FINAL YEAR PROJECT // 2026

BlockEvidence

Secure Digital Crime Evidence Management System

Progress Report

February 19, 2026

PROTOTYPE COMPLETE

PHASE 5 / 7

CLASSIFICATION	BUILD STATUS	NEXT MILESTONE
Confidential	Exit Code 0	UAT

01 Executive Summary

BlockEvidence is a secure, digital Crime Evidence Management System engineered to guarantee the absolute integrity of digital forensic evidence throughout its entire lifecycle — from field collection through courtroom presentation. Built on robust cryptographic foundations and presented through a purpose-designed Dark Cyber-Security interface, the platform provides a tamper-proof chain of custody that satisfies both operational and legal requirements.

As of February 2026, the project has successfully completed Phase 5 (Polish & Integration). The application compiles cleanly with zero TypeScript errors (Exit Code: 0), all core features are fully implemented, and the system is ready to enter end-to-end User Acceptance Testing (UAT). The remaining work is focused on advanced integrations — blockchain anchoring, physical device connectivity, and enhanced legal-export capabilities.

Metric	Status
Build Status	Exit Code 0 — No Errors
Current Phase	Phase 5 — Polish & Integration COMPLETE
Next Phase	User Acceptance Testing (UAT)
Core Features	Fully Implemented
Pending Items	3 Advanced Integration Tasks
Last Updated	February 19, 2026

02 Project Vision & Core Mechanics

Vision: To create a digital fortress for forensic evidence that prevents tampering and maintains a strict, verifiable chain of custody from the moment of collection to its presentation in a court of law.

Core Workflows

Crime Box Flow	Role-Based Access (RBAC)	Legal Ticket System
A secure digital container protected by a dual-key system. A Public Key enables view-only access while a Private Key grants authorised decryption and modification rights — enforcing strict case-level access control.	A granular permission layer. Investigating Officers may submit and tag evidence; Judges and Defence Attorneys receive strict Read-Only access, allowing integrity verification without any capability to alter source files.	A proactive security mechanism. Any unauthorised access attempt does not merely fail — it generates a cryptographically signed "Legal Ticket" (Incident Log), creating an indisputable audit trail of attempted tampering.

Design & User Experience

The platform adopts a distinctive **Dark Cyber-Security** aesthetic characterised by deep slate backgrounds paired with emerald/neon-green accents, reinforcing the forensic security context at every interaction. A signature **Biometric Fingerprint Scanner** animation greets users on the login and registration portals, immediately establishing the high-security atmosphere appropriate to a law-enforcement tool. All UI elements use a consistent 0.5rem border-radius to maintain a precise, technical feel throughout.

03 Milestones Achieved

Backend Infrastructure

- **Database Schema.** Finalised Prisma schema encompassing Evidence, Case, CrimeBox, CustodyEvent, AccessLog, LabResult, and Notification models — providing a complete relational foundation for all system data.
- **Secure API.** Implemented robust RESTful endpoints with JWT authentication and strict permission middleware, ensuring every request is validated and authorised before execution.
- **Evidence Management.** Full CRUD operations for evidence items, including bulk upload support and a rich tagging system for rapid categorisation and retrieval.
- **Case Management.** Business logic to group individual evidence items and Crime Boxes into cohesive case files, mirroring real-world investigative workflows.
- **Public Verification.** A dedicated /verify/:hash endpoint combined with QR code generation enables external parties — including the public and jury members — to independently confirm evidence authenticity without system access.

Frontend Application

- **Dashboard Ecosystem.** A comprehensive operator dashboard featuring Analytics, Activity Feed, Notifications, and Case Management views — providing a unified command centre for investigators.
- **Evidence Detail View.** An enhanced detail view with tabbed navigation for Comments, Lab Results, and the full Chain of Custody timeline, giving officers a complete picture of any evidence item.
- **Interactive Analytics.** Real-time charts visualising evidence submission trends and status distribution, enabling supervisors to monitor caseload and flag anomalies.
- **Public Verification Portal.** A standalone, unauthenticated page designed for jury members or the public to verify evidence authenticity via hash input or QR code scan.

Security & Collaboration

- **Access Request Workflow.** A formalised "Request → Approve/Deny" loop for restricted evidence. Supervisors are automatically notified of incoming access requests, and all decisions are logged immutably.
- **RBAC Implementation.** Role checks enforced at the route level for four distinct permission tiers: Admin, Officer, Analyst, and Viewer. No role can exceed its defined access boundary.

04 Current Phase & Project Status

The project has just completed **Phase 5: Polish & Integration**. This phase focused on resolving all outstanding TypeScript compilation errors, tightening UI consistency, and ensuring all modules integrate cleanly. The application now builds without errors (Exit Code: 0) and the full feature set has been merged to the main branch.

The system is now cleared for **end-to-end User Acceptance Testing (UAT)**, the next formal milestone. UAT will involve structured testing scenarios covering the primary workflows: evidence submission, chain-of-custody tracking, RBAC enforcement, access request resolution, and public verification.

Phase	Description	Status
Phase 1	Core Infrastructure & Database Schema	**Complete**
Phase 2	Authentication, RBAC & Secure API	**Complete**
Phase 3	Evidence & Case Management	**Complete**
Phase 4	Frontend Dashboard & Verification Portal	**Complete**
Phase 5	Polish, Integration & TypeScript Resolution	**Complete**
Phase 6	User Acceptance Testing (UAT)	**In Progress**
Phase 7	Blockchain Anchoring & Physical Device Integration	*Pending*

05 Pending Tasks

Three items remain before the system can be considered feature-complete for production deployment. These are advanced integrations that extend the platform beyond its current prototype scope.

1

Blockchain Integration

Although the cryptographic key infrastructure is in place, the Legal Ticket and Custody Event logs are not yet anchored to a public distributed ledger. Integrating with a platform such as Ethereum or Hyperledger Fabric will provide immutable third-party verification of every chain-of-custody event, removing any reliance on the BlockEvidence system itself as the sole source of truth.

2

Physical Device Integration

A prototype interface is required to bridge physical evidence bags — tagged with NFC or RFID chips — with their corresponding Digital Crime Box records. This integration will close the loop between physical and digital evidence handling, ensuring every movement of a physical item is automatically reflected in the system's audit trail.

3

Advanced Legal Export (Feature 14)

Initial work on generating fully legal-compliant PDF reports has commenced but requires additional polish to meet court-submission standards. The final export must include complete chain-of-custody records, cryptographic hashes, officer attestations, and formatted metadata in a format acceptable to legal authorities.

06 Challenges & Technical Blockers

The Activity Feed and Analytics Dashboard currently require a full page refresh to display newly submitted evidence or updated case statuses. WebSocket integration (Socket.IO) or a long-polling mechanism is recommended for the UAT phase to provide the live updates expected in an operational forensic environment.

Throughout the development cycle, the running API server occasionally failed to pick up newly registered routes without a manual restart, creating friction in the development workflow. Adopting a file-watcher tool such as nodemon or tsx watch is recommended for all future development cycles to eliminate this issue.

BlockEvidence — Final Year Progress Report	February 19, 2026 | Phase 5 Complete | UAT Ready	*Confidential — Academic Use Only*