THEORY OF DIGITAL TRACES IN CRIMINALISTICS

JUDr., prof. **Jozef Metenko**,
Akadémia Policajného zboru v Bratislave,
Katedra kriminalistiky a forenzných vied,
Podhajska 197, 90086 Budmerice, Slovakia,
<jmetenko@hotmail.com>

PaedDr. **Miriam Metenkova**,
Kriminalistický a expertízny ústav,
Podhajska 197, 90086 Budmerice, Slovakia,
<miriam.metenkova@gmail.com>

Acknowledgements

Whatever the next path and decisions of Professor Vidmantas Egidijus Kurapka, we would like to thank you here for the furrow that this criminalist has showed not only in the field of Lithuanian Criminalistics. When we thought about how to contribute to this laudation, we had a large field of possibilities that show the breadth of its scope. We chose the Theory digital trace not only because it is one of our predecessors who tried to significantly innovate criminalistics knowledge. We wanted to emphasize the predictive importance of building criminalistics theory, but especially the fact that despite the long-standing theory, the practical level of knowledge and its use is still – with exceptions, behind theory, which should be at the forefront of criminalistics development. So, as followers of the esteemed professor, we have something to do and what to follow in.

Annotation

The authors compare the reality and perspective of the use of digital traces in this study, including a brief characteristic of the digital traces and their theory. In the context of a vision of considerably wider application in criminalistics and forensic research, they point to the possibility of exploiting the digital traces and its content as a new part of classical criminalistics and forensic traces. The basis for this analysis is probably the only first complex work in Slovakia in this area so far, especially the content of its first – theoretical part. The detailed processing of knowledge was carried out as part of the research within the project of the Center of Excellence in Security Research, including three major outputs of dissertants involved in the project. Digital traces are typical of crime related to the misuse of information and communication technologies, which

is also the mistake in opinion of most experts. Unfortunately, according to published research, great deficiencies are also shown in the field of police knowledge of the digital traces. But as reality shows, they are part of virtually every all activity of our present life. The authors in the study distinguish in the traces of criminal activities a number of divisions – many kinds of digital traces. Extensive research during and after the project in research activity 3.3., Center of Excellence of Security Research, ITMS code: 26240120034, co-financed by the Operational Program Research and Development, shows a great diversity of basic features of digital traces.

Keywords: trace, digital trace, criminalistics and forensic examination, research, perspective of digital traces, criminalistics theory of digital trace.

Introduction

At present, there is practically no branch of human activity where we would not encounter electronics objects and its connected digitalized applications. The near future will be characterized by an ever greater and deeper integration of information and communication technologies with other, now common home and office devices[1] (television, telephone, car, refrigerator, etc.).If we analyze the automatic processing of data and information that penetrates everywhere known as internet of things, it is clear the development of modern human society is currently based on the use of new technologies. Technology will surround us at every turn and it will still be honey[2].

On the other hand, it is new and unused or unknown technologies as a means or goal of the activity that often raise doubts as to whether this is a proceeding that is criminal or, for various reasons, punishable or still permitted [3]. The absence of corresponding provisions in criminal law raises and may raise doubts about the criminality of such a procedure, or about the need and possibility of sanctioning such activity otherwise. Knowledge of socially unacceptable processes related to the misuse of communication and information technologies[4] has been the subject of Criminalistics for a long time. In many countries, often under the strong influence of English-speaking IT professionals, it is combined with a forensic approach, as, according to several

1 Meteňko, J., Meteňko, M., Hejda J. (2005). Digital trace. In.: *7th International Symposium on Forensic sciences*. Slovak Republic. 55–79.

2 Rak, R. (2000). *Informatika v kriminalistické a bezpečnostní praxi*. 471.

3 Meteňko, J. *a kol. (2004). Kriminalistické metódy a možnosti kontroly sofistikovanej kriminality*. 26–120.

4 We use in the text CaI.

criminalistics scientists, "criminalistics does not have its own methods of examining trace related to CaI technologies"[5].

In our opinion, this "non-existence of our own methods of criminalistics" was associated primarily with a theoretical and practical shortcoming – the failure to process knowledge about the existence of a traces in general, especially digital trace. The forensic concept of digital recording or digitized object has been used in English-speaking countries for quite some time, a comprehensive concept of the digital trace as a separate type of trace has not yet been developed in criminalistics as full accepted knowledge. Only if we accept the division of all material criminalistics traces into substance traces, field traces and memory traces, presented in last years, we accept this knowledge and evolution including criminalistics. Then, in connection with digital traces, we can talk about one of the groups of field traces, in addition to traces related to electric charge and various forms of radiation. In this study, we will try to analyse the possibilities of examining the digital tracesits concept and its content, as a new part of forensic and criminalistics traces. The basis for this analysis is so far probably the only one comprehensive work in Slovakia in this area, especially the content of its first part[6]. The detailed elaboration was carried out as part of the research of some of the dissertationsas results of this research project[7]. Digital traces are typical of crime related to the misuse of information and communication technologies. The authors in the study distinguish a number of divisions in the residues of criminal activities – many types of digital traces. Extensive research during and after the project in research activity 3.3., Center for Excellence in Security Research, ITMS code: 26240120034, co-financed by the Operational Program Research and Development, shows a great diversity of basic features of digital traces.

Problems of investigation of digital trace

Due to the "long-term" novelty of the issue, we can find attempts to

[5] Kurilovská, L., Svoboda, I., Beňuš, R., Krajníková, M., Masnicová, S., Samek, M., Šišulák, S. (2017). *Kriminalistika*. 1. vyd.

[6] Meteňko, J. a kol. (2004). *Kriminalistické metódy a možnosti kontroly sofistikovanej kriminality*.

[7] Meteňko, M. (2018). Traces in information systems. Dissertation thesis, Informatic and management department of Academy of the Police Force, supervisor doc. RNDr. Ľudmila Gragušová; Mikulaj, D. Možnosti kriminalistickej analýzy digitálnych dát /Possibilities of Criminalistic Analysis of Digital Information. *Policajná teória a prax*, Ročník XIII, 2; Marcinov, P. (2015). *Metódy a postupy vyhľadávania, zaisťovania a skúmania stôp v digitálnom prostredí*. Dissertation thesis, of Academy of the Police Force, supervisor PROF. JUDr. Jozef Meteňko.

characterize the content of digital trace in the monograph, which we characterized as a basic and unsurpassed source for the theory of digital forensic and criminalistics trace. The Czech criminalistics scientists Porada and Rak, who were also co-authors of the monograph, have a significant share in the analysis of the digital trace. One of the significant problems that many forensic scientists pointed out in connection with the digital trace was the fact of relative rigidity to individual identification. Meteňko, J. et al. however, they also point to a solution in the form of the use of metadata, which was later elaborated by their successors into actually used methods enabling individualization in criminalistics research here as well. Data files often contain, in addition to primary content that is expressed through peripherals, such as text, photos, audio, video, and so on, and the so-called metadata that characterizes important information about the file that characterizes it – individualizes it, among other objects. Maybe then e. g. determine when the picture was taken, under what lighting conditions, with what settings and type of digital camera, or even the owner of the device is marked, etc. This information, found on a computer that is in some way related to the crime, can provide essential information for forensic and criminalistics investigations and the processing of their results as well as for police investigations.

Digital trace characteristics

Every technological device that acquires, processes, transmits or stores data leaves records – in terms of forensic those are evidence and off criminalistics those are trace, as reflections on its activities. These records are forensic evidence. According to the classical theory of reflection, a person (or another object or subject related to his activity) triggers, modifies, etc. software, such as its settings, or otherwise controls electronic technology[8]. These activities and the changes caused by them are then reflected in the material environment, inside the technology and out of the environment of the technology[9]. In terms of communication and information crime, the problem of devices working with data is much broader than just computer activity[10]. In some works by renowned Czech

[8] Meteňko, J. *a kol*. (2004). *Kriminalistické metódy a možnosti kontroly sofistikovanej kriminality*.

[9] Shevchuk, V., (2021), Problems of formation and prospect for development of Criminalistic innovation. In: Zachar, Š., Meteňko, J., Meteňková, M., (2021) *Kriminalistika a forenzné vedy: veda, vzdelávanie, prax : 17. medzinárodný kongres*. Zborník príspevkov, 323–338.

[10] Shepitко, V., Shepitко, M. (2021). The formation of digital Criminalistics as a strategic direction for the development of science. In: Zachar, Š., Meteňko, J., Meteňková, M., (2021) *Kriminalistika a forenzné vedy: veda, vzdelávanie, prax : 17. medzinárodný kongres*. Zborník príspevkov, 187–198.

or Slovak authors, we encounter the term computer trace, which is intuitively used rather than factually defined. The concept of computer trace originated in the same period of time as the concept of computer crime, ie approximately in the second half of the 1980s[11]. It is clear that the term "computer" (footprint) is no longer sufficient today, because other electronic devices leave traces that have the same or similar nature, character, general or individual characteristics as a computer trace. There are several very similar definitions in the foreign literature, defining their commonly used term digital evidence – in the meaning of digital evidence. It should be noted that the word "records" has a special meaning when using a computer. For example, if legally purchased software is used to falsify an official document for scanning and subsequently for graphic editing (eg Photoshop). Both the application and the computer work completely by default. The only evidence of an act is a data file with the finished result of the forgery stored on a computer and records that it was processed by the software, at a certain time, by a certain person, etc. However, there was no disruption to functionality or security measures. In English – in relation to forensic practice – the primary meaning is "evidence". We do not find the word "trace" in connection with modern technologies in foreign literature (we can find the meaning of "potential digital evidence", which has a close meaning of the term "trace"). The reason is simple and pragmatically based – foreign theory and practice are strongly oriented to the outcome of the criminal process, t. j. the trace must be acceptable to the court[12]. Therefore, in the perception and subsequent use of terms in English, there is an automatic identification of the terms trace and evidence (English evidence). Today, it is most often used in foreign literature, and it can be said that even the widest circle of forensic specialists accepted the definition, which was proposed in 1999 by the working group SWGDE – Scientific Working Group on Digital Evidence. Digital evidence / evidence is any information with informative value, stored or transmitted in digital form. Another definition showing the development of the term is from the lecture of its author in 2011: A digital trace can be defined as any information that is stored or transmitted in digital form and that is related to the investigated event and can be secured, fixed and decoded by current forensic or technical means and methods. Our concept is more criminalistically oriented, in terms of the priority of the concept of criminalistics trace: forensic trace: A

[11] Porada, V. (1987). *Teorie kriminalistických stop a identifikace. Technické a biomechanické aspekty.*

[12] Olber, P. (2011). The impct of computer Forensic on Polish criminal procedure development.. In: Zachar, Š., Meteňko, J., Meteňková, M., (2021) *Kriminalistika a forenzné vedy: veda, vzdelávanie, prax : 17. medzinárodný kongres.* Zborník príspevkov, 158–167.

digital trace is any change in a digitized environment, characterizing any information related to a criminalistics relevant event that is searchable by criminalistics informatics methods, is available, stored, or transmitted in digital form.[13] This definition is open to any digital technology. The digital trace defined in this way covers both the area of computers soft and hardwareand computer communication, as well as the area of digital transmissions (mobile phones, but also digital TV in the future, etc.), videos, audio, digital photographs, camera data (CCTV) systems, electronic security data. systems, and any other technologies potentially associated with Hi-tech crime. The digital trace must be usable not only for crime control, forensics, but also for general forensic investigations conducted by state authorities (civil disputes, commercial laws, etc.), but also for the needs of the commercial base, for the needs of independent internal or external audits and under[14]. To a similar extent, we define the digital trace even today. In connection with digital traces, other processes and entities are defined, which are logically connected with digital traces and are important for the whole further process of working with digital traces[15]:

- securing digital traces,
- data objects,
- physical objects,
- digital trace originals,
- duplicate digital trace,
- a copy of a digital trace.

Criminalistics processes and objects limiting the study of digital traces

Digital trace processes are the process that begins when information or devices are identified or found as stored or registered for screening and peer review. The detention process must be adequate for the knowledge of criminalistics and other sciences and legal in relation to the work with evidence in the given legal system (state or other legally defined territory). Physical and data objects become evidence only if they are acceptable to law enforcement authorities. Data objects are non-material material objects or information with a credible informative value, while they are associated with tangible elements of

13 Meteňko, J. *a kol*. (2004). *Kriminalistické metódy a možnosti kontroly sofistikovanej kriminality*.

14 Lall, A., Tohter M., Öpik, R. (2011). Some aspectsof Digital Forensic in the Republic of Estonia.. In: Zachar, Š., Meteňko, J., Meteňková, M., (2021) *Kriminalistika a forenzné vedy: veda, vzdelávanie, prax : 17. medzinárodný kongres*. Zborník príspevkov, 133–146.

15 Meteňko, J. *a kol*. (2004). *Kriminalistické metódy a možnosti kontroly sofistikovanej kriminality*.

substance. Data objects can have different formats, but they can never change the original information. Examples of data objects are databases, directories, files, virtual memory content, digital video or audio recordings, and many other forms. Physical objects (tangible, directly registered by the human senses) are elements – most often carriers on which data objects are stored and through which they are transmitted. In practice, these are computer hard disks, various storage media (floppy disks, CDs and DVDs, memory cards, data tapes, etc.) In a broader sense, they are entire devices (e. g. computers, printers, network components, etc.) in addition to digital traces, other information. Serial numbers, dactyloscopic or mechanical or biological traces and others that prove the logical relationship of the physical device (ownership, user, time, etc.) to its user / perpetrator and the crime or other activity that are the subject of the investigation are especially important for criminology, investigation. Physical objects are often the subject of a generally broader criminalistics interest than just the study of digital traces. As appropriate, all common methods of forensic investigation are used. An original digital trace is a physical or data object that is secured for the needs of expert forensic or forensic research. Original digital traces are the basic evidence. For work purposes, users (perpetrators) or investigating authorities create working duplicates or copies of digital traces from them. The process of their creation is unambiguous and there is no change in the information content. This process is fully reversible, when the basic conditions are met, it is always repeatable with the same results. Users and independent experts then have the material obtained or created by them for further research with the same information value as the original. This guarantees the immutability of the original digital trace as evidence. Because duplication creates a reproduction of all data objects, logical and physical interrelationships are preserved. You can work with the duplicate comfortably, safely and fully. We create duplicates of digital traces mainly for research purposes, so that we can submit the original material (archived, protected) for re-examination or re-examination. This is especially necessary for independent experts in those cases where the physical object itself (company computer) cannot, for various reasons, be directly secured to the work needs of the bodies active in the investigation. In practice in the field of personal computers, the so-called "Image" of discs, which is a faithful duplicate of its content, a kind of mirror of its original content stored in digital form. A copy of a digital trace is an accurate reproduction of information from the original physical object to another, physically

independent data medium[16]. When creating a copy of a digital trace, we create data objects with the same information content, but on a physical medium, which may be of a different type. Not all data objects of the original physical object are necessarily reproduced on the copies, but only some of them are selected. As a result, not all functional and logical links with other data objects may be maintained. We make copies if it is expedient for the purposes of the investigation, e.g. due to the size of the digital track data volume. Copies contain only a portion of the data objects of the original physical object. However, the information value of each copied object does not change from its original[17].

Criminalistic, forensic and otherwise usable digital traces

The human activities, the tools and means used and the objective circumstances of these activities can be very diverse. Digital traces are the result of a whole complex of these factors. When examining digital traces in the first phase, it may not always be clear whether the digital traces correspond to criminal activities, or whether they can be used for forensic investigations of a more general nature, or whether they are common traces that will not normally be investigated as a legitimate offender. So it depends on what we investigate, what we are looking for. In any case, any relevant clues, research hypotheses and working investigative versions should be validated or refuted[18].

Traces – all in the material environment in terms of our subject of research can be divided into three basic categories according to their applicability to different types of research and investigation[19]:

16 Meteňko, J., Meteňko, M., Hejda J. (2005). Digital trace. In.: *7th international symposium on forensic sciences Sep 29th – Oct 1st, 2005*, Slovak Republic. 55–79*;* Meteňko, J., Meteňková, M. (2020). Digital trace and their attributes evaluate for criminalistic. In: *Naukovij visnik Dnipropetrovskogo deržavnogo universitetu vnutrišnich sprav [print, elektronický dokument]: naukovij žurnal. 216–227.*

17 Digital Evidence: Standards and Principles. Report of Scientific Working Group on Digital Evidence (SWGDE) and International Organization on Digital Evidence (IOCE): http://www.fbi.gov/hq/lab/fsc/backissu/april2000/swgde.htm

18 Mikulaj, D. Možnosti kriminalistickej analýzy digitálnych dát /Possibilities of Criminalistic Analysis of Digital Information. *Policajná teória a prax*, Ročník XIII, 2; Olber, P. (2011). The impact of computer Forensic on Polish criminal procedure development.. In: Zachar, Š., Meteňko, J., Meteňková, M., (2021) *Kriminalistika a forenzné vedy: veda, vzdelávanie, prax : 17. medzinárodný kongres.* Zborník príspevkov, 158–167; Shepitко, V., Shepitко, M. (2021). The formation of digital Criminalistics as a strategic direction for the development of science. In: Zachar, Š., Meteňko, J., Meteňková, M., (2021) *Kriminalistika a forenzné vedy: veda, vzdelávanie, prax : 17. medzinárodný kongres*. Zborník príspevkov, 187–198.

19 Meteňko, J. *a kol.* (2004). *Kriminalistické metódy a možnosti kontroly sofistikovanej kriminality.*

Criminalistic traces.

They apply to the investigation of criminal offenses and misdemeanours specified by law. For the needs of forensic (as well as forensic) practice, high quality and objectivity of seized tracks and the process of seizure and research is required. We understand criminalistics traces as a subset of forensic traces.

Forensic traces.

These are generally any clues that can be used for forensic investigations, including investigations by law enforcement agencies. However, unlike the classic criminal investigation, this also includes the investigation of the nature of forensic audits in the civil or commercial sphere. The results of the investigation are prepared in such a way that their quality and formal processing stand up to the judicial authorities. In practice, we encounter cases where a criminal report is filed on the basis of an internal audit or the activities of an independent (non-state) expert institution. The seized evidence (traces) should be handed over by the audit authorities to a law enforcement agency of sufficient, standard quality. Securing the originals of some digital tracks is a unique process. In such a case, other authorities will no longer be able to secure the traces already seized (at all or in the required quality so that they are acceptable).

Other usable traces.

This type of traces reflects all other activities of objects and entities that do not fall into the two categories above. These are the consequences of the legitimate activities of the user or the objective action of external forces and energies, which have no logical connection to forensic footprints, and which can be used e.g. in a variety of analyses aimed at increasing the performance or improving the functionality of equipment, economy of operation, availability of services, security level, etc. The quality and form of track processing in this case usually serves the purpose for which the outputs are to be used. These are often also internal materials for internal control of compliance with institutional rules, etc. Due to its nature and quality, this type of footprint may not (but may) be acceptable to judicial authorities.

In the available literature we will find some basic views on the categorization of traces. We most often distinguish traces by:

- material nature – all traces are material (substance's, fields or memory);
- the content of information on the basic structure of the operating objects (traces of external features, and the internal structure of the operating objects);
- the origin of the predominant characteristics of the object or entity being reflected (traces of a biological, chemical or physical nature);

- the subject of examination of the information content of the trace (blood traces, dactyloscopic traces, trasological traces, digital traces, defectoscopic traces, etc.);
- the object, weight, dimensions or visibility of the trace left (macro and micro traces),
- the method of interaction in the event of a trace (traces of layering or stratification – imprints, traces of dynamic or static, area or volume, created by the transfer or removal of energy or matter, etc.).

The scheme of the digital traces and its practical use in theory and practice according to Meteňko, Porada, Rak also correspond to this concept[20].

Each traces can be assigned to each of the six categories. In other words: the trace is always material, either substances, field, or memory; it reflects information about the basic internal or external structure of the object. If it is of a substance nature, then it was created in a biological, chemical or physical way (or a combination thereof), for each trace, its information content can be examined, each trace is a macro-trace or micro-trace (and we choose the appropriate procedures, means and tools for its search, securing and research), each trace arose from a specific way of interaction between interacting objects.

Digital trace categorization and classification

According to one of the above definitions, a digital trace is any information of informative value relevant to the investigation of a particular act or activity, stored or transmitted in digital form. Information is essentially intangible. However, for our case, it is created, transmitted and stored and archived in digital form, in the form of electrical, magnetic, optical or other similar manifestation of the field. At the moment of its storage, it materializes in the environment of the storage medium, and its recording has the character of an array. In order to be able to analyze the transmitted information, we must first capture it technologically and then store it permanently or temporarily on a storage medium. The digital trace has a non substantive, but material character. In general, the characteristics of the internal structure of the acting, reflected object are transferred to the reflecting object. Thus, the digital trace is a trace of the internal structure of the reflected object, the external characters are manifested in the format in which it is currently stored.

The digital trace is in its primary form, i. e. in the "form" in which it is stored or transmitted, with some minor exceptions, it is, according to the Prada

[20] Meteňko, J. *a kol.* (2004). *Kriminalistické metódy a možnosti kontroly sofistikovanej kriminality.*

nadRak, a micro-trace[21].

Technological equipment or user, system and especially subsequently criminalistics, forensic or informatics software are needed for its visibility. The simplest, user-friendly technologies include monitors or displays displaying digital information in a human-acceptable (perceptible) format (font, images, sound, video, vibration, etc.). These "communication peripherals" also allow the transfer of digital data to a native storage medium suitable for the needs of users – e.g. office paper, classic photography. We are able to perceive such transformed digital (information / data) tracks with our senses, especially sight and hearing, or tactile (Braille).

User software (text, graphic editors, spreadsheets) can display common traces, similar to system software, which is significantly remote for ordinary users in terms of perception and possibilities of use. Specialized software of criminalistics and forensic nature can also read information about deleted files, break passwords protecting access to encrypted information, etc.[22].

The digital trace is created mainly by the action of physical forces and energies. We classify the digital trace among the physical traces of the field of technological character as a reflection of the direct or indirect action of artificial artefacts or external natural forces of a physical nature.

By direct action of artificial artefacts we mean direct, automatic, random or pre-programmed action of one technological element (artefacts) on another.

In the case of indirect action, we mean human action on the artefact (in the form of software or technical equipment or technology). Theoretically and practically (so far to a limited extent determined by research and development workplaces) the technology of storing or transmitting a digital traces can be based on principles other than physical – i. e. chemical or even biological.

For today's technologies and trends in the transmission, processing and storage of digital information, it is striking to strive for maximum miniaturization of devices and the highest possible density of stored information (the largest possible data volume in the smallest possible physical volume of the storage medium). From this point of view, the physical principles seem to be

21 Rak, R., Porada V. (2003). Obecné a specifické charakteristiky identifikace a verifikace osob a věcí z pohledu využití IT v bezpečnostní praxi ve vztahu ke kriminalistice a forenzním vědám. *Kriminalistika a forenzné vědy,* Zborník z odborného seminára. 25–63.

22 Chaževskas, A., Belovas, I., Marcinkevičius,V. (2021). Forensic password examination in leaked user databases. In: Zachar, Š., Meteňko, J., Meteňková, M., (2021) *Kriminalistika a forenzné vedy: veda, vzdelávanie, prax : 17. medzinárodný kongres*. Zborník príspevkov, 241–257.

exhausted in some respects, and scientific attention is focused on technologies close to the biological or biochemical way of processing information, i. e. a process similar or directly taking place in the human brain. Therefore, generally no nature-friendly characteristics of information storage and processing can be ruled out in the future.

Sources of digital traces as their carriers

Obviously, there are a large number of diverse sources of digital traces. Their number and type diversity increases from day to day. It is therefore expedient to divide data sources into several typical groups, in which digital traces have a similar character and thus the method of their search, retrieval, processing and further use is similar. A typical group requires specific technical equipment and knowledge of narrowly oriented digital traces specialists.

In different including foreign literature, we often encounter a logical arrangement into groups:

Open computer systems. This includes everything that people usually think of as a computer and its immediate peripherals – PCs (desktops), laptops, hard drives, keyboards, monitors, servers, etc. Their disk capacity is always limited (but devices with ever-increasing disk space are constantly being produced), they contain a huge amount of information and therefore digital traces. Ordinary data file – e.g. Word document – with its content and system information (so-called metadata) it can serve as a key means of evidence and significantly influence and accelerate the course of the investigation.

Communication systems. Traditionally, this group includes traditional landlines, wireless telecommunications systems, computer networks and the Internet. Mobile phones, personal digital assistants (PDAs), etc. All of these can provide digital tracks. For example, e-mail is transmitted all over the world via Internet services. The time the e-mail was sent or the author, its contents, the log files of the mail servers that transmitted the e-mail, these are all very important digital traces.

Devices with integrated computer chip. Smart cards and many other computer chip devices, which are also a very valuable source of data for investigation. GPS-based navigation technologies can determine the position of both the vehicle and the individual, the black box of the aircraft remembers all flight characteristics, similarly to diagnostic modules of computer control units of automobile engines store basic operating and service data types of service (speed, brake operation, mileage, fault diagnosis, types of service, etc.). Another group of devices equipped with an integrated chip and intended for use in

the ordinary household contains important information and thus additional sources of footprints. In addition, these devices can communicate with the outside world, other devices, and environments, including the Internet, by default, usually wirelessly. In practice known usually as an Internet of thinks.

Despite the tremendous development of digital technologies, there are still few specialists who can effectively read and draw relevant conclusions in digital traces that can be used by law enforcement or other authorities. Many times we are not technically, knowledgeable or legally prepared to work with digital traces. These are often overlooked or underestimated, incorrectly collected or inefficiently analysed.

Digital traces and their properties and features[23]

Digital traces, after all, like any other type of criminalistics traces, have their general and individual species characteristics and characteristics, which from the point of view of law enforcement or other authorities have typical positive and negative aspects and consequences. These aspects then need to be kept in mind at all times and at all stages of working with digital traces. Digital traces are created by human – user / perpetrator action, application or system software, digital device functionality, or automatic action from one device to another. This should be the most important element determining the success of their usability for individual criminalistics identification.

Unfortunately, given the current level of knowledge, this is not the case at all. Digital traces therefore, to an unusually high degree, reflect the specific characteristics of high-tech with the rich diversity of the human spirit of their users who use them. The specifics of digital traces are reflected in their features:

- the mass of digital traces as field traces,
- latency of digital traces,
- time traceability of digital traces,
- high content of digital traces,
- very low digital traces life,
- large data volume of digital traces,
- the data density of digital traces is declining with the development of new technologies, extreme dynamism of the digital traces environment,
- heterogeneity and complexity of the digital traces environment,
- location of space with digital traces,

[23] Meteňko, J., Bacigal., I. (2010). Zdroje a skúmanie digitálnych stôp. In: Straus, J. (2010). *Pokroky v kriminalistice, Sborník příspěvku z IV. mezinárodní konference,* 12*;* *Meteňko, J. a kol.* (2004). *Kriminalistické metódy a možnosti kontroly sofistikovanej kriminality.*

- high level of data protection,
- the digital trace is automatically identifiable and processable by specialized means,
- high level of eradication of digital traces by qualified offenders,
- partial or complete restoration of destroyed digital traces,
- originality of digital traces,
- currently, the low level of investigation and judicial acceptance of digital traces in legal and forensic practice,
- the preservation and quality of digital traces is influenced by a number of subjective factors,
- manifestation of digital traces as field traces.

Conclusion

The authors tried to analyse in the study the theoretical knowledge of the use of digital traces in the criminalistics and the perspective of the usability of digital traces. They outlined this problem from a criminalistics point of view, including a brief description of the digital traces theory. Within the vision of significantly wider possibilities of use in criminalistics and forensic research, they point to the possibilities of exploring the digital traces and its content, as, unfortunately, still a new part of criminalistics and forensic traces[24]. The basis for this analysis is so far probably the only comprehensive work in Slovakia in this area, especially the content of its first part. The detailed processing of the knowledge was carried out as part of the research within the project of the Center for Excellence in Security Research, including three large outputs of dissertants involved in the project. Digital traces are typical of crime related to the misuse of information and communication technologies, this is a typical opinion of most experts. At present, however, they already make up a significant part of the trace of any crime. Some results show that in reality there are 80–90% of cases where digital traces occur and our estimate is similar. Not only inconsistent knowledge of digital trace theory, its forms and types is a theoretical burden for its use / non-use. Unfortunately, there are major shortcomings in the field of police use of the digital traces, according to previously published research. But as reality shows, these traces are part of virtually every activity in our lives today. The authors of the study distinguish between a number of

[24] Sachypov, N., G, Myrzanov, E., N, (2021) Innovation and application of special knowledge of technical sciences in criminalistic. In: Zachar, Š., Meteňko, J., Meteňková, M., (2021) *Kriminalistika a forenzné vedy: veda, vzdelávanie, prax : 17. medzinárodný kongres.* Zborník príspevkov, 305–311.

divisions in the traces of criminal activities – many types of digital traces. Extensive research during and after the project in research activity 3.3., Center for Excellence in Security Research, ITMS code: 26240120034, co-financed by the Operational Program Research and Development, shows a great diversity of basic features of digital traces.

SKAITMENINIŲ PĖDSAKŲ TEORIJA KRIMINALISTIKOJE

Jozef Metenko,
Miriam Metenkova

Santrauka

Autoriai straipsnyje lygina skaitmeninių pėdsakų panaudojimo realybę ir perspektyvą, įskaitant trumpą skaitmeninių pėdsakų charakteristiką ir jų teoriją. Žymiai platesnio taikymo kriminalistikoje ir ekspertiniuose tyrimuose kontekste jie nurodo galimybę panaudoti skaitmeninius pėdsakus ir jų turinį kaip naują klasikinės kriminalistikos dalį. Šios analizės pagrindas – bene vienintelis kol kas pirmasis šios srities kompleksinis darbas Slovakijoje, ypač jo pirmosios – teorinės dalies turinys. Detalus žinių apdorojimas buvo atliktas vykdant Saugumo tyrimų kompetencijos centro projektą, įskaitant tris pagrindinius projekte dalyvaujančių disertantų rezultatus. Skaitmeniniai pėdsakai visuomenės nuomone yra būdingi nusikaltimams, susijusiems su piktnaudžiavimu informacinėmis ir ryšių technologijomis, o tai yra klaida, nes jų panaudojimas yra ženkliai platesnis. Deja, remiantis paskelbtais tyrimais, didelių trūkumų matyti ir policijos žinių apie skaitmeninius pėdsakus srityje. Tačiau, kaip rodo realybė, jie yra beveik visos mūsų dabartinio gyvenimo veiklos dalis. Tyrimo autoriai nusikalstamos veiklos pėdsakuose išskiria daugybę skirsnių – daugybę skaitmeninių pėdsakų. Išsamūs tyrimai projekto metu ir po jo 3.3. tyrimo veikloje, Saugumo tyrimų kompetencijos centras, ITMS kodas: 26240120034, iš dalies finansuojamas iš Veiksmų programos Mokslinių tyrimų ir plėtros lėšomis, rodo didelę pagrindinių skaitmeninių pėdsakų ypatybių įvairovę.

Raktiniai žodžiai: pėdsakas, skaitmeninis pėdsakas, kriminalistika ir teismo ekspertizė, tyrimai, skaitmeninių pėdsakų perspektyva, kriminalistika, skaitmeninio pėdsako teorija.