Lesson 1.3.2 Electronic Evidence Practice & Procedure

|  |  |  |
| --- | --- | --- |
| Lesson 1.3.2 Electronic Evidence Practice & Procedure | | Duration: 120 minutes |
| **Resources Required:**   * PC/Laptop loaded with software versions compatible with the prepared materials * Internet access (if available) * PowerPoint or other presentation * Computer hardware examples (if available) \* * Copy of the Council of Europe Electronic Evidence guide * Copy of the electronic evidence pre-read for this course * Printed copies of the appendices of the guide used in this session   \* It is recommended that the trainer obtains various pieces of computer hardware to use in the following section. These should include items that will contain evidence and others that do not, such as chargers, cables etc. These may then be handed to the delegates and each one asked if the piece of equipment they hold, may or may not contain electronic evidence. It is important to emphasise during the session that in addition to electronic evidence, items may contain traditional evidence such as fingerprints or DNA. The slides, numbered 18 to 42, depicting and describing devices are present to aid a trainer where it has not been possible to acquire physical devices for the course. The trainer may simply hide these slides where devices are used or use them for supporting materials. | | |
| **Session Aim:**  The aim of this session is to provide judges and prosecutors with the knowledge of issues relating to electronic evidence such as the various types that they may encounter, how it is recovered and handled during investigations and produced for criminal trials. Further knowledge about the challenges of retrieving such evidence from other jurisdictions is also provided. In addition, the transition of electronic evidence from seizure to examination and production is dealt with in the short session outlining the science of digital forensics. The level of detailed knowledge required by the delegates may vary, depending on the legal system in the country and the extent of involvement of the delegates in the investigation phase. The session builds upon the knowledge that should have been acquired by the delegates through the course pre-read that has been prepared to allow for the reduction in the time allocated for this session from the original 180 minutes to the current 120 minutes. | | |
| **Objectives:**  By the end of this session delegates will be able to:   * Discuss the contents of the COE Electronic Evidence Guide * Discuss various types of electronic evidence * Explain the principles of best practice relating to the seisure and handling of electronic evidence * Identify the challenges offered by “dead box”, “live data” and Internet sources of electronic evidence, including evidence in the “cloud”. * Discuss the admissibility of electronic evidence in judicial proceedings * Explain the proper planning and preparation of a search raid where digital evidence may be found. * Explain how a crime scene would be secured and documented, where digital evidence occurs. * Explain the term Digital Forensics * Compare Digital Forensics to traditional forensic sciences * Define at least three sub-branches of Digital Forensics * Identify the four steps in Digital Forensics examinations * Differentiate the two categories of digital traces * Describe how Digital Forensics can support investigations | | |
| **Trainer Guidance**  The session on electronic evidence has been reduced in this version of the course and a pre-read produced for the delegates to consider in advance of the course. The trainer may consider a short knowledge check at the beginning of the session to check that the pre-read has been used. This could take the form of a quiz. The content of the pre-read introduced the delegates to different forms of devices that may contain electronic evidence. The trainer may also consider obtaining a variety of electronic devices, some of which may contain electronic evidence. Passing these round at the beginning of the session is another way of assessing the extent to which the delegates have assimilated the information in the pre-read. As with the other sessions, this one provides additional information in the slide notes to assist the trainer.  The slides that form the pre-read have been left in the deck for the trainer, who may wish to use them to reinforce information or to display while answering questions. They are not intended to be used as a delivery method during the lesson.  There is information in the lesson about the search and seizure of electronic evidence. This rangers from the preparation and planning to equipment to take and on to the actual seizure and associated considerations. Depending on the legal system of the countries of the delegates, this will be of more or less interest. In common law jurisdictions, judges have no role in the investigation or any associated activities such as search and seizure. They will, however need to understand evidence when it is produced before them, so an overview of the issues may be appropriate. In other jurisdictions, the judge may have a role in the investigation, and prosecutors may be legally responsible for the investigation. In these cases, the issue of search and seizure. Each trainer is responsible for ascertaining the role of the delegates and adapting the training materials accordingly. The trainer should consider the overall time that is available when deciding the emphasis to be placed on materials, remembering the overall context of the teaching objectives, which are the foundation of lesson. | | |
| **Lesson Content** | | |
| **Slide Numbers** | **Content** | |
| 1 to 6  Mandatory Slides | The opening slides are the introduction to the session and include the Agenda and the session objectives. The trainer should ensure that these are amended where it has been decided to exclude sets of slides.  Slide 6 is to begin the discussion wih the delegates. The trainer should begin a discussion with the group by identifying types of electronic evidence and encouraging the participants to give details of their knowledge of the issue. The trainer should then list the types highlighted on a flip chart or white board. The trainer should complete the list if the audience does not highlight types of evidence. The list should include both types of evidence e.g. dead box, live data, memory, Internet, as well as sources of evidence such as those dealt with in the technology section of the course. | |
| 7 to 12  Important Slides | These slides set out the definitions of evidence and electronic evidence. To some extent this is also a refresher of the information in the pre-read materials.  The trainer should prepare for the course, by establishing if there are national definitions in the jurisdiction in which the training is being undertaken, and if so, include this information in the presentation. | |
| 13 to 46  Not Essential Slides | These slides repeat the content of the pre-read and should therefore not be used to deliver the learning. The trainer has an option to use any of the slides should there be a need during the session to reinforce a point or answer a delegate question. These slides should be hidden during the presentation and it is the responsibility of the trainer to prepare the slides for each delivery of the course. | |
| 47 to 148 | The slides in the following sections deal with the COE Electronic Evidence Guide, which is an important aspect of the training. The presentation is broken down into sections as described in the following sections up to slide 148. | |
| 47 to 63  Mandatory Slides | These slides cover the introduction to and explanation of the guide. They detail how it is structured and explain the levels at which information is provided. | |
| 64 to 71  Mandatory Slides | This section deals with the principles of electronic evidence. The principles and links between them should be clearly explained by the trainer. The principles were included in the pre-read, however there should be sufficient time allocated during the course to ensure the delegates are familiar with them. | |
| 72 to 80  Important Slides | These slides cover the initial considerations and the planning and preparation for seizure of electronic evidence. The slides are supported by additional information in the slide notes. | |
| 81 to 88  Not Essential Slides | This explains what and who to take to a search scene. As mentioned previously, the relevance of this will depend on whether the audience is involved in the investigation process. If not the trainer should consider whether to include this information, and hide slides as appropriate. | |
| 89 to 98  Not Essential Slides | This section deals with securing the scene and first actions at the scene. Once again, the consideration as to whether to use these slides will depend on the involvement of the audience in the search and seizure activities. | |
| 99 to 104  Not Essential Slides | These slides explain how the scene should be documented. | |
| 105 to 125  Important Slides | This section deals with the types of material that may be encountered at the scene and describe the considerations and methods of seizure. The slides are supported by additional information in the slide notes. The final slide is a flow chart for search and seizure and could be used by the trainer to introduce the range of similar appendices to the guide. | |
| 126 to 139  Mandatory Slides | The issue dealt with in this section is that of volatile data; including live data forensics, remote storage and Internet evidence. This is an important section as it deals with the capture of data that may be altered, and explains the processes to be followed to ensure that the integrity of evidence is maintained. There is another COE flow chart that differentiates between “dead box” and “live data” capture. The slides are supported by additional information in the slide notes. | |
| 140 to 147  Not Essential Slides | This group of slides deal with the importance of correct labelling, transport and storage of electronic evidence and data storage devices. This will be of limited interest to those not involved in the investigation process. | |
| 148 to 166  Mandatory Slides | This section deals with the important subject of digital forensics, in other words, how the seized data is processed once in the laboratory situation. This section was moved from the advanced course to the introductory course due to its increasing relevance to the judiciary. The slides are animated to allow the trainer to pause and involve the audience in the explanations. There is a comparison between analogue and digital forensics and an explanation of the process, as well as the relevance of the entire process. The slides are heavily supported by animations and additional information that is in the slide notes. | |
| 167 to 170  Mandatory Slides | The final slides allow the trainer to review the learning objectives with the audience so that they may be sure that they have been achieved. It is also an opportunity for the delegates to raise any issues that may be outstanding or where they have not fully understood the subjects presented. In addition, the trainer may use the session to check the knowledge learned by asking questions of the participants. This is important as there is no formal assessment for the course. | |
| **Practical Exercises**  No practical exercises are envisaged in this lesson. | | |
| **Assessment/Knowledge Check**  No knowledge check or assessment has been requested for this session. | | |