**DIGITAL FORENSICS**

**CASE STUDY**

**Case Scenario: Digital Forensics Investigation Using the Digital Forensic Tool**

**Incident Overview**

A financial organization detected anomalies in its security logs, raising concerns about unauthorized access and potential data tampering. Employees reported unusual modifications in critical financial documents, prompting an urgent forensic investigation.

**Incident Timeline & Investigation Phases**

**1. Investigation Phase**

**Incident Detection**

* The IT security team detected anomalies in system logs.
* Multiple failed login attempts were recorded from an unknown IP address.
* Unauthorized modifications were made to financial records.
* The incident was flagged as a potential data breach, triggering a forensic investigation.

**2. Collection Phase**

**Evidence Collection**

* A forensic team was deployed to secure and analyze the compromised files.
* Logs, emails, and suspicious executable files were extracted for timeline reconstruction.
* Critical files were preserved, ensuring their integrity for forensic examination.

**3. Examination Phase**

**Verifying File Integrity**

* The investigator uploaded the collected files to the forensic tool’s **Hash Calculator** module.
* Selected a cryptographic hashing algorithm (e.g., SHA-256).
* The tool computed and displayed the hash values.
* Hashes were recorded for integrity verification in later stages.

**Metadata Analysis**

* Suspicious files were uploaded to the **Metadata Analyzer** for deeper examination.
* Extracted metadata included:
  + Creation and modification timestamps.
  + Author information and potential embedded GPS data (if applicable).
* Anomalies in timestamps and unauthorized user access flagged as suspicious.

**Log Analysis for Suspicious Activities**

* System logs were analyzed to trace unauthorized access patterns.
* The tool scanned logs for **ERROR, WARNING, or unauthorized access attempts**.
* Patterns of failed login attempts and unauthorized file transfers were identified.
* Anomalous user behavior and suspicious external connections were flagged.

**4. Analysis Phase**

**File Integrity Comparison**

* Investigators used the **Hash Integrity Checker** to compare original and current file versions.
* If the hashes matched, no changes were made; if they differed, tampering was confirmed.
* Confirmed unauthorized modifications to critical financial records.

**Findings & Conclusion**

* The forensic investigation revealed:
  + A compromised employee account accessed restricted customer records.
  + Unauthorized modifications to sensitive files were made.
  + Log analysis traced the attack source and provided a timeline of malicious activities.
  + Metadata analysis exposed attempts to manipulate timestamps and cover tracks.
* The financial institution revoked compromised credentials and strengthened access controls.

**5. Final Reporting Phase**

**Forensic Documentation & Legal Proceedings**

* The forensic team compiled a **detailed investigation report**, including:
  + Hash integrity verification results.
  + Metadata analysis findings.
  + Log analysis summaries.
* The report was submitted as legal evidence to aid in regulatory actions and possible prosecution.
* Additional cybersecurity measures were implemented to prevent future incidents.

**Conclusion**

This case highlights the significance of digital forensic tools in cybercrime investigations. By integrating **hash integrity checks, metadata extraction, and log analysis**, forensic teams can effectively detect unauthorized access, verify data integrity, and trace security breaches. The structured forensic approach ensures the accuracy, reliability, and admissibility of digital evidence in legal proceedings.