ADVANCED FACT-CHECKING USING OSINT

Training Module

Developed by Inform Africa in collaboration with CIPESA
Supported through the Africa Digital Rights Fund (ADRF)
Version 1.0 | December 2025

Module Overview

This training module provides a practical, methods-first approach to advanced fact-checking using Open Source Intelligence (OSINT). It focuses on verifying claims, tracing sources, authenticating images and videos, confirming location and time, validating documents and data, and documenting findings in a transparent way that others can reproduce.

At a glance

Audience: **Fact-checkers, journalists, newsroom researchers, and media professionals**
Level: **Intermediate to advanced**
Delivery: **Three-day intensive or six-session online series**
Core outputs: **Verification logs, an evidence matrix, and a publish-ready fact-check draft**

Acknowledgement

This work was carried out in the context of the Africa Digital Rights Fund with support from the Collaboration on International ICT Policy for East and Southern Africa (CIPESA).

Contact and attribution

Inform Africa (HaqCheck / Research Unit)
Email: **haqcheck@gmail.com**
Phone: **+1(202) 993-8087**
Websites: https:/informafrica.net/ **and** https://haqcheck.org/

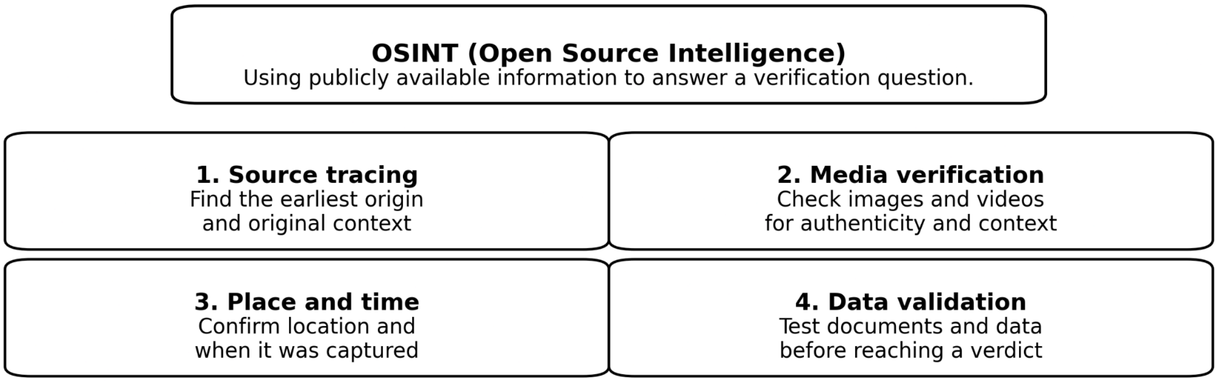
Table of Contents

A) What This Module Is (And Why It Matters)

This advanced, hands-on training module equips fact-checkers with Open Source Intelligence (OSINT) methods and tools to verify claims, images, videos, and online narratives and to publish transparent, evidence-based fact-checks.

Inform Africa developed the module in collaboration with the Collaboration on International ICT Policy for East and Southern Africa (CIPESA) as part of activities supported through the Africa Digital Rights Fund (ADRF). ADRF provides flexible, rapid-response support for initiatives that advance digital rights, including digital literacy and digital security skills building. CIPESA supported this work under ADRF to help bridge operational and programming gaps for past and present CIPESA partners and subgrantees. For public reference, this work is acknowledged as having been carried out in the context of the Africa Digital Rights Fund, with support from CIPESA.

The module responds to the reality that people make real-life decisions based on the information they consume, yet false and misleading content spreads quickly across social media and messaging platforms. Unverified information can trap communities in a web of false information and can contribute to fear, panic, social tension, and even violence. Because false information often spreads faster than facts, the module treats verification as a professional responsibility: verify first, document the steps, and publish conclusions that others can check and trust.



OSINT (Open Source Intelligence)
Using publicly available information to answer a verification question.

1. Source tracing
Find the earliest origin and original context

2. Media verification
Check images and videos for authenticity and context

3. Place and time
Confirm location and when it was captured

4. Data validation
Test documents and data before reaching a verdict

B) Audience, Level, And Prerequisites

Audience: This module is designed for fact-checkers, journalists, newsroom researchers, digital investigators, and civil society actors who regularly assess public claims and online content and need a stronger OSINT-based verification practice.

Level: Intermediate to advanced. It is most effective for participants who already understand basic fact-checking concepts and want to deepen their ability to verify complex claims and digitally manipulated or mis-captioned content.

Prerequisites:

- Ability to use a web browser confidently (search, tabs, saving links, screenshots).
- Familiarity with major platforms (Facebook, X, YouTube, TikTok, Telegram) and how content is shared.
- Basic writing skills to document verification steps and produce a short fact-check narrative.
- Access to a laptop (preferred) or smartphone, a stable internet connection, and an email address for tool access.
- Willingness to follow ethical and safety practices, including avoiding unnecessary amplification and protecting sensitive data.

C) Learning Outcomes And Competencies

By the end of the module, participants will be able to:

1. **Identify and frame fact-checkable claims**
   - Separate verifiable claims from opinions, predictions, and vague assertions.
   - Rewrite a claim into a precise, checkable form (who, what, when, where, how much).
2. **Apply a structured OSINT verification workflow**
   - Follow a repeatable process: claim intake, source tracing, evidence collection, expert consultation (when needed), conclusion, and transparent write-up.
   - Keep a verification log that another person can audit and reproduce.
3. **Verify digital sources and provenance**
   - Trace the earliest available version of a claim, image, or video across platforms.
   - Assess source credibility using basic provenance questions (origin, context, motive, consistency).
4. **Verify images using OSINT**
   - Run reverse image searches and compare contexts.
   - Identify common manipulation and mis-caption patterns.
   - Produce an image verification log with links and a confidence rating.
5. **Verify videos using OSINT**
   - Extract keyframes, locate prior uploads, and check context.
   - Identify edits, cropping, and misleading captions.
   - Produce a video verification log with steps and evidence.
6. **Conduct basic geolocation and chronolocation**
   - Use visible clues (landmarks, signage, terrain, architecture) and mapping tools to confirm location.
   - Use time clues (weather, shadows when appropriate, event timelines, upload history) to estimate when content was captured.
7. **Assess data quality and evidence strength**
   - Evaluate whether a dataset or document actually supports the claim.
   - Check relevance, recency, methodology, and limitations before reaching a verdict.

8. **Publish a transparent, ethical fact-check**
   - Write a publish-ready fact-check that clearly explains the method, sources, evidence, and uncertainty.
   - Apply safety and do-no-harm principles, including avoiding unnecessary amplification.

D) Module Structure And Delivery Format

This module is delivered through short lectures, guided demonstrations, and hands-on verification labs. Each day ends with a concrete output (logs, worksheets, or a draft fact-check) so progress is measurable, and the learning is practical.

A short **OSINT Orientation** is included early in the training to define OSINT in a fact-checking context and introduce the core verification toolkit categories. This ensures all participants share a common language and can complete the labs efficiently.

Option 1: 3-day intensive (in-person or virtual)

Total time: 18 to 21 hours
Daily flow: 2 instructor-led sessions plus labs, with daily submissions.

- Day 1 (Foundations and workflow)
  - Information disorder, bias control, and claim selection
  - OSINT Orientation and toolkit overview (30 to 45 minutes)
  - Claim intake, source tracing, and building an evidence plan
  - Daily output: Claim intake sheet + evidence matrix

- Day 2 (Image and video verification)
  - Image verification methods and tools, documentation discipline
  - Video verification methods and tools, context tracing
  - Daily output: Image verification logs + video verification logs
- Day 3 (Geolocation, data quality, and publishing)
  - Geolocation and time verification using open tools
  - Evidence quality checks, expert use, and transparent writing
  - Daily output: Publish-ready fact-check package (capstone)

Option 2: 6-session online series

Total time: 15 to 18 hours
Format: 6 sessions (2.5 to 3 hours each), plus optional office hours.

Session 1: Information disorder, bias checks, claim framing
Session 2: Verification workflow + OSINT Orientation and toolkit overview + evidence matrix
Session 3: Image verification OSINT (tools + lab)
Session 4: Video verification OSINT (tools + lab)
Session 5: Geolocation and time verification (lab)
Session 6: Data quality + writing + capstone presentations

Training approach

- Practice-first: most time is spent in labs, not slides.
- Documentation-first: every exercise requires a verification log.
- Methods-first: tools are introduced as examples, but the focus is on repeatable workflows.
- Team-based learning: participants work in pairs or small teams to simulate newsroom workflows.
- Ethics and safety throughout: do-no-harm, privacy, and minimizing amplification are applied in every lab.

E) Foundations And OSINT Workflow (Day 1)

Day 1 purpose

Day 1 builds the discipline that makes OSINT work: selecting the right claims, defining them precisely, tracing sources, planning evidence before searching, and documenting every step so another person can reproduce the findings.

Session 1: Information disorder, verification mindset, and bias control

Duration: 2.5 to 3 hours

Objectives

By the end of this session, participants can:

- Recognize common patterns of misinformation and manipulation tactics.
- Apply a "verify before sharing" mindset in professional workflows.
- Identify personal and newsroom bias risks that can distort verification decisions.

Key content (facilitator-led)

1. Information disorder patterns
    - Miscaptioning and recycled media
    - Cropped clips and selective edits

- False attribution and impersonation
- Fabricated screenshots and fake documents.
- Satire presented as news

2. High-risk signals (red flags)
    - Emotional language designed to trigger outrage or fear
    - Urgency: "breaking", "share now", "before it is deleted"
    - Anonymous sourcing or "my friend works at…" claims
    - Screenshots without links or a traceable origin
    - Suspicious handles, URLs, spelling variants, cloned pages
3. Bias control
    - Why do we accept information that matches what we already believe?
    - The pause habit: "What evidence would convince me I am wrong?"
    - Separating what we want to be true from what we can prove

Demonstration (15 to 20 minutes)

Facilitator models a rapid triage on one viral post:

- Is it fact-checkable?
- What is the exact claim in one sentence?
- What is the first verification step?
- What should not be amplified while checking?

Lab 1: The Triage Drill

Duration: 45 minutes

Group format: pairs or small teams

Participants review 6 sample posts (mix of text, image, and video thumbnails). For each post, they answer:

1. What is the checkable claim (one sentence)?
2. What is the potential harm if false (low, medium, high)?
3. What should be verified first (source, date, location, media authenticity)?
4. What should not be repeated or amplified during verification?

Output to submit (end of Session 1)

- Completed the Triage Drill worksheet for all six posts

Quick knowledge check (10 minutes)

5 short questions on:

- Claim vs opinion
- What makes a claim checkable
- First verification action
- One bias risk and one control technique

Facilitator notes

- Push precision: if the claim is unclear, verification will fail.
- Encourage calm pace: speed is not accuracy.
- Reinforce that "uncertain" is a valid interim outcome.

Session 2: OSINT Orientation, claim intake, source tracing, and evidence planning

Duration: 2.5 to 3 hours

Objectives

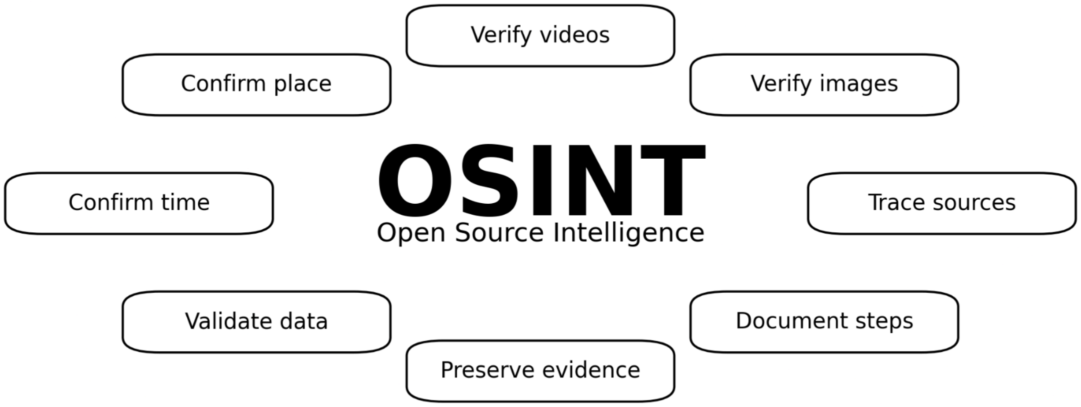
By the end of this session, participants can:

- Define OSINT in a fact-checking context and name the major tool categories.
- Select suitable claims for fact-checking and define them precisely.
- Trace the earliest available version of a claim or media item.
- Build an evidence matrix and a verification plan before conducting a deep search.
- Maintain a verification log that captures steps, links, screenshots, and conclusions.

Part 1 (30 to 45 minutes): OSINT Orientation and toolkit overview

What does OSINT mean in this training?

OSINT (Open Source Intelligence) is the systematic collection and analysis of information that is legally and publicly accessible to answer a specific question. In fact-checking, OSINT is used to trace sources, verify images and videos, confirm time and location, validate documents and datasets, and document evidence in a transparent and repeatable way.



Major OSINT tool categories used in this module

1. Search and source tracing
    - Search operators and clever query design
    - Platform search and cross-platform tracing
2. Web archiving and evidence preservation
    - Archiving pages and capturing links
    - Screenshots and folder discipline
    - Maintaining a verification log
3. Image verification
    - Reverse image search workflows
    - Visual clue analysis and basic forensics when needed
4. Video verification
    - Keyframes and thumbnail checks
    - Finding earlier uploads and context
5. Geolocation and time verification
    - Maps, satellite imagery, Street View comparisons
    - Event timeline checks and context confirmation

6. Data and document verification
    - Credible data sources and methodology checks
    - Authenticity red flags and triangulation

Mini activity (10 minutes): Tool readiness

Participants confirm they can:

- Open multiple tabs and keep search trails
- Save links and take screenshots
- Create a simple folder for evidence
- Use a verification log template

Part 2: Claim intake and claim selection (30 minutes)

Claim selection criteria

A strong fact-check claim is:

- Specific and checkable (not vague)
- Important or harmful enough to matter
- Likely to have evidence available
- Clear on who/what/when/where/how much

Claim clarification checklist

Participants rewrite the claim to include:

- Who is making the claim
- What exactly is being claimed
- Place and timeframe
- Units or measurements (if any)

- Definitions of key terms

Part 3: Source tracing and "earliest trace" discipline (30 to 40 minutes)

Source tracing fundamentals

Participants learn to:

- Identify the earliest available post or publication
- Capture original wording and media
- Record author/handle, timestamp, and link
- Separate "where it went viral" from "where it started."

Evidence preservation minimum standard

For every key step, capture at least one of the following:

- URL link
- Screenshot showing timestamp and account/page
- Archived link (when possible)
- Notes in the verification log describing what was observed

Demonstration (20 to 25 minutes)

The facilitator takes one sample claim and completes:

- Claim Intake Sheet
- Evidence Matrix
- A short verification plan with top checks in order
- A simple verification log entry showing links and screenshots captured

Lab 2: Claim Intake + Evidence Matrix + Verification Plan

Duration: 60 to 75 minutes

Group format: pairs or small teams

Participants choose 1 claim from the case pack and complete:

1. Claim Intake Sheet
    - Exact claim wording
    - Where it was found (platform, link, date/time)
    - Who made the claim (speaker/account)
    - Earliest traceable version
    - Definitions and assumptions
    - What would make it true or false
2. Evidence Matrix
    - What questions must be answered to verify the claim?
    - What evidence is needed for each question?
    - Which sources are strongest?
    - What was found (with links and notes)
    - Confidence rating for each evidence line (high, medium, low)
3. Verification Plan (5 bullets)

    Participants list top checks in order, with a reason for each.

Output to submit (end of Session 2)

- 1 completed Claim Intake Sheet
- 1 completed Evidence Matrix
- 5-bullet Verification Plan
- Verification log entries (links and screenshots) attached or referenced

Day 1 wrap-up (10 minutes)

- Two teams share their claim and verification plan.
- Facilitator highlights strong practices and common errors:
  - Unclear claim framing
  - Starting tools before defining the question
  - Missing source capture (no links, no screenshots)
  - Jumping to a verdict too early

Materials needed for Day 1

- Case pack (posts, screenshots, links)
- Triage Drill worksheet
- Claim Intake template
- Evidence Matrix template
- Verification Log template (simple table or document)
- Folder structure guidance (how to name and store evidence)

F) Image And Video Verification OSINT (Day 2)

Day 2 purpose

Day 2 builds practical skills for verifying visual content that spreads quickly and can cause harm, such as photos, screenshots, and videos. Participants learn to recover the original context, detect manipulation or miscaptioning, and document every step with evidence.

Session 3: Image verification OSINT

Duration: 2.5 to 3 hours

Objectives

By the end of this session, participants can:

- Verify whether an image is authentic, edited, recycled, or miscaptioned.
- Trace an image to its earliest available appearance and original context.
- Use visual clues to test where and when an image was taken.
- Produce a transparent, repeatable image verification log.

Key content (facilitator-led)

1. **Image verification workflow**
    - Preserve the original post (link, screenshot, archive if possible)
    - Identify the claim the image is being used to support
    - Extract the best available copy of the image
    - Run reverse image searches and compare results
    - Examine visual clues and context
    - Conclude with confidence grading and uncertainty notes
2. **Common image misinformation patterns**
    - Old photo used as new
    - Correct photo, wrong location, or wrong event
    - Cropped image that hides key context
    - Edited image (additions, removals, text overlays)
    - Screenshots presented as official documents
3. **Visual clue analysis**
    - Language and signage
    - Landmarks, terrain, architecture, road features
    - Weather, shadows, seasonal indicators
    - Uniforms, license plates, vehicle models
    - Consistency checks inside the image (lighting, edges, repetition)
4. **Core tools and methods (overview)**
    - Reverse image search (multiple engines, not just one)
    - Browser extensions that speed up reverse search
    - Basic image forensics tools, when needed (use carefully and interpret cautiously)

Demonstration (20 to 25 minutes)

Facilitator verifies one image step-by-step:

- Defines the claim being made with the image
- Runs reverse searches and identifies the earliest context
- Uses visual clues to test location or event
- Documents steps in the Image Verification Log
- Concludes with confidence rating

Lab 3: Image verification sprint

Duration: 60 to 75 minutes

Group format: pairs or small teams

Lab task

Participants verify six images from the case pack:

- 2 recycled images (old content presented as new)
- 2 miscaptioned images (wrong place or wrong event)
- 1 edited or manipulated image
- 1 authentic image used correctly (control case)

Output to submit

For each image, participants submit a completed **Image Verification Log,** including:

- Link to where the image appeared and a screenshot capture
- The exact claim the image is being used to support
- Reverse search results (with links or screenshots)
- Earliest known appearance and original context
- Key visual clues used (with notes)
- Conclusion and confidence rating (high, medium, low)
- What remains uncertain (if anything)

Facilitator notes

- Require multiple reverse-search attempts when results are weak.
- Push participants to separate "is the image real?" from "is the caption true?"
- Reinforce: avoid amplifying harmful content while verifying.

Session 4: Video verification OSINT

Duration: 2.5 to 3 hours

Objectives

By the end of this session, participants can:

- Verify whether a video is old, edited, miscaptioned, or authentic.
- Extract keyframes and trace the video across platforms.
- Confirm context using timelines, upload history, and external sources.
- Produce a video verification log with evidence and confidence grading.

Key content (facilitator-led)

1. **Video verification workflow**
    - Preserve the original post (link, screenshot, archive if possible)
    - Define the claim attached to the video
    - Extract keyframes (clear still images from the video)
    - Reverse-search keyframes and look for earlier uploads
    - Check platform metadata (upload date, channel context where relevant)
    - Compare with credible reporting, official sources, or on-the-ground evidence
    - Document steps, conclude with confidence grading
2. **Common video misinformation patterns**
    - Old footage reused for a new event
    - Edited clips that remove context
    - Audio swapped or captions added to mislead
    - Compilation videos presented as a single event
    - Re-uploads across platforms that hide the original source
3. **Core tools and methods (overview)**
    - Keyframe extraction and video verification plugins

- Thumbnail and upload-date checks for platform videos
- Reverse-searching still frames
- Cross-platform tracing using quotes, hashtags, landmarks, and handles

Demonstration (20 to 25 minutes)

Facilitator verifies one short video:

- Extracts keyframes
- Finds earlier versions and identifies original context
- Checks timing and narrative framing
- Documents steps in the Video Verification Log
- Concludes with confidence rating

Lab 4: Video verification sprint

Duration: 60 to 75 minutes

Group format: pairs or small teams

Lab task

Participants verify three videos from the case pack:

- 1 recycled footage case
- 1 edited or clipped case
- 1 authentic video with a misleading caption

Output to submit

For each video, participants submit a completed **Video Verification Log,** including:

- Link to the video post and screenshot capture
- The exact claim the video is being used to support
- Keyframes extracted (or screenshots of keyframes)
- Reverse search results for keyframes (with links or screenshots)
- Earliest known upload or closest traceable source
- Context confirmation (what it actually shows, where, when, who)
- Conclusion and confidence rating (high, medium, low)
- What remains uncertain (if anything)

Facilitator notes

- Encourage "context before verdict": what is happening, where, when, who filmed it.
- Do not treat missing metadata as proof of falsity.
- Require at least two independent confirmations for high-confidence verdicts.

Day 2 add-on: Synthetic media awareness (AI-generated content)

Duration: 20 to 30 minutes

Purpose

Participants learn basic warning signs and safe reporting practices when synthetic or AI-altered media is suspected.

Key indicators to discuss

- Unnatural hands, fingers, teeth, and accessories
- Repeating patterns, warped backgrounds, and inconsistent text
- Strange shadows or lighting inconsistencies
- "Too perfect" skin texture or unnatural edges around hair and objects

Output (short)

Participants flag which of the 6 sample images are "likely synthetic," "uncertain," or "likely real," and list two reasons for each choice.

Day 2 wrap-up (10 minutes)

- Two teams share one image case and one video case.
- Facilitator highlights:
  - Strong documentation habits
  - Best examples of "earliest trace" work
  - Common errors (jumping to conclusions, not capturing links, confusing authenticity with context)

Materials needed for Day 2

- Case pack (images and videos with links and screenshots)
- Image Verification Log template
- Video Verification Log template
- Keyframe extraction or verification plugin guidance (short handout)
- Evidence folder naming guidance (simple standard)

G) Geolocation, Data Validation, And Publishing (Capstone)(Day 3)

Day 3 purpose

Day 3 brings OSINT work to a publishable standard. Participants learn how to confirm location and time, assess the strength of evidence and datasets, apply ethics and safety consistently, and produce a transparent fact-check package that can be edited and published.

Session 5: Geolocation and time verification (chronolocation)

Duration: 2.5 to 3 hours

Objectives

By the end of this session, participants can:

- Geolocate visual content using open mapping tools and visible clues.
- Confirm or narrow down when content was captured using context, timelines, and platform signals.
- Write a clear "how we know" explanation that links evidence to the conclusion.
- Grade confidence and document uncertainty.

Key content (facilitator-led)

1. Geolocation fundamentals
    - Start from what you can see: signage, language, road markings, landscapes, architecture, landmarks, businesses, uniforms, vehicle clues.
    - Build hypotheses: "this looks like a city center," "this looks like highland terrain," "this looks like a border checkpoint," etc.
    - Use open mapping tools to test hypotheses:
        - Maps and satellite views for matching the layout
        - Street-level imagery when available
        - Compare shapes: intersections, rivers, hills, building footprints
2. Chronolocation (time verification)
    - Time verification is often contextual:
        - Upload timing and repost history
        - Weather or seasonal indicators (used cautiously)
        - Known events: public rallies, disasters, conflicts, elections
        - Cross-reference with credible reporting or official statements
    - Distinguish: "this was uploaded on X date" vs "this was recorded on X date."
3. Confidence and uncertainty discipline
    - High confidence requires multiple independent matches.
    - "Unconfirmed" is acceptable when evidence is insufficient.
    - Document what would raise confidence.

Demonstration (20 to 25 minutes)

Facilitator geolocates one image/video frame:

- Lists visible clues
- Searches maps and satellite imagery
- Matches at least two strong indicators

- Write a short "how we know" paragraph
- Adds confidence rating and notes remaining uncertainty

Lab 5: Geolocation and time verification

Duration: 75 to 90 minutes
Group format: pairs or small teams

Lab task

Participants geolocate and time-verify two cases:

- Case A (medium): clear landmark clues
- Case B (hard): limited clues, requires careful hypothesis testing

Output to submit

For each case, participants submit a completed Geolocation and Time Verification Worksheet, including:

- Source post link and screenshots
- Key visual clues listed (minimum 6)
- Hypotheses considered and why rejected/accepted
- Map evidence (screenshots or links) showing matched features
- Time verification notes (what is known, what is inferred, what is unknown)
- "How we know" paragraph (150 to 250 words)
- Conclusion and confidence rating (high, medium, low)

Facilitator notes

- Require a minimum standard: two independent matching features for location.
- Caution against overreliance on weak indicators (e.g., one similar building).
- Encourage explicit uncertainty statements.

Session 6: Data and document validation, ethics, and writing the fact-check

Duration: 2.5 to 3 hours

Objectives

By the end of this session, participants can:

- Assess the credibility and relevance of data sources and documents.
- Decide when and how to use experts.
- Write a transparent fact-check that shows method, evidence, and limitations.
- Apply do-no-harm and anti-amplification practices.

Key content (facilitator-led)

1. Data and document validation

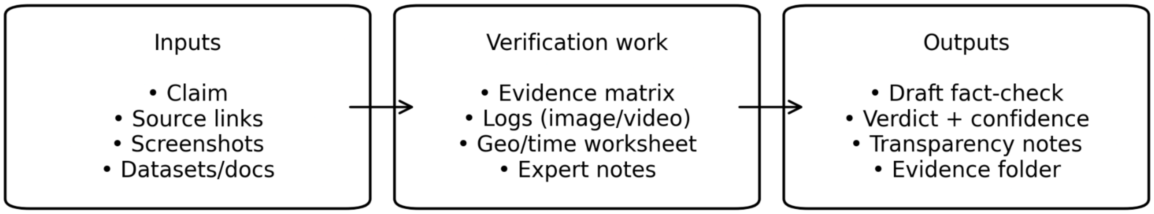
   Participants learn to test evidence strength using a simple checklist:
   - Who produced the data/document and why?
   - Date, scope, and relevance to the claim
   - Methodology and limitations
   - Sample size and representativeness (where applicable)
   - Independent confirmation or cross-checking
   - Whether the evidence truly supports the claim as stated
2. Using experts responsibly
   - Experts clarify definitions, methods, and interpretation.
   - Do not outsource the verdict to one voice.
   - Use experts to validate your interpretation of evidence.
3. Writing the publishable fact-check

   A standard structure that participants follow:
   - The claim and why it matters
   - What we checked and how we checked it
   - What we found (evidence, links, archived sources)
   - What we cannot confirm (limitations)
   - Verdict and confidence
   - Transparency notes (sources, methods, corrections readiness)
4. Ethics and safety
   - Avoid unnecessary amplification of harmful content.
   - Protect vulnerable people: blur faces, remove identifying details when needed.
   - Respect privacy and legal boundaries: use only publicly available information.
   - Correct errors openly and promptly.

Demonstration (15 to 20 minutes)

The facilitator shows a model "publish-ready" fact-check package:

- Evidence table
- Verification log excerpts
- Transparent methodology paragraph
- Verdict with confidence grading



Capstone Lab: Publish-ready fact-check package

Duration: 90 to 120 minutes

Group format: teams of 3 to 5

Capstone task

Teams choose one case from the pack (or a locally relevant case provided by the facilitator) and produce a complete fact-check draft and evidence bundle.

Output to submit (capstone package)

1. Draft fact-check (600 to 900 words or equivalent newsroom format)
2. Evidence folder (links, screenshots, archives)
3. Verification logs (image/video/geolocation as relevant)
4. Expert notes (if used): who, why, and what they clarified
5. Final verdict with confidence rating
6. Transparency and corrections note

Presentation (optional, 20 to 30 minutes)

Each team presents:

- The claim and harm level
- The three strongest pieces of evidence
- What was uncertain
- Final verdict and confidence

Assessment and completion criteria (Day 3)

Participants are assessed on:

- Documentation quality (can another person reproduce the steps?)
- Evidence strength and triangulation
- Clarity of reasoning from evidence to conclusion
- Ethical handling and minimizing harm
- Quality of final write-up and transparency

Completion requires:

- All lab outputs submitted

- Capstone package completed
- Minimum score on the capstone rubric (set by facilitator)

Day 3 wrap-up (10 minutes)

- Key lessons and common pitfalls
- Personal action plan: one workflow improvement each participant commits to using immediately

Materials needed for Day 3

- Geolocation and Time Verification Worksheet
- Data and Document Validation Checklist
- Fact-check writing template
- Capstone rubric
- Case pack (geolocation cases + datasets/documents as required)

H) Training Materials Package

This document serves as the core training module and curriculum. It sets out the learning objectives, session structure, teaching approach, and the practical exercises that guide participants from claim selection to a publish-ready fact-check. It is designed to be flexible so it can be delivered as a three-day intensive or as a multi-session online series.

To deliver the training effectively, the module is intended to be used with a small set of supporting materials prepared as separate documents and adapted to the specific audience, country context, and delivery format. These supporting materials include a facilitator guide, which provides session-by-session delivery notes, timings, demonstrations, and tips for trainers. A participant workbook supports learners with clear instructions, short reference notes, and space to complete exercises. Standard verification templates provide ready-to-use forms for claim intake, evidence planning, and verification logs, helping teams document their work consistently and transparently.

The package is strengthened by an exercise case pack containing curated practice cases with links or screenshots for labs, and by a capstone assessment guide that sets simple criteria and a rubric for scoring the final publish-ready fact-check package. Because OSINT tools, risks, and examples vary across contexts, organizations are encouraged to develop or customise these supporting materials to match their needs while maintaining the module's workflow, documentation discipline, and quality standards.

I) Monitoring And Evaluation Plan

This module uses a practical monitoring and evaluation approach focused on three questions: Did participants learn the workflow? Can they apply it to real verification tasks? Does the quality of their outputs improve? Measurement remains evidence-based and straightforward, combining short tests with a review of actual work produced during training.

Learning gains are measured using a short pre-test and post-test administered at the start of Day 1 and the end of Day 3. The tests assess core concepts such as claim framing, source tracing, visual verification basics, and ethical decision-making. Participants also rate their confidence across key skills before and after the training. Improvement is assessed by comparing average test scores and confidence ratings across the cohort.

Practical skills are measured through completion and quality of training outputs. Participants submit required lab products each day, including claim intake and evidence planning tools, verification logs for images and videos, and a geolocation and time verification worksheet. The capstone deliverable is a publish-ready fact-check package. Facilitators assess these outputs using a simple rubric that checks claim clarity, strength of evidence, transparency of steps, handling of uncertainty, ethical considerations, and clarity of writing.

To support continuous improvement during delivery, the module uses quick daily feedback and facilitator observation notes. Participants share what was most useful, what was unclear, and what they struggled with, allowing facilitators to adjust pacing and support in real time. Facilitators also document recurring challenges such as tool access, weak documentation habits, or common reasoning errors, which inform improvements for future deliveries.

Finally, post-training impact can be assessed through a brief follow-up check around 30 days after delivery. This captures whether participants have applied the workflow in their work, whether they produced or improved fact-checks using the module's methods, and which templates they continued to use. For organizations, an optional quality review of a small sample of fact-checks produced after training can provide deeper insight into sustained improvement.

For reporting and accountability, trainers retain basic evidence, including the agenda and attendance, aggregated pre-/post-test results, aggregated rubric scores, selected anonymised samples of participant outputs, and, where applicable, a summary of follow-up findings.

J) Sustainability And Integration Plan

After delivery, the OSINT module is designed to be integrated into routine editorial and verification workflows rather than treated as a one-time training. Organizations can adopt the module's core templates (claim intake, evidence matrix, verification logs, and geolocation worksheet) as standard documentation for high-risk claims, especially those involving images, video, or fast-moving public narratives. This improves consistency and quality because conclusions are supported by a traceable evidence trail and a transparent method that editors and peers can review.

To keep the module usable over time, the training package includes simple mechanisms for maintenance and updating. A designated focal person or small team can periodically refresh the toolkit handout as tools evolve, update the case pack with locally relevant examples, and maintain a small internal library of strong verification logs and completed fact-check packages for reference. This prevents the training from becoming outdated and supports continuous learning without requiring repeated external facilitation.

Sustainability is reinforced through lightweight practice routines that fit real newsroom constraints. Teams can run short verification clinics, one case at a time, apply peer review to verification logs to strengthen documentation discipline, and use the capstone rubric as a quality benchmark for publish-ready investigations. This approach helps individual fact-checkers and organizations maintain skills, standardise decision-making, reduce avoidable errors, and reuse the module for onboarding and future training.