

# NOTICE OF DIGITAL EVIDENCE PRESERVATION METHODOLOGY

\*\*IN THE UNITED STATES DISTRICT COURT\*\*

\*\*FOR THE DISTRICT OF MARYLAND\*\*

\*\*MARVIN TUTT\*\*

\*Plaintiff,\*

v.

\*\*STATE OF MARYLAND, et al.\*\*

\*Defendants.\*

\*\*Case No.: 8:25-cv-02006-TDC\*\*

---

## NOTICE OF DIGITAL EVIDENCE PRESERVATION METHODOLOGY

Plaintiff hereby notifies all parties that comprehensive digital forensics methodology is being employed to preserve evidence integrity in this matter.

## GITFORENSICS IMPLEMENTATION

Full methodology available at **gitforensics.org**

Plaintiff utilizes Git-based cryptographic verification systems that create:

- Immutable timestamps through distributed repositories
- Cryptographic hashes preventing undetectable tampering
- Multiple independent verification points
- Public transparency ensuring accountability

### ## BEHAVIORAL PATTERN DOCUMENTATION

**All behavioral patterns are being documented**, including but not limited to:

- Repository access patterns
- Document viewing frequencies
- Timing correlations with case events
- Evidence of monitoring by parties
- Attempts to access or modify evidence

### ## WHAT THIS MEANS FOR ALL PARTIES

1. **Every interaction creates evidence** - Access logs are preserved
2. **Tampering is mathematically detectable** - Hash chains reveal modifications
3. **Transparency prevents denial** - Public repositories create witnesses

4. **\*\*Behavioral patterns reveal intent\*\*** - Monitoring patterns show consciousness

## ## SPECIFIC IMPLEMENTATIONS

- Case documentation repository with full version control
- Cryptographic signatures on all evidence
- Distributed backup systems preventing single-point failure
- Real-time monitoring of access patterns
- Correlation analysis of behavioral responses

## ## THE NETWORK EFFECT

Each party accessing documentation creates additional verification points:

- Cloning creates timestamps
- Downloads leave traces
- Monitoring reveals interest levels
- Patterns demonstrate consciousness of issues

## ## LEGAL SIGNIFICANCE

This methodology ensures:

- Evidence tampering becomes provably detectable
- Spoliation attempts create their own evidence

- Good faith interactions are documented
- Bad faith behaviors are revealed

### ## INVITATION TO VERIFY

All parties are invited to:

- Clone repositories for independent verification
- Examine cryptographic proofs
- Verify timestamp integrity
- Confirm evidence authenticity

**\*\*Transparency ensures evidence manipulation is mathematically detectable.\*\***

### ## FAIR NOTICE

This notice serves to inform all parties that:

1. Digital preservation methods are active
2. All interactions are being documented
3. Behavioral patterns create evidence
4. Transparency is the goal

Parties should govern themselves accordingly.

**\*\*Respectfully submitted,\*\***

/s/ Marvin Tutt

Marvin Tutt

Pro Se Plaintiff

**\*\*Date:\*\* July 15, 2025**

---

## **## CERTIFICATE OF SERVICE**

I hereby certify that on July 15, 2025, I served a true and correct copy of the foregoing Notice of Digital Evidence Methodology upon the following parties via certified mail and first-class mail:

Charles County Child Support Administration

200 Kent Avenue

La Plata, MD 20646

Charles County Department of Social Services

200 Kent Avenue

La Plata, MD 20646

State of Maryland

c/o Office of the Attorney General

200 Saint Paul Place

Baltimore, MD 21202

Charles County, Maryland

200 Charles Street

La Plata, MD 20646

Shara Gabrielle Hendler, Esq.

c/o Charles County Child Support Administration

200 Kent Avenue

La Plata, MD 20646

Andrea Khoury

c/o Charles County Circuit Court

200 Charles Street

La Plata, MD 20646

Mistey L. Metzgar

c/o Charles County Circuit Court

200 Charles Street

La Plata, MD 20646

I certify under penalty of perjury that the foregoing is true and correct.

/s/ Marvin Tutt

Marvin Tutt

Pro Se Plaintiff

Date: July 15, 2025