

## DIGITAL FORENSIC EXAMINATION CERTIFICATE

### CASE AND COMPUTER IDENTIFICATION

**Case:** Seized laptop examination (ID: CASE-FEXAM)  
**Case number:** CC/2026/0042  
**FIR number:** FIR-2026-77  
**CNR number:** MHPN01-001234-2026  
**Court:** Court of the Chief Judicial Magistrate, Pune  
**Investigation agency:** Pune City Cyber Police  
**Analyst:** Pallavi Pawar  
**Organisation:** Innovativa SoftTech  
**Computer:** LAPTOP-PL914FQ9  
**Operating system:** Windows 11 10.0  
**Software:** e-Dex v1.4.0  
**Algorithms used:** SHA-256  
**Period covered:** 2026-06-01 IST to 2026-06-18 IST  
**Chain of custody:** Recorded in the application's tamper-evident, hash-chain'd audit log (append-only; altering any one entry breaks every following record).

### SOURCE DEVICE (EVIDENCE)

**Device name:** Seized laptop HDD  
**Device type:** Hard Disk Drive  
**Make:** Western Digital  
**Model:** WD10EZEX  
**Serial number:** WD-WX21A1234567  
**Operating system:** Windows 11 Pro  
**Ownership:** Accused

### EXAMINATION

**Methodology:** Write-locked acquisition; keyword and timeline analysis; manual review of recovered artifacts.

**Tools used:** e-Dex 1.4.0, Autopsy 4.21, hardware write-blocker

### FINDINGS

Examination of the seized hard disk recovered 14 deleted documents relevant to the matter. The artifact timestamps are consistent with the period under investigation. No evidence of anti-forensic wiping was observed. The recovered items and their cryptographic hashes are listed in the annexure to this certificate.

### ANNEXURE - EVIDENCE RECORDS AND HASH VALUES (hashes per algorithm, as labelled)

#	FILE	SIZE	STATUS
1.	<b>evidence-1.dd</b> SHA-256: 874e9c3ea2b3c4dda2b3c4e5a2b3c4eda2b3c4f5a2b3c4fda2b3c505a2b3c50d <b>Integrity: MATCH - computed hash equals the recorded expected hash.</b>	51.0 MB	<b>Verified</b>
2.	<b>evidence-2.dd</b> SHA-256: 913213d9a3b4c5dea3b4c5e6a3b4c5eea3b4c5f6a3b4c5fea3b4c606a3b4c60e <b>Integrity: MATCH - computed hash equals the recorded expected hash.</b>	52.0 MB	<b>Verified</b>
3.	<b>evidence-3.dd</b> SHA-256: 9b158b74a4b5c6dfa4b5c6e7a4b5c6efa4b5c6f7a4b5c6ffa4b5c707a4b5c70f <b>Integrity: MATCH - computed hash equals the recorded expected hash.</b>	53.0 MB	<b>Verified</b>

---

## VERIFICATION RESULT

Files checked: 3  
Integrity verified: 3  
Integrity failed: 0

**RESULT: INTEGRITY VERIFIED - all recorded files match their expected hash values.**

## DECLARATION

I certify that I conducted the digital forensic examination described in this certificate, that the methodology and tools recorded above were used, that the cryptographic hash values of the examined items are reproduced in the annexure, and that the findings stated above are a true and accurate record of the results of that examination to the best of my knowledge, information and belief.

## CERTIFICATION

I, the undersigned, do hereby affirm that the examination, the methodology and tools employed, and the findings set out in this certificate are true and correct to the best of my knowledge, information and belief, and were recorded without alteration.

Signature: \_\_\_\_\_  
Name (printed): \_\_\_\_\_  
Designation: Senior Forensic Analyst  
Place: Pune  
Date: \_\_\_\_\_

---

e-Dex generates this certificate as a workflow aid from the recorded examination particulars and hash values. The examiner is solely responsible for the correctness of the methodology, findings and every fact stated, and for the sufficiency of this certificate for its intended purpose. The vendor makes no warranty of fitness for any particular use.

All times are stamped in UTC and shown in IST (Asia/Kolkata, UTC+5.30). Times displayed by third-party archive or extraction tools may differ due to local timezone conversion.

**SAMPLE - NOT REAL EVIDENCE**