Digital Forensic Investigation and Acquisition Service Definition

Document title	Digital Forensic Investigation and Acquisition Service Definition		
Reference No.	IF-SER-019	**Version**	1.0
Author	Lisa Washer, Head of Cyber		
Reviewed by	Adam Whitbread, Principal Digital Forensics Analyst		
Issue date	28/01/2026		

Document Control

Version	Name	Comment	Date
0.1	Lisa Washer	Initial Draft	07/01/2026
0.2	Adam Whitbread	Review and comments	26/01/2026
0.3	Jake Blythe	Review and comments	26/01/2026
0.4	Lisa Washer	Amendments	26/01/2026
0.5	Adam Whitbread	Review and amendments	26/01/2026
1.0	Lisa Washer	Final review and publish	28/01/2026

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

Contents

1. Digital Forensic Investigation and Acquisition Service

1.1 Service Overview

1.1.1 The Digital Forensics and Acquisition Services are delivered by IntaForensics, an accredited digital forensics provider operating under a UKAS-accredited ISO/IEC 17025 quality management framework, with ISO/IEC 27001 certification for information security management. Services are delivered by qualified practitioners holding recognised professional certifications and operating in alignment with CREST and established digital forensic best practice.

1.1.2 The service provides specialist, forensically sound identification and acquisition of digital evidence from computers, mobile devices, servers, removable media, and cloud-based data sources to support investigations, litigation, regulatory enquiries, and incident response activities. All acquisition activities preserve evidential integrity, authenticity, and admissibility, with auditable chain-of-custody maintained throughout, ensuring outputs meet the expectations of courts, regulators, and legal professionals.

1.2 Service Objectives

1.2.1 The objectives of the Digital Forensics and Acquisition Services are to:

a) Acquire digital evidence in compliance with ISO/IEC 17025 forensic requirements

b) Preserve integrity, authenticity, and continuity of evidence

c) Maintain full chain-of-custody documentation suitable for legal proceedings

d) Support investigations, litigation, regulatory enquiries, and incident response

e) Deliver defensible, auditable outcomes aligned to ISO/IEC 27001 security controls

2. Service Features

2.1.1 Key features of the service include:

a) **Accredited Delivery** – UKAS-accredited ISO/IEC 17025 forensic processes

b) **Information Security Assurance** – ISO/IEC 27001-certified handling environments

c) **Forensic Soundness** – Evidence handled in line with recognised principles

d) **Validated Tooling** – Use of industry-recognised and validated forensic tools

e) **Audit-Ready Documentation** – Complete, court-ready chain-of-custody records

3. Service Benefits

3.1.1 The service provides the following benefits:

a) Evidence acquisition defensible under legal and regulatory scrutiny

b) Reduced risk of evidence contamination or challenge

c) Confidence in admissibility and integrity of digital evidence

d) Alignment with court, regulator, and law enforcement expectations

e) Assurance provided by accredited forensic and security frameworks

4. Scope of Service

4.1.1 The service is delivered in accordance with recognised forensic principles and is governed by IntaForensics' UKAS-accredited ISO/IEC 17025 laboratory framework, which defines the quality, validation, and assurance processes used within the accredited laboratory environment. For services or activities conducted outside the formal scope of accreditation, these same quality and governance processes are applied as a control framework to support consistency, transparency, and evidential defensibility. Evidence handling is aligned with the expectations of courts, regulators, and legal professionals. Where required, engagement may be coordinated through legal counsel to support legally privileged handling.

4.1.2 During the engagement scoping phase, IntaForensics will clearly identify and document which elements of the proposed examination, analysis, or reporting fall within the scope of its UKAS-accredited ISO/IEC 17025 laboratory activities and which elements sit outside the formal scope of accreditation. Any activities conducted outside the accredited scope will be explicitly declared to the client, including the tools, methods, and controls to be applied, and will be governed by IntaForensics' established quality and assurance processes. This approach ensures transparency, informed client consent, and continued evidential defensibility.

4.2 In-scope activities

4.2.1 Delivered under IntaForensics' accredited frameworks, the service includes:

a) Forensic scoping and acquisition planning

b) Identification of relevant devices, systems, and data sources

c) Forensic acquisition of desktops, laptops, servers, and storage media

d) Logical and physical imaging using validated forensic tools

e) Mobile device acquisition and extraction (where technically supported)

f) Acquisition of cloud-hosted data where lawful authority exists

g) Capture of volatile data where required and feasible

h) Integrity verification using cryptographic hashing

i) Secure handling, transport, and storage of evidence

j) Maintenance of auditable chain-of-custody records

4.2.2 All activities are performed in accordance with IntaForensics' ISO/IEC 17025-accredited procedures and ISO/IEC 27001 security controls.

4.3 Out-of-scope activities

4.3.1 Unless agreed separately, the following are excluded:

a) Substantive forensic analysis or interpretation

b) Live remediation, rebuild, or system recovery

c) Provision of legal advice or representation

d) Continuous monitoring or managed forensic services

4.4 Assumptions, Dependencies and Constraints

4.4.1 Delivery of the Digital Forensics and Acquisition Services is based on the following assumptions:

a) The client has lawful authority and a valid legal basis to identify, access, acquire, and preserve all in-scope devices, systems, accounts, and data sources.

b) Engagement is initiated promptly following identification of an incident, investigation, or legal requirement to minimise the risk of data alteration or loss.

c) Systems, devices, and data sources remain available for acquisition and have not been materially altered prior to forensic acquisition, except where required for safety, business continuity, or containment.

d) Relevant logging, audit trails, and data retention mechanisms were enabled and operational at the time of the incident or event.

e) The client will provide timely access to premises, systems, credentials (where authorised), and knowledgeable personnel to support forensic acquisition activities.

f) Any legal privilege, confidentiality, or evidential sensitivity requirements are identified and communicated at the outset or as they arise.

g) Acquisition activities can be conducted in accordance with IntaForensics' UKAS-accredited ISO/IEC 17025 procedures without deviation unless explicitly documented and agreed.

4.4.2 Service delivery is dependent on the following factors:

a) Availability and accessibility of in-scope devices, systems, cloud platforms, and storage media at the time of acquisition.

b) Cooperation from internal stakeholders, including IT, security, facilities, and operational teams, to support safe and timely access.

c) Cooperation from third-party service providers or vendors where systems or data are hosted externally or managed by third parties.

d) Stability of systems and environments to support forensic acquisition without unacceptable operational or safety risk.

e) Timely input and decision-making from client legal, compliance, and investigation stakeholders regarding scope, prioritisation, and handling requirements.

f) Availability of appropriately accredited forensic practitioners, validated tooling, and secure environments in line with ISO/IEC 17025 and ISO/IEC 27001 requirements.

4.4.3 The following constraints may impact the scope, timelines, or completeness of forensic acquisition activities:

a) Volatile data may be lost if systems are powered down, restarted, or modified before acquisition can occur.

b) Full-disk encryption, secure enclaves, or proprietary technologies may restrict acquisition without credentials, keys, or vendor assistance.

c) Physical damage, device failure, or environmental factors may limit acquisition options or completeness.

d) Acquisition activities may be constrained by business continuity, safety, or operational requirements, requiring prioritisation or staged approaches.

e) Accredited forensic practice prioritises evidential integrity, repeatability, and auditability over speed, which may affect response timelines.

f) Findings and preserved evidence represent a point-in-time snapshot and may not capture subsequent or historical changes.

g) Service delivery is subject to specialist availability, validated tool support, and agreed commercial terms.

5. Service Delivery Model

5.1 Engagement Model

5.1.1 The service is delivered on an ad-hoc consultancy basis under IntaForensics' accredited operating model. Scope, timelines, and deliverables are agreed prior to commencement, ensuring activities remain compliant with ISO/IEC 17025 requirements for controlled forensic processes.

5.1.2 Services may be delivered on-site, remotely, or via a hybrid approach. All locations and environments used for evidence handling comply with ISO/IEC 27001 information security controls.

5.1.3 All evidence is handled within ISO/IEC 27001-certified environments, using controlled access, encryption, and confidentiality safeguards. Evidence is retained only for the agreed purpose and duration.

5.2 Delivery Phases

5.2.1 Delivery typically includes:

a) Engagement initiation and accredited forensic scoping

b) Evidence identification and prioritisation

c) Forensic acquisition and integrity verification

d) Secure storage and chain-of-custody management

e) Evidence handover and engagement closure

5.2.2 Each phase is documented to support auditability and reproducibility.

5.3 Reporting and Deliverables

5.3.1 Deliverables produced under IntaForensics' accredited frameworks may include:

a) Forensic acquisition logs

b) Hash verification and validation reports

c) Chain-of-custody documentation

d) Evidence inventories and preservation summaries

5.3.2 All documentation is suitable for legal disclosure, regulatory review, and expert witness use.

6. Exit and Offboarding

6.1.1 Upon completion, evidence is securely transferred, retained, or destroyed in accordance with client instructions, legal obligations, and IntaForensics' accredited retention and disposal procedures. Access is revoked and formal closure confirmed.

7. Roles and Responsibilities

7.1 IntaForensics Responsibilities

7.1.1 IntaForensics is responsible for delivering the Digital Forensics and Acquisition Services in accordance with the agreed scope, applicable legal and regulatory requirements, and its UKAS-accredited ISO/IEC 17025 forensic quality framework and ISO/IEC 27001 information security management system**.**

7.1.2 Key responsibilities include advising on forensic acquisition strategy and proportionality; identifying and prioritising evidence sources based on volatility, relevance, and risk; and executing forensically sound acquisition of digital evidence from devices, systems, and data sources. As standard, acquisition activities are conducted using validated and accredited tools and documented procedures to ensure evidential integrity, repeatability, and admissibility.

7.1.3 In exceptional circumstances, where accredited tools are unavailable, unsuitable, or technically incapable of achieving the required outcome, non-accredited tools may be used subject to prior client agreement. Any such use is risk-assessed, fully documented, and supported by validation, verification, and transparency of method to ensure findings remain defensible and limitations are clearly understood.

7.1.4 IntaForensics is responsible for maintaining full chain-of-custody records, performing integrity verification using cryptographic hashing, and ensuring secure handling, transport, and storage of evidence within ISO/IEC 27001-certified environments. All actions, assumptions, limitations, and deviations from standard procedures are fully documented to support auditability and legal scrutiny. IntaForensics will provide regular status updates and will promptly escalate risks, access issues, or factors that may impact evidential integrity, timelines, or scope.

7.2 Client Responsibilities

7.2.1 The client is responsible for confirming lawful authority and legal basis to access, acquire, and retain in-scope digital evidence. This includes identifying relevant devices, systems, accounts, custodians, and locations; facilitating timely access to premises, infrastructure, and personnel; and ensuring internal stakeholders cooperate with forensic activities.

7.2.2 The client retains responsibility for defining investigation scope, legal strategy, and subsequent use of acquired evidence. The client is also responsible for decisions relating to system shutdowns, containment actions, business continuity measures, or remediation activities that may affect forensic acquisition. Where required, the client will review and approve acquisition plans, receive custody of acquired evidence, and determine retention or disclosure requirements.

7.3 Legal Counsel Responsibilities (Where Applicable)

7.3.1 Where internal or external legal counsel is engaged, legal counsel is responsible for advising on evidential requirements, legal privilege, disclosure obligations, and admissibility considerations. Legal counsel may instruct or oversee forensic acquisition activities, approve scope and prioritisation, and ensure that acquisition and documentation support use in legal or regulatory proceedings. Legal counsel may also coordinate legally privileged handling of communications and outputs.

7.4 IT, Security, and Operational Stakeholders (Where Applicable)

7.4.1 IT, security, and operational stakeholders are responsible for supporting safe and effective access to systems, devices, and environments. This includes providing technical knowledge of systems, assisting with credentials or access mechanisms where authorised, and advising on operational, safety, or business continuity risks. These stakeholders support acquisition activities while ensuring that organisational security and operational requirements are appropriately managed.

7.5 Joint Responsibilities

7.5.1 IntaForensics and the client share responsibility for effective communication, timely decision-making, and escalation of issues that may impact evidential integrity, operational impact, legal obligations, or delivery timelines. All parties are responsible for maintaining confidentiality, supporting transparency and auditability, and ensuring that digital forensic acquisition activities are conducted proportionately, defensibly, and in alignment with applicable legal, regulatory, and accreditation requirements.

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