What are HPAs and DCOs and why do they matter?

What is the HPA?

The Host Protected Area (HPA) is an area of memory on a hard drive that is not normally visible to a computer's Operating System (OS) – for example, it would not be available for the user to store files on. It was implemented so information could be stored that is not easily modified, changed, or accessed by the user, BIOS, or the OS. This means that a drive may contain more than the 'advertised' capacity. This part can only be made accessible using specific tools or commands.

There are numerous reasons why an HPA is created on a drive:

- A vendor can store the necessary files to install or recover the computer's operating system i.e. perform a factory reset.
- Other software may be installed here such as diagnostic programs or other utilities.
- Some malware may hide inside the HPA to avoid detection.
- Users who wish to go to great lengths to hide data may utilise the HPA. (This would require a degree of skill beyond that of regular computer users)

What is the DCO?
Computer system vendors may use the Device Configuration Overlay (DCO) when they wish to have a series of hard drives of varying capacities (possibly because they are from different vendors) that all exhibit the exact same storage volume from the perspective of the OS. For example, the hard drives that a vendor wishes to deploy in their systems may contain more addressable areas (i.e. storage capacity) than is required. Using the DCO feature, the vendor could modify these drives so they consistently display the same amount of usable storage. They effectively hide the additional areas from the user's view without any indication that they even exist.

Why do these matter?
If the DCO or HPA area is not removed by our software then it is not possible to overwrite the data in these areas as it is inaccessible. It is the requirement of some overwriting standards to remove and erase these hidden areas. Failure to remove these can impact on the perceived success of the erasure process. The theory behind this requirement is that both areas could potentially contain some kind of remnant data and they should be removed in order to ensure that all of the potentially user addressable areas are available for erasure.

Blancco erasure software currently has the capability to remove DCO and HPA areas but the possibility to do this requires that the BIOS on a computer does not freeze lock the necessary commands. More information about freeze locks can be found in another FAQ article – here. More information about HPA/DCO removal reporting can be found in another FAQ article – here.

Further Reading

- Gupta M., Hoeschele M., Rogers M., Hidden Disk Areas: HPA and DCO, International Journal of Digital Evidence, Purdue University, 2006. http://www.utica.edu/academic/institutes/ecii/publications/articles/EFE36584-D13F-2962-67BEB146864A2671.pdf
- Wikipedia's entry on HPA: http://en.wikipedia.org/wiki/Host_protected_area
- Wikipedia's entry on DCO: http://en.wikipedia.org/wiki/Device_Configuration_Overlay