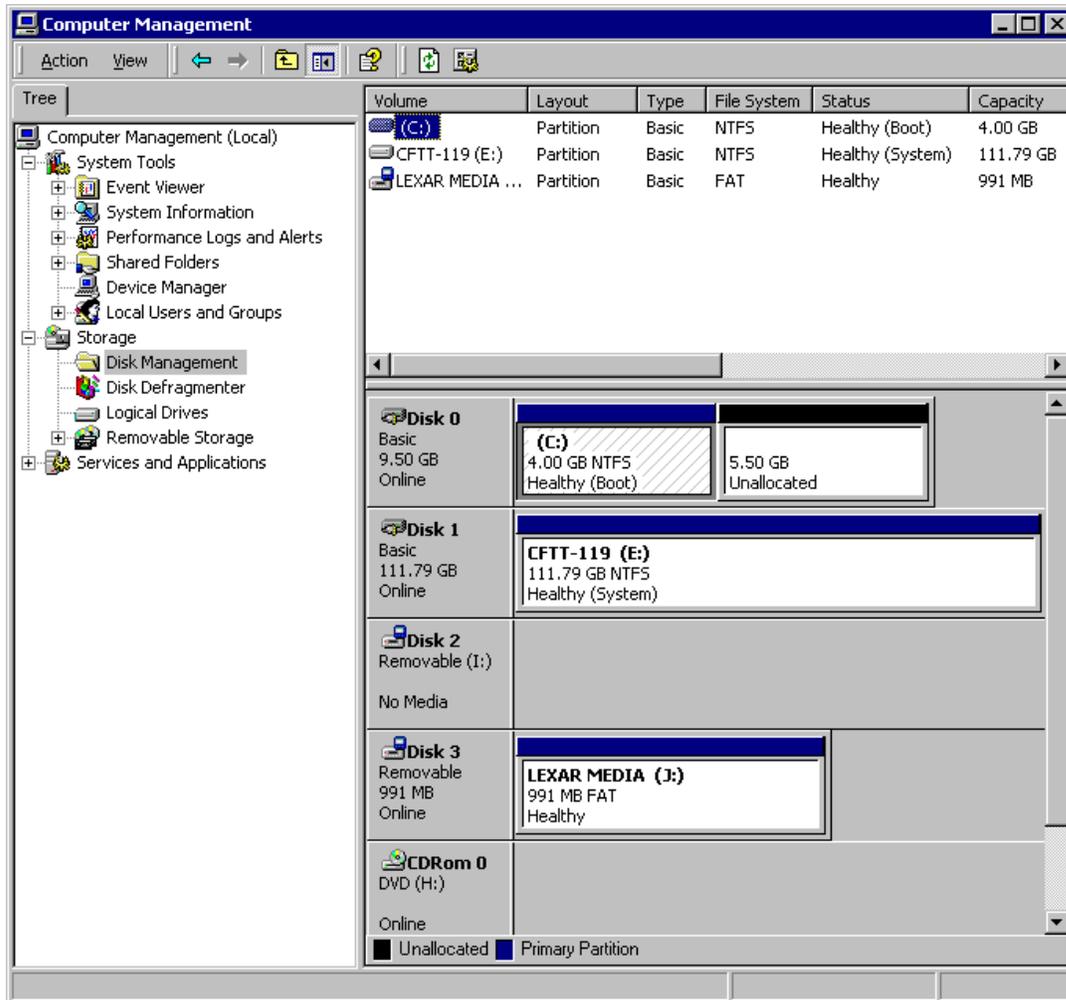
9.1.5 Test result analysis

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

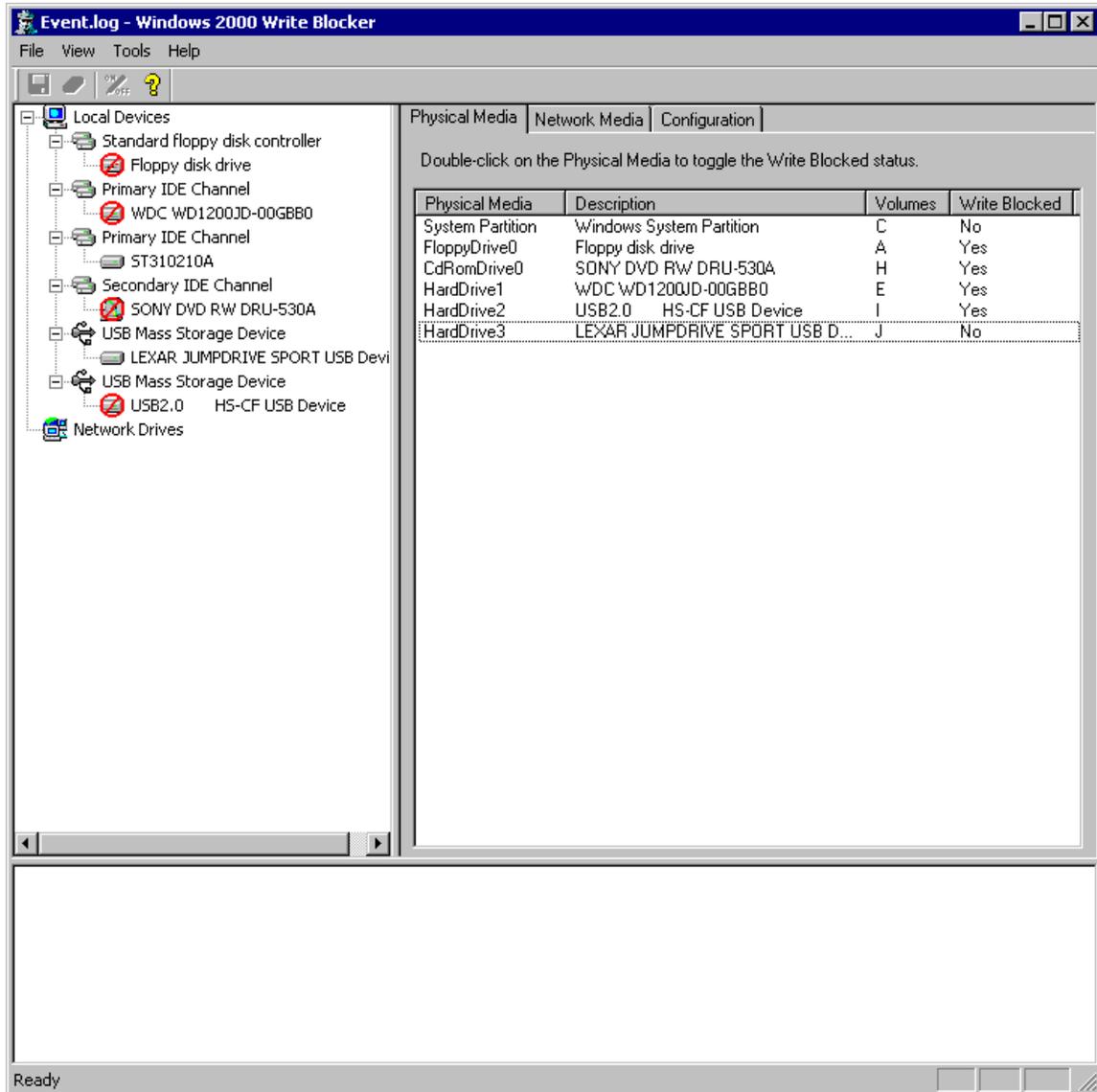
9.2 Test case SWB-02

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
Wed Mar 29 11:20:34 2006

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	9381A9693638EF9BDD2B83ACC7E6B2F94157C83A
	After	9381A9693638EF9BDD2B83ACC7E6B2F94157C83A

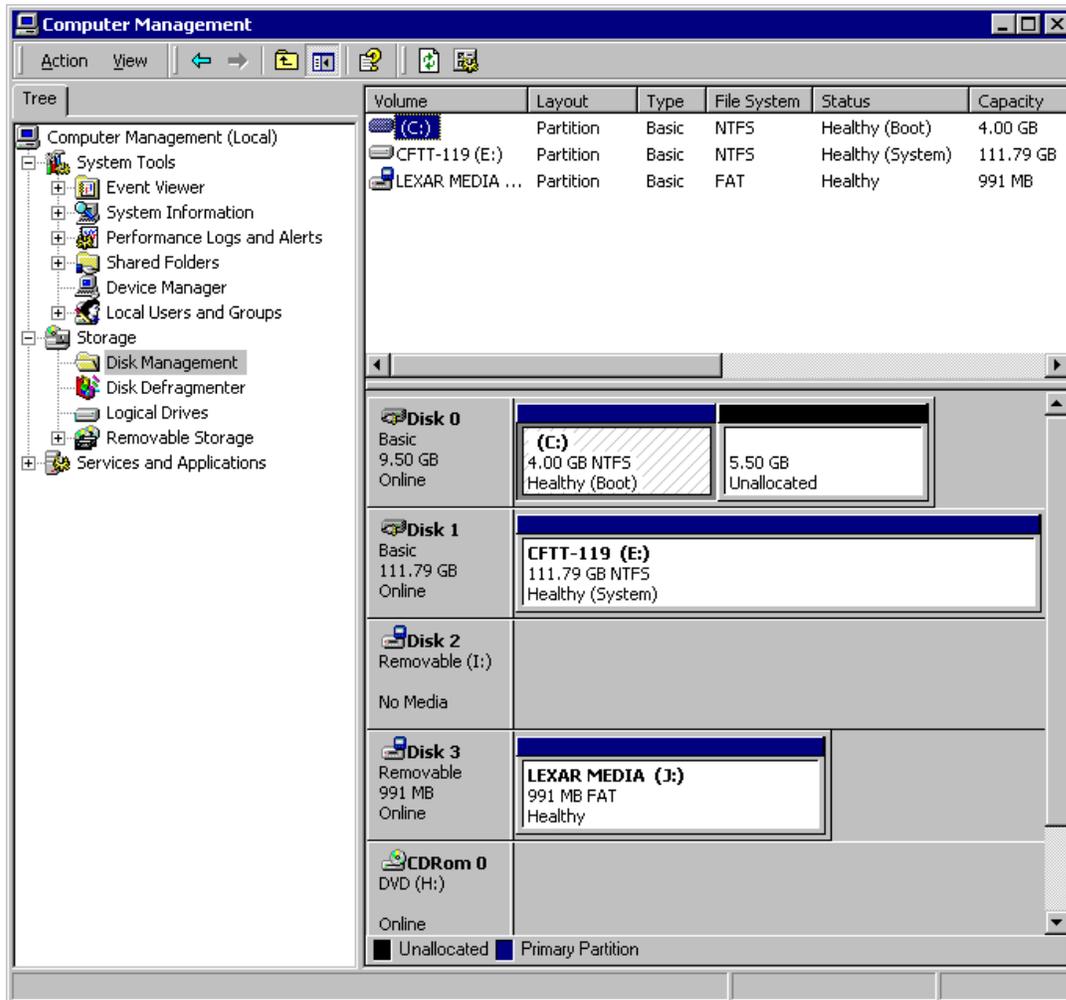
9.2.5 Test result analysis

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

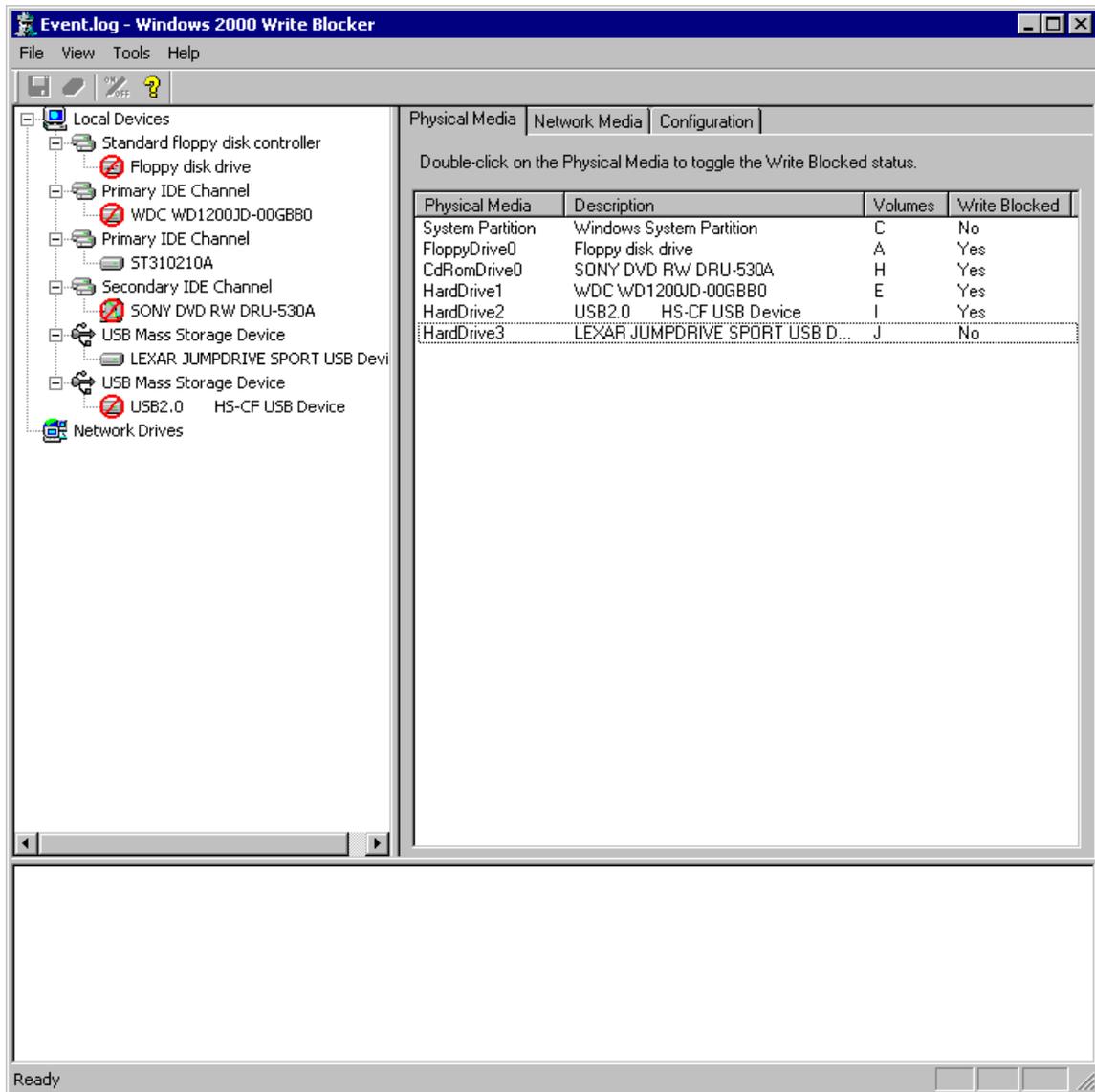
9.3 Test case SWB-03

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
Wed Mar 29 11:21:42 2006

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	9381A9693638EF9BDD2B83ACC7E6B2F94157C83A
	After	9381A9693638EF9BDD2B83ACC7E6B2F94157C83A

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 sysytem level
IRP_MJ_SET_QUOTA	0x1A	Appears to be blocked at file system level

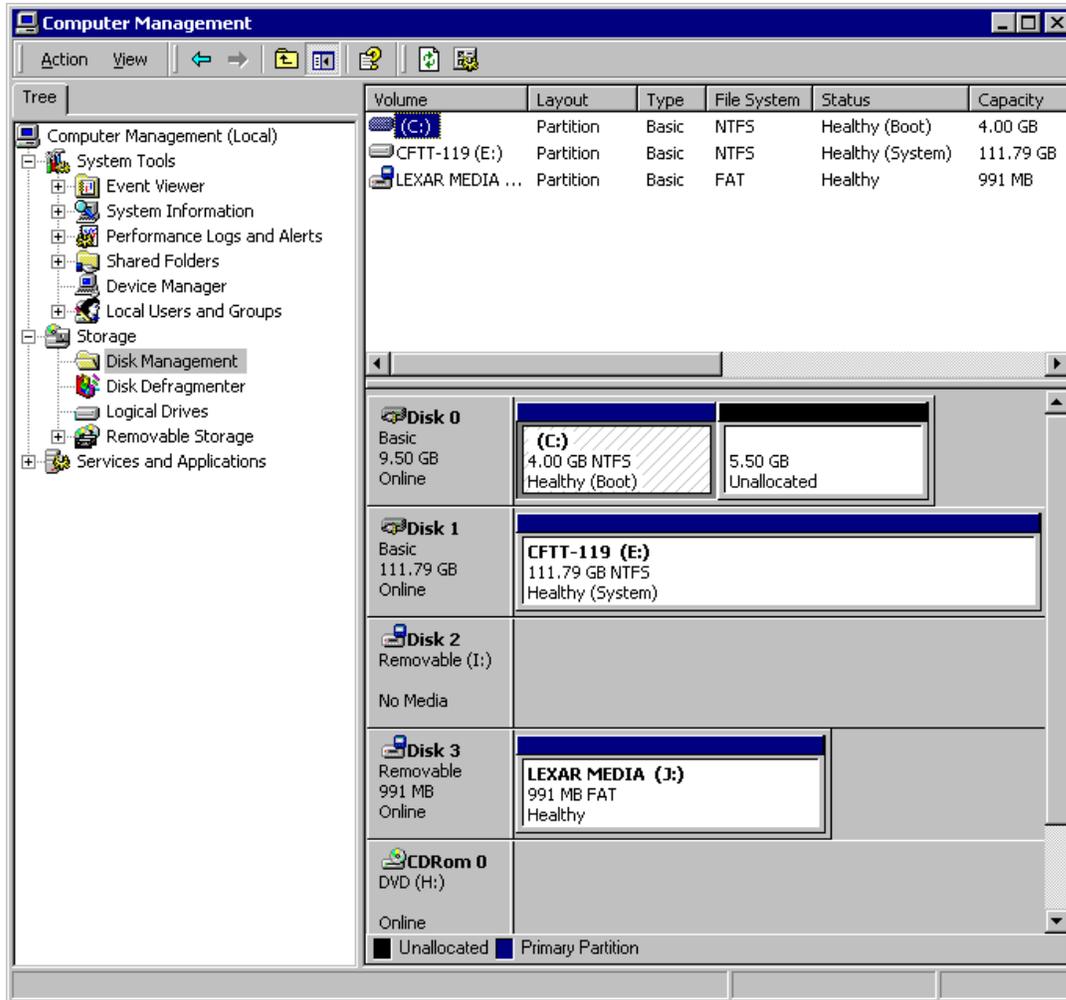
- The tool also failed to block 22 of the 34 SCSI CDB's in the WRITE category issued by the test application. The 22 SCSI commands that were not blocked by the tool are:

SCSI Comamnd 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

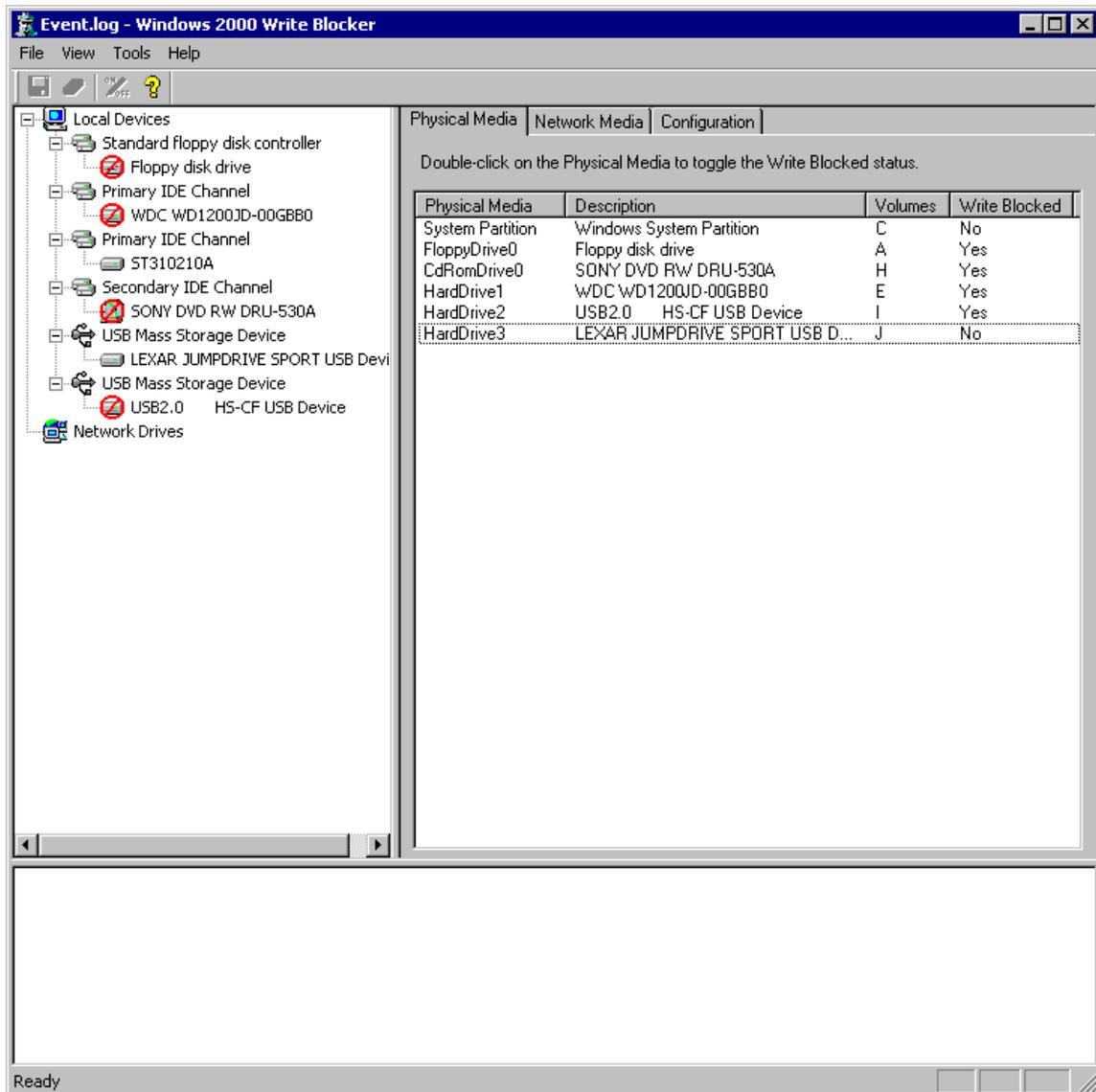
9.4 Test case SWB-04

This test case test's the tools 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
Wed Mar 29 11:22:29 2006

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 Specific 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	9381A9693638EF9BDD2B83ACC7E6B2F94157C83A
	After	9381A9693638EF9BDD2B83ACC7E6B2F94157C83A

9.4.5 Test results analysis

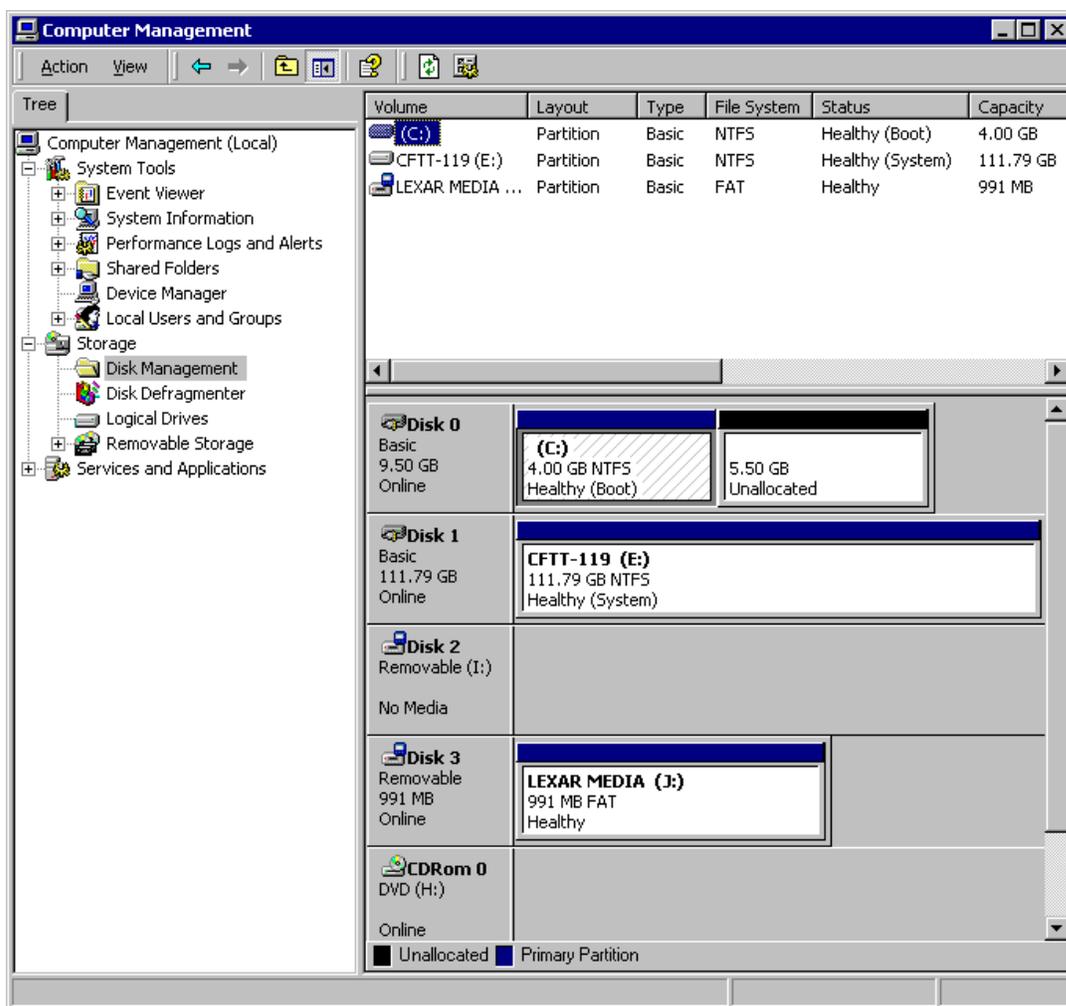
- The tool failed to produce the expected result
- The hard disk was not modified
- The tool failed to block any of the commands issued. The commands passed by the tool are shown below

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

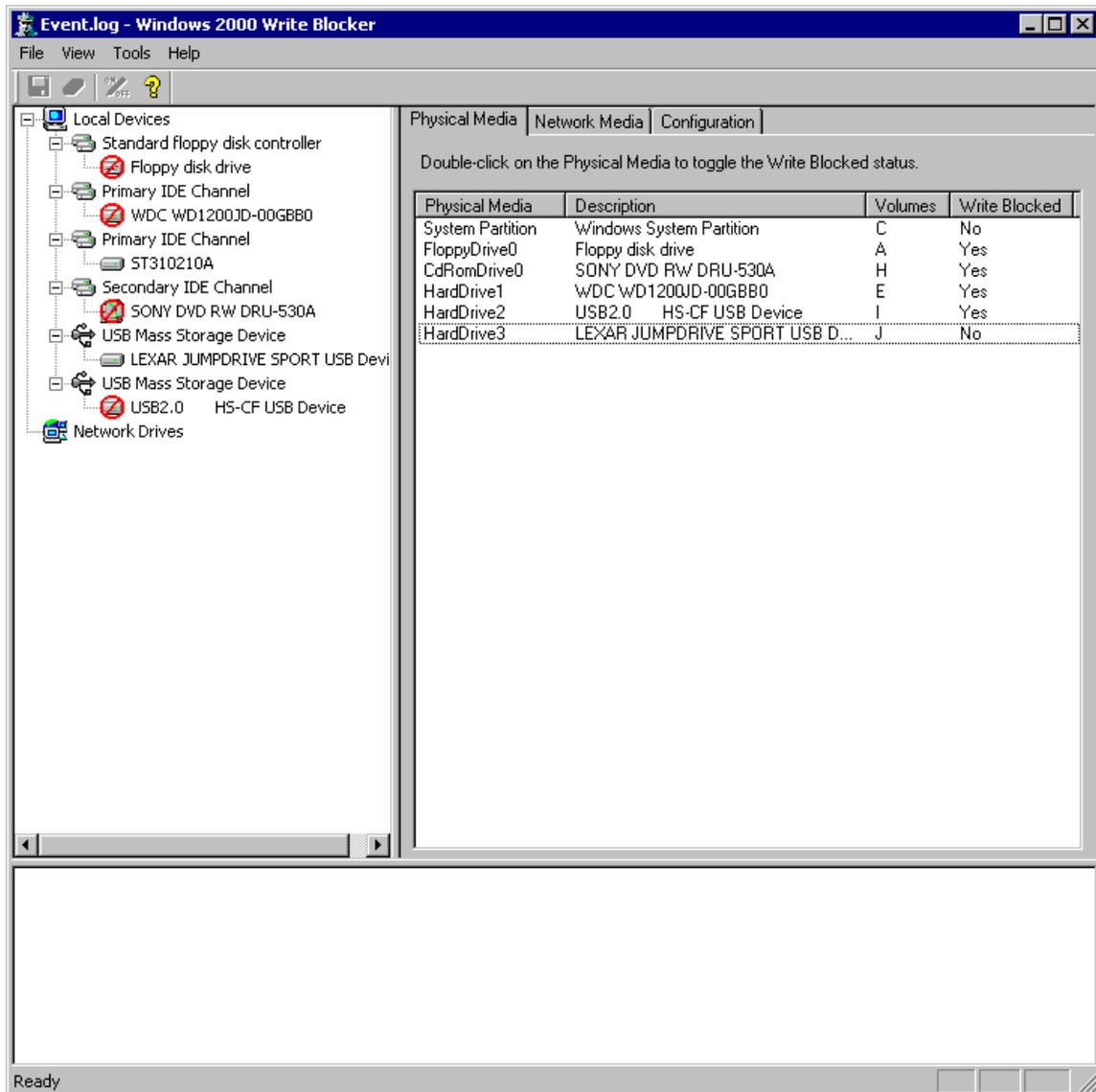
9.5 Test case SWB-05

This test case test's the tools 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
Wed Mar 29 11:22:53 2006

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	9381A9693638EF9BDD2B83ACC7E6B2F94157C83A
	After	9381A9693638EF9BDD2B83ACC7E6B2F94157C83A

9.5.5 Test results analysis

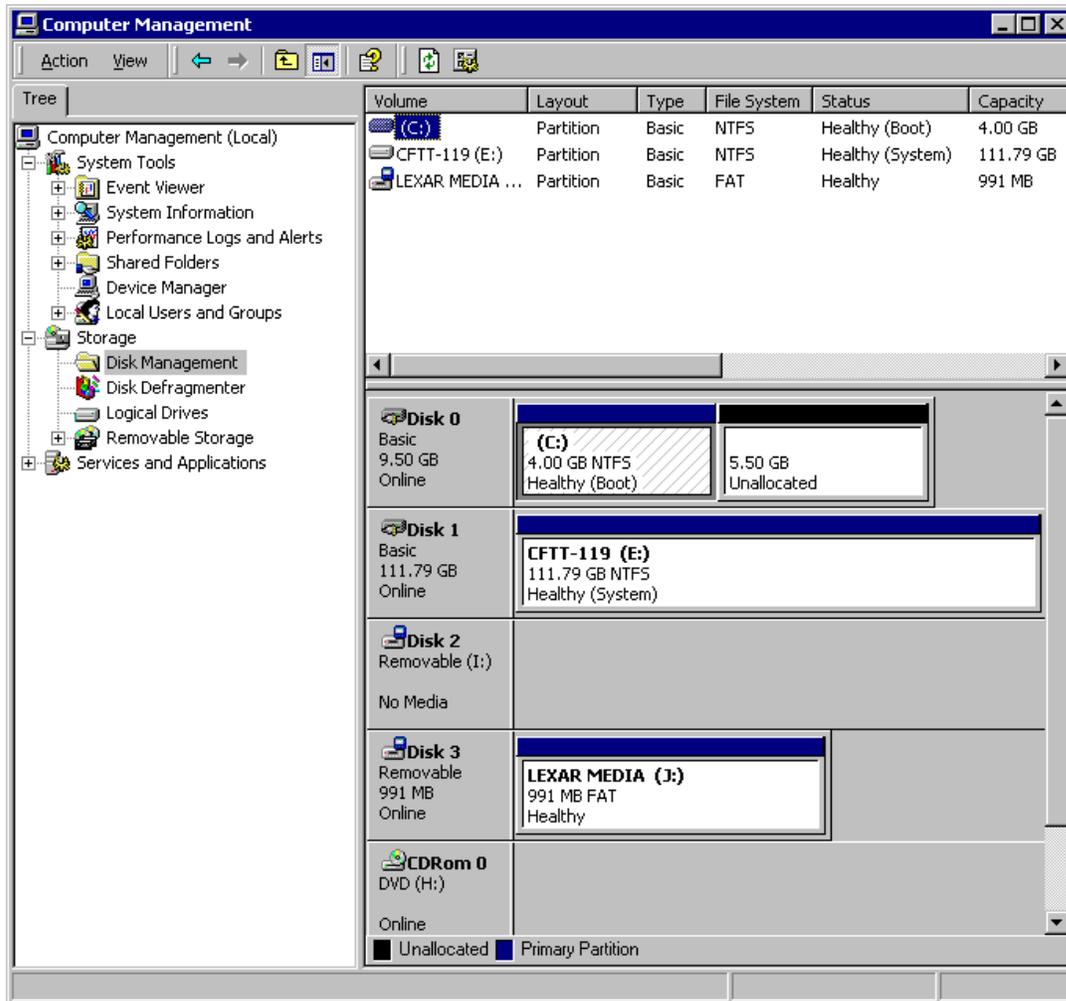
- The tool failed to produce the expected result.
- The hard disk was not modified.
- The tool did not block any of the commands in the UNDEFINED category. The UNDEFINED commands allowed by the tool are shown below.

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	

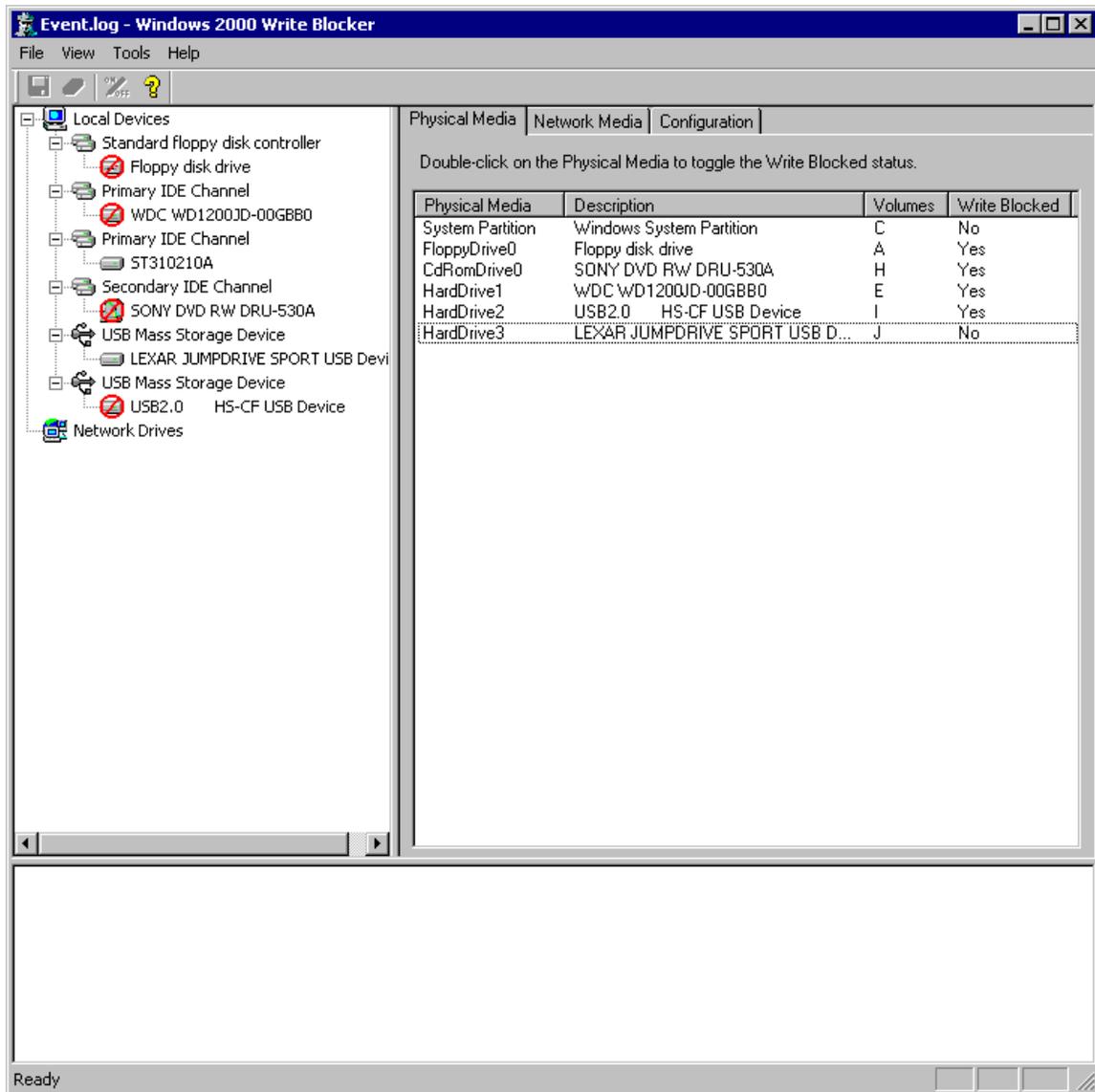
9.6 Test case SWB-06

This test case tests the tools 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
Wed Mar 29 11:23:14 2006

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	9381A9693638EF9BDD2B83ACC7E6B2F94157C83A
	After	9381A9693638EF9BDD2B83ACC7E6B2F94157C83A

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 test's the tools 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

The screenshot displays the Windows Computer Management console, specifically the Disk Management section. The left-hand tree view shows the navigation pane with 'Disk Management' selected. The main pane is divided into two sections: a table of volumes and a graphical representation of the disks.

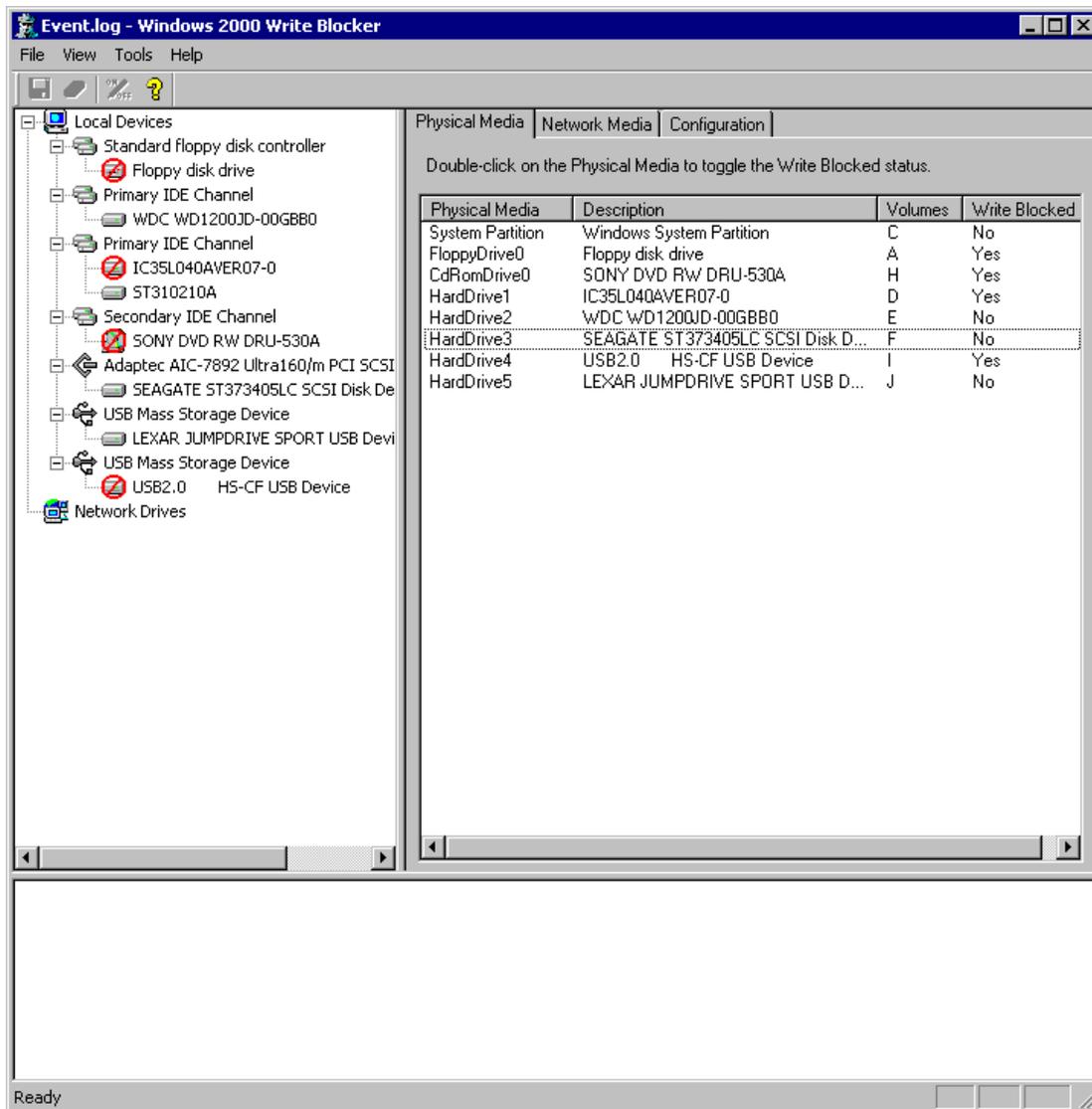
Volume	Layout	Type	File System	Status	C
(C:)	Partition	Basic	NTFS	Healthy (Boot)	4
CFTT-25 (F:)	Partition	Basic	NTFS	Healthy	6
CFTT-70 (D:)	Partition	Basic	NTFS	Healthy (Active)	1
CFTT-119 (E:)	Partition	Basic	NTFS	Healthy (System)	1
LEXAR MEDIA...	Partition	Basic	FAT	Healthy	9

The graphical representation below the table shows five disks:

- Disk 0:** Basic, 9.50 GB, Online. Contains a 4.00 GB NTFS partition (C:) and 5.50 GB of unallocated space.
- Disk 1:** Basic, 38.34 GB, Online. Contains a 1.37 GB NTFS partition (D:) and 36.97 GB of unallocated space.
- Disk 2:** Basic, 111.79 GB, Online. Contains a 111.79 GB NTFS partition (E:).
- Disk 3:** Basic, 68.36 GB, Online. Contains a 68.36 GB NTFS partition (F:).
- Disk 4:** Removable (I:), No Media.

A legend at the bottom indicates that black represents unallocated space and blue represents a primary partition.

9.7.2 Write blocker configuration



9.7.3 Test output summary

NIST Software Write Blocker Test Suite V1.2
Wed Mar 29 15:25:12 2006

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 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

9.7.4 Hard disk hash results

Drive Identification		Computed	SHA1 Value
\\.\PhysicalDrive1 (CFTT-70)	P	Before	1CF7082C7986BF78F9C6D80336FA73CF95742ED0
		After	1CF7082C7986BF78F9C6D80336FA73CF95742ED0
\\.\PhysicalDrive2 (CFTT-119)	U	Before	9381A9693638EF9BDD2B83ACC7E6B2F94157C83A
		After	183C6516E79819BC6A939438AC5A743C09F2D9F6
\\.\PhysicalDrive3 (CFTT-25)	U	Before	4F7C4571B9E48F9F597B8B74358888227BEC4FAB
		After	EF80683EC71BE95972B369220975D28448287152

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 test's the tools 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

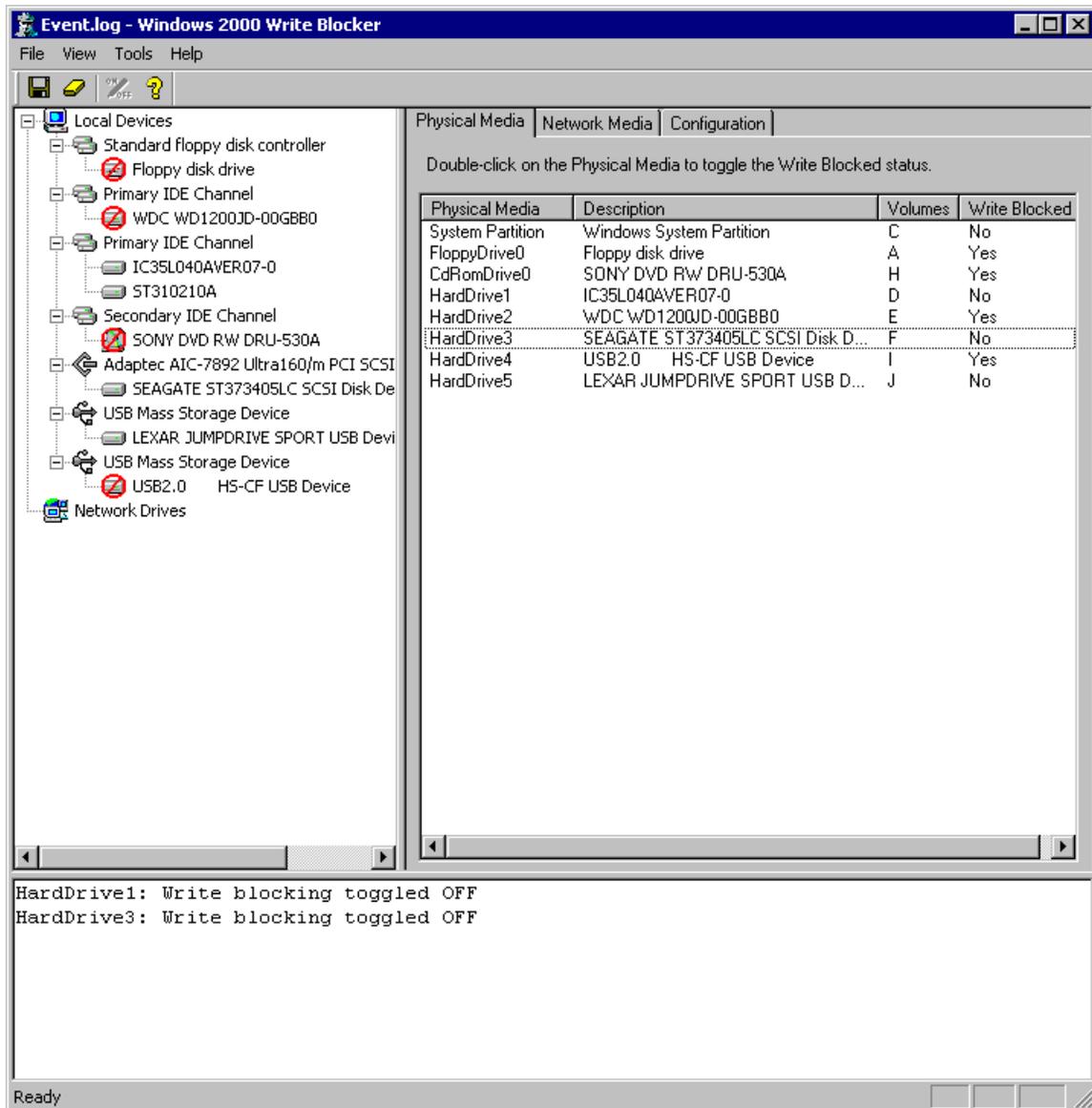
The screenshot displays the Windows Computer Management console, specifically the Disk Management section. The left-hand tree view shows the navigation pane with 'Disk Management' selected. The main area is divided into two panes. The top pane is a table listing the system's volumes, and the bottom pane is a graphical representation of the physical disks and their partitions.

Volume	Layout	Type	File System	Status	C
(C:)	Partition	Basic	NTFS	Healthy (Boot)	4
CFTT-25 (F:)	Partition	Basic	NTFS	Healthy	6
CFTT-70 (D:)	Partition	Basic	NTFS	Healthy (Active)	1
CFTT-119 (E:)	Partition	Basic	NTFS	Healthy (System)	1
LEXAR MEDIA...	Partition	Basic	FAT	Healthy	9

Disk	Capacity	Online	Partitions
Disk 0	9.50 GB	Online	(C:) 4.00 GB NTFS Healthy (Boot); 5.50 GB Unallocated
Disk 1	38.34 GB	Online	CFTT-70 (D:) 1.37 GB NTFS Healthy (Active); 36.97 GB Unallocated
Disk 2	111.79 GB	Online	CFTT-119 (E:) 111.79 GB NTFS Healthy (System)
Disk 3	68.36 GB	Online	CFTT-25 (F:) 68.36 GB NTFS Healthy
Disk 4	Removable (I:)	No Media	

Legend: ■ Unallocated ■ Primary Partition

9.8.2 Write blocker configuration



9.8.3 Test output summary

NIST Software Write Blocker Test Suite V1.2
 Thu Mar 30 10:37:14 2006

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 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

9.8.4 Hard disk hash results

Drive Identification		Computed	SHA1 Value
\\.\PhysicalDrive1 (CFTT-70)	U	Before	1CF7082C7986BF78F9C6D80336FA73CF95742ED0
		After	E26F57A42CCC32489F6BD382FC01A66690719C2F
\\.\PhysicalDrive2 (CFTT-119)	P	Before	183C6516E79819BC6A939438AC5A743C09F2D9F6
		After	183C6516E79819BC6A939438AC5A743C09F2D9F6
\\.\PhysicalDrive3 (CFTT-25)	U	Before	EF80683EC71BE95972B369220975D28448287152
		After	1B86BD633B94FF54CE3ED3E6357F1B68DBD79547

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 test's the tools 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

The screenshot displays the Windows Computer Management console, specifically the Disk Management section. The left-hand tree view shows the navigation pane with 'Storage' expanded and 'Disk Management' selected. The main pane is divided into two sections: a table of logical volumes and a graphical disk layout.

Volume	Layout	Type	File System	Status	C
(C:)	Partition	Basic	NTFS	Healthy (Boot)	4
CFTT-25 (F:)	Partition	Basic	NTFS	Healthy	6
CFTT-70 (D:)	Partition	Basic	NTFS	Healthy (Active)	1
CFTT-119 (E:)	Partition	Basic	NTFS	Healthy (System)	1
LEXAR MEDIA...	Partition	Basic	FAT	Healthy	9

Disk	Capacity	Online	Partitions	Unallocated
Disk 0	9.50 GB	Online	(C:) 4.00 GB NTFS Healthy (Boot)	5.50 GB Unallocated
Disk 1	38.34 GB	Online	CFTT-70 (D:) 1.37 GB NTFS Healthy (Active)	36.97 GB Unallocated
Disk 2	111.79 GB	Online	CFTT-119 (E:) 111.79 GB NTFS Healthy (System)	
Disk 3	68.36 GB	Online	CFTT-25 (F:) 68.36 GB NTFS Healthy	
Disk 4	Removable (I:)		No Media	

Legend: ■ Unallocated ■ Primary Partition

9.9.2 Write blocker configuration

The screenshot shows the 'Event.log - Windows 2000 Write Blocker' window. The left pane displays a tree view of 'Local Devices' with several items marked with a red 'X' icon, indicating they are write-protected. The right pane shows the 'Physical Media' tab with a table of physical media and their write-protected status.

Physical Media	Description	Volumes	Write Blocked
System Partition	Windows System Partition	C	No
FloppyDrive0	Floppy disk drive	A	Yes
CdRomDrive0	SONY DVD RW DRU-530A	H	Yes
HardDrive1	IC35L040AVER07-0	D	No
HardDrive2	WDC WD1200JD-00GBB0	E	Yes
HardDrive3	SEAGATE ST373405LC SCSI Disk D...	F	No
HardDrive4	USB2.0 HS-CF USB Device	I	Yes
HardDrive5	LEXAR JUMPDRIVE SPORT USB D...	J	No

Below the table, the event log shows the following messages:

```

HardDrive1: Write blocking toggled OFF
HardDrive3: Write blocking toggled OFF
  
```

The status bar at the bottom of the window indicates 'Ready'.

9.9.3 Test output summary

NI ST Software Write Blocker Test Suite V1.2
Thu Mar 30 11:48:48 2006

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 \\.\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

9.9.4 Hard disk hash results

Drive Identification		Computed	SHA1 Value
\\.\PhysicalDrive1 (CFTT-70)	U	Before	E26F57A42CCC32489F6BD382FC01A66690719C2F
		After	BDEB66F73ECABCA326F047C95761AE4A89C6DBE7
\\.\PhysicalDrive2 (CFTT-119)	U	Before	183C6516E79819BC6A939438AC5A743C09F2D9F6
		After	5AC51BAA663778A3677F08A502B91F4689D6029F
\\.\PhysicalDrive3 (CFTT-25)	P	Before	1B86BD633B94FF54CE3ED3E6357F1B68DBD79547
		After	1B86BD633B94FF54CE3ED3E6357F1B68DBD79547

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 test's the tools 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

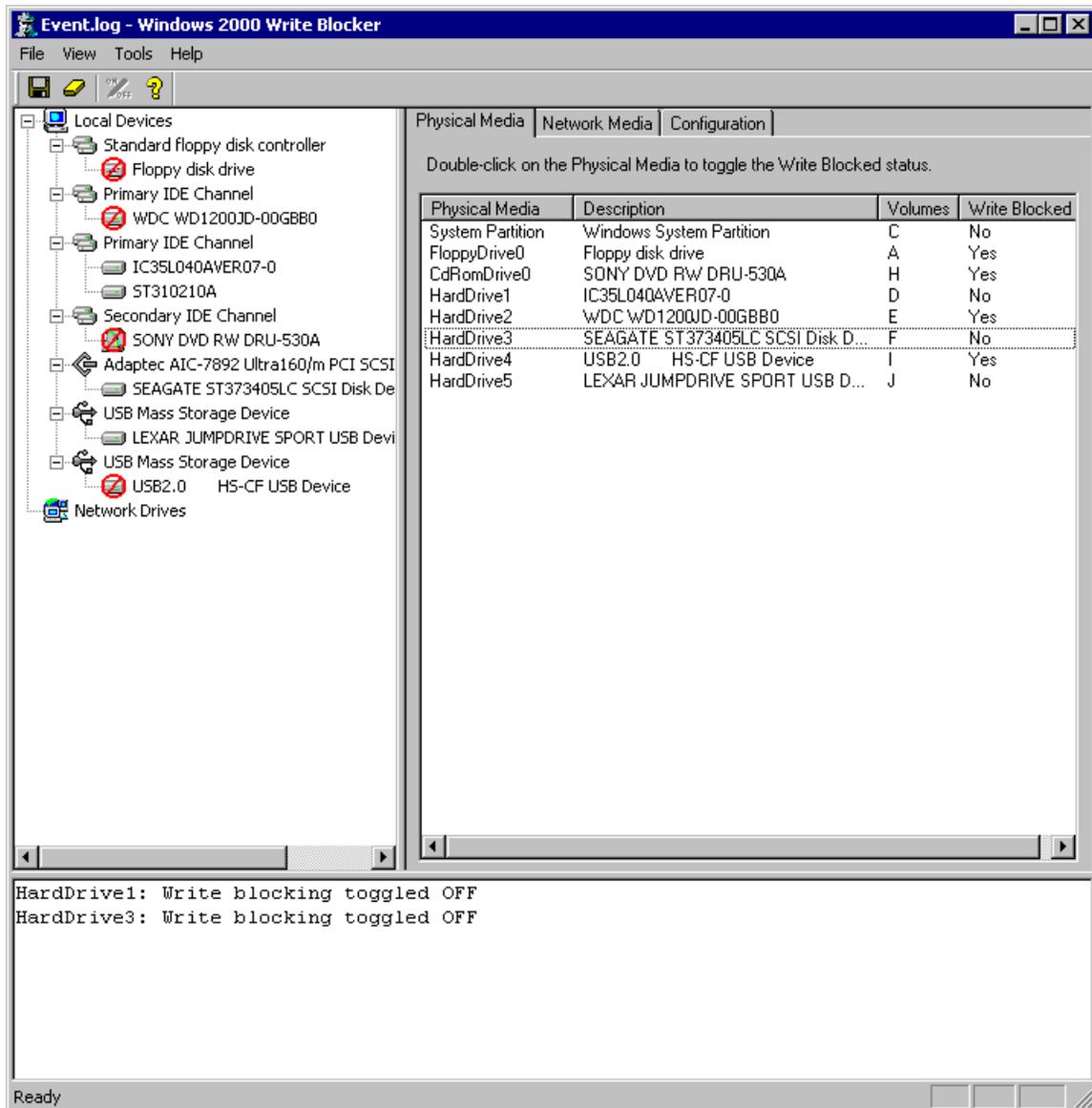
The screenshot displays the Windows Computer Management console, specifically the Disk Management section. The left pane shows the navigation tree with 'Storage' expanded to 'Disk Management'. The main pane shows a table of disk configurations and a graphical representation of the disks below.

Volume	Layout	Type	File System	Status	C
(C:)	Partition	Basic	NTFS	Healthy (Boot)	4
CFTT-25 (F:)	Partition	Basic	NTFS	Healthy	6
CFTT-70 (D:)	Partition	Basic	NTFS	Healthy (Active)	1
CFTT-119 (E:)	Partition	Basic	NTFS	Healthy (System)	1
LEXAR MEDIA...	Partition	Basic	FAT	Healthy	9

Disk	Capacity	Layout	Type	File System	Status
Disk 0	9.50 GB	(C:)	Basic	4.00 GB NTFS Healthy (Boot)	5.50 GB Unallocated
Disk 1	38.34 GB	CFTT-70 (D:)	Basic	1.37 GB NTFS Healthy (Active)	36.97 GB Unallocated
Disk 2	111.79 GB	CFTT-119 (E:)	Basic	111.79 GB NTFS Healthy (System)	
Disk 3	68.36 GB	CFTT-25 (F:)	Basic	68.36 GB NTFS Healthy	
Disk 4	Removable (I:)		Removable	No Media	

Legend: ■ Unallocated ■ Primary Partition

9.10.2 Write blocker configuration



9.10.3 Test output summary

NI ST Software Write Blocker Test Suite V1.2
Thu Mar 30 14:56:39 2006

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 \\.\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

9.10.4 Hard disk hash results

Drive Identification		Computed	SHA1 Value
\\.\PhysicalDrive1 (CFTT-70)	U	Before	BDEB66F73ECABCA326F047C95761AE4A89C6DBE7
		After	3E60FCFC2CCA0F89C757FCC608E1F71012F042AC
\\.\PhysicalDrive2 (CFTT-119)	P	Before	5AC51BAA663778A3677F08A502B91F4689D6029F
		After	5AC51BAA663778A3677F08A502B91F4689D6029F
\\.\PhysicalDrive3 (CFTT-25)	P	Before	1B86BD633B94FF54CE3ED3E6357F1B68DBD79547
		After	1B86BD633B94FF54CE3ED3E6357F1B68DBD79547

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 test's the tools 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

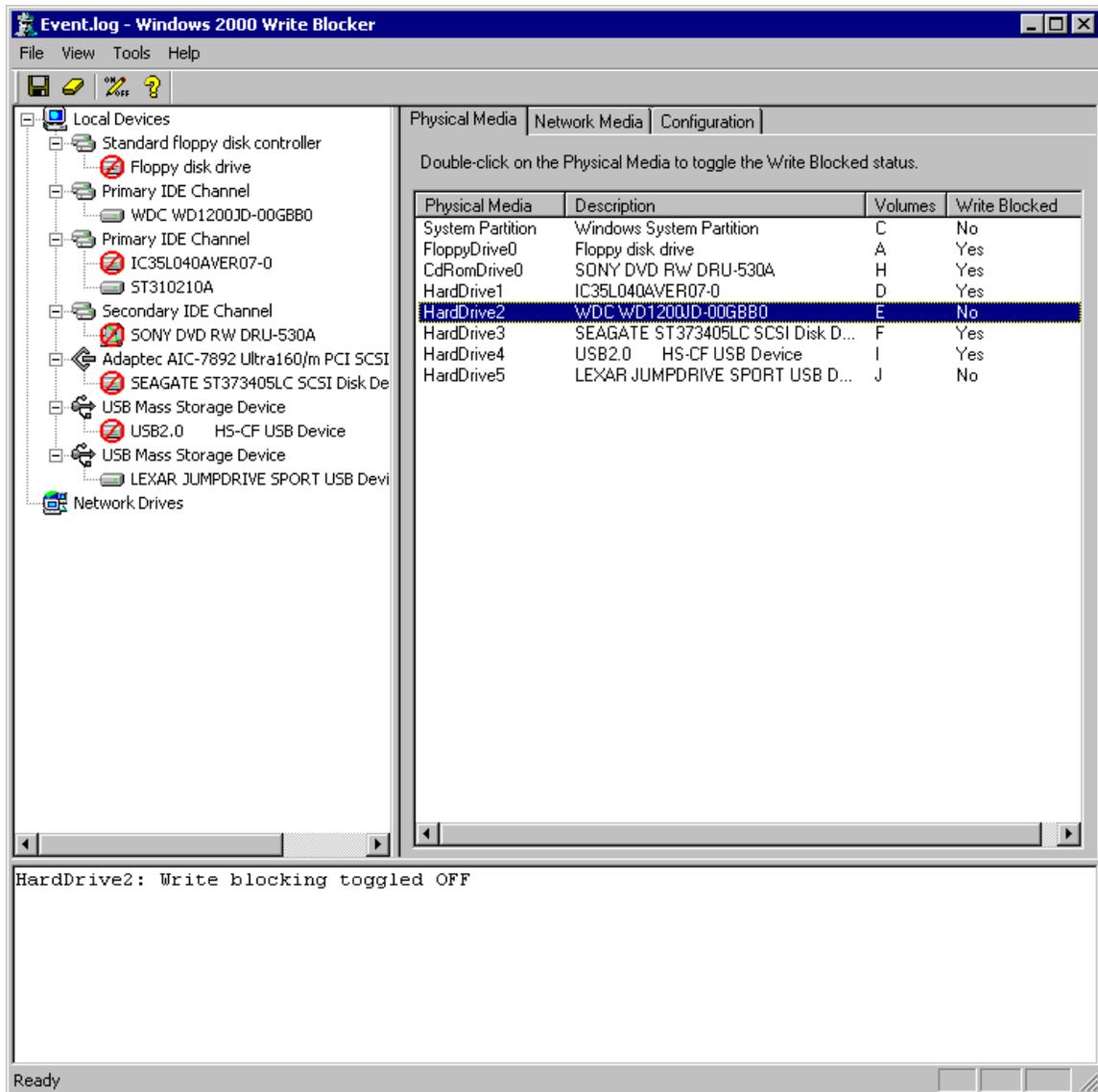
The screenshot displays the Windows Computer Management console, specifically the Disk Management section. The left-hand tree view shows the navigation pane with 'Storage' expanded to 'Disk Management'. The main pane is divided into two sections: a table of volumes and a graphical disk layout.

Volume	Layout	Type	File System	Status	C
(C:)	Partition	Basic	NTFS	Healthy (Boot)	4
CFTT-25 (F:)	Partition	Basic	NTFS	Healthy	6
CFTT-70 (D:)	Partition	Basic	NTFS	Healthy (Active)	1
CFTT-119 (E:)	Partition	Basic	NTFS	Healthy (System)	1
LEXAR MEDIA...	Partition	Basic	FAT	Healthy	9

Disk	Capacity	Layout	Type	File System	Status
Disk 0	9.50 GB	(C:) 4.00 GB NTFS Healthy (Boot)	Basic	NTFS	Online
Disk 1	38.34 GB	CFTT-70 (D:) 1.37 GB NTFS Healthy (Active)	Basic	NTFS	Online
Disk 2	111.79 GB	CFTT-119 (E:) 111.79 GB NTFS Healthy (System)	Basic	NTFS	Online
Disk 3	68.36 GB	CFTT-25 (F:) 68.36 GB NTFS Healthy	Basic	NTFS	Online
Disk 4	Removable (I:)	No Media	Removable		Offline

Legend: ■ Unallocated ■ Primary Partition

9.11.2 Write blocker configuration



9.11.3 Test output summary

NIST Software Write Blocker Test Suite V1.2
 Thu Mar 30 16:27:02 2006

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 \\.\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

9.11.4 Hard disk hash results

Drive Identification		Computed	SHA1 Value
\\.\PhysicalDrive1 (CFTT-70)	P	Before	3E60FCFC2CCA0F89C757FCC608E1F71012F042AC
		After	3E60FCFC2CCA0F89C757FCC608E1F71012F042AC
\\.\PhysicalDrive2 (CFTT-119)	U	Before	5AC51BAA663778A3677F08A502B91F4689D6029F
		After	7B4D517D0D330103FCD6677AC4BC44C39BB637A1
\\.\PhysicalDrive3 (CFTT-25)	P	Before	1B86BD633B94FF54CE3ED3E6357F1B68DBD79547
		After	1B86BD633B94FF54CE3ED3E6357F1B68DBD79547

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 test's the tools 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

The screenshot displays the Windows Computer Management console, specifically the Disk Management section. The left-hand tree view shows the navigation pane with 'Storage' expanded to 'Disk Management'. The main pane shows a table of disk configurations and a graphical representation of the disks below.

Volume	Layout	Type	File System	Status	C
(C:)	Partition	Basic	NTFS	Healthy (Boot)	4
CFTT-25 (F:)	Partition	Basic	NTFS	Healthy	6
CFTT-70 (D:)	Partition	Basic	NTFS	Healthy (Active)	1
CFTT-119 (E:)	Partition	Basic	NTFS	Healthy (System)	1
LEXAR MEDIA...	Partition	Basic	FAT	Healthy	9

Disk	Capacity	Layout	Type	File System	Status
Disk 0	9.50 GB	(C:)	Basic	4.00 GB NTFS 5.50 GB Unallocated	Online
Disk 1	38.34 GB	CFTT-70 (D:)	Basic	1.37 GB NTFS 36.97 GB Unallocated	Online
Disk 2	111.79 GB	CFTT-119 (E:)	Basic	111.79 GB NTFS	Online
Disk 3	68.36 GB	CFTT-25 (F:)	Basic	68.36 GB NTFS	Online
Disk 4	Removable (I:)		Removable	No Media	

Legend: ■ Unallocated ■ Primary Partition

9.12.2 Write blocker configuration

Event.log - Windows 2000 Write Blocker

File View Tools Help

Local Devices

- Standard floppy disk controller
 - Floppy disk drive
- Primary IDE Channel
 - WDC WD1200JD-00GBB0
- Primary IDE Channel
 - IC35L040AVER07-0
 - ST310210A
- Secondary IDE Channel
 - SONY DVD RW DRU-530A
- Adaptec AIC-7892 Ultra160/m PCI SCSI
 - SEAGATE ST373405LC SCSI Disk De
- USB Mass Storage Device
 - LEXAR JUMPDRIVE SPORT USB Devi
- USB Mass Storage Device
 - USB2.0 HS-CF USB Device
- Network Drives

Physical Media | Network Media | Configuration

Double-click on the Physical Media to toggle the Write Blocked status.

Physical Media	Description	Volumes	Write Blocked
System Partition	Windows System Partition	C	No
FloppyDrive0	Floppy disk drive	A	Yes
CdRomDrive0	SONY DVD R/W DRU-530A	H	Yes
HardDrive1	IC35L040AVER07-0	D	Yes
HardDrive2	WDC WD1200JD-00GBB0	E	Yes
HardDrive3	SEAGATE ST373405LC SCSI Disk D...	F	No
HardDrive4	USB2.0 HS-CF USB Device	I	Yes
HardDrive5	LEXAR JUMPDRIVE SPORT USB D...	J	No

```

HardDrive3: Create Blocked
HardDrive1: Create Blocked
HardDrive2: Create Blocked
HardDrive3: Create Blocked
HardDrive1: Create Blocked
HardDrive2: Create Blocked
HardDrive3: Create Blocked
HardDrive3: Write blocking toggled OFF
  
```

Ready

9.12.3 Test output summary

NIST Software Write Blocker Test Suite V1.2
Thu Mar 30 16:27:02 2006

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 SPeci fi c CDB's	80	0	80
Undefi ned 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 fi c CDB's	80	0	80
Undefi ned 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 fi c CDB's	80	0	80
Undefi ned CDB's	53	0	53

9.12.4 Hard disk hash results

Drive Identification		Computed	SHA1 Value
\\.\PhysicalDrive1 (CFTT-70)	P	Before	3E60FCFC2CCA0F89C757FCC608E1F71012F042AC
		After	3E60FCFC2CCA0F89C757FCC608E1F71012F042AC
\\.\PhysicalDrive2 (CFTT-119)	P	Before	7B4D517D0D330103FCD6677AC4BC44C39BB637A1
		After	7B4D517D0D330103FCD6677AC4BC44C39BB637A1
\\.\PhysicalDrive3 (CFTT-25)	U	Before	1B86BD633B94FF54CE3ED3E6357F1B68DBD79547
		After	ADF1579F0B4ACB5A17D0F647868C78ACD8C6109F

9.12.5 Test results analysis

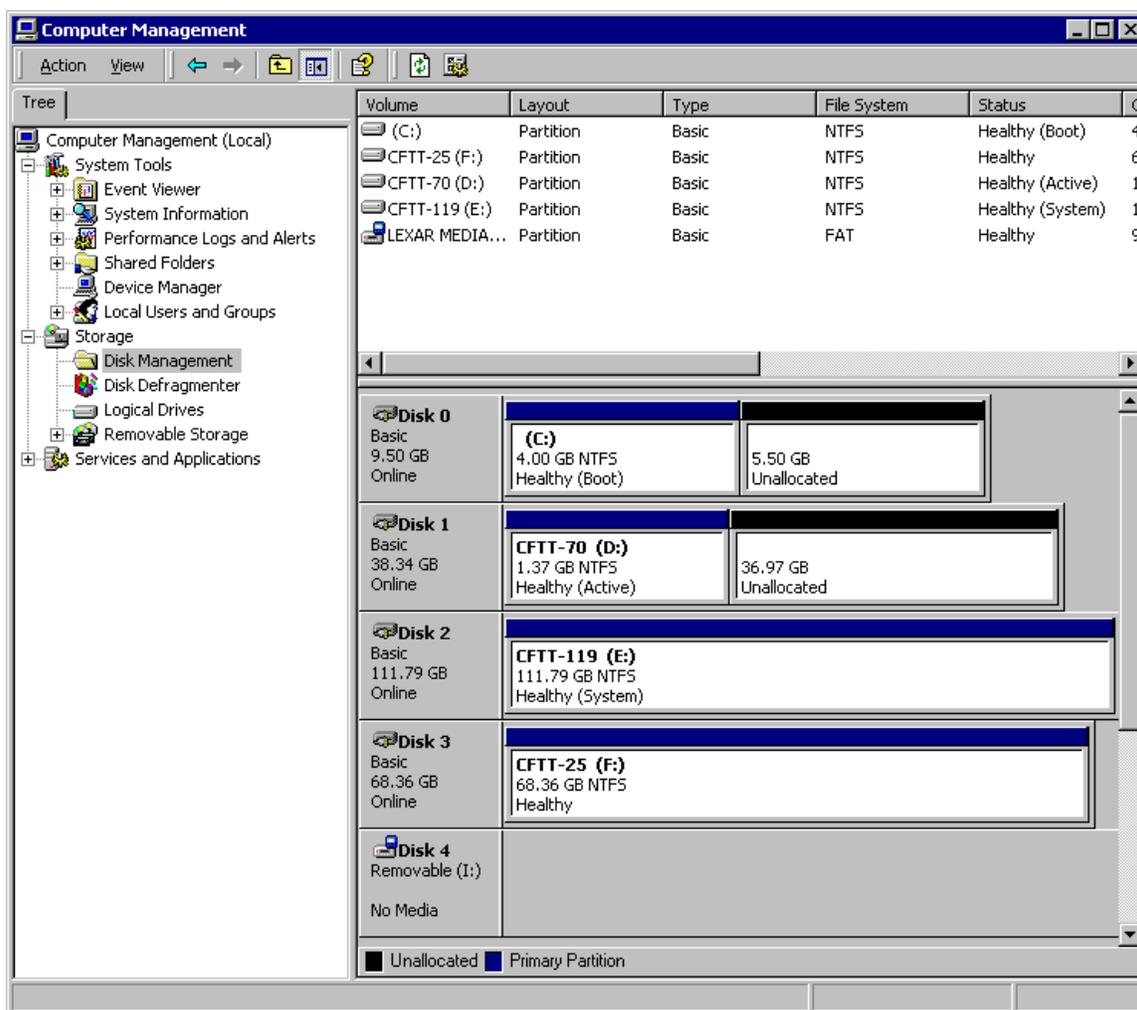
The tool failed to produce the expected result. The number of drives configured and the pattern of protection applied did not alter the ability of the tool to protect designated drives. However, the tool failed to block all commands in the protected categories. The protection failures observed were identical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

9.13 Test case SWB-13

This case test's the tools 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



The screenshot displays the Windows Computer Management console, specifically the Disk Management section. The left-hand tree view shows the navigation pane with 'Disk Management' selected. The main pane is divided into two sections: a table of volumes and a graphical disk layout.

Volume	Layout	Type	File System	Status	C
(C:)	Partition	Basic	NTFS	Healthy (Boot)	4
CFTT-25 (F:)	Partition	Basic	NTFS	Healthy	6
CFTT-70 (D:)	Partition	Basic	NTFS	Healthy (Active)	1
CFTT-119 (E:)	Partition	Basic	NTFS	Healthy (System)	1
LEXAR MEDIA...	Partition	Basic	FAT	Healthy	9

The graphical disk layout shows five disks:

- Disk 0:** Basic, 9.50 GB, Online. Contains a 4.00 GB NTFS partition (C:) and 5.50 GB of unallocated space.
- Disk 1:** Basic, 38.34 GB, Online. Contains a 1.37 GB NTFS partition (D:) and 36.97 GB of unallocated space.
- Disk 2:** Basic, 111.79 GB, Online. Contains a 111.79 GB NTFS partition (E:).
- Disk 3:** Basic, 68.36 GB, Online. Contains a 68.36 GB NTFS partition (F:).
- Disk 4:** Removable (I:), No Media.

A legend at the bottom indicates that black represents unallocated space and blue represents a primary partition.

9.13.2 Write blocker configuration

Event.log - Windows 2000 Write Blocker

File View Tools Help

Local Devices

- Standard floppy disk controller
 - Floppy disk drive
- Primary IDE Channel
 - WDC WD1200JD-00GBB0
- Primary IDE Channel
 - IC35L040AVER07-0
 - ST310210A
- Secondary IDE Channel
 - SONY DVD RW DRU-530A
- Adaptec AIC-7892 Ultra160/m PCI SCSI
 - QUANTUM ATLAS10K3_18_SCA SCSI
 - SEAGATE ST373405LC SCSI Disk De
- USB Mass Storage Device
 - LEXAR JUMPDRIVE SPORT USB Devi
- USB Mass Storage Device
 - USB2.0 HS-CF USB Device
- Network Drives

Physical Media Network Media Configuration

Double-click on the Physical Media to toggle the Write Blocked status.

Physical Media	Description	Volumes	Write Blocked
System Partition	Windows System Partition	C	No
FloppyDrive0	Floppy disk drive	A	Yes
CdRomDrive0	SONY DVD RW DRU-530A	H	Yes
HardDrive1	IC35L040AVER07-0	D	Yes
HardDrive2	WDC WD1200JD-00GBB0	E	No
HardDrive3	SEAGATE ST373405LC SCSI Disk D...	F	No
HardDrive4	QUANTUM ATLAS10K3_18_SCA SC...	G	Yes
HardDrive5	USB2.0 HS-CF USB Device	I	Yes
HardDrive6	LEXAR JUMPDRIVE SPORT USB D...	J	No

HardDrive2: Write blocking toggled OFF
HardDrive3: Write blocking toggled OFF

Ready

9.13.3 Test output summary

NIST Software Write Blocker Test Suite V1.2
 Fri Mar 31 13:43:24 2006

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 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 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	3E60FCFC2CCA0F89C757FCC608E1F71012F042AC
		After	3E60FCFC2CCA0F89C757FCC608E1F71012F042AC
\\.\PhysicalDrive2 (CFTT-119)	U	Before	7B4D517D0D330103FCD6677AC4BC44C39BB637A1
		After	88C9DC6AA3001F10C1F1109C061A614BCBD62C1B
\\.\PhysicalDrive3 (CFTT-25)	U	Before	ADF1579F0B4ACB5A17D0F647868C78ACD8C6109F
		After	F4D25FF778F15A3C43239400BA2A900CDD9ED64F
\\.\PhysicalDrive4 (CFTT-27)	P	Before	21B811181FFFF4D8237461C1848343FF3F477CE7
		After	21B811181FFFF4D8237461C1848343FF3F477CE7

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 test's the tools 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

9.14.1 Hard disk configuration

The screenshot shows the Windows Computer Management console, specifically the Disk Management section. The left pane shows the tree view with 'Disk Management' selected. The main area displays a table of disk configurations and a graphical representation of the disks.

Volume	Layout	Type	File System
(C:)	Partition	Basic	NTFS
CFTT-25 (F:)	Partition	Basic	NTFS
CFTT-27 (G:)	Partition	Basic	FAT32
CFTT-70 (D:)	Partition	Basic	NTFS
CFTT-119 (E:)	Partition	Basic	NTFS
LEXAR MEDIA...	Partition	Basic	FAT

Disk	Capacity	Health	Partition	File System	Capacity	Health	File System
Disk 0	9.50 GB	Online	(C:)	4.00 GB NTFS	5.50 GB	Unallocated	Unallocated
Disk 1	38.34 GB	Online	CFTT-70 (D:)	1.37 GB NTFS	36.97 GB	Unallocated	Unallocated
Disk 2	111.79 GB	Online	CFTT-119 (E:)	111.79 GB NTFS			Healthy (System)
Disk 3	68.36 GB	Online	CFTT-25 (F:)	68.36 GB NTFS			Healthy
Disk 4	17.12 GB	Online	CFTT-27 (G:)	8.47 GB FAT32	8.65 GB	Unallocated	Unallocated

Legend: ■ Unallocated ■ Primary Partition

9.14.2 Write blocker configuration

Event.log - Windows 2000 Write Blocker

File View Tools Help

Local Devices

- Standard floppy disk controller
 - Floppy disk drive
- Primary IDE Channel
 - WDC WD1200JD-00GBB0
- Primary IDE Channel
 - IC35L040AVER07-0
 - ST310210A
- Secondary IDE Channel
 - SONY DVD RW DRU-530A
- Adaptec AIC-7892 Ultra160/m PCI SCSI
 - QUANTUM ATLAS10K3_18_SCA SCSI
 - SEAGATE ST373405LC SCSI Disk De
- USB Mass Storage Device
 - LEXAR JUMPDRIIVE SPORT USB Devi
- USB Mass Storage Device
 - USB2.0 HS-CF USB Device
- Network Drives

Physical Media | Network Media | Configuration

Double-click on the Physical Media to toggle the Write Blocked status.

Physical Media	Description	Volumes	Write Blocked
System Partition	Windows System Partition	C	No
FloppyDrive0	Floppy disk drive	A	Yes
CdRomDrive0	SONY DVD RW DRU-530A	H	Yes
HardDrive1	IC35L040AVER07-0	D	No
HardDrive2	WDC WD1200JD-00GBB0	E	No
HardDrive3	SEAGATE ST373405LC SCSI Disk D...	F	Yes
HardDrive4	QUANTUM ATLAS10K3_18_SCA SC...	G	Yes
HardDrive5	USB2.0 HS-CF USB Device	I	Yes
HardDrive6	LEXAR JUMPDRIIVE SPORT USB D...	J	No

HardDrive1: Write blocking toggled OFF
HardDrive2: Write blocking toggled OFF

Ready

9.14.3 Test output summary

```

NIST Software Write Blocker Test Suite V1.2
Fri May 12 10:13:47 2006

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 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 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

9.14.4 Hard disk hash results

Drive Identification		Computed	SHA1 Value
\\.\PhysicalDrive1 (CFTT-70)	U	Before	6D96DA3851D7C4F4F124D29D0F02636E47DA3219
		After	61A09D9D3DC9B836C0100DE40F5FA72A93241A80
\\.\PhysicalDrive2 (CFTT-119)	U	Before	50A1A42EE6C058B621DB374FA52FF68EFD14390
		After	1DA330F4A9A535E0FB27E049745F39E7477C8371
\\.\PhysicalDrive3 (CFTT-25)	P	Before	F96F2865DC588885DC005E9E6B38E58358CEB1EF
		After	F96F2865DC588885DC005E9E6B38E58358CEB1EF
\\.\PhysicalDrive4 (CFTT-27)	P	Before	21B811181FFFF4D8237461C1848343FF3F477CE7
		After	21B811181FFFF4D8237461C1848343FF3F477CE7

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 test's the tools 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 shows the Windows Computer Management console, specifically the Disk Management section. The left pane shows the tree view with 'Disk Management' selected. The right pane displays a table of disk configurations and a graphical representation of the disks.

Volume	Layout	Type	File System
(C:)	Partition	Basic	NTFS
CFTT-25 (F:)	Partition	Basic	NTFS
CFTT-27 (G:)	Partition	Basic	FAT32
CFTT-70 (D:)	Partition	Basic	NTFS
CFTT-119 (E:)	Partition	Basic	NTFS
LEXAR MEDIA...	Partition	Basic	FAT

Disk	Capacity	Health	Partition	File System	Capacity	Health	Unallocated
Disk 0	9.50 GB	Online	(C:)	4.00 GB NTFS	5.50 GB	Unallocated	
Disk 1	38.34 GB	Online	CFTT-70 (D:)	1.37 GB NTFS	36.97 GB	Unallocated	
Disk 2	111.79 GB	Online	CFTT-119 (E:)	111.79 GB NTFS			
Disk 3	68.36 GB	Online	CFTT-25 (F:)	68.36 GB NTFS			
Disk 4	17.12 GB	Online	CFTT-27 (G:)	8.47 GB FAT32	8.65 GB	Unallocated	

Legend: ■ Unallocated ■ Primary Partition

9.15.2 Write blocker configuration

Event.log - Windows 2000 Write Blocker

File View Tools Help

Local Devices

- Standard floppy disk controller
 - Floppy disk drive
- Primary IDE Channel
 - WDC WD1200JD-00GBB0
- Primary IDE Channel
 - IC35L040AVER07-0
 - ST310210A
- Secondary IDE Channel
 - SONY DVD RW DRU-530A
- Adaptec AIC-7892 Ultra160/m PCI SCSI
 - QUANTUM ATLAS10K3_18_SCA SCSI
 - SEAGATE ST373405LC SCSI Disk De
- USB Mass Storage Device
 - LEXAR JUMPDRIVE SPORT USB Devi
- USB Mass Storage Device
 - USB2.0 HS-CF USB Device
- Network Drives

Physical Media | Network Media | Configuration

Double-click on the Physical Media to toggle the Write Blocked status.

Physical Media	Description	Volumes	Write Blocked
System Partition	Windows System Partition	C	No
FloppyDrive0	Floppy disk drive	A	Yes
CdRomDrive0	SONY DVD RW DRU-530A	H	Yes
HardDrive1	IC35L040AVER07-0	D	No
HardDrive2	WDC WD1200JD-00GBB0	E	Yes
HardDrive3	SEAGATE ST373405LC SCSI Disk D...	F	Yes
HardDrive4	QUANTUM ATLAS10K3_18_SCA SC...	G	Yes
HardDrive5	USB2.0 HS-CF USB Device	I	Yes
HardDrive6	LEXAR JUMPDRIVE SPORT USB D...	J	No

HardDrive1: Write blocking toggled OFF

Ready

9.15.3 Test output summary

```

NIST Software Write Blocker Test Suite V1.2
Thu Apr 06 10:29:16 2006

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 \\.\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

9.15.4 Hard disk hash results

Drive Identification		Computed	SHA1 Value
\\.\PhysicalDrive1 (CFTT-70)	U	Before	DD28B6EB3F83631A6B917A07EE73A7AD123EEEEAD
		After	0AE96E7A9BF49335BD2F64553D4BB917626CE63C
\\.\PhysicalDrive2 (CFTT-119)	P	Before	DBA4F06AFA484833AE3C2EE3F91C5E42623C9205
		After	DBA4F06AFA484833AE3C2EE3F91C5E42623C9205
\\.\PhysicalDrive3 (CFTT-25)	P	Before	F4D25FF778F15A3C43239400BA2A900CDD9ED64F
		After	F4D25FF778F15A3C43239400BA2A900CDD9ED64F
\\.\PhysicalDrive4 (CFTT-27)	P	Before	21B811181FFFF4D8237461C1848343FF3F477CE7
		After	21B811181FFFF4D8237461C1848343FF3F477CE7

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 test's the tools 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

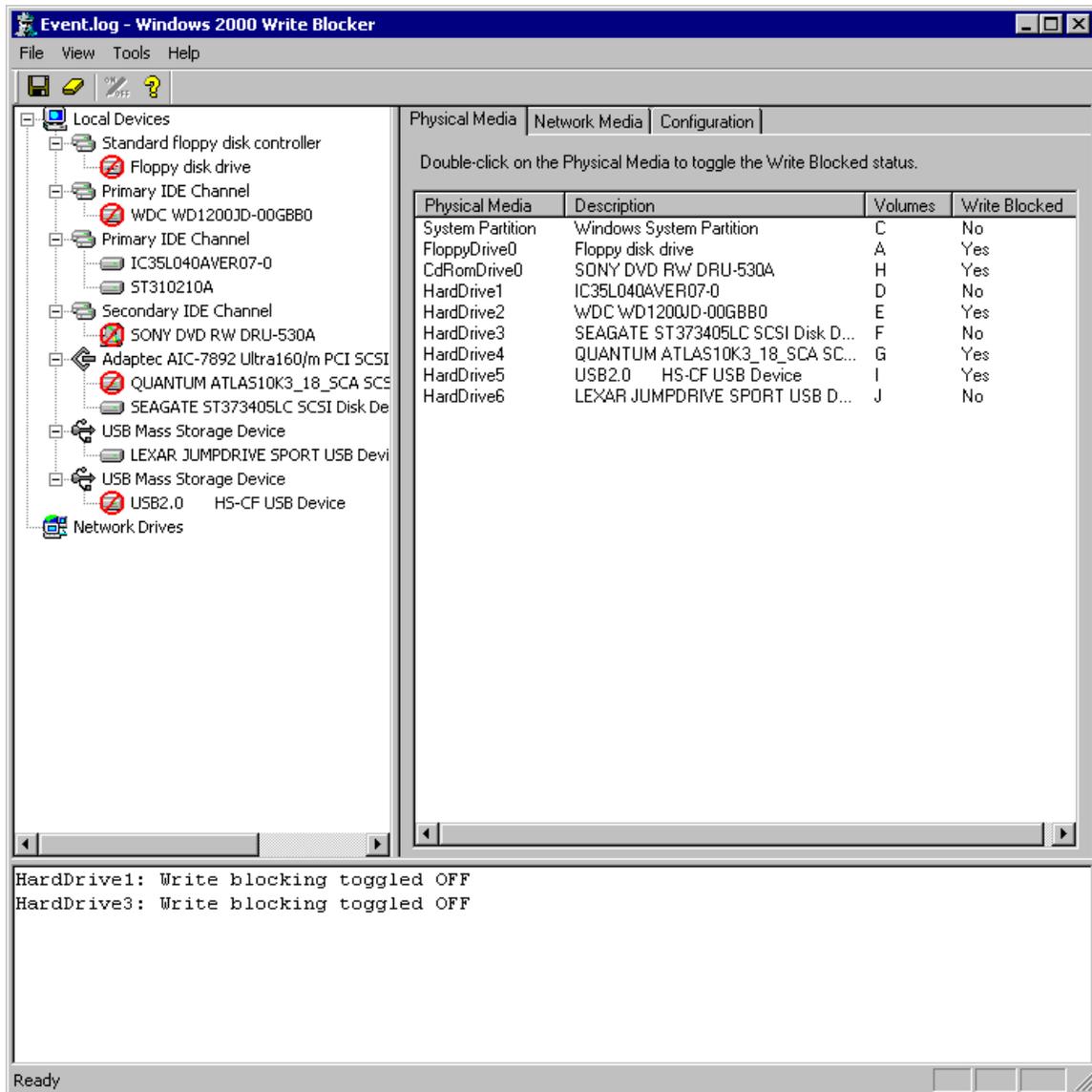
The screenshot shows the Windows Computer Management console, specifically the Disk Management section. The left pane shows the tree view with 'Disk Management' selected. The main area displays a table of volumes and a graphical representation of five disks.

Volume	Layout	Type	File System
(C:)	Partition	Basic	NTFS
CFTT-25 (F:)	Partition	Basic	NTFS
CFTT-27 (G:)	Partition	Basic	FAT32
CFTT-70 (D:)	Partition	Basic	NTFS
CFTT-119 (E:)	Partition	Basic	NTFS
LEXAR MEDIA...	Partition	Basic	FAT

Disk	Capacity	Health	Partition	File System	Capacity	Health	File System
Disk 0	9.50 GB	Online	(C:)	4.00 GB NTFS	5.50 GB	Unallocated	Unallocated
Disk 1	36.34 GB	Online	CFTT-70 (D:)	1.37 GB NTFS	36.97 GB	Unallocated	Unallocated
Disk 2	111.79 GB	Online	CFTT-119 (E:)	111.79 GB NTFS			Healthy (System)
Disk 3	68.36 GB	Online	CFTT-25 (F:)	68.36 GB NTFS			Healthy
Disk 4	17.12 GB	Online	CFTT-27 (G:)	8.47 GB FAT32	8.65 GB	Unallocated	Unallocated

Legend: ■ Unallocated ■ Primary Partition

9.16.2 Write blocker configuration



9.16.3 Test output summary

NIST Software Write Blocker Test Suite V1.2
Thu Apr 06 15:07:26 2006

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 \\.\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

9.16.4 Hard disk hash results

Drive Identification		Computed	SHA1 Value
\\.\PhysicalDrive1 (CFTT-70)	U	Before	0AE96E7A9BF49335BD2F64553D4BB917626CE63C
		After	ECB0F9D42242E83F9CFF624E0D5F408A9FA7E6DD
\\.\PhysicalDrive2 (CFTT-119)	P	Before	DBA4F06AFA484833AE3C2EE3F91C5E42623C9205
		After	DBA4F06AFA484833AE3C2EE3F91C5E42623C9205
\\.\PhysicalDrive3 (CFTT-25)	U	Before	F4D25FF778F15A3C43239400BA2A900CDD9ED64F
		After	9C5EA8DA3F847431EAE01816D403D223714AD1FA
\\.\PhysicalDrive4 (CFTT-27)	P	Before	21B811181FFFF4D8237461C1848343FF3F477CE7
		After	21B811181FFFF4D8237461C1848343FF3F477CE7

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 test's the tools 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

The screenshot shows the Windows Computer Management console, specifically the Disk Management section. The left pane shows the tree view with 'Disk Management' selected. The main area displays a table of volumes and a graphical representation of five disks.

Volume	Layout	Type	File System
(C:)	Partition	Basic	NTFS
CFTT-25 (F:)	Partition	Basic	NTFS
CFTT-27 (G:)	Partition	Basic	FAT32
CFTT-70 (D:)	Partition	Basic	NTFS
CFTT-119 (E:)	Partition	Basic	NTFS
LEXAR MEDIA...	Partition	Basic	FAT

Disk	Capacity	Health	Partition	File System	Size	Unallocated
Disk 0	9.50 GB	Online	(C:)	4.00 GB NTFS	5.50 GB	Unallocated
Disk 1	36.34 GB	Online	CFTT-70 (D:)	1.37 GB NTFS	36.97 GB	Unallocated
Disk 2	111.79 GB	Online	CFTT-119 (E:)	111.79 GB NTFS		
Disk 3	68.36 GB	Online	CFTT-25 (F:)	68.36 GB NTFS		
Disk 4	17.12 GB	Online	CFTT-27 (G:)	8.47 GB FAT32	8.65 GB	Unallocated

Legend: ■ Unallocated ■ Primary Partition

9.17.2 Write blocker configuration

Event.log - Windows 2000 Write Blocker

File View Tools Help

Local Devices

- Standard floppy disk controller
 - Floppy disk drive
- Primary IDE Channel
 - WDC WD1200JD-00GBB0
- Primary IDE Channel
 - IC35L040AVER07-0
 - ST310210A
- Secondary IDE Channel
 - SONY DVD RW DRU-530A
- Adaptec AIC-7892 Ultra160/m PCI SCSI
 - QUANTUM ATLAS10K3_18_SCA SCSI
 - SEAGATE ST373405LC SCSI Disk De
- USB Mass Storage Device
 - LEXAR JUMPDRIVE SPORT USB Devi
- USB Mass Storage Device
 - USB2.0 HS-CF USB Device
- Network Drives

Physical Media | Network Media | Configuration

Double-click on the Physical Media to toggle the Write Blocked status.

Physical Media	Description	Volumes	Write Blocked
System Partition	Windows System Partition	C	No
FloppyDrive0	Floppy disk drive	A	Yes
CdRomDrive0	SONY DVD RW DRU-530A	H	Yes
HardDrive1	IC35L040AVER07-0	D	Yes
HardDrive2	WDC WD1200JD-00GBB0	E	No
HardDrive3	SEAGATE ST373405LC SCSI Disk D...	F	Yes
HardDrive4	QUANTUM ATLAS10K3_18_SCA SC...	G	No
HardDrive5	USB2.0 HS-CF USB Device	I	Yes
HardDrive6	LEXAR JUMPDRIVE SPORT USB D...	J	No

HardDrive2: Write blocking toggled OFF
HardDrive4: Write blocking toggled OFF

Ready

9.17.3 Test output summary

```

NIST Software Write Blocker Test Suite V1.2
Thu Apr 06 16:25:12 2006

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 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 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	ECB0F9D42242E83F9CFF624E0D5F408A9FA7E6DD
		After	ECB0F9D42242E83F9CFF624E0D5F408A9FA7E6DD
\\.\PhysicalDrive2 (CFTT-119)	U	Before	DBA4F06AFA484833AE3C2EE3F91C5E42623C9205
		After	131A45DDF90F036AAE15A9D18A140833AF932A07
\\.\PhysicalDrive3 (CFTT-25)	P	Before	9C5EA8DA3F847431EAE01816D403D223714AD1FA
		After	9C5EA8DA3F847431EAE01816D403D223714AD1FA
\\.\PhysicalDrive4 (CFTT-27)	U	Before	21B811181FFFF4D8237461C1848343FF3F477CE7
		After	21B811181FFFF4D8237461C1848343FF3F477CE7

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 test's the tools 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

The screenshot shows the Windows Computer Management console, specifically the Disk Management section. The left pane shows the tree view with 'Disk Management' selected. The main pane displays a table of disk configurations and a graphical representation of the disks below.

Volume	Layout	Type	File System
(C:)	Partition	Basic	NTFS
CFTT-25 (F:)	Partition	Basic	NTFS
CFTT-27 (G:)	Partition	Basic	FAT32
CFTT-70 (D:)	Partition	Basic	NTFS
CFTT-119 (E:)	Partition	Basic	NTFS
LEXAR MEDIA...	Partition	Basic	FAT

Disk	Capacity	Health	Partition	File System	Size	Unallocated
Disk 0	9.50 GB	Online	(C:)	4.00 GB NTFS	5.50 GB	Unallocated
Disk 1	36.34 GB	Online	CFTT-70 (D:)	1.37 GB NTFS	36.97 GB	Unallocated
Disk 2	111.79 GB	Online	CFTT-119 (E:)	111.79 GB NTFS		
Disk 3	68.36 GB	Online	CFTT-25 (F:)	68.36 GB NTFS		
Disk 4	17.12 GB	Online	CFTT-27 (G:)	8.47 GB FAT32	8.65 GB	Unallocated

Legend: ■ Unallocated ■ Primary Partition

9.18.2 Write blocker configuration

Event.log - Windows 2000 Write Blocker

File View Tools Help

Local Devices

- Standard floppy disk controller
 - Floppy disk drive
- Primary IDE Channel
 - WDC WD1200JD-00GBB0
- Primary IDE Channel
 - IC35L040AVER07-0
 - ST310210A
- Secondary IDE Channel
 - SONY DVD RW DRU-530A
- Adaptec AIC-7892 Ultra160/m PCI SCSI Controller
 - QUANTUM ATLAS10K3_18_SCA SCSI Disk Drive
 - SEAGATE ST373405LC SCSI Disk Drive
- USB Mass Storage Device
 - LEXAR JUMPDRIVE SPORT USB Device
- USB Mass Storage Device
 - USB2.0 HS-CF USB Device
- Network Drives

Physical Media | Network Media | Configuration

Double-click on the Physical Media to toggle the Write Blocked status.

Physical Media	Description	Volumes	Write Blocked
System Partition	Windows System Partition	C	No
FloppyDrive0	Floppy disk drive	A	Yes
CdRomDrive0	SONY DVD RW DRU-530A	H	Yes
HardDrive1	IC35L040AVER07-0	D	Yes
HardDrive2	WDC WD1200JD-00GBB0	E	Yes
HardDrive3	SEAGATE ST373405LC SCSI Disk D...	F	No
HardDrive4	QUANTUM ATLAS10K3_18_SCA SC...	G	No
HardDrive5	USB2.0 HS-CF USB Device	I	Yes
HardDrive6	LEXAR JUMPDRIVE SPORT USB D...	J	No

HardDrive3: Write blocking toggled OFF
HardDrive4: Write blocking toggled OFF

Ready

9.18.3 Test output summary

NIST Software Write Blocker Test Suite V1.2
Tue Apr 18 10:58:26 2006

Test case: SWB-18
Command set: RWOVU
Number of drives: 4
Protection pattern: PPUU
Test administered by: DPS
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 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 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	ECB0F9D42242E83F9CFF624E0D5F408A9FA7E6DD
		After	7CA790CE7D88AE88DB474EA036D2FBA0CBE46609
\\.\PhysicalDrive2 (CFTT-119)	P	Before	131A45DDF90F036AAE15A9D18A140833AF932A07
		After	336468E49C86BCF47D6B6EC157C83F6546F680E7
\\.\PhysicalDrive3 (CFTT-25)	U	Before	9C5EA8DA3F847431EAE01816D403D223714AD1FA
		After	1855E34326E0786F34737DDC72197977980BBB77
\\.\PhysicalDrive4 (CFTT-27)	U	Before	21B811181FFFF4D8237461C1848343FF3F477CE7
		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 test's the tools 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

The screenshot shows the Windows Computer Management console, specifically the Disk Management section. The left pane shows the tree view with 'Disk Management' selected. The main area displays a table of volumes and a graphical representation of five disks.

Volume	Layout	Type	File System
(C:)	Partition	Basic	NTFS
CFTT-25 (F:)	Partition	Basic	NTFS
CFTT-27 (G:)	Partition	Basic	FAT32
CFTT-70 (D:)	Partition	Basic	NTFS
CFTT-119 (E:)	Partition	Basic	NTFS
LEXAR MEDIA...	Partition	Basic	FAT

Disk	Capacity	Health	Partition	File System	Capacity	Health	File System
Disk 0	9.50 GB	Online	(C:)	4.00 GB NTFS	5.50 GB	Unallocated	Unallocated
Disk 1	36.34 GB	Online	CFTT-70 (D:)	1.37 GB NTFS	36.97 GB	Unallocated	Unallocated
Disk 2	111.79 GB	Online	CFTT-119 (E:)	111.79 GB NTFS			Healthy (System)
Disk 3	68.36 GB	Online	CFTT-25 (F:)	68.36 GB NTFS			Healthy
Disk 4	17.12 GB	Online	CFTT-27 (G:)	8.47 GB FAT32	8.65 GB	Unallocated	Unallocated

Legend: ■ Unallocated ■ Primary Partition

9.19.2 Write blocker configuration

Event.log - Windows 2000 Write Blocker

File View Tools Help

Local Devices

- Standard floppy disk controller
 - Floppy disk drive
- Primary IDE Channel
 - WDC WD1200JD-00GBB0
- Primary IDE Channel
 - IC35L040AVER07-0
 - ST310210A
- Secondary IDE Channel
 - SONY DVD RW DRU-530A
- Adaptec AIC-7892 Ultra160/m PCI SCSI
 - QUANTUM ATLAS10K3_18_SCA SCSI
 - SEAGATE ST373405LC SCSI Disk De
- USB Mass Storage Device
 - LEXAR JUMPDRIVE SPORT USB Devi
- USB Mass Storage Device
 - USB2.0 HS-CF USB Device
- Network Drives

Physical Media | Network Media | Configuration

Double-click on the Physical Media to toggle the Write Blocked status.

Physical Media	Description	Volumes	Write Blocked
System Partition	Windows System Partition	C	No
FloppyDrive0	Floppy disk drive	A	Yes
CdRomDrive0	SONY DVD RW DRU-530A	H	Yes
HardDrive1	IC35L040AVER07-0	D	Yes
HardDrive2	WDC WD1200JD-00GBB0	E	No
HardDrive3	SEAGATE ST373405LC SCSI Disk D...	F	No
HardDrive4	QUANTUM ATLAS10K3_18_SCA SC...	G	No
HardDrive5	USB2.0 HS-CF USB Device	I	Yes
HardDrive6	LEXAR JUMPDRIVE SPORT USB D...	J	No

HardDrive2: Write blocking toggled OFF
HardDrive3: Write blocking toggled OFF
HardDrive4: Write blocking toggled OFF

Ready

9.19.3 Test output summary

```

NIST Software Write Blocker Test Suite V1.2
Tue Apr 18 14:51:16 2006

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 Specific 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 test's the tools 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

The screenshot shows the Windows Computer Management console, specifically the Disk Management section. The left pane shows the tree view with 'Disk Management' selected. The main pane displays a table of disk configurations and a graphical representation of the disks below.

Volume	Layout	Type	File System
(C:)	Partition	Basic	NTFS
CFTT-25 (F:)	Partition	Basic	NTFS
CFTT-27 (G:)	Partition	Basic	FAT32
CFTT-70 (D:)	Partition	Basic	NTFS
CFTT-119 (E:)	Partition	Basic	NTFS
LEXAR MEDIA...	Partition	Basic	FAT

Disk	Capacity	Health	Volume	Capacity	File System	Health	Unallocated
Disk 0	9.50 GB	Online	(C:)	4.00 GB	NTFS	Healthy (Boot)	5.50 GB
Disk 1	36.34 GB	Online	CFTT-70 (D:)	1.37 GB	NTFS	Healthy (Active)	36.97 GB
Disk 2	111.79 GB	Online	CFTT-119 (E:)	111.79 GB	NTFS	Healthy (System)	
Disk 3	68.36 GB	Online	CFTT-25 (F:)	68.36 GB	NTFS	Healthy	
Disk 4	17.12 GB	Online	CFTT-27 (G:)	8.47 GB	FAT32	Healthy	8.65 GB

Legend: ■ Unallocated ■ Primary Partition

9.20.2 Write blocker configuration

Event.log - Windows 2000 Write Blocker

File View Tools Help

Local Devices

- Standard floppy disk controller
 - Floppy disk drive
- Primary IDE Channel
 - WDC WD1200JD-00GBB0
- Primary IDE Channel
 - IC35L040AVER07-0
 - ST310210A
- Secondary IDE Channel
 - SONY DVD RW DRU-530A
- Adaptec AIC-7892 Ultra160/m PCI SCSI
 - QUANTUM ATLAS10K3_18_SCA SC...
 - SEAGATE ST373405LC SCSI Disk De
- USB Mass Storage Device
 - LEXAR JUMPDRIVE SPORT USB Devi
- USB Mass Storage Device
 - USB2.0 HS-CF USB Device
- Network Drives

Physical Media | Network Media | Configuration

Double-click on the Physical Media to toggle the Write Blocked status.

Physical Media	Description	Volumes	Write Blocked
System Partition	Windows System Partition	C	No
FloppyDrive0	Floppy disk drive	A	Yes
CdRomDrive0	SONY DVD RW DRU-530A	H	Yes
HardDrive1	IC35L040AVER07-0	D	No
HardDrive2	WDC WD1200JD-00GBB0	E	Yes
HardDrive3	SEAGATE ST373405LC SCSI Disk D...	F	Yes
HardDrive4	QUANTUM ATLAS10K3_18_SCA SC...	G	No
HardDrive5	USB2.0 HS-CF USB Device	I	Yes
HardDrive6	LEXAR JUMPDRIVE SPORT USB D...	J	No

HardDrive1: Write blocking toggled OFF
HardDrive4: Write blocking toggled OFF

Ready

9.20.3 Test output summary

```

NIST Software Write Blocker Test Suite V1.2
Tue Apr 18 16:24:06 2006

Test case:          SWB-20
Command set:        RWOVU
Number of drives:   4
Protection pattern: UPPU
Test administered by: DPA
Details logged to file: SWB-20.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 \\.\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	ECB0F9D42242E83F9CFF624E0D5F408A9FA7E6DD
		After	EB74D63A59F2CB623A9AC581E8ACCC904B1F7704
\\.\PhysicalDrive2 (CFTT-119)	P	Before	BCAD400D8ECBFDB2B99DBB7B2D319DC218EDEB31
		After	BCAD400D8ECBFDB2B99DBB7B2D319DC218EDEB31
\\.\PhysicalDrive3 (CFTT-25)	P	Before	F35DD2C28F83DDDA9B4A828B425442F520FDDDDDE
		After	F35DD2C28F83DDDA9B4A828B425442F520FDDDDDE
\\.\PhysicalDrive4 (CFTT-27)	U	Before	21B811181FFFF4D8237461C1848343FF3F477CE7
		After	21B811181FFFF4D8237461C1848343FF3F477CE7

9.20.5 Test results analysis

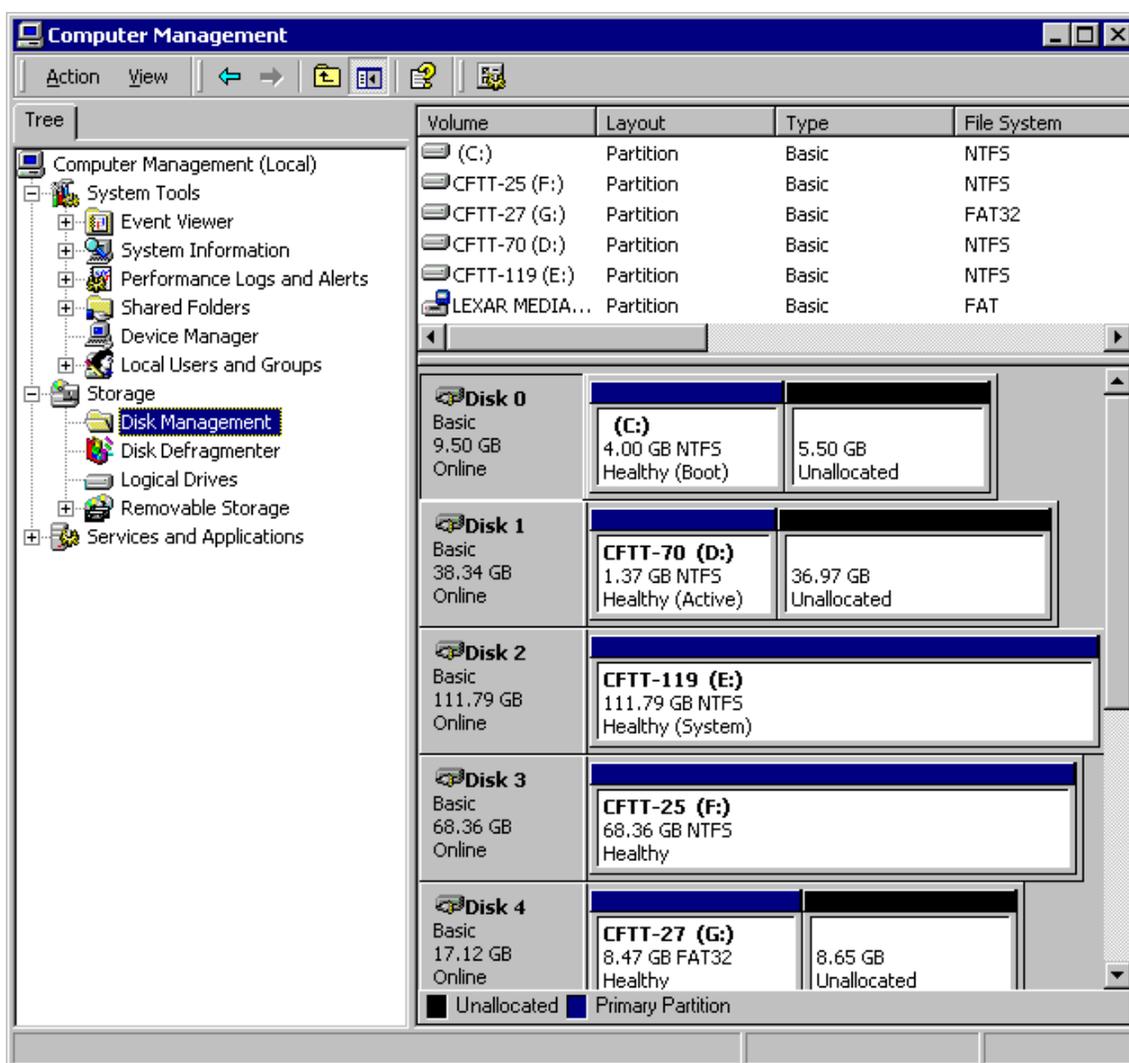
The tool failed to produce the expected result. The pattern of protection did not affect the ability of the tool to protect designated drives but the protection applied failed to block all commands in the protected categories. The protection applied for protected drives was identical to tests SWB-03,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

9.21 Test case SWB-21

This case test's the tools 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



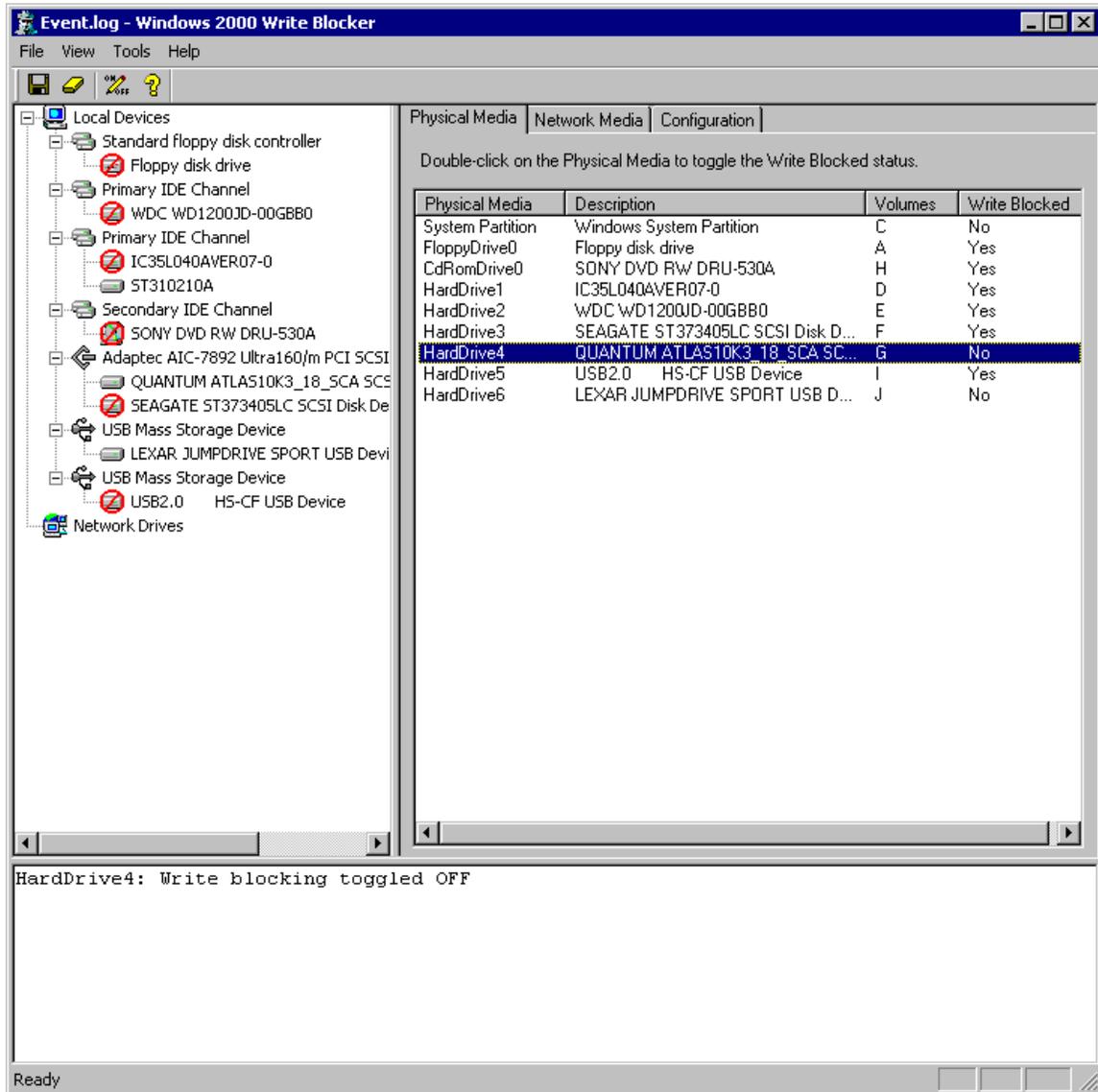
The screenshot shows the Windows Computer Management console. The left pane displays the 'Storage' tree with 'Disk Management' selected. The right pane shows a table of disk configurations and a detailed view of each disk.

Volume	Layout	Type	File System
(C:)	Partition	Basic	NTFS
CFTT-25 (F:)	Partition	Basic	NTFS
CFTT-27 (G:)	Partition	Basic	FAT32
CFTT-70 (D:)	Partition	Basic	NTFS
CFTT-119 (E:)	Partition	Basic	NTFS
LEXAR MEDIA...	Partition	Basic	FAT

Disk	Volume	Layout	Type	File System	Size	Health	State
Disk 0	(C:)	4.00 GB NTFS	Basic	NTFS	5.50 GB	Healthy (Boot)	Unallocated
Disk 1	CFTT-70 (D:)	1.37 GB NTFS	Basic	NTFS	36.97 GB	Healthy (Active)	Unallocated
Disk 2	CFTT-119 (E:)	111.79 GB NTFS	Basic	NTFS		Healthy (System)	
Disk 3	CFTT-25 (F:)	68.36 GB NTFS	Basic	NTFS		Healthy	
Disk 4	CFTT-27 (G:)	8.47 GB FAT32	Basic	FAT32	8.65 GB	Healthy	Unallocated

Legend: ■ Unallocated ■ Primary Partition

9.21.2 Write blocker configuration



9.21.3 Test output summary

```

NIST Software Write Blocker Test Suite V1.2
Wed Apr 19 10:56:26 2006

Test case:          SWB-21
Command set:       RWOUV
Number of drives:  4
Protection pattern: PPPU
Test administered by: DPA
Details logged to file: SWB-21.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 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	EB74D63A59F2CB623A9AC581E8ACCC904B1F7704
		After	EB74D63A59F2CB623A9AC581E8ACCC904B1F7704
\\.\PhysicalDrive2 (CFTT-119)	P	Before	BCAD400D8ECBFDB2B99DBB7B2D319DC218EDEB31
		After	BCAD400D8ECBFDB2B99DBB7B2D319DC218EDEB31
\\.\PhysicalDrive3 (CFTT-25)	P	Before	F35DD2C28F83DDDA9B4A828B425442F520FDDDE
		After	F35DD2C28F83DDDA9B4A828B425442F520FDDDE
\\.\PhysicalDrive4 (CFTT-27)	U	Before	21B811181FFFF4D8237461C1848343FF3F477CE7
		After	21B811181FFFF4D8237461C1848343FF3F477CE7

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 test's the tools 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

The screenshot displays the Windows Computer Management console, specifically the Disk Management section. The left-hand tree view shows the navigation path: Computer Management (Local) > Storage > Disk Management. The main area is divided into two panes. The top pane is a table listing disk volumes, and the bottom pane is a graphical representation of the disks.

Volume	Layout	Type	File System
(C:)	Partition	Basic	NTFS
CFTT-25 (F:)	Partition	Basic	NTFS
CFTT-27 (G:)	Partition	Basic	FAT32
CFTT-70 (D:)	Partition	Basic	NTFS
CFTT-119 (E:)	Partition	Basic	NTFS
LEXAR MEDIA...	Partition	Basic	FAT

Disk	Capacity	Volume	File System	Health	Unallocated
Disk 0	9.50 GB	(C:)	4.00 GB NTFS	Healthy (Boot)	5.50 GB Unallocated
Disk 1	38.34 GB	CFTT-70 (D:)	1.37 GB NTFS	Healthy (Active)	36.97 GB Unallocated
Disk 2	111.79 GB	CFTT-119 (E:)	111.79 GB NTFS	Healthy (System)	0 GB Unallocated
Disk 3	68.36 GB	CFTT-25 (F:)	68.36 GB NTFS	Healthy	0 GB Unallocated
Disk 4	17.12 GB	CFTT-27 (G:)	8.47 GB FAT32	Healthy	8.65 GB Unallocated

Legend: ■ Unallocated ■ Primary Partition

9.22.2 Write blocker configuration

Event.log - Windows 2000 Write Blocker

File View Tools Help

Physical Media Network Media Configuration

Double-click on the Physical Media to toggle the Write Blocked status.

Physical Media	Description	Volumes	Write Blocked
System Partition	Windows System Partition	C	No
FloppyDrive0	Floppy disk drive	A	Yes
CdRomDrive0	SONY DVD RW DRU-530A	H	Yes
HardDrive1	IC35L040AVER07-0	D	No
HardDrive2	WDC WD1200JD-00GBB0	E	No
HardDrive3	SEAGATE ST373405LC SCSI Disk D...	F	No
HardDrive4	QUANTUM ATLAS10K3_18_SCA SC...	G	Yes
HardDrive5	USB2.0 HS-CF USB Device	I	Yes
HardDrive6	LEXAR JUMPDRIVE SPORT USB D...	J	No

HardDrive1: Write blocking toggled OFF
HardDrive2: Write blocking toggled OFF
HardDrive3: Write blocking toggled OFF

Ready

9.22.3 Test output summary

```

NIST Software Write Blocker Test Suite V1.2
Thu Apr 20 11:19:17 2006

Test case:          SWB-22
Command set:        RWOVU
Number of drives:   4
Protection pattern: UUUP
Test administered by: DPA
Details logged to file: SWB-22.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 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

9.22.4 Hard disk hash results

Drive Identification		Computed	SHA1 Value
\\.\PhysicalDrive1 (CFTT-70)	U	Before	EB74D63A59F2CB623A9AC581E8ACCC904B1F7704
		After	6D96DA3851D7C4F4F124D29D0F02636E47DA3219
\\.\PhysicalDrive2 (CFTT-119)	U	Before	BCAD400D8ECBFD2B99DBB7B2D319DC218EDEB31
		After	DBA79F2A76A66B62B8D1DE2531926DD8E24A4212
\\.\PhysicalDrive3 (CFTT-25)	U	Before	F35DD2C28F83DDDA9B4A828B425442F520FDDDDDE
		After	ED8EBA001023BF8A13F30EB2C368B0C80EC0E711
\\.\PhysicalDrive4 (CFTT-27)	P	Before	21B811181FFFF4D8237461C1848343FF3F477CE7
		After	21B811181FFFF4D8237461C1848343FF3F477CE7

9.22.5 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.

9.23 Test case SWB-23

This case test's the tools 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

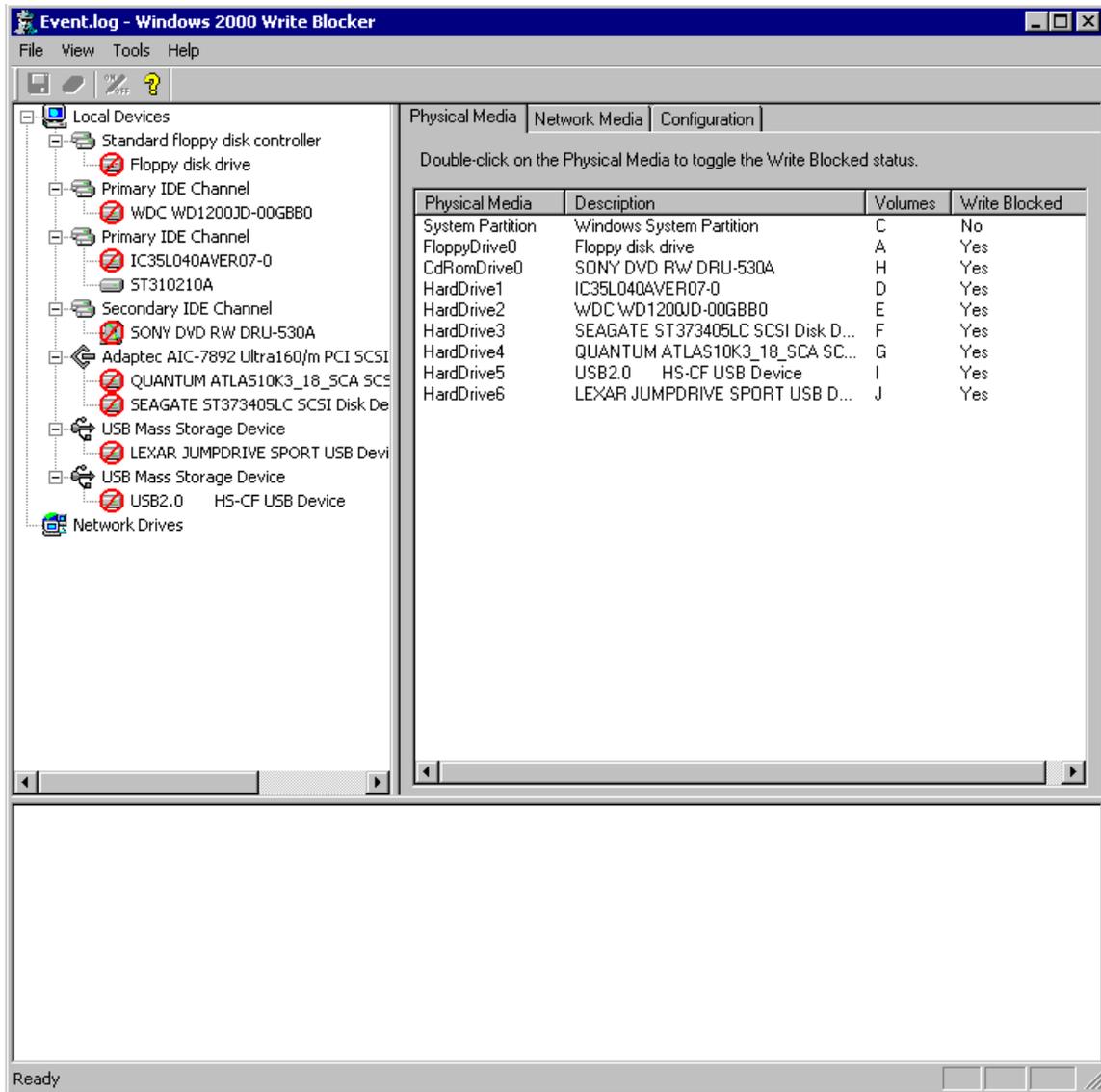
The screenshot shows the Windows Computer Management console, specifically the Disk Management section. The left pane shows the tree view with 'Disk Management' selected. The main pane displays a table of disk configurations and a graphical representation of the disks.

Volume	Layout	Type	File System
(C:)	Partition	Basic	NTFS
CFTT-25 (F:)	Partition	Basic	NTFS
CFTT-27 (G:)	Partition	Basic	FAT32
CFTT-70 (D:)	Partition	Basic	NTFS
CFTT-119 (E:)	Partition	Basic	NTFS
LEXAR MEDIA...	Partition	Basic	FAT

Disk	Capacity	Volume	File System	Health	State	Unallocated
Disk 0	9.50 GB	(C:)	4.00 GB NTFS	Healthy (Boot)	Online	5.50 GB Unallocated
Disk 1	38.34 GB	CFTT-70 (D:)	1.37 GB NTFS	Healthy (Active)	Online	36.97 GB Unallocated
Disk 2	111.79 GB	CFTT-119 (E:)	111.79 GB NTFS	Healthy (System)	Online	0 GB Unallocated
Disk 3	68.36 GB	CFTT-25 (F:)	68.36 GB NTFS	Healthy	Online	0 GB Unallocated
Disk 4	17.12 GB	CFTT-27 (G:)	8.47 GB FAT32	Healthy	Online	8.65 GB Unallocated

Legend: ■ Unallocated ■ Primary Partition

9.23.2 Write blocker configuration



9.23.3 Test output summary

```

NIST Software Write Blocker Test Suite V1.2
Thu Apr 20 15:12:19 2006

Test case:           SWB-23
Command set:        RWOVU
Number of drives:   4
Protection pattern: PPPP
Test administered by: DPA
Details logged to file: SWB-23.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 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	6D96DA3851D7C4F4F124D29D0F02636E47DA3219
		After	6D96DA3851D7C4F4F124D29D0F02636E47DA3219
\\.\PhysicalDrive2 (CFTT-119)	P	Before	DBA79F2A76A66B62B8D1DE2531926DD8E24A4212
		After	DBA79F2A76A66B62B8D1DE2531926DD8E24A4212
\\.\PhysicalDrive3 (CFTT-25)	P	Before	ED8EBA001023BF8A13F30EB2C368B0C80EC0E711
		After	ED8EBA001023BF8A13F30EB2C368B0C80EC0E711
\\.\PhysicalDrive4 (CFTT-27)	P	Before	21B811181FFFF4D8237461C1848343FF3F477CE7
		After	21B811181FFFF4D8237461C1848343FF3F477CE7

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 test's the tools 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

The screenshot shows the Windows Computer Management console, specifically the Disk Management section. The left pane shows the tree view with 'Disk Management' selected. The main pane displays a table of disk configurations and a graphical representation of the disks.

Volume	Layout	Type	File System
(C:)	Partition	Basic	NTFS
CFTT-25 (F:)	Partition	Basic	NTFS
CFTT-27 (G:)	Partition	Basic	FAT32
CFTT-70 (D:)	Partition	Basic	NTFS
CFTT-119 (E:)	Partition	Basic	NTFS
LEXAR MEDIA...	Partition	Basic	FAT

Disk	Capacity	Health	Volume	Capacity	File System	Health	Unallocated
Disk 0	9.50 GB	Online	(C:)	4.00 GB	NTFS	Healthy (Boot)	5.50 GB
Disk 1	36.34 GB	Online	CFTT-70 (D:)	1.37 GB	NTFS	Healthy (Active)	36.97 GB
Disk 2	111.79 GB	Online	CFTT-119 (E:)	111.79 GB	NTFS	Healthy (System)	
Disk 3	68.36 GB	Online	CFTT-25 (F:)	68.36 GB	NTFS	Healthy	
Disk 4	17.12 GB	Online	CFTT-27 (G:)	8.47 GB	FAT32	Healthy	8.65 GB

Legend: ■ Unallocated ■ Primary Partition

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
Undefi ned 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 SPeci fi c CDB's	80	0	80
Undefi 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 test's the tools compliance with mandatory assertions 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

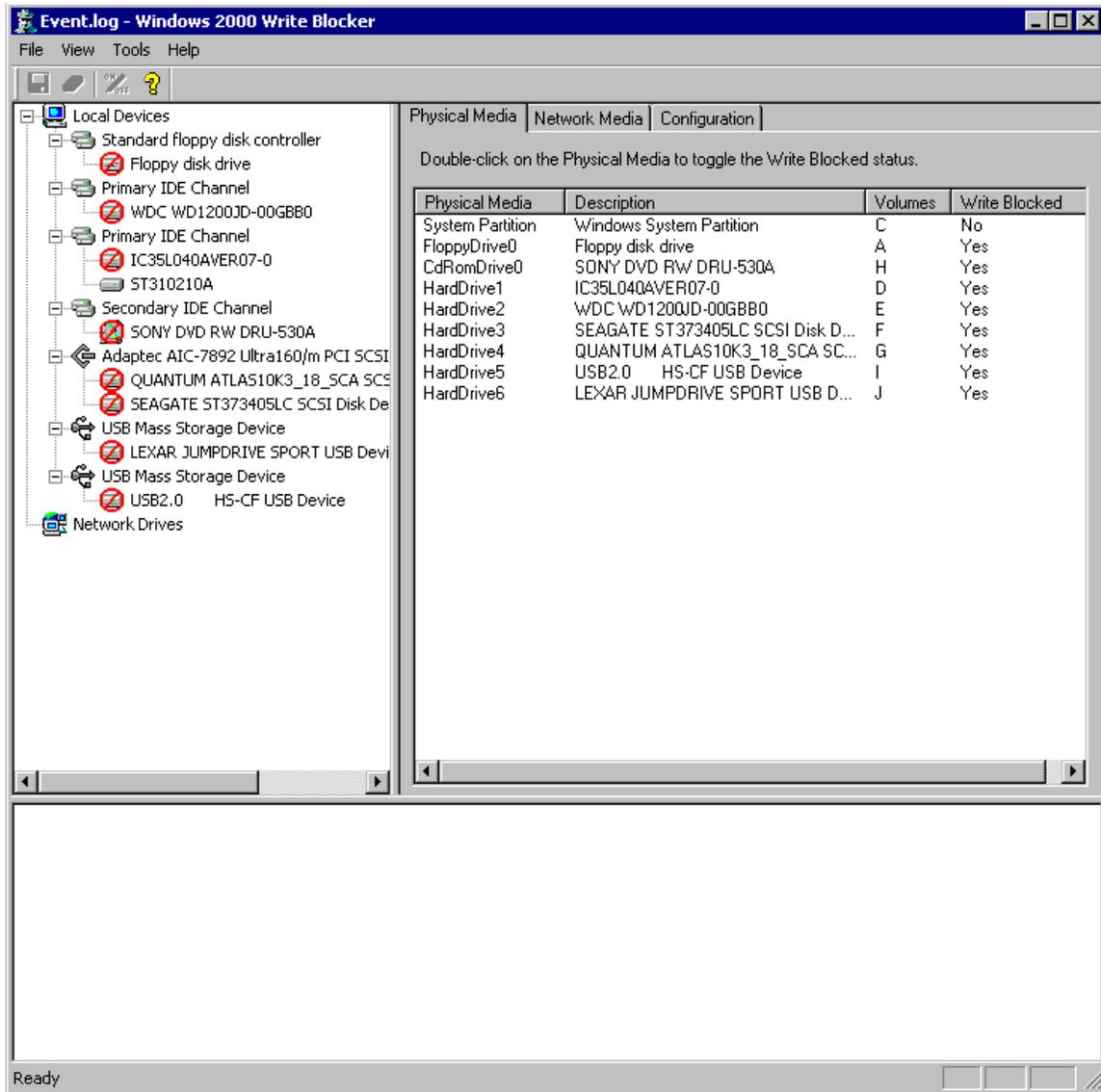
The screenshot shows the Windows Computer Management console, specifically the Disk Management section. The left pane shows the tree view with 'Disk Management' selected. The main area displays a table of disk configurations and a graphical representation of the disks.

Volume	Layout	Type	File System
(C:)	Partition	Basic	NTFS
CFTT-25 (F:)	Partition	Basic	NTFS
CFTT-27 (G:)	Partition	Basic	FAT32
CFTT-70 (D:)	Partition	Basic	NTFS
CFTT-119 (E:)	Partition	Basic	NTFS
LEXAR MEDIA...	Partition	Basic	FAT

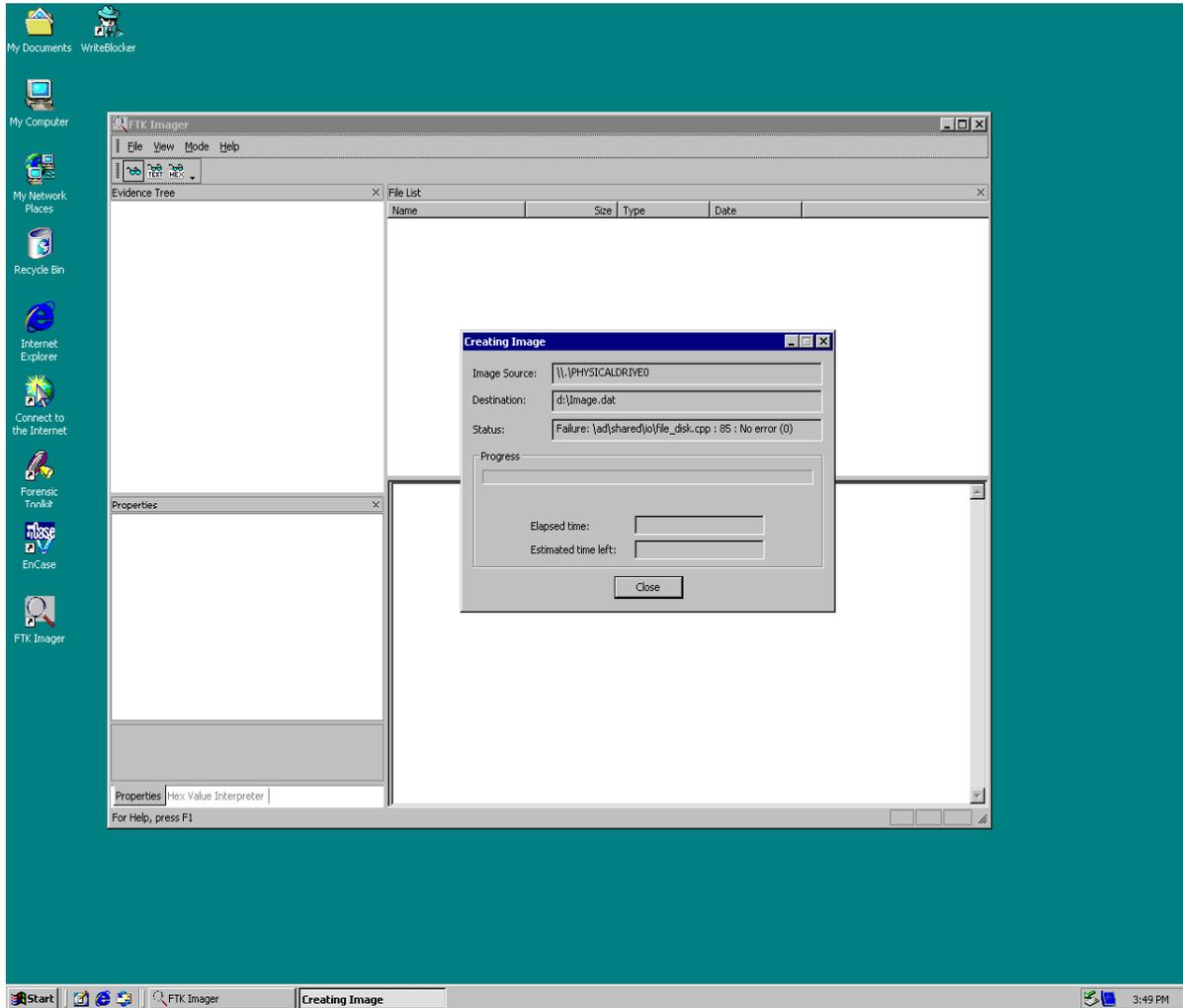
Disk	Capacity	Health	Partition	File System	Capacity	Health	File System
Disk 0	9.50 GB	Online	(C:)	4.00 GB NTFS	5.50 GB	Unallocated	Unallocated
Disk 1	36.34 GB	Online	CFTT-70 (D:)	1.37 GB NTFS	36.97 GB	Unallocated	Unallocated
Disk 2	111.79 GB	Online	CFTT-119 (E:)	111.79 GB NTFS			Healthy (System)
Disk 3	68.36 GB	Online	CFTT-25 (F:)	68.36 GB NTFS			Healthy
Disk 4	17.12 GB	Online	CFTT-27 (G:)	8.47 GB FAT32	8.65 GB	Unallocated	Unallocated

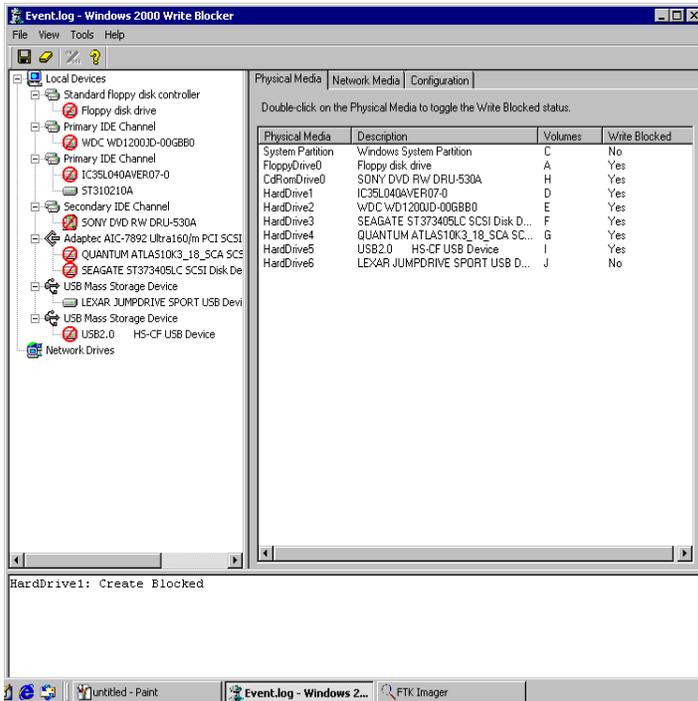
Legend: ■ Unallocated ■ Primary Partition

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)	Before	6D96DA3851D7C4F4F124D29D0F02636E47DA3219
	After	6D96DA3851D7C4F4F124D29D0F02636E47DA3219

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.

9.26 Test case SWB-26

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.

9.26.1 Hard disk configuration

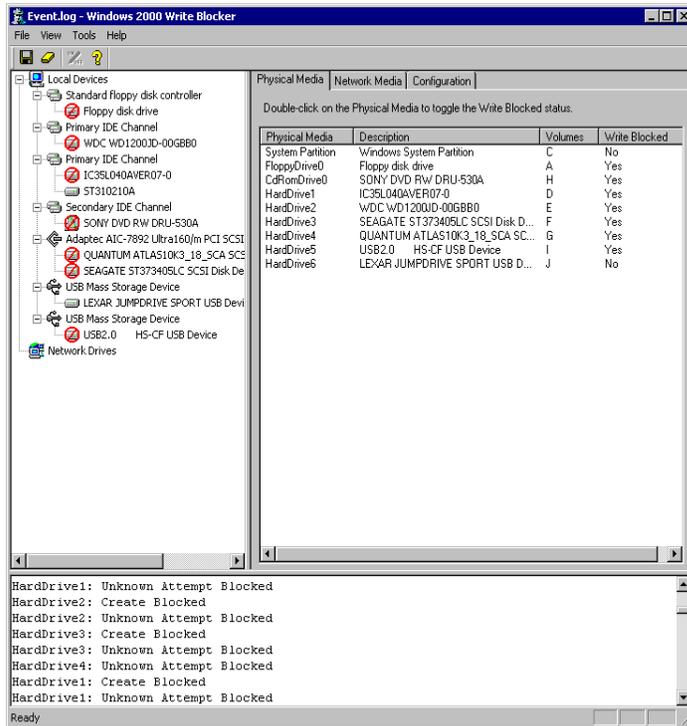
The screenshot shows the Windows Computer Management console, specifically the Disk Management section. The left pane shows the tree view with 'Disk Management' selected. The right pane displays a table of disk configurations and a graphical representation of the disks.

Volume	Layout	Type	File System
(C:)	Partition	Basic	NTFS
CFTT-25 (F:)	Partition	Basic	NTFS
CFTT-27 (G:)	Partition	Basic	FAT32
CFTT-70 (D:)	Partition	Basic	NTFS
CFTT-119 (E:)	Partition	Basic	NTFS
LEXAR MEDIA...	Partition	Basic	FAT

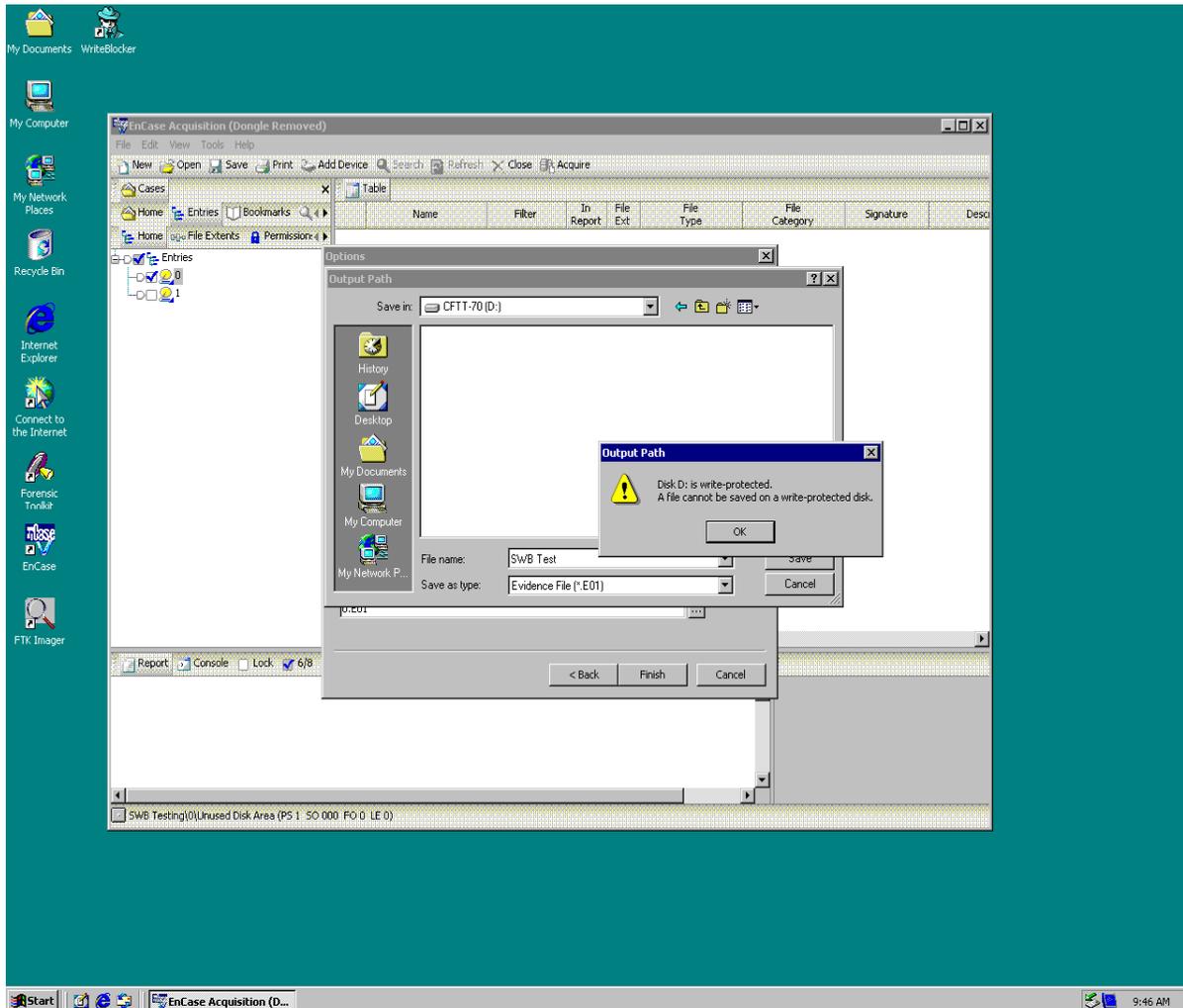
Disk	Capacity	Health	Partition	File System	Capacity	Unallocated
Disk 0	9.50 GB	Online	(C:)	4.00 GB NTFS	5.50 GB	Unallocated
Disk 1	38.34 GB	Online	CFTT-70 (D:)	1.37 GB NTFS	36.97 GB	Unallocated
Disk 2	111.79 GB	Online	CFTT-119 (E:)	111.79 GB NTFS		
Disk 3	68.36 GB	Online	CFTT-25 (F:)	68.36 GB NTFS		
Disk 4	17.12 GB	Online	CFTT-27 (G:)	8.47 GB FAT32	8.65 GB	Unallocated

Legend: ■ Unallocated ■ Primary Partition

9.26.2 Write blocker configuration



9.26.3 Test output summary



9.26.4 Hard disk hash results

Drive Identification		Computed	SHA1 Value
\\.\PhysicalDrive1	P	Before	6D96DA3851D7C4F4F124D29D0F02636E47DA3219
		After	6D96DA3851D7C4F4F124D29D0F02636E47DA3219

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 test's the tools 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

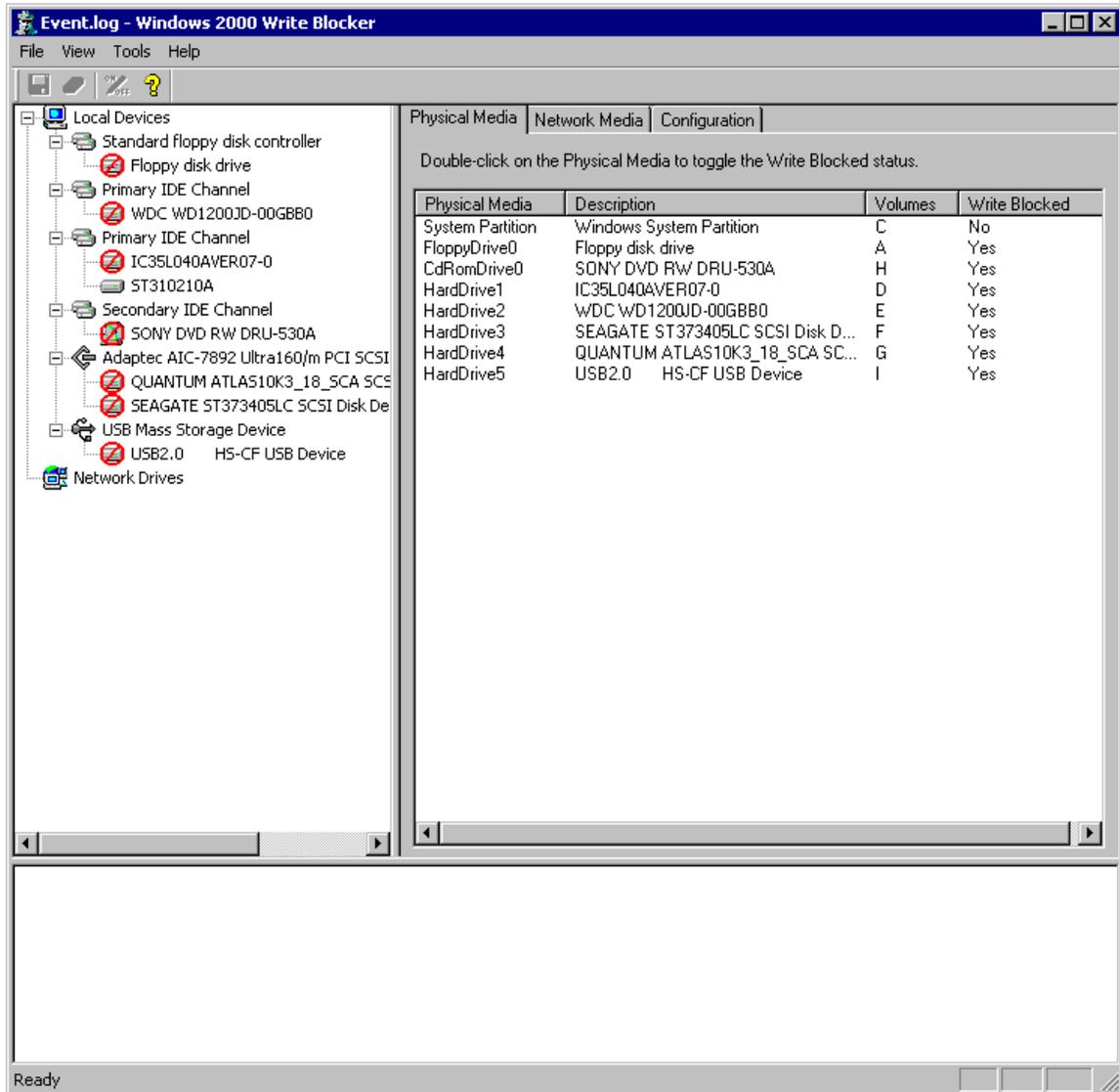
The screenshot displays the Windows Computer Management console, specifically the Disk Management section. The left-hand tree view shows the navigation pane with 'Storage' expanded to 'Disk Management'. The main area is divided into two panes. The top pane is a table listing the system's volumes. The bottom pane is a graphical representation of the physical disks and their partitions.

Volume	Layout	Type	File System	Status
(C:)	Partition	Basic	NTFS	Healthy
CFTT-25 (F:)	Partition	Basic	NTFS	Healthy
CFTT-27 (G:)	Partition	Basic	FAT32	Healthy
CFTT-70 (D:)	Partition	Basic	NTFS	Healthy
CFTT-119 (E:)	Partition	Basic	NTFS	Healthy
LEXAR MEDIA...	Partition	Basic	FAT	Healthy

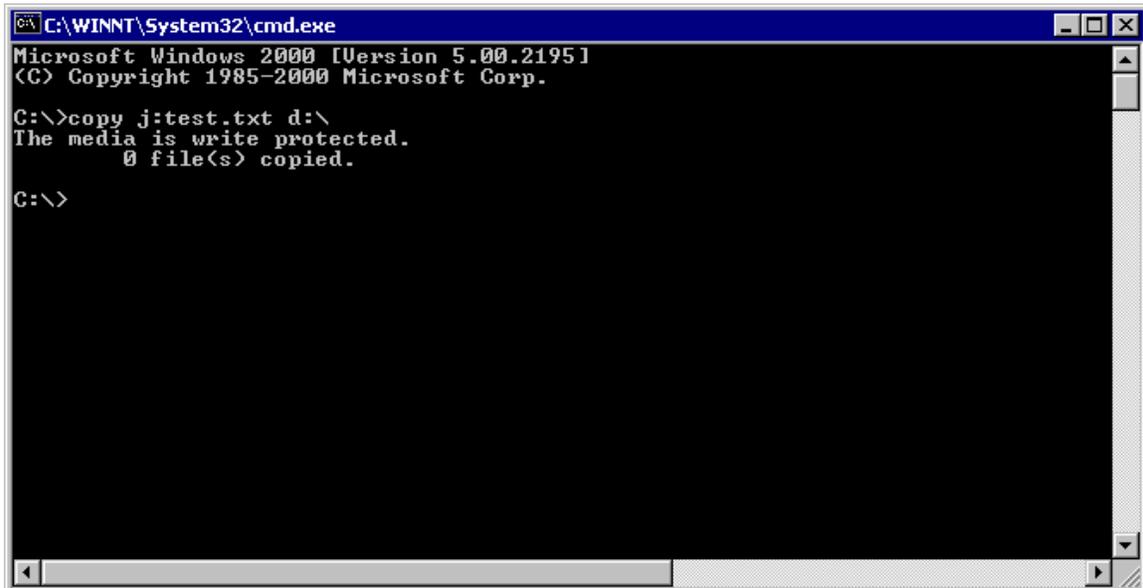
Disk	Capacity	Online	Partitions
Disk 0	9.50 GB	Online	(C:) 4.00 GB NTFS (Healthy Boot), 5.50 GB Unallocated
Disk 1	38.34 GB	Online	CFTT-70 (D:) 1.37 GB NTFS (Healthy Active), 36.97 GB Unallocated
Disk 2	111.79 GB	Online	CFTT-119 (E:) 111.79 GB NTFS (Healthy System)
Disk 3	68.36 GB	Online	CFTT-25 (F:) 68.36 GB NTFS (Healthy)
Disk 4	17.12 GB	Online	CFTT-27 (G:) 8.47 GB FAT32 (Healthy), 8.65 GB Unallocated

Legend: ■ Unallocated ■ Primary Partition

9.27.2 Write blocker configuration



9.27.3 Test output summary



```
C:\WINNT\System32\cmd.exe
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

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

C:\>
```

9.27.4 Hard disk hash results

Drive Identification		Computed	SHA1 Value
\\.\PhysicalDrive1	P	Before	6D96DA3851D7C4F4F124D29D0F02636E47DA3219
		After	6D96DA3851D7C4F4F124D29D0F02636E47DA3219

9.27.5 Test results analysis

The tool produced the expected result. The COPY operation failed with a write protection error and the hash value of the target disk was unchanged after the test.

9.28 Test case SWB-28

This case test's This case test's the tools 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

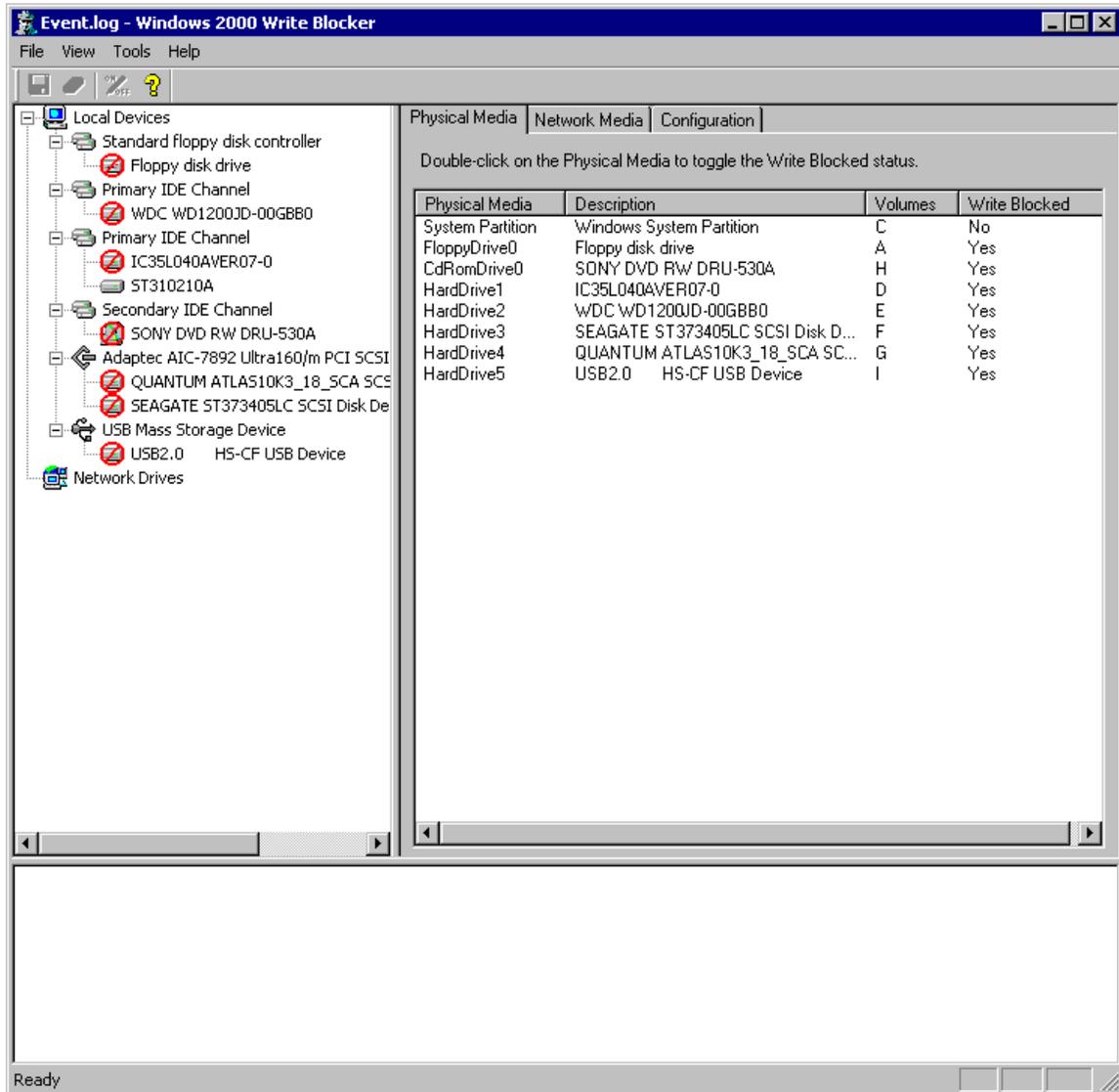
The screenshot displays the Windows Computer Management console, specifically the Disk Management section. The left pane shows the tree view with 'Storage' expanded to 'Disk Management'. The main pane shows a table of volumes and a detailed view of the disk configuration.

Volume	Layout	Type	File System	Status
(C:)	Partition	Basic	NTFS	Healthy
CFTT-25 (F:)	Partition	Basic	NTFS	Healthy
CFTT-27 (G:)	Partition	Basic	FAT32	Healthy
CFTT-70 (D:)	Partition	Basic	NTFS	Healthy
CFTT-119 (E:)	Partition	Basic	NTFS	Healthy
LEXAR MEDIA...	Partition	Basic	FAT	Healthy

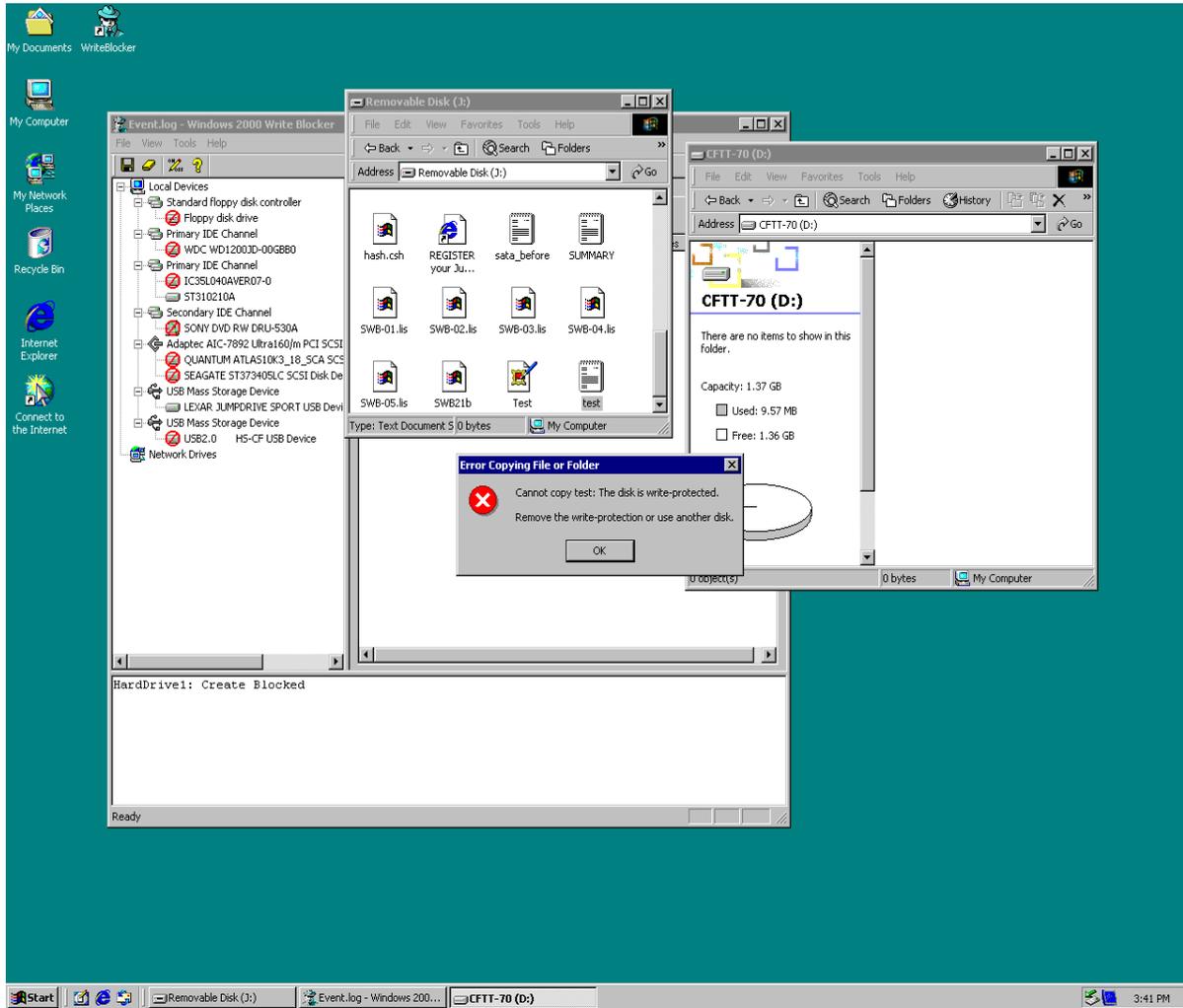
Disk	Capacity	Layout	Type	File System	Status	Unallocated
Disk 0	9.50 GB	(C:)	Basic	4.00 GB NTFS Healthy (Boot)	Online	5.50 GB Unallocated
Disk 1	38.34 GB	CFTT-70 (D:)	Basic	1.37 GB NTFS Healthy (Active)	Online	36.97 GB Unallocated
Disk 2	111.79 GB	CFTT-119 (E:)	Basic	111.79 GB NTFS Healthy (System)	Online	
Disk 3	68.36 GB	CFTT-25 (F:)	Basic	68.36 GB NTFS Healthy	Online	
Disk 4	17.12 GB	CFTT-27 (G:)	Basic	8.47 GB FAT32 Healthy	Online	8.65 GB Unallocated

Legend: ■ Unallocated ■ Primary Partition

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	6D96DA3851D7C4F4F124D29D0F02636E47DA3219
		After	6D96DA3851D7C4F4F124D29D0F02636E47DA3219

9.28.5 Test results analysis

The tool produced the expected result. The DROP operation failed with a write protection error message, 1 blocked commands (CREATE) were logged by the write blocker tool, and the hash value of the target disk was unchanged after the test.

9.29 Test case SWB-29

This case test's the tools 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

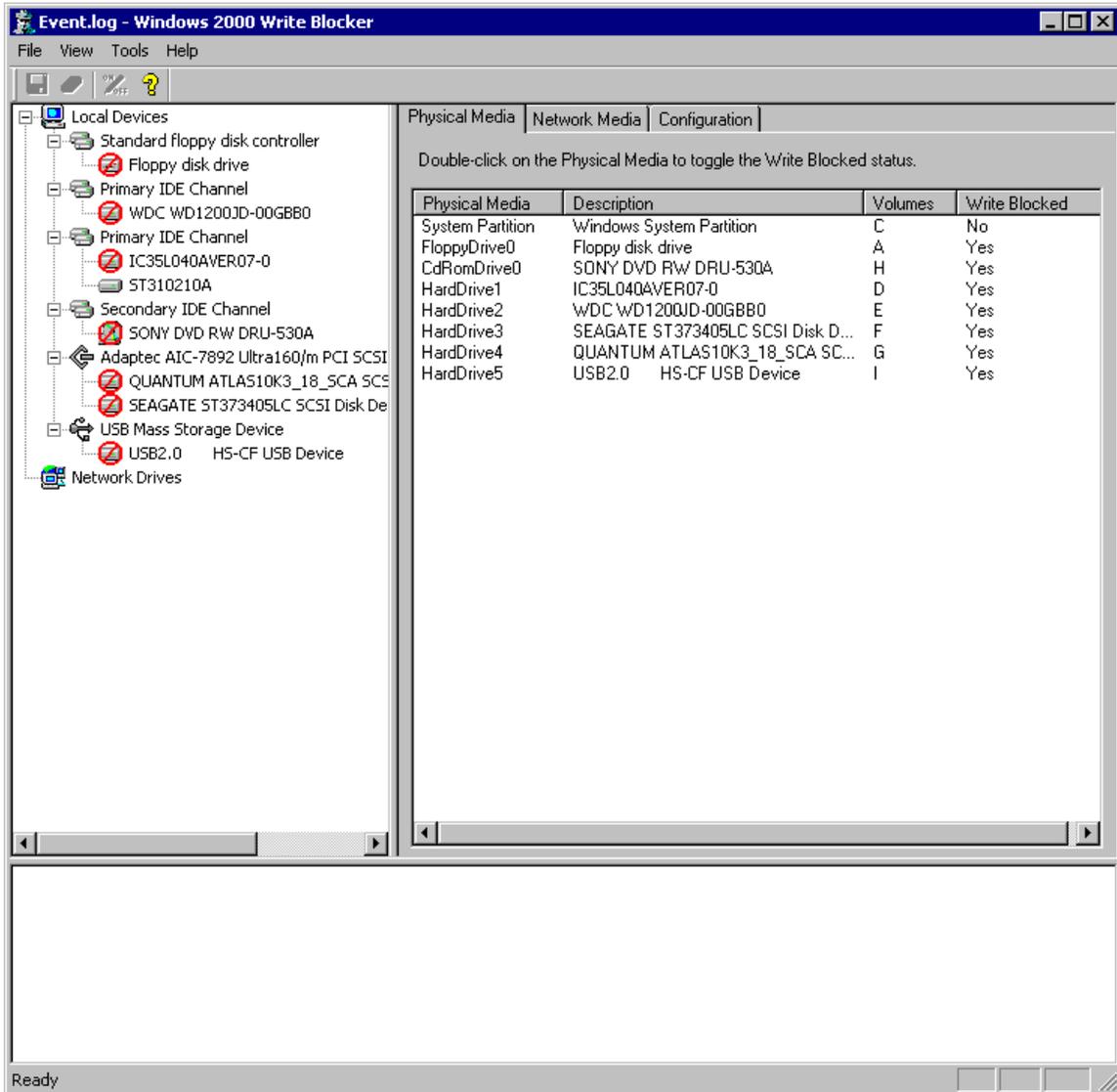
The screenshot displays the Windows Computer Management console, specifically the Disk Management section. The left-hand tree view shows the hierarchy: Computer Management (Local) > Storage > Disk Management. The main pane is divided into two sections. The top section is a table listing the system's volumes. The bottom section is a graphical representation of the physical disks, showing their total capacity, online status, and the layout of their partitions.

Volume	Layout	Type	File System	Status
(C:)	Partition	Basic	NTFS	Healthy
CFTT-25 (F:)	Partition	Basic	NTFS	Healthy
CFTT-27 (G:)	Partition	Basic	FAT32	Healthy
CFTT-70 (D:)	Partition	Basic	NTFS	Healthy
CFTT-119 (E:)	Partition	Basic	NTFS	Healthy
LEXAR MEDIA...	Partition	Basic	FAT	Healthy

Disk	Capacity	Online	Partitions
Disk 0	9.50 GB	Online	(C:) 4.00 GB NTFS (Healthy Boot), 5.50 GB Unallocated
Disk 1	38.34 GB	Online	CFTT-70 (D:) 1.37 GB NTFS (Healthy Active), 36.97 GB Unallocated
Disk 2	111.79 GB	Online	CFTT-119 (E:) 111.79 GB NTFS (Healthy System)
Disk 3	68.36 GB	Online	CFTT-25 (F:) 68.36 GB NTFS (Healthy)
Disk 4	17.12 GB	Online	CFTT-27 (G:) 8.47 GB FAT32 (Healthy), 8.65 GB Unallocated

Legend: ■ Unallocated ■ Primary Partition

9.29.2 Write blocker configuration



9.29.3 Test output summary



Event.log - Windows 2000 Write Blocker

File View Tools Help

Physical Media Network Media Configuration

Double-click on the Physical Media to toggle the Write Blocked status.

Physical Media	Description	Volumes	Write Blocked
System Partition	Windows System Partition	C	No
FloppyDrive0	Floppy disk drive	A	Yes
CdRomDrive0	SONY DVD RW DRU-530A	H	Yes
HardDrive1	IC35L040AVER07-0	D	Yes
HardDrive2	WDC WD1200JD-00GBB0	E	Yes
HardDrive3	SEAGATE ST373405LC SCSI Disk D...	F	Yes
HardDrive4	QUANTUM ATLAS10K3_18_SCA SC...	G	Yes
HardDrive5	USB2.0 HS-CF USB Device	I	Yes
HardDrive6	LEXAR JUMPDRIVE SPORT USB D...	J	No

HardDrive1: Create Blocked

Ready

9.29.4 Hard disk hash results

Drive Identification		Computed	SHA1 Value
\\.\PhysicalDrive1	P	Before	6D96DA3851D7C4F4F124D29D0F02636E47DA3219
		After	6D96DA3851D7C4F4F124D29D0F02636E47DA3219

9.29.5 Test results analysis

The tool produced the expected result. The DROP operation failed with a write protection error message, 1 blocked command (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 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 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

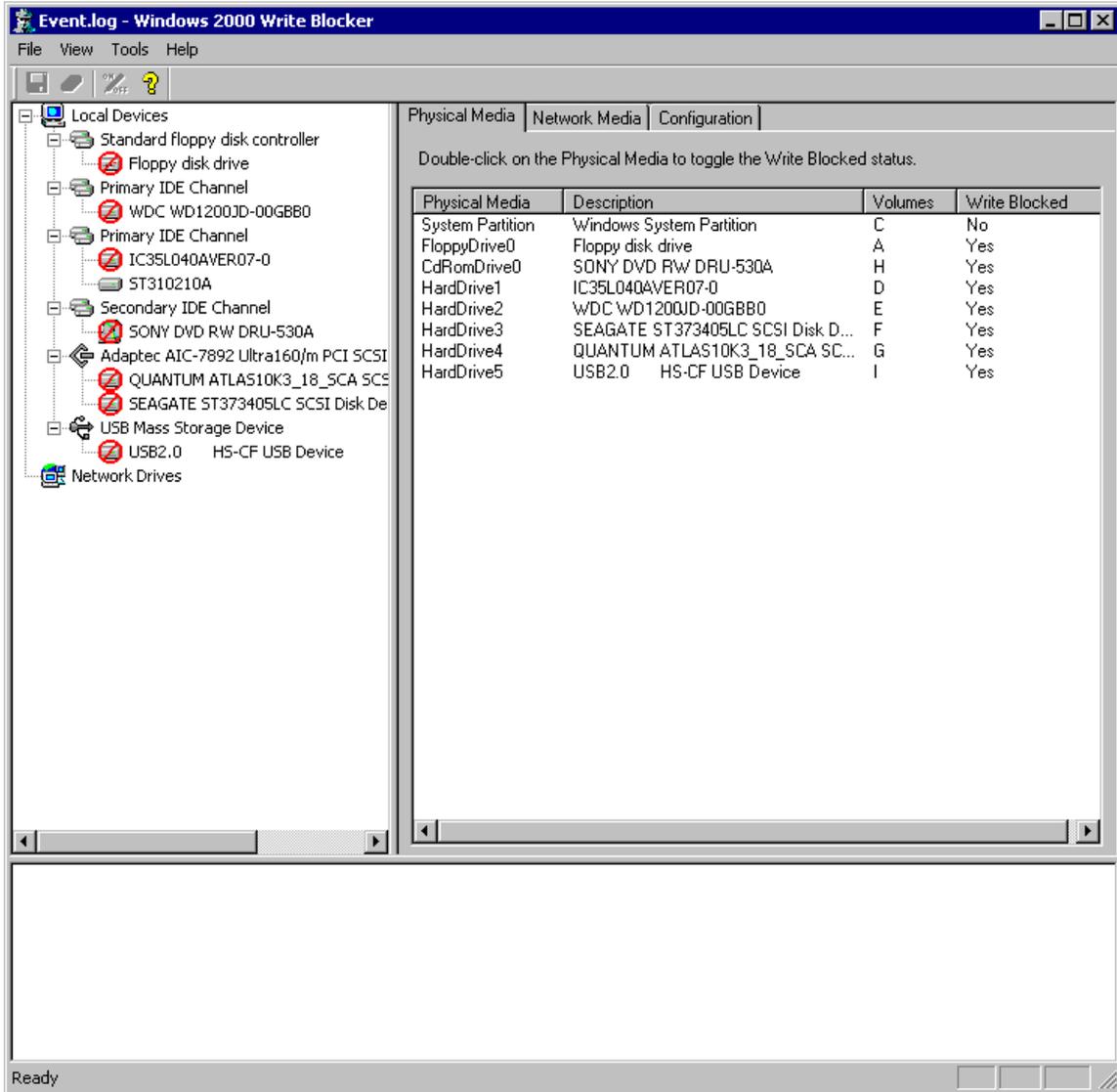
The screenshot shows the Windows Computer Management console. The left pane shows the tree view with 'Storage' expanded to 'Disk Management'. The right pane displays a table of volumes and a graphical disk layout.

Volume	Layout	Type	File System	Status
(C:)	Partition	Basic	NTFS	Healthy
CFTT-25 (F:)	Partition	Basic	NTFS	Healthy
CFTT-27 (G:)	Partition	Basic	FAT32	Healthy
CFTT-70 (D:)	Partition	Basic	NTFS	Healthy
CFTT-119 (E:)	Partition	Basic	NTFS	Healthy
LEXAR MEDIA...	Partition	Basic	FAT	Healthy

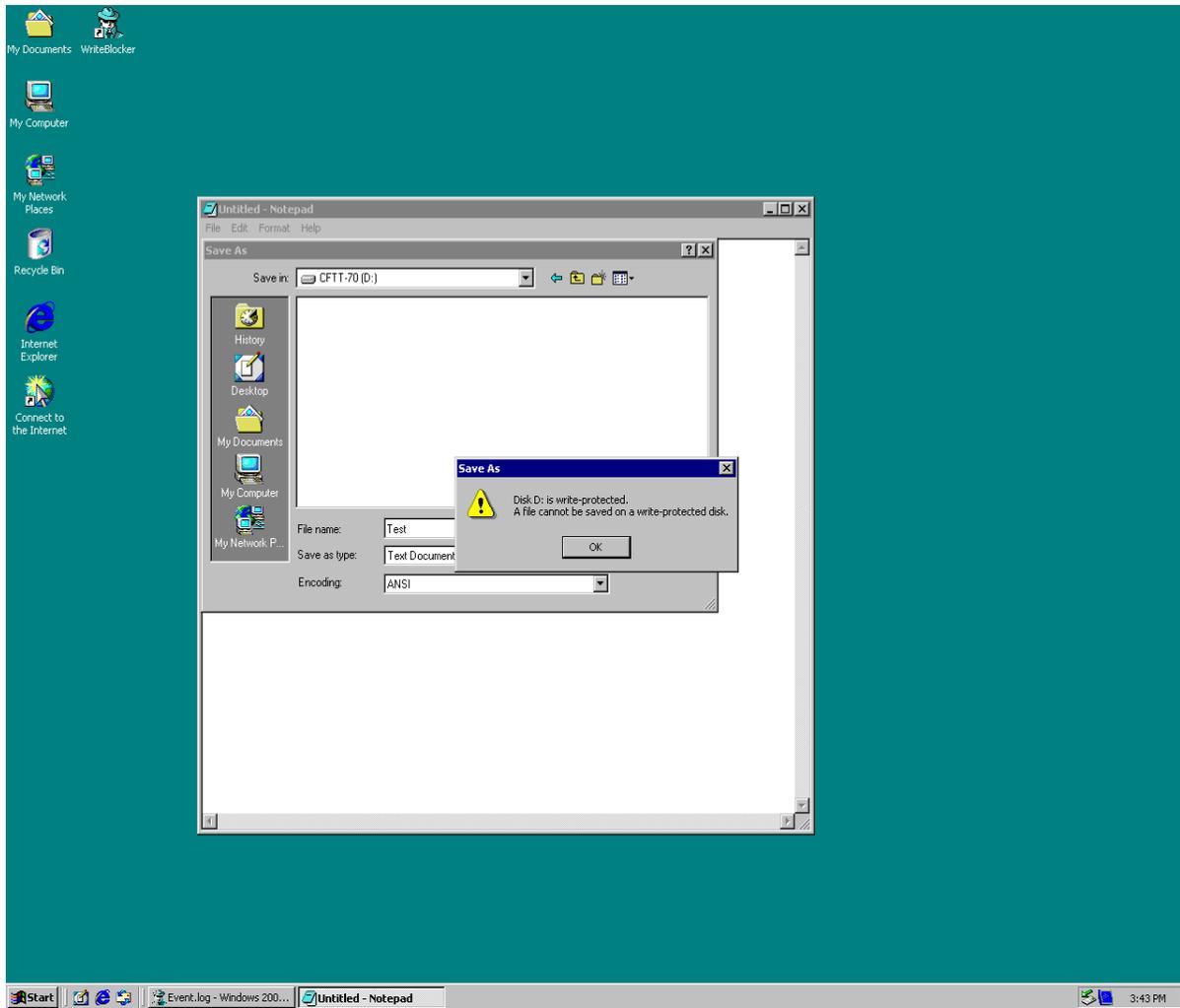
Disk	Capacity	State	Volume	Volume Capacity	Volume File System	Volume Status	Unallocated
Disk 0	9.50 GB	Online	(C:)	4.00 GB	NTFS	Healthy (Boot)	5.50 GB
Disk 1	38.34 GB	Online	CFTT-70 (D:)	1.37 GB	NTFS	Healthy (Active)	36.97 GB
Disk 2	111.79 GB	Online	CFTT-119 (E:)	111.79 GB	NTFS	Healthy (System)	
Disk 3	68.36 GB	Online	CFTT-25 (F:)	68.36 GB	NTFS	Healthy	
Disk 4	17.12 GB	Online	CFTT-27 (G:)	8.47 GB	FAT32	Healthy	8.65 GB

Legend: ■ Unallocated ■ Primary Partition

9.30.2 Write blocker configuration



9.30.3 Test output summary



9.30.4 Hard disk hash results

Drive Identification		Computed	SHA1 Value
\\.\PhysicalDrive1	P	Before	6D96DA3851D7C4F4F124D29D0F02636E47DA3219
		After	6D96DA3851D7C4F4F124D29D0F02636E47DA3219

9.30.5 Test results analysis

The tool produced the expected result. The drag and drop operation failed with a write protection error 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
Mon Mar 27 15:59:44 2006

Test case:          SWB-01
Command set:        RWOVU
Number of drives:   1
Protection pattern: U

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	Result
TEST_UNIT_READY	(0x00)	ALLOWED
REWI ND	(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_BUFFER_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

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

READ_GENERATI ON	(0x29)	ALLOWED
WRI TE10	(0x2A)	ALLOWED
SEEK10	(0x2B)	ALLOWED
ERASE10	(0x2C)	ALLOWED
VENDOR_SPECI FIC_CDB	(0x2D)	ALLOWED
WRI TE_AND_VERI FY10	(0x2E)	ALLOWED
VERI FY	(0x2F)	ALLOWED
SEARCH_DATA_HI GH	(0x30)	ALLOWED
SEARCH_DATA_EQUAL	(0x31)	ALLOWED
SEARCH_DATA_LOW	(0x32)	ALLOWED
SET_LI MI TS	(0x33)	ALLOWED
READ_POSI TI ON	(0x34)	ALLOWED
SYNCHRONI ZE_CACHE	(0x35)	ALLOWED
LOCK_UNLOCK_CACHE	(0x36)	ALLOWED
READ_DEFECT_DATA	(0x37)	ALLOWED
MEDI UM_SCAN	(0x38)	ALLOWED
COMPARE	(0x39)	ALLOWED
COPY_COMPARE	(0x3A)	ALLOWED
WRI TE_DATA_BUFF	(0x3B)	ALLOWED
READ_DATA_BUFF	(0x3C)	ALLOWED
UNDEFI NED_CDB	(0x3D)	ALLOWED
READ_LONG10	(0x3E)	ALLOWED
WRI TE_LONG10	(0x3F)	ALLOWED
CHANGE_DEFI NI TI ON	(0x40)	ALLOWED
WRI TE_SAME10	(0x41)	ALLOWED
READ_SUB_CHANNEL	(0x42)	ALLOWED
READ_TOC	(0x43)	ALLOWED
READ_HEADER	(0x44)	ALLOWED
PLAY_AUDI O	(0x45)	ALLOWED
GET_CONFI GURATI ON	(0x46)	ALLOWED
PLAY_AUDI O_MSF	(0x47)	ALLOWED
PLAY_TRACK_I NDEX	(0x48)	ALLOWED
PLAY_TRACK_RELATI VE	(0x49)	ALLOWED
GET_EVENT_STATUS	(0x4A)	ALLOWED
PAUSE_RESUME	(0x4B)	ALLOWED
LOG_SELECT	(0x4C)	ALLOWED
LOG_SENSE	(0x4D)	ALLOWED
STOP_PLAY_SCAN	(0x4E)	ALLOWED
UNDEFI NED_CDB	(0x4F)	ALLOWED
XDWRI TE10	(0x50)	ALLOWED
XPWRI TE10	(0x51)	ALLOWED
XDREAD10	(0x52)	ALLOWED
XDWRI TucRead10	(0x53)	ALLOWED
SEND_OPC_I NFORMATI ON	(0x54)	ALLOWED
MODE_SELECT10	(0x55)	ALLOWED
RESERVE_UNI T10	(0x56)	ALLOWED
RELEASE_UNI T10	(0x57)	ALLOWED
REPAI R_TRACK	(0x58)	ALLOWED
UNDEFI NED_CDB	(0x59)	ALLOWED
MODE_SENSE10	(0x5A)	ALLOWED
CLOSE_TRACK_SESSI ON	(0x5B)	ALLOWED
READ_BUFFER_CAPACI TY	(0x5C)	ALLOWED
SEND_CUE_SHEET	(0x5D)	ALLOWED
PERSI STENT_RESERVE_I N	(0x5E)	ALLOWED
PERSI STENT_RESERVE_OUT	(0x5F)	ALLOWED
UNDEFI NED_CDB	(0x60)	ALLOWED
UNDEFI NED_CDB	(0x61)	ALLOWED
UNDEFI NED_CDB	(0x62)	ALLOWED
UNDEFI NED_CDB	(0x63)	ALLOWED
UNDEFI NED_CDB	(0x64)	ALLOWED
UNDEFI NED_CDB	(0x65)	ALLOWED
UNDEFI NED_CDB	(0x66)	ALLOWED
UNDEFI NED_CDB	(0x67)	ALLOWED
UNDEFI NED_CDB	(0x68)	ALLOWED
UNDEFI NED_CDB	(0x69)	ALLOWED
UNDEFI NED_CDB	(0x6A)	ALLOWED
UNDEFI NED_CDB	(0x6B)	ALLOWED
UNDEFI NED_CDB	(0x6C)	ALLOWED
UNDEFI NED_CDB	(0x6D)	ALLOWED
UNDEFI NED_CDB	(0x6E)	ALLOWED
UNDEFI NED_CDB	(0x6F)	ALLOWED
UNDEFI NED_CDB	(0x70)	ALLOWED
UNDEFI NED_CDB	(0x71)	ALLOWED
UNDEFI NED_CDB	(0x72)	ALLOWED
UNDEFI NED_CDB	(0x73)	ALLOWED
UNDEFI NED_CDB	(0x74)	ALLOWED

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

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
MEDIA_MOVE	(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_VOLUME_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

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

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
IRP_MJ_PNP	(0x1B)	ALLOWED

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

***** 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

Figure A-2 – Logfile output listing for test SWB-03

```

NI ST Software Write Blocker Test Suite V1.2
Mon Mar 27 16:06:32 2006

Test case:          SWB-03
Command set:        W
Number of drives:   1
Protection pattern: P

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

IRP Function	Code	Result
IRP_MJ_CREATE	(0x00)	ALLOWED
IRP_MJ_WRITE	(0x04)	BLOCKED
IRP_MJ_SET_INFORMATION	(0x06)	BLOCKED
IRP_MJ_SET_EA	(0x08)	BLOCKED
IRP_MJ_FLUSH_BUFFERS	(0x09)	ALLOWED
IRP_MJ_SET_VOLUME_INFORMATION	(0x0B)	BLOCKED
IRP_MJ SCSI	(0x0F)	

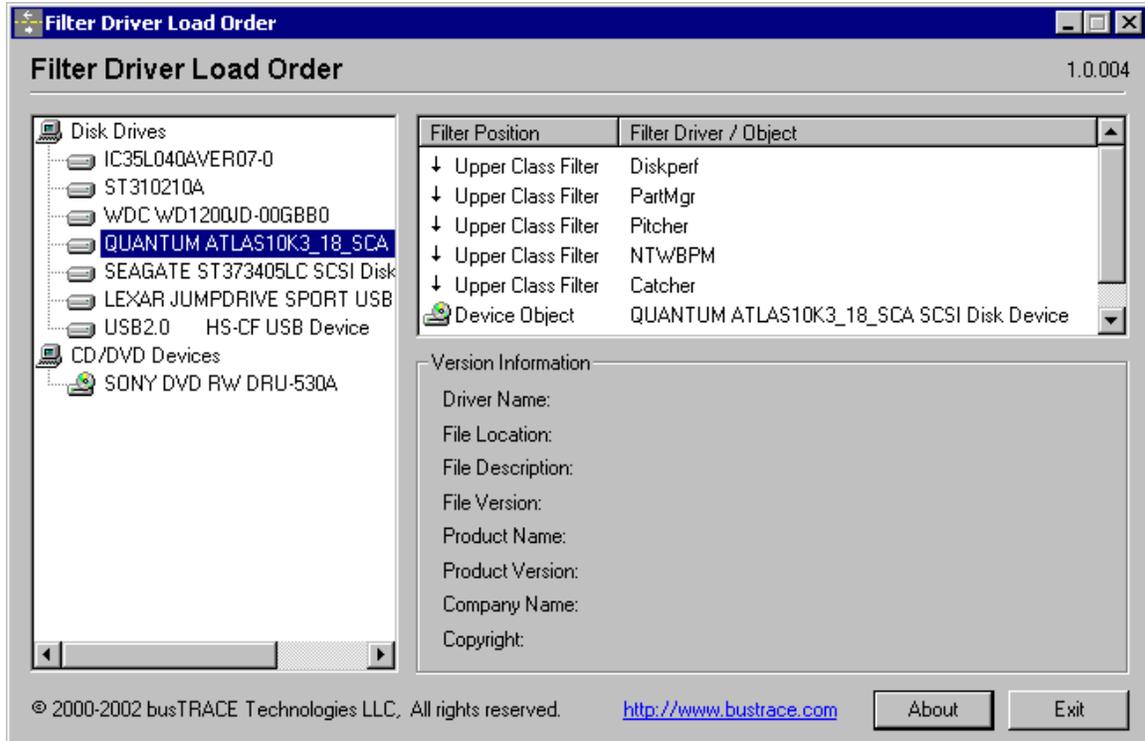
SCSI Operation	Opcode	Result
FORMAT UNIT	(0x04)	BLOCKED
REASSIGN_BLOCKS	(0x07)	ALLOWED
WRITE6	(0x0A)	BLOCKED
WRITE_FILEMARKS	(0x10)	ALLOWED
COPY	(0x18)	ALLOWED
ERASE	(0x19)	ALLOWED
WRITE10	(0x2A)	BLOCKED
ERASE10	(0x2C)	BLOCKED
WRITE_AND_VERIFY10	(0x2E)	BLOCKED
SYNCHRONIZE_CACHE	(0x35)	BLOCKED
COPY_COMPARE	(0x3A)	ALLOWED
WRITE_DATA_BUFFER	(0x3B)	BLOCKED
WRITE_LONG10	(0x3F)	ALLOWED
WRITE_SAME10	(0x41)	ALLOWED
XDWRITE10	(0x50)	ALLOWED
XPWRITE10	(0x51)	ALLOWED
XDWRITE10Read10	(0x53)	BLOCKED
REPAIR_TRACK	(0x58)	BLOCKED
CLOSE_TRACK_SESSION	(0x5B)	BLOCKED
SEND_CUE_SHEET	(0x5D)	ALLOWED
UNDEFINED_CDB	(0x7F)	ALLOWED
XDWRITE_EXTENDED	(0x80)	ALLOWED
REBUILD	(0x81)	ALLOWED
REGENERATE	(0x82)	ALLOWED
EXTENDED_COPY	(0x83)	ALLOWED
ATA_PASSTHROUGH16	(0x85)	ALLOWED
WRITE16	(0x8A)	ALLOWED
WRITE_AND_VERIFY16	(0x8E)	ALLOWED
SYNCHRONIZE_CACHE16	(0x91)	ALLOWED
WRITE_SAME16	(0x93)	ALLOWED
ATA_PASSTHROUGH12	(0xA1)	BLOCKED
WRITE12	(0xAA)	BLOCKED
ERASE12	(0xAC)	ALLOWED
WRITE_AND_VERIFY12	(0xAE)	ALLOWED

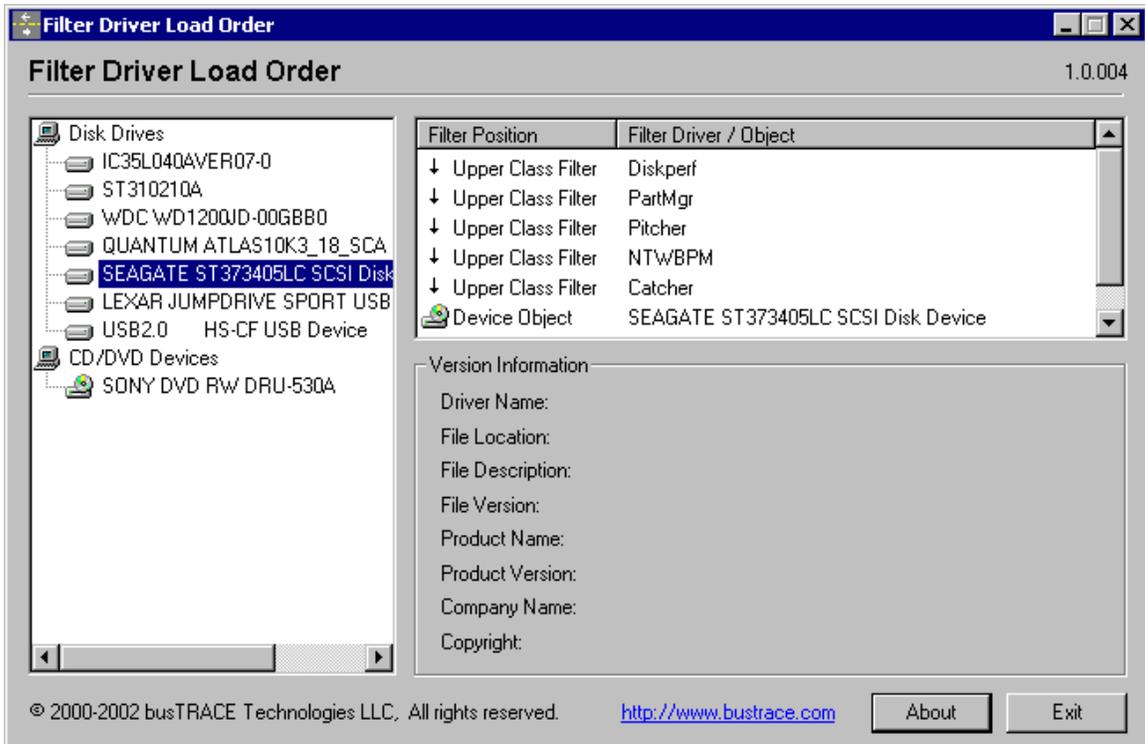
IRP_MJ_SET_SECURITY	(0x15)	ALLOWED
IRP_MJ_SET_QUOTA	(0x1A)	ALLOWED

***** TEST RESULTS SUMMARY *****

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

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:

[NIJ Website](#)

or contact:

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