ELECTRONIC EVIDENCE AND ITS SIGNIFICANCE IN INVESTIGATIONS

Prof. Svetlana Nikoloska, Phd
University "St. Kliment Ohridski "- Bitola
Faculty of Security - Skopje
svetlananikoloska@hotmail.com

Maria Gjosheva, Phd
gjoshevamarija@gmail.com

APSTRACT

Cyber crime is a specific form of criminality with a number of emergent forms where the computer appears as a means or object of a criminal attack. The quality of the provided evidence depends on the initiation of a criminal procedure against perpetrators of criminal offenses in the area of cyber crime. Cyber crime constitutes crimes that have a digital dimension, which means that the evidence pointing to a specific crime and its perpetrator are in digital form. The entire process of criminal investigation or investigation is followed by a system of measures and actions for providing electronic evidence, their correlation with other material evidence and connection with suspected perpetrators as a prerequisite for complete clarification and initiation of criminal proceedings.

The subject of this paper is the study of electronic evidence, the process of their provision through the application of legal measures and actions and the rules of digital forensics and case analysis from the Macedonian criminal practice.

Keywords: cyber crime, electronic evidence, digital forensics, investigation.

1 professional paper
INTRODUCTION

Electronic evidence is crucial in proving all forms and forms of computer criminality, and their security is subject to criminalistic research through the application of legal measures and actions and compliance with the rules and techniques of digital forensics. The criminal investigation is under the jurisdiction of the criminal police in coordination of the public prosecutor as a competent body for prosecuting perpetrators of criminal acts prosecuted ex officio. The main direction of the criminal investigation and the overall investigation are always the suspects, and then searching for electronic and other material evidence in order to successfully conduct the criminal procedure and to prove the guilt of the perpetrators for a specific computer crime.

The new ways of committing crimes that are performed through electronic devices and the only evidence in these cases are the electronic evidence. The very nature of data and information stored in electronic form, unlike traditional ones, makes it easier to manipulate.

The development of the Internet and its applications offer many opportunities, social media, web pages, interaction, and recently the ability to store data in a cloud (virtual space) where data is stored. It is very important to know, in order to keep the case electronically required in such places to store data, especially when it is important for the case.

1. CRIMINAL INVESTIGATION

Criminal investigation should be well planned and coordinated with individuals who will participate in the investigation process with specific tasks in accordance with the legal authorizations for the implementation of investigative measures and actions and in certain cases depending on the needs and determination of special investigative measures.

When it comes to criminal investigation of cyber crimes, special attention is paid to the investigation team that should include a public prosecutor, a criminal investigator and an expert in the field of computer science with knowledge of
criminology in the direction of proper search, security, keeping electronic evidence and putting it in a form acceptable to the judiciary (Nikoloska, 2013).

The criminal investigation process starts from general suspicions or clues, and ends with the provision of relevant evidence on the basis of which the Public Prosecutor raises the charge and represents it before the Criminal Court.

The degree of doubt may and does not have to have a decisive factor, most often the initial information determines: the shape, content and stages of the detective function, that is, the pre-trial procedure (criminal or operational activity), as well as the criminal procedure in general (Angeleski).

The criminal investigation of the cyber incident should in fact respond to the nine golden criminal questions (Vodinelić, 1984): WHAT (happened), WHO (committed the crime), WHEN (the crime was done), WHERE (the crime was done), HOW (the crime was done), WHAT (was done), WHO WITH (the crime was done), WHO or WHAT (has been damaged- victim), WHY (the crime has been done).

In principle, the investigation of cyber incidents should be investigated "step by step". Different authors define the steps of the criminal investigation in various ways. According to Rosenblatt, this is a 4-step investigation and that (Rosenblatt, 1995):
1. Initial investigation,
2. Entering the trail of the attacker,
3. Detecting the identity of the attacker and
4. Arrest or arrest.

While, according to Peter Stivenson, the research process divides into seven distinct steps and that (James & Norby, 2009):
1. Eliminate what is obvious;
2. Formulate a hypothesis for the attack;
3. Reconstruction of the crime;
4. To detect the computer from which the attack was carried out;
5. To analyze the computers those are the source, target of the attack and those who served as intermediaries;
6. To gather evidence, if possible, and the computers themselves;
7. To give the conclusions and evidence material to the investigators and to persons who, according to the law, prosecute the perpetrators (the plaintiff).
2. DIGITAL FORENSICS

Digital Forensics deals with the collection of digital evidence from the cyber crime scene. The cyber crime scene is one computer (or more computers) that attacks another computer (or more computers) through some means. It is important that evidence material provided from the crime scene can be used as evidence and to be complete in the context of the investigated case.

There are three types of forensics that refer to computer systems and electronic evidence. Evidence does not have to be created from a computer, but from something else we always associate with a computer, for example from a printer, a router, or a pocket computer (James & Norby, 2009).

• The first type is the traditional digital forensics which is the collection of digital evidence from a computer, disk or from a device that includes a computer or is considered to be able to create or process electronic (digital) data.

• The second type of digital forensics is cyber-forensics or network forensics. It involves gathering evidence showing that certain digital data has crossed through a medium between two points in the network. The evidence collected in this way is always collected by making conclusions from a device in the path.

For example: physically we can not see the data passing on the Internet. However, a sniffer can be used to record packets of data as they are sent and to get an interpretation of that data packet. Or we need to make a comparison between the sender's and the receiver's receipts from the two devices that are considered to have been transmitted between them and to conclude the transfer from the records, most often you need to make a direct collection of data from the hard disk.

• Forensic analysis of software that deals with identifying the author, on the part of the software code of the code itself.

Digital forensics provides the provision of relevant electronic evidence necessary for the process of proving the criminal offense before the court and the guilt of the perpetrators.

But do we always have the most appropriate evidence that:
A right has been violated, some damage was done, something is unauthorized posted, published, displayed, distributed or otherwise reached under someone else's law, someone is the owner of the law (Maričić, 2006).
In the procedure for detection of cyber crimes, what should also be taken into account is the fact that digital data can be manipulated with the help of a remote terminal and it is very fast, which in fact makes it difficult and impossible for their monitoring, supervision and control (Banović, 2002).

3. ELECTRONIC (DIGITAL) EVIDENCE

**Digital evidence** is any information in a digital form that has probative value and is transmitted in such a form. The term digital evidence includes computer stored or generated evidence information, digitized audio and video evidence signals, digital cell phone signals, information on digital fax machines and signals from other digital devices.

It is any information generated, processed, stored or transmitted in a digital form that the court can accept as evidence-proof.

In the procedure for **collecting and analyzing digital evidence**, the authorized persons of the investigation should adhere to the principles that are part of the planning concept of the investigation, that is:

• In dealing with digital evidence, all general forensic procedural principles must be strictly enforced;
• Before and during the provision of digital evidence, no action taken must cause a change in the digital evidence;
• Only a well-trained person can access the original digital evidence when there is a need for it;
• All activities related to the collection, storage, access or transfer of digital evidence must be documented, stored and made available for inspection by interested parties in the procedure (victim, suspect, attorney, etc.).
• The official person handling the digital evidence materials is responsible for all activities in relation to digital evidence.
• Digital evidence is transmitted only on the basis of an inventory of both parties (the one who gives them and the recipient) in accordance with the legal regulations.
• Ensuring the appropriate transfer or transport of digital evidence as well as appropriate conditions for their storage.
There are three categories of electronic evidence in cyber incidents:

- **Transient data or information that is lost after shutting down the computer**, such as open working memory connections, resident memory programs, etc. This data can be lost even by turning off the computer. Before turning off the computer, the sensitive and encrypted data should be immediately examined, located, and extracted, since it may happen after disconnecting them from reaching them.
- **Sensitive data or data that is scaled on the hard disk** that can be easily edited, for example log files and the like.
- **Temporary access data or data stored on the hard disk** that can only be accessed at a specified time.

There are several recommendations in the world, among which are the recommendations of **IOCE (International Organization on Computer Evidence)** (IOCE, 1999), which defines the procedures for collecting and processing the evidence material **that mainly refers to** which media and what kind of media features are acceptable for storing the original evidence, what documentation for image processing should be, how the verification of the original and the images processed should be regarded as irreconcilably confirming that the integrity of the original digital evidence has not been violated, the original should be kept in the system of investigation from the very initiation of the investigation and the disclosure of evidence to the testimony at the court and administrative arrangement of each document and a report in the entire investigation with the data of the responsible person for each written document that would mean the existence of responsibility to keep digital evidence of changes, damages or deletion (disappearance).

4. ANALYSIS OF ELECTRONIC EVIDENCE

The analysis of electronic evidence is the most subtle part of the criminal investigation, since without a good analysis of each evidence individually and analysis of its connection with other evidence there is no case documenting.

In the Republic of Macedonia, after the establishment of the **Cyber Crime and Digital Forensic Unit**, the laboratory for Digital forensic of digital evidence is continuously upgraded and their collection and adoption in a condition acceptable to the judiciary. Computer processing of evidence is applied almost in all forms of criminality.
There are several tools or utilities that are appropriate for analyzing forensic evidence on a drive. Despite the differences in implementation, everyone has several similarities. In any case, the forensic utility allows the analyst (James & Norby, 2009):
• Make a bitmap image on the target drive.
• Make text searches, general and specific.
• Write specific search records.
• Make MD5hash on disks and files.
• Make a list of files and directories on the target disk.
• Search for deleted files and data, data in file slack and data in cache or exchange files.

Documenting electronic evidence is the final phase of the criminal analysis and everything needs to be found, extracted and analyzed, "put down on paper" or made a report on all the evidence individually and then a summary analysis of all the evidence and a final document - Expertise.

5. EXAMPLE FROM THE PRACTICE IN THE REPUBLIC OF MACEDONIA

The Cyber Crime and Digital Forensics Unit in June 2015 filed a Criminal Application on the basis of a reasonable suspicion of committing a criminal offense foreseen and punishable under Art.251 "Demage and unauthorized entry into a computer system" by the Criminal Code of the Republic of Macedonia.

Namely, A.T. unauthorized intercepted with an administrator user in a computer owned by a legal entity from Skopje to which the website www.exploringmacedonia.com was hosted and then gaining administrator privileges has changed the official content of the website, that is, unauthorized uploaded new files, making the computer data unusable and useless. From the submitted logs for all unauthorized logs carried out to the host server, their analysis was performed, where the IP addresses from which it was accessed with time and date were determined, and with the further investigation the user - the person AT - was identified, and therefore the perpetrator of the crime. In this connection, a search was carried out in the home and the premises of the reported where the computers were found through which A.T. made unauthorized access to the computer server owned by the legal entity.
Due to the provision of digital evidence, a digital forensic analysis was carried out - an expert report on the confiscated computer equipment found during the search.

By using standardized forensic procedures and using special licensed forensic software, a greater number of deleted fragments from accessing IP addresses have been reconstructed, then URL paths from the Internet search engines Google Chrome and Mozilla Firefox and digital photos.

The found elements of Internet access from the IP addresses compared to the analyzed logs and the attached files at the critical date and time of the damaged host server, it was found that the same IP addresses, URL paths and files obtained from the expertise of the temporarily confiscated computer equipment by AT. are in compliance with which there are reasonable doubts that the unauthorized access to the server has been committed, ie it committed the crime (HETIPEC, 2015).

The analysis of this case shows the importance of electronic evidence, especially in criminal cases where electronic evidence is a single piece of evidence.

CONCLUSION

This paper presents an introduction to the significance of electronic evidence and their application in the litigation of criminal offenses. Nowadays, when we live in a world where unimaginable functioning is possible without the use of information technology and using electronic devices that make our work easier, electronic evidence is all around us.

The collection of evidence through international legal assistance needs to be put at the highest level, and be a priority in the future, because this is the only way to get the necessary electronic evidence no matter where they are. The resources of the international institutions Interpol, Europol, EC3, Selek et al.

For successful investigation it is very important, the public prosecutor to have computer knowledge, to understand the reports of the experts, to advise, give directions to the police during the investigation, and to monitor the collection of electronic evidence to comply with the law. The prosecutor should be able to determine the most appropriate jurisdiction to prosecute particularly when it comes to cross-border crime.
REFERENCES

7. Banović B *Providing evidence in the criminal investigation of criminal acts of economic crime*, Higher School of Internal Affairs, Belgrade, 2002;