Advances in Networks
2026, Vol. 13, No. 1, pp. 1–8
https://doi.org/10.11648/j.net.20261301.11

Research Article

European Directive 2013/40 and Digital Forensics

Ljubiša Zdravković[1, *], Milica Zdravković Jovanović[2]

[1]Faculty of European Legal and Political Studies, Kallos European University, Belgrade, Serbia

[2]Faculty of Electronics Niš, University of Niš, Niš, Serbia

Abstract

European Directive 2013/40 is the first comprehensive document created by the EU in the field of cyber security. It represents the EU's comprehensive vision of how to best prevent and respond to cyber interference and attacks, and on the other hand, enable the development of information technologies. It promotes respect for basic EU values, defines illegal behavior, advocates the application of existing international regulations in the field of high-tech crime, assists other countries outside the EU in building capacity to fight high-tech crime, and promotes cooperation in this area. The speed of technological development has influenced the development of digital forensics as a young scientific discipline, which, together with the parallel development of other sciences, applies new methods that affect the speed and simplicity of collecting solid evidence, investigates anti-forensic activities, with the aim of discovering the truth about committed illegal act. In response to high-tech crime, there was a need for the development of a new scientific discipline that will deal with it, as well as the regulation of legal bases related to the successful prosecution of criminal offenses in this area. Digital forensics is the application of investigation methods and analysis techniques in order to find suitable evidence for the court, in high-tech crimes. In order to prove the committed illegal acts and prosecute and sanction their perpetrators, it is necessary to apply the procedures of digital forensics as a scientific discipline with extremely significant practical application. Precisely digital forensics as a relatively new scientific discipline (established in 1999 by IECO - International Organization on Digital Evidence) provides the only reliable tool for the investigation of high-tech crime, the acquisition and analysis of digital data and the preparation and presentation of digital evidence before the court. It should be emphasized that for a digital forensic scientist, the monitoring and development of information technologies is of crucial importance. Sometimes differences in the operating system or version of a program are essential. That is why it is important to have digital forensic experts profiled according to their professional field (operating systems, databases, network systems, as well as profiling according to other ICT systems).

Keywords

European Directive, Digital Forensics, Digital Evidence, Forensic Investigation, High-tech Crime

1. Purpose

The question arises, what exactly does high-tech crime, or cybercrime (the American name for this type of crime that has taken root in many world languages) mean? A unique answer to this question does not yet exist, but what is common to many definitions that determine this term, a common element can be observed - the use of a computer or computer network and the Internet. In the world of high-tech crime research, we find such a narrow interpretation of this term in a large

*Corresponding author: ljubisa.zd@gmail.com (Ljubiša Zdravković)

Received: 1 September 2025; **Accepted:** 15 September 2025; **Published:** 16 January 2026

Copyright: © The Author(s), 2026. Published by Science Publishing Group. This is an **Open Access** article, distributed under the terms of the Creative Commons Attribution 4.0 License (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution and reproduction in any medium, provided the original work is properly cited.

number of internet encyclopedias and dictionaries, so cybercrime is defined as "criminal activity committed using computers and the Internet.[1]".

Legislative solutions related to the field of high-tech crime in the legislation of the Republic of Serbia move in three directions. The first group of activities consists of the Law on the Organization and Competence of State Bodies for the Fight against High-Tech Crime (Official Gazette of the RS, no. 61/05 and 104/09), which establishes the organization and competence of special state bodies in the fight against this type of crime.

The law represents an expression of the understanding of the risk that carries with it the commission of criminal acts in this area and contributes to the establishment of high-tech security. The law is the result of the understanding that such a negative social phenomenon, due to its nature and its distinct transnational character, cannot be fought without adequate legal regulations of a national character and coordinated international cooperation on these issues, and the normative basis for this is precisely this legal text. In addition, by adopting this law, Serbia has complied with the requirements of the Council of Europe Convention on High-tech Crime, which establishes a minimum standard that is necessary, in the opinion of the international community, to meet national legislation in order to effectively fight against high-tech crime.

The second group of regulations in the legislation of the Republic of Serbia concerning high-tech crime consists of regulations of a material nature. First of all, it is the Criminal Code (Official Gazette of the RS, no. 85/2005, 72/2009 and 35/2019), which prescribes crimes in the field of high-tech crime. Observed in relation to earlier legal solutions of this type, it can be stated that this legal text, when it comes to high-tech crime, is characterized by the following peculiarities. The Code provides for criminal acts related to the field of high-tech crime that were also provided for in earlier laws, while some new criminal acts that did not previously exist as a criminal offense were also prescribed. The case of e.g. with the criminal offense of unauthorized use of a computer or computer network from Article 304 of the Criminal Code.

The Code of Criminal Procedure [2] (Official Gazette of the RS, no. 35/2019 and 27/2021.) is the representative of the third group of regulations in the legislation of the Republic of Serbia when it comes to the criminal law issue of high-tech crime in general. The Code contains provisions of a procedural nature, which provide for procedural mechanisms and powers of all participants in criminal proceedings with regard to the detection of perpetrators of criminal acts, collection of evidence, prosecution and trial. [3].

In the Convention on Cybercrime (Convention on Cybercrime) of the Council of Europe, a computer system is defined as any device or group of interconnected devices that perform automated data processing. This further implies that without them and without computer networks, this form of crime does not exist. Cybercrime presented in this way covers a large number of different criminal activities, including attacks on computer data and computer systems, attacks related to computers, content or intellectual property, so in the literature it is most often referred to as one general term - umbrella.

We can also single out one of the most complete, although perhaps not the most precise, definitions of the complex concept of cybercrime presented at the UN at the Tenth Congress of the United Nations, dedicated to the Prevention of Crime and the Treatment of Perpetrators since April 2000 (Crime related to computer networks 2011,) [4]. Cybercrime is crime that refers to any form of crime that can be committed with computer systems and networks, in computer systems and networks, or against computer systems and networks. It actually implies some criminal act that engages a computer system or network as a means or as a goal of committing criminal acts or that is realized in an electronic environment. The characteristic of cybercrime is that it is done with intent and not by accident.

Furthermore, in support of this degree of topicality of the social danger of this type of crime, the fact that the Internet connection of not only all countries in the world but almost even their smallest territorial units is today a feature of the world as a whole should be emphasized. There is almost no part of the globe that is not connected to its other parts by the Internet, regardless of which continent and country it belongs to, which has led to complete computer control of the most important social processes. Considering this, it is expected that a lot of abuses will result from such a large process.

Then, there is the fact that according to the latest data in the so-called almost a third of humanity is in cyberspace, which conditions new rules of behavior, new customs, and entails new dangers. [5].

Cyber security includes challenges that cross state borders, while the answers to them, which are also insufficient, mostly remain in the state's horizons. There are huge gaps in our understanding of this problem, as well as in the technical and systems capabilities necessary to deal with it. In addition, problems of democratic governance are almost completely absent in the debate, especially when it comes to issues of control, supervision and transparency. These problems in online security of all kinds are made even more drastic by the large role of the private sector (both independently and in cooperation with governments). Given the pace at which states and private companies are strengthening online security in preparation for cyberwarfare, paying attention to issues of democratic governance has never been more urgent. [6].

The European Directive 2013/4 represents the first comprehensive document that the EU has created in the field of cyber security. It represents the EU's comprehensive vision of how to best prevent and respond to cyber interference and attacks, and on the other hand, enable the development of information technologies. It promotes respect for basic EU values, defines illegal behavior, advocates the application of existing international regulations in the field of high-tech crime, helps other countries outside the EU in building ca-

pacity to fight high-tech crime and promotes cooperation in this area.

What is particularly important when we talk about high-tech criminality or so-called cybercrime, as well as the inestimable importance of the European directive 2013/40, is certainly the importance of digital forensics.

Digital forensics is the application of investigation methods and analysis techniques in order to find suitable evidence for the court, in high-tech crimes. In order to prove the committed illegal acts and prosecute and sanction their perpetrators, it is necessary to apply the procedures of digital forensics as a scientific discipline with extremely significant practical application. Precisely digital forensics as a relatively new scientific discipline (established in 1999 by IECO - International Organization on Digital Evidence) provides the only reliable tool for the investigation of high-tech crime, the acquisition and analysis of digital data and the preparation and presentation of digital evidence before the court.

2. Access

The Convention on Cybercrime (CETS 185), developed by the Council of Europe with the cooperation of Canada, Japan, South Africa and the USA, was opened for signature in Budapest in November 2001 and has been in force since July 2004. It is open for access by any country and is the only binding international agreement on this topic that has been adopted to date. The Protocol on Punishment of Acts of Racism and Xenophobia Committed Through Computer Systems (CETS 189) was opened for signature in January 2003 and has been in force since March 2006.

The convention requires signatory countries to create the basic legal infrastructure necessary to effectively combat cybercrime and to assist other signatory countries in the investigation and prosecution of cybercriminals. The Convention includes: criminal acts; unauthorized access to a computer system; unauthorized interception, data corruption; jamming the system; misuse of the device; computer forgery and fraud; child pornography; infringement of copyright and related rights; and means for effective investigation and protection. It applies to any offense committed through a computer system and to all evidence in electronic form.

This Convention has been ratified by 28 countries (EU countries and USA); it was signed by 46 of them (EU countries, Canada, Japan, South Africa, all NATO member countries); five countries have been invited to accede (Chile, Costa Rica, the Dominican Republic, Mexico and the Philippines) and several significant non-signatory countries (Russia and China). It is used as a guideline, reference standard or model for laws in more than 100 countries. In addition, the Convention is supported and referred to by other organizations, including: the European Union; Organization of American States; OSCE; Asia-Pacific economic cooperation; Interpol, as well as members of the private sector.

Although there has been widespread international acceptance of the Convention, some have criticized it as insufficient to properly address actions with national security implications. First, the Convention treats attacks on IT systems as crimes against public and private property and thus ignores the consequences of such attacks on national security. Second, it does not distinguish between attacks on ordinary computer systems and attacks on critical infrastructure information systems, nor between small and large attacks.

Despite this, the Convention represents a basic but essential part of international legislation. It provides a good collection of legal and technical definitions from which other cooperative agreements can be developed. Since there is significant overlap between cybercrime, cyberterrorism and cyberwar, the Convention's criminalization of all forms of cyberattacks, regardless of motive, means that signatory states are obligated, when requested to do so, to apprehend and prosecute all international cyberattackers, regardless of whether the host state considers them criminals, terrorists, or even laudable patriots.

The documents of the Council of Europe are: - Recommendation on criminal activities related to the use of computers, from 1989, - Recommendation that regulated issues related to procedural rules related to information technologies, from 1995, - Convention on the protection of individual rights in connection with automatic processing of personal data, from 1981, entered into force in 1985, - Convention and Additional Protocol of the Council of Europe on high-tech crime, the convention is from 2001 and entered into force on July 1, 2004, the additional protocol from 2003, entered into force on March 1, 2006, - Convention on the Prevention of Terrorism, from 2005, - Convention on the Protection of Children from Sexual Exploitation and Sexual Abuse, from 2007.

Directive 2013/40/EU was adopted by the European Parliament on August 20, 2013 and refers to attacks directed against information systems. The directive changes the Council's framework decision 2005/222/JHA and is an integral part of the so-called "ACQUI COMMUNAUTAIRE" - the common framework of the member states of the European Union. [7].

The aim of the Directive is to bring the field of attacks against information systems closer to the criminal legislation of the member states of the Union, by establishing minimum rules related to the definition of criminal offenses and appropriate criminal-legal sanctions, as well as improving cooperation between competent authorities that include members of the police and other specialized law enforcement agencies of the Union members, as well as competent specialized agencies and bodies of the European Union itself such as EUROJUST, EUROPO or its European Center for Cybercrime (EC 3), as well as the inclusion in the work of the European Agency for Network and Information Security (ENISA). [1].

Information systems within this Directive are identified as a key element of political, social and economic interaction in the Union itself. Societies are currently very, and in the near future will be even more dependent on the use of these systems. Unhindered use of such systems, as well as their secu-

rity within the member states of the Union, is of vital interest for the development of both internal markets and a modern, innovative and competitive market economy. These types of attacks represent a threat to achieving the goal of a safer information society, and they also represent a threat to the areas of freedom, security and justice. For these reasons, they require a response at the level of the European Union through the improvement of cooperation and coordination at the international level.

The fact is that there are a large number of objects in their physical or software form that represent parts of critical infrastructure, and the interruption of work or the destruction of this type of infrastructure would result in significant damage both directly to the residents of the European Union and to their property. It has become clear that there is a need to define critical infrastructure as an asset, system or part of an asset from a system, which is of essential importance for the maintenance of vital social functions, such as the health, safety, economic or social well-being of the people. Systems such as power plants, transport networks or communication networks in the service of national governments, the disruption or destruction of which would lead to, quite possibly, catastrophic consequences.

There is evidence that indicates a tendency of increasing danger and repetition of attacks on a large scale and strength directed against IT systems, which are of critical importance for the member states of the Union. This tendency was accompanied by the development of sophisticated methods, such as the production and use of the so-called "botnets", which involve several levels of criminal execution, where each of these levels can pose a significant risk to the public interest.

This Directive, among other things, introduces criminal sanctions for a new criminal offense in the form of making and using the so-called "botnets", as an act of establishing remote control over a significant number of computers by infecting them through the installation of malicious software, and through precisely targeted cyber attacks. Once such a network is created, it constitutes a "botnet" that can be activated without the knowledge and consent of the computer user in order to launch an attack on a wide scale and reach, which usually has such a capacity, ie. ability and strength to cause significant harm in the manner described in the Directive.

These types of large and widespread attacks can cause significant economic damage, both through the disruption of information systems and communications and the loss or alteration of commercially important confidential information and data. Special attention should be directed towards raising the awareness of small and medium-sized companies and enterprises in order to identify this type of danger, as well as the vulnerability of those enterprises in this sense, through their growing dependence on the use of information systems. It is also important to emphasize that this Directive prescribes the level of criminal sanctions, i.e. at least for those crimes that are not considered less socially dangerous.

Member States of the Union may prescribe what constitutes less socially dangerous acts in accordance with their national legislation and practice. For example, a criminal offense in this sense can be harming the integrity of computers, computer systems and data to such an extent, and in such a way, that does not exceed a certain threshold of criminal liability that requires the reaction of detection and prosecution authorities within the framework of criminal proceedings. On the other hand, the Directive, especially in the area of attacks against information systems, requires effective, proportionate and sufficiently deterrent criminal-legal sanctions and their level, as well as the improvement of cooperation between judicial and other competent authorities, all of which cannot be achieved only by individual member states, but should be achieved at the level of the European Union itself, for which reasons the Union can implement such types of measures, which are in accordance with the principle of subsidiarity prescribed in Article 5 of the Treaty on European Union.

In its further text, the Directive provides the elements of the criminal offense of unauthorized access to the information system, unauthorized interference with the system, unauthorized interference with data, and the use of means for the execution of these criminal acts.

In particular, it should be emphasized that in Article 9, which refers to the type and level of sanctions, the Directive obliges the member states of the European Union to introduce, within their domestic legislation, such types of criminal sanctions for the specified criminal acts that will be effective, proportionate and sufficiently deterrent in relation to the perpetrators of criminal acts. In this regard, the Directive envisages the obligation to impose a prison sentence with a maximum term of at least 2 years for the above-mentioned criminal acts, and for criminal acts that are not considered less socially dangerous.

Also, for the criminal acts of unauthorized interference with the system and unauthorized interference with data when they were done with intent, they must be punished with a maximum of at least 3 years, when there was significant damage to the information system and their number through the use of tools referred to in Article 7 of the Directive, i.e. devices and programs that are designed or adapted primarily for this purpose. Also, for criminal acts from Articles 4 and 5, the Directive provides that it should be threatened, ie. prescribed maximum penalty of at least 5 years in prison in cases where:

1) are such criminal acts committed by a criminal organization defined through the framework decision 2008/841/JHA, regardless of the punishment prescribed for the organization itself;
2) if the execution of the criminal offense caused serious damage;
3) if the criminal offense was committed against the information system of the critical infrastructure.

In its Article 17, the Directive obliged the European

Commission to submit a report to the European Parliament and the Council by September 4, 2017, within which there will be an assessment of the implementation of this Directive by the member countries, in terms of whether they have taken the necessary measures to comply with the Directive, and if necessary, submission of legislative proposals. The Commission will also take into account technical and legal developments in the field of cybercrime, especially with regard to the scope of this Directive.

The European Union is a key player at the international level when it comes to information security. CIIP, information society and information security are considered key topics. The European Union has launched initiatives and research programs to study various aspects of the information revolution and its impact on education, business, health and communications.

The Communication of the Commission of the European Community (EU Commission) on the protection of critical infrastructure in the fight against terrorism, adopted on October 20, 2004, provides a definition of critical infrastructure (CI), lists identified key sectors and discusses criteria for determining potential CIs. In the following publication of the European Commission, Green Paper on the European Program for CIP on November 17, 2005, CIIP was defined. In 2008, the European Commission launched a political initiative related to CIIP.

Other initiatives and policies include:

1) Research for the Commission on Availability and Robustness of Electronic Communications Infrastructures (ARECI).
2) Information System for Warning of Key Infrastructures (CIWIN).
3) The European System and Information Security Agency (ENISA), created in March 2004, began operating in September 2005 in Crete. The challenge for ENISA is to achieve a high level of electronic communications security at the level of the European Union.
4) TESTA: Trans-European service for communication between administrations. It represents the EU's private network, separated from the Internet, which allows officials from different ministries to communicate in a secure way at the trans-European level.

EU initiatives still under study include:

1) Society of Information Technology (IS) FP6 and FP7,
2) European security research program,
3) Coordination of studies of key infrastructures (CI2RCO),
4) Service and software architecture, infrastructure and engineering.

Relevant EU laws and legislation include:

1) Data Protection Directive 1995,
2) Electronic Signature Directive 1999,
3) Directive for the Protection of Privacy in the Electronic Communications Sector 2002,
4) Framework Directive 2002,
5) Framework decision of the Council on attacks on information systems in 2005,
6) Data Retention Directive 2006.

3. Findings

The speed of technological development has influenced the development of digital forensics as a young scientific discipline, which, together with the parallel development of other sciences, applies new methods that affect the speed and simplicity of collecting solid evidence, investigates anti-forensic activities, with the aim of discovering the truth about the committed illegal act. In response to high-tech crime, there was a need for the development of a new scientific discipline that will deal with it, as well as the regulation of legal bases related to the successful prosecution of criminal offenses in this area.

Digital forensics is the application of investigation methods and analysis techniques in order to find suitable evidence for the court, in high-tech crimes. In order to prove the committed illegal acts and prosecute and sanction their perpetrators, it is necessary to apply the procedures of digital forensics as a scientific discipline with extremely significant practical application.

Digital forensic investigation is a process that, using scientific methods and technology, develops and tests theories through hypotheses, analyzing digital devices, which represent relevant evidence in court proceedings. The goal of such an investigation is to establish the truth about anti-money laundering activity and all the circumstances related to the perpetrator and the way the crime was committed.

In all legal proceedings in which digital evidence is used, it must be obtained or extracted from the suspected machine thanks to forensic tools, according to precisely defined procedures. It is extremely important that the digital evidence, which is presented to the court, must be in the original record, ie. it is prohibited to experiment, modify or test them while the investigation is ongoing. This is precisely why copies of digital evidence are used, which can be used for investigative procedures by a digital forensic scientist and which are not brought before the court authorities.

What is certainly the most important in detecting and proving crimes in the field of high-tech crime is digital evidence. In the case of high-tech crime, evidence is often information stored electronically in computers, sometimes thousands of kilometers away, and they can be copied, deleted and changed in a few fractions of a second, without damaging the originals and leaving no material traces.

The application of operational-tactical actions and measures of investigative actions, which include going to the scene and securing it, conducting investigations, collecting information, searching, reconstructing and expert witnessing, temporarily confiscating objects, questioning the accused and hearing witnesses, surveillance, monitoring and identification, necessary deprivation of liberty, etc., should be carried out

according to known criminal principles, with mandatory adaptation of the specifics of traces and objects of high-tech crime, taking strict account of procedural provisions, so as not to lead to the question of the relevance of the found traces and objects.

Evidence is what separates a hypothesis from an unsubstantiated claim. He can confirm or refute the hypothesis, so the question of his integrity is of utmost importance, which can be accepted or rejected before the court. That is why 1991 is a very important date for digital forensics as a young scientific discipline. Namely, in Portland (Oregon), that year, a session of the International Association of Computer Scientists IACIS (International Association of Computer Specialists) was held, where it was stated and decided that "digital evidence" is equal to evidence collected in a traditional way, i.e. physical objects.

Under the concept of digital evidence as defined by the IOCE in the field of forensic science, digital evidence is any information in digital form that has probative value and that is either stored or transmitted in such form. Therefore, digital evidence includes computer-stored and generated evidentiary information, digital audio and video signals, digital photography, digital cell phone recording, digital fax machine information, and information from other digital devices. Therefore, digital evidence is any information generated, processed, stored or transmitted in digital form that the court can rely on as authoritative, as well as other possible copies of the original digital information that have probative value and on which the court can rely, in the context of forensic acquisition, analysis and presentation.

The places where digital forensics in practice find potential evidence are the following: log files; configuration files; backup files; file system artifacts; printer spool files; internet cookies; swap/page files; system files; history files; temporary files; Internet bookmarks; Internet Favorites; and hibernation files.

The types of files in which forensic scientists find potential evidence include: password-protected files; hidden files; compressed files; tabular files; database files; calendar files; multimedia files (audio, video, graphic files); directory files; and email files.

In order for the court to recognize digital evidence, there are certain conditions and procedures that must be met: analysis, storage, and reproducibility of the complete investigation procedure, if the court requires it from the digital forensic expert. In all legal proceedings in which digital evidence is used, it must be obtained or extracted from the suspected machine thanks to forensic tools, according to precisely defined procedures. [1].

4. Original Value

Permanent monitoring of novelties in the field of computer systems is necessary, which is also a prerequisite for the valid acquisition of evidence from them. Also, it should be noted that, on the one hand, there is an increase in the number of data protection methods, while on the other hand, it complicates and slows down the work of forensic scientists and requires new advanced knowledge. Digital evidence, as an element of the investigation, is much more vulnerable than physical evidence, so it is easier for a skilled attacker to remove them, and careless and unprofessional conduct of the investigation can also lead to the loss of key data. That is why practice has shown that a digital forensic scientist works as a team with a protection specialist, in order to ensure acceptable protection of computer systems and secure operation of the computer network in business systems.

It should be emphasized that for a digital forensic scientist, the monitoring and development of information technologies is of crucial importance. Sometimes differences in the operating system or version of a program are essential. That is why it is important to have digital forensic experts profiled according to their professional field (operating systems, databases, network systems, as well as profiling according to other ICT systems).

The fantastic development of ICT poses great challenges to digital forensics experts who must have permanent and daily education in order to be one step ahead of perpetrators who carry out illegal activities (those activities that are contrary to regulations) in the digital environment. The speed of technological development has influenced the development of this young scientific discipline, which, together with the parallel development of other sciences, applies new methods that affect the speed and simplicity of collecting solid evidence, investigates anti-forensic activities, with the aim of discovering the truth about the committed illegal act.

Digital forensics has a wide range of applications, from police-judicial and military intelligence activities, civil and banking sectors and insurance companies to companies of various profiles. All these entities must be extremely careful with the data they have, because otherwise immeasurable damage can be caused due to industrial espionage, abuse of ICT systems, but also some other forms of illegal actions.

A physical crime scene investigation uses the laws of nature to find physical evidence, and a digital crime scene investigation uses them to find digital evidence. When it comes to the investigation of the physical scene of the crime, the dominant theory is Locard's law of exchange: When two objects come into interaction (contact), there will be an exchange of matter between them. An example of a hair from a criminal, is very often kept at the physical scene of the crime. When it comes to a digital crime scene, temporary files, RAM memory content recorded on disk and deleted files or their parts may exist due to the influence of the program or Operating System that the suspect used or executed. Therefore, data that enters a digital place leaves traces of digital evidence behind in different places: memory, hard disk, portable memory.

The United States and other countries have established specialized groups to investigate computer crime at the na-

tional level. However, due to the large amount of requests received by these groups, existing resources were exceeded. The next step was the creation and development of regional centers for the processing of digital evidence. However, these regional centers also became overburdened, resulting in the creation and development of digital evidence handling units at local law enforcement agencies. Illustratively, it would be shown as follows: incident situations are responded to by persons with basic skills in collecting and reviewing digital evidence, and it is these persons at the local level who solve most cases. If it is about processing complicated cases, support comes from regional laboratories. In the most demanding cases, national centers are involved. These centers conduct research and also develop tools that can be used at regional and local levels.

It is extremely important that the digital evidence, which is presented to the court, must be in the original record, ie. it is prohibited to experiment, modify or test them while the investigation is ongoing. This is precisely why copies of digital evidence are used, which can be used for investigative procedures by a digital forensic scientist and which are not brought before the court authorities.

In addition to digital evidence, there is also physical evidence that can be collected at the incident site and that can have probative value in the sense that a suspect was present at that site. Such evidence provides confirmation of the connection between a particular device and the suspect who carried out the illegal act.

How important is the forensic response and how sensitive it is, perhaps the most vivid description of the search for digital data was given by Friedman in the following sentences of his book: "All data leaves a trace. The search for data leaves a trace. The deletion of data leaves a trace. The absence of data under certain circumstances can leave the clearest trace of all.".

If we are talking about any type of high-tech crime, answers must be found to the questions that the digital forensic scientist should ask: who committed the illegal act, when it happened and how, why the act was committed, where the incident took place, what was the goal, and it is further up to the prosecution to prove the cause-and-effect relationship between the act and the perpetrator as well as the intention to commit the act (guilt). The answers to these questions will be provided by three types of evidence: temporal evidence (they will help reveal sequences or patterns in temporal events and answer the question "when"), relational evidence (include the elements of illegal activities, their relationship and positions answer the questions "who, what and where") and functional evidence (provide insight into what is possible and what is not by answering the question "how").

In order to gather all relevant information and evidence, whether digital or physical, it is necessary to analyze not only the target computer, but also those from which some illegal activity was initiated. Also, those computers that indirectly participated in the illegal act are analyzed. When all that information and evidence is collected, it is submitted to the competent authorities in the event that there was a threat to state and public security, or to the corporate authorities, if the incident occurred within its framework.

The Republic of Serbia is obliged to adopt and implement a strategy and action plan for the effective resolution of high-tech crime in accordance with the strategic and operational approach to the European Union (EU) regarding high-tech crime. The stated obligation primarily derives from the Negotiating Criteria for Chapter 24 - Justice, Freedom, Security. The European Union stated that the Republic of Serbia ratified the Convention on High-tech Crime (made in Budapest, English Budapest Convention) in 2009 and called on the Republic of Serbia to further harmonize its legislation with Directive 2013/40/EU on attacks on information systems.

The Government of the Republic of Serbia adopted a strategy for the fight against high-tech crime for the period 2019-2023. [8].

The Ministry of Internal Affairs, in accordance with the Law on Ministries [9] is responsible for drafting the aforementioned strategic document in cooperation with other state institutions, i.e. interested parties.

In the plan to support the transformation of the Western Balkans within the Strategy for a credible perspective of enlargement and enhanced cooperation with the countries of the Western Balkans, the need for increased support in capacity building in the field of high-tech crime, including cooperation with the European Group for training and education on high-tech crime and future participation in the European Network and Information Security Agency, is highlighted.

Within the Action Plan for Chapter 24 - Justice, Freedom and Security, where the Ministry of Internal Affairs is responsible for the activities, there are three recommendations with eight defined activities, which the Republic of Serbia should fulfill within the EU accession process, with a focus on improving organizational, personnel and technical capacities, analyzing the current normative and organizational framework and taking actions with the aim of harmonizing with the EU legal acquis in the field of high-tech crime and strengthening cooperation between state bodies and institutions. Bearing in mind that one of the main characteristics of high-tech crime acts is their transnational nature, the process of European integration is expected to increase the expediency of work in high-tech crime cases, in terms of a faster flow of information needed for the detection and prosecution of perpetrators of criminal acts, and a faster response to mutual requests for the provision of international legal assistance, all through strengthening the capacities of the state authorities of the Republic of Serbia, especially the Special Prosecutor's Office for the fight against high-tech crime.

Since 2010, the special prosecutor's office for high-tech crime within the European Union, the Council of Europe and the OSCE and other international organizations has been participating in projects aimed at facilitating international

cooperation, speeding it up and responding in a timely manner when committing high-tech crimes. In addition, the Special Prosecutor for High-Tech Crime has been designated as the contact point of the 24/7 network prescribed by the Budapest Convention. In this way, direct cooperation was established with other contact points from the countries that are signatories to the Convention, with the aim of more efficient handling of cases with a foreign element.

Conflicts of Interest

The authors declare no conflicts of interest.

References

[1] Zdravković Lj., 2015., High-tech crime, Niš, Vocational School for Criminology and Security.

[2] Criminal Procedure Code (Official Gazette of RS, no. 35/2019 and 27/2021.).

[3] Bejatović S., 2008., Criminal procedural law, Belgrade, JP Official Gazette.

[4] Crime related to computer networka http://www.uncjin.org/Documents/congr10/10e.pdf 10. 12. 2021.

[5] Criminal Code (Official Gazette of RS, no. 85/2005, 72/2009 and 35/2019).

[6] Bejatović S. 2012., High-tech crime and criminal law instruments of confrontation, Proceedings - Suppression of crime and European integration with reference to high-tech crime, Laktaši, 18-30.

[7] Benjamin S. Bucland, Fred Schreier, Theodor H. Winkler, Democratic Governance and Cyber Security Challenges, Geneva 2010, 7.

[8] Strategy for the fight against high-tech crime for the period 2019-2023. (Official Gazette of the Republic of Serbia, number 71/2018), Law on the Organization and Competence of State Bodies for the Fight against High-Tech Crime (Official Gazette of the RS, no. 61/05 and 104/09).

[9] By the Law on Ministries ("Official Gazette of RS", no. 44/14, 14/15, 96/15 - other laws and 62/17).