

Evaluation of Software Write Blocking In SAFE Block XP V1.1

University of Rhode Island Digital Forensics Center

Web: dfc.cs.uri.edu

June 30, 2008

Technical Report 2008-52-1

Sean Alvarez

University of Rhode Island Digital Forensics Center

Peter Cho

University of Rhode Island Department of Computer Science

Ren Jin

University of Rhode Island Department of Electrical Engineering

Abstract. This report applies the U.S. government's National Institute of Standards (NIST) *NIST Software Write Blocker Test Suite V1.2* [1] to *SAFE Block XP V1.1* [2], a software write blocker prototyped at the University of Rhode Island and marketed by ForensicSoft, Inc. The results demonstrate that *SAFE Block XP V1.1* meets all NIST base requirements, and all NIST mandatory and optional test assertions. To facilitate comparison, this report generally follows the format of the NIST report "*ACES Software Write Block Tool Test Report: Writeblocker Windows XP Version 6.10.0*" January 2008 [3]. However, this is not a NIST report and should in no way be construed as NIST-conducted tests, or NIST-approved results.

Contents

1	NIST Base Requirements And Our Conclusions	3
2	Deviations From Expectations	3
2.1	Variation From NIST's Expected Behavior	3
2.2	Same Hash Test Result	3
2	SAFE Block Description	4
4	Test Case Selection	4
5	Test Results By Assertion	5
6	Test Environment	7
7	Test Results	9
7.1	Test Case SWB-01	10
7.2	Test Case SWB-02	12
7.3	Test Case SWB-03	14
7.4	Test Case SWB-04	16
7.5	Test Case SWB-05	18
7.6	Test Case SWB-06	20
7.7	Test Case SWB-07	22
7.8	Test Case SWB-08	25
7.9	Test Case SWB-09	28
7.10	Test Case SWB-10	31
7.11	Test Case SWB-11	34
7.12	Test Case SWB-12	37
7.13	Test Case SWB-13	40
7.14	Test Case SWB-14	43
7.15	Test Case SWB-15	46
7.16	Test Case SWB-16	49
7.17	Test Case SWB-17	52
7.18	Test Case SWB-18	55
7.19	Test Case SWB-19	58
7.20	Test Case SWB-20	61
7.21	Test Case SWB-21	64
7.22	Test Case SWB-22	67
7.23	Test Case SWB-23	70
7.24	Test Case SWB-24	73
7.25	Test Case SWB-25	76
7.26	Test Case SWB-26	78
7.27	Test Case SWB-27	80
7.28	Test Case SWB-28	82
7.29	Test Case SWB-29	84
7.30	Test Case SWB-30	86

1 NIST Base Requirements And Our Conclusions

SAFE Block XP V1.1 shall not allow a protected drive to be changed.

SAFE Block XP Version 1.1 blocked all test commands from the protected categories that were sent to protected drives, and there were no changes to the protected drives.

SAFE Block XP V1.1 shall not prevent obtaining any information from or about any drive.

SAFE Block XP Version 1.1 did not prevent obtaining information from or about any drive.

SAFE Block XP V1.1 shall not prevent any operations to a drive that is not protected.

SAFE Block XP Version 1.1 did not alter or block any test commands sent to unprotected drives.

Thus, SAFE Block XP V1.1 meets all base requirements.

2 Deviations From Expectations

This section explains two deviations, or apparent deviations, from expected behavior in our test results. One is a deviation from NIST's specified behavior, which is documented as a design decision in the SAFE Block XP V1.1 tool. The second explains what at first appears to be strange SHA-1 hash results on unprotected disks, but is actually correct.

2.1 Variation From NIST's Expected Behavior

The NIST test specification expects all commands from its "Other" category to be allowed (see test assertion SWB-AO-05 in [3]; which is also summarized in Section 5.2 below). SAFE Block XP Version 1.1 does this, except that it blocks the WRITE_ATTRIBUTE "Other" command. The SAFE Block XP Version 1.1 documentation explains that this command could possibly alter the data of a disk so in its default conservative mode, SAFE Block XP Version 1.1. blocks it. We refer to this as Variation 1 when analyzing test results in Section 7.

a. Same Hash Test Result

In many of our tests the SHA-1 hash value before and after a write test to an unprotected disk were the same, which at first glance is unexpected. This behavior can also be found in the NIST report pages 101 and 105 [3].

This is actually correct behavior for these reasons:

- The NIST Software Write Blocker Test Suite V1.2 tests the issuing of write commands with a control structure that specifies zero bytes to write, and does not actually pass the command through. This is sufficient for the NIST Software Write Blocker Test Suite V1.2 because the test suite intercepts write commands to determine if they pass the blocking tool. However, the testing software will not actually ever write any data to the disk.
- In NIST's original report [3], hash values changed on all NTFS disks, but did not change on FAT32 disks (see pages 101 and 105 of [3]). This is likely due to the fact that NTFS itself writes a log file to its disks, FAT32 does not. Since, as stated above, NIST Software Write Blocker Test Suite V1.2 does not write to the disks, we speculate that the changes in the hashes in the NIST test are a result of the NTFS log being written while the testing software executed.
- In our tests, our disks are very small which means that testing and hashing can occur before Windows flushes its write buffer to actually write the NTFS log. We saw changed hashes during write tests to unprotected disks in two tests, test SWB-07 in Section 6.7 and test SWB-22 in Section 6.22 of this report. This occurred when the timing of Windows flushing its write buffer allowed the NTFS log to be written.
- We verified that on larger disks, the hash value to unprotected NTFS disks does change using the NIST Software Write Blocker Test Suite V1.2 with SAFE Block XP V1.1 installed, and does not change for larger FAT32 disks.

Neither of these seemingly unexpected behaviors are concerns for SAFE Block XP V1.1's ability to protect and unprotect disks.

3 SAFE Block Description

SAFE Block XP Version 1.1 consists of a block-level device driver and a GUI application that runs as a service. This is similar to the NTWBPM driver used by WriteBlocker XP that NIST tested in [3], which makes the NIST testing software that tested that NTWBPM driver applicable to SAFE Block XP Version 1.1 evaluation, for the reasons NIST puts forth in [3].

4 Test Case Selection

The test cases are the 30 tests used in the NIST report [3], most of which are implemented in NIST Software Write Blocker Test Suite V1.2 [1].

5 Test Results by Assertion

This section evaluates SAFE Block XP V1.1 using the NIST test assertions [3]. The meaning of the test assertions is that described in Section 7 of the NIST report [3].

5.1 NIST Mandatory Assertions SWB-AM-01 If a drive is unprotected then SAFE Block XP V1.1 shall not block any command.

SAFE Block XP Version 1.1 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 SAFE Block XP V1.1 shall not block the command.

SAFE Block XP Version 1.1 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 SAFE Block XP V1.1 shall block the command.

SAFE Block XP Version 1.1 blocked all 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 SAFE Block XP V1.1 shall block the command.

SAFE Block XP Version 1.1 blocked all of the 80 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 SAFE Block XP V1.1 shall block the command.

SAFE Block XP Version 1.1 blocked all of the of the 53 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 SAFE Block XP V1.1 shall not block the command.

SAFE Block XP Version 1.1 blocked one test command from the OTHER category sent to a protected drive, as explained in Section 2.1 above.

SWB-AM-07 If SAFE Block XP Version 1.1 is executed then SAFE Block XP V1.1 shall issue a message indicating SAFE Block XP Version 1.1 is active.

This is not applicable to the driver, which runs continually from the point of installation to the point of de-installation. The GUI application being active is indicated by a tray icon. A pop-up message from the tray indicates when SAFE Block blocks and unblocks devices, including automatic blocking specified as default behavior.

SWB-AM-08 If SAFE Block XP V1.1 is executed then SAFE Block XP V1.1 shall issue a message indicating all drives accessible by the covered interfaces.

The SAFE Block GUI application displays a tree of all channels and devices accessible by the covered interfaces.

SWB-AM-09 If SAFE Block XP V1.1 is executed then SAFE Block XP V1.1 shall issue a message indicating the protection status of each drive connected to a covered interface.

The SAFE Block GUI application displays the protection status of all devices connected to covered interfaces.

Thus SAFE Block XP V1.1 meets all NIST mandatory assertions.

a. NIST 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.

SAFE Block XP Version 1.1 blocked all 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.

SAFE Block XP Version 1.1 blocked 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.

SAFE Block XP Version 1.1 blocked 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.

SAFE Block XP Version 1.1 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.

SAFE Block XP Version 1.1 blocked one of the test commands from the OTHER category sent to the drives, as described in Section 2.1.

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

SAFE Block XP Version 1.1 did not block any commands sent to unprotected drives.

SWB-AO-07 If SAFE Block XP V1.1 is active and SAFE Block XP V1.1 is deactivated then no commands to any drive shall be blocked.

No commands to any drive were blocked after SAFE Block XP Version 1.1 was de-installed.

SWB-AO-08 If SAFE Block XP V1.1 blocks a command then SAFE Block XP V1.1 shall issue either an audio or visual signal.

SAFE Block XP Version 1.1 does not issue its own signal, however, in most instances Windows itself detects the blocking and issues an informational dialog box that the drive is write-protected.

Thus, SAFE Block XP V1.1 meets all NIST optional assertions, with a caveat on SWB-AO-05 (explained in Section 2.1).

6 Testing Environment

All tests were run at the University of Rhode Island Digital Forensics Lab. The test computer consisted of:

Model: Dell Precision Workstation 690

CPU: Intel Xeon 5110 [Socket 771 LGA; 1.66 GHz; 1066 FSB; 4MB L2 Cache]

RAM: Hyundai Electronics 2048MB [Quad Channel 512MBx4; PC2-5300; CAS Latency 5; 5-5-5-15]

Motherboard: Dell Inc 0MY171 [Intel 5000X; Intel 6321ESB Southbridge]

BIOS: Dell Inc. vA05

3 Standard SATA slots

4 RAID slots

2 IDE Channel

Hard Drive(s): Seagate Barracuda ST380815AS [RAID 0; 7200.10 RPM; 80GB]

PCI Card(s): Adaptec AHA-2940AU PCI SCSI Controller

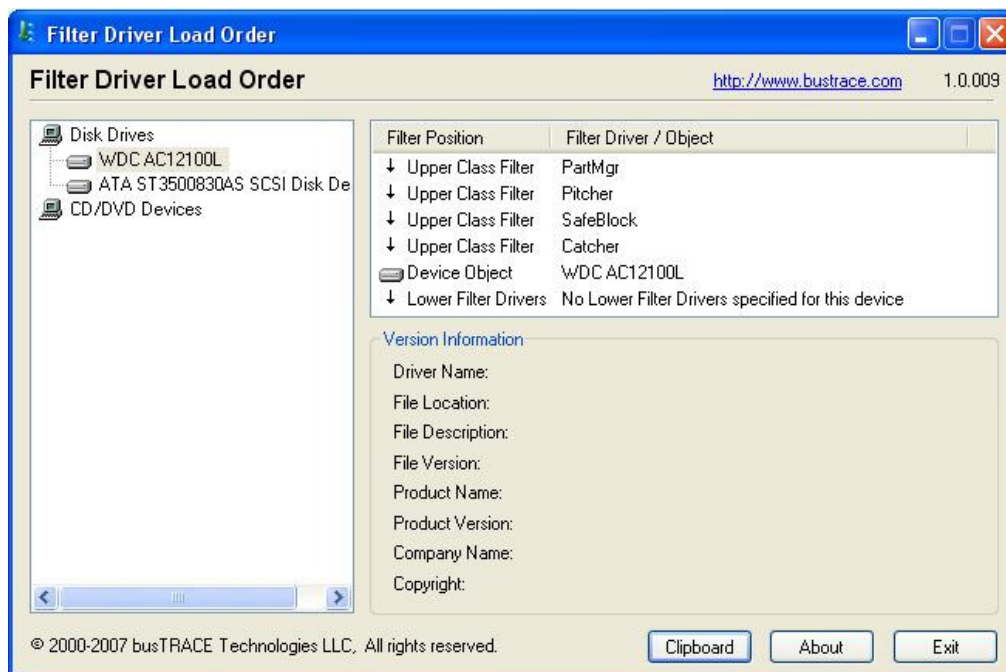
Operating System: Microsoft Windows XP Professional [Version 2002; Service Pack 3]

The hard drives and removable drives in the test computer were:

Model	Interface	Useable Sectors	Size (MB)
CONNER CP3040A	SCSI	82080	40
WDC AC12100L	PATA	4124736	2007.04
PNY Attaché (two of these)	USB Flash	246272	120

Note that “MB” is correct – these are small drives to facilitate fast hashing.

The testing was performed using *NIST Software Write Blocker Test Suite V1.2* [1] installed on the test machine as per installation instructions included in [1]. A screenshot of the busTRACE Filter Driver Load Order v1.0.009 tool [5] showing the NIST filters installed properly can be seen below. Hashes were computed using AccessData FTK Imager 2.5.3 [4].



Driver Order showing NIST test drivers and SAFE Block XP V1.1

7 Test Results

Each of the test results in the following subsections show the disk configuration active on the test machine using the Windows Computer Management interface. It is followed by a screen shot of the SAFE Block XP Version 1.1 interface with the blocked/unblocked disk configuration for the test. The use of a lock icon over the drive icon in the device tree on the left in the SAFE Block XP Version 1.1 GUI indicates that the drive is protected (blocked), a non-lock icon indicates that the disk is unprotected (not blocked).

The test results are shown by summary text displayed by the NIST Software Write Blocker Test Suite V1.2, the general format and meaning of which is fully described in the NIST report [3]. The key elements of the display are

- Line 7 which shows the pattern of blocked disks that the test software expects. In this display
 - U = Unprotected (unblocked) disk
 - P = Protected (blocked) disk
- For instance:
- U = only the first disk of the disks described in Section 6 is sent commands and it is expected to be unblocked.
 - PU = the first two disks of the disks described in Section 6 are sent commands and it is expected that disk 1 is protected and disk 2 is unprotected.
 - UUP = the first three disks of the disks described in Section 6 are sent commands and it is expected that disks 1 and 2 are unprotected and disk 3 is protected.
- The summary which shows how many of each type of command got through the SAFE Block XP Version 1.1 tool.

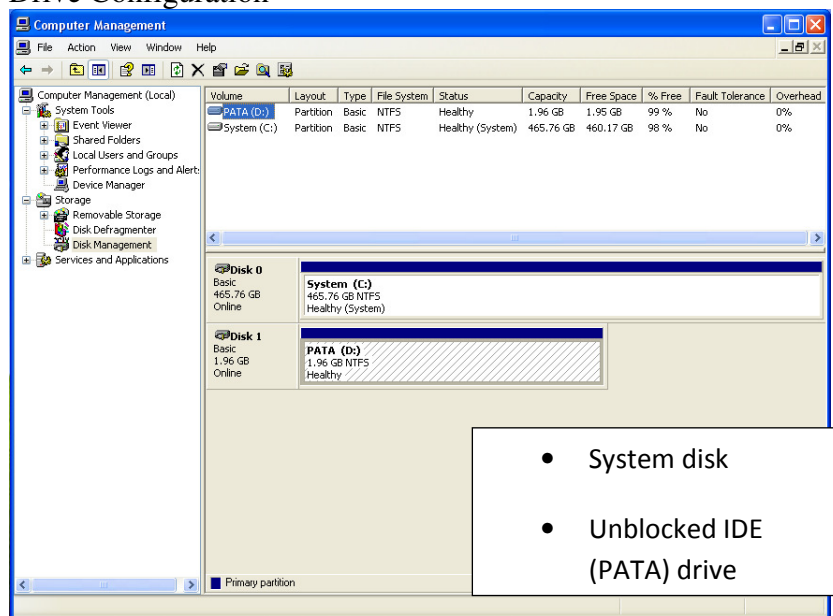
Each test also contains before and after SHA-1 hash values of all disks involved in the test. The SHA-1 hash serves as digital signature of the bits on the disk. If the SHA-1 hash value changes, the disk was written to, if the SHA-1 hash value remains the same, then it is generally accepted that the disk was not written to

We now provide a subsection for each of the 30 NIST software write blocker tests. Each subsection is patterned after similar subsections in Section 9 of the NIST report.

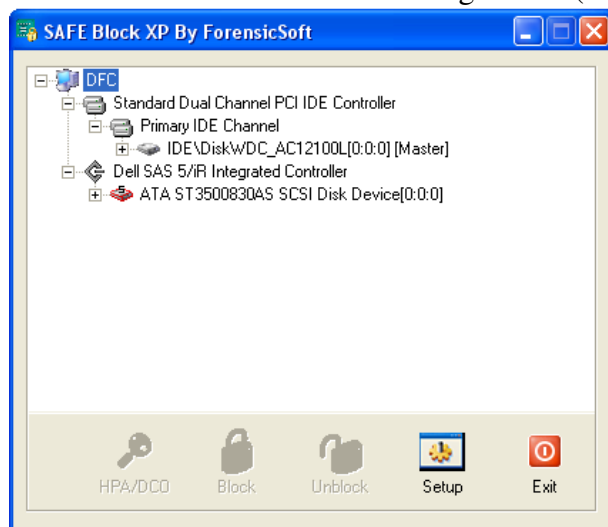
7.1 Test Case SWB-01

This test case's primary purpose is to test SAFE Block XP V1.1's compliance with SWB-AM-01. It issues all possible I/O commands to a single unprotected disk drive.

Drive Configuration



SAFE Block XP Version 1.1 Configuration (



SHA-1 Hash Values

Before	fd3a7e577e0c2b130fb73eb4452eb8fef344babe
After	fd3a7e577e0c2b130fb73eb4452eb8fef344babe

NIST Software Write Blocker Test Suite V1.2 Output Summary

NIST Software Write Blocker Test Suite V1.2
Mon Jun 16 15:01:15 2008

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

**** Test results summary (see log file 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

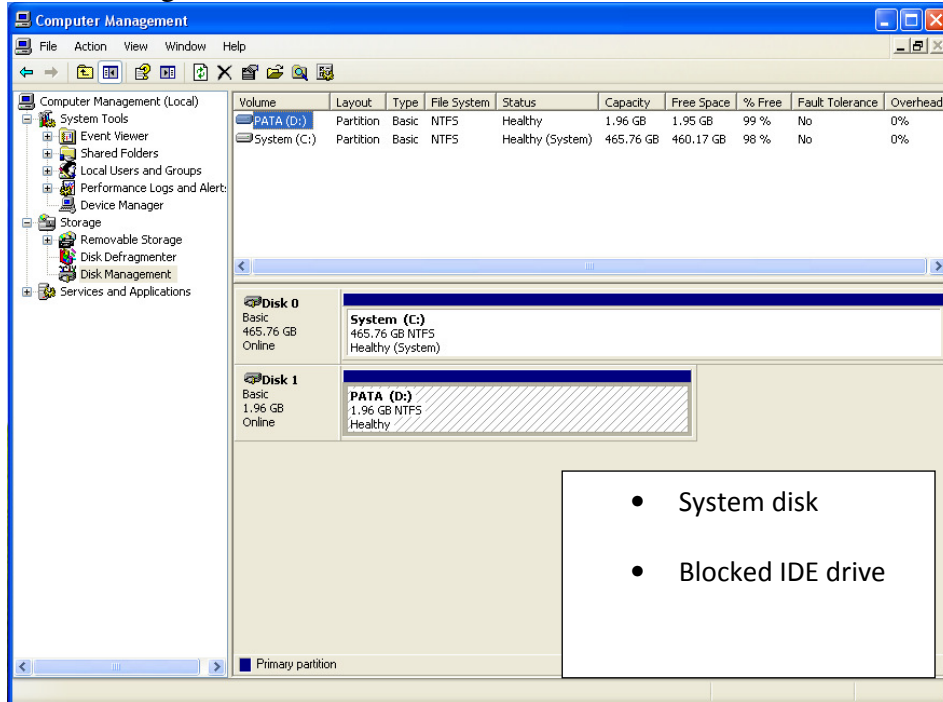
SWB-01 Test result analysis

SAFE Block XP Version 1.1 performed correctly - all commands were issued and all were allowed on the unblocked disk.

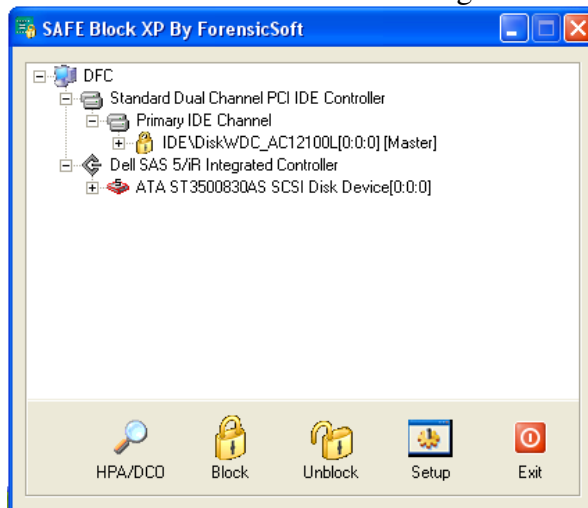
7.2 Test Case SWB-02

This test case tests SAFE Block XP V1.1's compliance with SWB-AM-02. It issues all possible READ commands to a single protected disk drive. The expected result is that SAFE Block XP V1.1 will not block any READ command issued by the test application.

Drive Configuration



SAFE Block XP Version 1.1 Configuration



SHA-1 Hash Values

Before	badd8c494fe2dbeb27030c50b5ac254f9ef5f6ff
After	badd8c494fe2dbeb27030c50b5ac254f9ef5f6ff

NIST Software Write Blocker Test Suite V1.2 Output Summary

NIST Software Write Blocker Test Suite V1.2
Mon Jun 16 14:44:56 2008

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

**** Test results summary (see log file 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

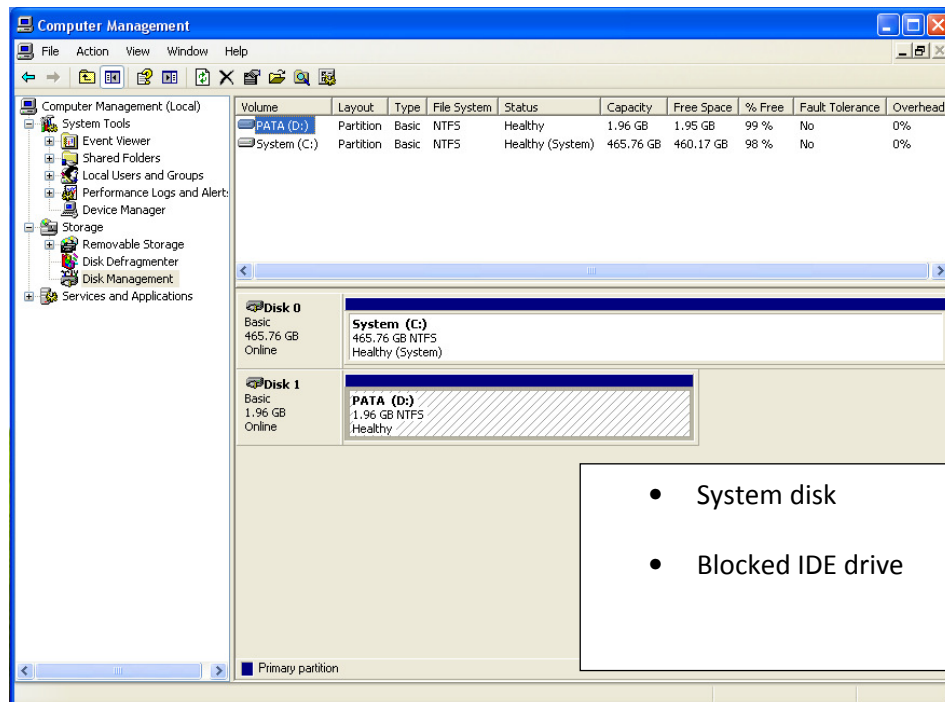
SWB-02 Test result analysis

SAFE Block XP Version 1.1 performed correctly - only Read commands were issued and all were allowed on the blocked disk.

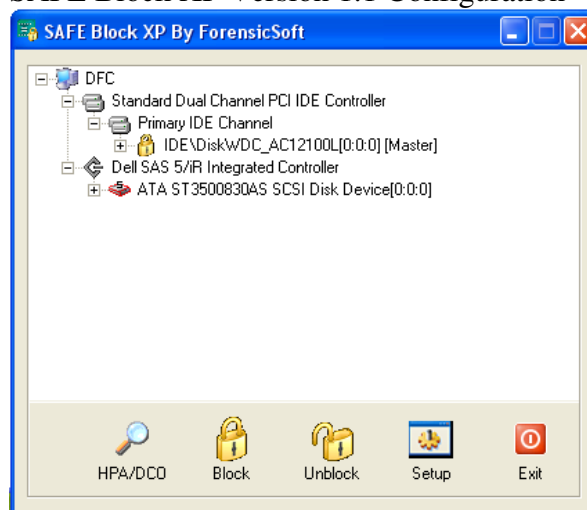
7.3 Test Case SWB-03

This test case tests SAFE Block XP V1.1'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 SAFE Block XP V1.1 will block all commands issued by the test application.

Drive Configuration



SAFE Block XP Version 1.1 Configuration



SHA-1 Hash Values

Before	badd8c494fe2dbeb27030c50b5ac254f9ef5f6ff
After	badd8c494fe2dbeb27030c50b5ac254f9ef5f6ff

NIST Software Write Blocker Test Suite V1.2 Output Summary

NIST Software Write Blocker Test Suite V1.2
Mon Jun 16 14:38:49 2008

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

**** Test results summary (see log file 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	8	8
Other IRP's	0	0	0
Read CDB's	0	0	0
Write CDB's	0	34	34
Other CDB's	0	0	0
Vendor Specific CDB's	0	0	0
Undefined CDB's.....	0	0	0

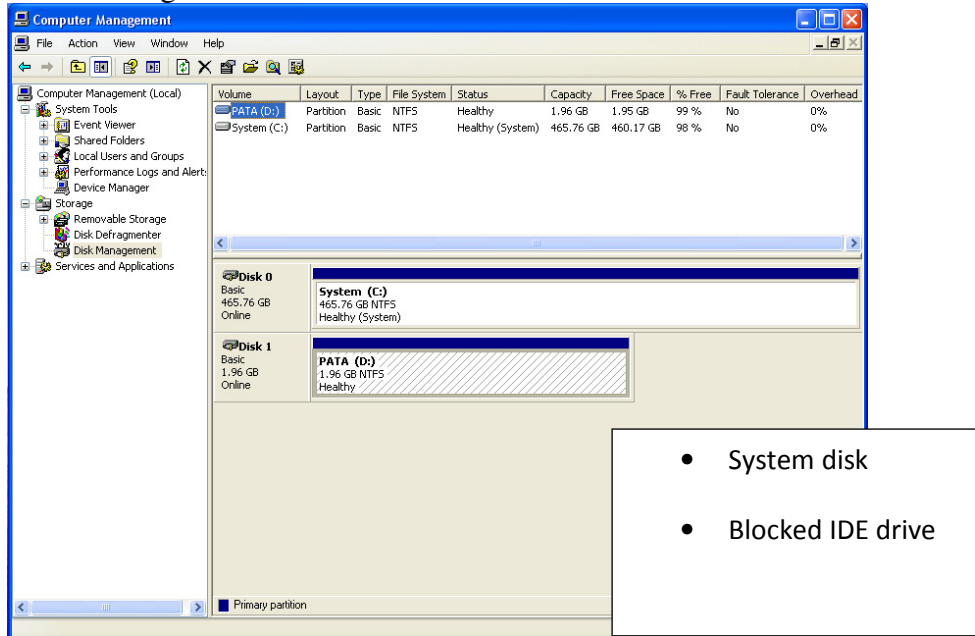
SWB-03 Test result analysis

SAFE Block XP Version 1.1 performed correctly - only Write commands were issued and all were blocked on the blocked disk.

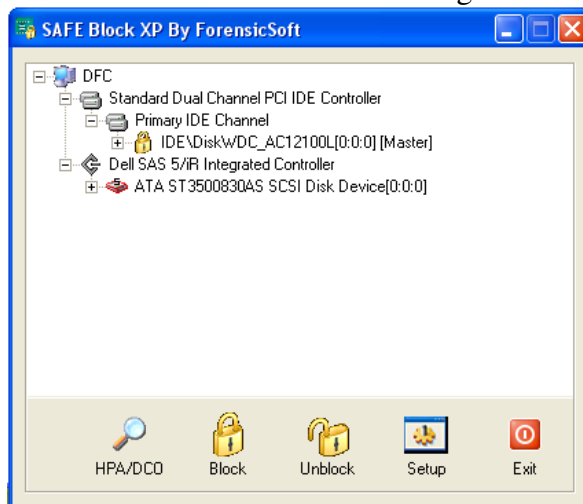
7.4 Test Case SWB-04

This test case tests SAFE Block XP V1.1's compliance with SWB-AM-04. It issues all possible commands from the VENDOR_SPECIFIC command set to a single protected disk drive. It uses the same hard drive setup as SWB-03. The expected result of this test is that SAFE Block XP V1.1 will block all commands issued by the test application.

Drive Configuration



SAFE Block XP Version 1.1 Configuration



SHA-1 Hash Values

Before	32259d7bf92b76acd5c9ffba9bf02637d8dd0de7
After	32259d7bf92b76acd5c9ffba9bf02637d8dd0de7

NIST Software Write Blocker Test Suite V1.2 Output Summary

NIST Software Write Blocker Test Suite V1.2
Mon Jun 16 15:14:16 2008

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

**** Test results summary (see log file 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	80	80
Undefined CDB's.....	0	0	0

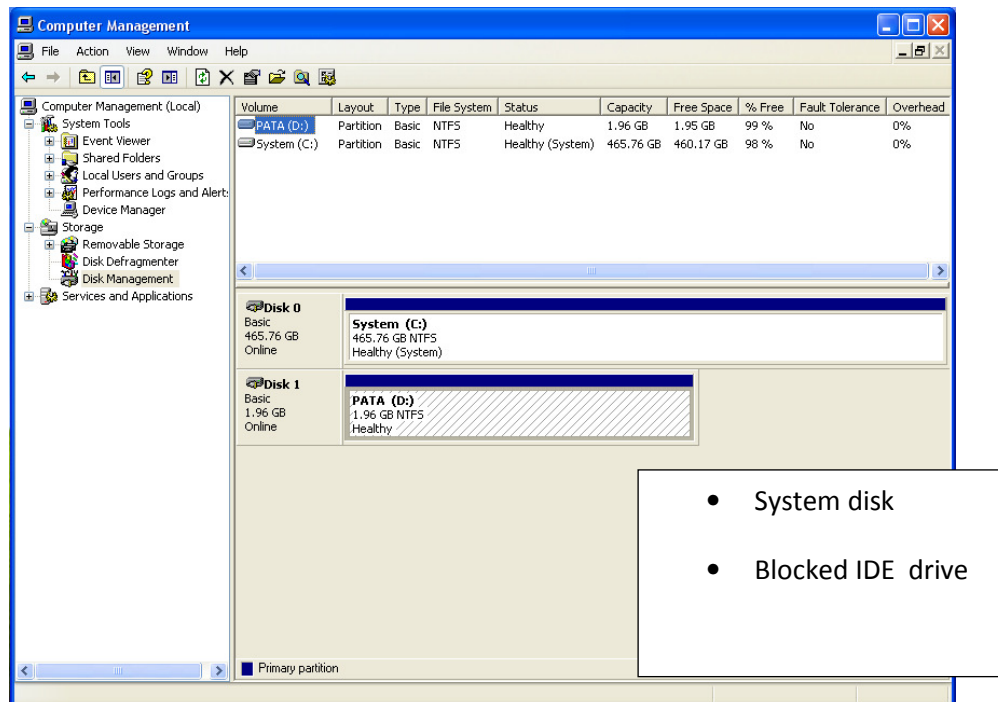
SWB-04 Test result analysis

SAFE Block XP Version 1.1 performed correctly - only Vendor Specific commands were issued and all were blocked on the blocked disk.

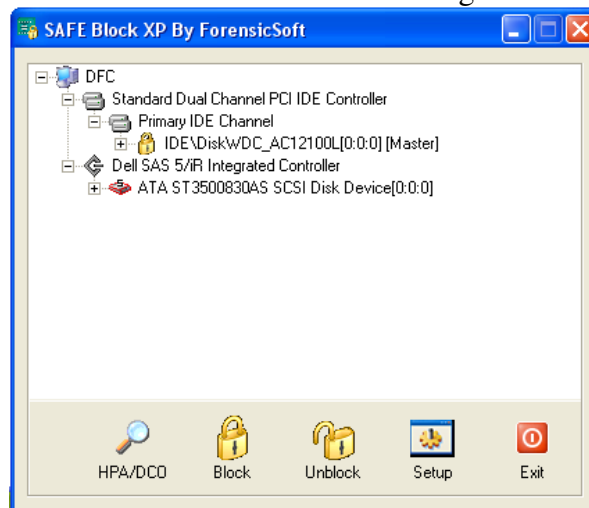
7.5 Test Case SWB-05

This test case tests SAFE Block XP V1.1's compliance with SWB-AM-05. It issues all possible commands from the UNDEFINED command set to a single protected disk drive. It uses the same hard drive setup as SWB-04. The expected result of this test is that SAFE Block XP V1.1 will block all commands issued by the test application.

Drive Configuration



SAFE Block XP Version 1.1 Configuration



SHA-1 Hash Values

Before	32259d7bf92b76acd5c9ffba9bf02637d8dd0de7
After	32259d7bf92b76acd5c9ffba9bf02637d8dd0de7

NIST Software Write Blocker Test Suite V1.2 Output Summary

NIST Software Write Blocker Test Suite V1.2
Mon Jun 16 15:28:55 2008

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

**** Test results summary (see log file 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.....	0	53	53

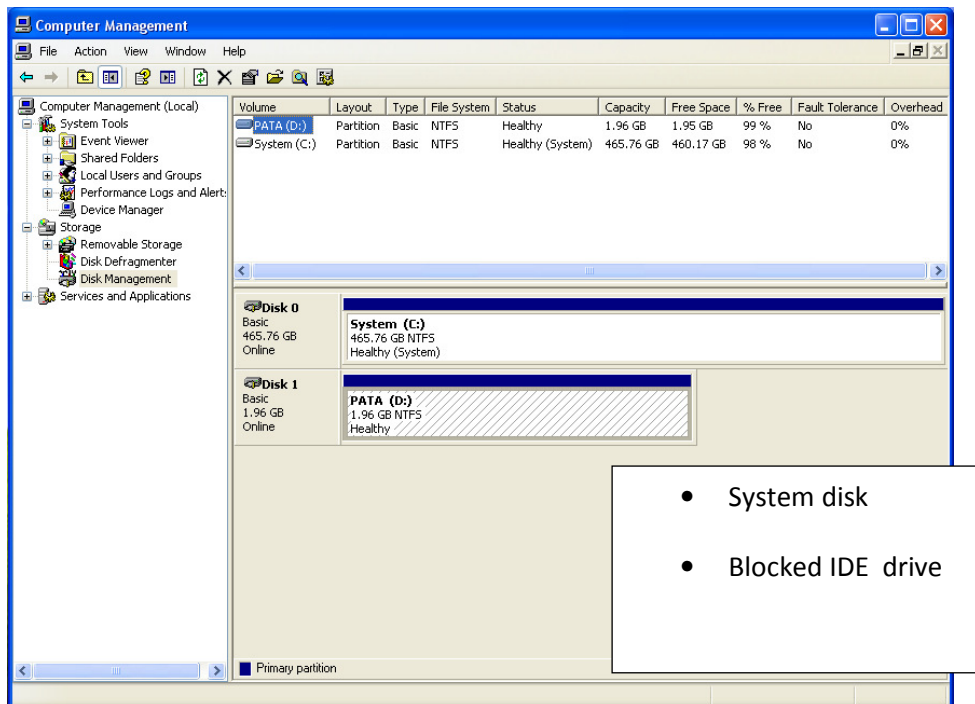
SWB-05 Test result analysis

SAFE Block XP Version 1.1 performed correctly - only UNDEFINED commands were issued and all were blocked on the blocked disk.

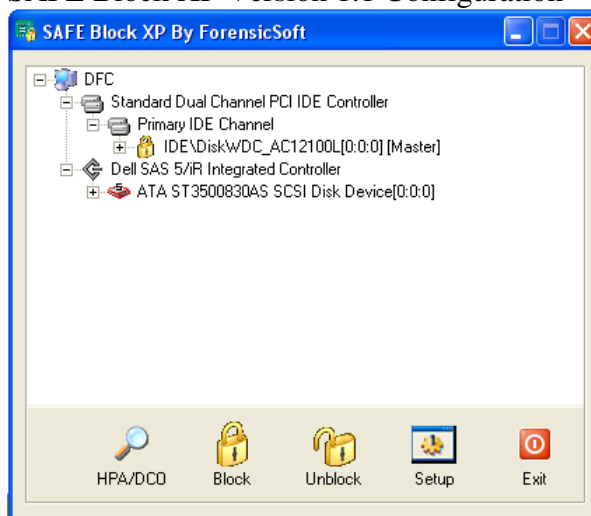
7.6 Test Case SWB-06

This test case tests SAFE Block XP V1.1's compliance with SWB-AM-06. It issues all possible commands from the OTHER command set to a single protected disk drive. It uses the same hard drive setup as SWB-05. The expected result of this test is that SAFE Block XP V1.1 will allow all commands issued by the test application.

Drive Configuration



SAFE Block XP Version 1.1 Configuration



SHA-1 Hash Values

Before	032bf070fa6da083ffe31ca87d48d5cf8991f57b
After	032bf070fa6da083ffe31ca87d48d5cf8991f57b

NIST Software Write Blocker Test Suite V1.2 Output Summary

NIST Software Write Blocker Test Suite V1.2
Mon Jun 16 16:51:31 2008

Test case: SWB-06
Command set: O
Number of drives: 1
Protection pattern: P
Test administered by: SPA
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	61	1	62
Vendor Specific CDB's	0	0	0
Undefined CDB's.....	0	0	0

SWB-06 Test result analysis

SAFE Block XP Version 1.1 had one unexpected result in this test – Variation 1 described in Section 2.1. Note that this is conservative blocking, which is generally considered good for forensics. Otherwise, SAFE Block XP V1.1 allowed all commands issued by the test application.

7.7 Test Case SWB-07

This case tests SAFE Block XP V1.1's compliance with optional assertions SWB-AO-01 through SWB-AO-06. It issues all possible commands to a set of three drives protected with the pattern PUU. The expected result of this test is SAFE Block XP V1.1 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

Drive Configuration

Volume	Layout	Type	File System	Status	Capacity	Free Space	% Free	Fault Tolerance	Overhead
C:	Partition	Basic	NTFS	Healthy	1.96 GB	1.95 GB	99 %	No	0%
G:	Partition	Basic	NTFS	Healthy	40 MB	38 MB	95 %	No	0%
F:	Partition	Basic	FAT	Healthy (Active)	120 MB	30 MB	25 %	No	0%

- System disk
- Blocked USB disk
- Unblocked SCSI

SAFE Block XP Version 1.1 Configuration

SAFE Block XP By ForensicSoft

- DFC
 - Standard Dual Channel PCI IDE Controller
 - Primary IDE Channel
 - IDE\Disk\WDC_AC12100L[0:0:0] [Master]
 - Dell SAS 5/iR Integrated Controller
 - ATA ST3500830AS SCSI Disk Device[0:0:0]
 - Adaptec AHA-2940AU PCI SCSI Controller
 - SCSI\Disk\CONNER[0:0:0]
 - USB Mass Storage Device
 - USBSTOR\Disk[0:0:0]

Buttons: HPA/DCO, Block, Unblock, Setup, Exit

SHA-1 Hash Values

Before USB	8d4a759a29a99b9a5320d7b7f9a06fd288215d40
After USB	8d4a759a29a99b9a5320d7b7f9a06fd288215d40
Before SCSI	a92a3c8776c049fe30d6590fd4ca32599614735b
After SCSI	37177deabf3008315d65799ba824dfaa383d83d2
Before IDE	1299f5fb2c4e1ced13a93e4f472f99665f5f20af
After IDE	e2b40b714345e7d8af326eabe3881b43e16167de

NIST Software Write Blocker Test Suite V1.2 Output Summary

NIST Software Write Blocker Test Suite V1.2
Tue Jun 17 10:17:09 2008

Test case: SWB-07
Command set: RWOVU
Number of drives: 3
Protection pattern: PUU
Test administered by: PC
Details logged to file: SWB-07.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	8	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	0	34	34
Other CDB's	61	1	62
Vendor Specific CDB's	0	80	80
Undefined CDB's.....	0	53	53

Testing device \\PhysicalDrive2
Device is software WRITE ENABLED

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

Testing device \\.\PhysicalDrive3
Device is software WRITE 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

SWB-07 Test result analysis

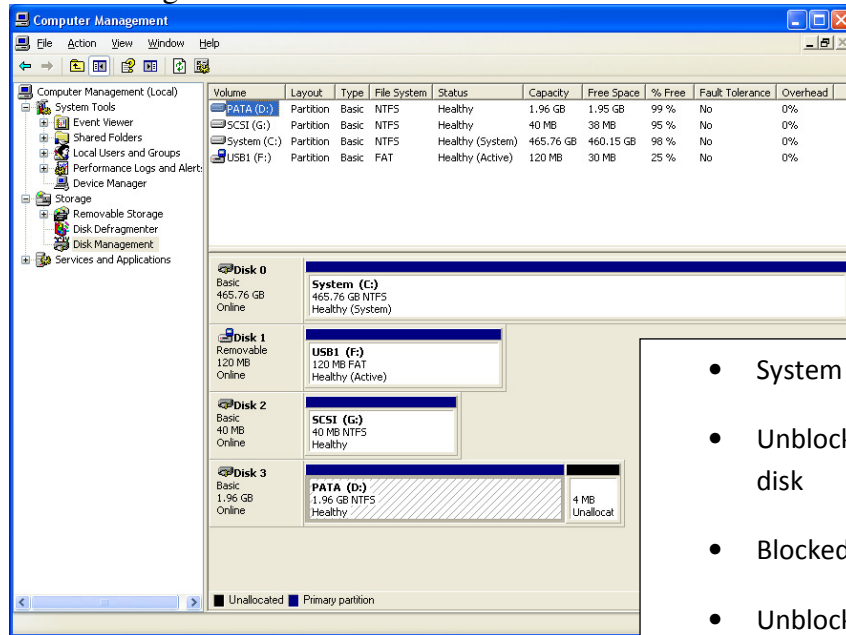
SAFE Block XP Version 1.1 had one unexpected result in this test – Variation 1 described in Section 2.1. Note that this is conservative blocking, which is generally considered good for forensics. Otherwise, all write commands were blocked to the protected disk and no commands were blocked on the unblocked disks.

7.8 Test Case SWB-08

This case tests SAFE Block XP V1.1's compliance with optional assertions SWB-AO-01 through SWB-AO-06. It issues all possible commands to a set of three drives protected with the pattern UPU. The expected result of this test is SAFE Block XP V1.1 will:

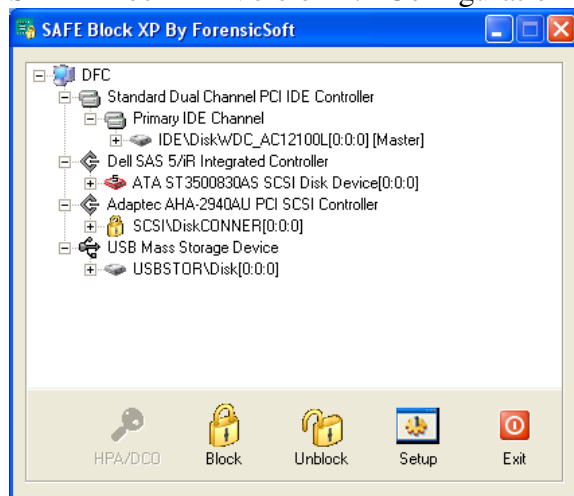
- Block all commands from the WRITE, VENDOR_SPECIFIC, and UNDEFINED categories issued to protected drives
- Pass all commands from the READ and OTHER categories issued to protected drives
- Pass all commands from all categories issued to unprotected drives

Drive Configuration



- System disk
- Unblocked USB disk
- Blocked SCSI
- Unblocked IDE

SAFE Block XP Version 1.1 Configuration



SHA-1 Hash Values

Before USB	8d4a759a29a99b9a5320d7b7f9a06fd288215d40
After USB	8d4a759a29a99b9a5320d7b7f9a06fd288215d40
Before SCSI	15565a3b4ebc6be0ddf2db76c453cf08687969e8
After SCSI	15565a3b4ebc6be0ddf2db76c453cf08687969e8
Before IDE	e2b40b714345e7d8af326eabe3881b43e16167de
After IDE	e2b40b714345e7d8af326eabe3881b43e16167de

NIST Software Write Blocker Test Suite V1.2 Output Summary

NIST Software Write Blocker Test Suite V1.2

Tue Jun 17 10:35:26 2008

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

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

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

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

Testing device \\.\PhysicalDrive2
Device is software WRITE PROTECTED

Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	0	8	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	0	34	34
Other CDB's	61	1	62
Vendor Specific CDB's	0	80	80
Undefined CDB's.....	0	53	53

Testing device \\.\PhysicalDrive3
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

SWB-08 Test result analysis

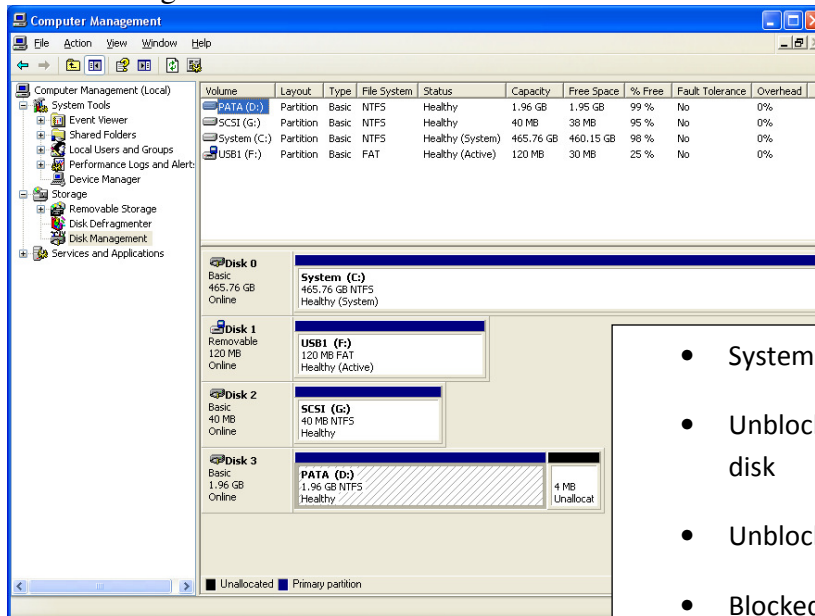
SAFE Block XP Version 1.1 had one unexpected result in this test – Variation 1 described in Section 2.1. Note that this is conservative blocking, which is generally considered good for forensics. Otherwise, all write commands were blocked to the protected disk and no commands were blocked on the unblocked disks.

7.9 Test Case SWB-09

This case tests SAFE Block XP V1.1's compliance with optional assertions SWB-AO-01 through SWB-AO-06. It issues all possible commands to a set of three drives protected with the pattern UUP. The expected result of this test is SAFE Block XP V1.1 will:

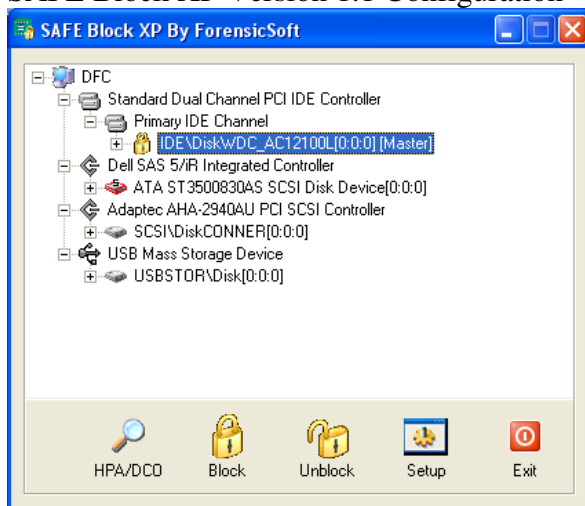
- Block all commands from the WRITE, VENDOR_SPECIFIC, and UNDEFINED categories issued to protected drives
- Pass all commands from the READ and OTHER categories issued to protected drives
- Pass all commands from all categories issued to unprotected drives

Drive Configuration



- System disk
- Unblocked USB disk
- Unblocked SCSI
- Blocked IDE

SAFE Block XP Version 1.1 Configuration



SHA-1 Hash Values

Before USB	8d4a759a29a99b9a5320d7b7f9a06fd288215d40
After USB	8d4a759a29a99b9a5320d7b7f9a06fd288215d40
Before SCSI	9b295f3c95b155876dc771aa69a61f6364f76c22
After SCSI	9b295f3c95b155876dc771aa69a61f6364f76c22
Before IDE	5ec2c4e7fce5d2954453271b2ec92d3d20da8f53
After IDE	5ec2c4e7fce5d2954453271b2ec92d3d20da8f53

NIST Software Write Blocker Test Suite V1.2 Output Summary

NIST Software Write Blocker Test Suite V1.2
Tue Jun 17 10:50:42 2008

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

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

Testing device \\PhysicalDrive1
Device is software WRITE ENABLED

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

Testing device \\PhysicalDrive2
Device is software WRITE ENABLED

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

Testing device \\.\PhysicalDrive3
Device is software WRITE PROTECTED

Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	0	8	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	0	34	34
Other CDB's	61	1	62
Vendor Specific CDB's	0	80	80
Undefined CDB's.....	0	53	53

SWB-09 Test result analysis

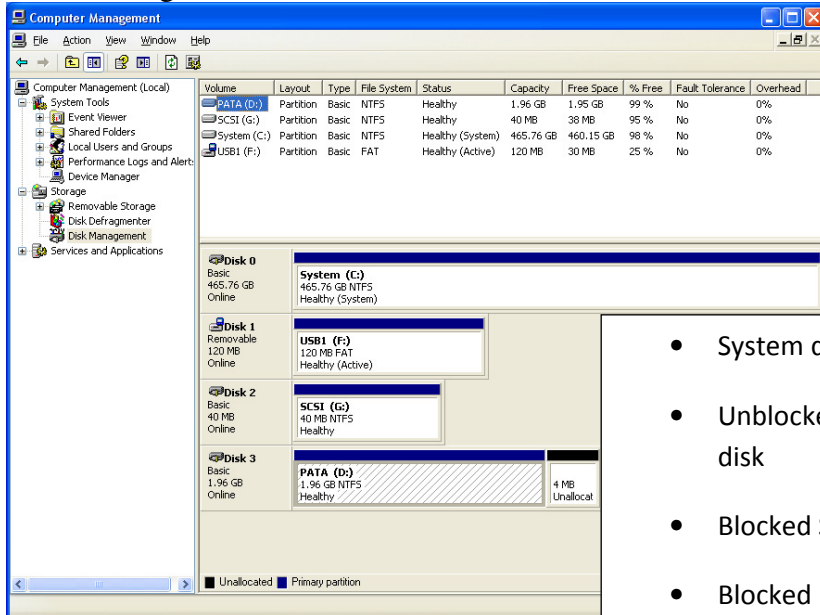
SAFE Block XP Version 1.1 had one unexpected result in this test – Variation 1 described in Section 2.1. Note that this is conservative blocking, which is generally considered good for forensics. Otherwise, all write commands were blocked to the protected disk and no commands were blocked on the unblocked disks.

7.10 Test Case SWB-10

This case tests SAFE Block XP V1.1's compliance with optional assertions SWB-AO-01 through SWB-AO-06. It issues all possible commands to a set of three drives protected with the pattern UPP. The expected result of this test is SAFE Block XP V1.1 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

Drive Configuration



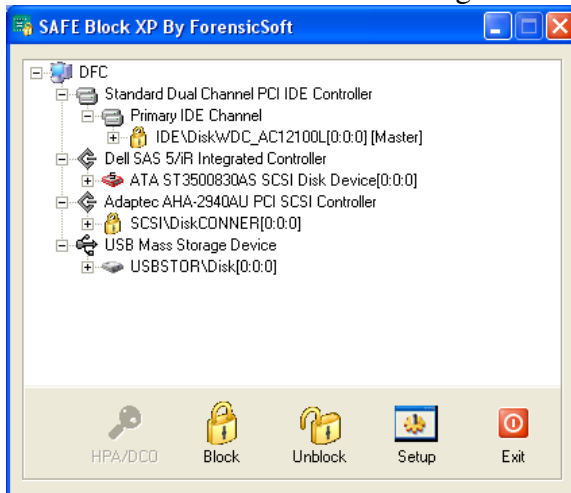
The screenshot shows the Windows Computer Management console. The 'Disk Management' section is expanded, displaying a list of disks and their partitions. The table below summarizes the data from the screenshot:

Volume	Layout	Type	File System	Status	Capacity	Free Space	% Free	Fault Tolerance	Overhead
PATA (D:) [C:]	Partition	Basic	NTFS	Healthy	1.96 GB	1.95 GB	99 %	No	0%
SCSI (G:) [E:]	Partition	Basic	NTFS	Healthy	40 MB	30 MB	95 %	No	0%
System (C:) [F:]	Partition	Basic	NTFS	Healthy (System)	465.76 GB	460.15 GB	98 %	No	0%
USB1 (F:) [H:]	Partition	Basic	FAT	Healthy (Active)	120 MB	30 MB	25 %	No	0%

Below the table, the disk layout is visualized. Disk 0 (465.76 GB) is the System disk (C:). Disk 1 (120 MB) is the USB disk (F:). Disk 2 (40 MB) is the SCSI disk (G:). Disk 3 (1.96 GB) is the PATA disk (D:). The legend indicates that the System disk, USB disk, and SCSI disk are 'Unlocked', while the PATA disk is 'Blocked'.

- System disk
- Unlocked USB disk
- Blocked SCSI
- Blocked IDE

SAFE Block XP Version 1.1 Configuration



The screenshot shows the 'SAFE Block XP By ForensicSoft' configuration window. The 'DFC' (Disk Filter Chain) is expanded, showing the following components:

- Standard Dual Channel PCI IDE Controller
 - Primary IDE Channel
 - IDE\Disk\WDC_AC12100L[0:0:0] [Master]
- Dell SAS 5/iR Integrated Controller
 - ATA ST3500830AS SCSI Disk Device[0:0:0]
- Adaptec AHA-2940AU PCI SCSI Controller
 - SCSI\Disk\CONNER[0:0:0]
- USB Mass Storage Device
 - USBSTOR\Disk[0:0:0]

At the bottom, there are five buttons: HPA/DCO, Block, Unblock, Setup, and Exit. The 'Block' button is highlighted, indicating that the selected drives are currently blocked.

SHA-1 Hash Values

Before USB	8d4a759a29a99b9a5320d7b7f9a06fd288215d40
After USB	8d4a759a29a99b9a5320d7b7f9a06fd288215d40
Before SCSI	3780054dacf3f07b5e08dcf08e3f770cbb2ac159
After SCSI	3780054dacf3f07b5e08dcf08e3f770cbb2ac159
Before IDE	e3d114d0ed64ea8a702e038df1f12ae0afa6122d
After IDE	e3d114d0ed64ea8a702e038df1f12ae0afa6122d

NIST Software Write Blocker Test Suite V1.2 Output Summary

NIST Software Write Blocker Test Suite V1.2

Tue Jun 17 11:03:50 2008

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

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

Testing device \\PhysicalDrive1

Device is software WRITE ENABLED

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

Testing device \\PhysicalDrive2

Device is software WRITE PROTECTED

Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	0	8	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	0	34	34
Other CDB's	61	1	62
Vendor Specific CDB's	0	80	80
Undefined CDB's	0	53	53

Testing device \\.\PhysicalDrive3
Device is software WRITE PROTECTED

Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	0	8	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	0	34	34
Other CDB's	61	1	62
Vendor Specific CDB's	0	80	80
Undefined CDB's.....	0	53	53

SWB-010 Test result analysis

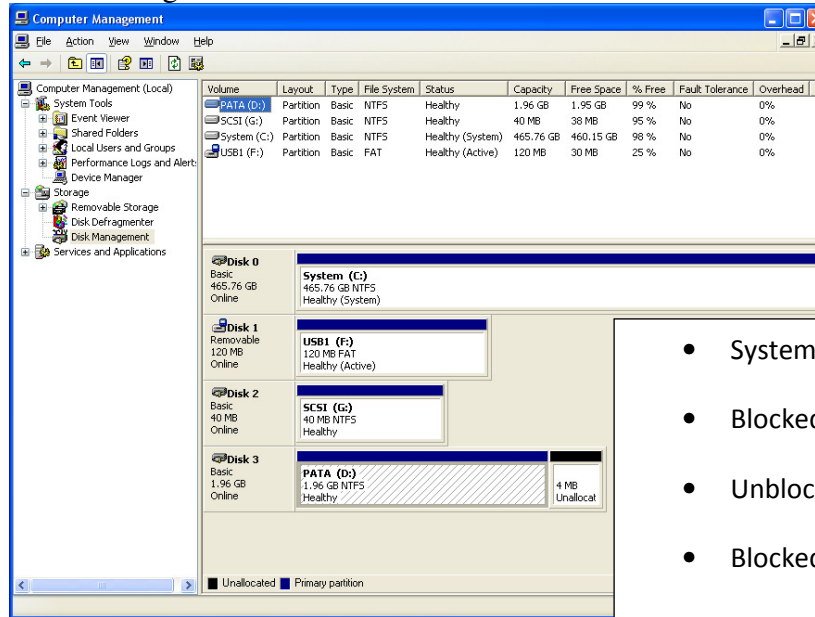
SAFE Block XP Version 1.1 had one unexpected result twice in this test – Variation 1 described in Section 2.1. Note that this is conservative blocking, which is generally considered good for forensics. Otherwise, all write commands were blocked to the protected disk and no commands were blocked on the unblocked disks.

7.11 Test Case SWB-11

This case tests SAFE Block XP V1.1's compliance with optional assertions SWB-AO-01 through SWB-AO-06. It issues all possible commands to a set of three drives protected with the pattern PUP. The expected result of this test is SAFE Block XP V1.1 will:

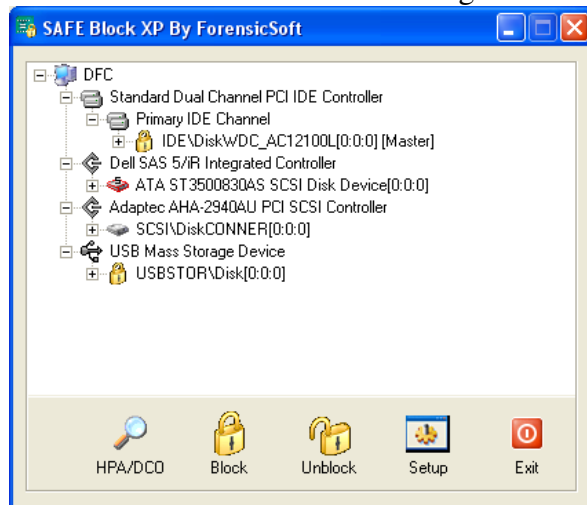
- Block all commands from the WRITE, VENDOR_SPECIFIC, and UNDEFINED categories issued to protected drives
- Pass all commands from the READ and OTHER categories issued to protected drives
- Pass all commands from all categories issued to unprotected drives

Drive Configuration



- System disk
- Blocked USB disk
- Unblocked SCSI
- Blocked IDE

SAFE Block XP Version 1.1 Configuration



SHA-1 Hash Values

Before USB	8d4a759a29a99b9a5320d7b7f9a06fd288215d40
After USB	8d4a759a29a99b9a5320d7b7f9a06fd288215d40
Before SCSI	16f4af461687e4e9eeea2c69bd797c594496e139
After SCSI	16f4af461687e4e9eeea2c69bd797c594496e139
Before IDE	75fd8b59c0645a2e9c1564e0dd98cfb168e2a5b8
After IDE	75fd8b59c0645a2e9c1564e0dd98cfb168e2a5b8

NIST Software Write Blocker Test Suite V1.2 Output Summary

NIST Software Write Blocker Test Suite V1.2

Tue Jun 17 11:16:34 2008

Test case: SWB-11
Command set: RWOVU
Number of drives: 3
Protection pattern: PUP
Test administered by: PC
Details logged to file: SWB-11.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	8	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	0	34	34
Other CDB's	61	1	62
Vendor Specific CDB's	0	80	80
Undefined CDB's	0	53	53

Testing device \\PhysicalDrive2

Device is software WRITE ENABLED

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

Testing device \\.\PhysicalDrive3			
Device is software WRITE PROTECTED			
Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	0	8	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	0	34	34
Other CDB's	61	1	62
Vendor Specific CDB's	0	80	80
Undefined CDB's.....	0	53	53

SWB-011 Test result analysis

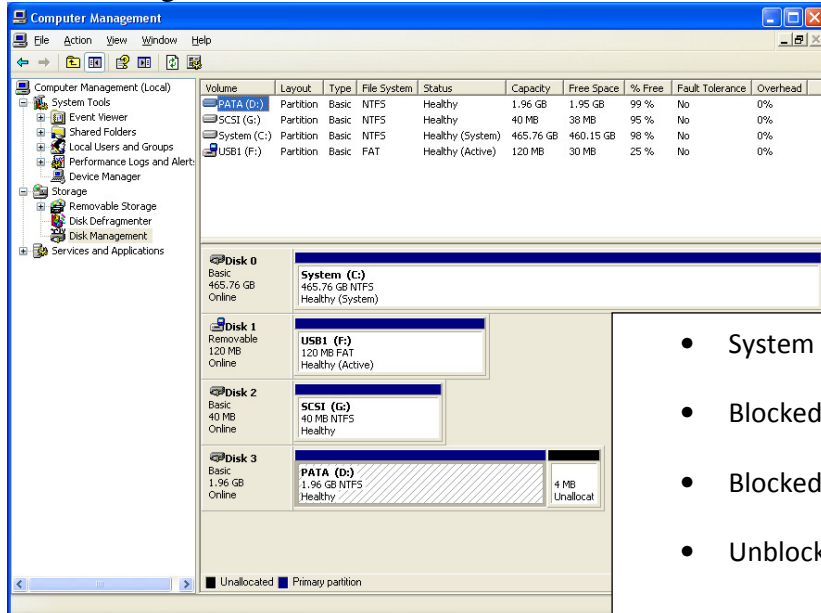
SAFE Block XP Version 1.1 had one unexpected result twice in this test – Variation 1 described in Section 2.1. Note that this is conservative blocking, which is generally considered good for forensics. Otherwise, all write commands were blocked to the protected disk and no commands were blocked on the unblocked disks.

7.12 Test Case SWB-12

This case tests SAFE Block XP V1.1's compliance with optional assertions SWB-AO-01 through SWB-AO-06. It issues all possible commands to a set of three drives protected with the pattern PPU. The expected result of this test is SAFE Block XP V1.1 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

Drive Configuration



The screenshot shows the Windows Computer Management console. The 'Storage' section is expanded, showing a list of disks and their partitions. The partitions are as follows:

Volume	Layout	Type	File System	Status	Capacity	Free Space	% Free	Fault Tolerance	Overhead
PATA (D:)	Partition	Basic	NTFS	Healthy	1.96 GB	1.95 GB	99 %	No	0%
SCSI (G:)	Partition	Basic	NTFS	Healthy	40 MB	30 MB	95 %	No	0%
System (C:)	Partition	Basic	NTFS	Healthy (System)	465.76 GB	460.15 GB	98 %	No	0%
USB1 (F:)	Partition	Basic	FAT	Healthy (Active)	120 MB	30 MB	25 %	No	0%

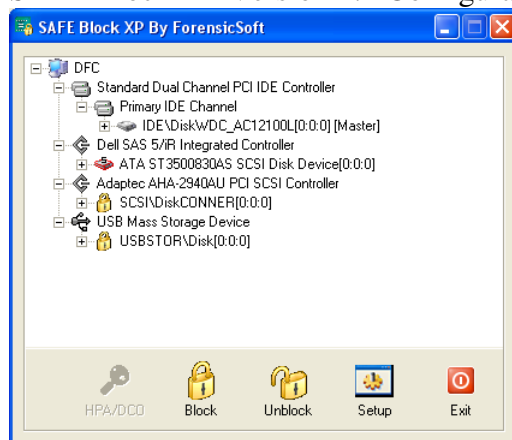
Below the table, the disk details are shown:

- Disk 0:** Basic, 465.76 GB, Online. Contains **System (C:)** (465.76 GB NTFS, Healthy (System)).
- Disk 1:** Removable, 120 MB, Online. Contains **USB1 (F:)** (120 MB FAT, Healthy (Active)).
- Disk 2:** Basic, 40 MB, Online. Contains **SCSI (G:)** (40 MB NTFS, Healthy).
- Disk 3:** Basic, 1.96 GB, Online. Contains **PATA (D:)** (1.96 GB NTFS, Healthy) and **4 MB Unallocated**.

Legend: ■ Unallocated ■ Primary partition

- System disk
- Blocked USB disk
- Blocked SCSI
- Unblocked IDE

SAFE Block XP Version 1.1 Configuration



SHA-1 Hash Values

Before USB	8d4a759a29a99b9a5320d7b7f9a06fd288215d40
After USB	8d4a759a29a99b9a5320d7b7f9a06fd288215d40
Before SCSI	c777efc1064c09bb2eda7df302ffc8fe5e5e8e1f
After SCSI	c777efc1064c09bb2eda7df302ffc8fe5e5e8e1f
Before IDE	830c1310c48045e0be371bb6724ee06f77cf4995
After IDE	830c1310c48045e0be371bb6724ee06f77cf4995

NIST Software Write Blocker Test Suite V1.2 Output Summary

NIST Software Write Blocker Test Suite V1.2

Tue Jun 17 11:28:48 2008

Test case: SWB-12
Command set: RWOVU
Number of drives: 3
Protection pattern: PPU
Test administered by: PC
Details logged to file: SWB-12.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	8	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	0	34	34
Other CDB's	61	1	62
Vendor Specific CDB's	0	80	80
Undefined CDB's.....	0	53	53

Testing device \\PhysicalDrive2

Device is software WRITE PROTECTED

Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	0	8	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	0	34	34
Other CDB's	61	1	62
Vendor Specific CDB's	0	80	80
Undefined CDB's.....	0	53	53

Testing device \\.\PhysicalDrive3
Device is software WRITE ENABLED

Test Category	Allowed	Blocked	Total
<hr/>			
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

SWB-012 Test result analysis

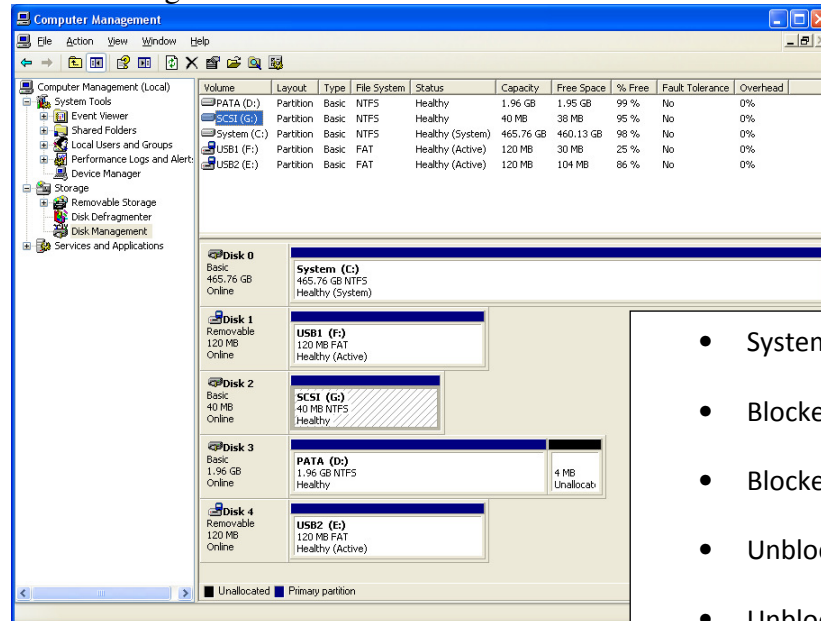
SAFE Block XP Version 1.1 had one unexpected result twice in this test – Variation 1 described in Section 2.1. Note that this is conservative blocking, which is generally considered good for forensics. Otherwise, all write commands were blocked to the protected disk and no commands were blocked on the unblocked disks.

7.13 Test Case SWB-13

This case tests SAFE Block XP V1.1's compliance with optional assertions SWB-AO-01 through SWB-AO-06. It issues all possible commands to a set of four drives protected with the pattern NOT_MIDDLE. The expected result of this test is SAFE Block XP V1.1 will:

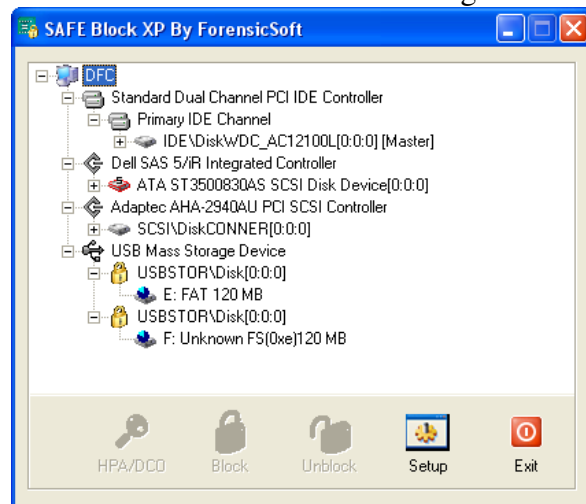
- Block all commands from the WRITE, VENDOR_SPECIFIC, and UNDEFINED categories issued to protected drives
- Pass all commands from the READ and OTHER categories issued to protected drives
- Pass all commands from all categories issued to unprotected drives

Drive Configuration



- System disk
- Blocked USB disk 1
- Blocked USB disk 2
- Unblocked SCSI
- Unblocked IDE

SAFE Block XP Version 1.1 Configuration



SHA-1 Hash Values

Before USB 1	8d4a759a29a99b9a5320d7b7f9a06fd288215d40
After USB 1	8d4a759a29a99b9a5320d7b7f9a06fd288215d40
Before SCSI	d11bfdd0071175d030015e9ceec97272e485074d
After SCSI	d11bfdd0071175d030015e9ceec97272e485074d
Before IDE	33e01a28a0ef29ebb6e06f646b515f4c4b3e28d5
After IDE	33e01a28a0ef29ebb6e06f646b515f4c4b3e28d5
Before USB 2	3424ac5ea2777220fcd694154bab6f3c3850eb93
After USB 2	3424ac5ea2777220fcd694154bab6f3c3850eb93

NIST Software Write Blocker Test Suite V1.2 Output Summary

NIST Software Write Blocker Test Suite V1.2

Tue Jun 17 12:09:23 2008

Test case: SWB-13
Command set: RWOVU
Number of drives: 4
Protection pattern: PUUP
Test administered by: PC
Details logged to file: SWB-13.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	8	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	0	34	34
Other CDB's	61	1	62
Vendor Specific CDB's	0	80	80
Undefined CDB's.....	0	53	53

Testing device \\PhysicalDrive2

Device is software WRITE ENABLED

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

Testing device \\.\PhysicalDrive3
Device is software WRITE 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	0	8	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	0	34	34
Other CDB's	61	1	62
Vendor Specific CDB's	0	80	80
Undefined CDB's.....	0	53	53

SWB-013 Test result analysis

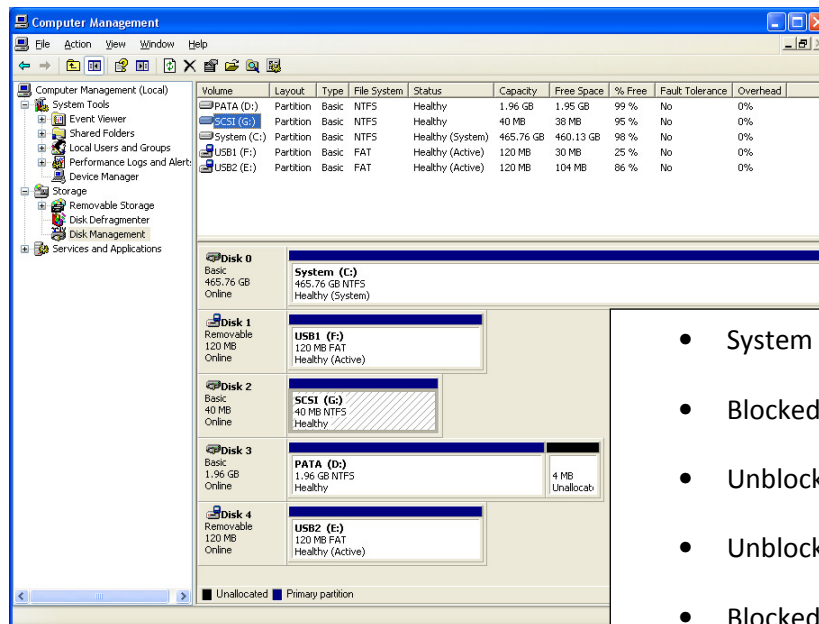
SAFE Block XP Version 1.1 had one unexpected result twice in this test – Variation 1 described in Section 2.1. Note that this is conservative blocking, which is generally considered good for forensics. Otherwise, all write commands were blocked to the protected disk and no commands were blocked to the unblocked disks.

7.14 Test Case SWB-14

This case tests SAFE Block XP V1.1's compliance with optional assertions SWB-AO-01 through SWB-AO-06. It issues all possible commands to a set of four drives protected with the pattern HIGH. The expected result of this test is SAFE Block XP V1.1 will:

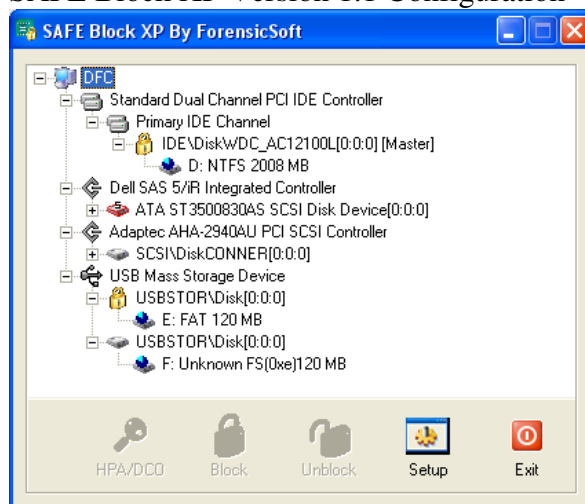
- Block all commands from the WRITE, VENDOR_SPECIFIC, and UNDEFINED categories issued to protected drives
- Pass all commands from the READ and OTHER categories issued to protected drives
- Pass all commands from all categories issued to unprotected drives

Drive Configuration



- System disk
- Blocked USB disk 1
- Unblocked USB disk 2
- Unblocked SCSI
- Blocked IDE

SAFE Block XP Version 1.1 Configuration



SHA-1 Hash Values

Before USB 1	8d4a759a29a99b9a5320d7b7f9a06fd288215d40
After USB 1	8d4a759a29a99b9a5320d7b7f9a06fd288215d40
Before SCSI	d11bfdd0071175d030015e9ceec97272e485074d
After SCSI	d11bfdd0071175d030015e9ceec97272e485074d
Before IDE	b0c02d76bbd3052c44c26d904fe6b79818dd11f3
After IDE	b0c02d76bbd3052c44c26d904fe6b79818dd11f3
Before USB 2	3424ac5ea2777220fcd694154bab6f3c3850eb93
After USB 2	3424ac5ea2777220fcd694154bab6f3c3850eb93

NIST Software Write Blocker Test Suite V1.2 Output Summary

NIST Software Write Blocker Test Suite V1.2
Tue Jun 17 12:22:31 2008

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

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

Testing device \\PhysicalDrive1
Device is software WRITE ENABLED

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

Testing device \\PhysicalDrive2
Device is software WRITE ENABLED

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

Testing device \\.\PhysicalDrive3
Device is software WRITE PROTECTED

Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	0	8	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	0	34	34
Other CDB's	61	1	62
Vendor Specific CDB's	0	80	80
Undefined CDB's.....	0	53	53

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

Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	0	8	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	0	34	34
Other CDB's	61	1	62
Vendor Specific CDB's	0	80	80
Undefined CDB's.....	0	53	53

SWB-014 Test result analysis

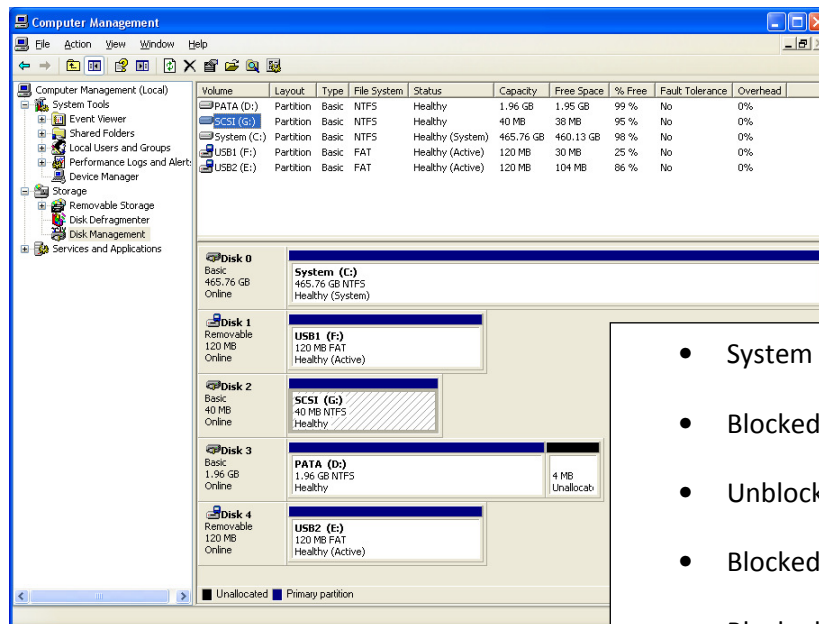
SAFE Block XP Version 1.1 had one unexpected result twice in this test – Variation 1 described in Section 2.1. Note that this is conservative blocking, which is generally considered good for forensics. Otherwise, all write commands were blocked to the protected disk and no commands were blocked to the unprotected disk.

7.15 Test Case SWB-15

This case tests SAFE Block XP V1.1's compliance with optional assertions SWB-AO-01 through SWB-AO-06. It issues all possible commands to a set of four drives protected with the pattern NOT_FIRST. The expected result of this test is SAFE Block XP V1.1 will:

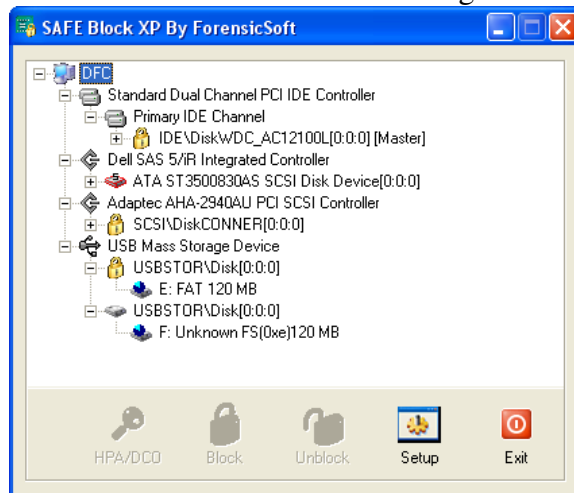
- Block all commands from the WRITE, VENDOR_SPECIFIC, and UNDEFINED categories issued to protected drives
- Pass all commands from the READ and OTHER categories issued to protected drives
- Pass all commands from all categories issued to unprotected drives

Drive Configuration



- System disk
- Blocked USB disk 1
- Unblocked USB disk 2
- Blocked SCSI
- Blocked IDE

SAFE Block XP Version 1.1 Configuration



SHA-1 Hash Values

Before USB 1	8d4a759a29a99b9a5320d7b7f9a06fd288215d40
After USB 1	8d4a759a29a99b9a5320d7b7f9a06fd288215d40
Before SCSI	97f16b28fad547842c5fdec1ea1711dad610b37a
After SCSI	97f16b28fad547842c5fdec1ea1711dad610b37a
Before IDE	c86242da0b0f5cd3b6a0f97d042a360720a9bd7f
After IDE	c86242da0b0f5cd3b6a0f97d042a360720a9bd7f
Before USB 2	3424ac5ea2777220fcd694154bab6f3c3850eb93
After USB 2	3424ac5ea2777220fcd694154bab6f3c3850eb93

NIST Software Write Blocker Test Suite V1.2 Output Summary

NIST Software Write Blocker Test Suite V1.2
Tue Jun 17 12:35:31 2008

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

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

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

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

Testing device \\.\PhysicalDrive2
Device is software WRITE PROTECTED

Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	0	8	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	0	34	34
Other CDB's	61	1	62
Vendor Specific CDB's	0	80	80
Undefined CDB's	0	53	53

Testing device \\.\PhysicalDrive3
Device is software WRITE PROTECTED

Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	0	8	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	0	34	34
Other CDB's	61	1	62
Vendor Specific CDB's	0	80	80
Undefined CDB's.....	0	53	53

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

Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	0	8	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	0	34	34
Other CDB's	61	1	62
Vendor Specific CDB's	0	80	80
Undefined CDB's.....	0	53	53

SWB-015 Test result analysis

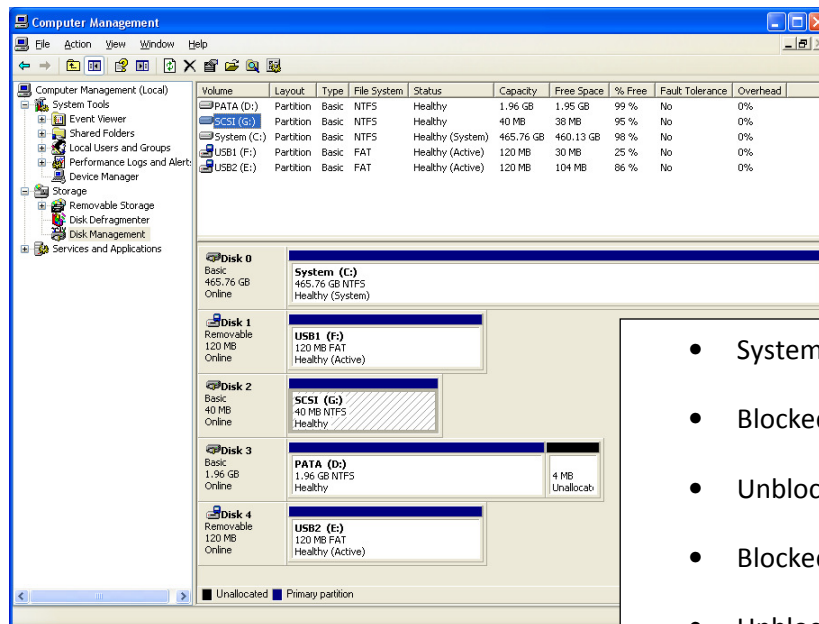
SAFE Block XP Version 1.1 had one unexpected result three times in this test – Variation 1 described in Section 2.1. Note that this is conservative blocking, which is generally considered good for forensics. Otherwise, all write commands were blocked to the protected disk and no commands were blocked to the unprotected disk.

7.16 Test Case SWB-16

This case tests SAFE Block XP V1.1's compliance with optional assertions SWB-AO-01 through SWB-AO-06. It issues all possible commands to a set of four drives protected with the pattern EVEN. The expected result of this test is SAFE Block XP V1.1 will:

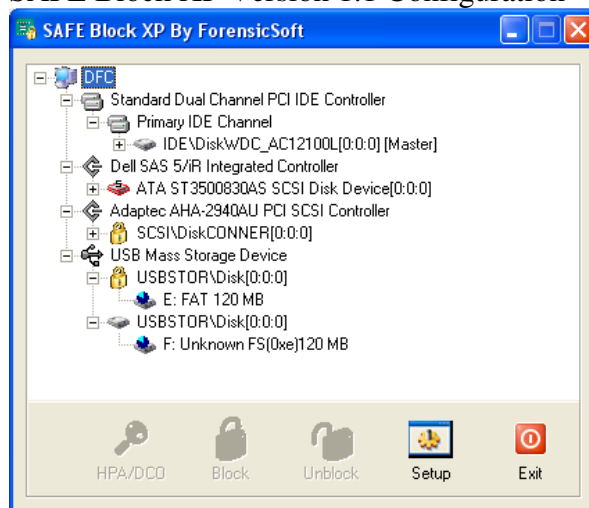
- Block all commands from the WRITE, VENDOR_SPECIFIC, and UNDEFINED categories issued to protected drives
- Pass all commands from the READ and OTHER categories issued to protected drives
- Pass all commands from all categories issued to unprotected drives

Drive Configuration



- System disk
- Blocked USB disk 1
- Unblocked USB disk 2
- Blocked SCSI
- Unblocked IDE

SAFE Block XP Version 1.1 Configuration



SHA-1 Hash Values

Before USB 1	1ee03a5e5c45f4c59db5060a50471fee8c3d6bdf
After USB 1	1ee03a5e5c45f4c59db5060a50471fee8c3d6bdf
Before SCSI	52854e406ac0edb5c7089ab87390b27634ae0dcb
After SCSI	52854e406ac0edb5c7089ab87390b27634ae0dcb
Before IDE	d0c63c21ea088e75be27099497a1c9a6e46113bc
After IDE	d0c63c21ea088e75be27099497a1c9a6e46113bc
Before USB 2	3424ac5ea2777220fcd694154bab6f3c3850eb93
After USB 2	3424ac5ea2777220fcd694154bab6f3c3850eb93

NIST Software Write Blocker Test Suite V1.2 Output Summary

NIST Software Write Blocker Test Suite V1.2
Tue Jun 17 12:56:41 2008

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

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

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

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

Testing device \\.\PhysicalDrive2
Device is software WRITE PROTECTED

Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	0	8	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	0	34	34
Other CDB's	61	1	62
Vendor Specific CDB's	0	80	80
Undefined CDB's	0	53	53

Testing device \\.\PhysicalDrive3
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	0	8	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	0	34	34
Other CDB's	61	1	62
Vendor Specific CDB's	0	80	80
Undefined CDB's.....	0	53	53

SWB-016 Test result analysis

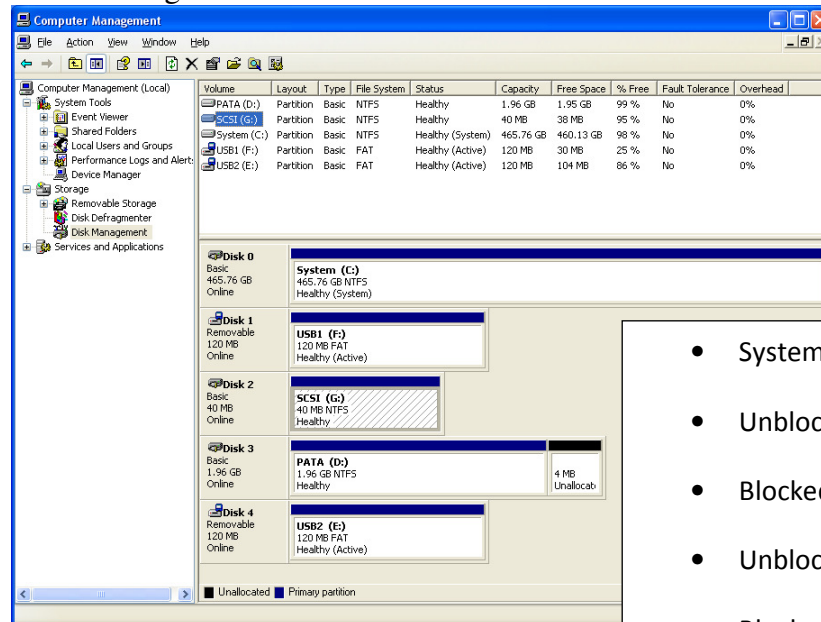
SAFE Block XP Version 1.1 had one unexpected result twice in this test – Variation 1 described in Section 2.1. Note that this is conservative blocking, which is generally considered good for forensics. Otherwise, all write commands were blocked to the protected disks and no commands were blocked to the unprotected disks.

7.17 Test Case SWB-17

This case tests SAFE Block XP V1.1's compliance with optional assertions SWB-AO-01 through SWB-AO-06. It issues all possible commands to a set of four drives protected with the pattern ODD. The expected result of this test is SAFE Block XP V1.1 will:

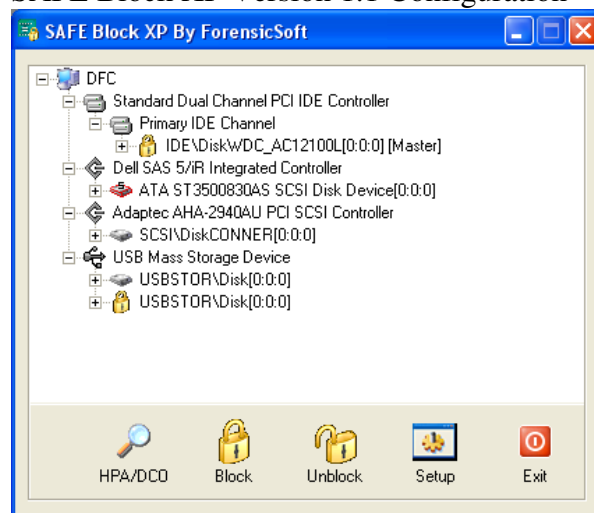
- Block all commands from the WRITE, VENDOR_SPECIFIC, and UNDEFINED categories issued to protected drives
- Pass all commands from the READ and OTHER categories issued to protected drives
- Pass all commands from all categories issued to unprotected drives

Drive Configuration



- System disk
- Unblocked USB disk 1
- Blocked USB disk 2
- Unblocked SCSI
- Blocked IDE

SAFE Block XP Version 1.1 Configuration



SHA-1 Hash Values

Before USB 1	8d4a759a29a99b9a5320d7b7f9a06fd288215d40
After USB 1	8d4a759a29a99b9a5320d7b7f9a06fd288215d40
Before SCSI	51c8292cce81e33df439ae0acf4c809d64fd08ac
After SCSI	51c8292cce81e33df439ae0acf4c809d64fd08ac
Before IDE	727332bd361aeac88c7daec37e2365642f9d0c05
After IDE	727332bd361aeac88c7daec37e2365642f9d0c05
Before USB 2	3424ac5ea2777220fcd694154bab6f3c3850eb93
After USB 2	3424ac5ea2777220fcd694154bab6f3c3850eb93

NIST Software Write Blocker Test Suite V1.2 Output Summary

NIST Software Write Blocker Test Suite V1.2
Tue Jun 17 13:06:57 2008

Test case: SWB-17
Command set: RWOVU
Number of drives: 4
Protection pattern: PUPU
Test administered by: PC
Details logged to file: SWB-17.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	8	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	0	34	34
Other CDB's	61	1	62
Vendor Specific CDB's	0	80	80
Undefined CDB's	0	53	53

Testing device \\.\PhysicalDrive2
Device is software WRITE ENABLED

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

Testing device \\.\PhysicalDrive3
 Device is software WRITE PROTECTED

Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	0	8	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	0	34	34
Other CDB's	61	1	62
Vendor Specific CDB's	0	80	80
Undefined CDB's.....	0	53	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

SWB-017 Test result analysis

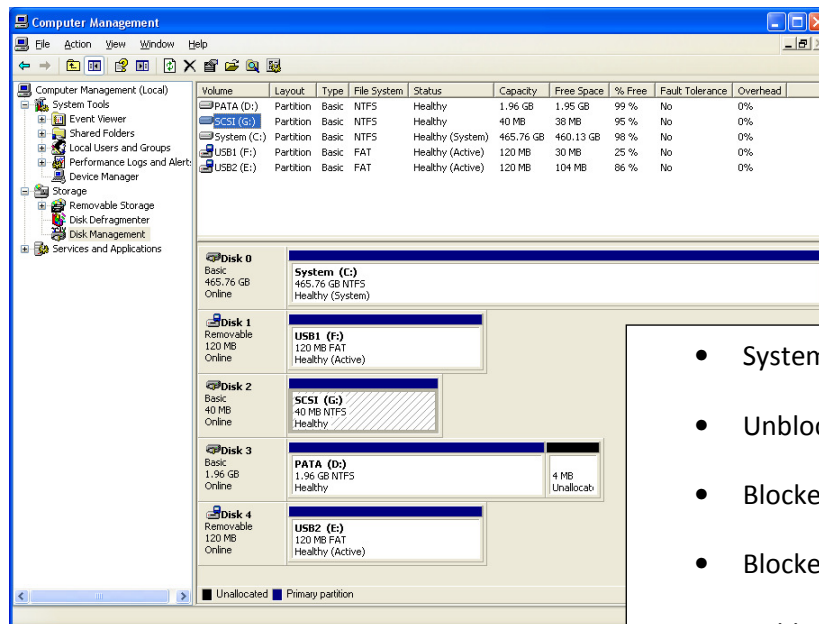
SAFE Block XP Version 1.1 had one unexpected result twice in this test – Variation 1 described in Section 2.1. Note that this is conservative blocking, which is generally considered good for forensics. Otherwise, all write commands were blocked to the protected disks and no commands were blocked to the unprotected disks.

7.18 Test Case SWB-18

This case tests SAFE Block XP V1.1's compliance with optional assertions SWB-AO-01 through SWB-AO-06. It issues all possible commands to a set of four drives protected with the pattern FIRST. The expected result of this test is SAFE Block XP V1.1 will:

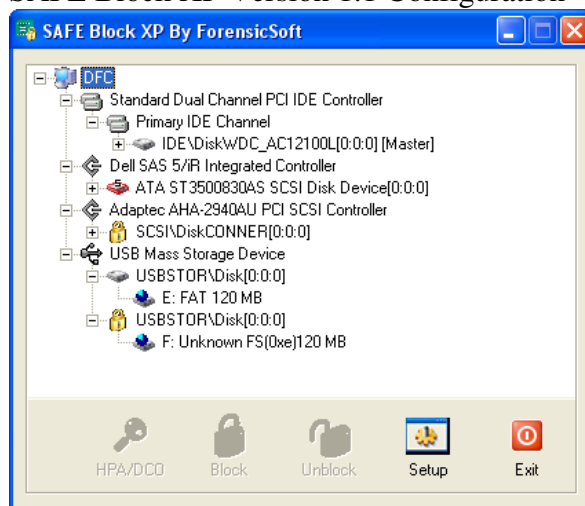
- Block all commands from the WRITE, VENDOR_SPECIFIC, and UNDEFINED categories issued to protected drives
- Pass all commands from the READ and OTHER categories issued to protected drives
- Pass all commands from all categories issued to unprotected drives

Drive Configuration



- System disk
- Unblocked USB disk 1
- Blocked USB disk 2
- Blocked SCSI
- Unblocked IDE

SAFE Block XP Version 1.1 Configuration



SHA-1 Hash Values

Before USB 1	1ee03a5e5c45f4c59db5060a50471fee8c3d6bdf
After USB 1	1ee03a5e5c45f4c59db5060a50471fee8c3d6bdf
Before SCSI	0ec8e25ab3ce5cb229b1a6a6c2190d65702f9e34
After SCSI	0ec8e25ab3ce5cb229b1a6a6c2190d65702f9e34
Before IDE	6071c4bff922c2d5503a388320056b274e114fc8
After IDE	6071c4bff922c2d5503a388320056b274e114fc8
Before USB 2	3424ac5ea2777220fcd694154bab6f3c3850eb93
After USB 2	3424ac5ea2777220fcd694154bab6f3c3850eb93

NIST Software Write Blocker Test Suite V1.2 Output Summary

NIST Software Write Blocker Test Suite V1.2
Tue Jun 17 13:18:27 2008

Test case: SWB-18
Command set: RWOVU
Number of drives: 4
Protection pattern: PPUU
Test administered by: PC
Details logged to file: SWB-18.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	8	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	0	34	34
Other CDB's	61	1	62
Vendor Specific CDB's	0	80	80
Undefined CDB's	0	53	53

Testing device \\.\PhysicalDrive2
Device is software WRITE PROTECTED

Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	0	8	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	0	34	34
Other CDB's	61	1	62
Vendor Specific CDB's	0	80	80
Undefined CDB's	0	53	53

Testing device \\.\PhysicalDrive3
 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

SWB-018 Test result analysis

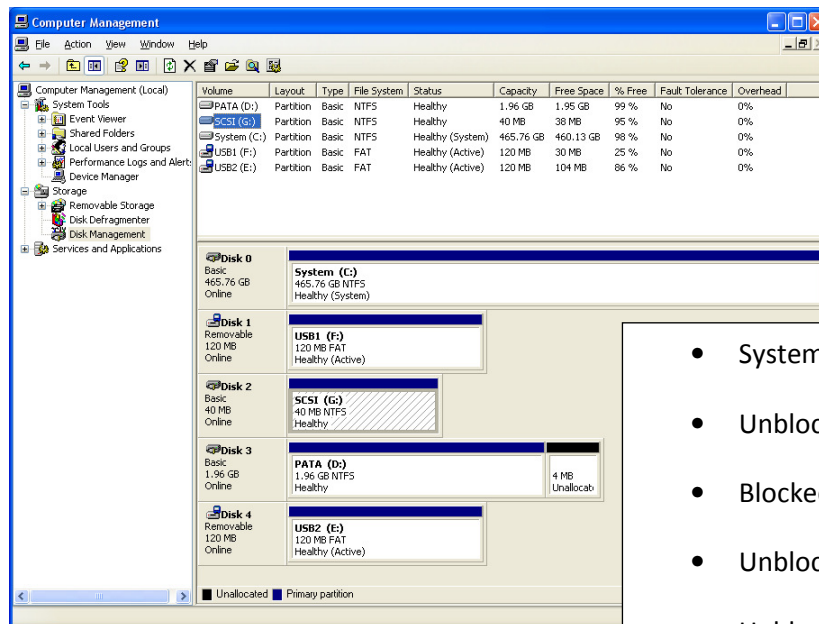
SAFE Block XP Version 1.1 had one unexpected result twice in this test – Variation 1 described in Section 2.1. Note that this is conservative blocking, which is generally considered good for forensics. Otherwise, all write commands were blocked to the protected disks and no commands were blocked to the unprotected disks.

7.19 Test Case SWB-19

This case tests SAFE Block XP V1.1's compliance with optional assertions SWB-AO-01 through SWB-AO-06. It issues all possible commands to a set of four drives protected with the pattern FIRST. The expected result of this test is SAFE Block XP V1.1 will:

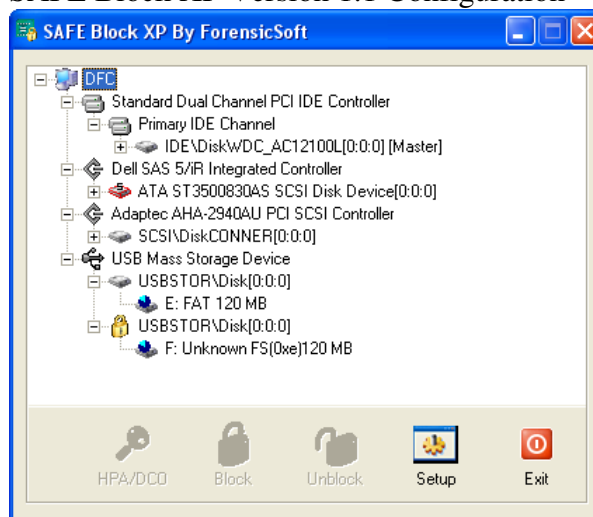
- Block all commands from the WRITE, VENDOR_SPECIFIC, and UNDEFINED categories issued to protected drives
- Pass all commands from the READ and OTHER categories issued to protected drives
- Pass all commands from all categories issued to unprotected drives

Drive Configuration



- System disk
- Unblocked USB disk 1
- Blocked USB disk 2
- Unblocked SCSI
- Unblocked IDE

SAFE Block XP Version 1.1 Configuration



SHA-1 Hash Values

Before USB 1	1ee03a5e5c45f4c59db5060a50471fee8c3d6bdf
After USB 1	1ee03a5e5c45f4c59db5060a50471fee8c3d6bdf
Before SCSI	355e7a794b51edeb4c23a8fea35205a6f4c3457e
After SCSI	355e7a794b51edeb4c23a8fea35205a6f4c3457e
Before IDE	6071c4bff922c2d5503a388320056b274e114fc8
After IDE	6071c4bff922c2d5503a388320056b274e114fc8
Before USB 2	3424ac5ea2777220fcd694154bab6f3c3850eb93
After USB 2	3424ac5ea2777220fcd694154bab6f3c3850eb93

NIST Software Write Blocker Test Suite V1.2 Output Summary

N IST Software Write Blocker Test Suite V1.2
Tue Jun 17 13:29:19 2008

Test case: SWB-19
Command set: RWOVU
Number of drives: 4
Protection pattern: PUUU
Test administered by: PC
Details logged to file: SWB-19.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	8	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	0	34	34
Other CDB's	61	1	62
Vendor Specific CDB's	0	80	80
Undefined CDB's.....	0	53	53

Testing device \\.\PhysicalDrive2
Device is software WRITE ENABLED

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

Testing device \\.\PhysicalDrive3
Device is software WRITE 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

SWB-019 Test result analysis

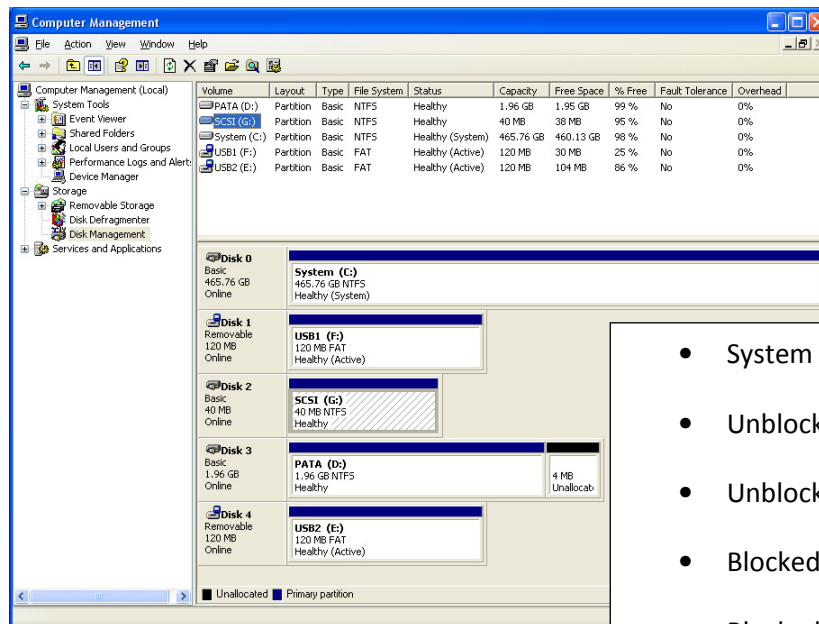
SAFE Block XP Version 1.1 had one unexpected result in this test – Variation 1 described in Section 2.1. Note that this is conservative blocking, which is generally considered good for forensics. Otherwise, all write commands were blocked to the protected disks and no commands were blocked to the unprotected disk.

7.20 Test Case SWB-20

This case tests SAFE Block XP V1.1's compliance with optional assertions SWB-AO-01 through SWB-AO-06. It issues all possible commands to a set of four drives protected with the pattern MIDDLE. The expected result of this test is SAFE Block XP V1.1 will:

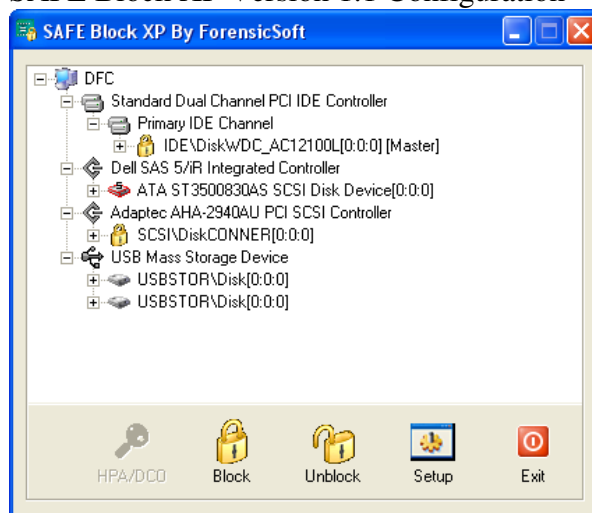
- Block all commands from the WRITE, VENDOR_SPECIFIC, and UNDEFINED categories issued to protected drives
- Pass all commands from the READ and OTHER categories issued to protected drives
- Pass all commands from all categories issued to unprotected drives

Drive Configuration



- System disk
- Unblocked USB disk 1
- Unblocked USB disk 2
- Blocked SCSI
- Blocked IDE

SAFE Block XP Version 1.1 Configuration



SHA-1 Hash Values

Before USB 1	1ee03a5e5c45f4c59db5060a50471fee8c3d6bdf
After USB 1	1ee03a5e5c45f4c59db5060a50471fee8c3d6bdf
Before SCSI	a8e28279edf82e5b7e0e0dbb27d635da62b4e98a
After SCSI	a8e28279edf82e5b7e0e0dbb27d635da62b4e98a
Before IDE	706eff40ffd59a55521a1e9c949567aa894dddb1
After IDE	706eff40ffd59a55521a1e9c949567aa894dddb1
Before USB 2	3424ac5ea2777220fcd694154bab6f3c3850eb93
After USB 2	3424ac5ea2777220fcd694154bab6f3c3850eb93

NIST Software Write Blocker Test Suite V1.2 Output Summary

NIST Software Write Blocker Test Suite V1.2
Tue Jun 17 13:40:02 2008

Test case: SWB-20
Command set: RWOVU
Number of drives: 4
Protection pattern: UPPU
Test administered by: PC
Details logged to file: SWB-20.log

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

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

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

Testing device \\.\PhysicalDrive2
Device is software WRITE PROTECTED

Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	0	8	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	0	34	34
Other CDB's	61	1	62
Vendor Specific CDB's	0	80	80
Undefined CDB's	0	53	53

Testing device \\.\PhysicalDrive3
Device is software WRITE PROTECTED

Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	0	8	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	0	34	34
Other CDB's	61	1	62
Vendor Specific CDB's	0	80	80
Undefined CDB's.....	0	53	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

SWB-020 Test result analysis

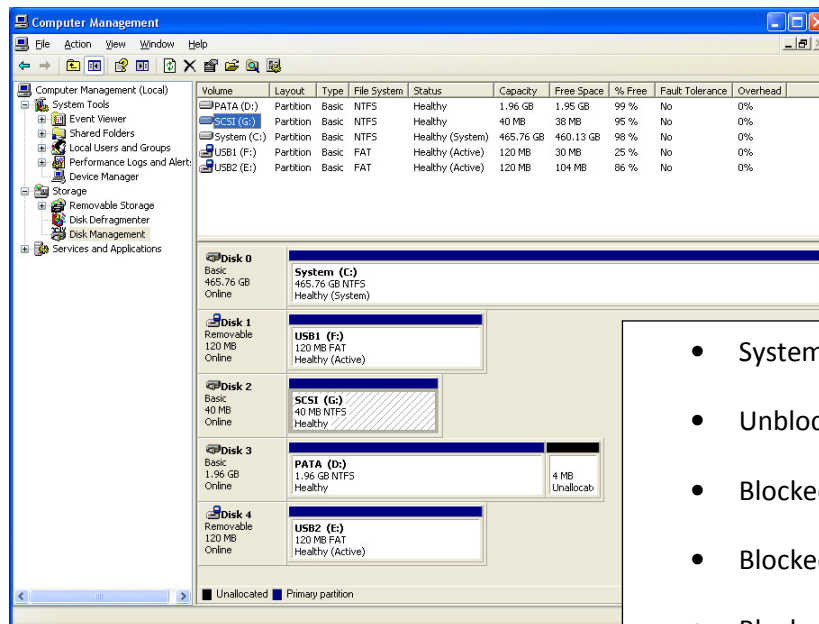
SAFE Block XP Version 1.1 had one unexpected result twice in this test – Variation 1 described in Section 2.1. Note that this is conservative blocking, which is generally considered good for forensics. Otherwise, all write commands were blocked to the protected disks and no commands were blocked to the unprotected disks.

7.21 Test Case SWB-21

This case tests SAFE Block XP V1.1's compliance with optional assertions SWB-AO-01 through SWB-AO-06. It issues all possible commands to a set of four drives protected with the pattern NOT_LAST. The expected result of this test is SAFE Block XP V1.1 will:

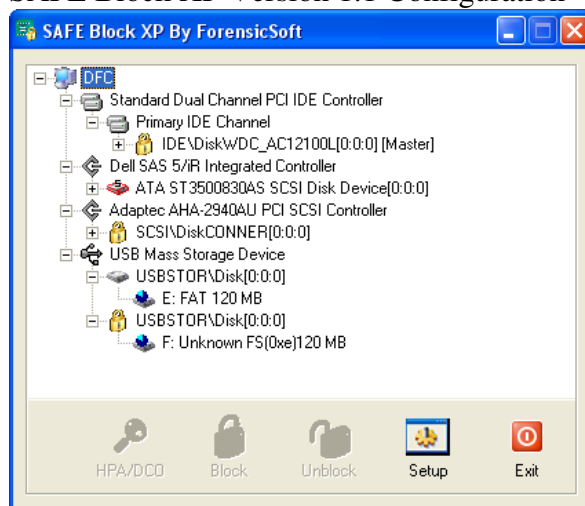
- Block all commands from the WRITE, VENDOR_SPECIFIC, and UNDEFINED categories issued to protected drives
- Pass all commands from the READ and OTHER categories issued to protected drives
- Pass all commands from all categories issued to unprotected drives

Drive Configuration



- System disk
- Unblocked USB disk 1
- Blocked USB disk 2
- Blocked SCSI
- Blocked IDE

SAFE Block XP Version 1.1 Configuration



SHA-1 Hash Values

Before USB 1	1ee03a5e5c45f4c59db5060a50471fee8c3d6bdf
After USB 1	1ee03a5e5c45f4c59db5060a50471fee8c3d6bdf
Before SCSI	f865eadcf33df57cc9dc82c259ebe31357722341
After SCSI	f865eadcf33df57cc9dc82c259ebe31357722341
Before IDE	7b7bf9786d64731040abd73016403caf760e7179
After IDE	7b7bf9786d64731040abd73016403caf760e7179
Before USB 2	3424ac5ea2777220fcd694154bab6f3c3850eb93
After USB 2	3424ac5ea2777220fcd694154bab6f3c3850eb93

NIST Software Write Blocker Test Suite V1.2 Output Summary

NIST Software Write Blocker Test Suite V1.2
Tue Jun 17 13:51:04 2008

Test case: SWB-21
Command set: RWOVU
Number of drives: 4
Protection pattern: PPPU
Test administered by: PC
Details logged to file: SWB-21.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	8	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	0	34	34
Other CDB's	61	1	62
Vendor Specific CDB's	0	80	80
Undefined CDB's.....	0	53	53

Testing device \\.\PhysicalDrive2
Device is software WRITE PROTECTED

Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	0	8	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	0	34	34
Other CDB's	61	1	62
Vendor Specific CDB's	0	80	80
Undefined CDB's.....	0	53	53

Testing device \\.\PhysicalDrive3
Device is software WRITE PROTECTED

Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	0	8	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	0	34	34
Other CDB's	61	1	62
Vendor Specific CDB's	0	80	80
Undefined CDB's.....	0	53	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

SWB-021 Test result analysis

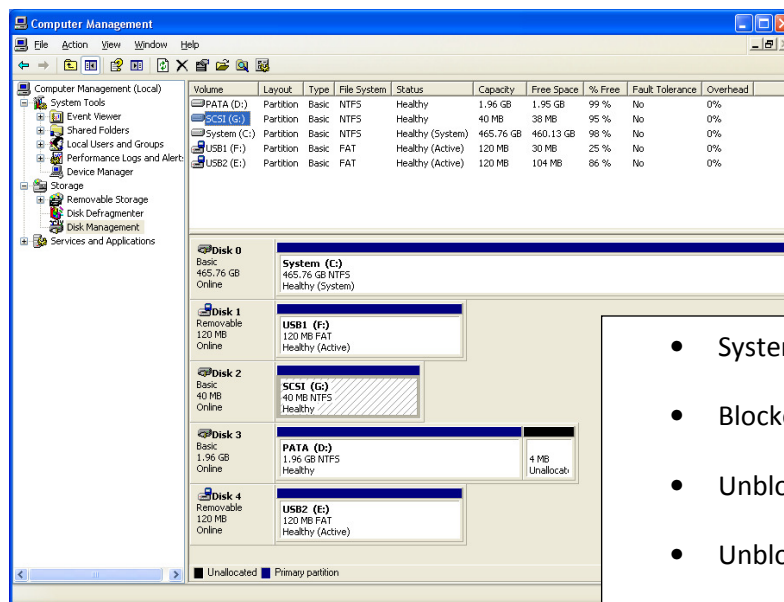
SAFE Block XP Version 1.1 had one unexpected result three times in this test – Variation 1 described in Section 2.1. Note that this is conservative blocking, which is generally considered good for forensics. Otherwise, all write commands were blocked to the protected disks and no commands were blocked to the unprotected disk.

7.22 Test Case SWB-22

This case tests SAFE Block XP V1.1's compliance with optional assertions SWB-AO-01 through SWB-AO-06. It issues all possible commands to a set of four drives protected with the pattern LAST. The expected result of this test is SAFE Block XP V1.1 will:

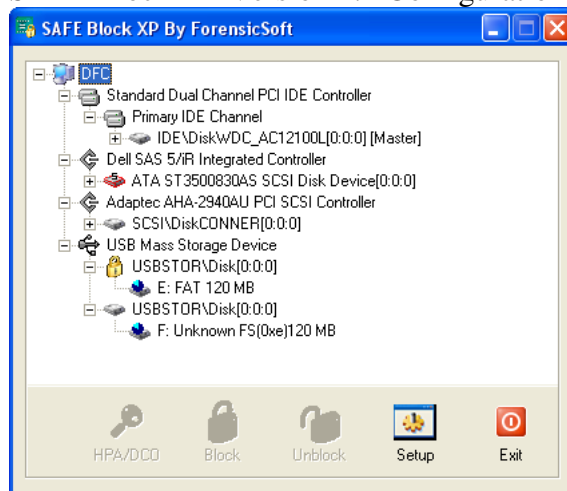
- Block all commands from the WRITE, VENDOR_SPECIFIC, and UNDEFINED categories issued to protected drives
- Pass all commands from the READ and OTHER categories issued to protected drives
- Pass all commands from all categories issued to unprotected drives

Drive Configuration



- System disk
- Blocked USB disk 1
- Unblocked USB disk 2
- Unblocked SCSI
- Unblocked IDE

SAFE Block XP Version 1.1 Configuration



SHA-1 Hash Values

Before USB 1	1ee03a5e5c45f4c59db5060a50471fee8c3d6bdf
After USB 1	1ee03a5e5c45f4c59db5060a50471fee8c3d6bdf
Before SCSI	7e4206eb3d9f22702638b07f5b8f308670c1a8ec
After SCSI	78ee07c6a66faa80c00c92328de3f03d6efd0711
Before IDE	51b99d344a97ddbfe9355fb10480bff687effcdd
After IDE	de0e9e62c81988a8a284880eeee5c2fbe2e39c70
Before USB 2	3424ac5ea2777220fcd694154bab6f3c3850eb93
After USB 2	3424ac5ea2777220fcd694154bab6f3c3850eb93

NIST Software Write Blocker Test Suite V1.2 Output Summary

NIST Software Write Blocker Test Suite V1.2
Tue Jun 17 14:02:21 2008

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

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

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

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

Testing device \\.\PhysicalDrive2
Device is software WRITE ENABLED

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

Testing device \\.\PhysicalDrive3
Device is software WRITE 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	0	8	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	0	34	34
Other CDB's	61	1	62
Vendor Specific CDB's	0	80	80
Undefined CDB's.....	0	53	53

SWB-022 Test result analysis

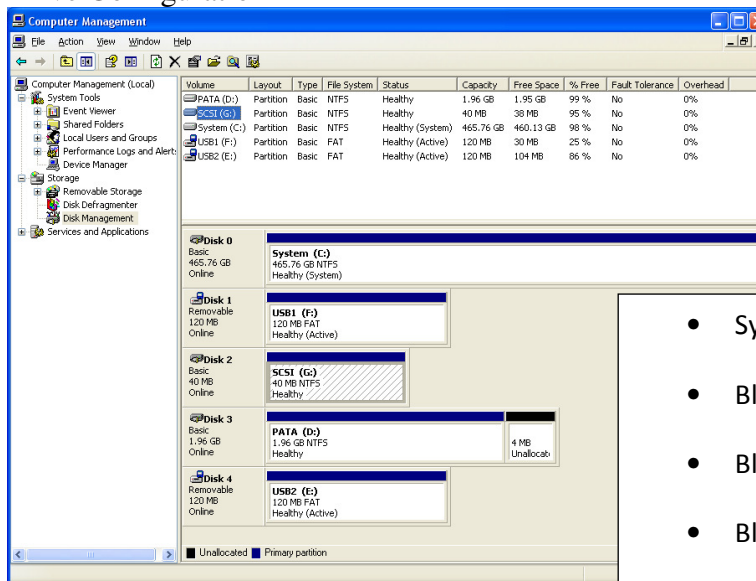
SAFE Block XP Version 1.1 had one unexpected result in this test – Variation 1 described in Section 2.1. Note that this is conservative blocking, which is generally considered good for forensics. Otherwise, all write commands were blocked to the protected disk and no commands were blocked to the unprotected disks.

7. 23 Test Case SWB-23

This case tests SAFE Block XP V1.1's compliance with optional assertions SWB-AO-01 through SWB-AO-08. It is run using the BOOT protocol, in which all configured drives are protected, the system is rebooted and all possible commands issued to all drives. The expected result of this test is SAFE Block XP V1.1 will:

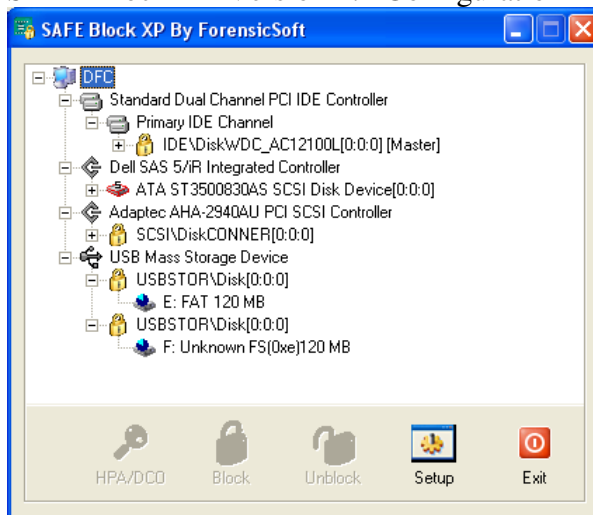
- Block all commands from the WRITE, VENDOR_SPECIFIC, and UNDEFINED categories issued to protected drives
- Pass all commands from the READ and OTHER categories issued to protected drives
- Pass all commands from all categories issued to unprotected drives
- Display a message indicating each command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

Drive Configuration



- System disk
- Blocked USB disk 1
- Blocked USB disk 2
- Blocked SCSI
- Blocked IDE

SAFE Block XP Version 1.1 Configuration



SHA-1 Hash Values

Before USB 1	1ee03a5e5c45f4c59db5060a50471fee8c3d6bdf
After USB 1	1ee03a5e5c45f4c59db5060a50471fee8c3d6bdf
Before SCSI	af19e2cc2a203a56a921893521472f22d1968109
After SCSI	af19e2cc2a203a56a921893521472f22d1968109
Before IDE	6b17ad14d7843475d7623b3fb89e46cede9f5fc0
After IDE	6b17ad14d7843475d7623b3fb89e46cede9f5fc0
Before USB 2	3424ac5ea2777220fcd694154bab6f3c3850eb93
After USB 2	3424ac5ea2777220fcd694154bab6f3c3850eb93

NIST Software Write Blocker Test Suite V1.2 Output Summary

NIST Software Write Blocker Test Suite V1.2
Tue Jun 17 14:14:58 2008

Test case: SWB-23
Command set: RWOVU
Number of drives: 4
Protection pattern: PPPP
Test administered by: PC
Details logged to file: SWB-23.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	8	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	0	34	34
Other CDB's	61	1	62
Vendor Specific CDB's	0	80	80
Undefined CDB's	0	53	53

Testing device \\.\PhysicalDrive2
Device is software WRITE PROTECTED

Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	0	8	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	0	34	34
Other CDB's	61	1	62
Vendor Specific CDB's	0	80	80
Undefined CDB's	0	53	53

Testing device \\.\PhysicalDrive3
Device is software WRITE PROTECTED

Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	0	8	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	0	34	34
Other CDB's	61	1	62
Vendor Specific CDB's	0	80	80
Undefined CDB's.....	0	53	53

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

Test Category	Allowed	Blocked	Total
Read IRP's	4	0	4
Write IRP's	0	8	8
Other IRP's	15	0	15
Read CDB's	27	0	27
Write CDB's	0	34	34
Other CDB's	61	1	62
Vendor Specific CDB's	0	80	80
Undefined CDB's.....	0	53	53

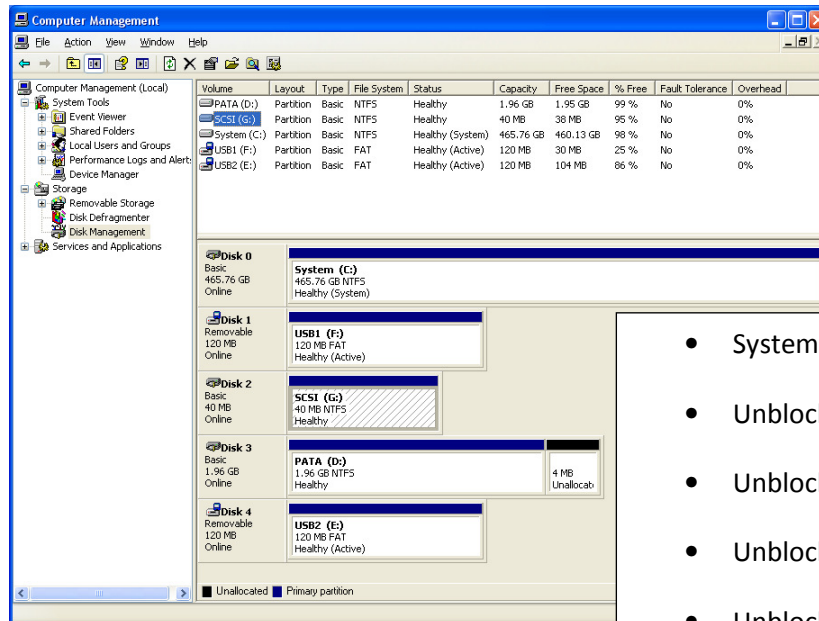
SWB-023 Test result analysis

SAFE Block XP Version 1.1 had one unexpected result four times in this test – Variation 1 described in Section 2.1. Note that this is conservative blocking, which is generally considered good for forensics. Otherwise, all write commands were blocked to the protected disks.

7.24 Test Case SWB-24

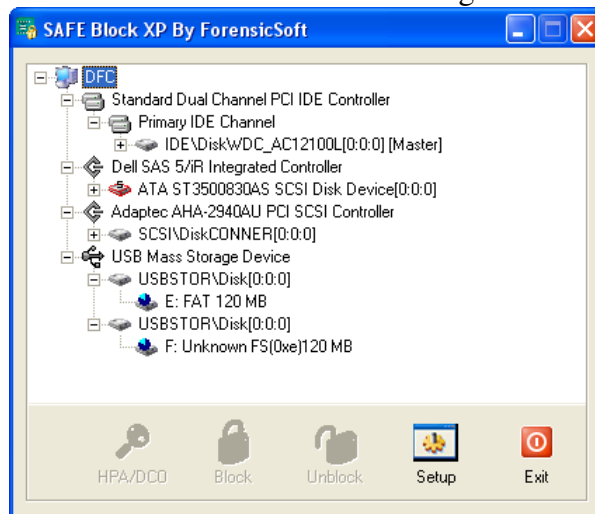
This case tests SAFE Block XP V1.1's compliance with mandatory assertions SWB-MO-03 through SWB-MO-09 and optional assertion SWB-AO-07. It is run using the UNINSTALL protocol, in which SAFE Block XP V1.1 is de-installed, the system is rebooted and all possible commands are issued to all drives. The expected result of this test is that commands from any category will not be blocked for any drive.

Drive Configuration



- System disk
- Unblocked USB disk 1
- Unblocked USB disk 2
- Unblocked SCSI
- Unblocked IDE

SAFE Block XP Version 1.1 Configuration



SHA-1 Hash Values

Before USB 1	1ee03a5e5c45f4c59db5060a50471fee8c3d6bdf
After USB 1	1ee03a5e5c45f4c59db5060a50471fee8c3d6bdf
Before SCSI	d7c4ecbbfec2a88e1194fdf124c082d4f243caec
After SCSI	d7c4ecbbfec2a88e1194fdf124c082d4f243caec
Before IDE	5acbe73935894f091ca07fa108bc2ac46438ea5c
After IDE	5acbe73935894f091ca07fa108bc2ac46438ea5c
Before USB 2	3424ac5ea2777220fcd694154bab6f3c3850eb93
After USB 2	3424ac5ea2777220fcd694154bab6f3c3850eb93

NIST Software Write Blocker Test Suite V1.2 Output Summary

NIST Software Write Blocker Test Suite V1.2
Tue Jun 17 14:24:57 2008

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

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

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

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

Testing device \\.\PhysicalDrive2
Device is software WRITE ENABLED

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

Testing device \\.\PhysicalDrive3
Device is software WRITE 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

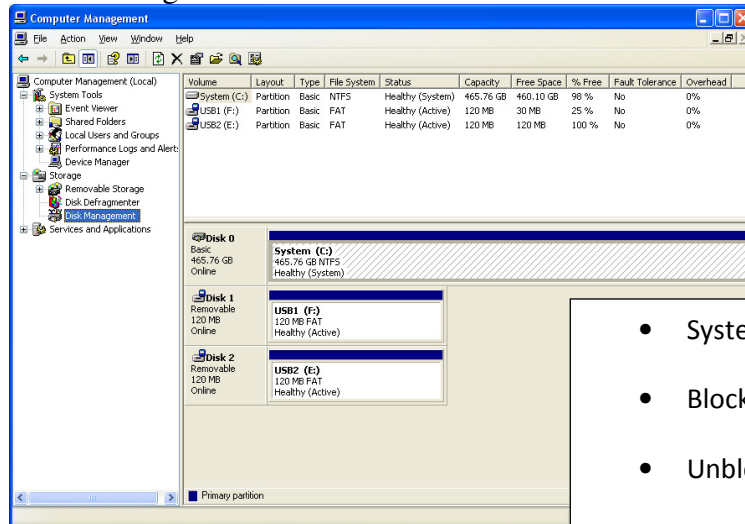
SWB-024 Test result analysis

SAFE Block XP Version 1.1 performed correctly - all commands were issued and allowed on the unprotected disks.

7.25 Test Case SWB-25

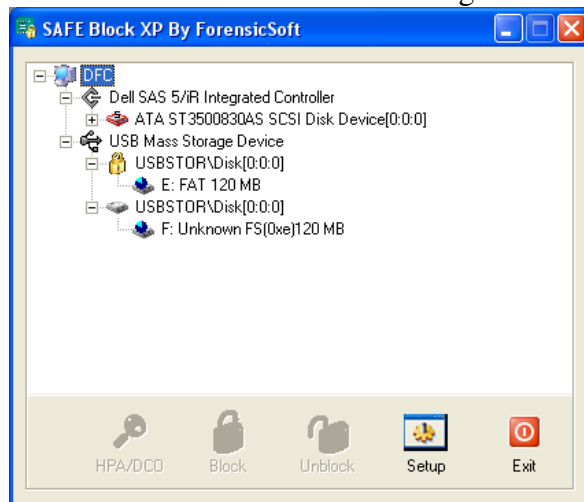
This case tests SAFE Block XP V1.1's compliance with mandatory assertion SWB-AM-10. The expected result of this test is that the IMAGE operation will fail with an I/O error and the disk hash of the test disk will be unchanged by the test.

Drive Configuration



- System disk
- Blocked USB disk 1
- Unblocked USB disk 2

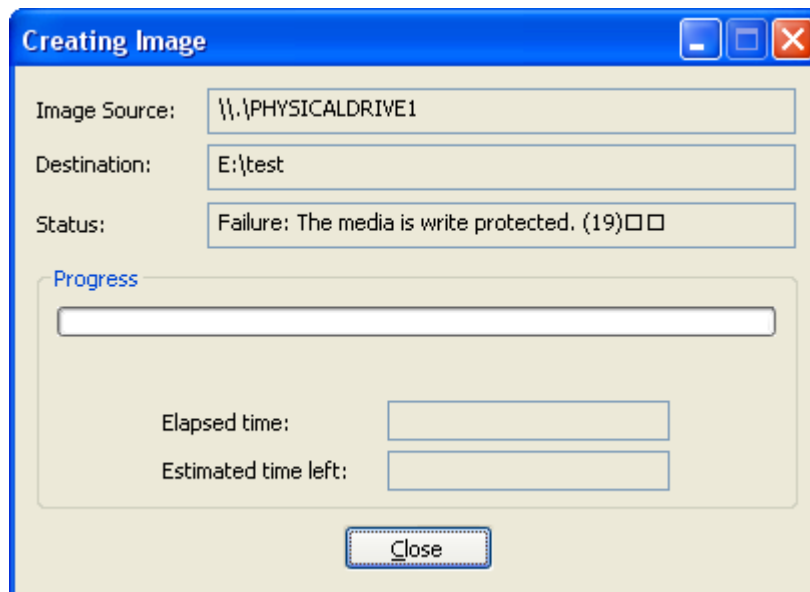
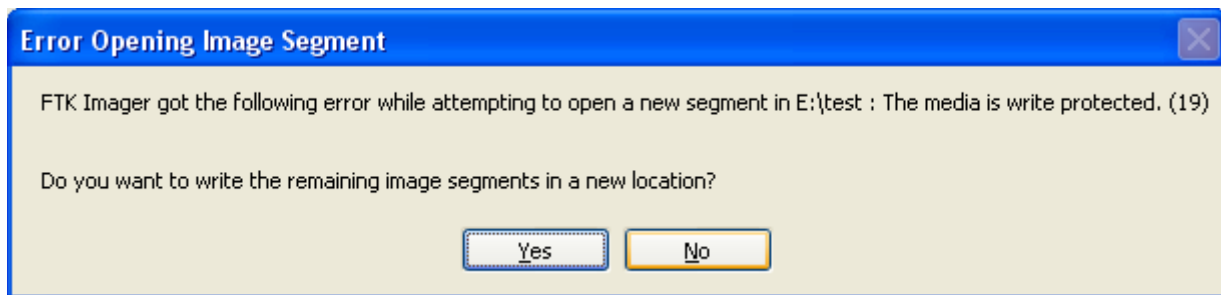
SAFE Block XP Version 1.1 Configuration



SHA-1 Hash Values

Before USB 1	0043d9207b826f30783b98290f9542cb235a291a
After USB 1	0043d9207b826f30783b98290f9542cb235a291a
Before USB 2	3424ac5ea2777220fcd694154bab6f3c3850eb93
After USB 2	3424ac5ea2777220fcd694154bab6f3c3850eb93

Output of imaging



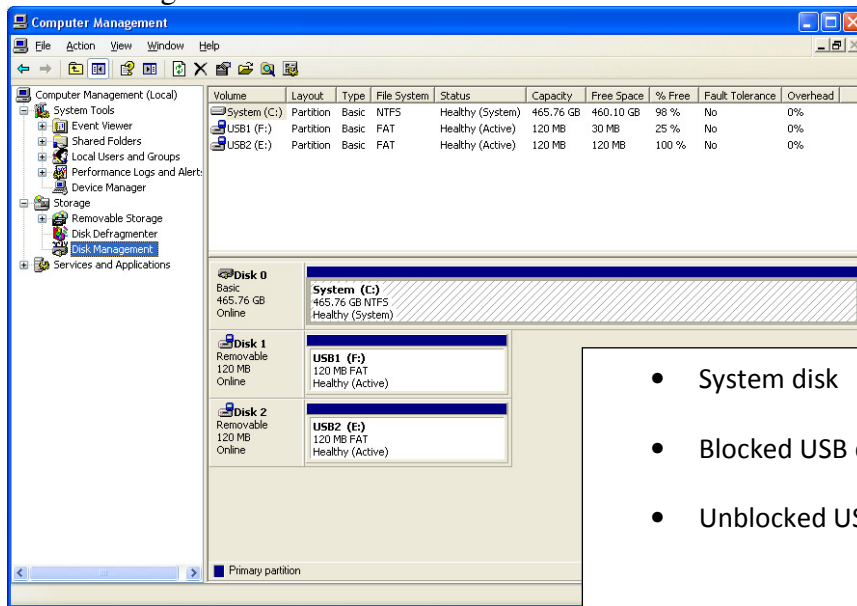
SWB-025 Test result analysis

SAFE Block XP Version 1.1 performed correctly - the image operation failed and the hashes did not change.

7.26 Test Case SWB-26

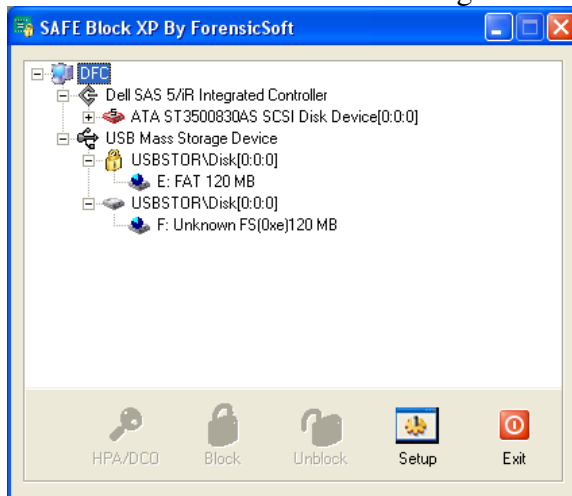
This case tests SAFE Block XP V1.1's compliance with mandatory assertion SWB-AM-10 and optional assertion SWBAO-08. The expected result of this test is that the ACQUIRE operation will fail with an I/O error, and the disk hash of the test disk will be unchanged by the test.

Drive Configuration



- System disk
- Blocked USB disk 1
- Unblocked USB disk 2

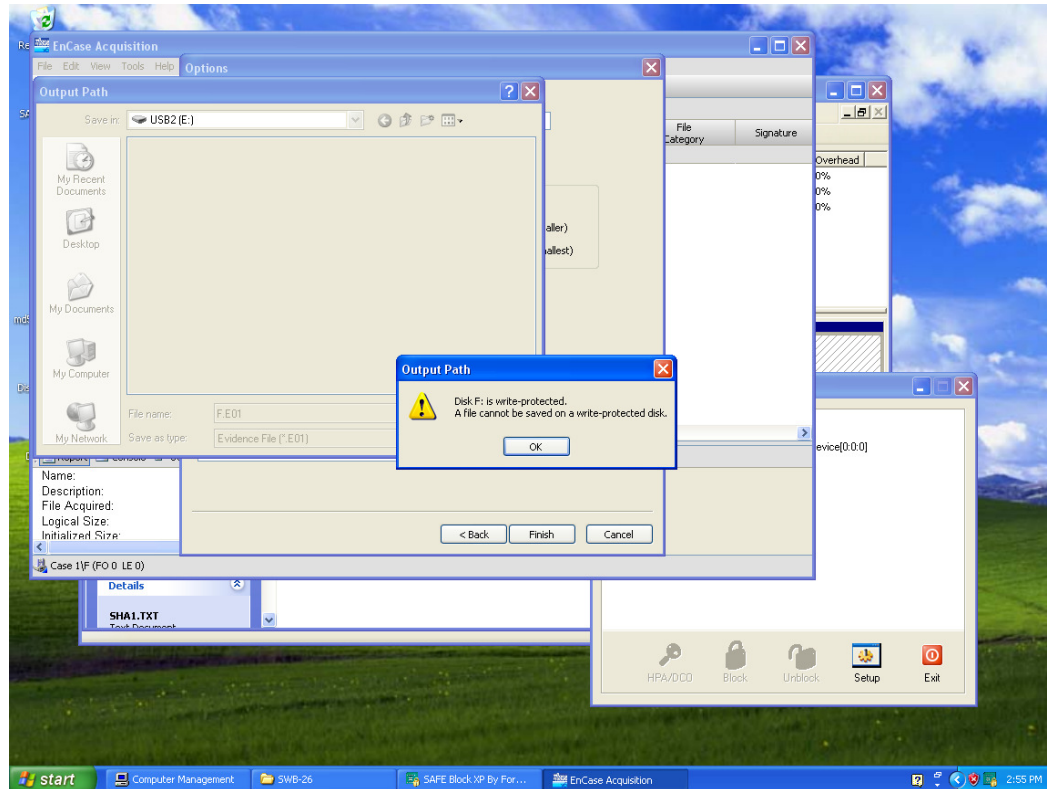
SAFE Block XP Version 1.1 Configuration



SHA-1 Hash Values

Before USB 1	0043d9207b826f30783b98290f9542cb235a291a
After USB 1	0043d9207b826f30783b98290f9542cb235a291a
Before USB 2	3424ac5ea2777220fcd694154bab6f3c3850eb93
After USB 2	3424ac5ea2777220fcd694154bab6f3c3850eb93

Output



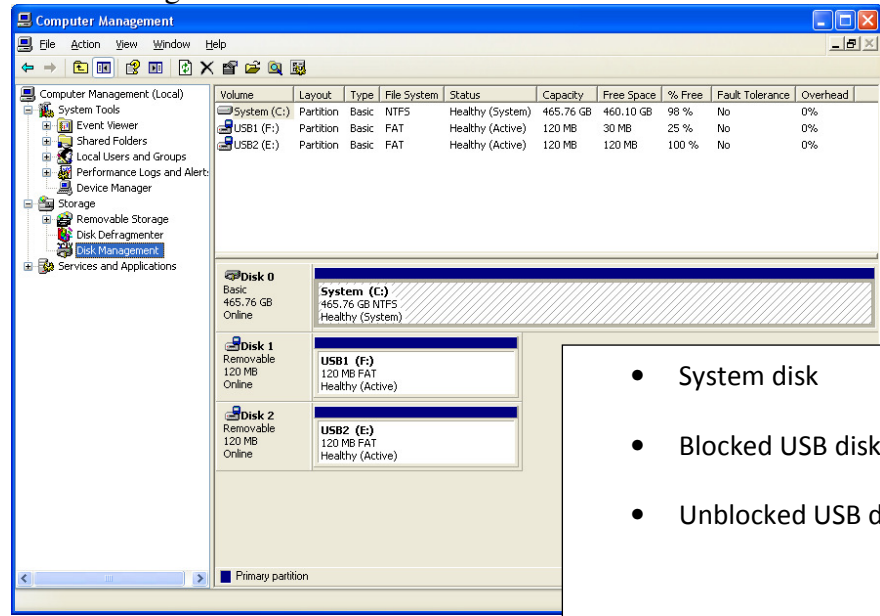
SWB-026 Test result analysis

SAFE Block XP Version 1.1 performed correctly - the operation failed and the hashes did not change.

7.27 Test Case SWB-27

This case tests SAFE Block XP V1.1's compliance with assertion SWB-AM-10. It is run using the typical protocol. The expected result of this test is that the COPY command will fail with an error message, and the hash value of the target disk will be unchanged after the test.

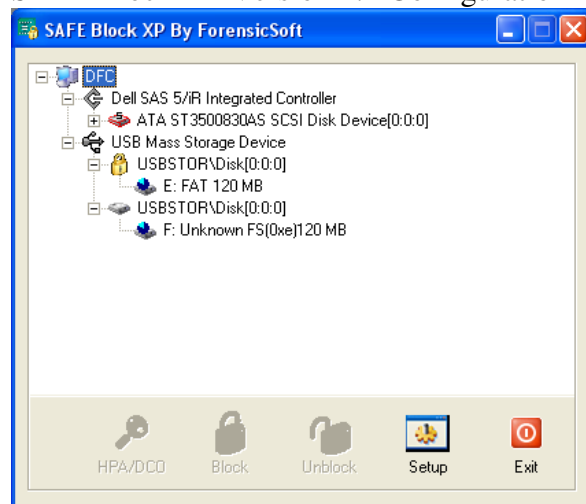
Drive Configuration



Volume	Layout	Type	File System	Status	Capacity	Free Space	% Free	Fault Tolerance	Overhead
System (C:)	Partition	Basic	NTFS	Healthy (System)	465.76 GB	460.10 GB	98 %	No	0%
USB1 (F:)	Partition	Basic	FAT	Healthy (Active)	120 MB	30 MB	25 %	No	0%
USB2 (E:)	Partition	Basic	FAT	Healthy (Active)	120 MB	120 MB	100 %	No	0%

- System disk
- Blocked USB disk 1
- Unblocked USB disk 2

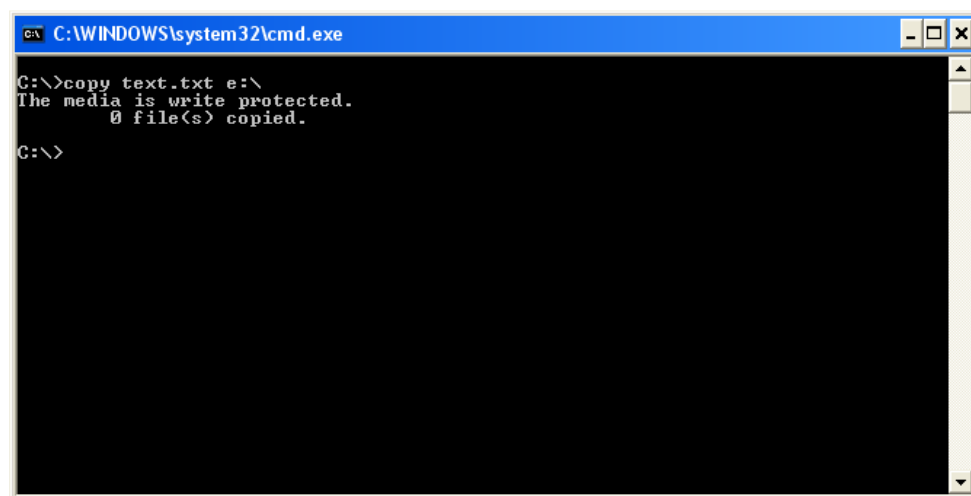
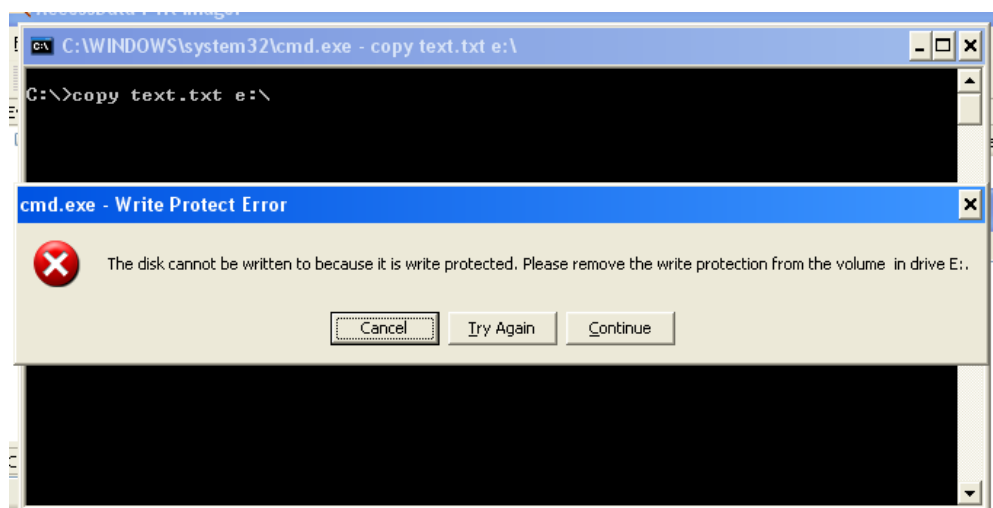
SAFE Block XP Version 1.1 Configuration



SHA-1 Hash Values

Before USB 1	0043d9207b826f30783b98290f9542cb235a291a
After USB 1	0043d9207b826f30783b98290f9542cb235a291a
Before USB 2	3424ac5ea2777220fcd694154bab6f3c3850eb93
After USB 2	3424ac5ea2777220fcd694154bab6f3c3850eb93

Output



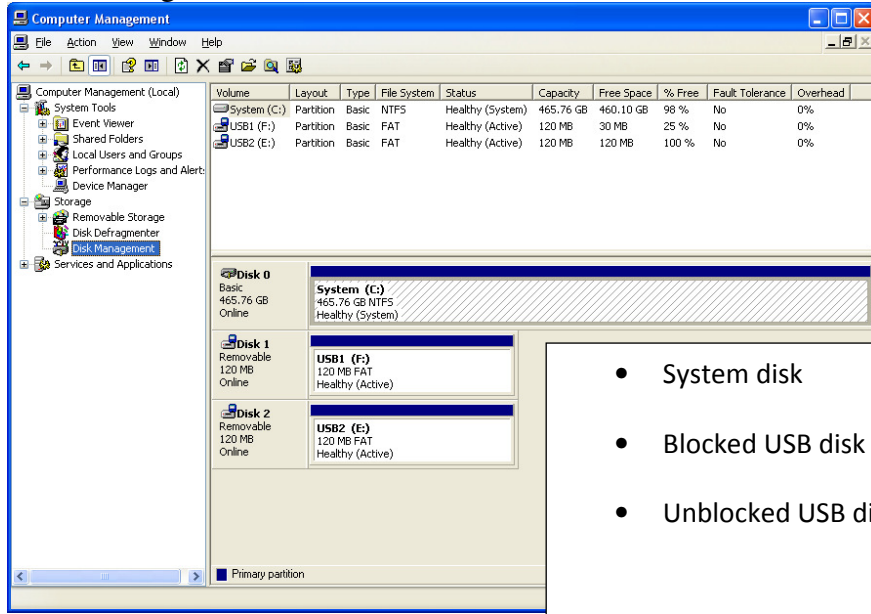
SWB-027 Test result analysis

SAFE Block XP Version 1.1 performed correctly - the operation failed and the hashes did not change.

7.28 Test Case SWB-28

This case tests SAFE Block XP V1.1's compliance with assertion SWB-AM-10. It is run using the typical protocol. The expected result of this test is that the DROP operation will fail with an error message and the hash value of the target disk will be unchanged after the test

Drive Configuration



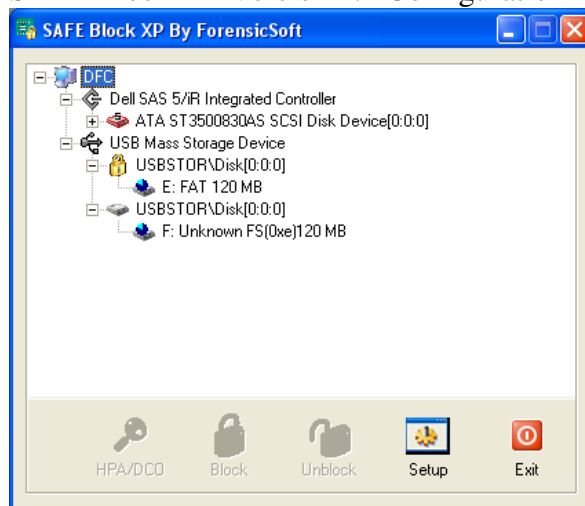
The screenshot shows the Windows Computer Management console. The left pane shows the tree view with 'Disk Management' selected. The right pane displays a table of volumes and a detailed view of the disks below it.

Volume	Layout	Type	File System	Status	Capacity	Free Space	% Free	Fault Tolerance	Overhead
System (C:)	Partition	Basic	NTFS	Healthy (System)	465.76 GB	460.10 GB	98 %	No	0%
USB1 (F:)	Partition	Basic	FAT	Healthy (Active)	120 MB	30 MB	25 %	No	0%
USB2 (E:)	Partition	Basic	FAT	Healthy (Active)	120 MB	120 MB	100 %	No	0%

Disk	Configuration
Disk 0	System (C:) 465.76 GB NTFS Healthy (System)
Disk 1	USB1 (F:) 120 MB FAT Healthy (Active)
Disk 2	USB2 (E:) 120 MB FAT Healthy (Active)

- System disk
- Blocked USB disk 1
- Unblocked USB disk 2

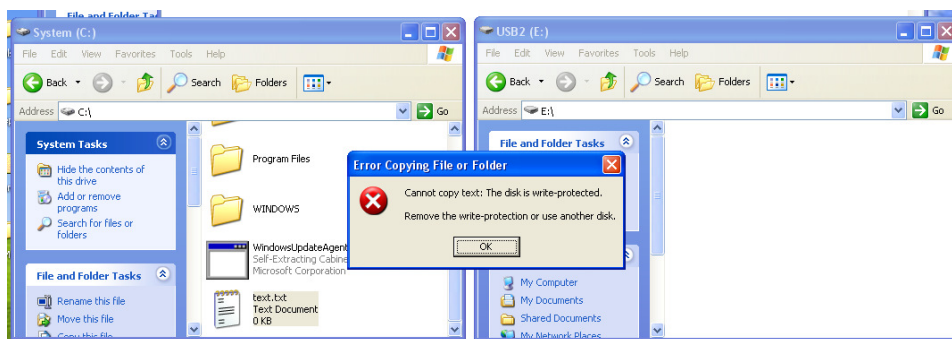
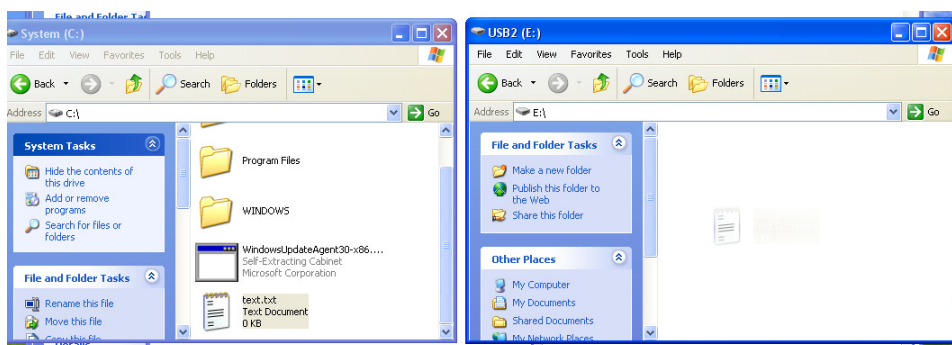
SAFE Block XP Version 1.1 Configuration



SHA-1 Hash Values

Before USB 1	0043d9207b826f30783b98290f9542cb235a291a
After USB 1	0043d9207b826f30783b98290f9542cb235a291a
Before USB 2	3424ac5ea2777220fcd694154bab6f3c3850eb93
After USB 2	3424ac5ea2777220fcd694154bab6f3c3850eb93

Output



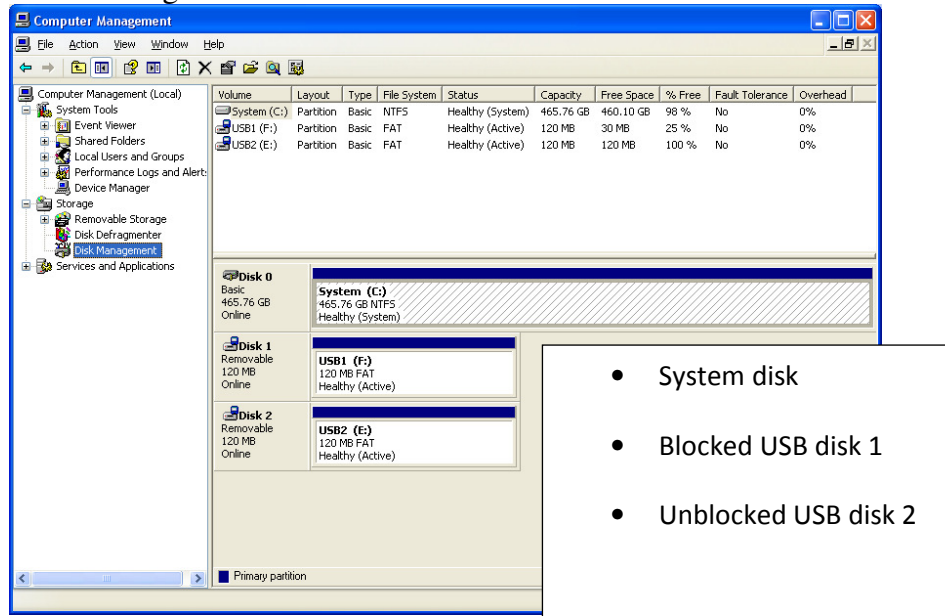
SWB-028 Test result analysis

SAFE Block XP Version 1.1 performed correctly - the operation failed and the hashes did not change.

7.29 Test Case SWB-29

This case tests SAFE Block XP V1.1's compliance with assertions SWB-AM-10 and SWB-AO-08. The expected result of this test is that the PASTE operation will fail with an error message, and the hash value of the target disk will be unchanged after the test.

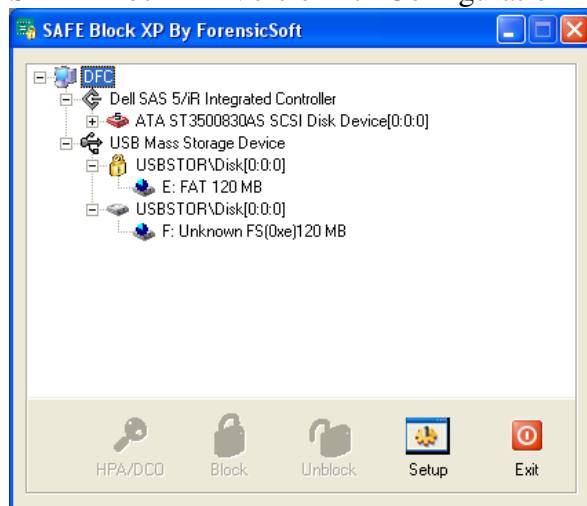
Drive Configuration



Volume	Layout	Type	File System	Status	Capacity	Free Space	% Free	Fault Tolerance	Overhead
System (C:)	Partition	Basic	NTFS	Healthy (System)	465.76 GB	460.10 GB	98 %	No	0%
USB1 (F:)	Partition	Basic	FAT	Healthy (Active)	120 MB	30 MB	25 %	No	0%
USB2 (E:)	Partition	Basic	FAT	Healthy (Active)	120 MB	120 MB	100 %	No	0%

- System disk
- Blocked USB disk 1
- Unblocked USB disk 2

SAFE Block XP Version 1.1 Configuration



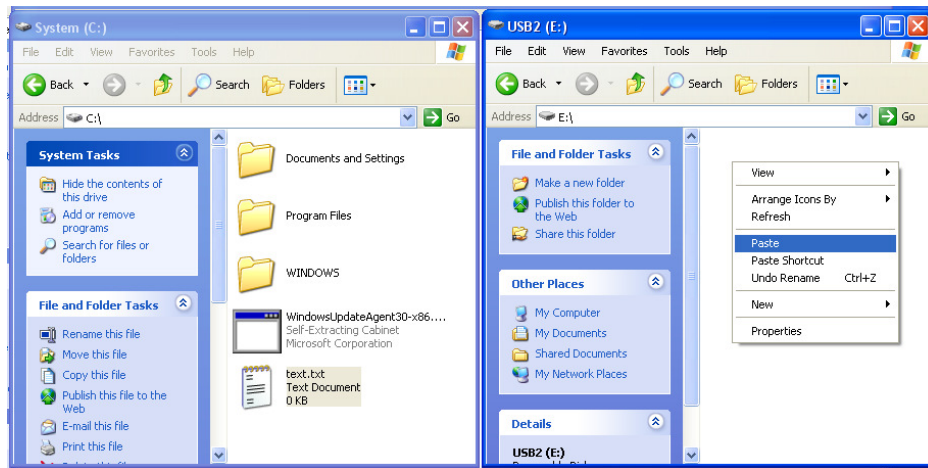
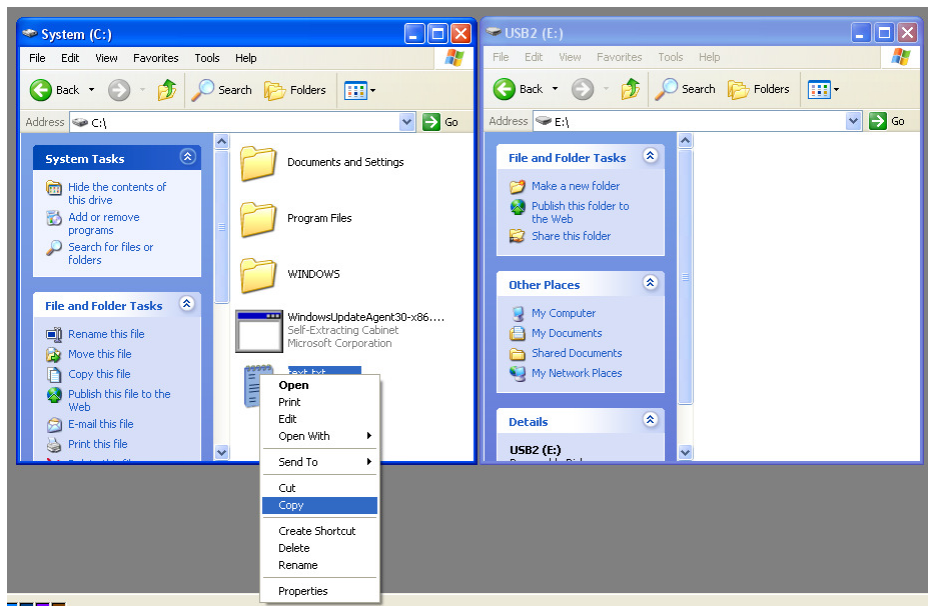
SAFE Block XP By ForensicSoft

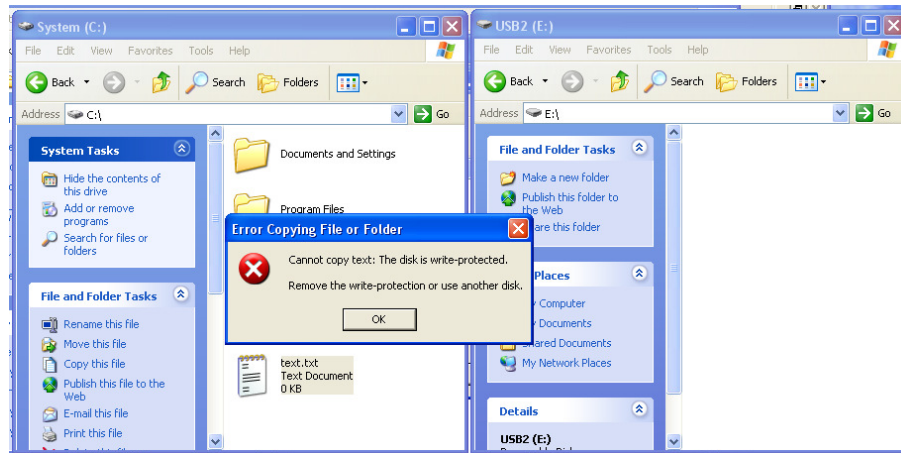
HPA/DCO Block Unblock Setup Exit

SHA-1 Hash Values

Before USB 1	0043d9207b826f30783b98290f9542cb235a291a
After USB 1	0043d9207b826f30783b98290f9542cb235a291a
Before USB 2	3424ac5ea2777220fcd694154bab6f3c3850eb93
After USB 2	3424ac5ea2777220fcd694154bab6f3c3850eb93

Output





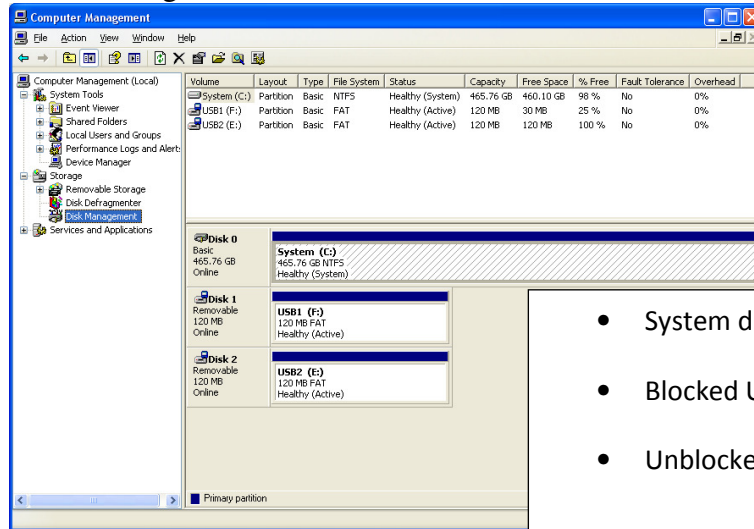
SWB-029 Test result analysis

SAFE Block XP Version 1.1 performed correctly - the operation failed and the hashes did not change.

7.30 Test Case SWB-30

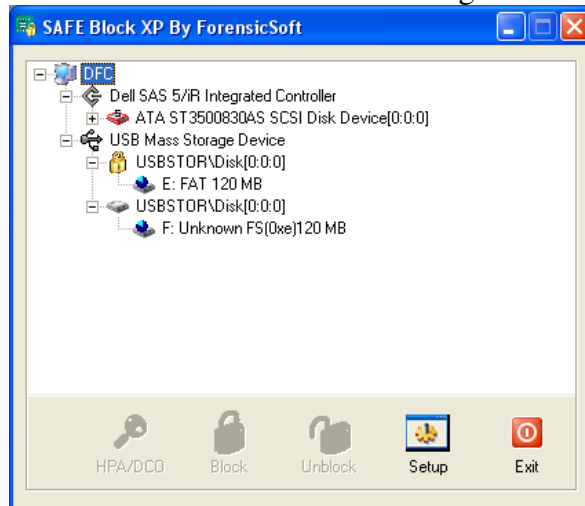
This case tests SAFE Block XP V1.1's compliance with mandatory assertion SWB-AM-10 and optional assertion SWBAO-08. The expected result of this test is that the SAVE AS operation will fail with an I/O error and the hash value of the test disk will be unchanged by the test.

Drive Configuration



- System disk
- Blocked USB disk 1
- Unblocked USB disk 2

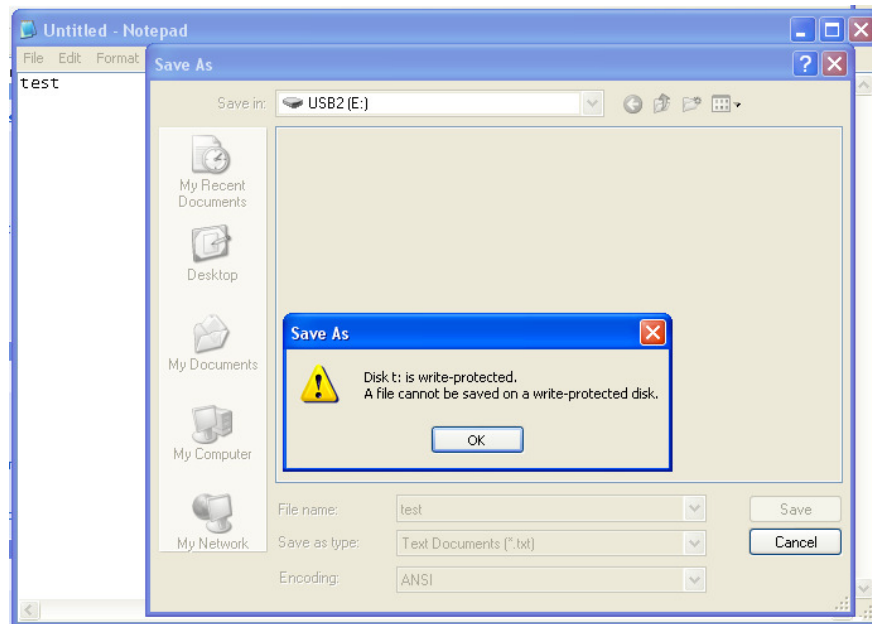
SAFE Block XP Version 1.1 Configuration



SHA-1 Hash Values

Before USB 1	0043d9207b826f30783b98290f9542cb235a291a
After USB 1	0043d9207b826f30783b98290f9542cb235a291a
Before USB 2	3424ac5ea2777220fcd694154bab6f3c3850eb93
After USB 2	3424ac5ea2777220fcd694154bab6f3c3850eb93

Output



SWB-030 Test result analysis

SAFE Block XP Version 1.1 performed correctly - the operation failed and the hashes did not change.

References

- [1] National Institute of Standards, *NIST Software Write Blocker Test Suite V1.2*; <http://www.cfft.nist.gov/ACES-test-support.zip>
- [2] ForensicSoft Inc, *SAFE Block XP V1.1*; <http://www.forensicsoft.com>
- [3] National Institute of Standards, *ACES Software Write Block Tool Test Report: Writeblocker Windows XP Version 6.10.0*; Jan 2008; http://www.nist.gov/cgi-bin/exit_nist.cgi?url=http://www.ojp.usdoj.gov/nij/pubs-sum/220222.htm
- [4] AccessData Inc, *FTK Imager2.5*; <http://www.accessdata.com>
- [5] busTRACE, Filter Driver Load Order v1.0.009; <http://www.bustrace.com/products/devfilter.htm>