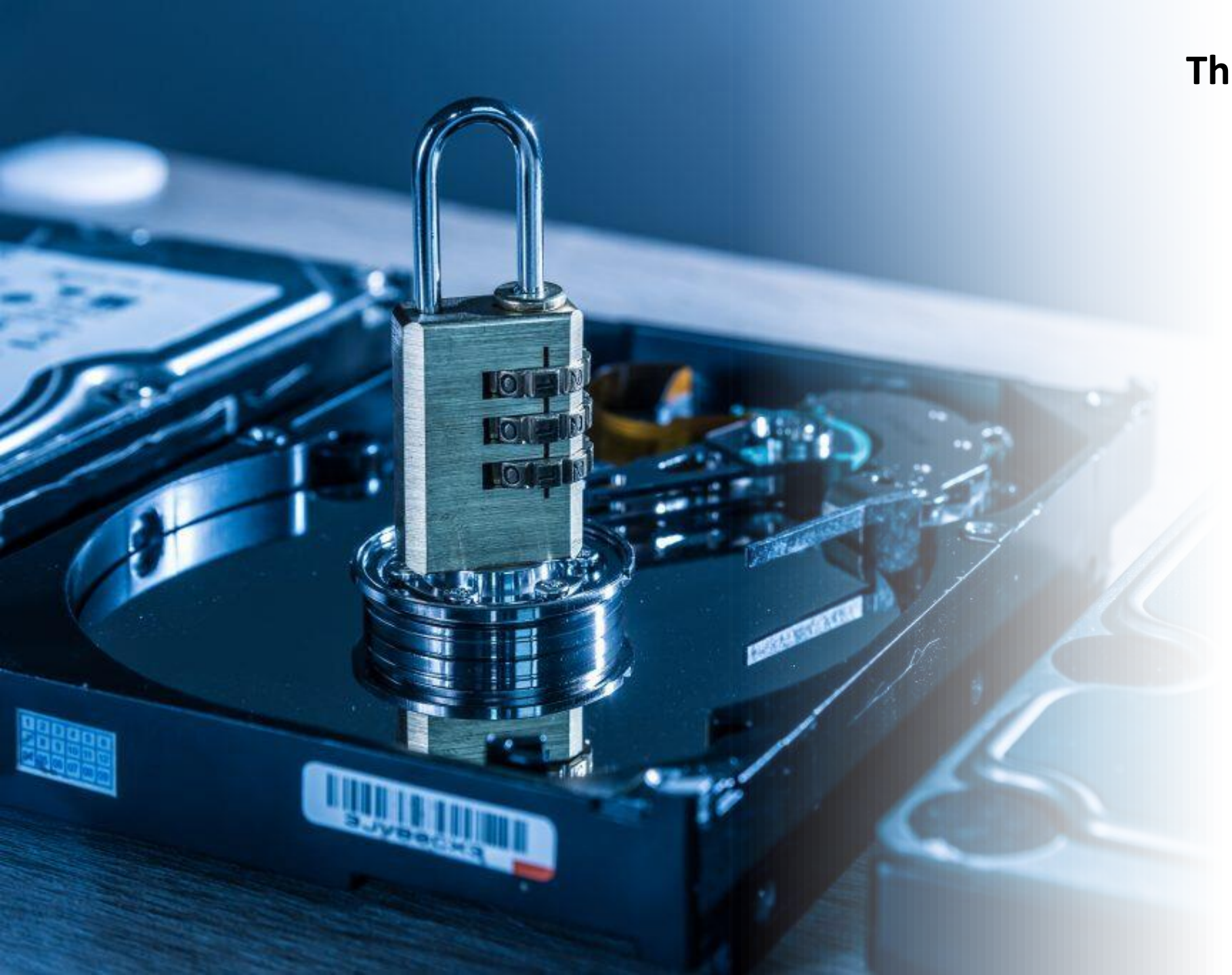

The Remapped / Reallocated Sector Conundrum

Why are remapped sectors important???

Dr. Philip Turner
BSc (Hons) PhD FBCS CITP CDRP
ADISA – Director of Technology
July 2023

Storage Media Reliability

- We depend on storage media to be reliable – we often take it for granted that it will be!
- We expect to be able to be able to retrieve exactly the information previously written to it without error.
- Why does storage media fail?
  - Damage
  - Power Supply Issues
  - Temperature variance
  - Electrostatic effects
  - Magnetic substrate degradation
  - Solid state write cycle endurance exceeded

Storage Media Reliability (2)

- Firmware Issues:
  - Bugs
  - F/W Corruption
  - Reallocated sector pool depleted

- Hardware Issues
  - Connector Damage
  - Head Crash
  - Controller Board Failure
  - Motor failure – bearing seizure / spindle sheered
  - Stiction – head stuck to platters
  - Solder oxidisation
  - Dirty Contacts

Reliability Mechanisms – Media Defect Management

- Permanent Defect List (P-List) – created and populated at drive manufacture
- Grown Defect List' (G-List) – populated during the working life of the device
- Self-Monitoring, Analysis and Reporting Technology (SMART) – used to be able to report the 'health' of the device:
  - Logs used to help predict device failure
  - Number of hours of operation
  - Amount of data transferred to/from the device
  - Operating temperature
  - Records the number of remapped / reallocated sectors

SMART - Logs / Attributes

- Not so SMART ! - user has to be proactive in monitoring some of the attributes that the drive maintains in order to mitigate the potential of drive failure and prevent data loss

- SMART Attributes

Attribute No.	Description
1	Read Error Rate
4	Start/Stop Count
5	Reallocated Sectors Count
9	Power-On Hours Count
12	Power Cycle Count
13	Soft Read Error Rate
173	Wear Leveller Worst Case Erase Count
176	Erase Fail Count
177	Wear Leveling Count
190	Temperature
191	G-Sense Errors
195	Hardware ECC Recovered
196	Reallocation Events
197	Current Pending Sectors
200	Write Error Rate
201	Soft Read Errors
233	Media Wearout Indicator
240	Head Flying Hours
241	Total LBAs Written
242	Total LBAs Read

Reallocated / Remapped Sectors – Examining the G-List

Western Digital WD64AA – 5 defects (Attrib: 5), vendor specific command code 0x61 and 0x21 (Read Sector w/out retry)

Cylinder	Head	Wedge	BFI	Length
0	0	11	801	1300
0	0	11	1311	1810
0	0	16	2850	2968
0	0	17	85	495
14945	0	5	95	993

Maxtor 4G160J8 – 179 defects (Attrib: 5), vendor specific command codes 0xC0 and 0xC1

NN	Init. LBA	Fin. LBA	Num	RLBA : Candidate
1	167088146	167088146	1	320647221 : false
2	167088147	167088147	1	320647222 : false
3	167088148	167088148	1	320647223 : false
4	167088149	167088149	1	320647224 : false
5	167088150	167088150	1	320647225 : false

HGST HUS724020ALE640 - 473 defects (Attrib: 5), in G-List, but actual number of defective sectors >9400

NN	Init. LBA	Fin. LBA	Num	Kind : KindNm	RemapInx
1	139667824	139667839	16	5 : Grn	320
2	139667872	139667919	48	5 : Grn	336
3	139667976	139667983	8	5 : Grn	384
4	139668320	139668335	16	5 : Grn	392
5	139668400	139668407	8	5 : Grn	408

Forensically reading the G-List

- In the absence of standardised commands to read remapped sectors the following process is suggested:

1) Always create and verify a full forensic image of the device (using established forensic tools and procedures) before any additional tools are used to examine the device.
2) Determine if the device reports remapped sectors by examining the SMART attributes reported by the device.
3) If remapped sectors are reported, read and backup a copy of the G-List module using specialist data recovery software.
4) Ascertain the number of remapped sectors that the device actually contains. This is required because the SMART value may only indicate the number of entries in the G-List table not the actual number of remapped sectors which could be much more.
5) The recovered G-List also needs to be examined to determine if it provides the original LBA of the remapped sector. Only if it does can you easily determine which specific sector numbers are remapped.
6) Clear the G-List using specialist data recovery software. This has the effect of mapping back in to the standard user addressable LBA space the 'faulty' sectors. Optionally clear the SMART log data, this resets all the SMART log counts.
7) Read the LBA of the sector numbers identified in the original G-List using read commands that ignore ECC and other data integrity validation checking.
8) The returned data should be the previous contents of the sector and may be out of context with the contents captured in the original forensic image.
9) Restore the original G-List module (saved in step 3) to return the drive to its original state.

Forensic / Data Sanitisation Issues

- Remapped Sectors are important because they can contain user data that is not available through the currently mapped user addressable space.
- Industry standard forensic tools don’t report SMART information or Remapped Sector count – so how do you know if you are missing anything!
- Few Data Sanitisation tools report SMART information
- No standardised way to read the remapped sectors (G-List) – use of vendor specific commands

Next Steps…

- Get all forensic and data sanitisation vendors to report if disks have remapped sectors… we don't know the scale of the problem is until we can routinely determine if a device has remapped sectors!
- More research on reading remapped sectors – discovery of vendor specific commands…
- … better still, get device manufacturers to publish how to do it or release their own utilities.
- … even better …make this issue disappear (in time)… influence the T10 / T13 standards committees to implement standard commands that permit remapped sectors to be read.

Questions / Collaboration

Phil Turner

ADISA Research Centre

DFRWS@adisa.global

www.adisarc.com