UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

JOSEPH D. KIRCHNER,
Plaintiff,

vs.

KEITH ELLISON, in his official capacity as Attorney General of the State of Minnesota,
Defendants.

Case No. _____

NETWORK FORENSIC EVIDENCE PACKAGE

EXHIBIT SUMMARY

This exhibit package documents a TCP RST injection attack targeting Plaintiff's encrypted DNS-over-HTTPS (DoH) connection on January 23, 2026, which caused email delivery failure to Minnesota law enforcement agencies while Plaintiff was gathering evidence for this Petition.

Sub-Exhibit	Description
G-1	Package Summary: Executive summary of attack evidence and key findings
G-2	TCP RST Attack Analysis: 6 injected RST packets in 65ms window
G-3	DNS Analysis: Infrastructure mapping showing Comcast DoH servers
G-4	DoH Connection Attack: Timeline of encrypted DNS connection termination
G-5	Anomaly Timestamp Reference: 1-microsecond FIN-to-RST gap proving injection

NOTICE REGARDING UNDERLYING FORENSIC DATA

Custody of Original Evidence

Plaintiff maintains custody of the complete forensic evidence package, including:

- **Original packet capture files** (`.pcapng` format) containing raw network traffic
- **SHA-256 cryptographic hash manifests** (`.sha256`) for verification of data integrity
- **Chain of custody documentation** establishing evidence handling procedures
- **Full technical analysis files** with complete packet-level forensic data

Evidence Specifications

Item	Description	Size
Primary capture file	`seg_20260123_155910.pcapng`	10,261,712 bytes (9.79 MB)
Hash verification	`02_HASHES.sha256`	—
Chain of custody	`01_CHAIN_OF_CUSTODY.md`	—
Complete analysis	Full technical documentation	—

Cryptographic Verification

The primary packet capture file can be verified using the following SHA-256 hash:

> File: 03_source_evidence/original/seg_20260123_155910.pcapng SHA-256:
> c57d32d759b7f56c98c4dfc1b15c86ed0c4b242f13b57da411f2e04cc5d4bfe2

This hash was computed at the time of evidence collection and can be used to verify that the file has not been modified.

Availability for Court Review

The complete evidence package, including all original `.pcapng` capture files and supporting forensic documentation, is **available upon request** by:

1. The Court — for in camera review or technical verification

2. Defendant — through formal discovery procedures

3. Court-appointed expert — if the Court requires independent technical analysis

Verification Procedure

Any party may verify the integrity of the forensic evidence through:

1. Hash verification: Original SHA-256 hashes computed at time of capture can be compared against current file hashes to prove data has not been modified

2. Independent analysis: The `.pcapng` files can be opened in Wireshark or equivalent network analysis tools for independent verification of the findings presented in Exhibits G-1 through G-5

3. Chain of custody review: Documentation establishing when, how, and by whom evidence was captured and preserved

Request Procedure

To request access to the complete forensic evidence package, contact:

Joseph D. Kirchner
Plaintiff, Pro Se
4440 Parklawn Avenue #203
Edina, MN 55435
Tel: (612) 552-2122
Email: legal@lawsofexistence.com

Plaintiff will provide the requested materials within **48 hours** of receipt of a valid request, or as otherwise directed by the Court.

CERTIFICATION

I, Joseph D. Kirchner, hereby certify that:

1. The forensic evidence summarized in Exhibits G-1 through G-5 is derived from original packet capture files in my custody;

2. The original `.pcapng` files have not been modified since capture, as verifiable through SHA-256 cryptographic hashes computed at the time of evidence collection;

3. I will produce the complete forensic evidence package, including all original capture files and supporting documentation, upon request by the Court or through proper discovery procedures;

4. The chain of custody for this evidence has been maintained and documented.

Dated: January 27, 2026

_____

JOSEPH D. KIRCHNER

Plaintiff, Pro Se

CORROBORATING EVIDENCE IN RELATED PROCEEDINGS

For additional forensic evidence documenting the broader attack pattern against Plaintiff, see the following exhibits filed in *Kirchner v. Johnson et al.*, No. 1:25-cv-02735-ACR (D.D.C.):

- ECF No. 13-52 (Network attack documentation)
- ECF No. 13-55 (Router forensic analysis)
- ECF No. 13-60 (ISP infrastructure evidence)

These exhibits document attacks spanning May 24, 2025 through January 2026, establishing the pattern of which the January 23, 2026 attack is part.