Lesson 2.1 Digital & Electronic Evidence

|  |  |  |
| --- | --- | --- |
| Lesson 2.1 Digital & electronic Evidence | | Duration: 90 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. | | |
| **Objectives:**  By the end of this session delegates will be able to:   * Discuss various types of electronic evidence * Summarise the key points from the CoE Electronic Evidence Guide especially the principles of seizure & handling * Identify differing challenges of ‘dead box’ & ‘live data’ forensics as well as ‘cloud based data’ * Discuss admissibility of electronic evidence * Compare ‘digital forensics’ to traditional forensics * Identify four key stages of a digital forensic examination | | |
| **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 4  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. | |
| 5 to 17  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. It also deals with some basic characteristics of data – and why it is so different to deal with.  Slide 6 is to begin the discussion with 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.  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. | |
| 18 to 27  Mandatory Slides | The slides in the following sections deal with the COE Electronic Evidence Guide, which is an important aspect of the training.  These slides look at the background to electronic evidence and why the guide came into being. It also considers who the guide is for and who should use it – and how.  It introduces the Principles of electronic evidence | |
| 28 to 34  Mandatory Slides | These slides look at the five principles of electronic evidence and allow the trainer to work through them explaining the purpose of them.  The principles should prompt some discussion and questions. Failing this, the trainer can prompt responses from the delegates | |
| 35 to 61  Mandatory Slides | These slides cover the electronic crime scene and how it should be approached. There are sections for preparation, intelligence and then the actual visiting of the crime scene – and the actions that should be taken there. | |
| 62 to 78  Important Slides | This section deals with the electronic evidence. The types of evidence and how it will appear before judges & prosecutors.  It differentiates between analog crime scenes & digital crime scenes.  It then steps the delegate through the steps of the digital forensics process explain how each works and fits with the previous to produce electronic evidence.  It finally looks at what digital evidence will look like and the types of evidence they will see. | |
| 79 to 80  Important Slides | These slides bring the session to a close – recapping the content and providing opportunity for the delegates to ask questions for clarification. | |
| **Practical Exercises**  There is one practical envisaged where the trainer hands out small devices relating to computers and allows the delegates to handle these devices – before moving amongst them and discussing with them what they have and whether it could have any use in a cybercrime. | | |
| **Assessment/Knowledge Check**  No knowledge check or assessment has been requested for this session. | | |