AUXILIARY QUESTIONS FOR EVALUATING ELECTRONIC EVIDENCE

Juhana Riekkinen

Researcher, University of Lapland, Faculty of Law
Yliopistonkatu 8, PO BOX 122, 96101 Rovaniemi, FI
juhana.riekkinen@ulapland.fi; http://bit.ly/2qvkbYk

Keywords: ***Computer Data, Criminal Procedure, Electronic Evidence, Evaluation of Evidence***

Abstract: *In a society where ICT and computer networks are ubiquitous, triers of fact are frequently confronted with real evidence in electronic and digital format. Computer data can be crucial in proving both online and offline events with links to suspected criminal acts, but it is often difficult for the trier of fact to determine the exact meaning and evidentiary value of such material. In this paper, a set of auxiliary questions are proposed to aid triers of fact in evaluating electronic evidence rationally. The proposed auxiliary questions relate to the origins, processing, and content of computer data proffered as evidence, as well as relations between such data, other evidence, and background knowledge.*

1. Introduction[1]

The current and developing Network Society is characterized by the ubiquity of ICT and computer networks. Because of this, real evidence in electronic and digital format is increasingly important in court proceedings. Different sorts of electronic traces consisting of computer data can be very useful in proving both online and offline events with links to suspected criminal acts, and can therefore be used as evidence in all kinds of criminal cases, including cybercrime and crime in the physical world. Computer data – as well as evidence consisting of computer data, in this paper termed *electronic evidence*[2] – are notoriously volatile, modifiable, duplicable, transferrable, voluminous, and dependent on machinery and software.[3] In the context of a criminal trial, it may be difficult to determine whether computer data (e.g., an e-mail message, a document file, a network log file, a photograph, or a video clip) proffered as evidence are authentic, and whether their integrity has

[1] This paper is based on my doctoral dissertation (Riekkinen, Sähköiset todisteet rikosprosessissa [=Electronic Evidence in Criminal Procedure], Alma Talent, Helsinki 2019 (forthcoming)), in which the idea of auxiliary questions for evaluating electronic evidence is further discussed.

[2] United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime, Draft, United Nations, New York 2013, p. 157 defines electronic evidence (in the context of criminal proceedings) in the following way: «Evidence is the means by which facts relevant to the guilt or innocence of an individual at trial are established. Electronic evidence is all such material that exists in electronic, or digital, form.» The European Commission defines electronic evidence as «data stored in electronic form – such as IP addresses, e-mails, photographs, or user names – that is relevant in criminal proceedings». European Commission, Security Union. Facilitating access to electronic evidence. https://ec.europa.eu/info/sites/info/files/placeholder_2.pdf (accessed on 27 November 2018), 2018, p. 1. Definitions for the term *digital evidence* are usually similar: e.g., Casey, Digital Evidence and Computer Crime. Forensic Science, Computers and the Internet 3rd Edition, Academic Press, Waltham 2011, p. 7: «any data stored or transmitted using a computer that support or refute a theory of how an offense occurred or that address critical elements of the offence such as intent or alibi». Cf. Schafer/Mason, The characteristics of electronic evidence. In: Mason/Seng (Eds.), Electronic Evidence 4th Edition, Institute for Advanced Legal Studies, London 2017, pp. 19-20, who use electronic evidence as an umbrella term for digital evidence (computer data) and *analogue evidence* (output of electronic but analogue devices). In this paper, analogue evidence is not considered, despite the choice of electronic evidence as the basic term.

[3] Generally, see Council of Europe, Explanatory Report to the Convention on Cybercrime. https://rm.coe.int/16800cce5b (accessed on 27 November 2018), 2001, paras 133-134, 155, 256, 282; Schafer/Mason, The characteristics of electronic evidence. In: Mason/Seng (Eds.), Electronic Evidence 4th Edition, Institute for Advanced Legal Studies, London 2017, pp. 18-35.

been compromised. Consequently, it may be difficult for the trier of fact to determine the exact meaning and evidentiary value of such material.

Evaluation of evidence may be approached from many different perspectives. Models proposed in the existing literature include probabilistic[4], story-based[5], explanation-based[6], and argumentation-based[7] approaches, as well as various combinations thereof[8]. I argue that regardless of the general model or method of evaluation employed, the evaluation of electronic evidence could be supported by considering certain auxiliary questions. The questions that I propose have the aim of helping the trier of fact to recognize misconceptions about the meaning or relevance of computer data presented as evidence, and to focus on issues that may have an effect on the evidentiary value of various kinds of electronic evidence (potential sources of error, in particular). A further goal is gaining a perspective on the entire path of the information with evidentiary value. The auxiliary questions are not designed to replace any of the existing models or methods of evaluation, but to complement them.

Throughout the paper, my primary focus is on criminal procedure and evaluation of evidence in the criminal trial. Naturally, electronic evidence can be useful in civil cases, as well. I believe that most of the ideas presented in this paper and the auxiliary questions themselves are largely applicable also to civil cases, and further, to evaluation of electronic evidence in any context.

2. Origins of electronic evidence

The first subset of auxiliary questions relates to the origins of the computer data used as evidence. Information is stored in machine-readable, digital and electronic form through various mechanisms that typically combine different kinds of manual, semi-automatic, and automatic processes.[9] The existence of electronic evidence relating to a criminal act is often a «happy accident»: computer data with evidentiary value is frequently processed and stored for some primary purpose other than use in a courtroom. While such accidental evidence may not be quite as good as computer data that are created and stored for the specific purpose of serving as evidence in the future,[10] such material is practically necessary in proving crimes in the Network Society.

---

4 Probabilistic approaches share a «mathematical» or «Pascalian» understanding of probability. In Anglo-American discussion, applications of Bayes' Theorem have been prevalent. See, e.g., Eggleston, Evidence, Proof and Probability 2nd Edition, Weidenfeld and Nicolson, London 1983; Robertson/Vignaux/Berger, Interpreting Evidence. Evaluating Forensic Science in the Courtroom 2nd Edition, John Wiley & Sons, Chichester 2016. In Finland, the discussion on mathematical probabilities and evidence was led by Hannu Tapani Klami and his research group, who further developed a version of Per Olof Ekelöf's Evidentiary Value method during the late 1980s and 1990s. See Klami/Gräns/Sorvettula, Law and Truth. A Theory of Evidence, The Finnish Society of Sciences and Letters, Helsinki 2000. Cf. the concept of «inductive» or «Baconian» probability adopted by Cohen, The Probable and the Provable, Clarendon Press, Oxford 1977.

5 E.g., Pennington/Hastie, A Cognitive Theory of Juror Decision Making: The Story Model, Cardozo Law Review, Volume 13, Issue 2-3, 1991, pp. 519-557; Wagenaar/van Koppen/Crombag, Anchored Narratives. The Psychology of Criminal Evidence, Harvester Wheatsheaf, Hemel Hempsted 1993. In mid-1990s, Christian Diesen proposed a «hypothesis model» of evaluation for criminal cases. Diesen's model, which has become highly influential in Nordic countries, focuses on disproving alternative hypotheses, and is related to the Anglo-American story-based models and Cohen's inductive reasoning. See Diesen, Bevisprövning i brottmål, Juristförlaget, Stockholm 1994.

6 E.g., Pardo/Allen, Juridical Proof and the Best Explanation, Law and Philosophy, Volume 27, Issue 3, 2008, pp. 223-268; Amaya, Inference to the Best Legal Explanation. In: Kaptein/Prakken/Verheij (Eds.), Legal Evidence and Proof. Statistics, Stories, Logic, Ashgate, Farnham 2009, pp. 135-159.

7 E.g., Bex/Prakken/Reed/Walton, Towards a formal account of reasoning about evidence: Argumentation schemes and generalisations, Artificial Intelligence and Law, Volume 11, Issue 2-3, 2003, pp. 125-165.

8 E.g., Bex/van Koppen/Prakken/Verheij, A hybrid formal theory of arguments, stories and criminal evidence, Artificial Intelligence and Law, Volume 18, Issue 2, June 2010, pp. 123-152; Vlek/Prakken/Renooij/Verheij, A method for explaining Bayesian networks for legal evidence with scenarios, Artificial Intelligence and Law, Volume 24, Issue 3, September 2016, pp. 285-324.

9 See Mason, Electronic evidence: dealing with encrypted data and understanding software, logic and proof, ERA Forum, Volume 15, Issue 1, 2014, pp. 31-32.

10 This is mostly because when computer data are generated and stored specifically to serve as evidence, their authenticity and integrity may be guaranteed by technical measures (such as digital signatures and/or hashing) from the beginning. However, in juris-

However, the original purpose of the processing may affect the design choices for the particular data processing activity or computer system, and this may be relevant for evaluation.

Regardless of whether the data have been created to serve as evidence or for some other purpose, the people who played a role in the creation (who in the subsequent criminal trial may be defendants, victims, witnesses, or third parties) may have had their own motives and reasons. Potentially biased individuals may have created the data to serve their particular needs and interests. Even when there is no identifiable human bias involved, the creators of the data or the designers and users of the (semi-)automated computer system that produced the data may have considered legal or evidential virtues to be insignificant. Therefore, the objectivity, accuracy, trustworthiness, and general evidential quality of the data may be limited, even if such data have been functional and usable for their intended primary purpose.

Identification of various manual and automated activities is important in order to focus the inquiry on the relevant types of potential sources of error. Roughly speaking, whenever data are generated or processed by automated systems, there is always a risk of user error, software error, hardware malfunction, or malicious interference. The first risk exists because very few systems are *completely* automated and free of any human interaction; the others can often be traced to a human error made earlier (for example, by a programmer, a system administrator, or a device manufacturer/designer). Whenever data are input or processed by natural persons, there is always a risk of unintentional human error, bias, or malice.[11]

Identification of both the primary purpose of data processing and the exact processing activities helps the trier of fact to determine the probandum for which the data are capable of attesting to directly. This is also helpful in determining the steps that need to be taken in order to get from the textual, audio-visual, or other observable content of the data to the ultimate probandum, i.e., a fact with direct legal implications and effects that is in dispute. Taking notice of the intermediary probanda, which are often numerous when it comes to electronic evidence,[12] is vital for recognizing different sources of error that may impair the link between the data and the probandum that a party tries to prove.[13] After such analysis, it might even be observed that a piece of evidence, which superficially appeared to be highly relevant, bears no evidentiary value in relation to the probandum to be proved.

Consequently, a number of potential sources of error may be probed by considering at least the following questions:

– How were the data originally created or how did they come to being?

---

dictions following the free theory of evidence there are usually no legal rules which require that «accidental» evidence be given less weight than «intentional» evidence, or other such rules that prescribe strict hierarchies of different categories of evidence.

11 See also Mason, The presumption that computers are «reliable». In: Mason/Seng (Eds.), Electronic Evidence 4th Edition, Institute for Advanced Legal Studies, London 2017, pp. 120-130, 143-145, 163-166.

12 See Schafer/Mason, The characteristics of electronic evidence. In: Mason/Seng (Eds.), Electronic Evidence 4th Edition, Institute for Advanced Legal Studies, London 2017, p. 35: «The nature of digital evidence, so our claim proposes, is that on a like-by-like comparison and allowing for the machine-mediated nature of electronic evidence, the evidence will be several steps further removed from the ultimate probandum when compared with traditional evidence.» See also Redford/Agah, Evidentialist foundationalist argumentation for multi-agent sensor fusion, Artificial Intelligence Review, Volume 42, Issue 2, August 2014, p. 219.

13 A crucial step in criminal cases is the attribution of online and digital acts to a specific natural person (United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime, Draft, United Nations, New York 2013, p. 169; see also Casey, Reconstructing Digital Evidence. In: Chisum/Turvey, Crime Reconstruction, Academic Press, Burlington 2006, pp. 431-433). To give a simple example: A log entry states that the user «johndoe» logged into a specific computer system at a specific time. If the trier of fact erroneously believes that this directly proves that the natural person John Doe logged into that system at that time, such attribution may be done baselessly. Instead, the trier of fact needs to recognize that such a log entry can only directly attest to the fact that someone, using the user account «johndoe», logged into the system at that time (and even this is not unequivocally proved, obviously, since the entry could have been forged or been produced by a malfunctioning system). Then, we may rationally further consider whether it is likely that someone other than John Doe could have used the username allocated to him and his password (or perhaps a biometric identifier) to log in to the system at the given time. By recognizing this intermediary step, we can more accurately evaluate the meaning and weight of this evidence as to the ultimate probandum.

- Who or what created the data or input them in a computer system?
- For what purpose were the data originally created?
- What roles did manual and automatic data processing play in the creation of the data?
- What specifically do the data depict or represent, and what conclusions can be drawn directly from them?
- Which steps lie between the data and their ultimate probandum?

3. Processing of electronic evidence

The second subset of questions concerns the further processing of computer data. Even if computer data were accurate and relevant to a legally significant probandum when they were created, their integrity may have been impaired subsequently. Any processing activity may result in loss or corruption of the original data, or the addition of new data. Data may be modified unintentionally or intentionally in various processing stages before the evidence is presented in the courtroom.

In criminal cases, the police or other law enforcement agencies process the computer data with evidentiary value. Authorities should be able to control and document these processing steps by using various technical, physical, organizational, and other safeguards, establishing an unbroken chain-of-custody and audit trail from the moment they took possession of the data. For example, any examination of the contents of a seized hard disk should be performed using generally accepted forensic methods, and be appropriately documented to allow for *ex post* review of the measures and their results. To guarantee the integrity of data in such examinations, operations should normally be performed on bit-for-bit copies (to avoid modifying or losing any data stored on the original device), and hash values should be calculated for all files at an early stage (to be able to demonstrate that the files have not been modified during the examination or tampered with).

In addition, third parties may have processed the data before collection by authorities. This kind of processing may be performed for purposes directly relating to the criminal proceedings (e.g., a telecommunications operator or a system administrator collecting data from a computer system in order to fulfil a production order), or for other purposes (e.g., automated copying and transfer of data between different cloud servers in order to guarantee efficient access to user-stored data or to maintain back-up copies). Law enforcement agencies do not have direct control over third party actions. Still, any information concerning such activities and measures taken to ensure or preserve the integrity of the data is relevant for the trier of fact.[14]

Processing steps that are taken in order to facilitate the presentation of evidence in the courtroom must not be forgotten. Transforming data into a more static format before presentation carries a risk of losing some of the data (often metadata or other «invisible» data), but also presenting evidence in native format (which may allow evidence to be presented more dynamically and flexibly) may cause modifications of the data during presentation.[15]

As already discussed in the previous section, information concerning the purpose and nature of any processing activities may help to isolate the critical issues that could potentially affect the evidentiary value of the data. If, for example, data have been selected from a larger data set and copied manually into a different file by a specific person in response to a specific data production request, possible human errors may need to be further

[14] Important electronic evidence is typically held by major Internet platform companies (such as Google, Apple, Microsoft, Facebook, and Amazon), telecommunications operators, various e-commerce platforms, and financial institutions. One widely recognized problem, particularly in cross-border investigations, is gaining access to such evidence. A different, far less emphasized set of problems relates to receiving the information needed to properly evaluate the evidence, i.e., sufficient information regarding the data processing practices and algorithms employed by these companies.

[15] About «native» or «live» and «static» format in presentation, see The Sedona Conference, The Sedona Conference Commentary on ESI Evidence and Admissibility. A Project of the Sedona Conference Working Group on Electronic Document Retention & Production (WG1). The Sedona Conference, 2008, pp. 18-19.

considered. If an algorithm has performed the selection and copying operations, it may be more useful to focus on the parameters used and the functionality of that algorithm.

Again, a list of key questions that may illuminate sources of error or other relevant issues relating to later processing steps can be presented. This subset of auxiliary questions includes at least the following questions:

- What manual and automatic data processing operations have the data been subjected to before being collected by the authorities, at the time of collection, and afterwards?
- Have the data been compiled, collated, selected, moved, copied, reformatted, or transformed during their life-cycle, and how have these operations been performed?
- What technical, physical, organizational, and other security measures have been employed in order to guarantee the authenticity and integrity of the data during their life-cycle?
- How have different data processing events been documented?
- Can an unbroken chain-of-custody be established reliably?

4. Content of electronic evidence and relations to other information

The third and final subset of questions directs attention to the content of computer data, as well as the relations between the content and other material available at trial, and between the content and general background knowledge. Naturally, the content of computer data is one of the most significant issues to consider in evaluation. If the content is textual information, the trier of fact needs to carefully analyze what the information means and whether it is generally believable in the sense that it is not unlikely, unrealistic, or flatly impossible in light of applicable general knowledge. The trier of fact also needs to analyze whether the content is internally consistent, and whether the document or file which is used to convey the information appears to be intact and whole, or whether something appears to be missing or out of place. Similarly, for audio-visual content such as digital pictures, videos, and audio recordings, the trier of fact needs to consider what it is that they can directly observe, as well as issues of believability, consistency, intactness, and wholeness.

With the help of modern IT, text, static pictures, sound, and even video can be manipulated with relative ease. For a layperson, it may be difficult to spot the more skillful forgeries with the naked eye, and settling concerns about the authenticity and integrity of documents or audio-visual material may require expert evidence based on thorough examination. However, sometimes even a sensory observation may still help to recognize impaired authenticity and integrity of the data. Another useful possibility is examining the metadata associated with or included in the file or message, which may be inconsistent with the purported content; for example, the Exif metadata of a JPEG file may reveal that the photograph was taken at a different time or at a different place than the party claims. Such inconsistencies, if left unexplained, may severely affect the evidentiary value of the evidence.

Of course, pieces of evidence cannot be evaluated solely in isolation. Probabilistic theories of evidence recognize this through mathematical formulas which allow for numerical evidentiary values or weights for individual pieces of evidence to be combined; probability values may be updated through the application of Bayes' Theorem, or different formulas may be utilized for evidentiary chains, corroboration, and contradiction. Other, more holistic theories of evidence focus on how well different pieces of evidence fit the stories, explanations, or hypotheses offered by parties. In this, the relations between different pieces of evidence obviously play some part. Regardless of the exact mechanism by which the mass of evidence as a whole is evaluated, consistency of evidence is clearly of importance in evaluation. This is not changed by the fact that (some of) the evidence is in electronic and digital format.

In case there are several pieces of evidence pointing in the same direction, the trier of fact needs to determine whether the pieces of evidence are independent or not. If the evidentiary mechanisms are sufficiently different,

the same sources of error are less likely to affect them, and concurring evidence can be given more weight in evaluation. However, if the pieces of evidence are products of the same mechanisms and processes, they may be affected by the same sources of error. If no sources of error can be ruled out, there is no corroboration, and the combined weight of the evidence as to a probandum is not (significantly) increased. Electronic evidence is often produced by mechanisms different from, i.e., eyewitness testimony, and these kinds of combinations of different types of evidence may be given considerable weight. Unfortunately, due to complexity, lacking transparency, and «black box» nature of many computer systems, it may be difficult to determine the level of independence when at least one of the pieces of evidence is the product of such a system. Triers of fact should be careful not to give excessive value to evidence pointing in the same direction when it is unclear if the pieces of evidence are truly independent or not.

Lastly, the trier of fact should consider possible explanations for any inconsistencies between content, metadata, other evidence, and general knowledge about the world. Some of the evidentiary value might be salvaged if there is a credible explanation that accounts for the inconsistency but also confirms or supports the notion that the piece of evidence is still logically capable of attesting for its intended probandum. For example, an inconsistency between the date marked on the first page of a PDF document and the «file created» timestamp data associated with the file might be explained by a) forgery or manipulation or b) unintentional update of the timestamp due to the file being copied to an external device. While the latter explanation might indicate bad forensic practices, it would allow the trier of fact to find that the content of the document is unmodified and its integrity has not been compromised in a way that would reduce its evidentiary value as to the probandum. The credibility (or «goodness») of explanations typically needs to be evaluated in light of other evidence. In the aforementioned example, support or counter-arguments for the two explanations might be found from documents concerning the chain-of-custody, testimonial evidence from people who handled the data, and expert evidence concerning the behavior of timestamps in the relevant file system. In addition, general knowledge about the basic operating principles of computer systems, or even about human behavior, could help to determine the quality of the possible explanations.[16]

As before, a non-exhaustive list of auxiliary questions may be compiled:

- Is the message, document file, media file, or other file consisting of computer data externally whole and intact?
- Is the textual or observable content generally believable?
- Is the textual or observable content internally consistent?
- Is the content consistent with metadata included or associated with the data?
- Is the content consistent with other evidence?
- Are the data independent in relation to concurring evidence, or have they been produced by an essentially similar (or the same) process?
- Is there a credible explanation for the internal and external inconsistencies related to the data?

5. Conclusions and limitations

Traditionally, the evaluation of real evidence has been based rather straightforwardly on the textual content of the document or directly observable qualities of the object. Unless there has been a specific reason to think otherwise, the material has been presumed authentic and unaltered. While the directly observable content of a given piece of electronic evidence is undeniably important in evaluation, it would be incorrect to ignore the perspectives of the first two subsets of auxiliary questions. Electronic evidence should not be presumed

[16] In generating and evaluating explanations for inconsistencies, the auxiliary questions relating to the origins and processing of the material may be very illuminating. Indeed, while considering explanations, the trier of fact should re-examine answers to questions such as: How, for what purpose, and by whom were the data created, and how have they been processed since?

inherently reliable, nor unreliable. Due to the nature of electronic evidence, focusing solely on the «end product» – i.e., the textual or audio-visual content of a computer file or printout presented in a courtroom as such – is unlikely to provide an objective and rational basis for evaluation. Together, the proposed auxiliary questions direct attention towards the life-cycle of data that are used as evidence, and encourage the trier of fact to consider the entire evidentiary process and the path of information that has led to this evidence being presented in court. Especially in the «post-truth» world of advanced digital data manipulation, evidentiary value needs to be derived increasingly from the history and the context of the evidence, not mere appearances.

I further submit that the party presenting electronic evidence – in the context of criminal trials, especially the prosecutor – should be prepared to provide adequate answers to such questions. Clearly, not every question must be thoroughly discussed during the trial in all situations and scenarios, especially if there are no challenges against the evidence from the opposing party. Nevertheless, if evidentiary value is derived from the history of the computer data and judges should consider these questions (as I suggest), then it is, of course, in the best interest of the parties to provide all possible information supporting the relevance, authenticity and integrity of their evidence, and to have explanations ready for any inconsistencies and weaknesses. Another point of view is that in the context of a criminal trial, the principle of equality of arms requires that the prosecution give the defendant access to information about the potentially exculpatory evidence gathered during the examination. In many countries, the prosecutor is also obliged to a certain degree of objectivity, which may require providing the court with exculpatory information, such as information concerning the possible weaknesses of the prosecution evidence.

The auxiliary questions, while useful, are not an all-encompassing solution for evaluation of electronic evidence. The list of questions presented in this paper is non-exhaustive, and further (similar and more specific) questions may be helpful in evaluation. Asking and answering the auxiliary questions does not mechanically lead to a correct decision, or even to any unquestionable, clear result. The auxiliary questions do not free the trier of fact from rigorous thinking and reasoning, and the precise effect of any answer to an auxiliary question needs to be determined by the trier of fact themselves, in the specific circumstances of each case. Further, the auxiliary questions are centered on the evidentiary value of a single piece of electronic evidence. As such, they do not directly aid in determining whether an individual, legally significant fact has been proved, whether the defendant's guilt has been proved beyond reasonable doubt, or whether some other standard of proof has been met.

However, an advantage of these auxiliary questions is that they do provide a framework for writing a well-founded judgment concerning factual issues (this obviously does not apply to *common law* jury trials or legal systems where a reasoned judgment on issues of fact is not required). Instead of flatly rejecting or accepting a piece of evidence or assigning it an arbitrary evidentiary value based on gut feeling, judges should, in general, adequately explain their reasoning on issues of fact. For electronic evidence, this is very difficult without an understanding of the life-cycle of computer data that are presented to the trier of fact in the courtroom. For any sort of rational reasoning concerning electronic evidence, it is important to recognize different kinds of potential sources of error that may be revealed by the three aforementioned subsets of auxiliary questions. I submit that considering these auxiliary questions and openly providing answers to them in the written judgment may lead to better justified and more transparent administration of justice.

6. References

Amaya, Amalia, Inference to the Best Legal Explanation. In: Kaptein, Hendrik/Prakken, Henry/Verheij, Bart (Eds.), Legal Evidence and Proof. Statistics, Stories, Logic, Ashgate, Farnham 2009, pp. 135-159.

Bex, Floris/Prakken, Henry/Reed, Chris/Walton, Douglas, Towards a formal account of reasoning about evidence: Argumentation schemes and generalisations, Artificial Intelligence and Law, Volume 11, Issue 2-3, 2003, pp. 125-165.

Bex, Floris/van Koppen, Peter J./Prakken, Henry/Verheij, Bart, A hybrid formal theory of arguments, stories and criminal evidence, Artificial Intelligence and Law, Volume 18, Issue 2, June 2010, pp. 123-152.

Casey, Eoghan, Reconstructing Digital Evidence. In: Chisum, W. Jerry/Turvey, Brent E., Crime Reconstruction, Academic Press, Burlington 2006, pp. 419-439.

Casey, Eoghan, Digital Evidence and Computer Crime. Forensic Science, Computers and the Internet, 3rd Edition, Academic Press, Waltham 2011.

Cohen, L. Jonathan, The Probable and the Provable, Clarendon Press, Oxford 1977.

Council of Europe, Explanatory Report to the Convention on Cybercrime. https://rm.coe.int/16800cce5b (accessed on 27 November 2018), 2001.

Diesen, Christian, Bevisprövning i brottmål, Juristförlaget, Stockholm 1994.

Eggleston, Richard, Evidence, Proof and Probability, 2nd Edition, Weidenfeld and Nicolson, London 1983.

European Commission, Security Union. Facilitating access to electronic evidence. https://ec.europa.eu/info/sites/info/files/placeholder_2.pdf (accessed on 27 November 2018), 2018.

Klami, Hannu Tapani/Gräns, Minna/Sorvettula, Johanna, Law and Truth. A Theory of Evidence, The Finnish Society of Sciences and Letters, Helsinki 2000.

Mason, Stephen, Electronic evidence: dealing with encrypted data and understanding software, logic and proof, ERA Forum, Volume 15, Issue 1, 2014, pp. 25-36.

Mason, Stephen, The presumption that computers are «reliable». In: Mason, Stephen/Seng, Daniel (Eds.), Electronic Evidence, 4th Edition, Institute for Advanced Legal Studies, London 2017, pp. 101-192.

Pardo, Michael S./Allen, Ronald J., Juridical Proof and the Best Explanation, Law and Philosophy, Volume 27, Issue 3, 2008, pp. 223-268.

Pennington, Nancy/Hastie, Reid, A Cognitive Theory of Juror Decision Making: The Story Model, Cardozo Law Review, Volume 13, Issue 2-3, 1991, pp. 519-557.

Redford, Chris/Agah, Arvin, Evidentialist foundationalist argumentation for multi-agent sensor fusion, Artificial Intelligence Review, Volume 42, Issue 2, August 2014, pp. 211-243.

Riekkinen, Juhana, Sähköiset todisteet rikosprosessissa, Alma Talent, Helsinki 2019 (forthcoming).

Robertson, Bernard/Vignaux, G. A./Berger, Charles E. H., Interpreting Evidence. Evaluating Forensic Science in the Courtroom, 2nd Edition, John Wiley & Sons, Chichester 2016.

Schafer, Burkhard/Mason, Stephen, The characteristics of electronic evidence. In: Mason, Stephen/Seng, Daniel (Eds.), Electronic Evidence, 4th Edition, Institute for Advanced Legal Studies, London 2017, pp. 18-35.

The Sedona Conference, The Sedona Conference Commentary on ESI Evidence and Admissibility. A Project of the Sedona Conference Working Group on Electronic Document Retention & Production (WG1). The Sedona Conference, 2008.

United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime, Draft, United Nations, New York 2013.

Vlek, Charlotte S./Prakken, Henry/Renooij, Silja/Verheij, Bart, A method for explaining Bayesian networks for legal evidence with scenarios, Artificial Intelligence and Law, Volume 24, Issue 3, September 2016, pp. 285-324.

Wagenaar, Willem A./van Koppen, Peter J./Crombag, Hans F., Anchored Narratives. The Psychology of Criminal Evidence, Harvester Wheatsheaf, Hemel Hempsted 1993.