**Lesson Plan**

Lesson 2.3.1 (Electronic Evidence)

|  |  |  |
| --- | --- | --- |
| Lesson 2.3.1 (Electronic Evidence) | | Duration: 90 minutes |
| **Resources Required:**   * PC/Laptop loaded with software versions compatible with the prepared materials * Projector and display screen. * Internet access (if available). * Student notepaper and pens. * Hard copies of the evidence file mail11.doc and the additional file mail11(hash).doc for each delegate * Copies of the COE Electronic Evidence Guide and the COE Digital Forensic Laboratory Guide | | |
| **Session Aim:**  The purpose of this session is to provide delegates with an opportunity to consider the challenges to the electronic evidence that is used in the BEC case study. | | |
| **Objectives:**  At the end of this session, delegates will be able to:   * Identify methods of validating electronic evidence. * Review admissibility issues for electronic evidence in the trial process * Examine and explain has values of electronic evidence files | | |
| **Trainer Guidance**  The main purpose of this session is to lead the delegates towards identifying the main admissibility issues involving electronic evidence and the importance of them being able to consider the them on the context of allowing or rejecting electronic evidence. They are introduced to the ability to check evidence by validating hashes of different files. There are limitations to being able to assess different types of evidence as the email evidence is created in MS word files and there are no artefacts to consider. | | |
| **Lesson Content** | | |
| **Slide Numbers** | **Content** | |
| 1 to 3 | The first slides lay out the structure and objectives of this session. Delegates will be given an opportunity to ask any preliminary questions that they may have regarding the structure and objectives of the session. | |
| 4 to 5 | These slides provide definitions of electronic evidence and list some of the unique characteristics. The delegates should be reminded that they were introduced to these issues in greater detail in the introductory course | |
| 6 to 11 | These slides set out in greater detail than covered in the introductory course, the considerations for the admissibility of electronic evidence. The trainer should ensure they cover all aspects of the slides | |
| 12 to 13 | These slides remind the delegates that their national legislation and practice takes precedence, and reminds them of the availability of COE documents that cover the issue of electronic evidence. The delegates should be encouraged to acquire them. | |
| 14 | The trainer should ask the questions on the slide and be prepared to discuss the real case examples before moving on to the course case study evidence. | |
| 15 to 16 | These slides list the documents used in the case study. The delegates should be asked if there are any admissibility issues they have identified with any of the documents and the trainer should lead a discussion about these. | |
| 17 to 22 | These slides are the demonstration of hashing of files and how one small change to a file can be identified by this process. The use of the files mail11.doc and mail11(hash).doc are fundamental to this session. It is recommended that the trainer gives a demonstration of hashing and comparing two files where there is one minor difference. | |
| 23 | This slide sets out some of the advantages of electronic evidence, how it may be validated and some questions judges may ask | |
| 24 to 25 | The trainer should recap the session objectives with the delegates and give them the opportunity to ask any questions relating to the materials covered in this lesson. | |
| **Practical Exercises**  The practical exercise is dealt with in slides 16 to 21. The trainer should consider a live demonstration of hashing on the lines shown. | | |
| **Assessment/Knowledge Check**  No formal assessment has been prepared for this session. The delegates will be expected to participate actively. | | |