Magnetic Storage – Key Concepts

- Logical Block Addressing (LBA) maps physical sectors of the media to logical addresses for that media.
- A small pool of unallocated blocks is kept by the drive to replace bad sectors in the LBA map.
- Aside from bad blocks being replaced, a read will always return the same logical sector.
- Sectors can be written to many times, directly atop old data.
- Aside from being overwritten, there is no requirement to erase a sector completely before overwriting.
- Two cycles – Read and Write.
- In general, traditional magnetic hard drives are devices that read and write only as instructed to do so by a host operating system (OS).
- Aside from the servicing of read and write requests, magnetic hard drives also perform idle-time media scans and other simple tasks.
Generalized Data Access Sequence for HDDs

MAGNETIC HDD
Read/Write

User LBA Request

Device LBA Servicing Response

Host Controller
Device SATA Controller
Physical Media
Generalized Data Access Sequence for SSDs

SSD (NAND)

Read/Write

User LBA Request

Device LBA Servicing Response

Host Controller  Device SATA Controller  Flash Translation Layer  Physical Media
SSDs Have Flash Microcontrollers

SSD (NAND)

- User LBA Request
- Device LBA Servicing Response

<table>
<thead>
<tr>
<th>Flash Micro Controller</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Controller</td>
</tr>
<tr>
<td>Device SATA Controller</td>
</tr>
<tr>
<td>Flash Translation Layer</td>
</tr>
<tr>
<td>Physical Media</td>
</tr>
</tbody>
</table>
SSDs are Similar in Many Ways to HDDs

- Both use ATA commands to access data
- Both use SATA device interface specification
- Both use the same form factors (1.8”, 2.5”, 3.5”)
- Behave nearly identical from a user’s perspective, except for throughput and response time
SSDs are Different in Less Obvious Ways

- New medium creates new possibilities that lift old storage restrictions.
  - Less heat
  - Less power
  - No noise
  - More IOPS
  - Faster random access times
  - Impervious to shock
NAND Flash Storage – Technical Differences

• This new medium brings with it new considerations and problems that older storage solutions did not have.
  • Erase cycle
    • Flash Translation Layer (FTL)
      • Garbage Collection
      • OS-Assisted Garbage Collection (TRIM)
    • Over-Provisioning
    • Wear-Leveling
    • Write-Amplification
  • Hardware-Embedded RAID levels
  • Increased prevalence of hardware encryption
  • Cryptographic Wipe APIs
  • Evolving storage standards
  • Proprietary APIs
  • Huge problems for forensic investigators
It’s All About Performance

• The entire purpose of the Flash Translation Layer is to hide the erase cycle and minimize its impact on the device
  • Flash pages must be fully erased before they can be re-written to
  • Writing partial pages is wasteful
  • Costly operation in terms of time
    • Real-time erase-before-write is avoided at all costs
    • Avoiding real-time erase-before-write creates the existence of garbage collection algorithms
  • Costly operation in terms of wear and tear on the device media
    • Flash media has orders of magnitude shorter mean time between failures (MTBF) for a given allocation of storage than magnetic media
    • Erasing a page of memory causes a write cycle to be lost before the actual write can be performed. This is known as write amplification.
Flash Translation Layer is the Solution

- FTL employs clever algorithms to overcome all of NAND flash’s implementation shortcomings
  - Wear-leveling algorithms attempt to ensure no page is written twice, before every page has been written once.
  - Wear-leveling algorithms work hard to fully write to every last byte of a flash page before moving on to a new page of flash.
  - Flash translation layer is sometimes referred to as a flash filesystem. These flash filesystems implement many variations of FTL algorithms.
    - Page-based algorithms
      - Simple and Fast – creates mapping tables between LBA and flash pages
      - Not Efficient in terms of physical space (RAM and flash pages)
    - Block-based
      - Resembles a complex filesystem, such as a superblock-based UNIX filesystem
      - Efficient use of space at a cost of complexity and processing time
Flash Translation Layer Continued…

- Really clever FTLs are very fast, space efficient, perform garbage collection in non-invasive ways, and effectively reduce write amplification
  - Write amplification comes in many forms
    - Wear-leveling
    - Garbage collection
    - Random access writes
    - Secure erasure (sanitization)
  - De-duplication is an effective technique employed to reduce write-amplification.
  - Delayed writes reduce WA
  - Compression algorithms reduce WA. This is significant because it illustrates the lengths manufactures will go to in pursuit of reducing WA.
Forensic Problems with SSDs

- Imaging is prone to integrity problems
- Sanitized data could be lost completely, but maybe not…
- There is a large area of drive space, called over-provisioned space, that is inaccessible to traditional forensic imaging techniques.
  - Between 8% and 32% of the entire media space of the drive, depending on the manufacturer’s feature set, FTL performance, and error-correction algorithms
  - Deleted data will often end up in over-provisioned space, at least until the garbage collector decides to re-claim the pages.
Identifying SSD Hard Drives

• Learn to identify an SSD hard drive
  • Since they require different handling, it’s important to know what the device is
  • Product features and forensic problems vary per-device
  • Probably safest method of identification is to look up product literature (Google), based on the information reported by the operating system about the device. If you can gain physical access to examine the device without powering off the system that is better.
  • Live analysis is preferred, at least until the state of hardware and software encryption is assessed
  • If product nomenclature is unavailable, there are physical clues.
    • SSDs do not spin, create no noise, and exhibit no characteristics of angular momentum, such as resistance to a change in position.
    • Tools exist for every platform that can read the results of the ATA Identify command.
SSD Identification

ATA Identify Command

- Presence of ATA8-ACS2 command set (TRIM Specification)
  - Most new devices will support some variant of TRIM
  - Not all TRIM implementations follow the specification. Some are proprietary and will not be identifiable via the Identify command.

Other Options

- Any device supporting the TCG Opal command set is an immediate red flag. This means hardware encryption support and commonly that this is an SSD as well.
- Search engines are very helpful here. Try to find product literature.
Working with Forensic Imaging Challenges

- The response to the presence of SSD hardware will probably be based on the capabilities of a given forensics shop.
- The most complete method available today for recovery of a complete forensic image from NAND flash SSDs involves laboratory tools and techniques
  - Chip removal
  - Chip reading
  - Decoding FTL algorithms
  - Re-constructing LBA zones
  - Carving over-provisioned space and FTL metadata
    - Can actually retrieve deleted data in some instances
    - Can track file change history in some instances, something not directly possible with magnetic HDDs (a new forensic possibility)
Practical Recommendations

- For shops that do not have access to extensive laboratory resources, the case may dictate involving an outside lab.
- For cases that do not dictate the need for a full forensic image, there is a work-around for the problem of data integrity guarantees, but not for deleted data file recovery.
- Garbage collection can occur at any time with SSDs, moving and re-claiming blocks of data. This currently cannot be controlled.
  - Consider using a software imaging technique with a write-blocker, creating a dictionary of hashes on a granular basis, such as a per-sector. If the garbage collector runs, it won’t affect the image hash of the entire volume, only specific sectors.
    - DCFLDD
    - Encase / FTK Imager
  - Creating many smaller hashes may help with legal arguments about the data integrity if some hashes do not match. They may not match on data that is irrelevant to the case.
Areas of Research

- Improving the state of practice of existing laboratory techniques
  - Identifying more variations of FTL and working with them.
  - Identifying weaknesses in hardware encryption implementations
  - Process automation
- The possibility exists for reverse-engineering the FTL via the ATA command layer
  - This would be a big win, if proven techniques could be discovered for accessing physical flash pages via only software.
  - Research in this area is ongoing
- Custom firmware / special purpose firmware could completely eradicate the forensic problems
  - Just remove the garbage collector
  - Make all write commands fail
  - Implement a new set of ATA commands to allow carving of the overprovisioned space
Contact Information

**Presenter / Point of Contact**
Considerations for Forensic Acquisition of Flash-Based Devices
CERT - DIID
Telephone: +1 412-268-3405
Email: djshepard@cert.org

**U.S. Mail**
Software Engineering Institute
Customer Relations
4500 Fifth Avenue
Pittsburgh, PA 15213-2612
USA

**Web**
www.cert.org/forensics
www.sei.cmu.edu
www.sei.cmu.edu/contact.cfm

**Customer Relations**
Email: info@sei.cmu.edu
Telephone: +1 412-268-5800
SEI Phone: +1 412-268-5800
SEI Fax: +1 412-268-6257