Hi Tech™ Data Group
Recover . Restore

EAST AFRICA®
HI-TECH SOLUTIONS
Enabling Business Continuity

CASE STUDY & PORTFOLIO

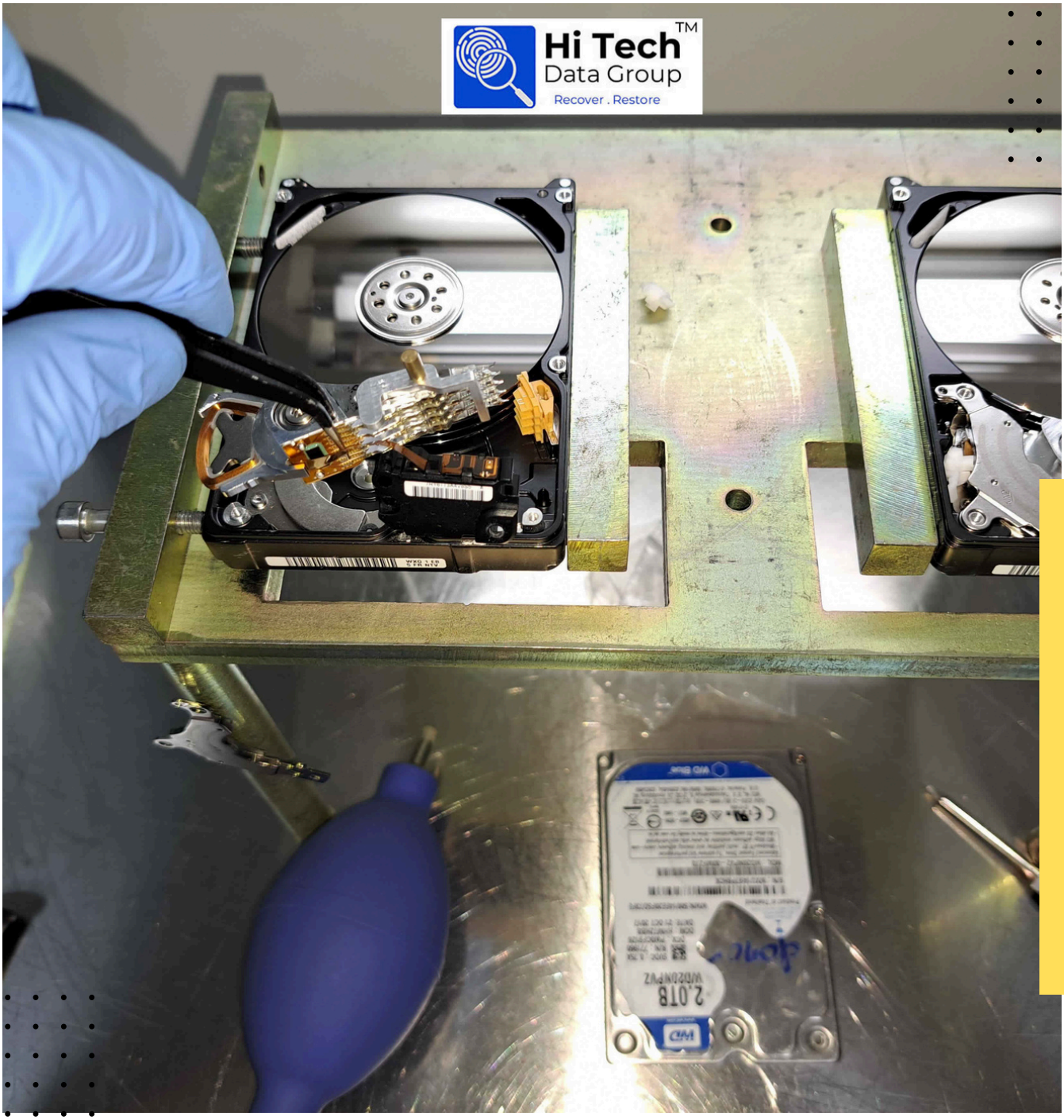


TABLE OF CONTENT

CASE 1 – SAS DRIVES: DELL SERVER RAID FAILURE:

Hi Tech Data Group successfully recovered data from a failed dell server under raid.

- **Type of Server:** Dell PowerEdge R740
- **RAID Configuration:** RAID 5 with 4 SAS Drive
- **Issue:** RAID configuration failure on a corporate server resulting in data inaccessibility.
- **Approach:** Thorough analysis of RAID array integrity, followed by meticulous raid reconstruction imaging and data extraction.
- **Result:** Successful restoration of critical business data with minimal downtime, ensuring business continuity.

CASE 2 – HP RAID SERVER CORRUPTION:

Hi Tech Data Group successfully recovered data from a corrupted HP Server under Raid.

- **Type of Server:** HP ProLiant
- **RAID Configuration:** RAID 0 with 5 drives
- **Issue:** Server corruption due to hardware malfunction, leading to data loss.
- **Approach:** Utilization of advanced recovery tools and techniques such successful reconstruction of custom file system to recover data from corrupted server drives.
- **Result:** Full recovery of lost data, including critical business documents and customer records, enabling seamless operations.

CASE 3 – SEAGATE NAS STORAGE FAILURE:

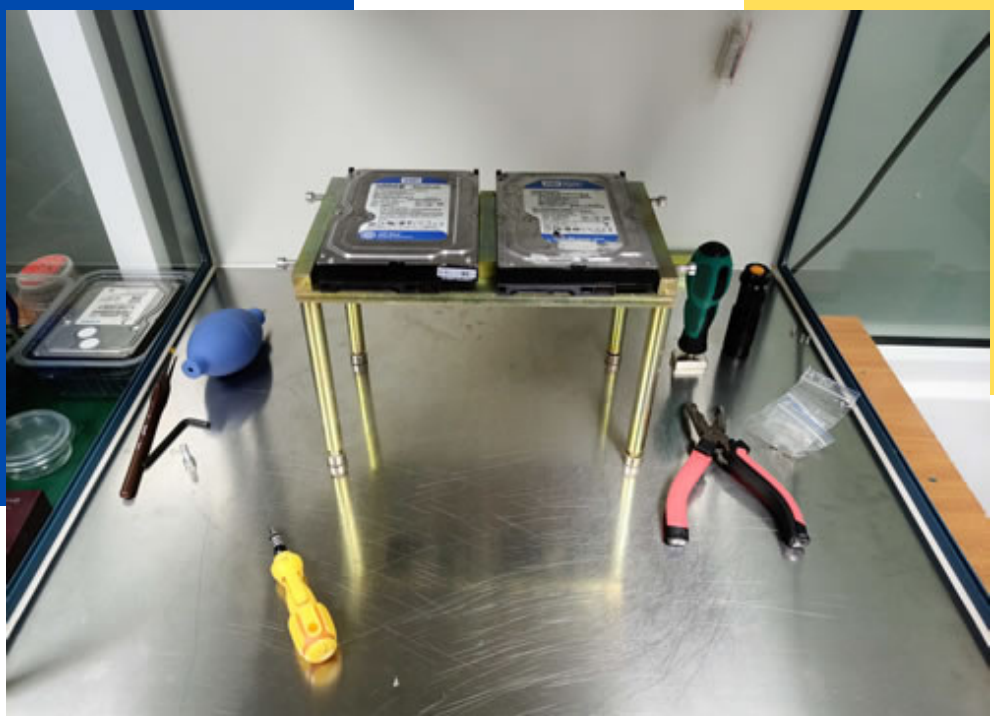
Hi Tech Data Group successfully recovered data from a Seagate NAS storage after failure.

- **NAS Model:** Seagate Business Nas
- **Number of Drives:** 4-drive RAID 5 configuration
- **Issue:** Failure of NAS storage system causing loss of multimedia files and project data.
- **Approach:** Comprehensive assessment of NAS storage components, followed by targeted data recovery procedures which include raid array rebuilding and data extraction.
- **Result:** Successful retrieval of multimedia files and project data, ensuring continuity in client operations and project delivery.

CASE 4 – SEAGATE PHYSICAL HEAD SWAP:

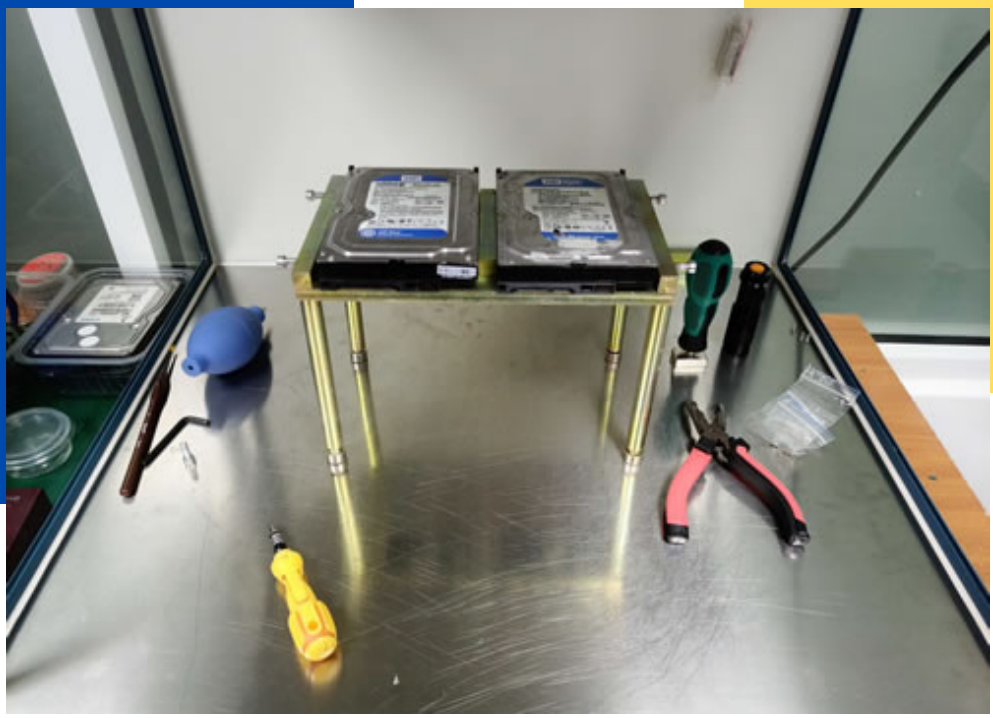
Hi Tech Data Group successfully recovered data from a Seagate hard drive producing clicking sounds.

- **Hard Drive Model:** Seagate 4TB
- **Cause of Damage:** Physical head crash
- **Issue:** Physical head damage in HDD resulting in data inaccessibility.
- **Approach:** Looking for a matching donor; whereby a matching donor is found. Delicate head swap procedure to restore data accessibility while ensuring data integrity.
- **Result:** Successful recovery of data from the damaged HDD, preserving data integrity and preventing further data loss.



CASE 5 – WESTERN DIGITAL HEAD REPLACEMENT: WITH COMPLEX FIRMWARE ISSUES

- **Hard disk Type:** Western Digital 500GB HDD
- **Hard Drive Model:** Western Digital WD
- **Issue:** Head failure in HDD causing data loss and disk inaccessibility.
- **Approach:** Looking for a matching donor; whereby a matching donor is found Precision head replacement technique to restore HDD functionality and Meticulous Firmware repair procedure e.g rebuilding of module 190
- **Result:** Complete recovery of data from the faulty HDD, safeguarding critical business information and preventing potential revenue loss.



CASE 6 – WD FIRMWARE CORRUPTION:

- **Hard Drive Model:** Western Digital 4 TB WD
- **Issue:** Firmware corruption in the storage drive leading to data loss.
- **Approach:** Firmware repair and recovery procedures to regain access to the inaccessible data.
- **Result:** Successful restoration of data from the corrupted drive, mitigating data loss risks and ensuring data availability.

CASE 7: SSD DATA RECOVERY – FIRMWARE DAMAGE

- **Hard Drive Model:** Disk Type: Solid State Drive – SSD
- **Issue:** SSD could not be accessed.
- **Approach:** We diagnosed the SSD and found out that it has a firmware damage. We repaired the firmware with our specialized tools and then imaged the entire disk for data extraction.
- **Results:** Family images and videos were successfully recovered.

CASE 8: HDD SUBMERGED IN WATER AFTER FLOODS

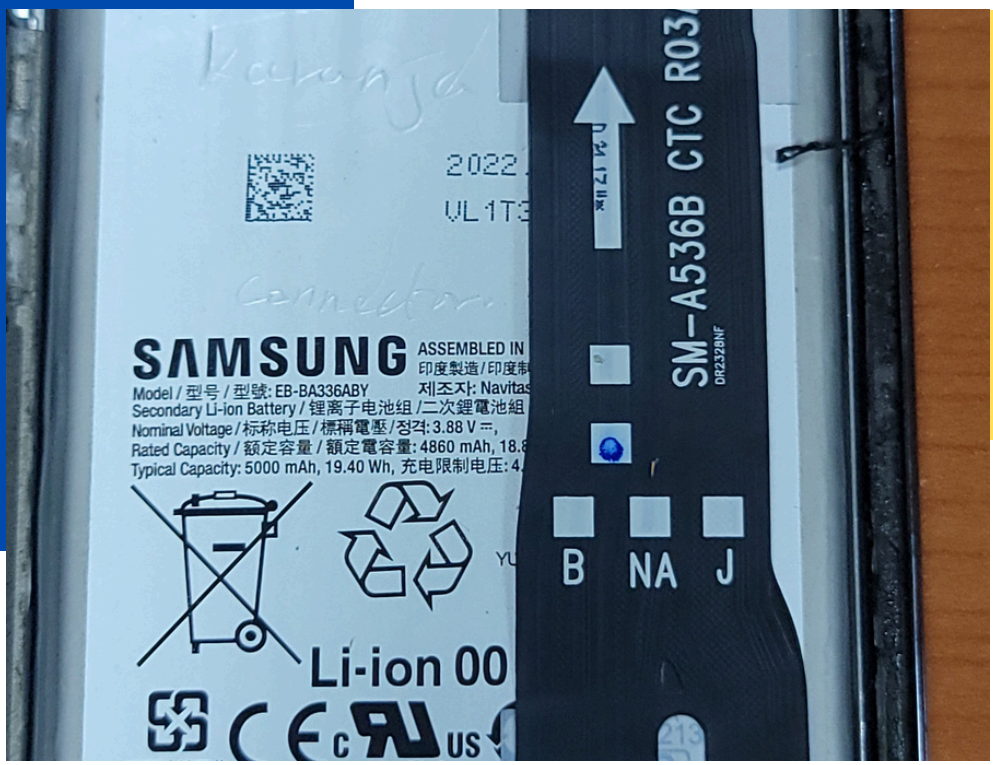
- **Disk Type:** Western Digital HDD
- **Issue:** Hard drive submerged in water after the recent flooding in Nairobi.
- **Approach:** We were able to repair the PCB, fix firmware issues, image the disk & extract data
- **Results:** All data was successfully recovered.

CASE 9 – TOSHIBA HDD BAD SECTOR RECOVERY:

- **Disk Type:** Toshiba 2.5″ HDD
- **Issue:** Bad sectors on the storage drive causing data read errors and data loss
- **Approach:** Advanced bad sector recovery techniques to retrieve data from affected areas. This includes meticulous firmware exploration of valid data sections
- **Result:** Efficient recovery of data from the drive with bad sectors, preserving data integrity and preventing further data loss.

CASE 10 – WD MYCLOUD NAS STORAGE:

- **NAS Model:** WD MYCLOUD HOME DUOS
- **Number of Drives:** 2-drives RAID 1 configuration
- **Issue:** NAS RAID array failure leading to the loss of financial records and client databases.
- **Approach:** RAID array reconstruction and meticulous recovery of financial and client data.
- **Result:** Restoration of critical financial records and client databases, facilitating seamless business operations and client services.



CASE STUDY 1: MOBILE FORENSICS AUDIT – EVIDENCE TAMPERING UNCOVERED

- **Objective:** To determine evidence tampering in a mobile device related to an ongoing investigation.
- **Process:**
  1. Conducted a comprehensive forensic audit on Mobile device
  2. Utilized advanced tools for data extraction, timeline analysis, and deleted data recovery.
- **Findings:**
  1. Clear evidence of tampering detected, including altered timestamps and deleted data.
  2. Recovery of intentionally deleted communication threads and manipulation of metadata and GPS data.
- **Conclusion: Hi Tech Data Group** successfully uncovered evidence tampering, highlighting the critical role of Digital Forensics Services in maintaining investigation integrity.

CASE STUDY 2: DVR/CCTV FORENSIC EXAMINATION – EMPLOYEE THEFT

- **Objective:** Conduct a forensic examination of DVR/CCTV footage to investigate the theft of $200,000 from the company safe, allegedly committed by an identified employee on his off days.
- **Process:**
  1. Collected DVR/CCTV footage covering the timeframe of the alleged theft.
  2. Scrutinized footage to trace the movements and activities of the identified employee.
- **Findings:**
  1. **Unauthorized Access:**
     - Identified the employee entering the premises on his scheduled off days.
     - Detected instances of the employee accessing the secure area containing the safe.
- **Conclusion:** Through meticulous DVR/CCTV forensic examination, Hi Tech Data Group successfully uncovered evidence of an employee stealing $200,000 from the safe during his off days.

CASE STUDY 3: DOCUMENT FORENSIC EXAMINATION – FORGED STAMP IMPRESSIONS AND SIGNATURE

- **Objective:** Conduct a document forensic examination to determine the authenticity of stamp impressions and a signature.
- **Process:**
  1. Received documents for forensic analysis.
  2. Employed advanced techniques to scrutinize stamp impressions and signatures.
- **Findings:**
  1. **Forged Stamp Impressions & Signature:**
     - Identified irregularities in the texture and alignment of stamp impressions.
     - Utilized microscopic analysis to reveal inconsistencies in ink composition.
- **Conclusion:** Hi Tech Data Group conclusively identified forged stamp impressions and a signature through meticulous document forensic examination.

CASE STUDY 4: DVR/CCTV FORENSIC EXAMINATION – RECORDING MODULE TAMPERING

- **Objective:** Conduct a forensic examination of CCTV footage to investigate the theft of cement, revealing suspicious activity suggesting the DVR recording module was intentionally switched off.

- **Process:**
  1. Collected DVR/CCTV footage covering the timeframe of the alleged theft.
  2. Examined the footage to identify any anomalies or irregularities.

- **Findings:**
  a. **Recording Module Tampering:**
     - Observed deliberate actions indicating the DVR recording module was switched off during the period of the theft.
     - Identified an individual with access to the system intentionally disabling the recording functionality.

- **Conclusion:** Through DVR/CCTV forensic examination, Hi Tech Data Group identified a case of recording module tampering, facilitating the theft of cement.

CASE STUDY 5: MOBILE DEVICE HACK AND IDENTITY FRAUD

- **Objective:** Investigate a mobile device hack linked to identity fraud.

- **Process:**
  1. **Examined compromised mobile device.**
  2. **Traced unauthorized access points and activities**

- **Findings:**
  1. **Identified an impersonator who hacked the device.**
  2. **Impersonator committed fraud using the victim's identity.**

- **Conclusion:** Hi Tech Data Group uncovered a mobile device hack leading to identity fraud, underscoring the need for enhanced digital security.

CASE 1: DATA SANITIZATION ON 30 LAPTOPS: HDDS AND SSDS

- **Objective:** Sanitize 30 Laptops that will then be resold or donated.

- **Process:**
  1. Sanitization done using NIST 3 Passes military standard.
  2. Report and Certificate created for each device.

- **Findings:**
  1. After data sanitization, the data cannot be recovered even by data recovery experts or forensics engineer.
  2. Data sanitization give the company peace of mind after disposing the laptops.

- **Conclusion:** Hi Tech Data Group was tasked to provide data sanitization & shredding services for client. The job was do with international military standards. Reports & Certificates provided.

CLIENTS SERVED

Embassy of Belgium
CIC GROUP
Cleanshelf
Dalberg
BROOKE EAST AFRICA
KenGen
Energy for the nation.
Mediamax Network
easycoach
experience dignity
HASS PETROLEUM
CITIZEN
ROYAL MEDIA SERVICE LTD
CHRIST IS THE ANSWER MINISTRIES [CITAM]
EMPIRE KENYA
Huduma
Realters Limited
NIRA
impax
BUSINESS SOLUTIONS
ITV
TANZANIA
inuka africa
IBERAFRICA
POWER LTD.
ivory
Health Solutions
AFFORDABLE QUALITY HEALTHCARE
NEXT
technologies
KAR00000
GRASK
HYGROTECH
SUSTAINABLE SOLUTIONS
GOLDEN AFRICA
KENYA LIMITED
KEMRI | Wellcome Trust
Runji Consulting Group
Engineering & Project Management
HOLY CROSS FAMILY MINISTRIES
KENYA
Izaak Walton Inn
EMBU
PRIMROSE MANAGEMENT
Orient Sacco Ltd
ENCORE
Technology
burn
life · saving · jikos
UMOJA
LOVE SHOES. LOVE UMOJA.
UHMC
Mountain Fresh
WHOLE MILK
SAVE THE ELEPHANTS
Taifa
Mobile Limited
SGA
SECURITY
WaterKiosk
UNIVERSITY OF NAIROBI
XC360
IT SUPPORT . CLOUD . BACKUP

HITECH DATA GROUP LIMITED

Bandari Plaza, Mezzanine 3, Woodvale Grove
Westlands, Nairobi, Kenya
6950-00100

inquiry@hitechdatagroup.com
inquiry@eastafricahitechsolutions.co

+254791814241
+254714883783

www.hitechdatagroup.com
www.eastafricahitechsolutions.co