AGORA International Journal of Juridical Sciences, www.juridicaljournal.univagora.ro
ISSN 1843-570X, E-ISSN 2067-7677
No. 2 (2013), pp. 85-90

PARTICULARITIES REGARDING COMPUTER SEARCH AND FIELD RESEARCH FOR ONLINE CRIMES

A.T. Drăgan

Alin Teodorus Drăgan
Juridical Sciences, Faculty,
West University "Vasile Goldiş", Arad, Romania
*Correspondence: Alin Teodorus Drăgan, 94 B-dul Revolutiei, Arad, 310025, Romania
E-mail: drept@uvvg.ro

Abstract

The criminal investigation of a computer, also known as computer forensic, presents certain specific aspects due on the one hand to the particularitiesof the computer and, on the other hand, to the volatile nature of the data that need to be preserved throughout the entire investigations.

Key words: *computer forensic, digital evidence, data preservation*

Introduction

Informatic Cybercrimes represent the new challenge of criminal crime systems around the world. This new type of crime is shown more and more often in official statistics, most often associated with organised criminal group. This phenomena is included in the context of an unprecedented development of information technology, the proliferation of computers and a more widespread and easy access to internet.

The search is a procedural act meant to find and collect objects that contain or present marks of a crime, corpus delicti, documents, known or unknown to the judicial body and that can serve to discovering the truth.[1]

As far as computer forensic is concerned, it is an evidence process consisting in searching through an informatics system or a data storage system by the criminal investigation authorities to discover and collect the evidences needed to solve the case. Computer forensic is usually ordered when reasonable suspicions exist that evidence regarding the crime for which the criminal investigation has been started can be found on the informatics system or the data storage system for which search has been ordered. [2]

Committing a crime attracts the obligation of competent judicial bodies to determine all the circumstances referring to the person who committed the crime and to the crime itself. To do so, criminal investigation bodies can decide to send to court or not, depending on the situation, the person who committed the crime. If the case is sent to trial, the judges need to establish the existence or inexistence of the crime. He can only do so based on the presented evidence.

In juridical literature, evidences have been defined as factual elements that have informative relevance on any aspect of the criminal case, or actions or circumstances that establish the existence of inexistence of factual elements that need to be taken into account. [3]

Referring to digital evidence, they could be defined as any sort of information or 'traces' of information stored, processed or transmitted in digital format using computerised

[1] Emilian Stancu, *Tratat de criminalistică*, 3rd edition, Universul juridic publishing, Bucharest, 2004, p. 449.
[2] Adrian Cristian Moise, *Metodologia investigării criminalistice a infracțiunilor informatice*, Universul juridic publishing, Bucharest, 2011, p. 205.
[3] Grigore Gr. Theodoru, *Drept procesual penal*, Cugetarea publishing, Iași, 1996, p. 287.

systems or communication networks and that can serve as evidence of a crime being committed or that helps identify the criminal.[4]

Most frequently, digital evidence are found on a computer's hard disk. These evidences are volatile and non-volatile data.

Volatile data is any kind of data that could be lost once the power supply has been interrupted.[5] Non-volatile data are data that are stored and preserved on the hard disk when the computer is turned off.

All the objects that are found at the crime scene are considered to be data and the investigator is obliged to analyse and interpret the objects to establish what information can be obtained and which of them are relevant for the investigation. The latter needs to be collected as evidence.

As a consequence, field research is one of the activities that essentially contribute to accomplishing the objective of a criminal trial.

Field research represents the evidence process that consists in the judicial body going to the scene of the crime, the place where the result of the crime was produced or where tracks have been left, in order to observe the situation at the scene of the crime, discover and establish the tracks or marks of the crime and establish the position and state of the material means of evidence, as well as the circumstances in which the crime has been committed.[6]

In the case of a cybercrime, a specialist or forensic expert in informatics must be part of the investigating team due to the particularity of the following steps that must be taken.

Step 1: Removing the suspect from the computer

It is of utmost importance for the investigators who are field searching for digital evidence to remove the suspect from the computer. It is very likely for him to try to completely destroy any evidence or at least to deteriorate it.

If, upon the arrival of the investigators at the scene of the crime, the targeted computer is turned on, there is a risk that the suspect uses one of the numerous existing softwares to codify his files, making the recovery of the evidence more difficult, if not impossible.

Computer users today are more and more knowledgeable in codifying or securing the computer. Henceforth, it is not at all unlikely for a suspect to install or download a security programme that deletes important evidence at the simple pressing of a key or a combination of keys.

It is possible that these actions do not make it impossible to fully recover digital evidence, but the formatting programme that rewrites over the hard-disk of a computer can make the process very long and expensive, due to the advanced equipment needed.

These deleting programmes are configured to allow the choice of a 'hot key' that launches formatting or a coding programme when pressed. [7]

A hot key, often also called a shortcut key due to its capacity to easily trigger an action, represents a combination of keys that launch an operating programme.

The suspect's advice are never taken in this matter as there is a high chance they are meant to lead to an opposite result then the one intended by the investigator. They can however be written down to check later on whether they were given with bad intentions.

Regardless of the method chosen by the investigators to remove the suspect from the computer (by use of force or by misleading), it is of utmost importance to forbid his access to

[4] Gheorghe-Iulian Ioniță, *Infracțiunile din sfera criminalității informatice*, Universul Juridic publishing, Bucharest, 2011, p. 290.
[5] Dave Kleiman, *The Official CHFI Study Guide (Exam 312-49) for Computer Hacking Forensics Investigations*, Syngress, Burlington publishing, Massachusetts, 2007, p. 139.
[6] Gheorghiță Mateuț, *Procedură penală, Partea generală*, vol. II, Chemarea publishing, Iași, 1996, p. 177.
[7] Robert Moore, *Cybercrime: investigating high-technology computer crime*, second edition, Elsevier inc., Oxford publishing, 2011, p. 206.

the computer at any later point as well. He needs to be informed that the computer will be properly handled by professional staff.

Step two: Securing the scene of the crime

After having removed the suspect from the computer, care needs to be put in securing the scene and starting the process of documenting it.

The goal of this process is finding all potential sources of digital evidence and taking well-grounded decisions regarding which digital evidence will be kept at the scene of the crime.

When investigators enter for the first time the scene of the crime, it is important for them not to be too restrictive in the initial inspecting process. Limiting themselves only to specific objects can lead to lost opportunities or evidences.

Digital evidence can be found in unexpected places, such as digital photography frames, watches or bracelets that are USB mass storage devices. It is also important to keep an eye out to find certain passwords, important phone numbers and any documents associated with computers and their use. Many suspects write down details and passwords of various accounts. This is also valid for those who illegally access other people's computers.[8]

A complete investigation of the scene of the crime must take into account instruction manuals for software and external drives. They can facilitate the work of investigators, offering them details about the hardware, software and backups, details that can save a lot of time.

At the same time, the presence of books dealing with coding, digital evidence or other technical subjects can help evaluate the technical abilities of the suspect and can determine what exactly to look for in his computer.

During this phase, it is mandatory to take photographs or film objects that present interest in their current state, including laptops, external drives, video cameras and in general, any electronic device that could have a link with the crime.

Both photo-cameras and video cameras can be used. It is however preferred for the investigating team to have a specific person video recording the operation. This can be particularly useful if the suspect pretends digital evidence have been placed on purpose by the investigators at the scene of the crime. The person who films the operation can also ensure a 360 degree image of the computer and the peripheral devices attached to it.

If the investigators choose to use a traditional photo-camera or a digital one, it is important to take pictures of the suspect's computer when the warrant is executed. This will allow investigators to come back on the later on and prove what programmes were operational when the confiscation took place. In some cases, these pictures can later be used to contradict the suspect if he denies having been involved in a particular kind of activity.[9]

The photograph of every object needs to clearly present the state in which the respective object was discovered. Particular attention needs to be given to all surrounding elements, immortalising in images objects that contain serial numbers, objects that are deteriorated and different existent connections.

Certainly not least, the cables of the informatics system are to be labelled so as to allow a later correct reconnection and reassembly.

Step three: Disconnecting any external control possibility

In this phase, all network connections in the respective building are observed and any possibility to connect the computer to internet must be eliminated.

These days, the investigator who confiscates a computer is very likely to discover a wireless network. This can be problematic as wireless network routers can be placed

[8] Eoghan Casey, *Digital evidence and computer crime: forensic science, computers and the internet*, third edition, Elsevier inc. publishing, San Diego, California, 2011, p. 241.
[9] R. Moore, op. cit., p. 208.

anywhere in the building which is why the investigating team needs to use a programme that detects networks. NetStubmbler is an example of such a programme. It offers detailed information on detected networks and the corresponding routers, as well as on access points. At the same time, currently, more and more cell-phones can detect the presence nearby wireless networks. If an investigator discovers a wireless network, he will have to disconnect the network's router, remove the network cable from the router and the router also has to be unplugged to guarantee that no files can be exchanged between the respective computer and another one.

Before a computer is disconnected from any network connection, the investigator can decide to photograph or video record the computer's screen and include notes regarding any files or programmes that are downloading at that moment or that have been recently downloaded. [10]

Step four: Turning off the computer

If the investigators decide that turning off the computer is necessary to conserve digital evidence, the method considered to be most efficient is disconnecting the power cord from the computer, rather than from the plug or by using the on/off button.

Removing the power cord from the back of the computer is usually recommended to avoid the possibility for an uninterruptible power supply to continue supplying electricity to the computer.[11]

As far as laptops are concerned however, one should not remove its supply cord. This would be insufficient as laptops operate on a double source of power. They use electricity from the plug, but most of the times, laptops are also equipped with a backup battery for when they are used far from an external power source. Removing the cord will not be as efficient as for computers, since this will only make the laptop switch to its alternative source of energy. Henceforth, removing the power cord needs to be mandatorily accompanied by removing the battery (attached to the lower part of the laptop).

What happens though when we are faced with a running computer? It should be mentioned that even if the screen is dark, the computer can actually be on and active. Moving the mouse can turn the monitor on, allowing investigators to visualise the display of the screen.

If a running computer had its power cord disconnected, volatile data would be deleted and thus lost if not collected previously.

At the same time, problems related to coding can appear. It is possible for the system or files not to be coded when the computer is running. Suddenly unplugging it can trigger the information's coding, thus risking to lose the respective evidence. [12]

Therefore, before turning off the system, the following steps need to be take:[13]

- The screen will be photographed to record the data displayed when the investigation was done;
- Volatile data will be conserved;
- An image copy of the confiscated hard-disk will be done;
- The integrity of the image copy will be checked to confirm it is an exact copy of it, by using a mathematical process called CRC (cyclic redundancy checker).

The copy of the hard-disk is also called a clone. The suspect's disk will be known as source-disk, while the disk on which it will be cloned will be called destination-disk. It goes

[10] R. Moore, op. cit., p. 210
[11] E. Casey, op. cit., p. 251
[12] John Sammons, *The basics of digital forensics*, Syngress, Waltham publishing, Massachusetts, 2012, p. 57
[13] D. Kleiman, op. cit., p. 146

without saying that the destination-disk needs to have a capacity at least equal to the one of the source-disk, if not bigger.

As hard-disks are rather fragile, it is recommended to make two such clones as a backup measure. One of the clones will be used to be investigated, whereas the other one will serve as backup. Ideally, all investigations are done on the clone copy and not on the original. As far as the court is concerned, a correctly obtained clone is as viable of an evidence as the original.[14]

In some situations, it is preferable to connect a different keyboard and a different mouse to the computer so as to conserve fingerprints and biologic evidence.[15]

Step five: Disassembling the computer

After disconnecting the computer from the power source, the next step for the investigator is to disassemble the computer and prepare it to be transported. Of course, when only one computer exists, this greatly simplifies the investigator's work. Occasionally, however, executing the warrant can lead to confiscating several computers. In these situations, it is necessary to disassemble the computers in such a way that enables the re-assembly of any computer in the laboratory.

It is recommended that every cable or device is labelled as soon as they are disconnected from the back of the computer. A label should be applied to the cable or respective device and another label should be stuck on the back of the computer on the connecting port from where the device had been removed. If the investigator found a computer with unused ports, these should be covered with cello tape and labelled as unused. [16]

Step six: Obtaining extra evidence from the scene of the crime

After disassembling the computer, the investigators can begin examinating the area, looking to find other evidence that can have a link to the confiscated computer. As it was previously mentioned, these evidences could be disks, CDs, USB sticks, external hard-drives, instruction manuals and other storage devices or documents related to using the computer.

Considering the small dimensions of memory cards, these could easily be hidden almost anywhere. For example, one such device could be hidden in a book, in a wallet, in the lining of clothes etc.

One will take into account as well the possibility to locate a potential list with passwords. This could be stuck on various surfaces around the location of the computer.

Once the digital data storage have been located (i.e. USB memory sticks), measures need to be taken to ensure files cannot be added or deleted from the device.

Step seven: Preparing the evidence to be transported

Once all the evidences have been collected, they need to be ready to be transported. If plastic bags are used, it is important to keep the hard-disks and the storage devices in a bag without static electricity to prevent deterioration of the content. If the evidences are put in boxes, wrapping materials is to be used to secure the computer and the other devices.

Regardless of the chosen wrapping method, the computer should not be placed in the trunk of the police car. It should be put on the back seat of the car and taken to a secure storage room. At least two arguments exist against the use of the trunk:

- The heat during warm months or extremely low temperatures can affect digital evidence;
- Electronic emissions – a lot of police car have equipment to control communication and it can deteriorate the evidences.

[14] J. Sammons, op. cit., p. 54
[15] E. Casey, op. cit., p. 250
[16] R. Moore, op. cit., p. 218-219

Conclusions

The presence of a computer expert is absolutely necessary and will ensure the right steps are followed in executing a warrant for digital evidence. Computer criminal forensic experts need to have sufficient knowledge in computer technology and understand how a hard-disk is structured, how the file system works and how data are recorded.

Bibliography:

John Sammons, *The basics of digital forensics*, Elsevier inc. Publishing, Waltham, Massachusetts, 2012;

Eoghan Casey, *Digital evidence and computer crime: forensic science, computers and the internet*, third edition, Elsevier inc. publishing, San Diego, California, 2011;

Robert Moore, *Cybercrime: investigating high-technology computer crime*, second edition, Oxford publishing, 2011;

Gheorghe-Iulian Ioniță, *Infracțiunile din sfera criminalității informatice*, Universul Juridic Publishing, Bucharest, 2011;

Adrian Cristian Moise, *Metodologia investigării criminalistice a infracțiunilor informatice*, Universul Juridic Publishing, Bucharest, 2011;

Dave Kleiman, *The Official CHFI Study Guide (Exam 312-49) for Computer Hacking Forensics Investigations*, Syngress publishing, Burlington, Massachusetts, 2007:

Emilan Stancu, *Tratat de criminalistică*, second edition, Universul Juridic Publishing, Bucharest, 2004;

Gheorghiță Mateuț, *Procedură penală, Parte generală*, "Chemarea" Publishing, Iași;

Grigore. Gr. Theodoru, *Drept procesual penal*, "Cugetarea" Publishing, Iaşi, 1996.