Testing Write Blockers

James R Lyle

CFTT Project

NIST/ITL/SDCT

November 06, 2006

DISCLAIMER

Certain trade names and company products are mentioned in the text or identified. In no case does such identification imply recommendation or endorsement by the National Institute of Standards and Technology, nor does it imply that the products are necessarily the best available for the purpose.

Project Sponsors

- NIST/OLES (Program management)
- National Institute of Justice (Major funding)
- FBI (Additional funding)
- Department of Defense, DCCI (Equipment and support)
- Homeland Security (Technical input)
- State & Local agencies (Technical input)
- Internal Revenue, IRS (Technical input)

Talk Outline

- Software Write Blocking
- Hardware Write Blocking

Protection Goals

- Prohibit any changes to a hard drive
- Prohibit changes by a malicious program
- Prohibit accidental change (blunder)
- Prohibit change by operating system
- Prohibit damage to a drive

Protection Strategies

- Standardized & validated procedures
- No Protection software or device
- Trusted OS & trusted tools
- Software write block program
- Hardware write block device

Software Write Blocking

- Blocking strategies
- Interrupt 0x13 command set
- Command usage observations
- NIST test results for RCMP HDL & Pdblock

Software Blocking Tools

- BIOS based interrupt 0x13 DOS TSR
- Driver based (e.g., Windows filter stack)
- Built in to OS: Windows XP service pack 2

Write Block Strategies

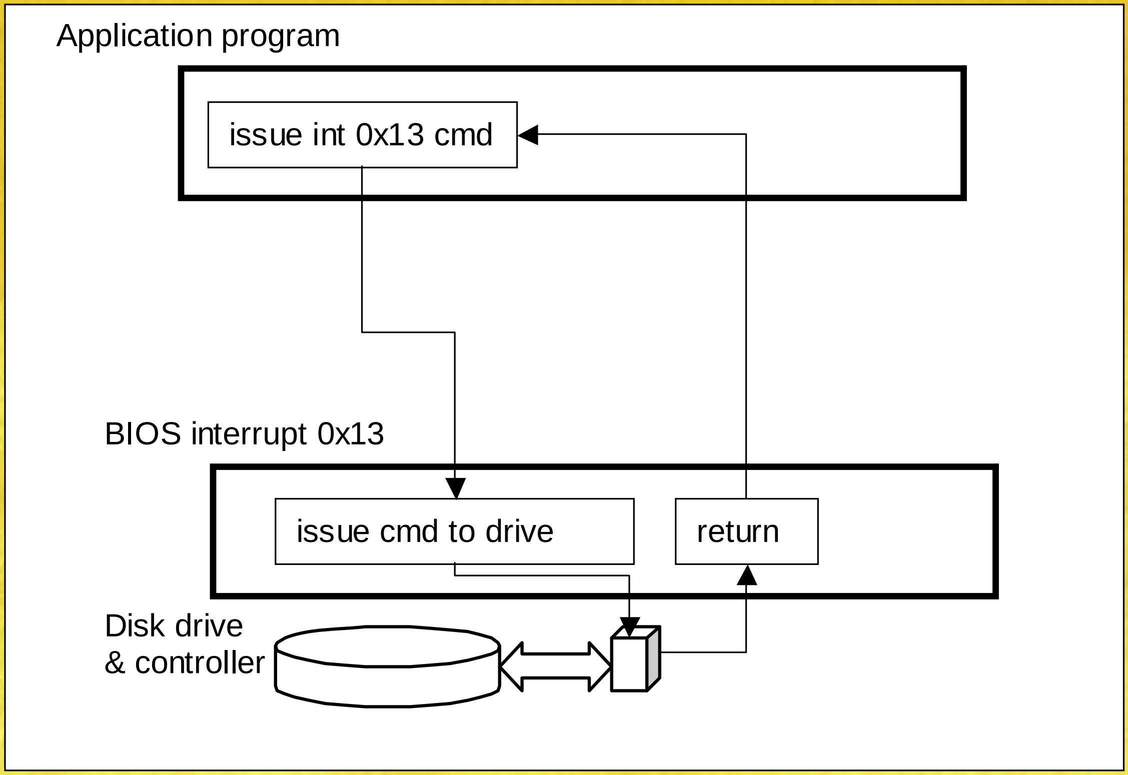
- Block unsafe commands, allow everything else
  - + Always can read, even if new command introduced
  - - Allows newly introduced write commands

- Allow safe commands, block everything else
  - + Writes always blocked
  - - Cannot use newly introduced read commands

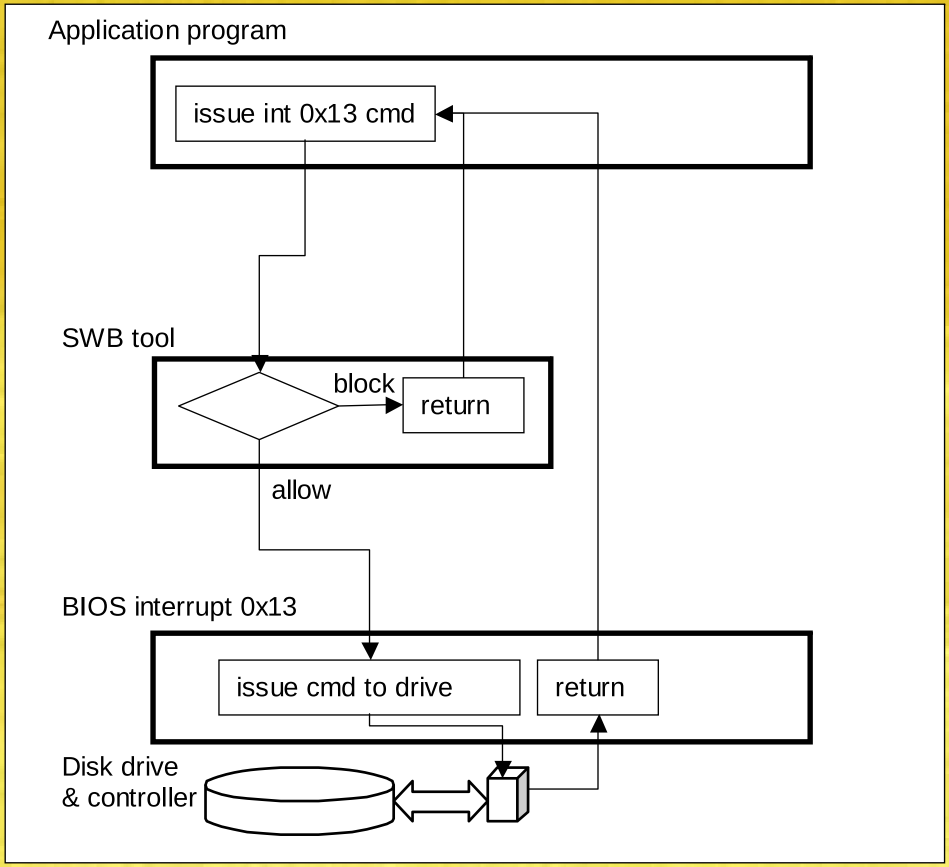
Interrupt 0x13 Commands

- 256 possible command codes
- Common BIOS has about 20 defined
- Many obsolete or discontinued commands
- Many commands defined for add on products see http://www.ctyme.com/rbrown.htm

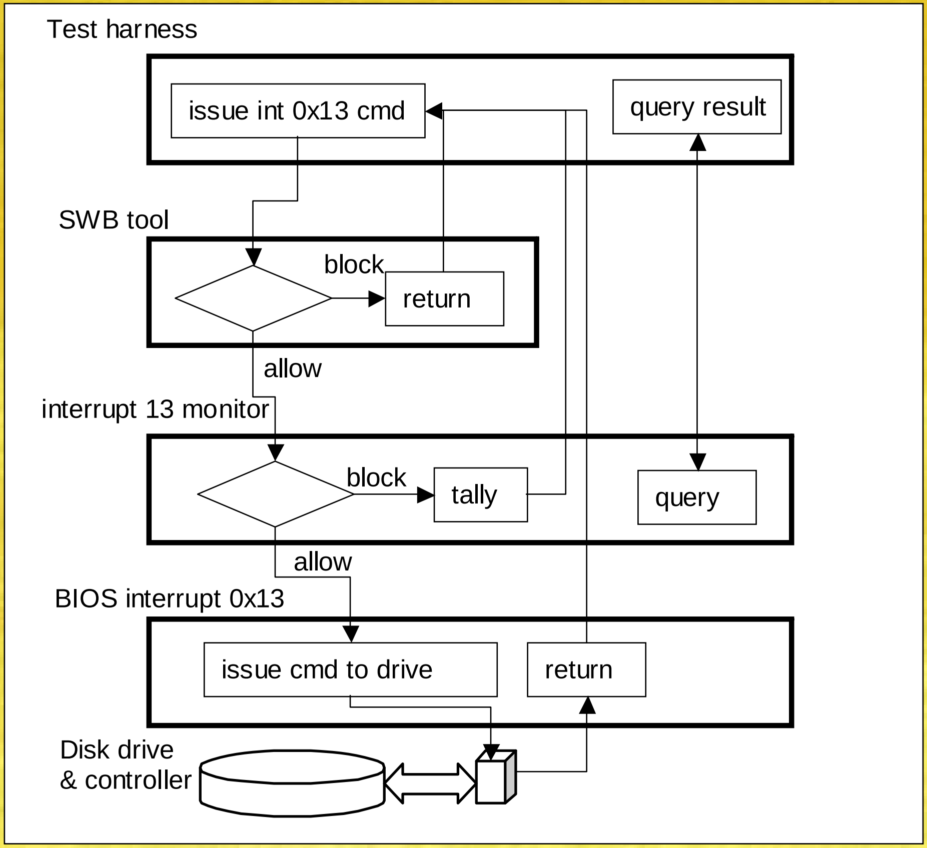
Hard Drive BIOS Access



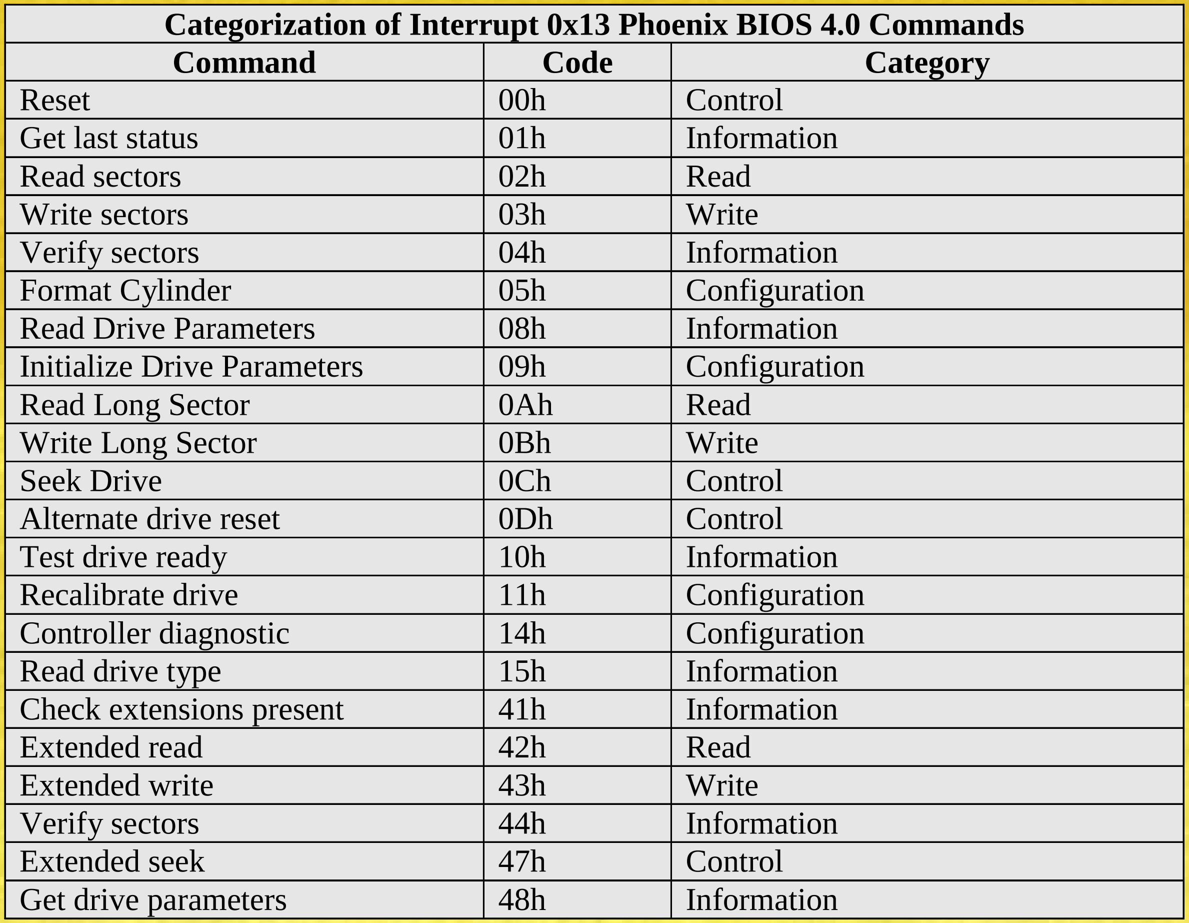
SWB Tool Operation



Test Harness Operation



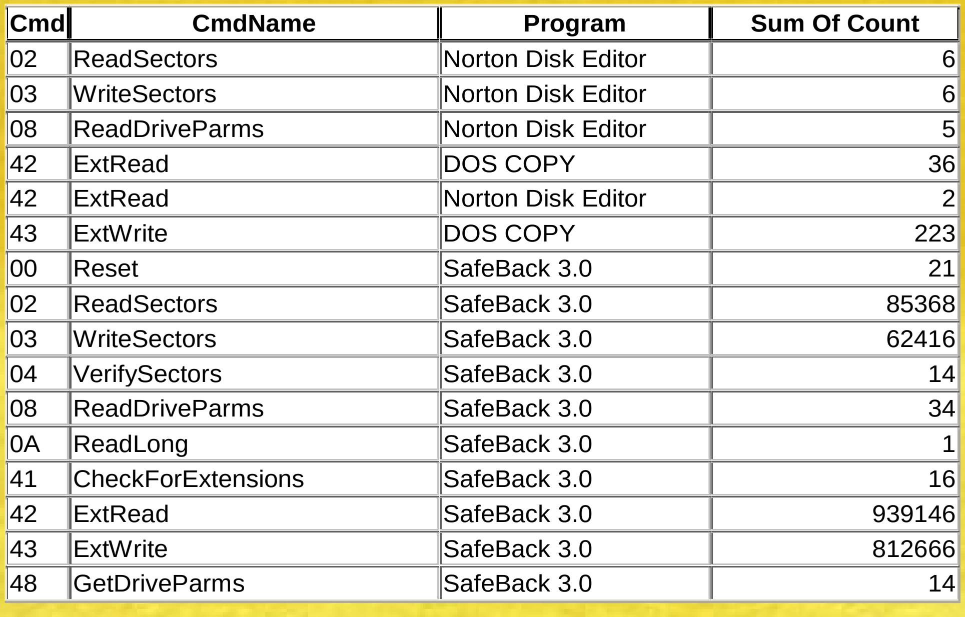
Phoenix BIOS 4.0



Categorization of Interrupt 0x13 Phoenix BIOS 4.0 Commands

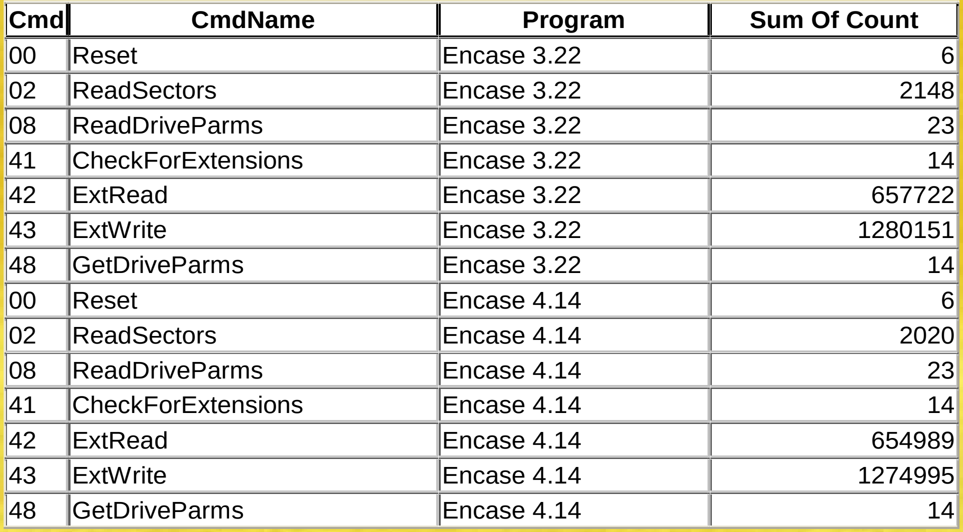
Command	Code	Category
Reset	00h	Control
Get last status	01h	Information
Read sectors	02h	Read
Write sectors	03h	Write
Verify sectors	04h	Information
Format Cylinder	05h	Configuration
Read Drive Parameters	08h	Information
Initialize Drive Parameters	09h	Configuration
Read Long Sector	0Ah	Read
Write Long Sector	0Bh	Write
Seek Drive	0Ch	Control
Alternate drive reset	0Dh	Control
Test drive ready	10h	Information
Recalibrate drive	11h	Configuration
Controller diagnostic	14h	Configuration
Read drive type	15h	Information
Check extensions present	41h	Information
Extended read	42h	Read
Extended write	43h	Write
Verify sectors	44h	Information
Extended seek	47h	Control
Get drive parameters	48h	Information

Observations of 0x13 Usage I



Cmd	CmdName	Program	Sum Of Count
02	ReadSectors	Norton Disk Editor	6
03	WriteSectors	Norton Disk Editor	6
08	ReadDriveParms	Norton Disk Editor	5
42	ExtRead	DOS COPY	36
42	ExtRead	Norton Disk Editor	2
43	ExtWrite	DOS COPY	223
00	Reset	SafeBack 3.0	21
02	ReadSectors	SafeBack 3.0	85368
03	WriteSectors	SafeBack 3.0	62416
04	VerifySectors	SafeBack 3.0	14
08	ReadDriveParms	SafeBack 3.0	34
0A	ReadLong	SafeBack 3.0	1
41	CheckForExtensions	SafeBack 3.0	16
42	ExtRead	SafeBack 3.0	939146
43	ExtWrite	SafeBack 3.0	812666
48	GetDriveParms	SafeBack 3.0	14

Observations of 0x13 Usage II



Cmd	CmdName	Program	Sum Of Count
00	Reset	Encase 3.22	6
02	ReadSectors	Encase 3.22	2148
08	ReadDriveParms	Encase 3.22	23
41	CheckForExtensions	Encase 3.22	14
42	ExtRead	Encase 3.22	657722
43	ExtWrite	Encase 3.22	1280151
48	GetDriveParms	Encase 3.22	14
00	Reset	Encase 4.14	6
02	ReadSectors	Encase 4.14	2020
08	ReadDriveParms	Encase 4.14	23
41	CheckForExtensions	Encase 4.14	14
42	ExtRead	Encase 4.14	654989
43	ExtWrite	Encase 4.14	1274995
48	GetDriveParms	Encase 4.14	14

Comments on 0x13

- Only two unsafe commands were in use
- Other unsafe commands unlikely to be used
  - Format: 05, 06, & 07
  - Diagnostic: 0E, 0F, 12, 13, & 14
  - Write long: 0B

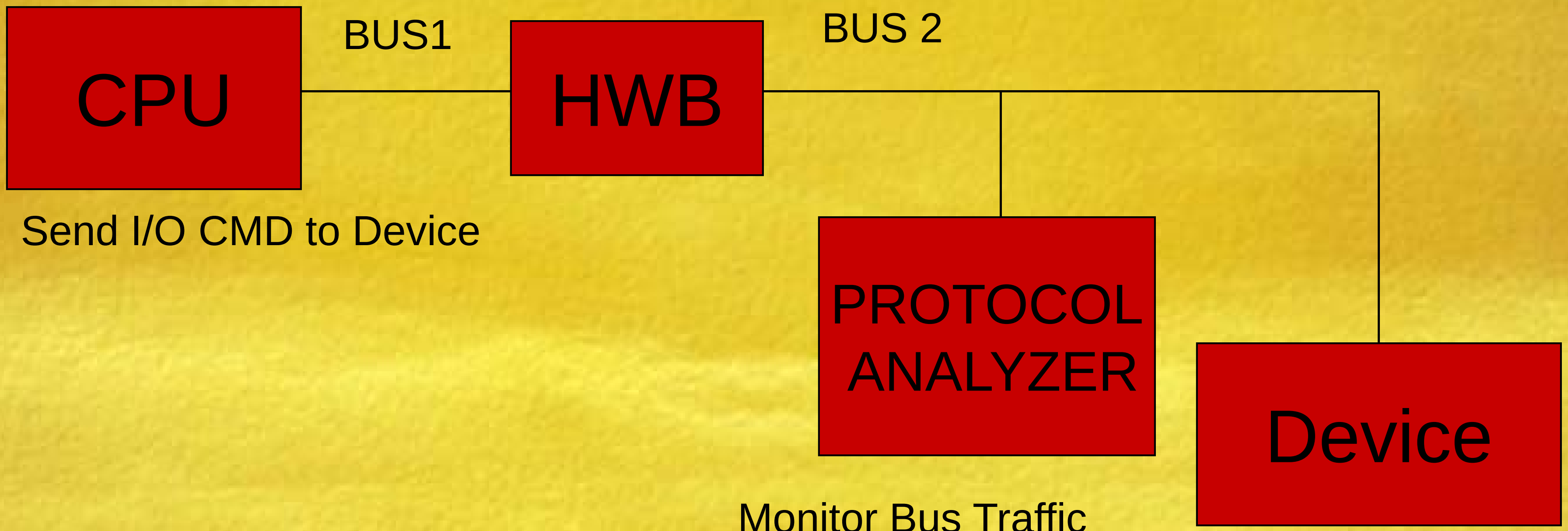
RCMP HDL & Pdblock

Command	Code	Category	Spec	0.4	0.5	0.7	0.8	PDB	PDL
Format Track	05h	Configuration	B	B	B	B	B	B	B
Format Track With Bad Sectors	06h	Configuration	B	B	B	B	B	B	B
Format Cylinder	07h	Configuration	B	B	B	B	B	B	B
Initialize Drive Parameters	09h	Configuration	B	A	A	A	B	A	A
ESDI Diagnostic (PS/2)	0Eh	Configuration	B	A	A	A	B	A	A
ESDI Diagnostic (PS/2)	0Fh	Configuration	B	B	B	B	B	B	B
Controller RAM Diagnostic	12h	Configuration	B	A	A	B	B	A	A
Drive Diagnostic	13h	Configuration	B	B	B	B	B	A	A
Controller Diagnostic	14h	Configuration	B	A	A	B	B	A	A
Reset	00h	Control	A	A	A	A	A	A	A
Seek Drive	0Ch	Control	A	A	A	A	A	A	A
Alternate Drive Reset	0Dh	Control	A	A	A	A	A	A	A
Recalibrate Drive	11h	Control	A	A	A	A	B	A	A
Extended Seek	47h	Control	A	A	A	B	B	A	A
Get Last Status	01h	Information	A	A	A	A	A	A	A
Verify Sectors	04h	Information	A	A	A	A	A	A	A
Read Drive Parameters	08h	Information	A	A	A	A	A	A	A
Test Drive Ready	10h	Information	A	A	A	A	A	A	A
Read Drive Type	15h	Information	A	A	A	B	A	A	A
Check Extensions Present	41h	Information	A	A	A	A	A	A	A
Verify Sectors	44h	Information	A	A	A	A	A	A	A
Get Drive Parameters	48h	Information	A	A	A	A	A	A	A
Read Sectors	02h	Read	A	A	A	A	A	A	A
Read Long Sector	0Ah	Read	A	A	A	A	A	A	A
Extended Read	42h	Read	A	A	A	A	A	A	A
Write Sectors	03h	Write	B	B	B	B	B	B	B
Write Long Sector	0Bh	Write	B	B	B	B	B	B	B
Extended Write	43h	Write	B	A	B	B	B	B	B
Undefined	other	Miscellaneous	B	A	A4	B	B	A3	A3

Write Blocking Hardware

- Blocking device actions
- ATA standards
- Observed ATA commands
- Device behaviors for two devices

HWB Testing



CPU

BUS1

HWB

BUS 2

Send I/O CMD to Device

PROTOCOL ANALYZER

Device

Monitor Bus Traffic

Return result to CPU

Write Blocker Actions

- The device forwards the command to the hard drive.
- The blocking device substitutes a different command to the hard drive. The is the case if the blocking device uses different bus protocols for communication with the host and hard drive.
- The device simulates the command without actually forwarding the command to the hard drive.
- If a command is blocked, the device may return either *success* or *failure* for the blocked operation. However, returning *failure* may sometimes cause the host computer to lock up for some commands issued by some operating systems.

ATA Standards

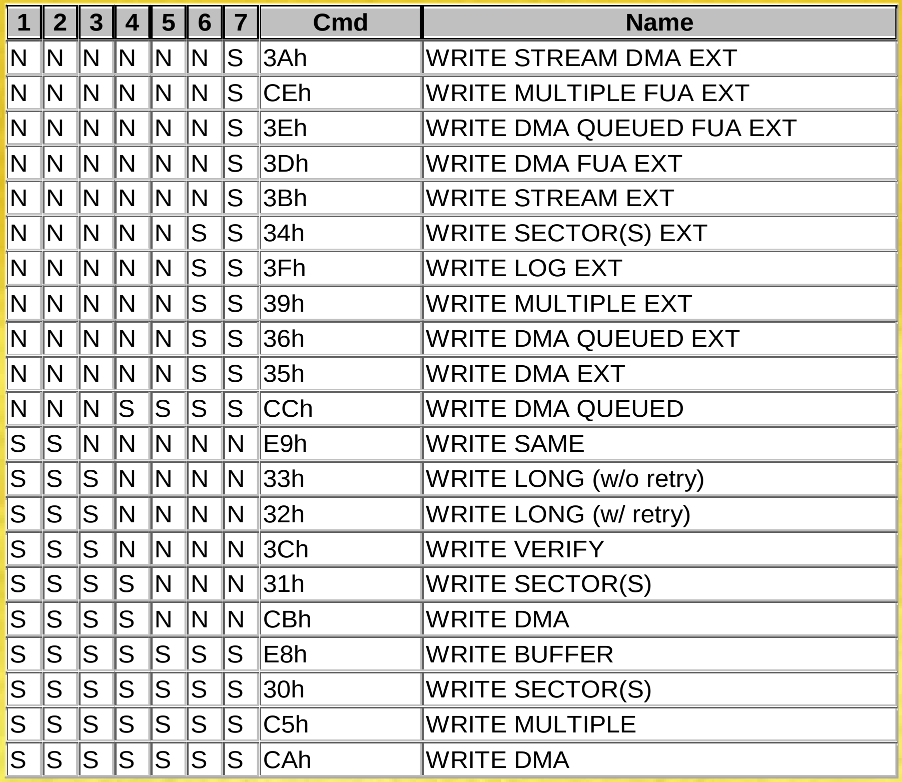
Last Draft Standard Before Final Version	**Approximate Publication Data**
ATA-1 X3T10/791D Revision 4c	1994
ATA-2 X3T10/0948D Revision 4c	March 18, 1996
ATA-3 X3T13 2008D Revision 7b	January 27, 1997
ATA/ATAPI-4 T13/1153D Revision 18	August 19, 1998
ATA/ATAPI-5 T13/1321D Revision 3	February 29, 2000
ATA/ATAPI-6 T13/1410D Revision 3	October 30, 2001
ATA/ATAPI-7 V1 T13/1532D Revision 4b	April 21, 2004

Using a Protocol Analyzer

Sent from Host	
20=READ W/ RETR	LBA=A003000
30=WRITE W/ RETRY	LBA=000000
20=READ W/ RETR	LBA=F013000
20=READ W/ RETRY	LBA=A00C400
C4=READ MULTIPLE	LBA=000C400
20=READ W/ RETRY	LBA=F01C400
20=READ W/ RETRY	LBA=A00C700
C7=READ DMA QUEUED	LBA=000C700
20=READ W/ RETRY	LBA=F01C700
20=READ W/ RETRY	LBA=A00C800
C8=Read DMA	LBA=000C800
20=READ W/ RETRY	LBA=F01C800
20=READ W/ RETRY	LBA=A00C900
C9=RD DMA W/O RETR	LBA=000C900
20=READ W/ RETRY	LBA=F01C900

Allowed by Blocker	
20=READ W/ RETR	LBA=A003000
20=READ W/ RETR	LBA=F013000
20=READ W/ RETRY	LBA=A00C400
C8=Read DMA	LBA=000C400
20=READ W/ RETRY	LBA=F01C400
20=READ W/ RETRY	LBA=A00C700
20=READ W/ RETRY	LBA=F01C700
20=READ W/ RETRY	LBA=A00C800
C8=Read DMA	LBA=000C800
20=READ W/ RETRY	LBA=F01C800
20=READ W/ RETRY	LBA=A00C900
20=READ W/ RETRY	LBA=F01C900

ATA Write Commands

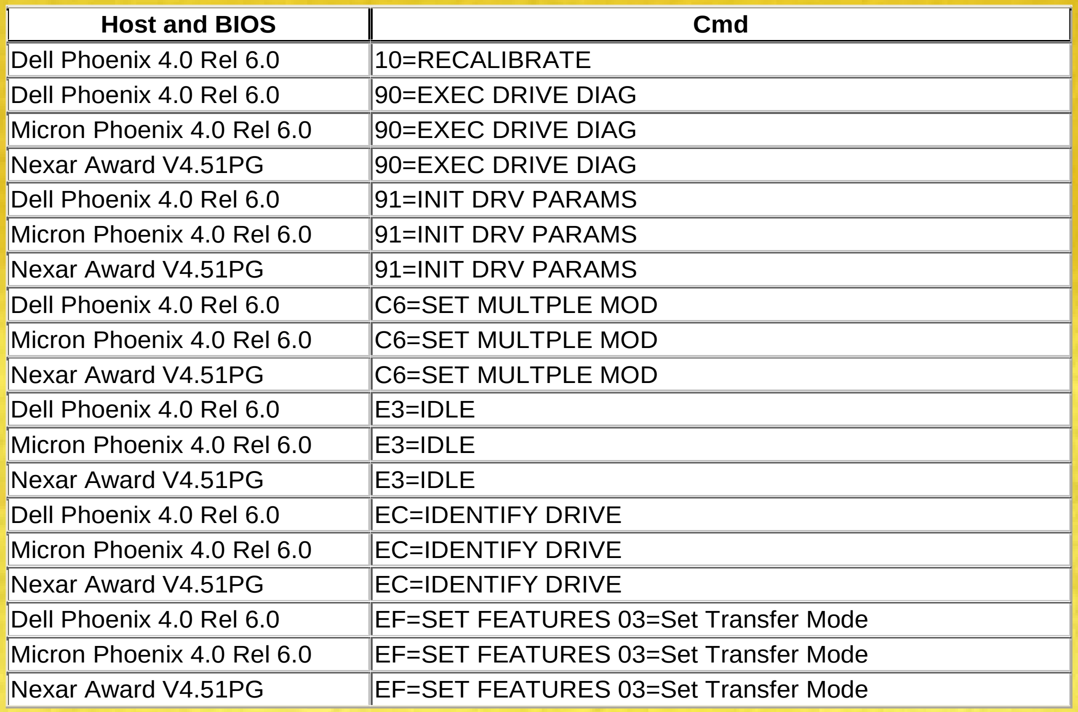


1	2	3	4	5	6	7	Cmd	Name
N	N	N	N	N	N	S	3Ah	WRITE STREAM DMA EXT
N	N	N	N	N	N	S	CEh	WRITE MULTIPLE FUA EXT
N	N	N	N	N	N	S	3Eh	WRITE DMA QUEUED FUA EXT
N	N	N	N	N	N	S	3Dh	WRITE DMA FUA EXT
N	N	N	N	N	N	S	3Bh	WRITE STREAM EXT
N	N	N	N	N	S	S	34h	WRITE SECTOR(S) EXT
N	N	N	N	N	S	S	3Fh	WRITE LOG EXT
N	N	N	N	N	S	S	39h	WRITE MULTIPLE EXT
N	N	N	N	N	S	S	36h	WRITE DMA QUEUED EXT
N	N	N	N	N	S	S	35h	WRITE DMA EXT
N	N	N	S	S	S	S	CCh	WRITE DMA QUEUED
S	S	N	N	N	N	N	E9h	WRITE SAME
S	S	S	N	N	N	N	33h	WRITE LONG (w/o retry)
S	S	S	N	N	N	N	32h	WRITE LONG (w/ retry)
S	S	S	N	N	N	N	3Ch	WRITE VERIFY
S	S	S	S	N	N	N	31h	WRITE SECTOR(S)
S	S	S	S	N	N	N	CBh	WRITE DMA
S	S	S	S	S	S	S	E8h	WRITE BUFFER
S	S	S	S	S	S	S	30h	WRITE SECTOR(S)
S	S	S	S	S	S	S	C5h	WRITE MULTIPLE
S	S	S	S	S	S	S	CAh	WRITE DMA

Other Unsafe ATA Cmds

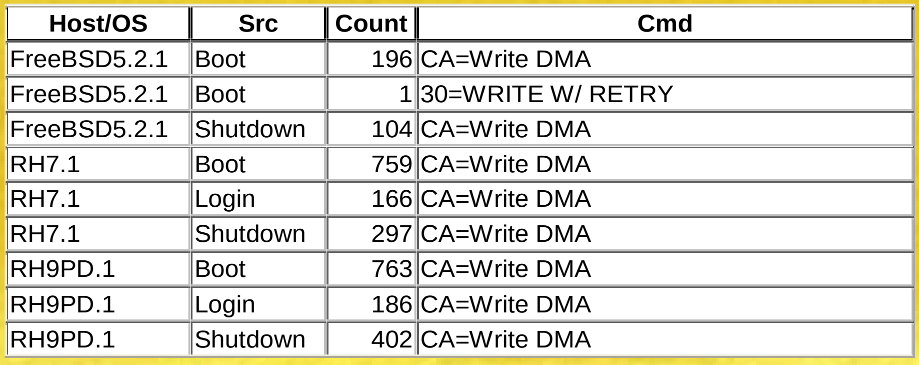
1	2	3	4	5	6	7	CMD	Command Name
N	N	N	S	S	S	S	C0h	CFA ERASE SECTORS
N	N	N	S	S	S	S	CDh	CFA WRITE MULTIPLE WO ERASE
N	N	N	S	S	S	S	38h	CFA WRITE SECTORS WO ERASE
N	S	S	S	S	S	S	92h	DOWNLOAD MICROCODE
S	S	S	N	N	N	N	50h	FORMAT TRACK
N	N	S	S	S	S	S	F3h	SECURITY ERASE PREPARE
N	N	S	S	S	S	S	F4h	SECURITY ERASE UNIT
S	S	S	S	S	S	S	EFh	SET FEATURES
N	N	N	S	S	S	S	F9h	SET MAX ADDRESS
N	N	N	N	N	S	S	37h	SET MAX ADDRESS EXT
N	N	N	N	N	N	S	B0h	SMART WRITE LOG
N	N	S	S	S	S	N	B0h/D6h	SMART WRITE LOG SECTOR

Commands Issued by BIOS



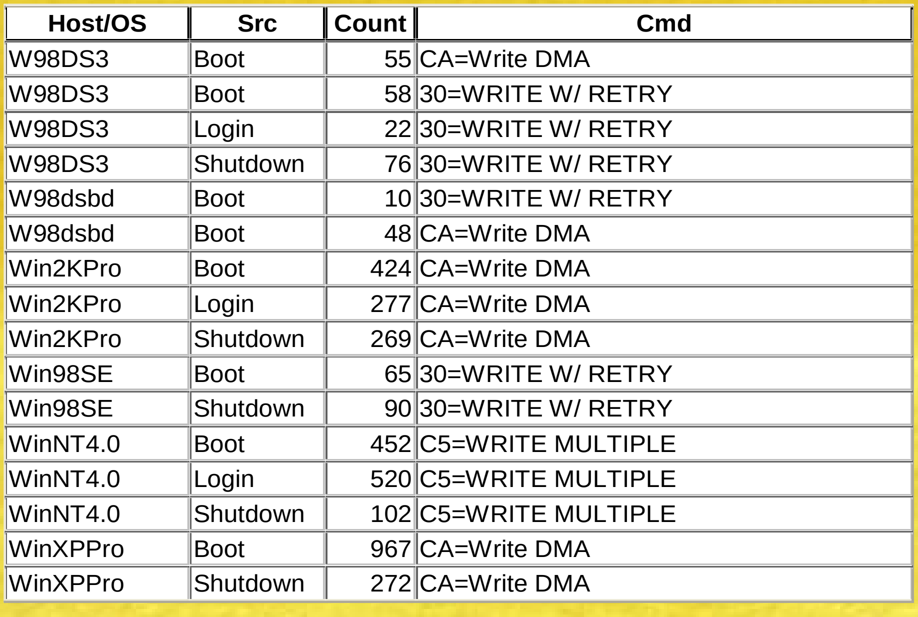
Host and BIOS	Cmd
Dell Phoenix 4.0 Rel 6.0	10=RECALIBRATE
Dell Phoenix 4.0 Rel 6.0	90=EXEC DRIVE DIAG
Micron Phoenix 4.0 Rel 6.0	90=EXEC DRIVE DIAG
Nexar Award V4.51PG	90=EXEC DRIVE DIAG
Dell Phoenix 4.0 Rel 6.0	91=INIT DRV PARAMS
Micron Phoenix 4.0 Rel 6.0	91=INIT DRV PARAMS
Nexar Award V4.51PG	91=INIT DRV PARAMS
Dell Phoenix 4.0 Rel 6.0	C6=SET MULTPLE MOD
Micron Phoenix 4.0 Rel 6.0	C6=SET MULTPLE MOD
Nexar Award V4.51PG	C6=SET MULTPLE MOD
Dell Phoenix 4.0 Rel 6.0	E3=IDLE
Micron Phoenix 4.0 Rel 6.0	E3=IDLE
Nexar Award V4.51PG	E3=IDLE
Dell Phoenix 4.0 Rel 6.0	EC=IDENTIFY DRIVE
Micron Phoenix 4.0 Rel 6.0	EC=IDENTIFY DRIVE
Nexar Award V4.51PG	EC=IDENTIFY DRIVE
Dell Phoenix 4.0 Rel 6.0	EF=SET FEATURES 03=Set Transfer Mode
Micron Phoenix 4.0 Rel 6.0	EF=SET FEATURES 03=Set Transfer Mode
Nexar Award V4.51PG	EF=SET FEATURES 03=Set Transfer Mode

Write Commands Issued by OS (Unix)



Host/OS	Src	Count	Cmd
FreeBSD5.2.1	Boot	196	CA=Write DMA
FreeBSD5.2.1	Boot	1	30=WRITE W/ RETRY
FreeBSD5.2.1	Shutdown	104	CA=Write DMA
RH7.1	Boot	759	CA=Write DMA
RH7.1	Login	166	CA=Write DMA
RH7.1	Shutdown	297	CA=Write DMA
RH9PD.1	Boot	763	CA=Write DMA
RH9PD.1	Login	186	CA=Write DMA
RH9PD.1	Shutdown	402	CA=Write DMA

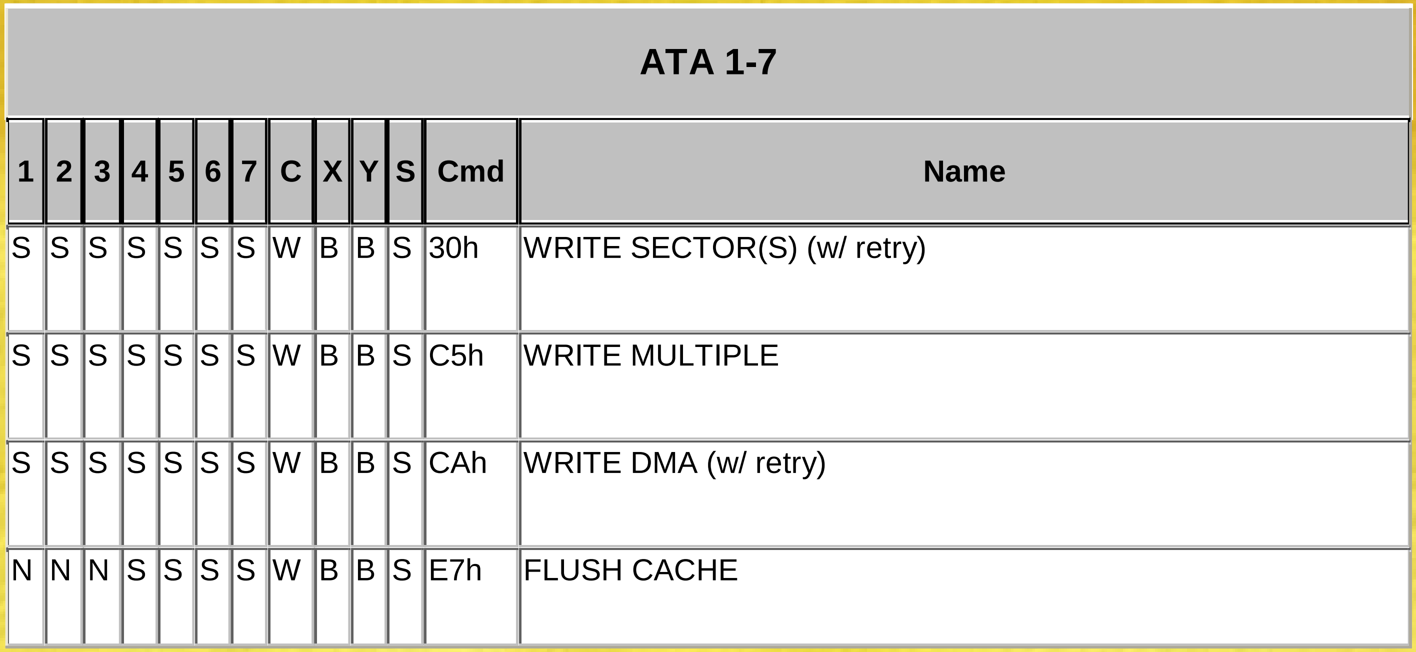
Write Commands Issued by OS (MS)



Host/OS	Src	Count	Cmd
W98DS3	Boot	55	CA=Write DMA
W98DS3	Boot	58	30=WRITE W/ RETRY
W98DS3	Login	22	30=WRITE W/ RETRY
W98DS3	Shutdown	76	30=WRITE W/ RETRY
W98dsbd	Boot	10	30=WRITE W/ RETRY
W98dsbd	Boot	48	CA=Write DMA
Win2KPro	Boot	424	CA=Write DMA
Win2KPro	Login	277	CA=Write DMA
Win2KPro	Shutdown	269	CA=Write DMA
Win98SE	Boot	65	30=WRITE W/ RETRY
Win98SE	Shutdown	90	30=WRITE W/ RETRY
WinNT4.0	Boot	452	C5=WRITE MULTIPLE
WinNT4.0	Login	520	C5=WRITE MULTIPLE
WinNT4.0	Shutdown	102	C5=WRITE MULTIPLE
WinXPPro	Boot	967	CA=Write DMA
WinXPPro	Shutdown	272	CA=Write DMA

Blocking Devices vs Writes

- Action by device X and device Y on observed write commands



ATA 1-7												
1	**2**	**3**	**4**	**5**	**6**	**7**	**C**	**X**	**Y**	**S**	**Cmd**	**Name**
S	S	S	S	S	S	S	W	B	B	S	30h	WRITE SECTOR(S) (w/ retry)
S	S	S	S	S	S	S	W	B	B	S	C5h	WRITE MULTIPLE
S	S	S	S	S	S	S	W	B	B	S	CAh	WRITE DMA (w/ retry)
N	N	N	S	S	S	S	W	B	B	S	E7h	FLUSH CACHE

Blocking Devices vs Reads

- Actions against observed read commands for two devices: X & Y
- Device Y replaces *read multiple* with *read DMA*

ATA 1-7												
1	**2**	**3**	**4**	**5**	**6**	**7**	**C**	**X**	**Y**	**S**	**Cmd**	**Name**
S	S	S	S	S	S	S	R	A	B	S	40h	READ VERIFY SECTOR(S)
S	S	S	S	S	S	S	R	A	C8h	S	C4h	READ MULTIPLE
S	S	S	S	S	S	S	R	A	A	S	C8h	READ DMA

Results for an ATA Device

The tested device allowed only the following commands:

```
20=READ W/ RETRY
24=READ SECTOR EXT
25=READ DMA EXT
27=RD MAX ADR EXT
37=SET MAX ADR EXT (volatile)
70=SEEK
91=INIT DRV PARAMS
B1=Device Config
C8=Read DMA
F8=RD NATV MAX ADD
F9=SET MAX ADDRESS (volatile)
```

On power on the device issues the following commands to the protected drive:

```
EC=IDENTIFY DRIVE
EF=SET FEATURES
C6=SET MULTPLE
EF=SET FEATURES
C6=SET MULTPLE MOD
```

Note that the **identify device** command is blocked if issued by the host, but the device returns the values obtained at power on.

Another ATA Device

- Although no commands were allowed by the write blocker that could change user or operating system data, some unsupported or atypical commands were allowed. Some examples are:

Command	**Comment**
Down load microcode (0x92)	This command allows reprogramming of hard drive firmware. While this could change drive behavior, the information to do so is drive model specific and not generally available.
Format Track (0x50)	This command is not defined in the current ATA hard drive specifications (ATA-4, through ATA-7). The command was defined in ATA-1, ATA-2 and ATA-3, however all three specifications have been withdrawn. The command could be used to erase information on an older drive that supports the instruction, but could not be used to change the content of any user or operating system data stored on a drive.
SMART write (0xB0,D6)	This command records information in a device maintenance log, not part of the data area where data files and operating system data is stored.
Vendor Specific commands	These are undocumented commands specific to a given model of hard drive.
CFA Erase Erase (0xC0)	This command applies to Compact Flash devices, not hard drives.
SATA Write FPDMA (0x61)	This command is noted by the protocol analyzer, but the command is only valid for Serial ATA (SATA) devices.

Notable Blocker Behaviors

- allow the volatile SET MAX ADDRESS, block if non-volatile
- cached the results IDENTIFY DEVICE
- substituted READ DMA for READ MULTIPLE
- allowed FORMAT TRACK
- Depending on OS version, might no be able to preview NTFS partition

Contacts

Jim Lyle
www.cftt.nist.gov
cftt@nist.gov

Doug White
www.nsrl.nist.gov
nsrl@nist.gov

Barbara Guttman
bguttman@nist.gov

Sue Ballou, Office of Law Enforcement Standards
susan.ballou@nist.gov