|  |  |
| --- | --- |
| Lesson: 12 – Admissibility of Electronic Evidence | **Duration: 120 Minutes** |
| **Resources required for an off-line delivery:**   * Laptop or PC running an operating system with an office suite (capable of showing pptx) * Projector and display screen * Internet access (if available) * Whiteboard * Whiteboard pens (at least 2 each of blue, black, red and green) * 2 Flipcharts with adequate paper * Student notepaper and pens * Blu tack or a similar product to allow for paper to be affixed to the walls temporarily * Files: Session 12 Admissibility of EE.pptx   **Resources required for an on-line delivery:**   * Laptop or PC for each trainee (if attending from home) or for a groups of trainees, depending on availability * A strong internet connection * An online tool should be provided that allows video conferencing and is specifically aimed at providing training. Due to the fact that the trainers have to stay in visual contact with the trainees, it is important that when the slides are shown, the trainers still see the trainees (in some online video conferencing tools only the slide can be seen). It is in any case also a plus to be able to provide online break-out rooms. * Files: Session 12 Admissibility of EE.pptx | |
| **Aim:** Trainees should be aware that going to court with electronic evidence can only succeed if all parts of the chain in het electronic evidence flowchart have been completed correctly. The assessment and evaluation of the admissibility of electronic evidence is a very important element in this respect before that electronic evidence can be judged. It is, as it were, the penultimate link in the chain. it is a crucial link in the chain.  However well the electronic evidence may be identified, however securely secured, however sound and well-reasoned the prior authorisations may be, however professional the extraction and analysis of the electronic evidence may be, if it is technically and legally inadmissible this electronic evidence, it cannot be used by a judge to make his judgment.  The objective can be achieved by understanding and safeguarding five fundamental principles: the authenticity, completeness, reliability, believability and proportionality of the electronic evidence. | |
| **Objectives:**  At the end of this session, delegates will be able to:   * distinguish between the technical and legal collection of electronic evidence and the assessment of that same electronic evidence * understand that as magistrates (public prosecutor or judge) they have a particular important role to play in the assessment of that evidence * know the different elements with which electronic evidence has to be assessed in order to be admissible before a court and the judgment of a case * understand that a judge's evaluation of the admissibility of electronic evidence is the cornerstone of the whole process | |
| **Introduction**  Session 12 deals with the admissibility of the evidence before the court and is therefore the penultimate stage before the digital evidence can be used as evidence by a judge to make his judgment.  The trainees have learned in the previous sessions how to technically access the evidence and within which legal framework and with which tools. The trainees now need to learn how to assess that evidence (in terms of admissibility). They must learn that no matter how good evidence may appear to be, when it is not admissible it is of no value. So, as magistrates, they have a crucial role to play in safeguarding this.  There are three main parts.  In the first stage, it is important to know that the evaluation of the evidence can be different in each country and there are roughly two major systems, the civil law system and the common law system, but there are also hybrid systems.  Secondly, in order to proceed with the requirements of admissibility, it is important to recognize five fundamental principles leading to the admissibility of electronic evidence: authenticity, completeness, reliability, believability and proportionality. These five fundamental principles are explained in more detail in the slides.  As far as the authenticity of the evidence is concerned, an exercise is also linked to this (see below).  Finally, because even fundamental principles have to find their way into practice, the slides put forward five measures to be taken in order to translate these five principles into practice:   1. Safeguarding the **integrity of the data** 2. Creating an **audit trail** 3. Foreseeing **specialist support** 4. Providing **appropriate training** 5. Ensuring **legality**   The content of these slides speaks for itself. In the blue boxes, each time the summary advice is given, it is useful for the trainer to underline this.  All information about this session is included in the PowerPoint presentation entitled “Session 12 Admissibility of EE.pptx” in the resource pack. The trainer is responsible for ensuring that the materials are up to date. Changes may be made, however the objectives should be achieved. | |
| **Practical Exercises**  *There is a practical exercise in the slides 9-12.*  As regards the 'authenticity' of electronic evidence, at the level of knowledge of magistrates, it is explained how the calculation of a hash value is a tool that can prove that two files are completely identical and the file submitted to the court is indeed the file that was seized and is therefore authentic.  Slide 9 indeed shows twice the same picture of which the trainer or trainees can calculate the hash value (file "alexander seger.png"). This calculation is possible with freely available tools such as these at https://www.fileformat.info/tool/hash.htm. Please pay attention to the SHA-1 as well as the MD5 values.  In slide 10 it is immediately noticeable that the text under the image was changed from "HEAD OF CYBERCRIME DIVISION, COUNCIL OF EUROPE" to "HEAD OF ORGANIZED CRIMEGROUP ARRESTED". It is clear to the trainees that something has changed in the image, but it also becomes clear when calculating the hash value, which is different for both SHA-1 and MD5 ("alexander seger2.png" file).  In slide 11 for the "*die hards*" in the classroom, an example is given of two photos that are undeniably different, but of which the MD5 value turns out to be the same (photos in the teaching package “plane.jpg” and “ship.jpg”). The lesson given here is that the SHA-1 is indeed different and therefore it is best to use more than one calculation method.  This is finally ultimately demonstrated by an example from practice in slide 12. It concerns three photographs from an observation file where two targets were observed and where the hash value SHA-1, MD5 was calculated at the time the specialised police services took the photograph. The hash values must be the same to prove that Photoshop was not used to put two people together on a photo that they never met in real life.  *If there is time left, trainees can be asked whether they are familiar with case law of the European Court of Human Rights on the admissibility of evidence.*  There are certainly two interesting and useful references here:  1. CASE OF RAMANAUSKAS v. LITHUANIA, 5 February 2008 (http://hudoc.echr.coe.int/eng?i=001-84935)  *52. … The admissibility of evidence is primarily a matter for regulation by national law and, as a rule, it is for the national courts to assess the evidence before them. The Court, for its part, must ascertain whether the proceedings as a whole, including the way in which evidence was taken, were fair (see, among other authorities, Van Mechelen and Others v. the Netherlands, 23 April 1997, § 50, Reports of Judgments and Decisions 1997-III; Teixeira de Castro, cited above, § 34; Sequeira v. Portugal (dec.), no. 73557/01, ECHR 2003-VI; and Shannon v. the United Kingdom (dec.), no. 67537/01, ECHR 2004-IV). In this context, the Court’s task is not to determine whether certain items of evidence were obtained unlawfully, but rather to examine whether such “unlawfulness” resulted in the infringement of another right protected by the Convention.*  2. CASE OF GÄFGEN v. GERMANY, 1 June 2010 (http://hudoc.echr.coe.int/eng?i=001-99015)  *164. In determining whether the proceedings as a whole were fair, regard must also be had as to whether the rights of the defence have been respected. In particular, it must be examined whether the applicant was given an opportunity to challenge the authenticity of the evidence and to oppose its use. In addition, the quality of the evidence must be taken into consideration, as must the circumstances in which it was obtained and whether these circumstances cast doubts on its reliability or accuracy. While no problem of fairness necessarily arises where the evidence obtained was unsupported by other material, it may be noted that where the evidence is very strong and there is no risk of its being unreliable, the need for supporting evidence is correspondingly weaker (see, inter alia, Khan, cited above, §§ 35 and 37; Allan, cited above, § 43; and the judgment in Jalloh, cited above, § 96). In this connection, the Court further attaches weight to whether the evidence in question was or was not decisive for the outcome of the proceedings (compare, in particular, Khan, cited above, §§ 35 and 37).* | |