NEDERLANDS
REGISTER
GERECHTELIJK
DESKUNDIGEN

Standards Digital Forensics (008.1 - 008.6)

Version 2.0
Date of approval: 14th of November 2019
Date of effect: 1st of December 2019

Inhoud

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 Court Experts Board (hereinafter: Board). The Board's core task is to rule on the applications for registration or repeat registration in the register of the NRGD (register). To that end the Board first defines the 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 applicants

The NRGD distinguishes two types of applicants: the initial applicant and the repeat applicant. The initial applicant is a reporter 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 repeat applicant is an expert who is already registered in the register for the field of expertise to which the application relates.

These two types of applicants are subdivided as follows:

Initial applicant

i. independent reporter: a reporter who has independently written and signed the required number of case reports;
ii. reporter without work of his own: a reporter who has not independently written and signed the number of case reports required for registration.
If the assessment is favourable, the reporter without work of his own will only qualify for provisional registration.

Repeat applicant

i. Repeat applicant after full registration;
ii. Repeat applicant after provisional registration.

The initial applicant is an applicant who at the time of submission of the application does not have an NRGD registration. An initial applicant could be:

- the independently reporting expert;
- the newly-trained expert;
- the applicant whose earlier application has been rejected by the Board;
- the applicant whose registration was previously stricken.

In respect of initial applicants, it is necessary to make a clear distinction between the independent reporter and the reporter without work of his own. An example of a reporter without work of his own is the newly-trained expert. This expert has completed the forensic training, 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 a reporter without work of his own is the reporter 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 a 'reporter 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 repeat applicants is important in the context of the assessment procedure: the documents a repeat applicant must submit, the composition of the Advisory Committee on 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) and the Experts in Criminal Cases Act (Wet 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 old 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. Core activities

The Digital Forensics field of expertise is described below.

Experts within the Digital Forensics field of expertise deal with digital material. Digital material covers all manifestations, input, output and processing of digital systems. A digital system processes information in discrete units. This contrasts to an analogue system in which a continuous representation of information is present. Digital material can occur in various sources, and the Digital Forensics field of expertise is characterised by a growing number of potential sources. This can be software, hardware or a combination of both.

Digital Forensics seek to examine - depending on the precise question posed - whether discovered digital evidence can be linked to natural persons. In order to achieve this, an expert will in principle carry out a reconstruction of how digital evidence ended up on the material to be examined.

Experts in the Digital Forensics field of expertise are in principle able to carry out every phase of Digital Forensics (data collection, data examination and data analysis) themselves. An expert can have parts of the data collection, data examination or data analysis phases carried out by someone else.[1]

The activities which fall within the Digital Forensics field of expertise are:

1. Data collection: Data collection involves the correct preservation (e.g. by copying) of digital data sources. 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.
   Knowledge of the following areas amongst others is thereby crucial: digital storage media (hard disks, multimedia memories etc.), data communications, mobile phones, and embedded digital devices. In this phase an expert must be familiar with the various collection options, and he must be able to assess which collection 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.
2. Data examination: Data examination relates to the investigation of forensic images of digital data sources in order to find potential evidentiary data. without interpreting the resultant findings in the context of the case. It may thereby be possible that the expert sets up their own experiment. In this phase the expert must be able to differentiate which evidence may and may not be relevant, and the expert must make this evidence suitable for in-depth analysis.
3. Data analysis: Data analysis involves the analysis, reconstruction, interpretation and providing a qualitative opinion of the evidence which is obtained from the digital data sources. In this phase the expert must be able to make a substantiated assessment. Interpreting is the crucial activity that sets data analysis apart from data examination.

§ 2. Relevant questions

The type of question coming from the court of law depends on the phase which the digital forensic examination has reached.

- Questions in the data collection phase

The following questions - amongst others - are relevant for the data collection phase within the Digital Forensics field of expertise:

[1] Please see the Code of Conduct of the Netherlands Register of Court Experts.

1. Is the electronic equipment correctly secured?
2. Is the bypassing of the access code correctly carried out?
3. Is the data correctly safeguarded out of complex infrastructures like industrial control systems?
4. Was the data preserved using validated tools and methods?
5. Was the data preserved using appropriate forensic image formats?
6. Was the preservation carried out in a manner that ensured minimum contamination?
7. How did you validate the tools that you used?
8. Did you use the appropriate legal authority to preserve the digital evidence?

- Questions in the data examination phase

The following questions - amongst others - are relevant for the data examination phase within the Digital Forensics field of expertise:

1. What data concerning the event in question can be found on what exhibit, what is the location of the data and by what means can it be retrieved?
2. Was the data accessible by use of software available to the suspect?
3. Can it be ascertained when the retrieved data has been stored on the data storage, when the data has been accessed, modified and/or changed?
4. In case of deleted information like text messages, photos and videos, has such information been correctly retrieved?
5. Is the exchange of data, captured in a network trace, correctly made visible?
6. Has the tool that you used correctly parsed out the data from the artefact that you are examining, and how can you confirm that this was the case?
7. What hypothesis can be generated from the digital evidence examined?

- Questions in the data analysis phase

The following questions - amongst others - are relevant for the data analysis phase within the Digital Forensics field of expertise:

- Questions relating to reconstruction
  1.a. Is digital evidence present on the material to be examined?
  1.b. What is the nature of the digital evidence on the material to be examined?
  1.c. How did the digital evidence end up on the material to be examined?
  1.d. What is the chronological and/or temporal sequence of events that can be determined from the analysis of the digital evidence?
  1.e. Can any user attribution be determined from the digital evidence analysed?
  1.f. Can the digital evidence analysed place the device at a particular physical location, and potentially at a particular time?

These questions are aimed at providing a reliable reconstruction of how digital evidence ended up on the material to be examined. After all, digital evidence can be produced in various ways.

- Questions relating to interpretation
  2.a. To what extent does the digital evidence analysed support any of the hypotheses generated?
  2.b. Does the analysed digital evidence suggest any alternative hypothesis that needs to be examined?
  2.c. To what extent does the analysed evidence support any of the legal elements of the matter under investigation?

- Questions aimed at providing a qualitative opinion
  3.a. How much knowledge and skill in the field of digital technology is required in order to achieve a particular result?
  3.b. Is a particular event or action technically difficult?

These can be follow-up questions to the reconstruction questions and are particularly aimed at providing clarity about the extent to which a particular event or action can be attributed to a person.

§ 3. Methodology

The applicant can adopt different models of rational legal approaches; e.g. Bayesian models, story-based models or argumentation-based models, since different questions may require different approaches. Part of the expertise is to extend a known or a newly developed methodology to a new case. Newly developed methodology should be validated on reference devices or test systems before adopting it to the actual case.

§ 4. Boundaries of the field of expertise

It is important that an expert is able to identify the limits of his expertise and act accordingly. This means that an expert must be able to recognise immediately that his own expertise or specialism is not adequate to carry out the digital forensic examination.

Interpretation that extends outside of the digital field does not come under the Digital Forensics field of expertise. Examples of activities that emphatically do not come under the Digital Forensics field of expertise are:

- Identification and comparison of persons and/or objects that might be visible on image fragments;
- Interpreting what might be audible on audio fragments;
- Interpreting what might be possible with an electronic analogue circuit;
- Measurements in (image) fragments;
- Photogrammetry: Determine the position/velocity of the vehicle?
- Facial comparison: Is the robber the same person as the suspect?
- Speaker recognition: Is the speaker in conversation <A> the same person as the speaker in conversation <B>?
- Crime scene visualisation.

§ 5. Registration

5.1. Registration

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

5.2. Defined sub-fields

Experts in the field of Digital Forensics have a shared knowledge of IT, which is supplemented with knowledge of at least one subfield. Knowledge in these areas changes rapidly. In view of this, the expert will be assessed based on the registration requirement (part III) and according to the assessment procedure (part IV) on the shared knowledge of IT and on the subfield(s).

The NRGD distinguishes the following subfields within the field of Digital Forensics. The expert must stipulate the subfield(s) from at least one of the categories below:

008.0 Digital Forensics
- 008.1 Computer Forensics
- 008.2 Software Forensics
- 008.3 Database Forensics
- 008.4 Multimedia Forensics
- 008.5 Device Forensics
- 008.6 Network Forensics

5.3. The subfields further explained[2]

Computer forensics

Computer forensics uses validated analysis techniques to gather potential evidence from storage media (such as a hard disk), RAM and other parts of desktops, laptops and server computers. For instance, traces of internet browsers or presence of certain file types (emails, documents, pictures etcetera). The investigation can also address questions about the manipulation of traces or their time stamps.

Examples of issues to be examined:

- Data recovery of deleted, encrypted or hidden computer files.
- Data recovery of a USB stick.
- Discovery of passwords.
- Determination of websites that have been visited.
- Files that have been uploaded or downloaded.
- When files were last accessed or deleted.
- User login times.
- Recovery of (deleted) e-mails.
- Determination whether a file has been copied.
- Determine what has been deleted.
- Determine what programs were executed and when.
- Reconstruct user activity.
- Reconstruct system activity through the examination of log files.
- Identification of the use of anti-forensic methods (es. Wiping tools, VPN/TOR, and so on)
- Determine if a chat application was used on the computer.
- Determine if P2P networks/tools were used.

Software forensics

Software forensics is concerned with with uncovering potential evidence through examining software. Reverse engineering is applied in order to answer the question to be examined. Software forensics covers for example operating system forensics, application software forensics and digital forensic analysis tools. Analysis tools are highly likely developed by the expert himself. On the one hand, questions may address the internal operation of software, in order to interpret or to explain certain behaviour. On the other hand, software forensics expertise may also be used to determine authorship of software, e.g. by comparing if two different software programs are the same.

Examples of issues to be examined:

- What happened within the software?
- Does it appear that the source code of program X has been copied from program Y?
- Examination of text codes and binary codes.
- Examination of malware.
- How does the software function and was it functioning as intended?

Database forensics

Database forensics focuses on databases and their related content and/or metadata (for example data about a document, e.g., author, language). Databases are structured data files that are administered and accessed through a database management system. Most (relational) databases are controlled through SQL (Structured Query Language). However, many variations and extensions exist subject to supported features. Questions in the field of database forensics may, for example, be about the interpretation of data or about determining when certain information was

[2] The ontology and the explanation is based on Karie, N. M. and Venter, H. S. (2014), Toward a General Ontology for Digital Forensic Disciplines. *Journal of Forensic Sciences*, 59: 1231–1241 and on Henseler, H. and Loenhout, S. van (2018). Educating judges, prosecutors and lawyers in the use of digital forensic experts. *Digital Investigation,* 24: S76-S82.

added to or modified in the database. This type of information depends on the database vendor and requires experience and research for a correct interpretation.

Examples of issues to be examined:

- Reconstructing meta-data.
- Identifying transactions within a database system or application that indicates evidence of wrongdoing.
- Recovering deleted data from within database structures

Multimedia forensics

Multimedia forensics deals with recovery, authenticity analysis and source identification of images, videos, audio and artefacts therein. Artefacts are the visual/aural aberration in an image, video, or audio recording resulting from a technical or operational limitation, and/or information or data created as a result of the use of an electronic device that shows past activity.[3]

Examples include discovery of the origin and/or location of pictures from file meta data. In some cases, it is even possible to match an audio recorder, video or photo camera

with a multimedia file. Also, investigation of possible manipulation (digital forgery) of pictures, video and audio content can be important questions for experts in this field of expertise.

Examples of issues to be examined:

- Speckles in a scanned picture.
- "Blocking" in images compressed using the JPEG standard.
- Is it possible to playback the recordings from <time interval>?
- Is this image authentic or has object <X> been added to the image?
- Was photo <X> taken with this particular camera?
- Has the image been manipulated?

Device forensics

Device forensics deals with the gathering of digital evidence from different types of devices. Devices may range from small-scale devices such as mobile phones, tablets, navigation systems, external hard drives, cameras etc., to large-scale devices such as the storage area network (SAN) and network attached storage (NAS) systems. Although many devices are basically computers, device forensics is considered a separate subfield because they are typically embedded and are "closed" in nature, and consequently require special knowledge and software to collect, examine and analyse internal data. With the rise of the "Internet of Things", investigators will be more frequently faced with equipment that has user documentation but which lacks documentation about its internal architecture and operation. Either such documentation is kept secret on purpose to hide it from competing manufacturers or it may simply be that internal software and hardware are changing so rapidly that documentation is useless and irrelevant for consumers.

Examples of issues to be examined:

- To what extent are the videos found on someone's telephone available?
- Recovery of internal memory of PDA devices, smart/mobile phones or tablets.Analisis of user activities on the smartphone (calls, messages, chats, emails and so on)
- Recovery of deleted contents from internal memory and from application databases.
- Determine application usage over the time.
- Analisis of devices connected to a smartphone (for example, a smartwatch).
- Analysis of phones that are or have been connected to a router/modem.
- Getting access to a locked mobile phone.

[3] SWGDE (2016, 23 June). Digital & Multimedia Evidence Glossary. Retrieved from https://www.swgde.org/documents/Current%20Documents/SWGDE%20Digital%20and%20Multimedia%20Evidence%20Glossary

- Repair of an embedded system.

Network forensics

Network forensics is a branch of Digital Forensics that focusses on data related to network technologies covering topics like telecom network forensics, internet forensics, wireless forensics or cloud forensics. As is the case with device forensics, the expertise in this field varies considerably.

For instance, cell site analysis is a completely different specialism from the type of analysis that is required for the interpretation of traces in firewall and network equipment after a hacker has breached the security defences of a network. The interpretation of traces in the cloud and from online data in social media is another specialization. One could even argue that the investigation of network communication traces on a computer is in fact computer forensics or, when investigated on the servers of the internet provider, as database forensics. In both cases, software forensics expertise may be needed if the traces are stored in a proprietary format by vendor specific software.

Examples of issues to be examined:

- Analysis of IP addresses.
- Capturing, recording and analysis of network traffic in order to determine the source of network security intrusions.

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.

§ 1. Article 12(2) sub-paragraph a

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

1.1 Initial applicant: independent reporter
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 annexe 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, at least 1 report 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 Initial applicant: reporter 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 annexe 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 and of which at least 1 report has been drawn up under 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 Repeat applicant: 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 annexe 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, at least 1 report 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 Repeat applicant: 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 annexe 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 during the registration period which have been subjected to collegial review;
  In case the applicant is also acting as a supervisor, 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).

§ 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 should:

- 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 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 should:

- be aware of the uses and limitations of any tools that have been employed previously in the investigation;
- be able to check the reliability of the tools and use tools and techniques appropriately;
- be able to demonstrate a methodical approach to the selection of their own forensic software tools;
- be able to ensure that the tools are appropriate to the task in hand and that the applicant himself is competent to use them;
- 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 use;
- if the applicant is using tools he has developed or commissioned himself, he 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 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 make defensible judgments about the respective weights to be attached to different finding;
- be able to justify his actions by explaining their relevance and implications;
- be able to check that the data collection phase was completely in accordance with the appropriate documented procedure;

- be able to sufficiently demonstrate contemporaneously logging and documenting the handling of items and the data examination and analysis process in a way that can be audited and permits the process to be repeated if appropriate;
- 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 able to reconsider the work done in the light of new findings and information;
- be able to identify alternative explanations of the material;
- be able to demonstrate awareness of the possibility that a particular set of data may have resulted from software default or error, user action or error, unauthorized use or direct editing;
- be ready to re-think a hypothesis in the light of new or modified information, look for valid indications to confirm or deny its validity and exclude and eliminate explanations, suspects or material;
- be aware of the reliance on the available hypotheses and be able to develop alternative hypotheses;
- be able to take steps to ensure that all relevant information is considered at each stage.

§ 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 what is likely to be of value to others and showing good judgment on how much technical detail to include or omit;
- be able to demonstrate appropriate use of evidence and intelligence; and to communicate information to others (including non-specialist) understandable and clearly in a way that avoids misunderstanding;
- be able to communicate an understanding of the technical issues, processes and procedures involved;
- be aware where he gives general technical explanations, to make sure that these are adequately related to the specific operating system or file system;
- be able to use generic terminology that is not specific to proprietary forensic software tools;
- use validated techniques and be able to explain what actions have been undertaken in order to validate the techniques used;
- be able to explain industry practice so that non-specialist can understand points of interpretation that depend on how particular services operate;
- 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;
- state provisional views clearly as to be provisional;
- distinguish alleged facts based on witness statements so that their own relevant views can be reviewed if questioned;

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 data and/or digital data sources received, with information on the date and manner of submission, whether originals were received or copies. Any other conditions of the data and/or digital data sources that might be relevant for the examination and analysis are mentioned as well;
- specification of questioned and reference data and/or digital data sources;
- 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 data;
- the method(s) used;
- results of the data examination;
- interpretation of data examination results;
- 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 Court Experts Board 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 applicant

2.1. Initial applicant: independent reporter

- Documents to be submitted:
- NRGD application form;
- Certificate of Good Conduct;
- 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;
- Overview Continuing Professional Development Digital Forensics;
- List of Case Information Digital Forensics;
- 3 case reports not older than 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 – 008.6). 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.
- 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 lawyer and two professional 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: registration, provisional registration or no registration.

2.2. Initial applicant: reporter without work of his own

Documents to be submitted:

- NRGD application form;
- Certificate of Good Conduct;

- 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;
- 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 – 008.6). 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 lawyer and two professional 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. Repeat applicant: after full registration
Documents to be submitted:

- NRGD application form;
- Certificate of Good Conduct;
- 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 – 008.6). 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 two people on the basis of the available written material. This ACA will in principle consist of a lawyer and a professional assessor; the assessors will first carry out the

assessment individually, without consultation, and will then discuss their findings. If they are unanimous in their opinion that the expert complies, a positive recommendation will be given to the Board.

phase c. substantive, by the ACA specified at b. to which one professional assessor is added, drawn from the same field of expertise as the applicant, on the basis of the available written material;

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 the second instance);

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

2.4. Repeat applicant: after provisional registration

Documents to be submitted:

- NRGD application form;
- Copies of documents relating to the highest level of professional qualification (if changed);
- An updated curriculum vitae (CV), preferably in English;
- Overview of Continuing Professional Development Digital Forensics;
- List of Case Information Digital Forensics;
- 2 case reports drawn up during the registration period 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 – 008.6). 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
  - 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 lawyer and two professional 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: registration, provisional registration or no registration.

Annex A Summary of concepts Digital Forensics

This document contains keywords for concepts of which an expert in the field of Digital Forensics should minimally have a basic knowledge.

See the SWGDE and SWGIT Digital & Multimedia Evidence Glossary. The terms relating to Video Analysis and Forensic Audio are excluded from the NRGD Summary of concepts in Digital Forensics.

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.

Assessor
: A member of an Advisory Committee for Assessment.

Board
: The Court Experts Board 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.

Independent reporter
: A reporter who has independently prepared and signed the required number of case reports

Initial applicant
: An applicant who makes an application to be entered in the register.

Intervision
: Intervision is a structured (interdisciplinary) meeting between people who are working or training in the same professional area. 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.

Repeat applicant

An expert who at the time of submitting a repeat application already has a NRGD registration, possibly for a provisional registration.

Reporter

An individual who issues a report for the administration of justice and/or gives testimony in court.

Reporter with no own work

A reporter who has not independently completed and signed the number of case reports required for registration.

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 engage a registered expert.

Annex C List of revisions

Version 2.0
Date: 1 December 2019
Revisions made:

- further clarification of subfields
- addition of requirements of initial applicant without work of his own

Version 1.1
Date: June 2018
Revisions made:

- 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

Version 1.0
Date: 18 February 2016
Revisions made:

- First edition