Information Technology Security Guide
Lead Agency Publication

RCMP Hard Disk Overwrite Software (DSX) User Manual

Technical Security Branch
Technical Operations
Royal Canadian Mounted Police
Issued: June 2001
Revised: May 2004

TABLE OF CONTENTS

1 Caveat

The ***RCMP Hard Disk Overwrite and Inspection Utilities*** suite is the property of the RCMP and is issued (on request) as licensed material to information technology security authorities of departments and agencies of the Government of Canada and provincial governments of Canada, subject to the following conditions:

- This suite is restricted for use by IT security authorities of departments and agencies of the Government of Canada and provincial governments of Canada. This suite may not be used, distributed nor otherwise disclosed beyond control of the departmental information technology security authority.

- No portion of this suite may be used for commercial profit or trade, and

- Departments and agencies that choose to use this suite do so at their own risk. There is no guarantee that the software contained in this suite functions as documented.

The DSX program has not been formally approved for clearing/sanitizing information on hard disks, and there is no claim of compliance with any hard disk sanitization standard.

2 Introduction

2.1 General

This document was last revised in October 2002. The revision date in the footer is to show that all the newly formatted and issued information relating to DSX are current. Anyone holding a document with an October 2002 revision date has the most up-to-date version.

The intended recipients of this software package are information technology security authorities of departments and agencies of the Government of Canada and of provincial governments of Canada.

This software overwrites and allows inspection of serviceable standard magnetic hard disk media used in IBM-PC/compatible systems. Overwriting (clearing) information is a measure intended to prevent information disclosure when serviceable hard disk media is removed from service.

The software described in this package is not formally approved for declassifying (sanitizing) hard disks.

2.2 Risk factors

Questions have been raised about the effectiveness of using software to “overwrite” hard disks. There are three significant risk factors associated with overwriting hard disks:

a. **Human factors** – e.g. level of technical knowledge. If, for example, a hard disk is overwritten while being incorrectly configured, the amount overwritten may be less than the rated capacity. This risk can be mitigated by providing appropriate training and by using procedures/checklists.

b. **Level of sensitivity/value of the information and threat agent** - regardless of the hard disk being overwritten correctly, information may be retrieved from data remanence [1] recovery (via microscopy) present at track boundaries. The risk level varies with information value and threat agent capabilities.

c. **PC/Hard disk combinations and technology advancements** - due to the ever-increasing number of PC/hard disk combinations and technology advancements, certain combinations of equipment may exist where overwriting fails to address every sector on a hard disk. Examples include bad sector re-mapping, misconfigured hard disks, equipment limitations (e.g. legacy BIOSs) and host protected areas (HPA).

2.3 Recovering information

There are two methods for recovering information from hard disks. **Method 1**, referred to as a "keyboard attack", uses software to recover information. **Method 2** requires laboratory techniques to recover information from magnetic remanence found at track edges.

Overwriting hard disks, when correctly performed, renders information unrecoverable using Method 1. However, residual information located at track edges (data remanance) **may** remain vulnerable to recovery using Method 2. Data recovery using Method 2 is a complex process that requires specialized equipment and knowledge.

Due to variations in host PCs and storage technology as well as human factors, there is no assurance that all information is sufficiently cleared by overwriting. For these reasons, **hard disks containing classified or otherwise sensitive information should be sanitized by approved methods**, unless determined otherwise by a threat and risk assessment and approval by the departmental IT security authority.

3 Installation

This package contains the following software:

DSX (Hard Disk Overwrite) - The DSX program overwrites an entire Int_13 type hard disk by geometry expressed in cylinders, sides and sectors/track. Int_13 accessible hard disks are those that are visible via the FDISK and PARTINFO programs. This version of DSX is capable of overwriting hard disks having a capacity greater than 8.4 GB and can operate in CHS and LBA disk access modes. Due to the potential for unauthorized use, DSX is password protected.

DV (Disk Viewer) - The DV program is used for inspecting hard disks before and after overwriting. DV displays disk contents on screen and allows manual disk navigation and content viewing.

IDE (E/IDE Hard disk Identification) - The IDE program displays E/IDE hard disk geometry, make/model and serial number (see Appendix A).

Copy the utilities onto an authentic (and virus free) copy of an MS-DOS V6.22 (or higher) bootable diskette, then **write protect the diskette**. The PC should be booted using this diskette to ensure that the

[1] CSE, *Clearing and Declassifying Electronic Data Storage Devices (ITSG-06), August 2000* http://www.cse-cst.gc.ca/en/services/publications/itsg/ITSG-06.html
- and -
U.S. National Computer Security Center (NCSC), *A Guide to Understanding Data Remanence in Automated Information Systems (TG-025), September 1991* http://security.isu.edu/pdf/dataremanence.pdf

utilities operate in isolation, free of software that may cause interference. For convenience, copy the CHKDSK, SYS, FDISK and FORMAT (MS-DOS programs) to this diskette for re-initializing hard disks for use following overwrite (if required). **Record the DSX password for future reference**.

4 Problem Reporting

The utilities have been tested, however, it is impossible to account for all possible hardware, software and hard disk configurations and technology changes. If a problem occurs, it is important to report it so that it may be resolved.

The following information must accompany a problem report:

a. Name of IT security authority, department/agency, address, telephone number and E-mail address.

b. Program name, version and release date.

c. A brief description of the command(s) used when the problem occurred, and where possible, a sample/description of the erroneous or unexpected results. Also, an indication as to whether the problem can be readily duplicated. Also, state the impact of the problem.

d. State the disk media type/model used (where applicable), and state the numbers and types of hard disk and/or diskette drives in the system configuration.

e. Other software products installed, including TSRs and device drivers (DEVICE=....) in config.sys and autoexec.bat.

f. The operating environment (e.g. DOS version) and CPU type (e.g. ‘386, ‘486, Pentium etc.), make/model of hard disks and adapters.

g. Direct problem reports and questions via your departmental IT security authority by mail, E-mail or fax to:

RCMP – TSB Client Services
Technical Security Branch
Technical Operations Directorate
1426 St. Joseph Blvd.
Ottawa, Ontario K1A 0R2

Attn:	TSB Client Services
Fax:	(613) 998-4832
E-mail:	TSB-clientservices@rcmp-grc.gc.ca

Please do not submit sensitive information!

5 Revision Summary

PROGRAM	CHANGES
DSX	Modified detection scheme for detecting highest read/writable sector on disk (V1.40; 2002-08-02) Added MBR pre-zero function to prevent PC's BIOS from adapting incorrect hard disk geometry, and enable verify for last pass only (V1.39; 2002-05-02) Minor modification for large hard disks (V1.38; 2001/08) Modified to reset the hard disk following the high cylinder auto-probe operation (Version 1.36) Modified to detect highest usable sector to prevent excessive disk write errors being reported at the upper bound. Last readable track potentially not being overwritten (Version 1.35; 2000-01-19) Modified to detect returned LBA values (formerly detected unreliable CHS values)
DV	Upgrade to V0.81 Upgraded as per DSX changes (V0.80) Modified to reset hard disk after high cylinder auto-probe operation (Version 0.79)
IDE	V1.11 Fixed displayed values V1.11 V1.12 Display capacity IDE Host Protected Area (HPA) V1.13 Display address offset feature setting

6 DSX Hard Disk Overwrite V1.40

6.1 General

There are situations where an entire hard disk has to be cleared to prevent information disclosure. Available methods include overwriting, degaussing and physical destruction. Selecting the appropriate clearing method should be based on factors such as: information sensitivity, disk re-use requirements, threat/risk factors and equipment serviceability.

For unserviceable hard disks, options are limited to repairing then overwriting (where practical), degaussing or physical destruction by approved methods. Serviceable media may be overwritten by using DSX to clear information (where appropriate). The clearing method should be appropriate with information sensitivity, threat and risk level.

The introduction described two recovery methods. The term **clearing** implies that information is overwritten and there is reasonable confidence that information cannot be recovered using Method 1. **Purging** implies protection from both Methods 1 and 2. Purging provides assurance that information cannot be recovered using laboratory techniques; this is usually performed by physical destruction or degaussing - thus rendering the hard disk unusable.

Using MS-DOS programs such as FDISK and FORMAT renders hard disk information inaccessible by MS-DOS. However, these programs merely initialize filesystem structures (see Glossary at Appendix B), leaving file data intact and recoverable using Method 1. In order to overwrite the entire disk, the DSX program may be used to clear information. DSX does not protect information from being recovered using Method 2, thus, using DSX alone should not be considered adequate to declassify hard disks.

6.2 Purpose

The DSX program overwrites standard IBM-PC/compatible magnetic hard disk media normally accessed via BIOS Int_13. DSX does not provide low level formatting of media. Due to the overwrite methodology, overwriting occurs independent of the installed filesystem. Hard disks accessible via the BIOS Int_13 interface are those visible using the “FDISK /STATUS” MS-DOS command.

6.3 Hard disk geometry and capacity

DSX determines the hard disk’s geometry and capacity via the system BIOS, thus if the hard disk is misconfigured a portion of the hard disk **may** remain intact. Thus, it is important to confirm the hard disk geometry and capacity using alternate means, such as:

a. Obtaining the make/model and technical information from the hard disk. This requires research to determine the correct geometry and capacity. One method is to browse the disk manufacturer’s Internet Web site (e.g. www.seagate.com); and

b. Using the IDE program, if the hard disk is E/IDE technology, to determine the hard disk make/model, geometry and capacity for verification.

Hard disk geometry is measured in cylinders, number of sides (heads) and sectors/track. These values (reported by DSX) should match the manufacturer’s specifications. DSX reports hard disk capacities in MB (= 1024 x 1024 bytes).

Where the PC does not have a Plug & Play BIOS (e.g. 386/486 PCs) and the hard disk is less than 504 MB in capacity, please refer to Appendix A.

Either a single or triple-pass overwrite may be selected. When the triple-pass option is selected, binary zeros (0s) are written on the first pass, binary ones (1s) on the second pass and an ASCII text pattern composed of the DSX version number and date/time stamp is written on the third pass. The last overwrite pass is followed by a verify pass. Selecting a single pass overwrite is identical to the final pass of the triple pass overwrite. Media I/O errors are reported and diagnosed to the sector level. Where disk errors occurred, it is conceivable that intelligible information remains in areas not successfully overwritten.

Where an overwrite report is required, the CTRL-P keys can be pressed simultaneously at the DOS prompt (A:\>) causing displayed output to be echoed to an attached printer (LPT1). Repeat the sequence (CTRL-P) to disable printer output.

Following overwrite, the Disk Viewer (DV) program should be used to inspect hard disk contents, **especially at the upper cylinder range**.

DSX is terminated by pressing the CTRL and C keys simultaneously. However, when DSX is terminated before normal completion the read-back verification cycle is not completed, as verification is performed only after the last overwrite cycle regardless as to whether a triple-pass or single-pass overwrite option was selected.

DSX accesses hard disks via the BIOS Int_13 interface, thus IDE and SCSI hard disks are accessible.

NOTE: When overwriting SCSI hard disks, the adapters' SCSI BIOS must be enabled at boot time; and SCSI ASPI drivers are not required.

6.4 DSX usage

The target hard disk's technical information should be obtained from the manufacturer's specifications (rated capacity per make/model) to verify the amount to be overwritten. If the capacity reported by DSX is less than the manufacturer's specifications, the excess portion will not be overwritten. Where hard disk technology is E/IDE, the IDE.EXE program can be used to determine visible size vs. rated size. See Appendix A if the PC is a 386/486 and the hard disk is greater than 504 MB.

Given the disk geometry in cylinders, number of heads and sectors per track, the disk's storage capacity in bytes is computed as:

Capacity = Cylinders x Heads x Sectors/Track x 512 bytes/sector

Ensure that the capacity computed by DSX matches the manufacturer's specifications because it is conceivable that the hard disk parameters in CMOS (or disk adapter) do not accurately reflect the hard disk storage capacity. *If the hard disk technology is E/IDE, the IDE.EXE program should be used to confirm the hard disk's storage capacity. DSX attempts to probe beyond the highest cylinder to determine if there is accessible storage space beyond the defined disk geometry.*

6.5 Launching the DSX program

a. Cold boot (Power-on) the PC using the prepared boot diskette in A: drive. Do not install or use any other software products. DSX should only be used in this environment.

b. Run DSX by entering: A:\> DSX

DSX displays the following:

DSX -- Hard disk Overwrite V1.xx 99xxxx (C)Copyright RCMP 1989-2002
Royal Canadian Mounted Police
UNAUTHORIZED USE / DISTRIBUTION PROHIBITED

For Gov't of CANADA official use only.

Reg'd to: DEMO COPY
Password:

c. Enter the assigned password. If an incorrect password is entered or if DSX.EXE has changed, DSX responds with the error message:

DSX -- FATAL: A:\DSX.EXE Failed SELF AUTHENTICATION!

Otherwise, DSX identifies INT_13 type hard disks available for overwriting:

Type	Id	Cyls	Heads	Spt	Size(Mb)	Mode
HardDisk	**0**	**751**	**8**	**17**	**49.8**	**CHS**
HardDisk	**1**	**733**	**5**	**17**	**30.4**	**CHS**

Enter HardDisk Id:

d. Due to changes in identifying the highest accessible sector on the hard disk, DSX may appear to stall while this activity is in progress.

Enter 0 to overwrite hard disk Id 0. DSX prompts for any changes required. If changes are required, DSX displays the current values and requests changes, then re-displays the revised hard disk characteristics.

Accept these parameters [Y / N] ?

If N is entered, DSX allows manual entry of cylinders, heads and sectors/track information and remains in the geometry modification cycle until the parameters are accepted.

e. Upon acceptance of the displayed parameters, the overwrite options are displayed.

1 = Single overwrite/verify pass
2 = Three overwrite/verify passes

Enter Option [1 or 2] ?

f. DSX responds with **"Are you ABSOLUTELY sure ?"** message. Respond with either Y (proceed) or N (restart).

This step is necessary to ensure that the PC's BIOS does not adopt the MBR partition table values as the disk geometry.

The hard disk's MBR/partition table is examined for pre-existing disk information. If the MBR/partition table contains non-zero data, DSX prompts for a response of either R or Z. R means resume (proceeds to overwrite), Z means zeroize the MBR/partition table then exit to DOS, the PC must be re-booted with the MS-DOS diskette and DSX must be re-started.

The overwrite process begins. The last overwrite pass is verified. The time required will vary with the overall PC/hard disk performance characteristics. However, the displayed begin/end time stamps of each pass provide some indication of the time required.

g. Hard disk contents should be visually inspected following overwrite. The DV program is provided for this purpose. Refer to the DV program documentation for operating instructions.

If the hard disk is to be re-used, it will be necessary to re-boot using a MS-DOS bootable diskette, then use the FDISK program to initialize partitions, then FORMAT each partition.

6.6 DSX example

The following is an example of the overwriting of a 20 MB hard disk.

Dimensions are as follows:

- cylinder range is 0 to 610 (611 cylinders),
- 4 sides (0 to 3), and
- 17 sectors/track (1 to 17).

```
A:\>DSX
DSX --  Disk Sanitizer V1.30 971120 (C)Copyright GKH 1989-1997

        For Government of CANADA official use only.

        Demo Version <Licenced agency name>

        Type  Id Cyls Heads Spt Size (Mb) Mode

        HardDisk 0  611  4 17  20.2 CHS

        Enter drive Id ? 0    <===== First hard disk

DSX --  Hard Disk # 0 Parameters:
        HardDisk # .....…….. 0
        Number of Heads.….... 4 ( 0 - 3 )
        Number of Cylinders... 611 ( 0 - 610 )
        Highest Sector....……. 17 ( 1 - 17 )
```

Drive capacity is 21272576 bytes <===== Make sure this value matches the mfgr's specs. for make/model
Accept disk parameters [Y/N] ? Y <===== Accept values

OverWrite options:

1 = Single Overwrite/Verify pass
3 = 3 OverWrite/Verify passes

Enter option [1 or 3] ? 3 <===== Select 3 pass option

Are you ABSOLUTELY sure [Y/N] ? Y <===== Final confirmation

DSX begins the triple-pass overwrite process and displays the status for each pass. At completion, it is recommended that the DV program now be used to inspect the hard disk. Performance will vary depending on the CPU type and hard disk.

7 DV Disk Viewer V0.81

7.1 Introduction

The DV program provides services to view standard hard disk and diskette media independent of the filesystem structure. Disks are accessed physically through the BIOS Int_13 services by drive number, cylinder, head and sector. DV is issued with the DSX program to provide the ability to inspect the contents of hard disks prior to and following overwriting.

7.2 Limitations

DV operates on IBM-PC/compatible systems operating with MS-DOS V2.0 to V6.22. Disks must be pre-formatted and conform to the standard DOS disk characteristics (i.e., 512 bytes/sector). Additionally, hard disks must be accessible via BIOS Int_13.

At start-up, DV determines the number of each physical hard disk and/or diskette type. DV cannot access logical drives such as network and assigned logical drives, as these are not physical drives. Diskettes are addressed as drives A or B, hard disks as 0 to 3 for the first to fourth hard disks respectively.

DV self-authenticates at start-up when used with MS-DOS V3.0 and later versions. Authentication failure implies loss of image integrity.

DV does not restrict the upper cylinder boundary for floppy diskettes. For hard disks, however, the upper cylinder boundary is limited to 10 cylinders beyond the highest reported, subject to the 1024 cylinder limit. This limitation exists to prevent possible hard disk damage when attempting to seek beyond the uppermost cylinder boundary, as some controller/disk combinations allow unchecked cylinder addressing.

The number of sectors per track is limited to the reported number (by the disk controller) for hard disks and to 63 sectors per track for diskettes. DV obtains the disk dimensions from the disk controller.

7.3 Usage

DV displays data in one of four modes:

- 64 ASCII characters per line with offset address labels (default),
- 80 ASCII characters per line (full display page format),
- 16 hexadecimal bytes per line with offset address labelling and ASCII interpretation, or
- eight hex integers (16 bit) per line with offset address labelling and ASCII interpretation.

Graphic character display is controlled by the F9 key (state toggle). The default mode is ASCII, where non-ASCII and non displayable ASCII characters are represented by a period (.).

Data extraction/output services are implemented by the F3 and F4 functions. F4 controls the output device/file specification and mode; F3 triggers the output action.
Two data output modes (TEXT and UNFORMATTED) are supported by function F4. The output disposition can be selected between LPT1: and a named DOS output file. The output mode can be

selected between TEXT and UNFORMATTED. TEXT mode means that whenever the F3 key is pressed, a text (ASCII) representation of the current display screen is written to the selected output device or file. In UNFORMATTED mode, each time F3 is pressed, the entire current track is written to the output file. UNFORMATTED output is restricted to an output file.

DV provides data search services in both ASCII and hexadecimal modes. The search function allows either EXACT or case insensitive ASCII string searches. The search function is entered via F5 function (to define the search string), and depending on the current display mode, may be either in hexadecimal or ASCII. The string search function does not include strings that span track boundaries.

Once started, the current disk number, cylinder and head positions are displayed at the top of the display. The function keys are displayed on the bottom two lines.

The command line format is:

A:\> **DV { disk }** (disk = physical disk spec: A, B, 0, 1, 2 or 3)

At start-up, DV displays the title/help screen, then self-authenticates. To start DV, press the ENTER key following self-authentication. The F8 (disk parameter) function is invoked automatically. When the disk and dimension parameters are selected, DV displays the contents of the starting cylinder and track. The function keys are enabled and are described below.

7.4 DV function key description

F1 Toggles the display mode. The next mode is highlighted. Available modes are HEX, TXT64 (default), TXT80 and HXINT, where 352, 1408, 1760 and 352 bytes per page respectively are displayed. The title/help screen is displayed as the fifth display mode. While in this screen, only the F1 and F10 function keys operate.

F2 Toggles the address labelling for HEX and TXT64 display modes, inoperable in TXT80 display mode. There are four labelling formats: decimal bytes, hexadecimal bytes, sector number with hex offset (default) and sector number with decimal offset. The address labels are located on the left side of the display.

F3 Either the current display screen (TEXT) or the entire track (UNFORMATTED) is written to the selected output device or file. The default output device is LPT1. The F4 function allows the user to specify the disposition and mode (formatted TEXT or UNFORMATTED). The F10 key terminates an active output cycle. When output is to a named DOS file, the F3 function monitors the remaining available storage space on the output volume.

Unformatted output may be selected only when the output is directed to a file. In unformatted mode, the entire current track is written to the target file, regardless of the current display page position within the track.

For TEXT mode output, each line is highlighted when written. In unformatted mode, the entire display window is highlighted for the duration of the write operation. Graphic characters are substituted with a dot (.) when written to the output file.

F4 Selects the output mode and device/file for data extraction. Output to LPT1 or DOS file is supported in TEXT mode. In unformatted mode, only a named DOS file is allowed. When LPT1: is selected, the output mode is fixed at TEXT mode. If file is selected, DV allows the user to select the output mode, either TEXT or UNFORMATTED. TEXT implies that each time F3 is pressed, the current display page is written in ASCII text. When F3 is pressed in UNFORMATTED mode, the entire contents of the current track are written to the output file. UNFORMATTED mode is restricted to file output. When TEXT mode is selected, a CAPTION may be entered to label the TEXT mode output.

TEXT or UNFORMATTED mode is selected by movement of the left arrow (<-) or right arrow (->) or space keys, followed by pressing the ENTER key. The selection is then highlighted. If FILE output is selected, the filename must be entered, followed by ENTER.

F5 Selects the string search function based on current display mode. When the current display mode is either TXT64 or TXT80, an ASCII string may be entered. When the display mode is HEX, a HEXADECIMAL string is expected. A maximum of 32 bytes may be entered. The search is activated when the string is terminated by the ENTER key. F10 terminates the search function. Searches in HXINT display mode are inhibited.

F6 Resumes a string search starting from the currently displayed page and mode (F1). The F10 key terminates the search. F5 and F6 causes searching to proceed in advancing sectors, tracks and cylinders starting from the current display page. When the string is found, the page is displayed and the search string is highlighted. If unsuccessful or aborted by F10, the page displayed prior to invoking the search is re-displayed.

F7 The track editing feature is not implemented in this release.

F8 The disk to be viewed is selected and its parameters may be altered by this option. The range of available diskettes and hard disks are displayed. Diskettes may be specified as either A or B, and hard disks as 0 or 1 (first or second hard disk). Enter the desired disk id at the "Select Disk" prompt then press ENTER. The disk's parameters are obtained and displayed. Parameters may be altered by cursor positioning and data entry beside the appropriate dimension then set by pressing the ENTER key. The cylinder scan increment/decrement value may be adjusted up to a value representing 25% of the total cylinder count. The default cylinder scan increment is approximately 5% of the disk's cylinder count.

To accept an existing parameter value, press the down arrow or ENTER keys. By pressing either the down arrow or ENTER key when the cursor is adjacent to the Cylinder Scan Increment, F8 exits and disk viewing begins.

The reported number of cylinders for the hard disk may be exceeded by +10 cylinders in CHS mode, e.g., if an adapter reports 613 cylinders, the maximum allowable cylinder value is 618.

In CHS mode disk geometry is limited by the BIOS; the highest cylinder number is 1023, the highest head is 254 and the highest sector is 63, the maximum disk capacity supported in CHS mode this approximately 8 GB. LBA mode extends disk geometry such that capacities exceed this barrier.

The initial Access Mode is CHS mode. If the BIOS extensions are present, LBA mode can be used to access hard disks larger than 8 GB. To change modes, enter either C for CHS mode or L for LBA mode at the Access mode field.

F9 This is a graphic character display filter. F9 toggles between ASCII/Graphic and ASCII only. In the latter state, graphic characters are replaced by a dot (.).

F10 Terminates Disk Viewer or active functions. If pressed while processing functions F3, F4, F5, F6 or F8, the functions are terminated and DV returns to command mode. In command mode, F10 prompts [Y/N] for termination.

7.5 DV disk display navigation

Disk display navigation is performed by the following keys:

Home Displays the beginning of the current track (starting at lowest sector).

PgUp Displays the previous page of the current track.

PgDn Displays the next page of the current track.

End Displays the last page of the current track.

ENTER The next track is displayed starting at the lowest sector position. Advances to next track/cylinder as required.

BkSp The previous track is displayed starting at the lowest sector position. Decrements the cylinder position as required.

Ins Increment the cylinder position. Does not alter head and sector position.

Del Decrement the cylinder position. Does not alter head and sector position.

[Scroll to previous Display page. Decrements by sectors/head/cylinder as required.

] Scroll to next Display page. Advance sectors/head/cylinder as required.

SPACE Repeats the last scroll page command, either [or].

\+ Increments the current cylinder position by the pre-set cylinder scan increment (as defined by F8). The maximum allowable increment is limited to 25% of the selected disk's total cylinder count. The default increment is approximately 5% of the total cylinder count. However, the increment may be manually adjusted from one cylinder to a number representing up to 25% of the disk's cylinder count. The adjustment is made while processing the disk parameters via function F8.

\- Identical to the + key, except that the current cylinder position is decremented by the cylinder scan increment. The + and - cylinder positioning is intended for use in scanning disk contents.

>	The right arrow increments the display offset by one byte within the currently displayed track.
<	The left arrow decrements the display offset by one byte within the currently displayed track.
^	The up arrow scrolls the currently displayed track by one line
v	The down arrow scrolls the currently displayed track by one line.

7.6 DV error messages

DV accesses disk media on a track-by-track basis. When a sector within a track is inaccessible, DV re-reads the track sector by sector. For inaccessible sectors, DV places the error message within the display buffer for the inaccessible sector.

8 IDE E/IDE Hard Disk Identification V1.13

8.1 Introduction

The IDE program acquires ATA (IDE) hard disk identification information from master and slave IDE hard disks on the primary and secondary IDE ports (1F0h and 170h). The purpose of directly acquiring IDE hard disk information is to display the hard disk identification information independent of the PC's BIOS functions. Identification information including geometry, capacity, host protected area (HPA) and address offset presence/use are displayed.

8.2 Usage

IDE is launched at the command line, ideally via the autoexec.bat file of the forensic boot diskette. The parameters for each hard disk attached to ports 1F0h and 170h are displayed. Information includes:

- Make / Model
- Serial number
- Adapter revision
- Disk geometry (adapter vs. BIOS) and capacity
- Host Protected Area (HPA) and LBA Address Offset information

The command line format is:

```
A:\> IDE { /R=a:\report.ide /P /C }
```

IDE has three processing options via command line only, described as:

/R Causes IDE to write displayed output to a named file (recommended).

/P Causes HPA changes to be made permanent (default is volatile).

/C Allows creating an HPA only when current sectors = native maximum sectors. If an HPA partition exists, re-run IDE using the /C option to temporarily change the HPA sector value to be equal to the max native sectors value. This remains in effect until the disk is reset (volatile), or, if the /P option was included, the change is permanent. It is recommended that the /R option be used to produce a softcopy record of these values.

8.3 IDE – Example 1

Display IDE hard disk information of installed E/IDE hard disks (port addresses 1F0h and 170h). The hard disk - originally approximately 40 GB - has been made to look like 20 GB.

```
A:\> IDE /R=A:\REPORT.IDE
```

```
IDE -- Identify IDE Hard disk V1.13 020915 (C)Copyright RCMP/GRC 1996-2002
 1 Hard disks reported via BIOS Int 13h.

IDE Hard disk 0: Adapter Port 1F0h Master
ATA Std(s): ATA-5 ATA-4 Res ATA-3 Obs. Obs.
 Host Protected Area..: Supported, Enabled.  <= HPA capability, used
```

```
Address Offset...……...: Supported, Disabled. <= Address Offset, unused
Disk Model.....……...: MAXTOR6L040J2
Serial Number...……...: 362205220886
Adapter Rev...…….....: A93.0500

IDE Disk Geometry                    Direct    BIOS
------------------ ----------------------------------------------------
Cylinders.....…….....:  38792        38792
Heads.....……...:  16              16
Sectors/Track…….....:  63             63
Capacity.(Sectors)……....: 39102336  39102336          <= User accessible sectors
Capacity.( ~ Mb )……..: 19092.93   19092.93
Max Native Sectors……..: 78177792                      <= Maximum sector count
Max Capacity.( ~ Mb )……..: 38172.75
Hidden sectors…….....: 39075456                       <= Amount hidden from user
IDE -- FATAL: (IDE) IDE Disk Adapter Port 1F0h Slave timed out ( No disk attached ).
IDE -- FATAL: (IDE) IDE Disk Adapter Port 170h Master timed out ( No disk attached ).
IDE -- FATAL: (IDE) IDE Disk Adapter Port 170h Slave timed out ( No disk attached ).
IDE -- INFO: Total of 1 Int_13 IDE Hard disks located.
```

8.4 IDE – Example 2

Example using R and P options:

```
A:\> IDE /R=A:\report.ide /P
```

Display the ASCII/Hex dump of device identification, create a report file and if HPA changes are made, make it permanent. Both master and slave devices of each IDE port (maximum of four disks) are queried.

8.5 Restrictions

The IDE program should be included on a forensic boot diskette to record hard disk profiles. IDE functions in native MS-DOS mode only, applies only to standard I/O port addresses 1F0h and 170h respectively, and does not apply to SCSI hard disks.

Limited testing indicates that changing the HPA value leaves the user data area content intact. As this function is actually performed by the hard disks' onboard electronics, there is no guarantee that all hard disks will leave user data intact.

The Host Protected Area (HPA) is defined as an area of hard disk storage that is made to be inaccessible. The HPA (when used) starts from a specified address and extends to the highest (native maximum) sector of the hard disk.

HPA information is displayed (assumes 28 bit LBA addressing) if supported. If the native maximum sector count exceeds the reported current capacity in sectors value, the user is prompted for "Y" to reset the current capacity to the native maximum capacity to allow access to the hidden area. This setting remains in effect until the next disk reset command or power off/on cycle, unless the /P option is specified, in which case the change is made permanent. When the HPA value is changed, it is necessary to re-boot the system so that the BIOS can re-evaluate the hard disk parameters.

The /C option is used to create an HPA, by allowing setting the HPA to a value to create a hidden partition. The /C option is only effective when the HPA is set to the native maximum number of sectors

(no hidden space). The hidden partition size in sectors is the native maximum size less the HPA value entered.

Appendix A - Non-Plug & Play BIOS PC & Disks > 504 MB

This section applies to PC systems in the XT, 286, 386 and 486 class range. PCs have pre-programmed functions in Read Only Memory (ROM) referred to as the system BIOS. One of the BIOS functions is to interface the operating system to physical devices such as keyboards, monitors and hard disks. This technical note explains why and under what circumstances the DSX program may not always be able to overwrite an entire hard disk. If the hard disk to be overwritten is E/IDE technology, the IDE program can be used to determine if the entire disk is mapped by the BIOS.

Non-plug & play BIOSs (older) accommodate hard disks up to 504 MB. This value is derived from the following calculation:

1024 cyls X 16 heads X 63 Sectors/Head X 512 bytes/Sector = 528,482,304 bytes

- where 528,482,304 / (1024 X 1024) = 504 MB.

The basis for the values is due to the design limitations of DOS & BIOS. Disk geometry limits are:

- 1024 cylinders
- 16 heads
- 63 sectors/track

It is possible to install a hard disk having a capacity greater than 504 MB on a non-Plug & Play system. The most common scheme is to use software called a DDO (or Dynamic Disk Overlay program). The DDO is loaded at system boot, becoming memory resident and serving as supplemental BIOS software that translates access to the hard disk. Typically, many modern hard disks exceed 1024 cylinders. The mapping methodology extends the head limit from 16 to 255, thus, by manipulating the cylinder and head numbers, it can physically map hard disks up to approximately 8 GB while remaining within the geometry limits. In the absence of the DDO, a hard disk having a capacity greater than 504 MB cannot be entirely overwritten.

The recommended solution is as follows:

> Install the hard disk (> 504 MB) into a Pentium class PC. At power-on, enter the CMOS SETUP function then “AutoDetect/Configure” the hard disk to its maximum capacity. Re-boot using a MS-DOS V6.x diskette, run the IDE program to confirm disk size, then run DSX. Ensure that the hard disk’s visible capacity matches the manufacturer’s values for the hard disk model. At completion, use the DV program to inspect the hard disk.

Also, be aware that some early Pentium class PCs are limited to handling hard disks up to 8.4 GB. Hard disks larger than 8.4 GB can only be accessed by the BIOS Extended I/O Functions, as low level access requires LBA mode beyond the 8.4 GB barrier.

Appendix B - Glossary

BIOS BIOS is the acronym for Basic Input Output System. The BIOS is the permanent set of programs that reside on (E)EPROM (permanent memory) on the PC's motherboard. The BIOS contains programs that are executed when the PC is powered on. These programs perform system initialization at power on and serve as the software interface between the operating system and the system peripheral hardware.

CHS Refers to Cylinder, Head and Sector. These are geometry measurements for hard disks (legacy). CHS values are limited to 1024 cylinders, 256 heads and 63 sectors/track.

Degauss A process performed by a degauser, which sanitizes magnetic media via exposure to a strong, fluctuating magnetic field. The magnetic field strength (measured in Oersteds) must be of prescribed strength depending on type of media being degaussed. Under prescribed conditions, this is an approved method of declassifying media, but it renders the hard disk unusable.

FileSystem **(**a.k.a. volume) A filesystem is informally defined as a disk structure that is used for file organization. An MS-DOS filesystem is composed of a boot record, FAT(s), a root directory and the remaining space is available for file storage. A filesystem is addressable by drive letter.

GB Acronym for Giga bytes (1024 x 1024 x 1024 bytes)

KB Acronym for Kilo bytes (1024 bytes)

LBA Acronym for Logical Block Address. LBA mode is the method of accessing hard disks that exceed the legacy CHS limits. LBA addressing of a disk is via 28 or 48 bit sector number rather than cylinders, heads and sectors/ track.

MB Acronym for Mega byte (1024 x 1024 bytes)