DIGITAL INNOCENCE INITIATIVE

National Digital Evidence Readiness Framework

For Public Defense

From the next case through post-conviction

THE READINESS PROBLEM

Evidence of noninvolvement often exists.

Modern life creates overlapping digital footprints across devices, accounts, providers, cameras, vehicles, wearables, businesses, and connected systems.

But the best evidence may be time-sensitive.

BEGIN EVERY CASE WITH THREE QUESTIONS

1 WHAT WAS COLLECTED?

What digital evidence was collected, examined, and disclosed?

2 WHAT IS MISSING?

What should reasonably exist but is missing, incomplete, inaccessible, or unexplained?

3 WHAT MAY DISAPPEAR?

What missing evidence is time-sensitive and risks being overwritten?

Discovery is a baseline—not the universe of evidence. Investigate the blank spaces.

EARLY ASSESSMENT PROCESS

1 **ASSESS** — Evidence universe

2 **BASELINE** — State's work

3 **TRIAGE** — Loss risk

4 **COLLECT / REQUEST** — Preserve and obtain

5 **REVIEW / ESCALATE** — Verify and get help

You do not need to become a forensic examiner.

Recognize the source • protect the opportunity • request the underlying evidence • know when to get help

THREE PATHWAYS INTO THE FRAMEWORK

INDIVIDUAL

Digital Evidence Toolbox

Free practical resources for the next case.

ACCESS THE TOOLBOX

AGENCY

Digital Evidence Review Unit — DERU

Make early assessment repeatable. Begin with one person and one case.

START DERU

POST-CONVICTION

Assessment Criteria + Technical Guide

Screen appropriate older cases for renewed digital-evidence review.

BEGIN PRIORITY REVIEW

BEGIN NOW

One defender. One checklist. One early assessment.

Toolbox: digitalevidencetoolbox.com

Framework + DERU: digitalinnocence.com

Digital evidence should be a standard part of defense—from day one to post-conviction.