Association *of* Internet Research Specialists

ONLINE VIDEOS AUTHENTICATION & EVIDENCE MANAGEMENT

Authenticating Online Videos & Images

May 10, 2026

Submitted by:
Naveed Manzoor
Association of Internet Research Specialist | AOFIRS

USVA7777904052027

ONLINE VIDEOS AUTHENTICATION & EVIDENCE MANAGEMENT

CIRS Training Notes

Authenticating Online Videos & Images

CIRS™ Reference Edition — June 2026 Reprinted
Association of Internet Research Specialists (AOFIRS)

By: Naveed Manzoor

Disclaimer of Accuracy and Liability*. The information, references, tools, statistics, case studies, and third-party content presented in this publication are provided for general educational and professional reference purposes only. While every reasonable effort has been made to ensure that the material contained herein is accurate, current, and complete at the time of writing, the author and the Association of Internet Research Specialists (AOFIRS) make no representations or warranties of any kind, express or implied, as to the accuracy, reliability, completeness, suitability, or availability of any information, tools, software, services, or related content referenced or described in this document. The rapidly evolving nature of internet research, digital forensics, artificial intelligence, and related technologies means that information, tool capabilities, software versions, and regulatory frameworks may change at any time without notice. Readers are advised to independently verify all information, consult qualified legal, technical, or professional advisers as appropriate, and exercise their own professional judgement before relying on any content herein for investigative, legal, or operational purposes. The author and AOFIRS accept no responsibility or liability for any loss, damage, claim, or expense — whether direct, indirect, incidental, or consequential — arising from the use of, or reliance upon, any information or materials contained in this publication, or from any errors, omissions, or inaccuracies therein, whether caused by negligence or otherwise.* ***Jurisdictional Note.*** *References to legislation, regulatory guidance, and legal standards in this document are provided for informational context and do not constitute legal advice. Applicable laws and regulations vary by jurisdiction and may have changed since publication. Readers operating in specific legal or regulatory environments should seek independent legal counsel.*

TABLE OF CONTENTS

1. Online Video Market — Size & Background 7
   1.1 Types of Online Video Content 7
2. Online Videos Requiring Authentication 9
   2.1 News Story Videos 9
   2.2 Social Media Video Clips 9
   2.3 Video Evidence in Legal Proceedings 9
   2.4 Political Views & Campaign Videos 9
   2.5 User-Generated Video 9
   2.6 Historical Examples of Video Evidence in International Justice 9
3. Video and Photo Evidence — Legal Requirements 11
   3.1 Foundations of Digital Evidence Admissibility 11
      3.1.1 Relevance of Evidence 11
      3.1.2 Evidence Authenticity and Reliability 11
      3.1.3 Digital Evidence Cannot be Hearsay 11
      3.1.4 Best Evidence or Corroborative Evidence 11
      3.1.5 Probative Value Must Outweigh Any Prejudicial Effect 11
   3.2 Chain of Custody 11
4. Video Tampering — Classification, Types & Forensic Detection 13
   4.1 Spatial Tampering 13
   4.2 Object Manipulation Attacks 13
      4.2.1 Object Removal 13
      4.2.2 Object Copy-Move (Copy and Paste Attacks) 14
      4.2.3 Object Modification 15
      4.2.4 Pixel-Level Tampering 16
   4.3 Temporal Tampering 17
   4.4 Spatio-Temporal Tampering 17
5. Video Technology — File Formats, Codecs & Containers 19
6. Metadata in Camera (Videos and Photos) 21
   6.1 Types of Video Metadata 21
7. Fake Video & Voice Production Software & Tools 22

7.1 Image Translation AI (NVIDIA GAN) 22
7.2 Audio-Track Changes Matching Facial Expressions & Lip Movements 22
7.3 Face-to-Face Facial Expression Mimic (Face2Face) 23
7.4 Photorealistic Video-Editing Tools (CGI) 24
7.5 VoCo — Adobe's Audio Alteration Tool 24
7.6 CycleGAN — Video Image-to-Image Translation Tool 25
7.7 Voice Manipulation and Mimicking Anyone's Voice (Lyrebird) 26
8. Identifying Fake Videos — Social Media Analysis 28
8.1 Issues and Difficulty of Identifying Fake Videos 28
8.2 Notice Sudden Spikes and Lows in Video Views 28
8.3 Extensions to Obtain Important Data from YouTube 29
8.3.1 VIDLOG (Vidooly YouTube Extension) 29
8.3.2 vidIQ Vision for YouTube 30
8.3.3 Frame by Frame Extension 30
8.3.4 Fact Checker Extension for YouTube 31
9. Verify Time, Date, Context & Examine Frames — Step-by-Step 33
9.1 YouTube Search 33
9.2 Amnesty International YouTube Data Viewer 33
9.3 Frame-by-Frame Extraction 34
10. InVID — Video Verification Platform 37
10.1 InVID Core Capabilities 37
10.1.1 Check for Any Prior Use of the Video 37
10.1.2 Check the Video's Origin and Rights 37
10.1.3 Check Video Forensics 37
10.2 InVID Applied Example 39
11. AI-Powered Deepfake Detection for OSINT Investigators (2026) 43
11.1 How Modern Deepfakes Are Created 43
11.2 AI-Powered Deepfake Detection Platforms 43
11.3 Key Detection Techniques 44
11.3.1 Visual Artefact Analysis 44
11.3.2 Photoplethysmography (rPPG) Liveness Analysis 44
11.3.3 Audio-Visual Synchronisation Analysis 44
11.3.4 Acoustic Analysis & Voice Cloning Detection 45

11.3.5 Geolocation & Environmental Consistency Analysis 45
12. Use Case: Verifying a Conflict Zone Video Using the CIRS Protocol 46
13. The CIRS™ Programme — Learning Video Verification Professionally 48
13.1 What the CIRS™ Programme Covers in Video Verification 48
13.2 Who the CIRS™ Programme Is Designed For 48
13.3 The Habit That Makes the Difference 49

1. Online Video Market — Size & Background

As digital trends evolve with the growth of the Internet and its social media networks we see trends favoring online videos over textual content. Research consistently shows that people respond more effectively to visual information than plain text, with estimates placing the advantage at roughly 40 percent (WebMarketingGroup, 2018).

According to an e-Market Reports article (2018), approximately 2.38 billion people globally were watching streaming or downloaded digital video content at least once per month. In social media platforms, YouTube alone reported 100 hours of video uploaded every minute. About 72% of online adults use video-sharing sites like YouTube or Vimeo (Pew Research Center, 2013).

Source: Pew Research Center (2013); e-Market Reports (2018)

2026 Update: By 2026, global online video viewership has grown to over 3.5 billion monthly viewers. Short-form video (TikTok, Instagram Reels, YouTube Shorts) now dominates consumption. AI-generated video content is a significant and growing portion of total uploads, requiring new authentication approaches (Europol, 2025).

1.1 Types of Online Video Content

The original CIRS module categorises online video into the following primary types, each requiring different verification considerations (AOFIRS, 2020):

- News & Broadcast Media (Broadcast Journalism, Video Journalism, Citizen Journalism)
- Educational Videos (DIY, Demo Videos, Tutorials & Training Videos)
- Entertainment Related Videos (Music Videos, Films, TV Clips, Documentaries)
- Video Interviews, Political Views & Campaigns, Propaganda Videos
- Surveillance and CCTV Footage
- Video Evidence (incidents, accidents, humanitarian crises, war zones, citizen recordings)
- Live Videos Streaming (Twitter, YouTube Live, Facebook Live, Instagram, Snapchat)
- Social Media Videos (Personal shares, Group Videos, Marketing Videos)
- User-Generated Videos (Bloggers, Serial Video Makers with Large Followings)

Video authentication aims to ensure the trustworthiness of the video by verifying the integrity and source of video data (Stamm et al., 2012). When verifying a video clip, practitioners are in fact dealing with three types of multimedia formats in a single video:

- **Video Streams —** Video Streams
- **Image Frames —** A video is made up of frames — still images that when updated rapidly each second become a moving image to the human eye.
- **Voice (Audio Files) —** Formats like MP3, MP4 are audio formats enclosed within container formats, containing the audio track that plays voice inside a video.

All three (3) components require verification to deem authentic. Especially, deep fake software has made use of technology that allows users to digitally superimpose a face onto someone else's body or imitate voice in unison with altered natural lip movements of the subject (Tolosana et al., 2020).

2. Online Videos Requiring Authentication

2.1 News Story Videos

News media is the largest information source today. However, because of the undue bias and the advent of Fake News making its way into the mainstream online news channels, it has now become the least-trusted institution globally. It is estimated that 7 in 10 people worry about false information or fake news being used as propaganda machinery by the government and different interest groups (Reuters Institute, 2022).

2.2 Social Media Video Clips

Social media is the most dangerous force for spreading misinformation and false information rapidly and recklessly (Vosoughi et al., 2018). Videos are routinely spliced, re-contextualised, and re-posted with fabricated captions. A clip filmed in one country is regularly presented as evidence of events in another.

2.3 Video Evidence in Legal Proceedings

Videos and photos serve as an important part of evidence collection needed to prove a civil lawsuit or criminal acts (Mason, 2017). Key questions arise: Where and how were the videos made? By whom? And with which device? What is the trail of evidence and chain of custody?

2.4 Political Views & Campaign Videos

Fake video and audio are a serious threat not just to individual political campaigns, but to the entire political system (Chesney & Citron, 2019). These usually include fake images, inflammatory quotes, edited material, rigged campaign ads, and fake websites containing fake videos.

2.5 User-Generated Video

With smartphones, camera drones, patrol-car dashboards, body-worn cameras, and CCTV surveillance cameras, video evidence is now standard in most court cases (Casey, 2011). Citizen journalists often risk their lives to capture unusual events that expose injustice or atrocities.

2.6 Historical Examples of Video Evidence in International Justice

- Lubanga child soldier case (ICC): Video clips sparked the investigation, though could not independently prove the age of children (ICC, 2012)
- Ghouta and Bhopal chemical attacks: Video served as lead evidence but not direct linkage evidence (OPCW, 2013)
- Darfur, Sudan: Sufficient visual evidence existed to move the case forward in international court (ICJ, 2010)
- Al-Houlah Massacre, Syria: Footage triggered a UN special inquiry (UN Human Rights Council, 2012)

- Video of General Ratko Mladic Speech: Served as linkage evidence connecting senior officials to command decisions (ICTY, 2013)
- Serbian journalist manipulated video evidence in the Srebrenica case, demonstrating video can be an instrument of deception (ICTY, 2004)
- Videos on human rights abuses in Sri Lanka: Used before the U.N. High Commissioner for Human Rights in Geneva (UNHCR, 2010)

Video evidence can be: Crime-based Evidence (proves a crime occurred), Linkage Evidence (proves who committed it), Lead Evidence (suggests further investigation), or Corroborative Evidence (backs up other proof). Authentication requirements differ across these categories (Casey, 2011).

3. Video and Photo Evidence — Legal Requirements

The collection of digital evidence from the Internet is a discipline of digital forensics dealing with the securing of data as evidence from the Internet (Casey, 2011). An online researcher must understand that any video clips and images collected from the web as evidence must comply with Digital Evidence Law, covering Authentication, Techniques and Procedures.

3.1 Foundations of Digital Evidence Admissibility

3.1.1 Relevance of Evidence

The evidence must be relevant to the claims asserted, i.e., it must have "any tendency" to prove or disprove a consequential fact in the litigation (Mason, 2017).

3.1.2 Evidence Authenticity and Reliability

Authenticity establishes that digital data or a document is what it is represented to be. Reliability establishes whether a piece of evidence is what it purports to be (Casey, 2011). A video can be authentic (not manipulated) but unreliable (the events depicted were staged).

3.1.3 Digital Evidence Cannot be Hearsay

Hearsay is an out-of-court statement introduced for the truth of the matter asserted. Machine-generated records are generally not hearsay; human-created content embedded in digital records may be (Mason, 2017).

3.1.4 Best Evidence or Corroborative Evidence

A best evidence standard applies if there are no originals of digital evidence. In Prosecutor v. Karemera, the International Criminal Court Tribunal held that a broadcast transcript authenticated the date of the video (ICTR, 2006).

3.1.5 Probative Value Must Outweigh Any Prejudicial Effect

The court may exclude relevant evidence if its probative value is substantially outweighed by the danger of unfair prejudice, or by considerations of graphic nature, undue delay, or waste of time (Mason, 2017).

3.2 Chain of Custody

To become authentic evidence in court, electronic data must show an "unbroken chain of custody" (Casey, 2011). The source of the multimedia file must have a clear trail showing exactly how the file was handled from creation to presentation.

- An unbroken, linear timeline showing chronological activity from capture to evidence submission
- Proof of controls ensuring the video is the same, unaltered digital file as the day it was stored (SHA-256 hash is the current standard)
- Absence of any gaps in custody documentation

- Activity logs tracking all relevant events with user identity, IP address, SHA-256 fingerprint, and timestamp

For video and photos, chain of custody requires answers to: What kind of recording device was used? Who had access? Who owned it? Was information retrieved from a network or cloud? Was the information password protected? Where is the original file stored? Has it been transcoded or compressed?

4. Video Tampering — Classification, Types & Forensic Detection

The scientific community has classified video tampering attacks into three primary categories, following the taxonomy adopted in the original CIRS training module from the International Journal of Computer Science Issues (Stamm et al., 2012):

4.1 Spatial Tampering

Spatial tampering occurs at the image frame level and can be performed at two levels:

- Block Level — manipulation of groups of pixels (macro-blocks)
- Pixel Level — manipulation of individual pixels

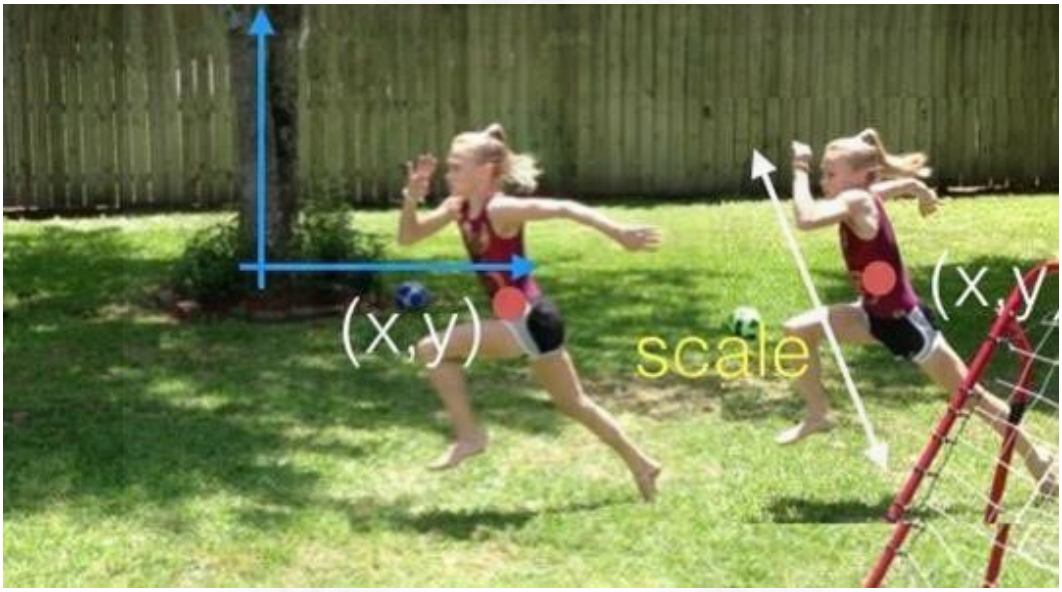

Figure 2 — Spatial Tampering at Block Level and Pixel Level — Objects, Foreground and Background

4.2 Object Manipulation Attacks

4.2.1 Object Removal

In object removal attack, objects of the frames of the video are eliminated. This kind of attack is commonly performed where a particular person wants to hide their presence in a certain sequence of frames (Stamm et al., 2012).

Figure 3 — Object Removal: A soldier is removed from the background and the grass is blended with the scene

4.2.2 Object Copy-Move (Copy and Paste Attacks)

In this attack, an object from another image is copied and pasted into the original image. The object can be moved around the frame, resized or blended with the background to conceal the manipulation:

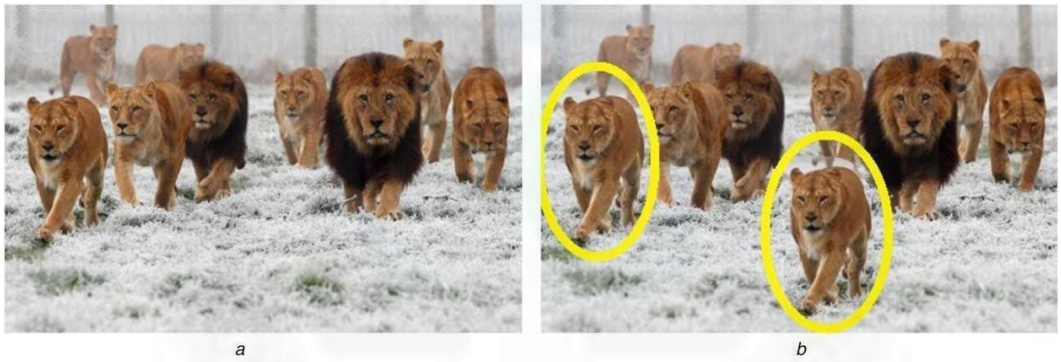

Figure 4 — Object Copy-Move: A Lioness is copied and moved to the foreground

Example of Removing the Background Object — wire removed from the background as an object in frame:

Figure 5 — Background Object Removal: Wire removed from the background of a surveillance frame

4.2.3 Object Modification

Object modification involves changing specific attributes of objects within frames:

Figure 6 — Object Modification: Foreground and background objects altered

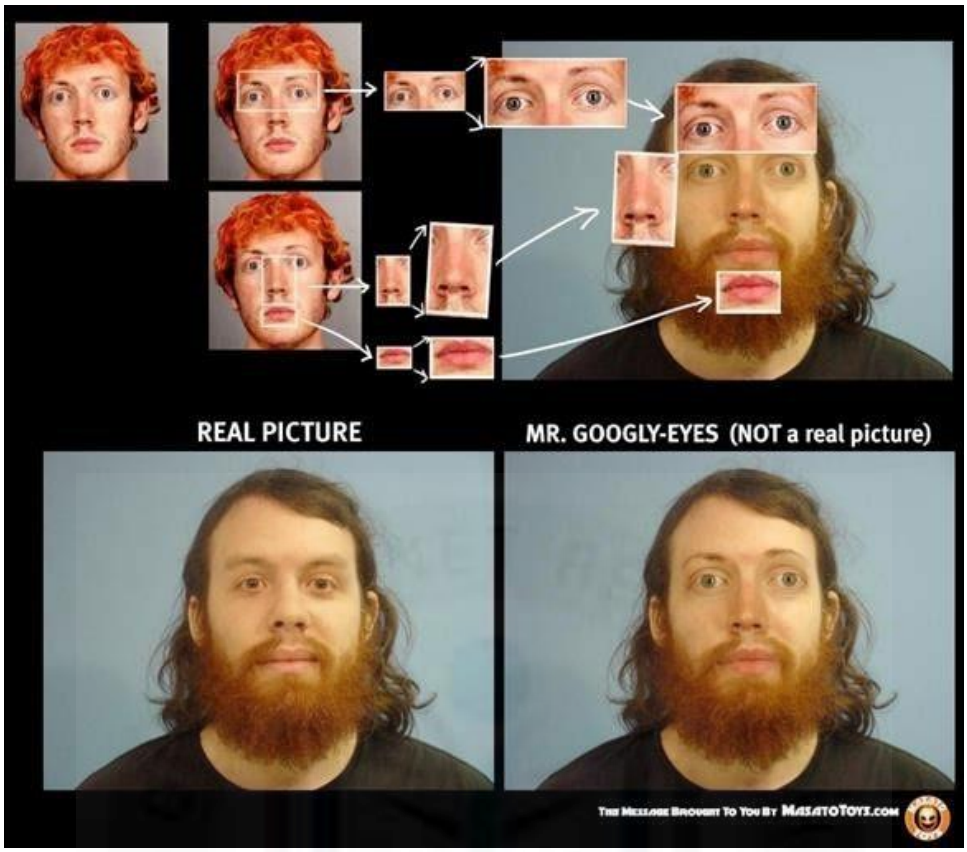

Figure 7 — Object Modification: Face of a person changed; a new person's face introduced in the altered frame

4.2.4 Pixel-Level Tampering

Tampering performed at the pixel level for more sophisticated manipulations:

Figure 8 — Pixel-Level Tampering: Real face of a person (left) vs. Modified face of a person (right)

4.3 Temporal Tampering

Temporal tampering manipulates the time sequence of the video rather than its spatial content (Stamm et al., 2012):

- **Frame Removal —** Frame Removal — Eliminating frames from a sequence to remove actions or events from the record
- **Frame Addition —** Inserting frames from other recordings to fabricate events
- **Frame Modification —** Altering individual frames within a sequence
- **Time Sequence Modification —** Reordering events chronologically to misrepresent causation or context

Figure 9 — Temporal Tampering: Frames in group (A) and (B) altered — time sequence modification

4.4 Spatio-Temporal Tampering

The most sophisticated category, combining both spatial and temporal manipulation. Commonly used in advanced deepfake operations where objects or persons are consistently removed, inserted, or replaced across multiple consecutive frames (Tolosana et al., 2020).

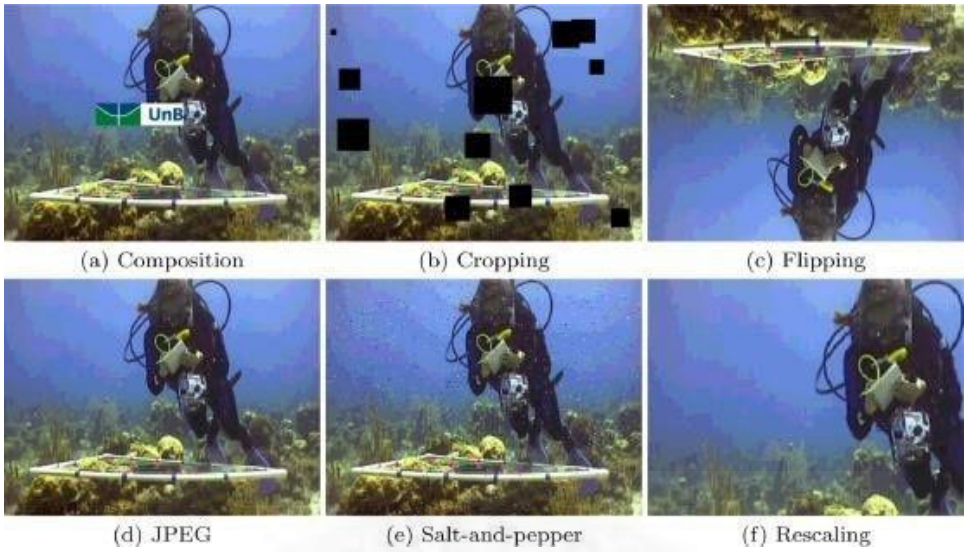

Figure 10 — Spatio-Temporal Tampering: Combined spatial and temporal manipulation across frames

Key Principle from CIRS Module 8: The taxonomy of video tampering (spatial, temporal, and spatio-temporal) is the foundational framework every investigator must understand before applying any forensic tool. Knowing what type of attack is present determines which detection method to deploy.

5. Video Technology — File Formats, Codecs & Containers

A video file format is a structure in which information is stored in a computer file. A video codec is an electronic circuit or software that compresses or decompresses digital video. Containers are bundles of media files that may also contain subtitles. Popular containers include .mp4, .mov, and .avi.

Common video file formats investigators will encounter:

Figure 11a — AVI Format

Figure 11b — ASF Format

Figure 11c — MOV Format

Figure 11d — AVCHD Format

Figure 11e — FLV Format

- AVI (Audio Video Interleave) — Microsoft format; long-running digital video workhorse. Open with: Windows Media Player, VLC.
- ASF (Advanced Systems Format) — Microsoft container; houses WMA/WMV codec files; offers DRM copy protection.
- MOV / QT (QuickTime) — Apple QuickTime Movie format; supports a wide range of codecs; cross-platform.
- AVCHD (Advanced Video Coding, High Definition) — Panasonic and Sony collaboration; used for digital camcorders; high-quality HD recording.
- FLV / SWF (Flash Video) — Flash Video format; common for online streaming historically; largely deprecated.
- MP4 (MPEG-4 Part 14) — Most widely used container for online video; excellent compression. Used by all modern platforms.

6. Metadata in Camera (Videos and Photos)

When someone takes a picture or video with a digital camera, the exact date and time of the shutter-release are recorded to the image file, along with many other bits of metadata. Digital cameras append metadata according to a standard format called EXIF, short for "Exchangeable Image File" (Friedman & Rosenfeld, 2008).

In Photoshop, someone can edit certain parts of the EXIF data. So if you don't have direct access to the camera and photos are already downloaded, there is a chance that the metadata has been tampered. The original timestamp is 'read-only' with standard software, but a utility called ExifTool can be used to edit timestamps.

6.1 Types of Video Metadata

- **Operational Metadata —** Operational Automatically Gathered Metadata: Equipment used, software applied, creation date, GPS coordinates, frame rate, codec settings, exposure details.
- **Human-Authored Metadata —** Titles, descriptions, tags, and other fields entered by the publisher — as on YouTube. Entirely user-controlled and therefore unauthenticated.

Key metadata fields investigators examine:

- Date-Timestamp: Recorded when shutter releases; also when file is written to memory card
- GPS coordinates: Location data where location services were enabled (can be falsified using ExifTool post-capture)
- Device identifiers: Manufacturer, model, and sometimes firmware version
- DCIM folder structure: Digital Camera Images folder (DCF standard from 2003)
- THM files: Thumbnail and metadata files accompanying .MP4 recordings on camera-type devices

2026 Update: ExifTool has become the industry standard for metadata and file forensics in 2026, supporting images, video, audio, and documents. OSINT analysts use it to extract timestamps, geolocation, device details, and edit history — all critical signals when validating evidence or checking whether media has been tampered with (Harvey, 2023).

7. Fake Video & Voice Production Software & Tools

The following section documents the key technologies that investigators must understand — both to recognise when they have been used and to apply appropriate countermeasures (Chesney & Citron, 2019).

7.1 Image Translation AI (NVIDIA GAN)

Researchers from Nvidia created an image translation AI using Generative Adversarial Networks (GANs) — two neural networks working against each other; one generates content while the other critiques its work (Goodfellow et al., 2014). Applications include day-to-night transformation, season substitution, and species swapping.

Figure 12 — NVIDIA Image Translation AI: Day-to-night and environment transformation using GAN technology

Source: Liu et al. (2017)

7.2 Audio-Track Changes Matching Facial Expressions & Lip Movements

Researchers at the University of Washington created a tool that takes audio files, converts them into realistic mouth movements, and grafts those movements onto existing video (Suwajanakorn et al., 2017). Demonstrated using 17 hours of Obama footage.

Figure 13 — Audio-to-Lip-Sync AI: Obama mouth movements generated from audio of a different speech (Suwajanakorn et al., 2017)

Source: Suwajanakorn et al. (2017)

7.3 Face-to-Face Facial Expression Mimic (Face2Face)

In 2016, Face2Face researchers demonstrated real-time transfer of facial expressions between individuals, processed in approximately 30 milliseconds (Thies et al., 2016). Demonstrated using George W. Bush, Vladimir Putin, and Donald Trump.

Figure 14 — Face2Face: Real-time facial expression transfer (Thies et al., 2016)

7.4 Photorealistic Video-Editing Tools (CGI)

Professional CGI used in Hollywood has become accessible at consumer price points. The reconstruction of Peter Cushing (deceased since 1994) in Star Wars: Rogue One previewed the techniques now routinely used in both entertainment and disinformation (Allen, 2017).

Figure 15 — Hollywood CGI: Peter Cushing's face reconstructed digitally in Star Wars: Rogue One

7.5 VoCo — Adobe's Audio Alteration Tool

Adobe's VoCo lets you edit recorded speech to alter what that person said or create entirely new sentences from their voice. Users type new words and the system constructs them from the speaker's phoneme library (Jin et al., 2017). Requires approximately 20 minutes of training audio.

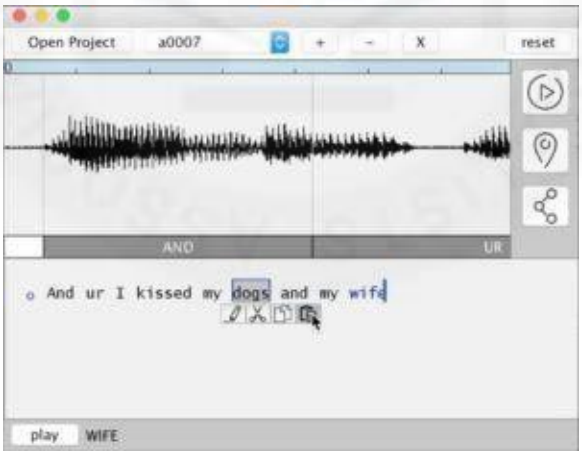

Figure 16 — Adobe VoCo: Copy and paste existing words within the audio transcript

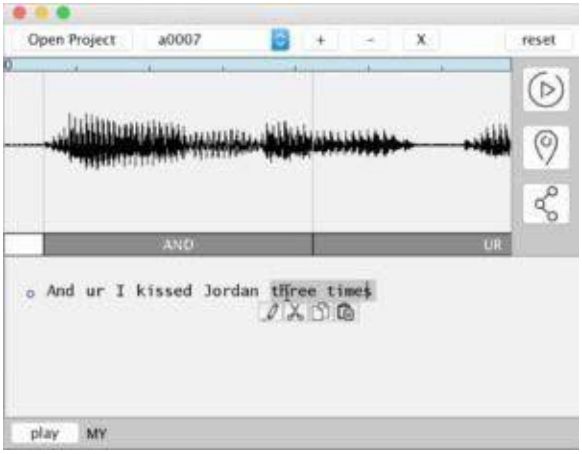

Figure 17 — Adobe VoCo: Write whole new words and VoCo synthesizes them in the speaker's voice

Figure 18 — VoCo in action: Complete audio editing interface showing word-level manipulation of recorded speech

Source: Jin et al. (2017); Arstechnica (2016)

7.6 CycleGAN — Video Image-to-Image Translation Tool

CycleGAN can generate photos from paintings, turn horses into zebras, perform style transfer, and more without requiring input-output pairs (Zhu et al., 2017):

Figure 19 — CycleGAN: Transforms Horses into Zebras in both still images and video (Zhu et al., 2017)

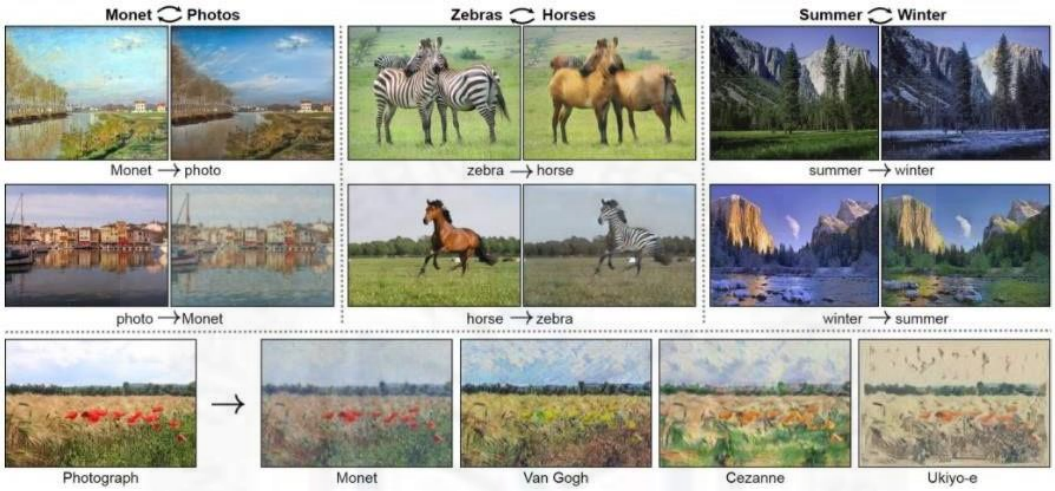

Figure 20 — CycleGAN: Other examples — painting to photo, summer to winter, and more

Source: Zhu et al. (2017)

7.7 Voice Manipulation and Mimicking Anyone's Voice (Lyrebird)

LYREBIRD allows anyone to create their digital voice with only one minute of audio (Oord et al., 2016). Simply record yourself for at least one minute and you can generate any sentence you like with your digital voice.

Figure 21 — Lyrebird: Voice synthesis interface — creating a digital replica of any person's voice from just one minute of audio

2026 Update: By 2026, commercial voice cloning services (ElevenLabs, Resemble AI, Murf, HeyGen) can produce convincing voice replicas from as little as 3 seconds of audio. These tools are used in sophisticated fraud operations, CEO impersonation scams, and political disinformation campaigns (FBI IC3, 2025).

8. Identifying Fake Videos — Social Media Analysis

Social media is where smartphone cameras really score. Most people upload video clips and pictures using smartphones because of their portability. However, with this convenience comes the spread of fake video clips and news stories as a genuine problem (Wardle & Derakhshan, 2017).

Figure 22 — Issues and Difficulty of Identifying Fake Videos (AOFIRS Training Module 8)

8.1 Issues and Difficulty of Identifying Fake Videos

- Videos spread across social media in a way that makes the version you first see unlikely to be the original (Vosoughi et al., 2018)
- Videos may be spliced, diced and reposted with a different context
- Sophisticated tools alter form, colour, pixel, background, and object placement so important traces from the original video may disappear
- Difficulty in identifying the primary source, the device used, the date and time stamp
- Pressure to deliver news quickly results in un-verified and un-filtered content being published
- Fake views are acquired via bots or scripts that game the system, resulting in inflated numbers and increased ad revenues

8.2 Notice Sudden Spikes and Lows in Video Views

The video views spike right after publishing, and then there is almost nothing after that — almost like views were bought and all delivered very quickly:

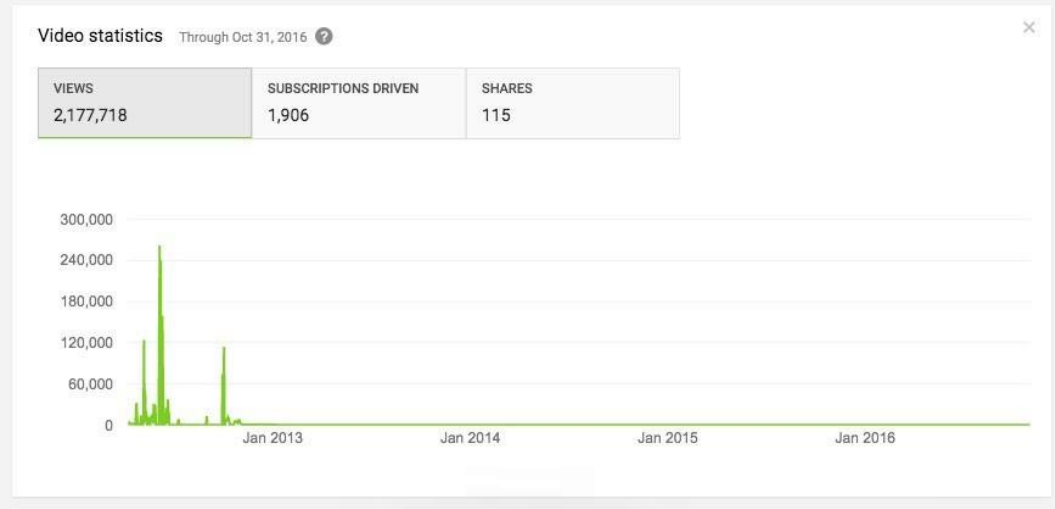

Figure 23 — YouTube Views Analytics: Sudden spike after upload followed by near-zero subsequent activity — classic indicator of purchased views

8.3 Extensions to Obtain Important Data from YouTube

8.3.1 VIDLOG (Vidooly YouTube Extension)

Vidooly's YouTube Chrome Extension 'vidlog' can help you find out the estimated earning of any video and gives a detailed performance analysis across all Social Media Platforms.

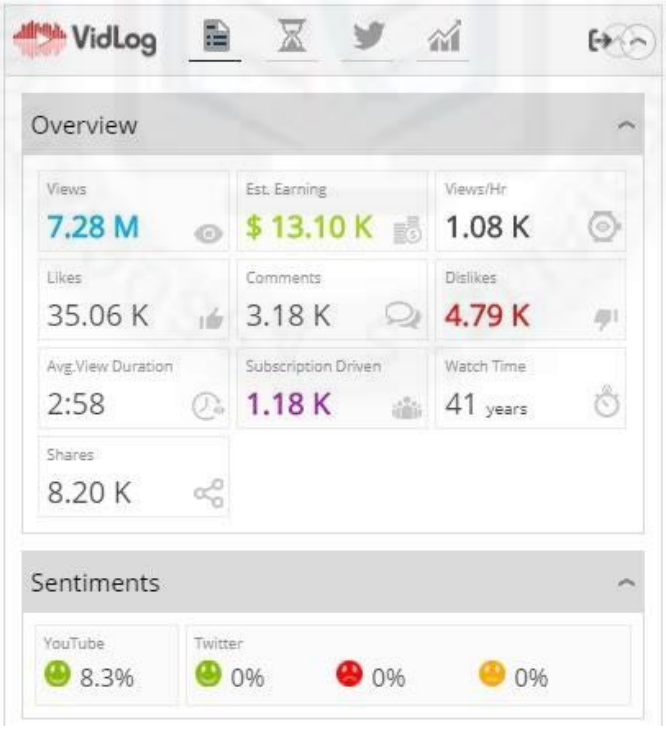

Figure 24 — vidlog: Performance analysis and estimated earnings for any YouTube video

8.3.2 vidIQ Vision for YouTube

vidIQ Vision for Google Chrome helps you understand why videos are promoted in Related Videos, Search, and Recommended Videos — essential for identifying channels using SEO manipulation to promote misleading content.

Figure 25 — vidIQ: Interface showing video analytics — useful for detecting manipulated promotion patterns

8.3.3 Frame by Frame Extension

A Chrome extension adding frame-by-frame navigation to the YouTube player. Pause the video, then press < or > (comma and period keys) to go one frame forward or backwards — essential for detecting inserted or modified frames.

Figure 26 — Frame by Frame Extension: YouTube player with frame-by-frame navigation enabled

8.3.4 Fact Checker Extension for YouTube

The Fact Checker extension enables evidence sharing with browser annotations on any fact-checked web page, making evidence available exactly when and where it is needed most.

Figure 27 — Fact Checker Extension: Browser toolbar showing annotation and fact-checking controls

Figure 28 — Fact Checker: Interface showing fact-check annotations overlaid on web video content

9. Verify Time, Date, Context & Examine Frames — Step-by-Step

The following demonstrates a practical video verification workflow using the Amnesty International YouTube Data Viewer and the InVID platform. Example query: [Aleppo Hospital Bombing]

9.1 YouTube Search

Begin with a YouTube search for the video clip using relevant keywords. Copy the video link URL for use in verification tools.

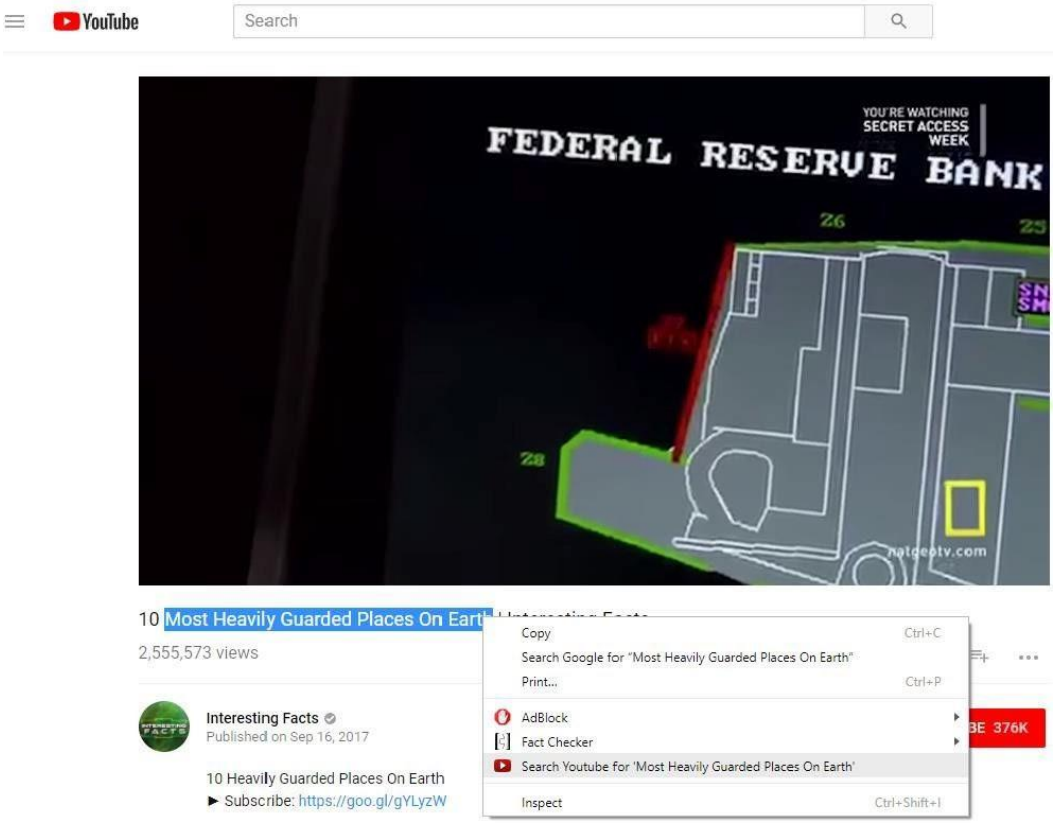

Figure 29 — YouTube Search: Searching for the Aleppo Hospital Bombing video clip and copying the URL for verification

9.2 Amnesty International YouTube Data Viewer

Insert the YouTube video link in the Amnesty International Data Viewer (citizenevidence.amnestyusa.org) to extract the exact upload time (Amnesty International, 2015):

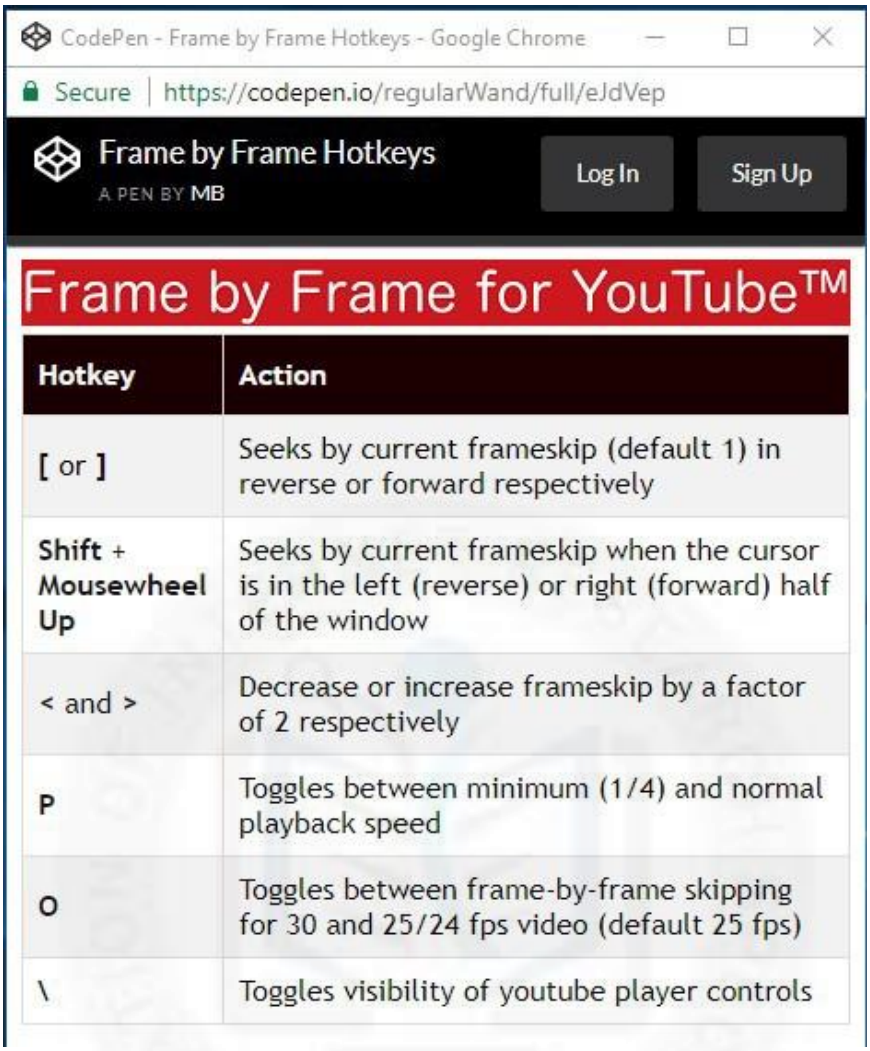

Figure 30 — Amnesty International YouTube Data Viewer: Showing Video Clip Title, Contextual Description, Video ID, Date of Upload and Time

9.3 Frame-by-Frame Extraction

The video clip is broken into several frames that can then be used for reverse image search to determine if the footage appeared elsewhere online before the claimed date (Dubberley et al., 2020):

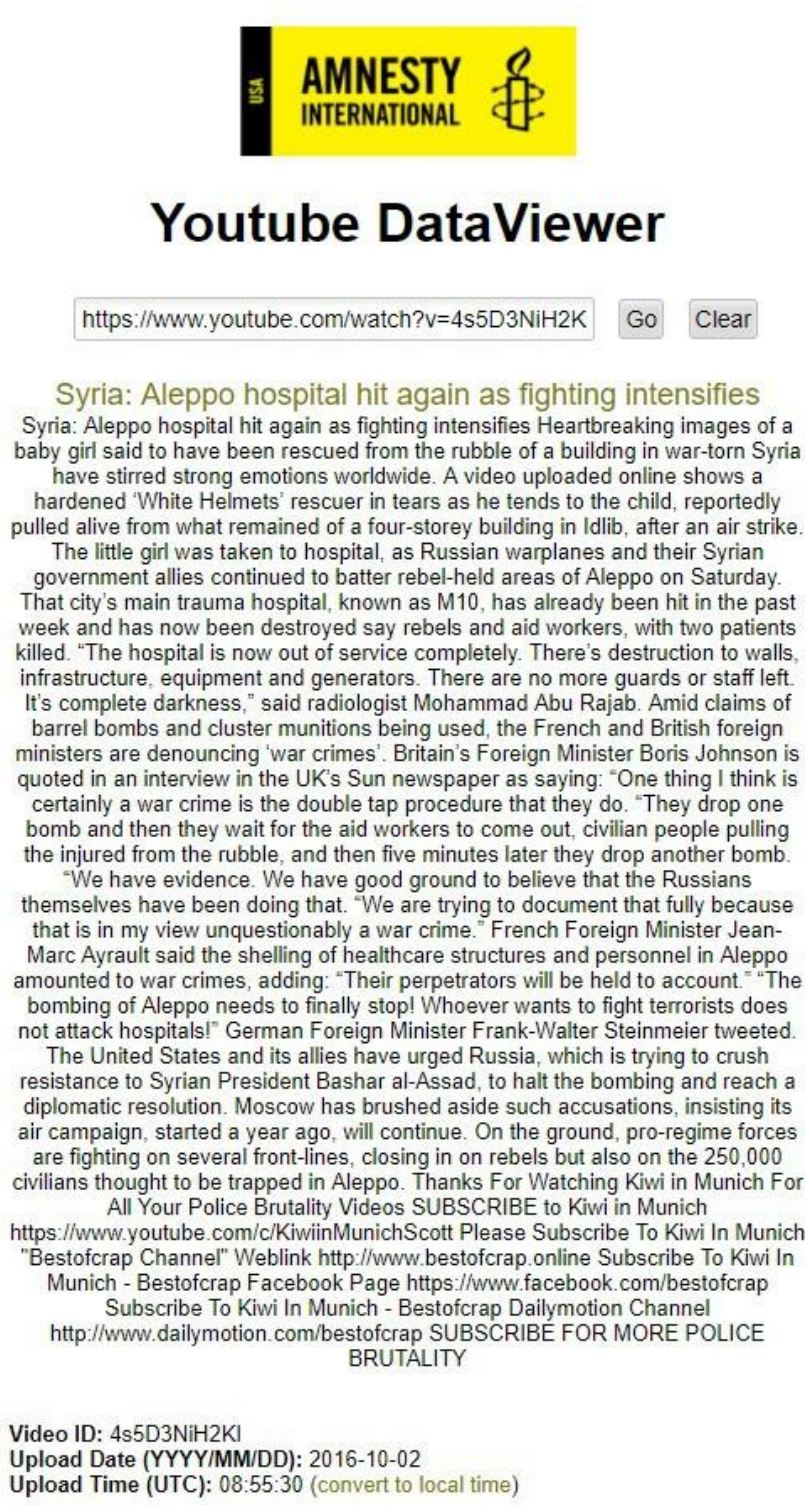

Figure 31 — Data Viewer Frame Extraction: Four extracted keyframes from the video at different timestamps — used for reverse image search

10. InVID — Video Verification Platform

InVID provides a platform to detect, authenticate and check the reliability and accuracy of newsworthy video files and video content spread via social media (Papadopoulos et al., 2017). InVID has evolved through successive EU-funded research projects (InVID, WeVerify, VeraAI) and is now the primary OSINT video verification toolkit used by journalists, fact-checkers, and human rights defenders worldwide, with over 57,000 weekly active users.

10.1 InVID Core Capabilities

10.1.1 Check for Any Prior Use of the Video

- Performing reverse video search on the InVID repository via parallel video playback functionality
- Performing reverse video search on the Web using provided video thumbnails (applicable for YouTube videos)

10.1.2 Check the Video's Origin and Rights

- Performing video logo detection
- Applying social-media-based contextual analysis
- Assessing location, time and other video metadata, as well as historical weather data

10.1.3 Check Video Forensics

- Applying advanced video forensic filters
- Performing frame-level inspection of the video in the user interface player

Figure 32 — InVID: Toolbar interface with video URL input field

Figure 33 — InVID: Sidebar showing verification tools — reverse search, metadata, forensic filters, and frame analysis options

Figure 34 — InVID: Frame analysis grid showing multiple extracted frames from the video clip under investigation

10.2 InVID Applied Example

The following screenshots show InVID applied to a real video verification case (Papadopoulos et al., 2017):

Figure 35 — InVID: Video forensic filter applied — noise analysis reveals compression inconsistencies indicating possible manipulation

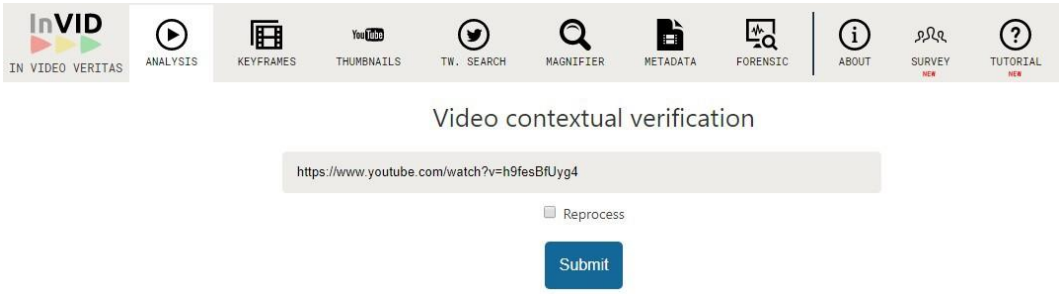

Figure 36 — InVID: Frame comparison results showing keyframes extracted and queued for reverse image search

Video:

Video title	15 Bizarre Recently Discovered Creatures
Video description	You won't believe these 15 amazing and shocking animal discoveries from a giant bizarre looking bat to rare new species! Subscribe to Knowledge Feed for Myth Mania Mondays, Fact Tree Tuesdays, Wildlife Wednesdays, Origin Thursdays, Fun Fact Fridays & Wildcard Weekends. 9. Albino Sea Turtle Volunteers cleaning up the shores of Australia spotted a very rare albino green sea turtle in February. The creature, which hatched on February 6 was seen wandering on the beach until it eventually headed into the sea. Sadly, the adorable turtle's chances of survival are not high. A common green turtle only has a one in one thousand shot of surviving to maturity, and the albino's shot is even worse as its light pigment makes it an easy target for predators. 8. Sparklewing Researchers have been busy in central Africa lately. They have discovered 60 new species of dragonflies and damselflies throughout the continent, which is the most to be documented at one time in over a ce

Figure 37 — InVID: Reverse image search results — showing whether extracted frames appear in other online sources before the claimed date

Video view count	1464525
Like count	4987
Dislike count	947
Duration	00:06:54
Upload time	2016-12-02, 18:30:04 (UTC)
Licensed content	true
Description mentioned locations	
Recording location description	

Figure 38 — InVID: Metadata extraction results showing device information, upload date, and geographic data

Channel:

Channel description	Join us for Myth Mania Mondays, Fact Tree Tuesdays, Origin Wonder Wednesdays & Fun Fact Friday with amazing and fun educational videos every week about culture and our w orld.
Channel created time	2013-12-11, 07:07:10 (UTC)
Channel view count	32034676
Channel page	https://www.youtube.com/channel/UCrDCvog6xEovYPAB3wlZpvA
Channel location	US

Figure 39 — InVID: Forensic analysis filter results showing ELA (Error Level Analysis) applied to a video frame

Figure 40 — InVID: Advanced forensic view showing noise pattern analysis across multiple frames

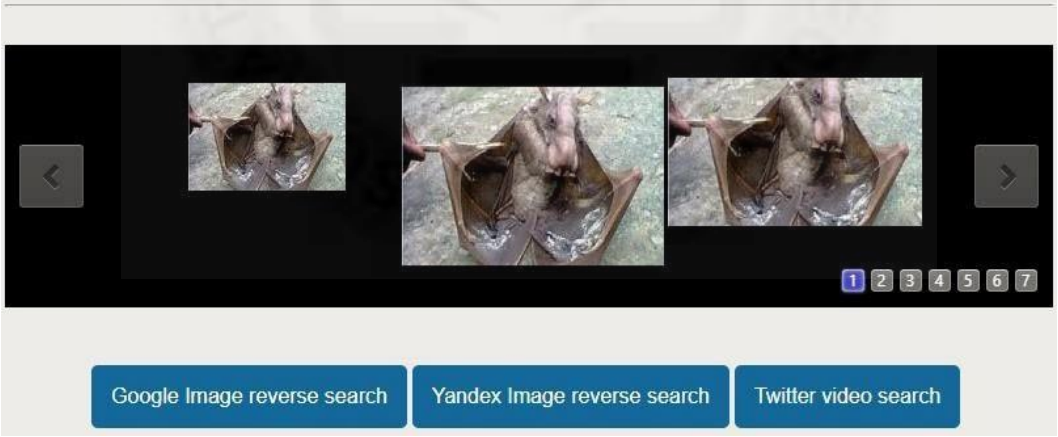

Figure 41 — InVID: Final verification summary panel showing authentication status across all analytical dimensions

2026 Update: InVID v0.89 (updated March 2026) now includes a dedicated Deepfake tab powered by an ensemble of five CNN-based detectors (Xception, EfficientNet-B4, Capsule-Forensics++, and two proprietary models), outputting a 0–1 probability score per frame. A Hiya-powered voice clone detector and WACZ disinformation archiving module have also been added (VeraAI Consortium, 2026).

11. AI-Powered Deepfake Detection for OSINT Investigators (2026)

This section extends the original CIRS Module 8 curriculum with current methods and tools. The techniques taught in the original module remain foundational — this section adds the AI detection layer that addresses threats that did not exist when the module was first written.

Deepfake technology has moved from a research curiosity to an operational threat. An estimated 8 million deepfakes were shared in 2025 alone — up from 500,000 in 2023, representing a 16-fold increase in two years (European Parliamentary Research Service, 2025). The FBI's 2025 IC3 Annual Report recorded 22,364 AI-related fraud complaints generating nearly $893 million in losses — the first year the FBI formally classified AI-facilitated crime as its own category (FBI IC3, 2025).

The visual impression of reality is something that can be manufactured at consumer scale. A convincing, contextually appropriate video can be produced in hours by someone with a subscription to commercially available AI tools and no specialist technical knowledge (Tolosana et al., 2020).

11.1 How Modern Deepfakes Are Created

- Face-swap networks: Deep learning models that map one person's facial geometry onto another person's video, frame by frame (Rossler et al., 2019)
- Face reenactment: Driving a target person's face using a source actor's movements (Thies et al., 2016)
- Full-body deepfakes: Extending face manipulation to full body posture and motion
- Voice cloning with lip sync: Combining a cloned voice with synchronized lip movements (Wang et al., 2018)
- Text-to-video (Sora, Runway Gen-3, Pika): A text prompt plus a single photograph can generate a convincing short video — no source footage required (OpenAI, 2024)

11.2 AI-Powered Deepfake Detection Platforms

Tool / Platform	Primary Function	Best For
CloudSEK	Real-time deepfake detection across video, audio, and images; threat intelligence; dark web visibility for deepfake-for-hire services	Enterprise SOC teams, fraud analysts, brand protection
Sensity AI	Multilayer forensic analysis: visual artefacts, acoustic patterns, metadata; court-ready forensic reports; API access; 95–98% cited accuracy	Law enforcement, legal teams, journalists needing court-admissible documentation

Reality Defender	Patented multi-model approach analysing video, image, audio, and text simultaneously; forensic analysis for biometric anomalies	Enterprise trust-and-safety; comprehensive media type coverage
Intel FakeCatcher	Analyses blood-flow patterns (photoplethysmography / rPPG signals) — real faces show physiological responses; ~96% accuracy (Demir & Tarhan, 2022)	High-accuracy liveness verification; newsroom pre-publication screening
Pindrop Pulse	Real-time multi-signal detection during live video calls: voice analysis, video frame analysis, and location intelligence simultaneously	Enterprises using video conferencing for high-stakes interactions
HyperVerge	AI models detecting synthetic faces and manipulated video in KYC and remote onboarding workflows	KYC/AML compliance, identity verification, financial services
Deepware Scanner	Accessible deepfake video scanning; URL and file upload; visual deepfake detection	Individual researchers and journalists needing accessible scanning
InVID Deepfake Tab	CNN ensemble (Xception, EfficientNet-B4, Capsule-Forensics++); 0–1 probability score; per-frame thumbnails; integrated into browser plugin	OSINT investigators, journalists, fact-checkers — most accessible entry point

11.3 Key Detection Techniques

11.3.1 Visual Artefact Analysis

Examining video frames for signs of manipulation: facial boundary artefacts, eye and blinking anomalies, lighting inconsistency, temporal flickering, and characteristic GAN compression artefact patterns (Rossler et al., 2019).

11.3.2 Photoplethysmography (rPPG) Liveness Analysis

Intel's FakeCatcher analyses subtle blood-flow patterns in the face. Real human faces contain physiological signals invisible to the naked eye: subtle colour changes driven by blood flow. GAN-generated faces lack these signals because they are constructed mathematically, not captured from a living person (Demir & Tarhan, 2022).

11.3.3 Audio-Visual Synchronisation Analysis

Measuring cross-correlation between phoneme boundaries in the audio track and corresponding oral aperture measurements in video frames. Genuine speech shows consistent temporal alignment; synthetic audio-visual pairs often show systematic timing offsets (Korshunov & Marcel, 2018).

11.3.4 Acoustic Analysis & Voice Cloning Detection

- MFCC anomalies: Synthesised voices show statistical regularities in MFCC distributions that differ from natural speech (Wang et al., 2018)
- Phase spectrum analysis: Voice cloning tools introduce characteristic artefacts in the phase spectrum detectable even after lossy compression
- Environmental mismatch: A cloned voice applied to an environment whose acoustic characteristics are inconsistent with what the audio implies

11.3.5 Geolocation & Environmental Consistency Analysis

Cross-referencing visual content — architecture, signage, vegetation, shadows, sun position — against known-good geographic data (Dubberley et al., 2020).

- SunCalc: Verifying shadow direction and approximate time of filming from sun position
- Sentinel Hub EO Browser: High-resolution satellite imagery for historical location cross-reference
- Google Maps / Street View: Architecture and landmark matching

> Core Principle — Convergent Evidence: No single detection signal is conclusive. The leading detection platforms and the best OSINT practitioners apply multiple independent lines of evidence. Five tools pointing to the same conclusion are defensible. One tool alone is a hypothesis (Dubberley et al., 2020).

12. Use Case: Verifying a Conflict Zone Video Using the CIRS Protocol

SCENARIO: A 47-second video clip is posted to Telegram and rapidly shared across social platforms, claiming to show an airstrike on a hospital in an active conflict zone. The video carries a caption stating the date, location, and the identity of the attacking force. A human rights organisation contacts an OSINT researcher to verify the clip before submitting it as evidence to an international tribunal. The researcher applies the full CIRS video verification protocol as taught in Module 8 (Dubberley et al., 2020).

#	Action	Tools & Notes
1	**Secure & Hash**	Download the original .mp4 file in a sandboxed research environment. Calculate SHA-256 hash immediately. This fingerprint verifies the file has not been modified at any subsequent stage of analysis.
2	**Metadata Extraction**	Device: Xiaomi Redmi Note 11 (consistent with region). Codec: H.264 at 30fps 1080p. GPS: 34.8021°N 38.9965°E (central Syria). Timestamp: consistent with claimed date. No post-processing software detected. Initial assessment: no red flags.
3	**Timestamp Verification**	Local weather records checked for GPS coordinates on stated date via archived data. Weather reports confirm overcast conditions with intermittent smoke — consistent with visual appearance of footage.
4	**Reverse Video Search**	InVID plugin extracts eight keyframe thumbnails. Reverse search across Google, Yandex, TinEye, DBKF: no prior appearance online before stated upload date. No match in Database of Known Fakes.
5	**Geolocation**	Distinctive water tower matched against satellite imagery at GPS coordinates. Building facade confirmed against Sentinel Hub pre-event archive. Road junction and Arabic signage confirmed against pre-conflict mapping data. Location confirmed.

6	**Frame Forensics (ELA)**	Error Level Analysis applied to twelve keyframes: uniform error levels consistent with a single recording session. No regions showing anomalously different compression histories. No object insertion artefacts or temporal discontinuities.
7	**AI Deepfake Detection**	Video shows no identifiable human faces (exterior scene). Facial deepfake tools not applicable. This limitation is formally noted in the verification report.
8	**Audio Analysis**	Ambient sound: distant explosions, vehicle noise, one partially audible Arabic voice at 0:31. Acoustic environment consistent with open exterior location. No electronic distortion. Audio-to-video sync consistent throughout.
9	**Open-Source Cross-Ref**	A Syrian monitoring network, a Turkey-based news agency, and satellite imagery from a commercial provider document an incident at the same location within a 40-minute window of the stated timestamp.
10	**Document & Report**	SHA-256 chain of custody documented. All tool outputs preserved with timestamps. Verification report prepared with five independent analytical layers and three independent external sources supporting authenticity assessment.

2026 Update: Outcome: The video is assessed as consistent with authentic, unmanipulated footage of the claimed event. The report is submitted to the tribunal's evidence intake process with full methodology documentation and SHA-256 chain of custody records.

13. The CIRS™ Programme — Learning Video Verification Professionally

Why the CIRS™ Certification Is the Ideal Framework: The Certified Internet Research Specialist (CIRS™) programme, offered by AOFIRS, is unique among professional research credentials for the depth and specificity of its technical content. This paper has been drawn directly from Unit 20 (Training Module 8) of the CIRS™ curriculum. The programme addresses how the underlying technology works at a protocol and algorithmic level — because that is the only basis on which a practitioner can reason clearly about what a given result means.

13.1 What the CIRS™ Programme Covers in Video Verification

- Video file anatomy: codecs, containers, frame structures, and compression schemes
- Metadata forensics: EXIF, XMP, DCIM standards; extraction tools; manipulation detection; legal admissibility implications
- Tampering taxonomy: spatial, temporal, and spatio-temporal manipulation — with forensic indicators for each class
- Authentication standards and digital evidence law: chain of custody requirements, admissibility criteria across jurisdictions
- Practical tool training: InVID-WeVerify, Amnesty Data Viewer, ExifTool, YouTube analytics extensions, and geolocation tools
- Deepfake awareness: AI-generated video and audio creation technologies, forensic signatures, and appropriate detection approaches
- Convergent evidence methodology: the discipline of building a verifiable finding from multiple independent analytical sources

13.2 Who the CIRS™ Programme Is Designed For

The programme requires no prior technical background. It is designed for working professionals who encounter online media evidence and need to evaluate it rigorously (AOFIRS, 2020):

- Online investigators and OSINT researchers
- Fraud analysts and compliance officers
- Journalists and fact-checkers
- Human rights defenders and civil society researchers
- Legal practitioners (attorneys, paralegals, judicial support staff)
- Law enforcement and government intelligence analysts
- HR investigators and background screening professionals
- Academic researchers in digital media, political science, and security studies

13.3 The Habit That Makes the Difference

The most important outcome of CIRS™ training is not tool knowledge. It is the habit of systematic analysis: the reflex to run the metadata before trusting the caption, to perform reverse search before citing the footage, to verify the geolocation before accepting the stated location, and to demand convergent evidence before reaching a conclusion.

In 2026, video is no longer self-authenticating. What cannot be easily fabricated is the technical record: the metadata left by the recording device, the server logs, the satellite imagery that predates the event, the forensic signals that authentic video leaves in its compression structure (Tolosana et al., 2020).

> That technical record — read systematically, cross-referenced rigorously, and documented defensibly — is where the truth about a video actually lives. Learning to read it is what the CIRS™ programme is built to teach.

REFERENCES

All references are formatted in APA 7th edition style.

Allen, G. C. (2017). "Rogue One" and the future of digital actors. Center for a New American Security. https://www.cnas.org

Amnesty International. (2015). YouTube data viewer. Citizen Evidence Lab. https://citizenevidence.amnestyusa.org

AOFIRS. (2020). Online videos authentication & evidence management: Training Module 8, Unit 20. Association of Internet Research Specialists.

Chesney, R., & Citron, D. K. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. California Law Review, 107(6), 1753–1820. https://doi.org/10.15779/Z38RV0D15J

Casey, E. (2011). Digital evidence and computer crime: Forensic science, computers and the internet (3rd ed.). Academic Press.

Demir, B., & Tarhan, A. (2022). FakeCatcher: Detection of synthetic portrait videos using biological signals. IEEE Transactions on Pattern Analysis and Machine Intelligence. https://doi.org/10.1109/TPAMI.2022.3147526

Dubberley, S., Griffin, E., & Bal, H. M. (2020). Digital witness: Using open source information for human rights investigation, documentation and accountability. Oxford University Press.

e-Market Reports. (2018). Digital video viewer statistics 2018. eMarketer.

European Parliamentary Research Service. (2025). Deepfakes and artificial intelligence: Regulatory responses (Report No. PE 757.583). European Parliament.

FBI IC3. (2025). 2025 Internet Crime Report. Federal Bureau of Investigation Internet Crime Complaint Center. https://www.ic3.gov

Friedman, M., & Rosenfeld, A. (2008). EXIF metadata standards for digital imaging. Digital Imaging Group.

Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A., & Bengio, Y. (2014). Generative adversarial nets. Advances in Neural Information Processing Systems, 27, 2672–2680.

Harvey, P. (2023). ExifTool documentation (Version 12.65). https://exiftool.org

ICC. (2012). The Prosecutor v. Thomas Lubanga Dyilo (Case No. ICC-01/04-01/06). International Criminal Court.

ICJ. (2010). Case concerning the application of the convention on the prevention and punishment of the crime of genocide (Bosnia and Herzegovina v. Serbia and Montenegro). International Court of Justice.

ICTR. (2006). The Prosecutor v. Edouard Karemera et al. (Case No. ICTR-98-44-T). International Criminal Tribunal for Rwanda.

ICTY. (2004). The Prosecutor v. Slobodan Milosevic (Case No. IT-02-54-T). International Criminal Tribunal for the former Yugoslavia.

ICTY. (2013). The Prosecutor v. Zdravko Tolimir (Case No. IT-05-88/2-T). International Criminal Tribunal for the former Yugoslavia.

Jin, Z., Finkelstein, A., Mysore, G. J., & Lu, J. (2017). VoCo: Text-based insertion and replacement in audio narration. ACM Transactions on Graphics, 36(4), Article 96. https://doi.org/10.1145/3072959.3073702

Korshunov, P., & Marcel, S. (2018). DeepFakes: A new threat to face recognition? Assessment and detection. arXiv preprint arXiv:1812.08685.

Liu, M.-Y., Breuel, T., & Kautz, J. (2017). Unsupervised image-to-image translation networks. Advances in Neural Information Processing Systems, 30.

Mason, S. (Ed.). (2017). Electronic evidence (4th ed.). University of London Press.

OPCW. (2013). Report of the OPCW fact-finding mission in Syria regarding alleged use of chemical weapons in the Ghouta area of Damascus on 21 August 2013. Organisation for the Prohibition of Chemical Weapons.

OpenAI. (2024). Sora: Creating video from text. https://openai.com/sora

Oord, A. v. d., Dieleman, S., Zen, H., Simonyan, K., Vinyals, O., Graves, A., Kalchbrenner, N., Senior, A., & Kavukcuoglu, K. (2016). WaveNet: A generative model for raw audio. arXiv preprint arXiv:1609.03499.

Papadopoulos, S., Zampoglou, M., Kompatsiaris, I., & Spyrou, E. (2017). InVID: A social multimedia verification tool. Proceedings of the 2017 ACM on Multimedia Conference, 1205–1206. https://doi.org/10.1145/3123266.3127910

Pew Research Center. (2013). Video-sharing websites. Pew Internet & American Life Project. https://www.pewresearch.org

Reuters Institute. (2022). Digital news report 2022. Reuters Institute for the Study of Journalism, University of Oxford.

Rossler, A., Cozzolino, D., Verdoliva, L., Riess, C., Thies, J., & Niessner, M. (2019). FaceForensics++: Learning to detect manipulated facial images. Proceedings of the IEEE/CVF International Conference on Computer Vision, 1–11.

Stamm, M. C., Lin, W. S., & Liu, K. J. R. (2012). Temporal forensics and anti-forensics for motion compensated video. IEEE Transactions on Information Forensics and Security, 7(4), 1315–1329. https://doi.org/10.1109/TIFS.2012.2205568

Suwajanakorn, S., Seitz, S. M., & Kemelmacher-Shlizerman, I. (2017). Synthesizing Obama: Learning lip sync from audio. ACM Transactions on Graphics, 36(4), Article 95. https://doi.org/10.1145/3072959.3073640

Thies, J., Zollhofer, M., Stamminger, M., Theobalt, C., & Niessner, M. (2016). Face2Face: Real-time face capture and reenactment of RGB videos. Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2387–2395.

Tolosana, R., Vera-Rodriguez, R., Fierrez, J., Morales, A., & Ortega-Garcia, J. (2020). Deepfakes and beyond: A survey of face manipulation and fake detection. Information Fusion, 64, 131–148. https://doi.org/10.1016/j.inffus.2020.06.014

UN Human Rights Council. (2012). Report of the independent international commission of inquiry on the Syrian Arab Republic (A/HRC/21/50). United Nations.

UNHCR. (2010). Report of the Secretary-General's Panel of Experts on Accountability in Sri Lanka. United Nations.

VeraAI Consortium. (2026). VeraAI final project report: AI-driven verification for journalism and open source intelligence (Grant No. 101070093). European Commission Horizon Europe.

Vosoughi, S., Roy, D., & Aral, S. (2018). The spread of true and false news online. Science, 359(6380), 1146–1151. https://doi.org/10.1126/science.aap9559

Wang, Y., Skerry-Ryan, R. J., Stanton, D., Wu, Y., Weiss, R. J., Jaitly, N., Yang, Z., Xiao, Y., Chen, Z., Bengio, S., Le, Q., Agiomyrgiannakis, Y., Clark, R., & Saurous, R. A. (2018). Tacotron: Towards end-to-end speech synthesis. arXiv preprint arXiv:1703.10135.

Wardle, C., & Derakhshan, H. (2017). Information disorder: Toward an interdisciplinary framework for research and policy making. Council of Europe.

WebMarketingGroup. (2018). Visual content marketing statistics. https://www.webmarketinggroup.co.uk

Zhu, J.-Y., Park, T., Isola, P., & Efros, A. A. (2017). Unpaired image-to-image translation using cycle-consistent adversarial networks. Proceedings of the IEEE International Conference on Computer Vision, 2223–2232.

INDEX

Key terms, tools, and concepts appearing in this reference paper. Page references are approximate and will update when the Table of Contents field is refreshed in Microsoft Word.

A

Acoustic analysis Sections 7.5, 11.3.4
Adobe VoCo Section 7.5, Figures 16–18
Admissibility (evidence) Section 3.1
AI-generated content Sections 1, 11
Amnesty Data Viewer Section 9.2, Figure 30
AOFIRS Cover, Sections 1, 13
Authenticity (evidence) Section 3.1.2
AVCHD format Section 5, Figure 11d
AVI format Section 5, Figure 11a

B

Best evidence standard Section 3.1.4
Block-level tampering Section 4.1
Body-worn cameras Section 2.5

C

Casey, E. References
Chain of custody Section 3.2
Chesney & Citron References
Citizen journalism Sections 1.1, 2.5
CIRS™ programme Section 13
CloudSEK Section 11.2
Codec Section 5
Compression artefacts Sections 4.1, 11.3.1
Container formats Section 5
Convergent evidence Sections 11.3.5, 12
CycleGAN Section 7.6, Figures 19–20

D

DCIM folder structure Section 6.1
Deepfake detection Section 11.2
Deepfakes Sections 7, 11
Deepware Scanner Section 11.2
Digital evidence law Section 3
DKIM N/A (Email paper)

E

ELA (Error Level Analysis) Sections 10.1.3, 12
EXIF metadata Section 6
ExifTool Sections 6, 6.1

F

Face2Face technique Section 7.3, Figure 14
FakeCatcher (Intel) Section 11.2
Fact Checker extension Section 8.3.4, Figures 27–28
FBI IC3 Report 2025 Sections 7.7, 11, References
FLV format Section 5, Figure 11e
Forensic filters Section 10.1.3
Frame by Frame extension Section 8.3.3, Figure 26
Frame manipulation Section 4.3

G

GAN (Generative Adversarial Networks) Sections 7.1, 11.1
Geolocation analysis Sections 9, 11.3.5
GPS metadata Section 6.1

H

Harvey, P. (ExifTool) References
Hearsay Section 3.1.3
Human rights evidence Sections 2.5, 2.6
HyperVerge Section 11.2

I

ICC (International Criminal Court) Section 2.6
InVID-WeVerify-VeraAI Sections 10, 10.2, Figures 32–41
Intel FakeCatcher Section 11.2
IP reputation N/A (Email paper)

K

Keyframe extraction Sections 9.3, 10.1.1
KYC compliance Section 11.2

L

Legal admissibility Section 3
Lip synchronisation AI Section 7.2, Figure 13
Lyrebird voice cloning Section 7.7, Figure 21

M

Mason, S. References

MFCC anomalies Section 11.3.4
Metadata Section 6
MOV format Section 5, Figure 11c
MP4 format Sections 5, 6.1

N

NVIDIA GAN Section 7.1, Figure 12
News media authentication Section 2.1

O

Object copy-move Section 4.2.2, Figure 4
Object modification Section 4.2.3, Figures 6–7
Object removal Section 4.2.1, Figure 3
OSINT Sections 10, 11, 12

P

Papadopoulos et al. References
Photoplethysmography (rPPG) Section 11.3.2
Pindrop Pulse Section 11.2
Pixel-level tampering Section 4.2.4, Figure 8
Political video evidence Section 2.4
Probative value Section 3.1.5

R

Reality Defender Section 11.2
Relevance (evidence) Section 3.1.1
Reliability (evidence) Section 3.1.2
Reverse video search Sections 9.3, 10.1.1
Rossler et al. References
rPPG signals Section 11.3.2

S

Sensity AI Section 11.2
SHA-256 hashing Sections 3.2, 12
Social media verification Section 8
Spatio-temporal tampering Section 4.4, Figure 10
Spatial tampering Section 4.1, Figure 2
Stamm et al. References
SunCalc Section 11.3.5
Suwajanakorn et al. References

T

Temporal tampering Section 4.3, Figure 9
Thies et al. References

THM files Section 6.1
Tolosana et al. References
Training Module 8 (CIRS) Cover, Section 13

U

User-generated content Sections 1.1, 2.5

V

VeraAI Consortium Section 10.2, References
Video codecs Section 5
Video containers Section 5
Video formats Section 5, Figures 11a–11e
vidIQ Section 8.3.2, Figure 25
vidlog (Vidooly) Section 8.3.1, Figure 24
VoCo (Adobe) Section 7.5, Figures 16–18
Voice cloning Sections 7.7, 11.1, 11.3.4
Vosoughi et al. References

W

Wang et al. References
Wardle & Derakhshan References
WACZ archiving Section 10.2

Y

YouTube Data Viewer (Amnesty) Section 9.2, Figure 30
YouTube verification Sections 8.2, 8.3, 9

Z

Zhu et al. (CycleGAN) References