Digital Investigation 24 (2018) S76–S82

Contents lists available at ScienceDirect

Digital Investigation

journal homepage: www.elsevier.com/locate/diin

DFRWS 2018 Europe — Proceedings of the Fifth Annual DFRWS Europe

Educating judges, prosecutors and lawyers in the use of digital forensic experts

Hans Henseler [a, *], Sophie van Loenhout [b]

[a] University of Applied Sciences Leiden, The Netherlands
[b] Netherlands Register of Court Experts, The Netherlands

Keywords:
Digital forensics
Registration requirements
Standards
Court experts

A B S T R A C T

Recent years have seen an exponential growth of evidence in digital forensic investigations. Digital Forensics (DF) experts are predicting, amongst others, a 'digital explosion' of ransomware in the coming years. The legal community must be prepared to deal with an increase of digital evidence in both volume and complexity. In cooperation with experts in the field, the Netherlands Register of Court Experts (NRGD) has recently developed standards and registration requirements for DF experts in the Netherlands. This article describes how these standards were established and provides insight into the requirements that a DF expert should meet to qualify as an NRGD registered expert. Registration is now open to all DF experts, both Dutch and non-Dutch. Furthermore, this article can be used by DF experts worldwide to educate judges, prosecutors and lawyers that make use of their reports. It illustrates what the legal community can expect from DF court experts, it provides a demarcation of the DF field based on DF literature and it presents examples of relevant questions that can or should be asked to a DF expert.

Introduction

Last year the world was shocked, again, by the outbreak of ransomware viruses (Wikipedia, 2017a, 2017b). The ransomware took files "hostage" from users on thousands of computers. In return for payment of a ransom the files were unlocked. However, payment does not necessarily guarantee decryption of the files. Digital forensics experts are predicting a "digital explosion" of ransomware this year (Hayter, 2015). The Dutch National Cyber Security Centre (National Cyber Security Centre, 2016) and the FBI are warning that the number of ransomware incidents continues to grow as individuals and organizations fail to take precautionary measures (FBI, 2016).

The warnings suggest that digital evidence continues to grow exponentially in investigations and prosecution of suspects. Not only in advanced cybercrime investigations, as in, ransomware investigations, but also through the use of digital forensics in homicide cases where the suspect's smartphone is examined for forensic purposes. Smartphones and other portable "wearable" electronics leave digital traces that can be linked to persons and locations. The exponential growth of digital traces, as well as the expansion of cybercrime, and digitization of investigative methods represent significant changes to society and lead to a broadening horizon of digital investigation (Casey, 2017).

In its triennial report, the Dutch expert group on "Forensic Research and Innovation" views digitization in investigations as a "major development" (Expertgroep Forensisch Onderzoek en Innovatie, 2016). The expert group describes the above mentioned exponential growth of digital traces, as well as the expansion of cybercrime, and the digitization of investigative methods as significant changes to society.

Prior to formulating its registration requirement, the Netherlands Register of Court Experts (cf. Table 1 below) conducted a survey among forensic experts and users of expert reports (e.g. judges, public prosecutors and lawyers) in 2014. The response showed that forensic experts and users of expert reports highly favour the introduction of Digital Forensics as a new field of expertise. Because of—amongst other things—the rapid developments in digital forensics as well as the survey results, the Board of Court Experts decided to set standards for the field of expertise Digital Forensics in 2014.

In this article, we will explain how these standards were developed in the Netherlands. In addition, we aim to inform the future users of expert reports, such as judges and lawyers, what

* Corresponding author.
E-mail address: henseler.h@hsleiden.nl (H. Henseler).

https://doi.org/10.1016/j.diin.2018.01.010

Table 1
The NRGD explained.

The NRGD

The Netherlands Register of Court Experts (Nederlands Register Gerechtelijk Deskundigen, NRGD) (NRGD, 2015) was created in response to government legislation entitled "Experts in Criminal Cases Act". This Act took effect on 1 January 2010 and sets legal requirements for the quality, reliability and competence of experts. The NRGD is the first register of experts with a legal basis and an independent status, which also receives structural public funding. The NRGD is headed by an independent Board of Court Experts (the Board). The Board has seven members, including three scientists and one member for each of the groups using the register: the Judiciary (the Chair), The Public Prosecution Service, the Police and the Defence.

Various fields of expertise

The register is open for applications in various fields of expertise, including: DNA analysis and interpretation, Forensic Toxicology, Forensic Weapon and Ammunition Examination, Forensic Psychiatry and Psychology and Forensic Pathology. Several new fields of expertise will be added to the register in the coming years. Recently, the NRGD set standards for the field of expertise of Legal Psychology.

The NRGD in numbers:

- >1000 applications received for registration and re-registration
- 80% of applications leads to registration-20% rejection
- 550 registered experts
- 58 objections to NRGD decisions
- 6 court appeals to NRGD decisions

standards the NRGD requires court experts in Digital Forensics to meet, and what these users can expect from a registered expert. Before doing this we will outline related developments in other regions.

Setting standards for digital forensics

The NRGD Standards on Digital Forensics and application instructions were published on the website of the NRGD (NRGD, 2015) in 2015. This paragraph explains how these standards were set.

Subfields

The first meeting of the Advisory Committee for Standards (ACS) Digital Forensics was held at the end of 2014. An ACS consists of (international) experts in a particular field of expertise and a lawyer. During these meetings, the committee determines the demarcation of the field of expertise. The major question for the ACS Digital Forensics was to decide what activities were to be include in the demarcation and to define the boundaries of the field of expertise.

Over the past twenty years, a variety of articles has been published about digital forensics demonstrating that the field consists of a wide range of specialisms (e.g (Henseler et al., 2000; Henseler and Siegel, 2000)). There is no such thing as an all-purpose "Digital Forensics expert". On the contrary, the field of expertise is divided into different subfields. The committee has based the categorization, among other things, on a recent ontology by Karie & Venter (Venter (2014). At the top level they distinguish six categories that are broadly defined, in consideration of the rapid developments in this particular field of expertise. A more narrowly defined list of (sub) specialisms for the Digital Forensics experts would risk being out of date when it was published.

Consultation

The process of setting standards for various fields of forensic expertise in general is demonstrated in Fig. 1. After the meetings of the Advisory Committee for Standards, a preliminary draft was formulated. This draft was subsequently published in the NRGD newsletter and on the NRGD website with a call for comments to digital forensic experts.

Additionally, the NRGD has also proactively approached experts to express their views. In 2015, the NRGD presented the preliminary draft at the annual European edition of the Digital Forensic Research Workshop (DFRWS) conference in Dublin. During this meeting, the NRGD not only received comments from Dutch experts, but also from foreign experts from countries including the United States, Italy and South Africa. These comments were incorporated into the final draft that the Advisory Committee for Standards (ACS) submitted to the Board.

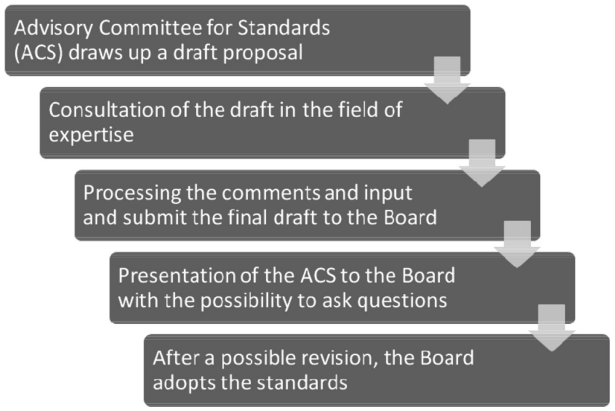

Fig. 1. Process of setting standards per field of expertise.

Establishment of standards for digital forensics and assessment of experts

The Standards Digital Forensics were finally codified by the Board of Court Experts in June 2015. Digital Forensics experts are assessed by the Advisory Committee for Assessment (ACA) on the basis of these standards. The Board has appointed experts from various countries as members of the ACA including the Netherlands, Germany, Italy, the United Kingdom and South Africa. Aspiring experts are informed of the requirements for the assessments by means of a workshop. Each application for registration is reviewed by a committee of at least three members consisting of two field experts and a lawyer. The lawyer is not necessarily knowledgeable on the field of expertise but is an expert on relevant Dutch (case) law and also has experience with assessments of experts in other fields of forensic expertise. For each application the ACA completes an advisory evaluation form and presents its recommendation to the Board.

The NRGD has so far received nine applications for registration for the new field of Digital Forensics. The assessments took place in July and December 2016. In total eight applicants have been registered and the registration of one applicant is on hold. These first applicants all practice digital forensics in the Netherlands. A

call to both Dutch and non-Dutch experts has been published for the next round of assessments, It is expected that more Dutch experts will apply as well as some of the non-Dutch members of the ACA, who have now had some experience with the registration process of the NRGD. After this second round enough experts will have registered for all subfields so that the register can be published. In 2017, 2018 the international Digital Forensics community will be approached to with a view to eventually getting more non-Dutch experts registered.

Demarcation of digital forensics

Core activities

The activities which fall within the Digital Forensics field of expertise are divided in three phases: data collection, data examination and data analysis. Data collection involves the correct preservation and copying of digital data sources. Data examination relates to the investigation of copies of digital data sources to find files, fragments etc. without interpreting the resultant findings in the context of the case. Data analysis involves the analysis, reconstruction, interpretation and qualification of the evidence which is obtained from the digital data sources. Digital Forensics experts are expected to be able (in principle) to carry out every phase of Digital Forensics (data collection, data examination and data analysis) themselves.

Relevant questions

The kind of questions experts under review are asked to address differ for each phase of the digital forensic investigation (cf. Tables 2–4).

Typically, standard tools i.e., both hardware and software and related procedures are used during the "data collection" phase. If other tools and/or methods are applied, an expert has to explain how the principle of forensic integrity is guaranteed.

Standard industry equipment can also be used during the "data examination" and "data analysis" phases. However, the expert will have more possibilities to do the examination depending on his own knowledge and understanding. Questions may include the following: how are deleted data reconstructed, what is the probability that data were manipulated, are patterns in network traffic correctly visualized, etcetera?

During the "analysis phase", it may be interesting to know how certain data ended up in a device. Relevant questions at this stage include: are preserved data more likely under a given scenario or under some alternative scenario? How much knowledge about digital forensics does a suspect need to manipulate evidence?

Table 2
Example questions in the data collection phase.

The following are some of the questions that are relevant for the "data collection phase" within the field of Digital Forensics:
1. Was the electronic equipment correctly secured?
2. The bypassing of the access code correctly carried out?
3. The data correctly safeguarded from complex infrastructures like industrial control systems?

Demarcation

As stated in paragraph 2.1, the field of Digital Forensics is the 8th field that is opened for registration after: 1. DNA-analysis and interpretation, 2. Handwriting Examination, 3. Forensic Psychology, 4. Forensic Toxicology, 5. Drugs-analysis and interpretation, 6. Weapons and Ammunition and 7. Forensic Pathology. Because of the complexity of the field, the ACS has decided to divide Digital Forensics in six subfields based on the ontology of Karie & Venter Venter (2014). An expert may be registered for one or more of the following subfields:

8.1 DF—Computer forensics
8.2 DF—Software forensics
8.3 DF—Database forensics
8.4 DF—Multimedia forensics
8.5 DF—Device forensics
8.6 DF—Network forensics

Computer forensics

Computer forensics uses analysis techniques to gather potential evidence from storage media (such as a hard disk) 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.

Software forensics

Software forensics deals with uncovering potential evidence through the examination of software. Software forensics covers for example operating system forensics, application software forensics and digital forensic analysis tools. 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.

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 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.

Table 3
Example questions in the data examination phase.

The following questions are among those that are relevant for the "data examination phase":
1. 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?
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 carrier when the data has been accessed, modified and/or changed?
4. In the 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?

Table 4
Example questions in the data analysis phase.

Questions relating to reconstruction:
1.a. Is digital evidence present on the material under examination?
1.b. What is the nature of the digital evidence on the material under examination?
1.c. How did the digital evidence end up on the material under examination?
These questions are aimed at providing a reliable reconstruction of how digital evidence ended up on the material under examination. After all, digital evidence can be produced in various ways.
Questions relating to interpretation:
2.a. Does the read data match a scenario outlined in advance?
2.b. Given alternative hypotheses, what can you say about the evidence that was found?
2.c. Given the evidence that was found, what can you say about the alternative hypotheses?
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.

Multimedia forensics

Multimedia forensics deals with the recovery and analysis of images, videos, and audio. 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. However, interpretation of multimedia content is not considered to be a part of the digital forensics field.

Device forensics

Device forensics is a subfield of Digital Forensics that deals with the gathering of digital evidence from different types of devices. These may range from small-scale devices such as mobile phones, tablets, navigation systems, external hard drives, cameras etcetera, to large-scale devices such as 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.

Network forensics

Network forensics is a branch of Digital Forensics that focuses 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.

Boundaries of the field of expertise

The above-mentioned examples in different subfields testify to the vast range of specializations that exist today. It is obvious that many new specialisms will arise in the future, while other specialisms might disappear. Think about the impact of the Internet of Things: devices will become "smarter" and communicate via the Internet. 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 recognize immediately that his own expertise or specialism is not adequate to carry out the digital forensic examination.

Complex investigations

In many cases, expertise will be required that covers multiple subfields. It is not unusual in such cases for multiple experts to collaborate if it is not possible to find a single expert that is registered for all relevant subfields. This problem is illustrated by a case with the codename "Dagger". This case was first reported on the website of the Dutch Public Prosecution Service in 2015 and came up for trial in January 2016 (Rechtstpraak, 2016).

In June 2013 the Dutch public prosecutor reported that criminals involved with drugs in the port of Antwerp in Belgium hacked the internet sites of two large container terminals (Parket, 2013; Pol, 2015). This enabled them to manipulate the location and movement of containers containing hidden drugs. Truck drivers from the criminal organization would subsequently show up at the terminal and pick up the containers before drivers from the official transportation company arrived.

Also, computers of forwarders and shipping companies in Belgium were manipulated by installing malware via phishing attacks. The emails originated from a Dutch IP-address. Screenshots and keystrokes were recorded and subsequently transmitted to an external server that belonged to the criminals. When this proved no longer effective the criminals broke into the premises and fitted key logging devices and other spying hardware (Bbcworldnewslive225, 2013).

This case involves a wide variety of digital traces. The phishing emails infected computers with a virus. This may require expertise in computer, software and network forensics. Furthermore, understanding the operation of key loggers and in particular of other small devices that were hidden in external hard drive casings and power extension cords to obtain remote access may require expertise in device forensics.

A lawsuit against the computer experts that are suspected of having assisted the criminals is still in progress in Belgium. According to Europol, hiring computer expert services by criminal

organizations is not unusual. There is evidence of a complete online service industry where organized crime can purchase hacking skills (Bateman, 2013).

Registration requirements digital forensics

General vs. specific registration requirements

The general registration requirements for forensic experts are stated in the second paragraph of Article 12 (Expert in Criminal Cases Decree). Similar to those for other fields of expertise, these general requirements are worked out in detail in the official registration requirements and assessment procedure for Digital Forensics, published on the NRGD website since February 2016.

In general, an expert must be competent to (a) elaborate on a strategy and answer relevant research questions, (b) to collect necessary data, and be able to document and evaluate this material in a forensic context, and, (c) to apply investigative methods and techniques in a forensic context.

It is especially important for Digital Forensics experts to be aware of the limitations of equipment used and methodologies applied, due to the rapid developments in this field. In most cases, the expert has to depart from forensic standards and use alternative tools. In such a situation, the expert should be able to demonstrate the methodology he applied. If he developed a new tool, a clear specification, design and evaluation must be available for non-specialists who do not know the limitations of the tool.

Education

Another registration requirement is related to the education of the Digital Forensics expert. An expert should have at least 3 years of relevant work experience at the level of an academic Master's Degree or at least 5 years at the level of an academic Bachelor's Degree, preferably in the field of technical IT.

In view of the rapid developments in the field of IT, an expert must also demonstrably have interpreted and reported a minimum of 5 case reports in the preceding 5 years and have followed a minimum of 50 h of forensically relevant professional development (e.g., attending conferences, running or attending courses, publications).

For each stipulated subfield the reporter should submit at least two case reports. The applicant should also have adequate knowledge of Dutch criminal law. If (foreign) experts do not (yet) meet this criterion, they may follow a tailor-made course “Introduction to Dutch (criminal) law for expert witnesses”, authorized by the NRGD (Faculty of Law, 2017a; Faculty of Law, 2017b).

Related developments

Netherlands-commission triennial report

The previously mentioned expert group “Forensic Research and Innovation” identifies several aspects for quality improvement in its triennial report. Besides the process of setting standards by the NRGD, two other aspects are important: the accreditation of laboratories, and professionalization through process control and protocolling (e.g., by documenting best practices).

In his response to the report, the Dutch Minister of Security and Justice underlined the importance of a “one-stop shop” in which the Netherlands Forensics Institute will function as a counter for all applications in forensic technical and medical examinations (Steur, 2015/16). The reason that is given for this is that the NFI is best informed about the range of forensic suppliers, their strengths and weaknesses, and as such is in the best position to guard their quality.

The objective is that the one-stop-shop is operational since January 1st, 2017. The “Forensic Research and Innovation” expert group recognizes the importance of a one-stop-shop in its report, but raises questions about the optimization of the quality assurance and the role of the NFI to achieve this.

It remains unclear to what extent the quality of digital forensics will benefit from these developments, especially as substantial investment in digitization in relation to (forensic) technical examination is not deemed necessary by the Dutch Minister. Moreover, both the Dutch National Police and the NFI are currently engaged in large reorganizations. Secondly, there is no extra budget available for the Ministry to make additional investments.

International-United Kingdom

Initiatives in the United Kingdom comparable to the NRGD stranded due to the lack of a legal basis and funding. However, the Forensic Regulator is currently developing quality standards (U. K. Forensic Science Regulator, 2015). While the Dutch NRGD focuses on the certification of individuals, quality assurance procedures in the UK are aimed at accreditation of standards for laboratories and codes of conduct. Because of the continuous developments in this field of expertise, Digital Forensics is the first focus point of the Forensic Regulator. The first forensic activities will be accredited in 2017 (cf. Table 5 below).

International-European Union

Improvement of the international approach of cybercrime was one of the priority points during the Dutch Presidency of the EU in the first half of 2016. This improvement relates predominantly to operational cooperation including the realization of a single European forensic science area. In cooperation with Europol, Eurojust and investigative authorities of other member states, the police and the Public Prosecution Service will analyse current and potential bottlenecks and subsequently draw up a list of recommendations. Efforts are also focused on strengthening the collaboration between European public prosecutors by establishing a network of dedicated cybercrime prosecutors (Steur, 2015/16).

The Netherlands aims at drafting a shared EU vision on jurisdiction in cyberspace. The recently adopted Action Plan (Presidency of the Council of the European Union, 2016) for the realization of a

Table 5
NRGD forensic quality symposium 2016.

On June 30th, 2016, the UK Forensics Regulator, Ms.G. Tully PhD, and Cybercrime and Digital Investigations professor at the University of Lausanne, Prof. E. Casey PhD, were guest speakers at the Forensic Quality Symposium of the NRGD. This annual symposium aims to exchange knowledge about the state of the art in the broader forensic field. Tully emphasized that digital forensics is a young field that is constantly developing. This in itself is a reason to develop standards and after a difficult start in the UK there is now progress. A cell site analysis pilot is being conducted with 7 participants from Police as well as private organizations. Also more than 95% of police organizations have implemented ISO 17025 procedures on the forensic acquisition of hard drives. Casey's presentation stressed the importance of trust in digital forensic evidence. He pleaded for the creation of a transparent culture which is necessary to increase trust in forensic evidence and digital forensic evidence in particular. The symposium was also attended by a number of the (inter national) members of the ACA Digital Forensics. In the morning they participated in a workshop about the ACA procedure. The day after the symposium they conducted the first assessments for applications of experts in various subfields of digital forensics.

European forensic science area plays an important role for the European Network of Forensic Science Institutes (ENFSI). The Working Group Forensic Information Technology of ENFSI prepared a Best Practice Manual (BPM) for digital forensics in 2015 (Working group on Forensic Information Technology, 2012). Founded in 1997, this working group exchanges knowledge and experience, and sets up mutual agreements to improve the quality of digital forensics.

In 2016 the University of Lausanne in Switzerland appointed Eoghan Casey as professor of Cybercrime and Digital Investigations (see Table 5). It may be expected that with his US background as well as the US and EU collaboration in the DFRWS conference the Digital Forensics standards between EU and US will be more harmonized, which will probably reflect on other regions in the world as well.

International-United States

There is less emphasis on the certification of individual experts in the United States, but all the more on the accreditation of tools, laboratories and description of best practice manuals. The Scientific Working Group on Digital Evidence (Website of the US Scientific Working Group on Digital Evidence, 2017) (SWGDE) is mainly active in developing best practices. Affiliated organizations to this working group reached consensus on the basic principles of accreditation (quality improvement) but do not want to create any mandatory requirements for forensic service providers.

At this moment, the SWGDE attempts to develop a complement to the ISO 17025 standard. This standard is used by authorities which are responsible for accreditation, such as the ASCLD (American Society of Crime Laboratory Directors).

The National Institute for Standards and Technology (NIST) has a Computer Forensics Tools Testing project (The National Institute for Standards and Technology, 2017) that is also well-known outside the United States. Digital Forensics software developers use this project to test their tools.

Additionally, NIST has composed a scientific committee for forensics named: Organization for Scientific Area Committees for Forensic Science (OSAC) (Website of the US Organization for Scientific Area Committees for Forensic Science, 2017a). Via the working group "Digital Evidence" (Website of the US Organization for Scientific Area Committees for Forensic Science, 2017b), NIST aims at informing digital forensics experts about quality improvement and accreditation of new testing methods, techniques and education related to storage or transfer of digital evidence. In the OSAC newsletter of August 2016 (Organization of Scientific Areas Committees for Forensic Sciences, 2016) this working group sent out a survey to understand how the digital forensics community feels about the accreditation of digital forensic labs, standards for digital evidence and certification of examiners.

Future developments

It is especially important in Digital Forensics to pay attention to the education of those who will be the "users" of expert reports. Better understanding of the (sub) field of expertise could help users to put the right questions to the expert. For the users it is equally important to decide in consultation with the expert whether the question falls within the expert's competence or if a different or additional expert should be consulted.

In addition, education helps with reading and interpreting expert reports and the presented results. On the one hand, this is important for improving the truth finding process. On the other hand, education will help stakeholders make an informed decision if it is necessary to request a second opinion. A critical review of an expert report by other experts will increase quality and trust. The register at the NRGD is in the public domain and can be accessed by judges, prosecutors as well as defence lawyers.

Acknowledgement

The authors would like to acknowledge the work done by the members of the Advisory Committee for Standards Digital Forensics (Mr E. van Eijk MSc, Mr. R. van der Knijff MSc, Mr. R.J. Mora, professor H. Prakken PhD, C. Prickaerts MA, Mr. H. Schut MSc and professor P. Sommer). The authors would also like to thank Mr. M.M.A. Smithuis MSc, L.LM. (Director Bureau NRGD) for his valuable comments on an earlier version of this article and Mr. A.P.A. Broeders PhD, for proofreading the English version of this article.

Appendix A. Supplementary data

Supplementary data related to this article can be found at https://doi.org/10.1016/j.diin.2018.01.010.

References

Bateman, T., 2013. Police Warning after Drug Traffickers' Cyber-Attack. BBC News. https://www.bbc.com/news/world_europe_24539417. (Accessed 12 January 2018).

Bbcworldnewslive225, 2013. Bbc News Police Say Crime Gangs Use Hackers to Traffic Drugs. https://youtu.be/eqnaKQ3jcPY. (Accessed 12 January 2018).

Casey, E., 2017. The broadening horizons of digital investigation. Editor. Digit. Invest. 21, 1–2.

Expertgroep Forensisch Onderzoek en Innovatie, 2016. Driejaarlijkse signalering forensisch onderzoek en innovatie. Kamerstukken II 2015/16, 29279, 328. https://www.rijksoverheid.nl/documenten/rapporten/2016/06/13/tk-bijlage-driejaarlijkse-signalering-expertgroep-forensische-onderzoek-en-innovatie. (Accessed 12 January 2018).

Faculty of Law, 2017. Specialisatieopleiding deskundige in strafzaken. Maastricht University. https://www.maastrichtuniversity.nl/nl/over-de-um/faculteiten/rechtsgeleerdheid/onderwijs/postacademisch-onderwijs-pao-0. (Accessed 12 January 2018).

Faculty of Law, 2017. Specialisatieopleiding gerechtelijk deskundige. Leiden University. https://www.paoleiden.nl/cms318-rechtsgebieden/burgerlijk-recht/1017-specialisatieopleiding-gerechtelijk-deskundige-leergang-19. (Accessed 12 January 2018).

FBI, 2016. Incidents of Ransomware on the Rise. https://www.fbi.gov/news/stories/incidents-of-ransomware-on-the-rise. (Accessed 12 January 2018).

Hayter, A., 2015. Will 2016 Be the Year of Ransomware? https://www.infosecurity-magazine.com/opinions/will-2016-be-ransomware. (Accessed 12 January 2018).

Henseler, J., 2000. Computer crime and computer forensics. In: Siegel, J. (Ed.), Encyclopedia of Forensic Sciences. Academic Press.

Henseler, J., Roording, J., 2000. Information technology. the development and regulation of new forensic investigative method. In: Nijboer, J., Sprangers, W. (Eds.), Harmonisation in Forensic Expertise: an Inquiry into the Desirability of and Opportunities for International Standards. Thela Thesis, Amsterdam, The Netherlands, pp. 233–255.

National Cyber Security Centre, 2016. Csbn 2016-ransomware is gemeen-goed en is nog geavanceerder geworden. https://www.ncsc nl/actueel/dossiers/csbn2016_ransomware.html. (Accessed 12 January 2018).

NRGD, 2015. Standards Digital Forensics and Registration Application Form. NRGD website. www.nrgd.nl/registreren/digitaal_forensisch_onderzoek.aspx. (Accessed 12 January 2018).

Organization of Scientific Areas Committees for Forensic Sciences, 2016. Osac Digital Evidence Subcommittee Survey on Accreditation, Standards and Certification. OSAC Newsletter of August 2016. https://www.nist.gov/topics/forensic-science/osac-newsletter-august-2016. (Accessed 12 January 2018).

Parket, L., 2013. Drugshandelaren hacken rederijen en ontvreemden containers met cocaïne. https://www.om.nl/vaste-onderdelen/zoeken/@31904/drugshandelaren/. (Accessed 12 January 2018).

Pol, W.v.d., 2015. Gehackte haven, cokesmokkel 2.0. Series of 6 articles. https://www.crimesite.nl/gehackte-haven-cokesmokkel-2-0-1. (Accessed 12 January 2018).

Presidency of the Council of the European Union, 2016. Draft council con- clusions and action plan on the way forward in view of the creation of an european forensic science area. https://data.consilium.europa.eu/doc/document/ST-8770-2016-INIT/en/pdf. (Accessed 12 January 2018).

Rechtstpraak, 2016. Uitspraak in mega zaak dagger. invoer cocaïne uit zuid-amerika. https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI. (Accessed 12 January 2018). NL:RBROT:2016:6465.

Steur, A.v.d., 2015/16. Kamerbrief met reactie op de 1e driejaarlijkse sig- nalering. Kamerstukken II 2015/16, 32317, 378. https://www.rijksoverheid.nl/documenten/kamerstukken/2016/06/13/tk- reactie-op-de-eerste-driejaarlijkse-signalering. (Accessed 12 January 2018).

The National Institute for Standards and Technology, 2017. Computer Forensics Tools Testing Project. https://www.dhs.gov/science and-technology/nist-cftt-reports. (Accessed 12 January 2018).

U. K. Forensic Science Regulator, 2015. Forensic Science Regulator Annual Report 2015. https://www.gov.uk/government/publications/forensic-science-regulator-annual-report-2015. (Accessed 12 January 2018).

Venter, N.K.H., 2014. Toward a general ontology for digital forensic disci- plines. J. Forensic Sci. 59, 1231–1241.

Website of the US Organization for Scientific Area Committees for Forensic Science, 2017. https://www.nist.gov/forensics/osac.cfm. (Accessed 12 January 2018).

Website of the US Organization for Scientific Area Committees for Forensic Science, 2017. Website of the OSCA "Digital Evidence" Sub-Committee. https://www.nist.gov/topics/forensic-science/organization- scientific-area-committees-osac/digital-evidence-subcommittee. (Accessed 12 January 2018).

Website of the US Scientific Working Group on Digital Evidence, 2017. https://www.swgde.org. (Accessed 12 January 2018).

Wikipedia, 2017. Wannacry Ransomeware Attack. https://en. wikipedia.org/wiki/WannaCry_ransomware_attack. (Accessed 12 January 2018).

Wikipedia, 2017. Peteya (Malware). https://en.wikipedia.org/wiki/Petya_(malware). (Accessed 12 January 2018).

Working group on Forensic Information Technology, 2012. Best Practice Man- Ual for the Forensics Examination of Digital Technology. https://enfsi.eu/wp-content/uploads/2016/09/1_forensic_examination_of_digital_technology_0.pdf. (Accessed 12 January 2018).