Digital Forensics

Question 1:

**A technician needs to collect a forensic disk image and ensure that they do not change the contents of the drive during the collection of the image. What tools should the technician use?**

* Degausser
* Software Write Blocker
* Hardware write blocker
* Drive Duplicator

Question 2:

**What does "bs" do when using the dd command in Linux, UNIX, or OS X?**

* Sends the output to a blank sector
* Sets the beginning sector of the drive image
* Sets the block size
* Removes error message and other error data from the image

Question 3:

**What tool is used to collect memory data for forensic analysis on a Linux system?**

* EnCase
* DumpITt
* WinPMem
* fmem