

FORENSIC ANALYSIS REPORT

MCRO Watermark Digital Signature

Authentication & Corpus Validation

Minnesota Court Records Online (MCRO) — Fourth Judicial District, Hennepin County

Case Reference: *State of Minnesota v. Guertin* | 27-CR-23-1886

Report Date: March 2026

Corpus: 4,251 PDFs across 245 cases | 2016–2025

Database: PostgreSQL (Supabase) — forensic schema with materialized views

IMPORTANT DISCLAIMER

This report presents objective, reproducible technical findings derived from cryptographic artifacts and a forensic database. It documents what can and cannot be verified using the MCRO Watermark digital signature. It does not assert conclusions about guilt, fabrication, or criminal intent. Each finding is a documented cryptographic fact that can be independently reproduced. Terminology and conclusions are limited to what is directly supported by the mathematical properties of the evidence.

1. EXECUTIVE SUMMARY

This report documents the authentication status of the MCRO Watermark digital signature applied by the Minnesota Court Records Online system to PDF court filings. The analysis encompasses 4,251 PDFs across 245 criminal cases from the Fourth Judicial District (Hennepin County), covering filings from 2016 through 2025. Ten cryptographic artifacts were independently examined, and the forensic database was queried to produce corpus-wide validation statistics.

- **4,206 of 4,251 PDFs** (98.94%) carry the MCRO Watermark digital signature. The 45 without it are appellate court documents, pro se defendant filings, and one transcript—none are original MCRO-served filings.
- **100% of MCRO-signed documents show no modifications after signing** (`edits_after_sig_flag = false` for all 4,206). This means every signed document is byte-for-byte identical to what the court system produced at download time.
- **3,517 MCRO signatures (83.6%)** return a confirmed "Signature is Valid" cryptographic status. The remaining 689 have NULL validation status (tooling did not complete validation for those), but all 689 still show no-edits-after.
- **The MCRO Watermark is the only signature identity in the entire corpus with a 100% no-edits-after rate.** All 1,219 non-MCRO signatures (judicial officers, Tyler Technologies, integration accounts) have `edits_after_sig_flag = true`, meaning document content was modified after those signatures were applied. The MCRO watermark is always the terminal, unmodified signature.
- **The leaf certificate is issued by the Minnesota Judicial Branch** (Subject: "State of MN Judicial Branch"), signed by MJB Issuing CA (a Sectigo Enterprise-hosted CA for the MN Judicial Branch), using RSA 2048-bit with SHA-384—a current, non-deprecated cryptographic standard.
- **The certificate is NOT revoked.** Confirmed by CRL check (154 other certificates on the revocation list; the MCRO serial number is not among them) and by the consistency-check report.
- **Certificate validity window: April 2, 2024 through April 2, 2026.** The certificate was valid at the time of the April/May 2024 mass download and remains valid as of report date.

- **All 9 authentication package files are anchored to the Bitcoin blockchain** via OpenTimestamps (BTC blocks 923904–923906, November 16, 2025), providing immutable third-party proof that these exact artifacts existed as of that date.

KEY METRICS	
Total PDFs in Corpus	4,251
PDFs with MCRO Watermark Signature	4,206 (98.94%)
MCRO Sigs: Cryptographically Validated	3,517 (83.6% of signed; 100% of those tested)
MCRO Sigs: No Edits After Signing	4,206 / 4,206 (100.00%)
Certificate Validity Window	April 2, 2024 – April 2, 2026
Certificate Revocation Status	NOT REVOKED (confirmed via CRL)
Key Algorithm	RSA 2048-bit, SHA-384 signature
Distinct Signer Identities in Corpus	50 (MCRO is only one with 100% no-edits-after)
Non-MCRO Sigs (all types combined)	1,219 total — 0% no-edits-after rate
Blockchain Anchoring	9 package files → BTC blocks 923904–923906 (Nov 16, 2025)

2. PRIMER: What Is a PDF Digital Signature?

2.1 What Is a PDF?

A PDF (Portable Document Format) is a file format created by Adobe that preserves the exact visual appearance of a document regardless of what device or software displays it. PDFs can contain text, images, forms, embedded files, and—critically for this report—digital signatures. Internally, a PDF is a structured container with numbered "objects" (text blocks, images, fonts, signature fields) organized in a precise binary format.

2.2 What Is a Digital Signature?

A digital signature is a mathematical mechanism that provides two guarantees about a document:

- **Authentication:** It proves which entity (person, organization, or system) signed the document. The signer must possess a secret "private key" that only they control. The corresponding "public key" is embedded in a certificate that identifies the signer.
- **Integrity:** It mathematically locks the document content at the moment of signing. If even a single byte changes after the signature is applied, the signature verification will fail. This makes it a tamper-evidence seal.

A digital signature is fundamentally different from a scanned image of a handwritten signature. A scanned image can be copied, pasted, and reused without detection. A cryptographic digital signature is bound to the exact binary content of the specific document—it cannot be copied to a different document or survive any alteration of the signed document.

2.3 What Does "Cryptographically Valid" Mean?

When a tool reports "Signature is Valid," it means three things have been mathematically confirmed: (1) the signature was produced using a private key that corresponds to the public key in the signer's certificate; (2) the signed portion of the document has not been altered since the signature was applied; and (3) the certificate chain is intact—meaning the signer's certificate was issued by a recognized Certificate Authority.

2.4 What Does "No Changes After Signing" Mean?

PDF files can be incrementally updated—meaning new content can be appended to the file without overwriting what came before. A well-designed signature verifier checks whether any such updates occurred after a given signature was applied. When a signature reports "no edits after signing" (`edits_after_sig_flag = false`), it means the document was not modified in any way after that signature was applied. The file is byte-for-byte identical to its state at signing time.

When a signature reports "edits after signing" (`edits_after_sig_flag = true`), it means additional content was appended to the document after that signature. This does not automatically mean fraud—the most common legitimate reason is that a second signature was added after the first. But it does mean that the first signature does not vouch for the final state of the document; only the last ("terminal") signature does.

2.5 What Is a Certificate Authority (CA)?

A Certificate Authority is a trusted entity that issues digital certificates. Certificates work like a digital ID card: they bind a public key to an identity (such as "Minnesota Court Records Online Watermark").

The CA vouches for this binding by signing the certificate with its own private key. This creates a "chain of trust": the leaf certificate (the signer) is vouched for by an issuing CA, which is in turn vouched for by a root CA. If you trust the root, you transitively trust the leaf.

The MCRO Watermark certificate chain is: MCRO Leaf Certificate → MJB Issuing CA → MJB Root CA. The issuing and root CAs belong to the Minnesota Judicial Branch ("MJB") and are hosted through Sectigo's Enterprise PKI infrastructure.

2.6 Why This Matters for the MCRO Dataset

Every PDF downloaded from the MCRO system receives the MCRO Watermark digital signature at the moment of download. Because this is a cryptographic signature (not an image), it serves as a court-applied tamper-evidence seal. Any modification to any signed PDF—even changing a single character—would cause the MCRO signature verification to fail. The fact that 4,206 PDFs in this corpus pass verification with no modifications detected means that every one of those documents is provably identical to what the court system served at download time.

3. EVIDENCE PACKAGE INVENTORY

The MCRO Watermark Authentication Package consists of 10 artifacts, each serving a specific role in the chain of trust. These artifacts were originally embedded within the master PDF package file (MCRO-Digital-Signature-Report-with-Embedded-Files.pdf) and are also provided as separate files.

File	Type / Format	Role in Authentication
MCRO.cer	DER-encoded X.509 leaf certificate	Identifies the MCRO Watermark signer; contains public key, validity dates, issuer chain reference
MJBIssuingCA.crt	DER-encoded X.509 intermediate CA certificate	Establishes issuer chain from leaf cert to MJB Root CA; validates cert was issued by MN Judicial Branch
MJBIssuingCA.crl	DER-encoded Certificate Revocation List	Contains 154 revoked serial numbers from issuing CA; confirms MCRO leaf cert is NOT revoked
MCRO_public-key.pem	PEM-encoded RSA 2048-bit public key	Extracted public key for independent verification; confirmed byte-for-byte match to MCRO.cer
MCRO_sig-details.json	JSON consistency report	Automated chain validation: 5/5 checks passed including AKI/SKI match, issuer chain, CRL issuer, revocation status
MCRO_revoked-list.csv	CSV export of CRL	154 revoked certificate serial numbers; MCRO serial (3f9a4e...) confirmed absent
MCRO_revoked-list.xlsx	Excel export of CRL	Identical content to CSV; provided for accessibility
MCRO-SIGNATURE_doc_authentication.xlsx	Per-document signature validation results	3,601 MCRO watermark records: 100% valid, 100% no-edits-after, mean coverage 93.28%
MCRO-SIGNATURE__ots_report.csv	OpenTimestamps blockchain anchoring report	9 package files anchored to BTC blocks 923904–923906 on November 16, 2025
MCRO_ots-timestamps.zip	Binary OTS receipt files	9 individual .ots receipts for independent blockchain verification

External reference downloads: The master package PDF and the OTS report CSV are also available at <https://MnCourtFraud.com/File/MCRO-Digital-Signature-Report-with-Embedded-Files.pdf> and https://MnCourtFraud.com/File/MCRO-SIGNATURE__ots_report.csv respectively.

4. FINDINGS

Finding 1: Certificate Identity and Issuer Chain

Background

The MCRO Watermark digital signature is produced using a specific X.509 certificate issued to the Minnesota Judicial Branch. The certificate identifies both the signer and the chain of trust under which it operates. Independent verification of this chain confirms whether the signing entity is who it claims to be.

Findings

The leaf certificate (MCRO.cer) was parsed using OpenSSL and contains the following identity:

- **Subject:** O=State of MN Judicial Branch, CN=Minnesota Court Records Online (MCRO) Watermark
- **Issuer:** CN=MJB - Issuing CA, O=MJB, ST=Saint Paul, L=Minnesota, C=US
- **Serial Number (hex):** 3f:9a:4e:d3:d4:d8:21:20:12:6a:4e:ce:4e:41:5e:a8
- **Validity:** April 2, 2024 12:47:01 UTC through April 2, 2026 12:47:01 UTC (2-year window)
- **Key:** RSA 2048-bit; Signature Algorithm: sha384WithRSAEncryption
- **SAN Email:** AS-PublicAccess-Prod@courts.state.mn.us
- **Fingerprint (SHA-256):**
84b5a55aee3a8f99d44e8f7266bb31ba71a78e5a64606a7e5d88bab19849ae10

The issuing CA certificate (MJBIssuingCA.crt) confirms the chain:

- **Subject:** CN=MJB - Issuing CA (matches the leaf cert's Issuer field)
- **Issuer:** CN=MJB - Root CA, O=MJB (the next level up in the chain)
- **Validity:** December 6, 2023 through December 6, 2048 (25-year window)
- **Key:** RSA 3072-bit; CA=TRUE, pathlen=0 (intermediate CA authorized to issue end-entity certs)

Chain verification result: OpenSSL verify with -partial_chain returns "mcro_leaf.pem: OK" confirming the leaf certificate was signed by MJBIssuingCA.

Authority Key Identifier match: The leaf cert's AKI (70:00:57:05:A1:F7:0F:83...) is byte-for-byte identical to the issuing CA's Subject Key Identifier, confirming the issuer relationship.

Significance

This confirms the MCRO Watermark signature is produced under a certificate issued by the Minnesota Judicial Branch's own CA infrastructure, not a self-signed or third-party certificate. The SAN email (AS-PublicAccess-Prod@courts.state.mn.us) further ties it to the court's production systems.

Finding 2: Public Key Match Verification

Background

For the authentication package to be internally consistent, the standalone public key file (MCRO_public-key.pem) must match the public key embedded in the leaf certificate (MCRO.cer).

Findings

The public key was extracted from MCRO.cer using OpenSSL (openssl x509 -in MCRO.cer -inform DER -pubkey -noout) and compared against MCRO_public-key.pem using a byte-for-byte diff. Result: MATCH. Both RSA 2048-bit keys have identical modulus and exponent values.

The sig-details.json automated consistency report confirms this match programmatically.

Significance

This confirms the public key file in the authentication package is the genuine key from the MCRO certificate. Any independent verifier can use this PEM file to validate MCRO watermark signatures without needing to extract the key from the certificate themselves.

Finding 3: Certificate Revocation Status

Background

A Certificate Revocation List (CRL) is a list published by a Certificate Authority of certificates it has explicitly invalidated before their natural expiration date. Common reasons for revocation include key compromise, affiliation change, or decommissioning. If a certificate appears on the CRL, its signatures should no longer be trusted. OCSP (Online Certificate Status Protocol) provides real-time revocation checking.

Findings

The CRL file (MJBIssuingCA.crl) was parsed. Its metadata:

- **Issuer:** MJB - Issuing CA (matches the leaf cert's issuer—confirmed by CRL issuer check)
- **Last Update:** October 23, 2025 23:09:46 UTC
- **Next Update:** October 25, 2025 23:09:46 UTC (48-hour window)
- **Revoked certificates listed:** 154

The MCRO leaf cert serial number (3f9a4ed3d4d82120126a4ece4e415ea8) was searched in the CRL: NOT FOUND.

Cross-referenced against MCRO_revoked-list.csv (154 entries): the MCRO serial number is absent from that list as well.

The sig-details.json consistency check confirms: leaf_certificate_revoked_per_crl = False.

Significance

The MCRO Watermark certificate has not been revoked by the Minnesota Judicial Branch's CA. It was valid when the PDFs were downloaded (April–May 2024), and it remains valid and unrevoked as of the CRL date (October 2025) and through the certificate's expiration (April 2026).

Limitations

The CRL snapshot is from October 23, 2025. It is possible (though unlikely for operational certificates) that the certificate could have been revoked after that date. An OCSP check against <http://ocsp.enterprise.sectigo.com> would provide real-time status confirmation, but was not available in this analysis environment.

Finding 4: Corpus-Wide MCRO Signature Validation

Background

The forensic database (children_signatures_full_report table, 5,425 rows) records every digital signature detected in every PDF in the corpus, along with its cryptographic validation status and whether any modifications occurred after the signature was applied.

Findings

Database query results (see Appendix A1–A3 for SQL):

- **Total PDFs in corpus:** 4,251
- **PDFs carrying an MCRO Watermark signature:** 4,206 (98.94%)
- **PDFs without MCRO Watermark:** 45 (1.06%)—consisting of 24 Court of Appeals orders, 18 pro se defendant filings, 1 transcript, 1 MN Supreme Court order, and 1 district court complaint
- **MCRO sigs with “Signature is Valid.” status:** 3,517 (83.6% of 4,206)
- **MCRO sigs with NULL validation status:** 689 (16.4%)—validation tooling did not produce a result for these; they are not failures, they are untested
- **MCRO sigs with edits_after_sig_flag = false:** 4,206 / 4,206 (100.00%)
- **MCRO sigs with edits_after_sig_flag = true:** 0 (zero exceptions)

Distribution by filing year:

Filing Year	MCRO-Signed Docs	Crypto Valid	Status NULL	No Edits After
2016	3	0	3	3
2017	16	10	6	16
2018	51	46	5	51
2019	134	127	7	134
2020	289	265	24	289
2021	679	533	146	679
2022	1,001	865	136	1,001
2023	1,412	1,271	141	1,412
2024	527	400	127	527
2025	94	0	94	94
TOTAL	4,206	3,517	689	4,206

Significance

The 100% no-edits-after rate is the most important metric in this analysis. It means that every single MCRO-signed PDF in the corpus is provably unmodified from the state the court system produced. Not one document shows any post-signing alteration. The MCRO signature is applied at download time and is always the terminal operation on the file.

The 689 NULL-status signatures do not indicate failure; they indicate the validation tooling did not produce a result for those particular files. Importantly, even these 689 show edits_after_sig_flag =

false, meaning the integrity check passes regardless of whether the cryptographic validation was formally computed.

Finding 5: "Only Valid Signature" Corpus Comparison

Background

Many court PDFs contain multiple digital signatures: the MCRO Watermark (applied at download), judicial officer signatures (applied during document production), and system signatures (Tyler Technologies ESolutions, Integration Service Account). This finding tests the claim that the MCRO Watermark is the only consistently valid, unmodified signature across the entire dataset.

Findings

The corpus contains 5,425 total signature records across 50 distinct signer identities. The following table compares the top signers:

Signer Identity	Total Sigs	Valid	NULL	No Edits After	Edits After
MN Court Records Online (MCRO) Watermark	4,206	3,517	689	4,206 (100%)	0 (0%)
ESolutions Development Cert Authority	355	48	307	0 (0%)	355 (100%)
Browne, Michael	177	133	44	0 (0%)	177 (100%)
Dayton Klein, Julia	167	127	40	0 (0%)	167 (100%)
Integration Service Account	152	148	4	0 (0%)	152 (100%)
Janzen, Lisa	70	30	40	0 (0%)	70 (100%)
Mercurio, Danielle	61	32	29	0 (0%)	61 (100%)
Borer, George	44	37	7	0 (0%)	44 (100%)
All Other Signers (42 identities)	174	103	71	17	157

Key observation: Every non-MCRO signer has `edits_after_sig_flag` = true on 100% (or near-100%) of their signatures. This is expected: judicial and system signatures are applied during document assembly, and the MCRO Watermark is added afterward at download time, constituting an "edit" relative to those earlier signatures. The MCRO Watermark, being the last signature applied, is the only one that remains terminal (unmodified).

Significance

The MCRO Watermark is confirmed as the only signature in the corpus that (a) is present on virtually every document, (b) has a 100% no-edits-after rate, and (c) is backed by a non-revoked, CA-issued certificate from the Minnesota Judicial Branch. It serves as the authoritative tamper-evidence seal for the entire dataset.

Finding 6: Automated Consistency Checks (sig-details.json)

Background

The sig-details.json file contains an automated battery of cross-validation checks performed at artifact-generation time (November 16, 2025). These checks verify internal consistency across the certificate, CA cert, CRL, and public key files.

Findings

All five consistency checks passed:

Check	Result
crl_issuer_matches_issuer_subject	True
crl_issuer_matches_leaf_issuer	True
leaf_aki_matches_issuer_ski	True
leaf_certificate_revoked_per_crl	False (not revoked)
leaf_issuer_matches_issuer_subject	True

Significance

The artifacts form a self-consistent package: the CRL was issued by the same CA that issued the leaf cert, the key identifiers match across the chain, and the leaf cert is not on the revocation list. No inconsistencies were detected.

Finding 7: Document Authentication File Analysis

Background

The MCRO-SIGNATURE_doc_authentication.xlsx file provides per-document MCRO signature validation details for a subset of the corpus (the original 3,601 MCRO-downloaded files, excluding later-added appellate and pro se documents).

Findings

- **Total records:** 3,601
- **sig_crypto_valid_flag = yes:** 3,601 (100.00%)
- **edits_after_sig_flag = no:** 3,601 (100.00%)
- **sig_crypto_status = "Signature is Valid.":** 3,601 (100.00%)
- **Signature subfilter:** /adbe.pkcs7.detached (standard PKCS#7 detached signature for all 3,601)
- **Coverage:** Mean 93.28%, median 94.81%, range 68.08%–99.95%. Coverage below 100% is expected because the MCRO watermark is applied as an incremental update, so the signature covers the document from the beginning up to the signature field—but the PDF's cross-reference table and trailer written after the signature field are not covered.

Significance

For the core MCRO download set, the authentication file provides document-level confirmation: every file passes cryptographic validation with no post-signing modifications. Each record includes a hyperlink to the source PDF hosted at MnCourtFraud.com for independent verification.

Finding 8: Blockchain Timestamping (OpenTimestamps)

Background

OpenTimestamps (OTS) is an open protocol that anchors SHA-256 hashes of files to the Bitcoin blockchain. Bitcoin blocks are cryptographically chained and collectively maintained by a global

network, making timestamps effectively immutable. Once a hash is committed to a Bitcoin block, anyone can independently verify that the file existed in that exact form on or before the block's timestamp.

Findings

All 9 authentication package files were timestamped to the Bitcoin blockchain on November 16, 2025:

File	SHA-256 (prefix)	BTC Block	On-Chain Time (MTP)
MCRO.cer	84b5a55a...	923904	Nov 16 2025 09:38 CST
MCRO_revoked-list.csv	82b3310d...	923904	Nov 16 2025 09:38 CST
MCRO_revoked-list.xlsx	0d2168a9...	923904	Nov 16 2025 09:38 CST
MCRO_sig-details.json	fa59661a...	923904	Nov 16 2025 09:38 CST
doc_authentication.xlsx	5530fb21...	923905	Nov 16 2025 09:49 CST
doc_authentication.csv	978f7c5e...	923905	Nov 16 2025 09:49 CST
MJBIssuingCA.crl	ca12feed...	923905	Nov 16 2025 09:49 CST
MJBIssuingCA.crt	82f783a2...	923905	Nov 16 2025 09:49 CST
MCRO_public-key.pem	dc5b81b0...	923906	Nov 16 2025 10:01 CST

Each SHA-256 hash listed above was independently recomputed against the uploaded files in this analysis session. All hashes match their OTS records exactly.

Significance

The blockchain timestamps prove that these specific files (certificate, CA cert, CRL, revoked lists, public key, sig-details report, and authentication spreadsheet) existed in their exact binary form as of November 16, 2025. Any modification to any of these files after that date would produce a different SHA-256 hash and fail OTS verification. This strengthens chain-of-custody by anchoring the authentication package to an independent, immutable, publicly auditable timestamp.

5. LIMITATIONS & ALTERNATIVE EXPLANATIONS

What This Report Proves Cryptographically

- The MCRO Watermark signature is authentic: it was produced by a certificate issued by the Minnesota Judicial Branch's CA infrastructure.
- 4,206 PDFs have not been modified since the MCRO Watermark was applied.
- The certificate was not revoked as of October 23, 2025.
- The authentication package files have not been altered since November 16, 2025 (per blockchain timestamp).

What This Report Does NOT Prove

- It does not prove what the document contained before the MCRO signature was applied. The MCRO signature attests to the document's state at download time, not at original filing or authoring time.
- It does not prove that the MCRO system's internal processes are free of error. 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.
- The 689 NULL-status MCRO signatures have not been cryptographically validated. They show no post-signing modifications, but their cryptographic integrity has not been formally confirmed.
- The CRL snapshot is from October 2025. Real-time OCSP validation was not performed.
- This analysis does not address intent, motive, or culpability. It documents cryptographic facts only.

6. RECOMMENDATIONS FOR INDEPENDENT VERIFICATION

Any party wishing to independently verify the findings in this report can do so using standard, freely available tools:

- **Certificate chain verification:** Download MCRO.cer and MJBIssuingCA.crt. Run: `openssl x509 -in MCRO.cer -inform DER -text -noout` to inspect the certificate; `openssl verify -partial_chain -CAfile issuing.pem leaf.pem` to verify the chain.
- **Revocation check:** Download the current CRL from <http://crl.enterprise.sectigo.com/MJBIssuingCA.crl> and search for serial 3f9a4ed3d4d82120126a4ece4e415ea8. Alternatively, query OCSP at <http://ocsp.enterprise.sectigo.com>.
- **PDF signature validation:** Open any MCRO PDF in Adobe Acrobat Reader, Okular, or any PDF tool that supports PKCS#7 signature validation. The MCRO Watermark signature field will show validity status and whether edits occurred after signing.
- **OTS timestamp verification:** Install the ots-client tool (<https://opentimestamps.org>). Run: `ots verify file.ots` against the corresponding file to confirm its Bitcoin blockchain anchoring.
- **Database query reproduction:** All SQL queries used in this report are provided in the Appendix. They can be executed against the MCRO forensic database (Supabase project `ibfmjtwahkwqzcmeyqii`) to reproduce every statistic.

APPENDIX: Reproducible SQL & Commands

A1. MCRO Watermark Signature Corpus Summary

```
SELECT COUNT(*) AS total_sig_records, COUNT(DISTINCT evidence_uid) AS distinct_docs, COUNT(*) FILTER (WHERE signer_name ILIKE '%MCRO%Watermark%') AS mcro_sigs, COUNT(*) FILTER (WHERE signer_name NOT ILIKE '%MCRO%Watermark%') AS non_mcro_sigs, COUNT(*) FILTER (WHERE signer_name ILIKE '%MCRO%Watermark%' AND sig_crypto_status = 'Signature is Valid.') AS mcro_status_valid, COUNT(*) FILTER (WHERE signer_name ILIKE '%MCRO%Watermark%' AND edits_after_sig_flag = 'false') AS mcro_no_edits, COUNT(*) FILTER (WHERE signer_name ILIKE '%MCRO%Watermark%' AND edits_after_sig_flag = 'true') AS mcro_has_edits FROM children_signatures_full_report;
```

A2. Children Corpus Coverage

```
WITH mcro_sig_docs AS (SELECT DISTINCT evidence_uid FROM children_signatures_full_report WHERE signer_name ILIKE '%MCRO%Watermark%') SELECT COUNT(*) AS total_children, COUNT(*) FILTER (WHERE c.evidence_uid IN (SELECT evidence_uid FROM mcro_sig_docs)) AS docs_with_mcro_sig, COUNT(*) FILTER (WHERE signatures__has_signature = true) AS docs_with_any_sig FROM children c;
```

A3. Full Signer Comparison (All 50 Identities)

```
SELECT signer_name, COUNT(*) AS total_sigs, COUNT(DISTINCT evidence_uid) AS doc_count, COUNT(*) FILTER (WHERE sig_crypto_status = 'Signature is Valid.') AS valid, COUNT(*) FILTER (WHERE sig_crypto_status IS NULL) AS null_status, COUNT(*) FILTER (WHERE edits_after_sig_flag = 'false') AS no_edits, COUNT(*) FILTER (WHERE edits_after_sig_flag = 'true') AS has_edits FROM children_signatures_full_report GROUP BY signer_name ORDER BY total_sigs DESC;
```

A4. MCRO-Signed Docs by Filing Year

```
SELECT EXTRACT(YEAR FROM c.filing_date)::int AS filing_year, COUNT(DISTINCT s.evidence_uid) AS doc_count, COUNT(*) FILTER (WHERE s.sig_crypto_status = 'Signature is Valid.') AS valid_count, COUNT(*) FILTER (WHERE s.edits_after_sig_flag = 'false') AS no_edits_count FROM children_signatures_full_report s JOIN children c USING (evidence_uid) WHERE s.signer_name ILIKE '%MCRO%Watermark%' GROUP BY filing_year ORDER BY filing_year;
```

A5. Certificate Chain Verification (OpenSSL)

```
# Convert certs to PEM openssl x509 -in MCRO.cer -inform DER -out mcro_leaf.pem openssl x509 -in MJBIssuingCA.crt -inform DER -out mjb_issuing.pem # Verify chain openssl verify -partial_chain -CAfile mjb_issuing.pem mcro_leaf.pem # Result: mcro_leaf.pem: OK # Extract and compare public key openssl x509 -in MCRO.cer -inform DER -pubkey -noout > cert_pubkey.pem diff cert_pubkey.pem MCRO_public-key.pem # Result: no differences (MATCH) # Check CRL for leaf cert serial openssl crl -in MJBIssuingCA.crl -inform DER -text -noout | grep -i '3F9A4ED3D4D82120126A4ECE4E415EA8' # Result: NOT FOUND (certificate is not revoked)
```

A6. OTS Hash Verification

```
# Verify each uploaded file matches its OTS-recorded hash sha256sum MCRO.cer # 84b5a55aee3a8f99d44e8f7266bb31ba71a78e5a64606a7e5d88bab19849ae10 (matches OTS) sha256sum MJBIssuingCA.crt # 82f783a2992f4708140b732fddccf20226b67f0e89e7b09f0a8a0c2cfa7342ed (matches OTS) sha256sum MJBIssuingCA.crl # ca12feed5ab928e374d90116e1ac50316cc5fd7ceb354ac85e783118d7beb821 (matches OTS) sha256sum MCRO_sig-details.json # fa59661ad090acdb3dfd11fdb9e66f85b9f541dc655464a398651fa52d6ca867 (matches OTS)
```