Hidden Disk Areas

Mayank R. Gupta, Michael Hoeschele & Marcus K. Rogers

INTRODUCTION

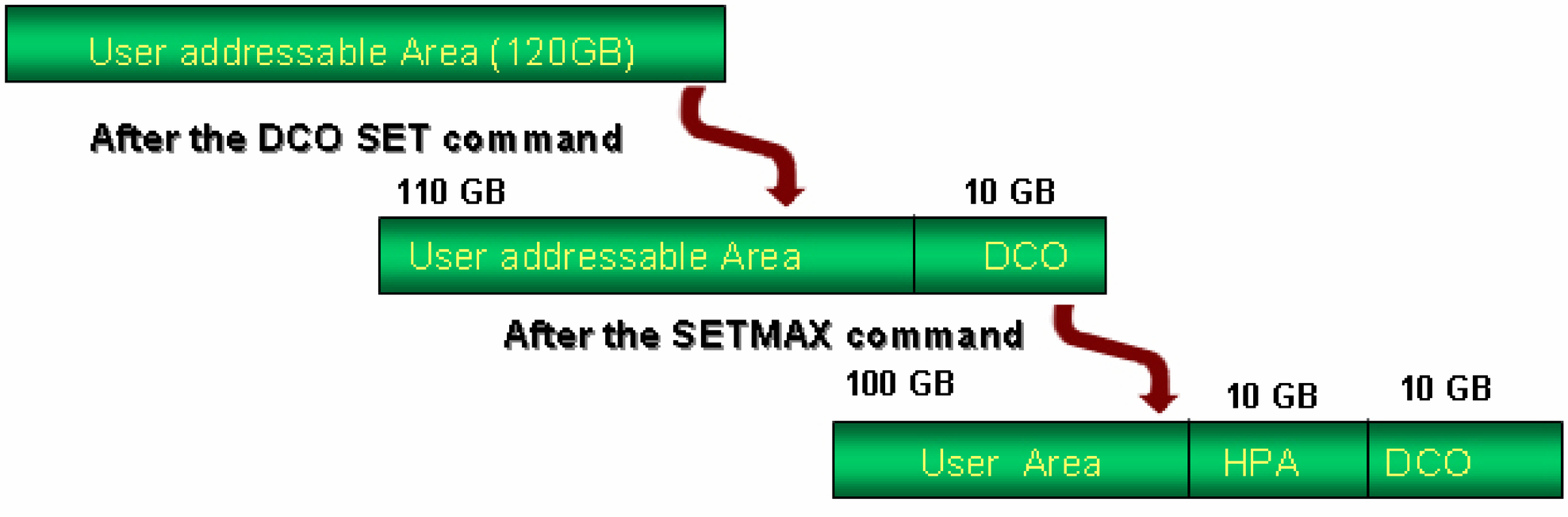
- The ability to store information on a hard drive in such a manner that it is invisible to forensic investigators is becoming a growing problem for Law Enforcement.
- It should be noted that these areas are hidden from the BIOS, user and OS.
- This project examines the forensic significance of these vendor hidden disk areas

HOST PROTECTED AREA (HPA)

- . Defined as an area for storing diagnostic utilities or boot code.
- It is possible to boot from HPA using the Address offset method

DEVICE CONFIGURATION OVERLAYS (DCO)

- System vendors can configure hard disks of varying sizes to have same number of sectors.
- HPA and DCO can co-exist on the same disk.



FORENSIC SIGNIFICANCE

- Forensic tools like Encase and Sleuth Kit can detect HPA, but not DCO.
- The acquisition phase can miss these areas.
- Integrity of the evidence is not affected.
- Crucial Evidence can be overlooked.

Results of this study submitted to the International Journal of Digital Forensics for publication.