Evaluation of Digital Evidence in Criminal Proceedings in Croatia with a Focus on Preservation Requirements and Role of Standard Operative Procedures

Nina Gumzej*, Nikola Protrka**
* University of Zagreb, Faculty of Law, Zagreb, Croatia
** Police College, Zagreb, Croatia
ngumzej@pravo.hr
nprotrka@fkz.hr

***Abstract* – Collection and analysis of digital evidence in criminal proceedings entails risks, such as the contamination of evidence during seizure and/or search of a computer system and the inability to establish its authenticity, which may affect its admissibility and credibility before the courts. For that purpose the requirement on digital evidence preservation is prescribed in the criminal procedure law, which should apply by default to all relevant actors. Analysis of available court decisions and rules of the Criminal Procedure Act confirms that the claims concerning mishandling and/or manipulation of digital evidence do not affect *ex lege* inadmissibility of such evidence. Such claims would be subject to examination on the credibility (reliability) of evidence before the courts. Any detailed technical procedures and measures to be implemented so as to ensure digital evidence preservation are best suited for regulation by standard operative procedures or perhaps even by sub-legal acts. To that effect, the standard operative procedures discussed in this paper have a proven ability to ensure the common goal of ensuring digital evidence preservation. Adherence to best practices stemming from standardized procedures has shown to be vital for ensuring that investigatory procedures and acquired digital evidence are valid and as such accepted throughout the criminal proceedings.**

Keywords –search of computer system; seizure of computer data; digital evidence; preservation of digital evidence; data preservation; standard operative procedures; computer forensic

I. INTRODUCTION

Digital evidence in criminal proceedings may include any data or information about a criminal offense that is located on a digital device, or which is being transmitted through such a device [1]. In the Croatian Criminal Procedure Act (hereinafter: CPA), digital (electronic) evidence signifies all data that was acquired as evidence in electronic (digital) form under that Act [2]. The collection and analysis of such evidence entails risks that may affect its admissibility and credibility before the courts. Outcomes of some of the most significant risks include the contamination of evidence during the process of seizure and/or search of a computer system [3] (including computer data [4]) and the inability to establish its authenticity. As it will be explained in this paper, not all procedural "flaws" in the process of collection and analysis of digital evidence lead to *ex lege* inadmissibility of such evidence, although it would in most cases need to be evaluated for credibility before the courts. Namely, in its Article 10 the CPA prescribes that court decisions must not be founded on unlawful evidence. Such is *inter alia* unlawful evidence *ex lege*, which is acquired in contravention of criminal procedure rules and as such expressly prescribed by the CPA (e.g. warrantless search of a computer in contravention of the CPA), and "fruit of the poisonous tree", i.e., evidence of which knowledge was gained from unlawful evidence (e.g. minutes on search and the related computer data obtained from the unlawfully seized computer). With certain exceptions [5], unlawful is also evidence acquired in contravention of certain human rights, including the right to privacy.

While depending on the criminal investigation stage different rules may apply, in focus here are the CPA rules on the collection and analysis of digital evidence by search of a computer system, including the seizure and analysis of computer data. After examination of CPA rules in next part of the paper, two decisions from judicial practice will be presented for the purpose of establishing in practice the types of irregularities that have been invoked in criminal proceedings, and the assessment of their ability to affect the legality of digital evidence. Both cases have at their core the concerns on digital evidence preservation, which may be described as "the process of maintaining and safeguarding the integrity and/or original condition of the potential electronic evidence" [6]. The issue of reliability or credibility of possibly corrupted digital evidence before the courts shall not here be examined on account of the currently still very limited availability of final court decisions examining it specifically in regard to analysed CPA rules. The premise of this paper is in any case that many, if not all, claims on irregularities in the collection and analysis of digital evidence should and could be minimized by adhering to proper technical procedures [7], which should be an elaboration of basic statutory data preservation requirements. Acknowledging the fact that the most

prominent role towards achieving above mentioned goal lies in that of practitioners executing criminal investigation and evidentiary actions, analysis in the paper concludes with a recommended basic overview of standard operative procedures (hereinafter: SOPs) that should to that effect be implemented. The arguments toward adopting such procedures for the seizure of computers and other digital carriers within the search authorities, for the purpose of securing formal requirements and use as evidence before the courts have already been provided in domestic literature [8]. On a broader level, the SOPs for the collection, analysis and presentation of digital evidence provide practical, technical and tactical guidance for investigators and specialists in different Law Enforcement Agencies (hereinafter: LEAs), and can be used for various uses on-scene, such as on-site securing of traces, live acquisition, transport and handling. In the later phases they may be used for presentation of collected traces [9].

II. COLLECTING DIGITAL EVIDENCE UNDER THE CPA

Digital evidence is collected by application of Article 257 on search of a movable, and Articles 262 and 263 on the temporary seizure of objects (Article 331), unless that Act prescribes otherwise.

A. Search of a computer and related devices

Under Article 257 of the CPA a search of a movable also includes search of a computer and devices connected with it, of other devices intended for collecting, saving and transferring data, for telephone, computer and other kinds of communication, and of data carriers. The person using a computer or having access to it or another device or data carrier, as well as telecommunications service provider must enable access to it at the search authority's request and provide necessary information for unhindered use and achievement of search goals. Upon order of the search authority they must also immediately take measures to prevent the destruction or modification of data, which measures the search authority may delegate (order) to an expert assistant. In cases of noncompliance without justifiable reasons they may be fined and further punished by imprisonment until compliance, but for no longer than a month. The defendant cannot be punished.

In addition to the here presented Article 257 other CPA general rules on search also apply, such as, *inter alia*, the following. Only documents and objects may be temporarily seized that are related to the search purpose, as well as certain other objects (specified in Article 249, paragraphs 1-2). Furthermore, search minutes must describe in detail the objects and documents seized, which is entered in the receipt. Where during the search objects are found that are unrelated to the criminal offence for which a warrant was issued, but which signalize the commission of another offence that is prosecuted by official duty, said objects must be described in the minutes and temporarily seized. A seizure receipt is issued immediately. On the other hand, where the State Attorney determines no ground for instituting criminal proceedings and there is no other statutory ground for the seizure, the said objects must be returned immediately and minutes thereon drafted. Objects used during the search must be returned to their users after the search unless they are necessary for further conduct of criminal proceedings. Personal data that were acquired by a search may only be used for the purposes of criminal proceedings. Once those purposes are resolved, they must be erased without delay (Articles 248 and 249 of the CPA).

B. Temporary seizure of computer data

The CPA provisions on temporary seizure of objects establish which objects, including computer data (Article 263: data stored in computers and devices connected thereto, as well as in devices used for collecting and transferring data, data carriers, subscription information in the possession of a service provider) may and may not be seized or be withheld, as well as the details on the minutes and receipt of a seized object, the keeping of seized objects and other (Articles 261-270 of the CPA). Key CPA rule in terms of analysis and management of data from digital devices is Article 263, which specifies that rules on temporary seizure (Article 261 of the CPA) also apply to computer data as specified above. This is with the exception of instances where temporary seizure is prohibited under Article 262 of the CPA. Such data must be handed over to the State Attorney at his or her written request, in an integral, original, legible and understandable form. Time limit for the handing over of data must be specified in the State Attorney's request. Where a person refuses to hand over the data, he or she may be fined and further punished by imprisonment until compliance, but for no longer than a month. The defendant and persons exempted from the duty to testify cannot be punished.

Article 263 further specifies that the authority taking the action records the data in real time, and that confidentiality and data protection rules must be observed in data acquiring, recording, preservation and storing (Articles 186, 187 and 188 of the CPA). Data unrelated to the criminal offence that is needed by the person against whom the measure is taken can be recorded on an appropriate medium and returned to him or her also before conclusion of proceedings. The person using the computer and service provider may file an appeal against the order of the judge of investigation imposing the measure, but the appeal does not stay the execution of the order. Finally, and importantly, Article 263 prescribes the possibility for the judge of investigation to order (upon State Attorney's motion) the preservation and storage of all mentioned computer data for as long as necessary, but not more than six months. Following that, the data must be returned, unless: 1) they concern the commission of criminal offences against computer systems, programmes and data (Title XXV of the Criminal Code; 2) they are related to commission of another criminal offence prosecuted by official duty that was committed by means of a computer system; 3) they are intended to be used as evidence of an offence in on-going proceedings.

As observed, the measures specified in Article 263 involve not only the real time recording of computer data, but also their analysis (e.g. to establish whether and if so which data stored in the computer system are relevant for the criminal offense, as well as to establish compliance with data protection rules, e.g. where sensitive data are stored). In connection with this it should be noted that in

2012 the Constitutional Court rejected the complaint in which it was argued that by its contents the measures specified in Article 263 should have been regulated as the so-called special evidentiary actions temporarily restricting constitutional rights (Article 332 of the CPA). Namely, the latter evidentiary actions may include *inter alia* the interception, collection and recording of computer data, and they may only be ordered in strictly regulated cases and other particular safeguards are prescribed on account of their intrusiveness. According to the complaint: "Art. 263 of the CPA introduced in fact covert acquisition of evidence without any control by the judiciary because the exclusion of data stored in computers and related devices used for data collection and transmission, data carriers and subscriber information available to the service provider, does not presuppose only the exclusion of information but also presupposes a special evidentiary action of their analysis, comparison and, in a practical way, in fact expertise". The Ministry of Justice responded to the claim, stating that this measure does not represent covert collection of evidence, and in particular that such collection of evidence is not conducted without judicial control. Basis for such taking of action is a court order, issued on the basis written request by the State's Attorney. The Court established that the temporary seizure of media for the recording of data (CD, DVD, hard disk) is regulated by rules on temporary seizure of objects, because the legislator cannot beforehand classify such media according to types of data. It also held that Article 263 contains adequate procedural guarantees stipulated in paragraphs 1 and 3, which prescribe the way of recording collected data and the secrecy thereof. The judge of investigation issues an order on that, and an appeal against that order is decided by the panel [10].

Related claims in criminal proceedings on the allegedly wrong basis for the taking of evidentiary actions of seizure and search of a computer (and/or server, etc.) and of the subsequent recording and analysis of computer data are not rare in domestic judicial practice, as a result of which disputed evidence may be asserted as obtained both in violation of the CPA and of defendants' privacy rights. In one such unsuccessful claim, for example, the Supreme Court held that since the computer data were already stored in the computer and on the server, their surveillance and interception as envisaged by the special evidentiary actions noted above, did not take place. Hence according to the Court both search of the computer and of the server, and the recording of computer data from the searched computer and server to a hard disk were executed in line with the CPA search and seizure rules applicable to movables (computer, server) and computer data, i.e., Articles 257, 261 and 263 [11].

C. Assessment

CPA rules on search of a movable such as a computer, server, USB stick or mobile phone show that the taking of immediate measures aimed at preventing data destruction or modification are not prescribed as a default statutory obligation, but depend on the order issued to that effect by the authorities conducting the search. Whether such measures are to be carried out by expert assistants or not is left to the discretion of search authorities, which issue is in practical terms also connected with the availability and adequate number of such assistants (Article 257, paragraph 2 of the CPA). Furthermore, the taking of mentioned immediate measures in the search of mentioned movables is not currently prescribed as a clear statutory duty applicable to search authorities themselves. While in case of non-adherence to the issued preservation order the persons using the computer (*inter alia*) may be punished (except for the defendant), the CPA does not envisage that evidence obtained without and/or in contravention of appropriate preservation measures would amount to unlawful evidence *ex lege*. This is supported by the case law, which will be examined in next section of the paper. As to the regulation of the more specific details concerning the requirement of preserving digital evidence in criminal proceedings, analysis confirms that beyond examined CPA rules there are no specific requirements for the processing and preserving of digital evidence [12].

III. EXAMPLES OF CLAIMS INVOKED IN RESPECT OF PRESERVATION REQUIREMENT

In 2019 the Supreme Court upheld the lower court's decision denying the defendant's request to exclude from files as evidence minutes on search of a laptop together with related evidence. The defendant argued that the police did not take measures to prevent the destruction or modification of data in her computer, which was seized and searched a while after the defendant was arrested, and implied that the data may have been manipulated with when the computer was out of her reach. While the Court held that such claims were not supported by proper arguments, it also found that they would not as such affect the legality of conducted search and of minutes of that search. Namely, the CPA does not explicitly prescribe that acting contrary to Article 257, paragraph 2 of the CPA would render the search or evidence obtained by the search illegal. Consequently, defendant's claims on possible manipulation of acquired digital evidence could only be examined from the point of view of reliability (credibility) in the next phase of proceedings [13].

The next Supreme Court decision is also presented with the purpose of providing an example of defendants' objections and claims that may arise in connection with the seemingly improper conduct of search of a computer system. While we were not able to obtain access to more detailed case information, i.e., the first and second instance judgments, this decision whereby the applicant's request for extraordinary review of final judgment was denied is in our opinion still helpful in describing the problematic aspects of a conducted search. It also confirms that the claims relating to "unprofessional" conduct during the search of a computer system typically would not lead to *ex lege* inadmissibility of thus obtained evidence, but can and should be examined before the courts on account of their credibility. Namely, here the applicant (accused) disputed the legality of a laptop search, claiming that the laptop was both subject of the search and the means for the otherwise illegal search of the SD card, since the contents of that card were examined on the subject laptop. The applicant also argued that the laptop search was performed "extremely unprofessionally", since allegedly no backup was performed prior to opening the files in the computer. In

consequence, it was no longer possible, during expert examination, to determine if files were opened at a specific time period. According to the applicant, memory cards were inspected on his laptop instead of on another computer. That made it possible to transfer files from memory cards to the computer and vice versa. After that, due to suspicion of contamination the accused alleged that both the computer and memory cards could not be credible evidence. In its decision the Court held, as follows: "The fact that on the same occasion, when the computer was searched, the SD memory card was searched on the same computer, for the search of which no warrant of the investigating judge was issued, so that part of the search record was separated as unlawful (by first and second instance court decisions), does not make the computer search illegal. These are two searches that each form a separate unit, and the fact that one protocol (minutes) was made of both did not result in a different qualification of these actions as separate evidence. […] illegality of the search of the SD memory card led to the exclusion of the part of search minutes related to search of that card. *The question, however, whether and to what extent the search of the SD memory card for which no warrant was issued by the investigating judge, could "contaminate" with its content the computer for which the warrant existed, is possibly an objection to the credibility of evidence, i.e., minutes of the computer search, which is essentially a question of fact, and on what grounds the filing of this extraordinary remedy is not permitted. Of the same meaning is the "unprofessional" way of conducting a computer search, which is explained in detail by the accused, i.e., the consequent inability to determine the earlier dates of access to individual files*. The first-instance and second-instance courts commented on these allegations of the accused, which actually warn of certain shortcomings and shortcomings of the probative value of conducted search, after an expert examination was conducted, during which all disputable issues were clarified, since that is also a matter of objection on credibility of evidence, and not its lawfulness." (emphasis added by authors) [14].

IV. STANDARD OPERATING PROCEDURES

LEAs use different tools and practices for the same or similar data acquisitions, which represent a vital part of their activities and include *inter alia* the obtaining or copying files from the computer system and/or storage media. The standardized operative procedures (SOPs) that apply in the Republic of Croatia and are recommended by the Cybercrime Program Office of the Council of Europe (hereinafter: C-PROC SOPs) have the purpose of providing a common standard for investigators in the seizure, securing, transportation and other handling of digital evidence. They relate both to procedural phases of analyzing acquired evidence and to the presentation of evidence during the trial [9]. Furthermore, of particular relevance for this area are the most recent European Network and Information Security Agency's (ENISA) guidelines and best practices from its report for Law Enforcement Agencies and Computer Security Incident Response Teams [15], as well as trainings provided by the European Cybercrime Centre (EC3). With its involvement in high-profile investigations and on-the-spot operational support, the EC3 represents one of the most important bodies related to digital forensics that also issues the acclaimed annual main strategic reports (Internet Organised Crime Threat Assessment - IOCTA) [16].

All of the here mentioned sources have been taken into account for the purpose of ensuing presentation and analysis of procedures to be taken when collecting and analysing digital evidence in criminal proceedings. However, in view of the limited scope of this paper emphasis will be provided to those procedures that we consider most relevant in relation to claimed irregularities, as discussed in two court decisions from the previous section of this paper. If applied properly, such procedures certainly do minimize the risks of manipulation and mishandling of digital evidence in criminal proceedings.

It is highly important that the investigators find out or at least estimate the kind of hardware or software they would use during the investigation and prepare adequate equipment for the handling of digital evidence. Furthermore, all stages of the forensic analysis process itself, and all used hardware and software should be documented. When documenting the software, it is desirable to note also the version of the software, so that the evidence discovered can be more easily presented in the future during the court proceedings.

The first case law example presented in the previous section of this paper has shown that the laptop was confiscated the day before the forensic analysis was performed [13]. While there is no dispute in the fact that the forensic analysis was performed a day later, without access to the case files it is not possible to determine if forensic analysis was performed on the seized computer, or in line with the C-PROC SOPs' recommendations, according to which a forensic backup of the computer is to be made and then the forensic analysis performed on that storage media. The advantage of using a forensic image instead of live acquisition on a seized computer is that the seized data remains in its original condition as found during the search or seizure, and that the investigators can later analyse the data on backups without fear of damaging the original evidence.

Namely, ensuring the integrity and authenticity of computer data, i.e., digital traces, is one of the most important principles to follow throughout the criminal investigation and proceedings. In recent years, digital signature has become a well-known tool serving to achieve this principle, with the MD5/SHA-1 hash algorithms mostly used by LEAs. They provide the means to ensure that the signed data remain exactly the same, since the checksum must be the same at the time of gathering of the data and at the time of presenting them. Most of the forensic investigation software automatically signs all examined data with one of the two mentioned algorithms. Integrity of each file needs to be verified using above-mentioned hash values, with which the investigators can guarantee that the seized data were untouched and that they can be presented before the court in their original state [17]. It is possible for the computer forensic investigators to use any digital trace processing software, but that software also needs to be documented.

Where cost is an issue, the use of effective open source forensic tools is not uncommon in LEAs' practice [18].

During seizure of the computer or any other electronic device, investigators should seal that device and ensure its safekeeping without the possibility of changing any computer data. The SOPs stipulate that during the investigation everything must be documented and even photographed during the seizure (e.g. sometimes, by looking at photos from the crime scene, investigators may find written passwords on post-it papers for logging into computer systems or open disputed files) [19].

In respect to the claims on unprofessional computer search and contamination of searched computer in the second presented case [14], the SOPs appear not to have been followed. Namely, forensic analysis was done for the computer and the storage media, i.e., the SD memory card. SOPs would require that two independent backups are performed, one for the computer and the other for the memory card. It also appears that the crucial flaw consisted in the use of the seized computer as search equipment in live forensic acquisition for the seized memory card, since the internal disk in the computer and the memory card could in this way be contaminated.

One of the most important recommendations in the SOPs is that the confiscated equipment (computer, mobile phone, etc.) is not turned on (if it is turned off) due to the possibility of contamination or even deletion of all data. Only forensic backup or cloned image of the data should be made. While without access to detailed case documentation it is not possible to comment on the circumstances of connection to a computer network or the Internet in the discussed case, we may note that this would normally also constitute a possible danger when performing a forensic analysis with the original device and that exactly for this reason creating a backup image (cloned data) of all seized storage media and their subsequent analysis is the best applicable practice.

In the SOPs there is also a recommendation for performing live data acquisitions on crime scenes in certain cases, but it is always recommended that whenever possible the computer is disconnected from the power supply by unplugging the power cord from the socket, or by removing the battery from the laptop.

When seizing any electronic device or storage media it is extremely important to mark it with at least basic information, such as: brief description, model, serial number, memory capacity, location where data or digital device is identified, date and time of seizure, and name and surname of the owner/user. All computer equipment must be seized in its original state, in which it makes up the computer system. It can include *inter alia* the attached monitor, keyboard and memory card readers. Namely, practice has shown that memory cards or other media storage devices such as USB memory keys can be found attached on peripheral equipment, where the disputed data may also be located.

Depending on the type of digital device, forensic image backups are divided into three groups: 1. *logical backup* (user-created data, images, audio-video materials, documents, etc.); 2. *file system backup* (all data from the logical section noted above and data created by installed applications), and 3. *physical backup* (complete image of all files, as well as unused memory space). The type of backup is determined by the investigator in accordance with the task and purpose of data analysis [20]. Certain software is available exclusively to LEAs for the purpose of providing digital forensic analysis.

The backup rules also apply to any media that can contain any data for forensic analysis, such as *inter alia* mobile phones, tablets, GPS devices, as well as smart-watches and drones. In that respect, it should here also be noted that more and more devices falling into the category of Internet of Things (IoT) have their own internal memory or memory card slot, and are connected to a computer network or the Internet, or communicate via a Bluetooth network. As such, they present entirely new challenges both for the legal acquisition of data and for the seizure and examination of potential digital evidence [21].

V. CONCLUSION

Judicial decisions in respect of the types of claims examined in this paper confirm that the non-compliance with the measures aiming at preventing data modification and destruction during search of a computer system and seizure of computer data are not as such grounds for *ex lege* illegality of acquired digital evidence, and that such claims are to be assessed before the courts for credibility of evidence, normally following expert examination. Until available case law piles up, it is in our opinion particularly important to take note of claims invoked in criminal proceedings such as those examined in the paper. By all means, the ever-growing production of digital evidence and increasing reliance on it in criminal proceedings requires the availability of evolving case law for the purposes of necessary legal research into this still underrepresented area. Our analysis has also shown that the domestic legal system contains specific rules on search of computer systems and the seizure of computer data, which include the requirement on the taking of measures to prevent data destruction and/or modification. While inclusion of the latter requirement in the CPA is commendable, on account of importance of digital evidence preservation in criminal proceedings it is necessary to clearly apply, and by default, to all actors involved, including search authorities themselves. To that effect, a comparative analysis of implemented legal solutions for the purpose of digital evidence preservation, as already adopted in some of the other EU Member States, would be beneficial [22]. Findings from this paper may serve as a starting point for any such further comparative research into relevant legislation and practice, leading *inter alia* to examination of the impact that the different national solutions on digital evidence preservation might have in investigations and prosecutions in cross-border cases [6], [23].

Any detailed technical procedures and measures to be implemented so as to ensure the preservation of digital evidence (e.g. during the seizure and search of computers and digital storage media, as well as the extraction and analysis of digital evidence) are in our opinion best suited for regulation by standard operative procedures or perhaps even by sub-legal acts. This is on account of their

significantly easier adaptability to the changing technical requirements [24]. To that effect, the standard operative procedures discussed in this paper have a proven ability to ensure the common goal of ensuring the preservation, i.e., authenticity and credibility of secured digital evidence. Adherence to best practices stemming from such standardized procedures has shown to be vital for ensuring that investigatory procedures and acquired digital evidence are valid and as such accepted throughout the criminal proceedings. Training is also very important, as well as availability of any relevant literature.

REFERENCES

[1] N. Protrka, "International Cooperation and Security in Combating Crime in Cyberspace" (Međunarodna suradnja i sigurnost u suzbijanju kriminaliteta u kibernetičkom prostoru), doctoral dissertation, Zadar, 2018, available at: https://urn.nsk.hr/urn:nbn:hr:162:834428 [acessesed 30.6.2021].

[2] Article 202, paragraph 2, item 33 of the CPA, Official Gazette no. 152/08, 76/09, 80/11, 121/11, 91/12, 143/12, 56/13, 145/13, 152/14, 70/17, 126/19 and 126/19.

[3] Article 87, point 18 of the Criminal Code, Official Gazette no. 125/11, 144/12, 56/15, 61/15, 101/17, 118/18 and 126/19 (definition of a computer system).

[4] Article 87, point 19 of the Criminal Code (definition of computer data).

[5] Article 10, paragraph 4 in connection with Article 10, paragraph 3 and Article 10, paragraph 2, item 2 of the CPA; Article 21 of the Act on the Office for the Supression of Corruption and Organized Crime, Official Gazette no. 76/09, 116/10, 145/10, 57/11, 136/12, 148/13 and 70/17.

[6] J. P. Mifsud Bonnici, M. Tudorica and J. A. Cannataci, "The European legal framework on electronic evidence: complex and in need of reform," in Handling and exchanging electronic evidence across Europe. Law, Governance and Technology Series, vol. 39, M. A. Biasiotti, J. P. Mifsud Bonnici, J. Cannataci and F. Turchi, Eds. Springer, 2018, pp. 189-234 at p. 191.

[7] B. Custers and L. Stevens, "The use of data as evidence in Dutch criminal courts", 2021, European Journal of Crime, Criminal Law and Criminal Justice, vol. 29, pp. 25-46 at p. 40, available at: https://doi.org/10.1163/15718174-bja10015 [acessesed 30.6.2021].

[8] N. Protrka and K. Filipić, "The role of forensic software EnCase with digital trace," (Uloga forenzičkog softvera EnCase pri radu s elektroničkim tragovima), Criminalistic theory and practice, vol. 3, no. 2, International Criminalistic Association, Zagreb, 2016, pp. 121-134 at pp. 125-127.

[9] Cybercrime Programme Office of the Council of Europe (C-PROC), "Standard operating procedures for the collection, analysis and presentation of electronic evidence", 2019, available at: https://rm.coe.int/3692-sop-electronic-evidence/168097d7cb [acessesed 12.4.2021].

[10] Constitutional Court of the Republic of Croatia, decision no. U-I-448/2009, 19.7.2012, points 222-225.1.

[11] Supreme Court of the Republic of Croatia, decision no. I Kž-Us 3/17.-4, 26.1.2017.

[12] EVIDENCE - European Informatics Data Exchange Framework for Courts and Evidence, Deliverable D3.1, "Overview of existing legal framework in the EU Member States," 30.10.2015, available at: http://s.evidenceproject.eu/p/e/v/evidence-ga-608185-d3-1-411.pdf, p. 95 [acessesed 12.4.2021]; D. Škrtić, "Remote control and search computers as special evidence collection procedure," (Daljinski nadzor i pretraga računala kao posebna dokazna radnja) Zbornik prispevkov 15. Slovenski dnevi varstvoslovja, B. Flander, I. Areh and M. Modic, Eds. Ljubljana: Fakulteta za varnostne vede, 2014, pp. 1-12 at p. 10.

[13] Supreme Court of the Republic of Croatia, decision no. Kžm 25/2019-4, 05.9.2019.

[14] Supreme Court of the Republic of Croatia, judgment no. III Kr 165/11-5, 19.9.2012.

[15] European Network and Information Security Agency (ENISA), European Union Agency for Cybersecurity, "Electronic evidence - a basic guide for First Responders," 2015, available at: https://www.enisa.europa.eu/publications/electronic-evidence-a-basic-guide-for-first-responders [acessesed 12.4.2021].

[16] European Cybercrime Centre (EC3), "Internet Organised Crime Threat Assessment (IOCTA)", Europol, 2020, available at: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment [acessesed 12. 4.2021].

[17] A. Arnes, Digital Forensic, Wiley, 2018, p. 147.

[18] C. Altheide and H. Carvey, Digital Forensics with Open Source Tools, Elsevier Inc., 2011, p. 47.

[19] UKEssays, "Digital forensics and incident response standard operating procedure (SOP)," 2018, available at: https://www.ukessays.com/essays/information-technology/digital-forensics-and-incident-response-standard-operating-procedure-sop.php?vref=1 [accessed 12.4.2021].

[20] K. Grun, A. Altenpohl, O. Radchuk, J. Winkler and J. Nachbaur, "From mobile phones to court – a complete FORensic investigation chain targeting MOBILE devices," 2020, available at: https://www.enisa.europa.eu/publications/csirts-le-cooperation [acessesed 12.4.2021].

[21] Z. A. Baig et al, Future challenges for smart cities: cyber-security and digital forensics, Digital Investigation, vol. 22, Elsevier Inc., 2017, pp. 1-11.

[22] Articles 247(1bis); 254(bis) and 354(2) of the Italian Criminal Procedure Law (Codice di procedura penale), available in Italian at: https://www.altalex.com/documents/codici-altalex/2014/10/30/codice-di-procedura-penale; Council of Europe, Country Wiki Italy: Cybercrime legislation, 1.5.2020, available at: https://rm.coe.int/octocom-legal-profile-italy/16809e59c9 [acessesed 30.6.2021].

[23] Ž. Karas, "The Role of National Systems in the Admissibility of EPPO Evidence with an Emphasis on Croatia," Croatian Annual of Criminal Sciences and Practice, vol. 27, 2020, pp. 359-386.

[24] iPROCEEDS Project on targeting crime proceeds on the Internet in south-eastern Europe and Turkey, "Assessment report on obtaining and using electronic evidence in criminal proceedings under domestic legislation in south-eastern Europe and Turkey," 5.3.2018, available at: https://rm.coe.int/3156-52-iproceeds-electronic-evidence-report-eng/16807bdfdf, p. 42 [acessesed 30.6.2021].