implementation of operative-search actions and secret investigative (search) actions (structural-logical schemes) by divisions of criminal police]: navch. posib. Za red. I. R. Shynkarenka. Dnipropetrovs′k: DDUVS, 224 s. [in Ukr.]

10. Stepanyuk, R. L. (2012) Kryminalistychne zabezpechennya rozsliduvannya zlochyniv, vchynenykh u byudzhetniy sferi Ukrayiny [Forensic support for the investigation of crimes committed in the budget area of Ukraine] : monohrafiya; za zah. red. d-ra yuryd. nauk, prof. A. F. Volobuyeva. KH.: NikaNova, 382 s. [in Ukr.]

SUMMARY

Ihor V. Pyrih, Srhii O. Prokopov, Denys V. Vodopyan. Current requirements and state realities of combating organized crime. The article describes in detail the concept of professional crime, it's devastating impact on Ukraine's democracy, and offers suggestions on ways to identify, prevent, and stop professional crimes. The importance of the operational units of the National Police of Ukraine in the fight against professional crime in the current conditions of law enforcement reform is considered, the problems of the legislative and practical significance of the units of the criminal police are described. The modern legislation which defines the general principles and tactics of combating professional crime is analyzed and proposals for its improvement are made. Attention is drawn to the fact that, in recent times, the danger is not even the possibility of bribery of officials by criminal groups, but the gradual entry of members of criminal organizations and, even, their leaders and organizers into power structures, state administration, control and law enforcement bodies.

Another problem we have outlined above is the lack of training and lack of professional experience of law enforcement officers in the fight against organized crime. The dismantling of the Organized Crime Offices and the establishment of Strategic Investigation Departments and their subordinate departments had a mixed effect on the results of combating crime. Positive, in our opinion, is the accession to the body of experts in the detection and investigation of crimes of economic orientation, as organized crime at the present stage, as noted above, aimed at including the commission of these crimes. The negative tendency is, in our opinion, the turnover of personnel, due to the sometimes rather harsh and unfair conditions of competitive selection of candidates, the lack of individual approach to the staff with many years of work experience. One way to solve this problem is to train specialists in strategic investigations departments in universities with specific conditions of study, followed by a mandatory internship under the guidance of mentors for at least three years.

Keywords: *organized crime, criminal proceedings, operational units, police, corruption.*

UDC 343.13(477)
DOI: 10.31733/2078-3566-2020-2-216-228

Prof. JUDr.
Jozef METEŇKO©
PhD

PaedDr.
Miriam METEŇKOVÁ©
PhD

(Academy of Police Forces in Bratislava and Forensic Science Institute, Slovak Republic)

DIGITAL TRACE AND THEIR ATTRIBUTES EVALUATE FOR CRIMINALISTIC

Йозеф Метешко, Міріам Метешкова. Цифрові сліди та їх оціночні характеристики для криміналістики. Здійснено спробу проаналізувати можливості вивчення та дослідження цифрових слідів та їх змісту, що являє собою новий розділ криміналістики в частині криміналістичних слідів. В основу цього аналізу покладено поки що перше на сьогодні комплексне наукове видання Словаччини у цій галузі, особливо зміст його першої частини. Детальний фаховий аналіз здійснено в рамках дослідження одного зі співавторів європейського дослідницького проєкту.

© Meteňko J., 2020
ORCID iD: https://orcid.org/0000-0002-0904-3803
jmetenko@hotmail.com

© Meteňková M., 2020
miriam.metenkova@minv.sk

Констатовано, що цифрові сліди характерні для злочинів, пов'язаних із нецільовим використанням інформаційно-комунікаційних технологій. Загалом, вони присутні в усіх видах злочинів. Однак їх використання знаходиться на нижньому рівні відносно інших типів слідів. Автори дослідження пропонують розрізняти кілька видів ознак та характеристик цифрових слідів у злочинній діяльності. Дослідження здійснено в межах науково-дослідної теми (реєстр №3.3) Центру досліджень у галузі безпеки, код ITMS: 26240120034, що фінансується за рахунок Оперативної програми «Дослідження та розробка», і показує широкий спектр характеристик для дослідження цифрових слідів.

***Ключові слова**: слід, цифровий слід, криміналістичні та експертні знання, дослідження.*

Introduction

Fast development of information and communication technology has an impact on all spheres of present-day society. An integration of telecommunication and information systems enables the speeding and improves the reliability of information processing, storage and transmission. It is the matter regardless the distance and way of communication. Thus opening a wide spectrum of possibilities in both - positive or negative directions. In its positive direction, this development causes and backs up huge economic and social changes not only in the Slovak Republic (Meteňko a kol., 2004), but in general over the world too. Technical equipment and technology are, in general, created to serve the people. Development of information and communication technologies (ICT) is very fast. Efficiency of using technics and technology is growing, and the areas where they are used are also spreading too.

At present time one may not find any branch of human activity where he would not meet the electronics equipment, his digital software and its application. Actual time is typical for a larger and deeper integration of information and communication technologies with all ordinary household and office equipment (television set, telephone, refrigerator etc.). We will be encircled by technologies on our every step and still in a larger extent (Rak, 2000). Big question is, if we by police and other security and law enforcement services are on the right situation and if we are prepared accept and realised this call in the crime control.

Some peculiarities and historical aspects of the digital trace theory and its applications in forensic science and criminalistics

The concept of cybercrime originated in the days of the big computers and the first PCs. Since then, however, this area has undergone stormy developments, and further trends also foresee ongoing developments in our time. In addition to mainframe and personal computers, other technological means that connect or suitably complement the computing capabilities with communication in a variety of forms are commonplace. Their common platform is to digitize almost everything that surrounds us. Is coming internet of things. Data files often contain, in addition to primary content (text, photos, audio, video, etc.) metadata that characterize additional file information, e.g. about the format, style, or data of birth or replace. It is then possible to determine when the picture was taken, or text revised, under what lighting conditions, what kind of setting, including a type of camera, author of text, etc. This information found on a computer that is in some way related to a criminal offense can provide important information for the investigation.

Everyday are used mobile phones, wireless data transfers from our personal electrical equipment (via WiFi, Bluetooth), electronic diaries, handhelders, digital watches audio digital recorders, digital camcorders and cameras, video and DVD players, or recorders, payment and ID cards, various recording media (CDs, DVDs, USB memory, digital camcorder and camera memories, optical media, etc.), rich accessories for various peripherals to all of the above mentioned devices. Many of the other technologies incorporate one or more dedicated processors to ensure the activity of the device - on-board computers, aircraft, ships, various security and monitoring devices, electronic identification of objects, goods, etc. All including smaller or bigger memories.

More of these devices leave criminalistics and/or forensic traces of their activity, which have their general and individual patterns and are practically usable. It is equally clear that the term "computer" crime has a much wider significance today than in the past. Computer crime has been logically correctly understood in the past in relation to computers only. Nothing else existed there. Where, but to include today's criminal activity, with payment or identification cards containing magnetic data carriers, modification of unprotected data during their wireless transmission, using cryptocurrencies, and the like? A number of technological devices, even if they are not a means or purpose of a crime, contain a large number of different data which in

the course of an investigation of another crime, offense or completely different activity in the first phase have the classic character of the criminalistic trace, and in the final stage ideally the character judicial evidence. Using all of these traces, it is then possible to examine the case investigations, collect evidence against the perpetrator, or confirm the alibi of innocents. Traces become direct or indirect evidence in the defence. On the data medium, records of the user's activity on a computer, a mobile phone list of the last calls of the crime victim, a video record of a department store or bank customers at the time in question, the vehicle's VIN number that the perpetrator forgot on mechanical falsification of other car numbers change, or did not know, in the call centre a listing of all calls made, GPS coordinates of an object (eg a car or victim) at a particular time, etc.

An important source of traces can be web cameras that capture a particular area of interest in real time. Live shots can be browsed via the internet from the other end of the globe. These cameras can be controlled remotely from our computer. Camera surveillance system operators are state and non-state institutions, private individuals. The cameras capture various objects and scenes, continuously capturing areas of crossroads, business houses, banks, cash dispensers, petrol stations, border crossings, technological or service spaces, tourist attractions, hotel lounges, etc. it is important that many applications working with webcams archive the images taken together with the time and place of establishment. Image frames, or their sequences, can thus also take the form of traces, evidence, and play an important role in investigating wholly common crimes. If, at the scene, the witnesses were interviewed and tried to best describe the situation, today we can - we have to assess whether the space was not monitored by means of digital outputs that could serve as traces, a basic guideline for the investigation, and then evidence of far greater redundancy (a much larger amount of objective information) than subjective descriptions of witnesses that can even differ in diametrically.

Definition of digital trace

Every technology device that is acquired, processed, handed over, or retains data leaves a record of its activities. These records from a criminalistic point of view are traces. According to the theory of reflection as a basis of interaction, such as a person or other object or entity / influence, controls, triggers, or modifies the SW equipment, or its settings, or otherwise controls the electronic device. These activities or changes are then reflected in the material environment in and out of the technology.

In the sense of computer or cybernetic crime or cybercrime defined, or the computer or cyber-related crime including complexity of data-processing devices is before defined concept much wider than just a computer. In some works by renowned Czech and Slovak authors, we come up with the concept of a “computer traces”, which is rather intuitively used than actually defined. The concept of computer trace originated at the same time as the concept of cybercrime, roughly in the second half of the 1980s. Obviously, the concept of a computer trace is not enough today, because other electronic devices also leave traces of the same nature, character, general or individual characteristics as a computer trace.

In the foreign literature, there are several similar definitions defining the commonly used term digital evidence (digital record). It is important to note that the word "evidence" has a primary meaning in English – proof. We cannot find a word about modern technology in foreign literature (we can find the meaning of a potential digital record that has a close sense of clue). The cause is simple and pragmatically based - foreign theories and practices are strongly oriented to the outcome of the criminal process, i. the trace/evidence must be accepted by the court and, therefore, in the perception and subsequent use of the terms, the trace and evidence are automatically identified. This concept is understand as a forensic concept of digital evidence. The definition of a digital trace in the home literature is a few. Any years before we use this concept based on research to 2010. Our concept of digital trace was presented at 2005 (Meteňko, J., Meteňko, M., Hejda J., 2005) : Any change in the material environment of hardware memory, or captured in such a hardware carrier for data, which has criminalistic relevance (related to criminalistic relevant event), is examinated (search, ensure and specific examination) with criminalistic – (forensic) informatics (cyber) methods and based on its examination is possible the identify for relationship of digital traces and object that created it.

Actually, we prefer the following definition - a digital trace: *A digital trace can be defined as any information that is stored or transmitted in digital form and which is related to the investigated event with which it can be searched, to investigate and decode in advance and in detail by current criminalistic or forensic methods and means* (Meteňko, M., 2018).

This definition is open to any digital technology. (Rak, R., Porada, V., 2000) In this way, the digital trace covers both the area of computers and computer communications, as well as the digital transmission area (mobile phones, but also future digital objects and equipment), videos, audio, digital photos, camera systems data, electronic security systems data and any other technologies potentially associated with Hi-Tech crime. The original proposal was about the binary form of stored or transmitted information. The word binary has been changed to digital because this term is more general (the binary form is a subset of the general digital form). Unlike other definitions, the definition is also general in the sense that the digital trace does not necessarily coincide with a criminal offense, which, as we shall see below, is very important. The digital trace must be available not only to force ministries, criminalistic, but also to general forensic investigations conducted by state authorities (civil law, commercial laws) and commercially for the needs of independent internal or external audits.

The International Organization of Computer Evidence (IOCE) originally defined a digital record, or a digital evidence or digital forensic trace, as any information stored or transmitted in binary form that can be submitted to the court as factual evidence. The word binary versus digital has already been discussed. In this definition, emphasis is placed on providing evidence to the court. In practice, for example, for forensic investigations on a commercial basis (consultant-forensics or other firm or individual), but no exit to court may be, the result of the study is submitted to the management or the company's shareholder. The concept of digital trace as any other trace should therefore be oriented only to the correct course of the investigation and, as a result, standardize the work practices, concepts and quality elements for any investigative body, and guarantee the portability of the evidence, investigation methods among the various participants in the investigation, between state authorities and independent expert bodies and entities.

In other proposals, the digital trace was defined as information characterizing or proving the commission of a criminal offense, or establishing a relationship between the offense committed and its victim, or criminal offense and perpetrator. Even here was the effort to link the trace only to the definition in connection with the offense committed. In the first definition below the digital trace, we also understand the outcome of the user's legitimate activity, which is in any way relevant to a general investigation, in-depth financial audit up to the level of IS technology. Such a definition is improperly narrowed and oriented only to a criminal offense, which may not always be true. In connection with digital traces, other related processes and entities are defined which are logically associated with digital traces and form a homogeneous whole. This is very important for the whole process of working with digital traces.

These terms were defined for our needs in the project Centrum excelentnosti bezpečnostného výskumu kód ITMS: 26240120034 supported by the Research & Development Operational Programme funded by the ERDF, task 3.3. by following way:

Ensuring digital traces is a process that begins when the information or device is secured or stored for preliminary or detailed expert examination. It is assumed that the digital trace will be finally accepted as evidence by the judicial authorities. It is further assumed that the retention process is reasonable and legal for working with evidence in a given geographical location (country). Physical and data objects become evidence only if they are acceptable to law enforcement agencies. Local differences and internal regulations are usually preferred in crime law processes.

Data forms. Objects or information with a credible information value when associated with physical elements. Data forms in different objects may have different formats, but they can never change the original information they are typical carriers for information. Data objects are e.g. databases, directories, files, virtual memory information, digital video, or audio recordings, and other forms of data recognised for human sensation.

Physical objects. Elements on which data objects are stored or through which they are transmitted. In our criminalistic concept known as carriers. Physical objects mean technological parts, devices designed to process, store, or transmit data. In practice, they are computer hard drives, various storage media (floppy disks, CDs and DVDs, data tape memory cards). In the broader sense, all devices (computers, printers, network elements) that contain, in addition to digital tracess, additional information such as production numbers, dactyloscopic, or mechanical or biological traces and others that demonstrate the logical relationship of the physical device), its user (offender) and criminal offense, or other activities of interest to the investigation. Physical objects are often and not only in Slovak police practice the subject of a broader widespread criminalistic interest, just as a “things traces” – those as substituents of real digital

trace. All common methods of criminalistic /forensic and crime investigation are used as appropriate.

Originals of digital trace. Those are data objects that are secured for expert-forensic/criminalistic searching and investigation purposes. Incorrect there are accepted physical and mater objects too. Originals of digital traces are the basic evidence. For the purposes of the user (perpetrator) or investigating authorities, work duplicates or copies of digital footage are created and with full acceptation. The process of creating them is unambiguous and there is no change in information content. This process, when the basic conditions are met, is always repeatable with the same results. Users and independent experts are then provided with acquired or created basic material for further investigation with the same information value. Thus, the immeasurability of the original digital trace as evidence is guaranteed.

Duplicate of digital trace. Exact digital reproduction of all data objects contained on the original data and physical object to physically the same type of data medium. Duplication of a digital traces is always created by copying all data objects of that physical object to another physical medium of the same type. Digital duplicates work quite well, especially in the complex digital environment of computers or other digital devices where there is a wide variety of links between individual data objects. Because the duplicate reproduces all data objects, both logical and physical relationships are maintained. The duplicate can be used comfortably, safely and fully. The disadvantage can be the giant amount of information stored on duplicates. The data volume and the information content of all data objects are in a ratio of 1: 1 between the original and the duplicate. Duplicates of digital traces are primarily created for the purposes of evidence investigations so that we can present the original material for re-searching and re-investigation to another, independent, knowledgeable person where the physical object itself can not be directly secured for the needs of the CPU for various reasons. In practice, the field of personal computers typically uses the image disk, which is a true duplicate of its content, a mirror of its original content stored in digital form.

A copy of the digital traces. Accurate reproduction of information from the original physical object to another, physically independent data medium. When creating a digital trace, we create data objects with the same information content but physical media that may be of a different type. In the copy creation process, all data objects of the original physical object need not necessarily be reproduced, but only some of them are selected, which are essential and therefore necessary for further investigation. An example of this can be copying a single digital photo from a digital camera memory card where a lot more photos are stored. In the case of computer systems or digital devices, we copy individual data objects, but we create them from the wider context of complex environments. As a result, all functional and logical links to other data objects may not be retained. We make copies if it is useful for the purpose of the investigation, for example, due to the size of digital trace data volume. Copies contain only part of the data objects of the original physical object. However, the information value of each copy object does not change from its original.

Ordinary copies of digital traces may not be sufficient proof because we were mistaken in choosing them, providing only a certain part, etc. From the point of view of criminalistic/forensic searching and investigation, it is therefore crucial to have originals of digital traces or their duplicates. It is possible to demonstrate transparently the eligibility and correctness of the chosen investigation procedure and the preparation of evidence.

Specific features of digital trace.

The concept of digital trace must always be understood in the wider context of evolving technologies. Below digital trace, we must not only represent the reflections of software and human activities in the physical environment of data storage media for computers. Digital trace are created by technologies that work based on modern electronics.

In various forensic/criminalistic laboratories of world police agencies or institutes, specialized audio and video laboratories have historically been established before analytical workplaces have started to focus on expert research on computers and their associated peripheral devices and technologies. Audio and video laboratories perform classical analysis of sound and video, whether recorded by analogue or digital technology.

The current world practice practice has a bearing on the problems of certain rivalry between all the above-described specialized areas. Each area has its own justification, its historical moments of origin, its specifics and its place in criminalistic and forensic practice. None of them is otherwise exceptional, priority over others.

Global trends in the globalization of information activities strongly erode the differences between the functionality of individual digital devices that are increasingly using common international standards for data exchange and transmission.

Everywhere there are digital trace that blend in between the most diverse digital devices and can denounce the course of many activities with much greater accuracy and content than we are able to preserve in our human memory for a long time.

From this point of view, practical criminalistic begins to perceive the integration of technological processes and objects and the expertise activity is understood in a complex way. Digital records their standardized data and communication formats are a sealant that combines exploration into the essence of digital traces and their character traits.

Digital traces as field traces

Although data and information are immaterial, material medium, with various technological equipment, format, data structure, reliability and lifespan etc., is needed in order to store them. The medium contains digital traces in the form of field and it is a physical component of means of evidence. In judicial practice they can be required as physical part of evidence, from which it is possible to acquire the same information again and at any time in order to determine expert's finding. Technologies for digital data processing for personal use (PC, notebooks, smart cards, tapes, floppy disks, CDs and DVDs, mobile phones, personal organizers – PDA etc.) are perceived in this way. If they are found on the crime scene they are secured and sent to laboratory for the expert examination.

Latency of digital traces

Digital traces are invisible. Latency is multiple. The records, which are processed or stored to the data medium, are invisible to the naked eye (with the exception of views of monitor screens, print screens, photographs or video recordings of screens and printed documents). The second level of invisibility is due to the fact that some of the records, files are invisible to the ordinary computer and digital technology users because there is a hidden attribute set, special settings of user's rights or special application or system means. Another category of latency of digital traces is comprised by deleted recordings, reformatted disks or data destroyed or changed by other means. Special software is needed in case of restoring them. In the same way we approach encrypted data, which although are visible to the user, they are without informative context.

Time traceability of digital traces

In comparison to other traces known in criminalistic or forensic practice in some case the digital traces can precisely determine time span of activities.

It depends on criminalist's knowledge, which enables him to fully use information and archival sources of application program equipment. Knowledge of user/perpetrator is significant as well. If the user does not have particular knowledge, then digital traces of great importance can be found in the document. A good example is utilization of functionality revision of Word. If the user is unaware of all the implications, he can unintentionally provide commercial competitor with restricted and internal information, which in extreme case can end up by filing a complaint (slander, information leak, information abuse in commerce, etc). If all versions of working documents are stored, internal audit can analyse procedure of document processing in similar way. This is determined by fact that the computers and other digital devices (camcorders, cameras etc.) have digital clock, which determines the activities of system SW or other activities of digital devices such as time lock.

It is common that accurate time setting by a larger system is executed by automatic synchronization by the Internet services and specialized transmitter so that the clock indication is absolutely credible. Then it is possible to determine when the user logged in/logged out, created, deleted, ordered services, sent and received an e-mail read it and replayed to it etc. If there are found digital traces with a time lock, they significantly document the process of particular activities in time.

Unless there is a clear identification of the user (perpetrator) in relation to computing or other digital technology and equipment, it is possible to use digital footprints to document all of its activities related to computers and other bearers with digital devices.

Content of digital traces

In specific cases digital traces have high information value on interests and activities of the person, the computer user or the perpetrator of the crime. From this point of view they are

very important for criminalistics and other forensic sciences and from the point of theory of the traces they are unique in comparison to other types of the traces. In many cases it is possible to study not only particular activities of the computer users (all the activities he has done), but also what information he was interested in, what information he acquired, processed, stored or handed in to the others. Due to these facts it is possible to determine some fields of the interest of the perpetrator, his motivation and to create psychological profile.

Examples include addresses (and contents) of browsed websites, content of photos, videos, text files, etc. Analyzing the contents of a personal digital device reveals a lot of professional and intimate about its owner. The current problems, such as Facebook or other commercially-oriented Internet projects, point to criminal abuse of such options.

Relatively low lifespan of digital traces

From criminalistic or forensic point view of digital traces, digital records are recorded to memory medium. They can be intentionally deleted by the user or systematically and automatically (without one's involvement) rewritten by other records. Read-only optical medium, intended for archival purposes, is exception. They are very expensive and not very commonly used in the practice. The mediums are intended for recording without possibility of deleting them with lifespan of 50-years and over. It is possible to restore deleted recordings with the help of special SW, but the restoring must be done very quickly before the memory medium is rewritten by system means. The promptness of restoring and fixation of particular data, capacity of the memory medium and intensity of user's activities when creating data files, play decisive role. Besides, data can be damaged by computer viruses or hidden programmes (e.g. Trojan horse).

When transmitting data by wire or wireless means, if we have access to sender or recipient filesystems (where the data is stored much longer than the transfer itself), the transmission time is very short and moves in a row in seconds (and even shorter!). Special means (monitoring software) that store data on the storage medium and without which it is practically impossible to detect meaningful real-time data content must be deployed. Trace detection in this way is operative and is typically performed only when checking different examinations or targeting the activities of the person concerned.

Large data capacity of digital traces

The volume of data in a medium-sized enterprise is in our range in a number of TBs. Strong centralization, arising from operational and economic reasons, is typical for computer and communication means. In our country data capacity is around tens TB in middle size companies. Only a small part has character of a digital trace.

In practice, it is often difficult to select the necessary relevant traces from such a large volume of data and evaluate them in the real short time necessary for a successful investigation. For similar reasons, it is very complicated to provide digital footprints from the Internet, where the amount of data grows with the number of (even short-term) connected servers being worked on. Digital tracks are also found on such remote servers. Data density of digital traces, among other data with development of new technologies, constantly decreases

The digital trace itself is not limited by physical capacity. New technologies for data comprising are developed. It means that larger data capacity is saved to the same capacity of data medium.

The data density of digital tracks between other data and the development of new technologies is steadily declining

The digital footprint itself is not in the normal sense limited by the physical volume. Still new data compression technologies are being developed, i.e., j. an ever larger amount of data is stored in the same volume of data medium. In parallel, new and new data media technologies are being created to save more data to the same or even smaller volumes (the 3.5 "disk has a capacity of 1.4 MB, CD up to 800 MB, DVD 9.5 GB and below .). In order for forensic analysis to be effective enough and fast to be analyzed, it must be directed to search for specific species or individual digital tracks. If we know what we're looking for, the process is very fast. Otherwise, the analysis will absorb a great deal of time and resources. The volume of data processed and stored with technology advances sharply. However, the amount of digital footprints left by perpetrators does not grow at the same rate. If we define the data density of the digital tracks as the ratio of the data volume of the digital tracks left behind by unwanted activities and the total volume of all data processed or stored, then this ratio - the density of the

digital tracks versus the data density will overall decrease in the future, j. criminal investigation and investigation or forensic investigations will become more and more challenging in scope. The digital footprint density, ie its distribution in the digital environment, is significantly prolonging the time of the investigation, partly because of the length of its search, and because of the obstacles to the effectiveness and speed of the international exchange of information and legal assistance.

Extreme dynamics of environment of digital traces

This particularity is typical mainly for common network environment in big institutions when data funds are distributed in real time. Comprehensive company applications are strongly centralized and dynamic with high requirements for application accessibility from the point of fulfilling information needs of the institution, economic and operational characteristics. Applications are included in critical company applications. It means that interruption of application function only for one minute (mainly in industry, transport, telecommunication, financial institutions etc.) can have disastrous existential consequences.

In the past, this was particularly true of large institutions. At present, it is even more pronounced in the dynamics of large network structures of social and business networks. Extensive enterprise applications are highly centralized, with a high demand for application availability, and are therefore very dynamic in terms of meeting the institution's information needs and economic-operating characteristics. There are a large number of internal users (most of the institution's employees) and / or external partners or customers. Applications have a major impact on meeting economic, competitive, security, and other goals. Critical applications must therefore be designed according to strict security rules (staff separation, logging - backup, data archiving, ongoing monitoring, etc.). If these rules are not observed in the development or operation, this directly compromises the safety and operability of the structure. Investigation, searching, detecting and searching for a perpetrator and tracking is a very complicated matter with a high degree of uncertainty of the outcome and a great deal of investment and time support in investigative processes (Peťovský, M., Loffler, B., 2017).

Heterogeneity and complexity of the environment of digital traces

Various operational systems, databases, application software and its versions, data interface among applications, data formats, transferable proceedings, proceedings of operational records, logo etc. are commonly and concurrently used in the same organizations. Concerning information and communication technologies know-how of each field is covered by all sorts of experts. Intricacy of investigation is determined by complexity of issue, which does not have to be apprehended in a conceptual way. Quality and promptness of secured digital traces are primary cause of low criminal detection in connection with information and communication technologies. The investigation is not entirely clear in the first phase - just as with every survey, what digital tracks we are looking for and, in addition, it is necessary to effectively coordinate the work of all specialists, operationally and if necessary direct their synergies and require them with clearly qualified search and reassurance operations. The search and seizure requirement is also complicated by a legal qualification that needs to be properly interpreted. Digital footprints can be found in a variety of parts - nodal storage points of information and communication technologies, not always having to be a complete object. Sometimes it can be just part of the structure of the digital footprint or the signer's signature. The problem is also the fact that sometimes the information structures only partly duplicate internal institutional processes, reflecting precisely in the structure of digital data processing technologies that have become the means or the goal of a certain form of assault of a crime. Taking into account the analogue of the offending criminal group, in the ICT environment, it is absolutely necessary to have a team of experts who know the complex problem even from specialists (for example e-mail administrators, operating systems, databases, SAP business applications (Meteňko, M., 2018) and below). Unlike in the case of a classical criminal outcast group, however, the police are not available for such cybercrime investigation teams. The daily rate of a top specialist in Information and Communication Technologies is calculated at 10 times the hourly rate of working time of forensic technicians.

The complexity of the environment is of paramount importance. For example, if the object is to examine a solitary piece (computer or other technological device intended to cover the needs of the user or owner - mobile, electronic diary, video camera, digital camera, vehicle control module, etc.), which can be easily selected from the environment, then can be sent for

analysis to a specialized forensic / forensic organization while preserving the process rules and functionality of the device and can be examined separately by a highly professional team in the lab. But if it is a large complex object, without the possibility of separation from the system, such an examination must be carried out on the spot.

Large geographic capacity of environment with geographic traces

Computers are connected together around the whole world with the help of private computer network and the Internet, so distribution of distant data and application is possible. A highly experienced perpetrator, who wants to leave minimum traces behind or to make investigation difficult, usually never uses the particular computer directly, but with help of other computers, which are theoretically and practically in absolutely different country or continent. Although the computer network does not recognize geographic boundaries, the investigation is always based on present laws of the country.

Crime scene, involving information and communication technologies, is in some cases impossible to restrict geographically to a particular territory, although the digital traces are limited by very small technological space - chip size, data disk etc. The crime scene can have virtual character due to the fact that some types of the applications use distributed processing concurrently on several distant servers.

Criminalistic and Forensic searching and Investigation thus introduce other aspects in the process that complicate the provision of digital tracks in geographically remote locations with completely different laws. In some countries, the case may not be a criminal offense either.

The crime scene determined by the way it is committed by means of information and communication technologies and in connection with the provision of digital footage, acquires a completely new dimension and content compared to the classic crime scene in the current understanding of forensic science. The crime scene for information and communication technologies can not, in some cases, be geographically trivial limited to a certain territory, although digital traces are limited by their very limited technological space - the size of the chip, data disc or other media is actually quite small. The crime scene may even have a virtual character because some types of applications use distributed processing simultaneously on several physically remote servers for various reasons.

Another factor contributing to large-scale digital footprint distribution is the compatibility of devices, their interfaces, data formats. An example example can be one and the same data file - e.g. Word document, or digital photo, e.g. * .jpg format, which can be stored both on the attacker's notebook and on a personal digital assistant (PDA as well as on a diskette, CD-ROM, USB key, or on a corporate server data server or on a remote server on another continent).

High level of data protection makes the work with the digital traces difficult or impossible

Due to the safety reasons there are a lot of data transitions and nodal points, mainly in file systems and databases, which are cryptographically protected

An important element here is also the personal substrate of protection, which now appears to be the most appropriate place to penetrate (Meteňko, M., 2012).

If we are not familiar with the particular algorithm or technological means, the data in digital form do not have value and information for the investigation and so it is not possible to identify them as digital traces and conduct any further investigation. To amateurs the encrypted file only contains mixture of unfamiliar data. We are able to find and read their content only after decoding them.

In some cases, it is difficult or impossible to continue investigations (offenders usually do not voluntarily announce their technological know - how and deliberately use state - of - the - art technologies that are not yet available to public authorities); in other cases, the injured entity may in certain circumstances provide the investigating authorities with the necessary knowledge , technological and technical means. A corrupted enterprise that has a cryptographically secure database where a defrauding type transaction has occurred, attempts to help identify the offender, discloses all information, and provides the highest system access privileges to investigators and Forensic and Criminal Intelligence Specialists.

A digital trace is automatically identifiable and process able by specialized devices

Since digital traces are generated as a final result by a certain technology, it is feasible to automatically assess the traces by technologies compatible with the former ones supposing

necessary conditions are preserved.

The part of digital traces is the output of the user or the system software. These software's are programmed by set systems and algorithms in a way that the outputs related to these programs have very specific logic and structure, the data format; which is possible to estimate to a certain degree of accuracy.

This aspect is exploited in particular cases by making use of specialized software, which manages to automatically assess digital traces made by algorithm devices, and identifies these traces with pinpoint accuracy.

This feature of digital traces also includes the possibility of searching them with datamining tools, which in the past was not applicable in the field of criminalistic traces, or only some of the advantages of this process - the procedure (perhaps in the future, methods of investigation), were partly used in typing and profiling in criminalistic (Meteňko, M., 2018).

One example is violating copyright laws by installing illegal software into corporate computers. Each installation of legal or illegal software leaves behind some information on the installed product in the system registers of OS Windows.

From the viewpoint of criminalistic and forensic practice, this information is equivalent to digital traces.

If we have general corporate database of officially purchased software products at our disposal and the computers are connected to the corporate network, it is possible to search/scan the system registers of all computers available and specialized user software and to compare the result with the given database.

The output is in fact the list of all installations illegally carried out in every PC, whereas the price of licenses not carried out can also be automatically ascertained.

High level of digital traces obliteration by qualified offenders

As practice shows, highly competent offenders whose professional education is associated with the field of information and communication technologies cause the largest traces.

The offenders are extremely familiar with the keystone of crucial technologies functioning as the ways of the technologies and data protection they have to and are able to avoid, are of great interest to them. At the same time, they are acquainted with the habits and behaviour of employees and the management of a particular organization.

The commonest tactics of hackers hacking computers is gaining unauthorized access to the administrator´s passwords which enables them to perform unlimited activities within the operation systems, including deleting operating and monitoring records/logos of user, distribution and system activities.

Thus, a hacker is proficient in gaining access rights that are a property of another, moreover he/she is able to make use of someone else´s user account and act under a new identity.

Supposing the identity is revealed, the attention is directed towards the innocent victim (Meteňko, M., 2012)

Damaged digital traces restoration

Under specific conditions, deliberately deleted or otherwise damaged digital traces can be restored.

As a rule, this is not true of other criminalist relevant traces. A footprint once deleted cannot be restored.

Digital traces restoration is conditioned by the keystone of operation systems functioning related to the information and communication technologies and techniques which may differ either slightly or substantially among each other, according to the same mechanisms of functioning.

If we delete a file in Windows or in the e-mail, it is possible to restore it in a user´s sense by retrieving it from "the thrash" or "deleted items".

Even if a user does away with these records in a file system, i.e. in its fragments on purpose, the information remains retained for a certain period of time and it may be restored, even completely by special software or by unique procedures. Similarly, hardware restoration is possible.

Digital traces originality

It is very easy to copy the data records, files and their carriers and to generate their duplicates.

During the files and data copying process, no data loss or distortion is caused. This results

from the keystone of digital technologies, respectively from the quality as a technological requirement imminent to digital technologies. That is why providing full proof of originality, i.e. discerning between the original and the copy becomes so intricate, as for instance when submitting proofs at trial proceeding. The above-mentioned problem, explained and perceived in a wrong way may, in extreme cases, result in mistrust towards digital and electronic traces as such.

In particular cases, digital traces can be easily modified without the process of modification leaving any visible tracks of its activity behind. Digital traces, either the copies or the original, may be damaged or destroyed, deliberately or randomly, irrespective of whether they are in memory medium stand still or just being distributed/transmitted over the net.

Digital traces may also be easily modified or destroyed right in the process of collecting or safeguarding it for the purposes of examination and investigation. Unless the standard procedures of digital traces safeguarding along with the thorough and overall documentation are observed, it is theoretically possible to handle even safeguarded digital traces. Naturally, these shortcomings need to be checked and eliminated in a methodical and organized manner so as to make the digital traces acceptable in the courtroom. However, changes may be achieved in positive direction, too. An example is a digital photography of lower quality, caused by a false exposure; a system-defective, blurred shot, balanced in incorrectly coloured way.

At present, specialized software is able to remove the shortcomings to the extent that it is feasible to recognize the face of a person or the license plate of a car. The flow of the process is exact and repeatable at any time with the same effect. Thus, appropriate software may change a primary/original trace which lacks the required information into a high-level quality digital trace which clarifies the investigation.

Low acceptance and knowledge of digital traces by judicial/legal and criminalistic practice

Digital records can catch hold of a picture, sound, different operating values and conditions, user´s activities or the activities associated with automated processes and programs, what is more, they record the values given by exact measurements, data transmission and many more.

Unlike subjective workings of human memory, we are able to reproduce the above-mentioned records over and over again in the same quality and in front of no matter how large the group of impartial observers and experts is.

The problematic issue related to digital traces is theoretical and in some cases also practical possibility of falsification and of challenging the legal quality of traces. However, this possibility occurs within all types traces processed in criminalistic and forensic way.

This leads to a relatively unworkable criminalistic but especially judicial practice of their acceptance and thus of search and exploration. This precedent is also reflected in the current legislation, which remains on the findings of more than 20 years, with reference to "sufficient modification of computer traces". Current trends, however, show that up to 40 percent of offenses are somehow linked to the way of committing or confiscating, which can be investigated using the knowledge of digital footprint theory. Estimates suggest that this percentage will grow for the long term, probably up to 60-80%.

In practice, we are more often confronted with the prejudices of individuals, which result largely from the ignorance of the issue much more than the real reference to the real weaknesses of the communication and information categories. Many information and communication information and related technologies are classified and certified to the same level as no other technologies and technical means. Communication and information technologies contain a sufficient number of logged information mechanisms, so that while observing objectively defined investigative and investigative procedures and corresponding handling of acquired digital footprints, these are credible and undisputable proofs of the activities that took place on the scene or through this technology.

The biggest problem at present is identifying the person who created the digital trace. At the moment, similar mechanisms of individualization and linking between the trace and its object are sought, as is the case with some criminalistic methods investigating static reflection. But more perspective is the plane of reflection of dynamic features known from handwriting, spoken speech, photographic recordings, as well as from the field of trasology or mechanoscopy.

Storing and quality of digital traces is influenced by subjective factors

From the point of safety storing and quality of digital traces is directly proportional to international, national or institutional legislation, experience of system administration and it depends on institutional culture. Regular monitoring and audit of key transactions, providing

storage backup and data archiving from important data sources to a special medium and their long-term storage, play primary role (Gragušová, Ľ., Greguš, M., Kreheľ, O., 2013).

Thus, it plays routine monitoring and audit of key transactions, backing up and archiving data from important data sources (corporate IS, e-mail, etc.) to special media - ideal disk arrays and their long-term storage and protection. From these media, it is then possible to restore required data if required, which are no longer available in production systems. The frequency and frequency of procurement of backup or archive media, the way they are preserved to avoid their harm, the observance of institutional standards and rules, defined primarily in the security information policy and subsequently in the operating order of the ICT department of the institution, are decisive.

The other side of this feature is the above-mentioned still low acceptance and the resulting ignorance and inability to search, secure and pre-examine - to decide on digital objects whether they are digital traces or not, and what will actually be a digital trace. The current situation not only in Slovakia, when we directly banned subjects for work in the city of crime, and during the tours, digital trace and mostly their carriers are ensured for long time unbearable. The need for substantial skills upgrading is a success story in this area, and the future in this area is no different than changing the current access to search and trace processes, as we have said in this section on the characteristics of digital traces.

CONCLUSION

We are exposed to prejudices of individuals made on grounds of unfamiliarity with the subject matter rather that to relevant reference to actual weak spots of communication and information categories. Much information and communication information along with the corresponding equipment is classified and certificated in the safety manner at such level that is simply incomparable with any other technologies. Communication and information technologies contain a satisfactory quantity of the record information mechanisms, so on condition the examination and investigation procedures, objectively defined are observed along with the appropriate handling with collected digital traces, these technologies are reliable and unimpeachable evidence of activities which took place at the crime scene or by means of this technology. Basis for searching, ensuring and research of digital traces are knowledge about criminalistic and forensic concept digital traces. Situation in the field is year pro year worst. More and more traces are not ensured for acknowledge in this area. There are other scientific problem too. One of the main problem is the identification of the person responsible for a particular digital trace.

Only long term basic and applicable criminalistic and forensic research can help to improve the negative situation in the area of digital traces.

This contribution is the result of the project implementation: Centrum excelentnosti bezpečnostného výskumu kód ITMS: 26240120034 supported by the Research & Development Operational Program funded by the ERDF, task 3.3.

References

1. Gregušová, Ľ., Greguš, M., Kreheľ, O., 2013: Štyri kľúčové disciplíny Corporate Governance a IT Governance. In: *Scientific reflection of new trends in management* : Zborník . - Praha: Policejní akademie České republiky, 2013. - S. 29-40.

2. Meteňko, J., et. al.. 2004: *Criminalistic methods and possibilities to check upon sophisticated crime*. Bratislava 2004. Academy of PF in Bratislava. ISBN 80-8054-336-4, EAN 9788080543365. 356 p., p. 7.

3. Meteňko, J., Meteňko, M., Hejda J., 2005: *Digital trace*. 7th International symposium on forensic sciences Sep 29th - Oct 1st, 2005, Častá - Slovak republic. KEU PZ PPZ. Bratislava 2005. (s.182) ISBN 80-969363-2-8. EAN 9788096936325. s. 55-79.

4. Meteňko, M., 2012: Hacker attack to IS, In.:. Ed. Jašek, R*., Internet, competitivneness and organizational security. Process management and the Use of Modern Technologies : mezinárodní konference, : XIV. Annual Internationalí conference :March 27.-28. 2012, Zlín. Czech republic, Univerzita T. Bati, Zlín 2012, CD anotácii a príspevkov. s. 65-69 , www.utb.cz, ISBN 978-80-7454-142-1.*

5. Meteňko, M., 2018: *Stopy v informačných systémoch*. Dizertačná práca, Katedra informatiky a managementu Akadémie Policajného zboru v Bratislave, školiteľka doc. RNDr. Ľudmila Gragušová, CSc.. Bratislava 2018, 167 str.

6. Peťovský, M., Löffler, B., 2017: Teoreticko-spoločenský a sociálny rozmer metód a postupov v služobnej činnosti policajtov. In*: Quo Vadis, sociální práce v ČR?* / David Zámek, Jana Firstová a kol. - Praha : Institut pro veřejnou správu, 2017. - ISBN 978-80-86976-46-4. - S. 196-203.

7. Raburu G., Omollo R, Okumu D.2018 : Applying Data Mining Principles in theExtraction of Digital Evidence, In.:*International Journal of Computer Science and Mobile Computing*, Vol.7 Issue.3, March- 2018, pg. 101-109, © 2018, IJCSMC All Rights Reserved, Available Online at www.ijcsmc.com, International Journal of Computer Science and Mobile Computing, A Monthly

Journal of Computer Science and Information Technology, 088X, IMPACT FACTOR: 6.017, IJCSMC, Vol. 7, Issue. 3, March 2018, pg.101 – 109. ISSN 2320, Dostupné na: https://www.academia.edu/36356745/Applying_Data_Mining_Principles_in_the_Extraction_of_Digital_Evidence.

8. Rak R., Janíček P. 2000: Identification in criminalistic and security practice supported by computer technology, *Expertise* n. *3/2000*, volume V, p. 30-38, 2000.

9. Rak, R.2000: Information science in criminalistic and security practice. Prague, Police Presidium CR, 2000. (471),

10. Rak, R., Porada V., 2003:General and specific features of identification and verification of persons and things from the viewpoint of IT use in security practice in relation to criminalistics and forensic sciences, *Criminalistics and forensic sciences*, Booklet from specialized seminar*, 2003*, Academy of PF in Bratislava, p. 25-63.

Received to editorial office 27.04.2020

SUMMARY

The authors attempted to analyse the possibilities of research and investigating the digital traces and its content, such as a new section of criminalistics and forensic traces. The basis for this analysis is the only first complex scientific book in Slovakia in this area, especially the content of its first part. Detailed knowledge processing was carried out as part of the research of one of the co-authors in European research project. Digital traces are typical of crime related to the misuse of information and communication technologies. In general are to see in all of type crime delicts. However, their using is on the down level opposite other type of traces. Authors in the study distinguish between breakdowns - many types of attributes and sights of digital traces in the criminal activities. In the framework of extensive research during and after the project in Research Activity 3.3, Center for the Excellence in Security Research, ITMS Code: 26240120034, co-financed by the Operational Program Research and Development, shows a wide variety of attributes for research digital traces.

***Keywords**: trace, digital trace, criminalistic and forensic knowledge, research.*

УДК 347.948.2
DOI: 10.31733/2078-3566-2020-2-228-235

Петро БАРАНОВ©
доктор геологічних наук, професор
(Дніпропетровський НДЕКЦ МВС України)

Роман КІРІН©
доктор юридичних наук, доцент
(Інститут економіко-правових досліджень ім. В.К. Мамутова НАН України)

ОСОБЛИВОСТІ СУДОВО-ГЕМОЛОГІЧНОЇ ЕКСПЕРТИЗИ ПЕРЛІВ І БУРШТИНУ

Проведено аналіз законів України, що забезпечують державне регулювання видобутку, виробництва, переробки коштовного каміння та контроль за їх реалізацією. Установлено перелік експертних завдань для дослідження перлів і бурштину, які визначаються походженням каміння та специфічними ринковими відносинами, а також визначено особливості їх судово-гемологічної експертизи.

***Ключові слова:** судово-гемологічна експертиза, перли, бурштин, експертні завдання, видобуток, культивовані перли.*

Постановка проблеми. Перли та бурштин, згідно зі ст. 1 Закону України «Про державне регулювання видобутку, виробництва і використання дорогоцінних металів і дорогоцінного каміння та контроль за операціями з ними» [1], належать до коштовних каменів органогенного походження. Утім, перебуваючи в одній групі, але маючи різні

© Баранов П.М., 2020
ORCID iD : https://orcid.org/0000-0002-3367-4277
pn2dsbaranov.com

© Кірін Р.С.
ORCID iD: https://orcid.org/0000-0003-0089-4086
kirinr@ukr.net