|  |  |
| --- | --- |
| Lesson: 9 – Practical Exercise  (Phase 2 – Assessment of Electronic Evidence) | **Duration: 120 Minutes** |
| **Resources required:**   * 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 * Stapler, hole punch and scissors * Blu tack or a similar product to allow for paper to be affixed to the walls temporarily * Printer to print the leaflet * Files: Session 9 – Phase 2 – Assessment of Electronic Evidence.pptx | |
| **Aim:**  The purpose of this session is to allow the participants to discuss the case in groups, and to encourage them to recognise both defensive and prosecutorial reflexes. Each group is divided into two teams: one attacking the electronic evidence and one defending the electronic evidence. The trainer/expert stimulates this discussion and follows up the groups and asks the right questions where necessary. | |
| **Objectives:**  By the end of the lesson the students will be able to:   * Assess gathered electronic evidence * Identify the arguments and potential problems that can be raised with regard to electronic evidence * Develop arguments to attack the electronic evidence, as well as arguments to defend the electronic evidence | |
| **Introduction**  This session is a practical session on the assessment of electronic evidence.  The participants will all receive a realistic case file(paperless) that contains basically all electronic evidence that has been gathered in this specific case scenario  Some organisational information about this session is included in the PowerPoint presentation entitled “Session 9 – Phase 2 – Assessment of Electronic Evidence.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**  Each group will include four people who will argue that certain evidence should be used in court, and four who will oppose the use of evidence in court [50-50]. The participants will be provided with a full case file that contains the events that happened (‘the story’), how the electronic evidence was obtained, statements, forensic reports, warrants/production orders...  Each group will have a debate /discussion on whether how the evidence should be presented, based on the scope of the authorisation and the manner it was collected. This practical exercise is neutral in terms of legal systems and is relevant in all target countries. The experts can overview and moderate the discussions, asking relevant questions if and when required. Therefor an **expert/trainer guide** is provided that should remain only in the possession of the expert, in order to raise the right questions and to stimulate the group activity.  The participants will all receive **a realistic case file** (paperless) that contains basically all electronic evidence that has been gathered in this specific case scenario:   * results of production orders * electronic evidence gathered with a remote (transborder) search and seizure * electronic evidence found on a smartphone that was unlocked by using face recognition (against the suspects will?) * statements of the defendant(s) saying that the evidence has been planted by the police * hashed electronic evidence * electronic evidence that has not been hashed * electronic evidence gathered through live-forensics on a running laptop * electronic evidence from a cloud-server without know location * the seizure of a bitcoin seed * IT-expert reports -...   Thus, in this phase the participants – although divided in groups (one half defends the evidence, the other half attacks it (‘The Devil’s Advocate’)) – will observe/investigate on the same material and will have the accomplish the same investigative tasks and will have to deal with the same electronic evidence challenges and problems.   |  |  |  | | --- | --- | --- | | Group 1 | Group 1.A: attack | Group 1.B: defend | | Group 2 | Group 2.A: attack | Group 2.B: defend | | Group 3 | Group 3.A: attack | Group 3.B: defend |   The discussions within the groups are moderated and guided by an expert. There will be one IT- expert/specialized LE officer, who can be called in by any group to clarify technical questions or issues where needed.  The groups work and discuss for 90 minutes within their group, with the 'attack' team and the 'defence' team discussing and listing their arguments.  At the end of this, a short plenary will be held (30 minutes) to allow the different groups to interact with each other and to check whether all groups have reached similar findings, or whether there may be cross-fertilization of different views. | |