True Data Disaster Recovery

Matthew Kinderwater
iCube Development (Calgary) Ltd.
True Data Disaster Recovery

❖ Who We Are:

❖ Provide data recovery / data redundancy / disaster plan consulting services worldwide.
❖ Operate one of the largest data recovery labs in Western Canada.
❖ Recipient of multiple data recovery awards.
❖ Published in mainstream media, featured educator for eForensics magazine, and received Global News coverage.
True Data Disaster Recovery

Presentation Overview:

- Review of device / array failures.
- Data Labs vs. “Users” / Administrators.
- Real world case study and how labs work.
- Avoiding / preventing data recovery situations.
- Data recovery facts and fiction.
- How to deal with disaster.
Failures, Signs, and Symptoms:

DEVICE & ARRAY FAILURES
True Data Disaster Recovery

- **Common causes of Single Disk Failures:**
  - 40% Bad Sectors (Mechanical & Firmware):
    - Common Cause(s): Heat and age.
  - 20% Firmware:
    - Common Cause(s): Error recording, sector reallocation, performance tweaks, garbage collection (SSD), and inaccurate translation data.
Common causes of Single Disk Failures:

- **20% Mechanical:**
  - Common Cause(s): Heat, physical impact and bad sector self-recovery attempts ("head-burn").

- **10% Electrical:**
  - Common Cause(s): PSU function and age.

- **10% Logical:**
  - Common Cause(s): User and / or software errors.
True Data Disaster Recovery

Common RAID Failures:

- Dependent on a disk failure (previous slide).
- Another drive member in the array fails during a rebuild process (common in RAID 5/50).
- RAID controller failures (firmware & cache).
- Power failures (battery backups).
- Operating system error(s) (open handles).
- User error(s) (accidental deletion).
True Data Disaster Recovery

- **Common Mechanical Failures:**
  - Excessive amount of bad sectors (freezing).
  - Non-functional read / write head(s) (clicking).
  - Parking Ramp ("Sticktion") (buzzing drive).
  - Spindle Failure (buzzing drive).
  - Bearing Failure (buzzing drive).
  - Surface Damage (clicking and scratching).
True Data Disaster Recovery

- **Mechanical Assessment:**
  - Includes the reading and writing heads, actuator arm, and the platters.
    - Visual Inspection / Specification Assessment
    - Digital High Resolution Microscope
    - Fog (Clean Box) Tests
      - Ring Formation Analysis (RFA)
    - Laser Diffraction Tests
      - Shows the quantity of pitting (surface damage)
      - Shows the quantity of scratches (surface damage)
Mechanical Failure: (Head Failure)

Client states the drive is now making a clicking noise.
Mechanical Failure: (Head Crash)

Client states the drive is now making a clicking noise.
Mechanical Failure: (Parking Ramp)

Cause: This drive was dropped by the client.
Mechanical Failure: (Bearing Failure)

Cause: This drive was dropped by the client.
Mechanical Failure: (Head Crash)

Cause: Spindle Seizure, suspect physical impact
Mechanical Failure: (Fire & Water)

Massive amounts of mechanical and electrical failures.
Mechanical Failure: (Fire & Water)

Drive involved in a fire (heat and water damage).
Drive has been prepped for DP after 4 hours of cleaning.
Mechanical Repair:
- Averages 6 to 12 hours to complete.
  - Availability of donor parts.
  - Quantity and quality of heads and platters.
  - Drive design (parking ramp vs. landing zone).
  - Storage capacity of the hard drive.
  - Location, amount, and type of surface damage.
  - Adaptive parameters.
  - Previous recovery attempts.
Mechanical Donors:

- Drives include numerous sub-models.
- Each manufacturer site (production factory) typically uses slightly different parts.
- Can be very expensive depending on the brand, size, and rarity of the hard drive.
- Often more than a single donor is required to complete a recovery.
Mechanical Repair: (Head Assembly)

This drive uses a parking zone (no parking ramp).
True Data Disaster Recovery

- **Common Electrical Failures:**
  - TVS Diode(s)
  - Motor IC and MCU (Processor) Failures
  - PreAMP Failure
  - USB Bridge Controllers

- **Hardware Encryption:**
  - Examples: Initio, Symwave, JMicron, ASMedia

- ROM Corruption
Electrical Failure: (MCU / Processor)

Note center of chip is slightly darker.
Electrical Failure: (Pre-Amplifier Chip)

Note chip bubbles on the bottom right corner.
Required a mechanical donor to facilitate recovery.
True Data Disaster Recovery

- **Electrical Assessment:**
  - Includes the external PCB and the internal head stack assembly components.
  - Can be performed even if a mechanical failure is present.
  - Thermal camera imaging.
  - Isolated circuit / dependencies circuit test.
  - ROM dump.
True Data Disaster Recovery

- **Electrical Repair:**
  - Averages 1 to 2 hours to complete.
    - May involve a mechanical repair.
    - Availability of donor parts.
    - Previous recovery attempts.
Common Firmware Failures:

- Extremely Brand & Model Specific
- SMART Logging Full
- Pending / Reallocation Mapping Full
  - P-List, G-List, and T-List
- Translation Failures
  - Physical to Digital geometric conversion.
- Corrupt / Un readable Modules
True Data Disaster Recovery

- **Firmware Assessment:**
  - Ability to read all copies of modules.
  - Comparison of unique module copies (SA-A, SA-B, SA-C) and those from a donor.
  - Firmware response (read and process) time.
  - Validity of module content.
Firmware Failure

Brand: Seagate
Problem: Pending Sector Reallocation
Cause: Excessive Bad Sectors / Weak Heads
Firmware Failure

Brand: Western Digital
Problem: Corrupt Modules
Cause: Bad Sector (Module 11)
True Data Disaster Recovery

Firmware Repair:
- Averages 1 to 4 hours to complete.
  - May require a working donor drive (hot swap).
  - Commonly requires the use of donor firmware.
  - Complicated by interface type and brand.
  - Requires proper operation of both electrical and mechanical components.
True Data Disaster Recovery

Unique Drive Attributes:

- Commonly known as Track 0, System Area, and sometimes firmware.
- Defect lists are completely unique to each drive in the production run.
- Adaptive parameters are specific to a drive's operational conditions.
Logical Assessment:

- Shares a close relationship with any Pre-Assessment Variables.
- Includes manual (offline) assembly of RAID.
- Identification of the partition and file systems with the quality of file index elements.
True Data Disaster Recovery

Logical Repair:

- Impossible to estimate completion time.
  - Heavily dependent on the Pre-Recovery Assessment Variables.
  - Complicated by degraded RAID volumes and read / write activities.
  - Often results in the same file being recovered numerous times (quality of data varies).
- Nameless recovery based on file signatures.
  - Used when file and folder asset data is corrupted.
Logical (File System) Inclusions:

- Priority is placed on the recovery of MFS (PC), Catalog (Mac), or Superblocks (Linux).
- Most file systems contain a backup of the file and folder names (alternate locations).
- Disregard security (ACL) NTFS or Metadata (Mac) extended attributes.
- Closed source file systems complicate the recovery process.
Limitations of what you can do yourself:

DATA LABS VS. USERS
True Data Disaster Recovery

Data Labs vs. “Users” / Administrators:

- Use specialized hardware and software to assemble an array without the use of a RAID controller.
- Use DE, DD, ID, and supporting evidence to make proper decisions regarding a recovery.
- Attempt to reduce and / or remove variables.
- Always assume a worst case scenario.
- Never work from source media.
True Data Disaster Recovery

“Users” / Administrators vs. Data Labs:

- Are limited by readily available hardware and software solutions.
- Typically unable to use DE, DD, and ID to make proper recovery decisions.
- Often create more variables.
- Attempt to solve symptoms not causes.
- Typically change / manipulate the source medium.
How we recover data:

REAL WORK CASE EXAMPLE
True Data Disaster Recovery

Real Case Example:

- Client has RAID 5 volume with x4 300GB 320UW SCSI HDD’s.
- Single drive will not power on.
- RAID volume was offline, clients attempts to rebuild the array to a new drive had failed.
- Client physically removed array members from the server and did not record / replace the drives back in the correct order.
True Data Disaster Recovery

Drive Evaluation Process (DE):

- **Mechanical:**
  - A moving part is not working correctly.

- **Electrical:**
  - Power, electrical shorts, integrated circuits.

- **Firmware:**
  - Manufacturer programming not fully functional.

- **Logical:**
  - Partition and file system errors.
Drive Duplication Process (DP):

- Combination of hardware and software technologies.
- Software is typically used on healthy drives.
- Specialized hardware is used to obtain partial images from drives which contain bad sectors.
- Target 1:1 images are stored on a high capacity, high speed storage array.
Image Identification Process (ID):

- Determine offsets (reserved area).
- Search for partition and file system signatures.
- Localize and read back RAID controller Disk Control Blocks (DCB’s).
- Allows the lab to confirm all members are present, disk order, and RAID type.
True Data Disaster Recovery

ID Process:

- Typically contains physical drive identification assets.
- Includes other RAID indicators such as disk order, stripe size, and parity rotation.

Eg: DELL (PERC) RAID 1:

Sector 312450847

<table>
<thead>
<tr>
<th>Offset</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>253F3E3E00</td>
<td>31 90 71 57 1E AF 1.qW.ŽoDéll</td>
</tr>
<tr>
<td>253F3E3E10</td>
<td>10 00 00 54 10 28 ...T.(.....$j...</td>
</tr>
<tr>
<td>253F3E3E20</td>
<td>30 31 2E 30 30 2E 01.00.00......“V</td>
</tr>
<tr>
<td>253F3E3E30</td>
<td>00 00 01 FF FF FF ...YYYYYYYYYYYY</td>
</tr>
<tr>
<td>253F3E3E40</td>
<td>FF FF FF FF FF FF YYYYYYYYYYYYY</td>
</tr>
<tr>
<td>253F3E3E50</td>
<td>FF FF FF FF FF FF YYYYYYYYYYYYY</td>
</tr>
<tr>
<td>253F3E3E60</td>
<td>00 00 00 00 12 9F .....ÝÝ.yyYYYYy</td>
</tr>
<tr>
<td>253F3E3E70</td>
<td>01 FF FF FF 00 00 .yy.........Ýb.</td>
</tr>
<tr>
<td>253F3E3E80</td>
<td>00 0F 00 0F 00 01 ..........YYYYy</td>
</tr>
<tr>
<td>253F3E3E90</td>
<td>FF FF FF FF FF FF YYYYYYYYYYYYY</td>
</tr>
<tr>
<td>253F3E3EA0</td>
<td>FF FF FF FF FF FF YYYYYYYYYYYYY</td>
</tr>
<tr>
<td>253F3E3EB0</td>
<td>FF FF FF FF FF FF YYYYYYYYYYYYY</td>
</tr>
</tbody>
</table>

Sector 312450843

<table>
<thead>
<tr>
<th>Offset</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>253F3E4000</td>
<td>22 22 22 22 DA AF &quot;&quot;&quot;&quot;O.„.....YYYY</td>
</tr>
<tr>
<td>253F3E4010</td>
<td>FF FF FF FF FF FF YYYYYYYYYYYYY</td>
</tr>
<tr>
<td>253F3E4020</td>
<td>FF FF FF FF FF FF YYYYYYYYYYYYY</td>
</tr>
<tr>
<td>253F3E4030</td>
<td>FF FF FF FF FF FF YYYYYYYYYYYYY</td>
</tr>
<tr>
<td>253F3E4040</td>
<td>41 54 41 20 20 20 ATA WD-WCAP</td>
</tr>
<tr>
<td>253F3E4050</td>
<td>30 32 33 31 31 35 02311508U.е....</td>
</tr>
<tr>
<td>253F3E4060</td>
<td>00 00 00 00 12 9E .....ž _ P.‘¥Nic.</td>
</tr>
<tr>
<td>253F3E4070</td>
<td>FF FF FF FF FF FF YYYYYYYYYYYYY</td>
</tr>
<tr>
<td>253F3E4080</td>
<td>41 54 41 20 20 20 ATA WD-WCAP</td>
</tr>
<tr>
<td>253F3E4090</td>
<td>30 32 33 30 31 33 02301378.hi.....</td>
</tr>
<tr>
<td>253F3E40A0</td>
<td>00 00 00 00 12 9E .....ž _ P.‘¥Nic.</td>
</tr>
<tr>
<td>253F3E40B0</td>
<td>FF FF FF FF FF FF YYYYYYYYYYYYY</td>
</tr>
</tbody>
</table>
True Data Disaster Recovery

- **Pre-Recovery Evidence Assessment:**
  - Only relates to information supported by the DE, DD, and ID processes.
  - This assessment determines 80% of what actions are needed and will be taken by the data recovery lab.
Pre-Recovery Variables Assessment:

- Involves information provided by the client.
- Includes any post-failure recovery attempts.
- Is often inaccurate and lacks important details which delays or complicates recovery.
- Is the greatest cost influencer.
- Directly affects the outcome of data recovery.
True Data Disaster Recovery

**Major Influential Variables:**

- A manual or automated rebuild attempt was performed and has failed / did not complete.
- Post-failure read and write operations have been performed.
- Drive order has been compromised or conflicts with DCB information.
- File system type.
Case Example Summary:

- A drive had an electrical failure.
- The array rebuild failed due to bad sectors on existing RAID member.
- Data recovery services required on the electrically failed drive.
- Manual RAID assembly written to a new storage array mounted in ESXi to view datastore (closed file system).
Keeping your data safe:

DATA RECOVERY
PREVENTION
True Data Disaster Recovery

Why the need for data recovery?

- Backups are missing, never tested, out of date, or produce corrupt data.
- Backup restoration time exceeds recovery time (often seen with cloud backup users).
- Hardware and storage capacity limitations.
- Limited IT resources (dishonesty, outsourcing, inventory management, and inadequate maintenance).
True Data Disaster Recovery

Understanding Data Endurance:

- Avoid the use of large 2TB + drives in a RAID array. More platters = more heads and therefore increases chance of disk failures.
- More smaller drives are better than less larger drives (both performance and redundancy).
- Consider SAS vs. SATA vs. SSD based on the application(s) and speed requirements.
- Always have both a “hot” and “cold” spare.
Recommended IT Policies:

- Choose correct hardware.
- Proper controller configuration.
- External audits.
- Written schedule.
- Assign IT personal liability.
- Test backups (virtualization).
- Standby equipment (hardware).
Choosing Correct Hardware:

- The most critical decision:
  - Avoid green (energy efficient) hard drives for any backup or high-use data storage functions.
  - Understand Enterprise vs. Desktop storage.
  - More drives vs. high density drives preferred.
  - Ensure backplane fully supports SPGIO.
  - RAID controller should support hardware polling and SMART schedule testing using own NIC.
  - Use temperature monitors in your server room.
Proper Rack Layout Concepts:

- Organize according to heat generation:
  - Heat generating devices should be at the top of your rack (UPS, Switch & Router exempt).
  - If possible use 1U spacers between servers and 2U spacers between SAN or NAS devices.
  - Cable management is critical to ensure proper air intake, circulation, and ventilation.
  - Equipment accessible for media replacement with clear view of all LED indicator lights.
Proper Controller Configuration:

- Performance is not everything:
  - Choose the best RAID type which suits the application(s). Challenge manufacturer defaults.
  - Always test new equipment by failing a drive and then document the replacement / rebuild process.
  - Use (local) ISP SMTP server and e-mail to text message address for any / all alerting functions.
  - Always utilize both a hot and cold spare.
True Data Disaster Recovery

External Audits:

- Provides management insight:
  - Determines what is really backed up.
  - Includes virtualization of your backup data.
  - Determine fragility and / or condition of the backup.
  - Calculates an accurate restoration time.
  - Introduces data disaster restoration practices and optimizes recovery workflow.
  - Adds security and privacy controls.
Written Schedule:

- Includes an offline copy of the following:
  - Initial purchase, replacement, and warranty expiration dates.
  - Drive manufacturer, model, serial number, and member assignment(s).
  - Last SMART (or RAID polling) test date.
  - RAID controller, array type, and configuration.
IT Liability:

- Includes an offline copy of the following:
  - Initial purchase, replacement, and warranty expiration dates (both server and drives).
  - Drive manufacturer, model, serial number, and member assignment(s).
  - Last SMART (or RAID polling) test date.
  - RAID controller, array type(s), and configuration(s).
  - Ensure accuracy by manager or third party.
What’s right and what’s wrong:

DATA RECOVERY
FACTS AND FICTION
True Data Disaster Recovery

Data Recovery Facts (Accreditations):

- The data recovery industry does not have international standards or a governing body (despite any association claims).
- Data recovery professionals are self-taught.
- Data recovery is the reverse engineering of what the manufacturer doesn’t want you to know. Real world experience is everything.
True Data Disaster Recovery

Data Recovery Facts (Yearly Costs):
- SATA Hardware Imager: $5,000 - $10,000
- SA / Firmware Programmer: $10,000
- Storage Array: $50,000
- Clean Room / Clean Box: $5,000 - $35,000
- Insurance: $25,000+
- Research & Development: $50,000+
- Staff (individual) $125,000+
Data Recovery Facts (Summary):

- There are only 3 lab recognized providers of data recovery hardware and software.
- Successful data recovery labs develop their own procedures and tools.
- New hardware requires lab to continuously purchase new equipment.
- Data recovery is expensive.
Data Recovery Fiction:

- Freezing a drive may have worked for older, lower density hard drives. It will not work for newer drives / causes data loss.
- Hitting or knocking a drive never works.
- Once data is overwritten it’s not recoverable (regardless of what the TV show CSI tells us).
- Clean boxes vs. clean rooms.
- Wearing a lab coat make us look smarter.
DEALING WITH A DATA RECOVERY SITUATION

Know your options before a lab is involved:
Dealing with Disaster:

- Immediately reduce and/or remove any read and write operations.
- Write down what the last execution(s) were.
- Consult your backup systems to determine last backup date/time.
- Immediately establish a working data recovery budget before you call a lab.
True Data Disaster Recovery

Choosing a Data Recovery Company:

- Ensure they do not outsource. Do they ship to another lab (referral)? Or perform the actual recovery at their office?
- Inquire about success rates (by model number) and the time needed to evaluate the storage device. Group or individual?
- Insist on a no data, no charge policy.
- Research industry reputation and history.
Thanks, and enjoy the conference!

MORE INFORMATION:  
WWW.ICUBEDEV.COM