

Deepfakes And Synthetic Media

AI-generated synthetic media, including deepfakes, challenges traditional notions of authenticity. This guide addresses the creation, detection, and authentication of such media, outlining common pitfalls and the role of digital forensic experts in UK litigation.

e-discovery.uk, Computer Forensics Lab. Published 2026-08-31.
<https://e-discovery.uk/library/deepfakes-and-synthetic-media>

DEEPFAKES & SYNTHETIC MEDIA · A GUIDE FOR UK LAWYERS Deepfakes and Synthetic Media Fake Video, Cloned Voices and the Liar's Dividend: Authenticating the Real COMPUTER FORENSICS LAB

§ ABOUT THE AUTHOR PREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAM
AUDIO & VIDEO AUTHENTICATION CPR PART 35 EXPERT REPORT S FULL
CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS In this guide 01 Executive summary 02 The problem in plain English: seeing is no longer believing 03 How synthetic media is made and misused 04 Detecting generation and manipulation in the media 05 Provenance and authenticating the genuine 06 The liar's dividend and honest limits 07 Deployment: fabrication, denial and the burden of proof 08 Source architecture: where else the evidence lives 09 Worked examples 10 Common mistakes and technical limitations 11 Questions to ask · Suggested wording 12 Checklist and red flags · When to involve a digital forensic expert 13 Frequently asked questions 14 Glossary · References · Disclaimer · How a specialist laboratory can assist

§ 01 · ORIENTATION Executive summary The headline point: AI can now fake video, voice and images convincingly, creating two dangers, the fake media forensics and provenance, with conclusions stated at honest confidence in either direction.

§ 02 · FIRST PRINCIPLES The problem in plain English: seeing is no longer believing

§ 03 · HOW IT IS MADE AND MISUSED How synthetic media is made and misused

§ 04 · DETECTING IN THE MEDIA Detecting generation and manipulation in the media

§ 05 · PROVENANCE AND THE GENUINE Provenance and authenticating the genuine

§ 06 · THE LIAR'S DIVIDEND AND HONEST LIMITS The liar's dividend and honest limits

§ 07 · DEPLOYMENT Deployment: fabrication, denial and the burden of proof

§ 08 · THE WIDER MAP Source architecture: where else the evidence lives CORROBORATING
CAPTURE NATIVE PLATFORM / CONTEMPORANEOUS EVENT SOURCE DEVICE ORIGINAL
ACCOUNT RECIPIENTS CORROBORATION THE MEDIA FILE GPS

§ 09 · IN THE WILD Worked examples EXAMPLE 1 · THE CLONED -
VOICE CALL THAT HAD NO ORIGIN EXAMPLE 2 · THE LIAR'S DIVIDEND REFUSED
EXAMPLE 3 · THE HONEST, BOUNDED FINDING

§ 10 · WHERE IT GOES WRONG Common mistakes and technical limitations Common mistakes
Technical limitations

§ 11 · INTERROGATORIES & DRAFTING AIDS Questions to ask · Suggested wording Ask your client Ask your opponent Ask your e Discovery / forensic provider SUGGESTED WORDING · INSTRUCTIONFORASYNTHETIC - MEDIA EXAM IN AT I ON

§ 12 · QUICK CONTROL Checklist and red flags · When to involve a digital forensic expert The synthetic-media checklist Red flags When to involve a digital forensic expert

§ 13 · COMMON QUESTIONS Frequently asked questions Can you just run a deepfake detector and get an answer? How do you prove a video or recording is fake? The other side says our genuine recording is a deepfake. What do we do? Does a clean forensic result mean the recording is genuine? Why does it matter whether we have the original file? Who has to prove whether it is real or fake?

§ 14 · REFERENCE Glossary Sources and authoritative references DISCLAIMER

§ HOW A SPECIALIST LABORATORY CAN ASSIST Working with Computer Forensics Lab Speak to a forensic examiner, not a salesperson. INSTRUCTTHELAB NEWENQUIRIESEMAILE - DISCOVERY

Questions and answers

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. cflab. u k · e-discove r y. u k ©2026 Computer Forensics Lab Ltd · cflab.uk · e-discovery.uk

Source: <https://e-discovery.uk/library/deepfakes-and-synthetic-media>. Free to read and share with attribution to Computer Forensics Lab, e-discovery.uk.