

OSINT verification checklist (short, printable)

OSINT Video Verification Checklist — Quick Reference

1. **Source verification**
 - Is the uploader a named person or newsroom? Can we contact them? Have they posted related local content previously?
2. **File provenance**
 - Was the original file provided (not re-upload)? Is there metadata/EXIF available? If metadata missing, did uploader explain why?
3. **Temporal consistency**
 - Upload timestamp consistent with claimed event time? Are weather/sun position consistent with claimed time/date?
4. **Geolocation**
 - Can we match skyline/street features to satellite or street-view imagery? Are unique landmarks present and consistent?
5. **Reverse search & archival check**
 - Frame grabs reverse-searched (InVID, Google) — any prior matches? Clip appears in news archives / earlier conflicts?
6. **Visual forensic checks**
 - Repeating patterns or cloned textures in frames? Motion/physics realistic (smoke, lighting, debris)? No obvious compositing seams?
7. **Audio analysis**
 - Does weapon sound match known audio of system claimed? Are ambient sounds consistent with location (language, traffic)?
8. **Cross-corroboration**
 - Is there satellite imagery (Planet Labs, Maxar) confirming event? Do other independent eyewitnesses or reporters corroborate?
9. **AI / Deepfake detection**
 - Run through AI-detection tools (e.g., synthetic media detectors) — flags? Look for impossible camera moves or hyper-real textures?
10. **Legal & ethical checks**
 - Is the footage graphic — has consent/ethics been considered? Is publication likely to endanger sources or victims?
11. **Publish decision**
 - Verified: publish with clear sourcing and verification notes.
 - Unverified but newsworthy: publish with clear caveats & “unconfirmed” label.
 - Do not publish: false, manipulated, or unverifiable within editorial standards.

Document reference:

reporter name,

contact,

file hash,

verification steps performed,

date/time,

handling editor initials.