COMPUTER FORENSICS LAB

London digital forensics & e-discovery · Established 2007

# Door Access, Swipe Cards and Building Logs

## Physical Presence Evidence and What a Badge Event Does and Does Not Prove

Who was in the building: the question beneath dismissal disputes, data-theft chronologies, harassment allegations, fraud timelines and alibi evidence: is answered by systems lawyers rarely think to ask for: door controllers logging every badge presented, turnstiles and barriers, lift-destination systems, visitor management platforms, desk-booking apps and alarm panels. Read carefully, these logs place a credential at a reader to the second, map movement through a building, and expose the "I was never there" and "I left at five" claims that other evidence cannot reach. Read carelessly, they convict the wrong person: cards are lent, doors are tailgated, and a badge event proves the card's presence, not the human's. This guide covers the access-control estate, what its logs record, attribution and its limits, collection before retention takes the record, and joining presence evidence to the digital timeline.

⏱ 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. Access-control evidence features across its employment, fraud and investigation casework: log collection from door controllers and building platforms, presence-timeline construction, attribution analysis against CCTV and device evidence, and CPR Part 35 reporting on what badge data supports. Its eDiscovery arm, **e-discovery.uk**, hosts presence data beside the documentary estate on one chronology.

ESTABLISHED 2007 · LONDON | ISO 17025-ALIGNED PROCEDURES | ACCESS-CONTROL & PRESENCE FORENSICS | TIMELINE CONSTRUCTION | CPR PART 35 EXPERT REPORTS | FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS

# In this guide

§ 0 1 · ORIENTATION

# Executive summary

**THE HEADLINE POINT: BADGE LOGS PLACE A CREDENTIAL PRECISELY: MAKING THEM PLACE A PERSON IS THE ANALYTICAL WORK**

Access-control systems log every credential event: card, reader, direction, result, to the second: and modern estates add turnstiles, lift-destination calls, visitor records and desk bookings, so a working building writes a continuous presence diary of everyone in it. For litigation this diary does two jobs: **positive placement** (the credential at the server-room door at 02:12) and **pattern evidence** (the departure hours that collapse an overtime claim; the weekend entries bracketing a data theft). The two disciplines that make it safe: **attribution**: a badge event proves the card, not the hand, so findings climb from credential to person via CCTV at the reader, anti-passback and movement coherence, device activity and witness evidence, stated to the rung reached: and **speed**: controller and platform retention runs from weeks to a couple of years by configuration, so the export happens before the argument does. Presence data then earns its keep interleaved with the digital timeline per guide 70: the badge-out at 17:03 against the login at 17:40 is where cases turn.

- **The estate is bigger than the front door:** internal readers, lifts, turnstiles, visitor and booking systems: censused and collected together.
- **Events prove credentials:** attribution to a human is built, not assumed: CCTV, coherence, devices, per the standing ladder.
- **Absence is weak alone:** tailgating, held doors and free-exit designs mean "no badge event" rarely proves "not there": stated honestly.
- **Retention is configured and short:** logs exported in week one, with the system's configuration and clock documented.
- **The join is the value:** presence against logins, CCTV, phones and documents: one corrected chronology per guide 70.

§ 0 2 · FIRST PRINCIPLES

# The problem in plain English: the building keeps a diary

Most litigants know their emails are evidence; almost none remember that the building logged them in and out for years. That asymmetry makes access data quietly devastating: witness statements are drafted about where people were, and then the controller export arrives with the seconds attached. The dismissed manager who "never worked past six" badged out after nine, forty-one times in the pleaded quarter. The defendant who "was never on the third floor" called the lift there twice on the disputed afternoon. Nobody shapes their story around a system they forgot exists.

The equal danger is over-reading. A badge event is a fact about a piece of plastic and a reader. Cards are lent, borrowed, stolen and cloned; doors are held open; exits are often unlogged by design. The lawyer's task is to demand this evidence early (it expires), and then to treat it as the skeleton of a presence case that still needs its joints: the corroboration of §5 and the joins of §7: before it bears weight in a pleading.

§ 0 3 · THE ESTATE

# The access-control estate: readers, controllers and platforms

- **Readers and credentials:** proximity cards and fobs, smart cards, PIN pads, mobile credentials on phones, biometric readers: each technology with its own attribution strength (a fingerprint reader answers §5 questions a lendable fob cannot).
- **Controllers and management platforms:** door controllers holding recent events locally, managed by head-end software (Paxton, Lenel, Gallagher, Honeywell and kin, plus cloud platforms) holding the fuller history, the credential register and the configuration.
- **Turnstiles, barriers and lifts:** logged pass-throughs at building entries; destination-control lifts recording which floor a credential called: movement inside the building, not just across its threshold.
- **Visitor and booking layers:** visitor management systems (invitations, sign-ins, host records, badge issues), desk and room booking platforms, muster and roll-call exports: the non-staff and intent layers of the diary.
- **Alarm and intruder systems:** set and unset events with user codes, zone activations, engineer logs: the after-hours chapter, often on longer retention than the doors.

§ 0 4 · THE RECORD

# What the logs record and how to read them

- **The event grammar:** timestamp, credential ID, cardholder record, reader, direction, result (granted, denied, invalid, door forced, door held): denials and anomalies are often more probative than grants: the fired employee's card tried at 23:50 is a finding either way.
- **The credential register:** who holds which cards, issue and revocation dates, access-level assignments and their change history: the register's own audit trail dates permission changes (who was given server-room access, when, by whom).
- **Direction and journey logic:** in and out readers, anti-passback rules, and reader topology turning events into movement paths: with free-exit doors (no out-reader) mapped so silence is read correctly.
- **System clocks:** controllers drift like DVRs: the offset measured against reference events (synchronised CCTV, IT logs) before seconds are pleaded: guide 77 §6's discipline, repeated here deliberately.
- **Configuration and admin trails:** schedule changes, door unlock periods, credential edits and log purges by administrators: read for mid-dispute acts per the standing trail-integrity rule.

§ 0 5 · WHOSE HAND

# Attribution: card, credential and human

- **The ladder, presence edition:** event proves credential; credential register names an assigned holder; the human is reached by corroboration: CCTV at the reader (the strongest join), biometric credentials, movement coherence (a plausible single journey through multiple readers), paired device activity, and witness evidence.
- **Lending and borrowing:** the commonest defence and sometimes true: tested against pattern (whose working rhythm do the events match), simultaneity contradictions (the card downstairs while its holder's login runs upstairs), and the lender's own account.
- **Tailgating and held doors:** unlogged entries behind logged ones: why absence of an event is weak evidence of absence, and why headcount-sensitive findings check turnstile and CCTV layers where they exist.
- **Cloning and technical spoofing:** legacy proximity technologies are copyable: raised where facts warrant (impossible journeys, simultaneous use), investigated through credential serial data and reader technology, not presumed.
- **The honest statement:** findings pleaded to the rung: "the credential assigned to X was presented" is always safe; "X entered" needs the corroboration named: the series' standing fairness rule at a door.

§ 0 6 · BEFORE IT GOES

# Collection and retention: getting the logs before they go

- **Retention is configured, not standard:** platform databases may hold months to years; controller-local buffers days to weeks; visitor and alarm layers on their own schedules: the census asks each system its retention on day one.
- **Export with structure:** event data in structured form (not PDF prints), with the credential register, reader map, configuration and admin trails: collected per guide 71's disciplines: the query, counts and hashes of the reproducibility bundle.
- **The building manager problem:** multi-tenant buildings put the estate under landlords and managing agents: the preservation letter goes to the operator, and the request is framed for a facilities audience: dates, doors, named exports.
- **Clock documentation at collection:** the system time recorded against reference time when the export is taken: the cheapest moment to anchor every second in the dataset.
- **UK GDPR handling:** presence data is personal data, sometimes revealing patterns (health appointments, prayer rooms, union offices): minimisation, need-to-know handling and third-party redaction built into the workflow.

§ 0 7 · THE JOIN

# Joining presence to the digital timeline

- **Presence against activity:** badge events beside logins, file access, sends and prints: the physical alibi tested against the digital one, and vice versa: the 17:03 badge-out against the 17:40 local login is a contradiction only the join reveals.
- **CCTV synchronisation:** reader events paired with camera frames on corrected clocks: attribution's strongest rung, built per guide 77 §6.
- **The remote-work era:** hybrid patterns mean absence from the building implies nothing about work: presence data reads against VPN, collaboration and booking layers before conclusions about working time.
- **Pattern deliverables:** per-person presence calendars, after-hours matrices, anomaly schedules (first-ever accesses, denial clusters, out-of-pattern floors): the aggregate analyses that turn events into narrative, baselined per the fairness rule.
- **One chronology:** everything lands in the guide 70 assembly: corrected clocks, source-attributed entries, gaps labelled: presence as one voice in the interleaved record, which is where it persuades.

§ 0 8 · THE WIDER MAP

# Source architecture: where else the evidence lives

Per this series' source-architecture discipline: the door controller is one witness among the building's several. Presence evidence also lives in: the platform database above the controllers (the fuller history); CCTV covering readers, lobbies and floors (guide 77's estate, the attribution partner); lift, turnstile and barrier systems with independent logs; visitor, desk-booking and meeting-room platforms; alarm panels with set/unset records; the digital periphery placing people without doors (VPN and Wi-Fi association, machine logins, print jobs, phone location per guide 124); payroll, time-and-attendance and clock-in systems where used; and the correspondence estate ("just badged in, see you in five"). When the controller's logs have rotated, the platform layer, the periphery and the paired systems rebuild presence: and disagreements between witnesses (the badge diary against the Wi-Fi diary) are findings, not noise.

| EVIDENCE | CONTROLLERS / PLATFORM | CCTV LAYER | LIFTS / TURNSTILES / VISITORS | DIGITAL PERIPHERY | TIME & ATTENDANCE | DELETED / RECOVERABLE |
|---|---|---|---|---|---|---|
| **Entry / exit events** | Y: retention-bound | Frames at readers | Independent logs | Wi-Fi joins bracket | Clock-ins mirror | Platform outlives controller buffers |
| **Movement inside** | Internal readers | Corridor coverage | Lift destination calls | Per-floor Wi-Fi APs | n/a | Multi-system rebuild |
| **Identity at the door** | Credential + register | Y: the face | Visitor photos / sign-ins | Device pairing | n/a | Attribution rung-bound |
| **After-hours presence** | Y + denials | Y | Alarm set/unset | Logins, prints | Overtime records | Alarm logs often longest-lived |
| **Permission changes** | Register audit trail | n/a | Host/invite records | IT ticketing | n/a | Trail-integrity rule applies |

Fallback strategy in one line: when the door logs are gone, presence rebuilds from the platform, the cameras, the lifts, the Wi-Fi and the alarm panel: buildings keep several diaries, and they rarely all rotate at once.

§ 0 9 · IN THE WILD

# Worked examples

### EXAMPLE 1 · THE OVERTIME THAT BADGED ITSELF OUT

A senior technician claimed 640 hours of unpaid overtime across two years, supported by a meticulous personal spreadsheet. The access export, obtained inside the platform's 24-month window with a documented clock offset of plus 94 seconds, told a different rhythm: on 78 of the 121 claimed late nights, his credential badged out through the staff turnstile before 17:30; on 19 more, it never badged in at all. The join completed it: his VPN records showed no evening sessions on the badgeless days, and the car park barrier agreed with the turnstile to the minute. Cross-examined on the diary against the building's, the claim settled at a twentieth of its pleaded value: with the tribunal's observation that the spreadsheet's neatness had been its least persuasive feature.

### EXAMPLE 2 · THE SERVER ROOM AT 02:12, AND WHOSE HAND

A database was exported from a locked server room at 02:14 on a Sunday; the room's reader logged the IT manager's credential at 02:12. He denied presence: his card lived in an unlocked desk drawer, he said, and anyone could have taken it. The corroboration ladder decided it: the lobby camera, synchronised to the corrected controller clock, showed him entering at 02:04 in a hooded jacket; his own phone's Wi-Fi joined the third-floor access point at 02:06; the server-room door's in-reader event was followed by his credential's out-event at 02:31, a plausible single journey with no simultaneity contradictions anywhere in the estate; and the export session on the console ran under his named account. Each rung alone was answerable; the ladder was not. The "borrowed card" defence was abandoned before trial.

### EXAMPLE 3 · THE ABSENCE THAT PROVED NOTHING, HONESTLY

A harassment grievance placed an accused manager on the fourth floor at lunchtime; his defence produced the access logs showing no fourth-floor reader events for his credential that day, pleaded as alibi. The examination report stated the system's honest limits: the fourth floor was reachable from the third by an open stairwell with no reader; the floor's doors were on free exit; and turnstile data placed him in the building throughout. The badge silence proved only that he had not badged: the tribunal was directed instead to the lift system (one destination call to floor four from his credential at 12:41) and the corridor CCTV, which resolved the afternoon the logs could not. The case is the series' standing caution in miniature: absence of an event is not evidence of absence, and saying so first is what keeps an expert's other findings believed.

§ 10 · WHERE IT GOES WRONG

# Common mistakes and technical limitations

## Common mistakes

- **The ask that comes too late:** retention windows spent on correspondence: Example 1's export exists because someone asked in week one.
- **PDF prints instead of structured exports:** the analysis layer surrendered at collection: guide 71's flattening error at the door.
- **Badge equals person:** §5 skipped, the lending defence unanswered: the finding overturned with the case's credibility.
- **Absence pleaded as alibi:** Example 3's inversion: free-exit doors and stairwells unmapped, the silence over-read.
- **Clocks unverified:** controller drift folded silently into a minute-critical chronology.
- **The register forgotten:** events collected without the credential and permission histories that give them meaning.
- **Multi-tenant blindness:** the landlord's systems (turnstiles, lifts, visitor desk) never requested because the client's own doors answered first.
- **GDPR shortcuts:** whole-building exports circulated unminimised: a parallel problem manufactured inside the evidence exercise.

## Technical limitations

- **Exit logging is often absent:** free-exit design means departure times may be unknowable from doors alone: bracketed from turnstiles, alarms and the periphery.
- **Retention is short at the edge:** controller-local buffers overwrite fast; the platform's window governs, and it is a configuration fact.
- **Legacy credentials are cloneable:** raised on evidence, not speculation: but impossible journeys are checked before attribution hardens.
- **Topology bounds inference:** unreadered routes, propped doors and lift-lobby designs cap what movement logic can prove: the reader map is part of the evidence.
- **Pattern needs baseline:** after-hours and anomaly findings mean nothing without the person's and the building's normal: baselined per the standing fairness rule.

§ 11 · INTERROGATORIES & DRAFTING AIDS

# Questions to ask · Suggested wording

## Ask your client

- Which systems make up the estate: doors, turnstiles, lifts, visitors, alarms, bookings: who operates each, and what is each one's retention?
- Is the structured export (events, register, reader map, configuration) commissioned, and the clock offset documented?
- For attribution: which readers have CCTV coverage, and are those recordings preserved per guide 77's race?

## Ask your opponent

- Please preserve and produce, in structured form, all access-control event data for [premises/period], together with the credential register and its audit trail, the reader map and directions, the system configuration including free-exit doors, and all administrator logs, stating the system, its retention settings and its clock accuracy at export.
- Please produce the corresponding turnstile, lift-destination, visitor-management, desk-booking and alarm set/unset records for the same period.
- Please identify any credential reported lost, lent, shared or cloned in the period, and any changes to [person]'s access levels, with the register entries recording them.

## Ask your eDiscovery / forensic provider

- What is the clock offset, and which reference anchors it?
- To which rung does attribution climb for the load-bearing events: and what corroboration is still gettable?
- What does the join against the digital timeline show: agreements, contradictions, gaps?

### SUGGESTED WORDING · ACCESS-CONTROL LIMB FOR THE PRESERVATION LETTER

> "Your client must immediately preserve all physical access-control data for [premises] for [period], including: (a) all event logs from door, turnstile, barrier, lift and alarm systems, in structured electronic form; (b) the credential register, access-level assignments and their audit trails; (c) the reader map, system configuration and administrator logs; and (d) all visitor-management and desk or room booking records. Automatic purging or overwriting of any such data must be suspended, and where retention limits cannot be extended the data should be exported forthwith with the system clock documented against reference time. Please confirm within [3] days, identifying each system, its operator and its retention period. Where systems are operated by a landlord or managing agent, please forward this request to them immediately and confirm you have done so."

§ 12 · QUICK CONTROL

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

## The access-control checklist

- ☐ Estate censused: doors, turnstiles, lifts, visitors, alarms, bookings, operators, retentions
- ☐ Preservation letters out within the shortest window, landlords included
- ☐ Structured exports with register, reader map, configuration and admin trails
- ☐ Clock offset measured and documented at collection
- ☐ Attribution built by the ladder; rungs stated in every finding
- ☐ Free-exit doors and unreadered routes mapped before absence is read
- ☐ CCTV at readers preserved and synchronised per guide 77
- ☐ Presence joined to the digital timeline per guide 70
- ☐ Pattern findings baselined against normal rhythms
- ☐ UK GDPR minimisation and redaction applied to productions

## Red flags

- Retention windows closing during pre-action correspondence: act now.
- Badge patterns contradicting sworn working hours: Example 1's class.
- Denial clusters and out-of-pattern events around key dates.
- Credentials used after revocation, or "lost" cards still active.
- Access-level changes to sensitive areas shortly before incidents.
- Simultaneity contradictions: one credential, two places.
- Alibis built on badge silence over free-exit topology: Example 3's caution.
- Administrator purges or configuration changes post-dispute.

## When to involve a digital forensic expert

At the census, where the estate and its retentions are mapped against the clock; at collection, where structured exports, clock anchoring and the reproducibility bundle keep the data evidential; at analysis, where attribution ladders, topology-aware movement reading and baselined patterns are built and joined to CCTV and the digital record (Examples 1-3's machinery); and at reporting, where presence findings state their rungs under CPR Part 35. Through **e-discovery.uk**, the building's diary sits on the same reviewed chronology as everything else the case knows.

§ 13 · COMMON QUESTIONS

# Frequently asked questions

### How long are swipe logs actually kept?

Anywhere from weeks to a few years: it is a configuration and platform fact, not a standard: controller-local buffers are shortest, head-end databases longest, and visitor and alarm layers run their own schedules. The only safe assumption is that a window is closing, which is why the census and the ask happen in week one.

### Can badge data alone prove someone was in the building?

It proves the credential was: the person follows from corroboration: CCTV at the reader, biometrics, journey coherence, paired device activity: per §5's ladder, and honest findings say which rung they stand on. Example 2 shows the ladder reaching certainty; a lone badge event never does by itself.

### The logs show no exit for our witness. When did they leave?

Possibly unknowable from the doors: free-exit design logs entries only: so departure brackets from the estate's other diaries: turnstiles and barriers, alarm set events, last logins and prints, final Wi-Fi association, car park systems. The bracket is often tight enough to plead; the door log alone was never going to be.

### Our client says a colleague borrowed their card. Hopeless?

Testable, both ways: lending is common and sometimes true: the examination checks whose rhythm the events match, hunts simultaneity contradictions (the card here, the holder's login there), reads CCTV at the readers, and hears the alleged borrower. Where the ladder's rungs point away from the holder, the defence stands up; where they converge on them, Example 2 is how it ends.

### Is building access data caught by disclosure duties like documents?

Fully: it is recorded information within a party's control, disclosable where relevant and preservable from the moment litigation is contemplated: purging it on schedule after that moment invites the adverse-inference conversation. The practical wrinkle is operational: the data often sits with facilities teams or landlords who have never met a disclosure obligation: hence the §11 letter's forwarding limb.

### Can employers freely use this data to investigate staff?

Purposefully, proportionately and transparently: presence data is personal data: investigation use needs a lawful basis, honest privacy notices help, minimisation is expected, and pattern analysis brushing sensitive inferences (health, religion, union activity) deserves particular care and usually a DPIA. Well-run investigations use the data confidently inside those rails: the rails are not the obstacle; ignoring them is.

§ 14 · REFERENCE

# Glossary

**Anti-passback**
Rules preventing credential reuse without a logged exit; a coherence check.

**Credential register**
The card-to-holder mapping with issue, revocation and level history.

**Destination control**
Lift systems logging which floor a credential called.

**Door forced / held**
Alarm events for unauthorised opening or propping; probative anomalies.

**Free exit**
Egress without a reader; the source of honest silence.

**Head-end**
The management platform above controllers; the fuller log store.

**Mobile credential**
Phone-based access; pairs presence with a personal device.

**Reader map**
The topology of readers, directions and unreadered routes.

**Tailgating**
Unlogged entry behind a logged one; the attribution caveat.

**Time and attendance**
Clock-in systems mirroring presence for payroll; a paired diary.

## Sources and authoritative references

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

- cflab.uk, digital forensics services (access-control collection, attribution analysis, presence timelines, CPR Part 35 reporting): cflab.uk/digital-forensics-services · guides library: cflab.uk/guides
- e-discovery.uk, EDRM Phase 01 · Identification, Phase 02 · Preservation and Phase 03 · Collection (building systems in the data map; retention-beating preservation; structured acquisition): e-discovery.uk/edrm/identification · 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
- ICO, UK GDPR guidance, employment practices and DPIA resources: ico.org.uk
- PD 57AD, CPR Part 31 and CPR Part 35: justice.gov.uk, PD 57AD · justice.gov.uk, Part 35
- ISO/IEC 27037 (identification, collection and preservation of digital evidence): iso.org, 27037

§ HOW A SPECIALIST LABORATORY CAN ASSIST

# Working with Computer Forensics Lab

Access-control instructions at the laboratory begin with the census: every diary the building keeps, every operator, every retention window: and the structured exports commissioned before the shortest one closes, clocks anchored at collection. Analysis builds the attribution ladders, topology-aware movement readings and baselined pattern schedules of Examples 1-3, joins presence to CCTV per guide 77 and to the digital record per guide 70, and states every finding to its rung under CPR Part 35: including, where the data demands it, the honest Example 3 report that the logs cannot answer the question asked. UK GDPR handling and third-party redaction run through the workflow. Through **e-discovery.uk**, the building's evidence sits reviewable beside the estate's. Conflicts checks, confidential scoping discussions and fixed-fee estimates are routine; and if your matter turns on who was where, the retention question goes to the facilities manager today.

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