Digital Investigation (2005) 2, 268–275

ELSEVIER

Digital Investigation

www.elsevier.com/locate/diin

Methods of discovery and exploitation of Host Protected Areas on IDE storage devices that conform to ATAPI-4

Mark Bedford

Information Science Department, School of Business, University of Otago, Commerce Building, P.O. Box 56, Dunedin, New Zealand

Received 14 November 2005; revised 14 November 2005; accepted 14 November 2005

KEYWORDS
Digital forensic tool testing;
Forensic examination;
Host Protected Area

Abstract This paper explains some of the issues that prevent the easy detection of Host Protected Areas on IDE drives and discusses a variety of methods which may enable examiners to reveal what may be overlooked evidence. We consider some exploitation methods and include a brief examination of EnCase 5.01 image capture as an example.
© 2005 Elsevier Ltd. All rights reserved.

Scenario

''Urgent analysis,'' your detective friend says as she makes a hasty departure from your work area. You already have more than enough cases and wonder if this one will be any different. After all, a case is just like any other, right? You follow operational procedure and start a new case record for the drive noting its details on the sheet. Locating the IDE write blacker and the USB to IDE adaptor, you connect all the bits together and boot up.

Running up Partition Magic will give you an idea of what might be in store for you — nothing, naught, blank, nope, no partition table to be found. Unfazed, you move onto the next step and bring up WinHex, where you go to head 0 track 0 sector 0 and start looking for boot code, nothing but zeros. You hold your finger on the page down key as screens full of zeros roll past and wonder what sort of a detective would give you a blank drive for evidence. Every drive has to have a boot sector or at least a partition table if it has ever been used, right? You check the description on the evidence bag to make sure this is evidence and not a new drive for someone. Yep, found in the suspects' room. Maybe the suspect just hadn't got around to installing it yet. You power down the laptop and head for the drive imager connected to the network so you can put an image on the evidence archive server and another image on the evidence analysis server. The EnCase

E-mail address: mbedford@infoscience.otago.ac.nz

1742-2876/$ - see front matter © 2005 Elsevier Ltd. All rights reserved.
doi:10.1016/j.diin.2005.11.006

capture program will work fine with this drive, as it is only a 8 GB unit. Connect the cables and power up, case number and all the other stuff and away it goes. You come back in an hour or so, as it will be ready for the second image to go to the analysis server.

Introduction

This paper will show that the examiner in the above scenario should have taken additional steps to check for hidden data on the hard disk drive. This paper explains possible potential causes of discrepancies between forensically sound images from the same drive by using hidden areas to store data in. Causes examined include BIOS limitations, enhanced BIOS limitations, ATA/ATAPI version limitations, Host Protected Areas (HPA) and Device Configuration Overlays (DCO). In an experiment using EnCase (version 5.01) to capture forensic images, the paper demonstrates how it is possible to use an HPA outside the manufacturers intended use and hide files in it.

Background

When hard disk drives were new to personal computers it was necessary to manually set values in the computer's basic input output system (BIOS) for the number of cylinders, heads, and sectors (CHS) for each hard disk drive attached to the computer (Brouwer, 2004a). This is so that the BIOS can address any block on the disk by specifying a CHS parameter. The BIOS interface to the disk I/O uses 24 bits to address a sector; 10 bits for the cylinder, 8 bits for the head, and 6 bits for the sector. Subsequently this interface cannot address more than $1024 \times 256 \times 63$ sectors, which is 8.4 GB (with 512 bytes per sector).

Over time, the number of hard disk drives available and their configuration lead the industry to develop and agree to a standard that became known as extended BIOS (T13, 2001).

This revised BIOS uses a series of extensions to interrupt 13 h to communicate to the drives controller. This method uses the ATA command `identify_drive` to obtain from the drive the optimal cylinder, head, and sector values. This removes the necessity of having to manually configure the BIOS values and has become an accepted and automated process for most personal computer systems. Extended BIOS uses a pointer to a Disk Address Packet that contains an 8 byte starting absolute block number.

The old ATA standard allows a drive to have at most 2^{28} addressable sectors (8 bits for the sector, 4 bits for the head, and 16 bits for the cylinder). With a 512 byte sector, this gives a capacity of 137.4 GB. As from ATA/ATAPI-6 the specification allows the addressing of 2^{48} sectors or 144 petra bytes (T13, 2002; Brouwer, 2004b).

Host Protected Area

A Host Protected Area (HPA) as defined by T13 in ATA/ATAPI-4 (T13, 1998):

A reserved area for data storage outside the normal operating system file system is required for several specialized applications. Systems may wish to store configuration data or save memory to the device in a location that the operating systems cannot change.

The implementation of an HPA is optional and the manufacturer determines if the device supports this feature. If the device supports an HPA and it is enabled, its effect is to lower the maximum addressable data block. This has the result of reducing the available storage capacity of the device (T13, 1998). The data blocks are not erased or altered; they are just made inaccessible by the drive's controller. For example: an 8.4 GB hard disk drive has 16,515,072 blocks addressable as blocks 0—16,515,071 (based on an example from Carrier, 2005, p. 37). If the drive has an HPA enabled of 1 GB then blocks 0—14,515,071 are accessible while blocks 14,515,072—16,515,071 are not as shown in Fig. 1.

The host is able to command the device to retain the HPA across power cycles and device resets by the use of a volatility control bit. This ensures that

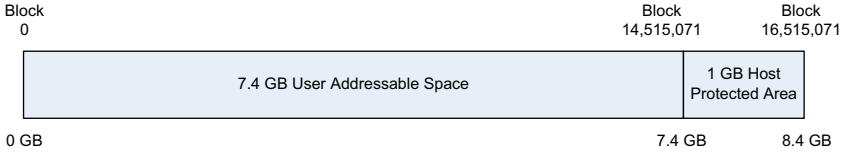

Figure 1 An 8.4 GB storage device with a 1 GB Host Protected Area (HPA) (based on a figure from Carrier, 2005, p. 37).

دریافت فوری ← متن کامل مقاله

ISIArticles
مرجع مقالات تخصصی ایران

✓ امکان دانلود نسخه تمام متن مقالات انگلیسی
✓ امکان دانلود نسخه ترجمه شده مقالات
✓ پذیرش سفارش ترجمه تخصصی
✓ امکان جستجو در آرشیو جامعی از صدها موضوع و هزاران مقاله
✓ امکان دانلود رایگان ۲ صفحه اول هر مقاله
✓ امکان پرداخت اینترنتی با کلیه کارت های عضو شتاب
✓ دانلود فوری مقاله پس از پرداخت آنلاین
✓ پشتیبانی کامل خرید با بهره مندی از سیستم هوشمند رهگیری سفارشات