SSD Drive Basics

Similar to hard disk drives, solid state disk drives (SSDs) are typically where a lot of digital evidence is stored and collected, so understanding how they work and where data can be hidden is important, allowing you to collect artifacts in future lessons. This lesson will cover the following SSD basics:

- Garbage Collection
- Trim
- Wear Leveling

WHAT ARE SSDs?

A solid-state drive (SSD) is a new generation of storage device. SSDs have evolved beyond traditional mechanical hard disks by using flash-based memory which is significantly faster, allowing SSDs to speed up computers significantly because of their low read-access times and fast throughputs. Instead of writing data to a magnetic disk, solid-state disks instead data is written to "pages", and once there's enough, it's written to a "block" on the actual drive.

GARBAGE

Garbage collection is a process used by solid-state drives to optimize space and improve efficiency. The goal of garbage collection is to keep as many empty blocks as possible, so that when the SSD needs to write data, it can do so without waiting for a block to be erased. The SSD's controller looks for any pages that are no longer being used, such as deleted data and modified data. It then moves used pages to new blocks, leaving behind the data that is no

such as deleted data and modified data. It then moves used pages to new blocks, leaving behind the data that is no longer needed. The controller then erases the block so that it's ready for use. This is a background process, handled by the SSD controller and the operating system.

Why is garbage collection important in regard to digital forensics? If we have crucial evidence on a system, there's always the risk that garbage collection will identify the blocks either legitimately or illegitimately as unwanted, and the controller will erase the blocks in order to free up space. If a computer is using solid-state drives, it needs to be powered off immediately to prevent this from happening, either with a hard shut-down (holding the power button until the system turns off), or pulling the plug so the power supply unit (PSU) receives no electricity. Shutting down the system via the operating system could execute a malicious script that works to destroy data contained on any attached drives, and could ruin an investigation (but we need to remember volatile evidence, which we'll cover later!).

TRIM

When files are sent to locations such as the Recycle Bin, they are not immediately deleted. Moving them to this location tells the operating system that it is ok to overwrite these files, as they are no longer wanted by the user. If a deleted file is 174192 bytes, and a new file is only 121 bytes, then there will still be 174071 bytes of the deleted file available, so we can recover this and attempt to fix the file so we can see what it was, even with some missing data. However, TRIM operates similarly to Garbage Collection, and instead of telling the SDD to make the size of the deleted file unallocated (available for overwriting), TRIM on an SSD will simply select the data and clear it, removing any chance of forensic investigations recovering the file, or parts of the file.

To counter this, we should take the same actions when dealing with Garbage Collection, as they work together. Power the system off with a hard shut-down or pull the plug (again, we need to remember volatile evidence, which we'll cover later!).

WEAR LEVELLING

Wear leveling is a technique that some SSDs utilize to increase the lifetime of the memory using a very simple approach: evenly distribute writing on all blocks of an SSD so they wear evenly. Using this method, all physical cells in the SSD receive the same number of writes, to avoid writing too often on the same blocks, causing damage over time.

Wear leveling is performed by the micro-controller or the firmware of the SSD device. The process of wear leveling is conducted by algorithms, of which there are two basic varieties.

- **Dynamic wear leveling** – When dynamic wear leveling is used blocks that undergo rewriting are repositioned to new blocks. The algorithm selects an empty block on which to write the data. The number of writes to each block are kept track of by the controller. A downside to dynamic leveling is that data blocks that are not frequently updated are not moved which can lead to uneven block wear.
- **Static wear leveling** – The same techniques are employed by static wear leveling with one important difference. Blocks of static data are moved when their block erase count falls below a certain threshold. This leads to more effective leveling which results in slightly slower write performance countered with enhanced longevity of the device.

Previous Topic
Mark Complete
Next Topic
Back to Lesson