COMPUTER FORENSIC IN FUNCTION OF CRIMINAL INVESTIGATION

Svetlana Nikoloska PhD
St Kliment Ohridski University – Bitola
Faculty of Security - Skopje
svetlana.nikoloska@uklo.edu.mk

Marija Gjosheva, PhD
gjoshevamarija@gmail.com

Abstract

Computer forensics is increasingly finding its place in the criminal investigation of criminal offenses in order to shed light on and provide the evidence necessary to initiate criminal proceedings against the perpetrators of crimes that have misused computer technology in criminal activities. Criminal investigation is a procedure of using tactics, techniques and methods aimed at detecting, clarifying and providing evidence through legally prescribed operational-tactical measures and actions, investigative actions and special investigative measures. The Macedonian legislator in the criminal procedural legislation envisages measures and actions for providing electronic evidence which is relevant in computer crimes, but also in specific criminal situations electronic evidence has its meaning in the process of clarification of other classic and economic crimes. This paper analyzes the steps and procedures for extracting, processing and presenting electronic evidence that represent data contained in computer devices, data transmitted through computer systems and networks in order to adapt them to a form acceptable to judicial authorities based on the analysis of all evidence bases the verdicts on the perpetrators who are charged with a specific computer or other crime. An analysis of the actions of the competent investigative and judicial bodies in the process from detection to verdict is made by analyzing reported, accused and convicted perpetrators of the most committed computer crimes, but an analysis will be made for the need of electronic evidence in other crimes through analysis of case.

Keywords: Computer forensics, Forensic research, Computer devices, Electronic evidence, Perpetrators of crime.
INTRODUCTION

Forensics is the process of using scientific methods to provide, analyze, and present evidence in court. The practice in ancient Rome in criminal charges was as follows: the case to be presented to a group of public officials at a court hearing, where the defendant and the plaintiff in public presented their facts and evidence to the Judicial Council in order to convince them of their a version of the veracity of the case, presenting material and intangible evidence, visible and invisible (latent) evidence on the basis of which the trial chamber renders the verdict. Some of the evidence is visible, material, but bigger part of it is invisible depending on the criminal situation, with "suspicion" that it exists, but it needs to be processed in special techniques and made visible and acceptable to the investigating and judicial authorities. It is a task of forensics, which is based on proven scientific methods and techniques, as well as procedures in the process of discovering and gathering evidence, and their provision and storage are aimed at enabling their application in court. The beginning of forensics in scientific circles was taken in 1248 when the Chinese physician Hei Dawn Yu wrote the book entitled "The washing away of wrong". This suggests that forensics began to be studied much earlier than in 1904, when the first facial dactyloscopy was performed, and in the United States it was not until 1930 that it was used. In the 1980s, DNA analysis and profiling of the perpetrator began to develop, and DNA was used as evidence in court only in the late 1990s (Ganiya, 2019).

The inclusion of forensics in the investigation and resolution of criminal offenses starts from the place of commission of the crime through effective detection of objects and traces as material evidence and objects bearers of traces for their provision for further expertise, analysis and storage. Upon discovery, objects and traces are specially packaged, marked, stored and transported to appropriate laboratories for their expertise. Really important is the fact that the "chain of custody" is established for each case as evidence from the moment of its discovery until its presentation in court (Jackson & Jackson, 2009).

With the development of the society, and especially the technological development, the benefits, in addition to the positive sides, also have negative
ones, which are most often manifested by the abuse of technology for criminal purposes. This is especially evident with the massiveness of information technology and its penetration into all pores of social life from application in the family, schools, state bodies and institutions, economic and industrial facilities and daily increasing the number of users of information technology represented by a large number of devices which are performing automatic data processing. There is also electronic communication through computer networks and systems on the Internet, which enables very fast private and business communication of citizens, but also communication of criminals who not only use communication for organization in committing crimes, but also abuse it as a tool of execution and the object of criminal action. The misuse of computer devices, systems and networks as a tool or object of a criminal attack, necessitates the provision of invisible "latent" electronic evidence.

This requires scientific methods and techniques of extracting electronic evidence in a form acceptable to the judicial authorities so that they can apply it in the overall analysis of all the evidence on the basis of which they will pass the judgment.

The need to apply scientific knowledge, skills and techniques for finding, providing and storing electronic evidence is the subject of a special branch of forensics, and that is the computer forensics. Computer forensics is a set of scientifically proven methods and specialized tools for identifying, collecting, storing, analyzing, and presenting evidence related to the reconstruction of computer devices, systems, and network abuse. Computer forensics enables the discovery, provision and storage of invisible electronic evidence in a form acceptable to the judiciary.

Criminal investigation is a process of operationalization of legal measures and actions aimed at detecting, clarifying and providing relevant evidence to investigate a criminal problem that has a complex nature and its clarification is a complex procedure of applying criminal tactics, techniques and methods. Criminology as a science, in addition to developing its own methods and techniques used in forensic research, also uses knowledge, skills, techniques and methods from other sciences that are adapted to illuminate and provide evidence of a specific criminal event.
CRIMINAL OFFENSE - PERPETRATOR - LAST

In cases of misuse of computer devices, computer systems and networks in the criminal activity of perpetrators, the team of investigators includes specialists in the field of computer forensics who contribute to the extraction, provision, storage and presentation of electronic evidence. Macedonian criminal law in recent years has accepted several recommendations from international conventions, especially the Convention on Computer Crime in terms of providing legal measures and actions to provide electronic evidence as special types of evidence that differ from material and ideal evidence that was recognizable and acceptable for the judiciary. In addition to the legal provisions for providing electronic evidence, Standard Operations Procedures for Computer Crime have been adopted on the manner and techniques of criminal police and forensic experts from the Ministry of Interior of the Republic of Northern Macedonia who are responsible for clarifying and providing electronic evidence and always participate. In operational teams for criminal investigation of criminal situations in which it is necessary to provide electronic evidence.

COMPUTER FORENSICS

Computer forensics is a branch of forensic science that deals with the legal methods of providing and processing electronic evidence extracted from a computer or other computer data carrier. Computer forensics investigates all media for extracting and transmitting data in order to find and analyze documentation or other electronic evidence related to a particular criminal activity. Nowadays, the term computer forensics is increasingly becoming digital forensics because in addition to computers as a means of execution, other digital devices are increasingly emerging such as digital cameras, mobile phones, smartphones, personal digital assistants, etc (Ćosić & Baća, 2010).

Computer forensics is the process of investigating the detection of illegal activities that have elements of a crime under the Criminal Code. This process consists of methods of collecting, securing, storing, analyzing and presenting evidence that can be found on personal computers, servers, radio stations, transmission media, computer networks, databases, mobile devices
and all other information and electronic devices that have the ability to process, transfer and store (store) data in electronic form. The investigation process must be based on scientifically proven methods and legally prescribed procedures in order for the evidence provided to have the value of evidence accepted by the judiciary. Computer forensics is based on computer science, but also on forensic science, because it collects and analyzes data that are further used as evidence in court in order to establish criminal liability for the perpetrator of a specific crime.

Computer forensics deals with the collection of electronic evidence from the site of a computer crime and the provision of evidence for the path of computer data and the consequent occurrence of each individual computer incident. There is a source, a path and a victim in every computer incident. What needs to be answered first is whether it is a computer incident, because very often the suspicions of a computer incident after providing the evidence are clarified that it is not an incident - a crime, but a technical error or something else (James & Norby, 2009).

**CRIMINAL INVESTIGATION**

Criminal investigation is developed in special disciplines, is different types of criminal investigation aimed at specific investigations of a special group of crimes (Rachel, 2010), that have the same or similar criminal characteristics. Criminal investigation is operationalization, investigation of a criminal problem that has a complex nature and depending on the initial knowledge and facts available, it is planned to activate the most adequate criminal-technical means, tactical methods and scientifically or practically based methods needed to determine the most optimal pathways on a specific operational (i.e. criminal) case (Angeleski, 1996).

Criminal investigation is a process or system that should be applied in the clarification of criminal situations, through the application of measures and actions and a continuous and connected process of action and coordination between operational and investigative bodies, in order to fully shed light on criminal cases by providing relevant evidence through legal proceedings and procedures according to "case studies" - the method of investigation of the criminal case in full, by clarifying and proving all committed crimes, which are is the perpetrators and their connection and
responsibility for the specific crimes committed and their criminal role in the criminal case.

The criminal investigation is related to several stages: the phase of obtaining information - operational information, and then follows the planning phase, the phase of implementation of specific measures and activities and the phase of submitting a report on the specific criminal situation by filing a criminal complaint or submitting a report to the public prosecutor, but certain measures and activities continue until a final court ruling.

Criminal investigation is a complex procedure and depending on the received report and the obtained operational knowledge of the police, a series of measures and actions are taken to confirm the initial information by applying legal measures and actions for which the police has authorization for their application (Criminal Procedure Code, NMK). All measures and actions are notified to the Public Prosecutor, and by order and coordination of the Public Prosecutor in the criminal investigation, investigative actions and special investigative measures are applied depending on the character and complexity of the criminal situation and the process of providing evidence for full clarification of criminal proceedings. Criminal investigation is a process of taking a series of measures and actions, but when the criminal situation indicates elements of abuse of computer devices, systems and networks, it is necessary to provide electronic evidence, but also to provide other items that are computer data carriers like personal computer digital cameras, cameras, mobile phones and media in which computer data is stored - USB, CD, DVD, etc. In the criminal investigation, especially in situations when it is necessary to find objects - computer devices and components and computer data contained in other media, the following investigative measures and actions are taken upon a reasoned order of the court at the request of the public prosecutor: research (Art. 180-192); Investigating a computer system and computer data (Article 184); Temporary provision and seizure of items or property (192 - 199); Temporary seizure of computer data (Article 198); Dealing with data that is a banking secret, property in a bank safe, monitoring of payment operations and transactions on accounts and temporary suspension of execution of certain financial transactions (Article 200); Recording of temporarily confiscated documents, documents and technical recordings (Article 201). Methods for securing evidence are most often used: Statement of the accused (Art. 205 - 211); Witnesses (Articles 212 - 232);
Expertise (Art. 236 - 243); Recordings and electronic evidence (Art. 250 - 251). For specific criminal offenses, which include some of the computer crimes, the application of special investigative measures is determined when there are grounds for suspicion. (Article 253) These are part of the legally prescribed investigative measures, the application of which can provide evidence, as follows: Monitoring and recording of telephone and other electronic communications in a procedure determined by a special law; Monitoring and recording in a home, closed or enclosed space belonging to that home or business space marked as private or in a vehicle and entering those premises for the purpose of creating conditions for interception of communications; Secret surveillance and recording of persons and objects with technical means outside the home or office space marked as private; Secret inspection and search in a computer system; Automatic, or otherwise, search and comparison of personal data and insight into realized telephone and other electronic communications. (Art. 252)

Depending on the nature of the criminal situation and the grounds for suspicion of criminal investigation, a police officer from cybercrime and a computer forensic officer from digital forensics are appointed to form an investigation team in order to contribute to the provision, analysis and storage of electronic evidence, and the participation in the preparation of a full report or criminal charge after which the public prosecutor further proceeds with the filing of an indictment.

THE ROLE OF COMPUTER FORENSICS IN CRIMINAL INVESTIGATION

Computer forensics is important for forensic research in the context of the increasing use of computer devices, networks and systems in the connection, preparation and execution of crimes. Just as criminals use information technology and computer systems and networks to connect, negotiate, organize, and carry out criminal activities, so do criminal investigators use measures, actions, and techniques to find, extract, and adjust electronic evidence that correlates with other evidence on confirmation of the grounds for suspicion to the extent of reasonable suspicion and indictment by the competent public prosecutor against the perpetrators of criminal offenses (Nikoloska, Methodology for Computer Crime Investigation, 2013). It is a complex procedure, but if the crime is fully investigated, then the effects of
the criminal investigation will be achieved, the purpose of which is undoubtedly not only to discover the crime, find the perpetrator and convict him, the ultimate goal is completely clarification on the basis of evidence, sanctioning of perpetrators and confiscation of criminally obtained proceeds.

The criminal investigation starts from the first moment of receiving any kind of information that a computer crime has been committed, or the information is directed to a perpetrator or a group of perpetrators for whom there is information that they are committing computer incidents. Through operational checks that are planned and undertaken in a short period of time, the general suspicions should be at the level of grounds for suspicion of taking more serious steps or taking measures and activities to determine the nature of the computer incident, and then planning and providing digital evidence as well as finding and apprehending the perpetrators. These are measures that are performed in the pre-investigation procedure, or pre-trial procedure, but this is the phase where the emphasis is on forensic research, because without a well-conducted criminal procedure, there is no good criminal procedure, then the perpetrators are "a step forward or an advantage". All missed actions or measures in the pre-investigation procedure, make "holes or evidence gaps" that are difficult to fill in the stage of the criminal procedure, and hardly any court would impose a sanction without good and relevant evidence.

Computer forensics, or computer forensic science, is a combination of technology and science that seeks to determine how a computer system is involved in a crime. The science of computer forensics includes knowledge of the methods and procedures used in analyzing and collecting data (evidence). Technology is a set of different tools that allow the application of methods and procedures that are subject to the scientific side of forensics. The criminal act can be committed on any computer connected to a local or global network regardless of its geographical location. Also, the computer-attacker can be geographically located at any point on the globe. Couple attacked computer - an attack computer can be within the borders of one country or be housed in different states. This means that they can be accommodated in the same country or in different countries, i.e. forensic scientists are often forced to collect digital evidence in one country and show it in court in other countries. This fact itself requires the introduction of certain rules for the collection, distribution and presentation of digital
evidence that will be relevant to all countries (Stoilkovski, Kaević, & Gelev, 2012).

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

- **The first type is traditional computer forensics**, which is the collection of digital evidence from a computer, disk, or device that includes a computer or is thought to be able to create or process electronic (digital) data.
- **The second type of computer forensics is cyber-forensics or network forensics.** It includes gathering evidence that certain digital data has passed through a medium between two points in the network. Evidence that is collected in this way is always collected by drawing conclusions from a device in the path. For example: physically we cannot see the data that passes through the Internet. But a sniffer analyzer can be used to record data packets as they are sent and to get an interpretation of that data packet. Or we should make a comparison between the transcripts of the sender and the recipient of the two devices that are thought to have been transferred between them and draw a conclusion from the transcripts, usually by directly collecting data from the hard disk.
- **Forensic software analysis** that deals with identifying the author, part of the software code from the code itself.

The criminal investigation of computer incidents is a step-by-step approach to the "truth". The first steps are undoubtedly tied to more indications and of course more versions. The first step taken should be to answer the question: Is it a crime or something else?, and then with the other steps taken and answer the other eight golden criminal questions - Who (committed the crime)?; When (it is done); Where (is it done)?; How (is it done)?; With what (is it done)?; With whom (is it done)?; Who or what (is damaged)? and Why (is it done) ? (Vodinelic, 1984).

Criminal investigation as a process should be well planned and coordinated with persons who will participate in the research process, concretizing their tasks in accordance with the legal powers and determining
the time and place of conducting specific investigative measures (apartment interest) or determining special investigative measures. - Which, over which persons and for what period of time? In principle, the investigation of computer incidents, as well as other criminal cases, should not be investigated spontaneously, but "step by step", and this should be proposed and implemented by authorized officials from the Department of Computer Crime and Digital Forensics.

Each step within one phase of the investigation leads to the other step and thus ensures the control of previous activities within each of the planned steps. This is an investigation in 4 steps (Rosenblatt, 1995):

- Initial investigation.
- Tracking the attacker.
- Discovering the identity of the attacker and
- Detention or arrest.

According to Peter Stevenson, the criminal investigation process is divided into seven separate steps (James & Norby, 2009):

- To eliminate what is obvious.
- To formulate a hypothesis for the attack.
- To reconstruct the crime.
- To detect the computer from which the attack was performed.
- Analyze the computers that are the source, the target of the attack and those who served as intermediaries.
- To gather evidence, if possible, the computers themselves.
- To hand over the conclusions and evidence to the investigators and the persons who are prosecuting the perpetrators (plaintiff) in accordance with the law.

It is indisputable that criminal research should be done "step by step", but depending on the criminal situation, it requires the need to act quickly, but also to act at the request of international cooperation due to the nature of the computer incident, whether and what evidence or measures are needed to be undertaken in one or more foreign countries. Rosenblatt’s (Rosenblatt, K. S. 1995) views on the categorization of the six objectives of conducting
research and providing evidence are precisely aimed at fully elucidating the criminal situation:

- Understand how the hacker enters the system.
- To obtain the necessary information to justify a wiretapping device in the telephone line used by the hacker.
- To find out why the hacker chose the victim's computer.
- Gather as much evidence of the breakthrough as possible.
- Gather information that could narrow the list of suspects or at least establish that the hacker is not an employee.
- Document the damage caused to the victim, including the time and effort the victim spent investigating the incident and determining the extent of the damage done to the computer.

In the implementation of the research process, appropriate procedures should be followed, which refer to the following actions: Checking the records, log files, and other information about the offspring.

- Gathering information from people who might know certain details about the case.
- Control of all stages of the investigation.
- Search engine optimization (locating a compromised computer).
- Search for the resources of the suspect / suspects (home, business premises, internet cafe, etc).
- Providing digital evidence and their analysis.

**ELECTRONIC EVIDENCE**

According to the international definition in the field of forensic science, electronic (digital) proof is any information in electronic form that has proof value and which is adapted or transmitted in such a form. The term electronic proof includes computer stored or generated evidence, digital audio and video proof signals, digital cell phone signals, digital fax machine information and signals from other digital devices. So, electronic evidence is any information generated, processed, stored or transferred in digital form that the court can accept as authoritative, is any information composed of digital 1 and 0, stored or transferred in digital form, as well as other possible
copies of the original digital information that has probative value and on which the court can rely, in the context of forensic acquisition, analysis and presentation.

The term "electronic proof" implies any relevant data sufficient to provide clarification and proof of a crime by the use of computer devices, networks and systems, which can be provided by extracting computer data in the form of texts, images, videos, phonograms, financial statements, etc.

In 1984, the FBI began developing a laboratory and computer evidence testing program that grew into a single CART (Computer Analysis and Response Team) team, which was later formed at several stations in the United States. In the United States today, forensic analysis is performed in well-equipped laboratories. The use of electronic evidence is reflected in the way the Federal Criminal Laboratory in the United States was set up in February 1999, SWGDE - Scientific Working Group for Digital Evidence. SWGDE members are under oath (judicial authorities) and experts who are not under oath are scientific workers. The FBI sponsors SWGIT (Scientific Working Group in Imaging Technologies), for the electronic processing of data and images for the needs of the judicial system after previously defining and specifying the terms for acquisition, storage, processing, analysis, transmission and output format - photography (Whitcomb, 2002).

There are three categories of electronic evidence in computer incidents:

- Transitional data or information that is lost after turning off the computer;
- Sensitive data or data that is scaled to the hard disk (HD).
- Temporarily accessible data or data stored on the HD hard drive.

Electronic proof (EP) consists of a number of indirect factual evidence, none of which must be excluded for any reason. The evidence must be complete, complementary (practically intertwined) or practically non-existent. n. crack at the conclusion, most importantly for the establishment of solid evidence. In the process of collecting and analyzing digital evidence, it is necessary for the authorized persons of the investigation to adhere to certain principles, which, among other things, are in some way part of the planning concept of the investigation or the most common or most appropriate way of conducting the investigation process, and that would be the following:
In dealing with digital evidence, all general forensic procedural principles must be strictly enforced.

Before and during the provision of digital evidence, no action shall be taken to change the digital evidence.

Only a well-trained person can access the original digital proof when it is needed.

All activities related to the collection, storage, access or transfer of digital evidence must be fully documented, stored and made available to the interested parties in the computer incident (the victim, the suspect, the lawyers - the defense counsels, etc.)

The official person handling digital evidence is responsible for all activities related to digital evidence when in his or her jurisdiction.

Digital evidence is transmitted only on the basis of a census from both parties (the one who gives it and the one who receives it), in accordance with legal regulations - usually with a certificate of submitted and received cases and evidence.

Providing appropriate transfer or transportation of digital evidence as well as appropriate conditions for their storage (Nikoloska, Methodology for Computer Crime Investigation, 2013).

Electronic proof management is a complex task that requires the preparation of special procedures for handling and managing digital evidence, which means a certain responsibility for authorized persons who participate in the extraction and management of digital evidence, if not acted upon. When it comes to digital evidence, technology has made it possible to create copies that are true to the original in every way. In this case, the presentation of copies is in principle acceptable, although originals exist and are available. In practice, it is even preferable to present copies to remove any doubts about the possibility of changing the original. Even a printed form of a digital document is considered valid unless it can display all the information necessary for the process.

The expert in the ICT research team should provide:

- No evidence should not be damaged, destroyed or compromised in any way in the forensic acquisition procedure and computer analysis;
- No possible computer virus should be inserted into the computer being tested during the acquisition and analysis process;
With the extracted potentially relevant evidence, it should be properly manipulated and protected from possible mechanical or electromagnetic damage;

To establish an uninterrupted chain of storage and maintenance of the integrity of the evidence;

The functional aspect to be compromised as soon as possible, or not at all;

To obtain any necessary information during the forensic acquisition and analysis, the suspect should gather all the necessary information from the forensic expert on the manipulations committed during the criminal act on the suspicious computer.

There are several tools that are suitable for analyzing forensic evidence on a disk. However, despite the differences in implementation, they all have several similarities. Today's forensic computer equipment differs in only one way: it is based entirely on DOS or allows analysis in MS Windows (of course, this does not apply to Unix-based tools). However, forensic equipment allows the analyst (James & Norby, 2009) to:

- Make a bitstream image of the target disk;
- Do text searches, general and specific (is either list search - specific or requesting an email address or jpeg file - in general).
- Write specific search entries;
- Make MD5 hash of disks and files;
- Make a list of files and directories on the target disk;
- To search for deleted files and data, data in file slack and data in cache or exchange files.

**Documentation of electronic evidence** is the final stage of the criminal analysis of digital evidence and everything that has been found, extracted and analyzed should be "put on paper" or a report of all evidence should be made individually, and then a comprehensive analysis of all evidence and prepares a final document - expertise. The responsibility for the analysis of the evidence and for the preparation of the report lies with the person who has the obligation based on a written act for analysis or expertise of the electronic evidence.
ANALYSIS OF REPORTED, ACCUSED AND CONVICTED PERPETRATORS FOR THE MOST IMPORTANT COMPUTER CRIMINAL OFFENSES IN THE REPUBLIC OF NORTH MACEDONIA FROM 2014-2018

Computer forensics has a major role to play in shedding light and providing evidence in cybercrime, as well as in providing indirect evidence in classical and economic crime. From the most conducted research on computer crime, data were obtained that the most committed crimes classified in the Criminal Code of the Republic of Macedonia are: Damage and unauthorized entry into a computer system under Art. 251 and Making and using a fake payment card under Art. 274 - b. Namely, according to the research for the period 2011 - 2016, the property and financial computer crimes as the most committed criminal act is Damage and unauthorized entry into a computer system under Art. 251 is for which 82.7% have been reported, for Preparation and use of a credit card under Art. 274 - b 15.1% were reported, only a small part were reported for other crimes. In order to continuously investigate this crime and analyze the perpetrators from the moment of reporting to their conviction, it is important to draw conclusions about the quality of the provided electronic evidence (Nikoloska, Computer crime in the Criminal Code of Republic of Macedonia with a special reference on computer crimes against property, 2017).

Table no. 1 Scope, structure and dynamics

<table>
<thead>
<tr>
<th>Year</th>
<th>Art. 251</th>
<th>Art. 274 – b</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>2013</td>
<td>41</td>
<td>33</td>
<td>27</td>
</tr>
<tr>
<td>2014</td>
<td>30</td>
<td>14</td>
<td>14</td>
</tr>
<tr>
<td>2015</td>
<td>50</td>
<td>20</td>
<td>20</td>
</tr>
<tr>
<td>2016</td>
<td>74</td>
<td>18</td>
<td>16</td>
</tr>
<tr>
<td>2017</td>
<td>74</td>
<td>18</td>
<td>17</td>
</tr>
<tr>
<td>Total</td>
<td>269</td>
<td>103</td>
<td>94</td>
</tr>
</tbody>
</table>
Based on the data shown in Table no. 1 for reported, accused and convicted perpetrators of the most committed computer crimes in the Republic of North Macedonia, it is concluded that the primacy of the most committed crime in the investigated period 2013-2017 is Damage and unauthorized access to a computer system under Art. 251 with 269 reported perpetrators from the total of 282 reported and 13 reported for Making and using a fake payment card under Art. 274 - b. Of the reported defendants, 142 perpetrators were convicted for the first offense, and a total of 131 perpetrators were convicted for the second 39, for the first offense 94 and for the second 37. The percentage of convictions against accused perpetrators is 92.3%, and in 48.7% were reported, which indicates the appropriate application of investigative measures and actions in the field of providing, analyzing and storing electronic evidence. According to the data on the structure of the works by years, it can be noticed that in certain years (2016 and 2017) there are no reported for the second crime, and there are defendants and convicts. This is a result of the re-qualification of the crime after the filing of the criminal complaint and as a result of the conducted investigation with the coordination of the public prosecutor and the comprehensive expertise of the electronic evidence the acts are re-qualified, but it can be the result of the procedures from reporting to sentencing.

**CASE STUDIES**

**Case number 1**

The Sector for Computer Crime and Digital Forensics has filed criminal charges to the Primary Public Prosecutor's Office in Skopje due to the existence of grounds for suspicion against the person A.T. from Skopje, for the criminal act Damage and unauthorized entry into a computer system, according to Article 251 paragraph 1 of the Criminal Code of the Republic of Macedonia. The suspect committed the crime in 2014 by unauthorized access to an administrator user in a computer system - computer server unit "WIN-KLS5VM0LT8C" owned by the company "Nextsense LLC" from Skopje, which hosted the website www.exploringmac.com and then acquired administrative privileges and changed the official content of the website, is unauthorizedly installed new files, making computer data unusable and
useless. From the submitted logs for all performed unauthorized announcements to the host-server, the same was analyzed where IP addresses were determined, from which it is accessed with time and date.

In the process of criminal investigation, several measures and actions have been applied in order to provide relevant evidence. A search was conducted in the home and the premises of the reported person, during which the computers were found and temporarily confiscated with a confirmation certificate. Based on the process of elucidating the provision and analysis of electronic evidence, investigators of Sector for Cybercrime and digital forensics found that the elements of Internet access, the accessed IP addresses and virtual memory media compared to the analyzed logs and attached files at the critical time from the damaged host server, that they are the same according to the IP addresses, URL paths and files obtained from the expertise of the temporarily confiscated computer equipment. The applicant unauthorized access to the server, using an administrator account to login to the server computer unit, as the final part of accessing the content attached to the specified computer system thus enabling and performing unauthorized access, change and damage to computer data - digital content hosted on the website on the server, thus making it difficult and normal for the computer system to function - the host server as well as the contents in it.

Case number 2

During 2015, the Sector for Cyber Crime and Digital Forensics, after previously received reports from Macedonian Banks, as well as a report from the one Embassy in Skopje for misuse of payment cards of their citizens in several Macedonian internet outlets. Appropriate measures and actions were taken, i.e. a search of a home, during which several invoices for ordered products from several points of sale, laptop computer, SIM cards, several mobile phones and USB sticks were found and confiscated.

Also, among the found products were a telephone set that used all three disputed mobile numbers used in the conduct of illegal transactions, as well as the number of which was falsely presented as a police inspector. After the case was clarified and the provided evidence, criminal charges were filed against A.K. from Skopje due to the existence of grounds for suspicion that he committed criminal offenses "Making and using a fake payment card" and "False representation". With the intention to gain illegal property gain, in the
period from January to May 2015, he obtained bank data from real payment cards, ie from the holders of foreign payment cards, with which he made several successful and unsuccessful illegal transactions on Macedonian Internet outlets. He bought a Samsung Galaxy S-G900F Galaxy S5, LTE Black Color, HTC Desire 500 white, LG G3 S D7 black, Samsung Galaxy S4 GT-I9506, Smartphone Samsung S5 Mini SM-G800 black. With that, the suspect realized nine successful illegal transactions with four counterfeit payment cards in the total amount of 104,439 denars and 13 unsuccessful illegal transactions with four different counterfeit payment cards in the total amount of 177,480 denars and 1,940 US dollars. In addition to the above, the defendant, with the intention to gain illegal property gain on February 6, called the owner of one of the points of sale and introduced himself as an employee of the Ministry of Interior, is as "Inspector Todorov" who managed the action and was in charge of delivery of the Samsung S5 phone, black, and said it was necessary to return the phone to the fast delivery company and deliver it to the person because they were working on the case.

**CONCLUSION**

Computer forensics will increasingly play an important role in the criminal investigation of cybercrime, but it will and will play a role in providing and analyzing indirect evidence in classic criminal offenses and electronic evidence will be direct and indirect evidence. in economic crimes, especially the acts committed in the business relations between the legal entities with elements of computer forgery. Primacy still has the crime that was first incriminated in the Macedonian Criminal Code, Damage and unauthorized entry into a computer system and is especially notable for criminal activities of unauthorized entry into a computer system.

In the Republic of North Macedonia, cybercrime is a real criminal phenomenon faced by police officers, prosecutors and judges. That is why attention is paid to the acquisition of knowledge in this area, but the key role in the enlightenment process is played by professional police officers from the Sector of Cyber Crime and Digital Forensics of the Ministry of Interior, which is responsible for enlightenment and access at all stages electronic evidence. Based on the analyzed cases from the practice, all of them have been acted upon by this Sector, regardless of which part of the State the
crime has taken place. Regarding the quality of the provided evidence, it can be concluded that in the process of the investigation over 90% of the defendants are convicted persons, which would mean that the electronic evidence is successfully extracted and is acceptable to the judicial authorities.

In non-cybercrime offenses, forensic experts mainly provide evidence of the use of electronic devices to communicate with perpetrators before, during, and after the commission of crimes, and in those criminal situations, expert examinations of electronic phones are made. Communication of the perpetrators, which gives a picture of the criminal organization and structure of the perpetrators.

REFERENCES

15. Thesis, Travnik International University, Faculty of Information Technology, Travnik.