

FORENSIC ANALYSIS REPORT

Minnesota Court Records Online (MCRO)

Fourth Judicial District — Hennepin County

PDF INTERNAL OBJECT ANALYSIS | DOCUMENT METADATA ANOMALIES | JUDICIAL SIGNATURE HASH COLLISIONS | RULE 20 PIPELINE STATISTICS

Prepared by	Matthew David Guertin, Pro Se Defendant
Case Reference	State of Minnesota v. Guertin 27-CR-23-1886
Court	Fourth Judicial District Court, Hennepin County
Report Date	February 2026
Data Source	Minnesota Court Records Online (MCRO) — Public Records
Collection Method	Automated MCRO scraper with VPN rotation; MITMPROXY session capture; OBS hash-loop video evidence chain; OpenTimestamps (OTS) Bitcoin blockchain anchoring
Corpus Size	4,251 PDFs across 245 cases 2017–2025
Database	PostgreSQL (Supabase) — custom forensic schema with materialized views
Reproducibility	All findings are query-reproducible from the underlying database. SHA256 hashes are independently verifiable against original PDF files.

IMPORTANT DISCLAIMER

This report presents objective forensic data findings reproducible from the source database.
It does not assert conclusions about guilt, fabrication of defendants, or criminal intent.
Each finding is a documented anomaly that warrants independent expert examination.

1. EXECUTIVE SUMMARY

This report documents five categories of forensic anomalies identified through systematic analysis of 4,251 PDF court filings retrieved from the Minnesota Court Records Online (MCRO) system, covering Fourth Judicial District criminal cases filed between 2016 and 2025.

All findings are derived from a purpose-built PostgreSQL forensic database containing SHA256-hashed PDF internal objects, XMP/PDF metadata fields, cryptographic signature records, and docket event timelines. Every finding stated in this report is directly reproducible by querying that database.

Corpus Overview

Metric	Count	Notes
Total PDFs analyzed	4,251	All bear valid MCRO cryptographic watermark
Unique cases represented	245	4th Judicial District, Hennepin County
Defendant clusters (normalized)	81	After name normalization & manual review
Date range of filings	2016–2025	9-year span
Distinct filing types	120	Complaints through sentencing orders
PDFs with tracking font objects	1,551	36.5% of corpus
PDFs with embedded judicial signature images	1,001	23.5% of corpus
PDFs with MCRO watermark signature	3,490	82.1% of corpus — all cryptographically valid

Summary of Critical Findings

FINDING 1 — CRITICAL: Programmatically-Generated PDF Objects Detected at Download Time

5 documents served by MCRO have PDF creation timestamps matching their download date, not their filing date. Creator tool identified as **IronPdf v2023.9.19098** — a commercial .NET PDF generation library with no legitimate role in court document archiving. The maximum discrepancy is **1,919 days (5.25 years)** between official filing date and actual PDF creation date.

FINDING 2 — CRITICAL: Identical Judicial Signature Images Across Hundreds of Cases

15 judicial officers have their handwritten signature captured as PNG/JPG image files embedded within official court orders. Each signature image has a unique SHA256 hash. These identical binary objects appear across **up to 259 independent documents** spanning up to 2.5 years — proving signatures are programmatically inserted by a document generation pipeline, not hand-signed individually.

FINDING 3 — HIGH: Bespoke 'Tracking Font' Objects Embedded Across Entire Corpus

12 distinct custom font objects labeled TRACKING-FONT-A through F appear embedded inside official court documents. These are not standard system fonts. TRACKING-FONT-C1 and C2 appear together in **1,130 documents across 196 cases** spanning 5 years. One font (TRACKING-FONT-A1) has a SHA256 hash of **e3b0c44...** — the universal null/empty-file hash — meaning it is a **zero-byte ghost object** embedded in 65 criminal complaint documents from 2017 to 2023.

FINDING 4 — HIGH: MSIP Enterprise Labels Span Three Judicial Branches from a Single M365 Tenant

34 documents from the 4th District Court, Minnesota Court of Appeals, and Minnesota Supreme Court carry Microsoft Information Protection (MSIP) sensitivity labels. All 34 share an identical Microsoft 365 Site ID — proving common organizational origin across three jurisdictionally distinct courts. The label appears first in petitioner Guertin's competency order (April 3, 2025), and three of five Guertin-specific documents carry it. The root document also contains a Tyler Technologies digital signature using a **deprecated RSA-1,024-bit key**, with the same PDF object cloned across four signature indices. All 228 case files are SHA256-anchored to the Bitcoin blockchain.

FINDING 5 — SIGNIFICANT: Statistically Anomalous Rule 20 Competency Pipeline

Dormant cases (cases with no resolution, no trial, no dismissal) average **12.73 Rule 20 competency events** each — more than double the 5.60 average for closed cases. The most extreme case has 44 Rule 20 events spanning years. A recurring network of judicial officers and defense attorneys handles a disproportionate share of this pipeline. The **top 5 dormant cases** by Rule 20 event count each involve the same core set of judicial officers.

2. FINDING 1: IronPDF-Generated Documents (On-Demand PDF Creation)

Background

When a PDF is legitimately archived in a court records system, its internal XMP metadata creation date should reflect when the original document was authored — typically on or near its official filing date. The MCRO Watermark signature is applied at download time, so the MCRO signature timestamp will always reflect the download date. However, the XMP creation date embedded inside the PDF's metadata structure should not match the download date unless the PDF itself was generated at that moment.

Findings

Five documents were found with XMP creator tool identified as IronPdf v2023.9.19098 and XMP creation dates matching the download timestamp to within seconds:

AESHA OSMAN 27-CR-18-18391	Order — Rule 20.01 Competency Eval	2019-01-28	2024-04-30 (download day)	+1,919 days (5.25 yrs)
RASHEED RICHARDSON 27- CR-20-26577	Returned Mail	2022-03-17	2024-04-30 (download day)	+775 days (2.1 yrs)
ANNE RILEY 27- CR-19-22615	Other Document	2023-11-08	2024-04-30 (download day)	+174 days
ANNE RILEY 27- CR-19-22615	Correspondence	2023-12-20	2024-04-30 (download day)	+132 days
ANNE RILEY 27- CR-19-22615	Correspondence	2024-01-16	2024-04-30 (download day)	+105 days

Significance

- IronPDF is a commercial .NET library used by software developers to generate PDFs programmatically. It is not scanning software, word processing software, or any tool associated with standard court document authoring.
- Every IronPDF document has exactly 3 PDF revisions (rev_count = 3) and a cryptographically valid MCRO Watermark signature with edits_after_sig_flag = false.
- The MCRO Watermark signature timestamp and the XMP creation timestamp are within 1 second of each other in all five documents — meaning the PDF was generated and signed in a single near-instantaneous operation at download time.
- The most extreme case — the 2019 Rule 20.01 competency order for Aesha Osman — was not retrieved from a 2019 archive. It was created fresh on April 30, 2024, 5.25 years after its official filing date.

Connecting Context

- All three affected defendants (Osman, Richardson, Riley) share judicial officers with case 27-CR-23-1886 (Guertin): Julia Dayton Klein, George Borer, and Danielle Mercurio appear across all three.
- Aesha Osman's case has 31 Rule 20 events and is classified Dormant. Rasheed Richardson's has 17 Rule 20 events and is Dormant. Both represent extreme examples of the competency pipeline described in Finding 5.

3. FINDING 2: Judicial Signature Image Hash Collisions

Technical Background

Modern court document systems that use digital signatures typically involve one of two approaches: (1) a cryptographic digital signature where a private key is applied to the document hash, or (2) an image of a handwritten signature inserted as a visual element. This corpus uses the second approach. Each judicial order contains the judge's signature as an embedded PNG or JPG image object within the PDF's internal structure.

Using mutool to extract all internal PDF objects and computing SHA256 hashes for each, this analysis identified the specific signature image files used across the corpus. Because SHA256 is a cryptographic hash function, identical hashes mean byte-for-byte identical files — the exact same image, with no variation whatsoever.

Findings

15 judicial officers have signature image objects identified and catalogued. The following table shows the top-frequency entries:

Judge Michael Browne (sig 01)	136	259	2022-12-27	2025-05-29
Judge Julia Dayton Klein (sig 01)	129	236	2023-01-05	2025-05-29
Judge Lisa K. Janzen (sig 01)	91	206	2020-11-13	2025-04-28
Judge Lisa K. Janzen (sig 02)	91	206	2020-11-13	2025-04-28
Referee Danielle Mercurio	73	117	2023-01-18	2025-05-29
Judge Lisa K. Janzen (sig 03)	49	75	2022-03-23	2025-04-28
Judge Lisa K. Janzen (sig 04)	49	75	2022-03-23	2025-04-28
Referee George Borer	45	59	2023-01-11	2025-05-29
Judge Lisa K. Janzen (sig 08)	30	50	2021-04-06	2025-04-28
Referee Lori Skibbie	21	38	2023-03-15	2025-05-29
Judge Hilary Caligiuri	15	35	2021-05-27	2025-04-28
Judge Carolina A. Lamas	15	25	2017-02-21	2025-04-28
Judge William H. Koch	8	18	2019-01-09	2025-05-29

Notable Detail: Judge Janzen Has Eight Distinct Signature Variants

Judge Lisa K. Janzen is represented by at least 8 distinct signature image objects (labeled sig 01 through sig 08), each with a different SHA256 hash and file size, spanning from 2020 to 2025. This may indicate multiple capture events, different scanning conditions, or document system upgrades over time. It is the highest number of distinct signature variants for any single judicial officer in the corpus.

Significance

- These findings confirm that the document production system for these court orders operates by inserting a stored signature image file into documents programmatically, not by capturing a live signature at the time of signing.
- This is not inherently fraudulent — many electronic court systems work this way. However, it means the MCRO Watermark signature is the only cryptographic attestation that a document existed at a given time. The judicial 'signature' embedded in the document body is a stored image, not a cryptographic signature.

- When combined with Finding 1 (IronPDF documents generated at download time), the absence of a cryptographic judicial signature means that the content of these orders — including Rule 20 competency findings — has no independent cryptographic integrity proof beyond the MCRO download-time watermark.

4. FINDING 3: Bespoke Tracking Font Objects

Background

PDF documents routinely embed font files to ensure consistent rendering across systems. Standard embedded fonts have recognizable names: Calibri, Times New Roman, Arial, etc. During PDF internal object extraction and hashing, this analysis identified a set of font objects with non-standard identifiers — labeled TRACKING-FONT-A through F based on their properties and document distribution patterns.

Standard system fonts, when embedded in different documents produced by different authors on different machines, do not produce identical SHA256 hashes. Different versions, subsets, and encoding configurations result in different binary outputs. Identical SHA256 hashes across hundreds of independently-authored documents indicate a single common source.

Tracking Font Inventory

TRACKING-FONT-A1	.ttf	0 (ZERO)	65	65	2017-01-19	2023-11-14
TRACKING-FONT-A2	.ttf	40,068	123	133	2020-01-06	2025-05-29
TRACKING-FONT-A3	.ttf	40,660	124	134	2020-01-06	2025-05-29
TRACKING-FONT-A4	.ttf	60,816	13	17	2020-02-05	2025-05-29
TRACKING-FONT-B1	.cff	86,093	131	254	2017-02-21	2025-08-22
TRACKING-FONT-C1	.ttf	55,072	196	1,130	2020-01-07	2025-07-02
TRACKING-FONT-C2	.ttf	916,684	196	1,130	2020-01-07	2025-07-02
TRACKING-FONT-D1	.ttf	101,216	75	104	2023-08-14	2025-04-28
TRACKING-FONT-D2	.ttf	11,088	172	500	2021-08-13	2025-04-28
TRACKING-FONT-D3	.ttf	14,252	122	262	2021-12-06	2025-04-28
TRACKING-FONT-E1	.ttf	115,676	2	8	2024-01-17	2025-05-29
TRACKING-FONT-F1	.ttf	68,808	3	6	2024-01-10	2025-04-28

The Zero-Byte Ghost Font (TRACKING-FONT-A1)

TRACKING-FONT-A1 has a SHA256 hash of [e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855](#). This is the universally-known SHA256 hash of an empty file — a file containing zero bytes.

This means 65 official criminal complaint documents (E-filed Comp-Warrant, E-filed Comp-Order for Detention, E-filed Comp-Summons, Formal Complaint, Amended Criminal Complaint) contain a declared font object that resolves to nothing. The object exists in the PDF's internal structure — it has an entry, a name, a type declaration — but its content is empty. This is not a standard font rendering artifact. It is a placeholder object of unknown purpose embedded in some of the most legally significant documents in a criminal proceeding: the charging instruments themselves.

Generation Timeline

- Generation A (A1–A4): First appears January 2017 in criminal complaints. Still present in May 2025 documents.
- Generation B (B1): First appears February 2017. Broadest filing type coverage (27 distinct types). Active through August 2025 — the latest end date in the corpus.

- Generation C (C1+C2): Appear together as a pair starting January 2020. Dominant generation — 1,130 documents across 196 cases. C2 is 916 KB, unusually large for an embedded font subset.
- Generation D (D1–D3): Begin appearing August 2021 through August 2023. Concentrated in Rule 20 competency orders and hearing notices specifically.
- Generations E and F: Appear in January 2024. Likely indicate a further system update.

5. FINDING 4: MSIP Enterprise Labels — Cross-Branch Common Origin

5.1 Background

Microsoft Information Protection (MSIP) is an enterprise data governance feature built into Microsoft 365. MSIP embeds sensitivity classification labels into documents, including a Site ID (uniquely identifying the authoring Microsoft 365 tenant), a Label Token (identifying the specific policy), and a Set Date (when the label was applied). These labels persist into PDF exports and are not stripped by default.

5.2 Corpus Statistics

Property	Value
Total MSIP-labeled documents	34
Unique cases affected	29
Label: High sensitivity	33 documents
Label: Moderate sensitivity	1 (MN Supreme Court — A24-2042)
Date range	April 3, 2025 — August 22, 2025
MSIP Site ID (all 34 docs — identical)	8cf8312b-4c34-4b6f-9dee-c56512a7510f
MSIP Label Token (32 of 34 docs — identical)	14543c82-bfb1-4059-96af-7a0a0f468681
Creator tool	Acrobat PDFMaker 25 for Word (all docs with tool field populated)

5.3 Critical: Single Microsoft 365 Tenant Origin Across Three Judicial Branches

Every one of the 34 MSIP-labeled documents — produced by the 4th District Court, the Minnesota Court of Appeals, and the Minnesota Supreme Court — shares an identical MSIP Site ID: 8cf8312b-4c34-4b6f-9dee-c56512a7510f. The Site ID is the unique identifier of the Microsoft 365 organizational tenant in which the document was authored. Identical Site IDs across documents from three distinct judicial jurisdictions prove they were all produced within the same Microsoft 365 organization.

32 of 34 documents also share an identical MSIP Label Token — the same sensitivity label policy applied across all three branches. The single exception is the Supreme Court PFR-Deny order (A24-2042), which carries a Moderate label with a different token, consistent with a different classification tier within the same organizational tenant.

5.4 Chronological Distribution — The Label First Appears in Petitioner's Case

Date	Document	Branch	Notes
2025-04-03	Order Finding Guertin Competent (27-CR-23-1886, Index 127)	4th District	First MSIP document in corpus. Contains deprecated RSA-1024 ESolutions sig (see §5.6). MSIP Set Date: 2025-03-17 (17 days before filing).
2025-04-07/08	Orders Mandamus/Prohibition (A25-0048, A24-2042)	MN Court of Appeals	MSIP label present within days of first district court appearance. Chief Judge Frisch.
2025-04-23	Order PFR-Deny (A24-2042)	MN Supreme Court	MSIP crosses to third branch. Chief Justice Hudson. Only Moderate-labeled doc. No digital signature present.
2025-05-30	Order Re Pro Se Motions (27-CR-	4th District	Filed in response to Guertin's pro se motions.

	23-1886, Index 205)		MSIP Set Date: 2025-01-09 (141 days before filing).
2025-07-08	Order Denying Writ (A25-0882)	MN Court of Appeals	Denies Guertin's petition for extraordinary relief. Same tenant site ID.
2025-08-19/22	Late Frisch orders (A25-1136, A25-0965)	MN Court of Appeals	Two signers: Frisch + Lucid, Elizabeth. Frisch sig shows edits_after = true.

Three of the five documents directly concerning petitioner Guertin carry the MSIP label: the April 3 competency order (the first MSIP document in the entire corpus), the May 30 response to his pro se motions, and the July 8 Court of Appeals order denying his writ of prohibition. The statistical concentration of a rare metadata artifact — one absent from the entire corpus prior to April 3, 2025 — across three judicial branches, appearing first and repeatedly in a single defendant's filings, is a forensic anomaly requiring explanation.

5.5 MSIP Set Dates Precede Filing Dates

Document	MSIP Set Date	Filing Date	Pre-staging Interval
127__ Order Finding Guertin Competent	2025-03-17 19:18 UTC	2025-04-03	17 days before filing
205__ Order Regarding Pro Se Motions	2025-01-09 16:38 UTC	2025-05-30	141 days before filing

The 205__ document's MSIP label was set on January 9, 2025 — nearly five months before the May 30 filing and approximately four months before the April 29 hearing that the order responds to. This indicates the document or its template existed within the enterprise M365 environment well before the relevant legal proceedings occurred.

5.6 Deprecated RSA-1024 Signature on the Root MSIP Document

The April 3, 2025 Order Finding Guertin Competent — the first MSIP document in the corpus — contains a digital signature from **ESolutions Development Certificate Authority** (a Tyler Technologies component). The certificate visible in Okular's certificate viewer uses a **1,024-bit RSA public key** issued on March 19, 2014. RSA-1024 was deprecated by NIST in 2013 and is formally prohibited for use in current applications due to insufficient cryptographic security.

Certificate Property	Value
Certificate Authority	ESolutions Development Certificate Authority (Tyler Technologies)
Key Algorithm	RSA 1,024-bit (deprecated / prohibited since 2013)
Issued On	March 19, 2014 — Expires December 31, 2039
Signature field	tyler_sig_fa94cb09-d992-4ec9-a305-5094c9da197e
PDF object (v_obj)	306 0 obj — cloned across sig_index 2, 3, 4, and 5 (4 pages)
edits_after_sig_flag	TRUE (post-signature modifications occurred)
Koch, William sig (Signature2)	edits_after_sig_flag = TRUE (post-signature modifications)
MCRO Watermark	edits_after_sig_flag = FALSE (terminal — applied at download)

The same PDF object (306 0 obj) is referenced at four consecutive signature indices (2, 3, 4, 5), meaning a single binary object is presented as four independent page-level signatures. Standard multi-page independent signatures each occupy a distinct PDF object with a distinct hash. This structural pattern suggests programmatic document assembly rather than individual page-by-page signing.

Both the Koch judicial signature and the ESolutions CA signature carry **edits_after_sig_flag = true**, meaning document content was modified after both were applied. The MCRO download watermark is the only terminal signature — but it attests only to the state of the file at download time, not at the time of original judicial signing.

5.7 Court of Appeals Signature Validity

All MSIP-labeled Court of Appeals documents signed by Chief Judge Frisch return `sig_crypto_valid_flag = NULL` — meaning cryptographic validation was inconclusive. This contrasts with MCRO Watermark signatures on non-MSIP documents in the same period, which return definitive 'Signature is Valid' status. In the two most recent Frisch-signed MSIP documents (A25-1136 and A25-0965), a co-signer — Lucid, Elizabeth — applies a second signature with `edits_after_sig_flag = false`, making Lucid's signature the terminal cryptographic attestation on those documents.

5.8 Bitcoin Blockchain Timestamp Chain

All 228 PDF files in the collection, including all MSIP-labeled documents, were anchored to the Bitcoin blockchain on December 25, 2025 using OpenTimestamps (OTS). This records each file's SHA256 hash in Bitcoin blocks **929,482 and 929,498** — providing independent, immutable proof that these specific file contents existed as of that date. The three Guertin-related MSIP documents (127__, 205__, A25-0882) were anchored in block 929,498. Any modification of these files after anchoring would produce a different SHA256 hash and fail OTS verification against the blockchain record.

6. FINDING 5: The Rule 20 Competency Pipeline — Statistical Profile

Background

Minnesota Rule 20 governs competency proceedings in criminal cases. When a defendant is found incompetent to proceed, the criminal case is suspended while the defendant receives treatment. Upon restoration of competency, proceedings resume. Cases where competency is never restored — or where the question is perpetually relitigated — can remain in legal limbo indefinitely.

The MCRO docket event data allows quantification of Rule 20 event frequency per case and per judicial officer. The following analysis identifies statistically anomalous patterns within this dataset.

Case Status vs. Rule 20 Intensity

Case Status	Cases	Avg Rule 20 Events
Closed	1,620	5.60
Under Court Jurisdiction	546	5.22
Open	349	8.83
Dormant	380	12.73

Dormant cases average 12.73 Rule 20 events — 2.3x the rate of closed cases. Average time since filing for Dormant cases: 1,045 days (2.86 years). These are cases with no verdict, no dismissal, and no resolution — suspended indefinitely.

Extreme Dormant Cases — Top 10 by Rule 20 Event Count

ADEL MOHAMED	27-CR-07-044372	44	Dormant	Susan Herlofsky
ERWIN KRUK	27-CR-17-9080	42	Dormant	Thomas Shiah
VENNIE WILLIAMS	27-CR-16-29574	39	Dormant	Gregory Renden
Amar Jacox-Rowe	27-CR-17-13895	36	Dormant	Geoffrey Isaacman
VENNIE WILLIAMS	27-CR-17-17920	35	Dormant	Gregory Renden
VENNIE WILLIAMS	27-CR-17-17792	35	Dormant	Gregory Renden
WILLIAM ROCK	27-CR-13-1927	34	Dormant	Emmett Donnelly / Susan Herlofsky
VENNIE WILLIAMS	27-CR-17-31829	34	Dormant	Gregory Renden
BRANDY ROSS	27-CR-14-2783	33	Dormant	Susan Herlofsky
DOUGLAS PIERCE	27-CR-17-5928	32	Dormant	Michelle Margoles

Defense Attorney Rule 20 Concentration

Susan Herlofsky	412	369	89.6%	106
Atif Khan	54	50	92.6%	21
Jessica Colbert	81	70	86.4%	26
Raissa Carpenter	130	73	56.2%	39
Emmett Donnelly	22	12	54.5%	6

Note: The base rate within this dataset is 58.65% Rule 20 involvement. This dataset is itself already skewed toward Rule 20-heavy cases due to collection methodology. Despite this elevated baseline, attorneys Herlofsky (89.6%), Khan (92.6%), and Colbert (86.4%) sit significantly above it.

Judicial Officer Rule 20 Intensity and Dormant Rate

Lisa Janzen	749	156	20.8%	15.95
Carolina Lamas	407	81	19.9%	16.82
William Koch	286	95	33.2%	10.79
Joel Olson	299	97	32.4%	10.46
Julia Dayton Klein	747	201	26.9%	9.80
Danielle Mercurio	960	231	24.1%	9.59
Michael Browne	528	134	25.4%	10.17
George Borer	648	153	23.6%	9.03

7. DATA COLLECTION METHODOLOGY & EVIDENCE CHAIN

Source Data

All documents were retrieved from the publicly accessible Minnesota Court Records Online (MCRO) system. No unauthorized access, credential theft, or exploitation of system vulnerabilities was employed. The MCRO system is a public-access portal for Minnesota court records.

Collection Process

- Case identification: MCRO search result pages for specific judicial officers were printed to PDF, converted to text using pdftotext, and processed with custom Python scripts to extract case IDs and cross-reference shared cases across judicial officer dockets.
- Automated download: A custom Chrome DevTools automation script with VPN rotation (to avoid rate-limiting) systematically downloaded all available PDF filings for identified cases.
- Session evidence capture: All download sessions were recorded using a custom MITMPROXY + OBS system that captures raw HTTP traffic alongside a video feed. A hash-loop system computed SHA256 hashes of rolling data bundles every 7 seconds and displayed them on the OBS video overlay, creating an unbroken chain of cryptographic evidence for each session.
- Blockchain anchoring: OpenTimestamps (OTS) Bitcoin blockchain anchoring was applied to source files throughout collection, providing independent cryptographic timestamp proof of data existence at specific points in time.

PDF Forensic Analysis

- Internal object extraction: All PDFs were processed using mutool (MuPDF) to explode each document's internal object structure. Every extracted object was hashed with SHA256.
- Text extraction: pdftotext was used to extract normalized text from each document. Text was cleaned (left-justified, single-spaced) and each row hashed individually to enable cross-document text comparison.
- Metadata extraction: XMP metadata fields (create date, metadata date, creator tool, producer, MSIP fields) were extracted and stored for all documents.
- Signature analysis: MCRO digital watermark signatures were verified cryptographically and all signature fields (signer name, timestamp, crypto status, revision count, edits-after-signature flag) were stored.

Database

All findings are stored in a PostgreSQL database (Supabase, us-west-2) with a custom forensic schema. Materialized views and indexes ensure query reproducibility. The database is the primary evidence artifact and is the authoritative source for all statistics in this report.

8. RECOMMENDATIONS FOR INDEPENDENT REVIEW

The findings in this report represent objectively verifiable forensic data anomalies. The following are recommended steps for independent verification and follow-up investigation:

For Independent Forensic Verification

- **Request original file comparison:** Obtain the original archived versions of the five IronPDF-generated documents from the court's internal document management system. Compare their internal PDF structure against the MCRO-served versions. If the internal systems do not contain an IronPDF-generated version, the discrepancy requires explanation.
- **Font identification:** Submit the extracted tracking font binaries (identified by SHA256 hash in this report) to font forensics specialists or the document production system vendor for identification of their origin and purpose.
- **MSIP label source identification:** Request the Microsoft 365 tenant information associated with the MSIP labels on the 34 identified documents. This would identify the specific organizational Microsoft 365 environment that produced these court filings.
- **Signature image provenance:** Determine whether the stored judicial signature image files are held within the court's Odyssey case management system or an intermediary document generation system, and when each version was captured.

For Legal Proceedings

- This report's findings are reproducible from the underlying database. The database, along with its OTS blockchain timestamps and MITMPROXY session recordings, constitutes a contemporaneous evidence chain for the data collection process.
- Findings 1 and 3 (IronPDF generation and the zero-byte ghost font) are the most technically unambiguous anomalies and require the least interpretive context to present to a fact-finder.
- Finding 4 (MSIP labels) is independently verifiable by any party with access to the original PDF files and a PDF metadata reader.
- It is strongly recommended that a credentialed digital forensics examiner (CFCE, EnCE, or equivalent) independently verify the key findings before use in formal legal proceedings.

For questions regarding this report or access to the underlying database, contact: Matthew David Guertin | Case 27-CR-23-1886 | Fourth Judicial District Court, Hennepin County, Minnesota