COMPUTER FORENSICS LAB

London digital forensics & e-discovery · Established 2007

Deepfakes and Synthetic Media

Fake Video, Cloned Voices and the Liar's Dividend: Authenticating the Real

Synthetic media, video, audio and images generated or manipulated by AI, has moved from novelty to courtroom problem. A cloned voice can put words a person never said into a phone call; a face-swapped video can place someone at an event they never attended; a wholly generated image can look like a genuine photograph. Two dangers follow. The obvious one is the fake presented as real: fabricated audio-visual evidence introduced to deceive. The subtler and, in practice, more common one is the liar's dividend: genuine, authentic recordings dismissed as deepfakes by the party they incriminate, so that the mere existence of the technology is used to cast doubt on real evidence. Neither problem is solved by an intuitive glance or a single detector. It is met, as with documents, by provenance and by rigorous media forensics: where did this file come from, does its history support its account, and does technical analysis of the media itself reveal generation or manipulation? This guide sets out for UK lawyers how synthetic media arises, how genuine and fake are told apart, and how the real is authenticated against a challenge as firmly as the fake is exposed.

⏱ Estimated reading time: 25 min read

§ ABOUT THE AUTHOR

PREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAM

Computer Forensics Lab is a London-based digital forensics and electronic disclosure practice established in 2007. Its image and audio-visual authentication work now spans the synthetic-media problem from both sides: testing suspected deepfake video, audio and images for signs of generation and manipulation, and, just as often, authenticating genuine recordings challenged as fakes. The approach pairs media forensics with provenance and is reported under CPR Part 35 and CrimPR Part 19, with conclusions stated at honest confidence rather than as false certainty in either direction.

ESTABLISHED 2007 · LONDON | ISO 17025-ALIGNED PROCEDURES | DEEPFAKE & MEDIA ANALYSIS | AUDIO & VIDEO AUTHENTICATION | CPR PART 35 EXPERT REPORTS | FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

In this guide

©2026 Computer Forensics Lab Ltd ·cflab.uk ·e-discovery.uk ·info@cflab.uk ·+44 (0)20 7164 6915

§ 0 1 · ORIENTATION

Executive summary

The headline point: AI can now fake video, voice and images convincingly, creating two dangers, the fake presented as real and the real dismissed as fake, and both are met not by a glance or a single detector but by media forensics and provenance, with conclusions stated at honest confidence in either direction.

How it is made (§3): face-swaps and generated video, cloned voices in audio, and wholly synthetic images, used to fabricate events, statements and depictions. **Detecting the fake (§4):** technical analysis of the media, compression and encoding artefacts, physiological and physical inconsistencies, generation signatures, and audio spectral analysis, indicative but not infallible, so used as evidence, not oracle. **Provenance (§5):** as with documents, where the file came from, its capture device and metadata, and its existence and history across the estate, often decides authenticity more reliably than analysis of the pixels alone. **The liar's dividend (§6):** the growing tactic of branding genuine recordings deepfakes, met by positively authenticating the real through provenance and capture evidence, and by honest confidence rather than false certainty. **Deployment (§7):** exposing fabricated media, resisting the reflexive deepfake denial of genuine evidence, and the practical question of who must prove what.

- **Seeing is no longer believing:** video, voice and images can be convincingly faked by AI.
- **Two dangers, not one:** the fake presented as real, and the real dismissed as fake (the liar's dividend).
- **Detectors are indicative:** media analysis helps but is not infallible and is used as evidence, not proof.
- **Provenance often decides it:** capture device, metadata and history across the estate authenticate or expose.
- **Authenticate the genuine:** real recordings are positively proved, not merely asserted, against a deepfake challenge.

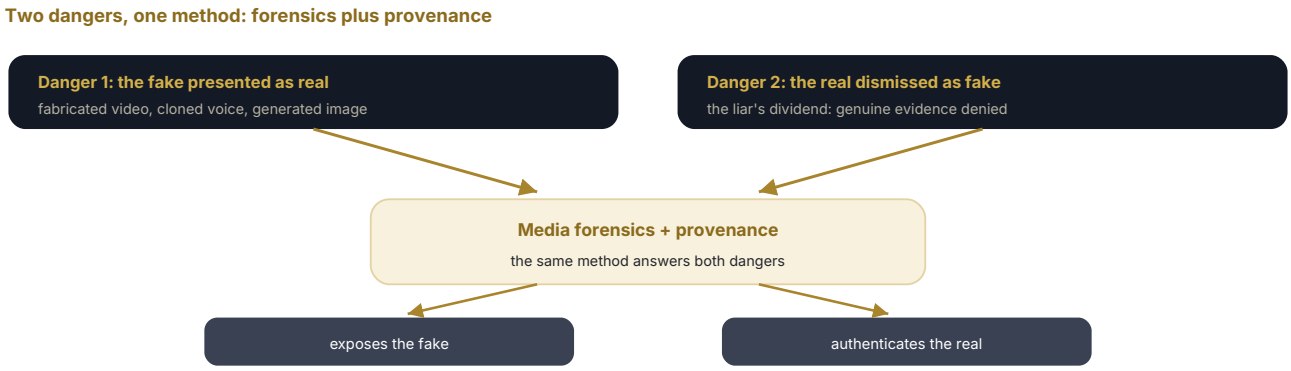

Figure 1 - the same pairing of media forensics and provenance answers both dangers: it exposes fabricated media and authenticates genuine media challenged as fake.

§ 0 2 · FIRST PRINCIPLES

The problem in plain English: seeing is no longer believing

For as long as there have been photographs and recordings, courts have leaned on them as a kind of objective witness: a video showed what happened, a recording captured what was said. Synthetic media undermines that trust. AI tools can now swap one face for another in a video, clone a person's voice so convincingly that a fabricated phone call sounds exactly like them, and generate a photograph of an event that never took place, at a quality that defeats the naked eye. The comfortable assumption that a recording is self-authenticating no longer holds, and the courtroom has to adjust to a world where audio-visual evidence, like documentary evidence before it, must be proved rather than assumed.

This creates a symmetrical pair of problems. The first is the obvious fraud: a fabricated video or recording introduced as if it were genuine, to prove an event or a statement that never occurred. The second, and in day-to-day litigation the more corrosive, is the liar's dividend: a party faced with a genuine, incriminating recording simply asserts that it is a deepfake, exploiting the general awareness that such things are now possible to cast doubt on real evidence they cannot otherwise answer. Both problems resist intuition, a convincing fake looks convincing, and a genuine recording cannot prove its own honesty by being watched, and both resist any single automated detector, because detection tools are indicative, fallible and quickly outdated. The reliable response mirrors the response to fabricated documents: pair technical media forensics, which looks for the fingerprints of generation and manipulation in the media itself, with provenance, which asks where the file came from, on what device it was captured, and whether its history and the surrounding evidence support its account. Together these expose the fake and, just as importantly, authenticate the real. This guide sets out how.

©2026 Computer Forensics Lab Ltd ·cflab.uk ·e-discovery.uk ·info@cflab.uk ·+44 (0)20 7164 6915

§ 0 3 · HOW IT IS MADE AND MISUSED

How synthetic media is made and misused

- **Face-swap and reenactment video:** one person's face or expressions mapped onto another's in video, placing someone at an event or making them appear to act or speak as they did not: the fabricated video the analysis must test (§4).
- **Fully generated video and images:** video and photographs generated from scratch by AI, depicting people, places or events that never existed, at increasing realism: the wholly synthetic depiction.
- **Voice cloning:** a person's voice modelled from samples and used to generate speech they never uttered, fabricating phone calls, voice notes and recorded admissions: the audio deepfake, tested by spectral and acoustic analysis (§4).
- **Manipulated genuine media:** real recordings altered, edited, spliced, partially replaced, rather than wholly generated, a spectrum from light editing to substantial fabrication that blurs the genuine and the fake (guide 121's audio-video discipline).
- **The two misuses:** synthetic media deployed to fabricate evidence, and the anticipation of it deployed to deny genuine evidence (the liar's dividend), so the technology harms both by what it fakes and by the doubt it lends to the real (§6).

©2026 Computer Forensics Lab Ltd ·cflab.uk ·e-discovery.uk ·info@cflab.uk ·+44 (0)20 7164 6915

§ 0 4 · DETECTING IN THE MEDIA

Detecting generation and manipulation in the media

- **Compression and encoding artefacts:** generation and re-encoding leave traces in the compression structure, quantisation and encoding history that can indicate manipulation or synthesis (guide 121's codec discipline): a technical signature, read carefully.
- **Physiological and physical inconsistencies:** unnatural blinking, lighting and shadow that do not match, reflections and geometry that are subtly wrong, edges and blending artefacts around a swapped face: the tells that generation, though improving, still leaves.
- **Audio spectral analysis:** cloned and synthesised speech analysed for spectral, prosodic and background-noise inconsistencies, splice points and the absence of natural recording artefacts (guide 121 §4.5's spectrogram discipline): the audio equivalent of the visual tells.
- **Generation signatures and models:** some synthetic media carries statistical signatures of the generation process, and detection models can indicate synthesis, but both are fallible, defeated by post-processing and outpaced by new generators: used as indicative evidence, never as an infallible oracle (guide 100).
- **Honest confidence:** media-forensic findings expressed as levels of support for manipulation or synthesis, with their uncertainty stated, not as binary certainty, because the technology moves and detection is imperfect (§6): the survivable conclusion.

©2026 Computer Forensics Lab Ltd ·cflab.uk ·e-discovery.uk ·info@cflab.uk ·+44 (0)20 7164 6915

§ 0 5 · PROVENANCE AND THE GENUINE

Provenance and authenticating the genuine

- **Provenance often decides it:** as with documents (guide 126), where a file came from frequently answers authenticity more reliably than pixel analysis: the capture device, the original file and its metadata, and its history across the estate (§8): the objective record around the media.
- **The capture device and original:** the genuine recording traced to the device that captured it, with the native original (not a re-shared, re-encoded copy) and its EXIF or container metadata, capture timestamps and device signatures examined (guides 4, 108): the recording tied to a real camera and moment.
- **Existence and corroboration:** a genuine recording corroborated by where it exists and what surrounds it, the device that made it, the account it uploaded to, the people who received it at the time, and independent evidence of the event, while a fabrication typically lacks this web of corroboration (§8): authenticity built from context.
- **Authenticating against a challenge:** the crucial defensive use, positively proving a genuine recording authentic through its capture provenance and corroboration so that a bare deepfake assertion cannot displace it (§6): the real evidence defended, not merely maintained.
- **Chain of custody from capture:** the recording's continuity from the capturing device to the court preserved and documented (guides 2, 3), because provenance and integrity together are what let a court rely on media in a world where it can be faked.

©2026 Computer Forensics Lab Ltd ·cflab.uk ·e-discovery.uk ·info@cflab.uk ·+44 (0)20 7164 6915

§ 0 6 · THE LIAR'S DIVIDEND AND HONEST LIMITS

The liar's dividend and honest limits

- **The liar's dividend defined:** the tactic of dismissing genuine, incriminating media as a deepfake, exploiting general awareness of the technology to manufacture doubt: countered by positively authenticating the real, not by merely denying the denial (§5).
- **Authentication beats assertion:** a bare "it's a deepfake" carries no weight against a recording positively authenticated by capture device, native metadata and corroboration, so the answer to the dividend is affirmative provenance evidence (§5): proof against assertion.
- **Detection is indicative, not infallible:** the honest limit on the offensive side, that media forensics indicates manipulation or synthesis with a level of confidence and can be wrong, so it is corroborated with provenance and stated at honest confidence (§4).
- **Absence of tells is not proof of authenticity:** a clean forensic result does not prove a recording genuine, and the presence of some artefacts does not prove it fake, since ordinary editing and re-compression also leave marks: the two-sided caution (guide 100).
- **Who must prove what:** the practical and legal question of the burden, whether the party relying on media must authenticate it or the challenger must substantiate a deepfake allegation, addressed with evidence rather than rhetoric on either side (§7).

©2026 Computer Forensics Lab Ltd ·cflab.uk ·e-discovery.uk ·info@cflab.uk ·+44 (0)20 7164 6915

§ 0 7 · DEPLOYMENT

Deployment: fabrication, denial and the burden of proof

- **Exposing fabricated media:** a deepfake put to the court as fabricated, on the combined strength of media-forensic tells and the absence of genuine provenance, its lack of a capture device, native original and corroboration (§4, §5, guide 98).
- **Resisting the deepfake denial:** a genuine recording defended against a liar's-dividend challenge by affirmative authentication, so the tribunal is given proof of provenance rather than left with unresolved doubt (§6): the real evidence held.
- **Framing the burden:** the party relying on a recording prepared to authenticate it, and a party alleging a deepfake pressed to substantiate the allegation with more than assertion, so the issue is decided on evidence (§6).
- **Early expert involvement:** media authenticity raised and addressed early, because native originals, capture devices and metadata must be preserved before re-sharing and re-encoding strip them (§5, guide 121's preservation urgency).
- **Sensitive contexts:** synthetic media's acute harms, non-consensual intimate imagery, fabricated statements, impersonation, handled with the appropriate legal framework and care, and with the person depicted protected (guide 20 and the relevant offences and civil remedies).

©2026 Computer Forensics Lab Ltd ·cflab.uk ·e-discovery.uk ·info@cflab.uk ·+44 (0)20 7164 6915

§ 0 8 · THE WIDER MAP

Source architecture: where else the evidence lives

Per this series' source-architecture discipline: a piece of media is never only the file in issue, and its authenticity is decided largely by the sources around it. The file holds its own encoding and metadata. But a genuine recording has a capture device that made it and still bears its traces; a native original exists before any re-sharing flattened it; the account it was uploaded to and the platform hold copies with server-side records; the people who received it at the time hold independent copies with their own timestamps; and the event itself is corroborated by other recordings, CCTV (guide 121), location (guide 124) and witnesses. The discipline is to test the media against this web, because a fabrication typically lacks a capture device, a native original and a corroborating web, while a genuine recording is embedded in all of them. When a suspected deepfake exists only as a shared file with no capture device or native original, that absence, with the forensic tells, exposes it; and when a genuine recording is challenged, its capture device, native original, contemporaneous copies and event corroboration authenticate it against the bare denial.

CORROBORATING SOURCE	THE MEDIA FILE	CAPTURE DEVICE	NATIVE ORIGINAL	PLATFORM / ACCOUNT	CONTEMPORANEOUS RECIPIENTS	EVENT CORROBORATION
Video	Encoding, metadata	Y: camera / phone	Y: pre-share original	Y: upload records	Y: who received it	CCTV, witnesses
Audio	Spectral profile	Y: recording device	Y: original file	Voice-note account	Y: call/message logs	Other-side records
Image	EXIF, artefacts	Y: camera	Y: original capture	Cloud photo library	Shared copies	Location, other photos
Capture time / place	Claimed metadata	Y: device clock/ GPS	Original timestamps	Upload timestamps	Received time	Location, CCTV
Continuity	Hash of the file	Device custody	Original custody	Platform logs	n/a	n/a

Fallback strategy in one line: test the media against its capture device, native original and corroborating web; a fake usually lacks all three, and a genuine recording embedded in them is authenticated against a bare deepfake denial.

©2026 Computer Forensics Lab Ltd ·cflab.uk ·e-discovery.uk ·info@cflab.uk ·+44 (0)20 7164 6915

§ 0 9 · IN THE WILD

Worked examples

EXAMPLE 1 · THE CLONED-VOICE CALL THAT HAD NO ORIGIN

A party produced a recording of a phone call in which the other side's director appeared to make a damaging admission, in his own voice. The §4 audio analysis found spectral and prosodic inconsistencies and splice-like transitions consistent with synthesised speech, indicative but, alone, not conclusive. The §5 provenance analysis made it conclusive: the recording existed only as a file the producing party supplied, with no corresponding entry in any call log, no capture on any device, no native original and no contemporaneous copy anywhere, the §8 absence a genuine recorded call could not show. The combination, forensic tells plus a total lack of genuine provenance, exposed the recording as a voice-cloned fabrication. Neither element alone would have sufficed; together they were decisive. The lesson is §5's: a deepfake is exposed most reliably by pairing media forensics with provenance, and a fabricated recording that exists nowhere a genuine one would, and bears the tells of synthesis, cannot stand.

EXAMPLE 2 · THE LIAR'S DIVIDEND REFUSED

A genuine video, capturing a party clearly doing what he later denied, was met with the now-common response: he asserted it was a deepfake. There were no forensic tells of manipulation, but, as §6 notes, absence of tells does not by itself prove authenticity, so the answer was affirmative authentication. The §5 provenance evidence was decisive: the video was traced to the specific phone that captured it, the native original was recovered with intact metadata and matching capture timestamp and location (guide 124), it had been sent to two other people that same evening who still held their copies, and the event was corroborated by independent CCTV (guide 121). Against that web of §8 corroboration, the bare deepfake assertion carried no weight. The lesson is §6's: the liar's dividend is defeated not by denying the denial but by positively authenticating the real, and a genuine recording embedded in its capture device, native original, contemporaneous copies and event corroboration cannot be waved away by the mere possibility of fakery.

EXAMPLE 3 · THE HONEST, BOUNDED FINDING

A short video was challenged as a face-swap deepfake. The §4 analysis found some artefacts around the subject's face, but, applying §6's caution, the examiner recognised that heavy compression and re-sharing, through several messaging platforms, also produce such artefacts, so the tells were not, by themselves, proof of synthesis. The §5 provenance was partial: a native original could not be located, only re-shared copies. The honest conclusion, stated at §6 confidence, was that the analysis raised a real question about the video's authenticity but could not, on the available material, conclude it was a deepfake, and that locating the capture device and native original was necessary to resolve it. That measured finding, neither overclaiming a fake nor pronouncing it genuine, was more useful and more credible than false certainty either way. The lesson is §6's: media forensics is indicative, not infallible, and the honest expert states the level of support and what is needed to resolve it, rather than forcing a binary answer the evidence does not support.

©2026 Computer Forensics Lab Ltd ·cflab.uk ·e-discovery.uk ·info@cflab.uk ·+44 (0)20 7164 6915

§ 10 · WHERE IT GOES WRONG

Common mistakes and technical limitations

Common mistakes

- **Trusting a single detector:** a deepfake-detection tool's verdict relied on as conclusive, when detection is indicative and fallible (§4, Example 3).
- **Ignoring provenance:** the media analysed in isolation, without asking where it came from and whether it exists where a genuine one would (Example 1, §5).
- **Working from a re-shared copy:** the native original never sought, so capture metadata and clean artefacts are lost to re-encoding (Example 3, §5).
- **Reading compression artefacts as fakery:** ordinary re-compression tells mistaken for signs of synthesis (Example 3, §6).
- **Accepting a bare deepfake denial:** a genuine recording abandoned because it was called a fake, without affirmative authentication (Example 2, §6).
- **Overclaiming certainty:** a binary "fake" or "genuine" asserted where the evidence supports only a level of confidence (§6).
- **Delaying preservation:** capture devices and native originals lost to re-sharing before they are secured (§5, §7).
- **Treating a clean result as proof of authenticity:** absence of tells taken as positive proof the media is genuine (§6).

Technical limitations

- **Detection is imperfect and moving:** tells are indicative, defeated by post-processing, and outpaced by new generators: the central limit (§4).
- **Compression mimics manipulation:** re-encoding and re-sharing produce artefacts that resemble tampering: a source of false positives (§6).
- **Absence of the original weakens analysis:** without the native capture, metadata and clean artefacts are unavailable (§5).
- **Neither result is conclusive alone:** clean does not prove genuine, and artefacts do not prove fake, without provenance (§6).
- **The field evolves quickly:** methods and generators change, so conclusions are dated and confined to current capability (§4).

©2026 Computer Forensics Lab Ltd ·cflab.uk ·e-discovery.uk ·info@cflab.uk ·+44 (0)20 7164 6915

§ 11 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- For any key recording, do we have the native original and can we identify the device that captured it, so provenance can be established?
- Where else should a genuine version exist, recipients at the time, the upload account, other recordings of the event, so it can be corroborated?
- If our genuine recording is likely to be called a deepfake, what capture and corroboration evidence can we assemble now to authenticate it?

Ask your opponent

- Please produce the native original of [recording], identify the device that captured it, and confirm every account and person that held a copy at the time.
- Please provide the capture metadata, timestamps and any device or platform records for [recording].
- If it is alleged that [genuine recording] is a deepfake, please state the basis for that allegation and produce any technical evidence relied on.

Ask your eDiscovery / forensic provider

- Does media analysis indicate manipulation or synthesis, and at what honest confidence, allowing for compression artefacts?
- Does provenance, capture device, native original, corroboration, support or undermine authenticity?
- What is needed to resolve the question, and what can and cannot be concluded on the current material?

SUGGESTED WORDING · INSTRUCTION FOR A SYNTHETIC-MEDIA EXAMINATION

> "We instruct you to examine the authenticity of the media at Schedule 1, which is [alleged to be a deepfake / relied on and likely to be challenged as a deepfake]. Please: (1) obtain and examine the native original, not a re-shared or re-encoded copy, preserving integrity, and identify the device that captured any genuine recording; (2) conduct media-forensic analysis for signs of generation or manipulation (compression and encoding artefacts, physiological and physical inconsistencies, and, for audio, spectral and acoustic analysis), distinguishing genuine manipulation tells from artefacts produced by ordinary compression and re-sharing; (3) analyse provenance, capture device and metadata, capture time and place, and the media's existence and corroboration across the estate (native original, upload account, contemporaneous recipients, independent event evidence); (4) where the media is challenged as a deepfake and is in fact genuine, assemble the affirmative authentication needed to meet that challenge; and (5) state conclusions at honest confidence, distinguishing indication from proof, noting that a clean result does not prove authenticity and artefacts do not prove fabrication, and identifying what further material would resolve any open question."

©2026 Computer Forensics Lab Ltd ·cflab.uk ·e-discovery.uk ·info@cflab.uk ·+44 (0)20 7164 6915

§ 12 · QUICK CONTROL

Checklist and red flags · When to involve a digital forensic expert

The synthetic-media checklist

- ☐ Native original obtained, not a re-shared or re-encoded copy
- ☐ Capture device identified for any genuine recording
- ☐ Media-forensic analysis for generation and manipulation tells
- ☐ Compression and re-sharing artefacts distinguished from tampering
- ☐ Capture metadata, time and place examined
- ☐ Existence and corroboration tested across the estate
- ☐ Genuine recordings positively authenticated against challenge
- ☐ Detection treated as indicative, not conclusive
- ☐ Conclusions stated at honest confidence, not binary certainty
- ☐ Capture devices and originals preserved before re-sharing strips them

Red flags

- A decisive recording existing only as a shared file, no capture device or original: Example 1.
- A genuine recording waved away as a deepfake with no substantiation: Example 2.
- A deepfake case resting solely on one detector's verdict.
- Only re-shared copies available, no native original: Example 3.
- Compression artefacts asserted as proof of fakery.
- A clean forensic result claimed as proof of authenticity.
- Binary certainty asserted where confidence is all the evidence supports.

When to involve a digital forensic expert

As soon as the authenticity of any audio-visual evidence is genuinely in issue, on either side, because the reliable method pairs specialist media forensics with provenance and both need early action: capture devices and native originals must be preserved before re-sharing strips their metadata (§5, §7); the expert tests the media for generation and manipulation while distinguishing genuine tells from compression artefacts, and pairs that with provenance across the estate, so a fake is exposed by tells plus absent origin (Example 1) and a genuine recording is authenticated against the liar's dividend by capture device, native original and corroboration (Example 2); and every conclusion is stated at honest confidence, indication distinguished from proof, with what would resolve an open question identified (Example 3). Reports run under CPR Part 35 or CrimPR Part 19. Through **cflab.uk** and **e-discovery.uk**, synthetic-media work answers both dangers with one disciplined method: it exposes the fabricated and, just as importantly, authenticates the real, so that neither a convincing fake nor a convenient denial is allowed to decide a case that the evidence, properly examined, can.

©2026 Computer Forensics Lab Ltd ·cflab.uk ·e-discovery.uk ·info@cflab.uk ·+44 (0)20 7164 6915

§ 13 · COMMON QUESTIONS

Frequently asked questions

Can you just run a deepfake detector and get an answer?

No, not a reliable one on its own (§4, Example 3). Detection tools are indicative, produce errors, are defeated by post-processing and are outpaced by new generators, so a detector's verdict is evidence, not proof. The reliable approach pairs media-forensic analysis, read with an understanding that compression itself creates artefacts, with provenance: where the file came from, its capture device and its corroboration (§5). Together those answer the question far more safely than any single tool.

How do you prove a video or recording is fake?

By combining forensic tells with absent provenance (Example 1, §5). Media analysis may indicate synthesis or manipulation, and provenance asks whether the recording has a capture device, a native original and a corroborating web of contemporaneous copies and independent event evidence. A fabrication typically has the tells and lacks the provenance, existing only where the producing party supplied it (§8). That combination, not either element alone, exposes the fake.

The other side says our genuine recording is a deepfake. What do we do?

Authenticate it positively, do not merely deny the denial (§6, Example 2). Trace it to the device that captured it, recover the native original with its metadata and capture time and place, identify the people who held copies at the time, and corroborate the event with independent evidence like CCTV or location. A bare "it's a deepfake" carries no weight against a recording embedded in that web of provenance. The liar's dividend is beaten by proof, not by argument.

Does a clean forensic result mean the recording is genuine?

Not by itself (§6). Absence of manipulation tells does not prove authenticity, just as the presence of some artefacts does not prove fakery, since ordinary compression and re-sharing also leave marks. A clean result is one input; authenticity is established positively through provenance and corroboration. The honest conclusion combines both and is stated at a level of confidence, rather than treating a clean scan as a certificate of genuineness.

Why does it matter whether we have the original file?

Because provenance and clean analysis both depend on it (§5, Example 3). Re-sharing through messaging and social platforms re-encodes media, stripping capture metadata and adding compression artefacts that both weaken forensic analysis and can be mistaken for tampering. The native original, from the capturing device, preserves the metadata and the cleanest version of the media, which is why preserving it early, before it is re-shared, is essential.

Who has to prove whether it is real or fake?

That is a legal question addressed with evidence rather than rhetoric (§6, §7). In practice, a party relying on a recording should be ready to authenticate it, and a party alleging a deepfake should be pressed to substantiate the allegation rather than merely assert it. The forensic role is to supply the evidence, of provenance and of media analysis, that lets the tribunal decide the issue on a proper basis instead of on the unaided possibility that fakery exists.

©2026 Computer Forensics Lab Ltd ·cflab.uk ·e-discovery.uk ·info@cflab.uk ·+44 (0)20 7164 6915

§ 14 · REFERENCE

Glossary

Synthetic media
Video, audio or images generated or manipulated by AI.

Deepfake
Media in which a person appears to do or say what they did not.

Face-swap
Mapping one person's face onto another in video.

Voice cloning
Synthesising a person's voice to fabricate speech.

Liar's dividend
Dismissing genuine media as fake by invoking deepfakes.

Media forensics
Technical analysis of media for signs of manipulation.

Compression artefact
A mark left by encoding, easily mistaken for tampering.

Native original
The file as captured, before re-sharing re-encoded it.

Provenance
Where the media came from, its device and history.

Honest confidence
A stated level of support, not binary certainty.

Sources and authoritative references

The synthetic-media disciplines in this guide draw on materials published by our laboratory and e-discovery practice, referenced here as sources:

- cflab.uk, digital forensics services (deepfake and synthetic-media analysis, audio and video authentication, CPR Part 35 and CrimPR Part 19 reporting): cflab.uk/digital-forensics-services · guides library: cflab.uk/guides
- e-discovery.uk, EDRM Phase 06 · Analysis (media authentication and provenance as practised): e-discovery.uk/edrm/analysis · practice method: e-discovery.uk
- e-discovery.uk, Knowledge Centre: e-discovery.uk/knowledge
- Forensic Science Regulator, Code of Practice v2 (image and audio-visual analysis and its limits): gov.uk, FSR Code · Courts and Tribunals Judiciary, AI guidance (including synthetic evidence): judiciary.uk, AI guidance
- NIST, media forensics and authenticity research resources: nist.gov · ICO, UK GDPR guidance (image and biometric data): ico.org.uk
- CPR Part 35: justice.gov.uk, Part 35 · PD 57AD: justice.gov.uk, PD 57AD · CPR Part 31: justice.gov.uk, Part 31

DISCLAIMER

This publication provides general information about deepfakes and synthetic media as at August 2026. Generation and detection technology change rapidly; media-forensic detection is indicative rather than infallible, and conclusions about authenticity should combine media analysis with provenance and be stated at honest confidence. The worked examples are fictional. This guide is not legal advice, does not create a professional relationship, and should not be relied upon in place of advice on the facts of a specific matter from a qualified lawyer or a suitably qualified forensic practitioner. Links were live at the date of publication.

§ HOW A SPECIALIST LABORATORY CAN ASSIST

Working with Computer Forensics Lab

The laboratory approaches synthetic media as a two-sided problem answered by one method. Media-forensic analysis tests a recording for the tells of generation and manipulation, compression and encoding artefacts, physiological and physical inconsistencies, and, for audio, spectral and acoustic analysis, while carefully distinguishing genuine tells from the artefacts that ordinary compression and re-sharing produce (§4). That analysis is paired with provenance, because where a file came from often decides authenticity more reliably than the pixels: the capture device, the native original and its metadata, and the recording's existence and corroboration across the estate (§5, §8). On the offensive side, a fabrication is exposed by forensic tells together with the absence of any genuine origin (Example 1); on the defensive side, and increasingly often, a genuine recording is authenticated against the liar's dividend by proving its capture device, native original, contemporaneous copies and independent event corroboration, so a bare deepfake denial cannot displace it (Example 2). Every conclusion is stated at honest confidence, indication distinguished from proof, with what would resolve an open question identified (Example 3). Reports run under CPR Part 35 or CrimPR Part 19. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine; and because originals and capture devices degrade with every re-share, the first step is always to preserve them.

INSTRUCT THE LAB

Speak to a forensic examiner, not a salesperson.

Describe your matter in confidence and an examiner will respond the same working day. Conflicts checks and scoping calls with US counsel are routine.

NEW ENQUIRIES
+44 (0)20 7164 6971

EMAIL
info@cflab.uk

E-DISCOVERY
e-discovery.uk

Computer Forensics Lab Ltd · Euro House, 133 Ballards Lane, Finchley, London N3 1LJ, United Kingdom
cflab.uk · Customer service +44 (0)20 7164 6915 · ICO ZB395023 · NPCC · ISO 17025 aligned practice · UK Gov Digital Marketplace