Digital Data Forensic Recovery and Expert Witness Service Definition

Document title	Digital Data Forensic Recovery and Expert Witness Service Definition		
Reference No.	IF-SER-016	**Version**	1.0
Author	Lisa Washer, Head of Cyber		
Reviewed by	Adam Whitbread, Principal Digital Forensic Analyst		
Issue date	23/01/2026		

Digital Data Forensic Recovery and Expert Witness Service Definition

Document Control

Version	Name	Comment	Date
0.1	Lisa Washer	Initial draft	07/01/2026
0.2	Adam Whitbread	Review and amendments	22/01/2026
1.0	Lisa Washer	Final review and publish	23/01/2026

Correlation Chart

Clause	FSR Code of Practice v2	ISO/IEC 17025:2017	ILAC-G19 :06/2022	ISO 9001:2015	ISO/IEC 27001:2022
Review of Requests, Tenders and Contracts	16	7.1	4.1, 4.7	8	4.2

Digital Data Forensic Recovery and Expert Witness Service Definition

Contents

1. Forensic Device Data Recovery Service

1.1 Service Overview

1.1.1 The Forensic Device Data Recovery Service provides specialist forensic data recovery and examination support for damaged, failed, corrupted, or inaccessible digital devices. The service is designed to recover data from individual devices while preserving evidential integrity and maintaining forensic soundness.

1.1.2 The service supports legal, regulatory, investigative, insurance, and internal review requirements by enabling the recovery and validation of data that may be critical to understanding events, establishing facts, or supporting proceedings.

1.1.3 Services are delivered by qualified digital forensic practitioners operating in accordance with recognised forensic standards and best practice. Engagement is provided on an ad-hoc consultancy basis and may be initiated without a pre-existing contract, subject to appropriate authorisation.

2. Service Features

2.1.1 Below is a list of the core capabilities and characteristics of the Cyber Incident Investigation service, describing what is delivered and how the service operates:

a) **Device Assessment and Triage** - Initial examination to determine device condition, failure type, recovery feasibility, and priority data targets.

b) **Forensic Data Recovery -** Recovery of data from damaged, failed, corrupted, deleted, or inaccessible storage media using forensic techniques that preserve evidential integrity.

c) **Logical and Physical Acquisition -** Forensically sound logical and physical imaging of storage media, including partial or targeted acquisition where full imaging is not possible.

d) **File System and Data Structure Reconstruction -** Reconstruction of damaged file systems, partitions, and metadata to enable recovery of user and system data.

e) **Deleted and Residual Data Recovery -** Identification and recovery of deleted files, unallocated space artefacts, and residual data fragments where technically feasible.

f) **Mobile Device Data Recovery -** Specialist recovery from mobile phones and tablets, including extraction of user data, application artefacts, and system records where supported.

g) **Secure Evidence Handling and Preservation -** Controlled handling, storage, and documentation of devices and recovered data in line with forensic chain-of-custody requirements.

h) **Data Validation and Integrity Verification -** Use of cryptographic hashing and validation techniques to demonstrate data integrity and reproducibility.

i) **Technical and Evidential Reporting -** Clear documentation of recovery methods, limitations, findings, and outcomes suitable for legal, regulatory, or investigative use.

j) **Expert Advisory Support -** Guidance on recovery feasibility, evidential value, limitations, and next steps based on recovered data.

3. Service Benefits

3.1.1 The Forensic Device Data Recovery Service provides organisations with reliable, defensible access to critical data from damaged or inaccessible devices. Key benefits include:

a) **Recovery of Critical Information -** Enables access to data that would otherwise be unavailable due to device failure, damage, or corruption.

b) **Forensic Soundness and Evidential Integrity -** Ensures recovered data can withstand legal, regulatory, or investigative scrutiny.

c) **Reduced Risk of Data Loss -** Applies specialist techniques beyond standard IT recovery methods, improving recovery success rates.

d) **Legal and Regulatory Confidence -** Supports litigation, insurance claims, regulatory enquiries, and internal investigations.

e) **Clear Understanding of Data Limitations -** Provides transparent explanation of what data can and cannot be recovered and why.

f) **Independent Specialist Expertise -** Delivered by experienced forensic practitioners independent of internal IT or operational teams.

g) **Controlled and Secure Handling -** Minimises risk of further damage, data contamination, or evidential compromise.

4. Scope of Service

4.1 In-scope activities

4.1.1 The Forensic Device Data Recovery Service covers the recovery and forensic handling of data from individual digital devices and storage media. In-scope activities include:

a) **Device Intake and Assessment -** Initial evaluation of device condition, damage type, storage technology, and recovery approach.

b) **Forensic Acquisition and Recovery -** Forensically sound recovery of data from supported devices and media, including partial or targeted recovery where required.

c) **Evidence Identification and Preservation -** Identification, collection, documentation, and preservation of recovered data and artefacts.

d) **Data Reconstruction and Analysis -** Reconstruction of file systems, directories, and data structures to enable meaningful access to recovered data.

e) **Data Validation and Verification -** Integrity checking and validation of recovered data using forensic hashing and verification processes.

f) **Reporting and Documentation -** Preparation of technical and evidential reports detailing methods, findings, and limitations.

g) **Advisory Support -** Expert guidance on evidential relevance, recovery outcomes, and potential next steps.

h) **Legal and Regulatory Support -** Support for legally privileged engagements when instructed via external legal counsel, preparation of court-ready documentation, and provision of expert witness services subject to separate agreement.

4.2 Out-of-scope activities

4.2.1 The following activities are not included within the standard scope of the Forensic Device Data Recovery Service:

a) Live enterprise system recovery or business continuity restoration

b) Ongoing managed recovery or monitoring services

c) Provision of legal advice or legal representation

d) Investigation of systems or devices without appropriate authorisation

e) Destructive repair techniques unless explicitly agreed and documented

f) Data reconstruction requiring hardware manufacturer intervention unless separately arranged

4.3 Assumptions, Constraints and Dependencies

4.3.1 The delivery of the Forensic Device Data Recovery Service is subject to the following assumptions and constraints:

a) **Client Authority -** The client must have legal authority to submit devices and authorise forensic examination and recovery.

b) **Device Condition -** Recovery success depends on device condition, damage severity, encryption status, and storage technology.

c) **Encryption and Security Controls -** Encrypted devices may limit or prevent recovery without valid credentials or lawful authority.

d) **Point-in-Time Recovery -** Recovered data reflects the state of the device at the time of acquisition and may not represent all historical activity.

e) **Non-Destructive Priority -** All recovery efforts prioritise non-destructive methods unless destructive techniques are explicitly authorised.

f) **Third-Party Dependencies -** Certain recoveries may rely on vendor support, specialist hardware, or external laboratories.

5. Onboarding

5.1.1 Onboarding begins upon service initiation and focuses on secure intake, authorisation, and scoping.

5.1.2 During onboarding, device details, ownership, legal authority, and recovery objectives are confirmed. Device condition and handling requirements are documented, and any prior actions taken on the device are recorded to assess potential impact on recovery and evidential integrity.

5.1.3 Scope, success criteria, reporting requirements, and delivery timelines are agreed. Chain-of-custody documentation is initiated, and secure storage and handling arrangements are confirmed.

6. Service Delivery Model

6.1.1 The service is delivered using a structured forensic recovery approach aligned with recognised digital forensic methodologies.

6.2 Engagement Approach

6.2.1 A dedicated forensic practitioner is assigned to conduct the recovery, overseen by a service manager responsible for quality assurance, governance, and client communication. Engagements are evidence-led and proportionate to the device condition and recovery objectives.

6.3 Delivery Phases

a) **Assessment and Scoping -** Evaluation of device condition, feasibility, and recovery strategy.

b) **Forensic Acquisition and Recovery -** Execution of agreed forensic recovery techniques and data extraction.

c) **Validation and Review -** Integrity checking, data validation, and quality assurance.

d) **Reporting and Close-Out -** Delivery of findings, documentation, and recovered data in agreed formats.

6.4 Typical Timelines

6.4.1 Timelines vary based on device type, condition, data volumes to be recovered and complexity:

a) **Low Complexity (1–3 days):** Logical recovery from functioning devices or removable media

b) **Moderate Complexity (3–7 days):** Corrupted file systems, partial damage, mobile device recovery

c) **High Complexity (7–15+ days):** Physically damaged media, degraded storage, encrypted or unsupported devices

6.5 Delivery Modes

6.5.1 Services may be delivered on-site, remotely (where imaging is possible), or through secure laboratory-based recovery, depending on device sensitivity and condition.

7. Support Model

7.1.1 The Forensic Data Recover Service consists of two support models:

a) **Standard Support** - Business-hours delivery including recovery activities, status updates, and reporting.

b) **Enhanced Support -** Accelerated or out-of-hours recovery for time-critical or legal matters, subject to agreement.

8. Service Level Agreements

8.1.1 The following service levels describe indicative performance targets for the Forensic Device Data Recovery Service. These service levels are provided for guidance and planning purposes and do not constitute guaranteed commitments unless expressly agreed in writing.

8.1.2 Where a pre-existing contract, framework agreement, or retainer arrangement is in place, the service levels and response commitments defined within that agreement take precedence over the indicative service levels outlined below.

8.2 Service Request Acknowledgement

8.2.1 Initial acknowledgement is provided following receipt of a service request and confirmation that appropriate authorisation and device intake requirements can be met.

a) **Standard Requests**: Acknowledged within 1 business day

b) **Urgent / Time-Critical Requests**: Acknowledged within 4–8 business hours, subject to availability

8.2.2 Acknowledgement includes confirmation of receipt, initial eligibility assessment, and next steps for device intake and scoping.

8.3 Engagement Initiation

8.3.1 Formal engagement commences once authorisation, scope, and commercial terms are agreed and the device is accepted for examination.

a) **Standard Engagements:** Initiation within 1–2 business days of device receipt

b) **Urgent Engagements:** Initiation within 24 hours of device receipt, subject to resource availability

8.4 Recovery Commencement

8.4.1 Formal engagement commences once authorisation, scope, and commercial terms are agreed and the device is accepted for examination.

a) **Standard Engagements:** Initiation within 1–2 business days of device receipt

b) **Urgent Engagements:** Initiation within 24 hours of device receipt, subject to resource availability

8.5 Delivery Timeframes

8.5.1 Delivery timeframes vary depending on device type, condition, encryption status, data volumes to be recovered and recovery complexity.

8.5.2 Indicative delivery targets:

a) **Low Complexity:** 1–3 business days

b) **Moderate Complexity:** 3–7 business days

c) **High Complexity**: 7–15+ business days

8.5.3 Timeframes are confirmed following initial assessment and may be revised if device condition or technical constraints change.

8.6 Reporting Commitments

8.6.1 Reporting deliverables are provided in line with agreed scope and evidential requirements.

a) **Interim Updates**: Provided at agreed milestones or upon material changes to recovery status

b) **Final Recovery Report:** Typically delivered within 3–5 business days of recovery completion

c) **Court or Regulatory Reports:** Delivery timelines agreed based on jurisdictional and procedural requirements

8.6.2 All reports document methods used, recovery outcomes, data integrity validation, and known limitations.

8.7 Escalation and Priority Handing

8.7.1 Priority handling may be applied where recovery is required to meet:

a) Legal or court-imposed deadlines

b) Regulatory reporting obligations

c) Time-sensitive investigative or insurance requirements

8.7.2 Escalation requests are reviewed by the Forensic Service Manager and prioritised subject to resource availability and agreed commercial terms.

8.8 Service Limitations

8.8.1 Service levels are subject to the following limitations:

a) Physical damage severity may impact recovery timelines

b) Encrypted devices may significantly delay or prevent recovery

c) Third-party dependencies (e.g. vendor support) may introduce delays

d) Destructive recovery techniques, where authorised, may require extended lead times

8.9 SLA Exclusions

8.9.1 The following are excluded from SLA commitments:

a) Recovery outcomes or success guarantees

b) Data volume or completeness guarantees

c) Delays caused by incomplete authorisation or device information

d) Client-caused delays in device delivery or decision-making

9. Roles and Responsibilities

9.1.1 The following roles are defined to ensure effective governance, evidential integrity, and clear communication throughout the delivery of the Forensic Device Data Recovery Service. Clear delineation of responsibilities supports accountability, quality assurance, and defensible forensic outcomes.

9.2 Account Manager

9.2.1 The Account Manager is responsible for overall engagement governance and commercial oversight. This role ensures that the service is delivered in line with agreed scope, contractual terms, and client expectations. Key responsibilities include:

a) Acting as the primary commercial point of contact for the client

b) Confirming engagement scope, service levels, and commercial terms

c) Managing engagement changes, extensions, or scope variations

d) Handling commercial and strategic escalations

e) Ensuring appropriate resourcing and priority alignment

f) Supporting client decision-making where commercial or scheduling impacts arise

9.2.2 The Account Manager does not direct forensic methodology or influence technical findings.

9.3 Forensics Service Manager

9.3.1 The Forensic Service Manager provides operational leadership and quality assurance across the engagement. This role ensures forensic standards, governance, and evidential requirements are consistently applied. Key responsibilities include:

a) Overall oversight of forensic recovery activities

b) Validation that methods align with recognised forensic best practice

c) Review and assurance of reports, findings, and documentation

d) Approval of recovery approaches, including any destructive techniques

e) Managing operational escalations and risk issues

f) Ensuring chain-of-custody and evidence handling requirements are met

9.3.2 The Forensic Service Manager is accountable for forensic integrity and methodological defensibility.

9.4 Forensic Practitioner

9.4.1 The Forensic Practitioner is responsible for executing the technical data recovery and forensic examination activities. Key responsibilities include:

a) Conducting device intake, assessment, and recovery activities

b) Applying forensic acquisition and recovery techniques

c) Maintaining evidential integrity throughout handling and analysis

d) Documenting actions, tools, and decisions in a defensible manner

e) Validating recovered data using hashing and verification methods

f) Identifying technical limitations and recovery constraints

g) Contributing to technical and evidential reporting

9.4.2 The Forensic Practitioner operates independently and objectively, guided by evidence rather than outcome expectations

9.5 Client Representative

9.5.1 The Client Representative acts as the authorised liaison between the organisation and the forensic team. Key responsibilities include:

a) Confirming legal authority to submit devices for examination

b) Authorising scope, objectives, and any changes to engagement parameters

c) Coordinating device handover, access credentials, and supporting information

d) Facilitating internal stakeholder communication

e) Approving delivery timelines and priority requests

f) Receiving and managing recovered data and reports

9.5.2 The Client Representative is accountable for ensuring that devices and data submitted are lawfully owned or controlled.

9.6 Legal Counsel

9.6.1 Where legal privilege, litigation, or regulatory exposure is anticipated, legal counsel may be involved in the engagement. Key responsibilities include:

a) Defining legal objectives and disclosure requirements

b) Advising on privilege, confidentiality, and regulatory considerations

c) Coordinating instructions for expert reporting or testimony

d) Reviewing forensic outputs for legal use

e) Managing interactions with courts, regulators, or insurers

9.6.2 Legal counsel does not influence forensic methods or technical conclusions.

9.7 Client Stakeholder and Subject Matter Experts

9.7.1 Client SMEs provide contextual and technical information necessary to support effective recovery and interpretation of data. Key responsibilities include:

a) Providing device history, usage context, and incident background

b) Supplying access credentials where lawfully permitted

c) Clarifying system or application behaviour relevant to recovered data

d) Assisting in interpreting recovered artefacts where required

9.7.2 SMEs are consulted to provide context but are not responsible for forensic decisions.

9.8 Role Interaction and Authority Model

9.8.1 Forensic decisions are owned by the Forensic Practitioner and overseen by the Forensic Service Manager

9.8.2 Commercial and scheduling decisions are owned by the Account Manager

9.8.3 Scope and legal authority are owned by the Client Representative, with legal counsel support where applicable

9.8.4 Findings and conclusions are evidence-led and not subject to client approval or amendment

9.8.5 This separation ensures independence, defensibility, and trust in forensic outcomes

10. Technical Requirements

10.1.1 Delivery of the Forensic Device Data Recovery Service requires appropriate technical, procedural, and environmental conditions to ensure forensic soundness, evidential integrity, and effective recovery outcomes. These requirements are confirmed during onboarding and reviewed throughout the engagement as necessary.

10.2 Legal Authorisation and Ownership

10.2.1 Written confirmation must be provided that the client has legal ownership, custody, or lawful authority over the device(s) submitted for recovery.

10.2.2 Authorisation must explicitly permit forensic examination, data recovery, and analysis activities.

10.2.3 Where devices contain third-party or personal data, confirmation of lawful processing grounds must be provided.

10.2.4 For legally privileged or litigation-related matters, written instructions from external legal counsel may be required prior to commencement.

10.3 Device Intake and Condition

10.3.1 Devices must be submitted in their current state without further use, repair, or modification wherever possible.

10.3.2 The client must disclose any known damage, prior repair attempts, exposure to environmental hazards (e.g. water, fire, impact), or previous data recovery efforts.

10.3.3 Device details must be provided, including make, model, serial numbers, storage type, operating system (if known), and accessories supplied.

10.3.4 Any deviation from original device condition must be documented at intake to assess impact on recovery and evidential reliability.

10.4 Secure Transfer and Storage

10.4.1 Devices must be transported using secure, trackable methods appropriate to the sensitivity and evidential value of the device.

10.4.2 Packaging must protect devices from electrostatic discharge, physical damage, and environmental exposure.

10.4.3 Upon receipt, devices are stored in controlled, access-restricted environments with documented chain-of-custody records.

10.4.4 Storage conditions are maintained to prevent further degradation, particularly for damaged or unstable media

10.5 Access Credentials and Security Controls

10.5.1 Where available and lawfully permitted, relevant access credentials (e.g. PINs, passwords, passcodes, patterns) should be provided to support logical acquisition and recovery.

10.5.2 The absence of credentials, presence of encryption, or use of secure enclaves may limit or prevent recovery and must be acknowledged.

10.5.3 Any attempt to bypass security controls is undertaken only where legally authorised and technically supported.

10.6 Forensic Handling and Evidence Preservation

10.6.1 Where possible, we will always use forensic and accredited tools for handling, imaging, and recovery activities; however, sometimes other non-forensic tools may have to be used to achieve the required outcome.

10.6.2 Cryptographic hash values are generated and recorded to verify data integrity at relevant stages of recovery.

10.6.3 Full documentation of tools, versions, methodologies, and actions taken is maintained to support reproducibility and auditability.

10.6.4 Original devices are preserved wherever possible, with analysis conducted on forensic copies unless technical constraints require direct interaction.

10.7 Technical Feasibility and Limitations

10.7.1 Recovery feasibility depends on storage technology (HDD, SSD, NAND, NVMe, flash), damage severity, encryption status, and device architecture.

10.7.2 Certain recovery techniques may involve increased risk to data integrity; such techniques are only undertaken with explicit client authorisation.

10.7.3 The client acknowledges that not all data may be recoverable and that recovery success cannot be guaranteed.

10.7.4 Estimated recovery timelines may change if additional technical constraints are identified during examination.

10.8 Client Information and Context

10.8.1 Provision of relevant contextual information improves recovery effectiveness and interpretation, including:

10.8.2 Device usage patterns and timelines

10.8.3 Known deletion, corruption, or failure events

10.8.4 Relevant applications or data types of interest

10.8.5 Contextual information is used to guide recovery priorities but does not influence forensic findings.

10.9 Secure Communications and Data Transfer

10.9.1 Secure, encrypted communication channels are used for all sensitive information exchange.

10.9.2 Recovered data is transferred using agreed secure mechanisms (e.g. encrypted media, secure portals).

10.9.3 Data formats, naming conventions, and delivery methods are agreed in advance to meet client and legal requirements.

10.10 Third-Party Dependencies

10.10.1 Some recoveries may require specialist hardware, vendor cooperation, or external laboratory services.

10.10.2 Access to manufacturer documentation, firmware behaviour, or proprietary storage designs may be limited.

10.10.3 Third-party dependencies may impact recovery timelines, cost, or feasibility and are communicated as soon as identified.

10.11 Health, Safety, and Environmental Controls

10.11.1 Handling of damaged devices (e.g. swollen batteries, fire-damaged media) is subject to safety controls and may require specialist facilities.

10.11.2 Devices presenting safety risks may require stabilisation or isolation prior to forensic work.

10.11.3 Recovery may be delayed or declined if device condition presents unacceptable safety risks.

10.12 Retention and Disposal Requirements

10.12.1 Recovered data, forensic images, and documentation are retained securely for the agreed retention period.

10.12.2 At the end of retention, data is securely destroyed or returned in accordance with client instructions and regulatory requirements.

10.12.3 Disposal of devices or media is performed only with written client authorisation.

11. Exit and Offboarding

11.1.1 The Forensic Device Data Recovery Service concludes once all agreed recovery, validation, and reporting activities have been completed in accordance with the defined scope and engagement objectives

11.1.2 Service exit and offboarding are managed in a controlled and auditable manner to ensure clarity of outcomes, preservation of evidential integrity, secure handling of devices and data, and compliance with legal, regulatory, and contractual obligations.

11.1.3 No additional recovery, analysis, or advisory activities are undertaken beyond the agreed scope following service conclusion unless explicitly authorised under a new or extended engagement.

11.2 Final Deliverables

11.2.1 At service completion, the agreed deliverables are formally provided to the organisation or its authorised representative. Deliverables may include, subject to scope:

a) A forensic data recovery report detailing:

i. Device details and condition at intake

ii. Recovery objectives and scope

iii. Methods, tools, and techniques used

iv. Recovery outcomes and limitations

v. Data integrity validation results

b) Recovered data provided in agreed formats and media

c) Forensic images or working copies, where applicable

d) Chain-of-custody records and evidence handling documentation

e) Expert statements or declarations, where separately agreed

11.2.2 All deliverables are reviewed internally for quality assurance prior to release to ensure accuracy, completeness, and forensic defensibility.

11.2.3 Delivery formats, encryption requirements, and transfer mechanisms are agreed in advance to meet legal, regulatory, and operational needs.

11.3 Knowledge Transfer and Close-Out

11.3.1 Where appropriate, a formal close-out meeting is conducted with the client to review recovery outcomes, explain findings, and confirm understanding of technical limitations or evidential considerations. The close-out session may include:

a) Explanation of recovery techniques and results

b) Clarification of data integrity and validation methods

c) Discussion of evidential reliability and limitations

d) Guidance on the appropriate use of recovered data

e) Identification of potential follow-on actions or services

11.3.2 Knowledge transfer is tailored to relevant stakeholders, which may include legal counsel, investigators, compliance teams, insurers, or management, depending on engagement context.

11.4 Device Return, Retention or Disposal

11.4.1 Original devices are handled in accordance with agreed instructions following completion of recovery activities.

11.4.2 Options for device disposition include:

a) Secure return to the client or nominated third party

b) Secure storage for an agreed retention period

c) Secure destruction or disposal, subject to written authorisation

11.4.3 Any continued retention of devices beyond service completion is subject to agreed terms and may incur additional costs.

11.5 Data Handling and Retention

11.5.1 All recovered data, forensic images, working files, and documentation are handled in accordance with agreed data protection, confidentiality, and retention requirements.

11.5.2 During the engagement, data is stored in secure, access-controlled environments appropriate to its sensitivity and evidential value.

11.5.3 Following service completion, data is:

a) Securely transferred to the client or authorised recipient, and/or

b) Retained for an agreed period to support legal, regulatory, or evidential needs

11.5.4 At the end of the agreed retention period, all retained data is securely destroyed using methods appropriate to the data type and sensitivity, unless alternative instructions are received in writing.

11.6 Acceptance of Deliverables

11.6.1 Deliverables are deemed accepted once they have been formally issued and no material issues are raised within an agreed review period.

11.6.2 Requests for clarification or minor amendments may be addressed as part of service close-out. Requests for additional recovery, analysis, or rework beyond the agreed scope require a new or amended engagement.

11.7 Service Closure

11.8 The service is formally closed once the following have been completed:

a) All agreed deliverables have been provided

b) Device and data disposition has been completed

c) Retention and disposal instructions have been confirmed

11.8.1 Any further assistance required following service closure, including additional recovery attempts, expert testimony, or follow-on forensic services, is subject to a separate agreement.

*****END OF DOCUMENT*****