ÖZET

Çalışmamızın konusu, klasik deliller ile karşılaştırıldığında daha yeni bir delil türü olan dijital delillerdir. Dijital delillerin kendilerine has yapıları sebebiyle, bu delillerin elde edilişinden mahkeme önüne getirilmesine kadar olan sürecin ayrıntılı bir şekilde incelenmesi gerekmektedir. Dijital delillerin adli bilişim süreci, uzmanlık gerektiren bir alandır. Bu sürecin titizlik ile yürütülmesi muhakeme açısından büyük öneme sahiptir. Konunun adli bilişimle ilgili kısmını sınırlı tutmaya çalışarak, ceza muhakemesi hukuku açısından gerekli olan kısımlarını çalışmamızda ortaya koymayı hedefledik. Türk hukukunda dijital delillerin elde edilmesine yönelik mahallinde ve mahallinden uzakta aramayı kapsayan CMK m.134 hükmü çalışmamızın önemli bir kısmıdır. CMK m.134, Bilgisayar, Bilgisayar Programları ve Kütüklerinde Arama, Kopyalama ve Elkoyma, özel bir arama ve elkoyma türüdür. Bu tedbirin önemi, dijital delillerin elde edilmesinde arama ve elkoymanın usul hükümlerini ortaya koymasıdır. Tedbir, temel hak ve özgürlükleri ihlal etmeyecek şekilde delillerinin elde edilmesini amaçlamaktadır. Dijital delillerin elde edileceği bilişim cihazına, şifrenin çözülememesinden dolayı girilememesi, gizlenmiş bilgilere ulaşılamaması veya işlemin süresinin uzun sürecek olması hallerinde, bilişim cihazlarına elkonulabilecektir. Dijital deliller, adli bilişim ile bağlantılı bir elde edilme sürecine tabidir bu sebepten, adli bilişime dair hususlar yeterince bilinmediği takdirde bu durum uygulamada eksikliklere yol açabilecektir. Adli bilişim sürecinden geçen dijital delillerin muhakemeye esas alınması için gerekli şartlar, bu delillerin tek başına mahkumiyet için yeterli olup olamayacağı, hukuka aykırı ve tesadüfen elde edilen delillerin durumu ispat kısmında açıklanacaktır. Çalışmamızın gerek teorik gerekse uygulama açısından fayda sağlamasını temenni ediyoruz.

ABSTRACT

The subject of our study is digital evidence, which is a newer type of evidence compared to classical evidence. Due to the unique nature of digital evidence, it is necessary to examine the process from the acquisition of this evidence until it is brought before the court in detail. The forensic informatics process of digital evidence is an area that requires expertise. The meticulous execution of this process is of great importance for the judgment. By trying to limit the part of the subject related to forensic informatics, we aimed to reveal the parts that are necessary in terms of criminal procedure law in our study. The provision of Article 134 of the Criminal Procedure Code, which covers on-site and remote searches for obtaining digital evidence in Turkish law, is an important part of our study. Article 134, Search, Copying and Seizure of Computers, Computer Programs and Logs, is a special type of search and seizure. This measure is important because it sets out the procedural provisions of search and seizure in obtaining digital evidence. The measure aims to bring evidence in a manner that does not violate fundamental rights and freedoms. Information devices may be seized in cases where the information device from which the digital evidence is to be obtained cannot be accessed due to the inability to decrypt the password, the concealed information cannot be accessed, or the process will take a long time. Digital evidence is subject to a process of acquisition in connection with forensic informatics; therefore, issues related to forensic informatics. If not sufficiently known, this situation may lead to deficiencies in practice. The conditions necessary for digital evidence that has gone through the forensic informatics process to be taken as a basis for the judgment, whether this evidence alone can be sufficient for conviction, and the status of evidence obtained illegally and incidentally will be explained in the proof section. We hope that our study will be beneficial both in terms of theory and practice.