Legal and Practical Aspects in the Computer Science Investigation

Florin Cosmin Trandafir
IT&C Security Master
Cybernetics and Economic Informatics Faculty, Bucharest
ROMANIA
tfc_soft@yahoo.com

Abstract: The present article makes a short introduction in the legal and practical aspects of the computer science investigation. It is well known the fact that a computer can represent an invaluable source of pieces of evidence, both in the civil cases as well as in the criminal ones because it contains data regarding the activities carried out by the suspect with the help of the IT equipment.

Key words: computer science violations, computer science delinquency, computer science forensic

1. Introduction

The computer can represent an invaluable source of pieces of evidence, both in the civil as well in the criminal cases because it contains data regarding the activities carried out by the suspect with the help of IT equipment.
Whether it is about an illegal activity from the point of view of the civil law or the criminal law, the investigator, or by the case, the competent authorities must take into account a few aspects in the attempt of obtaining the incriminating pieces of evidence against the suspect. Thus, in the civil cases, the investigator, whether it is an IT specialist or a specialized person for such investigations can check a computer without the agreement of the user, if the respective equipment is the property of the company in which he is employed. The investigator must obtain the agreement of the management of the company requesting the investigation.
In the cases related to the application of the criminal law, the investigation of the competent authorities is made only after the obtaining of a computer science search warrant from a judge. Next we will discuss more about the aspects related to the practical part of the computer science search than about the ones of obtaining the search warrants and other bureaucratic aspects.

This is a post conference paper. Parts of this paper have been published in the Proceedings of the 3rd International Conference on Security for Information Technology and Communications, SECITC 2010 Conference (printed version).

2. The phenomenon of computer science crime appearance and awareness

When did the computer science crime appear? The answer to this question is difficult to render with precision but we can state that shortly after the appearance of the computer the idea that the new invention could also be used and exploited in unauthorized purposes was born.

In the last period of historical evolution of the computer, when this was a huge, very expensive and also well kept machinery (we should not forget that the first computers have been developed in America under the coordination of the Department of Defence), the committing of crimes in connection with the computer was difficult and was limited only to the stealing to some mechanical components of these. In that period, many people did not know about the existence of the computer let alone about how to use it. As computers have reduced in size and have become cheaper, entering as well in the possession of common people, these, including the criminals have begun to familiarize with the functioning of the computers, with their programs, have

ISSN 2067 – 4074

been able to improve their knowledge and also to explore the weaknesses of the computer science systems.

2.1. Types of computer science violations

In Romania, an important legal regulation applicable in this moment in the matter of the computer science criminality is the Law 161 on 04.09.2003 regarding some measures for the ensuring of the transparence and the exercising of the public dignities, of the public functions and the business environment, the prevention and the sanction of corruption.

This introduces a number of 7 crimes corresponding to the classifications and definitions presented with the analysis of the provisions of the Convention over the computer science criminality grouped in the content of Title III in the law - **The prevention and the fight against the computer science criminality**. The text has been a quick adaptation of the provisions of the Convention of the European Council over the Computer Science Criminality to the Romanian environment and it represents an efficient instrument in the fight against this disaster. In the law 161/2003 there are three categories of crimes, incriminated in the following way:

Crimes against the confidentiality and integrity of the data and the computer systems:

- The crime of illegal access to a computer system;
- The crime of illegal intercepting of a transmission of computer data;
- The crime of alteration of the integrity of the computer data;
- The crime of disruption of the functioning computer systems;
- The crime of making illegal transactions with computer devices or programs.

Computer crimes:

- The crime of computer forgery; The crime of computer fraud.

Child pornography through the computer systems

Also, in the sense of the present law, the person who is in one of the following situations acts unlawfully:

a) is not authorized, based on a law or on an agreement;
b) exceeds the limits of the authorization;
c) has no permission, from the competent natural or legal person, according to the law to grant, use administrate or control a computer system or to carry out scientific researches or any other operation in a computer system.

The offence charged in article 42 clearly distinguishes between the three stages of the access to a computer system, respectively the simple access (which most of the times is accidental), the access with the purpose of obtaining computer data (manifested most often) and the access by violating the security measures (which requires technical knowledge and is much more difficult to carry out).

There will also exist simple access in the case the intruder, by manipulating its personal peripherical equipment, from the distance, finds and uses an external connection to enter another computer system. It is the typical case of accessing a working station which is in a network.

Next we will present a few types of computer crimes:

a. attacks by breaking the password;
b. the attack of passwords by raw force;
c. the attacks by TCP embezzlement;
d. session embezzlement;
e. attacks by password;
f. packages interception;
g. attacks by desynchronization;
h. embezzlement of the session by post-synchronization;
i. frauds by the online buyers;
j. frauds in online investments;
k. business frauds;
l. the fraud of a public service (utility);
m. sabotage through computer;
n. business opportunities – Home online working.

3. Software used by the investigators

From the most experienced up to the usual users, everyone should know that it is not indicated to alienate a rewritable storage environment without taking the necessary security measures. As you well know, the simple deleting is only announcing the computer that in case this wishes to overwrite the respective memory area, it can do it. The formatting of the device is a better method than the simple deleting but it is not efficient because the formatting process deletes only the address tables not the stored data.
A safer method of deleting the data on the sorting devices is the use of a "disk wiping" process. This process assumes the rewriting of each sector of the storing device with aleatory or predefined information. The rewriting is made by using specialized softwares for this process, some of these offering the user the possibility of choosing the number of iterations desired for rewriting. In the case of the free of charge software "Eraser" (http://eraser.heidi.ie/) this process of rewriting can be repeated up to 35 times by using the algorithm developed by Peter Gutmann. The author of the software is Sami Tolvanen.
In order to prove how easy the data from a storage device can be recovered, we will use a free of charge software offered by the company Piriform called "Recuva" (http://www.piriform.com/recuva). After the installation of the program, from the main window we can choose the partition or the storage device for which we wish to verify the existence of some files apparently deleted.

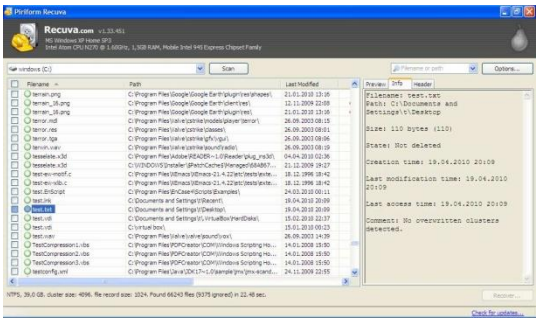

Figure 1.Recuva file details

In order to verify these aspects, on the desktop we have created a txt file format named "test", in which we have repeated the word test several times. After deleting it by using the command SHIFT+DELETE (in order for the file not to pass through the Recycle Bin) I have tried the scanning of the hard – disk for the recovery of the file with the help of Recuva.
As we can observe in the following images the file has been found with the help of the software, its recovery being only a click away. This software offers at the same time information regarding the files found again in the list:
Taking into consideration the fact that the software used for this test is one free of charge, it is not difficult to realize that not only an expert can carry out operations for the recovery of the data from a storage device which we lost or alienated.

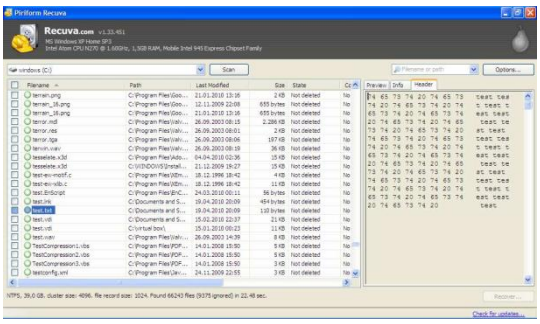

Figure 2. Recuva Header

Computer Online Forensic Evidence Extractor, shortly "COFEE", is a program exclusively destined for the institutions which have as objective defending the law. The program is made by Anthony Fung, who is now working at Microsoft, being offered free of charge for the institutions authorized to gather pieces of evidence against the people violating the law. In seeking to provide this software free of charge Microsoft collaborates with the Interpol and National White Collar Crime Center (NW3C).
It so happens many times that when the intervention forces enter the house of a suspect with a search warrant they observe that he had the computer opened. In this case, before the COFEE appeared, the law enforcement people had no other solution but to disconnect the computer from the source which supplied the

ISSN 2067 – 4074

energy. The attempt to extract information about the respective system and the programs running on it was destined only for the specialists and could last between 3-4 hours. With the help of the software developed by Microsoft, these operations can be executed in less than 10 minutes, without needing the presence of a specialist.

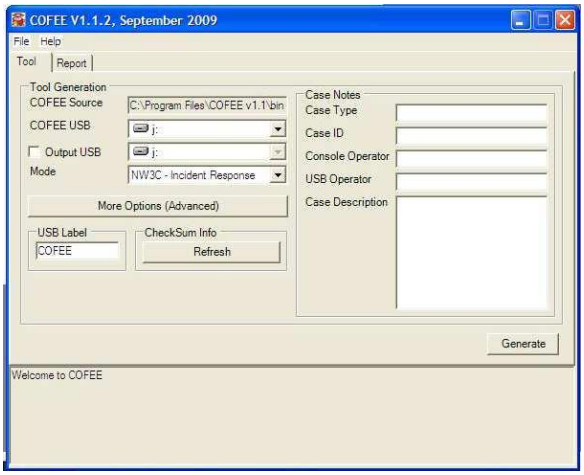

Figure 3. Cofee Tool Page

On November 6th 2009, only 2 months after the appearance of the 1.1.2 version, this appeared on the Internet being downloaded by anyone who wished it. Shortly after this, the access to these sources has been restricted, but it had been free of charge long enough to enable the appearance of a program to counteract the COFEE actions. This software was called DECAF and may successfully delete the orders executed by COFEE over the computer; however these orders being executed with the help of other software or by launching some programs in order line. COFEE has a pretty simple interface, as we can see from the following images, which contain two main menus, one for the creation of a USB flash drive to run the tools necessary for the data collection on the defendant's computer and another for the extracting of these pieces of information under the form of a report in an easy to read XML format.

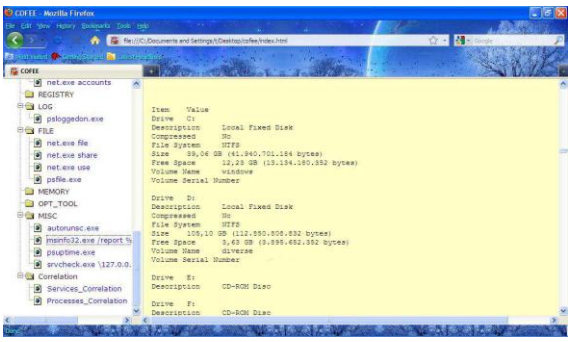

Figure 4: Cofee XML Report

The following images present the aspects of the program execution and of the obtaining of the report in XML format as seen in the next figure:

Another two applciations used by the invesitgators are EnCase Forensic and X-Ways which we will detail in the following chapters.

3.1 Data acquisition process

The most important part of the investigation of any incident is the collection of the pieces of evidence, but more important is that these can be successfully presented in front of a court of justice. No matter how well prepared is the investigator or how many pieces of evidence he might have, if the defense can demonstrate that in the process of obtaining these pieces of evidence the integrity of the equipment investigated or their content have been affected, the case will suffer a great deal or can even be lost. Next we will discuss about the collection of the pieces of evidence from a system with an IDE (Integrated Device Electronics), SATA (Serial AT Attachment) or SCSI (Small Computer System Interface) hard-drive type. Naturally, during an investigation the investigated system must be shut down (by direct disconnection from the supplying source) and restarted with an operation system that will not affect the integrity of the pieces of evidence, because, as we know, the commercial operation systems modify certain registers upon each starting of the system. The disconnection moment of the system of the supplying source or its shut down is considered to be the moment after which no modification of the pieces of evidence is allowed. In most cases, the

hard-disk is removed from the system and connected to another system to integrate both a specialized soft for the collection and/or investigation of the data, as well as equipment called „write blocker". This equipment prevents the writing of any information on the attached storing device by the fact that upon the receiving of the writing command on the device this returns the true value to the system without executing it. The creation of a faithful copy of the storing device is made only upon the express request of the court of justice, thus pieces of evidence will be searched directly on the respective device. For the creation of the faithful copies of the storing devices as well as for the discovery and investigation of the pieces of evidence, many specialized firms and authorized institutions from the world use software made by Guidance Software, called „EnCase Forensic". For the following stages of the investigation process we will refer to the capabilities of this software, thus the data acquisition process being carried out in the following way:

a. the storing device is connected to the system of the investigator by being used a write-blocker type hardware device, called FastBloc, which prevents the data writing on the investigated device;
b. the FastBloc device is connected to the investigator's system;
c. the EnCase software is started;
d. whether the creation of an image of the investigated storing device is desired or just its investigation, a new case will be created by using the New button from the top left corner of the window opened by the program;
e. in the dialogue window which will open, data related to the name of the case and the investigator will be introduced as well as the location where the data resulted from the investigation will be saved;
f. for the beginning of the investigation it is necessary to add the investigated storing device in the afferent list to the above created case; this will be done by pressing the Add Device button;
g. because the investigated storing device is attached to the investigator's system the option Local Drives will be selected and will be continued with Next (from the previous image one can observe the fact that there are other options for the data acquisition such as the network connecting to the investigated system);
h. from the next window will be selected the device over which the investigation is carried out (will be selected the entire device even if there is the possibility of selecting only one partition of it);
i. will continue with Next and Finish.

The Write Blocked column is checked only in case the EnCase software recognizes the connecting of the investigated storing device by the FastBloc use.

For the creation process of a faithful image of the hard-disk it is necessary a storing capacity at least equal to the one of the investigated device. After this problem is solved we can pass to the acquisition of the stored data by the creation of the image of the device. This is made by pressing the Acquire button; from the menu that appears being selected the actions that the software will carry out after finishing the data acquisition, as well as the data necessary for the subsequent identification of the case or the path where the image of the device will be saved, the dimension to which the image will be divided to be stored on another support than the hard-disk, etc.

After the carrying out of these steps the software will begin the acquisition of the data, a process which can last according to the dimension of the device from a few minutes up to several hours. After finishing this process the software will carry out a verification of the data integrity which can last quite long. In case of the acquisition and verification of a hard-disk with a storing capacity of 160 GB, EnCase has estimated the carry out of these operations in approximately 8 hours.

ISSN 2067 – 4074

In order to be able to demonstrate in front of the court the fact that the data present on the investigated storing device are identical to the ones in the image created by EnCase, a hash of these can be carried out in order for the results to be compared. If these are identical, then the resulted image is identical to the one of the investigated device.

In case the court orders the „cloning" of the device, the investigator will search for pieces of evidence within the image previously created with EnCase. The pieces of evidence will be searched directly or by using some specialized search tools. EnCase provides the investigators with the possibility of creating by themselves searching tools, either by adding in a list of some key words or by the creation by the investigator of some scripts which will later run within EnCase.

3.1.2. Finding the pieces of evidence

E pieces of evidence about the activity of the suspect can be searched and found in many places, hidden in sight on the storage device of the searched system. If the investigator suspects that the suspect has used software to achieve the deleting and the overwriting of the sectors from a storing device he will verify first the registers especially the file log UserAssist. Here he will search among the programs installed on the respective system from the last formatting of such programs. Usually these programs create themselves their own temporary files which can have names like BCW.001, where the number increments by 1 for each new formed file.

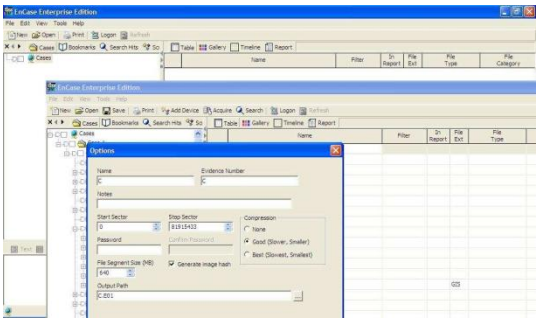

Figure 5. Encase aqusition options

Another characteristic of the existence of the activity of „wiping" is the total lack from the analyzed storing device of the traces of some deleted files. Of course that the lack of such files it does not obligatory means that the process of "safe deletion" has taken place but corroborated with other characteristics can lead to the conclusion that the process of deletion has taken place. In such cases the investigator must know the fact that during the lifetime of a storage device it can suffer more processes of „wiping". Some security programs and even some anti viruses use the process of "safe deletion" in case they can not clean certain files or can not send them to quarantine. After the end of this stage one can pass to the recovery of the deleted files. This can be done with the help of the EnCase software with a simple right click on the storage device added to the case under investigation. Form the menu that appears the option "Recover Folders" will be chosen which will start the search of the directors marked as deleted.
During the investigation the investigator can recover one of the files marked as deleted by right clicking above the respective file choosing from the menu that appears the option „Copy/UnErase...", as you can see from the following image.

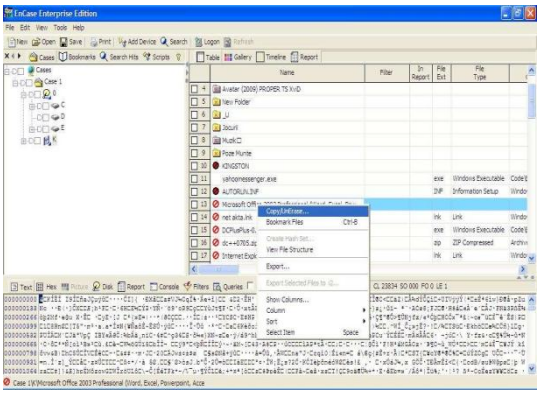

Figure 6. EnCase Copy/UnErase

It is chosen the location desired for the copy of the file and is waited for the software to carry out the command.
The investigator will also choose information related to the softwares that the suspect has installed and/or ran on the searched system. This can be made by verifying the log files created in Windows by UserAssist. UserAssist is a characteristic

implemented beginning with Windows2000, which is neither well implemented nor understood by the large public but which for an investigator can be a godsend. This application behaves like a spyware incorporated in windows, which registers the use of the applications according to certain factors like the frequency of the use. The logs created by UserAssist are encrypted, but fortunately this encryption is made by using a very simple algorithm called ROT-13. The encryption involves „turning" each letter with the thirteenth one that follows in the alphabet. Thus the letter „a" becomes „n" and so one, the numbers and other characters being ignored. The files created by UserAssist can be found in the registers under

KEY_CURRENT_USER\Software\Microsoft \Windows\CurrentVersion\Explorer\UserAssist.

The following images show us an example of decryption of one of the keys found in the UserAssist registers:

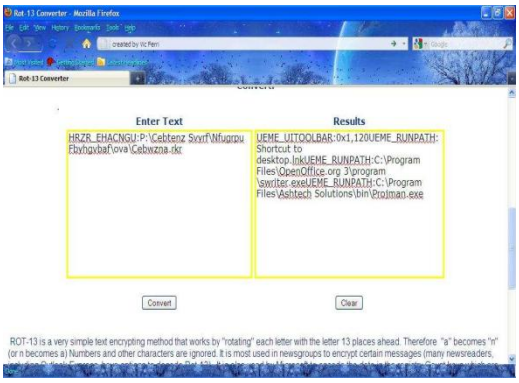

Figure 7. UserAssist decription

Another place where incriminating pieces of evidence can be found about the activities of the accused is the unused or unallocated space on the storing device. A cluster is the logic storing unit of a file on a hard-disk. A file occupies in most cases less or more than a cluster, the spaces remaining between the written file and the cluster having the name of "slack space". With the help of EnCase the investigator can see this space as well and can verify the existence of the pieces of evidence within it. Because the unallocated space does not have a structure defined, automatic tools can not be used to recover files from this space. The investigator can however use a search by certain key words inside this space. Another program used by the law enforcement officers from whole world is X- Ways Trace (http://www.x-ways.net/trace/), made by a German company called X-Ways Software Technology. The program is used to decipher the content of the file "index.dat" created by Internet Explorer, but also "history.dat" of Mozilla/Firefox or "dcache4.url" created by Opera. With the help of this program one can see the last files accessed as well as their URL, the date of the last access etc.

3.2. Efrauda.ro

In order to support the Romanian people, on February 23rd 2004 the Ministry of Communications and Computer Science Technology has issued a

communication which announced the opening of the efrauda.ro portal, described as being „the portal for the receiving of the complaints regarding the illegal activities in the field of computer science society services which carry out the direct interaction between the suppliers and consumers of services of the computer science society and the competent authorities in the field". On that date as well the Minister of Communications and Computer Science Technology on that time, Dan Nica, stated the following: „We want to catch everyone who has „sport" activities related to the computer science criminality and we must be extremely serious in this matter. It is like in the visas system, one has the right to travel freely in Europe but we must keep things under control. As you probably know, there are sites which do not accept online shopping from the Romanian citizens and the MCCST wishes to change this because it is not fair that for these practices the bill be paid by 21 million Romanian people" The communication also offered the following information regarding the existence of the portal: The system has a public part and a private one such that it can be accessed both by unregistered users – the citizens as well as by the registered one – the public authorities. The access of the public authorities is made by using a security authentication mechanism and the

ISSN 2067 – 4074

updating of the content of the portal implies both the authorities with competences in the field of computer science services of the societies and the ones with investigation attributions as well as the professional associations.

The eFrauda portal is a virtual center which has been created with the purpose of ensuring the protection of the suppliers and consumers of services of the computer science society, the decrease of the bureaucracy and the increase of transparency in the relation of the citizen with the authorities. The project is part of the strategy of development of the public services provided by electronic means of the MCCST and has legal support the Law no.161/2003 Title III „The prevention and the fight against the computer science criminality". The last date on which the existence of the site is mentioned is February 20th 2006 when the Minister of Communications and Computer Science Technology, Zsolt Nagy, has participated to the "Electronic Communications and IT" seminar, organized during the "Training Campaign of the Business Community in Romania for the Integration in the European Union, at the headquarters of the Chamber of Commerce and Industry of Romania". In this moment the simple attempt to access the portal will return the following response:

Figure 8. Efrauda.ro site

On the e-guvernare.ro site we can still find on the main page a link to a „IT Antifraud Portal" which directs the user to the same inexistent portal efrauda.ro.
The lack of interest of the public authorities towards the phenomenon of computer science criminality is visible by this inexplicable disappearance of the efrauda.ro portal from the landscape of the local sites.

In the United States the site through which complaints can be made regarding violations through Internet is www.ic3.gov. This centre of complaints is the product of a partnership between FBI (Federal Bureau of Investigation), NW3C (National White Collar Crime Center) and BJA (Bureau of Justice Assistance). The site provides the persons interested with much useful information related to the computer science criminality, out of which I wish to debate the part related to the methods of crime committing through internet. The explanations related to these methods begin by presenting the phenomenon of false electronic biddings, through which the victims are attracted to pay important sums for products they never receive or which don't correspond to the description on the bidding site. The reason for which I wished to bring into discussion this site was that immediately after the general presentation of the aspects related to the fraudulent biddings, the presentation continues with information regarding the fraudulent biddings carried out through the Internet on the territory of Romania. This is the only reference made to a phenomenon of criminality for which it is mentioned as well the country on whose territory the respective activities are carried out.

Figure 9. Internet Crime Complaint Center

According to the site, the phenomenon of the fraudulent biddings carried out through the Internet is representative for Romania, the number of the case and the complexity of the actions of the persons implicated in this phenomenon increasing continuously. The degree of dangerousness of the Romanian delinquents is given by the fact that these have filled up the Internet with such bidding sites which seem to be on the

territory of the United States and which offer the buyers the possibility of paying only half of the price of the product before the delivery following that the rest of the payment to be carried out at the moment the package is received. Because the victims never receive the ordered products the delinquents get half the sum paid for these for the fictional products. The payment is carried out most of the times through cash transfers MoneyGram or Western Union, these payment methods allowing the victims few chances of recovering the sums paid as advance for the ordered products.

4. Conclusions

In the real world the delinquents are very inventive and always find new methods of breaking the law. The people dealing with the maintaining under control of the phenomenon of criminality generally and of the computer science criminality especially must always be one step ahead of the delinquents. The investigators count on the fact that the delinquents are people and this is why sooner or later they make mistakes which most of the times lead to catching them. But, to be able to quickly observe these mistakes of the delinquents the people implicated in the finding and catching them must be trained and hold the last information and technologies appeared in the field.

This is why I believe that the law enforcement people in Romania, implicated in such investigations must be provided with such revolutionary technologies at the same time with the organizing of classes and seminars on the themes of interest in this field. The continuous training of the people implicated and their becoming used to the new methods used by the criminals can be the only method of controlling a phenomenon which is more and more difficult to control, that of computer science criminality. The quick expansion of the phenomenon is helped by the transnational character of this. Thus, because of this „network of networks", as Internet is also called, the worldwide criminals can obtain detailed information about how to commit a crime or may commit crimes that affect the citizens of another country without leaving the comfort of their own homes.

We are hoping that the present article, as well as the complaints made to the authorities may draw a warning regarding this phenomenon of criminality which up to the taking of concrete measures continues to increase.

References

[1] I.Vasiu, *Drept şi Informatică. Protectia juridică a programelor, Studii de drept Românesc*, Ed. Academiei Române, 1993

[2] I.Vasiu, *Totul despre Hackeri*, (in Romanina), Ed. Nemira, 2001

[3] Costică Voicu et al., *Globalizarea şi criminalitatea economico-financiară*, (in Romanian) Editura Universul Juridic, Bucureşti, 2005

[4] EnCase Forensic user manual, ver. 4.2, 2004

[5] Philipp Aaron, *Hacking Exposed. Computer Forensics*, Second Edition, 2010

[6] Bainbridge, *Computers and the Law*, Ed. Pitman, Londra, 1990

[7] J. Gurak, *Persuasion and Privacy in Cyberspace*, Yale University Press, 1997.

[8] Edward Harris, Web Becomes a Cybertool for Political Activists, *Wall Street Journal*, August 5, 1999