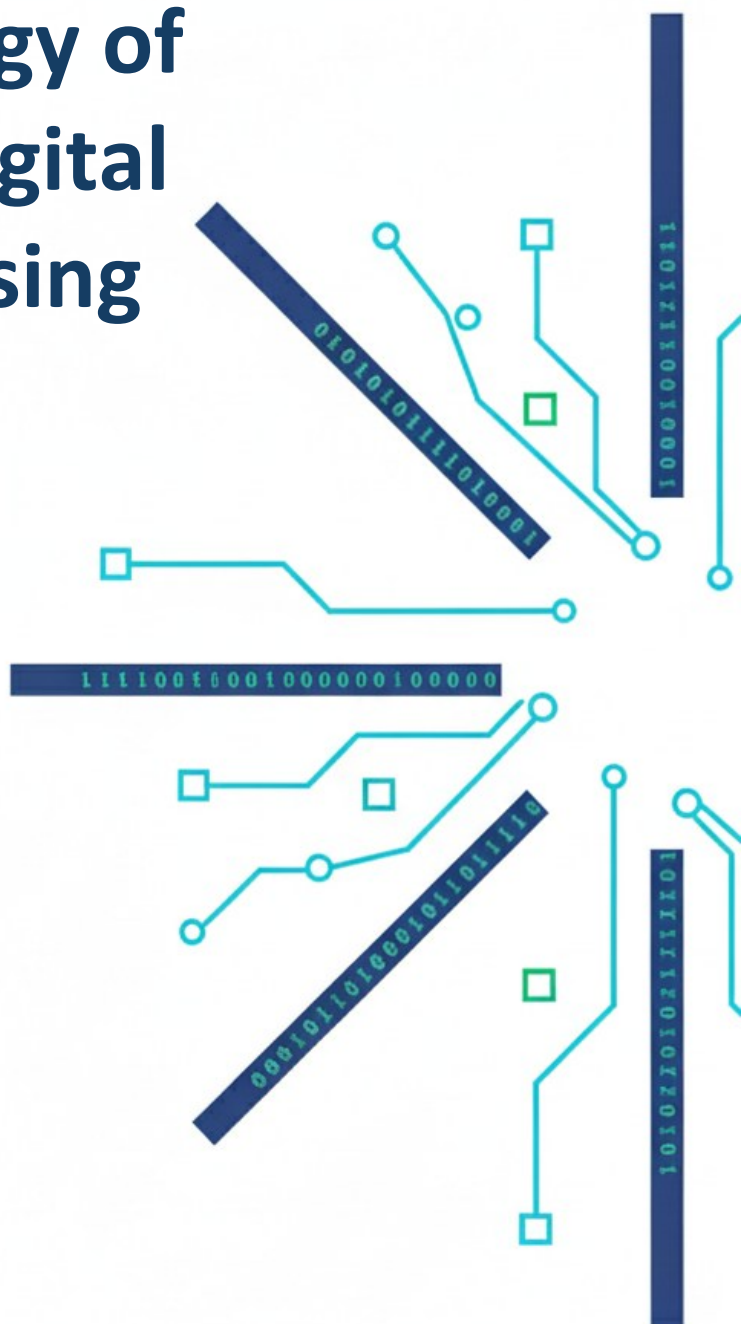


D3 – Methodology of Procedure for Digital Evidence Processing



The Automation of Digital Forensic and Incident Response (ADFIR) project is funded by the European Union – NextGenerationEU through the Recovery and Resilience Plan of the Slovak Republic under project No. 09I05-03-V02-00079.

Contents

1 Project Description	3
2 Introduction	4
3 Task KPB1.3.....	4
3.1 Basic Principles.....	5
3.2 Principles governing the collection, preservation and interpretation of digital evidence 9	
3.2.1. Identification of the necessary (reasonable) scope of the investigation.	9
3.2.2. Acquisition of a sufficient amount of relevant information	10
3.2.3. Record-keeping and chain of custody, transparency, verifiability and credibility .	12
3.2.4. Impartiality and objectivity	14
3.2.5. Risk analysis, tactics, professionalism	14
3.3 Stages of digital analysis.....	16
3.3.1. Identification of digital information	16
3.3.2. Data collection.....	17
3.3.3. Data retention	17
3.3.4. Verification of data and procedures	18
3.3.5. Data analysis and interpretation	19

1 Project Description

The project 'Automation of Digital Forensic and Incident Response' (hereinafter 'ADFIR') is funded by the European Union – Next Generation EU through the Recovery and Resilience Plan of the Slovak Republic under project number 09I05-03-V02-00079. This project addresses one of the key challenges in the field of cyber security and information security – how to process the vast amount of digital evidence generated during cyber security incidents or forensic investigations. At present, this process is very demanding in terms of human resources and time. Automation using machine learning methods can therefore significantly improve the quality of digital forensic analysis and reduce the time required to carry it out. Overall, this enables security teams to respond more effectively to cyber threats. The main benefits of this project are:

- **Faster resolution of cyber security incidents.** The ADFIR project introduces automated approaches to the collection, processing and analysis of digital traces. This enables security teams to identify the causes of incidents more quickly and take effective measures to resolve them.
- **Reduced workload for forensic analysts.** Routine and time-consuming tasks associated with processing digital traces will be replaced by automated methods. This will allow analysts to focus on more complex cases and strategic decision-making.
- **Higher quality and consistency of outputs.** The use of standardised methodologies and tools ensures that processed digital evidence will be more accurate, consistent and easier to verify. This significantly reduces the risk of errors caused by human factors.
- **Potential use in criminal proceedings.** The project's outputs will be developed in accordance with legal requirements and standards, enabling digital traces to be accepted as relevant evidence for investigations and court proceedings.

2 Introduction

The aim of work package KPB1 is **to analyse and address the legal issues relating to the proposed project**. This work package defines the minimum standards and legal safeguards necessary to ensure the application of the legal framework for the protection of personal data when processing digital evidence and the admissibility of the outputs of automated forensic analysis as evidence in criminal proceedings, whilst taking into account ethical, legal aspects, as well as issues of legitimacy and proportionality relating to the extraction of digital evidence using machine learning. The characteristics of digital evidence (integrity, authenticity, admissibility and relevance) are also the subject of examination.

Given the absence of provisions that would comprehensively address the issue of standards for securing digital evidence, the aforementioned methodology establishes a minimum documentation standard to ensure that the analysis of digital traces is admissible as evidence, regardless of whether they were processed manually by an expert, automatically based on an algorithm, or using machine learning. The concept of evidence in criminal proceedings constitutes a legally regulated process involving the parties to criminal proceedings (law enforcement agencies, the court, the defendant, the victim, interested parties, etc.).

3 Task KPB1.3

Task KPB1.3 – Analysis of the conditions for the admissibility of processed digital evidence as evidence in criminal proceedings. Ethical guidelines for the acquisition of digital evidence based on machine learning. Cyber defence tactics in relation to forensic investigation and the recovery of digital evidence, including the use and admissibility of automated analysis (EISI).

Digital traces may include a wide range of different information with evidential value, stored or transmitted in digital form.¹ Specific information contained in digital traces may be subject to legal protection under various legal provisions. If digital traces are to be examined and processed by authorities or other bodies² for the purposes of criminal proceedings, they must

¹ Scientific Working Group on Digital Evidence (SWGDE). *Digital Evidence: Standards and Principles*. In *Forensic Science Communications*. 2000, No. 2. Available: <https://archives.fbi.gov/archives/about-us/lab/forensic-sciencecommunications/fsc/april2000/swgde.htm#Introduction>

² As Dražová notes, “*Within the scope of their remit, various entities outside criminal proceedings also routinely deal with the seizure of data as potential electronic evidence, for example national or government cyber security incident response teams, public authorities for the purposes of civil or administrative proceedings, digital investigation teams operating in the commercial sector, and so on.*” Dražová, P. Electronic evidence in criminal proceedings. Dissertation thesis, 2021. Available:

comply not only with specific applicable regulations but also with the procedural rules of criminal proceedings. In the following chapters, we outline the necessary steps that must be taken to enable the further use of digital evidence in criminal proceedings.

The following chapters discuss:

- Basic Principles
- Principles of the collection, preservation and interpretation of digital evidence
- Stages of digital analyses

3.1 Basic Principles

The taking of evidence constitutes a key and indispensable component of criminal proceedings, as it is on the basis of the results of the evidence gathered that the court decides on the guilt or innocence of a person charged with a criminal offence. The concept of the taking of evidence refers to a procedure governed by law involving the parties to criminal proceedings (law enforcement agencies, the court, the accused, the victim, interested parties, etc.), the purpose of which is to seek out, secure, present and evaluate information relevant to establishing the factual circumstances on the basis of which decisions are made in criminal proceedings, in particular regarding the accused's guilt and sentence, but also regarding other legally relevant facts (e.g. the victim's claim for damages).³

Given the absence of provisions that would comprehensively address the issue of standards for the securing of digital evidence, it is necessary to make several systemic observations regarding the procedure and minimum standards to ensure that the analysis of digital evidence is admissible as evidence regardless of whether they were processed manually by an expert, automatically using an algorithm, or using machine learning.

Digital evidence encompasses a wide range of data originating from electronic devices, or secured remotely without physical possession or control of the device or data storage medium. **The purpose and principle of digital evidence analysis is to search for and evaluate digital information as evidence.**

<https://opac.crzp.sk/?fn=detailBiblioFormChildA52T&sid=4BD9478A3A7038F60D223DAC8853&seo=CRZP-detail-kniha>

³ ČENTĚŠ, J. et al.: Criminal Procedure Law. General Part. Šamorín: Heuréka, 2016, p. 328.

Compared with other types of forensic evidence, digital traces are characterised by specific properties, namely:

- the intangible nature of digital traces,
- the latent nature of digital traces,
- the traceability of digital traces over time,
- the high information density of digital traces,
- the very short lifespan of digital evidence,
- the preservation and quality of digital traces are influenced by many subjective factors,
- the large volume of data in digital traces,
- the data density of digital traces is constantly decreasing over time and with the development of new technologies,
- the extreme dynamism of the digital footprint environment,
- the heterogeneity and complexity of the digital footprint environment,
- the vast geographical extent of the area containing digital traces,
- a high level of data protection complicates or prevents work with digital traces,
- digital traces can be automatically identified and processed using specialised tools,
- the high level of digital evidence obfuscation by skilled perpetrators,
- the recoverability of destroyed digital traces,
- the authenticity of digital traces,
- the low level of acceptance of digital traces by the courts and law enforcement agencies.⁴

Digital traces may take the form of physical traces (originating from devices designed for the processing, storage or transmission of data, such as a computer's hard drive or a memory card,

⁴ Ibid.

but in a broader sense also a computer, printer, etc.), data traces (derived from various databases, recipients and files) or traces derived from metadata (metadata is essentially data about data, i.e. related information concerning the date and time of a file's creation, the date of its modification, the file owner, file size, etc.)

Physical and digital objects only become evidence once they have been accepted by the criminal justice authorities or the court. The key issue is therefore the verifiability of the axiom that the digital trace was located at a specific place and that, during the process from its seizure to the completion of the expert examination, it was not modified in any way. For this reason, a duplicate of the digital trace is used; this is an exact digital reproduction of all data objects found on the original physical object, created on a physically identical type of data storage medium.⁵ The data volume and information content of all data objects are in a 1:1 ratio between the original and the duplicate. Duplicates of digital traces are created for the purposes of expert evidence, so that the original material can be submitted at any time for re-examination by another expert (note: this will most often be the case where the accused commissions an expert report), if the physical object itself (for example, a computer) cannot be seized for various reasons. In practice, in the case of computers, a disk *image* is commonly created, which is a faithful duplicate of the disk's contents—that is, a mirror of its original contents stored in digital form.⁶

Digital forensic analysis involves the examination of traces related to information and communication technologies for the purpose of using them as electronic evidence in criminal proceedings. It comes into play after a law enforcement agency or a court has concluded that, in order to prove the facts in accordance with Section 119 of the Criminal Procedure Code, it will be necessary to obtain a certain volume of data which, provided certain criteria are met, may take on the nature of electronic evidence.

Electronic evidence should therefore meet the following conditions:

- lawfulness (the evidence must be obtained in the manner prescribed by law),
- authenticity (genuineness; there must be a causal link between the evidence and the facts),
- integrity (the evidence must be complete and unaltered),

⁵ SMEJKAL, V.: Current Approaches to Combating Cybercrime. In *Data Security Management*. 2016, No. 4, pp. 18–23.

⁶ PORADA, V., RAK, R.: Digital Traces in Criminalistics and Forensic Sciences. In Forensic Engineering. 2006, No. 17, pp. 3–23.

- reliability (the method of obtaining and handling the evidence must under no circumstances give rise to reasonable doubt as to the authenticity and credibility of the evidence),
- credibility (only evidence obtained in the manner prescribed by law, and in respect of which there are no reasonable doubts as to its authenticity, integrity and reliability, may be regarded as credible evidence).

The procedures outlined in this methodology are intended to ensure that, when followed, a digital trace can be considered evidence and evaluated as such. However, for this methodology to serve its purpose and for the secured digital traces to be considered evidence, it is first and foremost necessary to meet the fundamental requirement of the lawful acquisition of digital traces; pursuant to Section 119(2) of Act No. 301/2005 Coll. the Criminal Procedure Code, as amended (hereinafter “CPC”), *anything that may contribute to the proper clarification of a case and that was obtained from means of evidence pursuant to this Act or pursuant to a special Act may serve as evidence*. In light of the above, digital traces may be secured under various legal regimes, not only under the regime for securing digital evidence by law enforcement authorities and courts pursuant to the CPC.

One possibility is a lawyer acting in the procedural capacity of a defense counsel, an agent of the injured party, or a guardian of an injured person with limited legal capacity, if the person’s legal representative is unable to exercise their rights, since, pursuant to Section 2(10) of the Criminal Procedure Code, the parties also have the right to obtain evidence (general enabling clause). According to Section 7(1) of the Rules of Professional Conduct for Attorneys, *an attorney has the right to seek out and obtain evidence (witnesses, documents, expert opinions, etc.), and to ascertain the factual circumstances of the case; however, he or she must not influence witnesses or alter or distort the evidence and facts ascertained. A lawyer may prepare a written record of the established facts and have it signed by the witnesses. With the consent of the persons concerned, a lawyer may also make an audio, video, or audio-visual recording of the established facts, provided that it is used in accordance with the law and the lawyer’s duty of professional confidentiality is observed. A lawyer may also seek out witnesses and gather evidence and facts regarding a case through third parties*.

Another case involves an entity providing legal services to an essential service operator under Act No. 69/2018 Coll. on Cybersecurity, as amended (hereinafter “ZKB”); one of the essential obligations of an essential service operator under Section 19(6)(d) of the Cybersecurity Act is to secure evidence or means of proof at the time of a cybersecurity incident so that it may be used in criminal proceedings. For these purposes, it is particularly necessary to follow the aforementioned methodology, as the law establishes a legal obligation to act in such a way that the digital traces of a cybersecurity incident secured are admissible as evidence in criminal proceedings; however, it does not specify the procedure by which an essential service provider must proceed to fulfill this legal obligation.

Another possible legal framework for securing digital evidence is the case of a service provider's legal representative under Section 4 of Act No. 329/2025 Coll. on Certain Administrative Measures Related to the Collection of Electronic Evidence in Criminal Proceedings, which transposes Directive (EU) 2023/1544, which establishes harmonized rules for the designation of designated establishments and the appointment of legal

In other situations under the provisions of Section 135a of Act No. 513/1991 Coll. Commercial Code, as amended, where executive officers are required to perform their duties with professional care and in accordance with the interests of the company and all its shareholders, or pursuant to Section 82 of Act No. 311/2001 Coll. Labor Code, as amended, when performing the duties of senior executives.

3.2 Principles governing the collection, preservation and interpretation of digital evidence

In most legal systems and organisations, digital evidence is governed by three fundamental principles: relevance⁷, reliability⁸ and sufficiency⁹. Given the lack of uniform standards and definitions, we have decided to follow the technical standards and guidelines set out in ISO 27037 – Guidelines for the identification, collection, acquisition and preservation of digital evidence¹⁰, as the key elements ensuring the credibility of an investigation are the methodologies applied during the process¹¹, without focusing on specific tools or methods as well as the method of identification, collection, and analysis, which may be performed manually by a qualified person, automatically using algorithms, or using machine learning. It is therefore necessary to adhere to certain principles when acquiring digital evidence:

3.2.1. Identification of the necessary (reasonable) scope of the investigation.

The identification process involves searching for available storage locations and addresses that contain potential information about the object being sought, which should be necessary to achieve the objective. This process also involves prioritising the collection of information

⁷ Relevance is understood to mean the value of information for an investigation, which constitutes the reason for its collection, as set out in the ISO-EIC 27037 standard, p. 6.

⁸ The attribute of consistent results and expected procedures: ISO EIC 27037, Terms and Definitions, 3.15

⁹ Information justifying the conclusion that sufficient material has been gathered to carry out an analysis leading to reasoned conclusions. ISO-EIC 27037, p. 6

¹⁰ Published in 2012

¹¹ ISO EIC 27037, Introduction

based on its volatility¹², which may prevent its loss or minimise damage, with the aim of obtaining the best and most authentic information, including metadata and system data.¹³

The correct identification and prioritisation of information relating to the subject under investigation should lead to the selection of only relevant information. The identification of relevant information should be viewed as a mapping exercise rather than a simple search, as the proper documentation of the identification of relevant information will also be used in subsequent steps.

The necessary and appropriate scope may be:

- temporal (the relevant period under investigation), or
- content-based (searching by key attributes)
- personal (the analysis should not cover the collection of information on individuals outside the scope of the assignment; if it does, this relationship should be clear and comprehensible – e.g. a partner, a person living in the same household, etc.);¹⁴

In the case of an automated identification algorithm, the person using it must be able to document and explain the basis on which and the reasons why the algorithm arrived at the identified scope. This also applies to the automated identification of digital traces using machine learning, so that these procedures are verifiable and transparent. It is therefore not acceptable, for example, to consider the machine learning procedures used to identify digital traces as a trade secret of the entity that performed the identification or provided the application or software containing these elements.¹⁵

3.2.2. Acquisition of a sufficient amount of relevant information

For a better understanding, it should be noted that ISO 27037 distinguishes between the collection and the acquisition of digital evidence:

¹² ISO EIC 27037, p. 8.

¹³ ISO-EIC 27037, p. 8.

¹⁴ Berkeley Protocol on Digital Open Source Investigations; A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law; Human Rights Centre and UN Office of the High Commissioner for Human Rights; New York and Geneva, 2022, eISBN: 978-92-1-005343-3, p. 13, available on 10 March 2026 at: <https://www.ohchr.org/en/publications/policy-and-methodological-publications/berkeley-protocol-digital-open-source>

¹⁵ US DOJ vs. Sterlingov, Misty Fog, available on 29.08.2026 na: <https://caselaw.findlaw.com/court/us-dis-crt-dis-col/115886148.html>

- collection refers to the physical gathering or removal of physical objects containing potential digital evidence, and
- acquisition means creating a copy of data from a specified file (the result is a copy of digital evidence)¹⁶

We will adhere to this terminology and continue to use the term ‘acquisition’, as the subject of digital analysis is the acquisition of digital data, not physical devices.

Obtaining a sufficient amount of information means that enough material has been gathered to carry out a proper digital analysis and to provide a reasoned answer to the questions posed or the facts established. An expert conducting a digital analysis should be able to state how much material was taken into account and collected in total, and what procedures were used to determine how much and what kind of material was sought for the purposes of the analysis, including the use of an automated data collection system employing algorithms or machine learning methods.

When obtaining relevant information during a digital analysis, a hash¹⁷ should be *used* to preserve the integrity and original state of the information at the time¹⁸, so that it is not possible to alter the evidence after it has been obtained.¹⁹

¹⁶ ISO EIC 27037, Terms and definitions, p. 2

¹⁷ A string of bits that is the output of a hash function. In: ISO EIC 27037, Terms and definitions

¹⁸ See also the Berkeley Protocol on Digital Open Source Investigations; A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law; Human Rights Centre and the Office of the UN High Commissioner for Human Rights; New York and Geneva, 2022, eISBN: 978-92-1-005343-3, p. 58, available on 10 March 2026 at: <https://www.ohchr.org/en/publications/policy-and-methodological-publications/berkeley-protocol-digital-open-source>

¹⁹ ISO-EIC 27037, p. 9

3.2.3. Record-keeping and chain of custody, transparency, verifiability and credibility

Providing accurate data and records regarding the use of the data storage medium, as well as identifying the person who used that medium, is essential for the ability to retrospectively review²⁰ digital analysis and its admissibility as evidence in criminal proceedings.²¹

The principle of record-keeping also requires that the analysis specify the particular tools²² used for the acquisition, recovery or retrieval of information. The purpose is to document the entire procedure and the tools used for any subsequent review and to ensure verifiability. The principle of record-keeping also requires, where the analysis is carried out by more than one person, documentation of the scope of these persons' actions and the manner in which information and tasks were handed over at the time.²³

The verifiability and evaluation of a digital analysis are not possible without basic data on the period (when the analysis was carried out), the locations and sources used in the analysis, and the time-stamping of the information obtained. This is necessary in particular because the digital analysis itself may be used as evidence even a considerable time after it was carried out, by which time certain tools used at the time of processing may no longer be functional, or a particular provider (particularly a social network) may no longer support the functionality in question, either publicly or at all.²⁴ At the same time, the very concept of auditability, in

²⁰ Traceability in accordance with ISO 27037, p. 7, also means that at any point during the conduct of a digital analysis, or subsequently during its evaluation, it is possible (e.g. for a third party) to go back and repeat the process of obtaining relevant information for the digital analysis, provided that the specified sources are available.

²¹ Berkeley Protocol on Digital Open Source Investigations; A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law; Human Rights Centre and UN Office of the High Commissioner for Human Rights; New York and Geneva, 2022, eISBN: 978-92-1-005343-3, pp. 11–12, 15, available on 10 March 2026 at: <https://www.ohchr.org/en/publications/policy-and-methodological-publications/berkeley-protocol-digital-open-source>

²² A fundamental prerequisite is the use of licensed tools and procedures that do not infringe intellectual property rights. An open question arises regarding the use of free versions of forensic tools that are available for a limited time, or for a limited number of operations, or with limited functionality. This in itself does not pose a problem, provided that the procedure can be retrospectively verified using that free version and its use does not affect the reliability of the conclusions.

²³ ISO 27037, pp. 10–11.

²⁴ Open source investigations in the age of Google / editors, Henrietta Wilson, SOAS University of London, UK & King's College London, UK, Olamide Samuel, University of Leicester, UK, Dan Plesch, SOAS University of London, UK. Description: New Jersey: World Scientific, [2024] | Series: Security science and technology, 2059–1063; Vol. 4, p. 47

conjunction with the justification and identification of relevant information for digital analysis, has a direct bearing on the credibility and reliability of the digital analysis itself.²⁵

The chain of custody in identifying and acquiring a sufficient amount of relevant information is, in essence, chronological documentation consisting of records of individuals' access to and activities concerning this digital evidence at each stage, as outlined above and as will be discussed below.

ISO standards do not specify how long these records should be retained. Logically, they should be retained for the same period as the digital analysis itself, particularly where it is anticipated that such digital analysis will also be shared with other judicial or investigative authorities as evidence.²⁶ In principle, it can be stated that the retention period for this documentation is also determined by the specific record-keeping periods for the particular state authority acting as the record-keeper²⁷, which are laid down in the relevant ministerial record-keeping regulations.²⁸ For the sake of completeness, we would add that the retention of this documentation must also be examined in light of the nature of the information, e.g. accounting documentation²⁹ or medical records.³⁰ For general information, we note that Act No. 382/2004 Coll. on experts, interpreters and translators and on amendments to certain acts, as amended, stipulates in Section 17(10) that an expert is obliged to retain an expert report for 10 years.

²⁵ ISO 27037, p. 6.

²⁶ ISO EIC 27037, p. 10.

²⁷ Section 16 of Act No. 392/2002 Coll. on archives and records management and amending certain acts, as amended.

²⁸ Section 17 of Act No. 392/2002 Coll. on archives and records management and amending certain Acts, as amended.

²⁹ Section 35(1) and (2) of Act No. 431/2002 Coll. on Accounting, as amended; Section 76 of Act No. 222/2004 Coll. on Value Added Tax, as amended

³⁰ Section 22(2), (4) to (5) of the Act on Healthcare, Services Related to the Provision of Healthcare and on Amendments to Certain Acts, as amended.

3.2.4. Impartiality and objectivity

As with any other search for evidence, a person searching for and assessing digital evidence must approach it impartially and objectively, without any conflict of interest³¹, which must not only not exist, but must not even appear to exist – the so-called ‘appearance theory’.³²

In light of the above, it is essential that a digital analysis includes a justification if a particular source of information or medium has not been used or taken into account. In conjunction with record-keeping and the chain of custody, the requirement for impartiality and objectivity in digital analysis should be guaranteed by the person responsible for the overall digital analysis.

3.2.5. Risk analysis, tactics, professionalism³³

All persons involved are responsible for ensuring the security of the chosen forensic procedures—which should be tested before being applied to a real-world case—³⁴, and the persons concerned; this responsibility does not rest solely with the expert, forensic technician or specialist involved in the digital analysis. The professionalism of those involved in digital

³¹ Berkeley Protocol on Digital Open Source Investigations; A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law; Human Rights Centre and UN Office of the High Commissioner for Human Rights; New York and Geneva, 2022, eISBN: 978-92-1-005343-3, pp. 12, 15, available on 10 March 2026 at: <https://www.ohchr.org/en/publications/policy-and-methodological-publications/berkeley-protocol-digital-open-source>

³² ECHR judgment in the case of PARLOV-TKALČIĆ v. Croatia, No. 24810/06, para. 86, available on 11 June 2026 at: [https://hudoc.echr.coe.int/eng#{%22itemid%22:\[%22001-96426%22\]}](https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-96426%22]}); ECHR judgment in the case of MOISEYEV v. RUSSIA, no. 62936/00, para. 184, available on 11 June 2026 at: [https://hudoc.echr.coe.int/eng#{%22itemid%22:\[%22001-88780%22\]}](https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-88780%22]}); ECtHR judgment in the case of ŞAHİNER v. TURKEY, no. 29279/95, para. 44, available on 11 June 2026 at: [https://hudoc.echr.coe.int/eng#{%22itemid%22:\[%22001-59666%22\]}](https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-59666%22]}); ECHR judgment in the case of KYPRIANOU v. CYPRUS, no. 73797/01, para. 118, available on 11 June 2026 at: [https://hudoc.echr.coe.int/eng#{%22itemid%22:\[%22001-71671%22\]}](https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-71671%22]}); ECHR judgment in the case of MIKHAIL MIRONOV v. Russia, no. 58138/09, para. 36, available on 11 June 2026 at: [https://hudoc.echr.coe.int/eng#{%22itemid%22:\[%22001-204834%22\]}](https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-204834%22]}); ECHR judgment in the case of KHODORKOVSKIY and LEBEDEV v. RUSSIA, nos. 51111/07 and 42757/07, para. 430, available on 11 June 2026 at: [https://hudoc.echr.coe.int/eng#{%22itemid%22:\[%22001-200333%22\]}](https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-200333%22]})

³³ Berkeley Protocol on Digital Open Source Investigations; A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law; Human Rights Centre and the Office of the United Nations High Commissioner for Human Rights; New York and Geneva, 2022, eISBN: 978-92-1-005343-3, p. 44, available on 10 March 2026 at: <https://www.ohchr.org/en/publications/policy-and-methodological-publications/berkeley-protocol-digital-open-source>

³⁴ ISO EIC 27037, p. 6

analysis stems from their prudence, knowledge and skills.³⁵ To this end, it is necessary to adopt measures relating to infrastructure, including hardware, software and networks involved in digital forensics, and measures relating to the conduct of persons who are involved to some extent in the digital forensics process, including law enforcement agencies and operational units.

A risk analysis, carried out prior to the investigation itself, as well as the tactics and planning of digital analysis, should take into account all types of risks, including technological, financial, legal, physical and psychosocial risks. A risk analysis of the use of digital procedures must address, in particular, issues relating to the proportionality of seizing entire storage media and devices, the copying of digital information and the scope of such copying. They should keep their professional activities separate from their personal online activities. Personal devices should not be used for professional digital forensics, and professional devices should never be used for personal activities. General security requirements for devices on which a person will carry out digital analysis should be governed by the cyber security principles set out in ISO 27001, in particular by implementing appropriate measures at entry points and access points³⁶, including the physical security of offices, rooms and facilities,³⁷ in particular monitoring to prevent unauthorised physical access³⁸ and eavesdropping³⁹ including the lifecycle of storage media during their acquisition, use, transport and disposal, and the requirements for their handling⁴⁰. In principle, it can be summarised that provided the aforementioned entity, department, or laboratory is certified to ISO 27001, or meets the requirements of ISO 27001, then the basic requirements for digital forensics as set out above, or as defined in ISO 27037 and ISO 27042, are also met.

The identification of vulnerabilities and their severity influences the very understanding of risks in the digital analysis process, which relate to the infrastructure and connectivity themselves, the equipment and storage used, reputational risks, as well as the personal safety of individuals.

³⁵ Annex A to ISO EIC 27037: During the information identification process, the professional is able to define information that may assist in an investigation, as well as the legal provisions relating to the handling of potential evidence from OSINT. They specify the requirements for the tools needed to collect and acquire data and equipment, and carry out a risk assessment. During the acquisition phase, they are able to apply requirements to ensure repeatability and auditability.

³⁶ Clause 7.2. Physical access ISO 27001

³⁷ Clause 7.3. Physical Access – ISO 27001

³⁸ Clauses 7.4 and 7.12: Physical access – ISO 27001

³⁹ Clause 7.10. Physical Access – ISO 27001

⁴⁰ Clauses 7.6 and 7.13: Physical Access – ISO 27001

Where it is determined that the data under investigation requires anonymisation, the next essential step is to ensure that the anonymisation process is carried out in accordance with the applicable data protection legislation.

3.3 Stages of digital analysis

The digital analysis process consists of five stages. These are:⁴¹

3.3.1. Identification of digital information

There are two main approaches to open-ended investigation and searching:⁴²

- searching using general or advanced (active) search methods; queries, algorithms and parameters should be structured precisely and clearly, with a certain degree of creativity when searching through various media. It is necessary to work with various keywords, conjectures and assumptions, even if these have not yet been proven. However, these hypotheses must be based on the investigation carried out and must be justified.
- monitoring (tracking and regular review) of the content of fixed sources; this is a process in which regularly updated, interrelated keywords are used⁴³. As a rule, automated tools are used for the regular monitoring of specific sources, with the aim of supplementing information already known.
- *Preliminary assessment/evaluation of data*; before collecting a sufficient amount of relevant information, it is necessary to evaluate it and document this evaluation. First and foremost, it is necessary to assess the relevance of the information and its contextual data to the investigation in question.⁴⁴ This determination can be particularly problematic in the early stages; however, regardless of this, the expert or

⁴¹ The stages outlined above are also consistent with the technical standards for securing digital evidence set out in ISO 27042, pp. 4–11, and ISO 27037, pp. 6–18, insofar as the prescribed standards can be inferred from the digital analysis documentation; see above.

⁴² Berkeley Protocol on Digital Open Source Investigations; A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law; Human Rights Centre and UN Office of the High Commissioner for Human Rights; New York and Geneva, 2022, eISBN: 978-92-1-005343-3, pp. 55–56, available on 27 March 2026 at: <https://www.ohchr.org/en/publications/policy-and-methodological-publications/berkeley-protocol-digital-open-source>

⁴³ The so-called 'Topic'. (author's note)

⁴⁴ See above

professionally qualified person carrying out the digital analysis should be able to explain why the data is, or should be, relevant to the investigation.

It is also necessary to assess the reliability or authenticity of the data, which involves evaluating metadata, linked information and the original source.

The expert carrying out the digital analysis should also assess the digital information and its storage media from the perspective of whether it is likely that the digital information will be deleted or that access to it will be restricted. The likelihood of content being removed can be assessed on the basis of several factors, including the nature of the medium, the location of the content and the content's compliance with the service provider's terms of use.

3.3.2. Data collection

This is the process described above and encompasses several methods of data acquisition.

3.3.3. Data retention

As a general rule, data is retained to ensure its availability and usability in investigations, so as to preserve its authenticity, availability and traceability.⁴⁵ This is achieved through documentation chaining, the creation of evidential, backup and working copies of data, and hashing.⁴⁶ In order to ensure this, individual pieces of information must be labelled as digital evidence and documented to show who accessed them, when, and what actions were taken with them.⁴⁷ The rule is that the actual analysis and processing of digital information is carried out on working copies, not on originals or evidential copies.⁴⁸ Ensuring the authenticity, availability and traceability of data is generally governed by cybersecurity principles, as set out in ISO 27001. To ensure that stored data complies with the general cybersecurity standards set out in ISO 27001, information stored on, processed by, or accessed via a user's end devices must be protected⁴⁹, in particular through the allocation and use of restricted and controlled

⁴⁵ Berkeley Protocol on Digital Open Source Investigations; A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law; Human Rights Centre and Office of the United Nations High Commissioner for Human Rights; New York and Geneva, 2022, eISBN: 978-92-1-005343-3, p. 61, available on 27 March 2026 at: <https://www.ohchr.org/en/publications/policy-and-methodological-publications/berkeley-protocol-digital-open-source>

⁴⁶ See above.

⁴⁷ ISO EIC 27037, p. 10

⁴⁸ ISO EIC 27037, p. 25

⁴⁹ Clause 8.1. Technical controls in ISO 27001

privileged access rights⁵⁰ and secure authentication technologies and procedures,⁵¹ measures to prevent data leaks,⁵² the creation of backup copies and regular testing in accordance with an agreed specific backup policy,⁵³ the creation, retention, protection and analysis of activity logs, failures and exceptions,⁵⁴ synchronisation of system clocks,⁵⁵ segregation of roles⁵⁶, management of access to external websites,⁵⁷ rules for the effective use of cryptography, including cryptographic key management,⁵⁸ and secure coding practices,⁵⁹ separate and secure development, testing and production environments must be kept separate and secure.⁶⁰

3.3.4. Verification of data and procedures

Data verification is carried out in relation to other sources or media. Generally, when verifying information, the reliability of the source and the verifiability (credibility) of the information are assessed within a 4x4 or 6x6 matrix⁶¹, where A1 is information from a consistently reliable source that is confirmed or verifiable by another source, whilst information in category D4 or F6 comes from a previously unknown source and cannot be verified by any other means.⁶² The certainty (or accuracy) or vagueness of the information is also part of this assessment.⁶³

⁵⁰ Clause 8.2. Technical control under ISO 27001

⁵¹ Clause 8.5. Technical control under ISO 27001

⁵² Clause 8.12. Technical control under ISO 27001

⁵³ Clause 8.13. Technical control under ISO 27001

⁵⁴ Clause 8.15. ISO 27001 Technical Control

⁵⁵ Clause 8.17. ISO 27001 Technical Control

⁵⁶ Clauses 8.20 and 8.22. ISO 27001 technical controls

⁵⁷ Clause 8.23. ISO 27001 technical control

⁵⁸ Clause 8.24. ISO 27001 technical control

⁵⁹ Clause 8.28. ISO 27001 technical control

⁶⁰ Clause 8.31. ISO 27001 Technical Control

⁶¹ NATO AJP-2.1 Source Reliability and Information Credibility Scales, available at: https://cld.pt/dl/download/40e71e02-28d0-4c6e-b2f4-248aebd8ca49/CPOS_HERANCA/Fase%20Conjunta/Anexos/6-AEOM/%28DCM%29%20-%20Joint%20Military%20Doctrine/General%20Bibliographic%20References/AJP-2.1%20EDB%20V1%20E_JUN16.pdf?download=true

⁶² Ibid.

⁶³ Berkeley Protocol on Digital Open Source Investigations; A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law; Human Rights Centre and Office of the UN High Commissioner for Human Rights; New York and Geneva, 2022, eISBN: 978-92-1-005343-3, p. 63, available on 10 March 2026 at: <https://www.ohchr.org/en/publications/policy-and-methodological-publications/berkeley-protocol-digital-open-source>

3.3.5. Data analysis and interpretation

The analysis itself consists of:

- metadata analysis and
- content analysis.

Metadata is data that describes other data and provides information about it. It may be created by the user who created the object in question, by other users, by a communications service provider, or by any device on which the data is created, transmitted, received or viewed. Metadata is important for describing an object and the circumstances of its creation, distribution or modification. Metadata may include the author of the file, its creation date, upload details, modifications, file size and location data. Metadata also includes image formats with supplementary data on cameras, scanners, etc., as well as information on the source code of programmed web pages, which may contain hidden or modified content and reveal the structure of links and broken links.⁶⁴

Content analysis involves, for example, geolocation based on the position of an object, an activity, or the place from which a particular element was created. Such techniques may include, for instance, the identification of unique geographical features in a photograph and their actual location on a map. Further data processing, such as translations or format conversions, may be necessary for the content analysis itself. Any processing of a digital object must be documented (chain of custody).⁶⁵ ⁶⁶ This procedure also involves digital analysis and data extraction as 'preparation' for another professionally qualified person, e.g. an anthropologist, paediatrician, auditor, accountant, linguist, translator, etc.

⁶⁴ Berkeley Protocol on Digital Open Source Investigations; A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law; Human Rights Centre and UN Office of the High Commissioner for Human Rights; New York and Geneva, 2022, eISBN: 978-92-1-005343-3, p. 64

available on 10 March 2026 at: <https://www.ohchr.org/en/publications/policy-and-methodological-publications/berkeley-protocol-digital-open-source>

⁶⁵ See above

⁶⁶ Berkeley Protocol on Digital Open Source Investigations; A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law; Human Rights Centre and Office of the United Nations High Commissioner for Human Rights; New York and Geneva, 2022, eISBN: 978-92-1-005343-3, pp. 65–67

available on 10 March 2026 at: <https://www.ohchr.org/en/publications/policy-and-methodological-publications/berkeley-protocol-digital-open-source>

This is a cycle that may be repeated several times, as new information may come to light. Those carrying out the digital analysis are required to document their activities during each phase.⁶⁷

When analyzing and interpreting digital traces intended for use as evidence in criminal proceedings, the final step must always involve an assessment by a professionally qualified person, even if the analysis is performed automatically using algorithms or machine learning principles and procedures. It is essential that analytical outputs are always verified by a human and, at the same time, explainable, transparent, and verifiable. It is therefore not acceptable, for example, to consider that machine learning procedures used to identify digital traces constitute a trade secret of the entity that performed such identification or provided the application or software containing these elements.⁶⁸

The findings of digital analysis, whether relating to the data collected or to conclusions drawn from that data, may be used as evidence in criminal proceedings, provided that the principles set forth above are observed, through:⁶⁹

- the questioning of a person (orally), including questioning via videoconference. Visualisations of the digital analysis in the form of notes may also be used during questioning.
- or in writing by means of an expert statement or an expert report. A written expert statement or expert report may also include visualisations of the results and procedures involved in carrying out the digital analysis, supplemented by any questioning of a person as referred to in the point above.

From a legal standpoint, it is irrelevant whether the identification, collection, and preservation were performed manually by a qualified person or through automated means. The purpose of the above-mentioned procedures is, in particular, to ensure the

⁶⁷ Berkeley Protocol on Digital Open Source Investigations; A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law; Human Rights Centre and UN Office of the High Commissioner for Human Rights; New York and Geneva, 2022, eISBN: 978-92-1-005343-3, p. 66, available on 10 March 2026 at: <https://www.ohchr.org/en/publications/policy-and-methodological-publications/berkeley-protocol-digital-open-source>

⁶⁸ US DOJ vs. Sterlingov, Misty Fog, available on 29.08.2026 at: <https://caselaw.findlaw.com/court/us-dis-crt-dis-col/115886148.html>

⁶⁹ See the Berkeley Protocol on Digital Open Source Investigations; A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law; Human Rights Centre and UN Office of the High Commissioner for Human Rights; New York and Geneva, 2022, eISBN: 978-92-1-005343-3, p. 82, available on 10 March 2026 at: <https://www.ohchr.org/en/publications/policy-and-methodological-publications/berkeley-protocol-digital-open-source>

legality of acquisition, authenticity, integrity, credibility, the preservation of documentation of the procedure, and the possibility of its subsequent review.

The procedures outlined above ensure that electronic evidence will meet the following conditions:

- Lawfulness - the evidence must be obtained in the manner prescribed by law;
- Authenticity - genuineness; there must be a causal link between the evidence and the facts;
- Integrity - the evidence must be complete and unaltered;
- Reliability - the method of obtaining and handling the evidence must not, under any circumstances, give rise to reasonable doubt regarding the authenticity and credibility of the evidence;
- Credibility - only evidence obtained in a manner prescribed by law may be considered credible, provided there are no reasonable doubts regarding its authenticity, integrity, and reliability).

The application of this methodology will provide the operator of an essential service with a certain degree of legal certainty under Section 19(6)(d) of the ZKB in the process of resolving a cybersecurity incident, so that digital traces from the resolved cybersecurity incident are admissible as evidence in criminal proceedings. For these purposes, it is particularly necessary to follow the aforementioned methodology, as the law establishes a legal obligation to act in such a way that the secured digital traces of a cybersecurity incident are admissible as evidence in criminal proceedings; however, it does not specify the procedure by which the operator of an essential service must proceed to fulfill this legal obligation.