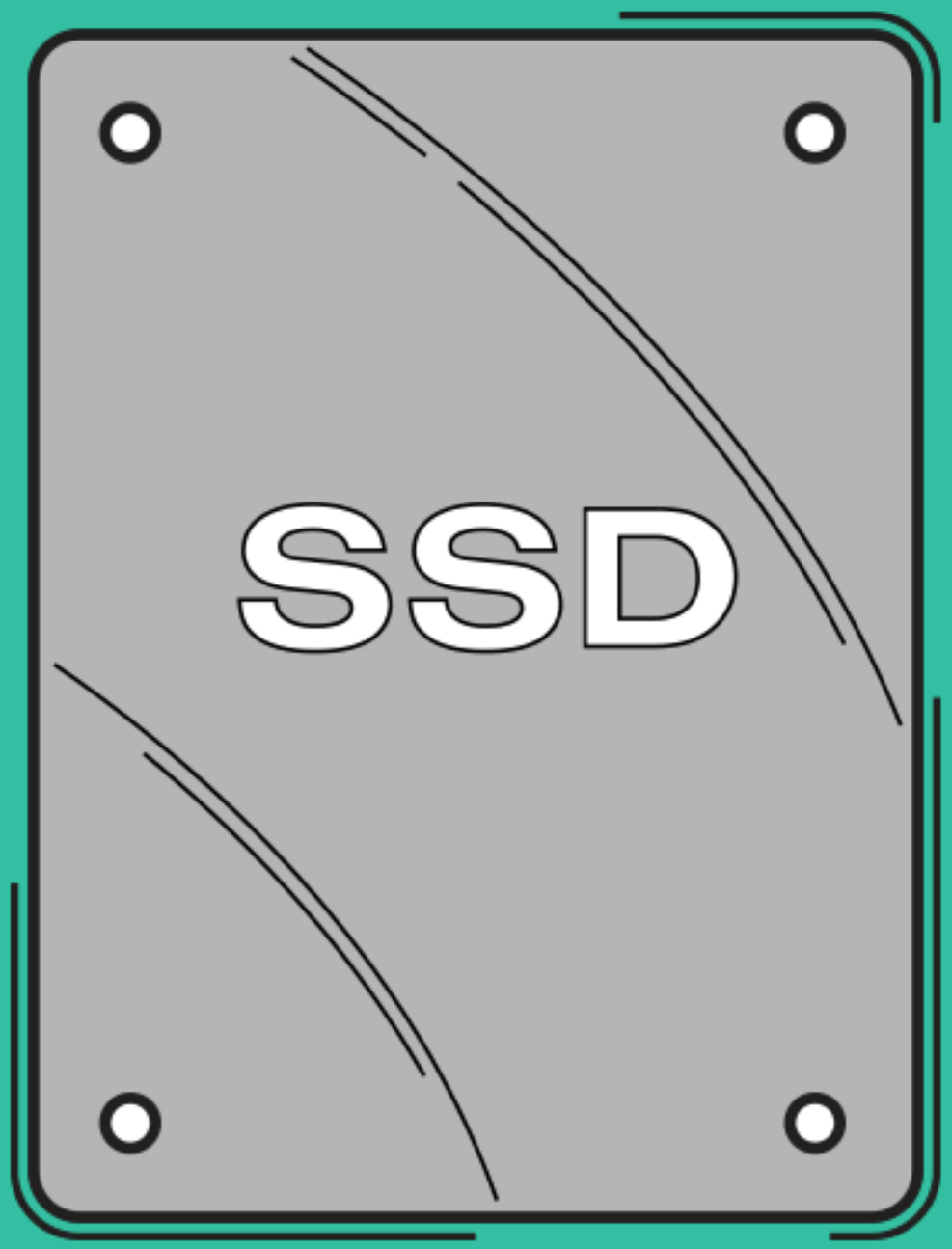
Sentient Storage:

Do SSDs have a mind of their own?

Tom Kopchak :: @tomkopchak

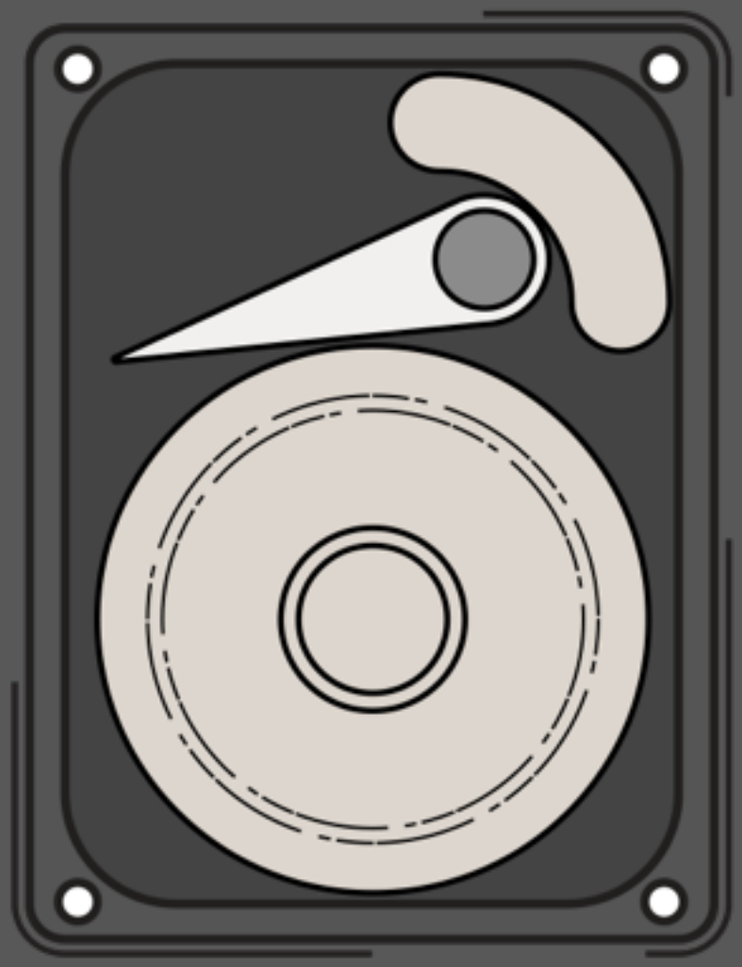
About me

Why we're here

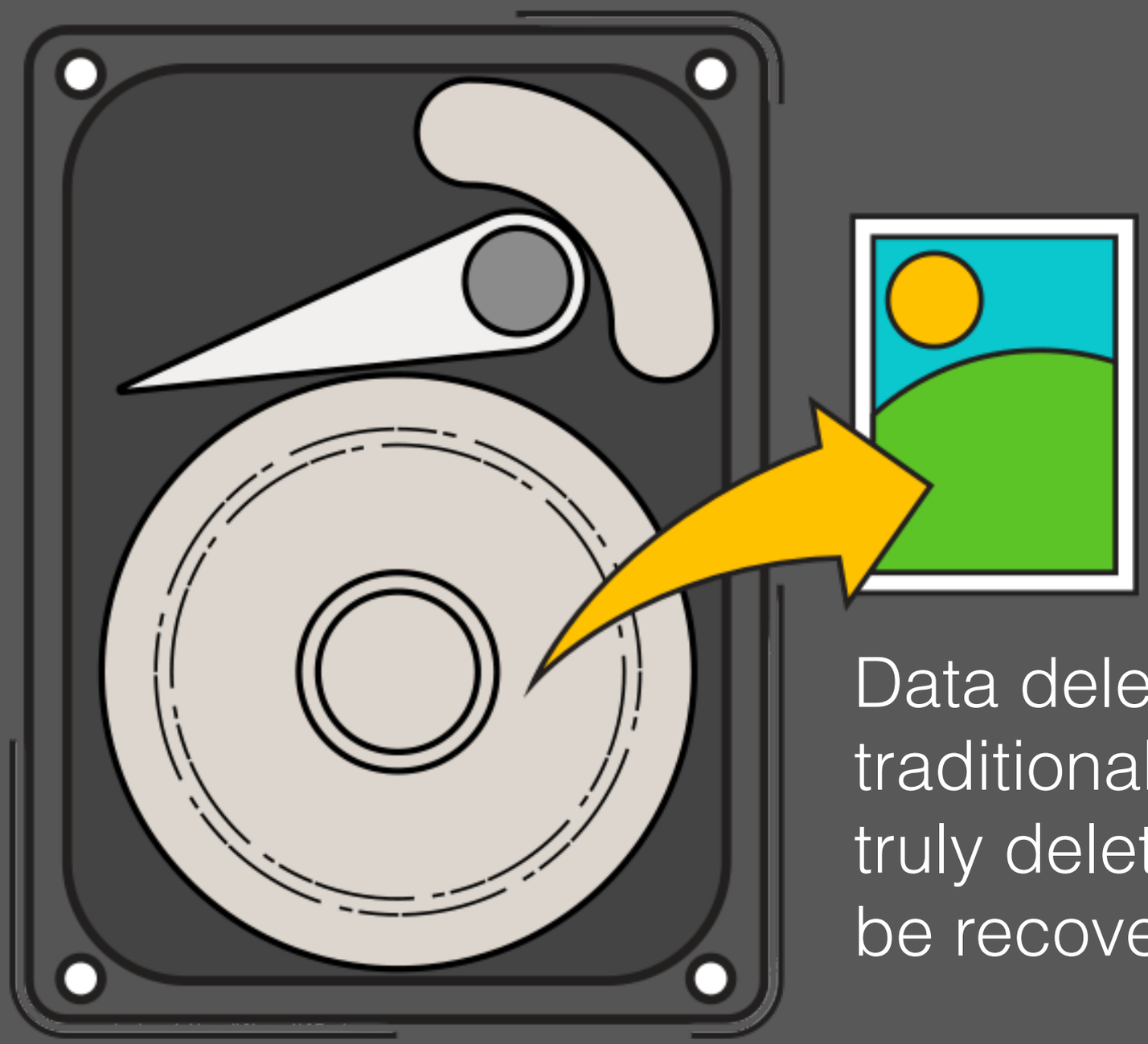


- Current forensic practices for working with hard drives are well-defined
- Solid state drives behave differently and present new challenges
- This presentation will explore these differences in detail

Forensics:
Traditional Hard Drives



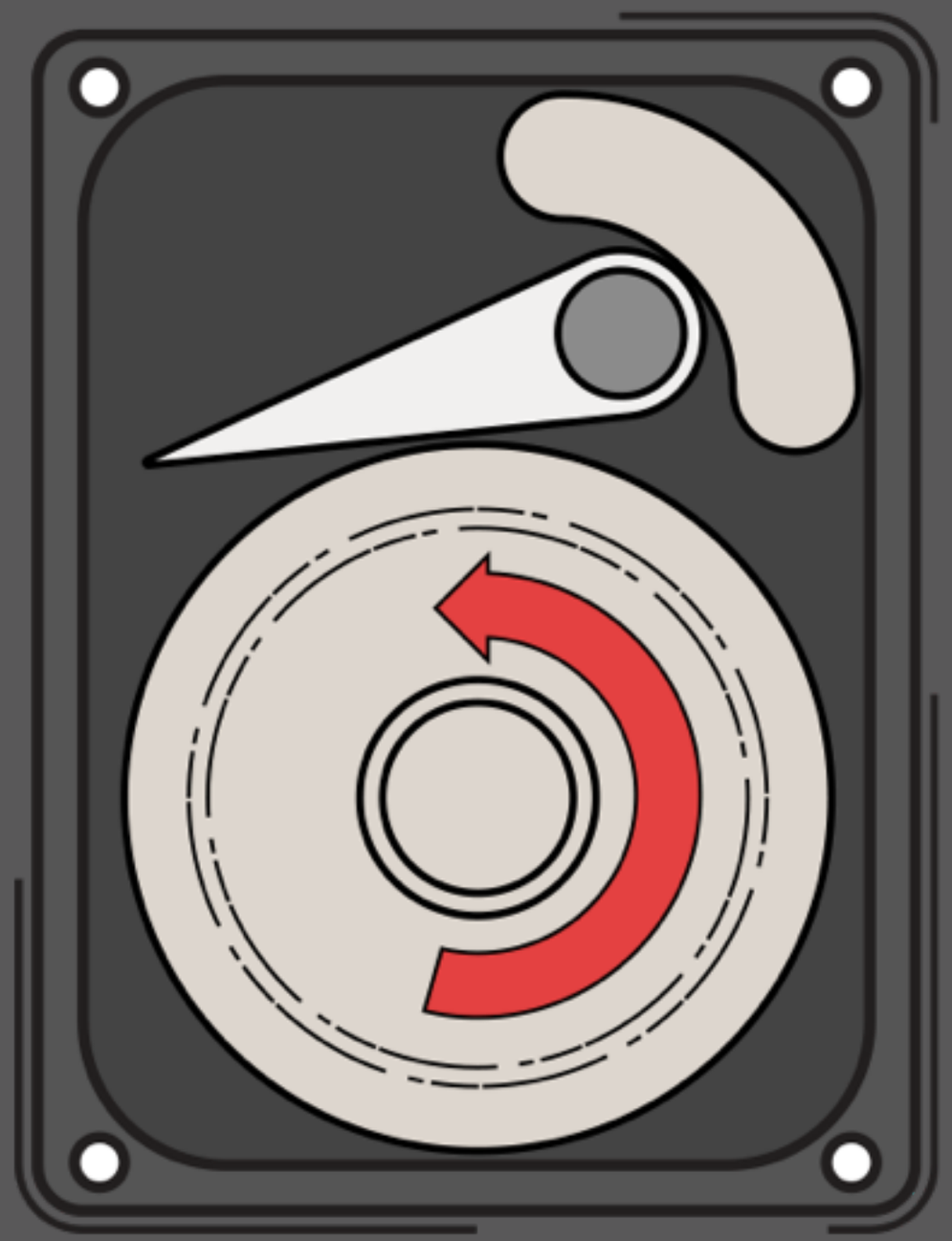
What do we already know?



Data deleted on a traditional hard drive is not truly deleted and can often be recovered quite easily

What do we already know?

Quick formatting a hard drive doesn't actually delete or purge data from the drive

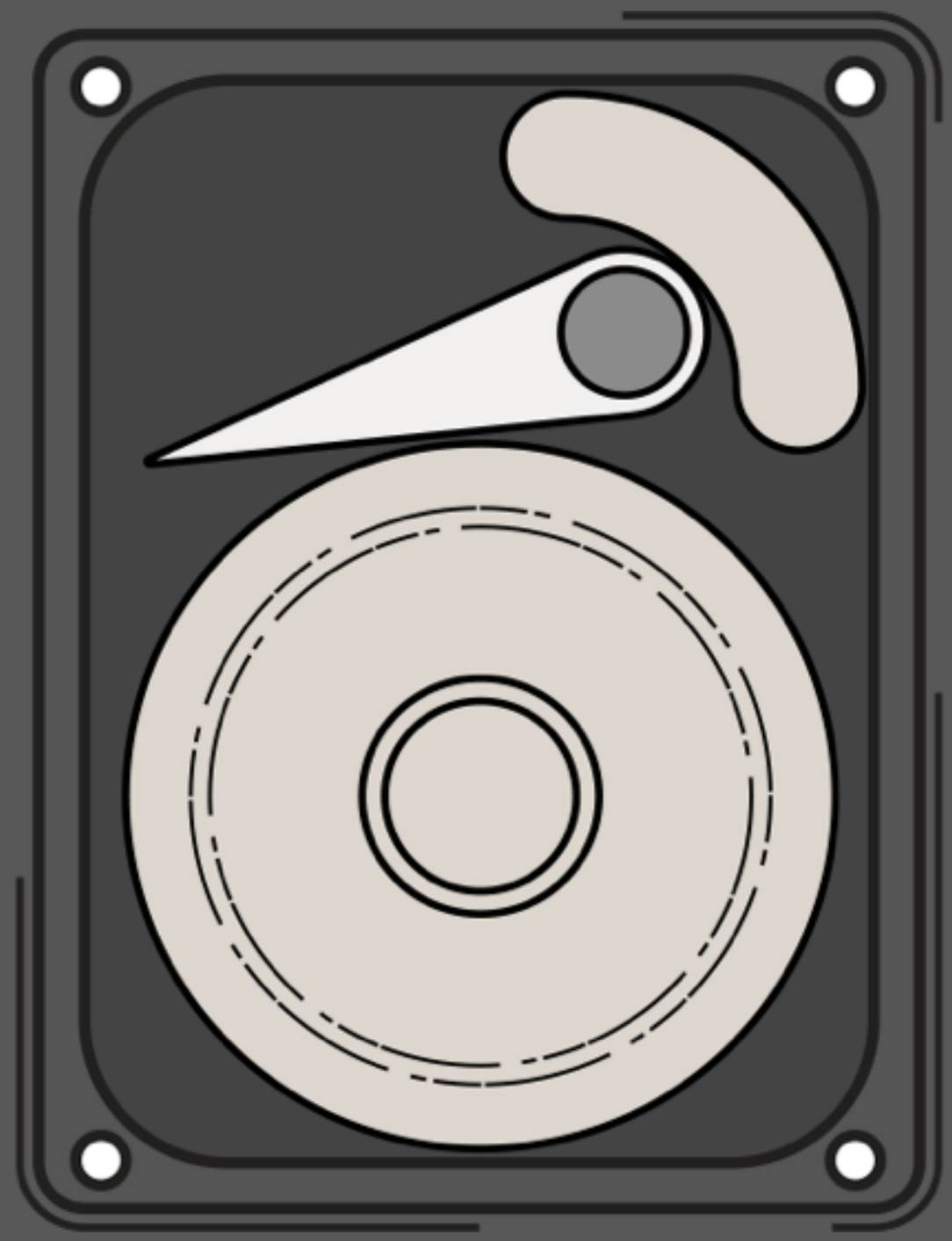


What do we already know?

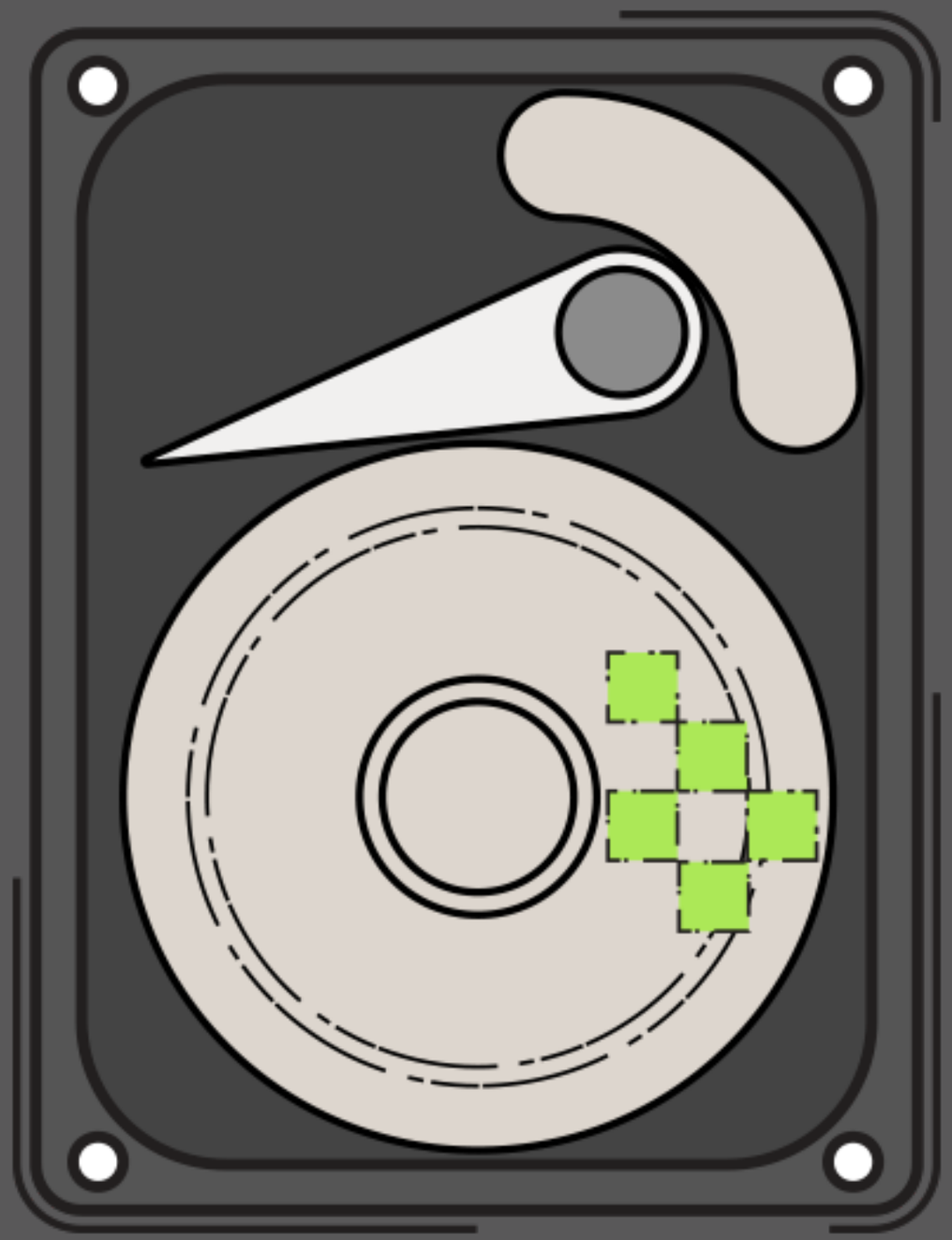
In order for data to be deleted from a traditional hard drive, it must be completely overwritten at least once

What do we already know?

Traditional hard drives do not manipulate or optimize incoming data



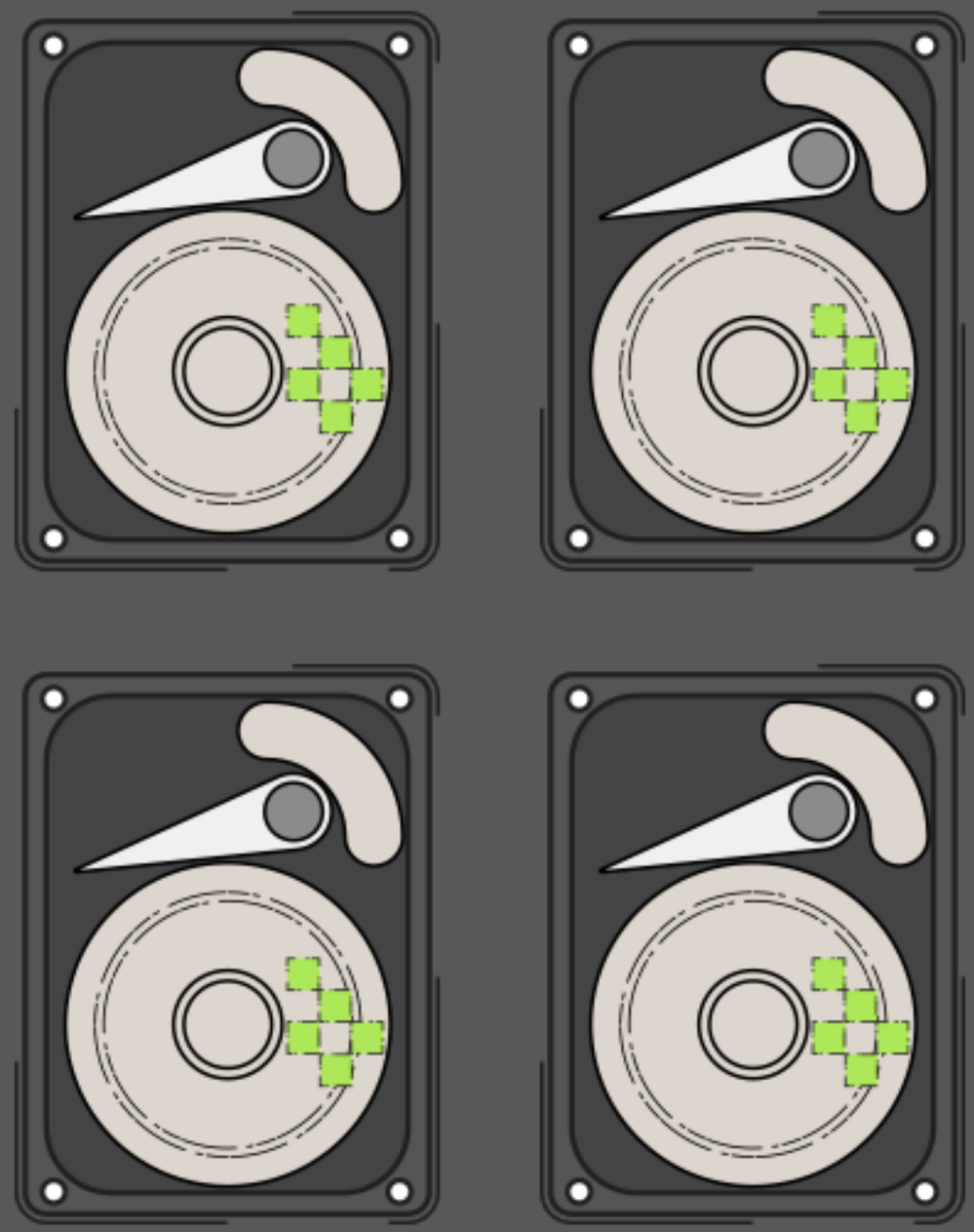
What do we already know?



Traditional hard drives do not change the physical location of a block of data independently of the operating system

What do we already know?

These behaviors are consistent across all traditional hard drives, regardless of manufacturer, capacity, or firmware revision

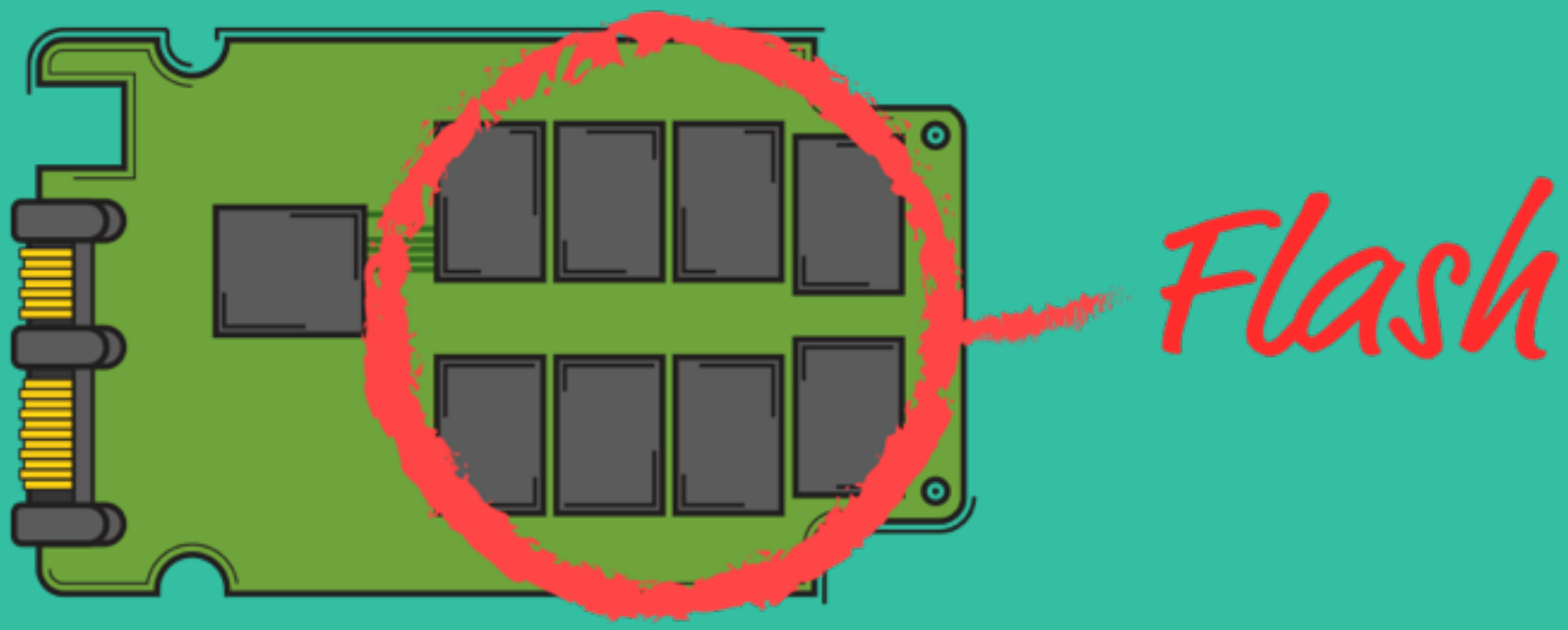


Solid State Drives

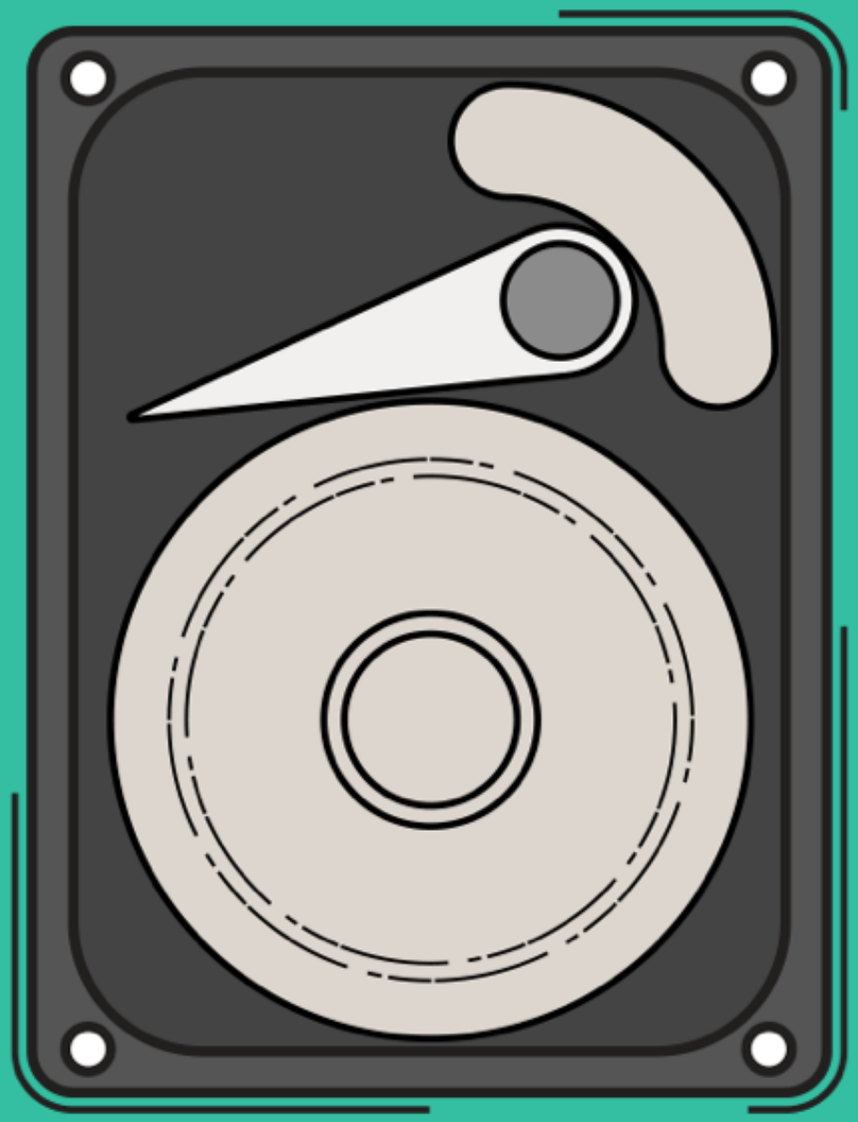
change all of this

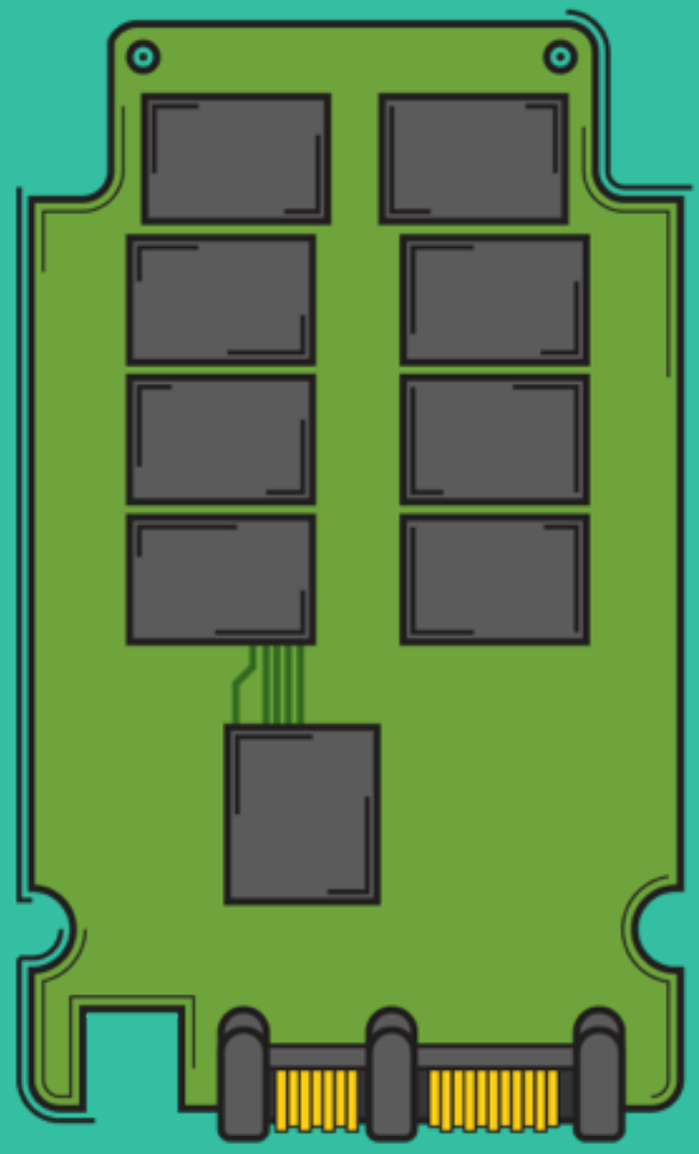
Let's talk about flash memory

- Flash memory is where data is stored on a solid state drive
- An SSD will be composed of a number of flash memory chips to reach its desired capacity
- The drive controller is the glue that holds all of this together
- Commonly referred to as the Flash Translation Layer (FTL)



Drive Types Compared

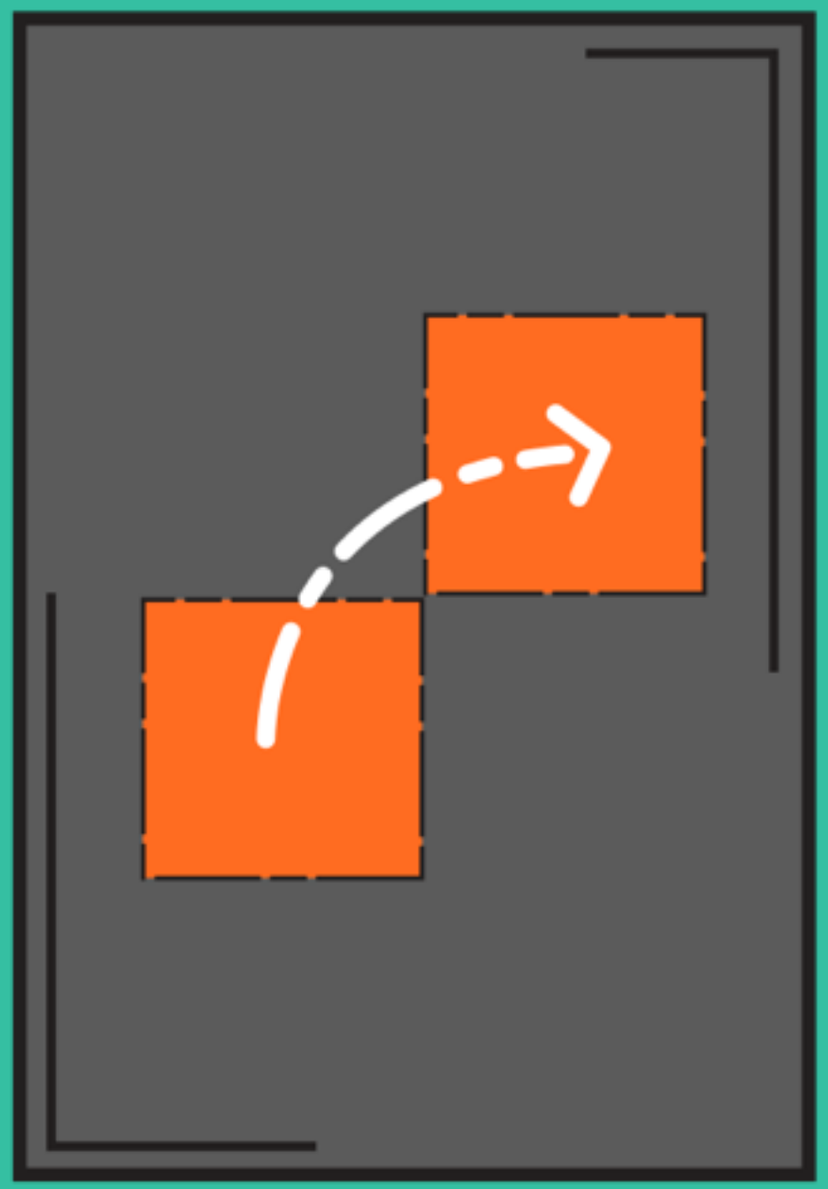




Physical Flash Architecture

- There are different types of flash memory - single level cell (SLC) and multi-level cell (MLC)
  - SLC - one bit per cell: 0 or 1
  - MLC - two bits per cell: 00, 01, 10, or 11
  - A blank cell is represented in all 1s

Physical Flash Architecture



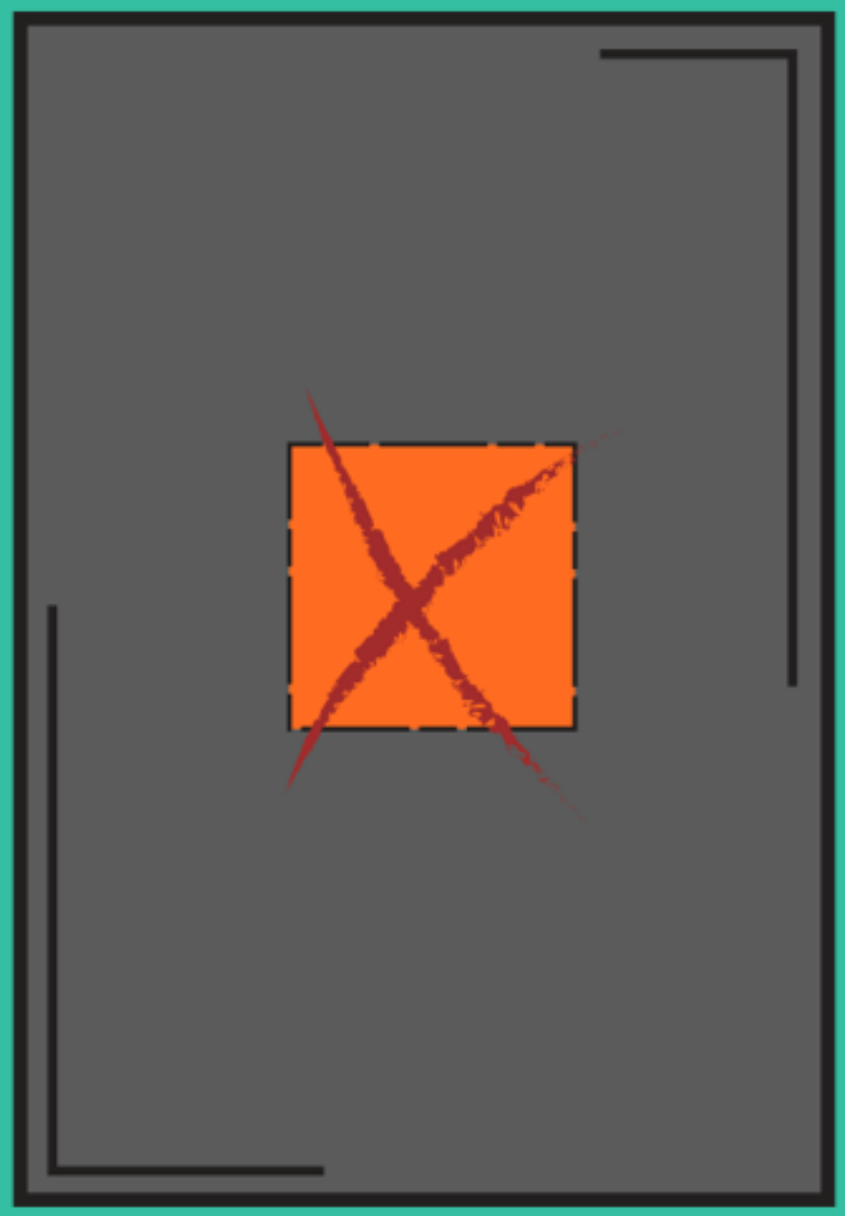
- Pages are the smallest addressable unit in a flash memory cell
- Pages cannot be overwritten, due to the fact that erasing them might modify adjacent cells in a block
- Only entire blocks are erased at a time

Erasing Flash Blocks

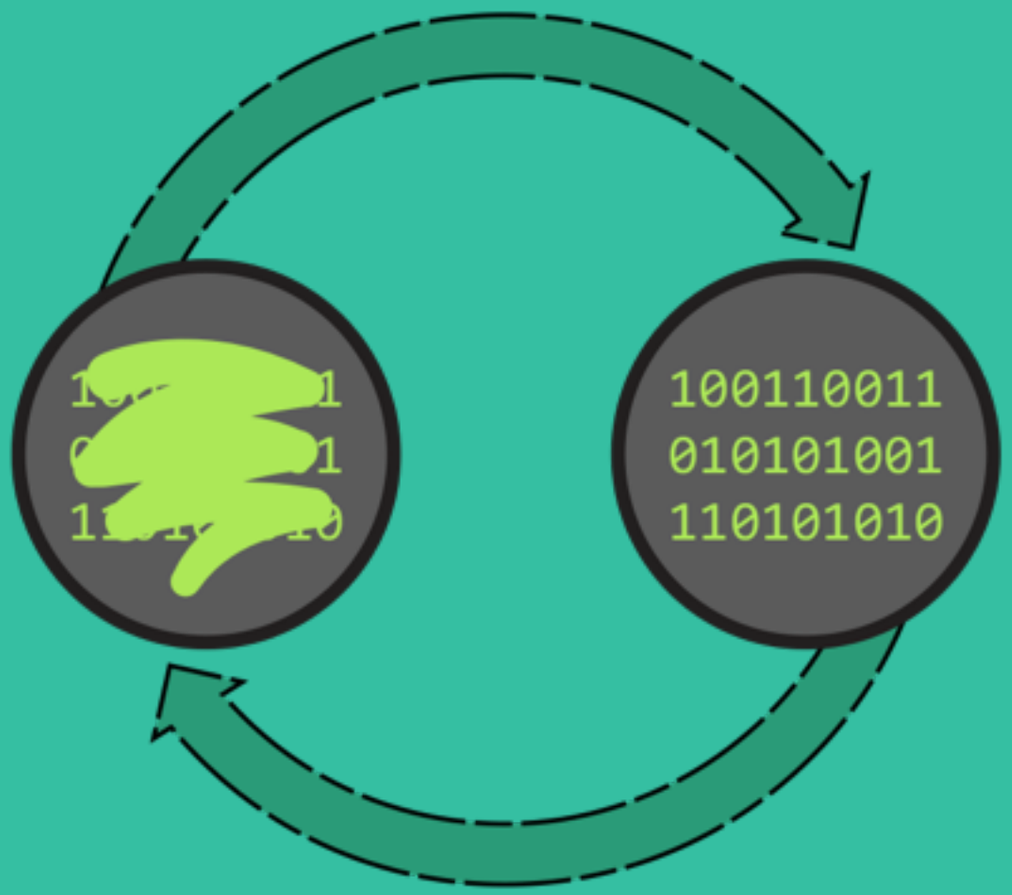
- When data is deleted, the blocks containing this data are marked as invalid

- They cannot be reused without first being reset/ erased

- Erasing a block of flash memory is expensive in terms of electrical current and time



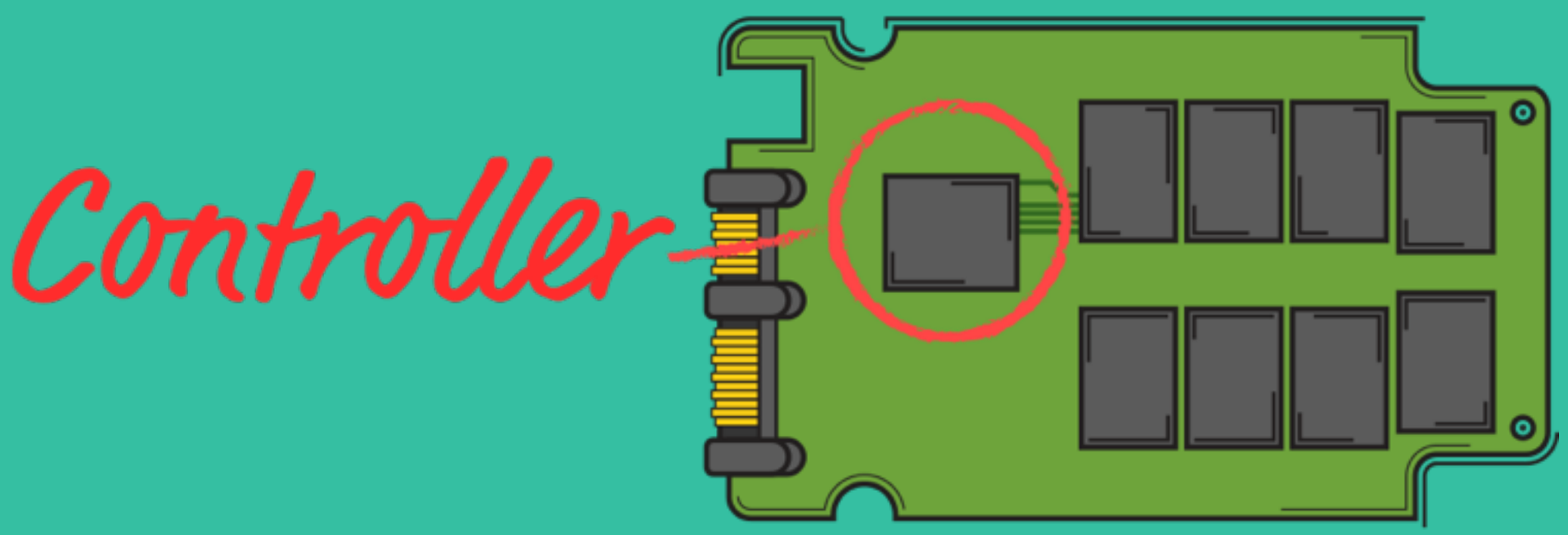
Flash Wear



- Flash cells have a finite number of write/erase cycles
- Wear can be uneven, e.g., some files are written more frequently than others
- This is managed by the drive controller

Drive Controllers

- Controllers are the heart of an SSD
- From the perspective of the operating system and user, SSDs perform the same function as a hard drive
- Drive controllers handle managing, reading, and writing flash cells
- Controllers also manage erasing flash cells and leveling of flash memory wear



Drive Controllers

- There are many different controllers manufactured
- Individual firmware revisions also exhibit different behavior
- Some controllers also include additional optimizations, such as deduplication of incoming data
- Most drives perform garbage collection to recycle flash blocks as data is deleted from the drive - but how do they know?

Garbage Collection

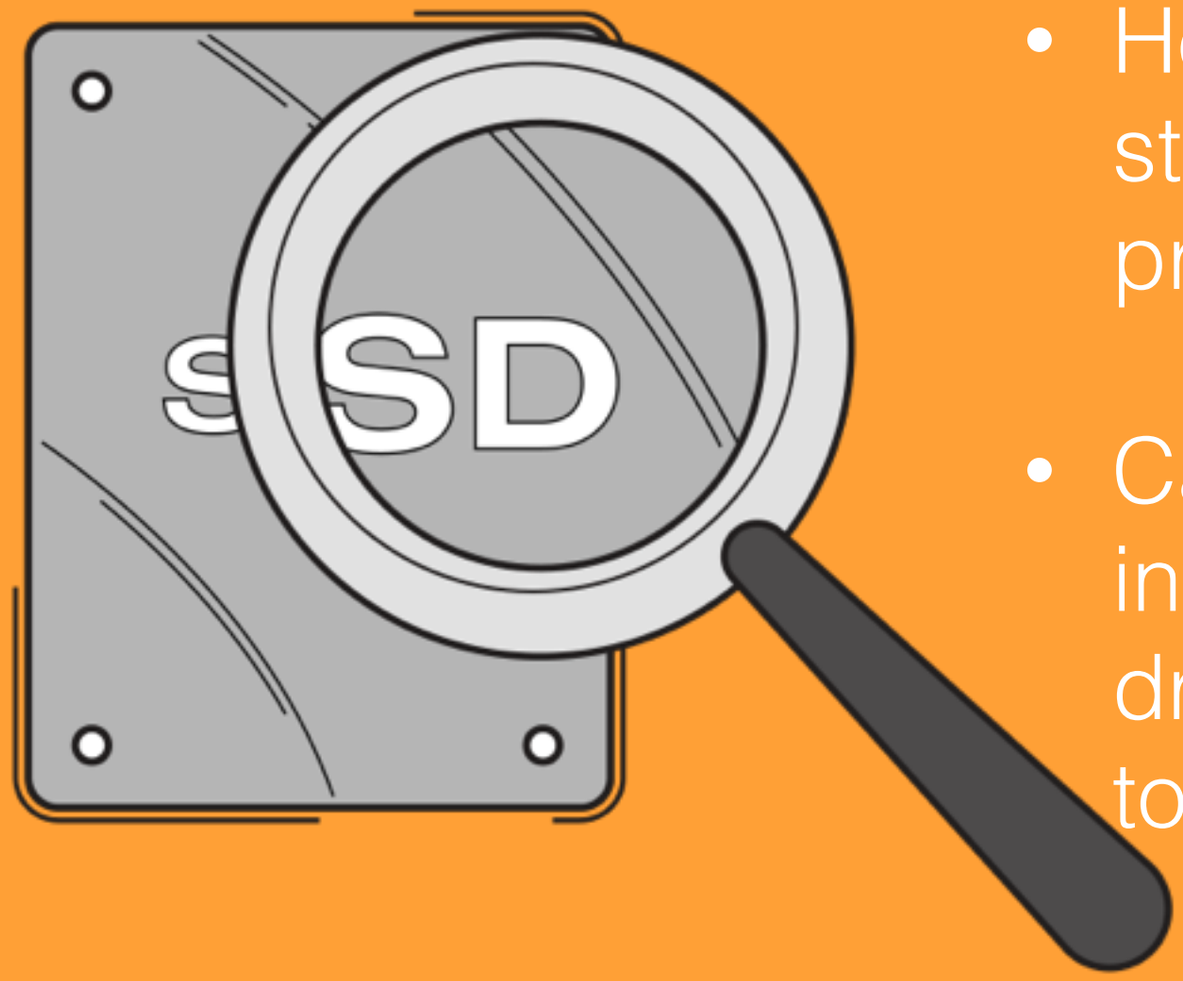
- Periods of read/write are relatively infrequent
- Idle time is ideal for performing operations to optimize drive behavior and performance (garbage collection and wear leveling)

TRIM

- ATA command for notifying the SSD of deleted pages
- Frequently accelerates the garbage collection process

In general:
SSDs behave more like an enterprise SAN or RAID array than simply a hard drive

Forensic Implications?



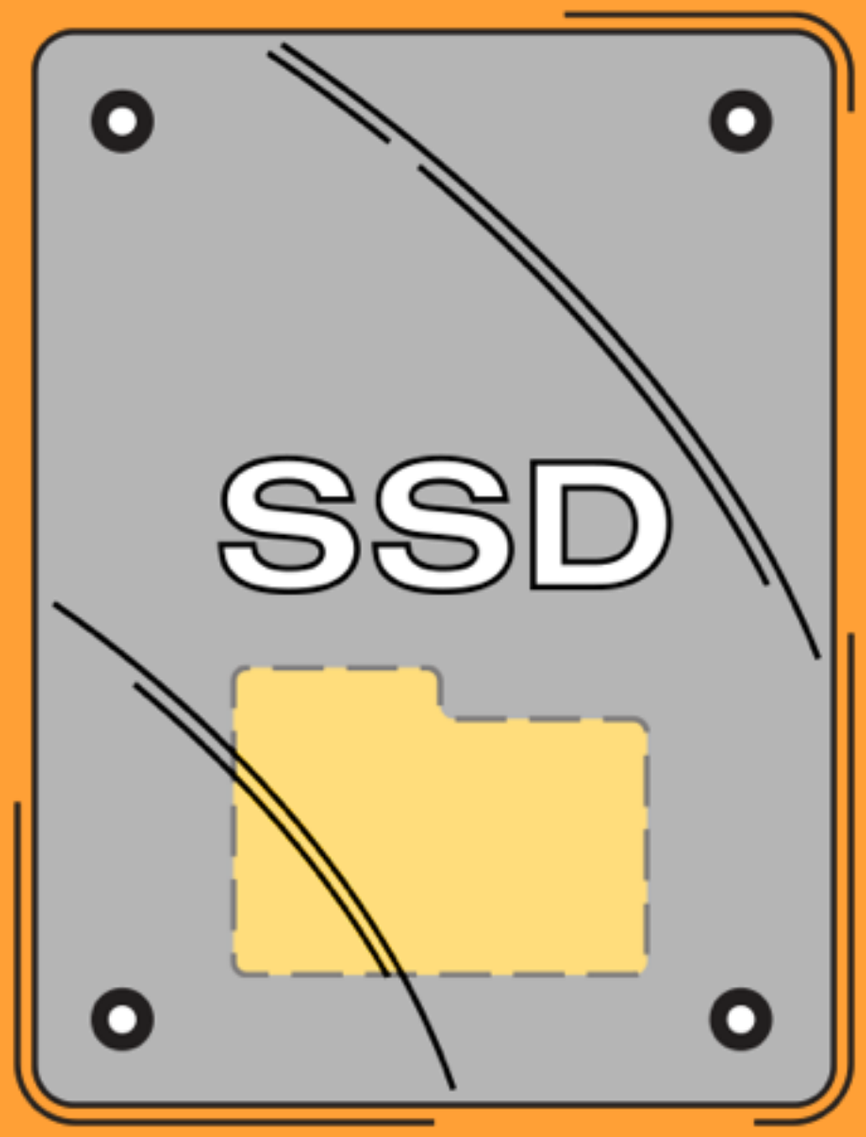
- How do we determine if solid state drives impact forensics process?
- Can SSDs be treated by investigators like standard hard drives or do procedures need to change?

Previous research

The research

- Represents one of the most comprehensive studies of the recoverability of deleted files on SSDs to date

- Eleven different two-part tests conducted across a pool of seven drives, exploring how subtle differences impact the likelihood of deleted file recovery



Purpose

- Comprehensively study the impact of solid state drives on the forensics data acquisition and investigation process
- Focus on the impact of these drives on current forensics practices involving deleted file recovery
- Determine if traditional forensics approaches are sufficient for recovering deleted files from a solid state drive

Experimental design

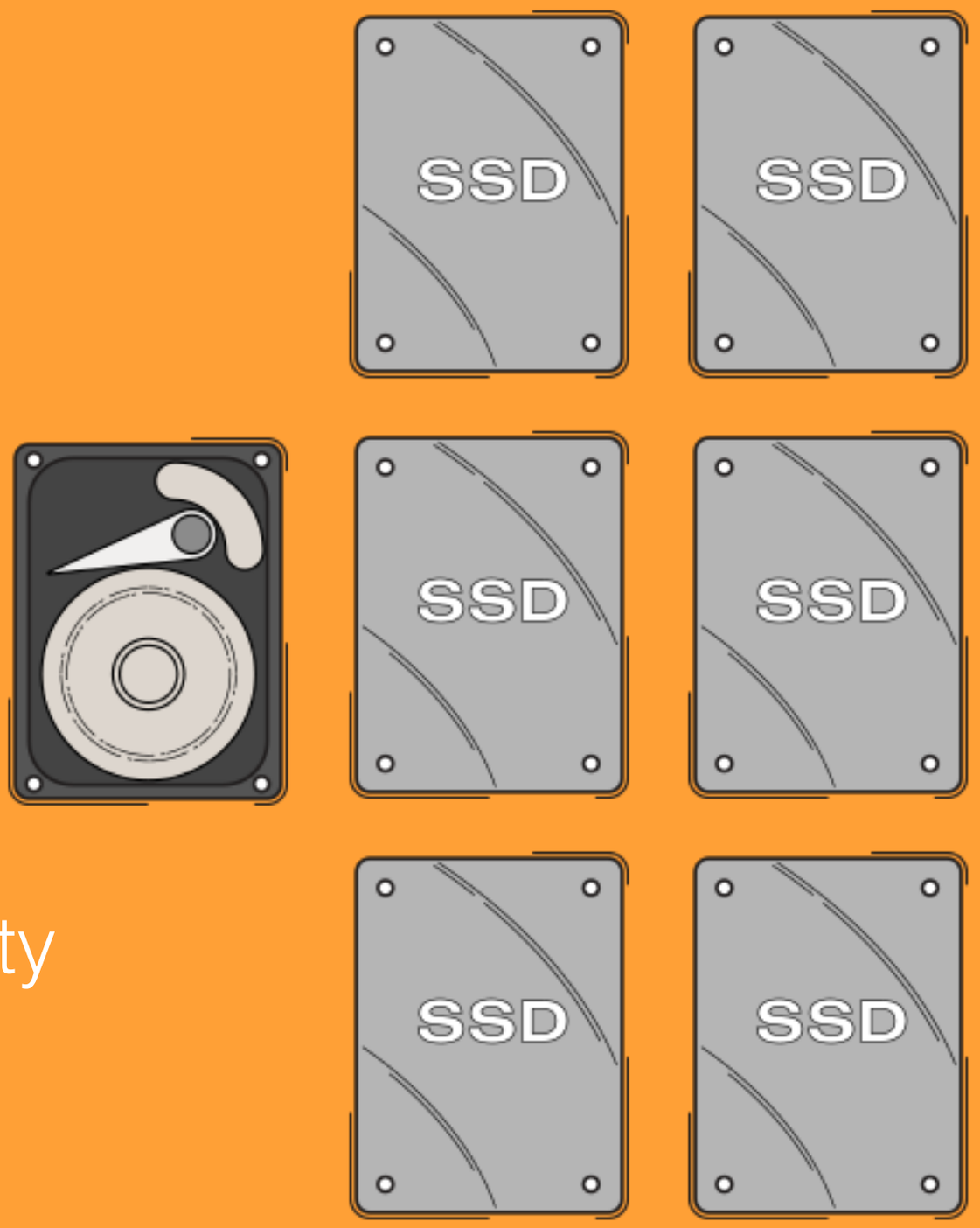
- Tests built on each other
- Designed to use the smallest possible changes incrementally to trigger differences in drive behavior
- Each test - two parts
  - Deleted file test
  - Quick format test

Types of tests

- All tests isolated variables
- TRIM state (as a result of OS configuration or support, or interface support)
- Number of files present (single file versus multiple)
- Files deleted over a period of time

Sample Drives

- Seven total drives - six SSDs and one control hard drive
- Seagate control hard drive
- SSDs: Crucial, Intel, OCZ, Patriot, Samsung, SuperTalent
- SSDs were selected for a variety of factors

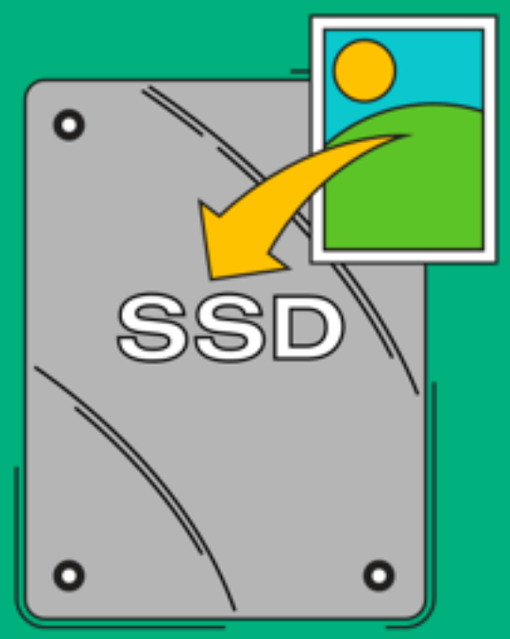


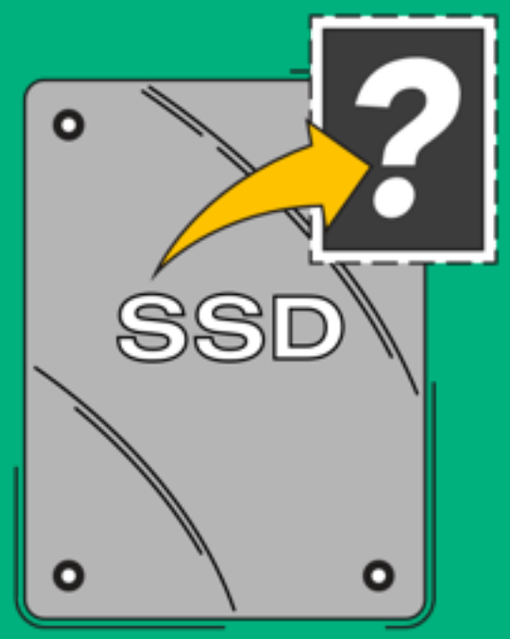
Forensics Lab

- Dedicated evidence creation and evidence collection machines
- Test drives did not run the operating system to minimize variables
- Open source tools (Caine Linux) used wherever possible
- Evidence collected using forensics writeblocker

Sample test

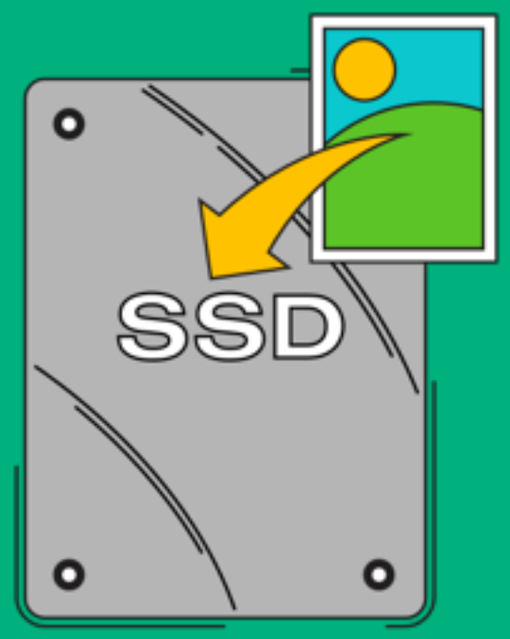
- Experiment: write a single image file to disk, unmount the disk to ensure it is not cached, then delete the file and attempt recovery
- Expected results: file is recoverable
- Actual results: file is not always recoverable
- Why?

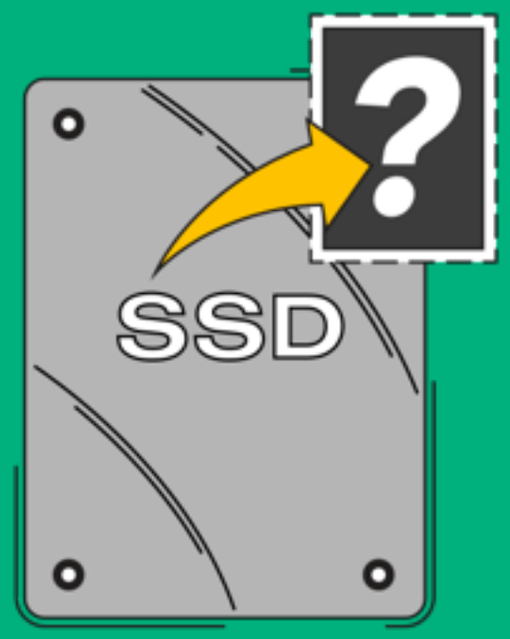




Sample test - part 2

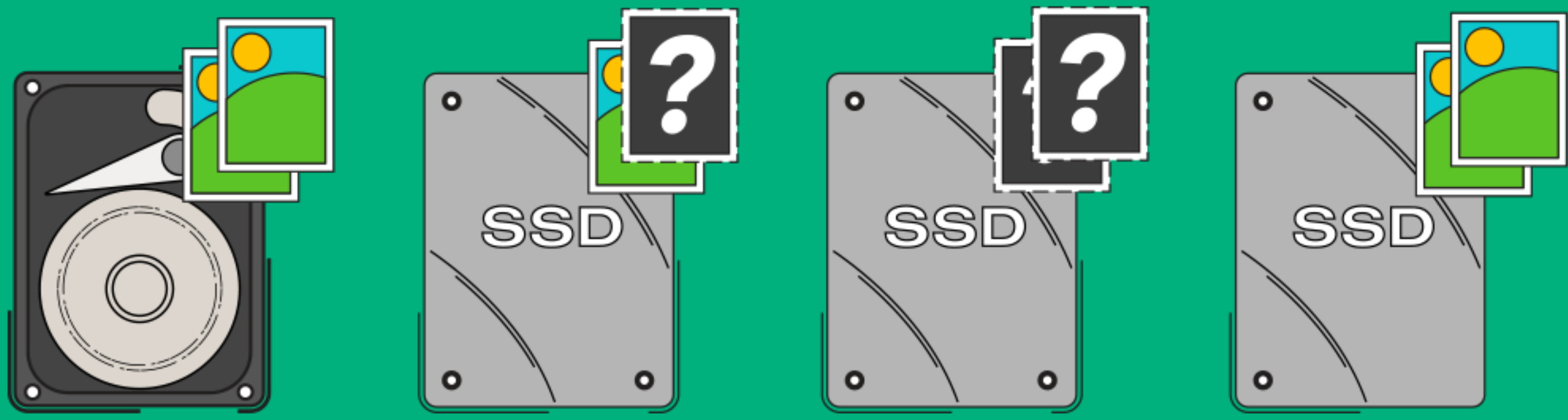
- Experiment: quick format of drives from previous test, followed by a recovery attempt (including file carving)
- Expected results: file is recoverable
- Results: file is not always recoverable
- Why?





Patterns observed

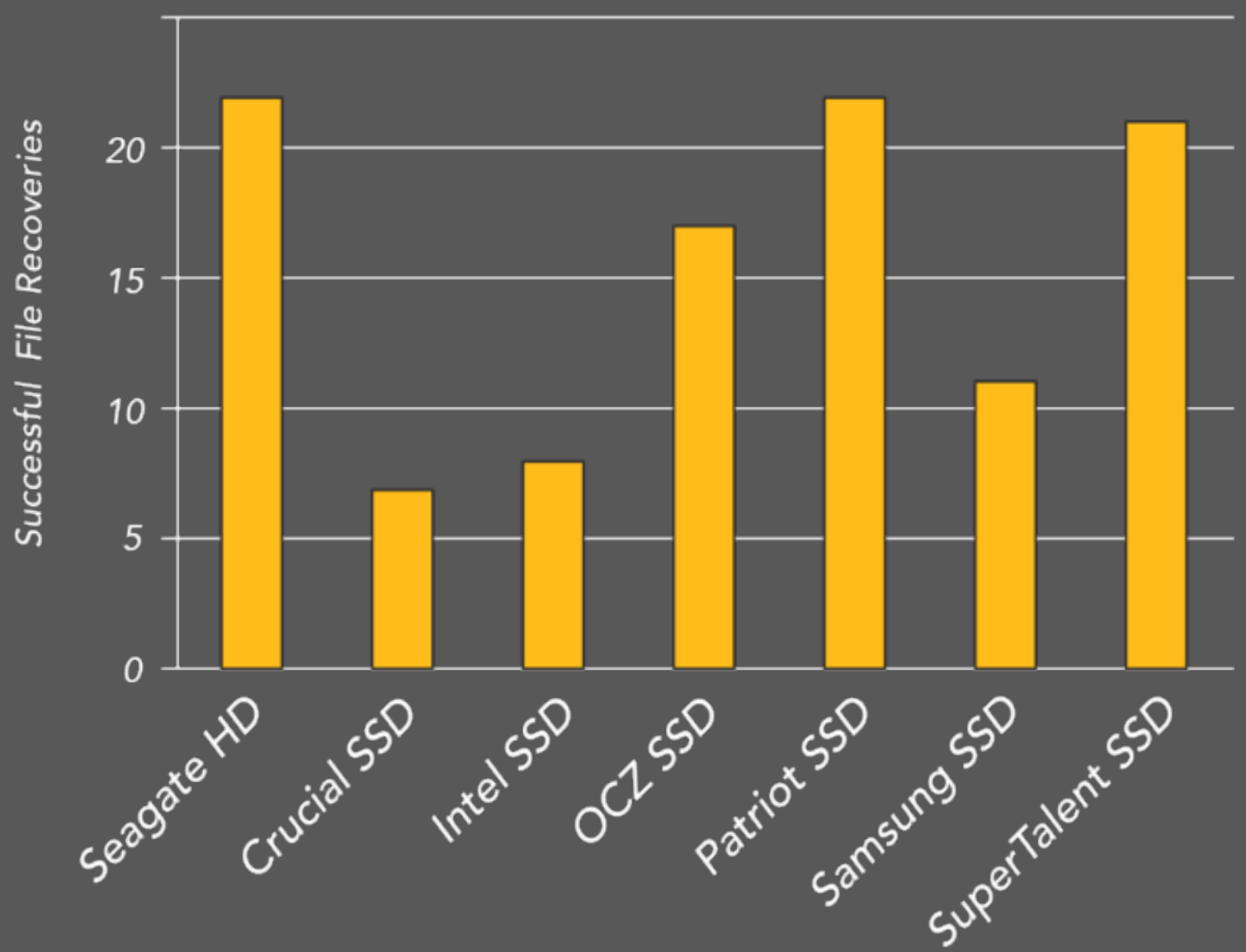
- All files recoverable from control drive nearly every time
- Significant differences in SSD behavior
- Some behave very similarly to control drive
- Others offer very low recoverability



Factors impacting recoverability

Drive firmware behavior and controller

fig 7



Factors impacting recoverability

TRIM State - On and Off

fig 10

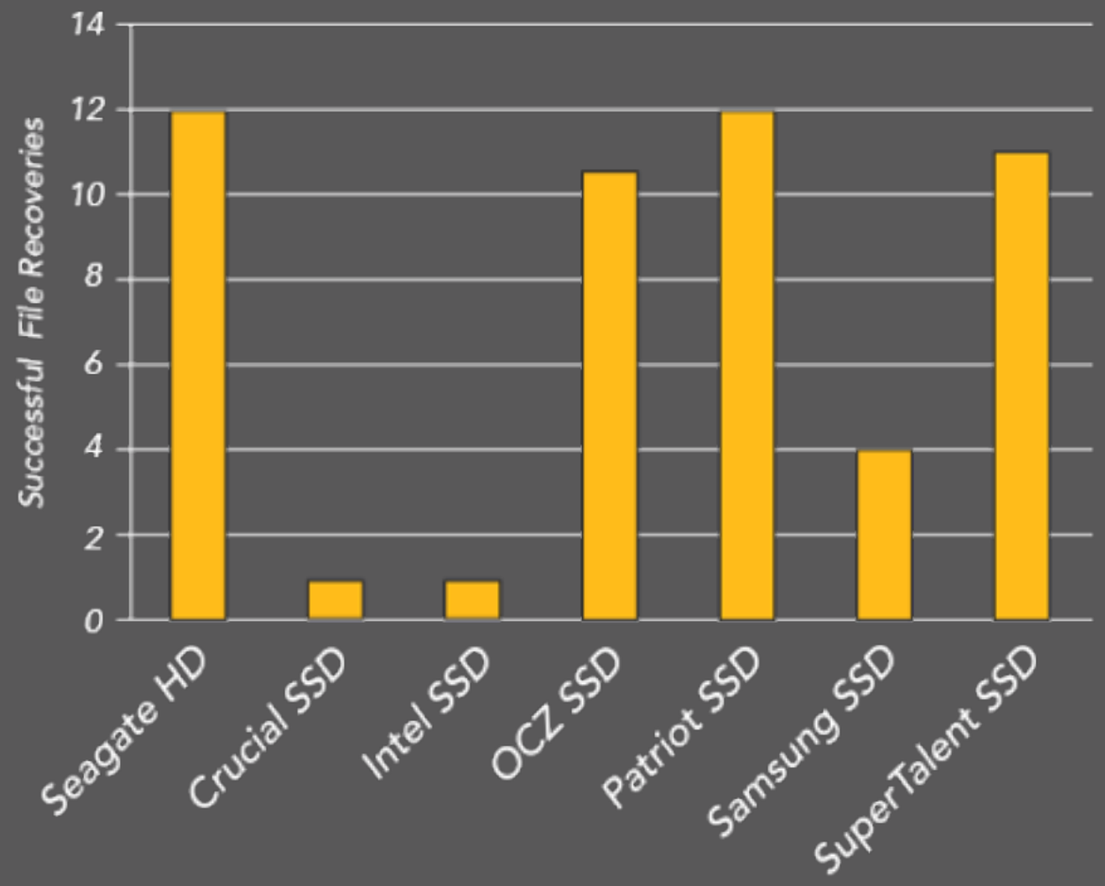
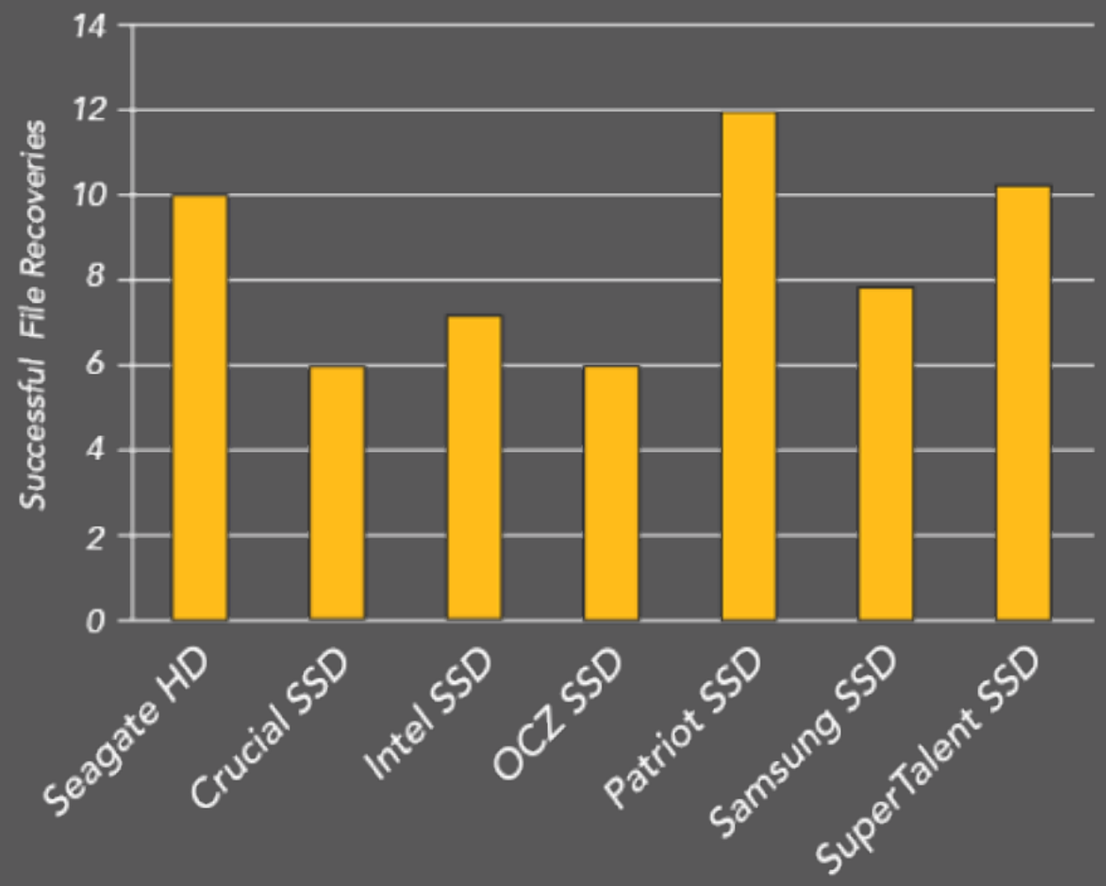
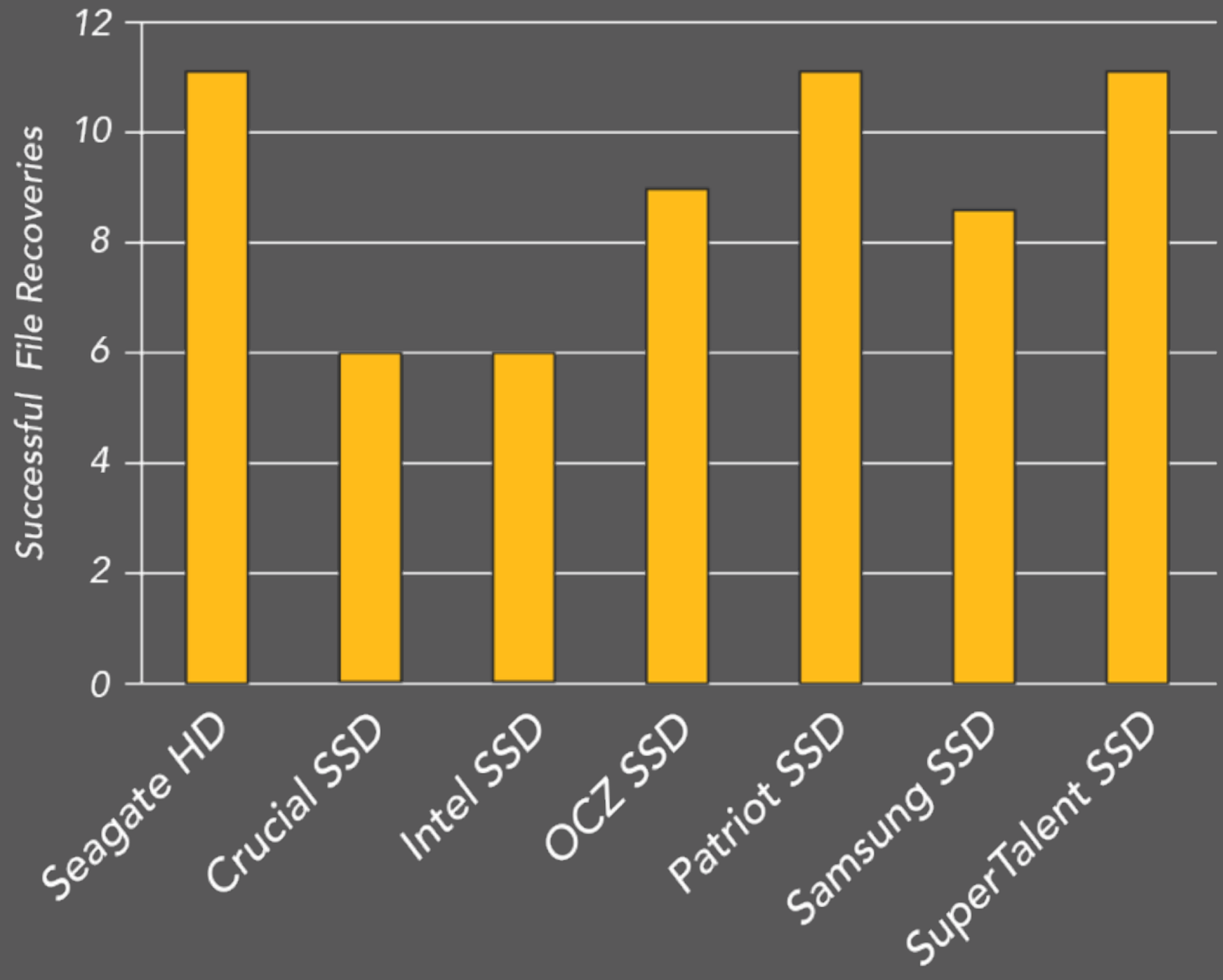


fig 11



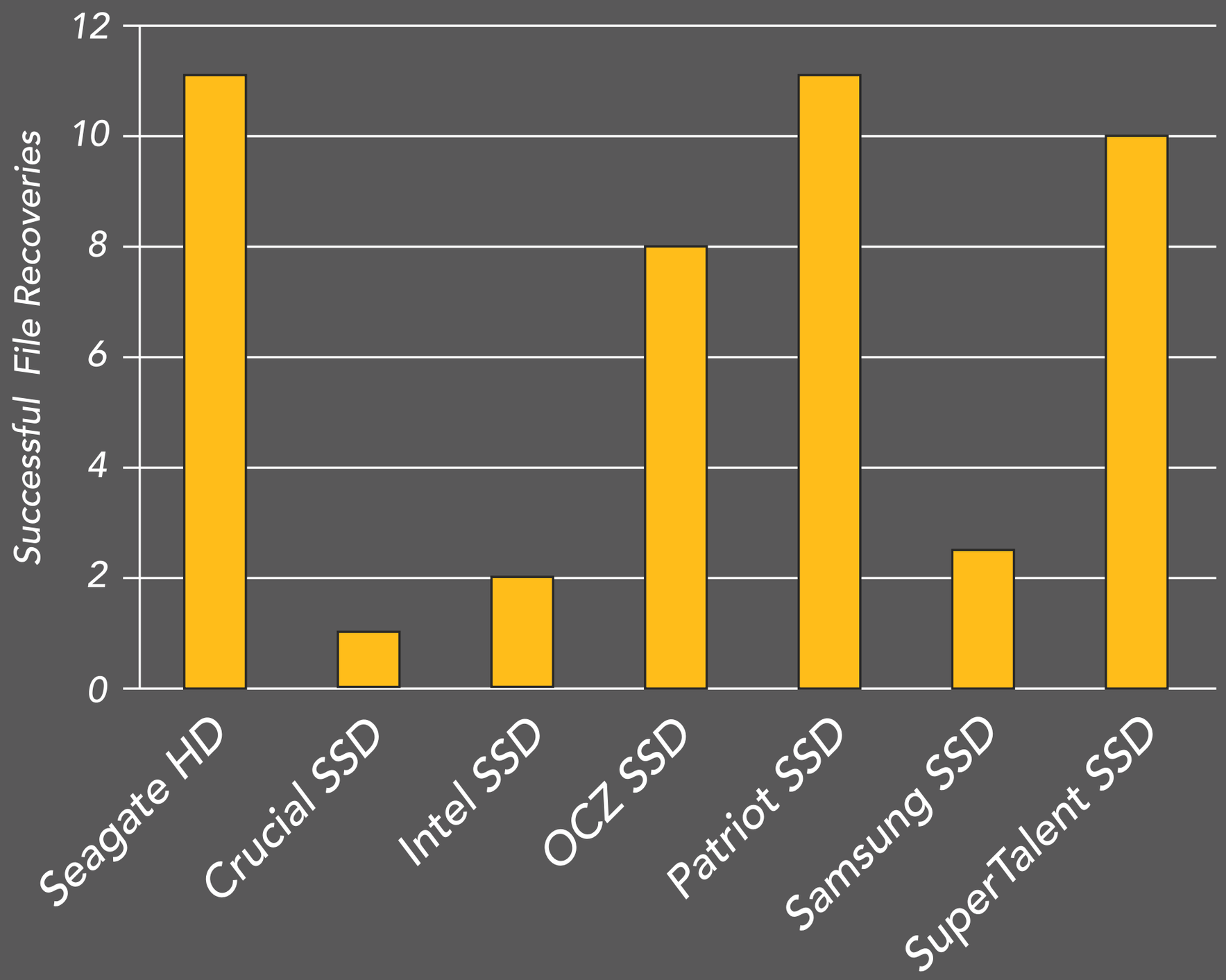
File deletion recoverability

fig 8



Quick format recoverability

fig 9



General observations

- Solid state drives cannot be considered to behave identically to a traditional hard drive from a forensics perspective
- Deleted file recoverability varies significantly
- Several factors can be used to gauge the likelihood of successful file recovery

Contributions

- This research may be referenced when attempting to recover a deleted file from an SSD to help understand the possibility for successful recovery
- Similar tests can be run on new drive models and/or different firmware revisions to determine likelihood of recoverability
- Impact of TRIM command on current forensics techniques is clearly demonstrated

Conclusions

- Forensics investigators must be acutely aware of drive differences when collecting evidence from these drives
- SSDs negatively impact the likelihood of deleted file recovery
- Forensics practices must change to adapt to these different behaviors

Future Work

Acknowledgements:

Dr. Yin Pan, RIT
Dr. Sumita Mishra, RIT
Prof. Bill Stackpole, RIT
Bill Mathews, Hurricane Labs

Questions?

Contact Info:

tom@hurricanelabs.com | @tomkopchak

hurricanelabs.com | @hurricanelabs