Ready for your agency's review.

DEVI is one digital forensics workspace for the whole case, from the first call to the courtroom. This brief answers what IT, security and legal teams ask first: where evidence lives, who can get in, how files are checked and where DEVI stands on CJIS.

WHERE EVIDENCE LIVES

In your agency's DEVI Cloud workspace, encrypted with your agency's own key. The Windows tools work on your own computer.

WHO CAN GET IN

Only people your agency's administrator adds, each with a role. An account alone opens nothing.

HOW FILES ARE CHECKED

Every release file has a published SHA-256, and the Windows apps are Authenticode-signed.

WHERE CJIS STANDS

Built to CJIS Security Policy controls. A readiness review is in progress, one requirement at a time.

Where the case lives

In DEVI Cloud

Cases live in your agency's workspace. Each agency has its own encryption key.

Hashed on arrival

Every upload is hashed when it arrives and kept as received. Every action names a person.

On your own computer

The Windows tools verify evidence, open iCloud returns and look up app records without sending evidence to DEVI.

Accounts and access

1. **Request a demo.** Tell us who you are, your agency or firm and your role.
2. **DEVI sets up your agency** and its first administrator, who gets an email to sign in.
3. **Your administrator adds your team,** each person with the role they need.

Sign-in

Every DEVI Cloud account signs in with a password and an authenticator code.

Only people your agency's administrator adds can sign in, each with a role.

A lost device can be signed out of every session.

How evidence is handled

Verification is read-only: DEVI recomputes hashes and compares them with values from another tool or process.

Hashing, verification and provider-return decryption never use the network. Keys and passphrases are not saved.

The desktop tools make one network request: an optional, signed update check.

CJIS, in plain words

DEVI is being built to the controls of the FBI CJIS Security Policy, with a readiness review in progress.

Each agency decides, with its CJIS Systems Agency, whether a tool meets its requirements. Some requirements belong to the agency.

Independent assessments will be listed on the Trust Center as they are completed.

Encryption

Current TLS to every service.

Data at rest in our infrastructure is encrypted. Cases in DEVI Cloud use keys that belong to your agency.

Administrative access to our cloud environment is restricted, requires multi-factor authentication and is logged.

Downloads

Downloads come only through the department's DEVI link.

Every release file has a published SHA-256. Check it with Get-FileHash or certutil before you run it.

Windows apps, installers and uninstallers are Authenticode-signed with a timestamp.

Changes and reporting

Infrastructure is defined as code and changed through a reviewed process.

Report a vulnerability to security@deviops.app. A security.txt is published at /.well-known/security.txt.

Each lab should validate DEVI under its own procedures before relying on it.

See DEVI on a test case.
No contract, no payment details, no commitment.

deviops.app/demo