THE CONCEPT OF HASH VALUE AND THE COLLISION OF HASH VALUE AS THE WAY TO PROVIDE UNASSAILABILITY OF DIGITAL EVIDENCE

Sayısal Delilin Değiştirilemezliğinin Sağlanmasının Yolu Olarak Özet Değer Kavramı ve Özet Değer Çakışması[1]

Prof. Dr. Olgun DEĞİRMENCİ*

Abstract: The evidence used to prove the material fact which is subject to the criminal procedure should not be changed until it is brought before the court. It is relatively easy to ensure the accuracy of physical evidences by taking them into judicial custody. However, it is difficult to ensure the accuracy of the digital evidence since it is easy to copy and modify it. Digital evidences are used to provide the technological means to ensure accuracy. The hash value, which provides a one-way summarization value, can be applied to digital evidence such as a fingerprint and helps to ensure the accuracy of the numerical evidence. However, a collision of hash value, known as the hash value conflict, which occurs when two different digital data have the same hash value, is a problematic area in ensuring the accuracy of numerical evidence. In this study, the concept of summary value as a means of ensuring the accuracy of numerical evidence will be explained and the possible effects of the hash value collision will be discussed.

Keywords: evidence, digital evidence, hashing, proof, collision of hash value.

Öz: Ceza muhakemesine konu maddi olayı ispatlamak için kullanılan delil, mahkemenin önüne getirilene kadar değiştirilmemelidir. Fiziksel delillerin, adli emanete alınması suretiyle doğruluklarını sağlamak nispeten kolaydır. Bununla birlikte sayısal delillerin kolayca kopyalanabilmeleri ve değiştirilebilmeleri, doğruluklarının sağlanması güçtür. Sayısal delillerin doğruluklarını temin etmek için teknolojik olanaklardan yararlanılmaktadır. Tek yönlü özetleme değeri sağlayan özet değer (hash value), bir parmak izi gibi sayısal delile uygulanabilmekte ve sayısal delilin doğruluğunu sağlamaya yardımcı olmaktadır. Ancak iki farklı sayısal verinin aynı özet değere sahip olması olan özet değer çakışması, sayısal delilin doğruluğunu sağlamada sorunlu bir alandır. Bu çalışmada sayısal delilin doğruluğunu sağlama aracı olarak özet değer kavramı açıklanacak ve özet değerin çakışmasının muhtemel etkilerine değinilecektir.

Anahtar Kelimeler: delil, sayısal delil, özetleme, ispat, özet değer çakışması.

[1] This paper were formed by developing the author's opinions in these articles ("Bilgi Toplumunun Delil Türü: Sayısal Delil ve Bilimselliği" (Terazi Law Journal, Vol. 9, No. 97, September 2014, ss. 14 – 28) and "Yargılama Makamı İçin Şüphe, Müdafi İçin Savunma Nedeni: Adli Bilişimde Özet Değer (Hash Value) Kavramı ve Özet Değer Çakışmasının Ceza Muhakemesine Etkileri" (Terazi Law Journal, Vol. 13, No. 137, February 2018, ss. 120 – 126)

* TOBB University of Economics and Technology, Faculty of Law, Faculty Member of Criminal and Criminal Procedure Law, odegirmenci@etu.edu.tr, ORCID: 0000-0002-0700-2549

Makale Geliş Tarihi: 22.08.2022, Makale Kabul Tarihi: 22.11.2022

I. CONCEPT OF EVIDENCE IN CRIMINAL PROCEDURE LAW

The fact that the criminal procedure is handled as *"the matter of determining the situation of the material fact according to the norms"*[2] does not fully express the purpose, since it creates the impression that the concrete case is outside the determination of the criminal procedure. Basically, two cases are analyzed in criminal procedure. Between these two, the first case, which also needs to be resolved first, is the material event, The subjects of the trial contribute to the issue of how the event subject to the trial takes place in the outside world, and in this way, it is tried to ensure that a conscientious opinion is formed in the trial authority. Conscientious opinion must be the one that is free from any reasonable doubt. The second case, which is relatively easy to solve, is revealing the status of the concrete case against the legal norms through interpretation.[3]

In fact, the solution of the material event actually falls within the field of activity of all sciences, and when the word "forensic" is brought to the beginning of any science, that discipline can be used for the solution of the material event subject to criminal procedure. [4] Since the material event took place chronologically before the trial phase of the criminal procedure, we need to decide on the event with the remnants of that event. Everything that has been transferred to the present day regarding the event in the past is examined under the concept of evidence. With the evidence we have, we are reconstructing the material event and restructuring the crime.[5]

Evidence is any tool that allows us to understand how the material event has occurred and it has some features. [6] In Article 217/1 of the Turkish Criminal Procedure Code (TCPC)[7], it is stated that the judge can

---

[2] Nurullah Kunter, Ceza Muhakemesi Hukuku, Revised and Enhanced 4th Edition, İstanbul, 1970, s. 33.

[3] Sami Selçuk, "Temyiz Denetiminin Sınırları ve Bu Sınırlara Uymamanın Kaçınılmaz Sancılı Sonuçları/Açmazları/Tehlikeleri", Vol. 19, No. 2, 2013, Marmara Üniversitesi Hukuk Araştırmaları Dergisi, Prof.Dr. Nur Centel'e Armağan, s. 332 (ss. 319 - 361); Cumhur Şahin, Ceza Muhakemesinde İspat (Delillerin Doğrudan Doğruyalığı İlkesi), Yetkin Publications, Ankara, 2001, s. 19.

[4] Among the most well-known, forensic medicine, forensic physics, forensic chemistry, forensic accounting, forensic theology, forensic literature etc. See about it, Nedir Bu Adli Bilimler/Kimdir Bu Adli Bilimciler, Adli Bilimciler Derneği Yayını, Ankara, 2019.

[5] W. Berry Chisum / Brent E. Turvey, Crime Reconstruction, Academic Press, 2007, s. XV.

[6] Doğan Gedik, Öğreti ve Yargısal İçtihatlar Işığında Ceza Muhakemesinde Şüpheden Sanık Yararlanır İlkesi (In Dubio Pro Reo), Adalet Publications, 2016, s. 11; Koray Doğan, Ceza Muhakemesinde Belirsizlik Kuşkudan Sanık Yararlanır İlkesi "in dubio pro reo", Seçkin Publications, Ankara, 2016, s. 235; Mehmet Yayla, Ceza Muhakemesi Hukukunda İspat ve Şüphe, Seçkin Publications, Ankara, 2016, s. 96.

[7] The Power of Discretion Regarding the Evidence

only base his decision on evidence and the features related to the evidence that can be the basis for the judge's decision are emphasized. From this point of view, it is stated that the conscientious opinion of the judge can only be based on evidence, there will be no conviction without evidence[8], and the material truth closest to the absolute truth can only be reached with evidence. [9]

The event experienced in the past, which is the material subject of the criminal procedure, will be revived in the mind of the judge jointly during the trial, with the participation of the parties. In other words, material truth will be revealed in the form of learning past based on today. [10] Evidence is the means by which the animation in question or, in other words, carries parts of the past event to the present. [11] When we look at the doctrine, it is seen that the characteristics of the evidence are generally expressed as follows; be realistic, reasonable, representative of the event, legal and collective.[12] Some specific issues related to our subject will be briefly mentioned, and after the boundaries of the concept of evidence are drawn, the concept of digital evidence will be explained.

First of all, the evidence must be representative of the material event subject to the criminal procedure.[13] The representativeness of the evidence is a concept related to being a part of the material event or reflecting the material event.[14] Although the reliability of the evidence were also evaluated under this title by some authors in the doctrine[15], we will evaluate it under a separate title due to the importance of the subject.

Article 217 – (1) The judge shall only rely upon the evidence, which was presented and discussed at the hearing, while delivering a decision. This evidence shall be evaluated freely by the judge on the basis of his/her conscientious opinion

(2) The imputed offence may be proven by using and king of legally obtained evidence.

See for the text of the TPPC, Buğra Erdem / Nimet Mediha Işıtman, Basic Legal Documents of Turkish Criminal Law, Seçkin Publications, Ankara, 2021, s. 412.

8 Devrim Aydın, Ceza Muhakemesinde Deliller, Yetkin Publications, 2014, s. 38.

9 Mahmut Koca, "Ceza Muhakemesi Hukukunda Delilleri", Vol. 1, Nu. 2, December 2016, Journal of Criminal Law, s. 207 (ss. 207 – 225); Gedik, s. 12.

10 Cumhur Şahin / Neslihan Göktürk, Ceza Muhakemesi Hukuku – II, Revised and Updated 8th Edition, Seçkin Publications, Ankara, 2019, s. 25.

11 Vahit Bıçak, Suç Muhakemesi Hukuku, 4th Edition, Seçkin Publications, Ankara, 2018, s. 457; Ali Eryılmaz, Ceza ve Disiplin Hukukunda Hukuka Aykırı Delil, HUKAB Publications, Ankara, 2013, s. 13.

12 Gedik, s. 12, 13; Koca, s. 213.

13 Nur Centel / Hamide Zafer, Ceza Muhakemesi Hukuku, 14th Edition, Beta Publications, İstanbul, 2017, s. 235.

14 Bıçak, s. 426.

15 Şahin / Göktürk, II, s. 30.

Evidence is tools that belong to the external world, the objective field, not the inner world of people. In this respect, evidences are tangible and the things that do not have a material structure, and that's why can not be perceived by the five senses, cannot be evidence.[16]

Evidence must be available or accessible. Presenting the the means of proof, which is not available, to the court and debating over it is not possible. [17]

Evidence must have been obtained lawfully. The principle that everything can be evidence in criminal procedure does not enable us to come to a conclusion that any method can be used and that evidence can be obtained without considering the procedures and principles laid down by law.[18]

Evidence must be reliable.[19] In this context, the accuracy and integrity of the evidence must be ensured from the moment it is obtained until it is brought before the criminal judge. Evidence should not be changed. Essentially, our study is concerned with this feature of the evidence. As a matter of fact, the representative quality of the evidence should not be damaged until it is moved from the crime scene to the hearing, and the evidence should be trusted by the court.

The collectiveness of the evidence should be ensured by being discussed in the criminal procedure.[20] The commonality of the evidence will be ensured by discussion at the hearing. In order for the evidence to be discussed at the hearing, the parties must have access to the evidence or the evidence must be reported to the parties (TCPC art. 179, 181). [21]

---

16 Centel / Zafer, 235; Şahin / Göktürk, II, s. 30.

17 Centel / Zafer, 235; Şahin / Göktürk, II, s. 30.

18 Bkz. Claus Roxin, "İspat Hukukunun Esasları", Translator Yener Ünver, Y. 4, No. 8, Fall 2005, İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi, s. 273 (ss. 265 – 289).

19 Centel / Zafer, s. 235.

20 Centel / Zafer, s. 235.

21 Centel / Zafer, s. 235.

Notifying the accused and the public prosecutor of the names and adresses of the witnesses summoned

Article 179 – (1) The accused shall notify the public prosecutor in reasonable time of the names and addresses of the experts and witnesses whom he/she is going to have summoned directly or bring along to the hearing.

(2) If the public prosecutor intends to summon persons other than those named in the indictment or other than the witnesses and experts invited at the request of the accused, either by decision of the president of the court or the judge or by his/her own motion, he/she shall notify the accused in reasonable time of the names and addresses of those persons.

Notificaiton of the day of of hearing the witness and the accused

Article 181 – (1) The day set for the hearing of the witness and experts shall be notified to the public prosecutor, the injured party, his/yer representative, to the accused and

The judge will be able to base his decision only on the evidence brought to the hearing and discussed before him. In terms of each evidence, the parties to the case should be given the right to refute the evidence in question and to express their thoughts on the evidence.

Evidence must be rational and scientific. [22] Rationality will be determined by drawing conclusions from the principles of logic, freed from prejudices.[23] Irrational evidence cannot be used in judgment. [24]

II. DIGITAL EVIDENCE AS A TYPE OF EVIDENCE AND ITS FEATURES

As it is often expressed, we believe that the saying *"wherever society is, there is law"* (Ubi societas ibi jus) [25] evolved with the transition to the information society and turned into *"wherever society concentrates, law should concentrate there"*. The fact that information systems are used more in social life causes the society to concentrate there. Crime, a phenomenon created by society, naturally concentrates on information systems. We can say that the evidence to be used as a proof of the crime has also evolved into digitalization due to the necessity of searching for that evidence in the place where the crime is concentrated. The

---

his/her defense counsel. A copy of the record shall be delivered to the public prosecutor and the defense counsel, who are present.

(2) In cases, where there is need to repeat the judicial inspection or examination, the provisions of the abovementioned paragraph shall apply.

(3) The accused, who is under detention, may only request to be present during such procedures to be conducted in the court located in the place where he/she is detained. However, in cases where the judge or the court deems it obligatory, it may be decided that the suspect or the accused, who is under detention, be present during such procedures.

See Erdem / Işıtma, s. 396, 397.

22 Centel / Zafer, 235; Tosun stated that the evidence passes through two stages in the historical flow, irrational and rational. According to the author, people have respected irrational evidence for many years. For example, they checked the accuracy of their statements by dipping the accused's hand into hot oil. Over time, the stage of rational proofs has passed. (Öztekin Tosun, Türk Suç Muhakemesi Hukuku Dersleri Vol.:1, İstanbul, 1984, 713 vd.); Feyzioğlu, the stages of the proof system; examined by classifying them as ethnic phase, religious phase, legal phase, conscientious phase and discussed whether scientific proof is possible or not. (Metin Feyzioğlu, Ceza Muhakemesinde Vicdani Kanaat, Ankara, 2002, s. 38 vd.).

23 Bıçak, s. 429.

24 On the scientificity of the evidence, see also. Olgun Değirmenci, "Bilgi Toplumunun Delil Türü: Sayısal Delil ve Bilimselliği", Vol. 9, No. 97, Terazi Law Journal, Septermber 2014, ss. 14 – 28.

25 See. Ahmet Ulvi Türkbağ, "Hukuka Gerçekçi Eleştirel Bakış: Hukuk Sosyolojisi", Issue 16, 2008/1, Sosyoloji Dergisi, 3rd Series, s. 43 – 54.

expression "Crime is digitizing" [26] can be easily translated into "crime and evidence are digitizing".

Digital evidence is all kinds of data held, created, stored and transmitted in digital media.[27] The essence of numerical evidence is that it is data. As in every data, digital evidence basically consists of bits in the form of 1 and 0. [28] However, it is the fact that it is related to the material event that is the subject of the criminal procedure that gives the data in question the quality of evidence. In technical terms, numerical evidence is defined as any data that supports or disproves a hypothesis about the state of the data or the numerical case.

Digital evidence; can be found in computer programs, computer networks, or other electronic devices.[29] Digital evidence can exist in various ways in its environment. It can be created during the transaction, for example as a document of a business transaction. It can be found in the digital environment as a document or it can take place in the appropriate environment as an audio/visual recording.[30] Today, we can say that transactions in all areas of social life have a digital aspect. In other words; it covers a wide range of areas, from health records to building construction projects, from the drug information you buy at the pharmacy to the records of the day care center that takes care of your child.[31] As *Casey* states, almost every case today is solved in some way in connection with e-mail.[32] The fact that digital evidence is used to illuminate not only the events related to cybercrime, but also almost all kinds of events, causes its importance to increase day by day. Digital evidence is also increasing in importance in criminal proceedings, and it is one of the most important evidences in criminal cases.[33] It is also

---

[26] John E.D. Larkin "Compelled Production of Encrypted Data", Vol. 14, Number 2, Winter 2012, Vanderbilt Journal of Entertainment and Technology Law, s. 254 (ss. 253 – 278).

[27] Olgun Değirmenci, Ceza Muhakemesinde Sayısal (Dijital) Delil, Seçkin Publications, Ankara, 2014, s. 248.

[28] Christina M. Schuck, "A Search for the Caselaw to Support the Computer Search 'Guidance' in United States v. Comprehensive Drug Testing", Vol. 16, No. 2, 2012, Lewis & Clark Law Review, s. 749 (ss. 741 – 781).

[29] Wayne Jekot, "Computer Forensics, Search Strategies, and the Particularity Requirement", Vol. VII, Spriing 2007, Pittsburgh University Journal of Technology Law and Policy, https://doi.org/10.5195/tlp.2007.29, s. 6.

[30] Larry Daniel / Lars Daniel, Digital Forensics for Legal Professionals Understanding Digital Evidence From The Warrant To The Courtroom, Syngress, USA, 2012, s. 4.

[31] Daniel / Daniel, s. 4.

[32] The author states this opinion such that "nearly every event we deal with has an element of e-mail that is steaming." (Eoghan Casey, "Reconstruction Digital Evidence", in: Crime Reconstruction, Edited by W. Jerry Chisum – Brent E. Turvey, 2006, s. 419, 420).

[33] Expressed by Susan Brenner in her blog. See. http://thinkexist.com/quotes/susan_brenner/, accessed 01 February 2014.

stated that in some cases, for example, child pornography acts, it is impossible to reach any evidence other than numerical evidence by taking the case one step further.[34]

The concept of digital evidence first appeared as computer evidence. In these periods, what is understood by a computer evidence is a printout of a file on the computer. However, with the development of technology, the concept of computer evidence has been replaced by digital evidence. What is expressed by the concept is no longer just a printout, but all information stored, processed and transferred in information systems, storage units, regardless of whether it is produced by a human or a system.[35]

With the development of social media (Twitter, Facebook and MySpace etc.), people have begun to share their daily activities, personal images, thoughts and their locations with others. With the sharing of daily activities, real life is recorded digitally in information systems. In addition, with the increase of "blogs", people write their thoughts and opinions about daily events like a journalist and create their own media organs. [36] All these outputs of technology mobilize the society and the crime stemming from the society, hence the evidence of crime from physical to digital.

Digital evidence has some features. First of all, it is invisible and hidden. Understanding the existence of digital evidence, unlike analog or physical evidence, is possible with auxiliary tools or equipment.[37] The equipment in question; consists of hardware and software. For example, it will be possible to see the data in a word processor file, to take a printout from the printer or via the screen. In case of computer output or screen output of digital evidence, it will not be possible to see metadata[38], which is defined as the data of the data stored with the said data. In this context, any tool that makes digital data understandable for humans can give us information about only a part of the digital data in question. The fact that metadata, which contains many important information about digital evidence, such as the time of creation, copying

---

[34] Digital Evidence in the Courtroom: A Guide for Preparing Digital Evidence for Courtroom Presentation, The National Center for Forensic Science, 2003, http:/www.ncfs.org/DE_courtroomdraft.pdf, accessed: 10.09.2011.

[35] Schatz, s. 1.

[36] Daniel / Daniel, s. 4.

[37] Göksu, s. 30; Peter Sommer, "Downloads, Logs and Captures: Evidence from Cyberspace", Vol. 5, Journal of Financial Crime, s. 142.

[38] Metadata is like the history of a document. Every entry made to the document is recorded in the corresponding document (Adam Israel, "To Scrub or Not to Scrub: The Ethical Implications of Metadata and Electronic Data Creation, Exchange, and Discovery, Vol. 60, 2009, Alabama Law Review, s. 472, 73).

or modification, cannot be seen in the printouts[39], emerges as a major deficiency in terms of the authorities evaluating the evidence. However, it should be noted that in digital proofs, what constitutes evidence is not the printout that can be taken from the screen or the printer, but the data itself in the digital environment.[40] Therefore, since it is the data in the digital environment itself, the metadata that informs us about the data in question are also within the scope of the digital evidence.

Digital evidence has a delicate structure. Failure to comply with certain rules in the collection of evidence from the crime scene may result in the loss of evidence as well as falsification of evidence. [41]

The possibility of falsifying digital evidence brings along the problem of reliability of the evidence. A study conducted in the member states of the European Union reveals that there is no consensus among the judges about the reliability of the evidence. As a matter of fact, some judges are of the opinion that electronic evidence is more reliable and can be used in the trial since it is objective and certain. On the other hand, some other judges consider that electronic evidence is more open to abuse and less reliable than classical evidence due to the difficulty of verifying its authenticity.[42]

It is possible for digital evidence to gain meaning only by examining the information system as a whole. Analyzing the digital evidence separately from the whole, unlike the physical evidence, will either cause the digital evidence to lose its representative quality of the event or it will lose it to a great extent. Verification of digital evidence is possible with a complete examination of the system or confirmation from another source. For example, confirming the accuracy of an e-mail through service providers can be given as an example in this respect. [43]

Digital evidence is mixed with data that is not related to the event in its environment. A small part of the data in a disk drive may be related to the criminal case. It is necessary to find the digital data related to the event, extract it and make it understandable [44] This will only be possible if the people who will convert the digital data into evidence

---

[39] Metadata; can provide us with the person who prepared the document, when the document was prepared, a list of the last ten people who made changes to the document, when the document was reviewed, changes to the document, and other information (Favro, 7; Beckham, s. 2 vd.). In some cases, these documents include information considered important to criminal investigations, such as the name of the network server, where the document was saved on the hard disk (David Hricik, "The Transmission and Receipt of Invisible Confidential Information", http//www.hricik.com/eethics/Metadata1103.doc, accessed: 06 Ocak 2013).

[40] Göksu, s. 30.

[41] Ünal, 17; Ademu – Imafidon – Preston, s. 175.

[42] Insa, s. 29.

[43] Göksu, s. 31.

[44] Casey, 2004, s. 15.

specialize in this matter. In addition to specialization, the time factor is one of the important factors affecting the process of converting digital data into digital evidence. Obtaining digital evidence is also a time-consuming activity.

Physical evidence can be diminished by examining the evidence. However, digital evidence can be easily copied exactly and the copy can be processed as if it were real. In practice, the examination of numerical evidence is done on copies.[45]

Digital evidence is more vulnerable to tampering than physical evidence.[46] Digital evidence may be falsified by the perpetrators in order to obscure the evidence, or they may be inadvertently falsified during the collection of digital evidence. [47]

The complete destruction of digital evidence, unlike physical evidence, is only possible with the irreversible destruction of the physical environment that contains it.[48] Therefore, digital evidence can be obtained by forensic experts, even though it is perceived as destroyed. Digital evidence can be recovered even if a file is deleted or the hard disk drive is formatted.[49]

Digital data often do not have direct evidence. Although they are related to the event that is the subject of the criminal procedure, they often do not fully reflect the relationship between the perpetrator, the act or the victim. For example, in the crime of insulting by e-mail, the word processor file on the computer may give an idea that the e-mail containing the insult was first prepared as a draft on the computer. However, it does not really indicate that this file was created by the suspect. This does not affect the quantitative evidence's qualifications as evidence, but sometimes it may require supporting it with other evidence.[50]

III. HASHING AS A WAY TO ENSURE THE INVISIBILITY OF DIGITAL EVIDENCE

A. GENERALLY

Compared to the physical evidence, the fact that a one-to-one copy can easily be made, the possibility of adding or subtracting from

[45] Casey, 2004, s. 15.

[46] Göksu, s. 32.

[47] Casey, 2004, s. 15; digital evidence can be falsified as long as it is stored in the information system or during transmission. (Sommer, Downloads, s. 142).

[48] Göksu, s. 32.

[49] Casey, 2004, s. 15.

[50] Yusuf Uzunay / Mustafa Koçak, "Bilişim Suçları Kapsamında Dijital Deliller", Academic Informatics Conference, Gaziantep, February 2005, s. 3.

the original data, and the possibility of accidentally changing the data, especially during the forensic copying stage, has pushed the world of forensic sciences to rely on mathematical calculations proving that the numerical evidence has not been changed. As a result, the use of the summarization function has emerged as a suitable tool in terms of obtaining numerical evidence and being a basis for the judgment of the court during the trial.

The hash function, as a cryptographic function, maps an arbitrary length of input (file, data, or an entire disk) to a fixed-length hash value. In order for this function to achieve its intended purpose, it is also necessary to meet some requirements. These requirements are; a) first of all, there are no two different outputs as hash value of the same input, b) there are no two different outputs for the same input, and c) it is not possible to reach the input through the hash value.[51]

B. USE OF HASH VALUE TO ENSURE RELIABILITY OF NUMERICAL EVIDENCE

As stated above, the most important feature of digital evidence is that it can be easily changed, deleted, destroyed, in short, manipulated. This issue, which *Casey* calls *"evidence dynamics"*, is related to the said feature of digital evidence. It is necessary to ensure with the chain of custody that the digital evidence is not changed from the crime scene where it is collected until it is taken as basis in the judgment of the court.

The principle of *"preserving the authenticity of the evidence"* here is valid from the forensic copying of the digital evidence from the data medium at the crime scene until the moment when it is subjected to expert examination. This can only be achieved with some mathematical calculation methods.

Considering the nature of the evidence, one of the most important principles in taking the data from the medium and subjecting it to the analysis is not to damage the evidence and therefore the data. The fact that the evidence is damaged during both acquisition and examination will cast doubt on the evidence, which in this case will lead to the assertion that the evidence has been falsified. In order to prevent this, forensic experts always work on a copy of the digital evidence. The fact that digital evidence can easily be reproduced makes this method possible.

Therefore, it is necessary to verify first that the copy made during the acquisition of the data is error-free, and then that the forensic expert

[51] Florian Mendel / Norbert Pramstaller / Christian Rechberger / Marcin Kontak / Janusz Szmidt, "Cryptanalysis of the GOST Hash Function", in: CRYPTO 2008, LNCS 5157, D. Wagner (Ed.), Springer 2008, s. 162 (ss. 162 – 178).

is working on the error-free copy. This verification is possible with hash value generation/hashing. [52]

Hash or hash generation is the process of converting a computer file, which is an information string (or any data string of non-constant size), into another character or symbol, by subjecting it to mathematical process.[53] When performed with one-way hash functions, it is done by converting each finite and variable-length data into a fixed-length output. As a result of this process, regardless of the size of the input, a unique output is obtained, consisting of a combination of the the letters A,B,C,D,E,F and digits of 0,1,2,3,4,5,6,7,8,9 according to the hashing function used.

Hashing is built on three basic principles. First, the hash function should easily convert numeric data to a specific hash value, regardless of the size of the input. Second, data should not be reached through the summary value. And finally, two different information strings with the same hash value should not be encountered.

There are different algorithms used in hash value calculation. The algorithms in question are named in different ways according to the number of bits used in the hash value and the manufacturer. Hash values are automatically calculated by the system according to the type of software and hardware used in taking the forensic copy and are kept in a log file.

The point that should be known about the hash value is that the hash value calculation is done simultaneously with the first intervention in the search in information systems. In the case of adding data after intervening in the system in which the data is located and then obtaining the summary value, it is not possible to understand that the data was added in the summary values obtained afterwards. Therefore, during the search, it is essential for both the forensic expert and the suspect or the lawyer who supervises the search, to supervise while the forensic copy of the system is taken and then to record the summary value resulting from the copying in the search and seizure report.

---

[52] Tyler Newby / Joel M. Schwarz, "Rethinking The Storage of Computer Evidence", UNAFEI Resource Material Series No. 79, December 2009, Tokyo, s. 44

[53] Stephen Hoffman, "An Illustration of Hashing and Its Effect on Illegal File Content in the Digital Age", Vol. 22, No. 4, Intellectual Property & Technology Law Review, April 2010, s. 6 (ss. 6 – 14); Lily R. Robinton, "Courting Chaos: Conflicting Guidance from Courts Highlights The Need for Clearer Rules to Govern the Search and Seizure of Digital Evidence", Vol. 12, 2010, Yale Journal of Law and Technology, s. 326 (ss. 311 – 147); Danielle Sutton, "Computer Forensics and Child Pornography Investigations", Vol. 2, 2011, Stevenson University Forensics Journal, s. 31; Michael Harrington, "A Methodology for Digital Forensic", Vol. 7, 2004, T.M. Cooley J. Parc. & Clinical L., s. 73; Marcia Hoffmann, "Arguing for Suppression of 'Hash' Evidence", May 2009, The Champion, s. 20, 21.

In the table shown below, there are some hash algorithms and the bit lengths they use. It should be stated that the longer the hash value, which is the result of the algorithm, the less likely the hash values of the files whose hash values are calculated to overlap (to be equivalent), which will be discussed later.

MD-5	SHA-1	SHA-256	SHA-512	RIPEMD-160
128	160	256	512	160

After presenting the subject in detail, it would be appropriate to make a summary value application. As stated above, the size of the input is not important in the hash calculation. In this context, the input can be an entire disk, data on a disk, or a simple file or characters.

The MD5 summary values of the data that we have entered from a web site that could be easily accessed on the internet[54] and which have only 1 letter difference with each other but have serious differences in meaning, are given below. As can be seen here, even with 1 letter difference the summary value will be completely different from one antoher.

Input	**MD5 Hash Value**
Digital evidence is very important for proof.	51ab9405f3aabff67b57bcbf19c66b2f
Digital evidence iz very important for proof.	5079586472bbd41885f9971e52f836e6

IV. HASH COLLISIONS AND ITS CONSEQUENCES

The debate about the validity and reliability of algorithms used to get hash values has been made for a long time and different opinions are expressed in the literature on this issue. For example, in the case of the MD5 hash value, which has a length of 32 bits, opinions are divided under two views ,. According to the supporters of the first view, hashing with the MD5 method gives extremely reliable results. It is stated that, apart from controlled environments at least, it is not possible for the method to break and produce the same results for different bit strings. In fact, it has been stated by some authors that the MD5 hash value gives at least as valid and reliable results as DNA evidence. [55]

[54] https://md5.hesaplama.net/hesaplama.do, accessed 05 Aralık 2017.

[55] Warren G. Kruse / Jay G. Heise, Computer Forensic: Incident Response Essentials, 2002, s. 89.

The second opinion on this issue states that it is possible to create two overlapping summary values developed as a result of studies especially in Israeli and Chinese technology universities.[56]

Considering the possibility of hash value collision, it may be possible to produce the same hash value later by making additions on the obtained data. This, in turn, will cause the defense authority to argue that the digital data required for the proof of the material event is unreliable, and gives a way to be hesitant about the use of the said evidence in the judgment since there is a doubt on the authenticity of the said evidence.

First of all, it will be necessary to evaluate the probability of collision. Let's try to explain the issue with an example. During a search made within the scope of TCPC art. 134[57], let's assume that some data on the computer used by the suspect were sufficient to prove the crime charged by the Public Prosecutor's Office, and therefore the hash value was calculated first, the result of the hash value was given to the defense, and then a forensic copy was taken and kept. If some additions are made to the forensic copy in question later in the judicial custody or expert

---

[56] Eric Thompson, "MD5 Collisions and the Impact on Computer Forensics", Vol. 2, 2005, Digital Investigation, s. 36 (ss. 36 – 40); Alaeldin Mansour Safauq Maghaireh, Jordanian Cybercrime Investigations: A Comparative Analysis of Search for and Seizure of Digital Evidence, Thesis Submitted in Fulfilment of the Requirements for the Award of the Degree, University of Wollonong, 2009, s. 135.

[57] Searching, Copying and Seizure of Computers, Computer Programs and Files

Article 134 – (1) In the investigation conducted due to an offence, if there ise strong suspicion based on concrete evidecen and there are no other ways to obtain evidence, the judge or, where delay is prejudicial, the public prosecutor may deliver a decision to search, the computer, computer programs and files used by the suspecet and to take the image of computer records and to put into text such records after transcription. (Three sentences added on 25.7.2018 by the Law No. 7145 Art. 16) The decisions delivered by the public prosecutor shall be submitted to the approval of the judge within twenty-four hours and the judge shall render a decision within twenty-four hourse, at the latest. If the time expires or the judge decides otherwise, the images taken and transcribed texts shall be destroyed immediately.

(2) If computers, computer programs and files are inaccessible due to failure to decryption or hidden information is unreachable or the process would take a long time, such devices and tools may be seized for decryption and image taking purposes. Upon decryption of the code and taking the necessary images, the seized devices shall be returned without any delay.

(3) During the course of seizure of computers or computer files, a backup of all the data in the system shall be taken.

(4) A copy of the backup taken according to paragraph three shall be produced and given to the suspect or his/her representative and this procedure shall be registered in the records with signature.

(5) A copy of the entire data or some of the data in the system may be taken without seizing the computer or computer files. The data copied shall be written on paper, registered in the records and signed by the relevant parties.

examination and the hash value is calculated again, the same hash value will be considered as hash value conflict.

In the above-mentioned possibility, the credibility of the evidence will be shaken, and there will be hesitations by both the defense and the trial authorities. Therefore, it will be necessary to mention whether the possibility of collision is negligible. As stated in the statement in the introduction, there is never a certainty in science. Therefore, the possibility of collision in terms of hash values does not always indicate that the applied method is not scientific and causes forensic errors. What needs to be revealed is the mathematical ratio of the probability of the collision. In order to reveal this ratio, we have to start with some assumptions.

In terms of the trials held in our country after 15 July 2016 (due to coup attempt trials and membership in an armed terrorist organization), we would like to explain the issue by making probability calculations for the numerical material seized as evidence. In this context, let's assume that the number of people who have been sued is 100,000 and that 5 data medium (such as mobile phones, computers, portable memory) should be examined for each person. Accordingly, the probability of having the same summary values in 500.000 reviews, although they actually contain different data, is given in the table below. [58]

Algorithm	MD-5	SHA-1	SHA-256	SHA-512	RIPEMD-160
The Bit Number	128	160	256	512	160
The probability of collision (in 500.000 materials)	$3{,}673412 \times 10^{28}$	$8{,}552829 \times 10^{38}$	$1{,}079518 \times 10^{66}$	$9{,}322907 \times 10^{144}$	$8{,}552829 \times 10^{38}$

We can also add the following value to this probability. Let's take for granted that there are 1,000 files as system and user files on the seized devices in each investigation. In this case, we need to calculate the probability of hash conflict between 500,000,000 entries.

[58] The website http://davidjohnstone.net/pages/hash-collision-probability was used for the calculation and the probability of collision between the bit number of each algorithm and the material examined was examined.

Algorithm	MD-5	SHA-1	SHA-256	SHA-512	RIPEMD-160
The Bit Number	128	160	256	512	160
The probability of collision (in 500.000.000 material)	3.673419×10^{-22}	8.552847×10^{-32}	1.079521×10^{-60}	$9.322925 \times 10^{-138}$	8.552847×10^{-32}

The possibilities given above mean the following. The probability that the hash values of 500,000,000 different file inputs, taken from 500,000 data storage materials, are the same despite the change in the input data, are the numbers given in an increasing manner according to the number of bits of the algorithm. We can interpret this issue as follows, if there are 500,000,000 files in the digital material belonging to a person, the probability of two different files having the same summary value is as stated above.

V. CONCLUSION

The conclusion we will draw from here is, yes, since the hash values are mathematical formulas, there is a possibility of the same hash value in two different data inputs. However, these possibilities are not at a level to prevent the use of hash values that ensure the integrity of the data or to cast doubt on the evidence.

In addition, it is almost impossible that the hash values of the copied data storage devices (Hard disk, USB memory, etc.) will be the same as the hash value of the copied data storage device in another investigation or lawsuit. If two storage devices with the same hash value are detected, both devices should be subject to forensic investigation and explain why the hash values are the same. In the studies carried out to date; It is scientifically explained that the data storage devices that have the same hash value are either the same brand and model data storage device that has never been used, or they are a copy (clone) of each other.

Another issue is that the hash values of the files in the forensic copies are the same. This event applies to files in almost any forensic copy, since the hash values of standard files of operating systems will be the same. Examining and evaluating the content and metadata (metadata) information of the files with the same summary values is also a known and mostly done study in field of forensics.

REFERENCES

Aydın D, Ceza Muhakemesinde Deliller, Yetkin Publications, Ankara, 2014.

Bıçak V, Suç Muhakemesi Hukuku, 4th Edition, Seçkin Publications, Ankara, 2018.

Casey Eoghan, "Reconstruction Digital Evidence", in: Crime Reconstruction, Edited by W. Jerry Chisum – Brent E. Turvey, 2006.

Centel N / Zafer H, Ceza Muhakemesi Hukuku, 14th Edition, Beta Publications, İstanbul, 2017.

Chisum W B / Turvey B E, Crime Reconstruction, Academic Press, 2007, s. XV.

Cumhur Ş, Ceza Muhakemesinde İspat (Delillerin Doğrudan Doğruyalığı İlkesi), Yetkin Publications, Ankara, 2001.

Daniel L / Daniel L, Digital Forensics for Legal Professionals Understanding Digital Evidence From The Warrant To The Courtroom, Syngress, USA, 2012.

Değirmenci O, "Bilgi Toplumunun Delil Türü: Sayısal Delil ve Bilimselliği", Vol. 9, No. 97, Terazi Law Journal, September, 2014, ss. 14 – 28.

Değirmenci O, Ceza Muhakemesinde Sayısal (Dijital) Delil, Seçkin Publications, Ankara, 2014.

Digital Evidence in the Courtroom: A Guide for Preparing Digital Evidence for Courtroom Presentation, The National Center for Forensic Science, 2003, http:/www.ncfs.org/DE_courtroomdraft.pdf, accessed: 10.09.2011.

Doğan K, Ceza Muhakemesinde Belirsizlik Kuşkudan Sanık Yararlanır İlkesi "in dubio pro reo", Seçkin Publications, Ankara, 2016.

Erdem B/Işıtman N M, Basic Legal Documents of Turkish Criminal Law, Seçkin Publications, Ankara, 2021.

Eryılmaz A, Ceza ve Disiplin Hukukunda Hukuka Aykırı Delil, HUKAB Publications, Ankara, 2013.

Feyzioğlu M, Ceza Muhakemesinde Vicdani Kanaat, Ankara, 2002.

Gedik D, Öğreti ve Yargısal İçtihatlar Işığında Ceza Muhakemesinde Şüpheden Sanık Yararlanır İlkesi (In Dubio Pro Reo), Adalet Publications, 2016.

Harrington M, "A Methodology for Digital Forensic", Vol. 7, 2004, T.M. Cooley J. Parc. & Clinical L.

Hoffman S, "An Illustration of Hashing and Its Effect on Illegal File Content in the Digital Age", Vol. 22, No. 4, Intellectual Property & Technology Law Review, April 2010, ss. 6 – 14.

Hoffmann M, "Arguing for Suppression of 'Hash' Evidence", May 2009, The Champion.

Hricik D, "The Transmission and Receipt of Invisible Confidential Information", http//www.hricik.com/eethics/Metadata1103.doc, accessed: 06 Ocak 2013.

http://thinkexist.com/quotes/susan_brenner/, accessed 01 February 2014.

https://md5.hesaplama.net/hesaplama.do, accessed 05 Aralık 2017.

Israel A, "To Scrub or Not to Scrub: The Ethical Implications of Metadata and Electronic Data Creation, Exchange, and Discovery, Vol. 60, 2009, Alabama Law Review.

Jekot W, "Computer Forensics, Search Strategies, and the Particularity Requirement", Vol. VII, Spriing 2007, Pittsburgh University Journal of Technology Law and Policy, https://doi.org/10.5195/tlp.2007.29.

Koca M, "Ceza Muhakemesi Hukukunda Deliller", Vol. 1, Nu. 2, December 2016, Journal of Criminal Law, ss. 207 – 225.

Kruse W G/Heise J G, Computer Forensic: Incident Response Essentials, 2002.

Kunter N, Ceza Muhakemesi Hukuku, Revised and Enhanced 4th Edition, İstanbul, 1970.

Larkin J E D, "Compelled Production of Encrypted Data", Vol. 14, Number 2, Winter 2012, Vanderbilt Journal of Entertainment and Technology Law, ss. 253 – 278.

Maghaireh A M S, Jordanian Cybercrime Investigations: A Comparative Analysis of Search for and Seizure of Digital Evidence, Thesis Submitted in Fulfilment of the Requirements for the Award of the Degree, University of Wollonong 2009.

Mendel F/Pramstaller N/Rechberger C/Kontak M/Szmidt J, "Cryptanalysis of the GOST Hash Function", in: CRYPTO 2008, LNCS 5157 (Ed. D. Wagner), Springer 2008, ss. 162 – 178.

Nedir Bu Adli Bilimler/Kimdir Bu Adli Bilimciler, Adli Bilimciler Derneği Yayını, Ankara, 2019.

Newby T/Schwarz J M, "Rethinking The Storage of Computer Evidence", UNAFEI Resource Material Series No. 79, December 2009, Tokyo.

Robinton L R, "Courting Chaos: Conflicting Guidance from Courts Highlights The Need for Clearer Rules to Govern the Search and Seizure of Digital Evidence", Vol. 12, 2010, Yale Journal of Law and Technology, ss. 311 – 147.

Roxin C, "İspat Hukukunun Esasları", Translator Yener Ünver, Y. 4, No. 8, Fall 2005, İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi, ss. 265 – 289.

Schuck C M, "A Search for the Caselaw to Support the Computer Search 'Guidance' in United States v. Comprehensive Drug Testing", Vol. 16, No. 2, 2012, Lewis & Clark Law Review, ss. 741 – 781.

Selçuk S, "Temyiz Denetiminin Sınırları ve Bu Sınırlara Uymamanın Kaçınılmaz Sancılı Sonuçları/Açmazları/Tehlikeleri", Vol. 19, No. 2, 2013,

Marmara Üniversitesi Hukuk Araştırmaları Dergisi, Prof.Dr. Nur Centel'e Armağan, ss. 319 – 361.

Sommer P, "Downloads, Logs and Captures: Evidence from Cyberspace", Vol. 5, Journal of Financial Crime.

Sutton D, "Computer Forensics and Child Pornography Investigations", Vol. 2, 2011, Stevenson University Forensics Journal.

Şahin C/Göktürk N, Ceza Muhakemesi Hukuku – II, Revised and Updated 8th Edition, Seçkin Publications, Ankara, 2019.

Thompson E, "MD5 Collisions and the Impact on Computer Forensics", Vol. 2, 2005, Digital Investigation, ss. 36 – 40.

Tosun Ö, Türk Suç Muhakemesi Hukuku Dersleri Vol.:1, İstanbul, 1984.

Türkbağ A U, "Hukuka Gerçekçi Eleştirel Bakış: Hukuk Sosyolojisi", Issue 16, 2008/1, Sosyoloji Dergisi, 3rd Series, s. 43 – 54.

Uzunay Y/Koçak M, "Bilişim Suçları Kapsamında Dijital Deliller", Academic Informatics Conference, Gaziantep, February 2005.

Yayla M, Ceza Muhakemesi Hukukunda İspat ve Şüphe, Seçkin Publications, Ankara, 2016.