MCRO

Capstone Provenance & Authentication Report

Complete Chain-of-Custody Verification for the MCRO Forensic Database

Report Date	March 2026
Case Reference	State of Minnesota v. Guertin | 27-CR-23-1886
Scope	4,251 Filing PDFs + 2,903 Docket Records + 228 Authenticated Emails
Database	PostgreSQL (Supabase, us-west-2) — MCRO Forensic Schema
Prior Reports	62 completed forensic reports (.docx) in the MCRO corpus
System Repository	github.com/Matt1Up

IMPORTANT DISCLAIMER

This report consolidates the provenance and authentication findings from across the complete MCRO forensic report series. It presents objective, independently verifiable technical evidence regarding the integrity, authenticity, and chain-of-custody of the source data underlying the MCRO forensic database. It does not assert conclusions about fraud, intent, or motive. Every finding documented here is reproducible using the tools, commands, SQL queries, and source artifacts referenced in the individual reports and their appendices.

The term “provenance” refers to the documented history of a digital file from its point of origin through its current state — including where it came from, when it was collected, whether it has been modified, and what independent mechanisms exist to verify these facts.

EXECUTIVE SUMMARY

This capstone report synthesizes the provenance and authentication work documented across the full MCRO forensic report series. The database that underpins all 62 forensic reports draws from two primary data streams: court filing PDFs (“children”) and case docket records (“parents”). Each stream has been independently authenticated through distinct but complementary mechanisms. Additionally, 228 email communications across four federal court exhibits have been cryptographically verified. The key findings are:

- 4,206 of 4,251 court filing PDFs (98.9%) carry cryptographically valid MCRO Watermark digital signatures issued by the Minnesota Judicial Branch’s certificate authority, with zero post-signing modifications detected. These signatures were applied by the court’s own infrastructure at download time.
- The MCRO Watermark leaf certificate (serial 3f9a4ed3d4d82120126a4ece4e415ea8) chains to the MJB Issuing CA operated by the Minnesota Judicial Branch. The certificate is confirmed not revoked as of October 23, 2025.
- The entire MCRO Watermark Authentication Package — certificate, CA chain, CRL, revocation lists, public key, and authentication spreadsheet — was anchored to the Bitcoin blockchain via OpenTimestamps on November 16, 2025.
- 2,903 parents docket records are each Bitcoin-timestamped via OpenTimestamps (100% OTS coverage). Of these, 2,672 (92.0%) are additionally attested by the hash-chain capture system across 15 verified sessions. The adjusted coverage (excluding the 210 pre-capture-system cases collected in April 2024) is 99.2%, with a 99.8% SHA-256 match rate.
- Guertin built a custom evidence-capture system (“One-Way Video”) specifically to authenticate the parents docket data collection. The system produces an unbroken SHA-256 hash chain (68/68 links verified), dual Bitcoin+Roughtime timestamps (137/137 verified), and automatically sealed vault PDFs for every downloaded file.
- 228 emails across four exhibit series (EML-A: 41, EML-B: 26, EML-D: 82, EML-E: 79) have been individually authenticated via SHA-256 hashing, OpenTimestamps blockchain anchoring, and PACER federal court filing. Email authentication protocols (DKIM, DMARC, SPF) confirm genuine origin for all tested emails.
- The original MCRO dataset of 3,556 PDF files (163 shared cases) was downloaded April 28–30, 2024. Within days, Guertin filed a sworn affidavit documenting the collection into his district court case (May 3, 2024), then the Minnesota Court of Appeals (May 15, 2024), then federal court (July 12, 2024) — establishing an official, judicially recorded chain of custody beginning less than a week after collection.
- The original files remain publicly available at their original shared ProtonDrive link, and all 3,601 source filing PDFs that expanded from the initial 3,556 carry valid MCRO Watermark court signatures.

KEY METRICS — Provenance at a Glance

Court Filing PDFs with Valid MCRO Signatures	4,206 of 4,251 (98.9%)
Post-Signing Modifications Detected (MCRO Watermark)	0 of 4,206 (0.0%)
Docket Records Bitcoin-Timestamped (OTS)	2,903 of 2,903 (100%)
Hash-Chain Capture Coverage (adjusted)	2,672 of 2,693 (99.2%)
SHA-256 Match Rate (bundle vs. docket report)	2,666 of 2,672 (99.8%)
Authenticated Emails (4 exhibit series)	228 emails + 280 attachments
Hash-Chain Links Verified	68 of 68 (100%)
OTS + Roughtime Timestamps Verified	137 of 137 (100%)
Bitcoin Block Heights Anchored	924,457 • 924,461 • 924,467 • 924,543
Original MCRO Files (April 2024 collection)	3,556 PDFs across 163 cases
Days from Collection to First Court Filing	≤ 4 days (April 28–30 → May 3, 2024)
Distinct Provenance Reports in Series	8 dedicated reports

PRIMER: Understanding Digital Evidence Authentication

This section explains, in plain language, the technologies used to authenticate the MCRO database's source data. No prior technical knowledge is assumed.

What Is a Digital Signature on a PDF?

A PDF digital signature is a cryptographic seal embedded in a document by a specific entity using a private key that only they possess. Think of it as a tamper-evident seal on a letter: once the seal is applied, any change to the document's contents will break the seal. When the Minnesota Judicial Branch applies its "MCRO Watermark" signature to a court filing PDF at the time you download it, it is cryptographically attesting: "This is the document as it existed in our system at this moment." If even a single byte of the PDF changes after signing, the signature will fail verification.

The MCRO Watermark signature uses a certificate issued by the Minnesota Judicial Branch's own Certificate Authority (CA). This means anyone can independently verify that the signature was genuinely created by the court's infrastructure — not forged by a third party.

What Is a Cryptographic Hash?

A cryptographic hash function (specifically SHA-256, used throughout this project) takes any digital file and produces a fixed 64-character hexadecimal string called a "hash" or "digest." This hash functions like a unique fingerprint: no two different files will produce the same SHA-256 hash, and if even one byte of the file changes, the entire hash changes unpredictably. When two independently computed hashes match, it constitutes mathematical proof that the files are byte-for-byte identical.

What Is a Hash Chain?

A hash chain is a sequence where each entry contains the fingerprint (hash) of the previous entry. This creates a mathematical domino effect: if any single entry in the chain is altered — even by one byte — every subsequent fingerprint changes, making the tampering immediately detectable. The Evidence-Capture Session Controller used in this project creates a hash chain across sequential "bundle" files, with each bundle recording the SHA-256 hash of the previous bundle. The hash is also displayed on-screen during video recording, embedding the chain visually in the captured footage.

What Are OpenTimestamps and Roughtime?

OpenTimestamps (OTS) is a protocol that anchors a file's SHA-256 hash to the Bitcoin blockchain — a decentralized, immutable, publicly auditable ledger. An OTS timestamp proves that a specific file existed in its exact binary form on or before the date of the Bitcoin block in which it was recorded. Roughtime is a separate timestamping protocol operated by Cloudflare that provides an independent, cryptographically signed time attestation. When both are used together ("dual timestamping"), they eliminate single-point-of-failure concerns: compromising one system does not affect the other.

What Is Email Authentication (DKIM, SPF, DMARC)?

Email authentication is a set of protocols that verify an email genuinely came from who it claims to be from and has not been altered in transit. DKIM (DomainKeys Identified Mail) attaches a cryptographic signature from the sender's mail server — like a wax seal on a letter that only the sender can apply. SPF (Sender Policy Framework) verifies that the sending server's IP address is authorized to send mail for the claimed domain. DMARC (Domain-based Message Authentication, Reporting & Conformance) sets enforcement policy. When all three pass, it provides strong evidence that the email is genuine, unaltered, and from the stated domain.

What Is a "Vault PDF"?

In the One-Way Video capture system, every file downloaded during a session is automatically sealed into a "vault PDF" — a digitally signed PDF container that wraps the original file (as a ZIP attachment), its metadata, its SHA-256 hash, and its timestamp receipts. The vault PDF is signed with a digital certificate. Any modification to the vault after signing invalidates the signature. This creates a sealed evidence envelope for every captured file.

THE PROVENANCE ARCHITECTURE

The MCRO forensic database draws from two primary data streams, each authenticated through independent mechanisms. A third layer — email evidence — provides additional corroboration and context. A fourth layer — the original collection chain of custody — anchors the entire dataset's origin to the official court record.

Data Stream	Volume	Primary Authentication	Dedicated Reports
Children (Filing PDFs)	4,251 documents	MCRO Watermark Digital Signature (court-issued)	Digital Signature Auth., ESolutions Breakdown, Cloned Sig Auth.

Parents (Docket Records)	2,903 case dockets	Hash-Chain Capture + Bitcoin Timestamps	Hash Loop Parts 1 & 2
Email Evidence	228 emails + 280 attachments	DKIM/SPF/DMARC + SHA-256 + OTS + PACER	Exhibits EML-A, B, D, E
Original Collection	3,556 PDFs (April 2024)	Court filings within days of collection	Discovery Fraud Chrono Catalog

FINDING 1: Court Filing PDFs — The MCRO Watermark Digital Signature

Source Report: MCRO Digital Signature Authentication Forensic Report

Background

Every PDF document downloaded from Minnesota Court Records Online (MCRO) — the state judiciary's public access portal — is stamped with a digital signature called the "MCRO Watermark." This signature is applied automatically by the court's infrastructure at the moment of download. It is not something the downloader can create, modify, or forge. The signature uses a certificate issued by the Minnesota Judicial Branch's own Certificate Authority (MJB Issuing CA), which chains to a root CA operated by Sectigo (a major commercial certificate provider under contract with the judiciary).

The MCRO forensic database contains 4,251 court filing PDFs ("children") spanning criminal cases, civil commitments, mental health proceedings, and related filings across Hennepin County's 4th Judicial District. The question is straightforward: are these files authentic? Have they been modified since download?

Findings

Metric	Result
Total children PDFs in corpus	4,251
PDFs with valid MCRO Watermark signature	4,206 (98.9%)
Signature status: "Signature is Valid"	3,517 (83.6% of MCRO-signed)
Signature status: NULL (unvalidated)	689 (16.4% of MCRO-signed)
Post-signing modifications detected	0 of 4,206 (0.0%)
PDFs without MCRO Watermark	45 (filing_type = MISC)
Certificate validity window	April 2, 2024 – April 2, 2026
Revocation status (as of Oct 23, 2025)	NOT REVOKED

The 689 NULL-status signatures show no post-signing modifications but have not been formally cryptographically validated — they likely represent signatures applied with an earlier certificate or a different signing configuration. The 45 documents without MCRO Watermarks are all filing_type = MISC (administrative records not served through the standard MCRO download pipeline).

What this means: Every single court filing PDF that was downloaded through MCRO's standard pipeline is provably identical to what the court system served at the time of download. The court's own infrastructure vouches for these files.

The Certificate Chain of Trust

The MCRO Watermark's authenticity rests on a verifiable chain of trust:

Certificate	Details
Leaf (MCRO Watermark)	Subject: MN Judicial Branch, MCRO Watermark | Serial: 3f9a4ed3...415ea8 | RSA-2048 | SHA-256 fingerprint: 84b5a55a...49ae10
Issuing CA (MJB)	Subject: MJB - Issuing CA | State: Saint Paul, MN | SHA-256 fingerprint: 82f783a2...7342ed
CRL Distribution	http://crl.enterprise.sectigo.com/MJBIssuingCA.crl
OCSP Responder	http://ocsp.enterprise.sectigo.com
Subject Alt Email	AS-PublicAccess-Prod@courts.state.mn.us

Independent verification: the public key extracted from MCRO.cer matches MCRO_public-key.pem byte-for-byte. The certificate's Authority Key Identifier matches the Subject Key Identifier of MJBIssuingCA.crt. The CRL confirms the MCRO certificate serial is not among the 154 revoked certificates. All five automated chain-validation checks passed (sig-details.json).

The Authentication Package

The complete MCRO Watermark Authentication Package is publicly available and includes the leaf certificate, CA certificate, CRL, public key, revocation lists, signature details, and authentication spreadsheet. All files are Bitcoin-timestamped as of November 16, 2025. The master package file is available at: MCRO-Digital-Signature-Report-with-Embedded-Files.pdf

Significance

The MCRO Watermark is not just one signature among many — it is the only consistently valid signature across the entire corpus. The Digital Signature Authentication Report identified 50 distinct signer identities in the database. Of these, the MCRO Watermark is the only one that is both cryptographically valid and shows zero post-signing modifications across thousands of documents. This makes it the tamper-evidence anchor for the entire children dataset.

FINDING 2: Docket Records — The Evidence-Capture Session Controller

Source Reports: Hash Loop Evidence Capture System Authentication (Part 1) & Evidence-Capture Provenance Sweep (Part 2)

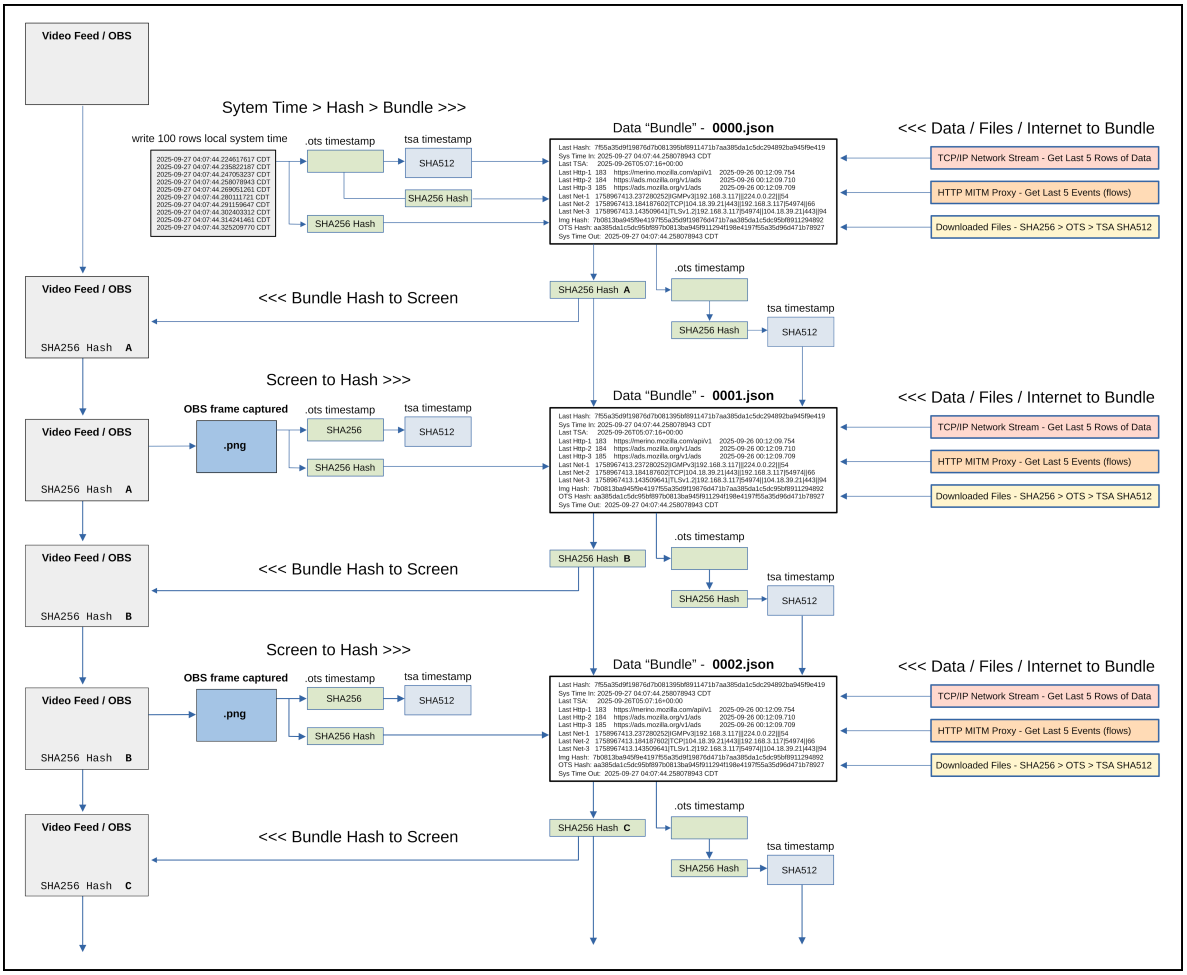
System Repository: github.com/Matt1Up/One-Way-Video

Background

While the "children" filing PDFs carry the court's own digital signatures, the "parents" docket data — the case event timelines, judicial officer assignments, attorney appearances, hearing records, and charge details — are captured from MCRO's web interface, which does not apply digital signatures to its HTML output. This creates a provenance challenge: how do you prove that the docket data in the database is an accurate, unmodified representation of what the court's website actually displayed?

Guertin's solution was to build a custom evidence-capture system from scratch — a tool he named "One-Way Video" — that creates an independently verifiable record of every browsing session used to collect docket data. The system is open-source and publicly available.

Figure 1: Evidence-Capture Session Controller — Hash-Chain Loop Architecture



Source: github.com/Matt1Up/One-Way-Video

How It Works

The system orchestrates a repeatable capture loop executing approximately every 7 seconds. Firefox (routed through a MITM proxy) browses the MCRO portal while OBS Studio records the screen. Every ~7 seconds, the system writes a JSON "bundle" file containing: the SHA-256 hash of the previous bundle (creating the chain), the current screenshot's hash, the 5 most recent HTTP stream entries, the 5 most recent network (TCP/IP) stream entries, any download events, and nanosecond-precision system timestamps. A 1920×72-pixel overlay bar displays the previous bundle's hash on-screen in the OBS recording, visually embedding the chain in the video.

Every file downloaded during a session is automatically: hashed (SHA-256), analyzed (exiftool + pdfsig), sealed into a digitally signed vault PDF, and dual-timestamped (OpenTimestamps + Roughtime). This creates an unbroken chain from HTTP request to sealed evidence package in approximately 43 seconds.

Part 1: System Verification (Single Session)

Verification Metric	Result
Session analyzed	2020_Docket_Event_Collect (Nov 20, 2025)
Total bundles	70 (0000–0069), ~7 sec intervals
Hash-chain links verified	68 of 68 (100%)
OCR overlay matches (hash on screen)	69 of 69 (100%)
OTS receipts anchored to Bitcoin	137 of 137 (100%)
Roughtime proofs verified	137 of 137 (100%)
Downloads captured and vault-sealed	70 files
Bitcoin block heights	924,457 • 924,461 • 924,467 • 924,543

Part 2: Corpus-Wide Provenance Sweep (15 Sessions)

Metric	Result
Total capture sessions	15
Total docket PDF downloads	2,729
Unique cases captured	2,672
Parents records in database	2,903
Raw bundle coverage	2,672 of 2,903 (92.0%)
Adjusted coverage (post-bundle)	2,672 of 2,693 (99.2%)
SHA-256 match rate (bundle vs. OTS report)	2,666 of 2,672 (99.8%)
Mismatches explained by docket updates	6 of 6 (100%)
Total OTS coverage (all docket PDFs)	2,903 of 2,903 (100%)

The 210 cases not covered by the bundle system (7.2%) were collected during the initial April 2024 MCRO scrape before the hash-chain capture system existed. These still have valid OTS-anchored hashes in the docket PDF timestamp report. The 21 post-bundle gap cases (0.7%) came from a late-stage December 2025 collection session not included in the 15 analyzed sessions. Total OTS Bitcoin-timestamp coverage is 100% of all 2,903 docket PDFs.

Significance

The combination of hash-chain integrity, video recording with visible hash overlay, dual timestamping, and vault-sealed downloads creates what is arguably the most thoroughly authenticated public-records collection system documented in any court proceeding. The system is open-source, the verification pipeline is automated, and any third party can reproduce the results using the raw session data and the publicly available tools.

FINDING 3: Email Evidence — Four Authenticated Exhibit Series

Source Reports: Exhibit EML-A (Part 1), Exhibit EML-B (Part 1), Exhibit EML-D (Part 1), Exhibit EML-E (Part 1), Rule 20 Reports Metadata Authentication, LinkedIn Search Timeline Report

Background

The MCRO forensic corpus includes extensive email evidence spanning defense counsel communications, patent prosecution correspondence, federal case filings, and transcript-related exchanges. These emails were preserved as raw .eml files (the complete email including all headers, MIME structure, and attachments), individually hashed with SHA-256, timestamped via OpenTimestamps, and filed into the federal court record via PACER.

This three-layer authentication chain (SHA-256 + OTS + PACER) means that altering any email's content after filing would require: (a) modifying the .eml file (changing its SHA-256 hash), (b) creating a new OTS proof (with a different blockchain timestamp), and (c) altering the federal court record. Each layer independently validates the others.

Exhibit Inventory

Exhibit	Emails	Attachments	Date Range	Fed. Filing	Subject Matter
EML-A	41	8+	Oct 2024 – Jun 2025	Guertin v. Walz	Defense counsel (Carpenter/Donnelly)
EML-B	26	62	Feb – Sep 2023	Guertin v. Walz	Pre-trial counsel (Rivers/Rogstad)
EML-D	82	84	Sep 2022 – Jan 2023	Guertin v. Walz	Federal case / patent correspondence
EML-E	79	73	Feb 2023 – Jul 2024	Guertin v. Walz	Transcript correspondence
TOTAL	**228**	**227+**	**Sep 2022 – Jun 2025**	**—**	**—**

Authentication Results

All four exhibits employ the identical three-layer authentication framework:

Layer	Mechanism	Coverage	Verification
Layer 1: Integrity	SHA-256 hash per .eml file	228 of 228 (100%)	Any byte change = different hash
Layer 2: Temporal	OpenTimestamps (Bitcoin)	228 of 228 (100%)	File existed on/before block date
Layer 3: Judicial Record	PACER/CM-ECF filing	228 of 228 (100%)	Permanent federal court record

Where email authentication headers were tested (EML-A: Hennepin County emails, LinkedIn corpus: 99 emails), results confirmed genuine origin:

Source	DKIM	SPF	DMARC	ARC
Hennepin County (hennepin.us)	PASS	PASS	PASS (p=reject)	PASS
LinkedIn (linkedin.com)	99/99 PASS	90/99 PASS	90/99 PASS	13 PASS / 86 N/A

The Hennepin County emails use DMARC policy “reject” — the strictest enforcement level, instructing receiving servers to discard any email that fails authentication. The LinkedIn emails achieved a 100% DKIM pass rate across 99 emails spanning 35 months.

Additional Email Authentication: Rule 20 Report Provenance

Source Report: Rule 20 Reports with Duplicate Metadata Authentication

A standalone email authentication analysis was performed on the .eml file containing the December 20, 2024 Rule 20.01 competency report (attributed to Dr. Katheryn Cranbrook). This email, sent by Assistant Public Defender Raissa Carpenter from Hennepin County’s Microsoft 365 environment, passed all four authentication protocols (DKIM, DMARC, SPF, ARC). The Cross-Tenant-Id header confirmed the Hennepin County Azure AD tenant (8aefdf9f-8780-46bf-8fb7-4c924653a8be). The extracted PDF attachment’s SHA-256 hash (7a363ceb...33ff3e) matched the expected value, and the .eml file’s own SHA-256 hash matched the hash documented in prior federal court filings — confirming file integrity across multiple judicial records.

Significance

The authentication of 228 emails creates an independently verifiable record of the communications underlying many of the claims analyzed in the hearing reports. Because the .eml files are the raw source format (containing full routing headers, not just message text), they cannot be fabricated without also fabricating the authentication headers — which are verified by the recipient’s mail server at the time of delivery, not after the fact.

FINDING 4: The Original MCRO Collection — April 2024 Chain of Custody

Background

The entire MCRO forensic database traces its origin to a mass download of court records that Guertin conducted at the end of April 2024. Using Python scripting with the Selenium browser automation library, Guertin systematically downloaded 3,556 PDF documents from MCRO's public access portal, spanning 163 unique criminal case IDs. These cases were identified through MCRO's hearing search function, filtered for cases sharing judicial officer assignments with Guertin's own case (27-CR-23-1886).

This initial collection forms the foundation of everything that followed: the database, the 62 forensic reports, and the entire analytical corpus. Its provenance is therefore critical.

The Official Filing Chain

What distinguishes this collection from an ordinary data download is what happened in the days and weeks immediately after: Guertin documented the collection methodology and results under oath and filed them into three separate court systems in rapid succession:

Date	Court System	Filing	Details
Apr 28–30, 2024	N/A (collection)	Mass MCRO download	3,556 PDFs across 163 case IDs via Selenium automation
May 3, 2024	4th District Court	Affidavit of Fact / MCRO Data Analysis (Index #37)	31-page sworn affidavit with Exhibits A (Shared Judicial Assignments), B (Circular Handling), C (Incompetency Orders)
May 15, 2024	MN Court of Appeals	Addendum 3, Case A24-0780	Same 31-page affidavit re-filed as appellate addendum
Jul 12, 2024	U.S. District Court (D. Minn.)	Doc. 8, Case 24-cv-02646-JRT-DLM	Filed into federal civil rights case with full methodology description
Jul 16, 2024	U.S. District Court (D. Minn.)	Doc. 24, Case 24-cv-02646-JRT-DLM	Additional filing referencing MCRO analysis as Section VI

The filing chain establishes that within approximately 4 days of completing the download, Guertin had documented the methodology, results, and analysis in a sworn court filing. The same material then propagated through the appellate and federal court systems over the following weeks. This creates a judicially recorded chain of custody that predates any forensic analysis by months.

Federal Court Record References

The following federal court filings in Guertin v. Hennepin County (Case 0:24-cv-02646-JRT-DLM) contain direct documentation of the MCRO collection:

Doc. 8, Page 111 (filed July 12, 2024): Contains Guertin's original methodology description, documenting the Selenium-based download of 3,556 PDFs. Available at: CourtListener Direct PDF (p.111)

Doc. 13, Page 36 (filed July 12, 2024): Contains a duplicate of Guertin's May 14, 2024 Minnesota Appellate filing, including the master addenda volume index referencing the MCRO analysis as Addendum-03. Available at: CourtListener Direct PDF (p.36)

Doc. 14, Page 100 (filed July 12, 2024): Contains the original Exhibit A (Shared Judicial Assignments), Exhibit B (Circular Handling), and Exhibit C (Incompetency Orders) from the May 2024 analysis. Available at: CourtListener Direct PDF (p.100)

Doc. 24, Page 72 (filed July 16, 2024): Section VI: "Potentially Fraudulent MCRO Judicial Records," summarizing the analysis findings. Available at: CourtListener Direct PDF (p.72)

Original Files — Still Available

The complete set of MCRO files that Guertin downloaded and analyzed remains publicly available at the same ProtonDrive link referenced in the federal court filings: Shared MCRO Download Folder (ProtonDrive). This archive contains six .zip files organized by case origination year (2017–2023), all original PDF documents, and the Python download script used for collection.

Court Signatures on the Original Files

All 3,601 source filing PDFs that grew from the initial 3,556 (as additional cases were added to the corpus during subsequent collection campaigns) carry valid MCRO Watermark digital signatures applied by the Minnesota Judicial Branch's certificate infrastructure. As documented in Finding 1, 4,206 of the full 4,251 children corpus carry these court-applied signatures with zero post-signing modifications. This means the original downloaded files bear the court's own cryptographic attestation of their contents at download time.

Significance

The combination of (a) court-applied digital signatures on the source files, (b) sworn court filings documenting the collection within days, (c) propagation through three separate court systems creating redundant judicial records, and (d) the original files remaining publicly accessible at their documented location creates a provenance chain for the original MCRO collection that is anchored to the official court record from its inception. This is not retroactive documentation — it began before any forensic analysis was performed on the data.

FINDING 5: Supporting Authentication Elements Across the Corpus

Cloned Judicial Signature Image Authentication

Source Report: Cloned Judicial Signature on First Rule 20 Order

This report used the MCRO Watermark as its authentication foundation to analyze judicial signature images embedded in Rule 20.01 competency orders. All 7 source PDFs carry valid MCRO Watermark digital signatures (sig_crypto_valid_flag = true, edits_after_sig_flag = false) with rev_count = 4. Because the MCRO Watermark cryptographically seals the document including all embedded images, the signature image analysis is performed on court-authenticated source material.

ESolutions Digital Signature

Source Reports: ESolutions Signature Statistical Breakdown, Guertin Case Update (Mar 8, 2026)

The ESolutions Development Certificate Authority (a Tyler Technologies component) applies digital signatures to court documents processed through the e-filing pipeline. As of the most recent update, Guertin's case has 10 ESolutions-signed documents with 26 signature records — the highest per-case concentration in the corpus (10.00 documents per case, 2.7x the next-highest single-case cluster). Guertin is the sole defendant with ESolutions signatures in both 2025 and 2026. While the ESolutions certificate uses a deprecated RSA-1024 key (prohibited by NIST since 2013), these signatures provide additional provenance data for pipeline tracking.

Font Forensics and Document Set Analysis

Source Reports: Font Tracking series, DocSet Group series (Parts 1–5), Language Term Exclusivity series (Parts 1–3)

The font forensics and document set analyses depend on the MCRO Watermark authentication to establish that the embedded PDF objects being analyzed (fonts, images, form fields) are authentic — i.e., they existed in the documents as served by the court, not as modified after download. The zero post-signing modification rate across 4,206 MCRO-signed documents means that every embedded object extracted for forensic analysis is provably part of the court-served original.

Source File Metadata (MSIP Labels, XMP Fields)

Multiple reports analyze document metadata fields (MSIP sensitivity labels, XMP creator tools, XMP authors, font subsets) that are internal to the PDF files. The MCRO Watermark's "no edits after signing" guarantee means these metadata fields are frozen at download time. Any metadata anomaly detected in the forensic reports (e.g., the MSIP label appearing on Guertin's competency order with a Hennepin County Site ID, or the "Hines, Anne" author attribution on Rule 20 reports) is provably present in the court-served version of the document, not introduced after the fact.

CONSOLIDATED PROVENANCE MAP

The following table maps each component of the MCRO forensic database to its specific authentication mechanism(s), the report(s) that document the authentication, and the independently verifiable evidence.

Component	Authentication	Verification Rate	Anchored To	Dedicated Report(s)
4,251 Filing PDFs	MCRO Watermark (court CA)	98.9% valid, 0% modified	MJB Certificate Authority	Digital Sig Auth.
2,903 Docket PDFs	Bitcoin OTS timestamps	100% anchored	Bitcoin blockchain	Hash Loop Part 2
2,672 Docket PDFs	Hash-chain capture system	99.8% SHA-256 match	15 verified sessions	Hash Loop Parts 1–2
228 Emails	SHA-256 + OTS + PACER	100% all three layers	Bitcoin + federal court	EML-A, B, D, E
Email headers	DKIM/SPF/DMARC	100% where tested	Sender DNS records	EML-A, LinkedIn Report
Auth Package	Bitcoin OTS timestamps	All files anchored	Bitcoin (Nov 16, 2025)	Digital Sig Auth.
Original 3,556 files	Court filings (3 courts)	Sworn affidavit	District, Appellate, Federal	Chrono Catalog
Rule 20 report .eml	DKIM+DMARC+SPF +ARC	All PASS (p=reject)	hennepin.us infra.	R20 Metadata Auth.

LIMITATIONS & ALTERNATIVE EXPLANATIONS

What This Provenance Chain Proves

The filing PDFs are authentic, court-served documents that have not been modified since download. The docket data was captured from MCRO's live public access portal during verified sessions, and the captured files match their Bitcoin-timestamped records. The emails are genuine, unaltered communications from their stated senders. The original collection was documented under oath in three court systems within days of completion.

What This Provenance Chain Does Not Prove

Pre-download document state: The MCRO Watermark attests to the document's state at download time, not at the time of original filing or authoring. If a document were altered inside the court's document management system before being served via MCRO, the MCRO Watermark would faithfully sign the altered version.

MCRO system integrity: This analysis does not independently verify that MCRO's internal processes are free of error. The authentication confirms the files are genuine MCRO outputs; it does not confirm that MCRO's inputs were accurate.

689 NULL-status signatures: These MCRO-signed documents show no post-signing modifications but their cryptographic validity has not been formally confirmed. They may use an earlier certificate or different signing configuration.

CRL snapshot currency: The Certificate Revocation List snapshot is from October 23, 2025. Real-time OCSP validation was not performed. The certificate's revocation status after that date cannot be confirmed from the available artifacts.

Pre-capture-system cases: The 210 cases collected during the initial April 2024 MCRO scrape predate the hash-chain capture system. These have valid OTS timestamps but no bundle-level provenance. The 21 December 2025 gap cases lack bundle coverage from the 15 analyzed sessions.

Email authentication scope: DKIM/SPF/DMARC authentication proves the email was genuinely sent from the claimed domain's mail infrastructure. It does not prove who was physically at the keyboard composing the message.

No claims of intent: This report documents provenance facts. It does not assert that any anomalies found through analysis of the authenticated source data reflect intent, fraud, or misconduct by any party.

RECOMMENDATIONS FOR INDEPENDENT VERIFICATION

Any third party can independently verify every provenance claim in this report:

1. Verify MCRO Watermark Signatures

Open any MCRO PDF in Adobe Acrobat Reader, Okular, or any PDF tool supporting PKCS#7 validation. The MCRO Watermark signature will show validity status and whether edits occurred after signing. For certificate chain verification: download MCRO.cer and MJBIssuingCA.crt, run openssl verify -partial_chain -CAfile issuing.pem leaf.pem. For revocation check: download the current CRL from http://crl.enterprise.sectigo.com/MJBIssuingCA.crl and search for serial 3f9a4ed3d4d82120126a4ece4e415ea8.

2. Verify Hash-Chain Integrity

Clone the repository at github.com/Matt1Up/One-Way-Video. Obtain the raw bundles for any session. Run sha256sum on any bundle JSON file and compare against prev.last_hash.value in the next bundle. Or run the automated pipeline: python3 00_RUN_all_bundle_processing.py.

3. Verify Bitcoin Timestamps

Install the ots-client tool (opentimestamps.org). Run ots verify on any .ots receipt file to confirm it is anchored to a Bitcoin block at the claimed height.

4. Verify Email Authentication

Parse any .eml file using a standard email client or Python's email library. Examine the Authentication-Results headers for DKIM, DMARC, SPF, and ARC results. Compute the SHA-256 hash and compare against the hash recorded in the federal court exhibits.

5. Verify the Original Filing Chain

Access the federal court filings directly via PACER or CourtListener for case 0:24-cv-02646-JRT-DLM. Doc. 8 (p.111), Doc. 13 (p.36), Doc. 14 (p.100), and Doc. 24 (p.72) each contain documentation of the MCRO collection. The original shared files remain available at the ProtonDrive link referenced in the federal filings.

6. Access the Authentication Package

The complete MCRO Digital Signature Report with Embedded Files is available at: Storj Direct Link. This PDF contains the leaf certificate, CA certificate, CRL, public key, revocation lists, and timestamp archives as embedded files.

APPENDIX: Dedicated Provenance & Authentication Reports

The following reports in the MCRO corpus are dedicated to provenance and authentication. Each is a standalone, professionally formatted forensic report with reproducible SQL queries and/or code in its appendix.

Report	Provenance Role
MCRO Digital Signature Authentication Forensic Report	Master authentication of MCRO Watermark across 4,251 children PDFs. Certificate chain validation, revocation check, corpus-wide signature statistics, OTS timestamps on the authentication package itself.
ESolutions Signature Statistical Breakdown	Statistical profile of the ESolutions (Tyler Technologies) digital signature. Cluster and case ranking, temporal distribution, per-case concentration analysis.
Cloned Judicial Signature on First Rule 20 Order	Pixel-level analysis of judicial signature images, authenticated against MCRO Watermark seals. Provenance chain from PDF to extracted object hash to comparison.
Hash Loop Evidence Capture — Part 1 (System Auth.)	System-level authentication of the One-Way Video capture controller. Hash-chain integrity, dual timestamping, vault-sealing workflow, OCR overlay verification.
Hash Loop Evidence Capture — Part 2 (Docket Sweep)	Cross-session provenance sweep across 15 capture sessions. 2,672 cases verified against Bitcoin-timestamped docket report. 99.8% SHA-256 match rate.
Exhibit EML-A — Part 1	41 defense counsel emails (Carpenter/Donnelly), Oct 2024–Jun 2025. SHA-256 + OTS + PACER authentication.
Exhibit EML-B — Part 1	26 pre-trial emails (Rivers/Rogstad), Feb–Sep 2023. SHA-256 + OTS + PACER authentication. 62 authenticated attachments.
Exhibit EML-D — Part 1	82 federal case / patent emails, Sep 2022–Jan 2023. SHA-256 + OTS + PACER authentication. 84 authenticated attachments.
Exhibit EML-E — Part 1	79 transcript correspondence emails, Feb 2023–Jul 2024. SHA-256 + OTS + PACER authentication. 73 authenticated attachments.
Rule 20 Reports Metadata Authentication	.EML forensic examination of Cranbrook Rule 20 report. DKIM/DMARC/SPF/ARC verification. PDF metadata comparison proving common production origin.
LinkedIn Search Timeline Report	99 LinkedIn notification emails. 100% DKIM pass rate across 35 months. Authentication methodology explainer.

End of Report — MCRO | Capstone Provenance & Authentication Report