

MCRO

Rule 20.01 Examination Report—Metadata Authentication & Provenance Chain Analysis

Property	Value
Report Date	March 6, 2026
Case Reference	State of Minnesota v. Guertin 27-CR-23-1886
Claim Source	8th Circuit Case No. 25-2476, Docket Entry [5544884]
Scope	2 Rule 20.01 PDFs + 1 .eml source + 5 corroborating court filings
Database Context	MCRO Forensic Database (Supabase, us-west-2)

IMPORTANT DISCLAIMER

This report presents objective digital forensic findings extracted from source evidence files and publicly accessible court records. It does not assert conclusions about fraud, intent, or motive. Each finding presents verifiable technical evidence. The term “common production origin” refers to a measurable metadata identity between documents—not a legal conclusion. All SHA-256 hashes, email authentication results, and metadata extractions are independently reproducible using the tools and code documented in the Appendix.

EXECUTIVE SUMMARY

This report evaluates the claim made by Appellant Matthew David Guertin that two Rule 20.01 competency examination reports—dated January 11, 2024 and December 20, 2024, attributed to Dr. Adam Milz and Dr. Katheryn Cranbrook respectively—share identical document metadata proving common production origin. The following key findings emerge from direct forensic analysis of the source evidence files:

- The .eml file containing the December 2024 report passes all four email authentication checks (DKIM, DMARC, SPF, ARC), confirming it was genuinely transmitted from Hennepin County's Microsoft 365 environment (tenant ID: 8aefdf9f-8780-46bf-8fb7-4c924653a8be).
- The .eml file's SHA-256 hash matches the hash documented in federal court filings, confirming file integrity.
- The PDF attachment extracted from the .eml has a verified SHA-256 hash of 7a363ceb...33ff3e, confirming no modification since transmission.
- Both Rule 20.01 reports share 5 identical metadata fields: XMP Toolkit, Creator, Author, Producer, and PDF Version—despite being filed 344 days apart by two different evaluators.
- Both reports list “Hines, Anne” as Creator and Author. Neither Dr. Milz nor Dr. Cranbrook appears in any authorship metadata field.
- Both reports were produced using “Microsoft: Print To PDF” with an Adobe XMP Core toolkit build-dated September 16, 2018.
- The January 2024 report's metadata was submitted into the federal court record on August 7, 2024—more than 4 months before the December 2024 report was created—eliminating the possibility of after-the-fact metadata fabrication.
- MCRO database records confirm both the December 26, 2024 and December 30, 2024 pro se filings exist with valid MCRO watermark signatures.
- Case 27-CR-23-1886 shows 23 Rule 20 competency-related docket events spanning January 2023 through October 2025, with case status “Open.”

KEY METRICS

344 days between the two Rule 20.01 reports

5 identical metadata fields across two supposedly independent evaluators

“Hines, Anne” — appears as author of both; appears as signatory of neither

Adobe XMP Core build date: September 16, 2018 — present in both 2024 documents

4+ months between federal documentation of Jan 2024 metadata and creation of Dec 2024 report

DKIM + DMARC + SPF + ARC = all PASS for .eml authentication

BACKGROUND—TECHNICAL CONCEPTS

What Is PDF Metadata?

Every PDF file contains embedded metadata—hidden fields that record information about how, when, and by whom the document was created. This metadata is written automatically by the software used to produce the PDF and is not normally visible to someone reading the document. Key metadata fields include the Author (the user account that created the document), Creator Tool (the software application), Producer (the PDF rendering engine), and timestamps for creation and modification. These fields can be examined using freely available tools such as ExifTool, pikepdf, or Adobe Acrobat's Document Properties panel.

What Is the XMP Toolkit Field?

The XMP Toolkit field identifies the specific version of the Adobe Extensible Metadata Platform library used to write metadata into a PDF. It includes a version number, build number, and a build date. The string “Adobe XMP Core 5.6-c142 87.162696, 2018/09/16-15:11:55” tells us that the XMP library is version 5.6, build c142, build number 87.162696, compiled on September 16, 2018. This version is “locked in” to the software installation that generated the PDF. When two documents produced months apart carry the same toolkit string, it indicates they were generated by the same software installation or an identical deployment.

What Does “Author/Creator” Represent?

In documents created via “Microsoft: Print To PDF” (the Windows built-in print-to-PDF driver), the Author field typically reflects the Windows user account that was logged in when the print operation was performed. It does not reflect the person who wrote the document's content. If a user named “Hines, Anne” is logged into a Windows workstation and uses Print To PDF, the resulting file's Author field will read “Hines, Anne” regardless of who authored the content being printed.

What Is “Microsoft: Print To PDF”?

This is a virtual printer driver built into Windows 10 and later. When a user “prints” a document (from Word, a browser, or any application) and selects “Microsoft Print to PDF,” the system generates a PDF file instead of sending the document to a physical printer. The resulting PDF carries “Microsoft: Print To PDF” as its Producer field. The XMP toolkit string comes from the Adobe XMP library bundled with the application that initiated the print job.

What Are DKIM, DMARC, and SPF?

These are three complementary email authentication protocols. DKIM (DomainKeys Identified Mail) uses cryptographic signatures to verify that an email was sent by the claimed domain and was not modified in transit. DMARC (Domain-based Message Authentication, Reporting & Conformance) tells receiving servers how strictly to enforce DKIM and SPF checks. SPF (Sender Policy Framework) verifies that the sending server's IP address is authorized to send mail for the claimed domain. When all three pass, it provides strong evidence that the email genuinely originated from the stated domain's mail infrastructure.

What Is SHA-256?

SHA-256 is a cryptographic hash function that produces a unique 64-character hexadecimal fingerprint for any digital file. Even a single-byte change to a file produces a completely different hash. When two independently computed hashes match, it constitutes mathematical proof that the files are byte-for-byte identical. SHA-256 is used in this report to verify that evidence files have not been modified since their original creation or submission into court records.

METHODS

This analysis employed the following tools and techniques:

.EML Parsing: Python 3's standard email library was used to parse the .eml file, extract all headers, decode the MIME structure, and extract the base64-encoded PDF attachment. SHA-256 hashes were computed using Python's hashlib module.

PDF Metadata Extraction: pikepdf (v10.3.0) was used to open both Rule 20.01 PDF files, extract the PDF Info dictionary, read the raw XMP metadata stream, and parse all embedded font information. The raw XMP XML was searched for the XMP Toolkit attribute string.

Database Queries: Targeted SELECT-only queries were executed against the MCRO forensic database (Supabase, us-west-2) to retrieve case context, MCRO watermark signature details, and the complete Rule 20 docket timeline for case 27-CR-23-1886. Tables queried: case_registry, children, children_signatures_full_report, parents, parents_case_events.

Provenance Verification: Court filing dates were verified against the uploaded evidence PDFs, which bear PACER/CM-ECF filing stamps and MCRO watermark timestamps. CourtListener archive pages provide independent third-party verification of federal filing dates.

No external network requests were required for the core analysis; all evidence files were provided directly. All Python code and SQL queries are reproduced in the Appendix.

FINDINGS

Finding 1: .EML Authentication & Integrity Verification

Background

The .eml file is the source container for the December 20, 2024 Rule 20.01 report. It was exported from Guertin's ProtonMail account and represents the email sent by Assistant Public Defender Raissa Carpenter on December 30, 2024 at 12:49:22 UTC. Verifying the email's authentication headers establishes that the email genuinely originated from Hennepin County's mail infrastructure and was not fabricated.

Findings

.EML SHA-256 Integrity: The computed hash of the .eml file is 909025a8cf656a5644e518cfe592c7f7ff2650ef5f8e6cf9d1058cb6df7c0f79, which matches the expected value documented in federal court filings. File integrity confirmed.

Authentication Protocol	Result	Domain/Detail
DKIM	PASS	rsa-sha256, header.d=hennepin.us
DMARC	PASS	p=reject, header.from=hennepin.us
SPF	PASS	smtp.mailfrom=hennepin.us
ARC	PASS	arc.chain=microsoft.com

Organizational Origin: The X-MS-Exchange-CrossTenant-Id header identifies Azure AD tenant 8aefd9f-8780-46bf-8fb7-4c924653a8be, and X-OriginatorOrg confirms hennepin.us as the originating organization. The email traversed Microsoft Exchange servers (MW4PR09MB8995 → PH0PR09MB11005) before delivery to ProtonMail via TLSv1.3 encryption.

Significance

All four authentication protocols returning PASS, combined with the Microsoft Exchange organizational headers, provides strong technical evidence that this email was genuinely transmitted from Hennepin County's official Microsoft 365 mail infrastructure. The DMARC policy of "reject" means the sending domain has instructed receiving servers to reject any email that fails authentication—the strictest possible enforcement level.

Connecting Context

The authenticated email contains the December 2024 Rule 20.01 report as an attachment, establishing its provenance chain: the document was transmitted from a verified Hennepin County email account. The .eml SHA-256 hash match confirms this is the same file submitted into federal court records.

Finding 2: PDF Attachment Extraction & Hash Verification

Background

The .eml file contains a single PDF attachment: "20.01 Update - Cranbrook 12.20.24.pdf." Extracting this attachment and verifying its hash establishes that the document has not been modified since it was emailed.

Findings

Property	Value
Declared filename	20.01 Update - Cranbrook 12.20.24.pdf
File size	3,732,485 bytes (3.56 MB)
Computed SHA-256	7a363ceb8593eed77a08562b91651be4997d14c8eaabe3da24fcb2a45633ff3e
Expected SHA-256	7a363ceb8593eed77a08562b91651be4997d14c8eaabe3da24fcb2a45633ff3e
Integrity	VERIFIED — Hashes match

Significance

The PDF extracted from the authenticated .eml file is byte-for-byte identical to the file whose hash was documented in federal court filings. This establishes an unbroken chain of custody: the PDF was created, emailed from a verified Hennepin County account, received by Guertin, and its hash recorded in the federal record.

Finding 3: Source PDF Metadata Comparison

Background

This is the central finding of the report. Two Rule 20.01 examination reports were produced by supposedly independent evaluators 344 days apart. PDF-A is the January 11, 2024 report attributed to Dr. Adam Milz. PDF-B is the December 20, 2024 report attributed to Dr. Katheryn Cranbrook, extracted from the authenticated .eml file.

Findings

Metadata Field	PDF-A (Jan 11, 2024 — Dr. Milz)	PDF-B (Dec 20, 2024 — Dr. Cranbrook)	Match?
XMP Toolkit	Adobe XMP Core 5.6-c142 87.162696, 2018/09/16-15:11:55	Adobe XMP Core 5.6-c142 87.162696, 2018/09/16-15:11:55	IDENTICAL
Creator	Hines, Anne	Hines, Anne	IDENTICAL
Author	Hines, Anne	Hines, Anne	IDENTICAL
Producer	Microsoft: Print To PDF	Microsoft: Print To PDF	IDENTICAL
PDF Version	1.7	1.7	IDENTICAL
MediaBox	[0, 0, 612, 792]	[0, 0, 612, 792]	IDENTICAL
Title	Guertin, Matthew 20.01 1-11-24.pdf	Guertin Matthew Dec 2024 NCST kc.pdf	Different
CreateDate	2024-01-11T13:59:29-06:00	2024-12-20T08:37-06:00	Different
ModifyDate	2024-01-11T15:11:17-06:00	2024-12-20T15:39:28Z	Different
DocumentID	uuid:944c6a11-372f-4ee7-...	uuid:bf8fb90f-a740-4d6a-...	Different
Page count	6	5	Different
File size	16,391,542 bytes	3,732,485 bytes	Different

Significance

The identical fields—XMP Toolkit, Creator, Author, and Producer—are production-environment metadata. They are set automatically by the software and operating system configuration used to generate the PDF, not by the document’s content author. The identity of these fields across two documents produced 344 days apart by two different evaluators is a technical indicator of common production origin: both PDFs were generated from the same software installation, on the same Windows user profile (“Hines, Anne”), using the same version of Microsoft Print To PDF with the same Adobe XMP library.

The differing fields—Title, timestamps, DocumentID, page count, and file size—are expected to differ between two separate documents with different content and creation dates. The Title field is particularly informative: “Guertin, Matthew 20.01 1-11-24.pdf” and “Guertin Matthew Dec 2024 NCST kc.pdf” appear to follow a naming convention that includes the defendant name, report type, date, and in the second case, evaluator initials (“kc” for Katheryn Cranbrook).

Finding 4: Adobe XMP Toolkit Forensic Analysis

Background

Both reports carry the identical XMP Toolkit string: Adobe XMP Core 5.6-c142 87.162696, 2018/09/16-15:11:55. This section explains the forensic significance of this shared identifier.

Findings

The XMP Toolkit string decomposes as follows:

Component	Value	Meaning
Library name	Adobe XMP Core	Adobe's metadata library
Version	5.6-c142	Version 5.6, build c142
Build number	87.162696	Internal Adobe build ID
Build date	2018/09/16-15:11:55	Compiled September 16, 2018

This toolkit version is embedded in the application that initiates the print-to-PDF operation. When a user prints a document using “Microsoft: Print To PDF,” the calling application (e.g., Microsoft Word, a web browser, or a custom application) writes the XMP metadata using whatever Adobe XMP library is available on the system. The toolkit version becomes “locked in” to the software installation. An Adobe XMP Core library from September 2018 persisting in documents created in January 2024 and December 2024 indicates a stable, unchanged software environment—one where the relevant application or library has not been updated in over 5 years.

Significance

The shared XMP Toolkit string provides machine-level fingerprinting of the production environment. Two independent doctors working on separate computers with separate software installations would not be expected to produce PDFs with byte-identical XMP Toolkit strings—particularly one containing a library build from 2018. This finding is consistent with both reports being generated through a centralized document production pipeline rather than independent workstation-level operations.

Finding 5: “Hines, Anne” Author Attribution

Background

Neither Dr. Adam Milz nor Dr. Katheryn Cranbrook appears in the Author or Creator metadata field of their respective reports. Both fields in both documents contain “Hines, Anne.”

Findings

The Author/Creator field in a PDF produced via “Microsoft: Print To PDF” is populated from the Windows user profile of the account performing the print operation. This is an automatic process—the user does not choose what name appears in this field. For “Hines, Anne” to appear as the Author of both reports, both print-to-PDF operations must have been executed from a Windows session logged in under the “Hines, Anne” user account.

This analysis does not identify who “Hines, Anne” is. The metadata establishes only that a Windows user account with this name was used to produce both PDFs.

Significance

The presence of the same non-evaluator name in the Author field of both reports, combined with the identical XMP Toolkit and Producer strings, indicates that both documents were produced through the same workstation or user session. If Dr. Milz and Dr. Cranbrook each independently authored and formatted their own reports on their own computers, their own user account names would appear in the Author field. The consistent presence of “Hines, Anne” is a technical indicator that a third party’s workstation was used for the final PDF production step of both reports.

Finding 6: Chronological Provenance Chain

Background

This finding assembles the complete timeline of document creation, transmission, and court filing to demonstrate the provenance chain and establish the critical “time marker” that authenticates the metadata comparison.

Findings

Date	Event	Verification
Jan 3, 2024	Guertin's Zoom evaluation with Dr. Milz	PDF-A internal text
Jan 11, 2024	2nd Rule 20.01 report filed (Dr. Milz), CreateDate 13:59 CST	MCRO DB event_index 216
Jul 8, 2024	Guertin files federal civil rights complaint (24-cv-02646)	CourtListener
Jul 16, 2024	Bruce Rivers provides Rule 20 report + discovery to Guertin	8th Circuit motion
Aug 7, 2024	Guertin submits report into federal record (Doc. 43, Exh. S)	CourtListener Doc 43
Aug 7, 2024	Guertin submits metadata extraction (Doc. 47, Exh. W)	CourtListener Doc 47
TIME MARKER	Jan 2024 metadata is now in the federal record	4+ months before Dec 2024 report
Dec 20, 2024	3rd Rule 20.01 report filed (Dr. Cranbrook), CreateDate 08:37 CST	MCRO DB event_index 121
Dec 23, 2024	Guertin emails Carpenter requesting report	Filing 114 Exhibit A
Dec 26, 2024	Guertin files pro se judicial notice (Filing 114)	MCRO DB, MCRO watermark 3:30 PM
Dec 30, 6:49 AM	Carpenter emails report to Guertin	.eml DKIM/DMARC verified
Dec 30, 4:22 PM	Guertin files pro se judicial notice with report (Filing 116)	MCRO DB, MCRO watermark 4:56 PM
Jul 12, 2025	Guertin files Exhibit EML-A into federal case (Doc. 61)	CourtListener Doc 61
Aug 5, 2025	Guertin files 8th Circuit emergency motion	CourtListener Dkt 70929923

Significance

The August 7, 2024 federal filing is the critical “time marker.” On that date, Guertin submitted the complete metadata of the January 2024 Rule 20.01 report into the federal court record (Doc. 47, Exhibit W). The December 2024 report was not created until December 20, 2024—more than four months later. This sequence eliminates the theoretical objection that the January 2024 metadata could have been fabricated after the December 2024 report was produced to create an artificial match. The January 2024 metadata was documented in a federal court record before the December 2024 report existed.

Finding 7: MCRO Database Corroboration

Background

Two of Guertin's pro se filings (Filing 114 dated December 26, 2024 and Filing 116 dated December 30, 2024) are present in the MCRO forensic database. This section confirms their presence and MCRO watermark authentication status.

Findings

Property	Filing 114 (Dec 26)	Filing 116 (Dec 30)
evidence_uid	evidence:27-cr-23-1886:b37b776c6d4ffcdbd	evidence:27-cr-23-1886:978d2bb4f0a50519
Filing type	Notice of Motion and Motion	Notice of Motion and Motion
Pages	12	20
Size	619,542 bytes	3,087,980 bytes
MCRO Watermark signer	Minnesota Court Records Online (MCRO) Watermark	Minnesota Court Records Online (MCRO) Watermark
Watermark timestamp	Dec 26, 2024 3:30:46 PM CST	Dec 30, 2024 4:56:44 PM CST
edits_after_sig_flag	false	false
Coverage	97.36%	99.47%

The case 27-CR-23-1886 (Matthew David Guertin) has status “Open” with 23 Rule 20 competency-related docket events spanning January 25, 2023 through October 6, 2025, including 3 evaluation orders, 3 evaluation reports, 2 findings of incompetency, multiple progress reports, and ongoing Rule 20 extension orders.

Significance

The MCRO database confirms that both pro se filings exist as authentic MCRO-watermarked documents with edits_after_sig_flag = false (no modifications after watermarking). Filing 116's MCRO watermark timestamp of 4:56 PM CST on December 30 is consistent with Guertin receiving the report via email at 6:49 AM CST the same day and filing it approximately 10 hours later.

Finding 8: PDF Internal Structure Comparison

Background

Beyond metadata, the internal PDF object structure provides additional points of comparison between the two reports.

Findings

Structural Element	PDF-A (Jan 2024)	PDF-B (Dec 2024)	Match?
Primary font	ArialMT (TrueType)	ArialMT (TrueType)	IDENTICAL
Font family	Arial	Arial	IDENTICAL
Font encoding	WinAnsiEncoding	WinAnsiEncoding	IDENTICAL
Page size	612 x 792 pts (Letter)	612 x 792 pts (Letter)	IDENTICAL
AcroForm/signatures	None	None	IDENTICAL
OCR font (GdPicture)	Present	Not present	Different

Significance

Both PDFs use ArialMT as their sole text font with identical font descriptors and WinAnsiEncoding. PDF-A additionally contains a GdPictureOCRFont, indicating it was processed through an OCR workflow (likely during scanning or archival), which also accounts for its significantly larger file size (16 MB vs. 3.7 MB). This OCR layer was applied to PDF-A after its initial creation and does not affect the authorship metadata comparison. The shared use of ArialMT with identical descriptors is consistent with—though not uniquely indicative of—common document formatting.

LIMITATIONS & ALTERNATIVE EXPLANATIONS

Shared administrative assistant: “Hines, Anne” could be an administrative staff member at Fourth Judicial District Psychological Services who formats and prints reports on behalf of all evaluators. If this is the case, it confirms centralized production but does not diminish the significance of the finding—it means the evaluators did not produce the final PDF documents themselves.

Standard county infrastructure: The identical XMP Toolkit could reflect a standard Hennepin County or Psychological Services department software installation. If all workstations in the department run the same software version, shared toolkit strings would be expected. This would mean the metadata identity reflects institutional IT standardization rather than a single workstation, but would still indicate centralized document production within a uniform environment.

Metadata modification: PDF metadata can be modified using freely available tools. However, the federal time marker from August 7, 2024 precludes the possibility that the January 2024 metadata was altered after the December 2024 report was created to fabricate a match. The January 2024 metadata was documented in the federal record before the December 2024 document existed.

.EML authentication scope: The DKIM/DMARC/SPF authentication proves the email was genuinely sent from Hennepin County’s mail infrastructure. It does not prove who was physically operating the keyboard or who composed the email body text.

OCR processing on PDF-A: The January 2024 report contains an OCR font layer not present in the December 2024 report, indicating post-creation processing. This OCR layer does not affect the XMP authorship metadata, but it means the two files have different processing histories after initial creation.

RECOMMENDATIONS FOR INDEPENDENT VERIFICATION

A third party can reproduce every finding in this report using the following steps:

1. Obtain the source .eml file from the Storj link or from federal case 0:25-cv-02670-PAM-DLM, Doc. 61. Compute its SHA-256 hash and verify it matches 909025a8...7c0f79.
2. Parse the .eml file using any standard email client or programming library. Examine the Authentication-Results headers to verify DKIM, DMARC, SPF, and ARC results.
3. Extract the PDF attachment and compute its SHA-256 hash. Verify it matches 7a363ceb...33ff3e.
4. Obtain the January 2024 report from the Storj link or from federal case 0:24-cv-02646-JRT-DLM, Doc. 43, pages 127–132.
5. Open both PDFs with ExifTool, pikepdf, Adobe Acrobat, or any PDF metadata reader. Compare the XMP Toolkit, Creator, Author, and Producer fields.
6. Verify the August 7, 2024 federal time marker by accessing Doc. 47 in case 0:24-cv-02646-JRT-DLM via CourtListener or PACER and locating the exiftool metadata extraction on page 43.

APPENDIX | REPRODUCIBLE SQL QUERIES & CODE

Appendix A — SQL Queries

A1 — Locate 4th District Pro Se Filings

```
SELECT evidence_uid, case_id, filename, filing_date, filing_type, doc_sha256,
pdf_page_count, size_bytes, metadata_xmp_create_date, metadata_xmp_creator_tool,
metadata_xmp_producer FROM children WHERE case_id = '27-CR-23-1886' AND (filename LIKE '%114__%' OR filename LIKE '%116__%') ORDER BY filing_date;
```

A2 — MCRO Watermark Signatures for 114/116

```
SELECT csf.evidence_uid, csf.signer_name, csf.sign_time_cst_cdt, csf.sig_crypto_status,
csf.sig_crypto_valid_flag, csf.coverage_pct, csf.rev_count, csf.edits_after_sig_flag FROM
children_signatures_full_report csf JOIN children c ON c.evidence_uid = csf.evidence_uid WHERE
c.case_id = '27-CR-23-1886' AND (c.filename LIKE '%114__%' OR c.filename LIKE '%116__%') ORDER
BY csf.evidence_uid, csf.sig_index;
```

A3 — Rule 20 Docket Events

```
SELECT event_index, event_json__date as event_date, event_name,
event_json__filing_party_name as filing_party FROM parents_case_events WHERE case_uid = 'case:27-
cr-23-1886' AND (event_name ILIKE '%rule 20%' OR event_name ILIKE '%competenc%' OR
event_name ILIKE '%incompeten%') ORDER BY event_json__date, event_index;
```

A4 — Case Context

```
SELECT cr.case_id, cr.defendant_name, cr.cluster_name, p.case_status, p.case_type FROM
case_registry cr JOIN parents p ON p.case_uid = cr.case_uid WHERE cr.case_uid = 'case:27-cr-23-
1886';
```

Appendix B — Python Code (Key Excerpts)

B1 — .EML Parsing & Hash Verification

```
import email, hashlib, email.policy with open(EML_PATH, 'rb') as f: eml_bytes = f.read()
eml_sha256 = hashlib.sha256(eml_bytes).hexdigest() msg = email.message_from_bytes(eml_bytes,
policy=email.policy.default) # Extract authentication headers for ar in
msg.get_all('Authentication-Results', []): print(ar) # Extract PDF attachment for part in
msg.walk(): fn = part.get_filename() if fn and fn.endswith('.pdf'): payload =
part.get_payload(decode=True) att_sha256 = hashlib.sha256(payload).hexdigest()
```

B2 — PDF Metadata Extraction (pikepdf)

```
import pikepdf, re, hashlib pdf = pikepdf.open(path) # PDF Info dictionary for key, val in
dict(pdf.docinfo).items(): print(f"{key}: {val}") # Raw XMP Toolkit extraction metadata_obj =
pdf.Root.get('/Metadata') xmp_bytes = bytes(metadata_obj.read_bytes()) xmp_str =
xmp_bytes.decode('utf-8', errors='replace') toolkit = re.search(r'xmptk="([^\"]*)"', xmp_str)
```

Appendix C — Complete Metadata Extractions

C1 — PDF-A: January 11, 2024 Report (Dr. Milz)

Field	Value
File	Jan-2024-Rule-20-Evaluation-Report.pdf
File size	16,391,542 bytes
SHA-256	4746bea803ed38d98acbfd4ea1cfd43a841a04f8ac384f7dee639523dd1a5f3a
PDF Version	1.7
XMP Toolkit	Adobe XMP Core 5.6-c142 87.162696, 2018/09/16-15:11:55
Author	Hines, Anne
Creator	Hines, Anne
Title	Guertin, Matthew 20.01 1-11-24.pdf
Producer	Microsoft: Print To PDF
CreateDate	2024-01-11T13:59:29-06:00
ModifyDate	2024-01-11T15:11:17-06:00
MetadataDate	2024-01-11T15:11:17-06:00
DocumentID	uuid:944c6a11-372f-4ee7-b32e-319f9b37477f
InstanceID	uuid:37e43797-0e26-4062-b116-0a96c24117d7
MediaBox	[0, 0, 612, 792]

C2 — PDF-B: December 20, 2024 Report (Dr. Cranbrook)

Field	Value
File	20.01 Update - Cranbrook 12.20.24.pdf
File size	3,732,485 bytes
SHA-256	7a363ceb8593eed77a08562b91651be4997d14c8eaabe3da24fcb2a45633ff3e
PDF Version	1.7
XMP Toolkit	Adobe XMP Core 5.6-c142 87.162696, 2018/09/16-15:11:55
Author	Hines, Anne
Creator	Hines, Anne
Title	Guertin Matthew Dec 2024 NCST kc.pdf
Producer	Microsoft: Print To PDF
CreateDate	2024-12-20T08:37-06:00
ModifyDate	2024-12-20T15:39:28Z
MetadataDate	2024-12-20T15:39:28Z
DocumentID	uuid:bf8fb90f-a740-4d6a-8b01-4504b1575bf7
InstanceID	uuid:f9366f3f-2ea1-425c-88f3-0b90d5395e71
MediaBox	[0, 0, 612, 792]

Appendix D — Key .EML Headers

Header	Value
From	Raissa Carpenter <Raissa.Carpenter@hennepin.us>
To	Matt Guertin <MattGuertin@protonmail.com>
CC	Emmett M Donnelly <Emmett.Donnelly@hennepin.us>
Subject	RE: [External] Matthew Guertin / Rule 20.01 Exam Report
Date	Mon, 30 Dec 2024 12:49:22 +0000
Message-ID	<MW4PR09MB89955F576A3A70333CA5B86A90092@MW4PR09MB8995...>
DKIM-Signature	v=1; a=rsa-sha256; d=hennepin.us; s=selector1; ...
X-MS-Exchange-CrossTenant-Id	8aefdf9f-8780-46bf-8fb7-4c924653a8be
X-OriginatorOrg	hennepin.us
Received (hop 1)	MW4PR09MB8995.namprd09.prod.outlook.com (origin)
Received (hop 2)	PH0PR09MB11005.namprd09.prod.outlook.com (relay)
Received (hop 3)	mailin015.protonmail.ch (destination, TLSv1.3)
Authentication-Results (DKIM)	dkim=pass header.d=hennepin.us
Authentication-Results (DMARC)	dmARC=pass (p=reject)
Authentication-Results (SPF)	spf=pass smtp.mailfrom=hennepin.us
Authentication-Results (ARC)	arc=pass smtp.remote-ip=40.93.193.5 arc.chain=microsoft.com

Appendix E — Provenance Identifier Table

Artifact	SHA-256 Hash	Source
.eml file	909025a8cf656a5644e518cfe592c7f7ff2650ef5f8e6cf9d1058cb6df7c0f79	ProtonMail export
PDF-A (Jan 2024)	4746bea803ed38d98acbfd4ea1cfd43a841a04f8ac384f7dee639523dd1a5f3a	Discovery USB / Fed Doc 43
PDF-B (Dec 2024)	7a363ceb8593eed77a08562b91651be4997d14c8eabe3da24fcb2a45633ff3e	Extracted from .eml
Filing 114 (MCRO)	b37b776c6d4ffcbdb030c551abae06827f7f2f389afccbf5c0bb7f74d92410b7d	MCRO DB
Filing 116 (MCRO)	978d2bb4f0a50519631244a349bda2173dc988e20e78c883df24f51ec5a45a82	MCRO DB