PARTICULARITIES OF THE INFORMATICS CRIMINALITY INVESTIGATION

Ph. D Lecturer **Elena-Ana Mihuţ**
AGORA University, Oradea
emihut@univagora.ro
emihut2005@yahoo.com
Senior Criminalist **Ioan Truta**
CLPE (Certified Latent Print)
Boston Police Department rtment,
Latent Print Unit
trutai.bpd@cityofboston.gov

Abstract:

Informatics criminality represents the social phenomenon characterized by the committing of criminal offences in the field of informatics. This category includes very different criminal offences, some of them being incriminated in certain states of the world while others are not. The computer provides a new object and a new tool for criminals.

Taking into account the complexity and variety of criminal offences in the field of informatics, as well as the rapidity of changes occurring in the field of Information Technology, forensics computing relate to the way in which the crimes were perpetrated.

Key words*:* informatics criminality, digital evidence, investigation.

I. General Considerations. The appearance of the first computers, more than half a century ago, caused a real change in human society. The progress of computer systems and the development of the Information Technology field led to an easy and quick access to various information stored and transmitted by computer systems. These days, there is no field of activity that is not at least partially dependent on computers.

Today, a significant part of the interaction between individuals, between individuals and public institutions or the business community relies on the use of networked computers and communication technology.

The computer is a very important criminogenic factor, as it provides the networked computers criminals with a new object — information, as well as with a new tool. The Internet, computer networks, embedded systems of data create new opportunities for criminals to achieve their goal by committing computer related crimes.

By the nature of computers, data can be stored, transferred, used and manipulated through long-distance contact. Thus, criminal offences in the field of informatics are different from the classical ones through several characteristics, among there are:

- the cross-border character, as the number of countries involved in this phenomenon is constantly increased, while the legislations are different. The international investigation of these activities, inquirers rely on the system provided by the Interpol, based on the national points of permanent contact, as well as on other connections with specialized international bodies.

- anonymity, as the perpetrator may be anywhere in the world;
- credibility, the perpetrator being able to create the appearance of a legal and honest business;
- rapidity, the data being transmitted almost instantly through information systems[201].

The notion of computer related criminal offence was present for the first time in the legislation of USA, where the authorities traced out a series of violations of the legislation in this field.

Informatics criminality may be divided into three categories:

- criminal offences where the computer is the target;
- criminal offences where the computer is the tool;
- criminal offences where the computer contains digital evidence related to other criminal activities[202].

II. Particularities of the forensic investigation in the case of committing criminal offences in the field of informatics. In order to determine the circumstances in which the crime was committed, the connection between various perpetrators, it is necessary to identify the devices used in the criminal activity, their location, the information, the hardware and software as a result of committing the crime and the perpetrator[203].

Taking into account the complexity and variety of criminal offences in the field of informatics, as well as the rapidity of changes occurring in the field of Information Technology, forensic computing relate to the way in which the crimes were committed.

With a view to facilitating the disclosure of the circumstances and conditions in which the criminal activity was carried out, it is recommended to follow Standard Operation Procedures (SOP): identifying the incident, preparing the investigation, formulating the approach strategy, securing, collecting, examining, analyzing, presenting and returning evidence.

The results and documentation obtained from the expertise achieved in the case in question must be correct and provide as much information as possible to allow another forensic examiner competent in the same area of expertise, to be able o identified what has been done and reach the same results independently. Thus, it is important that the data regarding the source of provenance of the evidence should be clear — which involves their authenticity, credibility and integrity. Also, the forensic tactics activities must proceed from the general rules applicable in any forensic investigation[204], starting from examining the

[201] See Ioana Vasiu, L. Vasiu, *The Prevention of Informatics Criminality*, Hamangiu Publishing House, 2006, pages 71-72.

[202] See Gh. Alecu, A. Barbăneagră, *Criminal Regulation and Forensic Investigation of Criminal Offences in the Field of Informatics*, Pinguin Book Publishing House, Bucharest, 2006, pages 24-25.

[203] See Ioana Vasiu, *Informatics Criminality*, First Edition, Nenuia Publishing House, 1998, page 18.

[204] See E. Stancu, *Treatise of Forensics,* Third Edition Revised and Enlarged, Universul Juridic Publishing House, Bucharest, 2004, pages 600-601; I. Mircea, *Forensics,* Lumina Lex Publishing House, Second Edition, 2001, Bucharest, pages 232-233; Elena-Ana Mihuţ, *Forensics. Forensic Technique and Tactics,* Publishing House of the University of Oradea, 2006, pages 202- 206; L. Cârjan, *Treatise of Forensics,* Publishing House Pinguin Book, Bucharest, 2005, pages 461-463.

entire crime scene to the examination of digital evidence. The applicable rules are as follows:

- the investigation must be performed as soon as possible;
- all existing evidence must be collected;
- the investigation must be performed in detail, taking note of all the particularities of the existing evidence;
- the integrity of all pieces of evidence must be ensured. For this purpose, the investigation team must include, beside crime scene investigation, computer forensic specialist in the field of computer science, so that the investigators can take special measures of protection in order to collect, preserve, transport and examine these pieces of evidence.
- the pieces of evidence must be conserved in special conditions, so as to avoid their contamination while being manipulated.

Digital evidences by their nature are fragile and can be easy alter, damage destroyed or compromised by improper handling or examination, they are not visible latent — investigation equipments and specific software being required in order to make them available, tangible and usable. The digital pieces of evidence must be searched, discovered, collected and examined by forensic specialists with an adequate preparation in this field. Examination is best conducted on a copy of the original evidence. The original evidence should be acquire in a manner that protects and preserve the integrity of the evidence.

Digital evidence includes informatics related evidence, digital audio, and digital video evidence, evidence produced, stored or transmitted through mobile phones, digital faxes, digital photo cameras, etc. These pieces of evidence have the following particularities:

- the way of storing, processing or transmitting them by means of an informatics system;
- their latent form of presentation.

Beside the digital evidence, in the case of investigating criminal offences in the field of informatics, attention is also paid to other categories of traces which may be found on the crime scene. For instance, latent prints, material and biological traces or remainders of objects found on the crime scene may be emphasized. In order to emphasize traces of reproduction in a latent state, it is not recommended to use magnetic powder because magnetic fields can be formed which might contaminate the digital evidence.

The tactical activity of hearing the persons involved will take place in accordance with the Code of Criminal Procedure and with the rules of forensic tactics. As a characteristic feature, we are mentioning the fact that the attention of the investigators will be channeled towards establishing the identity of all persons who have access to the place that is being investigated, who have used the respective device or who have knowledge about the use of and the data stored in the informatics system.

In case the perpetrator is present during the performance of the investigations or of the search the investigation team will carefully analyze his/her verbal and non-verbal behavior. At the same time, he/she will not be permitted to approach the computer. If he/she insists in giving help in order to shut it down, he/she will be requested to mention orally and in writing which are the operations he/she intends to perform, but without allowing him/her to perform them.

The forensic specialists and experts who will perform the technical and scientific findings, the expertise necessary in the case will be notified about the steps that the perpetrator would have wanted to execute in order to shut down the computer.

Also, if the case requires it, the performance of search-warrants might be ordered, and, if it is the computers that are going to be searched, this should be specifically mentioned.

As a consequence of performing the search warrants the authorities may take over any electronic equipment that might store traces of an electronic nature such as: computer memories, data storage devices, any other electrical, electronic or magnetic supports, such as the floppy disk, the hard-disk, the ZIP disk, optical disks (CD-ROM, CD-RW, DVDs), magnetic tapes, printer memories, cartridges of thermal printers or of matrix printers, memory cards, hand-held computers, electronic agendas, pagers, magnetic tape or digital report phones, cell phones, phone agendas, the last phone calls made, audio messages recorded on phone machines, digital cameras or video cameras, photography films, microfilms, negatives, photographs, papers with handwritten notes, drawings, drafts, etc.

Thus, the number, type and location of central processing units, the operating system, as well as the existence of environments for producing spare copies will be taken into account.

The entire forensic investigation on the crime scene and the tactical activities performed in the case are recorded through: a minute drawn up while the activities are being carried out, making sketches, taking the photographs required by the case, starting from the overall image to setting the screen of the computer (for this purpose, photographs of reference, sketches of main objects and of the details will be made), emphasizing reproduction traces in a latent state, collecting evidence, audio and video recording.

The investigating team must be provided with equipments and instruments specific to the investigation in the field of informatics, data storing environments, in a sufficient quantity and of a superior quality, in order to allow the copying of these data from the informatics system that is being investigated.

Special forensic kits are used to search, discover, record and collect digital evidence. The investigating team must be provided with kits specific to the forensic investigation of criminal offences involving an electronic system or equipment. Besides these special kits for collecting electronic traces, the investigators must have on the crime scene other equipments, such as:

- antistatic bags for packaging electronic components;
- various cables (serial, parallel power supply, USB, adaptor etc.);
- tongs for cutting wires, special screwdrivers, lanterns;
- floppy disks, compact flashes, memory cards;
- packing boxes, self-adhesive labels, and markers.

The examination and analysis of digital evidence are performed on faithful copies of the original evidence so that the original is kept intact, thus ensuring the possibility for third parties to check the results. It is recommended that the entire process of copying should be recorded in detail, mentioning the equipments, programs and storage environments used.