iPROCEEDS

Project on targeting crime proceeds on the Internet in South-eastern Europe and Turkey

Version 5 March 2018

Assessment report

on obtaining and using electronic evidence in criminal proceedings under domestic legislation in South-eastern Europe and Turkey

Funded by the European Union and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Implemented by the Council of Europe

Content

1. Introduction

Complete and effective legislation that meets human rights and rule of law requirements is the basis for criminal justice measures on cybercrime and the use of electronic evidence in criminal proceedings. This is particularly true for specific procedural law powers available under the Budapest Convention, as a comprehensive domestic criminal law framework for such powers it also facilitates international cooperation on cybercrime and electronic evidence with other Parties to the Convention. Clear notions of electronic evidence, categories of data and precise limits and conditions for procedural powers are essential in this regard. Thus, the adoption of complete and effective legislation on cybercrime and electronic evidence that meets human rights and rule of law requirements is considered a strategic priority.

The Council of Europe carried out an initial assessment of the national regulatory framework for obtaining and using electronic evidence in criminal proceedings in Albania, Bosnia and Herzegovina, Montenegro, Serbia, "the former Yugoslav Republic of Macedonia", Turkey and Kosovo*[1] based on a Questionnaire filled in by the national project team members. The results of the Questionnaire and the discussions during the regional workshop on obtaining and using electronic evidence held on 2-3 November 2017 in Bucharest, Romania served as the basis for this assessment report, which along with its corresponding recommendations will allow the national criminal justice authorities to further improve relevant national frameworks and develop guidelines for obtaining and using electronic evidence in criminal proceedings.

Under Result 3 of the iPROCEEDS project - *Cybercrime units, financial investigators and financial intelligence units cooperate with each other at the domestic level in the search, seizure and confiscation of online crime proceeds* – the project will assist the criminal justice authorities in improving the relevant national regulatory framework for obtaining and using electronic evidence in criminal proceedings through an assessment of the national framework, identification of gaps as well as putting forward corresponding recommendations.
This was carried out in three phases:

- Development of a Questionnaire on obtaining and using electronic evidence in criminal proceedings under the respective domestic legislation of the project countries/areas. The replies to the Questionnaire were completed by the national project team members, this process has been coordinated by the project staff;
- A regional workshop on obtaining and using electronic evidence in criminal proceedings was held in Bucharest from 2 to 3 November 2017, to discuss the preliminary findings, following the analysis of the replies to the Questionnaire and presentation of applicable notions of electronic evidence, relevant admissibility requirements and the processing of electronic evidence in the context of criminal investigations and proceedings, in line with the provisions and practice of the Budapest Convention on Cybercrime;
- This report assesses respective domestic legislation and regulations on obtaining and using electronic evidence in criminal proceedings, and includes corresponding recommendations that will allow the national criminal justice authorities to further improve the national framework and develop guidelines for obtaining and using electronic evidence in criminal proceedings. The information in this report is sourced from national legislation, responses to the Questionnaire, the outputs of the regional workshop held in Bucharest and further research.

[1] *This designation is without prejudice to positions on status, and is in line with UNSC 1244 and the ICJ Opinion on the Kosovo Declaration of Independence.

2. National Reports

2.1. Albania

Responses to the Questionnaire were provided by a prosecutor, a digital forensics expert and cybercrime investigator from the Albanian National Police, and a lawyer from the Albanian Bar Association.

Legal changes were made after the ratification of the Budapest Convention to state that electronic evidence is admissible in criminal cases.[2] Admissibility is generally decided based on the standards in the Criminal Procedure Code for the admission of any type of evidence. This approach can present legal and practical problems such as challenges to the reliability of the electronic evidence and its procurement via undercover operations or from other countries as well as the slowness of obtaining data from outside Albania.[3]

A judge authorises the search of computers or networks, specifying the right to access, search and obtain data and barring any further action that affects the integrity of the data or system. The search and seizure must follow this order exactly. A judge, prosecutor, or judicial police official may authorise forensic examinations of computers, imaging of data, and live acquisitions. Investigators are not required to seize physical objects to obtain data, but Albanian delegates reported that it is difficult to enforce seizures of data without the seizure of a physical object.[4] When no physical object is seized, investigators use live data acquisition (if the data is located abroad, Mutual Legal Assistance is used).[5]

There are no national guidelines for seizure of electronic evidence, so investigators within the Digital Forensic Unit follow internal standards. In its presentation at the regional workshop in Bucharest, Albania identified the lack of written standards for accessing electronic evidence and for investigative actions as problems, as well as the limited technical capacity of Internet Service Providers, law enforcement agencies, and the forensic institute.[6]

Investigators will search for assets held in electronic form in organised crime or financial crime cases. Such assets are seizable to the same extent as other electronic data.[7]
Following the court's issuance of the search order, the prosecutor may direct the search or can delegate the assignment to judicial police officers. The search and seizure may be kept confidential. Regardless of which office conducts the search, measures must be taken to ensure the integrity of the data.[8] Though there are no explicit rules in the Criminal Procedure Code covering chain of custody, general procedural standards are applied to guarantee the protection of the evidence. Thus, the prosecution or the judicial police officer delegated by the prosecution to conduct the search must take measures to prohibit access to the data or to remove the data from accessible computers. After seizure, the data is sent to the Computer Forensic Unit, which

[2] Questionnaire response (questions 1a and b); Presentation of the Albanians delegates during the regional workshop in Bucharest. All references to articles in this section are to the Criminal Procedure Code.
[3] Questionnaire response (questions 2 and 4); in addition, to preserve potential admissibility, the government must take measures to prevent access to electronic data pursuant to court orders; question 1c; Presentation of the Albanians delegates during the workshop in Bucharest.
[4] Questionnaire response (Questions 5-9, 34); Article 208a, Seizure of computer data (Presentation of the Albanians delegates during the workshop in Bucharest).
[5] Questionnaire response (questions 10, 12).
[6] Questionnaire response (question 13); Presentation of the Albanians delegates during the regional workshop in Bucharest.
[7] Questionnaire response (questions 37 and 39).
[8] Questionnaire response (questions 15 and 19).

performs the imaging and examination and provides a report. An expert may have up to 60 days for a complex examination. This period may be extended by 30 days at a time, but six months is the maximum permitted.[9] Outside experts may be used if necessary.[10] Thereafter, the evidence is stored by the prosecution and may be kept indefinitely.[11]

The defendant or a representative may be present during the search, imaging, and forensic examination. Having the defence present for the latter two processes may present obvious practical difficulties.[12] The defence is entitled to receive an electronic copy of the evidence and any defence forensic examination is done on the copy.[13] Various defence objections to electronic evidence, such as chain of custody defects or allegations that the defendant was the victim of hacking (presumably to place data on his/her computer) or did not own or use the data were raised.[14]

If electronic data is offered as evidence at trial and challenged by the defence, the prosecutor must prove the integrity of the data by calling judicial police officers and experts to testify about every procedure employed from the moment of the data's seizure to its presentation in court.[15] Article 152 of the CPC requires that the accuracy and authenticity of the evidence be established.[16] The reporting expert may be required to testify by the judge, prosecutor, or defence, particularly to explain the forensic report and answer questions related to the case. The expert may be held criminally responsible for misconduct.[17]

Equipment, data, and assets held in electronic form are returned to the owner (including a defendant) at the end of the case if there is no continuing need for them and if they were not instrumentalities of the crime or are per se illegal.[18]

It is possible to obtain data from third parties; there are specific legal bases in the CPC for doing so (Articles 191/a, 208/a, 299/a, and 299/b). In particular, Article 191/a provides for criminal proceedings regarding criminal offences in the information technology field, stating that "The Court upon request of the prosecutor or the plaintiff, shall order the holder or the controller to submit the electronic data stored in the computer or in any other storage device".

If necessary, investigators may also seize the data with the support of a court-appointed expert. Third parties may cooperate voluntarily with the prosecution and turn over data based on Articles 198 and 201 of the CPC. The matter may be kept confidential. Standard rules of digital hygiene are applied in these cases.[19] Evidence may be obtained from other countries via Mutual Legal Assistance.[20] Evidence from abroad is admissible only when obtained by formal Mutual Legal Assistance, reportedly there were cases in which foreign-procured evidence was not admitted because it had been procured informally.[21]
Albania has experience with the use of electronic evidence in court, but there are problems with its use. These include outdated hardware and software (experts may bring their own equipment or software, however). Only a few judges have even superficial knowledge of electronic forensic

[9] Questionnaire response (questions 14, 18 and 17).
[10] Discussion during the regional workshop in Bucharest.
[11] Questionnaire response (questions 1c and 14).
[12] Questionnaire response (questions 23-25).
[13] Questionnaire response (question 22).
[14] Questionnaire response (questions 22, 26, and 29).
[15] Questionnaire response (question 21).
[16] Questionnaire response (question 18).
[17] Questionnaire response (questions 20, 35, and 36).
[18] Questionnaire response (questions 27, 28, and 38).
[19] Questionnaire response (questions 40-42).
[20] Questionnaire response (question 16).
[21] Questionnaire response (questions 43 and 44).

analysis; in addition, proponents of evidence may encounter unreasonably short deadlines, lack of understanding of the forensic reports, or requirements to print out data, including to print out all the data when only a small portion is relevant.[22] Substitutes, such as expert examination reports and examinations of places and items, may be used in place of digital evidence.[23]

In the discussions at the regional workshop in Bucharest, and in response to Question 45, Albania made several recommendations:

- A definition of electronic evidence into the CPC would be welcomed.
- Regulations that establish standard operating procedures (SOPs) for handling of electronic evidence should be drafted. Changes in regulations are easier to be done than in the CPC.
- Clarifications in some form or regulations would encourage courts and prosecutors to prepare clearer, specific orders for searches (in the case of judges) and examinations (prosecutors).
- Legal amendments and definitions are needed to cover seizure, preservation, handling and managing data.
- Additional regulations are needed to cover such matters as undercover operations or identity theft cases.
- Legal changes are needed to gather user ISP data pursuant to a prosecutor order rather than a court order.
- Other legal changes are needed to cover undercover cybercrime operations, international cooperation on cybercrime, and criminal procedure as regards electronic assets (obtaining, administering, and confiscating them). [from the prosecutor and investigators]
- Data handling practices need to be improved and strictly observed – including at seizure, so that no action at that stage alters the data. If an action is necessary, it should be performed only by a trained expert, with meticulous documentation of every action.
- Statutory changes are needed to address obtaining data from the cloud, since much data is stored in clouds and their servers are almost always outside Albanian territory. [from the digital forensics investigators]
- It is necessary to establish the legal basis for the verification of evidence. This should be done live in the computer system by the defence after the government examination process. [from defence counsel]
- Continuous improvements are needed in the knowledge and understanding of technology on the part of police, prosecutors, and judges. Trainings for judges, prosecutors, and police should be continuous, not annual.

[22] Questionnaire response (questions 31-33).
[23] Presentation of the Albanians delegates during the workshop in Bucharest.

2.2. Bosnia and Herzegovina

Responses to the Questionnaire were provided by prosecutors, cybercrime investigators, digital forensics investigators, financial investigators, and defence lawyers from state, entities and district levels.[24]

Electronic evidence is not specifically defined in the legislation. Reference to electronic evidence is to be found in the operational guidance, namely Article 19 of the Rulebook on the manner and conditions of keeping material evidence, which describes the labeling and keeping of devices that contain digital evidence[25]. The Manual "Obtaining Legal Evidence in Criminal Proceedings" defines substantive and indirect evidence, personal and actual evidence, the evidence of the prosecution and the evidence of the defence, lawful and unlawful evidence[26].

According to the criminal procedure laws, the actions aimed at obtaining evidence are[27]:

- Search of dwellings, other premises and personal property
- Search of persons
- Seizure of mail and telegrams and other consignments
- Order issued to a bank or to another legal person
- Order to telecommunication operator
- Seizure of property
- Questioning of the suspect
- Examination of witnesses
- Conducting a crime scene investigation
- Reconstruction of events
- Expert evaluation
- Special investigative actions.

A number of provisions of the Criminal Procedure Code of Bosnia and Herzegovina (CPC of BiH) refer to types of evidence, namely:

- Article 20(n) of the CPC of BiH defines "the terms "writings" and "recordings" as referring to "the contents of letters, words, or numbers, or their equivalent, generated by handwriting, typewriting, printing, photocopying, photographing, magnetic impulse recording, mechanical or electronic recording, or other form of data compilation".
- Article 20(p) of the CPC of BiH defines the term "original" as referring to "an actual writing, recording or similar counterpart intended to have the same effect by a person writing, recording or issuing it. An "original" of a photograph includes the negative or any copy therefrom. If data is stored on a computer or a similar automatic data processing device, any printout or other output readable by sight is considered an "original".

[24] The Questionnaire was filled in: at **State level –** by the Prosecutor's Office of Bosnia and Herzegovina**;** State Investigation and Protection Agency of Bosnia and Herzegovina (SIPA)**;** Agency for Forensic and Expert Examination of Bosnia and Herzegovina**; at Entity level (Federation) –** by the Fedral Prosecutor's Office of the Federation of Bosnia and Herzegovina; Federal Ministry of Internal Affairs of the Federation of Bosnia and Herzegovina**; at Entity level (Republic of Srpska)-** by the Ministry of Internal Affairs of the Republic of Srpska; **Brcko District –** by the Prosecutor's Office of Brčko District of Bosnia and Herzegovina; Police of Brčko District of Bosnia and Herzegovina and Legal Aid Office of Brčko District of Bosnia and Herzegovina.
[25] Questionnaire response of the State Investigation and Protection Agency of Bosnia and Herzegovina (question 1).
[26] Questionnaire response of the Legal Aid Office of Brčko District (question 1).
[27] Chapter VIII of Criminal Procedure Code of Bosnia and Herzegovina (identical articles exist in the Criminal Procedure Code of the Federation of Bosnia and Herzegovina, the Criminal Procedure Code of Republic of Srpska and the Criminal Procedure Code of Brčko District).

- Article 65(6) of the CPC of BiH, related to orders for seizure of objects, states that "the provisions of Paragraph 5 of this Article shall apply to the data stored in devices for automated or electronic data processing. In obtaining such data, special care shall be taken with respect to regulations governing the maintenance of confidentiality of certain data".
- Article 51(2) of the CPC of BiH, related to search of dwellings, other premises and personal property, states that "search of personal property pursuant to Paragraph 1 of this article shall include a search of the computer and similar devices for automated data processing connected with it. At the request of the Court, the person using such devices shall be obligated to allow access to them, to hand over diskettes and magnetic tapes or some other forms of saved data, as well as to provide necessary information concerning the use of the devices. A person, who refuses to do so, although there are no reasons for that referred to in Article 84 of this Code, may be punished under the provision of Article 65 Paragraph 5 of this Code."

Electronic evidence is admissible in the courts in Bosnia and Herzegovina through the interpretation of such evidence in the context of search of movable items and as long as the evidence is collected legally.

A court authorises search of computers or networks. The following articles of the Criminal Procedure Codes were cited:

- Article 53(2) of the CPC of BiH states that a warrant may be issued by the court on the request of the prosecutor or on the request of authorized officials who have been approved by the prosecutor.
- Article 65 of the Criminal Procedure Code of the Federation of Bosnia and Herzegovina (CPC of FBiH) addresses search of dwellings, other premises and personal property:
    - Article 65(1): A search of dwellings and other premises of the suspect, accused or other persons, as well as his personal property outside the dwelling may be conducted only when there are sufficient grounds for suspicion that the perpetrator, the accessory, traces of a criminal offense or objects relevant to the criminal proceedings might be found there.
    - Article 65(2): Search of personal property pursuant to Paragraph (1) of this Article shall include a search of the computer systems, devices for automated and electronic data processing and mobile phone devices. Persons using such devices shall be obligated to allow access to them, to hand over the media with saved data, as well as to provide necessary information concerning the use of the devices. A person, who refuses to do so, may be punished under the provision of Article 79 Paragraph (5) of this code.
    - Search of computers and similar devices described in Paragraph (2) of this Article may be conducted with the assistance of a competent professional.

A court or prosecutor authorises forensic examination of electronic evidence. Article 96(1) of the CPC of BiH states that expert evaluation shall be requested in writing by the prosecutor or court. The request shall indicate the facts in regard of which the evaluation is conducted.

A prosecutor authorises imaging of data in accordance with a court order and also orders live acquisition of data in accordance with a court order (Article 35(2)(f) of the CPC of BiH).

The CPC of BiH allows for the seizing of data without seizing the physical object (computer/drive). In criminal matters, temporary seizure of objects is carried out for use in further criminal procedures. The details of a particular case, the situation in the field and the type of crime will determine whether the physical objects are seized or whether data is seized. It is reported in the questionnaire responses that generally speaking, company servers are not seized because the investigators do not want to obstruct the on-going business of a company and in such cases data

will be seized. PC and other memory devices are usually taken away for later forensic examination. Another questionnaire response answer indicated that it is required to seize physical objects to preserve electronic evidence in its original form. The exception is when the seizure of the physical objects causes more damage than the damage caused by a crime[28].

The questionnaire responses also provide several examples of the legal bases that have been used in practical cases or other practical steps involving seizure of data where no physical objects were seized, and/or for imaging of data onsite, as follows[29]:

- Conducting search of personal property pursuant to Article 51(1) of the CPC of BiH, includes a search of computer systems, devices for automated and electronic data processing and mobile phone devices. Persons using such devices shall be obligated to allow access to them, to hand over the media with saved data, as well as to provide necessary information concerning the use of the devices. A person who refuses to do so may be punished under the provision of Article 65(5) of the CPC of BiH.
- Anyone in possession of such objects must turn them over at the request of the preliminary proceedings judge. A person who refuses to surrender articles may be fined in the amount up to 50.000KM, and may be imprisoned if he persists in his refusal. Imprisonment shall last until the article is surrendered or until the end of the criminal proceedings, but no longer than 90 days. An official or responsible person in a state body or a legal entity shall be dealt with in the same manner (Article 65(6) of the CPC of BiH).
- The provisions in the previous paragraph shall also apply to the data stored in devices for automated or electronic data processing. In obtaining such data, special care shall be taken with respect to regulations governing the maintenance of confidentiality of certain data (Article 65(7) of the CPC of BiH).
- In the case of evidence on the Internet, by Article 92 and 94 of the CPC of BiH, police officers, technicians and experts if necessary seize data recorded on memory devices. The technicians create photo documentation, labelling digital evidence and packing as evidence, as well as creating a report of the criminal investigation for delivery to the court with the evidence.
- Created copies of hard drives, RAID arrays and virtual hard drives.
- Using various software solutions such as FAW (Forensic Acquisition of Websites), HTTrack website copier, PrintScreen or other software for video or photo capture of desktop view.

Several examples of guidelines/instructions for the seizure of electronic evidence were provided:

- Police agencies have instructions for the seizure and preservation of electronic evidence[30].
- Manual on search of computer systems, devices for storing computer and electronic data and mobile phones[31].
- Guidelines for searching computer systems, computer and electronic data storage devices and mobile phones[32].
- Educational model "Cybercrime, money laundering and financial investigations"[33].

---

[28] Questionnaire response of The Prosecutor's Office or Brčko District of Bosnia and Herzegovina, Police of Brčko District of Bosnia and Herzegovina, Legal Aid Offices of Brčko District of Bosnia and Herzegovina (response to question 9).
[29] Questionnaire responses of the Prosecutor's Office of Bosnia and Herzegovina and the State Investigation and Protection Agency of Bosnia and Herzegovina, Agency for Forensic and Expert Examination of Bosnia and Herzegovina (question 10).
[30] Questionnaire response of the Federal Prosecutors office of the Federation of Bosnia and Herzegovina (question 13).
[31] Questionnaire response of the Federal Ministry of Internal Affairs of the Federation of Bosnia and Herzegovina (question 13).
[32] Questionnaire response of the Prosecutor's Office of Brčko District of Bosnia and Herzegovina, Police of Brčko District of Bosnia and Herzegovina, Legal Aid Offices of Brčko District of Bosnia and Herzegovina (question 13).

Having seized electronic evidence, the CPC of BiH describes how that evidence is to be stored, as follows[34]:

- Upon temporary seizure of objects pursuant to a search warrant, an authorised official must draft and sign a receipt indicating the objects seized and the name of the issuing court (Article 63(1) of the CPC of BiH).
- The seized objects and documentation shall be deposited with the Court, or the Court shall otherwise provide for their safe keeping (Article 70 of the CPC of BiH).
- The opening and inspection of the seized objects or documentation shall be done by the prosecutor. The prosecutor shall be bound to notify the person or business enterprise from which the objects were seized, the preliminary proceedings judge and the defence attorney about the opening of the seized objects or documentation. When opening and inspecting the seized objects or documents, attention shall be paid that no unauthorised person gets the insight into their contents (Article 71 of the CPC of BiH).
- Objects that have been seized during the criminal proceedings shall be returned to the owner or possessor once it becomes evident during the proceedings that their retention runs contrary to the Criminal Procedure Code and that there are no reasons for their seizure listed under the provisions of the Criminal Procedure Code (Article 74 of the CPC of BiH).
- There are no time limits for keeping evidence, as long as the evidence is necessary for a criminal investigation.

The requirements for confidentiality of seizure of evidence are also addressed in the Criminal Procedure Code[35]:

- In obtaining data from computer systems, devices for automated and electronic data processing and mobile phone devices, special care shall be taken with respect to regulations governing the maintenance of confidentiality of certain data (Article 65(6) of the CPC of BiH).
- During an investigation, the defence attorney has the right to inspect the files and obtained items that are in favour of the suspect. This right can be denied to the defence attorney if the disclosure of the files and items in question would endanger the purpose of the investigation (Article 47(1) of the CPC of BiH).
- After the indictment is issued the suspect, accused or defence attorney have the right to inspect all files and evidence (Article 47(1) of the CPC of BiH).

Additional confidentiality requirements would also be in place in cases of special investigative actions such as surveillance and technical recording of telecommunications, access to computer systems and computerized data processing, surveillance and technical recording of individuals, means of transport and objects related to them, use of undercover investigators and informants, simulated and controlled purchase of certain objects and simulated bribery, supervised transport and delivery of the objects of a criminal offence[36].

---

[33] Questionnaire response of the Prosecutor's Office of Brčko District of Bosnia and Herzegovina, Police of Brčko District of Bosnia and Herzegovina, Legal Aid Offices of Brčko District of Bosnia and Herzegovina (question 13).
[34] Questionnaire response of The Prosecutors Office of Bosnia and Herzegovina, State Investigation and Protection Agency of Bosnia and Herzegovina, Agency for Forensic and Expert Examination of Bosnia and Herzegovina, Federal Prosecutors Office of the Federation of Bosnia and Herzegovina, Federal Ministry of Internal Affairs of the Federation of Bosnia and Herzegovina, Ministry of Internal Affairs of the Republic of Srpska, The Prosecutors Office of Brčko District of Bosnia and Herzegovina, Police of Brčko District of Bosnia and Herzegovina, Legal Aid Office of Brčko District of Bosnia and Herzegovina (question 14).
[35] Questionnaire response of Prosecutors Office of Bosnia and Herzegovina (question 15).
[36] Questionnaire response of Federal Prosecutors Office of the Federation of Bosnia and Herzegovina (question 15).

The Law on Protection of Classified information also defines the conditions under which the confidentiality of data is determined, as well as the restrictions regarding the handling of classified information[37].

It is possible, under the provisions that regulate international legal assistance to ask another country, international organisation or private party for assistance with a digital forensic examination[38]. Expert assistance can be sought with the order of a court or prosecutor, and Article 51(3) of the CPC of BiH indicates that "A search of computers and similar devices referred to in paragraph 2 of this Article may be undertaken with the assistance of an expert"[39].
There are no time limits for the examination specified in legislation for examination of electronic evidence except inasmuch as there is a general requirement (in accordance with European Court of Human Rights judgments) that criminal proceedings must be completed in a reasonable time. In some cases, deadlines for delivering results of examinations are stated in the court order for examination[40].

The prosecution must maintain oversight of the investigative process to ensure the legality and to request records and receipts for every access to electronic evidence[41], as well as establishing that the electronic search and examination has been property conducted[42]. The following articles of the Criminal Procedure Code were cited[43]:

- The seized objects and documents shall be deposited with the Court, or the Court shall otherwise provide for their safekeeping (Article 70 of CPC of BiH).
- The opening and inspection of the seized objects or documentation shall be done by the Prosecutor. The Prosecutor shall be bound to notify the person or the business enterprise from which the objects were seized, the preliminary proceedings judge and the defence attorney about the opening of the seized objects or documentation. When opening or inspecting the seized objects and documents, attention shall be paid that no unauthorised person gets the insight into their contents (Article 71 of CPC of BiH).
- While conducting search of computer systems, devices for automated and electronic data processing and mobile phone devices, persons using such devices shall be obligated to allow access to them, to hand over the media with saved data, as well as to provide necessary information concerning the use of the devices. Search of computers and similar devices, may be conducted with the assistance of a competent professional. (Articles 51(2) and (3) of CPC of BiH).

---

[37] Questionnaire response of the Federal Ministry of Internal Affairs of the Federation of Bosnia and Herzegovina, the Prosecutors Office of Brčko District of Bosnia and Herzegovina, Police of Brčko District of Bosnia and Herzegovina, Legal Aid Offices of Brčko District of Bosnia and Herzegovina (question 15).
[38] Questionnaire response of the Prosecutors Office of Bosnia and Herzegovina, Agency for Forensic and Expert Examination of Bosnia and Herzegovina, Federal Prosecutors Office of the Federation of Bosnia and Herzegovina, Federal Ministry of Internal Affairs of the Federation of Bosnia and Herzegovina, The Prosecutors Office of Brčko District of Bosnia and Herzegovina, Police of Brčko District of Bosnia and Herzegovina and Legal Aid Offices of Brčko District of Bosnia and Herzegovina (question 16).
[39] Questionnaire response of the Ministry of Internal Affairs of the Republic of Srpska, The Prosecutors Office of Brčko District of Bosnia and Herzegovina, Police of Brčko District of Bosnia and Herzegovina and Legal Aid Offices of Brčko District of Bosnia and Herzegovina (question 16).
[40] Questionnaire response of the Federal Prosecutors Office of the Federation of Bosnia and Herzegovina and the Agency for Forensic and Expert Examination of Bosnia and Herzegovina (question 17).
[41] Questionnaire response of the Federal Prosecutor's Office of the Federation of Bosnia and Herzegovina, the Prosecutor's Office of Brčko District of Bosnia and Herzegovina, Police of Brčko District of Bosnia and Herzegovina and Legal Aid Office of Brčko District of Bosnia and Herzegovina (question 18).
[42] Questionnaire response of the Prosecutor's Office of Bosnia and Herzegovina, the Prosecutor's Office of Brčko District of Bosnia and Herzegovina, Police of Brčko District of Bosnia and Herzegovina and Legal Aid Office of Brčko District of Bosnia and Herzegovina, the Federal Prosecutor's Office of the Federation of Bosnia and Herzegovina (question 19 and 20).
[43] Questionnaire response of the Prosecutor's Office of Bosnia and Herzegovina (question 18).

- The body ordering expert evaluation shall manage the expert evaluation. Before commencement of the presentation of expert testimony the expert shall be invited to carefully study the subject of his testimony, and shall precisely present everything he knows and finds, and shall be invited to present his opinion without bias and in conformity with the rules of his science or art. He shall be specifically warned that presentation of false testimony is a criminal offence (Article 99(1) of CPC of BiH).

To ensure admissibility of electronic evidence, the prosecution must identify the evidence in the indictment and assure the court that the evidence was not obtained through violation of the human rights and freedoms prescribed by the Constitution of Bosnia and Herzegovina, nor in violation of international treaties ratified by Bosnia and Herzegovina, nor through essential violation of the Criminal Procedure Code (Article 10(2) of CPC of BiH)[44]. Additionally, the prosecution may be asked to prove that the data was not altered since the seizure if the defence submits such an objection[45].

The defence may examine a forensic copy of the electronic evidence[46]. According to the Criminal Procedure Code:

- During an investigation, the defence attorney has a right to inspect the files and obtained items that are in favour of the suspect. This right can be denied to the defence attorney if the disclosure of the files and items in question would endanger the purpose of the investigation (Article (47(1) of CPC of BiH).
- After the indictment is issued the suspect, accused or defence attorney has a right to inspect all files and evidence (Article 47(3) of CPC of BiH).
- Upon confirmation of some or all counts in the indictment, preliminary hearing judge shall present the accused and his defence attorney with the indictment, including evidence supporting the charges in the indictment (Article 228(4) of CPC of BiH in relation with Article 227(1)(g) CPC of BiH).

A defendant or a representative may be present during the electronic search[47] and also during the imaging of data[48], but not during the forensic analysis (although the forensic report will be delivered to the defendant and they are allowed to engage an expert to conduct their own analysis)[49].

---

[44] Questionnaire response of the Prosecutor's Office of Bosnia and Herzegovina (question 21).
[45] Questionnaire response of the Prosecutor's Office of Brčko District of Bosnia and Herzegovina, Police of Brčko District of Bosnia and Herzegovina and Legal Aid Office of Brčko District of Bosnia and Herzegovina, the Federal Prosecutor's Office of the Federation of Bosnia and Herzegovina (question 21).
[46] Questionnaire response of the Prosecutor's Office of Bosnia and Herzegovina, State Investigation and Protection Agency of Bosnia and Herzegovina, Federal Prosecutor's Office of the Federation of Bosnia and Herzegovina, Ministry of Internal Affairs of the Republic of Srpska, the Prosecutor's Office of Brčko District of Bosnia and Herzegovina, Police of Brčko District of Bosnia and Herzegovina, Legal Aid Office of Brčko District of Bosnia and Herzegovina (question 22).
[47] Questionnaire response of the Prosecutor's Office of Bosnia and Herzegovina, Agency for Forensic and Expert Examination of Bosnia and Herzegovina, Federal Prosecutor's Office of the Federation of Bosnia and Herzegovina, Ministry of Internal Affairs of the Republic of Srpska, the Prosecutor's Office of Brčko District of Bosnia and Herzegovina, Police of Brčko District of Bosnia and Herzegovina, Legal Aid Office of Brčko District of Bosnia and Herzegovina (question 23).
[48] Questionnaire response of the Prosecutors Office of Bosnia and Herzegovina, Agency for Forensic and Expert Examination of Bosnia and Herzegovina, Federal Prosecutor's Office of the Federation of Bosnia and Herzegovina, Ministry of Internal Affairs of the Republic of Srpska, the Prosecutor's Office of Brčko District of Bosnia and Herzegovina, Police of Brčko District of Bosnia and Herzegovina, Legal Aid Office of Brčko District of Bosnia and Herzegovina (question 24).
[49] Questionnaire response of the Prosecutors Office of Bosnia and Herzegovina, Agency for Forensic and Expert Examination of Bosnia and Herzegovina, Federal Prosecutor's Office of the Federation of Bosnia and Herzegovina, Ministry of Internal Affairs of the Republic of Srpska, the Prosecutors Office of Brčko District of

Objects that have been seized during the criminal proceedings shall be returned to the owner or possessor once it becomes evident during the proceedings that their retention runs contrary to the criminal procedure law and there are no reasons for their seizure listed under the relevant provisions (Article 74 of CPC of BiH)[50]. An exception to this is described in Article 391(1) of the CPC of BiH wherein it states that the items that need to be forfeited under the Criminal Procedure Code shall be forfeited also when the criminal procedure is not completed by a verdict, which declares the accused guilty, if this is required by the interests of general security and morality. A separate ruling shall be issued on this[51]. If the owner is found guilty, the equipment is permanently kept[52].

Objections may be raised against the prosecution's electronic evidence on the following bases[53]:

- Relevance
- Legality of confiscation
- Legality of search
- Authenticity
- Improper handling of confiscated data
- Adding data or similar.

It was reported in the questionnaire that most courts have equipment for presentation of evidence in electronic form and have experience with electronic forensic analysis[54]. Several areas where challenges with the presentation of electronic evidence have been highlighted[55]:

- Courts may order electronic evidence to be printed out and submitted on paper.
- Courts do not have appropriate equipment for presentation of electronic data.
- Insufficient knowledge of this area by judges and prosecutors.
- Illegal/legal obtaining and handling of electronic data.
- Some courts do not recognise certified police officials for cyber and electronic forensics as expert witnesses.
- Problems with deadlines in orders and unclear orders.
- There are not enough experts for forensic analysis.

It is not a legal requirement that electronic evidence is introduced by an expert witness, although in most cases electronic evidence is in practice introduced by an expert[56]. Expert witnesses may be

---

Bosnia and Herzegovina, Police of Brčko District of Bosnia and Herzegovina, Legal Aid Office of Brčko District of Bosnia and Herzegovina (question 25).

[50] Questionnaire response of the Prosecutors Office of Bosnia and Herzegovina, State Investigation and Protection Agency of Bosnia and Herzegovina, Federal Prosecutors Office of the Federation of Bosnia and Herzegovina, Ministry of Internal Affairs of the Republic of Srpska, the Prosecutors Office of Brčko District of Bosnia and Herzegovina, Police of Brčko District of Bosnia and Herzegovina, Legal Aid Office of Brčko District of Bosnia and Herzegovina (question 27).

[51] Questionnaire response of the Prosecutor's Office of Bosnia and Herzegovina (question 28).

[52] Questionnaire response of the Ministry of Internal Affairs of the Republic of Srpska (question 28).

[53] Questionnaire response of the Prosecutor's Office of Bosnia and Herzegovina, the Prosecutors Office of Brčko District of Bosnia and Herzegovina, Police of Brčko District of Bosnia and Herzegovina, Legal Aid Office of Brčko District of Bosnia and Herzegovina (question 29).

[54] Questionnaire response of the Prosecutor's Office of Bosnia and Herzegovina, State Investigation and Protection Agency of Bosnia and Herzegovina, Agency for Forensic and Expert Examination of Bosnia and Herzegovina, Federal Prosecutor's Office of the Federation of Bosnia and Herzegovina, Ministry of Internal Affairs of the Republic of Srpska, the Prosecutor's Office of Brčko District of Bosnia and Herzegovina, Police of Brčko District of Bosnia and Herzegovina, Legal Aid Office of Brčko District of Bosnia and Herzegovina (question 32 and 33).

[55] Questionnaire response of the Prosecutor's Office of Bosnia and Herzegovina, Agency for Forensic and Expert Examination of Bosnia and Herzegovina, the Prosecutors Office of Brčko District of Bosnia and Herzegovina, Police of Brčko District of Bosnia and Herzegovina, Legal Aid Office of Brčko District of Bosnia and Herzegovina (question 31 and 33(a)).

called to introduce or authenticate electronic evidence, even if there is not a legal requirement, in cases where additional explanation is demanded by the court, prosecution or defence, or in cases where the defence raises an objection[57].

In cases involving assets held in electronic form, the legal basis in which these can be introduced in evidence is the same as for any other form of electronic evidence, as described in the Criminal Procedure Code[58], with the same rules regarding the return of copies of electronic evidence to the defendant as were outlined above.

It was reported that it is routine/expected that an examination of electronic evidence would search for assets held in electronic form (*e.g.* virtual currency wallets)[59].

It is possible, in accordance with the Criminal Procedure Code, to obtain electronic evidence from third parties. Specifically[60]:

- The Prosecutor has the right and duty to request information from governmental bodies, companies and physical and legal persons in Bosnia and Herzegovina.
- Objects that are the subject of seizure pursuant to the law or that may be used as evidence in the criminal proceedings shall be seized and their custody shall be secured pursuant to a court decision. The seizure warrant shall be issued by the court on the motion of the prosecutor or on the motion of authorised officials upon the approval of the prosecutor.
- Anyone in possession of such objects must turn them over at the request of the court. A person who refuses to surrender objects may be fined in an amount up to 50,000 KM and may be imprisoned if he persists in his refusal. Imprisonment shall last until the object is surrendered or until the end of the criminal proceedings, but no longer than 90 days.
- An official or responsible person in a governmental body or legal entity shall be dealt with in the same manner.
- This shall also apply to the data stored in a computer or similar devices for automatic or electronic data processing. In obtaining such data, special care shall be taken with respect to regulations governing the maintenance of confidentiality of certain data. A receipt shall be issued for seized objects.
- Forceful measures may not be applied to the suspect or accused or persons who are exempt from the duty to testify.

---

[56] Questionnaire response of the Prosecutors Office of Bosnia and Herzegovina, Agency for Forensic and Expert Examination of Bosnia and Herzegovina, Federal Prosecutors Office of the Federation of Bosnia and Herzegovina, Ministry of Internal Affairs of the Republic of Srpska, The Prosecutors Office of Brčko District of Bosnia and Herzegovina, Police of Brčko District of Bosnia and Herzegovina, Legal Aid Office of Brčko District of Bosnia and Herzegovina (question 35).

[57] Questionnaire response of the Prosecutors Office of Bosnia and Herzegovina, Federal Prosecutors Office of the Federation of Bosnia and Herzegovina, Ministry of Internal Affairs of the Republic of Srpska, The Prosecutors Office of Brčko District of Bosnia and Herzegovina, Police of Brčko District of Bosnia and Herzegovina, Legal Aid Office of Brčko District of Bosnia and Herzegovina (question 36).

[58] Questionnaire response of the Prosecutors Office of Bosnia and Herzegovina, Federal Prosecutors Office of the Federation of Bosnia and Herzegovina, Ministry of Internal Affairs of the Republic of Srpska, The Prosecutors Office of Brčko District of Bosnia and Herzegovina, Police of Brčko District of Bosnia and Herzegovina, Legal Aid Office of Brčko District of Bosnia and Herzegovina (question 37).

[59] Questionnaire response of the Prosecutors Office of Bosnia and Herzegovina, Federal Prosecutors Office of the Federation of Bosnia and Herzegovina, Ministry of Internal Affairs of the Republic of Srpska, The Prosecutors Office of Brčko District of Bosnia and Herzegovina, Police of Brčko District of Bosnia and Herzegovina, Legal Aid Office of Brčko District of Bosnia and Herzegovina (question 39).

[60] Questionnaire response of the Prosecutors Office of Bosnia and Herzegovina, Agency for Forensic and Expert Examination of Bosnia and Herzegovina, Federal Prosecutors Office of the Federation of Bosnia and Herzegovina, Federal Ministry of Internal Affairs of the Federation of Bosnia and Herzegovina, Ministry of Internal Affairs of the Republic of Srpska, The Prosecutors Office of Brčko District of Bosnia and Herzegovina, Police of Brčko District of Bosnia and Herzegovina, Legal Aid Office of Brčko District of Bosnia and Herzegovina (question 40).

All evidence, including evidence from third parties must be obtained with the order of a court. If a third party is willing to cooperate, it is possible for third parties to provide data by cooperation and collaboration rather than through coercive measures[61]. If data is obtained from third parties, or with their assistance, it is possible that they may be required to keep the matter confidential[62]. In cases where a private person reports a crime involving electronic evidence, the same procedures are followed in accordance with the Criminal Procedure Code, for collection of this evidence[63].

In cases involving electronic evidence obtained from another country, the procedure of international legal assistance is applied in such cases and is regulated by the Criminal Procedure Code and by international treaties. Under Article 274(2) and (3) of the CPC of BiH, to prove the content of writing, recording or photograph, the original writing, recording or photograph is required unless otherwise stipulated by the Criminal Procedure Code. A certified copy of the original may be used as evidence or the copy verified as unchanged with respect to the original. The term "original" refers to an actual writing, recording or similar counterpart intended to have the same effect by a person writing, recording or issuing it. An "original" of a photograph includes the negative or any copy therefrom. If data is stored on a computer or a similar automatic data processing device, any printout or other output readable by sight is considered an "original" (Article 20(1)(g) of CPC of BiH)[64].

Several problems, arising from the law (or lack of it), were highlighted in cases involving electronic evidence, namely:

- Problems in the interpretation of the term "original evidence".[65]
- There are two different approaches to electronic evidence, the first approach is that devices that contain digital evidence are collected as evidence on the basis of a court order for search according to Article 51 of the CPC of BiH in the presence of lawyers and suspects, in that procedure a forensic image is created. The forensic images are then analysed on the basis of the prosecutor's order for expert evaluation (Article 96 of the CPC of BiH). The second approach is that devices that contain digital evidence are collected as evidence on the basis of a court order for search (Article 51 of the CPC) and subsequently the prosecutor makes the order for expert analysis (Article 96 of the CPC).[66]

[61] Questionnaire response of the Federal Prosecutors Office of the Federation of Bosnia and Herzegovina, Ministry of Internal Affairs of the Republic of Srpska, The Prosecutors Office of Brčko District of Bosnia and Herzegovina, Police of Brčko District of Bosnia and Herzegovina, Legal Aid Office of Brčko District of Bosnia and Herzegovina (question 40(b)).
[62] Questionnaire response of the Federal Prosecutors Office of the Federation of Bosnia and Herzegovina, Agency for Forensic and Expert Examination of Bosnia and Herzegovina, Federal Prosecutors Office of the Federation of Bosnia and Herzegovina, Ministry of Internal Affairs of the Republic of Srpska, The Prosecutors Office of Brčko District of Bosnia and Herzegovina, Police of Brčko District of Bosnia and Herzegovina, Legal Aid Office of Brčko District of Bosnia and Herzegovina (question 41).
[63] Questionnaire response of the Federal Prosecutors Office of the Federation of Bosnia and Herzegovina, Agency for Forensic and Expert Examination of Bosnia and Herzegovina, Federal Prosecutors Office of the Federation of Bosnia and Herzegovina, Ministry of Internal Affairs of the Republic of Srpska, The Prosecutors Office of Brčko District of Bosnia and Herzegovina, Police of Brčko District of Bosnia and Herzegovina, Legal Aid Office of Brčko District of Bosnia and Herzegovina (question 42).
[64] Questionnaire response of the Prosecutors Office of Bosnia and Herzegovina, Federal Prosecutors Office of the Federation of Bosnia and Herzegovina, Ministry of Internal Affairs of the Republic of Srpska, The Prosecutors Office of Brčko District of Bosnia and Herzegovina, Police of Brčko District of Bosnia and Herzegovina, Legal Aid Office of Brčko District of Bosnia and Herzegovina (question 43).
[65] Questionnaire response of the Prosecutor's Office of Bosnia and Herzegovina (Question 4).
[66] Questionnaire response of the State Investigation and Protection Agency of Bosnia and Herzegovina (Question 4).

- In the CPC of BiH, the searching of electronic evidence is not described and this leads the judges to order a search instead of a forensic examination. This could be resolved if the law explained searching of electronic evidence.[67]
- The law does not adequately describe the handling of electronic evidence.[68]

Moreover, further research reveals that items seized pursuant to Article 51 of the CPC of BiH, an order for search of premises (paragraph 1), an order for search of movable objects (mobile phones, computers, server (paragraph 2), under Article 65, confiscation order or temporary seizure of objects, without an order under Article 66, are dealt with as follows:

- During a search, where objects are seized, including those containing digital evidence, a record is created, certificates are issued for the seizure of evidence, then the police officers write a court hearing report and the evidence seized, (including digital evidence) is submitted to the competent court where the evidence is retained.
- The prosecutor submits a request to the court for the removal of evidence from storage at the court's facility.
- The Prosecutor's Office organises the opening and identification of evidence under Article 71 of the CPC of BiH. There is an obligation to allow the presence of lawyers and suspects at opening of evidence, which is unpacked, identified and re-packaged. A full record is made of the actions.
- After opening and identifying evidence, the prosecutor provides evidence to the police or other relevant organisations for analysis.

After opening or identifying objects containing digital evidence, there are various practices for analysis of digital evidence. The practice that has been applied at the State level for the past eight years is that after the "opening of evidence" the prosecution issues an order for forensic expertise under Article 96 of the CPC of BiH. The new practice established in the Canton of Sarajevo and at the State level and gradually introduced by individual prosecutors is that once seizure has taken place and the opening and identification has been carried out, the prosecution again requests the court to issue an order for the search of movable things (such as those containing digital evidence) under Article 51, paragraph 2.

Such searches of "movable things" are organised in the premises of the Prosecutor's Office or the police. Police officers, forensic experts, criminal technician, two witnesses, suspects, court police and lawyers are present.

As there is no legislation or written practice, sometimes prosecutors require that the computer is turned on and searched for certain digital evidence that is then recorded on optical media (CD, DVD). In other cases, a hard drive is taken out and a forensic copy of a disk is taken that recorded onto an external hard drive.

A number of issues have arisen as a result of the current practice, as follows:

- Although the CPC of BiH does not foresee the presence of two witnesses during the search of evidence, some prosecutors demand the presence of two witnesses;
- In criminal cases involving several suspects and a large number of computers and mobile phones, a large number of persons (police officers, forensics, criminal technicians, lawyers,

[67] Questionnaire response of the Agency for Forensic and Expert Examination of Bosnia and Herzegovina (Question 4).
[68] Questionnaire response of the Prosecutor's Office of Brcko District oF Bosnia and Herzegovina, Police of Brcko District of Bosnia and Herzegovina, Legal Aid Office of Brcko district of Bosnia and Herzegovina (Question 4).

suspects, court officers, witnesses) are present at the very beginning of the search of the evidence. Where suspects are in detention, the judicial police must transport them.
- In mobile phone searches, batteries often have to be charged, with everyone waiting for the batteries to charge.
- It is often the case that after the first day of an evidence search, none of the extra people turn up, even though they are later required to sign the search report. This is seen as negating the benefits of the presence of these people at the search.
- During the search, it is not possible to perform a complete forensic analysis of all digital evidence, which is why the prosecutors often require an expert review under Article 96, paragraph 2, resulting in the work often being doubled.
- The time limit for the execution of the order is 15 days in case of large-scale cases. Often the police are obliged to request an extension of the deadline for the execution of the order (it is not clear in the law whether the extension is allowed) or sometimes there is a short deadline with a resultant risk that the court will reject evidence.

The practice of turning on computers and examining data is contrary to international practice and potentially may render any evidence obtained, as inadmissible. The fact that there are no procedures written in the CPC or by-laws is problematic, as prosecutors have no guidance on what to do, and the police, who object to this practice, have no legal basis to call upon.

The original practice of the prosecutor issuing an order for forensic expertise under Article 96 of the CPC of BiH, leads to correct forensic procedures being followed, and is the preferable option. Over 350 cases have been processed in this manner, with no admissibility issues being raised.
There is the potential that the practice of prosecutors insisting that computers are turned on and examined, without the protections offered by correct forensic procedures, will lead to digital evidence being deemed inadmissible in the future.

A recommendation made in the questionnaire responses was for the establishment of accurate written procedures of measures with electronic evidence (obtaining, confiscating, examining, searching, keeping, storing, deadlines) all with the aim of proving the legality of obtaining such evidences[69]. A similar recommendation was made by the law enforcement respondents, that procedures should be specified for the following actions with digital evidence: extraction, collecting, storage, analysis, sharing, presentation in court, cooperation with private sector[70]. A similar recommendation was made by law enforcement digital forensic investigators, that it is necessary to make national guidelines for working with electronic evidence (how to seize, how to store, how to prove integrity, how to do forensic analysis). Such guidelines should oblige collection of passwords for mobile phones and encrypted hard drives[71]. A similar recommendation was made by defence attorneys, that special procedures are required for collecting and using electronic evidence in civil and criminal procedures[72].

It is also recommended that the criminal procedure laws need to explain the search of electronic evidence and draw a distinction between search and forensic analysis[73].

---

[69] Questionnaire response of the Prosecutor's Office of Brčko District of Bosnia and Herzegovina, Police of Brčko District of Bosnia and Herzegovina, Legal Aid Office of Brčko District of Bosnia and Herzegovina (question 45(a)).
[70] Questionnaire response of the Ministry of Internal Affairs of the Republic of Srpska (question 45(b)).
[71] Questionnaire response of Agency for Forensic and Expert Examination of Bosnia and Herzegovina (question 45(c)).
[72] Questionnaire response of the Prosecutor's Office of Brčko District of Bosnia and Herzegovina, Police of Brčko District of Bosnia and Herzegovina, Legal Aid Office of Brčko District of Bosnia and Herzegovina (question 45(e)).
[73] Questionnaire response of Agency for Forensic and Expert Examination of Bosnia and Herzegovina (question 45(c)).

2.3. "The former Yugoslav Republic of Macedonia"

Responses to the Questionnaire were provided by a cybercrime investigator, a digital forensics investigator, a financial investigator (Financial Police), and a lawyer.

Article 198 of the Criminal Procedure Code (CPC) and the Law on Interception of Communications specifically mention electronic evidence among the items that may constitute evidence (computer data stored on computers, devices that process electronic data, devices for data transfer, subscriber information, and communications data are mentioned).[74] Admissibility of electronic evidence is derivable from the CPC and Criminal Code.[75] Electronic evidence is understood to be subject to the same admissibility rules as other types of evidence.[76]

According to Article 181 (2) of the CPC, searches of computers or networks must be authorised by a court pursuant to a request by the public prosecutor or, in limited cases, by the judicial police. Any search of a home and a search of a computer shall be ordered by the court with a written and elaborated warrant, upon request by the public prosecutor and if there is a danger of procrastination, upon request by the judicial police. [77]

Forensic examinations of computers may be authorised by the judge during trial or by a prosecutor during the investigative stage.[78] Either may authorise the imaging of data and live acquisitions, which should be mentioned specifically in the court order.[79] Seizure of computer data requires a written request from the public prosecutor. The data must be delivered to the public prosecutor within his/her deadline.[80] The seizure may be kept confidential.[81]

Article 198 of the CPC provides for temporary seizure of computer data, which includes "data stored in a computer and similar devices for automatic or electronic processing of data, devices for data collection and transfer, bearers data and subscriber information available to the service provider".[82] This information must be handed over to the public prosecutor within the deadline determined in the written request. The judge of the preliminary procedure may decide, upon proposal by the public prosecutor, to impose the safeguarding and storing of all computer data but for no more than 6 months. The data shall be returned once the period expires "unless they have been involved in the committing of the criminal offence of Damage and unauthorized access to a computer system as referred to in Article 251, Computer fraud from Article 251-b and Computer forgery from Article 379-a, all of them stipulated in the Criminal Code; they have been involved in the commission of another computer-assisted crime; and unless they are to be used as evidence for a crime".[83] The decision of the preliminary procedure judge may be appealed by the person using the computer and the person who provides the service within 24 hours; however, the appeal does not keep the execution of the decision.[84]

---

[74] Questionnaire response, question 1a. Except as otherwise noted, all references to articles in this section are to the Criminal Procedure Code.
[75] Questionnaire response, question 1b.
[76] Questionnaire response question 1b.
[77] Questionnaire response, question 5 ; Article 181 (2) of the CPC.
[78] Questionnaire response , question 6.
[79] Questionnaire response, questions 7, 8, 11, and 12.
[80] Questionnaire response, questions 9 and 10 ; Article 198 (1) of the CPC.
[81] Questionnaire response, question 15.
[82] Article 198 (1) of the CPC.
[83] Article 198 (2) of the CPC.
[84] Article 198 (3) of the CPC.

Investigators are required to seize physical objects to obtain data. [85] Article 184 of the CPC covers "searching a computer system and computer data: (1) At the request of the enforcement agent of the order, the person using the computer or having access to it or to another device or data recorder shall be obliged to provide access to them and to provide the necessary notification for the smooth realization of the purpose of the search.

(1) Upon the request of the enforcement agent, the person who used the computer or has access to it or other device or data bearer shall immediately take measures that prevent the destruction or alteration of the data.
(2) The person who uses the computer or has access to it or to another device or data recorder, who does not act in accordance with paragraphs (1) and (2) of this Article, and for this reason there are no justified reasons, the judge of the previous procedure shall be punished according to the provisions of Article 88 paragraph (1) of this Law".

Investigators follow the standard operating procedures for the seizure of electronic evidence and for digital forensics; there is also a guide for working with Multinational Internet Service Providers and a guide for prosecutors.[86] Assets held in electronic form are treated in the same way as other electronic evidence, but it is not routine to search for them.[87]

The court ordering the forensic examination determines the deadline for it. The deadline for examination can be extended for good cause shown by the expert. The evidence may be retained by the government for the period stated in the order for the forensic examination but for no more than six months.[88]

Use of domestic and foreign experts is regulated by the CPC. A foreign individual, who meets the qualifications to do a forensic examination according to the laws of "the former Yugoslav Republic of Macedonia", or a professional institution with such qualifications, may be appointed to perform the examination provided that no appropriate expert is available within the country, per Article 198 of the CPC:[89]

"(1) An expert opinion shall be determined when a finding and an opinion by a person who possesses the necessary expert knowledge is to be obtained for determining or assessing an important fact. Expertise is, as a rule, performed by experts in the register of expert witnesses. (2) The expertise shall be determined by written order. (3) During the previous procedure, the order shall be passed by the public prosecutor, and at the main hearing the court shall, in accordance with Article 394 paragraph 2 of this Law. (4) The order shall state in relation to which facts an expert's report is conducted and to whom it is entrusted. (5) If there is a higher education facility for a certain expert body, a scientific institution or an expert institution or an expert report may be carried out within the state administration body, such expert opinions, and especially the more complex ones, shall be entrusted, by rule, to such an institution or body. If an expert finding and an opinion of a state administration body is attached as evidence by the public prosecutor, and the defence disputes it, it may propose to the court to order an expert report, which will be performed by another institution or body. (6) As a rule, one expert will be appointed for the expertise, and if the expertise is complex, then two or more experts can be determined. (7) Exceptionally, an expert may be appointed for a person who has a place of residence abroad or a

[85] Presentation of the Macedonian delegates during the regional workshop in Bucharest.
[86] Questionnaire response, question 13; discussion during the regional workshop in Bucharest.
[87] Questionnaire response, questions 37 and 39.
[88] Questionnaire response, questions 14 and 17. However, in discussion during the regional workshop in Bucharest, the delegates commented that there may be no limit, depending on the crime, and that an examination may take years.
[89] Questionnaire response, question 16.

foreign professional institution that, according to the laws of the home country, meets the requirements for performing an expert's report, if there is no higher education facility, scientific institution or expert in the Republic of Macedonia institution, sole proprietor - expert or trade company registered for performing expert witnessing, for certain kind of expertise. (8) The body referred to in paragraph (3) of this Article that ordered the expert opinion after the previously obtained opinion from the expert shall determine the deadline for the expertise and for the delivery of the findings and the opinion, and that period can be extended only upon the reasoned request of the expert".[90]

For electronic evidence to be admitted at trial, best practices for search, seizure and analysis of the data and devices are required, including a chain of custody log, photo documentation of procedures, and a report that includes hash values.[91] Typical defence objections include procedural omissions in general: the methods of search and seizure, the tools and methods used for the data acquisition, and problems with the hardware for analysis – for example, whether the media are sterilised.[92] Electronic evidence is introduced by the expert.[93]

The rights of the defendant are protected in several ways. The defendant or, more commonly, defendant's lawyer may be present during the search at the defence's request if it takes place at defendant's residence. The defence will not be present during the imaging or forensic examination.[94] Defendant is entitled to a copy of the data both for examination and for preparation of the case.[95]

Equipment and data are returned to the owner (including a defendant) at the end of the case. However, items will not be returned when there has been proof that the evidence has been used in the commission of a crime or is per se illegal to possess.[96]

Data may be obtained from third parties through either their voluntary cooperation or legal mandate under Articles 198 (1) and 196 (1) of the CPC. The matter may be kept confidential. To obtain data from third parties by collaboration, the prosecutor will send an official request electronically. If a private person reports a crime, his/her data may also be obtained per the CPC. The public prosecutor would obtain a search warrant from the court.[97]

Data is obtained from third parties internationally through international police cooperation, cooperation with Multinational Service Providers, and Mutual Legal Assistance requests.[98]
Respondents to the Questionnaire generally felt that their country had experience using electronic evidence in court. However, there was a divergence of opinion about the proportion of courts that have the necessary equipment and regarding the degree of court experience with electronic forensic analysis. Two responders felt that court forensic experience was limited and that courts tended to set deadlines for analysis that were too short. One respondent reported many cases in which examiners were ordered to extract (presumably to print) even terabytes of data for delivery to the public prosecutor. [99]

---

[90] The presentation of the Macedonian delegates at the regional workshop in Bucharest.
[91] Questionnaire response, questions 18 - 21.
[92] Questionnaire response, question 29.
[93] Questionnaire response, question 34.
[94] Questionnaire response, questions 23-25.
[95] Questionnaire response, questions 22 and 26. One responder stated that defendant is not entitled to a copy of the data to prepare his/her case, but, considering other answers by the same responder, this response seems to be a mistake.
[96] Questionnaire response, questions 14, 27 and 28.
[97] Questionnaire response, questions 15, 40-43. One responder stated that all procedures are coercive.
[98] Questionnaire response, question 40.
[99] Questionnaire response, questions 30-33.

Delegates recommended more equipment, staff, and training on electronic evidence for every type of official in the justice process.

2.4. Montenegro

Responses to the Questionnaire were received from a judge and a defence lawyer, in advance of the regional workshop in Bucharest. Responses from a prosecutor, the cybercrime investigator and a digital forensics expert from the Special State Prosecutor's Office, were received after the event. There are differences in the responses given by the contributors and where these exist, each response has been included and the contributor identified by a footnote.

Article 75 – Article 163 of the Criminal Procedure Code deals with evidentiary actions and categories of evidence. They include:

- Search of living space, other premises, movable articles and persons
- Provisional seizure
- Testimony of the accused
- Witness testimony
- Crime scene search and reconstruction of the event
- Forensic examinations
- Photos and audio-visual tapes
- Surveillance.

There is no definition of electronic evidence in the Criminal Procedure Code, nor any specific rules on its admissibility. According to one response, electronic evidence is neither included nor excluded by the legislation. It is up to each judge to decide the issue in each case.

An example of a case where there was no physical device or object to seize is given, where a judge requested YouTube to deliver data in a civil case. YouTube did not comply because the request was not in the proper form, and the case was closed without the evidence.[100]

Respondents to the Questionnaire answered Question 1b positively by confirming that the law says that electronic evidence is admissible in criminal cases, except the defence lawyer.[101] The lack of law covering electronic evidence does cause issues to arise, because it is not possible to determine whether electronic evidence is admissible at all considering there is no procedure for obtaining and dealing with it.[102]

An example of the difficulty of analysing the Montenegro responses is the variation in the replies given where some are diametrically opposite. The table below gives an example.

Question	Lawyer	Cybercrime Unit	Prosecutor	Judge	Forensic Expert
1 (b)	No	Yes	Yes	Yes	Yes
1 (c)	No	Yes	Yes	No	Yes
1 (d)	No	Yes	Yes	No	Yes
1 (e)	No	Yes	Yes	No	Yes

[100] Questionnaire response - lawyer (question 10).
[101] See Appendix 4.2.
[102] Questionnaire response - lawyer (questions 1 to 4).

Interestingly, the responses to Question 2, which is only relevant if electronic evidence admissibility is not prescribed in law, is answered by all respondents, except the lawyer who reasserts that there is no law covering the subject and that each court is deciding the issue. Other responses include that it is covered in the Criminal Procedure Code, though there being no basis to decide admissibility, separately from the considerations of general rules of admissibility. Question 1b and 2 of the Questionnaire, in particular appear to have caused some confusion because question 1b specifically asks if the law covers the admissibility of electronic evidence. The positive responses appear to answer a more general practical question about whether it is deemed admissible in court.

Further contradiction is provided in the answers to Question 4 dealing with problems caused by the law or lack of it. Responses include:

- "Criminal Procedure Code does not consider electronic evidence as a special type of evidence, regarding the fact that pursuant to that law, search of digital evidence is considered as a search of movable articles". [prosecutor] "The Criminal Procedural Code does not treat electronic evidence (computers and similar devices for automatic data processing to which the computer is connected) as a special type of evidence. Electronic evidence is treated in the Criminal Procedure Code as movable article". (Article 75 condition 2)" [digital forensic expert]
- "Yes it does because it is not possible to determine whether that kind of evidence is admissible at all considering there is no procedure of obtaining it". [lawyer]
- "There are no problems". [judge]
- "It does create problems because not all law enforcement has enough education for collecting digital evidence and have no competences in first responders behaviour, and because collecting evidence is not prescribed by any Law except the Criminal Procedure Code it does create a lack of search and seizure of good electronic evidence" [cybercrime investigator].

A review of the CPC finds no definition of electronic evidence. There are numerous references to electronic communication and the use of electronic documents in various forms, but not in evidence.

Article 75 of the CPC states that: "(1) Search of dwellings and other premises of the accused persons or other persons as well as their movable articles outside the dwellings may be carried out if grounds for suspicion exist that in the course of search the perpetrator would be caught or that traces of the criminal offence or objects relevant to the criminal procedure would be found.

(2) The search of movable articles within the meaning of paragraph 1 of this Article shall include the search of computers and similar devices for automatic data processing to which the computer is connected. At the request of the court, the person using a computer shall enable access to the computer and removable storage used for storing information relative to the object of the search (discs, USB flash discs, USB hard discs, diskettes, tapes and alike), as well as give necessary information on the use of the computer. Persons who refuse to do so although reasons referred to in Article 111 of the present Code do not exist may be punished pursuant to Article 85 paragraph 3 of the present Code".

This article would appear to be the basis upon which some of the answers to Questions 1 to 4 are given.

The searches of computers and networks, forensic examination of seized devices, imaging of data and conducting live data acquisition, are based on court orders, requested by the prosecutor.[103]

[103] Questionnaire response - lawyer, cybercrime investigator and digital forensic expert (questions 5 to 8).

The response by the prosecutor is different and possibly indicates a misreading of the questions as the responses relate to identifying who carries out the activities rather than who authorises them. The issue of whether there is a requirement to seize physical objects, rather than data only produces different responses. Two replies indicate that the issue is not clearly regulated (prosecutor and forensic expert). The only other response is from the cybercrime investigator and indicates that there is a requirement to seize the physical objects.[104]

There is one example given by three respondents as to how they have dealt with cases where there is no physical object to seize. This involved obtaining an order from the court to search an online email account. An online backup of data was taken and a hash of the evidence created. Access to the account was obtained by using the credentials of the account owner.[105]

The issue of the ability to image or conduct live data forensics onsite, leads to a variety of responses ranging from "No", through "it is not sufficiently regulated", to "Yes, by virtue of the CPC". The inconsistency in the answers perhaps indicates that this subject area requires further clarification.[106]

It would appear that although there are no national guidelines on the collection and handling of electronic evidence, there are some instructions that are available to police officers at the practical level.[107]

Evidence is only stored by the police for the duration of the forensic examination of the material. Following that, it is forwarded to the prosecutor who is responsible for its retention. Seized evidence is stored in digital data warehouses. In the concrete case of the Special State Prosecutor's Office, the Professional Service for Digital Evidence retains evidentiary material. The material is retained until issue of the indictment, and if evidence that indicates the commission of the criminal offence is not found, it is stored for no more than six months. There is no common view as the ability for a seizure of electronic evidence to remain confidential.[108].

According to Article 137 (4) of the CPC and the Article 3 (2) of the Law on Judicial Experts it is possible to get third party assistance from abroad in conducting digital forensic examinations. A time limit of three months for conducting digital forensic examinations was highlighted by the cybercrime investigator.[109]

In order to establish that electronic evidence has been properly forensically examined, stored and not altered, the following steps are undertaken:

- The prosecution issues an order on the forensic examination stating the subject of examination, as well as the deadlines.
- Computers and phones are sealed, opened in the presence of the defendant and witnesses. After making a forensic image and generating the hash value, they are sealed again in the presence of the defendant and the witnesses. [digital forensic expert]
- Forensic tools and good practice of digital forensics are a guarantee that the evidence will not be altered (write blockers, checksums, etc.). [prosecutor][110]

[104] Questionnaire response - prosecutor, cybercrime investigator and digital forensic expert (question 9).
[105] Questionnaire response – prosecutor, cybercrime investigator and digital forensic expert (question 10).
[106] Questionnaire response – lawyer, prosecutor, cybercrime investigator and digital forensic expert (questions 11 and 12).
[107] Questionnaire response – prosecutor, cybercrime investigator and digital forensic expert (question 13).
[108] Questionnaire response – prosecutor and Forensic Expert (questions 14 and 15).
[109] Questionnaire response – prosecutor, digital forensic expert and cybercrime investigator (questions 16 and 17).
[110] Questionnaire response (questions 18 to 20).

The use of forensics tools, software and hardware (write blockers, checksums, etc.) and reporting, ensure that the forensic examination is conducted properly, but this is not regulated by the law.[111] For electronic evidence admissibility to be resolved, the prosecutor proposes in the indictment that the analysed electronic evidence is included into evidence, *i.e.* presented at the main hearing as evidence. Of course, the processors of digital evidence (expert witness, Forensic Centre, expert trained for forensic analysis) by using forensic procedures, postulates on the integrity of digital evidence and appropriate forensic hardware and software ensure integrity of the evidence itself. The defence is entitled to object to each piece of evidence which is proposed by the prosecution, including electronic evidence.[112]

The suspect and/or a representative has the right to be present during the search and seizure of electronic evidence. The person who conducts the search can only perform it in the absence of the defence in certain circumstances. The suspect and or their representative may be present during the imaging of data and the forensic analysis, although, rarely are they present for the latter, due to the length of time involved in conducting the analysis phase of the process. The defence is entitled to have a copy of each piece of evidence proposed in the indictment. After the decision on whether to issue an indictment is made, seized objects are returned, unless they are objects used for the commission of the criminal offence. In terms of defence objections to electronic evidence, an objection that the evidence itself was not collected in a lawful manner can be provided by the defence. In practice the frequency of such objections has not been established.[113]

Reportedly, courts are familiar with electronic evidence and are equipped to deal with such evidence in court. There is a professional service for information technology in the court, which helps the presentation of digital and other evidence in the court. One problem that is highlighted is that courts often require electronic evidence to be printed out. It is interesting to note that while the prosecution and digital forensic expert identify this as an issue, the responses from the judge suggest there are no problems. A judge may decide whether to exclude some evidence proposed by the prosecution, under the conditions prescribed by law.

The court regards the findings and opinion of an expert as evidence. A party may request, and the court shall permit and order, that the expert who made the analysis makes an oral statement regarding any objections – to be heard directly and to give possible clarification and answer the questions of the parties. The court may require an expert to supplement the analysis. The legislation allows for experts, who have the necessary professional knowledge and who assist the court in determining and evaluating important facts[114].

Although it is envisaged that evidence of assets in electronic form are admissible, there is no reported experience of this type of cases.[115]

The CPC allows for evidence to be obtained from third parties and the method of obtaining such evidence depends on the circumstances and the type of case. The prosecution considers this as requiring confidentiality until the indictment is issued. As with other actions, the obtaining of evidence from third parties is by court order or Mutual Legal Assistance, if the data is held abroad.[116]

For cases involving the obtaining of electronic evidence from abroad, a request for authenticity of the data may be requested, using forensic methods of verification using the checksum as these are the methods used in Montenegro. The court may declare electronic evidence inadmissible, if it

[111] Questionnaire response – prosecutor and digital forensic expert (questions 18 to 20).
[112] Questionnaire response – prosecutor (questions 21 to 22).
[113] Questionnaire response – prosecutor and digital forensic expert (questions 23 to 29).
[114] Questionnaire response – prosecutor, judge and digital forensic expert (questions 30 to 36).
[115] Questionnaire response – prosecutor, judge and digital forensic expert (questions 37 to 40).
[116] Questionnaire response – prosecutor, judge and digital forensic expert (questions 41 to 42).

was not obtained in a legally valid manner. An example is if evidence was obtained by enforcement of measures of secret surveillance without the appropriate authorisation.[117]
The prosecutor observed that with regard to rapidly growing rate of cybercrime, and increased use of digital warehouses as a means of commission and communication of criminal activity, this field should be regulated in more detail than it is under the existing legislation. No specific suggestions are made.[118]

There were a sufficient number of different answers to various questions asked in the Questionnaire, to conclude that the issues around the collection, analysis and admissibility of electronic evidence are worthy of review in Montenegro. The level of different responses is such that there is a need to formalise the procedures for dealing with electronic evidence and safeguarding the security and privacy of data seized during criminal investigations.

[117] Questionnaire response – prosecutor, judge and Forensic Expert (questions 43 to 44).
[118] Questionnaire response – lawyer, prosecutor, judge and digital forensic expert (questions 43 to 44).

2.5. Serbia

Responses to the Questionnaire were provided by a cybercrime investigator, digital forensics specialist and prosecutor. It should be noted that when identifying the source of the responses to the questionnaire, there were often common answers provide by different contributors. Where this was the case, the first contribution is acknowledged in the footnotes. A revised version of the questionnaire was sent by the delegates after the regional workshop in Bucharest, which comes to complement or clarify some of the initial responses, relevant reference to the document is done accordingly.

According to the Criminal Procedure Code of Serbia the methods of obtaining evidence fall into the following categories[119]:

- Interrogation of the defendant
- Questioning witnesses
- Expert examination
- Reconstruction of events
- Examination of a person, object and location
- Using record as proof
- Obtaining samples
- Checking accounts and suspicious transactions (acquiring data, monitoring suspicious transactions, temporary suspending suspicious transactions)
- Seizure of objects
- Search
- Special evidentiary actions (covert interception of communications, covert surveillance and audio and video recording, simulated (business) deals, computer search of data, controlled delivery, undercover investigator).

The CPC defines an instrument as an object or computer data suitable for or designated as proof of a fact being determined in proceedings. In that sense, computer data is admissible as electronic evidence in criminal cases[120]. The only precondition is that the evidence is gathered according to the law. There are no additional requirements[121]. Electronic evidence is also admissible in civil cases and there are no additional requirements for the admissibility of electronic evidence in civil cases[122].

Article 2 of the CPC deals with definition of terms. Electronic data is covered under sub-paragraphs 29 to 32 in the following way:

" 29) an electronic record is audio, video or graphical data in electronic (digital) form;
30) an electronic address is a set of characters, letters, numbers and signals intended for determining the origin of a connection;
31) an electronic document is a set of data which is defined as an electronic document under the law regulating electronic documents;
32) an electronic signature is the set of data which is defined as an electronic signature under the law regulating the electronic signature".

Article 147 of the CPC refers to objects being seized and specifies that this also include

[119] Revised Questionnaire response of Serbia (question 1(a)).
[120] Revised Questionnaire response of Serbia (question 1(b)).
[121] Revised Questionnaire response of Serbia (question 1(c)).
[122] Revised Questionnaire response of Serbia (question 1(d and e)).

"automatic data processing equipment and devices and equipment on which electronic records are kept or may be kept".

Article 152 of the CPC states that "a search of a dwelling or other premises or a person may be performed if it is probable that the search will result in finding the defendant, traces of the criminal offence or objects of importance for the proceedings. A search of a dwelling or other premises or a person is performed on the basis of a court order or exceptionally without an order, on the basis of a legal authorisation. The search of automatic data processing devices and equipment on which electronic records are kept or may be kept is undertaken under a court order and, if necessary, with the assistance of an expert".
It is identified that the collection of digital evidence is defined as the same as a police search of property and persons, which in practice produces a large number of procedural problems. However, no further details are provided in the responses to the questionnaire[123].
The instructions for the seizure of electronic evidence are covered in the CPC and the Law on Ratification of the Convention on Cybercrime. There are no separate national guidelines covering the subject[124]. There are however, police instructions/guidelines for the seizure of electronic evidence[125].
Article 147 of the CPC states that "The authority conducting proceedings will seize objects which must be seized under the Criminal Code or which may serve as evidence in criminal proceedings and secure their safekeeping", which as mentioned above may include "automatic data processing equipment and devices and equipment on which electronic records are kept or may be kept".

Computers and phones are sealed upon seizure and opened in the presence of the defendant and witnesses. After making a forensic image and generating the hash value, they are sealed again in the presence of the defendant and the witness. The Digital Forensics Unit does not store electronic evidence. After the collection of evidence and writing a report, the evidence is forwarded to the prosecutor, they keep only reports for use in testimony at the trial[126]. Any evidence seized during an investigation is stored by the prosecutor, who retains it until the indictment is filed with the court. It is the responsibility of the prosecution to ensure that seized evidence is safely kept in adequate conditions. There is no explanation of what constitutes adequate conditions.

No details are provided of the procedures for dealing with and storing electronic evidence, although the police do have their own guidelines for handling evidence. It appears that all evidence is sent by the police to the prosecutor, who is responsible for its storage until the court case. There seem to be no procedures in place to identify adequate conditions for storing of seized evidence or to ensure the integrity of evidence is maintained while on the possession of the prosecutor.

Within the Serbian legal system, according to the Law on confidential data, it is possible to require the seizure to remain confidential and have restrictions applied[127].

All searches of computers or networks are conducted according to the conditions of a court order. The authority conducting proceedings (prosecutor or court) will order an expert examination when professional knowledge is required for establishing or evaluating a certain fact in the proceedings.

[123] Questionnaire response – Digital Forensics Unit (question 4).
[124] Revised Questionnaire response of Serbia (questions 13).
[125] Questionnaire response – Digital Forensics Unit (question 13)
[126] Questionnaire response – Digital Forensics Unit (question 14 and 18).
[127] Revised Questionnaire response of Serbia (questions 14 to 15 and 18).

The authority conducting proceedings orders an expert examination by issuing a written order, ex officio or on a motion by a party and defence counsel, and if there is a danger of delay an expert examination may also be ordered verbally, with an obligation to compose an official note.
The imaging of data and conducting live data acquisition, are based on a prosecutor or court order. A special police unit or an expert witness carries out these activities. It is possible under Serbian law to seize both data and objects. In other words, it is not always necessary to seize physical devices, where data may be seized in isolation. Both data imaging and live data forensics may be conducted on site[128].

It is allowable for Serbian authorities to engage experts from the private sector, another country or an international organisation, should it be necessary and the required skills are not present within the Serbian authorities. Any examination of evidence should be conducted without delay, although there are no statutory time limits.[129]

All electronic searches, subsequent examination and admissibility of evidence rely upon the action being conducted in accordance with the law of Serbia. This requires that for each stage of the process the prosecutor has to make application to the court for an order to be issued. Any report submitted in respect of these actions must demonstrate compliance with the law[130].

The defence can examine prosecution's evidence, but only after the defendant is interrogated. Usually the defence requests to examine a copy of forensic reports, however access to the evidence itself may be undertaken. The defendant or their representative may be present during an electronic search, imaging of data, during the forensic analysis. In addition, they are entitled to receive a copy of the electronic evidence[131].

If during a search, objects are found which are not connected to the criminal offence for which the search was undertaken, but which indicate another criminal offence prosecutable ex officio, they will be described in the record and seized and a receipt on the seizure will be issued immediately. If the public prosecutor finds that there are no grounds to initiate criminal proceedings or if the reasons for which the objects were seized cease to exist, and the reasons for their confiscation do not exist, the objects will immediately be returned to the person from whom they were seized. In case of possessing any illegal material, it will not be returned to the person from whom they were seized.[132]

Among the objections raised by the defence in cases involving electronic evidence in criminal trials in Serbia, are the following:

- Objections to expert witnesses in terms of their expertise in this field, their references, the number of expert examinations carried out to date.
- The expert's findings and opinion are disputed with the assertion of the Defence that it is technically impossible for hundreds of documents to be deleted in the same hour, the same minute, or a precisely determined second, and even assuming that they were grouped and deployed would be chronologically deleted because deletion means at least one click keyboard or mouse.
- The "chain of custody" from the moment of the seizure to the presentation of the evidence before the court, is disputed on the basis that the written evidence shows that the computer

[128] Revised Questionnaire response of Serbia (questions 5 to 12).
[129] Revised Questionnaire response of Serbia (questions 16 to 17).
[130] Revised Questionnaire response of Serbia (questions 19 to 21).
[131] Revised Questionnaire response of Serbia (questions 22 to 26).
[132] Revised Questionnaire response of Serbia (questions 27 to 28).

and the external memory are handed over to other services, and that nobody knew before the expertise where the computer is located, who took it, when it was returned etc.
- The court failed to determine whether there was a possibility of manipulation of a computer that was not examined for some time after the day it was seized.
- The hash value of the hard disk was not taken in the presence of the defence counsel or the defendant.
- The time in the BIOS (Basic Input-Output System) was changed by the expert to show that events took place at a time that suits the prosecution.
- The admissibility of electronic evidence is incomprehensible, on the basis that the technology terms are in English language and are repeated in the statement (file, Recycle Bin, etc.) [133]
- Courts ordering that electronic evidence have to be printed out. It is the quantity issue that creates the problem, not only the nature of the materials to be printed[134].

There is no information provided as to whether any or all of these claims has led to electronic evidence being ruled as inadmissible.

There is experience in Serbia of using electronic evidence in court. The courts accept the production of electronic evidence in digital form, while the reports of the experts are produced in written form. The courts have equipment to deal with electronic evidence and view it. They also have experience of dealing with cases involving forensic analysis of electronic evidence. One of the main issues identified in the Questionnaire is that judges do not participate in specialised training in the same way as prosecutors and therefore there are challenges to them understanding the methods of obtaining and representing electronic evidence. In the Serbian police, it is considered that there are too few people who are engaged in digital forensics. There is no experience of court order limiting the scope of the search of electronic evidence during the forensic process. Within the Serbian system, evidence is introduced to the court by the prosecutor and it is not necessary for an expert to always be present. An expert witness may be called by court, prosecution or defence to clarify his findings and opinions or to add new findings and opinions.

There is no information provided about the number of courts that have facilities to deal with electronic evidence or the effect on the criminal justice system of the perceived lack of knowledge of judges and the sparsity of resources within the police, dealing with digital forensics; for example, is the latter leading to unacceptable delays in the processing of electronic evidence.[135]
In relation to assets held in electronic form, it is possible under the CPC to use this information in evidence. There is no obligation to return either the original or a copy of the assets held in electronic form. Where evidence of assets held in electronic form are discovered during a forensic examination, where they were not the target of the search, the finding will be recorded in the report of the examination.[136]

It is not clear from the answers if it is a routine exercise to search for electronic assets during all forensic examinations of electronic evidence, or if discovery is a matter of chance.

In terms of evidence obtained from third parties, the responses provided were limited to evidence from service providers. In these cases, the request is sent to the provider based on a court order. However, it is suggested that all third-party evidence is treated in this way. It is possible to collect evidence from third parties with their consent. In these cases, there is no need for coercive measures. It is possible according to the law to require a third party to keep the matter

[133] Revised Questionnaire response of Serbia (question 29).
[134] Questionnaire response – Digital Forensics Unit (question 31).
[135] Revised Questionnaire response of Serbia (questions 30 to 36).
[136] Revised Questionnaire response of Serbia (questions 37 to 39).

confidential. In circumstances where a report of a crime involving evidence is reported, the electronic evidence may be collected by requesting the reporting person to provide it in electronic form, or for example for the police to visit an identified web site and download the evidence themselves; the latter for example in the sale of counterfeit goods via the Internet (website names, Facebook profiles, etc.)[137]

It is not clear from the answers to the questionnaire if any specific procedures to ensure integrity of evidence collected in this way exist or if there are steps to ensure "chain of custody" is maintained.

Evidence obtained from other jurisdictions has not been deemed inadmissible on any proceedings in Serbia. There are no special requirements placed on the sending country, other than in compliance with the Budapest Convention on Cybercrime, through contact points and or the Mutual Legal Assistance request.[138]

According to the comments of the Serbian prosecutors, improvements are needed to the Mutual Legal Assistance procedure when dealing with electronic evidence. Simplification of that procedure is needed, bearing in mind that time is the key factor in obtaining electronic evidence, and the potential for evidence to be erased or compromised if it is not secured in a reasonable period of time.

[137] Revised Questionnaire response of Serbia (questions 40 to 42).
[138] Revised Questionnaire response of Serbia (questions 43 to 44).

2.6. Turkey

Responses to the Questionnaire were provided by a cybercrime investigator, digital forensics specialists, and prosecutor.
In the Turkish criminal justice system, the Code of Criminal Procedure (Law No. 5271) is the main source of legislation relating to categories of evidence. Regulations on its implementation and the case law of the courts set the guiding principles in terms of the Code's compliance with contemporary and technological developments[139]. The following list of categories of evidence was provided[140]:

- Declarations
- Documents
- Digital Evidence
- Trace Evidence.

The Code of Criminal Procedure indicates that electronic evidence is admissible in criminal cases. In particular, Article 134 of the Code of Criminal Procedure provides for safeguards (in obtaining evidence) in criminal proceedings[141]. According to this provision, in order for the electronic evidence to be admissible it must be obtained using particular methods and procedures. Otherwise, it is not considered as evidence[142]. Additionally, the admissibility of evidence is subject to the judge's decision upon a request made by the public prosecutors and in the particular case of confiscation, it is necessary that digital evidence should be encoded or confidential[143].

Electronic evidence is also admissible in civil cases, in accordance with the Code on Civil Procedure (Law No. 6100)[144]. In such cases evidence can be in the form of printed or published texts, official documents, drawings, plans, sketches, photographs, films, displays or sound recordings as well as all similar documents that contain information and electronic data. Additionally, in accordance with the Code on Civil Procedure, data created in accordance with procedure and with an electronic signature are considered as official documents. The judge shall carry out an ex officio examination of whether the document signed electronically and served as evidence to the court had been created by secure electronic signature. The judge shall request an expert examination in case data created with an electronic signature is rejected as evidence. The judge shall take that decision only if he/she was unable to form an opinion after hearing both parties. The parties are under the obligation to submit all the documents that they and the other party consider as evidence. Electronic documents shall be presented to the court after they are printed and when they are saved in an electronic database in a manner that is made available for the court's examination[145].
Several areas of the Code on Criminal Procedure were highlighted as needing refinement, and these were[146]:

- Seizure of data

[139] Questionnaire response of the Prosecutors Office (question 1(a)).
[140] Questionnaire response of the Cybercrime Unit and Digital Forensic Unit (question 1(a)).
[141] Questionnaire responses of the Prosecutors Office, Cybercrime Unit and Digital Forensic Unit and the Forensic Computing Department of the Council of Forensic Medicine (question 1(b)).
[142] Questionnaire response of the Prosecutors Office (question 1(c)).
[143] Questionnaire response of the Cybercrime Unit and Digital Forensic Unit (question 1(c)).
[144] Questionnaire response of the Prosecutors Office, Cybercrime Unit and Digital Forensic Unit and the Forensic Computing Department of the Council of Forensic Medicine (question 1(d)).
[145] Questionnaire response of the Prosecutors Office (question 1(e)).
[146] Questionnaire response of the Prosecutors Office (question 4).

- Research on the digital material of persons unrelated to the crime
- Decision of the public prosecutor on search and seizure in urgent matters.

The decision of a judge, upon the request of a prosecutor, is required to:

- Authorise a search of computers or networks[147]
- Authorise the forensic examination of computers/drives[148]
- Authorise imaging of data[149].

Although the Code of Criminal Procedure does not specifically regulate the issue of live acquisition of data, it is possible to carry out live acquisition on computers where these were seized physically on the basis of a search decision, if the circumstances allow it. In such cases the decision of a judge, upon the request of a prosecutor, is required[150].

Article 134 of the Code of Criminal Procedure provides that data can be obtained and seizure can be applied. It is possible under this legal provision to seize data without seizing physical objects. In cases where it is not possible to take an image at the location, an image of the entire system will be taken and physical objects will be returned. If it is not possible to create the image onsite, the physical objects will be seized and returned after the image is taken. Data captured in this way should be encoded or confidential[151]. Some examples of approaches used in practical cases where it was not possible to seize physical objects were provided in the questionnaire responses:

- If the data is in the possession of a third person or institution (e.g. in a cloud system), it is requested from them.
- Live access to the system was maintained and in this way the data was obtained through taking of images.

Article 134 of the Code of Criminal Procedure allows for both onsite imaging and live acquisition of data[152].

Different institutions maintain instructions/guidelines for the seizure of electronic evidence[153]. For example, there are guidelines for the principles and instructions regarding Forensic Informatics in the Law Enforcement[154]. Evidence seized by the investigative authority is stored in accordance with the procedures in the regulation of criminal assets. The storage of evidence is done by the investigating authority or by judicial authorities (judicial storage). According to the Code of Criminal Procedure, digital evidence shall be stored until its judicial copy is obtained (*i.e.* until a copy is provided to the prosecutor). Once the copy is obtained, it will be handed over to its owner[155]. The main principle in terms of maintaining confidentiality of electronic evidence is the

[147] Questionnaire response of Prosecutors Office, the Cybercrime Unit and Digital Forensic Unit and the Forensic Computing Department of the Council of Forensic Medicine (question 5).
[148] Questionnaire response of Prosecutors Office, the Cybercrime Unit and Digital Forensic Unit and the Forensic Computing Department of the Council of Forensic Medicine (question 6).
[149] Questionnaire response of Prosecutors Office, the Cybercrime Unit and Digital Forensic Unit and the Forensic Computing Department of the Council of Forensic Medicine (question 7).
[150] Questionnaire response of Prosecutors Office, the Cybercrime Unit and Digital Forensic Unit and the Forensic Computing Department of the Council of Forensic Medicine (question 8).
[151] Questionnaire response of Prosecutors Office, the Cybercrime Unit and Digital Forensic Unit and the Forensic Computing Department of the Council of Forensic Medicine (question 9).
[152] Questionnaire response of Prosecutors Office, the Cybercrime Unit and Digital Forensic Unit and the Forensic Computing Department of the Council of Forensic Medicine (question 11 and 12).
[153] Questionnaire response of the Forensic Computing Department of the Council of Forensic Medicine (question 13).
[154] Questionnaire response of the Prosecutors Office (question 13).
[155] Questionnaire response of the Prosecutors Office, Cybercrime Unit and Digital Forensic Unit (question 14).

confidentiality of the investigation[156]. The access to confiscated material can be limited and the legislation regulates who, and under what process, can have access to confiscated material[157].
Within the framework of international agreements, there are no obstacles to requesting assistance from another country, international organisation or private party with a digital forensic examination[158].

There are no time limits for the examination of electronic evidence but information must be given about the process, explaining the status of the examination, after a certain amount of time. The examination procedure shall be conducted as soon as possible during the investigation phase and the evidence shall then be transferred to the judicial authorities[159].

The evidence should quickly be stored by the judicial authorities when the procedures in the law enforcement authorities are completed. In addition, the practice of providing a sealed copy of the image to the owner of the device(s) was introduced to the Code of Criminal Procedure to prevent the distortion of evidence. In case there is an objection to the integrity of the evidence, the sealed image is handed over by the person from whom the evidence was obtained and examined[160]. Examination should primarily be conducted on the judicial copies of the digital evidence and the completeness/integrity of the evidence should be regularly checked using hash values[161]. Integrity of electronic evidence is also verified by checking logs, signatures and the physical condition of the evidence's container[162].

In order for the prosecution to establish that the electronic search has been properly conducted, it is important to ensure that the practices of searching, securing the presence of the person and/or their representative during imaging and the right of the person to request one of the duplicate images obtained are respected. If the image cannot be taken onsite, the person in question or his lawyer should be invited and an image should be taken after the image is sealed and brought to the law enforcement office[163]. To ensure that the forensic examination is properly conducted, the image received from law enforcement should be kept in storage and then sent to the forensic examination without opening its seal[164].

For electronic evidence to be admissible, it might be necessary for the investigation authority to prove that seized evidence has not been altered by the prosecutor. It is obligatory to prove that the seizure, confiscation and the examination carried out on the evidence have all been done in accordance with the regulations and that the chain and completeness of the evidence has been maintained. The practice of proving a suspect with a copy of the forensic image is intended to achieve this goal[165].
The suspect or his/her representative has a right to be present during the search and imaging (if conducted onsite). In fact, the presence of the suspect or his/her representative at the search and forensic imaging is the rule. The suspect is provided with a copy of the forensic image created at

[156] Questionnaire response of Cybercrime Unit and Digital Forensic Unit (question 15).
[157] Questionnaire response of Prosecutor's Office (question 15).
[158] Questionnaire response of Prosecutors Office, the Cybercrime Unit and Digital Forensic Unit and the Forensic Computing Department of the Council of Forensic Medicine (question 16).
[159] Questionnaire response of Prosecutors Office, the Cybercrime Unit and Digital Forensic Unit and the Forensic Computing Department of the Council of Forensic Medicine (question 17).
[160] Questionnaire response of the Prosecutor's Office (question 18).
[161] Questionnaire response of the Cybercrime Unit and Digital Forensic Unit (question 18).
[162] Questionnaire response of the Forensic Computing Department of the Council of Forensic Medicine (question 18).
[163] Questionnaire response of the Prosecutor's Office and the Cybercrime Unit and Digital Forensic Unit (question 19).
[164] Questionnaire response of the Prosecutor's Office (question 20).
[165] Questionnaire response of the Prosecutor's Office and the Cybercrime Unit and Digital Forensic Unit (question 21).

the time of imaging. Therefore they have a complete copy of the data and thus there are no provisions in the law concerning the presence of the suspect for procedures that could not have been completed based on data that was not captured at the time of the onsite examination. The suspect or his/her representative is not present during the forensic analysis[166].

According to the Code of Criminal Procedure, once the copy of the seized material is made, it will be handed over to its owner. Investigation and prosecution authorities can only keep the copy[167]. If it is identified that the material on the computer is illegal, in practice this data will be taken out of the digital environment and a request would be lodged with the court to return the data although there is no clarity in the legislation on this issue[168]. It is not appropriate, for examine to return a hard drive in a case of suspected terrorism or a hard drive containing illegal images[169].

The Questionnaire responses provide several examples of the respondents' experiences of defence objections to admissibility electronic evidence. These are[170]:

- If the forensic image is not created onsite the defendants may object because they have not been present during the imaging process.
- That the data was not obtained according to the correct procedures.
- That the data was not stored according to the correct procedures.
- That a copy of the data was not handed over to the suspect.
- That the data was altered after imaging/that the integrity of the evidence has been compromised.

It is reported in the responses to the Questionnaire that the courts have experience using electronic evidence, have equipment to view and use electronic evidence and have experience with electronic forensic analysis[171]. Examples of the problems experienced with presentation of electronic evidence are that[172]:

- Courts like to have printed reports but this can be addressed through communication and proper explanation.
- When electronic data examination report is submitted to the case file, it is obligatory to present the data on which the report was based with explanations or screen capture (picture or video) samples.

Further examples of the problems with forensic analysis were also cited relating to courts issuing orders for forensic analysis with unreasonably short deadlines for analysis[173].
It was reported during the regional workshop in Bucharest that the volume of artefacts collected due to the recent political situation in Turkey has meant that processes relating to collection and management of electronic evidence have not been followed in all cases. It would seem that existing national regulations and Standard Operating Procedures that put forward rules on

[166] Questionnaire response of Prosecutors Office, the Cybercrime Unit and Digital Forensic Unit and the Forensic Computing Department of the Council of Forensic Medicine (questions 22-26).
[167] Questionnaire response of the Cybercrime Unit and Digital Forensic Unit (question 27).
[168] Questionnaire response of the Prosecutor's Office (question 28).
[169] Questionnaire response of the Forensic Computing Department of the Council of Forensic Medicine (question 27).
[170] Questionnaire response of Prosecutor's Office, the Cybercrime Unit and Digital Forensic Unit and the Forensic Computing Department of the Council of Forensic Medicine (questions 29).
[171] Questionnaire response of Prosecutor's Office, the Cybercrime Unit and Digital Forensic Unit and the Forensic Computing Department of the Council of Forensic Medicine (questions 30, 32, 33).
[172] Questionnaire response of Prosecutor's Office and the Forensic Computing Department of the Council of Forensic Medicine (question 31).
[173] Questionnaire response of the Cybercrime Unit and Digital Forensic Unit and the Forensic Computing Department of the Council of Forensic Medicine (question 33(a)).

acquisition, handling and storage of data have not been always followed, especially regarding the observance of the chain of custody, documenting and reporting, presentation of information to the defence, etc. This raises questions regarding the authenticity of electronic evidence as well as endangers the principle of equality of arms and is likely to lead to challenges in due course when cases involving this evidence end up in front of a court.

It is not a legal requirement that electronic evidence is introduced to the court by an expert witness. In cases where a report and/or findings are not understood or clearly explained, the court can ask an expert witness to explain. Additionally, if the electronic evidence is collected by law enforcement officers then, on the request of the defence, the court may hear an expert witness for the disclosure and auditing of the procedures used[174].

The Code of Criminal Procedure allows for assets held in electronic form to be used in evidence[175]. It is rare in practice that examination of electronic evidence would search for assets held in electronic form (e.g. virtual currency wallets)[176]. It is mandatory under the law that the original and the copy are handed over to the suspect, except in cases where harm could be caused by returning them. In such cases the original and copy will not be handed over[177].

The Code of Criminal Procedure allows for obtaining of electronic evidence from third parties and in such cases the general principles of obtaining evidence are also applicable for electronic evidence[178]. However, it is not possible to obtain a search/inquiry decision against a person who does not willingly share electronic data and evidence within the context of a criminal investigation, efforts are made to obtain the evidence within the context of the statutory obligation to abide by a court order[179]. It is possible to obtain evidence from third parties with their consent. However, if there is no consent, it is possible to request the seizure of the evidence[180] and in such cases it is possible that they may be required to keep the matter confidential[181]. In cases involving individual persons' reports of crime a report will be taken and relevant evidence will be collected (with the person's consent)[182].

When evidence is obtained from another country, the integrity of the evidence is confirmed in the framework of the domestic technical rules. For the purposes of admissibility, it is sufficient to ascertain that the data was obtained in accordance with the domestic legislation of the foreign country. It is reported in the responses to the questionnaire that there have been cases where evidence from another country has been declared inadmissible in Turkey[183].
Some final recommendations that were made in the Questionnaire responses were[184]:

---

[174] Questionnaire response of the Prosecutor's Office and the Forensic Computing Department of the Council of Forensic Medicine (questions 35 and 36).
[175] Questionnaire response of the Prosecutor's Office, the Cybercrime Unit and Digital Forensic Unit and the Forensic Computing Department of the Council of Forensic Medicine (question 37).
[176] Questionnaire response of the Prosecutor's Office (question 39).
[177] Questionnaire response of the Prosecutor's Office and the Cybercrime Unit and Digital Forensic Unit (question 38).
[178] Questionnaire response of the Cybercrime Unit and Digital Forensic Unit (questions 40 and 40(a)).
[179] Questionnaire response of the Prosecutor's Office (question 40).
[180] Questionnaire response of the Prosecutor's Office and the Cybercrime Unit and Digital Forensic Unit (question 40(b)).
[181] Questionnaire response of the Prosecutor's Office and the Cybercrime Unit and Digital Forensic Unit and the Forensic Computing Department of the Council of Forensic Medicine (question 41).
[182] Questionnaire response of the Prosecutor's Office and the Cybercrime Unit and Digital Forensic Unit and the Forensic Computing Department of the Council of Forensic Medicine (question 42).
[183] Questionnaire response of the Prosecutor's Office and the Cybercrime Unit and Digital Forensic Unit (questions 43 and 44).
[184] Questionnaire response of the Prosecutor's Office and the Forensic Computing Department of the Council of Forensic Medicine (question 45).

- Prosecutors should be able to give a search order on electronic evidence in case of an emergency.
- When third parties do not consent to the examination, the examination should be ordered by the judge.
- A search related to cloud systems should be based on the legislation.
- Increasing the speed of digital evidence acquisition.
- Centralising the storage for forensic images.
- Using specific cases for the transportation and storage of digital evidence.
- Collaboration between digital forensic laboratories.
- Training for non-technical personnel.
- Increasing the number of digital forensics practitioners.

2.7. Kosovo*

The responses to the Questionnaire were provided by a cybercrime investigator, a digital forensics expert, a financial investigator, and a judge.

Electronic evidence is not mentioned explicitly in the Criminal Procedure Code (CPC). However, Article 105 of the CPC specifically mentions electronic equipment, including computers, cell phones, and mobile electronic equipment, thus implying that electronic evidence is one form of acceptable evidence[185]. Electronic evidence is understood to be subject to the same admissibility rules as other types of evidence[186].

A judge authorises the search of computers or networks and a judge or prosecutor may authorise forensic examinations of computers, imaging of data, and live acquisition. Rules regarding data searching are defined by law, and in certain cases the court may limit the search to specific files, names, periods, etc. Investigators are required to seize physical objects to obtain data; there is no provision for seizing data otherwise[187]. It is possible to image data on site and to conduct live data acquisition on site. Live digital forensics has been used when there was no physical object to seize[188]. It is possible to keep the matter confidential[189]. Investigators follow the Kosovo* Police's Standard Operating Procedures for the seizure of electronic evidence and expert advice, including the Council of Europe's Guidelines on Electronic Evidence[190]. Investigators will search for assets held in electronic form if the order requires it[191].

The seizure, storage and retention of electronic evidence are governed by provisions of Articles 105 (Search and Temporary Sequestration), 112 (Temporary Sequestration) and 115 (Permanent Confiscation of Temporarily Confiscated Items) of the CPC[192].

Article 105 states that "6. A search order shall be issued in writing upon a written application of the state prosecutor or, in exigent circumstances, the authorized police officer".

Article 112 provides that "9. Objects and property that are temporarily sequestrated are under the supervision and control of the state prosecutor. The state prosecutor may delegate the custody and control to an authorized police officer for objects and property temporarily sequestrated under paragraphs 5, 6 and 8 of this Article".

Article 115 states that "4. Objects that are temporarily sequestrated shall be photographed and maintained in appropriate containers or transparent plastic bags and the authorized police and state prosecutor shall maintain the photographic record and a record of the chain of custody for each object or set of documents" […] "9. Objects and property that are temporarily sequestrated are under the supervision and control of the state prosecutor. The state prosecutor may delegate the custody and control to an authorized police officer for objects and property temporarily sequestrated under paragraphs 5, 6 and 8 of this Article".

---

[185] Questionnaire response, question 1a.
[186] Questionnaire response, question 1b.
[187] Questionnaire responses, questions 34 and 5-8; Article 18 (Sequestration, Copy and Preservation of Data) of the Law on Cybercrime Fight and Prevention.
[188] Questionnaire response, questions 10-12.
[189] Questionnaire response, question 15.
[190] Questionnaire responses, questions 13 and 18; Kosovo* delegates presentation during the regional workshop in Bucharest.
[191] Questionnaire response, question 39.
[192] Questionnaire responses, questions 14 and 18.

According to Article 18[193] (Sequestration, Copy and Preservation of Data) of the Law on Cybercrime Fight and Prevention, copies of seized data are to be created through technical procedures that ensure the integrity and security of the data. If the law enforcement agency or the court determines that the seizure ("confiscation") of the data will have a serious effect on the possessor of the data, an exact copy of the data may be created and used instead, leaving the original data with the possessor.

The digital forensics investigator commented that requests by prosecutors and judges for forensic examinations should be as specific as possible. In addition, clear written rules are needed to specify the manner and duration of records retention after the exam is completed and for the examination of data in cloud systems[194].
There are no time limits on the examination and seized evidence may be retained by the government indefinitely[195].

Admissibility of the evidence is governed by the CPC, including Article 111 (1), which states detailed grounds on which evidence may be disallowed if:

"1.1. the evidence obtained by a search without a court order shall be inadmissible, if the search is not approved retroactively by the court, in compliance with the provisions of the Constitution;
1.2. the search was executed without an order from a competent judge in breach of the provisions of the present Code;
1.3. the order of the competent judge was issued in breach of the procedure provided for by the present Code;
1.4. the substance of the order of the competent judge was in breach of the requirements of the present Code;
1.5. the search was implemented in breach of an order of the competent judge;
1.6. persons whose presence is obligatory were not present during the search; or
1.7. the search was conducted in breach of Article 108 of this Code".

When the prosecution offers electronic evidence, it may use hash values, time stamps, etc., to prove its admissibility[196]. In certain cases, depending on the electronic evidence provided and the need to demonstrate the evidence, the presence of the expert is also required[197].

---

[193] Article 18 (Sequestration, Copy and Preservation of Data) of the Law on Cybercrime Fight and Prevention:
"1. For the purpose of Article 17, sub-paragraph 1.2. the prosecutor shall propose confiscation of objects, equipment containing computer data, information on traffic data, data on the user, from the person or service provider owning them, for the purpose to create copies that might serve as evidence.
2. In case objects, equipment containing data that refer to data of justice authorities in order to create copies, under paragraph 1 of this Article, court's order on forceful confiscation shall be communicated to the prosecutor, who will take measures to fulfil it.
3. Copies according to paragraph 1 of this Article are created through technical means, computer programs and procedures which ensure information integrity and security.
4. The prosecutor may at any time order search for the purpose of disclosure or collection of necessary evidence about computer system investigation or computer equipment for data storage.
5. In case the crime investigation body or the court considers that confiscation of object containing data that refer to paragraph 1 will have a great impact on the activities carried out by the persons who possess such objects, could order creation of copies that would serve as evidence and which are created in compliance with paragraph 3 of this Article.
6. In case during an investigation of a computer system or computer equipment for data storage is learned that the required computer data are included into another computer system or other computer data storage device and to which access is provided from the primary system or device, it could be ordered carrying out and search in order to investigate entire computer systems or computer device for the storage of demanded data.
[194] Questionnaire response, question 45c.
[195] Questionnaire response, question 17.
[196] Questionnaire response, question 21.
[197] Questionnaire response, question 36.

The rights of the defendant are protected in several ways. Articles 137 and 147 of the CPC provide that, before engaging an expert, the State Prosecutor must issue a decision that identifies an expert and states his/her expertise, specifies the expert's exact assignment, and orders access by the expert to the evidence. The defendant or a representative may sometimes be present during the search, depending on the circumstances of the case[198].

If an expert is used, Article 138 of the CPC requires the expert's report to be disclosed to the defence no fewer than five days prior to the pre-trial testimony and no more than ten days after its receipt by the prosecution[199]. In addition, Article 141 of the CPC states that the defence may request that the prosecutor obtain expert analysis on behalf of the defence. If the prosecutor refuses to do so, the defence may appeal the refusal to the judge. In addition, defendant may obtain and pay for expert analysis him/herself. The defence is responsible for the costs of this examination and must provide a copy of any report to the prosecution within fourteen (14) days of the report's completion[200]. Where the findings of two or more experts differ on essential points or if other (specified) material deficiencies exist, other expert opinions may be sought[201]. A State Prosecutor may also authorise a police officer or expert to examine, analyse, and search for evidence in electronic media or devices[202]. Outside experts may be retained when necessary[203].

In general, Article 115 (Permanent Confiscation of Temporarily Confiscated Items) of the CPC provides for the return of equipment and data to the owner (including a defendant) at the end of the case. Items will not be returned under certain circumstances, including when they have been proven at trial to have facilitated the offence or are a material benefit from the offence or if the data is itself illegal – child exploitation images, for example.[204] Article 115 states that:

"1. Objects, property, evidence or money that are temporarily sequestrated under Article 112 of this Code shall, at the end of the criminal proceedings, be returned to the owner or possessor under Article 116 of this Code, except if actions are taken under Paragraph 2 of this Article or another action permitted under law would provide a basis not to return the objects, property, evidence or money.

2. The single trial judge or trial panel shall order the items to be permanently sequestrated in accordance with the law if the state prosecutor:

2.1. describes in the indictment those objects, properties, evidence or money that should be subject to permanent sequestration,
2.2. if the objects, property, evidence or money that is temporarily sequestrated is proven during the main trial to be have facilitated the criminal offence or constitute a material benefit obtained from the commission of a criminal offence;
2.3. under the law they may be confiscated.

3. Objects, property, or evidence that is permanently sequestrated shall be sold and the proceeds used for restitution to the injured parties and any remainder transferred to the budget".

[198] Questionnaire response, question 23. The defence will not be present during the imaging or forensic examination (questions 24 and 25).
[199] Questionnaire response, question 26.
[200] Article 141 of the CPC (Experts Engaged by the Defendant), questions 22 and 29.
[201] Article 142 of the CPC, question 29.
[202] Questionnaire response, question 20.
[203] Kosovo* delegates presentation during the regional workshop in Bucharest.
[204] Questionnaire responses, questions 27 and 28.

It is possible to obtain data from third parties, including internationally. Internationally-obtained data is admissible only when obtained by formal Mutual Legal Assistance, however[205]. It is possible to keep confidential the fact that data has been obtained from domestic or international third parties. Standard rules of digital hygiene are applied in these cases[206]. The law enforcement cybercrime investigator noted, however, that obtaining data from other countries is challenging and it takes a long time to receive adequate answers.

There are practical difficulties in Kosovo* with the use of electronic evidence in court. These include lack of hardware and software or outdated versions. In some courts, only one room may have equipment, albeit outdated equipment. Judges also may be unfamiliar with computers and networks and with the more-technical aspects of electronic evidence such as steganography, cryptocurrencies, hash values, etc.[207]. The judge from the delegation suggested that investigators focus more on using electronic evidence, since increasingly it is relevant in every kind of case, and that the necessary equipment be provided in all courtrooms[208].

In discussions at the regional workshop in Bucharest, the delegates highlighted numerous challenges:

- Identification, seizure and confiscation of proceeds from cybercrime, including from the Darknet and cryptocurrencies, as well as attribution of ownership;
- Capacity-building is needed so that officials can keep up with technological trends and obtain training, including joint training;
- Domestic cooperation regarding threat assessments and public/private cooperation;
- International cooperation to overcome legal obstacles to obtain electronic evidence, including by using joint investigations;
- The need to review the CPC and define electronic evidence explicitly;
- The need to write procedures for handling electronic evidence not into the CPC but into standard operating procedures;
- Judges and prosecutors should specify in their respective orders the data to be seized and not order that all data be seized where a narrower search would suffice; and
- Resource upgrades are needed – for example, more storage and updated software and workstations. In particular, more expert examiners are needed.

[205] Kosovo* delegates presentation during the regional workshop in Bucharest.
[206] Questionnaire responses, questions 15 and 40-43.
[207] Questionnaire responses, questions 30-33.
[208] Questionnaire response, question 45d.

3. Recommendations

Recommendation: Criminal Procedure Codes should include a definition of electronic evidence and/or inclusion of electronic evidence in the list of types of evidence.

For those jurisdictions that do not have digital or electronic evidence listed in their Criminal Procedure Codes it is recommended that this be included. Some of the jurisdictions interpret the "document" or "movable object" evidence type as including electronic evidence but this interpretation can become strained when the practicalities of searching for, and seizing, electronic evidence are encountered. A good example of this is the question of live data forensics and whether data collected by live data forensics can be collected based on an order for a search, or whether an order for acquisition or analysis is required (depending on particularities in the various jurisdictions).

Recommendation: Development of written standards for searching for, seizing, storing and analysing electronic evidence.

For those jurisdictions that do not have written standards (e.g. Standard Operating Procedures) for the search, seizure, storage and analysis of electronic evidence, it is recommended that these be developed. There was a consensus amongst the participants at the regional workshop held in Bucharest (2-3 November 2017) that it would be unwise to include prescriptive operational detail in the Criminal Procedure Code because Standard Operating Procedures or other forms of operational documentation can be updated more rapidly in response to changing technical requirements. It may be appropriate to consider regulations as an alternative to amending the Criminal Procedure Code for the same reasons given for using Standard Operating Procedures.
Procedures for conducting online undercover operations may also be covered by Standard Operating Procedures, if permitted by domestic law. Several countries mentioned this issue.
In addition, countries may wish to address in their Standard Operating Procedures, the seizure and return of systems and data to third parties. Countries seemed to have relatively-clear rules in their Criminal Procedure Codes for returns to the defendant, but no country mentioned the rights of third parties – for example, innocent businesses whose activities may be halted by seizures relating to an employee.

Recommendation: Consider including search for virtual assets in procedures for search, triage and preliminary analysis of electronic evidence.

Certain of the jurisdictions are required, upon completion of acquisition of a forensic image, to return either the original evidence, a copy, or both to the suspect. There is an exception to this requirement when doing so would cause harm (e.g. computer containing illegal images). This creates a problem where the investigators may, due to the legal requirement to return a copy of the evidence, provide a suspect with the ability to move virtual assets beyond the reach of future asset seizure/forfeiture proceedings. Such assets can have considerable value. This risk will not be identified unless the search/triage of the electronic evidence, at the time of acquisition, contains a search for virtual assets (e.g. virtual currency wallets).
It is therefore recommended that procedures for search/acquisition/triage of electronic evidence be created/amended to include routine searching for virtual assets, to the extent that this is technically possible.

Recommendation: National training for judges/prosecutors should be developed/enhanced to address challenges with orders for search/analysis of electronic evidence.

Several of the jurisdictions indicated that there are challenges with the orders for search/analysis that are being requested by prosecutors and issued by courts. These challenges fall into two broad categories. Firstly, overly broad orders that order the searching of a computer for "all evidence" or something similar. Secondly, orders that have unrealistically short deadlines or timeframes attached. These challenges require raising of the awareness of the particularities of electronic evidence amongst judges and prosecutors. It is therefore recommended that training on electronic evidence be developed/enhanced to allow judges and prosecutors to consider these issues and have an awareness of challenges involved in the analysis of electronic evidence.

Recommendation: Consider introducing effective procedures for dealing with large volumes of cases and unmanageable backlogs of electronic evidence.

It was reported that where there is a very large volume of cases or a substantially unmanageable backlog procedures for the handling of electronic evidence may not be followed precisely in all cases. This may lead to challenges to the admissibility of this evidence in future court proceedings and to violations of due process. In such cases, countries could consider deploying a fully documented and risk assessed prioritization / triage model as the basis of a tiered forensic analysis hierarchy. In such a model first-responders (or relatively low skilled forensic analysts) can be provided with automated tools for filtering all seized electronic evidence, passing only the most relevant artefacts for further analysis by highly skilled forensic analysts. Any tools used for this purpose should be fully tested and validated before use. The users of these tools should be appropriately trained in their use and lawfully authorised to use them. Training should incorporate an understanding of relevance of items to be seized and prioritisation to avoid the seizure of unnecessary items. The principle of record keeping should be maintained throughout the process. The skilled forensic analysts can thereby spend a greater proportion of their time working on the most relevant artefacts instead of needing to spend substantial time imaging and then dispensing with relatively unimportant evidence. The legal and procedural basis for conducting this form of triage may also need to be considered. Any use of such methods would typically need to be fully disclosed during subsequent legal proceeding.

Recommendation: formalise the procedures for handling electronic evidence by way of law, by-law or other formal process.

One country has reported that there are well-established, but undocumented, procedures in place for dealing with electronic evidence, which have been accepted by the courts for many years. However, there are instances where these are not followed, due to the inexperience and lack of knowledge of the procedures on the part of prosecutors, who have overall responsibility for the investigation process. Direct access to original evidence is on occasions ordered by prosecutors, in contradiction of the procedures and best international practice for handling of electronic evidence, followed by digital forensics examiners. This may have a serious impact on the integrity of any evidence recovered and its admissibility and lead to violations of due process. It is recommended that when any similar occurrence in the future is encountered, the procedures are explained to the prosecutor and a written record made of any variance ordered.
To address the root cause of this issue, it is recommended that the authorities consider the adoption of national procedures by way of by law, by-law or other formal process, which will set out the correct procedures to be followed in all instances where electronic evidence is to be collected and examined during an investigation.

Recommendation: Introduce training for first responders that will enable them to better deal with collection of large quantities of electronic evidence from sources within the scope of the authority they are acting under.

Establish written protocols and train first responders accordingly so that searches are restricted to the minimum necessary. This will reduce the occasions of unnecessary evidence being collected that cannot be analysed to good forensic standards or cannot be analysed at all.

4. Appendices

4.1. Blank Questionnaire

No.	Law Regarding Evidence	(If "Yes" to any question, please provide details/wording of law)
1		
	a. Does your country's law say that electronic evidence is admissible in criminal cases?	Yes/No
	b. In criminal cases, are there specific requirements for electronic evidence to be admissible?	Yes/No
	c. Does your country's law say that electronic evidence is admissible in civil cases?	Yes/No
	d. In civil cases, are there specific requirements for electronic evidence to be admissible?	Yes/No
2	If your country has no written law, on what legal basis are questions of electronic evidence decided in criminal cases?	
3	If your country has no written law, on what legal basis are questions of electronic evidence decided in civil cases?	
4	Does the law, or lack of it, create specific problems in cases involving electronic evidence? If yes, please provide an outline of the issues involved.	
	Seizure of Electronic Data	
5	What person or authority authorizes search of computers or networks?	
6	What person or authority authorizes forensic examinations of computers/drives?	
7	What person or authority authorizes imaging of data?	
8	What person or authority authorizes live acquisitions?	
9	In criminal or civil cases, are you required to seize physical objects, such as computers/drives? Or may you seize data without seizing a physical object?	
10	If you have handled a case where there was no physical object to seize, please explain what you did to seize data.	
11	Is it possible to image data on site?	

12	Is it possible to conduct live data acquisition on site?	
13	Are there national instructions/guidelines for the seizure of electronic evidence?	
14	How is electronic evidence stored after it has been seized? Who stores it? How long may it be retained by the prosecution?	
15	Is it possible to require a seizure to remain confidential? Are there any restrictions on confidentiality?	
16	May your country ask another country, international organisation or a private party for assistance with a digital forensic examination?	
17	Are there any time limits for the examination of electronic evidence?	
	The Prosecution and the Defendant's Rights	
18	What must the prosecution do to establish that electronic evidence has been properly stored and not altered (chain of custody)?	
19	What must the prosecution do to establish that the electronic search has been properly conducted?	
20	What must the prosecution do to establish that the forensic examination has been properly conducted?	
21	What must the prosecution prove for electronic data to be admitted in evidence? For example, the prosecution may be asked to prove that the data was not altered by the prosecution after the seizure.	
22	May the defence examine the prosecution's electronic evidence? Does it examine the original or a copy?	
23	May the defendant or a representative be present during the electronic search?	
24	May the defendant or a representative be present during the imaging of the data?	
25	May the defendant or a representative be present during the forensic analysis?	
26	Is the defence entitled to receive an electronic copy of the electronic evidence to prepare its case?	
27	Is the prosecution required to return equipment or data to the owner, including the defendant? If yes, may the prosecution return a copy of the data, not the original?	

28	Do the answers to the three previous questions change if material held on the computer is illegal to possess (e.g. images of child sexual abuse)?	
29	Defendants may object to the prosecution's electronic evidence. Please list any defence objections that the group should discuss.	
	Electronic Data and the Courts	
30	Does your country have any experience using electronic evidence in court?	
31	If you are aware of problems with using electronic evidence, please list any that the group should discuss. For example, courts may order electronic evidence to be printed out and submitted on paper.	
32	Do courts have the equipment to view and use electronic evidence?	
33	Do courts have experience with electronic forensic analysis?	
	a. If yes, please list any problems that the group should discuss. For example, a court may set a deadline for the analysis that is too short to permit a proper examination.	
34	Do courts make rules for the prosecution about how data may be searched? For example, a court may order that the prosecution may only search for certain words, or may only search in certain areas of a seized drive.	
35	Is it a legal requirement in your country that electronic evidence is introduced by an "expert witness"?	
36	If there is no legal requirement that electronic evidence is introduced by an expert witness, in what circumstances must a witness be called to introduce or authenticate electronic evidence?	
	Assets Held in Electronic Form	
37	Is it possible to use in evidence, assets held in electronic form? If yes, what is the legal basis?	
38	If assets held in electronic form are identified, is the prosecution required to return either the original or a copy of the electronic evidence to the defendant?	

39	Is it routine/expected that an examination of electronic evidence would search for assets held in electronic form (e.g. virtual currency wallets)?	
	Obtaining Electronic Evidence from Third Parties (people, companies, and organizations that are not targets or defendants)	
40	Is it possible to obtain electronic evidence from third parties? If yes, what is the legal basis?	
	b. If yes, are all types of electronic evidence held by third parties obtained in the same way?	
	a. According to your country's law and practice, is it possible to obtain data from third parties by cooperation and collaboration, or are all procedures coercive? For example, if a third party is willing to turn over data from its system, may you collaborate to search the system, or must you execute a seizure?	
41	If data is obtained from third parties, or with their assistance, can they be required to keep the matter confidential?	
42	If a private person reports a crime where electronic evidence in involved, what procedures does law enforcement follow to preserve or obtain the person's data?	
	International Issues	
43	If electronic evidence is obtained from another country, are there special rules for authenticating the evidence?	
44	Have there been cases where such evidence has been declared inadmissible by courts in your country? If yes, please provide details.	
	Additional Questions	
45	It is important to obtain views on the use of electronic evidence from different participants in the criminal justice system. Are there any improvements that can be made to the use of electronic evidence in criminal and civil cases, and, if yes, what are those improvements? Please seek comments on both legal and practical aspects from the categories of participants below, if possible.	
	a) Comments from Prosecutors	

	b) Comments from Law Enforcement Crime Investigators (This may include cybercrime, financial crime and traditional crime investigators who encounter electronic evidence.)	
	c) Comments from Law Enforcement Digital Forensics Investigators	
	d) Comments from Judges	
	e) Comments from Defence Attorneys	
	f) Other Comments	