Applications of Data Recovery Tools to Digital Forensics:
Analyzing the Host Protected Area with the PC-3000
Richard Leickly and David Angell
*Circle Hook Data Recovery*
{ Richard, David}@CircleHookDR.com

Abstract
In digital forensics, it is necessary to analyze the data in the Host Protected Area (HPA)—a potentially large hidden region of the hard drive. The removal of the HPA can either be temporary or permanent depending on whether the changes occur in non-volatile or volatile memory locations. Permanently removing the HPA alters information in the Service Area—non-volatile storage regions on the platters; temporarily removing it alters the contents of the drive’s RAM—volatile storage on the drive’s circuit board. The implications of both procedures for forensic hard drive analysis are discussed. Typically, forensic tools are used to remove the HPA, but the PC-3000—a data recovery tool unfamiliar to many digital forensic examiners—can be used for either method, and offers some advantages over more commonly used forensic tools: the HPA can be removed in RAM, and files and folders in the HPA can be viewed and saved to disk, or the drive can be imaged to a destination drive.

Introduction
A Host Protected Area (HPA) is an area of a hard drive that is normally inaccessible to the user. Its existence is not reported to the BIOS or to the operating system of the host computer. In this sense, it is a hidden area of the hard drive that can contain data in many formats, ranging from raw code or files (possibly encrypted), to complete alternative system or data partitions, and even disk images of operating systems. It can range in size from a less than a megabyte to many gigabytes.

Host Protected Areas were introduced in 2001 via the ATA-4 specification which saw the addition of two ATA commands: *Read Native Max Address* and *Set Max Address*¹. When LBA-48 was introduced for drives larger than 137 GB, a revised standard (ATA-6) added two additional commands with the same purpose: *Set Native Max Address Ext* and *Set Max Address Ext*².

---
The stated purpose of the HPA is to offer computer manufacturers a region of the hard drive for the storage of diagnostic utilities, recovery programs, and even copies of the host operating system, in a manner that would prevent their deletion or manipulation by the user. If the host operating system becomes damaged, a computer with a manufacturer-installed HPA-hidden system partition can be instructed to boot from that partition.

Our intention is to show the digital forensic community how a data recovery tool—the PC-3000—examines the HPA. We demonstrate how it can be used to temporarily or permanently remove an HPA, and how it can then either create a clone or image of the drive, or expose and render accessible the drive’s partitions and file system. We also show how and where the removal of an HPA alters the drive, and the implications this has on the forensic process. To appeal to a wider audience, we assume little prior knowledge of hard drive architecture or internal operations.

**Forensic significance of the Host Protected Area**

A Host Protected Area can be relatively large in size, encompassing many gigabytes of data. Because most files are too large to be stored in file slack or in the empty sectors following the MBR (Master Boot Record), the large hidden area of an HPA provide an appealing, albeit unsophisticated, way to conceal information or malware. Compromising the executable code stored in the HPA is also possible, but would require a more sophisticated attack.

Digital forensic examiners are well-aware of the possibility that an HPA could be present on the hard drive they are examining. Many common digital forensics tools used for imaging or cloning can detect and remove a Host Protected Area; and many tools can detect and recover the data discovered in this region.

However, many forensic examiners may not be aware of the operations that occur on the hard drive when an HPA is created or removed, or be aware of the locations on the drive that are changed by those operations. They may also not be aware that removing an HPA is an alteration to the hard drive. In the final section of this article we will discuss the specific changes that are made to the hard drive and the implications this has for the forensic process.

**Materials and Methods**

*The PC-3000*

The PC-3000 (UDMA version) is an advanced data recovery device that is installed on a desktop computer. It has both software and hardware components. A full description of the device can

---

3 Ace Laboratories, Rostov-On-Dom, Russia
be obtained from the ACE Laboratories website\(^4\). Through the use of the supplied adapters, drives of any storage capacity, of any physical size, or in any combination of SATA or PATA interfaces, can be connected to the data and power leads that extend from the PC-3000 cards. Drives can be independently designated as source or destination drives. The drives are independently controlled, and it is possible to designate both drives as source drives, if desired, and to switch between them. Using the PC-3000 interface, drives can also be mounted and made accessible to the host operating system.

**HPA Creation**

Typically, computer manufacturers use proprietary software tools to create HPAs and to write diagnostic and recovery software to that area of the hard drive. The HPA becomes accessible during boot when permitted by the BIOS and the proprietary HPA-aware tools installed by the manufacturer. These tools make alterations to the MBR, and write an object containing configuration information, called the BEER (Boot Engineering Extension Record) to the last sector of the drive\(^5\). The specification for this is called PARTIES (Protected Area Run Time Interface Extension Services)\(^6\).

In order to assess the ability of the PC-3000 to analyze the HPA, we first needed to create one, and put a partition with some data into it. Not having access to the tools used by the computer manufacturers, we used a manual process that did not insert any special instructions into the MBR or write a BEER to the last sector. Since those changes are only needed to make the HPA accessible during boot, they would have had no effect on our results. Here we briefly outline the process we used to create an HPA. The details have been posted on the Circle Hook Data Recovery website\(^7\).

On a clean 2.5”, nominally 120 GB Samsung drive (Model: HM121H), we created two NTFS partitions: a normal data partition and a hidden data partition, in the following manner. Noting that the full capacity of the drive was 234,441,647 sectors (maximum LBA is 234,441,647), we used the PC-3000 to create an HPA that began at LBA 150,000,002. Using Windows XP, we created a normal partition in the space below LBA 150,000,002, and added a file there. We then used the PC-3000 to remove the HPA. Returning the drive to Windows XP; we put a partition in the formerly hidden area starting at LBA 150,000,001, and extended it to the end of the drive. We copied a different file there. We then returned the drive to the PC-3000 and re-created the

\(^{7}\) [CircleHookDR.com](http://www.circlehookdr.com)
HPA at LBA 150,000,002. Using a hex editor, we removed the entry for the second partition from the MBR. This last step prevented Windows XP from seeing the partition—making it a hidden partition. Without that last step, the partition’s existence was reported to the operating system, but its size was 0 bytes. It was unusable, but it wasn’t hidden.

In summary, we prepared a drive with two partitions: one normal data partition and one hidden data partition. The normal partition extended from LBA 0 to LBA 150,000,001; the hidden partition was approximately 40 GB and extended from LBA 150,000,002 to the end of the drive—LBA 234,441,647. Each partition contained a single unique jpeg image file. This drive was used for all subsequent analyses. We attached the drive attached to the PC-3000 to analyze the HPA we had created.

**Results**

The PC-3000 does not explicitly indicate the ATA commands that it uses. However, from the ATA specifications, we know which ATA commands are available and what they do. In the following paragraphs, we indicate the relevant ATA commands that are involved because it clarifies the actions performed by the PC-3000.

_Preliminary Analysis of the Hard Drive_

We used the PC-3000 to discover the physical locations of the Samsung drive’s firmware. The drive had firmware in both a ROM chip on the circuit board and in the Service Area on the platter. The amount of firmware on the platter was substantial: 64 cylinders were allocated to the Service Area, and 21 of these cylinders had firmware modules written to them.

_Temporary removal of the HPA_

To the Windows Disk Management utility, the Samsung drive appeared to have only a single partition: Disk 1, Mango-1; the partition in the HPA on Disk 1 (Mango-2) was not discovered by Windows Disk Management (Figure 1).

![Figure 1. Samsung drive as seen in Windows Disk Management.](image-url)
After invoking the ATA command—Identify Device—via the PC-3000’s Drive ID command, the drive was seen as having a useable capacity of 150,000,001 sectors (Figure 2).

As part of its drive-identification process, the PC-3000 had already discovered the drive’s true full capacity (234,441,647 sectors) by means of another ATA command—Read Native Max Address. We directed the PC-3000 to write this value to the drive’s RAM, which reset the drive’s capacity to that value (Figure 3).
This was done by issuing the ATA command—Set Max Address—with its volatility bit set to the value 0. (When the volatility bit is set to 0, the change to the drive is temporary, and will not persist after the drive is repowered.) After that, we again invoked the PC-3000’s Drive ID command and confirmed that the drive’s maximum LBA had been set to the value 234,441,648 (Figure 4)—its maximum possible value. The HPA had been removed.

![PC-3000 Drive ID result](image)

**Figure 4.** PC-3000. Results of Drive ID command after the HPA was removed from the drive.

The PC-3000 includes a utility called the Data Extractor. After the Data Extractor is invoked, there are two choices: either make an image of the entire drive, or proceed to the File Explorer interface to view the file tree and copy selected files. When the drive was opened in the Data Extractor’s File Explorer interface (Figure 5), we saw one NTFS partition and two other NTFS partitions (indicated by blue accent marks).
The PC-3000 refers to these as Virtual Boot Partitions. They are copies of the partitions on the drive. There is one virtual partition for each partition discovered on the drive. In the figure, the root of the lower virtual partition has been expanded, and is shown in the right panel. The entire directory of the hidden partition is exposed. From this screen, the files and folders in the right panel were opened and saved to a destination drive. Figure 6 shows analogous results for the partition that was never hidden.
Cycling the power on the drive restarted the initialization process. This cleared the value 234,441,647 from RAM and the drive initialized to a capacity of 150,000,001 sectors, indicating that the HPA was restored. This confirmed that the removal of the HPA was temporary.

**Permanent Removal of the HPA**

A permanent change to a hard drive means that the changes are preserved after the drive is repowered or sent a hardware rest command. To implement the permanent removal of the HPA, we returned to the menu shown in Figure 7.

![Figure 7. PC-3000. Settings for the permanent removal of the HPA](image)

This is the same menu shown in Figure 3, except that we elected to save the value of the maximum LBA returned by *Identify Device* to the Service Area—a non-volatile location. For this, the PC-3000 issued the ATA command—*Set Max Address*—and made the change permanent by changing the *volatility bit* for the command from the 0 to 1. From this point on, the results were identical to those of the temporary HPA removal procedure: the drive was seen as having 234,441,647 sectors and the File Explorer interface of the Data Extractor showed the same information as in Figure 5. As before, we had the option of making an image or proceeding to open or save files to a destination drive.

The removal of the HPA was permanent. Cycling the power on the drive had no effect on the capacity of the drive as seen by Windows: 234,441,647 sectors.

**Permanent removal of the HPA requires writing to the drive’s Service Area**

To make a permanent change, values must be written to non-volatile storage. All drives have two forms of non-volatile storage: ROM, either as a discrete chip on the circuit board or integrated into the MCU, and the Service Area on the platter. To identify which location was used, we conducted another experiment.
For each drive manufacturer, the PC-3000 presents a customized interface. This is necessary because each manufacturer uses a unique set of firmware modules and commands. Sometimes these differences allow the operator to investigate one drive in ways not available on another. We removed the Samsung drive from the PC-3000 and replaced it with a Seagate 7200.10. We powered the drive and connected a data cable; but sent instructions through a cable connected to the drive’s diagnostic pins to turn off the power to the platters. We then issued the PC-3000’s Drive ID command, which uses the ATA command—Identify Device. It was unable to return a value for the maximum LBA when the platters were not spinning. When we powered the platters, it was able to return the maximum LBA value. This demonstrated that the value of the maximum LBA was obtained from the Service Area, not from the ROM.

Discussion
We precede our discussion with an overview of hard drive architecture and operations, and end it by considering the implications for forensic hard drive analysis.

Hard drive firmware
Hard drives contain firmware: low-level code and stored parameters that control the operation of the hardware. Depending on the manufacturer, model, and vintage of the drive, the firmware can be located in any two, or in all three, of the following locations: (1) in a block of ROM in the MCU (Microcontroller Unit); (2) in a dedicated ROM chip; or (3) in specially designated cylinders on the platter, comprising the Service Area or System Area (SA). The cylinders comprising the Service Area are dedicated to the Service Area: they form a continuous annulus of cylinders—called the Reserved Area—that can be located at the circumference of the platter, the middle of the platter, or near the spindle. The location of the Reserved Area varies between and within manufacturers, but a PC-3000 can usually indicate its location. No user data are written to the Service Area. We can therefore think of the platter as being partitioned into a Service Area and a Data (or User) Area. The Data Area is also called the User Area because it is the area of the hard drive to which the user of the computer normally has access. An HPA—if it exists—will be in the Data Area; but the address of the HPA will be stored at a location in the Service Area.

Only a small amount of firmware is stored in the internal ROM of the MCU. Even when there is a dedicated ROM chip, there is also a large amount of firmware resident on the platter, and some of it is redundant with the firmware stored in the ROM chip. While ROM can be rewritten, it is not part of the ordinary operating procedure of the drive. Writing to the ROM is done at the factory; but it can also be accomplished with special commands when a drive is being repaired by a device like the PC-3000. For this reason, permanent firmware changes made
Applications of Data Recovery Tools to Digital Forensics: Analyzing the Host Protected Area with the PC-3000

Copyright 2012 – Richard C. Leickly and David K. Angell

during normal operation are made to sectors in the Service Area on the platter cylinders using specific ATA commands.

**Hard drive initialization**

When a hard drive powers on and initializes, it conducts a self-check, and then copies data from the Service Area to the RAM chip on the drive’s circuit board. If the drive has a separate ROM chip, or a designated area of its MCU, data from those areas will also be copied into RAM. RAM is used to hold data needed during the operation of the drive because reading from RAM is much faster than reading from ROM or from the platters. After initialization, the operations carried out by the MCU are based on values that it finds in RAM. When the operating system issues an ATA command, it is typically returns the value stored in RAM.

**Permanent versus temporary removal of the HPA**

The *Set Max Address* command changes the usable storage capacity of the drive by changing the value of the maximum LBA. The PC-3000 offers two different ways to write the LBA value using the *Set Max Address* command. One method changes the values only in the RAM chip; the other also changes the value in RAM, but, in addition, it changes the value on the Service Area. The first method (write to RAM only) causes a temporary resetting of the maximum LBA, resulting in the subsequent, temporary removal of the HPA. The change is temporary because RAM is volatile memory, and the LBA value is lost when the drive is repowered. The second method (write to RAM and to the Service Area) uses the same command, but also changes another parameter— the *volatility bit*— to the value 1. This causes the permanent removal of the HPA since the LBA value is written to the platter—a non-volatile form of storage that persists after a hardware reset or power cycling.

**Permanent changes to the HPA are written to the Service Area**

Since the change was permanent, new values were written to non-volatile storage. Hard drives have two forms of non-volatile storage: ROM and the Service Area on the platter. We have three arguments for our claim that values were written to the non-volatile storage in the Service Area, and not to the ROM:

1. Data are not written to ROM during ordinary drive operations. ROM is typically written at the factory, and rewritten when the firmware it holds is repaired.
2. The Service Area is on the platter. Platters cannot be read unless they are spinning. The ATA command—*Identify Device*—cannot read and return the value for the maximum LBA when the platters are not spinning.
Applications of Data Recovery Tools to Digital Forensics: Analyzing the Host Protected Area with the PC-3000

(3) The ATA specification states that the value returned to RAM by the ATA command—Set Max Address—is written to the Reserved Area\(^8\)—the cylinders on the drive that constitute the Service Area.

**Implications for the forensic analysis of hard drives**

We have argued that permanently removing the HPA requires a write to the Service Area—a reserved set of cylinders on the platter. There are several forensic hardware write blockers that can remove an HPA permanently. Why would a hardware write blocker allow a write to a protected drive when such an action seems inconsistent with its purpose?

The central requirement for a sound forensic examination of digital evidence is that the original evidence must not be modified, i.e., the examination or capture of digital data from the hard drives or other storage media of a seized computer must be performed so that the contents are not changed. The investigator follows a set of procedures designed to prevent the modification of original evidence. These procedures may include various write blocking techniques including the use of software tools or hardware devices to block modification of the contents of a drive\(^9\).

How can our observations be reconciled with that requirement? We will consider several arguments and supporting statements that might be offered by hypothetical critics taking opposing sides on the issue.

**Argument No. 1:** It may be more typical for drives to write the change to a non-volatile memory chip (e.g. ROM). The drive analyzed in this paper may be exceptional.

**Statement for**

Perhaps not all drives use the Service Area to store the information altered by the ATA command—Set Max Address. The WiebeTech\(^10\) Forensic UltraDock (version 5) hardware write blocker, when it removes an HPA permanently, does not write the value to any particular location. The hard drive manufacturer decides how to implement the Set Max Address command sent by the write blocker\(^11\). Perhaps some manufacturers design their drives to write to a non-volatile memory chip on the circuit board. While a write to a non-volatile chip is still a permanent alteration to the drive, it is irrelevant since no regions on the platter are touched. Besides, non-volatile memory chips have no forensic interest.

---

\(^8\) Information Technology – AT Attachment 8 – ATA/ATAPI Command set. T13/1699-D. 206.


\(^10\) WiebeTech. Wichita, KS, 67226. WiebeTech.com


Copyright 2012 – Richard C. Leckly and David K. Angell
Statement against
Writing to a non-volatile memory chip would violate the ATA specification. The ATA specification states that the write occurs to the Reserved Area, which is the physical region of the drive that contains the Service Area\(^12\). Are there any hard drives that permanently remove the HPA by writing the maximum LBA to a non-volatile memory chip? That information is proprietary and difficult to obtain. However, the results reported here prove that if it occurs, it cannot be general.

Argument No. 2: The write to the Service Area is allowed in forensic hardware write blockers

Statement for
The Computer Forensics Tool Testing (CFTT) program at the National Institute of Standards and Technology (NIST) has tested the commonly used forensic write blockers. NIST’s criteria state that hardware write blockers (HWB)\(^\text{”... shall not transmit any modifying category command to the protected storage device”}\(^13\). According to their categorization, the ATA commands—Set Max Address and Set Max Address Ext—are not modifying commands\(^14\). Therefore, a hardware write blocker is not required to block them.

Statement against
Part of the argument is semantic; the rest defers to the judgment of a respected testing authority. For a forensic examiner, the point is this: to avoid error, it is up to the examiner to know how NIST defines and tests hardware write blockers—regardless of how a testing authority may label or classify the commands sent to the protected drive.

Argument No. 3: No user data are affected

Statement for
It is acceptable to alter bits on the platter if the alterations occur in the Service Area—not in the Data Area. Since there are no user data in the Service Area, the write operation will not change the drive in any way that will matter in a forensic investigation.

Statement against
The premise in the above statement is that the Service Area has no forensic interest. The alteration made to the Service Area affects only the storage capacity of the drive—nothing else.

---
\(^12\) Information Technology – AT Attachment 8 – ATA/ATAPI Command set. T13/1699-D. 206.
\(^14\) Ibid. Appendix B.
This is a defensible position if the premise is true. The examiner’s ability to explain the nature and location of the alterations would strengthen the argument.

**Justifying the choice**
In order to forensically image or clone an entire drive containing an HPA, the HPA must be removed. We argue that the forensic examiner should carefully consider the choices available. Is it prudent to remove the HPA on a suspect’s drive permanently if the option to do it temporarily is available?

If a temporary removal of the HPA is impossible, a knowledgeable digital forensic examiner could defend a permanent removal of the HPA by arguing that, although the procedure wrote to the hard drive, the write made only a configuration change to the drive. The write occurred in the Service Area of the drive—a region of the drive that does not contain any user data.

Temporary removal may be the best course of action since it obviates the need to defend the choice. The examiner will have the data from the hidden area for the forensic analysis, but the source drive will be left unaltered.

**Conclusions**
Using a PC-3000, the Host Protected Area can be easily seen, and removed either permanently or temporarily. The data contained within the HPA is exposed using either method, but by using the temporary removal process, no writing to either the Data Area or to the Service Area of the hard drive will occur. In contrast, the permanent removal process writes to the Service Area on the platter of the drive.

After the HPA is removed by the PC-3000 by either method, the files and folders in the Data Area of the drive are presented within the PC-3000 File Explorer interface as a file directory tree, just as they would look under Windows Explorer, and the files can be directly opened or saved. The analyst can choose to image or clone the drive to a destination drive. Both of these options are possible even when the MBR is corrupted or is missing the entry for the partition containing those files.

We have demonstrated that the PC-3000 can remove the Host Protected Area and copy files from it without altering either the Service or the Data Areas of the hard drive. While a forensic examiner may choose to employ forensic tools to retrieve files from a Host Protected Area, we have demonstrated that a tool designed for data recovery can also be used for this purpose. The PC-3000 features: (1) transparency (*i.e.* it is easier to understand what you are doing); (2) choice (*i.e.* permanent or temporary HPA removal); (3) the ability to overcome missing or
corrupted partition entries in the MBR; (4) the ability to examine the data files in the native file directory tree, rather than in collections of vendor-designated categories, and (5) the ability to immediately clone the drive or create an image file, or to immediately copy the files from the directory tree to a destination drive.

Forensic examiners should not assume that hardware write blockers prevent all writes to the protected drive. It is in the best interest of forensic examiners to know which ATA commands are allowed through the write blocker, the specific values that could be changed, and the locations on the drive where those writes will occur. The results and arguments presented here are a step in that direction and will provide forensic examiners with some insight into an otherwise obscure process.

Acknowledgements
The authors thank Steve Hailey for his material and intellectual support.

All rights reserved
Copyright 2012, Richard C. Leickly and David K. Angell

All rights reserved. This edition of the work is protected against unauthorized copying under Title 17, United States Code.