

X posts, preserved with proof anyone can check

Same-day capture of X (Twitter) posts and X Spaces, each with a fingerprint, an independent timestamp and a custody record. Lightweight eDiscovery, sized for a few posts, not terabytes.

Today's alternative is a screenshot

- Posts get deleted, edited or hidden, often as soon as a dispute starts.
- A screenshot on its own is easy to fake, so it is easy to challenge. Opposing counsel only has to ask "how do we know this is real?"
- X Spaces (live audio rooms) are gone once the broadcast ends, along with who spoke and what the chat said.

Rapid response

When a client calls because someone has just posted about them, capture can start the same day. Once a post is captured, it stays in the record even if the author later deletes it or locks the account. Deleted-post checks then record when posts disappear from X, which matters if spoliation becomes an issue.

What we do

Posts from named accounts, over a date range, or matching key words; and X Spaces: who hosted and spoke, the room chat, X's live captions and, where available, the recording.

What you receive

ITEM	WHAT IT GIVES YOU
Exhibit packet (PDF)	Every post with its text, author, date and time, and a working link, Bates-numbered for production; the post list also as an editable Word file.
Picture of each post	An image of every post as X displayed it: author, text, photos, date and the likes and views, the way people are used to seeing it. Made from a thread, a search, a profile or a list of post links; as a PDF or one image file per post.
Posting date from X itself	X builds the moment a post was created into its ID. The date is decoded from that, not taken from a screenshot.
Account details	In the spreadsheet: the permanent user ID, @username, display name and follower count (both names can change later), plus a dated history of the profile (name, bio, location, followers) from the first capture.
Reach	In the spreadsheet: views, likes, reposts, replies and quotes as X reported them at capture.
Integrity fingerprint	A SHA-256 fingerprint of each post, taken at capture. Any later change to the record shows up as a mismatch.
Independent date proof	Each fingerprint is anchored in the Bitcoin blockchain (OpenTimestamps), proving the record existed no later than that date. Anyone can check it with free tools, without trusting us.
Proof files (.ots)	The Bitcoin timestamp proof for each post, for an expert to verify.

ITEM	WHAT IT GIVES YOU
Cross-check with X	At capture, X's own public embed service is asked to confirm the post's text and author.
Chain of custody	A tamper-evident log of every step taken with each record. Each entry is linked to the one before it, so a removed or edited entry is detected.
Declaration or certification	Signed by the person who made the capture: the federal form (28 U.S.C. § 1746) or a New Jersey certification in lieu of oath (Rule 1:4-4(b)).
Spreadsheet	All records as a CSV file (opens in Excel) for your own review.

The posting date, the fingerprint, the Bitcoin timestamp and the X cross-check can each be repeated by someone else, without trusting us or our software. That is what makes the evidence hard to attack.

What the record proves, and what it leaves to you

The record proves what an account posted, when, and that the copy has not changed since. Showing who was behind the account (authentication of authorship) remains part of your case, through the content itself, testimony or a subpoena to X. The preserved account details and posting history give you material to build that on.

Typical matters

- Family and custody disputes
- Employment disputes and workplace (HR) investigations: harassment, retaliation, misconduct
- Defamation, online harassment, restraining and protective orders
- Personal injury and criminal defense: a claimant's, witness's or complainant's own posts
- Impersonation and misuse of a brand

Why not a big eDiscovery vendor?

- Sized for a handful of posts up to a couple of thousand per exhibit, not for a whole company's email.
- A flat fee per matter, quoted up front.
- Nothing to install and nothing to learn: you send the accounts, you receive the packet.

How it works

1. Send us the accounts, the date range or key words, and any X Spaces rooms.
2. You receive a written flat-fee quote, usually the same day.
3. Capture starts the same day as your go-ahead. Posts are preserved even if they are deleted afterwards.
4. You receive the packet, the spreadsheet and the signed declaration. Payment terms are set out in the engagement terms.

Contact

ExhibitProof

Email: ozdemir@salesforcehub.us

Website: exhibitproof.com

Service area: New Jersey and nationwide

Captures are made of content visible to a standard signed-in X account, through the ordinary X website. Not a law firm; no legal advice is given, and admissibility is always for the court to decide. Not affiliated with or endorsed by X Corp. "X" is a trademark of X Corp. © Salesforce Hub LLC, Clifton, New Jersey. Salesforce Hub LLC is an independent software company. It is not affiliated with, endorsed by or sponsored by Salesforce, Inc. Salesforce is a trademark of Salesforce, Inc.

Terms used in this document

X AND ITS ACCOUNTS

X (Twitter)

The social network formerly called Twitter, renamed X in 2023. A "post" is what used to be called a tweet.

@username and display name

The @username (handle) is the account's address on X; the display name is the name shown above posts. The owner can change either at any time, so both are recorded at capture.

User ID

A permanent number X gives each account. Unlike the @username and display name, it never changes, so it identifies the account even after a rename.

Post ID

The long number at the end of a post's web address. X builds the exact moment the post was created into this number (X calls it a "Snowflake" ID), so anyone can decode the posting date with a public formula.

Locked (protected) account

An X account whose owner has limited who can see its posts. Posts captured before the account was locked stay in the record.

X Spaces

Live audio rooms on X. A host runs the room, co-hosts and speakers talk "on stage", and everyone else listens in the audience. X sometimes keeps a replay afterwards.

Live captions

The automatic text X shows on screen while people speak in a Space.

X's public embed service (oEmbed)

The service X itself provides so websites can display a post. Asking it about a post returns X's own copy of the text and author, which is compared with the capture.

PROOF AND INTEGRITY

SHA-256 fingerprint (hash)

A 64-character code calculated from a record's content. The same content always gives the same code; changing even one character gives a completely different one. So if the code still matches later, the record has not been changed. The code cannot be turned back into the content.

Tamper-evident

Any change leaves a visible trace. It does not mean change is impossible; it means a change cannot go unnoticed.

Chain of custody

A record of every step taken with a piece of evidence: who handled it, when, and what was done, to show it was not altered along the way. Here each entry is linked to the one before it, so a deleted or edited entry is detected.

Blockchain

A public record kept as identical copies on thousands of independent computers worldwide. Once something is written into it, nobody can quietly change or back-date it.

Bitcoin timestamp (OpenTimestamps)

OpenTimestamps is a free, open service that writes a record's fingerprint into the Bitcoin blockchain. That proves the record existed no later than that date. Only the fingerprint is sent, never the post itself.

Deleted-post check

A later look at X to see whether captured posts are still there. Posts that have disappeared are flagged; the preserved copy and its proof stay unchanged.

LEGAL TERMS

Authentication

Showing that evidence is what it is claimed to be (Federal Rule of Evidence 901; in New Jersey, N.J.R.E. 901). For a post, that includes showing who was behind the account.

Spoilation

The destruction or hiding of evidence a party had a duty to preserve, for example deleting posts after a lawsuit is expected. Courts can sanction it.

Declaration (28 U.S.C. § 1746)

A written statement signed under penalty of perjury, which federal law accepts in place of a notarized affidavit. New Jersey state courts accept a similar "certification in lieu of oath" (Rule 1:4-4(b)).

eDiscovery

Finding, preserving and handing over electronic information (email, files, social media posts) in a lawsuit. Large eDiscovery platforms are built for whole companies' data.

Production

Handing documents over to the other side during discovery. "Numbered for production" means ready to hand over.

Bates numbering

A unique, sequential number given to every page or item produced in a lawsuit (for example EX-0001), so each one can be cited and tracked without confusion.

Engagement terms

The written agreement between the firm and us for a matter: what is captured, the fee, confidentiality, and how long material is kept.

WHAT YOU RECEIVE

Exhibit packet

The set of documents delivered for a matter: the captured posts laid out and numbered, ready to attach to a filing as exhibits.

.ots proof file

A small file, one per post, that lets anyone check the Bitcoin timestamp with the free OpenTimestamps tools, without using this software.

CSV

A plain spreadsheet file that opens in Excel, Numbers or Google Sheets.