Digital Forensics **Case Study**

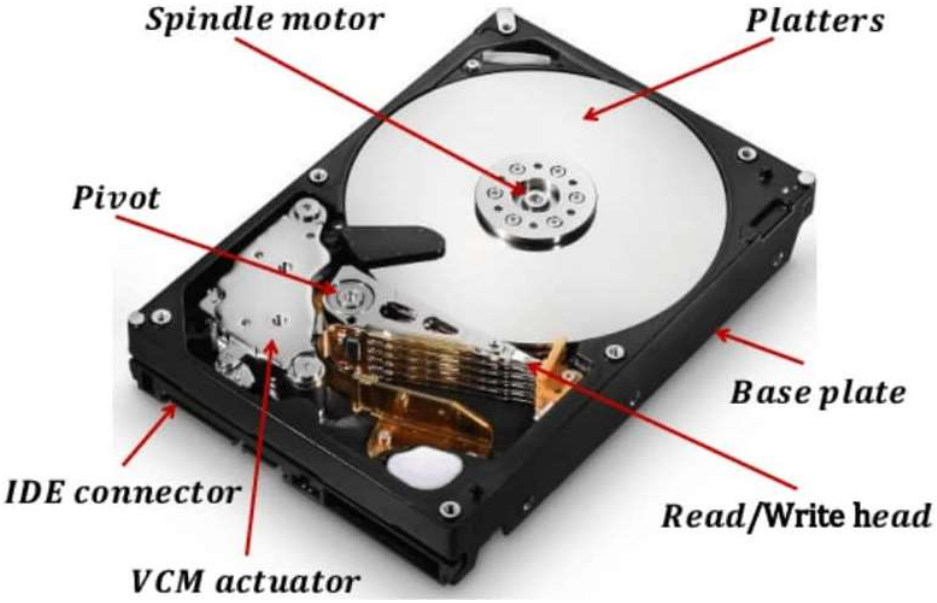
📝 Title: Detailed Procedure – Forensic Recovery of Damaged Hard Drive by Using Atola Imager

---

🔎 1. Background of the Case

- A **Law Enforcement Agency (LEA)** was handling a **sensitive criminal investigation**.
- A **hard drive** containing **critical digital evidence** related to the case had **stopped functioning**.
- The hard drive was a crucial piece of evidence in one of the criminal cases. The law enforcement agency had reason to believe that the hard drive contained important information related to the case.
- We need to acquire the **technical expertise and tools** required for data recovery from a **non-responsive** drive.
- To deal with this case we need **digital forensic expertise** and specialized equipment so we would be able to retrieve the data from the damaged hard drive.

HardWare



⚠️ 2. Key Challenges Faced

Challenge Area	Description
🧩 **Hardware Issues**	Possible failures in the **PCB**, **firmware**, **media surface**, or **head assembly**.
⚒️ **Inaccessibility**	The drive could not be accessed using **standard forensic tools**.
⏱️ **Time Constraint**	Evidence was needed for a **time-sensitive court case**.
⚖️ **Legal Sensitivity**	The recovery process had to be **forensically sound**, preserving **chain of custody** and ensuring data was **admissible in court**.
🧠 **Unknown Root Cause**	It was unclear whether the issue was electrical, mechanical, or firmware-based.

🛠️ 3. Tools & Technology Used

- 🔧 **Tool**: Atola Insight Imager
- 🔍 **Features**:
  - Automatic diagnosis of hard drive failures.
  - Analysis of components like **circuitry, heads, media surface, firmware**, and **file systems**.
  - Capability to operate on **damaged drives** without altering data.
  - Generates **comprehensive forensic reports**.


Atola
SERIAL
IDE
SOURCE 1
SOURCE 2
SOURCE 3
S1
S2
S3
USB
IDE
EXT
Source
Target
T1
T2
T3
USB
Write protection
DISKSENSE II


DSIEXT
20221010
7pcb
DSIMAIN
20221026
VBUS
RED WIRE
ON
OFF
CPU FAN BOOST

✅ 4. Step-by-Step Procedure

🔐 Step 1: Securing the Evidence

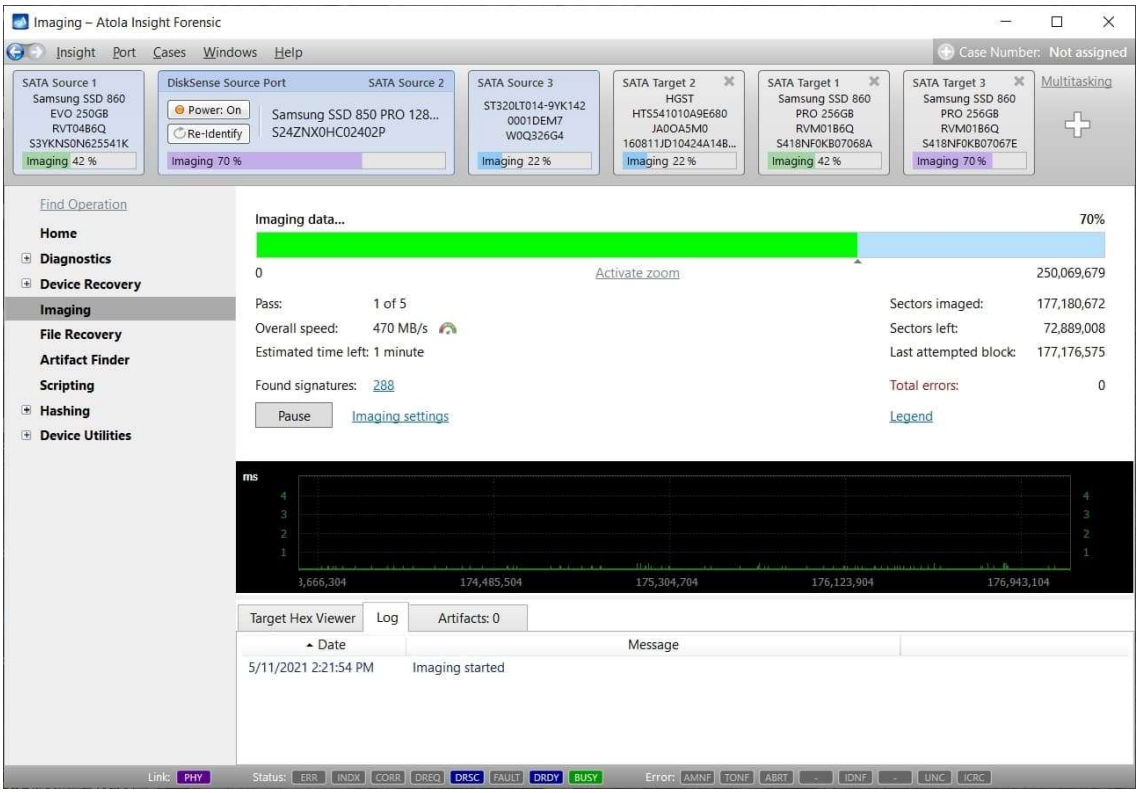
- The faulty hard drive was collected and **documented**.
- Chain of custody protocols were initiated to ensure evidence admissibility.

🔌 Step 2: Connecting to Atola Imager

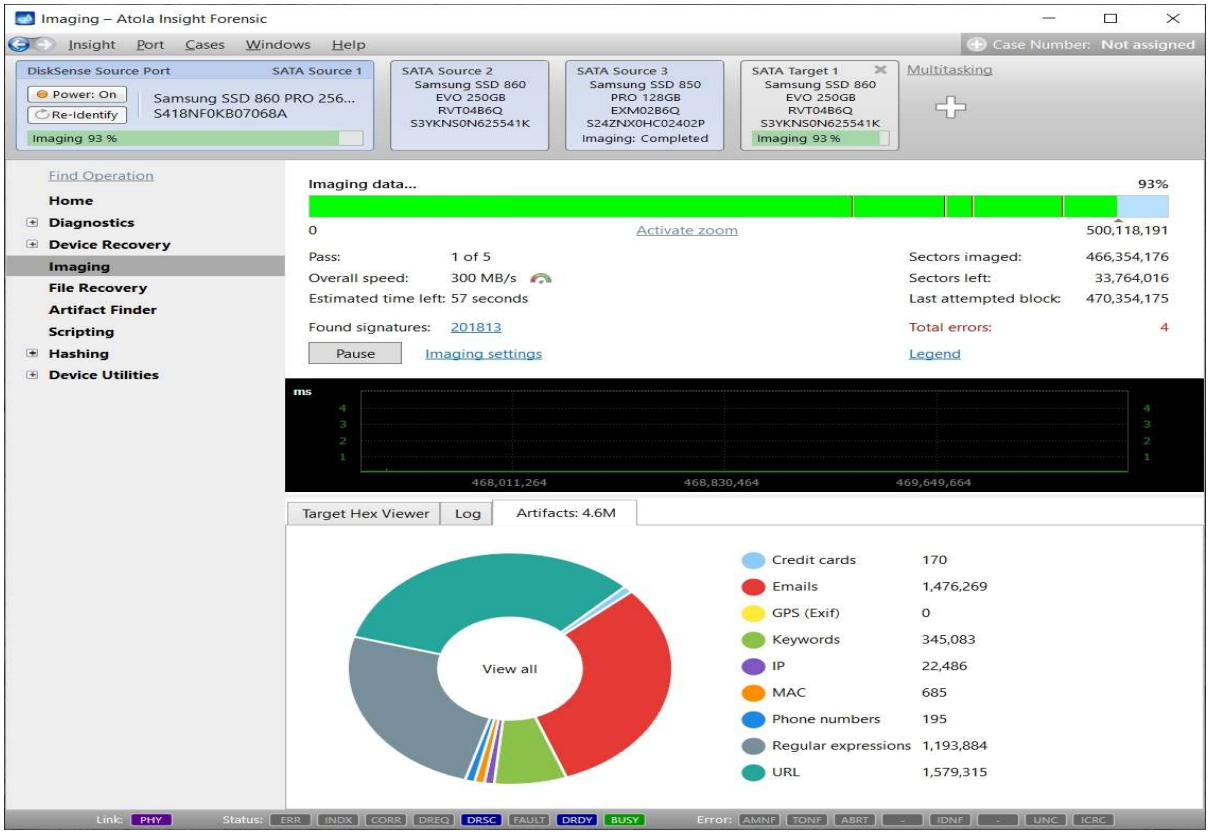
- The hard drive was safely connected to the **Atola Insight Imager**.
- Precautions were taken to prevent electrical surges or mechanical stress.

🧠 Step 3: Automatic Diagnosis

- Atola Imager began **comprehensive diagnostics**:
  - Checked power circuits and **PCB status**.
  - Scanned **firmware integrity** and version.
  - Assessed condition of **media surface** and **read/write heads**.
  - Attempted to **mount and read the file system**.



⚠ Step 4: Fault Identification



- Diagnosis revealed **PCB corruption** was the primary issue.
- This component prevented access to stored data.

🛠️ Step 5: Hardware Repair

- Using **precision tools**, Pelorus replaced the **corrupt PCB** with a matching functional one.
- Firmware from the old PCB was **cloned or transferred** to the new PCB to retain calibration and compatibility.

💾 Step 6: Forensic Data Recovery

- Once the drive was operational:
  - We used advanced **read-only forensic recovery tools** to extract data.
  - Ensured that **no data was modified or deleted**.
  - Created **bit-by-bit forensic images** for analysis and preservation.

🔐 Step 7: Data Integrity and Documentation

- Recovered data was validated using **hashing techniques (MD5/SHA-1)**.
- Reports were generated on:
  - Drive status pre and post-recovery.
  - Evidence handling logs.
  - Recovery steps taken.
- All actions were **documented for court presentation**.

📦 Step 8: Evidence Handover

- The recovered data and forensic reports were securely handed over to LEA.
- The chain of custody was **preserved and verified** at every step.

📈 5. Outcome of the Investigation

Result Area	Details
✅ **Data Recovery**	All crucial evidence was recovered from the damaged drive.
📜 **Legal Admissibility**	Evidence maintained forensic integrity and was used in court.
👨‍⚖️ **Impact on Case**	Provided **vital insights** that helped **advance the investigation** and **deliver justice**.
🧰 **Demonstrated Expertise**	Highlighted the critical role of **digital forensics** and the effectiveness of **Atola Imager** in real-world legal cases.

📊 6. Visual Flowchart of the Process

[Hard Drive with Critical Evidence]

↓

[Collected During collection phase]

↓

[Connected to Atola Imager for Diagnosis]

↓

[Fault Detected: Corrupt PCB]

↓

[PCB Replaced with Identical Component]

↓

[Drive Operational – Begin Read-Only Recovery]

↓

[Data Recovered using Forensic Software]

↓

[Data Verified, Documented, and Preserved]

↓

[Handover to LEA with Reports and Chain of Custody]

↓

[Evidence Used in Court – Case Progressed]

🧠 7. Key Takeaways

- Using advanced forensic tools like **Atola Imager**, even **severely damaged drives** can be recovered.
- **Forensic discipline and legal awareness** are essential during the entire process.
- **Technology + Expertise** = successful resolution of complex digital investigations.

Conclusion

The successful recovery of crucial evidence from a severely damaged hard drive demonstrates the importance of advanced forensic tools and expert intervention. The Law Enforcement Agency faced a major setback when standard methods failed to access the data due to PCB and potential firmware and hardware issues. We utilized the Atola Insight Imager, conducted a thorough diagnosis and identified the root cause—PCB failure. By carefully replacing the faulty component and preserving firmware integrity, We restored the drive's functionality. The evidence was then recovered using forensic imaging while maintaining a secure chain of custody. The data retrieved played a vital role in advancing the investigation and remained fully admissible in court. This case highlights the need for digital forensic readiness, collaboration with specialized agencies, and the critical role of technology in modern investigations.With the collected Digital Evidence we ensured justice was not delayed, reaffirming the value of expert digital forensic services in law enforcement.
