Association of
Title IX Administrators

NOT FOR DISTRIBUTION

Leveraging Technology in Civil Rights Investigations

An ATIXA Best Practices Workshop

WELCOME!

- Please log in to your ATIXA Event Lobby to access the training slides, supplemental materials, and to log your attendance.
- The ATIXA Event Lobby can be accessed by scanning the QR code or by visiting **www.atixa.org/atixa-event-lobby**.
- You will be asked to enter your registration email to access the Event Lobby.
- Links for any applicable training evaluations and learning assessments are also provided in the ATIXA Event Lobby.
- If you have not registered for this training, an event will not show in your Lobby. Please email **events@atixa.org** or engage the ATIXA website chat app to inquire ASAP.

Any advice or opinion provided during this training, either privately or to the entire group, is **never** to be construed as legal advice or an assurance of compliance. Always consult with your legal counsel to ensure you are receiving advice that considers existing case law in your jurisdiction, any applicable state or local laws, and evolving federal guidance.

Content Advisory

The content and discussion in this training will engage with protected characteristic-based harassment, discrimination, violence, and associated sensitive topics that can evoke strong emotional responses.

ATIXA faculty members may offer examples that emulate the language and vocabulary that educators may encounter in their roles including slang, profanity, and other graphic or offensive language. It is not used gratuitously, and no offense is intended.

Introduction

The primary focus of this workshop is to enhance investigation skills, including evidence gathering, authentication, and preservation by using technology.

Practitioners will learn how to use technology to gather and manage digital evidence during an investigation.

Our goal is to equip participants with the knowledge and skills needed to conduct civil rights investigations in the digital age.

Investigating in the Digital Age

Electronic Evidence

- Any information created, stored, or shared in digital form that can help establish facts
  - Communication in the form of emails, text messages, chat logs
  - Images, videos, and audio recordings
  - Social media content (e.g., posts, comments, likes)
  - Account information (e.g., username, profile, public activity)
  - System data such as timestamps, location information, IP addresses, and other metadata
- Electronic evidence often provides a record of behavior over time and can corroborate, clarify, or challenge other evidence

Open-Source Investigations

- Civil Rights Investigators can leverage technology to expand their own investigation practices and skills
- An open-source investigation practice that incorporates use of publicly available information to gather and verify evidence
  - Social media reviews
  - Reverse image searches
  - Username and platform searches
  - Timeline verifications
  - Metadata awareness
- Open-source practices can support fact-finding and corroboration

Technology in Civil Rights Investigations

Technology can support the civil rights investigation process by:

- Enhancing organization and efficiency through case management software and electronic evidence tracking
- Supporting evidence and credibility analyses with tools like metadata review, timelines, and deep search functions
- Facilitating information and process access and accessibility (e.g., transcription, translation)
- Strengthening communication and privacy protections through secure information-sharing platforms
- Helping verify and authenticate evidence

Role of Artificial Intelligence in Civil Rights Investigations

- Artificial Intelligence (AI) can be a useful tool to assist civil rights Investigators
  - Organizing and analyzing large volumes of evidence (e.g., sorting documents, identifying patterns)
  - Transcribing and summarizing interviews and recordings
  - Enhancing accessibility through translation, captioning, and language support
  - Flagging potential inconsistencies
  - Assisting with drafting reports and other documents
- Effective prompting for AI tools
- AI is a support tool; therefore, Investigators must maintain oversight and review of any material produced by AI to ensure accuracy

Managing AI-Written Materials

- Investigators may receive AI-generated materials from parties and/or witnesses
- AI can produce material that is highly polished, structured, and compelling
  - Focus on substance and not style
  - Ask follow up question to discover the interviewee's actual experience
    - "Is this in your own words?"
    - "Can you describe this in your own way?"
  - Look for consistency across statements and evidence (corroboration)
  - Manage your own personal biases (e.g., do not discount information simply because it may have been generated by AI)
- AI can compromise confidentiality; using it for report writing or decision-making analysis is not recommended and could violate the Title IX regulations

Administrative Process Limitations

- The administrative civil rights investigation process has several limitations compared to a criminal or civil (e.g., litigation-based) investigation
  - No subpoena power to compel individuals to provide evidence
    - Voluntary nature of the process often limits evidence access
  - Enforcement power is limited to sanctions/accountability measures as dictated by school/institutional policy
  - Investigators are constrained by school/institutional policy as well as federal and state laws
  - May not be able to compel removal or destruction of consensually obtained content

Leveraging Technology During Evidence Gathering

Understanding Metadata

- **Metadata** comprises data about data
  - Detailed information about an individual piece of data or a data set
  - Can be descriptive, technical, structural, administrative, or for preservation
- Examining available metadata can provide relevant information on:
  - Data creation
  - Data ownership
  - Data access and retrieval
- Metadata for files and emails is largely **automatically generated** by operating systems, applications, and network protocols, which makes it generally reliable but susceptible to system-level manipulations and environmental factors like time zone changes

Types of Metadata

- **System-Generated:** File systems automatically record file creation, modification, and access dates
- **Application-Embedded:** Applications like Microsoft Word or Excel create embedded properties (e.g., author, revision history, total editing time)
- **Email Routing:** Email metadata is appended incrementally by every mail server that handles a message, creating a “received” header chain that documents its journey
- **EXIF Data:** Digital photos and cameras automatically generate Exchangeable Image File Format (EXIF) data, including device settings, camera model, and GPS locations

Example: Email Metadata

From: jane.doe@student.edu

To: john.smith@student.edu

CC: —

Date: March 12, 2026, 9:42 AM (CST)

Subject: Re: Meeting yesterday

Message-ID: A1B2C3D4E5@mail.student.edu

IP Address: 192.168.1.45

Device: iPhone 14 (iOS 17.2)

Mail Client: Apple Mail

Sent Time (Server): March 12, 2026, 9:42:15 AM

Received Time: March 12, 2026, 9:42:18 AM

Time Zone: -0600 (Central Standard Time)

Attachment(s): IMG_4567.jpg

Attachment Metadata:

- Created: March 12, 2026, 9:30 AM
- File Type: JPEG
- File Size: 2.4 MB

Example: Photo Metadata

File Name: IMG_4567.jpg

File Type: JPEG

File Size: 2.4 MB

Date Taken: March 8, 2026

Time Taken: 6:42 PM (CST)

Time Modified: March 8, 2026, 7:05 PM

Device: iPhone 13 Pro

Camera App: Apple Camera

Lens: Wide Camera (1x)

GPS Location (if enabled):

- Latitude: 29.7604
- Longitude: -95.3698
- Location: City, XX

Image Dimensions: 4032 x 3024 pixels

Orientation: Landscape

Exposure Settings:

- ISO: 100
- Shutter Speed: 1/120 sec
- Aperture: f/1.5

If created using AI, that may be included in the device or camera app data

Example: Text Message Metadata

Sender: (555) 123-4567

Recipient: (555) 987-6543

Date: April 10, 2026

Time Sent: 8:14 PM (CST)

Time Delivered: 8:14 PM

Time Read: 8:16 PM

Message Type: SMS (text message)

Device: Samsung Galaxy S23

Operating System: Android 14

Carrier: AT&T

Message ID: 789456123

Thread ID: 11223344

Attachment: Yes

- **File Name:** video_04102026.mp4
- **File Type:** MP4
- **File Size:** 5.8 MB
- **Created:** April 10, 2026, 7:58 PM

Location Data (if available):

- Approximate Location: City, XX
- GPS Coordinates: 29.7604, -95.3698

Example: Video Metadata

File Name: VID_4582.mp4

File Type: MP4

File Size: 24.6 MB

Duration: 00:01:32 (1 minute, 32 seconds)

Date Recorded: April 9, 2026

Time Recorded: 10:18 PM (CST)

Time Modified: April 9, 2026, 10:25 PM

Device: Samsung Galaxy S23

Camera App: Camera

Resolution: 1920 x 1080 (1080p)

Frame Rate: 30 fps

GPS Location (if enabled):

- Latitude: 29.7604
- Longitude: -95.3698
- Location: City, XX

Audio: Yes (stereo)

Codec: H.264

Orientation: Portrait

Activity: Locating Metadata

Find Your Photo Metadata

- Open a recent photo from your cellphone or tablet
- On an Android device:
  - Swipe up on the photo or tap the three dots in the upper right corner and select “About” to show metadata
- On an Apple iOS device:
  - Swipe up on the photo or tap the “i” icon on the screen

Risks to Metadata Accuracy

- **Manipulation/Spoofing:** While hard to change, email headers can be spoofed, or timestamps altered by sophisticated users
- **File Handling Changes:** Copying a file can update the creation date to the moment of transfer, losing the original creation date
- **Format Conversion:** Converting a document to a different format (e.g., Word, PDF) often strips original metadata
- **Missing Metadata:** Printing a document or sending it through certain secure channels can result in a “dismembered” file with no metadata

Technology Interview Questions

- How does this app/platform work?
  - Does it notify users of screenshots, shares, edits, deletions?
- Can content be edited or deleted after posting?
  - If so, is there a record or indicator of changes?
- How are timestamps generated?
  - Are they based on device time, server time, or user settings?
- Who can see or access this content?
  - Is it public, private, close friends, disappearing messages (If, so how long does the message remain visible)?

Technology Interview Questions (Cont.)

- Does the app/platform store or log activity?
  - (e.g., message history, login activity, view receipts)
- Can accounts be impersonated or easily created?
  - How easy is it to fake or duplicate an account?
- What happens to messages or content over time?
  - (e.g., auto-delete, ephemeral content like Snapchat)

Credibility may depend on not only **what** the evidence shows,
but how the platform works

Introduction to Investigation Tools

Helpful tools, tips, and apps to gather and authenticate evidence

Investigation Tools

- Applications (apps) are programs or software designed and written to fulfill a particular user purpose
  - Apps can assist Investigators with evidence gathering and authentication
    - Detecting spyware
    - Unmasking anonymous emailers and phone numbers
    - Checking for deleted apps
    - Retrieving deleted files and texts
- Reverse location searches
  - Standard reverse image searches
  - Geolocating by language learning models
- Facial recognition image searches

Example Tools for Digital Footprint Mapping

- **Google search (advanced operators):** uncover linked accounts and content
- **Social media platform search (Instagram, TikTok, X):** identify activity and patterns
- **Sherlock/Namechk:** find usernames across multiple platforms
- **SpiderFoot:** automate collection of publicly available information
- **Spokeo Reverse Phone Lookup:** search records associated with a landline or cell phone number including owner, location, contact information, social media, family members, etc.

Note: Inclusion in this training is for awareness purposes and should not be construed as an ATIXA endorsement

Example Tools for Detecting Altered Material

- **Google Reverse Image Search/TinEye:** find where an image has appeared before
- **FotoForensics:** identifies potential image manipulation (error level analysis)
- **InVID:** analyzes videos and keyframes for verification
- **ExifTool:** extracts metadata to check for edits or inconsistencies
- **Forensically (online tool):** detects cloning, noise patterns, and alterations

Note: Inclusion in this training is for awareness purposes and should not be construed as an ATIXA endorsement

Example Tools for Deciphering Digital Slang

- **Urban Dictionary:** quick reference for slang and evolving terms
- **Know Your Meme:** explains trends, phrases, and cultural context
- **TikTok/X (Twitter) search:** see how terms are used in real time
- **Reddit:** useful for context and meaning in conversations

Note: Inclusion in this training is for awareness purposes and should not be construed as an ATIXA endorsement

Accessing Digital Evidence

- Investigators must receive **consent** from parties and witnesses to access their personal devices or private electronic accounts
  - Consent to access must be **voluntary**, **informed**, and **may be limited** to specific elements access
- Civil Rights Investigators lack subpoena power to compel individuals to provide evidence
- Investigators may need to contact local businesses to request access to their digital information (surveillance footage, sales receipts, etc.)
- Investigators will need to gather relevant digital evidence while respecting boundaries, privacy, and the limits of administrative authority

Best Practices for Accessing Digital Evidence

- Be transparent about the request
- Avoid language that suggest an obligation if none exists
- Narrow the scope
- Offer options for sharing
- Protect privacy
- Avoid directly handling devices when possible
- Coordinate with IT or legal counsel when needed
- Document consent and the process
- Be mindful of sensitive content

Example Recording and Transcription Tools

- **Recording Tools**
  - Zoom/Microsoft Teams/Google Meet
  - Case management system
  - Digital voice recorder or secure mobile app (in-person)
- **Transcription Tools**
  - Zoom/Microsoft Teams
  - Otter.ai
  - Rev.com
  - Descript (AI video editing tool)

Note: Inclusion in this training is for awareness purposes and should not be construed as an ATIXA endorsement

Internal Information Technology Resources

- Camera footage
- Entry/card access data
- Email, messaging apps
- Institutional computers, tablets, and cell phones
- File creation, modification, deletion, and access data
- Network usage and IP addresses
- Institutional device access logs
- User account access
- Social media posts

Managing Sensitive Evidence

Sensitive Information

- Offensive, triggering, or explicit language (e.g., slurs)
- Graphic images/videos
- Sexually explicit content, including child sexual abuse material (CSAM)
- Personally identifying information (PII)
- Intimate communications (e.g., sexts)
- Medical information, including test results
- Digital account data
- Location and tracking information
- Third-party information

Child Sexual Abuse Materials (CSAM)

- **CSAM:** Any visual, audio, or written content that depicts or involves the sexual abuse or exploitation of a minor
- Students intentionally sharing nude selfies and videos is very prevalent
- Under both state and federal laws, the possession and distribution of any such image of someone under the age of 18 is criminal behavior
  - The regulation of CSAM is extremely strict, even when the images or materials constitute evidence
  - May include synthetic CSAM

CSAM Evidence

- Administrators should exercise caution when addressing allegations involving CSAM
  - Administrators should not take custody of devices containing CSAM or intentionally access CSAM as part of an investigation
    - Law enforcement has many tools to recover deleted images
  - Work with school resource officer or law enforcement

Preserving Digital Evidence

Types of Evidence

Documentary Evidence	Supportive writings or documents
Digital Evidence	Photos, text messages, and videos
Physical Evidence	Physical objects
Direct or Testimonial Evidence	Personal observation or experience
Circumstantial Evidence	Not eyewitness, but compelling
Hearsay Evidence	Statement from outside the interview presented as truthful
Character Evidence	Evidence of a person's character or character traits

Evidence Authentication

- Not all evidence has the same degree of credibility
  - Less credible evidence may be less reliable evidence
- Investigator(s) should seek the **highest quality evidence** available
- Investigator(s) should try to **authenticate all evidence** provided
  - Check for possible evidence fabrication; use metadata
  - Corroborate information between parties and witnesses
  - Try to obtain complete, rather than partial, records when possible
  - Test assertions to verify accuracy when possible
    - Example: “I don’t remember sending that message, but the post appears on my social media account and is linked to my username”
- Avoid relying on a single photo, video, or audio file, no matter how real it appears

Open-Source Evidence Preservation

Take Screenshots

Capture the full screen including timestamp, URLs, visual context, etc.

Save Original URLs

Record direct links to content and note the access date and time

Download and Save

Save content in its original format when appropriate

Record Metadata

Usernames, platform, date/time of posting, and any relevant context

Open-Source Evidence Preservation, Cont.

Name Files Consistently

Clearly and consistently label files to maintain order

Store Evidence Securely

Use secure, access-controlled systems in line with institutional policies

Avoid Alteration

Maintain original versions; work from copies if necessary

Maintain Evidence Log

When, how, and by whom evidence was collected and any actions taken

Evidence Log

- All evidence gathered with:
  - Description
  - Date of receipt
  - Source
  - Method of receipt
- Any evidence verification/authentication information

Evidence Log Example

Date	Source	Method of Receipt	Type	Description	Authentication
1/10/26	Sam Smith	Email	Security video footage; USB drive	Elevator video footage from 9:10 – 10:10 PM on 12/10/25	Closed circuit from IT
1/11/26	Sally Harris	Social Media Screenshot	Social Media Screenshot	Post made by Respondent at 9:22 PM on 12/10/25	None
1/15/26	Sally Harris	In Person	Call Record	Phone call log from Complainant's cell phone carrier	Email with attachment from carrier to Complainant

Tips for Evidence File Sharing

- Use a secure file-sharing platform
  - Consider functional and time limit restrictions as appropriate
- Set a time limit for how long materials are available for review
- Consider restricting permissions (e.g., downloading, copying, or forwarding)
- Include a separate watermark for each party (parent/guardian/Advisor)
- Track access and activity
  - Maintain a log of who accessed evidence when (and from where)
- Provide clear instructions about privacy expectations and prohibitions on sharing or reproducing

Other Considerations

Investigation Considerations

- One-party/surreptitious recordings
- Redaction and annotation practices
- Managing large amounts of digital evidence
- Storing digital evidence
- Accessibility tools for people with disabilities
- Tools for language translation
- Secure communication practices

Association of
Title IX Administrators

Questions?

Stay Connected to ATIXA's Community

- Build skills with **20-Minutes-to…Trained** and get practical guidance at **Time with IX**
- Schedule a **Training and Certification course** and explore **Thought Leadership** from experts
- Expand your network with **Mentor Match** and **Community Connections**
- Stay informed with **ATIXA's "More Likely Than Not" Podcast**
- Refer Members. Earn **Rewards**.
- **K-12:**
  - Exchange ideas through **K-12 CommunityServ** and streamline your work: **TIXKit for K-12**
  - Access a complimentary **K-12 Community Membership**
- **Higher Education:**
  - Exchange ideas through the **ATIXA Listserv** and streamline your work: **TIXKit**

Acknowledgement

ATIXA thanks EndTAB for its contributions to the development of this workshop.

EndTAB helps organizations address technology-enabled abuse, online harms, and emerging digital safety risks through trainings, consulting, and resource development for professionals, schools, nonprofits, government agencies, and communities nationwide.

ATIXA Artificial Intelligence (AI) Disclaimer

Your access to these materials is governed by a limited, non-transferable license which bars modification and certain forms of dissemination. You may not copy or adapt these materials without ATIXA's explicit prior written consent. You are also prohibited from uploading, entering, transmitting, or otherwise disclosing these materials to any AI tool or platform, including but not limited to generative AI systems (e.g., ChatGPT, Copilot, Gemini, or similar technologies).

This license language may not be removed from any version of ATIXA materials. Except where explicitly authorized, should any non-licensee post these materials publicly or disclose them to any AI tool or platform, ATIXA will require the licensee to remove the content immediately, subject to copyright enforcement. These materials may not be used for any commercial purpose except by ATIXA.

ALL ATIXA PROPRIETARY TRAINING MATERIALS ARE COVERED BY THE FOLLOWING LIMITED LICENSE AND COPYRIGHT

By purchasing, receiving, and/or using ATIXA materials, you agree to accept this limited license and become a licensee of proprietary and copyrighted ATIXA-owned materials. The licensee accepts all terms and conditions of this license and agrees to abide by all provisions. No other rights are provided, and all other rights are reserved. These materials are proprietary and are licensed to the licensee only, for their use. This license permits the licensee to use the materials personally and/or internally to the licensee's organization for training purposes only.

If these materials are used to train Title IX personnel, they are subject to 34 C.F.R. Part 106. If you have lawfully obtained ATIXA materials by registering for ATIXA training, you are licensed to use the materials provided for that training.

34 C.F.R. 106.45(b)(10) (2020 Regulations) requires all training materials to be publicly posted on a Recipient's website. Licensees subject to the 2020 Title IX Regulations may download and post a PDF version of training materials for their completed training to their organizational website to comply with federal regulations. ATIXA will provide licensees with a link to their materials. That link, or links to the materials on that page only, may be posted to the licensee's website for purposes of permitting public access to the materials for review/inspection only.

You are not authorized to copy or adapt these materials without ATIXA's explicit written permission. No one may remove this license language from any version of ATIXA materials. Should any non-licensee post these materials to a public website, ATIXA will send a letter instructing the licensee to immediately remove the content from the public website upon penalty of copyright violation. These materials may not be used for any commercial purpose except by ATIXA.