

Questions Every Prosecutor Should Ask About Digital Evidence

Are you getting the most complete, secure and courtroom-ready evidence possible?

Digital evidence is now central to nearly every case, often spanning two to five devices or data sources.

Use these questions to ensure your office consistently applies the most current and defensible digital evidence practices, helping you uncover the complete story in every case.

1. Am I getting the full picture from each device?

- Do I know what type of extraction I've received — logical (user data only) or full file system (includes encrypted, deleted and hidden data)?
- Have I asked whether additional data sources — like cloud backups, third-party apps or deleted content — were captured?
- If I'm only receiving PDFs or screenshots, could key data be missing?

Why it matters: Understanding the extraction type helps you know how complete your evidence is and whether additional data may strengthen your case.

2. Is the evidence I receive verified and defensible in court?

- Does the package include a verification or hash report showing the data hasn't been altered?
- Is there a clear chain of custody from extraction through delivery?
- Was the data collected with a validated forensic method recognized by your jurisdiction?

Why it matters: Unverified or poorly documented evidence can be challenged or dismissed in court—undermining your case.

3. How securely and efficiently am I receiving evidence?

- Is evidence being transferred through a secure, trackable system with audit trails?
- Is my team still relying on physical media or email attachments that could be lost or delayed?
- Can I control/verify who has access to the report and when?
- Does the report I have exactly match the evidence extracted from the device (no missing or corrupted data)?

Why it matters: Lack of control increases the risk of data loss, tampering and compliance violations, all of which can jeopardize a case.

4. Can I collaborate on evidence securely without compromising integrity?

- Am I viewing reports in a read-only format that preserves authenticity?
- Can I confidently share tagged artifacts with defense or co-counsel knowing they remain unchanged?
- Do my current tools support tagging and commenting workflows that preserve chain-of-custody and ensure consistent review across parties?

Why it matters: Secure collaboration maintains evidence integrity, ensures consistent versions across parties and simplifies disclosure.

5. Does my team really know what they're looking at?

- Are investigators and analysts using current, validated forensic tools for extraction and evidence transfer?
- Are workflows tested and aligned with modern forensic standards?
- Have prosecutors and staff received recent training on interpreting digital reports?

Why it matters: When teams lack the right tools or training, cases slow down, trials are delayed and key evidence can be missed.

Next step:

Schedule time to discuss how these challenges may be impacting your prosecution success and case closure rates.

Cellebrite can help you evaluate your current process and ensure every case is built on complete, secure and court-ready evidence.