L300 Digital Forensics and Evidence for Legal Experts

Duration 2 days Beginner

Due to nature of the training contents, this training is only available in Turkish language.

As in the whole world, the number of cybercrimes in Turkey has been increasing exponentially over the years due to rapid advancements in digital technologies. In the Turkish legal system, digital evidence is regulated in Article 134 et seq. of the Criminal Procedure Code. While the classical evidence used in criminal procedures are visible and can be easily obtained by making confiscation and retention decisions, the electronic evidence in cybercrimes has an abstract structure - unlike classical evidence-. Electronic evidence requires the necessity of applying several technical examination and analysis methods that require high level of expertise. Electronic evidence can be quickly corrupted, changed, altered, lost, or destroyed. For this reason, examinations on digital devices are extremely important and reviews of a computer engineer, or programmer are often not adequate. The examination, evaluation and analysis of highly sensitive electronic evidence, the collection and preservation of which requires expertise, is also a very complex, specific, and costly process. In this training, digital forensics processes and the concept of digital evidence, which are often seen as complex for lawyers, will be discussed comprehensively. It is a training program created for lawyers, legal professionals, IT and technology specialists at different levels who want to improve their knowledge in this field.

MODULE 1 Evidence in Criminal Procedure	MODULE 4 Problems with Electronic Evidence Collection in Criminal Procedure Regulations on Principles to be Followed in the Collection of Electronic Evidence in International Law and Current Problems
MODULE 2 Electronic Media, Electronic Data and Electronic Evidence Concepts Digital Forensics and Evidence Collection	MODULE 5 Types of Cyber Crimes
MODULE 3 Acceptance, Verification and Assessment of Electronic Evidence	MODULE 6 Considerations in the Analysis of Technical Reports