



C O M P U T E R F O R E N S I C S L A B

London digital forensics & e-discovery · Established 2007

Recovering Deleted CCTV and DVR Footage

The Overwrite Clock, the Proprietary Recorder and the Race to Preserve the Frame

CCTV is the evidence that deletes itself. A digital video recorder holds only so many days of footage, and then it loops: the oldest recording is overwritten by the newest, continuously, automatically, so the frame that proves the case has a limited life measured in days or weeks from the moment it was captured. This makes CCTV unlike almost any other digital evidence: the priority is not analysis but preservation, and the clock is already running before anyone realises the footage matters. Around that overwrite clock sit further difficulties: proprietary recorder formats that ordinary players cannot open, timestamps that are casually wrong, export processes that quietly degrade the image, and the frequent confusion between the footage a system holds and the fragment someone filmed off the monitor with a phone. This guide sets out for UK lawyers how DVR and CCTV systems store and overwrite footage, how it is preserved and recovered forensically before the loop erases it, how deleted and overwritten footage can sometimes still be retrieved, and how to keep the recovered frame authentic and admissible.

🕒 Estimated reading time: 24 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. CCTV and DVR work is recurring laboratory work: urgent preservation before the overwrite loop erases footage, forensic export and recovery of deleted and overwritten recordings from DVR and NVR storage, proprietary-format decoding, and timestamp and authenticity analysis: reported under CPR Part 35 and CrimPR Part 19, with the recovery and any enhancement documented so the frame can be relied upon in court.

ESTABLISHED 2007 · LONDON

ISO 17025-ALIGNED PROCEDURES

CCTV & DVR RECOVERY

PROPRIETARY-FORMAT DECODING

CPR PART 35 EXPERT REPORTS

FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

In this guide

01	Executive summary
02	The problem in plain English: footage that overwrites itself
03	How DVR and CCTV systems store and overwrite footage
04	Preserving before the loop: the urgent first steps
05	Recovering deleted and overwritten footage
06	Formats, timestamps and authenticity
07	Deployment: disclosure, the lost frame and the filmed monitor
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

§ 0 1 · ORIENTATION

Executive summary

The headline point: CCTV overwrites itself on a loop, so the footage that proves the case has a life of days or weeks: preservation is the emergency, it comes before analysis, and the single most important act is to secure the recording, or the whole recorder, before the loop erases it.

How it stores footage (§3): a DVR or NVR records continuously to a fixed-size disk and, when full, overwrites the oldest footage with the newest, so retention is finite and the overwrite clock starts at capture. **Preserving (§4):** the urgent first steps are to identify the retention period, stop the overwrite (by exporting the relevant footage properly or securing the recorder), and preserve the native file with its metadata, not a phone video of the screen. **Recovery (§5):** deleted and even partly overwritten footage can sometimes be carved from the DVR's disk, because deletion and overwrite are not always immediate or complete, but the chance falls with every hour the system keeps recording. **Formats and authenticity (§6):** proprietary DVR formats need the right decoder, timestamps are frequently wrong and must be checked, and the native export with its metadata is the authentic evidence, not a re-recording.

Deployment (§7): disclosure of the footage, the adverse-inference case where a party let relevant footage overwrite after a request, and the weak evidential value of a monitor filmed on a phone.

- **The clock is always running:** footage overwrites on a loop, so retention is days or weeks, not forever.
- **Preservation beats analysis:** secure the native recording or the recorder first; everything else can follow.
- **Native export, not a filmed screen:** the authentic evidence is the recorder's own file with its metadata.
- **Recovery is possible but time-bound:** deleted footage can sometimes be carved, but the chance falls every hour the loop runs.
- **Timestamps lie:** DVR clocks are casually wrong and must be checked and reconciled before the footage is relied on.

The overwrite loop: newest footage erases oldest, continuously

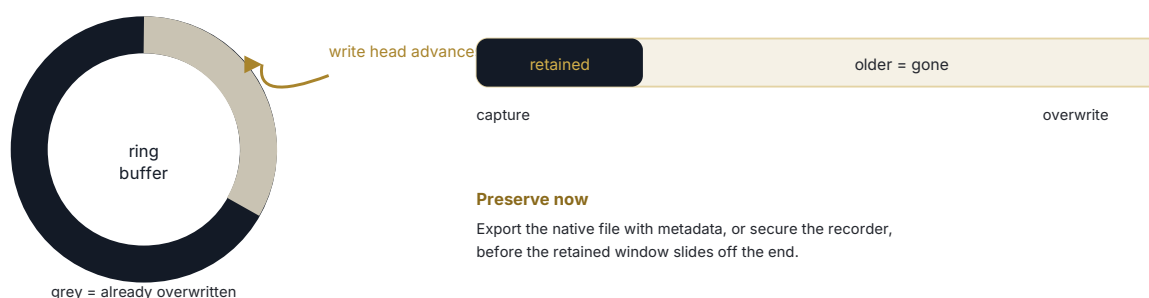


Figure 1 - the DVR records to a ring buffer with a finite retention window; once it fills, every new frame erases an old one, so the footage must be preserved before the window slides past it.

The problem in plain English: footage that overwrites itself

Most digital evidence sits still and waits. A file on a laptop is there next week and next year unless someone deletes it. CCTV is the opposite: it is designed to destroy itself. A digital video recorder has a disk of fixed size and records continuously, and when the disk fills, which it always does, it starts overwriting the oldest footage with the newest, going round and round like a tape that never stops. The retention period, how far back the footage goes, is simply how long it takes to fill the disk: a few days on a busy multi-camera system, a few weeks on a quieter one. The moment relevant footage is captured, a countdown begins, and when the loop comes round again, the frame is gone forever.

This single fact reorders every priority. With ordinary evidence the sequence is preserve, then collect, then analyse, at a measured pace. With CCTV the emergency is preservation, and it is genuinely urgent: by the time a dispute crystallises and lawyers are instructed, the footage may have days left, or may already be gone. The correct first move is not to analyse or even to view at length but to secure the recording, ideally the whole recorder, before the loop erases it. Around this run the secondary traps: the footage comes in proprietary formats an ordinary media player cannot open, the recorder's clock is very often wrong, the export process can silently degrade the image, and people routinely confuse the real evidence, the recorder's own file, with a shaky phone video of the monitor. This guide addresses the emergency first and the traps after.

§ 0 3 · HOW IT STORES FOOTAGE

How DVR and CCTV systems store and overwrite footage

- **Continuous recording to fixed storage:** a DVR (analogue cameras) or NVR (network cameras) writes camera streams continuously to an internal disk, and the disk size and the number and quality of cameras together set the retention period: finite by design, and shorter than most people assume.
- **The overwrite loop:** when the disk fills, the system overwrites the oldest footage first, in a continuous loop, so the retained window constantly slides forward and yesterday's footage has a fixed expiry: the overwrite clock that governs everything (§2).
- **Motion and event recording:** many systems record only on motion or events to save space, extending retention but leaving gaps, and some overwrite by event priority: the retention and the gaps established per system, not assumed uniform.
- **Proprietary storage and formats:** DVRs commonly use proprietary file systems and video formats that ordinary tools cannot read, requiring the manufacturer's player or forensic decoding: the footage locked in a format as much as on a disk (§6).
- **Cloud and hybrid systems:** modern and consumer systems (video doorbells, cloud cameras) store some footage in the cloud on a subscription-limited retention, alongside or instead of local storage: the cloud copy a second source with its own, often shorter, retention clock (§8).

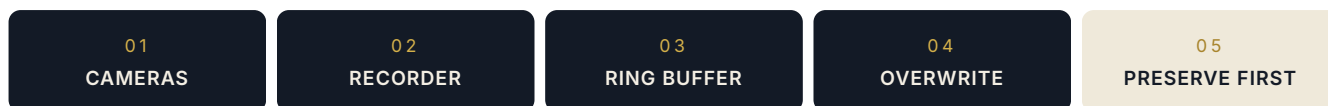


Figure 2 - the CCTV lifecycle ends in overwrite; preservation must interrupt the cycle before the relevant footage reaches the end of the loop.

Preserving before the loop: the urgent first steps

- **Identify the retention now:** the first question is how many days the system holds, so the deadline is known: a system with four days' retention and a three-day-old incident has, at most, one day: the urgency quantified before anything else (§2).
- **Stop the overwrite:** the relevant footage exported properly, or the recording halted, or the whole recorder secured, to stop the loop reaching the relevant frames: the single most important act, taken before analysis and before the window closes.
- **Preserve the native file, with metadata:** the footage exported in the recorder's native format with its metadata (timestamps, camera identifiers) intact, using the correct export function, not re-recorded, not screen-captured: the authentic evidence preserved, not a degraded copy (§6).
- **Secure the recorder where possible:** for anything contentious or where recovery of deleted footage may be needed, the recorder itself preserved and forensically imaged, because export alone captures only what the system chooses to give and not the deleted residue (§5): the disk as well as the clip.
- **Serve preservation on third parties fast:** where the footage is held by someone else, a shop, a neighbour, a local authority, the council or a transport operator, a preservation request served immediately, because their retention clock is running too and their systems loop just the same (guide 95's missing-evidence urgency).

§ 0 5 · RECOVERING DELETED AND OVERWRITTEN FOOTAGE

Recovering deleted and overwritten footage

- **Deleted is not always gone:** footage deleted by a user, or marked for overwrite but not yet overwritten, may still sit on the DVR disk and be recoverable by carving the video data from the raw storage (guide 4's deleted-data principle, for video): the recovery possible while the loop has not yet reached those sectors.
- **Carving proprietary video:** recovering video from unallocated DVR storage requires understanding the proprietary format's frame structure to reassemble coherent footage from fragments: a specialist recovery, not a generic file-carve, and more successful the sooner it is attempted.
- **The overwrite reality:** footage the loop has already overwritten is genuinely gone, replaced by newer recording: the honest limit, and the reason preservation cannot wait, because recovery competes directly with the continuing overwrite.
- **Partial and fragmentary recovery:** where footage is partly overwritten, fragments, individual frames or short sequences may still be recoverable even when continuous playback is not: partial evidence that can still place or time an event, honestly presented as fragmentary.
- **Stop recording to preserve the chance:** the crucial practical point, that a DVR left running keeps overwriting and destroying recoverable residue, so a system from which deleted footage may need recovery is taken out of service and imaged, not left recording (§4): the recovery chance preserved by stopping the loop.

Formats, timestamps and authenticity

- **Proprietary formats:** DVR footage often exports in formats no ordinary player opens, needing the manufacturer's player or forensic decoding into a standard format, done in a way that preserves rather than degrades the image and is documented: the format problem solved without altering the evidence (guide 84's processing discipline, for video).
- **Timestamps are often wrong:** DVR clocks are frequently set incorrectly, never adjusted for daylight saving, or drifted by minutes or hours: the recorder's time checked against a known reference and the offset established, so the footage is placed on the true timeline (guide 108's clock-drift discipline).
- **Export degradation:** re-encoding, transcoding or screen-capturing footage loses quality and metadata: the native export preserved, and any conversion for viewing kept separate from the authentic original (§4).
- **Authenticity and continuity:** the footage's authenticity supported by preserving the native file and its metadata and by a documented chain of custody from recorder to court (guides 2, 3): the frame trusted because its provenance is unbroken.
- **Enhancement, honestly bounded:** lawful enhancement (brightness, contrast, stabilisation, frame interpolation for viewing) distinguished from fabrication, applied transparently and reversibly with the original retained, and its limits stated, enhancement reveals what is present, it does not invent detail that was never captured (guide 100's honest-limits discipline).

Deployment: disclosure, the lost frame and the filmed monitor

- **Disclosure of the footage:** relevant CCTV disclosed as the native export with its metadata, the recorder identified as the source and its retention and clock offset stated, so the footage is placed correctly and its completeness understood (guide 94's known-sources discipline).
- **The footage let overwrite:** where a party held relevant footage and let it overwrite after a preservation request, or failed to preserve it when the duty had arisen, the adverse-inference and spoliation consequences (guides 95 §7, 110 §7): the overwrite dated against the request and its avoidability examined, because CCTV loss is often foreseeable and preventable.
- **The filmed monitor problem:** the common and weak substitute, a phone video of the monitor rather than a native export, degraded, undated, easily challenged: contrasted with the authentic recorder file, and its limitations explained where it is all that survives (§6).
- **The timestamp challenge:** footage whose timing is disputed reconciled through the established clock offset and corroborating sources (other cameras, transaction logs, phone records) so the true time is proven, not assumed from the on-screen stamp (guide 96's timeline discipline).
- **UK GDPR and third-party footage:** CCTV captures identifiable people, so its handling, disclosure and any onward use engage the UK GDPR, and third-party footage is obtained by request or order with data-protection care (guide 20's proportionality, for surveillance data).

Source architecture: where else the evidence lives

Per this series' source-architecture discipline: a CCTV recorder is one node with a short life, and the same event is very often captured by other cameras and recorded elsewhere with different clocks. The recorder holds the primary footage and its deleted residue, briefly. But neighbouring and overlapping cameras, the shop next door, the bus, the doorbell, the traffic camera, hold the same event from another angle on another retention clock; the cloud copy, on consumer and hybrid systems, holds a second copy with its own (often shorter) retention; exported clips already sent to police, insurers or managers survive the recorder's overwrite; and the recorder's own logs record access and export. The discipline is to map every camera that might have seen the event and preserve them all at once, because each has its own clock and its own countdown, and the angle that survives may not be the one first thought of. When the primary recorder has overwritten the frame, a neighbouring camera may still hold it; when the local footage is gone, an exported clip in someone's inbox survives; and where footage was deleted, the recorder's log may still record that it existed.

EVIDENCE	PRIMARY RECORDER	OTHER / OVERLAPPING CAMERAS	CLOUD COPY	EXPORTED CLIPS	RECORDER LOGS	DELETED / RECOVERABLE
The event footage	Y: until overwritten	Y: another angle	On cloud/ hybrid systems	Y: if already exported	n/a	Varies (carve, time-bound)
Timing	Y: subject to clock error	Y: cross-check	Cloud timestamps	Export metadata	Y: access/ export times	Fragments
That footage existed	Y: while retained	n/a	Y	Y	Y: even after deletion	Log persists
Who exported / accessed	Y: user actions	n/a	Cloud audit	Recipient records	Y: recorder log	n/a
Camera / scene detail	Y: native quality	Y: fills blind spots	Compressed	As exported	n/a	Partial frames

Fallback strategy in one line: preserve every camera that could have seen the event at once, because each has its own overwrite clock; and when the primary recorder has looped, a neighbouring camera, a cloud copy or an already-exported clip may still hold the frame.

Worked examples

EXAMPLE 1 · THE FOUR-DAY RETENTION AND THE ONE DAY LEFT

A personal-injury claim turned on how an accident in a shop had happened, and the shop's CCTV was the only objective record. By the time the claimant's solicitors were instructed and thought of the footage, it was three days old, on a busy multi-camera system with, it turned out, only four days' retention: the §4 first question, retention, revealed that the footage had roughly one day left before the loop reached it. A same-day preservation request was served on the shop, and the laboratory guided a proper native export of the relevant cameras with their metadata before the window closed. Twenty-four hours later the footage would have been gone. The claim was resolved on the preserved footage, which showed the sequence the parties disputed. The lesson is §2's: with CCTV the emergency is preservation, the clock is already running when instructions arrive, and the first act is to find the retention and beat it, not to analyse.

EXAMPLE 2 · THE DELETED FOOTAGE CARVED BEFORE THE LOOP CAUGHT IT

An employee alleged that footage exonerating her had been deleted from her employer's DVR by a manager. The manager said the footage had simply overwritten in the ordinary course. The §5 recovery settled it: the DVR was taken out of service immediately, before further recording could overwrite the residue, and imaged. Carving the proprietary video from the DVR's unallocated storage recovered the deleted sequence, which had been user-deleted, not overwritten, and the §6 recorder log recorded the deletion event, the account that performed it and the time, two days after the incident and after the employee had asked for the footage to be kept. The recovered footage supported the employee's account, and the deletion, dated and attributed, became evidence in itself. The lesson is §5's: deleted CCTV is not always gone, but the DVR must be stopped and imaged at once, because every hour it keeps recording destroys the recoverable residue.

EXAMPLE 3 · THE FILMED MONITOR AND THE NATIVE FILE THAT REPLACED IT

In a dispute over an altercation, one party relied on a shaky phone video of a CCTV monitor, low quality, undated, the on-screen timestamp barely legible and, it was alleged, wrong. It proved little and was easily challenged. The §4 and §6 approach recovered the real evidence: the recorder was still in service and, though the retention was nearly exhausted, the native footage of the relevant period was exported properly with its metadata, and the recorder's clock was checked against a known reference and found to be twelve minutes fast, an offset that, once corrected, reconciled the footage with the parties' phone records (§7). The authentic native file, correctly timed, replaced the filmed monitor entirely and resolved the timing dispute the phone video could not. The lesson is §6's: the filmed screen is a weak substitute for the recorder's own file, and where the recorder still holds the footage, the native export and the corrected clock are the evidence.

Common mistakes and technical limitations

Common mistakes

- **Delay:** the fatal error, treating CCTV like static evidence and preserving it days later, after the loop has erased it (Example 1): the retention unquantified and the deadline missed.
- **Filming the monitor:** a phone video of the screen taken instead of a native export, degraded, undated and weak (Example 3): the authentic file never captured.
- **Leaving the DVR recording:** a system from which deleted footage might be recovered left running, overwriting the residue hour by hour (Example 2, §5).
- **Trusting the on-screen clock:** the DVR timestamp taken as true when DVR clocks are routinely wrong, placing the footage on a false timeline (§6).
- **Re-encoding the footage:** the native file transcoded or screen-captured for convenience, losing quality and metadata (§4).
- **Preserving one camera:** the obvious camera secured while overlapping cameras with the same event on their own clocks are left to overwrite (§8).
- **Third-party footage not chased:** the neighbour's, shop's or council's footage requested too late, after their own loop erased it (§4, §8).
- **Enhancement overclaimed:** detail asserted from enhancement that the footage never actually captured (§6).

Technical limitations

- **Overwritten footage is gone:** once the loop has recorded over it, the footage is genuinely lost: the honest limit, and the reason preservation cannot wait (§5).
- **Recovery competes with recording:** a running DVR destroys recoverable residue continuously: the chance falls with every hour until the system is stopped and imaged (§5).
- **Proprietary formats resist:** some DVR formats are poorly documented and hard to decode or carve: solvable often, but not always, and the effort is stated.
- **Enhancement has limits:** enhancement reveals captured detail; it cannot create resolution or detail the camera never recorded (§6).
- **Retention is short and variable:** retention depends on disk size, camera count and settings, and can be far shorter than assumed: quantified per system, never guessed.

§ 1 1 · INTERROGATORIES & DRAFTING AIDS

Questions to ask · Suggested wording

Ask your client

- What cameras could have captured the event, who holds each recorder, and what is each one's retention period, so the deadlines are known now?
- Has the relevant footage been exported natively with its metadata, or only filmed off a monitor, and is any recorder still running?
- Is the recorder's clock known to be accurate, and against what reference can it be checked?

Ask your opponent (or a third-party holder)

- Please immediately preserve, and not allow to be overwritten, deleted or exported over, all CCTV footage from [cameras/recorder] for [period], export it in its native format with metadata intact, and confirm the system's retention period and the recorder's clock setting.
- Please confirm whether any relevant footage has been deleted, exported, re-recorded or allowed to overwrite since [date], and take the recorder out of service if deleted footage may need recovery.
- Please identify all cameras that may have captured the event, including any cloud-stored or third-party footage, and preserve each.

Ask your eDiscovery / forensic provider

- What is the retention, and how long do we have before the relevant footage overwrites?
- Should the recorder be seized and imaged to preserve deleted-footage recovery, or is a native export enough?
- What is the recorder's clock offset, and how does the footage reconcile with the other sources?

SUGGESTED WORDING · URGENT CCTV PRESERVATION REQUEST

"This is an urgent request to preserve CCTV evidence that may otherwise be automatically overwritten. You are asked immediately to: (1) preserve all footage from [cameras/recorder] for the period [dates/times], and prevent it being overwritten, deleted, re-recorded or exported over, by exporting it in the recorder's native format with all metadata (timestamps and camera identifiers) intact; (2) if there is any question of deleted footage requiring recovery, take the recorder out of service and do not allow it to continue recording, preserving the recorder and its disk intact for forensic imaging; (3) confirm the system's retention period, the recorder's current clock setting and any known clock error, and the make and model of the recorder; and (4) identify and preserve any additional or overlapping cameras, cloud-stored footage and third-party recordings that may have captured the same event. Given that CCTV systems overwrite footage automatically and continuously, time is critical, and footage lost after this request may be the subject of an application for adverse inferences. Please confirm the steps taken today."

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

The CCTV / DVR checklist

- ☐ Retention period quantified and the overwrite deadline known
- ☐ All cameras that could have seen the event identified
- ☐ Relevant footage exported natively with metadata, not filmed off a screen
- ☐ Recorder secured and imaged where deleted-footage recovery may be needed
- ☐ DVR taken out of service, not left recording, if recovery is in play
- ☐ Recorder clock checked against a reference; offset established
- ☐ Third-party and cloud footage preserved by prompt request
- ☐ Native original kept separate from any converted viewing copy
- ☐ Chain of custody documented from recorder to court
- ☐ Enhancement transparent, reversible and honestly bounded

Red flags

- Footage days old on a system whose retention is unknown: Example 1.
- A phone video of a monitor offered as the evidence: Example 3.
- A DVR left running when deleted footage might be recoverable: Example 2.
- An on-screen timestamp relied on with no clock check.
- Only the obvious camera preserved; overlapping cameras ignored.
- Relevant footage allowed to overwrite after a preservation request.
- Detail claimed from enhancement beyond what was captured.

When to involve a digital forensic expert

At once, because CCTV is the one evidence type where delay of a day can lose the case: the expert quantifies the retention, guides an immediate native export or secures the recorder, and stops the loop before it erases the frame (Example 1, §4); where footage has been deleted, to take the DVR out of service and image it before the residue is overwritten, and to carve the deleted video from proprietary storage (Example 2); on formats and timing, to decode proprietary footage without degrading it and to establish the clock offset so the frame is correctly placed (Example 3); and at deployment, where the native footage, its provenance and any enhancement are explained under CPR Part 35 or CrimPR Part 19, and any overwrite after a request is put as spoliation. Through **cflab.uk** and **e-discovery.uk**, CCTV work runs as an emergency preservation first and a forensic recovery second: because the footage that proves the case is erasing itself while the question is being asked.

§ 13 · COMMON QUESTIONS

Frequently asked questions

How long do we have before CCTV footage is gone?

Often days, sometimes only a few weeks, and occasionally less: retention is set by the disk size, the number of cameras and the recording settings, and busy multi-camera systems can hold as little as three or four days (§3, Example 1). The first step is always to find the retention period so the deadline is known, and then to preserve the footage before the loop reaches it. Assume the clock is short until proven otherwise.

Can we just film the CCTV monitor on a phone?

You can, but it is weak evidence and a poor substitute (§6, Example 3): a filmed screen is low quality, loses the metadata, and is easily challenged on timing and authenticity. The real evidence is the recorder's own native export with its metadata intact. Where the recorder still holds the footage, export it properly; the filmed monitor is a last resort for footage that no longer exists any other way.

Footage was deleted from the DVR. Can it be recovered?

Sometimes, if you act fast: user-deleted or not-yet-overwritten footage can be carved from the DVR's storage (§5, Example 2), and the recorder's log may record that the footage existed and who deleted it. But a running DVR keeps overwriting the residue, so the system must be taken out of service and imaged immediately. Footage the loop has already recorded over is genuinely gone.

The timestamp on the footage looks wrong. Does that matter?

It matters a great deal, and it is very common: DVR clocks are routinely set wrong, never adjusted for daylight saving, or drifted (§6). The recorder's clock is checked against a known reference to establish the offset, and the footage is then placed on the true timeline and reconciled with other sources like phone records or transaction logs (§7, Example 3). Never rely on the on-screen stamp without checking it.

The footage is dark or blurry. Can it be enhanced?

Within honest limits: lawful enhancement, brightness, contrast, stabilisation, can reveal detail that is present in the footage but hard to see, applied transparently and reversibly with the original kept (§6). What enhancement cannot do is invent resolution or detail the camera never captured: it reveals, it does not create. Any enhancement is documented and its limits stated, so the court knows what is real and what is interpretation.

The other side let the footage overwrite. Is there anything we can do?

Possibly: where they held relevant footage and let it overwrite after a preservation request, or failed to preserve it once the duty had arisen, the court may draw adverse inferences and impose spoliation consequences (§7), because CCTV loss is usually foreseeable and preventable. And the estate may still help, an overlapping camera, a cloud copy or an already-exported clip may hold the same event (§8). The overwrite of one recorder is not always the end.

§ 1 4 · REFERENCE

Glossary

DVR

Digital video recorder for analogue cameras.

NVR

Network video recorder for IP cameras.

Overwrite loop

Continuous recording that erases the oldest footage first.

Retention period

How long footage is held before the loop overwrites it.

Ring buffer

Fixed storage written round and round, oldest replaced by newest.

Native export

The recorder's own file with metadata, the authentic evidence.

Proprietary format

A DVR video format ordinary players cannot open.

Clock offset

The difference between the recorder's clock and true time.

Carving

Recovering video fragments from raw storage.

Enhancement

Revealing captured detail; not inventing what was not recorded.

Sources and authoritative references

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

- cflab.uk, digital forensics services (CCTV and DVR recovery, proprietary-format decoding, timestamp and authenticity analysis, CPR Part 35 and CrimPR Part 19 reporting): cflab.uk/digital-forensics-services · guides library: cflab.uk/guides
- e-discovery.uk, EDRM Phase 03 · Preservation and Phase 04 · Collection (urgent CCTV preservation and recovery as practised): e-discovery.uk/edrm/preservation · e-discovery.uk/edrm/collection
- e-discovery.uk, practice method and Knowledge Centre: e-discovery.uk · e-discovery.uk/knowledge
- Home Office / police guidance on the recovery and use of CCTV, and the Surveillance Camera Code of Practice: gov.uk, [Surveillance Camera Code](https://gov.uk/surveillance-camera-code) · ICO, video surveillance (CCTV) guidance: ico.org.uk, [CCTV](https://ico.org.uk/cctv)
- Forensic Science Regulator, Code of Practice v2 (including image and video work): gov.uk, [FSR Code](https://gov.uk/fsr-code) · ISO/IEC 27037: iso.org, [27037](https://iso.org/27037)
- PD 57AD (preservation) and CPR Part 31: justice.gov.uk, [PD 57AD](https://justice.gov.uk/pd-57ad) · justice.gov.uk, [Part 31](https://justice.gov.uk/part-31) · CPR Part 35: justice.gov.uk, [Part 35](https://justice.gov.uk/part-35)

DISCLAIMER

This publication provides general information about recovering and preserving CCTV and DVR footage as at August 2026. Recorder technology, formats, retention behaviour and recovery prospects vary by system and cannot be guaranteed; where footage is at risk of overwriting, act immediately. 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

CCTV work at the laboratory is run as an emergency, because it is one: the first call establishes the retention period and the deadline, and the immediate priority is to preserve the relevant footage as a native export with its metadata, or to secure the whole recorder, before the overwrite loop erases the frame (Example 1). Where deleted footage may need recovery, the recorder is taken out of service at once and imaged, because a running DVR overwrites the recoverable residue hour by hour, and the deleted video is then carved from the proprietary storage and the recorder's own log read for the deletion event (Example 2). Proprietary formats are decoded without degrading the image, the recorder's clock is checked against a known reference so the footage is placed on the true timeline, and any enhancement is applied transparently and honestly bounded (Example 3). The estate is mapped in parallel, every overlapping camera, cloud copy and already-exported clip preserved on its own clock, so a single overwritten recorder is not the end of the case. Reports run under CPR Part 35 or CrimPR Part 19. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine; and if CCTV might matter, the first message is the urgent one: find the retention and preserve the footage today, because it is erasing itself now.



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