

The image shows the exterior of a brick building, identified as Hogeschool Leiden. A large blue banner is suspended in front of the building, featuring the text 'Talent voor Jaar' and other smaller text. To the right, there is a logo for 'hogeschool Leiden' and the slogan 'Denk Doe Voel | t'. The building is surrounded by greenery and parked bicycles.

Educating Judges, Prosecutors and Lawyers in the Use of Digital Forensic Experts

Dr. Hans Henseler, University of Applied Sciences Leiden
Sophie van Loenhout M.Sc., Netherlands Register of Court Experts

DFRWS EU 2018

CONVITTO DELLA CALZA - Oltrarno Meeting Center
March 21-23, Florence, Italy

Content

- About the NRGD
- Working methods
- Open for certification
- Standards for Digital Forensics
- Demarcation
- Requirements
- Example questions for DF Court Experts

About the NRGD

- Experts in Criminal Cases Act + Register of Court Experts in:

Criminal Cases Decree

- legal basis, independent position and structural funding

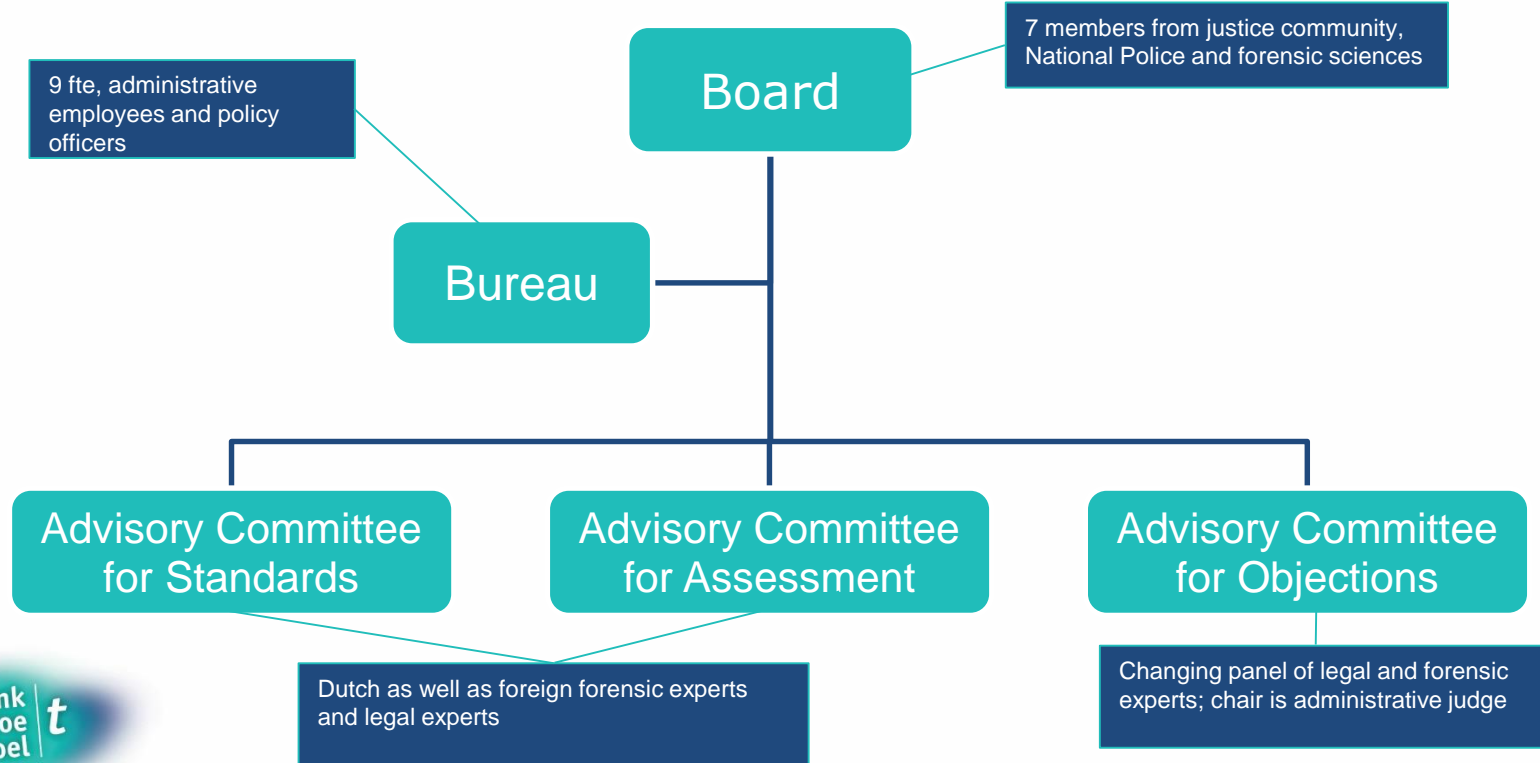
The NRGD contributes to *a fair administration of justice* by assuring the competence and quality of court experts and their reports through:

- Code of Conduct
- Standards per field of expertise
- Assessing & registering experts
- Periodic re-assessment

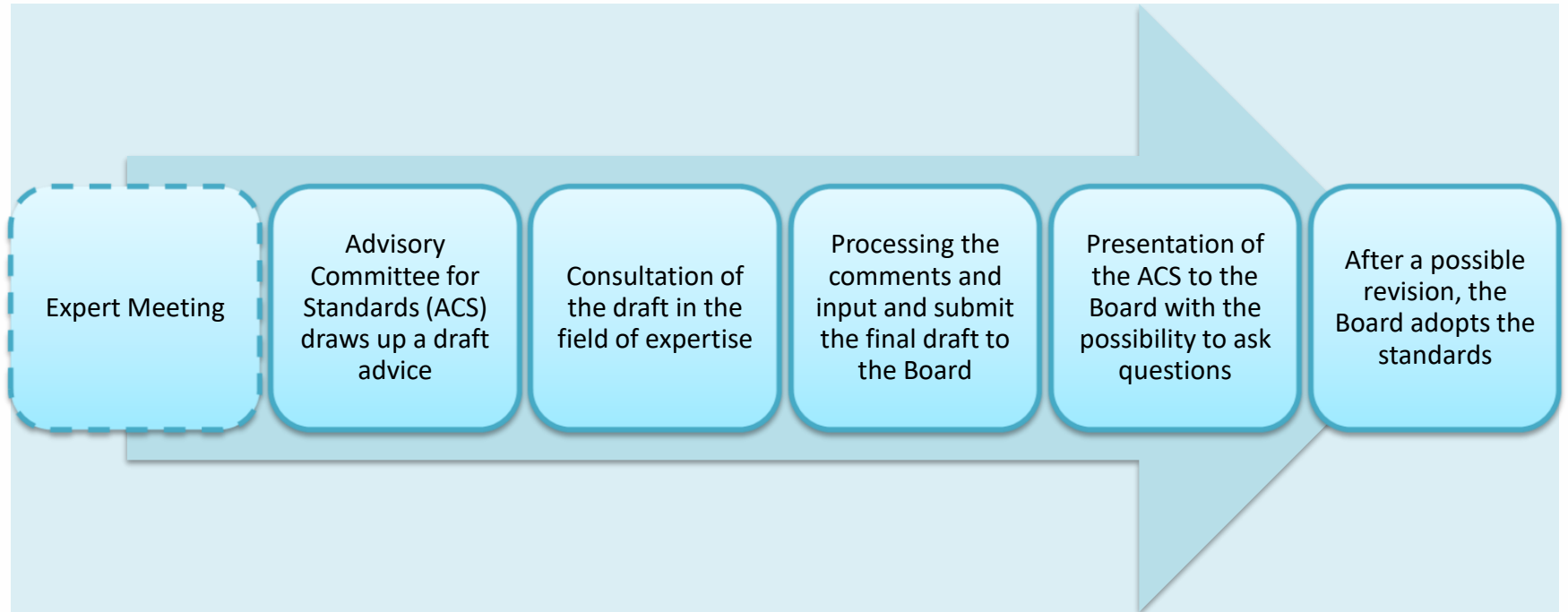
NRGD also provides advice on forensic competence assurance



About the NRGD (cont'd)



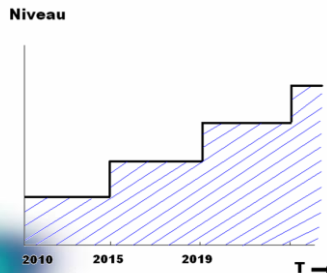
Setting standards per field of expertise



ACS: Set standards

- Specify requirements of article *12(2)a-i* of Decree (incl. Code of Conduct NRGD)
- Subject-matter + criminal law requirements (incl. role of expert-witness)
- Theory & practice requirements

In cooperation with subject-matter and legal experts
(acceptance/support)



- Define field of expertise:
 - Core activities
 - Boundaries
 - Subfields?



ACA: Assess applications (I)

- In cooperation with subject-matter and legal experts (acceptance/support):
 - Evaluation of written material and, if necessary, oral examination.
 - Application package:
 - CV
 - List of case information
 - Selection of 2-4 case reports
 - Evidence of competence (incl. collegial review + CPD)
 - Certificate of Good Conduct
 - Signed declaration



ACA: Assess applications (II)

- Advisory evaluation form:
 - Main/ Minor points
 - Strong/ Weak points
- Unanimous advice:
 - 5 year registration
 - 2 year registration
 - No independent work
 - Quality of non-essential elements must improve
 - After previous rejection on subject-matter expertise
- Check by Bureau >> decision by Board



NRGD is open for certification

- For the fields of expertise:
 1. DNA-analysis and interpretation
 2. Handwriting Examination
 3. Forensic Psychiatry and Forensic Psychology
 4. Forensic Toxicology
 5. Drugs-analysis and interpretation
 6. Weapons and Ammunition
 7. Forensic Pathology
 - 8. Digital Forensics**
 9. Legal Psychology
 10. DNA Activity Level (in progress)
 - expert meeting held in January 2018

Received (re)applications > 1000
Rejected 20% first phase

ACS: Digital Forensics

E.J. van Eijk MSc, CISSP

R.M. van der Knijff MSc

R.J. Mora RE, OSCP, CISSP

Professor H. Prakken LL.M, PhD

C.J.T. Prickaerts GCFA, CISSP

H. Schut MSc

Professor P. Sommer MA

Netherlands Forensic Institute, NL

Netherlands Forensic Institute, NL

Royal Dutch Shell, NL

Utrecht University, NL

Fox-IT, NL

High Tech Crime Unit (police), NL

De Montfort University, UK

Consulting ACS members:

C. Baardman LL.M

A. Kuijer LL.M

CoE Cybercrime, Dutch Public
Prosecution Service

CoE Cybercrime , Dutch Public
Prosecution Service

NRGD standards for Digital Forensics

- Competence standards consist of 3 parts:
 - Demarcation
 - Registration requirements
 - Assessment procedure
- Download:
 - <https://english.nrgd.nl/registration/digital-forensics.aspx>

Demarcation: Steps in the Forensics Process

Preserve &
Collect

- Collect Electronic Stored Information
- Create a forensic copy

Extract &
Examine

- Make electronic stored information readable
- Information culling

Analyse

- Data interpretation
- Connecting the dots

Demarcation: Digital Forensics

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

Registration Requirements – example (1)

An applicant Digital Forensics should:

Generic requirement:

12(2) a. (...) *have sufficient knowledge and experience in the field of expertise to which the application relates.*

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.
- (...)

Registration Requirements – example (2)

An applicant Digital Forensics should:

(...)

Basic requirements:

- 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 forensics investigations (e.g. crime scene investigation, chain of custody, principles of evidence)
- have adequate knowledge of collection, examination and analysis of data.

Registration Requirements – example (3)

An experienced reporter or a newly qualified reporter should:

Specific requirements:

- demonstrably have interpreted and reported 4 case reports (criminal, civil or administrative law) in the preceding 4 years that have been subjected to collegial review. For each stipulated subfield the reporter should have at least two case reports.
- have spent minimally 40 hours per year in the past 4 years on continued professional development (e.g. conference attendance, giving or attending lectures or courses, publications).

Documents to be submitted:

- Certificates for (proficiency) tests or courses attended
- An overview of forensically relevant continuing professional development

Preserve & collect phase questions

- Questions related to the “forensic soundness” of data collection, for example:
 - *Was the electronic equipment correctly secured?*
 - *Is the bypassing of the access code correctly carried out?*
 - *Is the data correctly safeguarded from complex infrastructures like industrial control systems?*

Extract & examine phase questions (1)

- Questions on identification and date & time, for example:
 - *What data concerning the crime can be found on what exhibit, what is the location of the data and by what means can it be retrieved?*
 - *When has the data been accessed, modified and/or changed?*
 - *Can it be ascertained when the retrieved data has been stored on the data carrier?*

Extract & examine phase questions (2)

- Questions on the methods of extraction, for example:
 - *Was the data accessible by use of software available to the suspect?*
 - *Was deleted information, e.g., messages, photos and videos, correctly retrieved?*
 - *Is the exchange of data, captured in a network trace, correctly made visible?*

Data analysis phase questions (1)

- Questions regarding the reconstruction of how digital evidence ended up on the material under examination, for example:
 - *Is digital evidence present on the material under examination?*
 - *What is the nature of the digital evidence on the material under examination?*
 - *How did the digital evidence end up on the material under examination?*

Data analysis phase questions (2)

- Questions relating to the interpretation of information, for example:
 - *Does the read data match a scenario outlined in advance?*
 - *Given alternative hypotheses, what can you say about the evidence that was found?*
 - *Given the evidence that was found, what can you say about the alternative hypotheses?*

Data analysis phase questions (3)

- Follow-up (qualitative) questions aimed at providing clarity about the extent to which a particular event or action can be attributed to a person, for example:
 - *How much knowledge and skill in the field of digital technology is required in order to achieve a particular result?*
 - *Is a particular event or action technically difficult?*

Status register for Digital Forensics

- Number of DF registrations in January 2018

Area	# experts
008.1 Computer Forensics	5
008.2 Software Forensics	5
008.3 Database Forensics	1
008.4 Multimedia Forensics	0*
008.5 Device Forensics	5
008.6 Network Forensics	2

* One application in progress

- How to assess expert witnesses with short reports, e.g., critically evaluating the report of another expert witness?

Thank you for your attention

henseler.h@hsleiden.nl
www.linkedin.com/in/henseler

