RAIS RESEARCH ASSOCIATION for INTERDISCIPLINARY STUDIES
August 2021

DOI: 10.5281/zenodo.5506942

Some Tactical Aspects of Computer Search

Nicoleta-Elena Hegheş[1], Nelu Niţă[2]

[1] "Dimitrie Cantemir" Christian University of Bucharest, Romania, nicoleta.heghes@ucdc.ro
[2] "George Bacovia" University of Bacău, Romania, nita_nelu@yahoo.com

ABSTRACT: Due to the process of globalization in general, and computer networks in particular, as a result of the continuous development of information and communication technology, in addition to the undeniable progress of society, new forms of crime specific to cybercrime have emerged and are spreading. It is also one of the greatest threats to humanity of all time. Computer search is an activity different from any other evidentiary procedure, requiring specific rules to take into account its nature. The computer search can be ordered during the criminal investigation by conclusion by the judge of rights and freedoms, and during the trial by the Court.

KEYWORDS: computer systems, cybercrime, computer search warrant, computer search, the tactic of conducting the computer search

Introduction

Cybercrime is based on the use of computer systems, consisting of any device or set of devices interconnected or in a functional relationship, of which one or more insures automatic data processing, using a computer program (see Popa 2002, 70). Even at this time, there is no unanimously accepted definition of the notion of cybercrime. Attempts to define the term are multiple, this being explained by the complexity and magnitude with which the phenomenon manifests itself. However, worldwide, computer crimes are defined as those committed with the help of a computer, committed in virtual space, have no borders and can touch any computer in the world. Cybercrime is a form of transnational crime, and highlighting it requires international cooperation.

The main forms of cybercrime known and committed frequently in Romania so far are: illegal access to computer systems; illegal interception of a computer data transmission; altering the integrity of computer data; disruption of the functioning of computer systems; forgery and computer fraud; child pornography via computer systems; forgery of electronic payment instruments; conducting electronic financial transactions fraudulently; document forgery fraud; economic crimes; distribution of information of an illegal or prejudicial nature; crimes against life; computer espionage; computer sabotage; electronic warfare etc.

To ensure the rapid progress of society, the Internet has created a huge potential for development in all areas of social life, its potential applications being virtually inexhaustible. At the same time, however, new technologies of computer devices and systems open up new horizons and perspectives for committing "classic" crimes, such as theft and fraud, but especially crimes specific to the computer field, with a much more sophisticated and extremely difficult to discover and prove. Thus, obviously, the ease of use, the low cost, the speed and the assurance of an anonymous character make the Internet an extremely favorable environment for committing computer crimes. Moreover, due to the global character of the computer network and its huge complexity, the possibilities of "hiding" of the author are practically unlimited, encouraging for this reason also the commission of crimes. Thus, cybercrime is "a way of life for criminals" (Dobrinoiu 2009, 1), being preferred by them because they can easily hide their identity and disguise their illegal activities.

The victims of cybercrime are not only individuals, but, as experts say, "victims of war in cyberspace can be individuals, large corporations or industrial and economic concerns and even states, the targets being government IT infrastructures, intelligence agencies or defense, the critical infrastructure of a country: electricity and gas distribution networks, power plants, nuclear power plants, communications systems, transmission networks, etc.“ (Postelnicu and Marmandiu 2012, 44).

All this is possible only due to the fact that the Internet has become the easiest way to commit a cybercrime, the place where with a simple “click” you can earn millions of euros or the damage can be so great that it can no longer be recovered nothing. And studies in this regard show that we are entering the “fourth era” of organized crime (www.baesystemsdetica.com).

In order to detect complex and sophisticated cybercrime crimes, it is necessary to use highly specialized specialists who have and can use equally sophisticated technologies, and at the same time keep up with the means and methods used by offenders. One of the important problems in preventing and combating cybercrime, the investigation of crimes committed in this way, which can also be cross-border, is frequently hit by national barriers, the lack or insufficiency of international regulations and even the lack of specific offenses in some laws long after the development of the phenomenon.

Computer searches are a probative process that involves investigating a computer system or data storage media by criminal investigation bodies in order to discover and gather the evidence needed to solve the case. Article 168 of the Code of Criminal Procedure contains rules on the procedural institution of the search. The provisions of the Code of Criminal Procedure concerning home searches are also properly applied in the case of IT searches. (Moise 2017, 2654).

According to the Romanian legal provisions (Art. 168 para. (1) of the Romanian Criminal Procedure Code), the computer search or of a computer data storage medium represents the procedure of research, discovery, identification and collection of evidence stored in a system computer or data storage medium, made by means of appropriate technical means and procedures, such as to ensure the integrity of the information contained therein.

The computer search will be ordered only when the measure is necessary and proportionate to the purpose pursued (Moise 2011, 205).

In practical terms, we appreciate that arranging and conducting a computer search, in addition to the preparatory activities mentioned above (case study, legislation study, computer science study, etc.), necessarily involves the development of specific activities, structured in four phases, respectively: 1. preparation of the computer search; 2. obtaining the computer search warrant; 3. execution of the computer search warrant; 4. performing the actual computer search.

Preparing the computer search

From a tactical point of view, it should be noted that, in order to establish the purpose and objectives of a computer search, the data and information resulting from the ongoing criminal investigation must be necessarily and usefully supplemented with data from investigations conducted by the investigative body to determine in particular: computer systems, their equipment (including peripherals) and any other devices that should be searched, as well as potential information that could be stored on them that could be useful to the criminal case in finding out the truth; network connections of suspicious computer systems; the natural and legal persons who own and manage them, including their addresses and the locations where the computer equipment is located.

As a result, the preparation of the computer search requires the observance of the following steps (Prună and Mihai 2008):

a) Collecting information on the computer systems to be searched, the type of data storage, the location of the equipment and storage devices etc.;

b) The choice of the moment of performing the computer search, which depends on two factors: the status of the computer system and the presence or absence of certain persons;

c) Establishing the participants in the computer search, in the sense that, in addition to the investigators, persons with adequate technical qualification (forensic scientists, system engineers, etc.) will also participate;

d) Establishing the place where the actual computer search will be carried out (at the place where the computer equipment and devices are discovered or in the laboratory), depending on the volume of the equipment and the technical difficulties related to their search, or depending on the severity with which the activity of the persons holding these objects is affected;

e) Establishing the logistics to be used (tools, software, unregistered storage media etc.).

Obtaining the computer search warrant

During the criminal investigation, in any situation where it is found that for the discovery and gathering of evidence it is necessary to search for a computer system or a computer data storage medium, including in the case of those seized during the home or vehicle search or baggage search, the prosecutor must make and submit to the judge of rights and freedoms a application requesting the approval of the computer search and the issuance of the computer search warrant. It should be noted that if, during a home search, the judicial body finds a computer system at the place of the search, in connection with which it considers it necessary to verify the stored data and information, it is necessary to obtain a separate search warrant distinct from the first, from the judge of rights and freedoms, other than the mandate that had as object the house search.

The application requesting the approval of the computer search must contain data on the computer media to be searched (stand-alone computers, computer networks and portable storage media, as appropriate), the location of the computer media to be searched, the place where the analysis of the computer samples will be carried out (the actual computer search), the place where they are discovered or in the laboratory, as well as the fact that they will be searched and any other storage media found at the location and which are considered of interest solving the case (Stancu 2011).

The judge of rights and freedoms thus notified, by conclusion, orders the admission of the request and the approval to carry out the computer search, when it is grounded, and immediately issues the computer search warrant.

The conclusion and the mandate of the computer search must include the following data: the name of the court; date, time and place of issue; the name, surname and capacity of the person who issued the warrant; the period for which the mandate was issued and within which the ordered activity must be performed; the purpose for which it was issued; the computer system or computer data storage medium to be searched, as well as the name of the suspect or defendant, if known; the judge's signature and the court stamp.

During the trial, the computer search is ordered by the court, ex officio or at the request of the prosecutor, the parties or the injured person. The warrant to carry out the computer search ordered by the court is communicated to the prosecutor, in order to carry out the computer search.

Tactics for enforcing the search warrant

Depending on the volume of the equipment and the technical difficulties related to its analysis, regarding the execution of the computer search warrant, the judicial body may take one of the following two decisions: 1. search the computer system at the place where it was found; 2. picking up the equipment of the computer system to be searched in the laboratory.

Also, if the removal of objects containing computer data would seriously affect the activity of persons holding these objects, the prosecutor may order the making of copies, which serve as evidence (Art. 168 para. (10) of the Romanian Criminal Procedure Code). Copies shall be made with appropriate technical means and procedures, such as to ensure the integrity of the information contained therein.

Regardless of the decision taken, the initiation of the activity of executing the computer search warrant, similar to the home search, takes place by presenting the team at the location where it was established that the computer system equipment to be subjected to the computer search for which the search warrant was obtained.

The search of a computer system or of a computer data storage medium can be carried out in the presence of the suspect or the defendant, the team carrying out the search must include specialists working within or outside the judiciary, or specialized police workers, acting in the presence of the prosecutor or the criminal investigation body.

Arriving at the location of the equipment for which a search warrant was obtained, similar to the home search, the team leader identifies himself and hands a copy of the search warrant to the person to be searched, his representative or a family member, and failing that, to any other person with full exercise capacity who knows the person to whom the computer search will be carried out and, if applicable, the custodian.

In the case of a search carried out at the premises of a legal person, the computer search warrant shall be handed to its representative or, in the absence of the representative, to any other person with full capacity who is in the premises or is an employee of that legal entity. These persons are required to voluntarily hand over the equipment of the computer systems and the objects containing the stored computer data sought. If they are handed over, the computer search may take place in the same location or may be carried out in order to carry out the computer search in laboratory conditions. If they are not handed over voluntarily, based on the computer search warrant, the equipment is searched within the location, without pursuing other goals and objectives, specific to home search. Once the searched computer equipment is discovered, as if it had been handed over voluntarily, the computer search can take place in the same location or it can be picked up in order to perform the computer search in laboratory conditions.

Regardless of the decision taken, from a tactical point of view, before proceeding with the search or seizure of computer systems, team members must consider compliance with the main rules of forensic tactics, consisting primarily in searching, discovering, fixing and tracking and other material means of proof on each component of the equipment that makes up the computer system, as well as on objects in their vicinity, such as: fingerprints and/or handprints, footprints, prints created by different parts of the computer human body, biological traces, etc. Also, from a tactical point of view, depending on the criminal acts investigated and the objectives of the computer search, if the computer, laptop or tablet looking for is running, the image displayed on the monitor screen when found by the team may have some relevance search, so that image is recommended from the point of view of forensic tactics to be fixed by photo and video recording. During the computer search of the location, team members must prevent any approach of the suspect to the computer system, to remove any possibility of alteration of data and information on it, by intentionally making orders taking advantage of their lack of attention.

In most cases, it is decided to pick up the computer equipment, in which case the following rules of forensic tactics must be observed:

a) *Description, photography and filming of computer equipment*, in order to ensure the conditions for the exact reconstruction of the system in the laboratory; the minutes of the lifting shall be record the spatial arrangement of the components of the computer system, including the modems and devices used to create a network of equipment and/or Internet access, insisting on photography and filming on the cables and connections between them;

b) *Ensuring data integrity and shutting down the system*, taking all necessary measures to protect against the destruction and alteration of all electronic evidence; If the computer system has been found closed, it no longer needs to be opened;

c) *Marking and labeling of components*, to ensure compliance with the configuration of the computer system when reconstituting it in the laboratory;

d) *Packaging, sealing and labeling of raised equipment*, to avoid any appeals concerning subsequent external interference with them and to ensure their veracity; it is recommended that the equipment be packed, sealed and labeled in its original packaging, if found, or in a special packaging that ensures their electrostatic protection; sealing is done in such a way that access to the equipment is not possible until the packaging is opened in the laboratory, so that the information stored on it is not disputed; the label on the packaging must contain information on the packaged components, the date, place and circumstances of their removal, the persons who packed them and their signatures, etc.,

e) *The transport of raised equipment is carried out* in such a way as to avoid shocks, vibrations and electromagnetic fields which could damage them;

f) The storage of packaged and sealed equipment is done in rooms without humidity or dust, in order to avoid their alteration or destruction and the information stored on them.

The activities carried out during the lifting of the computer equipment are recorded in a report that is signed on each page and at the end by the one who concludes it, by the person from whom the computer equipment was picked up, by his lawyer, if he was present, as well as by all persons present at the performance of the activities mentioned above. If any of these persons cannot or refuses to sign, this shall be stated, as well as the reasons for the impossibility or refusal to sign.

A copy of the report shall be left to the person from whom the computer equipment was taken or to the family member or representative who participated in its collection. The place where the computer equipment was found and picked up are photographed or audio-video recorded, all of which are attached to the lifting report, being an integral part of it.

Performing the actual computer search

The actual search of the computer in the location where the computer equipment was found or in laboratory conditions, consisting in the analysis of the information stored in the computer system or in the computer data storage media that were collected, is performed only in the presence of the suspect or the defendant (if possible) (art. 168 para. (11) of the Romanian Criminal Procedure Code), or a representative thereof or a witness, by making faithful copies (clones) of them, with the help of programs and special devices (Dascălu, Ştefan and Ţupulan 2008, 111).

Thus, the main stages of conducting the actual computer search are the following:

a) Unsealing computer systems or high storage media (after checking the integrity of the seal, in case of lifting them);

b) Identification of the correspondence between the devices raised and those mentioned in the computer search warrant;

c) Assembling the components in order to reconstruct the original computer system;

d) Making a copy of the data and information stored in each computer data storage medium;

e) Performing the actual computer search on the copies made on each computer data storage medium;

f) Making new copies of computer data, with data and information relevant to the criminal case, which were identified in the search process, to be submitted to the case file and to be considered in the administration of evidence;

g) Sealing the storage medium on which the copy on which the search was made is located;

h) Concluding the computer search report;

i) Restitution of equipment or resealing (as a final activity with the equipment lifted).

The technical aspects regarding the computer search are extremely numerous, and some of them present an extremely high degree of complexity. In these conditions, we consider that it is useful to present only two aspects that we consider to be of maximum interest, without trying an in-depth and *in extenso* analysis (Zlati 2014).

The first important aspect is that the actual computer search of each component of computer equipment differs depending on the technical means to be searched, respectively: server, computer, laptop, tablet, smartphone, printer, hard drive external disk, data storage stick, etc. In this respect, the different types of hardware and software at the level of storage media must be taken into account, depending on the type of equipment and devices searched. As a result, each time, in order to perform the computer search, different computer programs are used, depending on the searched computer environment.

A second important aspect is that the operating system through which the computer system user or a third party interacted with computer data, differs depending on the characteristics of the operating system (Microsoft Windows, Linux, Mac, iOS, Android etc.). In these circumstances, the practical consequence is that, depending on the computer system used by the suspect, it is possible those certain fingerprints cannot be identified, or that their identification may require a certain procedure.

Conclusions

As we said above, at the end of the computer search, the specialist who performed this search must conclude a computer search report, according to the rules stipulated by art. 168 para. (13) of the Romanian Criminal Procedure Code.

The prosecuting authorities must ensure that the computerized search is carried out without the facts and circumstances in the personal life of the person being searched being unjustifiably made public.

The computer data identified as secret shall be kept in accordance with the law so that their security can be ensured, depending on the nature of the classified information, including as regards persons investigating or prosecuting the criminal cases concerned.

References

Dascălu, Ioan, Cristian-Eduard Ştefan, and Marin-Claudiu Ţupulan. 2008. *Percheziţia judiciară [Judicial search warrants]*. Craiova: Sitech Publishing House.

Dobrinoiu, Maxim. 2009. "Provocarea legislativă a reţelelor Wi-Fi [The legislative challenge of Wi-Fi networks]" in *Intelligence.* Year VI, no 16, July.

Moise, Adrian Cristian. 2011. *Metodologia investigării criminalistice a infracțiunilor informatice [Forensic investigation methodology of cybercrime]*. Bucharest: Universul Juridic Publishing House.

Moise, Adrian Cristian. 2017. "Some technical-tactical aspects of computer search." In *Romanian Journal of Forensic Science* no. 4: 2654.

Organised Crime in the Digital Age: The Real Picture, Executive Summary of BAE Systems Detica and the John Grieve Center for Policing and Community Safety "Organised Crime in the Digital Age" research report, p. 3, study available at: http://www.baesystemsdetica.com.

Popa, Teodor. 2002. *Frauda informatică [Fraud Informatics]*. Oradea: Oradea University Publishing House.

Postelnicu, Carmen and Sorana Marmandiu. 2012. "Perspective teoretice asupra ameninţărilor cu incidenţă în domeniul securităţii [Theoretical perspectives on security threats]." In *Intelligence* no 23.

Prună, Ștefan and Mihai, Ioan-Cosmin. 2008. *Criminalitatea informatică [Cybercrime].* Craiova: Sitech Publishing House.

Romanian Criminal Procedure Code,

Stancu, Emilian. 2011. *Procedee tactice folosite în investigațiile penale. Evoluții. [Tactical Procedures Applied in Criminal Investigations. Evolutions].* Bucharest: AIT Laboratories Publishing House. Source:

http://www.criminalitatea-informatica.ro/tehnici-de-investigare/efectuarea-verificarilor-si-perchezitiilor-in-mediul-informatic/, accesed on 15 iulie 2021.

Zlati, George. 2014. “Procedura de percheziționare în mediul informatic – Efectuarea percheziției informatice propriu-zise [Search procedure in the computer environment].” *Universuljuridic.ro*. https://www.universuljuridic.ro/procedura-de-perchezitionare-mediul-informatic-efectuarea-perchezitiei-informatice-propriu-zise/.