International Journal of Criminal Investigation

Volume 1
Issue 4
187-194

FIXATION OF TRACES AND ORGANISATION OF INTERACTION WITH AN EXPERT IN INVESTIGATION OF ILLEGAL ACCESS TO COMPUTER INFORMATION OF A BANK

Kirill Kostomarov
Postgraduate of Ural Institute of the Russian Presidential Academy of National Economy and Public Administration. Ekaterinburg, Russian Federation

Abstract

One of the main problems for an investigation of illegal access to computer information of a bank for today is lack of special knowledge. Depending on a situation an expert can help inspector on each stage of an investigation of a crime. Without organization of qualified interaction with an expert it is difficult to obtain an evidentiary basis.

This research is a attempt to systematize knowledge on these issues and provide guidance for resolving difficult situations, optimize actions of inspector in revealing of information traces to a successful investigation. Special status of bank information causes specific procedures.

Keywords*: illegal access, bank, computer information, traces, expert*

Introduction

Revealing of computer crimes is impossible without mastering special knowledge by inspectors. However, according to the survey we conducted, only 16% of inspectors working on computer at user level. On the other hand the survey of computer experts uniquely pointed out that at current development of computer technologies without special knowledge it is extremely difficult to find hidden information and information traces in computer without risk of their destruction — so consider more than 90% of interrogated respondents.

Therefore it is possible to ascertain that help of experts at detection, fixation and withdrawal of traces of illegal access to computer information of bank is not reinsurance as it may seem at first sight. Necessity of help of an expert is caused by that evidentiary information held on machine carriers is in danger of destruction or modification during unqualified actions, and necessity of carrying out of such survey without attraction of an expert should be thought carefully over the person who is appointing and carrying out an inspection. Evidences of a crime, which are located on computer magnetic storage media, may be inadvertently and irrevocably destroyed, if not complied a special procedure of actions with information carrier as a technical device, and a special procedure for inspection of information contained in it [1]. With regard to computer information of bank, such recommendations should be built into an absolute, since any violation of integrity of an information system, loss or modification of data, could lead to material losses of bank and its customers.

However, it would be wrong to put an investigation in a complete dependence from an expert. For effective interaction with an expert it is necessary for inspector to know about character of searches; what kind of traces an expert searches; about actions which an expert should undertake for purpose achievement. Tracking picture at fulfilment of illegal access to computer information is specific enough that provides an originality of search, withdrawal and use of traces in a course of investigation (in forensic science there is even a suggestion to unite research of this issues in a new branch of forensic techniques - «forensic computer science»[2, 3]). By world measures, traces of crimes in sphere of computer information in Russian practice have started to research rather recently and have found a reflection in works of V.B.Vehov, V.V.Krylov, JU.V.Gavrilin, A.G.Volevodz [4, 5, 6, 7] and other scientists from the end of 90th years of the last century.

Features of computer information

From the standpoint of forensics, computer information has a number of features and properties without which it is difficult to exclude risk of its inadvertent modification or destruction during the manufacture of the investigation. Some duality of computer information is provides its technical nature: information by its nature is immaterial and should be noted that its content does not depend on a kind of the used material carrier; despite the non-material nature of the information, computer information can be found only on material carriers: first of all in computer (on a hard disk, in its RAM etc.) or computer system (for example, related peripherals, remote terminal units); in computer network (network cable, access points, radio broadcasting, RAM of communication devices, etc.). For today paper carriers can't be taken seriously as sources of the computer information (punched cards, punched tapes, a paper). It is not justified neither with criminal law, nor with forensic point of view. The volume of use of punched cards and punched tapes is minimal. Probably in the near future will refuse to use them at all. The main property of material carriers of computer information consist in the digital nature of its representation which is impossible to tell about a paper; computer information is very easy to destroy without essential time expenses. At the same time variants of preservation of data even after its removal are not excluded. In such cases first of all it is recommended to stop all work on the computer in order to avoid modification of the computer information, turn it off and give it to an expert. Further it is possible to use software products which allows to restore destroyed or changed information. Under the terms of the proper storage and use of a material carrier, computer information containing in it is not destroyed spontaneously when it is used, regardless of a number of transactions carried out. In due course there is a physical deterioration of a data carrier, but information only can become outdated and lose a relevance. For example, with use of illegal access to computer network of Sony company authorization data of bank cards have been stolen. However this theft is not dangerous to end users because this database more than three years old. To a person far from systems of electronic payments this information may seem insufficient, however to an expert of a corresponding profile it is clear that bank cards automatically reissued (with replacement of the data of authorization) with average periodicity in two-three years. Therefore criminals cannot really use stolen data directly.

Besides it fast both simple processing and transfer computer information by telecommunication channels wired, optical, wireless and various kinds of other communications. With existing technologies it is possible to transfer huge volumes of information almost on any distances for rather short time interval. Computer information can be created, modified, copied, used only with help of computer technology with necessary technical devices. From the point of view of forensic science important that computer information can be transferred on other machine carrier without leaving it on a primary source, or can be copied (left on the primary source). As a result the identical copy of content of computer information is created which can be made in any necessary quantity — this limited only by technical possibilities. This feature should be considered, for example, at investigation of illegal access to bank information located on round the clock functioning server. If there is no reserve server, then withdrawal of an entire server or all of the carriers of computer information from a server most likely will lead to a stop of work and significant losses, , whether material or reputation. More appropriately by means of an expert to make two copies of necessary information: one for an expert researches, one — as a backup.

Generalizing information nature we can assert that the most well-founded point of view on classification of traces in this category of cases is the classification designated in the works of JU.V.Gavrilin and N.G.Shuruhnova. Traces of crimes in sphere of computer information are classified on two big groups: traditional traces and information traces [8].

Traditional and information traces

At fulfilment of illegal access to computer information often remains traditional traces of criminal activity (were withdrawn in 76,9% of investigated criminal cases). It may be personal papers of suspected persons (hand-written records left on a workplace, draught copies, corporate notebooks etc.), documents on hardware and software, duty regulations, listings of telephone accounts, here it is necessary to carry traces of hands (on a system block, keyboard keys, on a desktop, on a surface under monitor and other

devices). In this part an expert is necessary only in a case when in documents appears technical terminology, jargons from a sphere of information technology, references on hardware and software.

Basis of a trace pattern of studied category of crimes — information traces. In scientific literature there is no unity on this question, and there is a variety of approaches to definition of information traces and their essence.

So, V.A.Meshcherjakov, displaying a definition, introduces the concept of "virtual traces", as a certain additional plane between traces material and ideal. «Virtual traces» he understands as any change in a state of automated information system, associated with an event of a crime and recorded in a form of computer information on a material carrier, adding it with concept of "cybernetic space" where includes everything that related with computer technologies. In our opinion, such difficultly perceived and transboundary concepts, without any necessity on that definitions of information traces complicating the formulation, are unnecessary. V.N.Tcherkasov adheres the same opinion [9]. F.G.Aminev described traces defines as traces of hi-tech data carriers - that is disputable enough decision as till now there is no settled practice on a question - what are hi-tech objects, and the circle of such objects is unreasonably wide.

Much more reasonable we see the definition of information traces as changes of information environment in a form of signals and codes on electronic and other physical carriers. It would be desirable to notice, that information environment it is always set of technical and software storage, processing and information transfer (i.e. both the information, and its carrier). Thus, the definition is burdened by reference on data carriers which in this case is not required.

This way, information traces are changes of computer information caused by influence on it of a criminal, using hardware and program components of computer technology. Result of such influence are changes in a state of these means of computer technics and information containing in them. According to some reports in 47% of cases information traces are reflected in the form of change of file structure, in 31 % - in the form of modifying of a content of computer information, in 17 % of cases were expressed in unusual kind of work of a computer. In borders of investigated information environment, search of given changes will be a primary purpose of interaction of an inspector with an expert.

The mechanism of formation of traces of illegal access to computer information of banks has essential features caused by specific conditions of formation, storage, use of electronic databases of these financial institutions.

Traces on "workplace" of a criminal (location of technical means by which illegal access was made, more often — a place of extraction of an information) on all kinds of computer information carriers. In cases of remote access it is difficult to reveal a "workplace" without preliminary technical training.

In a case when a crime is finished, there is a suspect and a place of extraction of information is revealed (earlier — more probability of that a criminal has not undertaken attempts to hide traces), certain changes can be found, first of all, in special logs of computer system such as: system log in which system processes and events are displayed; activity of drivers including hardware components of a computer; application log which displays activity of user programs, including all errors, logon attempts, changes in use of an information carrier; security journal which captures audit events, monitor changes in powers of user's security policy, access both to files and catalogues, as well as to a system. In these journals information traces represent records which are made by operating system and they are important sources of the data about time and types of processes occurring in a given specific computer. It is necessary to give special attention to information processes which have occurred in time borders when a crime happened. Further it is necessary to check up: suspected possessed qualities necessary for performance of revealed operations with computer facilities or not and whether they were reflected in traces of illegal access to computer information.

Intermediary carriers of computer information also can become an important source of evidentiary information, especially in situations of lack of information about a suspect. It can be intermediate servers, communication centres, network cables through which criminal carried out connection with computer system, subjected to illegal influence. Through them connection with attacked computers is usually carried out. An

expert in this case will help to reveal all potential carriers of necessary information. Such help is especially actual in conditions of complicated network structure of the bank, an extensive system of subordination and interaction of computers within local and global networks. To reveal them, it is enough to imagine an information transit since network traffic always leaves traces along a way on which it follows. Routers, firewalls, servers, sensors IDS — variety of network devices create audit logs where record network events. Existence of bank without such devices for today is hard to imagine. To give a full traces picture it is necessary to check up all available network devices on a way between an attacked computer and a system suspected of carrying out of attacks, but in practice to check up all logs of these network devices is extremely difficult. Usually logs are geographically scattered, fixed in a large variety of formats, sometimes created by several different operating systems. Their system time uncoordinated, and for access to them requires special software. All it complicates reconstruction of network event. Character of search in an absence of a suspect for situations of complete and proceeding crime has many general recommendations. However in a case of a proceeding crime it is necessary to direct all volume of knowledge of an expert on an establishment of a site of a criminal for his arrest. If there is no reliable information that a crime is ended, it is recommended to consider that its proceeding before vulnerability in information security will be eliminated, or till detention of a suspect in a commission of the crime. At any development of a situation, one of key problems of an expert - searching the place of extraction of information.

Search of "workplace" from network logs by IP-address — difficult enough procedure because it can be forged or be hidden behind a whole chain of transit sites from a true source of attack. The main difficulty consists in that an IP-address belongs to a computer, not a person... Accordingly, if time of illegal access is unknown, it is difficult to identify a person using a given IP-address at a moment of commission of a crime. Knowing the exact time of remote connection allows to narrow a circle of suspected persons. Because operating data sent by an attacker to a specific electronic address in network, it is possible to consider as a scene of crime a computer possessing the unique IP-address. It is known that a place of storage of information and a place of its withdrawal may not coincide. Therefore, at remote connection we suggest that as a place of its withdrawal it would be possible to consider a place of storage of information a computer with a unique IP-address. For an establishment of a connection time of a subscriber in network appropriate cooperation with a provider.

In course of search of a place of extraction of information it is necessary to not forget that at initial information vacuum all kinds of carriers of computer information on a place where occurred result of illegal access become basic sources of information traces (a computer of bank employee; a bank server etc.). Such traces are typical for crimes of a considered kind. It is connected by that first of all investigation begins with survey of computer system of bank. Thus studying of great volume of information quite often is required. In certain cases given actions become simpler. For example, if on attacked computer system anti-virus program provided a mode of preservation of suspicious files, this will allow to narrow search borders.

It is possible to upload to a computer special programs to search for hidden or deleted information [10, 11]. In our opinion, a given approach in an environment of bank information structure should be used only in cases of emergency caused by limitation of time for increasing possibility of revealing and detention of a guilty person, neutralisation of distribution of harmful programs in network of bank from a target computer and in other emergency operations. Such circumstances can take place at investigation of a proceeding crime. In all other cases it is necessary to search required information on an examined machine carrier without direct copying of software on it in objectively realized variants of connection that will exclude development of negative processes and consequences. Whenever possible, it is necessary to inform an expert in advance because for this approach hardware of the advanced level is necessary. Of course, material cost of such equipment is very high, but to draw your attention to the fact that most of modern hardware is back compatible (modern interface USB 3.0 is compatible to existing equipment USB 2.0; wireless communication standard 802.11n is back compatible to standard devices 802.11b or 802.11g in a range 2,4Ghz and with devices 802.11a in a range of 5 Ggz etc.), allows not select

a hardware component on each separate case and have a single universal set of hardware. Cost of such hardware equipment will be ten times less than a potential damage of bank from a loss of an information database in case of unsuccessful operations of an expert and an inspector directly on a bank computer. Therefore, in our opinion, in this part financing on these purposes should not be limited.

Without use of special testing tools in a search of information traces their range is poor enough: it is possible to reveal renaming's of files, change of their contents, size, revealing of new files, catalogues, logic disks, unsuccessful attempts of entrance or access to a file with a restricted access, network overload, stream of network packages of certain type for a short interval of time, failures in work of remote terminal units, execution of commands with failures, slowed down work of a system, sudden reboots, inquiries to services.

If you use special software for testing this will expand such important traces as: changes in system register, detailed information about password selection attempts, infringement integrity of files and folders, fixed facts about revealed DoS attacks in traffic, processes with virus maintenance, equipment inventory. These information traces are differs by a regularity of action and considerable volume of affected sites. Their importance is hard to exaggerate, because on a basis of these characteristics inspector puts forward version about kind of traces, ways and places of intrusion into system (or a network).

Fixation such traces is carried out is similar without dependence from a place of their revealing. With a help of an expert it is possible to observe actions of programs, contents of text files, databases, results of anti-virus work and test programs etc.

Russian literature in this case provides such operations procedure: to determine what program is carried out. For this purpose it is necessary to examine an image on a display screen and, if it possible, in details describe it and record by available means; stop program process [12]; record (reflect in a report) results of actions and computer reactions to them; to determine presence of external devices-stores of information on a rigid magnetic disk (winchester) at a computer; determine presence of external devices of remote access (for example, modems) at a computer and estimate their condition (reflect in a report). After that - separate network cables, so that nobody could modify or destroy information during survey (for example, disconnect a telephone cord), switch off energy giving in a computer and further operate under a scheme of situation with not working computer.

Necessity of a stop of execution of a program at a research initial stage seems to us disputable enough. The decision on it is necessary to take in a concrete situation in presence of certain circumstances taking into account opinion of an expert as in this case probability of loss of important data is high. When disconnecting power a content of computer technics RAM, which also may contain information necessary for a investigation, will be lost. There is also the opposite point of view which authors unequivocally specify expediency of greatest possibility of gathering of information from working system, at a stage of initial reaction. And in this case the term "working" is applied to all systems that are relevant to a case – it can be a system of storage of information, subjected to attack; intermediate system; and attacking system — on a place of withdrawal of information.

It is necessary to notice that this approach can achieve much more information than purely visual fixation of an event on a screen of a working computer and shouldn't underestimate information received with such a way.

Expert of appropriate level also is able to solve a problem of fixation of an information flow for a further analysis by inspector in various conditions of information environment. The level of development of computer technologies to date already initially implies a presence of network connection. But still, if there is no such a connection or a time for its organization is limited – it is easier to save files of a conclusion to trusted digital carriers or a hard disk of target system. In all other cases it is advisable to keep information at a remote workstation. Modern software for these purposes requires an IP-address of target network and a portable system with sufficient memory size to storage collected information.

Thus there is an information transfer through a target network for a future possibility to see it after reaction on an incident. After reception at an expert workstation is initiated and all entering

data is redirected to a file, by means of specialized software a check of integrity of files is made for exception of forgery and modification. It is strongly recommended to carry out this operations in presence of identifying witness [13].

Special conditions for a bank storage of information imposes additional specificity that is expressed in a necessity of encrypting of sent information. With reference to bank information (and to any other kind of confidential information) — this factor is a key in a choice of method of information transfer and software. Encrypting creates two serious advantages: network analyzer of an attacking cannot compromise received information; encrypting of data almost excludes risk of damage or substitution of information [13].

In a situation if a computer is turned off, follows [14]: reflect precisely in a report and in an applied scheme location of computers and peripherals; exactly describe a connection form among these devices with instructions of features (color, quantity of connection sockets, their specification) of wires and cables; before a separation of any cables it is useful to carry out videorecording or photographing of places of connection; preliminary provide all safety measures and separate computer devices; pack separately (with instructions in a report and on an envelope of a place of detection) carriers - diskettes, compact disks, flash stores and magnetic tapes (individually or groups) and place them into covers which are not carry a charge of statistical electricity; pack each device and connecting cables, wires, bearing in mind the need of an accurate transportation; protect hard drives, according to recommendations of the manufacturer. The important remark if during survey and withdrawal computer start is required - it is necessary to do it by means of own loading bootable carrier in order to avoid start of programs of a user [13].

The recommendations above are fair also in situations when a crime has been revealed already after plunder of money resources from a bank account. But there are some reservations since the main place of fixation of traces often become a computer of a bank client. For example, on a computer of bank client, search of information traces will be concentrated on a check of means of remote banking services, movement of material resources and ways to follow, contacts of a client via e-mail, technical possibilities of a remote authorization, search of espionage software, etc. Many information traces fixed on a computer of a bank client is more expedient to duplicate by vindication of certificates of a bank (about movement, removal, rest of material resources; about time and duration of RBS sessions etc.) . Clients of bank very often have low enough knowledge level of information technology. Even in conditions of an advanced systems of information security with use of EDS, there are variants when a client ignores all possibilities of protection featured to him: writes authorization data on a sheet of paper («not to forget») near computer on which RBS programs are installed; holds constantly connected EDS, i.e. it is constantly authorised; authorizations become well-known etc. Known facts of neglect protection also is necessary to fix in details.

Other conditions for searching traces are created by a situation when bank information became publicly available, or went on sale on the Internet. Originally in common with experts of bank it is necessary to fix that the given information really is a part of banking secrecy, and not a gimmick of swindlers or even more primitive – is a public. Fix all volume of confidential information become publicly available at the given stage. Further fixation of traces will already occur within limits of operative actions as a control purchase or a detention of criminal at crime scene. The main objective — fixing all volume of leak of bank information and a mechanism of illegal access to it during which it have been stolen. The last, most likely, will be possible to record only after revealing of a workplace of a criminal, following the recommendations given above in a situation of absence of a suspect.

Direct and remote access

In summary, it is necessary to note direct dependence of an arrangement of traces of illegal access to computer information of bank from a place of commission of a crime, thus special value has also a way of commission of a crime. For example, at direct access all traces of criminal influence are in one place - in a computer system, exposed to influence, and in a space of immediate proximity to this system. At remote access a search of traces becomes complicated, because through system of traces on an attacked computer it is necessary to track arisen changes in computer information including on intermediate servers and telecommunication lines, and then reveal a traces

picture on a computer from which illegal access was provided.

Fixation of all commands which are carried out on a computer is very important for investigation. It can help to reveal to inspector professional level of a criminal; degree of knowledge of a criminal about information environment of bank; reveal possible accomplices of a crime; reveal intention of a criminal. In cases when illegal access was subjected to whole computer network of a bank its employees should be instructed about preservation of traces of influence. It is necessary, that traces remained in an invariable form before their fixing and withdrawal by law enforcement officers. For this purpose it is expedient to specify to users of personal computers about inadmissibility of reboot of computers, reinstallation of an operating system or separate programs, removals or changes of files.

Against the background of the above it is difficult to overestimate importance of knowledge of an expert which is necessary for making well-founded decisions by an inspector during investigation of a criminal case. In case of use of data which subsequently has been not confirmed with an expert research, inspector conclusions about presence of signs of illegal access to computer information of bank can lead to unreasonable excitation of a criminal case. G.V.Semenov has precisely enough formulated the vision on this question, having designated, on the basis of practice of disclosing and investigation of crimes in sphere of computer information, that without special knowledge it is not only difficult, but sometimes it is impossible to solve a question on presence of signs of a crime in checked facts, and also to find out, fix and withdraw corresponding evidentiary information [5].

Frequently possibilities of a preliminary research of material traces with participation of an expert considerably complicated by various circumstances. It may be presence of any special protection frames of computer information from extraneous access to it (passwords, encoding, physical restriction of access, etc.), and impossibility to make reserve copying of initial information and, as consequence, significant complication of research of computer means outside of laboratory conditions. Such restrictions may not allow to receive necessary information in a required amount. Then decision on a criminal case excitation is taken proceeding from another checked up and confirmed information, then objects of computer technics are sent for production of research by an expert.

Professional knowledge of experts also is demanded in manufacture of investigatory actions and operatively-search actions — technical consultation is necessary for an inspector at detection, description, packing according to all requirements and subsequent transportation of withdrawn hardware of computer technics, machine and paper data carriers which may contain information traces of a crime, assistance in formulation of questions to an expert, etc. It should be noticed that information technology are various, and a choice of an expert for specific tasks at times difficult. V.V.Krylov adheres to such point of view and fairly notices that search of such experts should be spent beforehand at enterprises and institutions which are carrying out service and operation of computer and communication technics, in educational and research organisations, and in extreme cases - to involve employees of a suffered organisation.

For example, in a course of preliminary research of material traces you may need an expert possessing knowledge in a field of elements and devices of computers and control systems, familiar with questions of functioning of automated control systems in a case there will be a problem of withdrawal of technical means. The expert possessing in additional volume of knowledge in a field of software of computing systems and organisation of computing processes, and also knowing bases of methods of protection of information and information security can be irreplaceable at an establishment of facts of penetration of information systems from the outside. An expert with advance knowledge of hardware and software of computer complexes, systems and their networks, communication centres and information distribution possibly is required in researching computer system and their networks [5].

Conclusions

With today level of technology it is difficult to investigate cases of illegal access to computer information without help of an expert. In bank specific independent actions can lead to serious financial losses. Recommendations presented in this article will help to organize process of investigation with taking into account the

characteristics of both: computer information and bank information. Future research should focus on further development of the situational approach by taking into account details of new technologies.

References

1. Yakovlev A.N. Theoretical and methodological foundations of an expert research of papers on computer magnetic information carriers. **PhD dissertation;** 2000; 115.
2. Vekhov V.B. *On the question of subject, system and tasks of forensic computer science.* **Forensic readings dedicated to the 100th anniversary of birthday of Professor Boris Shevchenko: Sat. of articles;** 2004; 55.
3. Yablokov N.P., Golovin A.Y. **Forensic science: the nature and the system;** 2005; 134-135.
4. Vekhov V.B. *On the question of subject, system and tasks of forensic computer science.* **Forensic readings dedicated to the 100th anniversary of birthday of Professor Boris Shevchenko: Sat. of articles;** 2004; 63.
5. Krylov V.V. **Investigation of crimes in the sphere of computer information**; 1998; 170-198; 218.
6. Volevodz A.G. **The legal regulation of new areas for international cooperation in criminal proceedings**; 2002; 279-326.
7. Gavrilin Y.V., Lytkin N.N. *Definition, properties and forensic value of computer-technical traces of the crime.* **Bulletin of criminology** 4 (16); 2005; 49-55.
8. Shuruhnov N.G. **Investigation of illegal access to computer information: Manual**; 2004; 152-162.
9. Cherkasov V.N., Nekhorosheye L.B. *Who lives in a "cyberspace"?* **Management of information security**; 2003; 467-469.
10. Aleshin V.V. **Theoretical problems and practice of investigation of crimes involving foreclosure citizens**; 1999; 23.
11. Krylov V.V. **Information computer crimes**; 1997; 80-81.
12. Zubaha V.S., Usov A.I., Saenko G.V. **General provisions for an appointment and conduct of computer-technical expertise**; 2001; 189.
13. Mandia K., **Prosise C. Incident Response: Investigating Computer Crime**, 2005. 240-262
14. Krylov V.V. **Modern forensic science. Legal Informatics and Cybernetics;** 2007; 222-223
15. Semenov G.V. Investigation of crimes in the field of mobile telecommunications. **PhD dissertation**; 2003; 159.