Transforming Forensic Firearms Identification: Bridging Traditional Microscopy with Digital Annotation & Case Review

Harnessing Striae to Elevate Accuracy, Collaboration, and Courtroom Impact

Author: Stephen J. Lu, EMBA, SHRM-CP

Platform: Striae

Date: 09/26/2025

Executive Summary

Forensic firearms identification remains rooted in manual, disjointed workflows that compromise efficiency, accuracy, and collaboration. Examiners capture high-resolution comparison images but must leave specialized microscopy environments to annotate and document findings in general-purpose applications or other analog methods. This separation introduces transcription errors, version-control challenges, and time-consuming processes that slow case throughput and hinder peer review.

Striae transforms this paradigm by offering a cloud-native forensic annotation platform purpose-built for firearms examiners. Leveraging Cloudflare's global edge network, Striae integrates comparison microscopy image management, real-time annotation and linking, and cryptographically authenticated confirmations into a single, secure environment. Examiners benefit from intuitive, firearms evidence-focused annotation tools, tamper-evident AES-256-encrypted audit trails, and automated digital signatures that preserve chain of custody and support non-repudiation. Multi-examiner workflows (confirmations) ensure consistent reporting and verification, while version control and export services provide full historical context for quality assurance and clear courtroom presentation.

Reducing documentation time and reducing clerical errors can potentially yield significant labor-cost savings and backlog reduction. By centralizing data management, standardizing processes, and enhancing evidence integrity, Striae accelerates case processing, strengthens scientific rigor, and elevates the credibility of expert testimony. As the first cloud-native annotation solution for firearms identification, Striae effectively bridges traditional comparison microscopy with modern digital workflows—empowering laboratories to deliver faster, more reliable forensic results in service of justice.

Table of Contents

Introduction

What is Forensic Science?

Forensic science is simply that: a science. Since the days of Aristotle, Ibn al-Haytham, Johannes Kepler, and Galileo Galilei, the method of scientific investigation based on the observable and reproducible results of experimentation has been the bedrock and foundation of technological, biological, and physical advancements.

The framework is as follows:

1. Hypothesis
2. Experimentation
3. Observe Results
4. Analyze and Report
5. New Hypothesis

Through continual experimentation, hypotheses are modified, rejected, and accepted, each building on the one before.

Forensic scientists apply this model to investigate crimes in which physical evidence is available for examination. Forensic biologists ask, "What is the DNA profile from this bloodstain, and what is the probability this DNA profile comes from Person A rather than a random individual?"

Forensic firearms examiners ask, "Do the individual characteristics left on this questioned fired bullet match the individual characteristics left on this test-fired bullet from a known firearm?"

Forensic drug examiners ask, "Do the retention time and mass spectra of this unknown substance match those of a particular known reference?" And so on.

Forensic science is not a solo endeavor. To effectively advance forensic scientific achievement, one must collaborate and share ideas and results with the broader forensics community. This is quite evident in the existence of peer-reviewed journals, international professional organizations, and laboratories in which groups of scientists work together to provide services and advance their field of expertise.

The Evolution of Firearms Identification

Within forensic science, firearms identification has undergone particularly dramatic transformation since its inception in the early 20th century. The discipline's foundations were laid by pioneers like Victor Balthazard, who in 1913 first advanced the theory that every firearm leaves unique microscopic marks on fired bullets. This theoretical breakthrough was operationalized in the 1920s when Calvin Goddard and Philip Gravelle adapted comparison microscopy for forensic use, creating the first Bureau of Forensic Ballistics in 1925. The **comparison microscope** became the cornerstone tool, allowing examiners to simultaneously view bullets or cartridge cases side-by-side and identify matching striations and impressions.

For nearly a century, this fundamental approach remained largely unchanged, with improvements focusing primarily on optical enhancements, better lighting, and photographic capabilities. However, the digital age has ushered in a revolutionary shift from traditional 2D comparison microscopy to sophisticated 3D topographic analysis. Modern virtual microscopy systems now capture high-resolution three-dimensional surface measurements, enabling examiners to create digital archives, share evidence instantly across jurisdictions, and conduct more objective, reproducible analyses. Machine learning algorithms are beginning to automate pattern recognition tasks that once relied solely on human expertise, while cloud-based platforms facilitate unprecedented collaboration between laboratories and investigators worldwide.

The Future of Collaborative Forensic Science

The evolution of forensic science, particularly in firearms identification, demonstrates that technological advancement must be coupled with enhanced collaboration to truly serve justice. As digital transformation accelerates, the field faces both unprecedented opportunities and challenges. Cloud computing now enables real-time data sharing and collaborative analysis across geographic boundaries, while artificial intelligence promises to reduce human error and accelerate case processing. However, these advances also require new validation methodologies, standardized protocols for digital evidence handling, and robust security frameworks to maintain chain of custody integrity. The future of forensic firearms examination lies not in replacing the scientific method that has guided the discipline since Aristotle, but in leveraging modern technology to enhance its application. Digital annotation platforms, virtual microscopy, and cloud-native forensic tools represent the natural evolution of collaborative scientific practice—enabling forensic examiners to share observations, validate findings, and build upon each other's work with greater precision and efficiency than ever before. This technological foundation supports

the fundamental goal of forensic science: to provide accurate, reproducible, and scientifically sound evidence that serves the pursuit of truth and justice.

The Ultimate Purpose of Striae

By reading this white paper, readers will gain comprehensive insight into the fundamental challenges facing modern forensic firearms identification and discover how the Striae platform represents a paradigm shift toward more efficient, collaborative, and scientifically robust forensic practices. This document explores the technical innovations, methodological improvements, and practical benefits that position Striae as a transformative solution for the forensic community. Readers will understand not only the "what" and "how" of Striae's capabilities but also the deeper "why" behind its development—addressing critical gaps in current forensic workflows that impact case processing times, inter-laboratory collaboration, and the overall quality of forensic evidence presentation.

Target Audience and Applications

This document is specifically crafted for three primary constituencies within the forensic ecosystem. Firearms examiners will discover how Striae enhances their daily workflow efficiency, reduces time spent on routine documentation tasks, and provides powerful new tools for peer verification and case review. Laboratory directors will learn how the platform supports compliance with quality assurance standards, streamlines case management processes, and facilitates the audit trails and documentation requirements essential for accreditation maintenance. Representatives of forensic technology companies will gain insights into emerging best practices, industry trends toward cloud-native solutions, and the technical architecture principles that enable scalable, secure forensic platforms.

Open-Source Foundation and Broader Impact

Striae's commitment to open-source development reflects a fundamental principle of scientific advancement: transparency breeds trust, collaboration accelerates innovation, and shared knowledge benefits the entire forensic community. The platform's open codebase serves multiple strategic purposes beyond mere cost considerations. First, it enables peer review and validation of the underlying functions and methodologies, addressing calls for greater transparency in forensic sciences. Second, it provides educational value for academic institutions and training programs, allowing students and

researchers to examine, modify, and enhance the tools they will use in their professional careers. Third, it facilitates customization and integration with existing laboratory information management systems (LIMS) and workflow configurations, enabling laboratories to adapt the platform to their specific operational requirements.

The open-source approach also directly supports quality assurance objectives mandated by forensic standards. By making the source code publicly available, Striae enables the cross-verification capabilities that quality assurance protocols demand. Laboratories can validate the software's functionality, verify its compliance with established methodologies, and maintain the audit trails necessary for assessments and legal proceedings. This transparency is particularly crucial in an era where forensic evidence faces increasing scrutiny regarding scientific validity and reliability.

Furthermore, the information contained in this report and the public codebase creates a knowledge transfer mechanism that extends far beyond individual software implementation. Laboratories can use Striae's architectural patterns, security implementations, and workflow designs as templates for developing their own solutions or enhancing existing systems. This approach accelerates the adoption of best practices across the forensic community, ultimately advancing the entire field's technological capabilities and scientific rigor.

The platform's design principles and implementation strategies also serve as a reference model for future forensic technology development, demonstrating how modern cloud-native architectures can address the unique challenges of forensic evidence handling while maintaining the security, integrity, and chain-of-custody requirements essential for legal proceedings. By documenting these approaches and making them freely available, Striae contributes to the broader evolution of forensic science toward more standardized, efficient, and scientifically sound practices.

The Problem: Challenges in Traditional Firearms Identification

Current Pain Points

Traditional Comparison Microscopy and Manual Annotation: A Fragmented Workflow

The current state of forensic firearms examination presents a complex web of technological and procedural challenges that fundamentally compromise efficiency, accuracy, and scientific rigor. While modern digital comparison microscopes have advanced beyond their analog predecessors by allowing examiners to capture high-resolution snapshots of comparison fields, the subsequent documentation and annotation workflow remains surprisingly antiquated and fragmented.

Disjointed Documentation Processes

The primary limitation lies in the separation between image capture and annotation systems. After capturing comparison images through sophisticated microscopy equipment, examiners must transition to entirely separate software environments—typically general-purpose applications like Microsoft Word, Adobe Photoshop, or PowerPoint—to manually mark and label their findings. This workflow disruption creates multiple points of inefficiency and potential error introduction. Examiners lose valuable time switching between systems, manually importing images, and recreating the spatial context necessary for meaningful annotation.

The process becomes even more cumbersome when considering that each annotation must be manually created from scratch. Unlike integrated systems that might preserve metadata or contextual information from the original examination, these separate annotation workflows require examiners to manually recreate labels, measurements, and identifying markers. This manual recreation introduces both time delays and opportunities for transcription errors, as examiners must note and accurately reproduce their observations from one system to another.

Collaboration and Peer Review Bottlenecks

The challenges multiply exponentially when peer verification and collaborative review enter the equation. Current workflows may require physical handoffs of documents, email exchanges, or shared network drives to facilitate peer review. Multiple item examination in complex casework creates redundant work and extends case processing times. The lack of streamlined collaborative capabilities means that multiple examiners cannot efficiently review the same evidence, forcing fragmented review processes that can add days or weeks to case completion timelines.

Furthermore, the version control challenges inherent in paper-based workflows create additional complications. When multiple examiners contribute to a case file, tracking changes, managing different versions of annotated images, and maintaining a clear audit trail becomes increasingly difficult. Critical information can be lost among cross-outs and initials or re-printing, potentially compromising the integrity of the forensic examination process. At the very least, it becomes a cumbersome process.

Digital Evidence and Documentation Disconnect

Perhaps most problematically, current workflows create an artificial separation between digital evidence and examiner documentation. The comparison images captured by digital microscopy systems exist as one set of files, while examiner annotations, measurements, and conclusions exist as entirely separate documents. This separation means that annotations cannot be dynamically linked to specific original evidence images. If an examiner needs to reference a particular striation pattern or toolmark characteristic months or years later during testimony preparation, they must manually correlate their annotations with the original images, potentially requiring them to re-examine the evidence entirely.

Archival, Data Management, and Long-term Access Challenges

The documentation challenges extend into long-term archival, data management, and retrieval processes. Although digital comparison microscopy generates vast volumes of high-resolution image files, laboratories often face storage limitations and must manage terabytes of evidence across aging servers or on-premises network storage. This sheer volume of digital evidence strains budgets and complicates governance, potentially leading many organizations to implement tiered storage or purge policies that risk unintentional data loss.

Compounding storage constraints are access and retrieval issues. Annually, examiners and auditors may spend hours searching disparate file repositories—network drives, document management systems, or scanned PDF archives—to locate relevant case files or historical annotations. These siloed systems lack unified indexing, metadata standards, or search functionality, so users must rely on inconsistent naming conventions or directory structures to find the correct evidence.

Meanwhile, the examiner's analytical notes—typically preserved as scanned PDFs of handwritten sheets or exported Word documents—remain completely decoupled from the original microscopy images. With no direct linkage between annotations and specific evidence files, any request for retrospective review (e.g., re-examination, quality audits, or expert testimony preparation) triggers a labor-intensive process: manually matching scanned notes to images, re-opening legacy software, and recreating contextual metadata.

The absence of an integrated data management framework also hinders standardized audit trail maintenance. While digital microscopes produce quality images, they do not track or store case numbers, item numbers, or the examiner's notes. Quality assurance reviews cannot seamlessly trace each annotation back to its source image or validate that storage and access controls met chain-of-custody requirements.

Collectively, these archival, data management, and long-term access deficiencies undermine operational efficiency, expose laboratories to compliance risks, and can possibly weaken the scientific and legal robustness of firearms identification due to these fragmented links.

Quality Assurance and Audit Trail Deficiencies

From a quality assurance perspective, the fragmented workflow creates significant gaps in audit trail maintenance. While digital microscopy systems typically maintain detailed logs of image capture parameters, timestamps, and equipment settings, this technical metadata becomes divorced from the examiner's analytical process documented in separate annotation systems. Quality assurance reviews cannot easily trace the relationship between specific microscopy settings, captured images, and examiner conclusions, making it difficult to validate examination procedures or identify systematic errors.

The inability to create comprehensive, linked documentation also hampers efforts to establish consistent examination standards and performance metrics across laboratories. Without integrated systems that capture both technical parameters and examiner

observations in a unified format, it becomes challenging to conduct meaningful statistical analyses of examination practices, error rates, or inter-examiner consistency.

Impact on Scientific Validity and Legal Proceedings

These workflow challenges have broader implications for the scientific validity of forensic firearms identification. The analog nature of current annotation processes makes it difficult to implement systematic approaches to pattern recognition, measurement standardization, or statistical analysis of interpretation patterns. The separation between digital evidence and examiner documentation also complicates efforts to develop automated quality checks, consistency validations, or computer-assisted analysis tools that could enhance the reliability of forensic conclusions.

In legal proceedings, these documentation gaps can undermine the persuasiveness and credibility of expert testimony. Attorneys increasingly challenge forensic evidence based on questions about methodology, consistency, and scientific rigor. When examiners cannot demonstrate clear, traceable links between digital evidence and their analytical conclusions, or when documentation workflows appear ad hoc and inconsistent, the resulting testimony becomes vulnerable to effective cross-examination.

The cumulative effect of these challenges creates a forensic examination environment where technological capabilities far exceed workflow efficiency. While laboratories invest in sophisticated digital microscopy equipment capable of producing exceptional image quality and precise measurements, the downstream documentation and collaboration processes remain trapped in pre-digital paradigms that limit the realization of these technological investments.

Current State of Forensic Technology and Industry Trends

The forensic firearms market today is dominated by a handful of specialized digital comparison and identification platforms:

National Integrated Ballistic Information Network (NIBIN) / Integrated Ballistics Identification System (IBIS)

The ATF's NIBIN program, powered by Forensic Technology WAI™ IBIS, uses high-resolution imaging and proprietary correlation algorithms to compare cartridge cases and bullets against a national repository of digital evidence.

Evofinder® Automated Ballistic Identification System (Leeds Forensic Systems)

Evofinder combines both 2D and 3D imaging with automated correlation searches, virtual comparison microscopy, and customizable reporting. Virtual comparison microscopy enables forensic examiners to visually compare cartridge cases and bullets within the software environment, enabling detailed digital examinations.

TopMatch-3D (Cadre Forensics)

Cadre Forensics offers a suite of 3D imaging and virtual comparison microscopy (VCM) tools, with the flagship platform being TopMatch-3D. This system is used for high-resolution, 3D surface topography scanning and analysis primarily in forensic firearms and toolmark examinations. It enables advanced comparison and identification of marks on cartridge cases and bullets by leveraging patented hardware based on elastomeric gel sensors and highly validated matching algorithms. TopMatch-3D also supports advanced cloud-based collaboration for firearm forensics by enabling remote access, data sharing, and virtual comparison microscopy (VCM) between laboratories and examiners (Cadre Nexus).

The Cadre Forensics platform is recognized as a leading, validated, and widely adopted solution for 3D imaging and analysis in forensic firearms examination, supporting advances in speed, reproducibility, and defensibility of forensic findings.

Industry Trends

Movement Toward Cloud Solutions

Enterprise IT adoption data shows a decisive shift to cloud-hosted infrastructure and services. In 2025, over 90 percent of organizations worldwide run at least some workloads in public or private clouds, and 60 percent of production applications are cloud-native or hybrid, reflecting the need to scale storage and compute elastically.[1] Public cloud spending is projected to exceed $723 billion, underscoring laboratories' interest in off-loading capital-intensive servers and on-premises data centers in favor of operational expenditure models.[2] Forensic providers are beginning to offer cloud-managed case file archives and evidence-as-a-service (EaaS) platforms[3], enabling remote case access, automated backups, and disaster recovery capabilities that on-premise systems cannot match.[4]

These trends highlight the imperative for next-generation platforms—like Striae—that combine the proven capabilities of established forensic systems with the transparency, flexibility, and collaborative power of cloud-native technologies.

---

[1] "90+ Cloud Computing Statistics: A 2025 Market Snapshot," CloudZero, May 11, 2025. https://www.cloudzero.com/blog/cloud-computing-statistics

[2] "49 Cloud Computing Statistics You Must Know in 2025," N2WS, June 24, 2025. https://n2ws.com/blog/cloud-computing-statistics

[3] Cadre Forensics, "TopMatch-3D High Capacity: 3D Imaging and Analysis System for Firearm Forensics," https://www.cadreforensics.com/pdf/TopMatch-3D-HighCapacity.pdf

[4] "Beyond the Evidence Locker: Mastering Cloud-Based Evidence Management for Modern Law Firms," Katie Wolf, FileVine, September 17, 2024. https://www.filevine.com/blog/beyond-the-evidence-locker-mastering-cloud-based-evidence-management-for-modern-law-firms/

The Solution: Cloud-Native Forensic Annotation Platforms

Cloud-Native Architecture

Definition and Benefits

Cloud-native architecture is an approach to designing, building, and operating applications that fully leverage the advantages of cloud computing platforms. It emphasizes serverless microservices, containerization, and dynamic orchestration—enabling organizations to develop and deploy software in loosely coupled, independently scalable components. Key benefits include:

- **Resilience and Reliability**: Services are self-healing and distributed across multiple nodes, reducing single points of failure and ensuring continuous availability.

- **Cost Efficiency**: Pay-as-you-go models eliminate large upfront hardware investments and allow organizations to pay only for resources consumed.

- **Portability**: Containerized microservices can run across public, private, or hybrid clouds, mitigating vendor lock-in.

Scalability Advantages

Cloud-native systems can auto-scale individual microservices based on demand, thanks to orchestration platforms like Cloudflare or Kubernetes. This fine-grained scalability ensures optimal resource utilization and performance even under unpredictable workloads. Organizations report up to 50% faster scaling times compared to monolithic architectures, with no downtime during scaling events.

Security Considerations

Security is integral to cloud-native design, adopting a Zero Trust model that continuously verifies identities and access rights at every interaction. Cloud-native platforms leverage built-in features—such as pod-level isolation, encrypted service-to-service communication, and automated vulnerability scanning—to reduce attack surface and

enforce compliance controls. Regular automated patching and immutable infrastructure practices further enhance security posture.

Why This Approach Works for Forensics

Real-Time Collaboration Capabilities

Cloud-native platforms support concurrent access and annotation of evidence by multiple examiners, mirroring enterprise collaboration trends. Forensic teams can share case files, add comments, and track changes in real time—eliminating redundant or excessive email exchanges and potentially reducing review cycles from weeks to days.

Centralized Data Management

A unified, cloud-native repository consolidates all digital evidence, analytical metadata, and audit logs in one location. This centralized model simplifies data governance, indexing, and searching across large datasets, ensuring that examiners can retrieve relevant case data within seconds rather than hours.

Enhanced Security and Compliance

By leveraging cloud-native security controls—such as role-based access, end-to-end encryption (EAR and EIT), and immutable audit trails—laboratories can meet stringent regulatory and accreditation standards. Automated compliance checks and policy-as-code frameworks provide continuous monitoring and reporting to satisfy bodies like the FBI Quality Assurance Standards, OSAC, and ISO/IEC 17025.

Improved Accessibility

Investigators, examiners, and legal stakeholders gain secure, remote access to case files from any location, facilitating timely testimony preparation and multi-agency collaboration. Mobile and web clients ensure that critical evidence is available on demand, supporting geographically dispersed teams without VPN or on-premises VPN dependencies.

Technical Innovation

Modern Web Technologies

Cloud-native forensic platforms can employ single-page application frameworks (e.g., React, Vue.js) for responsive user interfaces. An API-first approach ensures that every functionality—image ingestion, annotation, search, user management—is exposed through well-documented RESTful or gRPC endpoints. This design facilitates automation, highly customizable integrations, and developer extensibility.

Integration Capabilities

Cloud-native systems provide open, standardized APIs and event-driven webhooks to integrate seamlessly with laboratory information management systems (LIMS), case management tools, and courtroom presentation software. These integrations enable end-to-end workflow automation—automatically linking evidence capture to chain-of-custody records, report generation, and case file archival without manual intervention.

Striae Platform Overview

Overview

Striae is a cloud-native forensic annotation application purpose-built for forensic firearms examination, delivering unparalleled accessibility, security, and operational efficiency for examiners worldwide. By leveraging Cloudflare's global edge infrastructure, Striae provides authenticated firearm identification confirmations with robust digital signatures and chain-of-custody maintenance, a comprehensive audit trail featuring tamper-evident, AES-256-encrypted logs, and collaborative annotation tools that support multi-examiner workflows with full version control. Its intuitive React and Remix interface, backed by Firebase authentication and TypeScript type safety, ensures a streamlined, compliant, and scalable solution for modern firearms forensic workflows.

Core Capabilities

Authenticated Digital Confirmations

Striae ensures that every case package is cryptographically signed, preserving complete case data integrity and supporting non-repudiation. During confirmation, a digital signature is generated using each examiner's unique cryptographic key and embedded in the confirmation record. The system logs examiner identity, timestamp, checksum verification, and a SHA-256–based signature to guarantee authenticity and immutability.

Chain of custody is maintained by recording every file upload, access, and modification in a single, append-only audit store in Cloudflare R2. Each audit entry includes metadata such as original file ID, upload method, and examiner UID, ensuring complete traceability from image acquisition through final confirmation.

Verification protocols involve multi-factor checks and integrity validation. When a confirmation file is retrieved, Striae re-computes the signature over the recorded data and compares it to the stored signature to detect tampering. Failed validations trigger security alerts and block further actions until re-authentication.

Comprehensive Audit Trail

All user and system actions are captured as structured audit entries, including case creation, annotation edits, PDF generation, and security violations. Each entry contains a workflow phase, result status, and detailed context for traceability.

Entries are tamper-evident, stored in daily JSON files on Cloudflare R2 with AES-256 GCM encryption at rest. Immutable append-only logs ensure that any modification attempt is detectable via cryptographic checksums.

Compliance reporting is facilitated through built-in audit trail export services. Auditors can generate detailed CSV or JSON structured data, or human-readable summary reports that include total events, success/failure counts, and security incident summaries, all filtered by date range or case number.

Collaborative Annotation

Striae supports real-time annotation of comparison images with synchronized updates across all databases. The Box Annotation uses a percentage-based coordinate model to ensure consistent annotation placement on varying display sizes and PDF exports.

Multi-examiner workflows enable consistent access to the same case data. Examiner actions (create/edit/delete annotation) are logged immediately and propagated via Cloudflare Workers, maintaining consistency and preventing conflicts.

Complete case data transfer is built into the case export process. JSON and CSV exports include all annotation data and timestamps, while ZIP packages preserve all case data and images in read-only mode for secure review and confirmation. The audit trail captures version control, recording complete previous versions of edited annotations and timestamps.

Technical Architecture

Cloud Infrastructure (Cloudflare)

Striae is built on Cloudflare's edge computing platform, leveraging Workers for microservices and R2 for persistent storage.

- Workers handle authentication, image processing, PDF generation, data storage, and audit logging across seven specialized microservices. Worker-to-Worker communication uses custom API keys retrieved from a dedicated authentication worker and validated via X-Custom-Auth-Key headers.

- Access requests are strictly limited to Striae's domain with Cross Origin Resource Sharing (CORS) support.

- R2 provides globally distributed, durable object storage (11 9s annual durability) for case files, annotations, and audit trails.

- KV is used for low-latency user profile and case list data.

- Cloudflare Images delivers optimized, tamper-evident, and temporary access-controlled images via signed URLs.

Security Implementations (AES-256 Encryption)

All data at rest in R2 and KV is encrypted using AES-256 GCM. Integrity checks via checksums guard against tampering. Communications between client and Workers occur over HTTPS/TLS, and signed URLs ensure time-limited, secure image access.

Authentication Systems (Firebase)

User authentication is managed through Firebase Authentication with email/password, multi-factor authentication (MFA) support, and JWT token issuance for frontend API calls.

Development Stack (React, Remix, TypeScript)

The frontend is built with React and Remix for full-stack routing and data loading, styled using Tailwind CSS and CSS Modules. TypeScript ensures type safety across components and shared API types. Vite powers the development build, with deployment to Cloudflare Pages and automated CI/CD pipelines.

User Experience

Intuitive Interface Design

Striae features a minimalist, intuitive, and examiner-focused UI. The sidebar provides case and file management, while the toolbar offers annotation visibility and PDF export tools with clear icons. Contextual tooltips and color-coded controls guide examiners through annotation workflows.

Accessibility Features

Striae adheres to WCAG guidelines with semantic HTML, ARIA labels, and full keyboard navigation. Color contrast ratios are maintained for annotation overlays. Modal dialogs trap focus and are escapable, and toast notifications announce success/failure to assistive technologies.

Benefits and Impact

For Individual Examiners

Striae empowers examiners to work more efficiently by automating routine tasks such as case exports, annotation and label placement, report generation, and digital authenticated confirmations. Examiners spend less time on manual processes like organizing images, adding labels and annotations, and data formatting, allowing them to focus on analytical judgment. Paper reports can be printed after confirmations are finalized, streamlining casework flow. The platform's organized workspace and integrated notes ensure that all case data is easily accessible and directly linked to specific files, reducing the risk of overlooked details. By minimizing repetitive steps and centralizing information, Striae enhances accuracy and reduces clerical errors.

For Forensic Laboratories

Laboratories gain a unified, standardized workflow for firearms identification, promoting consistency across cases and examiners. Near-real-time collaboration tools eliminate the need for ad-hoc file exchanges, reducing version conflicts and synchronization delays. Striae's cloud-native architecture significantly lowers upfront infrastructure costs and scales on demand, enabling labs to rapidly onboard new users without procurement delays. Fewer manual processes translate into reduced labor costs and faster turnaround times, improving overall throughput.

For the Justice System

By accelerating case processing and report delivery, Striae helps prosecutors and defense teams receive forensic findings sooner, which can shorten pretrial phases and reduce case backlogs. Standardized, professionally formatted, and authenticated reports—complete with digital signatures and easily accessible, tamper-evident audit trails—enhance the credibility of evidence presentation in court. Faster delivery of reliable forensic results increases stakeholder confidence and optimizes utilization of both laboratory and judicial resources.

Potential Measurable Outcomes

Cost Savings Example for a Forensic Laboratory

Assumptions

- Examiners: 6 (each salary $70,000/year)
- Workload: 10 firearms identification cases per examiner per month
- Evidence per case: 6 fired bullets and 6 fired cartridge cases
- Comparisons (ideally) per case:
    - Bullets: $n - 1 = 5$
    - Cartridge cases: $n - 1 = 5$
    - **Total comparisons:** 10 per case
- Documentation time per comparison:
    - Traditional: 5 minutes
    - Striae: 0.5 minutes (30 seconds)
- Work hours per year: 2,080 (52 weeks × 40 hours)
- Hourly rate: $70,000 ÷ 2,080 ≈ $33.65

Workflow Comparison

Metric	Traditional Workflow	Striae Workflow	Time Saved per Case
Comparisons per case	10	10	–
Time per comparison	5 min	0.5 min	4.5 min
Documentation time per case	50 min (0.83 h)	5 min (0.08 h)	45 min (0.75 h)
Monthly cases per examiner	10	10	–

Annual Time & Cost Savings

Metric	Value per Examiner	Total for 6 Examiners
Monthly time saved	10 cases × 0.75 h = **7.5 h**	7.5 h × 6 = **45 h**
Annual time saved	7.5 h × 12 = **90 h**	90 h × 6 = **540 h**
Hourly rate	$70,000 ÷ 2,080 ≈ **$33.65**	–
Annual cost saved	90 h × $33.65 ≈ **$3,028.50**	$3,028.50 × 6 ≈ **$18,171**

Intangible Benefits

- **Backlog Reduction:** Faster documentation accelerates case throughput, reducing evidence backlogs and improving lab turnaround times.
- **Enhanced Reputation:** Consistent, auditable outputs bolster credibility with prosecutors, defense attorneys, and courts.
- **Employee Effectiveness & Retention:** Reduced repetitive work increases job satisfaction, lowers burnout risk, and aids retention of skilled examiners.
- **Scalability:** Time savings free capacity for higher-value tasks and accommodate growth in caseload without proportional staffing increases.

Upfront Savings

The Striae platform is completely free to use.

The Origins of Striae

Through his experience as a forensic firearms examiner, Stephen encountered a critical bottleneck in the comparison workflow: making detailed, concurrent annotations on comparison images was both cumbersome and inefficient. Existing methods forced examiners to print images separately from the comparison workflow and mark them up by hand, providing no streamlined way to link annotations directly to the digital evidence. This time-consuming process could take up to an hour per casefile, especially in complex investigations.

Stephen envisioned a better way. Striae was created to streamline forensic comparison workflows by providing an intuitive, cloud-based platform for direct digital annotation and evidence linking. With Striae, examiners can quickly annotate comparison images, seamlessly associate notes with specific evidence, and create well-formatted reports, all in the same workflow environment. Striae transforms painstaking manual tasks into an efficient, integrated digital process, empowering examiners to focus on what matters most: analysis and reporting.

Striae is one of the first, and potentially the very first, cloud-native forensic annotation applications built specifically for forensic firearms examination—a highly specialized area seldom addressed by existing forensic technology platforms. This innovative solution harnesses global cloud infrastructure (leveraging Cloudflare) to deliver unmatched capabilities in accessibility, security, and operational efficiency for firearms examiners worldwide.

About the Developer

Lead Developer

Stephen J. Lu, EMBA, SHRM-CP

Stephen is a lifelong programmer who began his journey with BASIC and Turbo Pascal. During high school, he helped the Programming Club create the school's first website, and his first personal website—featuring detailed starship specifications and histories from Star Trek—was hosted by GeoCities in the 1990s.

Throughout his forensic career, Stephen has analyzed over a thousand cases and participated in hundreds of death investigations, including homicides, suicides, officer-involved shootings, autopsies, and custodial deaths. Most recently, he served for ten years as a Criminalist with the San Diego County Sheriff's Department, specializing in forensic biology, forensic firearms analysis, and crime scene investigation and reconstruction.

Stephen also spent six years as a contract assessor and trainer with the National Forensic Science Technology Center (now FIU Global Forensic and Justice Center), where he performed DNA laboratory audits and taught courses on DNA amplification, likelihood ratios, and population statistics. Prior to that, Stephen worked with the Arizona Department of Public Safety, performing casework in Forensic Biology, and the California Department of Justice's Richmond DNA Lab, where he contributed to the FBI's Combined DNA Index System (CODIS).

Over his career, Stephen has completed more than 2,000 hours of professional training in areas such as forensic biology, forensic firearms analysis, trajectory analysis, bloodstain pattern analysis, and courtroom testimony. He has testified as an expert witness in superior courts in Arizona and California, and in federal court for the U.S. District Court for the Central District of California. Stephen's courtroom experience has been noted for his ability to explain complex scientific concepts in an understandable and engaging way for juries and attorneys alike.

In addition to his forensic science work, Stephen served as the Regional Director South for the California Association of Criminalists (CAC), where he organized regional study groups and hosted presentations by experts, including a keynote address by Jeff Udvarhelyi, an Escondido Police Department Child Abuse Detective, on a significant child abuse case. As the Lead Webmaster for the CAC, he enhanced the organization's public presence by overhauling its website for better communication and engagement.

Since retiring from active casework, Stephen has shifted his focus towards leadership development in forensic science. His interest in leadership and public education is reflected in his recent book, *CSI to CEO*, where he covers forensic science topics such as DNA analysis, crime scene investigation, bloodstain pattern analysis, and forensic leadership for a general audience. In 2023, Stephen had the honor of graduating from the FBI San Diego's Citizens Academy as a demonstration of his continued dedication to public service. In 2025, he developed and shipped Striae, a modern web app that streamlines comparison image annotation for forensic firearms examiners.

He is an active member of the Association of Firearm and Tool Mark Examiners, the California Association of Criminalists, and the International Association for Identification, bringing decades of forensic expertise and technological innovation to the development of Striae.

Stephen holds an Executive MBA with Honors from Quantic School of Business and Technology and a Bachelor of Science with Honors, *magna cum laude*, in Biochemistry and Molecular Biophysics and Molecular and Cellular Biology from the University of Arizona. Stephen is a Society for Human Resource Management Certified Professional (SHRM-CP). In addition, he is a member of Phi Beta Kappa, an honor society recognizing exceptional academic achievements in the humanities, social sciences, natural sciences, and mathematics.

Further Reading

- **Cloudflare Security Documentation:**
  - Cloudflare R2 Data Security - Details on AES-256 encryption with GCM mode for object storage
  - Cloudflare KV Data Security - Details on AES-256 encryption with GCM mode for key-value storage
- **Government and Standards Documentation:**
  - The Organization of Scientific Area Committees for Forensic Science (OSAC)
  - ISO/IEC 17025: Testing and Calibration Laboratories
  - NIST SP 1319: Strategic Opportunities to Advance Forensic Science in the United States: A Path Forward Through Research and Standards
  - NIST Advanced Encryption Standard (AES) - Official NIST specification for AES encryption
  - NIST FIPS 197 - Federal approval and technical specifications for AES
  - NSA Commercial Solutions for Classified - Government approval of AES-256 for classified information
- **Cryptographic Analysis and Security Research:**
  - Cryptographic Analysis of AES-256 - Academic research on AES-256 security properties
  - Schneier on Cryptography - Expert analysis of AES security and brute force resistance
  - NIST FIPS 140-2 - Cryptographic module validation standards
- **Industry Adoption and Trust:**
  - Cloudflare Trust Hub - Comprehensive security and compliance information
  - Cloudflare Compliance Resources - Industry certifications and compliance documentation
  - Cloudflare Learning: What is Encryption? - Educational resource on encryption fundamentals