**Lesson Plan**

Lesson 3.x (Overview of Cybercrime Investigation: Country and International Experience)

|  |  |  |
| --- | --- | --- |
| Lesson 3.x(Basic Concepts on International Cooperation) | | 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. | | |
| **Session Aim:**  The overall purpose of this session is to present to delegates with an overview of the cybercrime investigation compared with international and local experiences. Delegates will be presented with description of the cybercrime authorities, their setup, substantive and procedural aspects of the investigation, basic of the investigation it self in different legal setups and some international and local concrete experiences. | | |
| **Objectives:**  By the end of the lesson the students will be able to:   * Understand the legal framework and practical organization of competent cybercrime suppressing and adjudicating authorities * Review and understand basic concepts of the cybercrime investigation and roles of the involved authorities * Learn about some International experiences regarding specialized authorities’ organization and cybercrime investigation * Learn about domestic experiences with this regard | | |
| **Trainer Guidance**  This session has been prepared to provide delegates with a comprehensive understanding of cybercrime investigation mechanisms. This session has been divided into four parts, in addition to an introduction and a conclusion. The first part covers the competent cybercrime authorities. The second part covers basic concepts of cybercrime investigation. The third part provides information about some international experiences with this regard. The fourth part provides information about domestic organization and experience. | | |
| **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 11 | These slides intend to provide the delegates with information about the idea of specialized cybercrime authorities, their competencies, setups and way how the should work.  In growing number of countries these authorities are being organized or planned to be introduced into the system of crime suppression.  Slides will list the number of the questions about LEA, Prosecution, Court and other authorities involved in the cybercrime cases and expert with delegates should be actively engaged in providing answers. | |
| 12 to 20 | These slides will present “rules” regarding concepts of the cybercrime investigation. Rules are not formal but more a result of the practitioner's experience from cybercrime investigations.  However, it may appear that some of the “rules” are obvious and describing already existing procedure in place, it is not simple as that. Namely, in the number of the countries although legal framework exists on general level lower level agreements which should more precisely define procedures for the cooperation and cooperation itself does not exist.  Often authorities are staying within the lines of their jurisdiction and they do not communicate direct or fast with others. With that kind of the behavior leads toward slow communication and exchange of evidence and facts and possible loss of the evidentiary material.  Also, slides will represents basic listing of the actions which Law Enforcement will and should undertake nduring the course of the cybercrime investigation, ones which should be undertaken by the Public Prosecution (regardless of the system, Public Prosecution represents an authority with is involved in one way or another with all criminal case participants, from LEA to the Court), role of the Judges and Courts, differences between Common Law and Civil Law systems, and role of the other authorities in the cybercrime investigation. | |
| 21 to 28 | These slides are representing one of the most successful international experiences in suppressing of the cybercrime.  Republic of Serbia from 2005 developed legal framework for combating cybercrime which included substantive, procedural and organizational laws. From 2005 Serbia is one of the rare countries to have highly specialized authorities in this area, including police, prosecution and court.  However, in accordance with the needs, expert may find and present additional examples. | |
| 29 to 31+ | These slides should present local examples | |
| 31 to 34+ | 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 module. | |
| **Practical Exercises**  No practical exercises are envisaged in this lesson. | | |
| **Assessment/Knowledge Check**  No formal assessment has been prepared for this session. The trainer is encouraged to check knowledge and understanding by asking relevant questions throughout the session. | | |