NEDERLANDS
REGISTER
GERECHTELIJK
DESKUNDIGEN

Standards
Digital Forensics
(008.1 - 008.3)

Version:	3.8
Date of approval:	###
Date of effect:	###

Contents

Part I. General Introduction to Standards

§ 1. Background to and aim of the Standards

Reporting forensic experts play a crucial role in the administration of justice. The NRGD aims to ensure justified confidence in forensic expertise for stakeholders. This confidence must be based on the demonstrable independently safeguarded quality of forensic investigators and their reports on the basis of (inter)national forensic-specific standards.

The NRGD is managed by the Board of Court Experts (hereinafter: Board). The Board has the legal duty to manage a public register of forensic experts who do comply with the Board's registration requirements. The registration requirements have been laid down in concordance with the field of expertise and have been demarcated in specific Standards per field of expertise. This is important in order to inform applicants, assessors and users of the register (e.g. judge, public prosecutor and attorney) about the activities an expert in the field of expertise in question engages in and about the activities that fall outside the field of expertise. The demarcation of the field of expertise is set out in Part II of these Standards.

The Board also determines the criteria on the basis of which an assessment is made for each field of expertise as to whether an application complies with the quality requirements. The generic requirements are set out in the Register of Court Experts in Criminal Cases Decree (Besluit register deskundige in strafzaken). These requirements are elaborated further for each field of expertise. This elaboration is set out in Part III of these Standards.

Furthermore the Board determines the assessment procedure. This procedure is described in Part IV of these Standards.

The NRGD has a system of periodic repeat registration. Court experts must demonstrate every four years that they still meet the requirements in force at that time. The Standards are dynamic and are being developed further in order to enhance the quality of the experts. These Standards set out the current state of the (sub-)field of expertise.

§ 2. Types of applications

The NRGD distinguishes two types of applications: the application for initial registration and the application for reregistration. The application for initial registration is submitted by an expert who at the time of submission of the application is not yet registered in the register for the field of expertise to which the application relates. The application for reregistration is submitted by an expert who is already registered in the register for the field of expertise to which the application relates.

These two types of applications are subdivided as follows:

Application for initial registration:

(i) independent expert: an expert who has independently written and signed the required number of case reports;
(ii) expert without work of his own: an expert who has not independently written and signed the number of case reports required for registration.

If the assessment is favourable, the expert without work of his own will only qualify for provisional registration.

Application for reregistration:

(i) after full registration;
(ii) after provisional registration.

The application for initial registration is submitted by an expert who at the time of submission of the application does not have a NRGD registration. This might be:
- the independently reporting expert;
- the newly trained expert;
- the expert whose earlier application has been rejected by the Board;
- the expert whose registration was previously stricken.

In respect of applications for initial registration, it is necessary to make a clear distinction between the independent expert and the expert without work of his own. An example of an expert without work of his own is the newly trained expert. This expert has completed the forensic training (training on drawing up forensic reports), but has not yet been able to independently write the number of reports required for the assessment because these are written under the supervision of a tutor during the training. Another example of an expert without work of his own is the expert whose earlier application was rejected and who has been working (partly) under supervision following this rejection.

The Board adopts the following principle. Every applicant must draw up a List of Case Information. This list must include a specific number of cases in a period specified by the Board immediately preceding the application. If the List of Case Information includes one or more cases which have been prepared under supervision, the applicant will be qualified as an ‘expert without work of his own’. Additional requirements apply to the applicant whose application was rejected earlier: the case reports must have been drawn up after the date of the Board’s decision rejecting the earlier application (Policy Framework for Application after Rejection).

The distinction between the various types of applications for reregistration is important in the context of the assessment procedure: the documents an expert must submit, the composition of the Advisory Committee for Assessment and the assessment method.

§ 3. Justification of Standards

The draft of these Standards has been published on the NRGD website for public consultation. These Standards have been established by the Board in accordance with the Register of Court Experts in Criminal Cases Decree (Besluit register deskundige in strafzaken).

§ 4. Validity of Standards

The Standards are valid from the date shown on the cover. The validity runs until the moment of publication of a new version. In principle it will be checked annually as being up to date. This check can lead to a new version. The aim is to publish the new version no more than once a year. Intermediate alterations can be incorporated in an addendum, which will be published on the NRGD website as well.

§ 5. Version management and formal revision history

All changes made to the Standards lead to a new version. Newer versions of (parts of) the Standards are designated with a higher version number.

5.1. Version management

In the case of editorial changes, the version number is increased by 0.1. Editorial changes have no substantive impact. In the case of substantive changes, the version number is increased by 1.

5.2. Formal revision history

The revision history starts with version 1.0 as the first formally approved version. Substantive changes made are briefly described in the revision history (Annex C). This makes it possible to trace at all times which Standards are valid at any given moment.

Part II. Demarcation of Digital Forensics

§ 1. Introduction

Experts within the Digital Forensic field investigate and examine;

> hardware (including mobile phones, laptops, USB drives, servers and routers); software (including operating systems, applications, and files); or a combination of both, to answer forensic questions.

Digital Forensic Science covers all manifestations (input, output and processing) of digital items[1]. Items appear in various forms, and Digital Forensic Science faces an increasing diversity of items submitted for examination.

Digital forensic investigations develop during the investigative phase of the inquiry, and digital forensic examinations during the evaluative phase of the inquiry.

Expertise is typically required within three phases:
Recovery (securing data),
Analysis (processing data to obtain observations),
Interpretation (infer the meaning of observations).

These steps encompass various forensic activities essential for the validity and reliability of the investigations and examinations and the integrity of the criminal justice chain.

These three steps are derived from the description of the forensic process in the "ISO international standard 21043 forensic sciences" and selected NIST Special Publications[2] related to digital forensic science. This integrated approach ensures that the terminology and structure used are both methodologically and technically accurate and aligned with internationally recognized frameworks. By harmonizing elements from multiple sources, the document aims to provide clarity, consistency, and practical applicability within the field of digital forensic science.

The three steps of the digital forensic investigation and examinations use verified or validated methods. Methods shall be verified or validated using digital systems and realistic scenarios for which the ground truth is known.

The steps are designed to follow procedures that comply with the legal framework, preserve the integrity of the data and the chain of custody. They are defined as follows:

- **Recovery**: recognition, collection, acquisition and preservation of potential digital evidence.
- **Analysis**: processing, measuring and/or comparing properties of data (e.g., emails, chat messages, pictures, but also log files), in order to obtain observations. Analysis can be instrumental, human-based, or a combination of the two.
- **Interpretation**: infer the meaning of observations, in order to provide expert opinions with respect to forensic questions asked. This is based on professional

[1] A list of definitions is included on page 27 (Annex A)
[2] SP 800-86, Guide to Integrating Forensic Techniques into Incident Response | CSRC

judgement, logic, expertise, relevant data, contextual information and, if applicable, statistical models.[3]

An expert is expected to demonstrate competence (knowledge, skill and experience) in one or more of these steps, particularly in relation to the increasing diversity of items recovered during investigation or submitted for examination.

The type of questions of the commissioning party depends on the phase which the digital forensic examination has reached.

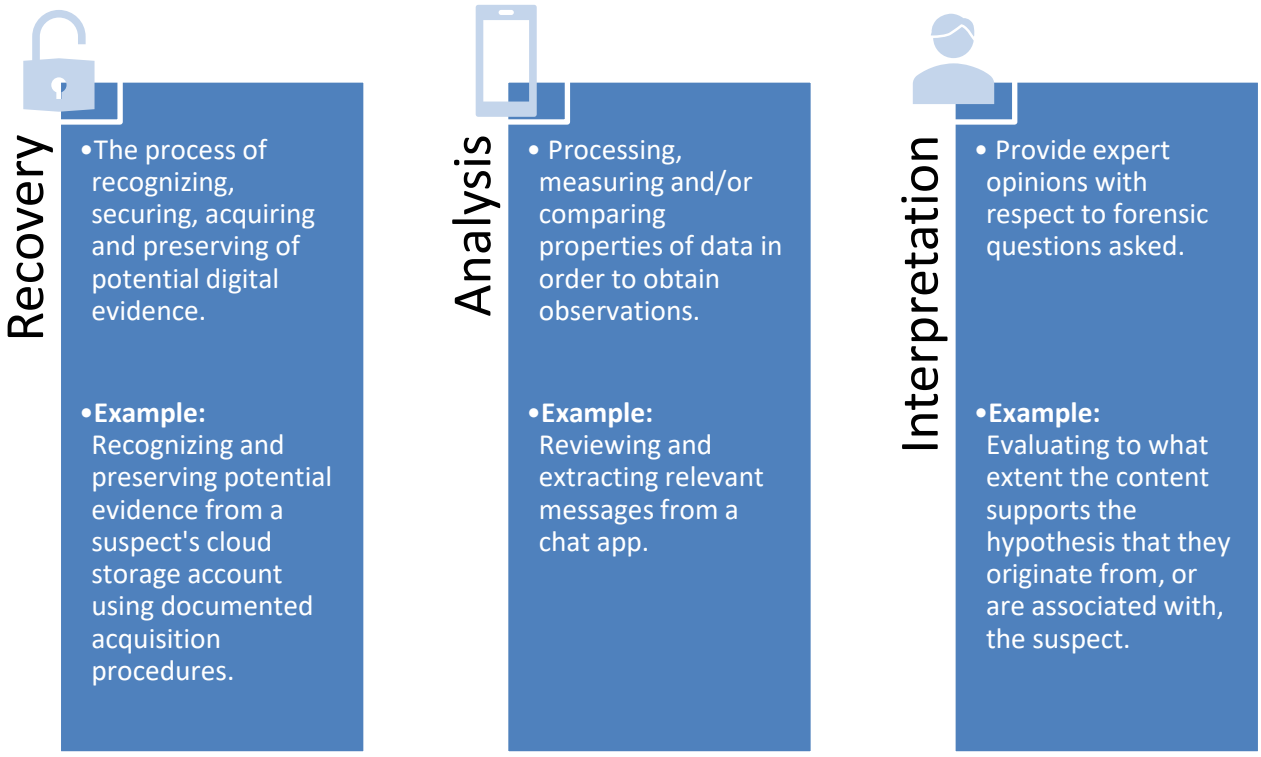

Figure 1: Examples of the different forensic phases.

§ 2. Relevant questions

The type of forensic questions and the phase of the inquiry (investigation or evaluation) determine what needs to be undertaken, how far the work should go, and how it should be carried out. This includes choosing the right methods, checking if they are suitable and reliable for the case, and making sure they meet legal requirements.

1.1 Questions in the subfield of data recovery

The recovery phase refers to the systematic process recognizing, collecting, acquiring and preserving of potential digital evidence e.g. digital items or data carriers, typically at the scene or during the investigative phase. This definition aligns with the scope of digital

[3] Combination of ISO/DIS 41043 and NIST 800-86

forensic recovery and does not refer to the technical restoration of deleted, corrupted, or lost data from storage media.

The following questions - amongst others - are relevant for the recovery phase:

- Does the item submitted for analysis contain data?
- Can the data be extracted from the item?
- Is the collected data relevant to fulfil the request?
- Is the recovered data suitable for analysis?

2.2 Questions in the subfield of data analysis

The following questions - amongst others - are relevant for the analysis phase:

- Are data/observations available to answer the forensic question at hand:
    - Who / what is the source of the data?
    - What is the quantity of data?
    - How the reconstruction information (location, time, sequence) contained in the data inform about the activities?

Which / how / when data been stored, accessed, modified, changed, exchanged?

2.3 Questions in the subfield of interpretation

This phase is about assessing the strength of evidence, based on the forensic question, the observations, and alternative propositions in the case.

The following questions - amongst others - are relevant for the interpretation phase:

- Do these log entries suggest normal use, or do they indicate possible tampering?
- What does the phone activity in the week prior to the incident reveal about how it was used?
- What is the significance of this search term being entered at that specific time?
- Is it possible to delete a message in this manner without having physical access to the device?

The following questions in the table below, provide examples of how observations can be interpreted when two or more alternative propositions are formulated. This comparative structure is aligned with the Likelihood Ratio (LR) framework, which is commonly used to assess the strength of evidence by evaluating the support for different propositions. Experts are not required to always formulate alternative propositions. The use of this comparative framework should be guided by the nature of the case and the specific forensic question posed.

If an expert applies the Likelihood Ratio (LR) framework in their analysis, the questions could be structured as follows, where alternative propositions are compared to assess the strength of the evidence:

Type of Question	*Subcategory*	*Main Question*	*Note*
Questions of Source	**What**	What is the degree of support for the observations if the source is item 1 vs. item 2?	
	Who	What is the degree of support for the observations if the source is person 1 vs. person 2?	May include aspects related to the person's level of knowledge.
Questions of Reconstruction	**Activity**	What is the degree of support for the observations if activity 1 took place vs. activity 2?	
	Location	What is the degree of support for the observations if the activity took place in location 1 vs. 2?	
	Time	What is the degree of support for the observations if the activity took place at time 1 vs. time 2?	
	Sequence	What is the degree of support for the observations if the activity occurred in sequence 1 vs. 2?	

Table 1: Examples of how observations can be interpreted

§ 3. Core activities

An expert is expected to demonstrate competence (knowledge, skill and experience) in one or more of these phases, particularly in relation to the increasing diversity of items recovered during investigation or submitted for examination.

3.1. Recovery

Recovery involves the correct preservation (e.g. by copying) of digital data sources including possible steps to bypass security or encryption mechanisms. Collection either means securing the original or taking a forensic copy of the data. Preservation implies the digital evidence is preserved so that it can be collected later (if necessary). For example, a company can be asked to preserve existing backup tapes by ensuring they are no longer recycled. If necessary, they can be collected later.

In this phase an expert must be familiar with the various recovery options, and must be able to assess which recovery option should be applied to a specific case. The expert

must also have knowledge of the possible locations where evidence might be found. Finally, the expert needs to know what knowledge and/or skills are required in order to safeguard evidence and minimise the impact on the source material.

Tasks:

- **Forensic question formulation**: Defining and recording the specific forensic question to be answered, based on the context of the case and applicable legal boundaries. This ensures that the scope of the recovery process remains proportionate and legally sound, and helps guide the selection and acquisition of relevant data sources.
- **Detection and selection**: The growing use of digital technology has created many sources of data. An expert shall be able to detect and accordingly to investigate which data should be selected.
- **Preservation:** The process of maintaining and safeguarding the integrity and authenticity of digital evidence from the time it is collected until it is presented.[4] This can mean, for example, that a laptop is kept on power during the transport to a laboratory. This also includes the secure long-term storage of digital evidence or forensic copies, ensuring that integrity is maintained and that data remains available for subsequent analysis, review, or legal proceedings.
- **Acquisition**: Conducted in a forensically sound manner, ensuring that the original data remains unchanged and that the acquired copy can be verified as accurate and complete through the use of cryptographic hash functions.[5] Initially acquisition is preferably done without altering the original data. In certain investigations there is no other alternative, e.g. chip-off techniques require to remove the chip from the evidence to implement a read out of the data and live imaging techniques require access to active devices on which data might change during acquisition.

3.2. Analysis

Involves the forensic processing of collected data using a combination of automated and manual methods. The expert isolates, examines, and organizes data features or patterns of potential relevance, while preserving the integrity of the data throughout the process. Depending on the case, the expert may conduct test-based procedures or simulations to explore hypotheses. In this phase, the expert distinguishes between potentially relevant and irrelevant data and prepares observations for subsequent interpretation.

The expert may use a variety of analysis techniques, including data correlation, pattern recognition, statistical methods, or other domain-specific tools, depending on the case. These techniques help identify meaningful patterns and correlations within the data, aiding the expert in distinguishing between relevant and irrelevant data.

Tasks:

- **Use standardized protocols**: Adhere to established forensic examination protocols to ensure that the examination process is consistent and standardized.
- **Assess quality and relevance**: Both the quality of the observations and their relevance determine the potential for the observations to answer the forensic question at hand. This phase may also involve bypassing or mitigating OS or application features that obscure data and code, such as data compression,

[4] ISO/IEC 27037
[5] ISO/IEC 27037

encryption, and access control mechanisms. For example, a certain log might hold millions of records, but only five of the records might be related to the event of interest.

3.3. Interpretation

Involves the reasoned assessment of the meaning and probative value of observations derived from digital data. This phase requires the expert to apply a clearly defined and validated methodology to assess the strength of the evidence in light of the forensic questions posed and hypotheses at hand.

The methods used for interpretation may be human-based, automated, or a combination of both. In all cases, they must be:

- validated,
- calibrated,
- and, where possible, operator-independent (i.e., yielding consistent results regardless of the analyst).

The expert must also take appropriate steps to reduce bias, such as using structured interpretation frameworks, scenario-based evaluation, or blind verification.

Tasks:

- **Designing or selecting** the appropriate interpretative approach for the question at hand.
- **Assessing how strongly the observations support** or refute one or more hypotheses.
- **Reporting a substantiated expert opinion**: including limitations and alternative explanations where applicable.

3.4 Reporting

For all phases the standards of reporting are the same.

- Reports shall be accurate, clear, transparent, complete, unambiguous, impartial, and suitable for their intended use.
- Experts shall not report beyond their area of expertise.
- Experts shall not report beyond what can be based on the available information.
- Known limitations of methods, procedures, observations, and opinions, should be stated clearly in the report or in an appendix attached to the report. If the limitations are not stated in the report or in an appendix to the report it shall be stated that the information on the limitations is available and shall be provided upon request.[6]

§ 4. Methodology

The different phases require different methodology.

Recovery: The expert employs validated forensic acquisition techniques to create reliable, forensically sound copies of digital evidence. These could include physical imaging (bit-for-bit copies of storage media) or logical imaging (file-level copies), aided by

[6] ISO international standard 21043 forensic sciences

write-blockers and integrity checks (e.g., cryptographic hashes). The expert's methodology is expected to follow guidelines from ISO/IEC 27037:2012 (recognition, collection, acquisition)**.** Use of new or proprietary acquisition tools requires pre-validation with reference devices or test systems to ensure accuracy and reproducibility before deployment in the actual case.

Analysis: The expert systematically processes and examines the acquired digital evidence. This involves using forensic tools[7] to parse file systems, extract metadata, reconstruct timelines, and correlate artifacts across data sources (e.g., chats, logs, network captures). The methodology adheres to both ISO/IEC 27037, which provides practical guidance on the handling and acquisition of digital evidence, and ISO 21043, which outlines the methodological and quality requirements for forensic examination and analysis. Analysts are required to validate any custom parsing or data-extraction techniques on test systems and reference data prior to live casework, ensuring consistency, accuracy, and defensibility in legal proceedings.

Interpretation: Since different questions may require different approaches, the expert can adopt different models; e.g. Likelihood Ratio, story-based models or argumentation-based models, Part of the expertise is to extend a known or a newly developed methodology to a new case. This phase of the forensic process is guided by ISO 21043, which provides methodological principles for evaluating the strength of evidence, comparing alternative propositions, and ensuring transparency and accountability in expert reasoning.

§ 5. Boundaries of the field of expertise

An expert needs to be able to determine the limits of their expertise and act accordingly. This means that an expert must be able to recognise immediately that their own expertise or specialism is not adequate to carry out the digital forensic examination.

Interpretation that extends outside of the digital forensic science discipline shall be undertaken in a multidisciplinary manner, bringing together experts from the relevant disciplines. Examples of activities that emphatically do not come under the Digital Forensics field of expertise are:

- Address the question of source for persons and objects depicted in images of movies.
- Intelligibility enhancement of speech audio recordings.
- Investigation and examination of electronic analogue circuits.
- Measurements of properties of objects in images or movies (e.g. photogrammetry to estimate the position/velocity of a vehicle) (image) fragments.
- Crime scene visualisation.

§ 6. Registration

6.1. Registration

The register lists the expert concerned as an expert in the field of Digital Forensics.

[7] For definitions see Appendix A

6.2 Defined subfields

In the context of digital forensic investigation and examination, expertise is typically required across three steps: recovery, analysis and interpretation. These steps encompass various forensic activities essential for the integrity of the criminal justice chain. These subfields are based on the description of the forensic process in the "ISO international standard 21043 forensic sciences" and selected NIST Special Publications[8] related to digital forensic science.

008.1 Digital Forensics – Recovery
008.2 Digital Forensics – Analysis
008.3 Digital Forensics – Interpretation

[8] SP 800-86, Guide to Integrating Forensic Techniques into Incident Response | CSRC

Part III. Registration requirements for Digital Forensics

The general (repeat) registration requirements are given below in italics with a reference to article 12 paragraph 2 in the Register of Court Experts in Criminal Cases Decree (Besluit register deskundige in strafzaken).

The second paragraph of article 12 of the Register of Court Experts in Criminal Cases Decree states:
An expert will only be registered as an expert in criminal cases upon submission of the application if, in the opinion of the Board, the expert:

a. has sufficient knowledge and experience in the field of expertise to which the application relates;
b. has sufficient knowledge of and experience in the field of law concerned, and is sufficiently familiar with the position and the role of the expert in this field;
c. is able to inform the commissioning party whether, and if so, to what extent the commissioning party's question at issue is sufficiently clear and capable of investigation in order to be able to answer it on the basis of their specific expertise;
d. is able, on the basis of the question at issue, to prepare and carry out an investigation plan in accordance with the applicable standards;
e. is able to collect, document, interpret and assess investigative materials and data in a forensic context in accordance with the applicable standards;
f. is able to apply the current investigative methods in a forensic context in accordance with the applicable standards;
g. is able to give, both orally and in writing, a verifiable and well-reasoned report on the assignment and any other relevant aspects of their expertise in terms which are comprehensible to the commissioning party;
h. is able to complete an assignment within the stipulated or agreed period;
i. is able to carry out the activities as an expert independently, impartially, conscientiously, competently, and in a trustworthy manner.

In this document, the following verbal forms are used:
— "shall" indicates a requirement;
— "should" indicates a recommendation;
— "may" indicates a permission;
— "can" indicates a possibility or a capability.

§ 1. Article 12(2) sub-paragraph a

(…) has sufficient knowledge and experience in the field of expertise to which the application relates.

1.1 Application for initial registration: independent expert

Basic requirements:	-	have at least 3 years of relevant work experience at the level of an academic Master's Degree preferably in the field of technical IT;
	or	

- have at least 5 years of relevant work experience at the level of an academic Bachelor's Degree preferably in the field of technical IT;

and

- be familiar with the summary of concepts (see annex A) and keep abreast of state of the art developments;
- keep up to date with technological and other developments in the field and taking active steps to maintain competence;
- be aware of fundamental principles of forensic investigations (e.g. crime scene investigation, chain of custody, principles of evidence);
- have adequate knowledge of the collection, examination and analysis of data.

Specific requirements:

- have drawn up at least 5 case reports not older than 5 years which have been subjected to collegial review;
  In case the applicant is also acting as a supervisor or reviewer, at least 3 reports on the List of Case Information should be independently prepared reports.
- have spent an average of 40 hours a year over the past 5 years on forensically relevant professional development (e.g. attending conferences, running or attending courses, publications).

1.2 Application for initial registration: expert without work of his own

Basic requirements:

- have at least 3 years of relevant work experience at the level of an academic Master's Degree preferably in the field of technical IT;

or

- have at least 5 years of relevant work experience at the level of an academic Bachelor's Degree preferably in the field of technical IT;

and

- be familiar with the summary of concepts (see annex A) and keep abreast of state of the art developments;
- keep up to date with technological and other developments in the field and taking active steps to maintain competence;
- be aware of fundamental principles of forensic investigations (e.g. crime scene investigation, chain of custody, principles of evidence);
- have adequate knowledge of the collection, examination and analysis of data.

Specific requirements:	- have drawn up at least 3 case reports not older than 2 years which have been subjected to collegial review and/or supervision; - have spent an average of 40 hours a year over the past 2 years on forensically relevant professional development (e.g. attending conferences, running or attending courses, publications).

1.3 Application for reregistration: after full registration

Basic requirements:

- have at least 3 years of relevant work experience at the level of an academic Master's Degree preferably in the field of technical IT;

or

- have at least 5 years of relevant work experience at the level of an academic Bachelor's Degree preferably in the field of technical IT;

and

- be familiar with the summary of concepts (see annex A) and keep abreast of state of the art developments;
- keep up to date with technological and other developments in the field and taking active steps to maintain competence;
- be aware of fundamental principles of forensic investigations (e.g. crime scene investigation, chain of custody, principles of evidence);
- have adequate knowledge of the collection, examination and analysis of data.

Specific requirements:

- have drawn up at least 5 case reports not older than 5 years which have been subjected to collegial review;
  In case the applicant is also acting as a supervisor or reviewer, at least 3 reports on the List of Case Information should be independently prepared reports.
- have spent an average of 40 hours a year over the past 5 years on forensically relevant professional development (e.g. attending conferences, running or attending courses, publications).

1.4 Application for reregistration: after provisional registration

Basic requirements:

- have at least 3 years of relevant work experience at the level of an academic Master's Degree preferably in the field of technical IT;

or

- have at least 5 years of relevant work experience at the level of an academic Bachelor's Degree preferably in the field of technical IT;

and

- be familiar with the summary of concepts (see annex A) and keep abreast of state of the art developments;
- keep up to date with technological and other developments in the field and taking active steps to maintain competence;
- be aware of fundamental principles of forensic investigations (e.g. crime scene investigation, chain of custody, principles of evidence);
- have adequate knowledge of the collection, examination and analysis of data.

Specific requirements:	- have drawn up at least 2 case reports not older than 2 years which have been subjected to collegial review; *In case the applicant is also acting as a supervisor or reviewer, at least 1 report on the List of Case Information should be independently prepared reports.* - have spent an average of 40 hours per year during the registration period on forensically professional development (e.g. attending conferences, running or attending courses, publications).

1.5 Application after rejection or after legally expired registration

In accordance with the policy framework 'Application after Rejection', registration requirements listed above under Application for Initial Registration apply for experts whose registration has been rejected by the Board in an application procedure or for experts whose registration has legally expired within the previous two years. Exclusively reports written after the date of the rejection will be assessed. Additionally, also reports of supervision and/or collegial review will be included in the assessment (see also Part IV).

§ 2. Article 12(2) sub-paragraph b

(…) has sufficient knowledge of and experience in the field of law concerned, and is sufficiently familiar with the position and the role of the expert in this field.

- In general an applicant should have adequate knowledge of Dutch criminal law:
  - context of criminal law:
    - Trias Politica, distinction between civil law, administrative law and criminal law.
  - criminal law procedure:
    - pre-trial investigation;
    - coercive measures;
    - stages of the proceedings;
    - actors in the criminal justice system (tasks/powers/responsibilities);
    - regulations concerning experts laid down in the Dutch Code of Criminal Procedure (position and powers of commissioning party, legal position of expert, position and powers of lawyer, forms of counter-analysis, register of experts in the context of criminal law);
    - legal decision-making framework of the court in criminal cases (decision-making schedule laid down in Section 350 of the Dutch Criminal Code of Procedure), also with a view to the relevance of the commission to the expert and to the question at issue;
    - course of the criminal trial;
    - position of the expert in the court procedure.
  - substantive criminal law:
    - sanctions and grounds for exemption from criminal liability (very basic).
  - knowledge of the legal context of safeguarding the quality of the expert and the analysis/investigation:
    - position and role of the co-operating organisations in the criminal justice system in safeguarding the quality of the reports;
    - professional codes and relevant regulations in relation to the NRGD Code of Conduct.

§ 3. Article 12(2) sub-paragraph c

(…) is able to inform the commissioning party whether, and if so, to what extent the commissioning party's question at issue is sufficiently clear and capable of investigation in order to be able to answer it on the basis of their specific expertise.

The applicant shall:
- have sufficient knowledge of the principles of related fields of expertise, including the other digital forensics specialisms and the boundaries of the field and to be able to adequately refer the commissioning party when relevant;
- demonstrate an awareness of his own limitations, and ensures he does not stray into evaluative work which he is not competent to undertake;
- be able to define the specific forensic question to be answered, based on the context of the case and applicable legal boundaries;
- be able to inform the commissioning party if on the basis of his specific expertise the commissioning party's questions should be adjusted in order to benefit the digital forensic examination.

§ 4. Article 12(2) sub-paragraph d, e and f

d. (…) is able, on the basis of the question at issue, to prepare and carry out an investigation plan in accordance with the applicable standards.
e. (…) is able to collect, document, interpret and assess investigative materials and data in a forensic context in accordance with the applicable standards.
f. (…) is able to apply the current investigative methods in a forensic context in accordance with the applicable standards.

An applicant shall:
- be able to check the reliability of the tools and use tools and techniques appropriately;
- be able to ensure that the tools are appropriate to the task in hand and that the applicant themselves is competent to use them;
- if the applicant is using tools they have developed or commissioned themselves, they should be able to demonstrate a specification, design and evaluation process that clearly identifies their limitations in a way that is intelligible to non-specialists;
- be able to make defensible judgments about the respective weights to be attached to different findings;
- be able to sufficiently demonstrate proper logging and documenting the handling of items in a way that can be audited and permits the process to be repeated if appropriate;
- be able to reconsider the work done in the light of new findings and information;
- be able to identify alternative explanations of the material.

An applicant should:
- be aware of the uses and limitations of any tools that have been employed previously in the investigation;
- be able to demonstrate a methodical approach to the selection of their own forensic software tools;
- be able to demonstrate the ability to compare software and hardware tools sufficient to detect and identify the limitations of, and discrepancies between, the tools the applicant uses;

- be aware of the pros and cons of various scientific methods used in the field, be aware of and be able to explain the possibilities and limitations of these methods and follow up on developments thereof;
- be aware of the reliance on the available hypotheses and be able to develop alternative hypotheses.

Specifically for Recovery, an applicant shall:
- be able to correctly acquire and preserve (e.g. by copying) digital data sources and safeguarding the integrity and authenticity of digital evidence from the time it is collected until it is presented[9];
- be familiar with the various recovery options and be able to assess which recovery option should be applied to a specific case;
- have knowledge of the possible locations where evidence might be found;
- be able to decide reliably when something is likely to be of evidential value. The applicant should select and prioritise logically and be able to explain why he focused on specific traces (out of many more).

Specifically for Analysis, an applicant shall:
- be able to decide reliably when something is likely to be of evidential value. The applicant should select and prioritise logically and be able to explain why he focused on specific traces (out of many more);
- be able to isolates, examines, and organizes data features or patterns of potential relevance, while preserving the integrity of the data throughout the process;

Specifically for Interpretation, an applicant shall:
- be able to apply a clearly defined and validated methodology to assess the strength of the evidence in light of the forensic questions posed and hypotheses at hand;
- take appropriate steps to reduce bias, such as using structured interpretation frameworks, scenario-based evaluation, or blind verification;
- be able to design or select the appropriate interpretative approach for the question at hand;
- be able to assess how strongly the observations support or refute one or more hypotheses.

§ 5. Article 12(2) sub-paragraph g

(…) is able to give, both orally and in writing, a verifiable and well-reasoned report on the assignment and any other relevant aspects of their expertise in terms which are comprehensible to the commissioning party.

An applicant should:
- be able to place appropriate emphasis on showing good judgment on how much technical detail to include or omit;

An applicant shall:
- be able to communicate an understanding of the technical issues, processes and procedures involved to others (including non-specialist) understandable and clearly in a way that avoids misunderstanding;

[9] ISO/IEC 27037

- be able to write a report that is accurate, clear, transparent, complete, unambiguous, impartial, and suitable for their intended use.
-
- be able to explain what actions have been undertaken in order to validate the techniques used;
- make it clear in the report when he is referring to opinions of others;
- structure his report so as to distinguish clearly between evidential fact (demonstrated or assumed), inference and opinion;
- clearly state the assumptions made in a case by themselves;
- be aware where they give general technical explanations, to make sure that these are adequately related to the specific operating system or file system;

Apart from the required administrative data (name of commissioning party, date of commission, date of report, reference commissioning party, own reference, number and type of appendices etc.) a digital forensics report contains the following information:

- description of the items received, with information on the date and manner of submission, whether originals were received or copies. Any other conditions of the items that might be relevant for the examination and analysis are mentioned as well;
- specification of questioned and reference items;
- question(s) asked by the commissioning party and, if necessary, all that has been discussed between the commissioning party and the examiner in conformity with Article 12 (2) c;
- any relevant background information which could influence the interpretation of the items;
- the method(s) used;
- results of the investigation;
- conclusions.

§ 6. Article 12(2) sub-paragraph h

(…) is able to complete an assignment within the stipulated or agreed period.

§ 7. Article 12(2) sub-paragraph i

(…) is able to carry out the activities as an expert independently, impartially, conscientiously, competently, and in a trustworthy manner.

An applicant should:

- comply with the NRGD Code of Conduct determined by the Board of Court Experts and published on the website of the NRGD.

§ 8. Hardship clause

If the applicant wants the Board to make an exception for him on the grounds of what is set out above, for example because the applicant does not yet (fully) comply with the requirement of article 12 (2) under a of the Decree, the applicant must submit a request for exception to the Board. The substantiated request must be submitted as an accompanying letter with the (repeat) application.

Part IV. Assessment procedure for Digital Forensics

§ 1. General

In all fields of expertise the assessment will be based on the written information provided, including as a minimum requirement case reports and items of evidence, supplemented in principle with an oral assessment. However, such an oral assessment will not be necessary if the applicant's expertise has already been clearly demonstrated by the written information.

The assessment will in principle be carried out on the basis of the information provided by the applicant:

- general information as part of the application package;
- documentary evidence of competence.

If it is felt necessary in the context of the assessment an additional case report and/or information, for example information about the way collegial review and/or supervision is organized within the organization, can be requested.

§ 2. Assessment procedure per type of application

2.1. Application for initial registration: independent expert

Documents to be submitted:

- NRGD application form;
- Certificate of Good Conduct (not older than 3 months);
- A clearly legible copy of a valid passport or identity card;
- Copies of documents relating to the highest level of professional qualification;
- A curriculum vitae (CV), preferably in English;
- Documentary evidence of the current academic working level, and proof of being an expert authorised to sign (if applicable);
- Overview Continuing Professional Development Digital Forensics;
- List of Case Information Digital Forensics;
- 3 case reports drawn up in the past 5 years selected by the applicant from the List of Case Information. For each subfield the applicant should have at least 2 case reports. When several subfields are combined in one case report, it is possible to provide the same case report for different subfields (008.1 – 008.3). If possible the case reports should also contain the testimony delivered in court. *The case reports should provide a clear and broad picture of the applicant's competencies. Subsequently, only independently written reports can be submitted.*
- If available:
  - proof of the forms of professional development referred to in the Overview Continuing Professional Development Digital Forensics;

- a statement concerning the level of accreditation of the applicant's working environment, where applicable.

Assessment method:
phase a. administrative, by the NRGD Bureau;
phase b. substantive, by an Advisory Committee for Assessment (ACA) made up of at least three people on the basis of the available written material, including possible supplementary written information. In principle this ACA consists of a legal assessor and two subject-matter assessors;
phase c. substantive, by same the ACA by means of an oral assessment. This oral assessment will be waived if the applicant's expertise has already been clearly established in phase b;
phase d. decision by the Board: registration, provisional registration or no registration.

2.2. Application for initial registration: expert without work of his own

Documents to be submitted:
- NRGD application form;
- Certificate of Good Conduct (not older than 3 months);
- A clearly legible copy of a valid passport or identity card;
- Copies of documents relating to the highest level of professional qualification;
- A curriculum vitae (CV), preferably in English;
- Documentary evidence of the current academic working level, and proof of being an expert authorised to sign (if applicable);
- Overview Continuing Professional Development Digital Forensics;
- List of Case Information Digital Forensics;
- 3 case reports drawn up in the past 2 years selected by the applicant from the List of Case Information. For each subfield the applicant should have at least 2 case reports. When several subfields are combined in one case report, it is possible to provide the same case report for different subfields (008.1 – 008.3). If possible the case reports should also contain the testimony delivered in court. *The case reports should provide a clear and a broad picture of the applicant's competencies.*
- If available:
  - proof of the forms of professional development referred to in the Overview Continuing Professional Development Digital Forensics;
  - a statement concerning the level of accreditation of the applicant's working environment, where applicable.

Assessment method:
phase a. administrative, by the NRGD Bureau;
phase b. substantive, by an Advisory Committee for Assessment (ACA) made up of at least three people on the basis of the available written material, including possible supplementary written information. In principle this ACA consists of a legal assessor and two subject-matter assessors;
phase c. substantive, by the ACA specified at b. by means of an oral assessment. This oral assessment will be waived if the applicant's expertise has already been clearly established;
phase d. decision by the Board: provisional registration or no registration.

2.3. Application for reregistration: after full registration

Documents to be submitted:
- NRGD application form;
- Certificate of Good Conduct (not older than 3 months);
- Copies of documents relating to the highest level of professional qualification (if changed);
- An updated curriculum vitae (CV), preferably in English;
- Overview Continuing Professional Development Digital Forensics;
- List of Case Information Digital Forensics;
- 2 case reports drawn up in the past 5 years selected by the applicant from the List of Case Information. For each subfield the applicant should have at least 2 case reports. When several subfields are combined in one case report, it is possible to provide the same case report for different subfields (008.1 – 008.3). If possible the case reports should also contain the testimony delivered in court. *The case reports should provide a clear and a broad picture of the applicant's competencies. Subsequently, independently written reports can be submitted.*
- If available:
  - proof of the forms of professional development referred to in the Overview Continuing Professional Development Digital Forensics;
  - a statement concerning the level of accreditation of the applicant's working environment, where applicable.

Assessment method:
phase a. administrative, by the NRGD Bureau;
phase b. substantive, by an Advisory Committee for Assessment (ACA) made up of at least two people on the basis of the available written material. This ACA will in principle consist of a legal assessor and a subject-matter assessor;
phase c. substantive, by the same ACA to which one subject-matter assessor is added, drawn from the same field of expertise as the applicant, on the basis of the available written material. This will not be necessary if

the ACA unanimously gives a positive recommendation to the Board in phase b;

phase d. substantive, by the ACA specified at c by means of an oral assessment. This oral assessment will be waived if the applicant's expertise has been clearly established in phase c;

phase e. decision by the Board: registration, provisional registration or no registration.

2.4. Application for reregistration: after provisional registration

Documents to be submitted

- NRGD application form;
- An updated curriculum vitae (CV), preferably in English;
- Copies of documents relating to the highest level of professional qualification (if changed);
- Overview of Continuing Professional Development Digital Forensics;
- List of Case Information Digital Forensics;
- 2 case reports drawn up in the past 2 years selected by the applicant from the List of Case Information. For each subfield the applicant should have at least 2 case reports. When several subfields are combined in one case report, it is possible to provide the same case report for different subfields (008.1 – 008.3). If possible the case reports should also contain the testimony delivered in court. *The case reports should provide a clear and a broad picture of the applicant's competencies. Subsequently, only independently written reports can be submitted.*
- If available:
  - proof of the forms of professional development referred to in the Overview Continuing Professional Development;
  - a statement concerning the level of accreditation of the applicant's working environment, where applicable.

Assessment method

phase a. administrative, by the NRGD Bureau;

phase b. substantive, by an Advisory Committee for Assessment (ACA) made up of at least three people on the basis of the available written material. In principle this ACA consists of a legal assessor and tow subject-matter assessors;

phase c. substantive, by the same ACA by means of an oral assessment. This oral assessment will be waived if the applicant's expertise has already been clearly established;

phase d. decision by the Board: registration, provisional registration or no registration.

2.5 Application after rejection or after legally expired registration (fast-track)

Documents to be

- NRGD application form;

submitted	- An updated curriculum vitae (CV), preferably in English; - Documentary evidence of the current (academic) working level, and proof of being an expert authorised to sign (if applicable); - Overview Continuing Professional Development Digital Forensics; - List of Case Information Digital Forensics, exclusively listing reports written after the date of the rejection by the Board or the date of the legal expiration; - 3 case reports drawn up after the date of rejection by the Board or the date of the legal expiration, selected by the applicant from the List of Case Information. For each subfield, the applicant should have at least 2 case reports. When several subfields are combined in one case report, it is possible to provide the same case report for different subfields. If possible the case reports should also contain the testimony delivered in court. *These case reports should provide a clear and broad picture of the applicant's competencies*. - All reports of supervision and/or collegial review related to the submitted case reports.
Assessment method	phase a. administrative, by the NRGD Bureau; phase b. substantive, by an Advisory Committee for Assessment (ACA) made up of at least three people on the basis of the available written material, including possible supplementary written information. In principle this ACA consists of a legal assessor and two subject-matter assessors; phase c. substantive, by the same ACA by means of an oral assessment. This oral assessment will be waived if the applicant's expertise has been clearly established in phase c; phase d. decision by the Board: provisional registration or no registration.

Part V. Annex A Summary of concepts Digital Forensics

Items:	Object from which digital data are collected, derived or extracted as part of the forensic process.
Examination:	Part of the forensic process consisting of the recovery and analysis of items and the interpretation of observations obtained from the analysis
Firmware:	A class of software permanently stored in non-volatile memory (such as ROM or flash), designed to provide low-level control of hardware functions. It is typically not modifiable by the user and may be tightly coupled with the physical device.
Hardware:	Digital storage media (hard disks, multimedia memories etc.), data communications, mobile phones, and embedded digital devices.
Investigation:	The process of searching for, recognizing, collecting, and initially analysing digital items or data in relation to a presumed incident or offence. The purpose of an investigation is to generate and explore hypotheses about what may have occurred. This phase typically takes place in the investigative phase of the inquiry, often at the scene, and may involve coordination between technical and investigative disciplines.
Software:	The set of programs and associated data—potentially including supporting documentation and artefacts—which may be dynamically written, modified, and executed by hardware. It includes applications, operating systems, utilities, and all the digital code that tells the hardware what to do.
Tools:	Combinations of software, hardware and firmware. These tools may include commercially available software that is widely accessible to forensic experts, as well as institution-specific tools developed by organizations. While industry-standard tools are generally available for use by forensic experts across various domains, access to organization-developed tools may be restricted and subject to specific conditions. If the applicant is using tools they have developed or commissioned themselves, they should be able to demonstrate a specification, design and evaluation process that clearly identifies their limitations in a way that is intelligible to non-specialists

Recovery:	Refers to the systematic process of recognition, collection, acquisition and preservation of potential digital evidence. This definition does not refer to the technical restoration of deleted, corrupted, or lost data from storage media. However, such restoration techniques may be applied as part of the recovery phase when they are required to make potential evidence accessible for subsequent analysis.

Annex B NRGD Glossary

Advisory Committee for Assessment	A committee appointed by the Board which advises the Board on the (repeat) applicant's (degree of) suitability for (repeat) registration.
Applicant	Natural person submitting an application to the NRGD in order to be (re)registered in the register.
Application for initial registration	An expert who submits an application to be entered in the register and does not or not yet have an NRGD registration at the time when the application is made.
Application for reregistration	An application submitted by an expert who at the time of submitting the next application already has a NRGD registration, possibly for a provisional registration.
Assessor	A member of an Advisory Committee for Assessment.
Board	The Board of Court Experts is the body as referred to in Section 51k(2) of the Code of Criminal Procedure and is charged with managing the register.
Brdis	Register of Court Experts in Criminal Cases Decree (Besluit register deskundige in strafzaken).
Bureau	The NRGD Bureau that supports the Board.
Collegial review	The assessment of another person's work for the purpose of continuous quality control of a person's expertise. There is thereby not a hierarchical but a horizontal relationship between colleagues specialised in the same subject area. The reviewer does not sign the report.
Continuing professional development	All (training) activities that contribute to the ongoing development of knowledge and skills, which is desirable and necessary in order to be able to continue performing the role of court expert in a professional manner.
Expert	An individual who issues a report for the administration of justice and/or gives testimony in court.
Expert without work of his own	An expert who has not independently completed and signed the number of case reports required for registration.
Forensic training on reporting	A coherent and structured arrangement of organised training activities in which the necessary knowledge and experience are acquired to report as a court expert in criminal law proceedings and that is completed by an exam.

Independent expert	An expert who has independently prepared and signed the required number of case reports.
Intervision	A structured (interdisciplinary) meeting between people who are working or training in the same professional area, not being an operations meeting. The subject of discussion is in any case the forensic work carried out and the associated problems. The aim is to enhance the expertise of those involved and improve quality of work. Unlike supervision, there is no hierarchical relationship between the participants.
NRGD	The Netherlands Register of Court Experts of which the Board and the Bureau form part.
Provisional registration	The registration of an expert for a period specified by the Board and possibly under certain conditions which must be met within that period. In principle the period to be specified by the Board is two years.
Register	The national public register as referred to in Section 51 k(1) of the Code of Criminal Procedure, which lists the court experts which the Board deems suitable.
Registered expert	An expert who is entered in the register.
Registration	Entry in the register.
Supervision	The assessment of another person's work, the joint consideration of the work and the supervision of a supervisee as part of a training or additional training process. Supervisor and supervisee are thereby in a hierarchical relationship. The supervisor will observe the subject of the investigation (the investigated person) in such a way that they can check the supervisee's investigation, and can endorse and take responsibility for the conclusions thereof. The supervisor will sign the report in all cases.
User	Someone who uses the register in order to find and potentially engages a registered expert.

Annex C Revision History

Version	Date	Revisions made
3.8	2-10-2025	Adjusted the Standards for a new three field division.
3.0	Q1 2021	Adjustments made on the basis of Template Standards 4.0: - Source file edited for the benefit of visually challenged readers - Generic textual changes and harmonisation - Definition of intervision - 'Expert' instead of 'reporter' - Terminology Application conform Dutch administrative law - Alteration of standard amount of assessors
2.0	1 December 2019	- Further clarification of subfields - Addition of requirements of initial applicant without work of his own
1.1	June 2018	Adjustments made on the bases of Template Standards 3.2: - Changes in policy e.g. provisional registration - Generic textual changes and harmonisation - Editorial changes in English terminology - Statement NRGD added to Application Form
1.0	18 February 2016	First edition