Advances in Social Science, Education and Humanities Research, volume 441
6th International Conference on Social, economic, and academic leadership (ICSEAL-6-2019)

Tracing Crimes in the Economic Activities in the Cyberspace: Leading Approaches and Practices

Vladimir Mecheryakov*
Central branch of Russian state university of justice
20-letiya Oktyabrya str., 95, 394006 Voronezh
Russian Federation
e-mail: netshuttle@mail.ru

Olesya Tsurluy
Central branch of Russian state university of justice
20-letiya Oktyabrya str., 95, 394006 Voronezh
Russian Federation
e-mail: kijalis@yandex.ru

Abstract The active introduction of modern information and telecommunications technologies in economic activities, such as the development of electronic advertising platforms, electronic communication systems and payments, leads to a noticeable reduction in the number of traditional traces of criminal activity and dramatically increases the number of traces in the cybernetic space. In this regard, the importance of developing methods and methods of their detection, fixation, withdrawal and subsequent use increases.
This paper aims to demonstrate the existing methods of working with traces in cybernetic space in the investigation of crimes in the field of economic activity, to identify their advantages and disadvantages. Our results highlight, the necessity of mandatory participation in the main investigative actions of a specialist in the field of computer technology and information and telecommunication systems.

Keywords: *tracing, crime, economic activity, cyberspace, leadership*

1 Introduction

The development of information and telecommunication technologies has a strong impact on all aspects of modern human life and, first of all, leads to the use of electronic means of communication, storage and use of information for various purposes exclusively in electronic form and, as a result, the displacement of paper as a traditional carrier of legally significant information.

Various forms of fraud and abuse in the economic sphere, falsification of registers of information, financial documents, legalization of money and other property, obtaining and disclosure of information constituting a different kind of secret, and other property theft in the modern world are committed to a greater extent through information and telecommunications technologies, which leads to the emergence of traces in the cybernetic space.

Such changes, of course, affected both the criminal sphere and the sphere of detection and investigation of crimes. Currently, an increasing amount of information that is important for the investigation of a crime must be searched, seized and stored in electronic form, which has its own distinct features.

The main problem in connection with the above is the fact that the methods of detection, fixation, removal, research and use of traces of crime in the material environment are unsuitable for similar manipulations with traces in cybernetic space. The purpose of the study is to identify, fix, remove, and investigate evidence-based information stored on digital media. The tasks include justifying the mandatory participation of a specialist in investigative actions, during which information stored in cyberspace is examined and seized, and formulating proposals for fixing electronic documents with unambiguous confirmation of its immutability during investigative and other procedural actions.

The problem under study is relevant at the world level, as evidenced not only by Russian but also foreign studies of the subject.

2 Leadership and leadership styles

Shipley and Bowken (2013) in their publication "Investigating Internet crimes" provide experienced and young investigators with the technical and tactical techniques and tools necessary to investigate crimes committed in cyberspace. The guide provides step-by-step instructions for investigating crimes on the Internet, including

detecting, interpreting, understanding, collecting, and documenting electronic evidence on the Internet for the benefit of the investigation.

Cybercrime is the fastest growing area of crime, as more and more criminals seek to use the speed, convenience, and anonymity that the Internet provides to commit various types of criminal activity. Today's Internet crime includes not only attacks on computer data and systems, identity theft, distribution of child pornography, but also penetrates into the economic and financial spheres, uses social networks for fraudulent actions via email, etc.

Terrorist attacks on computer centers, electronic fraud in international money transfer networks, viruses in our software, corporate espionage in business networks, and hacking of systems on the Internet...Computer criminals are becoming more technically sophisticated, which requires adequate methods of investigating these crimes. A guide to fighting computer crimes, prepared by Icove and et al. (1999), is dedicated to detecting, investigating, and solving crimes in cyberspace. The guide contains basic information about computer security, as well as recommendations for investigators, law enforcement officers, managers and administrators of computer systems. It describes various categories of computer crimes and profiles of computer criminals, risks to computer systems and personnel, and operational, physical, and communication measures that can be taken to prevent computer crimes. It also discusses the tasks of planning, means of detecting and investigating evidence in the course of investigating crimes committed with the use of computer technology, and features of registration and production of investigative actions aimed at forming evidence in the field of computer information.

The book edited by Grover (1989) "software Protection" is devoted to the protection of software from unauthorized access. A wide range of methods of protection is considered: physical, cryptographic, intellectual means of protection, as well as methods of identification of programs and problems of legal protection of copyright: patents, trademarks, license permissions.

The rising number of crimes in the sphere of economic activities involving the use of computer-telecommunication technology, their high latency, and the increase in the spatial scale of criminal activity and size of the damage put the study of this type of crime in a number of priorities for fighting crime at the present time. The presence of significant forensic features of the environment for committing crimes in cyberspace, the high rate of its changes, and the weak legal regulation of information relations both in Russia and abroad lead to the need to develop a generally accepted forensic methodology for investigating crimes committed in cyberspace, which is the subject of Meshcheryakov's (2002).

Vekhov (2008) notes that in modern conditions, computer crimes pose a serious threat to the national security of the Russian Federation, and the fight against them is a priority task of law enforcement agencies, the implementation of which is associated with significant difficulties.

Features of the mechanism of Commission of the considered criminal encroachments, specificity of trace patterns, high dynamics of their development and changes, insufficient legal regulation of public relations in the field of computer information, unequal level of development of telecommunications in different countries of the world, inconsistency of national legislation and the corresponding terminological apparatus in different States have a negative impact on the criminal situation and hinder the effective fight against computer crime. At the same time, the author notes that technical-forensic and information-computer support for the detection, disclosure, investigation and prevention of these crimes is under development; the process of forming forensic recommendations on the tactics of preparation and production of individual investigative actions related to the detection, fixation, seizure and research of computer information and its processing tools is not completed; the system of interaction between the investigation and specialized inquiry bodies and specialists in various fields of knowledge, foreign law enforcement agencies, as well as training in the relevant specialization, is far from perfect.

In the work of Milashev (2004), we consider the method of committing crimes using a computer, the trace pattern left by it, and the tactics of searching, fixing and removing the traces formed during this process. The study of the regularities of the mechanism of forming investigation in the interaction of computer information during the remote impact of computers and the nature of its influence on the resulting trace pattern; identified common approaches to the tactics of collecting data on remote exposure event in computer networks with a focus on the study of computer information; the features of searching for data about the crime event in the computer at the scene and in the attacker's computer, as well as the issues of tactics for removing the computer and computer information, are considered.

3. School principals as leaders

Traces of crimes committed in the economic sphere using information and telecommunication technologies have several features due to the way they are formed and the environment of their existence.

The first feature is the virtual representation of information that is significant for the criminal case under investigation, recorded on a material carrier in digital form. In this case, the main semantic value is not fixed properties of the material carrier, but only the structure and sequence of digital data that reflect the parameters of the formalized model describing the phenomenon of interest to the consequence.

The second feature that you should pay attention to when collecting computer information on cases of crimes committed in the economic sphere is the level of training and technical equipment of the specialist involved in the production of the necessary technological actions. The third feature is the need to determine the conditions for the formation of virtual traces that are removed.

The last feature that should be noted when using computer information during individual investigative actions is the requirement to ensure that the received digital copy remains unchanged.

Features of fixing and removing virtual traces of crimes in the economy are multiple. Detection, and especially fixation, removal and investigation of traces in cyberspace in the investigation of crimes committed in the sphere of economic activity, has the following features:

- the investigator cannot limit himself to direct perception of objects and phenomena, but must use special software and technical tools to perceive information;
- the investigator in addition to the perception of objects and phenomena provides an interactive exchange of information with the cyberspace.

Analysis of foreign legislation has shown that, for example, in the United States, any computer information or electronic document is recognized as evidence based on rumours, and therefore, the party presenting the evidence in electronic form must convince the court that:

- the document was created at a certain time by a knowledgeable person or based on information received from such a person;
- the document was created in the course of regular business practice;
- documentation was a common business practice.

Based on the requirements of the Russian criminal procedure legislation, information can be recorded not only in the form of reports and conclusions, but also presented in the form of other documents executed in writing or otherwise. On the basis of part 2 of article 84 of the code of criminal procedure, the material carriers of such information can be photo and film materials, audio and video recordings, as well as other media received, requested or submitted in accordance with article 86 of the code of criminal procedure. Based on the meaning of this article, the legislator does not make any differences in the forms of presentation of photo and film shooting, audio and video recording. They can be fixed in both traditional analogue and modern digital form.

According to item 11.1 of article 2 of the Federal law of 27.07.2006 No. 49-FZ "On information, information technologies and information protection", an electronic document is "documented information presented in an electronic format, that is, in a form suitable for human perception using electronic computers, as well as for transmission over information and telecommunication networks or processing in information systems" (Federal law 2006).

In accordance with State Standart 2.051-2013, an electronic document is obtained using software and hardware as a result of computer-aided design (development) or conversion of documents made in paper form into an electronic form. Along the way, it should be noted that the specificity of an electronic document is such that the content of a paper and electronic document may differ significantly from each other.

According to clause 3.1.9 of State Standart 2.051-2013, an electronic medium is a material medium used for recording, storing and reproducing information processed by means of computer equipment, that is, devices designed for permanent or temporary storage of data in a form suitable for their use in electronic computers, as well as transmission over information and telecommunication networks (GOST 2013).

This study is limited to the features inherent in the traces of crimes committed in the sphere of economic activity using information technologies and displayed in cyberspace.

The main task of the preliminary investigation is to form evidence in accordance with the procedure established by the current criminal procedure law, on the basis of which the court will make a decision about the event of a crime and all its essential attributes.

Evidence is generated by appropriate subjects based on traces detected on material objects of the environment. In this case, traces are recognized as any information that arose as a result of mutual reflection of objects of the material world, which we are able (as a result of knowledge of the type and nature of the relationship) to link with facts, events and circumstances related to the criminal case under investigation.

When forming material traces, the occurrence of information about an event or phenomenon that occurred is always due to the relationship of a completely understandable physical nature. For example, hitting an axe blade on a wooden door causes the shape of the door's edge Board to change. The shape of this change will match the shape of the axe blade. The classical mapping scheme that underlies the forensic understanding of the mechanism of trace formation. The change of the Board array is inseparable from its carrier – the door Board.

Arguments in favour of the possibility of separation forms by copy (for example, manufacturing in our case, the plaster cast) will not be accepted, since in the course of making the copy we have on one side to deteriorate the

quality of the imprinted form (and the worse, the larger will be part of the substance used for the manufacture of the cast), and on the other hand bring your extra change, due to imperfections in the instruments used and skills of a person are made a copy. In any case, it will never be possible to make a copy without loss of quality, and making a copy from a copy in General can lead to the fact that the resulting result will be unsuitable for solving not only identification, but also diagnostic forensic tasks.

A fundamentally different display scheme occurs when creating virtual traces (the digital form of fixing which we get from computer media). Let us take a case where a real phenomenon (for example, the same blow with an axe on a Board) is recorded by a video recorder. During this fixation, an electronic-digital display is performed, based on the use of a formal model of the real phenomenon to be registered, which has a number of very significant properties for criminology.

First, the mapping takes place in an artificial environment of a formal (most often mathematical) model, which reflects some features and properties of the simulated phenomenon with a given quality and completely ignores others. As a result, not all types of interaction of objects of the surrounding world that exist in nature are recorded, but only those that were provided by the Creator of this artificial environment.

Video recorder designed to capture images in the infrared range of electromagnetic waves will see warm objects well and will not register cold objects at all (which coincide in temperature with the environment).

Moreover, the quality of registration of changes in an artificial environment will be due to the technical capabilities (in our example resolution, viewing angle of the lens) or the settings of the data logger (for example, if the DVR is triggered from a motion sensor, depending on settings of the sensor it may not fix the slow changes such as unfolding flowers, changing the position of the solar shadows, etc.)

Secondly, it is not the formalized model itself that is subject to registration on a material carrier (it is usually embedded in the design or software of the registration tool) of the observed phenomenon, but only its parameters in the volume and quality that allow further forming an idea of the recorded phenomenon. In fact, digitally recorded virtual traces can be copied as many times as necessary without losing their forensic quality.

Third, the semantic essence (meaning) of virtual traces recorded in digital form is not fixed in the carrier material, as in the case of material traces, but in the structure and sequence and meaning of digital data. As a result, the connection of the trace with an event related to the criminal case under investigation is not determined by the properties of its material carrier. For example, an image with the same quality can be recorded on an optical disk (where the physical storage medium is the presence or absence of holes in the reflective layer), or on a magnetic disk (where the physical storage medium is a magnetic domain) or a solid-state NAND memory of a flash drive. Sometimes it is possible to convert the formats of this image (for example, JPEG, TIFF, etc.) without losing the forensic qualities of fixing traces.

Thus, when copying computer information in compliance with certain technological requirements (sometimes different for different forensic tasks) without loss of forensic quality, it is possible to use material carriers of different types, sizes and formats (the file system used), including some of their number.

Our analysis of Russian and foreign experience of investigation of crimes in the economic sphere has shown that the tangible media, most frequently during the investigation of criminal cases and sent for testing within the forensic computer forensics are the following objects:

- computer devices (workstations, personal computers, laptops, tablets, etc.);
- SIM cards;
- mobile phones, pagers, smartphones, voice recorders;
- flash cards, optical disks;
- cash registers;
- individual computer programs or its systems, as well as other objects of copyright, etc.

The vast variety of these objects already reflects the breadth of knowledge that should be possessed by the specialists for the production of copy in computer information from them. It’s necessary to work with various States of this technique (serviceable/faulty, on/off) only expands the range of required knowledge, skills and technical equipment.

Given the specificity of the formation and transformation of information stored and transmitted in electronic form, under procedural law investigative actions are performed with the obligatory participation of a specialist possessing the appropriate skills needed to produce the required action program-technical means and skills to use them and sufficient qualification.

The level of development of modern information technologies has recently increased so significantly that more than a dozen independent engineering specialties have been formed within this area, which differ significantly in both the volume and type of knowledge and skills covered. Moreover, these differences are not so obvious for an investigator or interrogator who has a classical higher legal education and has special knowledge in the field of radio electronics, computer technology and information technology. For example, finding out the differences in the qualifications of a radio-electronics engineer and an electronic engineer required to assess the

readiness of such a specialist to solve forensic tasks within the framework of a planned investigative action becomes a very non-trivial task.

In this regard, it is categorically impossible to agree that the requirement of the criminal procedure legislation to attract a specialist to remove electronic media is excessive and does not correspond to the current level of technical literacy of the entire population. The opinions expressed by some authors that modern information technologies are so easy to use that they practically do not require special skills and knowledge for their correct use seem unfounded to us.

The provisions of part 3 of article 164.1 of the criminal procedure code of the Russian Federation establish the right of the investigator to copy information contained on an electronic medium during the course of an investigative action. At the same time, the Protocol of the investigative action must indicate the technical means used for copying information, the procedure for their application, the electronic media to which these means were applied, and the results obtained. The Protocol must be accompanied by electronic media containing information, which is copied from other electronic media found during the investigation (Federal law 2001).

In our opinion, independent copying of information from electronic media by an investigator is permissible in exceptional cases, when the information received will be used solely as a guide and will not become the object of expert research in the future.

A separate conversation is required by the level of technical equipment of the specialist involved in solving problems of copying computer information. This primarily applies to the computer equipment used by them (portable computers, laptops, tablets), auxiliary switching equipment (various types of cables, adapters and adapters) and peripheral equipment (copiers, hubs and splitters), as well as special software.

The range of such equipment is extremely wide and is represented by both open Source and proprietary developments. Since there are no standard requirements for the selection of the composition and characteristics of such equipment, their selection is carried out by the specialist himself based on his own experience and ease of use for solving tasks.

In some cases, to solve a certain category of issues that arise during the investigation of a criminal case of economic orientation, not only the copied set of digital data itself is required, but also the equipment that registered the real process, as well as the original physical medium on which the corresponding record was made.

In this regard, in some cases, it is absolutely ineffective from the point of view of the investigation of a criminal case to use the right granted by the criminal procedure law to the investigator or investigator to independently copy information from electronic media, without their subsequent withdrawal. However, in accordance with the requirements of part 2 of article 164.1 of the criminal procedure code of the Russian Federation, electronic data carriers are seized during the course of investigative actions with the participation of a specialist.

One of the simplest and most effective ways to confirm the immutability of the computer information copied during the investigation is to count and fix the checksum (hash function) of the file.

In accordance with clause 3.1.5 of GOST R 34.11-2012, a hash code is a string of bits that is the output result of calculating a hash function (GOST 2012). This function allows you to build an unambiguous match of any set of digital data (one or more files, and even the entire material carrier of digital information) and a string of bits of set length. At the same time, the probability that the same hash function value will correspond to different data sets is negligible and changing at least one bit in the original data set leads to a drastic change in the hash function value.

This technology makes sure that the information seized during the investigation was unchanged in the future.

In this regard, in our opinion, in the Protocol of investigative action, during which computer information is copied (digital video or audio recording, computer program, database, etc.), it is necessary to reflect the value of the hash function of the seized information objects, as well as to inform the person from whom this information object was copied, with a mandatory note about this in the Protocol of investigative action.

4. Conclusions

Thus, the mandatory participation of a specialist in the production of investigative actions for the inspection and seizure of information contained in electronic media is a positive legislative requirement. This is also due to the position of investigative tactics, since the specialist can notice what is hidden due to the lack of special knowledge from the investigator. In working with electronic media, the investigator does not have enough General forensic knowledge.

According to this, we propose to Supplement the provisions of the criminal procedure legislation with the following content.

The Protocol of the investigative action must specify the hardware and software used in copying information, the procedure for their use, the electronic media used and their characteristics, as well as the values of hash amounts copied during the investigative action of information objects.

The tasks of further research within the topic will be the methods of research and use of electronic documents found and seized during investigative actions, taking into account the specifics of recording and storing information.

References

Gavrilin YuV, Investigation of illegal access to computer information: Studies. Handbook, 1st edn. (Moscow: Knizhny Mir, 2001), 88 p.

Grover D, The Protection of Computer Software: Its Technology And Applications, 1st edn. (Cambridge: Cambridge University Press, 1989), 279 p.

Icove D, Seger K, VonStorch W, Computer Crime: A Crimefighter's Handbook (Computer Security), 1st edn. (Massachusetts: O'Reilly Media, 1999), 351 p.

Kasatkin AV (1997) Tactics of collecting and using computer information in the investigation of crimes. Diss. Cand. The faculty of law sciences. Moscow: 215 p.

Lytkin NN (2007) The Use of computer-technical traces in the investigation of crimes against property. Diss. Cand. The faculty of law sciences. Moscow: Moscow University of the Ministry of internal Affairs of Russia: 201 p.

Meshcheryakov VA, Crimes in the field of computer information: fundamentals of the theory and practice of investigation,1st edn. (Voronezh: Voronezh state University Press, 2002), 408 p.

Milashev VA (2004) Problems of search tactics, fixation and removal of traces in case of illegal access to computer information in computer networks. Autoref. Diss. Cand. The faculty of law sciences. Moscow: 21 p.

Ostrovskiy OA (2019) Aspects of modern problems of the investigation of crimes related to the elimination of digital traces and the provision of relevant evidence. Vestnik of Altay academy of economics and law 3(1):146-151

Polyanskaya OY, International practice of the criminalization of computer crime, 1st edn. (Moscow: Federal state budgetary institution of science Institute of scientific information on social Sciences of the Russian Academy of Sciences,1998), 128 p.

Rosenblatt K, High-technology Crime: Investigating cases involving computers, 1st edn. (KSK Publications San Jose, 1995), 603 p.

Semikalenova AI, Ryadovskiy IA (2019) The use of special knowledge in detecting and fixing digital traces: analysis of modern practice. ResearchGate 7:57-60. doi: 10.17803/1994-1471.2019.103.6.178-185.

Shipley T, Bowker A, Investigating Internet Crimes, 1st edn. (Waltham, MA:Syngress, 2013), 496 p.

GOST (2013) State Standart 2.051-2013. http://docs.cntd.ru/document/1200106860 Accessed 29 Apr 2020

Vekhov VB, Fundamentals of forensic science about research and use of computer information and means of its processing. Monograph. (Volgograd: VA MVD of Russia, 2008), 401 p.

Zuev SV, Cherkasov VS (2016) New rules for removing electronic media and copying information. Zakonnost' 5: 40-43

Federal law (2001) Federal law 18.12.2001 N 174-FZ "Criminal procedure code of the Russian Federation". http://www.consultant.ru/document/cons_doc_LAW_34481/ Accessed 19 Apr 2020

Federal law (2006) Federal law 27.07.2006 No. 49-FZ "On information, information technologies and information protection". http://www.consultant.ru/document/cons_doc_LAW_61798/ Accessed 19 Apr 2020

GOST (2012) State Standart 34.11-2012. http://docs.cntd.ru/document/1200095035 Accessed 22 Apr 2020