Research Article

Received: 5 June 2021 / Accepted: 15 July 2021 / Published: 5 September 2021

Digital Evidence and Prohibitions of Evidence Evaluation

PhD. Muhammet Ali Eren

Hacettepe University, Institute of Science,
Beytepe, Ankara, Turkey

Dr. Mensur Morina

Hacettepe University, Institute of Science,
Beytepe, Ankara, Turkey;
UBT University, Kosovo

Assoc. Prof. Dr. Endri Papajorgji

Dean, Faculty of Law,
Tirana Business University, Albania

DOI: https://doi.org/10.36941/jesr-2021-0106

Abstract

Since the first moment of the history of humanity, various means of evidence and evidence have been used to reach and detect the offender. As crime types and means of crime have changed and evolved, evidence detection and analysis methods have changed over time. At this point, with the rapid advancement of technology, the emergence of various and new types of crime that can affect many people at the same time in the global world is inevitable. Wherever you are in the world, it is now possible to commit crimes in one way or another that affect one or more people on the other side of the world through the Internet and digital systems. This, in turn, has led states to safeguard their cyber security. For this reason, firstly, it has made a legal regulation to protect its own citizens in domestic law and then it has been forced to cooperate internationally. The way in which classic crime types are committed and the method of evidence is different from the crimes committed through digital systems. The main purpose of the methods of obtaining and proving evidence is to reveal the material truth for a past event. There are also legal requirements, technical methods and scientifically accepted methodologies that must be followed when uncovering material truth. Because digital evidence is both different and more open to manipulation than other classical proofs, it is a matter of adherence to laws and technical rules when obtaining evidence. In order to obtain digital evidence in the Code of Criminal Procedure No. 5271; It has been arranged as a search, copy and seizure protection measure in computers, computer programs and files. Although the heading of the respective substance is initially considered only as a protection measure for computers, it will find application for all devices and systems containing digital data, as detailed below.

Keywords: *Information Systems, Proof, Digital Evidence, Evidence Detection Methods,Computer Programs and Logs*

1. Introduction

In the historical process, science and technology progress every second to make people's lives easier. Law, on the other hand, responds to the development of society and guarantees the rights and freedoms of people. These two elements develop and change in parallel with each other.

Technology is used over time, in all areas of life and in every moment of people. Examples include digital-based systems, computers, smart mobile phones, tablets, car technology systems, vehicle tracking systems, cloud technologies, smart televisions, smart home systems and even smart cities. However, the two most important devices that occupy most of our time in daily life are computers and smart mobile phones. From waking up in the morning thanks to smart mobile phones, following daily, weekly and monthly business plans with assistant services, checking e-mail accounts, classical banking transactions, buying and selling stocks, foreign currency and commodities, daily phone calls, following social media accounts, photography and From video recording, to individual or group conversations, until the device is turned off, all operations are now carried out via smart mobile phones. It is no longer possible to do business without a computer in business life. The development and widespread use of social media has not prevented these two devices from becoming an indispensable part of our daily lives. As a result of the widespread use of technology in social life, it has become in need of certain legal regulations. Most importantly, it manifested itself in the Turkish Criminal Law.

It has become inevitable that no crime is committed by means of these technological devices that have entered all areas of life. While using technological devices, each of them contains digital evidence in the automated systems they contain. For this reason, digital proofs are obtained in these systems based on the motto that every click leaves a mark, including deletion. Although most users using technological systems think that this process disappears after deleting their transaction, this is not the case. Since deletion is also a click process, even this process leaves a digital trace behind it and its evidence is preserved.

The two most basic laws of Turkish criminal law are the Turkish Penal Code and the Criminal Procedure Law. Among these two laws, the Criminal Procedure Code regulates the articles on the investigation of the material truth regarding the crime and the criminal after the crime has been committed, and at the same time protects the rights of the victim, suspect and defendant. The purpose of the Law has been defined in Article 1 of the Turkish Penal Code. according to this : "*It is to protect the rights and freedoms of individuals, public order and security, the rule of law, public health and the environment, public peace, and prevent crime. The law regulates the basic principles of criminal responsibility, crimes, punishments and types of security measures in order to achieve this goal.*" in the form.

After a crime has been committed through digital systems, to investigate the material truth, uncover the crime and the criminal, and obtain digital evidence must be collected in methodwith Article 134 of the Turkish criminal procedure law. While collecting evidence, the evidence collection process should be viewed from both sides. On the one hand, there is the superior benefit of the victim and the society, on the other hand, there is a limitation on the fundamental rights and freedoms of the suspect. The balance here must be well maintained. Obtaining digital evidence requires separate expertise compared to other classical evidence. It is also open to change, deterioration and manipulation due to its structure. For these reasons, digital evidence must be collected in accordance with the law.

2. Methodology

In this study, various source books, articles, thesis studies, laws, regulations, security strategies, research publications of relevant local and international non-governmental organizations, the historical development and evolution of the subject, the changes made by the legislative and executive organs in the legislation, the changes made in the world on how to collect digital evidence,

legal regulations will be examined, theoretical concepts such as the synthesis of technical and legal concepts, and the literature and publications on the research process of the aforementioned subjects will be examined.

3. Evidence in General

Evidence, in general, is a means of proof that proves or refutes all or part of an alleged event in the law of reason. In other words, everything that serves to resolve a legal dispute or to prove a criminal act and whose substitution is prohibited by law is called a means of evidence or proof (Kaygısız, 2005). The evidence serves the judge to resolve the material event as a result of the judgment, to overcome his doubts about how the material event took place, to see whether the material event was fixed (Toroslu and Feyzioğlu, 2009). The concept of evidence is used as a means of proof in law. In this context, everything that serves to resolve a legal dispute or prove a criminal act and whose substitution is not prohibited by law is called evidence or means of proof (living/non-living, written/verbally). Evidence includes all kinds of means of evidence that serve to enlighten a crime and identify the perpetrators of the crime (Kaygısız, 2007).

The important thing in criminal proceedings is not to satisfy the parties but to reveal the truth (Toroslu and Feyzioğlu, 2009). The criminal trial in which material truth is sought begins with evidence and progresses with the acquisition of other evidence. All means to provide proof are only evidence. Although every means of proof is an evidence in the abstract, the evidence is subject to an evaluation at the trial stage and if necessary, they are not accepted as evidence. In this respect, the fact that something can be evidence and that something can be accepted as evidence are different things (Kunter and Yenisey, 2000) .

4. Digital Evidence (D-Evidence)

Today, by most scientists; it is called the internet, information technology or digital age. Most people can now do shopping and banking transactions from anywhere in the world where the internet can be reached, communicate with their social circle, make new friendships and even get married without leaving their homes. The biggest reason why digital systems have such a place in human life is that they can handle many tasks and make life easier with one click in seconds.

While the world's most valuable companies were once oil, industrial and automotive companies, they have now taken their place as technology companies such as Apple, Google, Amazon, Facebook, Oracle and Microsoft. The biggest reason for this is that internet and informatics are now functionally taking place in people's daily life.[1]

According to the data on the online statistics portal Statista, as of July 2019, internet usage in the world reached 4.33 billion people, reaching 56 percent. According to the data released in March 2019, when evaluated on a country basis, China ranks at the top in internet usage with 829 million users. China is followed by India with 560 million and the USA with 292 million. Internet, social media and mobile user statistics according to We Are Social 2020 Q2 report; 4.57 billion internet users, 59% of the world population, 3.81 billion social media users, 49% of the world population, 5.16 billion mobile users, 66% of the world's population. The increase in the number of Internet, Social Media and Mobile Users compared to the same period of the previous year; Number of Internet Users: 7.1% (301 million) Number of Social Media Users: 8.7% (304 million) Number of Mobile Users: 2.5% (128 million).When we look at the World Internet usage statistics for the year 2020, the number of general users has increased to 4.57 billion people in total. (59% of the world population).[2]

[1] *https://www.aa.com.tr/en/economy/most-valuable-brand-amazon-breaks-200b-mark-report/1710087* .
[2] *https://wearesocial.com/blog/2020/04/digital-around-the-world-in-april-2020.*

Turkey with 69 million users, according to data in the report is one of the countries with most Internet users.[3] Global social media agency We Are Social, and the results of research conducted by HootSuite according to published reports Digital Turkey in 2019, 98 percent of adults in Turkey with a population of 82.4 million population use mobile phones. In the report, it is underlined that Turks spend an average of 7 hours and 15 minutes a day on the internet, and 2 hours 46 minutes of this time on social media. While 59.4 million people, corresponding to 72 percent of the population, use the internet, 56.3 million of them connect to the internet through their phones.[4]

Assuming that a person sleeps an average of eight hours a day, half of the remaining 16 hours, according to this research, are spent on the internet. The fact that digital systems take up so much space in people's daily life brings along many legal and criminal disputes.

The most important feature that distinguishes digital evidence from other evidence is intangible, invisible and virtual. For this reason, digital evidence becomes meaningful only through the relevant hardware. For example, for an image file recorded on a CD, there should be a CD player and a screen to display it. If the image on this CD is to be printed on paper, a computer and printer will also be needed. As you can see, the existence of the CD alone is not enough to reach the image inside it.

Digital evidence can be obtained from any device with digital data. The most prominent and familiar ones; computer and computer based devices, fixed and portable data storage devices, CDs, printer, scanner, fax, photocopiers, smart cell phones, cameras, cameras, modems, firewalls, switching devices (switches), e-mails, are servers.

It is known that digital evidence is open to manipulation due to its nature. Although it has some aspects that are characteristic compared to other types of evidence, it is a means of proof in the criminal procedure system where the freedom of evidence is adopted. In the evaluation of the evidence, which is a means of proof, it is taken into consideration whether it has the qualifications prescribed for an evidence in the criminal procedure law. Matters such as the characteristics of the concrete incident, the way the crime was committed, and other evidences in the file are taken into consideration, and in particular; Matters such as the nature of the event represented by the evidence, the place, form and time of capture, and other characteristics of this evidence should be taken into consideration.

Digital evidence, such as chemical, biological and other similar evidences, are suitable for concealing, alteration, and corruption by the defendants or other persons in various ways. For this reason, it is very important to obtain and ensure reliability after obtaining.

If the matter that will shed all or part of the material truth is based on digital evidence, it will be subject to a different legal regime. The emergence of these legal regimes has also led to the formation of different and new terms. Among these concepts, a new type of evidence that is described as computer evidence, electronic evidence, digital evidence, and digital evidence has been encountered. First of all, these concepts should be defined correctly, and then legal regulations should be clarified.

Because of that, Digital evidence is subject to procedural law and is used to illuminate the alleged event, based on the binary number system (0-1) and creating a data, storing, working, transfers from one place to another, capable of producing results according to the logical command system. It is the type of evidence obtained from the systems. In other words, Digital evidence is forensic evidence obtained through information systems and storage devices within this scope (Henkoğlu, 2011). Unlike physical evidence such as written document, blood, saliva, hair; digital evidence they are open and sensitive evidence for manipulation.

With the differentiation and development of technology every day, the areas where digital systems are used are also increasing and the crime areas are expanding. Since the technology of

[3] *https://www.aa.com.tr/tr/bilim-teknoloji/dunyanin-yuzde-56si-internet-kullaniyor/1549033.*
[4] *https://wearesocial.com/blog/2019/01/digital-2019-global-internet-use-accelerates.*

digital systems changes in this context, the methods of obtaining evidence from these systems are also updated. For all these reasons, obtaining and ensuring its reliability are subject to strict formal requirements in the law of procedure and exclusively regulated. Although, according to the views in the legal system and some doctrines, digital evidence is referred to as computer evidence, it is clear that digital evidence cannot be obtained only from computers and computer-based systems. Limiting the systems from which digital evidence can be obtained to only computers will also be against the principle of revealing the material truth that prevails in the law of reason and will not establish justice.

5. General Digital Definitions

5.1 Data, Information, Computer, Information Technology, Informatics.

Based on its most classical definition, a phenomenon that is unprocessed and raw, which does not make sense on its own is called data, and what is found in a digital environment is called digital data. As soon as data is processed and begins to make sense, it becomes information. If this information is in digital environment, it will be called digital information. Data in the Law No. 5651 on Regulation of Broadcasts Made on the Internet and Fight Against Crimes Committed Through These Publications; As any value that can be processed by the computer; information is defined as the form of data that has gained meaning. As can be understood from these definitions, it is possible to reach the conclusion that every information is actually a data, but not every data is information.[5] Information will emerge when data or data come together to form something meaningful in the mind of the addressee.

It is possible to transfer, move or process data and information from one place to another. These can be in the physical paper environment as well as through digital systems. Here, the systems that process, transfer, transport, store and make a conclusion with software tools through digital systems are called computers. The ability of more than one computer and computer peripheral products to come together to process and transfer data and information with automatic software systems is called information systems. If we set out with another definition, digital systems that take a data, process this data and produce an output or result as a result are called information systems.

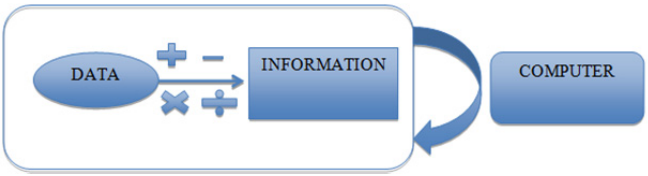

Figure 1: Data Processing Systematics

Information will emerge when data or data come together and be processed, creating something meaningful in the mind of the addressee. It is possible for data to be transferred, moved or processed from one place to another, just like information. These can be transported and processed through digital systems as well as in the physical paper environment. Here, the systems that process, transport and store data or information through software-based electronic and digital systems are called computers. While the hardware part of the computer is physical and tangible, the software side is virtual and abstract.

The structure that can combine more than one computer and computer peripherals (such as

[5] *https://www.mevzuat.gov.tr/MevzuatMetin/1.5.5651.pdf.*

printer, scanner, modem) and process and transfer data with automatic software systems is called information systems. If we set out with another definition, digital systems that take a data, process this data and produce an output or result as a result are called information systems. According to the great Turkish dictionary, the computer is the electronic device, the electronic brain, that performs and completes a task consisting of many arithmetic or logical operations according to a predetermined program. Informatics, on the other hand, has been defined as the science of processing information, which is the basis of science, which is used by human beings in their communication in technical, economic and social fields, in an orderly and rational manner, especially through electronic machines. In the justification of Article 243 of the Turkish Penal Code No. 5237, the information system is defined as magnetic systems that allow the data to be subjected to automatic processes after collecting and placing them. The Turkish Court of Cassation Criminal General Assembly (2009/193E - 2009/268K.), has defined the information system as magnetic systems that allow automatic processing after collecting and placing data. Turkish Court of Cassation 12th Penal Office (2015/10388E - 2017/1556K) in its decision, automatically processes the information system, evaluates the data entered to it in various ways, and presents it back in a reprocessed form and with certain evaluations upon the request of the user or performs a new transaction on the system with the contribution of the user defined as electromagnetic, digital and virtual networks and environments that provide recording. In the doctrine, it is defined as the whole of hardware and software elements that are suitable for realizing all the purposes expected from the computer, including all peripherals such as the Information System, printer and modem.

5.2 *Software and Computer Program*

In parallel with the development of first mechanical and then electronic and digital systems, efforts to ensure that these systems operate independently from human and automatic have been accelerated. As a result, software and programs that can perform both self-directed and user-based operations have been developed.

The system that processes, transmits, stores data according to certain commands within a certain logical systematic and produces results according to this certain logical command system is called a program. In a shorter definition, a program is a sequence of commands written to perform a certain task. Software, on the other hand, can be defined as codes that are outside of the physical hardware of the computer, but that indicate what data and what process these parts will do, when and how. Software is the basis of the operation of the programs.

In other words, software; as all the programs, procedures, programming languages and documentation that bring hardware to life and are used in computing in a computer. Computer program is defined as a computer command sequence arranged in a way that enables a computer system to perform a specific operation or task.

5.3 *Log*

In digital systems, the place where the data set is saved is called a log. According to the great Turkish dictionary, log is the name given to all records that are processed together and related to each other. In another definition, the logical storage unit where any data is stored in information systems is called a log. Logs can take names such as computer logs and database registers according to their location. Users create files, folders and other programs by creating these files.

The log is neither a hard disk, nor a flash drive, nor the computer itself. The log is the abstract digital storage place where interrelated data is stored. The log may contain photographs, videos or written documents, as well as diary records, database records, internet server records or application programs. The data sets in the registry can be created by the user or can be created automatically by automated software programs.

5.4 Definitions Of The Electronic And Digital

Historically, although the existence of technological devices dates back to the invention of the wheel, the basis of digital and electronic based technological systems goes back to the invention of electricity. In its simplest definition, electricity is the energy released by the movement of electron particles. Electronics, on the other hand, is the science of making various equipment by using the motion of negatively charged electrons. Electronics deals with the control of free electrons, and this structure forms the basis of many devices such as radio, television and computers (Karagülez , 2014). Electronics, according to its function, is divided into two as analog and digital. The signal transition in analog electronics is constantly changing and consists of sine waves in nature. The word digital is derived from the Latin word digitus, which is used to count numbers. It consists of zeros and ones, which are binary counting systems. It takes the value 1 if high voltage passes, and zero if weak voltage passes. It produces square wave as signal indicator.

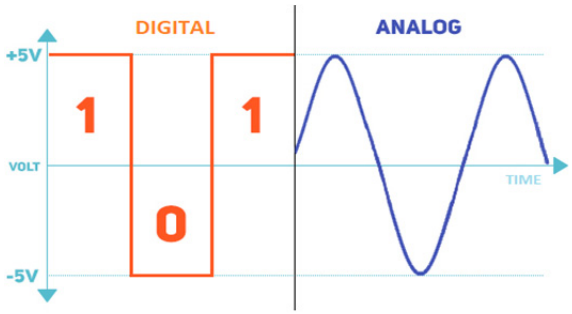

Figure 2: Analog and Digital Signal Display

Digital has distinct advantages over analog in electronic systems. One of them is that digital information can be processed and transmitted more effectively and securely than analog information. In addition, when information needs to be stored, digital information has a great advantage. In other words, it is easier to store information in digital systems. With the methods used in digital systems, it is possible to put information somewhere, to receive it and to keep it as needed. Digital circuit designs are easier than analog since the operations in the system are controlled by commands that can be stored. The operations in these circuits have a programmable structure. In digital circuits, it is possible to have more circuits integrated and their communication with each other. On the other hand, an analog signal can be converted to a digital signal (ADC-Analog to Digital Converter), and a digital signal to an analog signal (DAC-Digital to Analog Converter). Examining such intertwined concepts requires technical expertise.

6. Difference of Digital Evidence from Other Evidence

6.1 Difference of Digital Evidence from Conventional Evidence

Digital proofs are abstract in nature compared to other classical proofs and exist only in digital systems. But other evidence can be found everywhere and in concrete form. For example, a blood stain can be found on a shirt or knife, but digital evidence is only found in digital-based systems. For these reasons, in the Code of Criminal Procedure, digital evidence has been subjected to a unique regime such as search, copying and seizure, unlike physical evidence.

Digital evidence is invisible. For example, the physical state of the hard disk does not mean anything to the person concerned, but it becomes meaningful when the information in it is accessed

by experts through the computer system.

It is possible to reach deleted data in digital evidence, but this is not possible in classical evidence. For example, while it is possible to access a photo image deleted by the perpetrator, it is not possible for forensic medicine to reach them after the perpetrator erases and removes the hair, saliva and blood stains.

On the other hand, after a crime is committed, the first thing the perpetrator will do is to destroy the traces he left behind. When physical evidence is erased or changed, it is easier to understand than digital evidence. However, manipulation in digital evidence can be more difficult to understand.

Unlike conventional evidence, collecting, preserving, analyzing and evaluating digital evidence is more difficult and costly.

The most important feature that distinguishes digital evidence from physical evidence is that it cannot be taken as a basis for conclusive and convincing evidence, free from any doubts, when a judgment is made in court. Because digital evidence does not contain features such as fingerprints and DNA structures belonging to the person, therefore, there is no 100% certainty in digital evidence, but it can be supported by other evidence and cleared of suspicion.

On the other hand, it would be wrong to conclude that the judgment is not based on the ease of changing digital evidence and its virtual nature.

While it is often easily understood whether the classical evidence obtained at the scene of the crime is used in the crime, it cannot be established immediately as the digital evidence is found in a media environment. For this reason, computer forensic examinations should be performed on the device.

Digital evidence can be easily deleted, changed, copied, hidden, encrypted, examined on its copy, and compared with the original and copied form through appropriate programs. However, it is not so easy to apply these methods in classical evidence. For example, it is not possible to copy a blood sample and examine the copy.

6.2 DifferencesBetween Digital Evidence and Electronic Evidence

Digital evidence and electronic evidence are often confused and used interchangeably, both in practice and in doctrine. After understanding exactly what these concepts are, it will be easier to decide whether the evidence obtained is electronic or digital.

Electronics is the branch of science that studies the elements and systems that process, transport or store information using electricity. It is especially about the control of free electrons. Electronic circuit and its components are divided into two groups as analog and digital. Analog circuits are circuits that use uninterrupted and continuous (sinusoidal) signals. Digital circuits, on the other hand, are circuits that use discrete signals. A binary system with voltage levels of 0 or 1 is used.

Figure 3: Square Wave (Digital Signal) and Sine Wave (Analog Signal)

Digital has distinct advantages over analog in electronic systems. One of them is that digital information can be processed and transmitted more effectively and securely than analog information.

It is easier to store information in digital systems. With the methods used in digital systems, it is possible to put information somewhere, to receive it and to keep it as needed. Digital circuit designs are easier than analog because the operations in the system are controlled by commands that can be stored. The operations in these circuits have a programmable structure. In digital circuits, it is possible to have more circuits integrated and their connection with each other.

7. Features Of Digital Evidence

Digital evidence is the means of proof put forward to reveal the material truth in an event that is alleged to have happened in the past. In the criminal procedure, the evidence can be put forward at every stage of the case and the alleged event can be proven with all kinds of evidence. In accordance with the principle of circumstantial evidence, as a rule, everything can be evidence, but it is a must that they also have the necessary features in order to qualify as evidence. These features are necessary for the said means of proof to be qualified as evidence, and a means of proof that does not have the specified qualifications cannot be treated as evidence in criminal proceedings (Degirmenci, 2014).

The features that digital evidence should have can be listed as follows.

1) Must Represent the Material Event.
2) It must be rational, scientific and reliable.
3) Must Be Re-obtainable.
4) Should Have Been Discussed in Court.
5) Must Be Lawful (there should be no illegal evidence).

7.1 Prohibitions of Evidence Evaluation

There is no limitation in criminal procedure as to which issue can be proven by which evidence. The judge who made the trial; can use all kinds of evidence belonging to the concrete event, having the characteristics obtained in accordance with reason, science and logic and in accordance with the law. The judge must reach a conclusion free of doubt by investigating and evaluating the evidence against the accused as well as in favor of him. In the incident subject to jurisdiction, every instrument obtained by legal methods used for the purpose of proving the material truth is accepted as evidence.

The necessity for the evidence obtained to comply with the law may arise from both the constitution and the law. According to Article 38 of the Turkish Constitution; "*Findings obtained illegally cannot be accepted as evidence*" and in Article 206 of the Turkish Criminal Procedure Code "*evidence will be rejected if it has been obtained unlawfully*" and in Article 217, "*the crime can be proven by any evidence obtained in accordance with the law*" has been taken under provision.

Although some evidence is obtained by lawful means, when presented to the court authority, they cannot be used as evidence due to their content or obtainment. In the Turkish Code of Criminal Procedure, Article 148, Paragraph 3, it is stipulated that the statements obtained through prohibited procedures cannot be considered as evidence even if they are given with consent. For example, a doctor cannot present the information obtained without the consent and permission of his patient as evidence against him. On the other hand, it would be illegal to obtain a statement as a result of ill-treatment by threatening, blackmailing or torturing the person's family or property that violates the free will of the individual.

8. Conclusion

In criminal proceedings, the judicial authorities have to investigate all kinds of evidence in accordance with the law in order to reach a result. For both the accused and the victim, since criminal procedure is a branch of jurisdiction that directly interferes with fundamental rights and freedoms, during trial activities, fundamental rights and freedoms should not be violated with the understanding of finding evidence, nor should the law be abandoned in order to protect the rights.

The most important feature that distinguishes digital evidence from other evidence is that it is suitable for manipulation, intangible, invisible and virtual. For this reason, obtaining evidence from digital devices requires special expertise and should be done according to a certain procedure.

Obligation to obtain digital evidence in accordance with the law, in addition to establishing justice with real evidence, it is also a matter of fundamental rights and freedoms.

Digital evidences understood to be unlawfully obtained, cannot be taken into account in proving an incident by the judge. The way in which the evidence presented by the parties during the trial is obtained will be taken into account ex officio by the judge. In addition, if it is determined whether such evidence has been obtained legally through legitimate means and methods, and if it is determined that the evidence was obtained unlawfully by any means whatsoever, even if the other party does not make an objection in this regard, it should be decided that the evidence presented by the court is not permissible and should not be evaluated within the scope of the file.

9. Acknowledgement

This article is produced from the doctoral thesis of Hacettepe University, Institute of Sciences.

References

Degirmenci, O. (2014). Numerical Evidence in Criminal Procedure, Seçkin Publishing House.
Henkoğlu, T. (2011). Computer Forensics Analysis of Digital Evidence, 1st Edition Pusula Publications, Istanbul.
Karagülez, A. (2014). IT Crimes and Investigation - Prosecution Phases, Seçkin Publications 5.B., Ankara.
Kaygısız, M. (2007). Criminalistic Crime Scene Investigation Crime Scene and Event Security, Ankara: Justice Publishing House.
Kaygısız, M. (2005). Forensic Sciences, Seçkin Publications.
Kunter, N., Yenisey, M. (2000). Criminal Procedure Law as a Branch of Law of Procedure, 11th Edition, Istanbul: Beta Publishing House.
Toroslu, N., Feyzioğlu, M. (2009). Criminal Procedure Law, 7. Edition, Ankara: War Publications.
https://www.aa.com.tr/en/economy/most-valuable-brand-amazon-breaks-200b-mark-report/1710087
https://wearesocial.com/blog/2020/04/digital-around-the-world-in-april-2020
https://www.aa.com.tr/tr/bilim-teknoloji/dunyanin-yuzde-56si-internet-kullaniyor/1549033
https://wearesocial.com/blog/2019/01/digital-2019-global-internet-use-accelerates
https://www.mevzuat.gov.tr/MevzuatMetin/1.5.5651.pdf