FOI
SWEDISH DEFENCE
RESEARCH AGENCY

FOI-R--1638--SE
February 2005
1650-1942

Technical report

Computer Forensics and the ATA Interface

Arne Vidström

Command and Control Systems
Box 1165
SE-581 11 LINKÖPING
Sweden

Swedish Defence Research Agency
Command and Control Systems
Box 1165
SE-581 11 LINKÖPING
Sweden

FOI-R--1638--SE
February 2005
1650-1942

Technical report

Computer Forensics and the ATA Interface

Arne Vidström

Issuing organization Swedish Defence Research Agency Command and Control Systems Box 1165 SE-581 11 LINKÖPING Sweden	Report number, ISRN FOI-R--1638--SE	Report type Technical report
	Programme Areas C4ISTAR	
	Month year February 2005	Project no. E7091
	General Research Areas Commissioned Research	
	Subcategories C4I	
Author/s (editor/s) Arne Vidström	Project manager Mikael Wedlin	
	Approved by Johan Allgurén	
	Sponsoring agency Swedish Armed Forces	
	Scientifically and technically responsible	

Report title

Computer Forensics and the ATA Interface

Abstract

This report describes the parts of the ATA interface that are relevant to computer forensics. Only software techniques are covered. Some tests of forensics and disk wiping software are shown, toghether with a test of a hardware write blocker. The results show weaknesses in all the products tested.

Keywords

Further bibliographic information	Language English
ISSN 1650-1942	Pages 31
Distribution By sendlist	Price Acc. to pricelist Security classification Unclassified

Utgivare

Totalförsvarets forskningsinstitut
Ledningssystem
Box 1165
SE-581 11 LINKÖPING
Sweden

Rapportnummer, ISRN

FOI-R--1638--SE

Klassificering

Teknisk rapport

Forskningsområde

Ledning, informationsteknik och sensorer

Månad, år

Februari 2005

Projektnummer

E7091

Verksamhetsgren

Uppdragsfinansierad verksamhet

Delområde

Ledning med samband, telekom och IT-system

Författare/redaktör

Arne Vidström

Projektledare

Mikael Wedlin

Godkänd av

Johan Allgurén

Uppdragsgivare/kundbeteckning

FM

Tekniskt och/eller vetenskapligt ansvarig

Rapportens titel

Datautredning och ATA-gränssnittet

Sammanfattning

Den här rapporten beskriver de delar av ATA-gränssnittet som är relevanta vid datautredning. Endast mjukvarutekniker berörs. Några tester av mjukvara för datautredning och diskradering presenteras, tillsammans med ett test av ett hårdvaruskrivskydd. Resultaten visar på brister hos alla produkter som testats.

Nyckelord

Övriga bibliografiska uppgifter

Språk

Engelska

ISSN

1650-1942

Antal sidor

31

Distribution

Enligt missiv

Pris Enligt prislista

Sekretess Öppen

Contents

1 Introduction **7**

1.1 Background 7

1.2 Prerequisite knowledge 7

1.3 Scope 7

2 Playing tricks with the disk size **9**

2.1 Host Protected Area 9

2.1.1 HPA commands 9

2.1.2 HPA and computer forensics 9

2.2 Device Configuration Overlays 10

2.2.1 DCO commands 10

2.2.2 DCO and computer forensics 10

2.3 Interactions between HPA and DCO 10

2.4 Advice to the investigator 11

3 The use of SMART in computer forensics **13**

3.1 Documentation issues 13

3.2 Interesting attributes 13

3.2.1 Reallocated Sectors Count 13

3.2.2 Power-On Hours 13

3.2.3 Reallocation Event Count 13

3.3 Reliability of the information 13

3.4 Advice to the investigator 14

4 Defect Management **15**

4.1 The P-list and the G-list 15

4.2 Defect Management and computer forensics 15

4.3 How to gain access to defect sectors 15

4.3.1 Undocumented vendor proprietary commands 15

4.3.2 Using SMART 16

4.3.3 Format Track 16

4.3.4 Enhanced Erase Mode 16

4.3.5 Disabling Automatic Defect Management 17

4.4 Advice to the investigator 17

5 Other issues related to ATA and computer forensics **19**

5.1 The Security Mode feature set 19

5.1.1 Accessing with a known User Password 19

5.1.2 Accessing with a known Master Password 19

5.1.3 Accessing with a default Master Password 19

5.1.4 Other cases 20
5.2 Firmware updates 20
5.3 Advice to the investigator 20

6 ATA utilities useful in computer forensics 21
6.1 ATA Password Tool 21
6.2 HDAT2 21
6.3 HDD Erase 21
6.4 TAFT - The ATA Forensics Tool 21
6.5 Advice to the investigator 21

7 HPA and DCO capability tests with EnCase, DBAN, ExpertEraser, and CoreSHIELD 23
7.1 Hardware and software common among the tests 23
7.2 EnCase Forensic Edition 4.18a run in Windows 23
7.3 EnCase Forensic Edition 4.18a run in DOS 24
7.4 EnCase Forensic Edition 4.18a run in DOS with CoreSHIELD Rev 1.00 24
7.5 DBAN 1.0.4 24
7.6 ExpertEraser 2.0 25
7.7 Advice to the investigator 25

8 A test of the hardware write blocker CoreSHIELD 27
8.1 Requirements for a hardware write blocker 27
8.2 Information category operations 27
8.3 Operating system caching issues 28
8.4 Advice to the investigator 28

9 Questions which remain unanswered 29

Bibliography 31

1. Introduction

1.1 Background

The research described in this report has been performed as part of our research in the field of Intrusion Analysis. Even if the final result of such an analysis will not neccessarily end up in a court of law, it is still essential to have a sound procedure for collecting the evidence to be used as input for the analysis. Important evidence must not be left out, altered, or destroyed. In cases where evidence is to be collected from an ATA hard disk, it is necessary to be aware of all the relevant intricacies of ATA. Thus, this part of computer forensics is vital to Intrusion Analysis.

One goal of our ATA computer forensics research was to determine and document the current state of the art. The other goal was to add some new knowledge to the field, primarily gained by analysing the most recent draft revision (4b) of the latest ATA specification (ATA-7) from INCITS Technical Committee T13 [1].

1.2 Prerequisite knowledge

To be able to understand the report, the reader is assumed to have knowledge about ATA at a level where concepts like LBA and SMART are familiar. The reader is also assumed to have knowledge about computer forensics at a level where concepts like forensic imaging and disk wiping are familiar. Further, the reader is encouraged to experiment with the tools described in Chapter 6, since such experimentation is vital to fully understanding all the details covered in the report.

1.3 Scope

The topics covered in the report apply to ATA in general, that is, both to the newer S-ATA (Serial ATA) and classic P-ATA (Parallel ATA). However, some of the tools described in Chapter 6 are not able to work with S-ATA controllers that do not support the so called Compatibility Mode. This is not because the command sets of S-ATA and P-ATA are different, but because the commands are sent to the controller in a different way.

The report is concerned with what can be performed with software through the ATA interface. Alternative physical disk access methods exist, but these are not covered. Also, this is not a complete analysis even of the software connections between ATA and computer forensics. There are still issues left to research in this area other than the ones covered by this report.

2. Playing tricks with the disk size

It is important for an investigator to be aware of techniques that change the disk size, because otherwise a large piece of the disk could be missed out during an investigation. Also, disk wiping tools must be able to handle these issues or they will not wipe the whole disk.

2.1 Host Protected Area

Host Protected Area (HPA) is an optional feature that first appeared in the ATA-5 standard. Even though HPA is optional, I have never seen a modern disk without HPA support.

One legitimate use of HPA is system recovery. The original contents of a system installation can be stored in a protected area on the disk. [1] When needed, these original contents can be copied to the regular part of the disk for easy recovery. If HPA has been used for this purpose it might be possible for the investigator to find valuable evidence in the hidden recovery part of the disk.

2.1.1 HPA commands The central command in HPA is SET MAX ADDRESS, which is used to make a disk appear smaller than it really is. The 48-bit extended version is named SET MAX ADDRESS EXT. When both of these commands are referred to, the notation SET MAX ADDRESS (EXT) will be used. SET MAX ADDRESS (EXT) can be run in volatile or non-volatile mode, as specified in the parameters. In non-volatile mode the disk retains the new maximum size even when the power is turned off. A disk supporting HPA also has the READ NATIVE MAX ADDRESS command, and in the case of a 48-bit disk, also the READ NATIVE MAX ADDRESS EXT command. These commands show the highest factory default address of the disk. See Figure 2.1.

2.1.2 HPA and computer forensics It is possible to detect that HPA is being used by comparing the output from the IDENTIFY DEVICE and the READ NATIVE MAX (EXT) commands. When SET MAX ADDRESS (EXT) has been issued to make the disk smaller, the two commands will show different sizes. To gain access to the whole disk, one must run SET MAX ADDRESS (EXT) to restore the size to the factory default.

[1] The Address Offset Feature proposal (http://www.t13.org/technical/d98123r3.pdf) suggests SET FEATURES subcommands for logically swapping the protected and the non-protected areas.

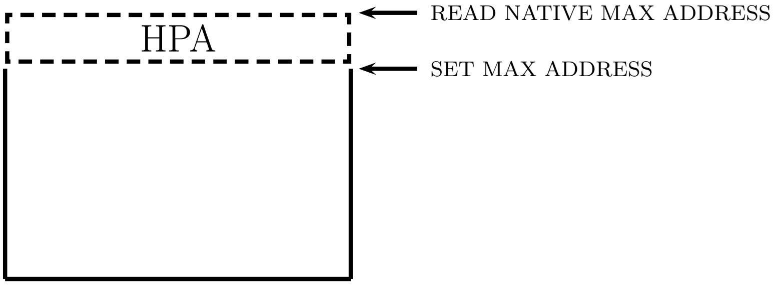

Figure 2.1: Using HPA, a disk can be made to look smaller than it really is.

2.2 Device Configuration Overlays

Device Configuration Overlays (DCO) is another but much less well-known optional feature set. It first appeared in the ATA-6 standard and because of this it is not supported by quite as many disks as HPA is.

2.2.1 DCO commands Modifying the disk size with the DEVICE CONFIGURATION SET command [2] is a bit more powerful than doing it with HPA. The reason for this is that the response from READ NATIVE MAX (EXT) is also changed when using DCO. There is however a command called DEVICE CONFIGURATION IDENTIFY that shows the true size of the disk. A DCO setting is always non-volatile.

2.2.2 DCO and computer forensics It is possible to determine the presence of a DCO setting through a comparison between the output of the commands DEVICE CONFIGURATION IDENTIFY and READ NATIVE MAX (EXT). Using the command DEVICE CONFIGURATION RESTORE it is possible to remove the DCO set, and thereby restore the original size of the disk.

2.3 Interactions between HPA and DCO

The DEVICE CONFIGURATION SET command fails to change the size of the disk if the SET MAX ADDRESS (EXT) command has already been issued to do the same. According to the ATA-7 specification draft [2] the reason for this behaviour is that the DEVICE CONFIGURATION SET command must not cause the loss of a possible HPA. I have not been able to find any statements about what should happen when the commands are run in the other order. Testing on a couple of disks showed that it was indeed possible to run SET MAX ADDRESS (EXT) after running DEVICE CONFIGURATION SET.

For restoration to the factory default size on a disk where both HPA and DCO have been used, SET MAX ADDRESS (EXT) must be run before DEVICE CONFIGURATION RESTORE. Running the commands in the other order will cause an error.

[2] DEVICE CONFIGURATION SET is not limited to setting the disk size - for example it can also disallow reporting of various feature sets.

2.4 Advice to the investigator

The general method used by an investigator should always be to compare the size of the forensic image with the sizes reported by the commands described above, as well as with the factory default size that can be found in the data sheet from the manufacturer. Any differences found should prompt further investigation of the issue. Using this method is important because there could possibly exist other ways to play tricks with the disk size except than with HPA and DCO. Also, an investigator should not automatically assume that the label on a disk is the original one.

When using forensic imaging tools or disk wiping tools it is essential to know if and how they handle HPA and DCO. Practical tests with some tools can be found in Chapter 7.

3. The use of SMART in computer forensics

The SMART feature set appeared already in the ATA-3 specification. All modern disks I have encountered have had SMART support to at least some extent.

3.1 Documentation issues

SMART is intented to give a view of the current health status of a disk, so as to make it possible to get an early warning before a possible breakdown.

The central SMART command is called SMART READ DATA and it retrieves a 512 bytes large data structure. Only the general layout of the structure is specified. More details can be found in the SFF Committee Specification for Self-Monitoring, Analysis and Reporting Technology (S.M.A.R.T.) [3]. But this specification does not reveal all details about SMART either.

The attributes available and the meanings of their values are vendor specific.

3.2 Interesting attributes

From the unofficial documentation [4] some attributes have been found interesting for computer forensics purposes.

3.2.1 Reallocated Sectors Count This attribute (5) contains the number of remapped sectors and will be discussed in more detail in Section 4.3.2.

3.2.2 Power-On Hours This attribute (9) tells the total power-on time of the disk. For example the value can be used to determine if a disk is fairly new or not. The value need not always be in hours as its name suggests - it can also be in minutes or seconds, depending on the manufacturer.

3.2.3 Reallocation Event Count This attribute (196) tells how many times the disk has tried, successfully or not, to perform defect sector remapping.

3.3 Reliability of the information

We have already seen that the main part of SMART is vendor specific and not officially documented. This in itself is a bad sign when it comes to using it in forensic investigations. The value of such evidence can indeed be quite doubtful.

A specific example can be found in the case of the Power-On Hours attribute. The unofficial documentation [4] tells us that this value can be in hours, *or* in minutes, *or* in seconds, all depeding on the manufacturer. If a tool would name this attribute simply "Power-On Hours" and give a number of for example 4572, the investigator could be led to believe that the disk has been in use for over half a year, when in fact it could have been in use no more than one-and-a-half hours.

According to [5], some disks even have a Power-On Hours attribute value that increases unpredictably, resets every 1092 hours, and/or is 7% off.

3.4 Advice to the investigator

Since SMART is not very well documented, investigators should be very careful before using any information retrieved by it as evidence. It is doubtful if any SMART values can be safely used except if retrieved by a disk manufacturer tool and interpreted with the guidance of the manufacturer.

4. Defect Management

It is very hard to manufacture disks that have a completely defect-free disk surface. A disk might also develop defects after leaving the factory, caused by anything from dropping it to general wear. Modern disks use a technology called *Defect Management* to handle both kinds of defects. A number of *spare sectors* are available, and defect sectors can be remapped without any visible loss of disk size.

4.1 The P-list and the G-list

Two internal lists in a disk are used to keep track of the defect sectors. The *P-list*, or *Primary Defect List*, is a list of the sectors that were already found to be defect at the factory. The *G-list*, or *Growing Defect List*, is a list of the sectors that are found to be defect after the disk leaves the factory. Thus, the G-list is updated dynamically while the disk is in use.

4.2 Defect Management and computer forensics

Defect Management is important in computer forensics for at least two reasons:

- It is important to know whether or not contents of defect sectors can be (and are) retrieved during an investigation

- It is important to know whether or not defect sectors can be (and are) wiped using a software tool

4.3 How to gain access to defect sectors

To answer the questions raised above we have to take a look at how to gain access to defect sectors in the first place.

4.3.1 Undocumented vendor proprietary commands It is possible to find statements here and there on the Internet about the use of undocumented vendor proprietary commands for the control of the P- and G-lists. However, I have not been able to find any documentation of such commands, neither leaked from manufacturers nor produced by reverse engineering. This does not mean that such commands do not exist - on the contrary it is quite possible that they do - but the field simply seems to be unexplored by researchers outside the disk industry.

4.3.2 Using SMART The most common use of SMART is to retrieve a list of attribute values through the SMART READ DATA command. The various attribute values are intented to represent the current health status of the disk, so as to make it possible to get an early warning before a possible breakdown.

The number of remapped sectors is contained in attribute number 5 on many disks (see Section 3.2.1). An imaging or disk wiping tool could quite easily check if this attribute value is zero or not. If the value is zero, one might feel inclined to assume that the P- and G-lists are empty. If they are not empty, the tool could warn that the disk cannot be completely imaged or wiped with software only.

A problem with the above assumption is that there is no official documentation that specifies exactly what attribute number 5 actually stands for in the case of a specific disk. Is it the number of sectors in both of the lists combined, in the G-list only, or something else completely?

Another SMART connection is the vendor specific subcommands E0h to FFh. Any of these *might* be a way to control the P-list and the G-list. There is at least one disk wiping tool that is claimed to wipe defect sectors on disks with SMART support. This is a hint that using the vendor specific subcommands might be a possibility in this case. But once again, things are too uncertain to make it possible to draw any definitive conclusions.

4.3.3 Format Track The ATA-1 specification contained a command named FORMAT TRACK to be used for low-level formatting. The effect of the command was explicitly stated to be vendor specific - and it could even do *nothing* when executed. One command parameter could be used to control sector remapping. However, the specification allowed this parameter to be completely ignored.

In the ATA-2 specification the FORMAT TRACK command was even less documented, this time it was only described as vendor specific without any details. It was even stated that use of the command is not recommended.

Finally, FORMAT TRACK was removed completely in the ATA-5 specification and onwards.

Using FORMAT TRACK to gain access to defect sectors *might* be possible, but it can certainly not be recommended considering the small amount of documentation available.

4.3.4 Enhanced Erase Mode If we only want to wipe defect sectors we might look at the *Security Mode feature set*. This feature set first appeared in ATA-3 and among other things it contains a command called SECURITY ERASE UNIT. Even though the command was intended for other purposes (see Section 5.1) it can be used by disk wiping tools.

It seems more or less certain that when run in the so called *Normal Erase Mode* the command will *not* wipe defect sectors. The specification does not state this explicitly though.

With ATA-5 came *Enhanced Erase Mode*, about which the ATA-7 draft [2] (page 239) clearly states that *"all previously written user data shall be overwritten, including sectors that are no longer in use due to reallocation"*.

Unfortunately, Enhanced Erase Mode does not seem to be supported in practice. I have not yet encountered a single disk with Enhanced Erase Mode support.

4.3.5 Disabling Automatic Defect Management In the ATA-3 specification a couple of new subcommands to the SET FEATURES command appeared. One of them was called *Enable all automatic defect reassignment* and the other *Disable all automatic defect reassignment*. The subcommands were vendor specific. By ATA-5 the commands had been made obsolete.

Since the commands are now obsolete, and vendor specific when they were in use, it does not seem to be a good idea to use them to disable Automatic Defect Management. Otherwise it would have been a possibility for an organization to disable automatic defect reassignment on new disks to keep their G-lists empty. This would have made it easier to perform more complete disk wipes.

4.4 Advice to the investigator

Some tools are claimed to be able to gain access to defect sectors, to wipe their contents securely, and so on. I have not been able to find any reliable documentation about how this is supposed to be performed. Forensic investigators and users of disk wiping tools should be aware of the possible risks associated with the use of such tools. As we have seen throughout this chapter, there are ways which *might seem* reliable if only a subset of the available documentation is studied. Before using a tool that is claimed to somehow work with defect sectors, the investigator should first ask for *specific evidence* of its correct function from the manufacturer.

5. Other issues related to ATA and computer forensics

We will conclude our look at ATA commands relevant to computer forensics by looking at a couple of issues that have not been covered yet: The Security Mode feature set and Firmware updates.

5.1 The Security Mode feature set

The *Security Mode feature set* was briefly introduced in Section 4.3.4. Its primary purpose is to password protect the data stored on a disk.

It is possible to set two different passwords. The *User Password* is the one normally to be used. If the User Password is forgotten, the *Master Password* can be used instead to unlock the disk. The way unlocking with the Master Password works depends on how the *Security Level* is set. In the *High Level* it is possible to use the disk straight away. In the *Maximum Level* the disk can only be used after issuing the commands SECURITY ERASE PREPARE and SECURITY ERASE UNIT. Then the disk can be used again, but its contents are wiped (see Section 4.3.4). The settings described are all performed using the SECURITY SET PASSWORD command.

5.1.1 Accessing with a known User Password When the User Password is known the disk can be unlocked until the next power cycle using the command SECURITY UNLOCK. Using the command SECURITY DISABLE PASSWORD on an unlocked disk turns off the password protection until it is manually activated again.

One important thing to note is that a User Password set from the computer BIOS does not necessarily correspond to the same password set by ATA utilities. The phenomenon was noticed in a test using the BIOS in a Dell Laptop to set the User Password and the ATA Password Tool [6] to unlock. The exact explanation is not clear, but perhaps it has to do with how the entered password is encoded before it is sent to the disk controller.

5.1.2 Accessing with a known Master Password When only the Master Password is known the disk must have High Level security, otherwise it cannot be unlocked without erasing its contents. When unlocking with the Master Password in High Level, the same commands can be used as when unlocking with the User Password.

5.1.3 Accessing with a default Master Password Some disks ship with a default Master Password specified in the data sheet. One example of a default

Master Password is a single ASCII space. If the default Master Password has not been changed, it can be used exactly like any other known Master Password.

5.1.4 Other cases A brute force or dictionary attack against a disk that adheres to the ATA specifications does not work since there is a counter that blocks the unlock commands after five failed attempts. To reset the counter the disk must be power-cycled - a DEVICE RESET command does not help.

Some data rescue companies claim to be able to unlock all disks, which would imply other cases than the ones described above. I have not seen any facts supporting the claims.

5.2 Firmware updates

Many disks support the DOWNLOAD MICROCODE command for downloading firmware updates to the disk. It is possible to specify if the disk should only use the update temporarily, or if it should use it permanently. The size of a firmware update cannot be larger than 32 MB.

The reason firmware updates are mentioned here is because using such an update it might be possible to change the way a disk works, preventing a successful forensic investigation. Also, updates might possibly be used to retrieve information otherwise impossible to retrieve, or wipe information otherwise impossible to wipe.

I have not studied firmware updates any closer. Since there seems to be very little documentation available it can probably be assumed that this topic would require quite a large amount of research for any significant progress to be made.

5.3 Advice to the investigator

Investigators should be careful with unlocking tools so as to not let a tool erase the entire drive while unlocking it if the security level is set to Maximum.

If both the User Password and the Master Password are unknown, a solution might be to get the default Master Password from the manufacturer of the disk or computer. Otherwise there are data rescue companies that might be able to help.

Even if the User Password is known, using an ATA utility might not work if the password was entered through the computer BIOS. In this case the investigator could be forced to unlock the disk using a BIOS from the same manufacturer.

Firmware updates is a topic little investigated and hence I do not have any specific advice to give regarding them.

6. ATA utilities useful in computer forensics

This chapter gives a very quick description of a number of ATA utilities which together cover all the commands mentioned so far in the report. These utilities are useful because through their menues it is possible to run ATA commands more or less one by one, passing the parameters needed.

6.1 ATA Password Tool

The ATA Password Tool v1.1 [6] supports the commands: SECURITY DISABLE PASSWORD, SECURITY ERASE PREPARE, SECURITY ERASE UNIT, SECURITY FREEZE LOCK, SECURITY SET PASSWORD, and SECURITY UNLOCK.

6.2 HDAT2

HDAT2 v4.01.08 [7] supports the commands: IDENTIFY DEVICE, SET MAX ADDRESS, READ NATIVE MAX ADDRESS, SMART READ DATA, DEVICE CONFIGURATION IDENTIFY, DEVICE CONFIGURATION SET, DEVICE CONFIGURATION RESTORE, DEVICE CONFIGURATION FREEZE LOCK, SECURITY SET PASSWORD, and SECURITY FREEZE LOCK.

6.3 HDD Erase

HDD Erase 2.0b [8] automates the use of SECURITY ERASE UNIT, and the commands that must be executed before it, to erase a disk.

6.4 TAFT - The ATA Forensics Tool

TAFT 1.0 [9] supports the commands: IDENTIFY DEVICE, READ NATIVE MAX ADDRESS, READ NATIVE MAX ADDRESS EXT, DEVICE CONFIGURATION IDENTIFY, SET MAX ADDRESS, SET MAX ADDRESS EXT, DEVICE CONFIGURATION SET, and DEVICE CONFIGURATION RESTORE.

6.5 Advice to the investigator

The ATA utilities described in this chapter are very useful for performing experiments with ATA functionality relevant to computer forensics. The investigator should be aware though that the utilities are freeware and there is no guarantee that they have been sufficiently tested to be useful in the extraction of evidence for a court or similar.

7. HPA and DCO capability tests with EnCase, DBAN, ExpertEraser, and CoreSHIELD

This chapter describes HPA and DCO capability tests with the forensics tool EnCase [10], the disk wiping tools DBAN [11] and ExpertEraser [12], and finally the hardware write blocker CoreSHIELD [13] (see Chapter 8 for more information about CoreSHIELD). These products were selected only because they were available in our research lab.

It is important to note that the DCO weaknesses described in this chapter are not specific to the software products tested here, but affect many similar products on the market. It also appears as even the disk firmware implementation of DCO is not completely reliable in some of the disks we have tested.

7.1 Hardware and software common among the tests

The disk used was a *Maxtor DiamondMax Plus 9 80GB ATA/133 HDD* [1] and the software used to set it up was TAFT 1.0 [9]. The disk was restored to its factory defaults between each of the test cases.

7.2 EnCase Forensic Edition 4.18a run in Windows

For each test case, a new forensic case was created and the disk was added with New Device. The tests resulted in the following:

- After SET MAX ADDRESS 0x8000 the highest sector seen was 32255 (=0x7DFF)
- After SET MAX ADDRESS EXT 0x8500 the highest sector seen was 33263 (=0x81EF)
- After DEVICE CONFIGURATION SET 0x9000 the highest sector seen was 36287 (=0x8DBF)

This test shows that EnCase Forensic Edition 4.18a run in Windows is not able to handle neither HPA nor DCO.

I have not found any statements from Guidance Software (the manufacturer of EnCase) about whether HPA and DCO are supported or not.

[1] Although they are not described here, we have repeated these tests with other disks, both from Maxtor and Seagate, with similar results.

7.3 EnCase Forensic Edition 4.18a run in DOS

For each test case, Mode was changed to "ATA". Then a Drive to Drive Acquisition without compression was performed. The tests resulted in the following:

- After SET MAX ADDRESS 0x8000 the number of sectors acquired was 160086528 (=0x98ABA00)
- After SET MAX ADDRESS EXT 0x8500 the number of sectors acquired was 160086528 (=0x98ABA00)
- After DEVICE CONFIGURATION SET 0x9000 the number of acquired was 36865 (=0x9001)

This test shows that EnCase Forensic Edition 4.18a run in DOS is able to handle HPA but not DCO.

I have not found any statements from Guidance Software (the manufacturer of EnCase) about whether HPA and DCO are supported or not.

7.4 EnCase Forensic Edition 4.18a run in DOS with CoreSHIELD Rev 1.00

The same test as above was performed with CoreSHIELD connected. The test resulted in the following:

- After SET MAX ADDRESS 0x8000 the number of sectors acquired was 32770 (=0x8002)
- After SET MAX ADDRESS EXT 0x8500 the number of sectors acquired was 34049 (=0x8501)
- After DEVICE CONFIGURATION SET 0x9000 the number of sectors acquired was 36865 (=0x9001)

This test shows that CoreSHIELD prevents EnCase from handling HPA. The reason for this will become clear in Section 8.2.

7.5 DBAN 1.0.4

The disk was wiped with DBAN 1.0.4 in DoD Short mode for each test case. After each wipe it was restored to factory default and EnCase was used to look at the contents of sector 58945 (=0xE641). This sector was chosen randomly, and before each test it was filled with some data that should be cleared with a successful wipe. The tests resulted in the following:

- After SET MAX ADDRESS 0x8000 old data was still found in the reference sector
- After SET MAX ADDRESS EXT 0x8500 old data was still found in the reference sector

- After DEVICE CONFIGURATION SET 0x9000 old data was still found in the reference sector
- After the disk was restored to factory default the reference sector was found to be wiped

This test shows that DBAN 1.0.4 does not handle HPA nor DCO. Thus, on a disk where a HPA or DCO setting has been applied to make the disk look smaller than it really is, only the visible part of the disk will be wiped.

I have not found any specific claims from Darik Horn (the author of DBAN) about whether HPA and DCO are supported or not. He has made the following general statement in the FAQ though: "*Q: Are you absolutely sure that DBAN works properly? A: No.*" [14].

7.6 ExpertEraser 2.0

The disk was wiped with ExpertEraser 2.0 in Level 1 Erasure mode. After each wipe it was restored to factory default and EnCase was used to look at the contents of sector 58945 (=0xE641). This sector was chosen randomly, and before each test it was filled with some data that should be cleared with a successful wipe. The tests resulted in the following:

- After SET MAX ADDRESS 0x8000 the reference sector was found to be wiped
- After SET MAX ADDRESS EXT 0x8500 the reference sector was found to be wiped
- After DEVICE CONFIGURATION SET 0x9000 old data was still found in the reference sector
- After the disk was restored to factory default the reference sector was found to be wiped

This test shows that ExpertEraser handles HPA but not DCO. Thus, on a disk where a DCO setting has been applied to make the disk look smaller than it really is, only the visible part of the disk will be wiped.

I have not been able to find any specific claims from IBAS (the manufacturer of ExpertEraser) about whether HPA and DCO are supported or not.

IBAS has made the following general claim though: "*[...] Version 2.0 covers the new standards ATA6/LBA 48 – erasing 100% of both old and new hard disks.*" [15]. It should be noted that DCO was introduced in ATA-6 (see Section 2.2).

I have been told by IBAS representatives that after 2005-05-13 they started shipping a fixed version of ExpertEraser as a result of being informed of this vulnerability.

7.7 Advice to the investigator

It is very important to test how forensic imaging and disk wiping tools handle HPA and DCO before using them in real and important cases. The tests described in this chapter are quite simple and yet they reveal several problems concerning the products tested. More extensive testing could for example involve disks where both DCO and HPA are being used at the same time.

Even though only a few products have been shown to contain weaknesses, it can most likely be assumed that the majority of such products currently available on the market have similar weaknesses.

8. A test of the hardware write blocker CoreSHIELD

This chapter contains a test of the hardware write blocker CoreSHIELD Rev 1.00. CoreSHIELD was selected because it was available in our research lab.

8.1 Requirements for a hardware write blocker

A hardware write blocker is a physical device which is connected between a disk and the disk controller. Its primary purpose is to protect the evidence on the disk by blocking writes to it.

The Hardware Write Blocker Device (HWB) Specification 2.0 [16] from NIST contains the following four requirements for a hardware write blocker:

- HWB-RM-01: A HWB shall not, after receiving an *operation of any category* from the host nor at any time during its operation, transmit any *modifying category operation* to a protected storage device.
- HWB-RM-02: A HWB, after receiving a *read category operation* from the host, shall return the data requested by the read operation.
- HWB-RM-03: A HWB, after receiving an *information category operation* from the host, shall return a response to the host that shall not modify any access-significant information contained in the response.
- HWB-RM-04: Any error condition reported by the storage device to the HWB shall be reported to the host.

This test of CoreSHIELD only covers HWB-RM-03. In particular, HWB-RM-01 is very important but also very hard to test; [17] (pages 54 and 77) elaborates further on this topic.

8.2 Information category operations

The disk used in this test was a *Maxtor DiamondMax Plus 9 80GB ATA/133 HDD*. TAFT 1.0 [9] and HDAT2 [7] were used to retrieve information from the disk both with and without CoreSHIELD.

The following differences were found when running the IDENTIFY DEVICE command:

- Firmware: "Rev 1.00" with CoreShield, and "YAR41BW0" without CoreSHIELD
- Model: "CoreSHIELD" with, and "Maxtor 6Y080P0" whithout

- HPA feature set: "Not supported" with, and "Supported" whithout

The following differences were also found:

- DEVICE CONFIGURATION IDENTIFY: failed with CoreSHIELD, and worked without CoreSHIELD
- SMART READ DATA: failed with, and worked without

It can be argued whether CoreSHIELD fulfills NIST requirement HWB-RM-03 or not. In any case it will make forensic imaging tools believe that the disk under investigation does not support HPA. This is indeed a problem as we could see Section 7.4. I have not been able to find any claims from CorePROTECT (the manufacturer of CoreSHIELD) about whether requirement HWB-RM-03 is fulfilled or not.

8.3 Operating system caching issues

Because an operating system usually has a cache for disk access, it might seem like changes are made to the disk when in fact they are not [18]. Testing with CoreSHIELD and Windows XP verified that this can indeed be a problem. Tampering with the contents of a disk will not actually change the disk contents, but can change what seems to be on the disk, and thus introduce errors into the investigation.

8.4 Advice to the investigator

The investigator should at least test how a hardware write blocker changes the information returned from the disk before using the blocker in a real and important case. Also, it is very important to understand that operating system chaching might introduce errors into the investigation as described in Section 8.3.

9. Questions which remain unanswered

Following is a list of some of the questions which still remain unanswered

- Is it possible to determine the size of, and access the contents of, the G-list sectors in a reliable way?
- Is it possible to find the default Master passwords used by the various disk manufacturers?
- Exactly how are firmware updates constructed and installed?
- What can be performed using a custom firmware update?
- How (if at all possible) can disk security with Security Mode be circumvented without any password?
- Which is the best way to test if a hardware write blocker fulfills the NIST requirements?
- Which other uses of DCO can affect computer forensics?

Bibliography

[1] INCITS, “Technical Committee T13 - AT Attachment,” http://www.t13.org/.

[2] ——, “ATA/ATAPI-7 revision 4b Vol. 1,” http://www.t13.org/#Project_drafts.

[3] SFF Committee, “SFF Committee Specification for Self-Monitoring, Analysis and Reporting Technology (S.M.A.R.T.).”

[4] Ariolic Software, “S.M.A.R.T. attributes meaning,” http://www.ariolic.com/activesmart/smart-attributes/.

[5] Allen, Bruce, “smartmontools FAQ,” http://smartmontools.sourceforge.net/#FAQ.

[6] Mina, Alex, “ATA Password Tool,” http://www.upsystems.com.ua/support/alexmina/atapwd.zip.

[7] L. Cabla, “HDAT2,” http://www.freewebs.com/hdat2/.

[8] Center for Magnetic Recording Research, “HDDErase,” http://cmrr.ucsd.edu/Hughes/SecureErase.html.

[9] A. Vidström, “TAFT - The ATA Forensics Tool 1.0,” http://vidstrom.net/stools/taft/.

[10] “EnCase,” http://www.guidancesoftware.com/products/EnCaseForensic.

[11] “DBAN,” http://dban.sourceforge.net/.

[12] “ExpertEraser,” http://www.ibas.com/.

[13] “CoreSHIELD,” http://www.coreprotect.com/core_shield.html.

[14] Darik Horn, “Darik’s Boot and Nuke Frequently Asked Questions,” http://dban.sourceforge.net/faq/index.html.

[15] IBAS, “Significant time-savings when erasing data,” http://www.ibas.com/press/articles/2003-02-13.news.

[16] NIST, “Hardware Write Blocker Device (HWB) Specification 2.0,” http://www.cftt.nist.gov/hardware_write_block.htm.

[17] Bengtsson, Johnny, “Forensisk hårddiskkloning och undersökning av hårddiskskrivskydd.”

[18] CoreSHIELD, “CoreSHIELD Installation Guide.”