Research Article

Received: 17 November 2022 / Accepted: 12 February 2023 / Published: 5 March 2023

Crime Scene in Cybercrime Criminal Offenses: Evidence Management and Processing

Mensur Morina[1]

Florent Azemi[2]*

Muhammet Ali Eren[3]

Ismail Zejneli[4]

Endri Papajorgji[5]

*[1]Hacettepe University, Institute of Science,
Beytepe, Ankara, Turkey;
Haxhi Zeka University, Peja, Kosovo
[2]UBT-College Higher Education Institution,
Prishtinë, Kosovo
[3]Hacettepe University, Institute of Science,
Beytepe, Ankara, Turkey
[4]South East European University,
Tetovo, North Macedonia
[5]Dean of the Faculty of Law of Tirana Business University,
Tirana, Albania
Corresponding Author

DOI: https://doi.org/10.36941/ajis-2023-0041

Abstract

Since the 1990s, when the first computers were introduced as workplace tools and the technological expansion began, computers, information technologies, and the internet have become an indispensable part of our daily lives. Computers are now an essential tool in all aspects of life, including business, telecommunications, and personal use. Given the increased use of information technologies in our businesses and daily lives, it is not surprising that computer-related crimes are on the rise. The widespread use of computers in our society has resulted in a rapid rise in issues and problems associated with crime, particularly cybercrime. As cybercrime committed via the internet and computer networks becomes more prevalent, courts require technical personnel who are experts in this field. The proper legal framework and division of investigative responsibility are not always clear. Law enforcement faces new challenges as it works to improve its capacity to investigate and prosecute cybercrime. This paper discusses crime scene management for cybercrime criminal offenses. So, we aim to research and present in the most meaningful way what the crime scene is, how site inspection is carried out, how the crime scene is preserved and secured, and what the crime scene documentation is, knowing that traces and material evidence in cybercrime cases occupy a special place in the investigative process.

Keywords: *Criminality, computer, Prosecutor, law enforcement, legislation, crime scene, evidence, traces*

1. Introduction

Parallel to the ever-changing and evolving technology, systems were sought that would eliminate national borders between people and businesses, allowing the financial system to operate quickly and securely regardless of time or place. On the one hand, digital technology as an innovation enabled this connection and provided many benefits to its users, but on the other hand, this technology exposed an environment of enormous security vulnerabilities to conduct criminal activities ranging from copying stolen identities to stealing confidential data.

The term "cybercrime" refers to any criminal activity that can be carried out using computers (in most cases) and any other type of device or technological apparatus that has Internet access. Cybercrime is a type of digital crime in which the perpetrator can be anyone, regardless of gender, whether male or female, or age, ranging from a small child to an elderly person who is still in good health and has knowledge in this field. Cybercrime is defined as a criminal activity carried out using telecommunications in the field of the Internet and is known as the manifestation of old crime via a new innovation. Cybercrime differs from other types of criminality in four ways: it is easily committed, fewer resources are required to cause significant damage, it is a crime in which the perpetrator does not necessarily need to be present physically and as the perpetrator of the criminal offense, he can be anywhere, and finally, as a crime punishable by law, it is often not completely transparent.

Special attention in this research has been attached to defining the actual crime scene of these criminal acts.o. Keeping in mind that crimes can occur anywhere and at any time, we also have different locations of the event that take place in different locations. The main challenge for professionals during field work in this regard is crime scene inspection and management, which includes tactics and techniques.

Preserving and securing and processing the crime scene is almost the main issue that concerns the progress of the entire inspection in general.

Inspection methods are also one of the critical issues that must be addressed during the work of inspecting and investigating the crime scene. To conduct a successful investigation, the team that conducts it must also take special care in documenting the crime scene. Documentation is almost entirely responsible for the work done at that crime scene. We made all of the writings, notes, sketches, photographs, and so on while documenting the crime scene.

Evidence obtained in a crime scene can be used in a variety of ways, including: proving whether or not a crime occurred, which is not always obvious at first glance; identification, evidence can help to identify the victim, the offender, and any other person who may have been involved in the crime. Among other things, this research will seek to provide definitive answers to the following question:

1. What are the issues with crime scene management that law enforcement faces when investigating a crime scene for cybercrime criminal offenses??

2. Desk Review

2.1 *Crime scene of the cybercrime criminal offenses (management)*

Arrival at the crime scene - Court officials search for evidence of how the incident occurred based on a suspicion of a crime. Technical cyber security professionals who are experts in the field of information technologies should take the necessary precautions at the scene of a cybercrime. First and foremost, it is necessary to determine whether cyber confidential information that is likely to be lost or changed has been compromised, and what steps have been taken to prevent its loss. Then, these individuals must determine how the cyber-attack occurred.

Turning off an operating information system can jeopardize a forensic investigation and result in the loss of data and evidence. As a result, cyber security professionals must quickly identify and understand which systems or servers are affected, which data can be lost when a computer or system is shut down, and which hard data is stored on which disks.

2.2 Securing and evaluating the scene of a cybercrime criminal offence

Commences after the scene has been secured, personnel must visually identify to ensure that the integrity of possible computer and traditional evidence has been preserved. Immediately everything must be photographed (Arkin, 1988).

The recommended steps are:

1. Following criminal policy for securing the scene.
2. All information technology devices, including personal portable devices, must be secured.
3. No unauthorized person should have access to the IT equipment at the scene.
4. Any help from unauthorized experts and persons should not be accepted.
5. People unrelated to the event must be excluded so that there is no evidence tampering.
6. Ensuring that the conditions of the electronic devices are not altered.
7. The closed information devices at the scene should be left closed in the same way.
8. Evidence such as hair, feathers, and fingerprints can be obtained as physical evidence from other information devices such as keyboards and mice, and crime scene response teams should take all precautions to ensure that these evidences are not compromised. (Conser, Carsone, & Snyder, 1988).

2.3 Crime scene documentation

It is critical to document the crime scene and ensure investigative security. IT and other digital storage devices should have their general description and condition accurately recorded. Competent people on the scene should keep in mind that not all computer evidence is found near the computer or other devices. In this case, the movement is not performed when the device is turned on because the computer evidence contained within it may be damaged. As a result, computers and other devices should never be moved without first turning them off. (Lee, 1998).

Video and photo shoots are essential for easily remembering all of the details when recording, documenting, and re-examining the crime scene and information evidence during acquisition. Information such as the location of computers in the office, peripheral devices, and so on should also be included in the documentation.[1]

Every computer connection that connects computers and other devices to other computers and the Internet must be identified and recorded. Computer links may indicate that evidence in addition to those collected at the main crime scene exists.

There are circumstances that prevent first responders to be the first at the crime scene and collect all or part of electronic equipment at a scene or other location (Icove, Seger, & VonStorch, 1995). Some laws in the legislation may prohibit copying or moving some data in information systems involved in crime; however, these digital data involved in the crime must be stated in the minutes kept at the crime scene. (Ealy, 2003).

Documentation of the crime scene should include:

- Written record;
- Sketches and drawings;
- Photography;
- Detailed video recording.

These are done to ensure that details can be verified later and assumptions about the process

[1] *Model Code of Cybercrime Investigative Procedure, Article VII, 2004*

can be checked and protected.[2]

All seized digital devices must be numbered and documented if more than one computing device is seized as digital evidence. Seized computers can later be sorted alphabetically. To ensure proper placement, connection and patch cords can be labelled with a specific computer letter and number. Electronic devices can improve the physical crime scene.

Evidence fixation - Similar to photography and dactyloscopy[3] in a physical crime case, security experts should use forensic imaging to record affected systems and related components. In this manner we log important network traffic to obtain cyber security and digital evidence, as well as a snapshot of the network at the time of the cyber-attack event. If system modifications or scene reconstruction are required later in the investigation, an accurate image of the broken network is saved for analysis.

After the process of gathering evidence at the crime scene is completed, all available information sources, including virtual digital devices, physical devices, and temporary memories, should be documented (Holland, 2014). To keep the information collected from changing and the data's integrity intact, it must be timestamped with a cryptographic fingerprint known as a hash code that can be easily verified later. (Geberth, 2015).

Evidence should not be rushed in the event of a cyber security attack. Before making statements to the press, cyber security professionals must obtain the necessary evidence within the legal framework and ensure that they have obtained sufficient supporting evidence.

A criminal offence committed using information technology can be just as difficult and complex as a physical criminal case. Digital evidence that has been secured and verified by cybersecurity experts should be obtained for an effective investigation, and care should be taken to protect the evidence. Relevant cybersecurity professionals should be cautious in providing information to the media and the general public until they can confirm the digital evidence they have obtained.

Fixation and recording of traces and material evidence. Characteristics of computer evidence and principles for their handling - Digital evidence can be obtained from any device or apparatus with digital data. Computer-based devices, fixed and portable data storage devices, CDs, printers, scanners, faxes, photocopiers, cell phones, cameras, modems, firewalls, switching devices (switches), and e-mails[4] are the most prominent and popular.

By definition, digital evidence is vulnerable to tampering. Although they differ from other types of evidence in some ways, they are used as evidence in the criminal justice system. (Morina, Papajorgji, & Eren, 2021)[5].

Computer evidence is a complex entity with unique traits that render its handling and management challenging. These characteristics require exceptional professional competencies and proper qualifications to effectively manage its evidence and storage. To elaborate, computer evidence, like physical evidence such as fingerprints or DNA, is invisible, capable of crossing legal boundaries with ease, susceptible to alteration, degradation, or elimination, and, of utmost importance, its significance diminishes rapidly over time. (Conser, Carsone, & Snyder, 1988) [6].

Evidence derived from information systems is a subset of evidence derived from digital systems. In other words, digital evidence is digital forensic evidence obtained through information systems and digital storage devices in the course of a crime. Digital information systems evidence, unlike physical evidence such as soil, blood, fingerprints, written documents, feathers, saliva, and hair, is susceptible to manipulation. (Eren, Morina, & Papajorgji, 2021)[7].

[2] *Manual for IT Experts, 2014*

[3] *Dactyloscopy - is a scientific discipline that deals with the study of papillary lines (fingerprints, footprints, etc.)*

[4] *Eren , Morina, &,Papajorgji, Journal of Educational and Social Research, P. 67-76, 2021.*

[5] *Morina, Papajorgji, & Eren, 2021, P 45-56.*

[6] *Conser, Carsone, & Snyder, Critical issues in criminal investigation, 1988.*

[7] *Eren , Morina, &,Papajorgji, Journal of Educational and Social Research, P. 67-76, 2021.*

Because of the unique characteristics and nature of computer evidence, the following principles must be strictly followed when dealing with it:

- After obtaining digital evidence, the evidence should be protected while being transported and should not be altered.
- Computer evidence can only be examined by people who are specially qualified for this field.
- Any action taken during acquisition, transportation or storage of digital evidence should be documented in the minutes.
- Criminals (police) must exercise extreme caution when blocking computer devices for evidence purposes. Improper access to data stored on a computer device may violate laws, so they may need to seek legal counsel before proceeding. (Finn, McGillis, & Sinnot, 1988). So, they should immediately contact the prosecution office to consult if their actions are in accordance with the law.

In addition to the legal issues, the criminalist must understand that tampering with data stored on a computer, or computer evidence in general, is extremely delicate. Only specially trained individuals should examine and analyse computer evidence (Conser, Carsone, & Snyder, 1988).

To ensure the reliability of judicial authorities' investigation and prosecution processes, digital evidence collection methods that have become the standard in obtaining digital evidence that is the subject of crime should be used. The more basic principles that are followed in the collection, acquisition, time stamping, packaging, hash value determination, and transportation of the digital evidence that is the subject of the crime, the more accurate the outcome of the trial will be. (Eren, Morina, & Papajorgji, 2021)[8].

The identification process is the second stage in the handling of physical or logical electronic evidence.

The field of data on tangible devices is included in the physical form. The virtual representation of data on the device is referred to as logical form. After potential electronic evidence is secured, identification is performed at the scene or during a home search.

The following steps are involved in identification: Searching for pertinent electronic evidence; Recognizing pertinent visible and hidden electronic evidence; Relevant electronic proof document (signature, license number, physical device damage; Check that the device's status (on/off) has not been changed during login. Photograph or otherwise document the contents of the device's screen. Identify relevant chargers, charging cables, and battery-powered devices to avoid data loss. Based on the sensitivity of the evidence, prioritize the collection of relevant electronic evidence. The identification of relevant electronic evidence at the crime scene or during the home search is critical to the rest of the process, because if it is not identified at this point, it may not exist at a later stage in the process[9].

> *"Crime Scene of Cybercrime Offences – As in any criminal case, obtaining evidence is crucial to reaching the right conclusion. Cybersecurity experts may need to bring computing devices that are not found during a standard search to the scene and collect evidence without losing or altering the originality of digital evidence." (Purdy, 1988)10.*

Computers are unique sources of evidence in several ways:

- Since information technology devices are powered by electricity, any power outage during data processing may result in loss of important information and therefore digital evidence.
- Computers have a structure that is prone to corruption even when turned off. To prevent damage to the information stored on the hard drive, necessary security measures must be

[8] *Eren , Morina, &,Papajorgji, Journal of Educational and Social Research, P. 67-76, 2021.*

[9] *Manual for IT Experts, 2014*

[10] *Purdy, Stephen R., Computer Crime Investigations: Draft Monograph, 1988.*

taken before the system is moved.

- Magnetic storage media where digital data is stored are sensitive and vulnerable to magnetic attacks produced by other magnetic systems.
- Many peripherals, such as printers, scanners, and cameras, can be connected to computers in computing devices. It is critical to consider how evidence will be obtained from these peripherals, as well as how and in what order these digital assets will be removed from the system, when obtaining digital evidence. Otherwise, digital evidence-related information may be lost.
- It is very important to be careful when disconnecting a computer peripheral from the information system.
- Because computers are designed to store information, investigators must take care not to alter or tamper with data while gathering evidence. This means that all removable drives must be write-protected. (Somers, 1984).
- When analysing digital evidence, security experts should work with duplicate evidence rather than original evidence. This method of working not only prevents the original evidence from being changed, but it also allows for the possibility of working with the original evidence in the event of rework. It also allows you to defend yourself against objections about evidence tampering.

Cyber security experts who detect digital evidence are unable to determine which IT inventory is present at the crime scene, narcotics officers for example can use trained dogs to find various drugs during a crime scene search, similarly, cybersecurity professionals must locate digital devices. (Somers, 1984)[11].

As a result, even if crime scene investigators are not trained in computer-related evidence collection, it is critical that cybersecurity professionals establish a standard procedure for computer evidence collection.

When analysing digital crime data from criminal information systems, it is necessary to be familiar with various operating systems and software. Technical experts who are experts in their field should collect physical evidence such as fingerprints, hairs and feathers, while obtaining digital evidence from the crime scene. (Southard, 1986)[12]. These materials, once evaluated, can reveal important information about computerized evidence.

Additional concerns about data protection and analysis arise in cases involving large computers. To protect information, a host computer cannot be easily isolated from the crime scene (Trew, 1986)[13].

Even the most well-trained forensic criminologists cannot be expected to be familiar with every computer system, piece of peripheral equipment, and programming language that may be encountered during a crime scene investigation. As a result, most relevant criminologists quickly realized that they needed to rely on a variety of experts to aid in investigations (Webster, 1985)[14].

When evaluating traces and material evidence, crime scene experts frequently asked whether the suspected object, such as traces or material evidence, is truly related to the case at hand. Traces and material evidence are also sought and discovered in facilities where the presence of the perpetrator of the crime is not justified, unless the criminal offense is committed (Thackeray, 1985).

The evaluation of evidence involves determining its veracity and probative value. Each test is analyzed and reviewed, and there is no default value. The court evaluates the evidence according to the conviction formed after examining it in its entirety (Conser, Carsone, & Snyder, 1988).

[11] *Somers, Leigh Edward, Economic Crimes: Investigative Principles and Techniques, 1984.*

[12] *Southard, Douglas K., To Catch a Thief: Criminal Law is Catching Up with High Tech's Information Thieves,1986.*

[13] *Trew, Andrew, Computer Law and Practice, P.178-181, 1986.*

[14] *Webster, W. H. ,Technology Transfer, Industrial Espionage, and Computer Crime: The FBI's Activities, Computer Security Journal, P.7-12,1985.*

In no case should one be hasty in determining whether or not this is a trace or material evidence; however, that determination should be made only after a safe check and the connection of that trace or material evidence with the circumstances, conditions, and opportunities available at the crime scene (Begeja, 2011).

Marking of traces and material evidence is done in such a way that the expert or the examiner will later be able to know where he/she got the trace or evidence and present it when asked to (Reimer, 1986).

Marking evidence ensures that characteristics and latent traces found in that evidence are not disturbed (Begeja, 2011). These markings or signs are placed in those places of the object, item, tool, etc., if possible, or in the box or wrapper, whether paper, plastic bag, etc., and are marked with signs that the expert will record in his/her minutes. Any pencil with a metal tip is preferred because the colour may rub off or be lost later.

These evidences must also have their own labels, which must include the date, time, location, name of the expert who took it, and a description of their distinguishing marks or designations. And each piece of evidence must have its own distinct mark from the same other piece of evidence in order to be distinguished and not combined as a single piece of evidence.

The special procedure for gathering electronic evidence. To inspect and gather evidence at a cybercrime scene, the person who arrives first must have the necessary competence, such as crime scene surveillance, approval, or a court order.

If a digital authorization issue arises, cybersecurity experts who arrive at the crime scene should be aware of the devices that can be used to obtain digital evidence, follow the instructions of the relevant agency, contact an official, or contact a prosecutor.

The digital evidence that is the subject of the crime should be analysed while maintaining the electronic device and the data it contains secure. Because digital evidence is subject to change and is susceptible to deterioration by magnetic effect, it should be stored in special packages. Electromagnetic fields, such as those produced by static electricity, magnets, radio transmitters, and other devices, can damage or alter acquired digital evidence. (Kovacich & Boni, 2006)[15].

To prevent electronic evidence from being altered during collection, the first person at the crime scene must initially:

I. Document the activity on the computer, its components, or hardware;
II. Should check if the computing device is turned on. Check the computer's status, including whether the computer or digital devices are turned on, flashing lights, running fans, and other sounds. If the status of the computer cannot be determined by these indicators, look at the monitor to see if it is on, off, or in sleep mode.

Because digital and information device evidence is extremely sensitive to heat, cold, humidity, magnetic effects, and impacts, great care should be taken during the packaging, transportation, and storage of digital evidence**.**

To prevent misappropriation, damage, and destruction of evidence, the first person on the scene must document, photograph, package, transport, and store electronic evidence (Kovacich & Boni, 2006)[16].

All transactions involving the acquisition, collection, packaging, transportation, and storage of digital evidence should be documented and recorded in the minutes.

When electronic evidence is packed for transport, the first person on the crime scene must:

- Individually mark, tag, document, photograph, and video record all of the collected digital evidence before it is packaged. It is critical to use this method so that the same digital system can be easily

[15] *Kovacich, Gerald; Boni, William C., High-Technology Crime Investigator's Handbook,P. 22-24, 2006.*

[16] *Kovacich, Gerald; Boni, William C., High-Technology Crime Investigator's Handbook,P. 22-24, 2006.*

assembled later.

- Be aware that electronic evidence may contain concealment, trace, or biological evidence, and take the necessary precautions to preserve it. Prior to conducting covert, trace, or biological evidence processes, electronic evidence (including minutes) must be recorded. (Inman & Rudin, 2001)[17] - Antistatic packaging should be used for all electronic evidence. Electronic evidence should be packaged using only paper bags and envelopes, paper boxes, and antistatic containers. Plastic materials should not be used for electronic evidence collection because they can generate or conduct static electricity and allow moisture and condensation to form, which can damage or destroy the evidence. (Why is Evidence Placed in a Paper Bag, 2022)[18].
- Ensure that all electronic evidence is chosen and packaged in a way that prevents bending, scratching, or other deformation.
- Clearly and neatly label all containers used for packaging and storing electronic evidence.
- Leave devices, such as cell phones or smart phones, in their original state (turned off or on).
- Collect all conductors and suppliers for all seized electronic devices (Kovacich & Boni, 2006).

Minutes, storage, and packaging of traces and material evidence must be created and formed by meticulously recording all relevant information about the traces and material evidence discovered. This is because the expert will require the minutes to determine the order of each piece of evidence one by one. In this regard, the minutes allow for the determination of numbers for each evidence separately. (Fisher, 2007).

The following information must be included in the minutes: the name of the case, the type of crime and case number, the number or mark, the date and time of discovery, the name of the person who discovered it, the location where it was placed, the chain of custody or transfers. (Bergman, 1988).

In case of dislocation of evidence, under any circumstance, from the place of its storage, or its transfer, among the various relevant persons, the name of all those persons who dealt with it must be recorded in the minutes (Ademaj, 2010).

Process of transportation - includes transporting relevant electronic evidence to a location where it will be stored and analysed later. Carrying can be done either physically or electronically. If the relevant electronic evidence is carried in electronic form, special safeguards, such as encryption and digital signature of the data, must be taken to ensure its integrity and chain of ownership.

Physical transportation – Electronic devices or apparatus at a crime scene or in a home as a search location should be carefully packaged with antistatic packaging material. Each item must be labelled and marked separately using the protocol's special number.

Items must be handled in such a way that the electronic device is not affected by strong magnetic fields, dust, or water during the transport process. The tools must be shielded from moisture and vibration. The transport vehicle must be capable of safely transporting the items. Computers and other devices should be powered on as much as possible throughout the transportation process.[19]

Transport in electronic form - Transporting relevant electronic evidence data over a network requires a secure SSH-TUNNEL connection or something similar. Wireless data transmission is not permitted. Some footage is small enough to be copied to CDs or DVDs.

In most cases, an external disk is required (portable USB). To prevent unauthorized access, the external disc must be encrypted. The encryption key should never be transported in the same

[17] *Inman, Keith; Rudin, Norah, Principles and Practice of Criminalistics: The Profession of Forensic Science,2001.*

[18] *Why is Evidence Placed in a Paper Bag, https://realonomics.net/why-is-evidence-placed-in-a-paper-bag/.*

[19] *Manual for It Experts, 2014*

container as the encrypted external disc. It is preferable to encrypt an entire partition on an external disc rather than individual folders or files.

Analysing and interpreting electronic process evidence - is based on a writing of the competent authority which contains:

- When deemed necessary or beneficial, identification of electronic evidence is requested from a copy of the original relevant electronic evidence (static analysis) or from a direct version of the relevant electronic evidence.;
- Examine the content of the relevant electronic evidence requested, keeping in mind the questions defined in the task's writing and the relevance of the contextual information provided by the authority in charge.;
- Interpretation of relevant electronic evidence is required to allow for fact-finding, consequence analysis, and the validity of results;
- Recording of gestures performed by forensic experts on computers during the analysis process and the results of the actions;
- Recording the chain of ownership;
- Reporting of analysis and interpretation results

The procedure's analysis phase is based on the tasks of the State Prosecutor or another competent authority. The identification and evaluation of relevant electronic evidence should be guided by the specific tasks defined in the state prosecutor's or other mandated authority's tasks document.

Any relevant electronic evidence source's content must not be altered, and the evidence must not be damaged during analysis. The analysis process must result in the identification and evaluation of evidence pertinent to the essential elements of the criminalized accused, which comprise the evident facts.

2.4 Mandatory institutions in the framework of the investigation of criminal offenses of computer criminality

State Prosecutor - Article 49 of the Criminal Procedure Code of Kosovo and Article 7 of the Law on the State Prosecutor[20] defines that the task of the State Prosecutor is to take appropriate procedural actions in accordance with the law for detection of criminal offenses and discovery of perpetrators of criminal offenses, and to investigate and prosecute criminal offenses. In addition, the State Prosecutor must make decisions on the initiation, continuation or termination of criminal procedures against persons suspected or accused of committing criminal offenses.

Article 66 of the CPC[21] states that all public institutions and their employees are obliged to provide necessary assistance to the judicial authorities and authorities in criminal proceedings.

Kosovo Agency on Forensic - Article 2 of Law No. 04/L-064 on Kosovo Agency on Forensic[22] describes that the Kosovo Agency on Forensic (KAF) is responsible to provide objective, unbiased scientific forensic analyses based on orders from courts, prosecutors or at the request of law enforcement agencies. According to Article 10 of the Law, KAF laboratories must be accredited based on international standards.

KAF's powers and responsibilities include assisting with crime scene examination and acting as an expert witness in court. Experts may be authorized by the KAF Council for Quality, Qualification, and Requalification.[23]

[20] *LAW No. 03/L-225 ON STATE PROSECUTOR OF THE REPUBLIC OF KOSOVO, 2010*

[21] *CRIMINAL No. 04/L-123 PROCEDURE CODE OF THE REPUBLIC OF KOSOVO, 2012*

[22] *LAW No. 04/L-064 ON KOSOVO AGENCY ON FORENSIC, 14.11.2011*

[23] *Manual for It Experts, 2014*

Kosovo Police - Article 69 of the Criminal Procedure Code[24] defines that the police, together with the State Prosecutor, must investigate possible criminal offenses to define whether to start criminal procedures.

> *According to the same code, Article 70 defines that the police must investigate if there is a reasonable doubt whether the criminal offense prosecuted ex-officio has been committed. The police must take all right steps to discover and preserve traces and other evidence of the criminal offense, as well as objects that can serve as evidence and collect all information that can be used in criminal procedures. In carrying out this task, the police must have the authority and powers to confiscate objects that may serve as evidence in criminal procedures and to discover, collect and preserve traces and evidence from the crime scene of the suspected criminal offense, as well as to order the forensic testing of the evidence by the forensic laboratory in accordance with Article 71 of the CPC25.*

According to Article 70 of the CPC, the police must record, photograph or have an official note of the actions they undertake and of the facts and circumstances that have been established by their investigation. (Annexes 3-8). Furthermore, Article 71 of the CPC[26] defines that the police must carefully collect evidence from the crime scene, preserve it in a proper manner that allows evidence to be tested by a competent laboratory. Article 6 of the Law on Police[27] declares that the police must implement the legal orders and instructions issued by the public prosecutor or the competent judge.
Other institutions - Article 75 of Law 03/L-222 on Tax Administration and Procedures[28] defines that officers of the Investigations and Tasks Unit must have the same powers and responsibilities with that of police officers authorized to conduct investigations and similar functions under the supervision of the public prosecutor and in compliance with the Criminal Procedure Code of Kosovo.

> *Assistance of forensic agencies personnel - Most jurisdictions have broadened the scope of their lists of experts. One of the best strategies is finding people within a relevant agency or agencies who have computer expertise. This may mean obtaining technical support by persons outside the unit that directly lead investigation, and that in this particular case are forensic agencies.*[29]

Personnel with expertise and skills in information technologies should be recruited in the same way that many modern countries hire experts who can perform chemical and biological analysis while performing fingerprint, saliva, hair, and DNA tests.

2.5 *Protection of data during investigations of cybercrime criminal offenses*

Special attention should be paid to the protection of personal data and secrecy of the operation when implementing actions under the standard work procedure. For data protection, the Law No. 03-L-172 on the Protection of Personal Data[30] and Law No. 03/L-178 on Classification of Information and Security Verification[31] must be applied.

Article 7 of the Law on Classification of Information and Security Verification[32] describes the

[24] *CRIMINAL No. 04/L-123 PROCEDURE CODE OF THE REPUBLIC OF KOSOVO, 2012*
[25] *CRIMINAL No. 04/L-123 PROCEDURE CODE OF THE REPUBLIC OF KOSOVO, 2012*
[26] *CRIMINAL No. 04/L-123 PROCEDURE CODE OF THE REPUBLIC OF KOSOVO, 2012*
[27] *LAW No. 04/L-076 ON KOSOVO POLICE, 2012*
[28] *LAW No. 03/L-222 ON TAX ADMINISTRATION AND PROCEDURES OF KOSOVO, 2010*
[29] *US. Department of Justice. Bureau of Justice Statistics, 2006*
[30] *LAW No. 03/L-172 ON THE PROTECTION OF PERSONAL DATA OF KOSOVO, 2010.*
[31] *LAW No. 03/L-178 ON CLASSIFICATION OF INFORMATION AND SECURITY VERIFICATION OF KOSOVO, 2010.*
[32] *LAW No. 03/L-178 ON CLASSIFICATION OF INFORMATION AND SECURITY VERIFICATION OF KOSOVO, 2010.*

officials in public institutions mandated for classified information. Material may be classified as "Top Secret", "Secret", "Confidential" or "Restricted".

The State Prosecutor and other authorities that give the tasks to the computer expert must ensure that the information and data processed during the computer analysis are preserved. Therefore, the task-giving authority must ensure that the expert responsible for the analysis is aware of data protection, classification and operational secrecy requirements. The computer expert must carry out his/her task and process data in compliance with orders and instructions given.[33]

2.6 Procedure Code of the Turkish Republic

The issue of who will contact the electronic evidence first is also critical. In this regard, there is a practice that varies by country. In some countries, such as the United States, special units (first responders) are trained in how to handle such evidence, whereas in others, law enforcement personnel (police officers) who are not adequately trained on the subject perform this task. In this context, it is clear that in Turkey these transactions are carried out by law enforcement personnel who have received adequate training.

This is regulated by relevant Articles of the Criminal Procedure Law (CPL) No. 5271, the Regulation on Judicial and Prevention Searches, and the Regulation on Criminal Items, which govern the procedural provisions that must be followed in the process of obtaining and safeguarding electronic evidence in Turkish law.

The evaluation of intangible, invisible computer data made up of electrical circuits as evidence in criminal proceedings is a new phenomenon. However, it is now widely accepted that the state obtains and stores data in computer programs as evidence within the framework of "protection measures. However, Criminal Procedure Code (CPC) m. 116 et al. and m, although 123 contains general provisions on search and seizure measures, obtaining such information necessitates a special search and seizure decision. Because searching for evidence within a computer or in a system where computers are linked together in a network and seizing it is a separate process.

In this regard, search, copying, and seizure measures in computers, computer programs, and logs, which express a special type of search and seizure measure of a general nature, are regulated in CPC m. in 134. Although the search measure is typically conducted on buildings and their annexes, vehicles, and people, the subject of the search in the said measure is computers, computer programs, and computer logs.

The measure's purpose is to gather electronic evidence. Searching, copying, and seizing computers, computer programs, and logs is critical, particularly when obtaining electronic evidence related to cybercrime. However, the aforementioned measure is also used in the investigation of traditional crimes. Because it is not possible to apply the provisions of the Criminal Procedure Code's classical search measure to the computer environment, our law also governs search, copying, and seizure measures in computers, computer programs, and logs.

In Turkish law, the procedures for obtaining electronic evidence have been attempted to be regulated by a single-article provision in the Criminal Procedure Code (CPC). The provision in Article 134 of the CPC regarding the protection measure of search, copying, and seizure in computers, computer programs, and computer logs is consistent with both Article 8 of the European Convention on Human Rights and the Constitution in terms of the protection of privacy and personal data, which are among the most important fundamental rights and freedoms. It does not violate Article 20 of the Convention on the Rights of the Child. However, it is also true that violations resulting from incorrect interpretation of the law's provisions or the wrong attitude of law enforcement during the measure's implementation are on the agenda.

[33] *Manual for IT Experts, 2014*

3. Methodology

The methods used in this paper are qualitative: The descriptive method has helped process collection of electronic evidence, analysis, packaging, transportation, steps in the inspection of the crime scene, the competences and responsibilities of the commanding institutions in this field of investigation of cybercrime criminal offenses.

Using this method of analysis, several cases encountered by investigative groups while investigating cybercrimes, particularly during the inspection of the crime scene of these delicate crimes, have been thoroughly investigated.

And, using the explanatory method, we have elaborated all of the important issues in the most understandable and detailed manner, always based on best practices, reports, and world literature in the field of cybercrime criminality investigations and evaluation and inspection of the scene, all the way up to the taking and preservation of evidence in cybercrime criminal offenses. In addition, issues concerning practical work, experience, and their compatibility with current laws were discussed.

4. Research Results

As a result, the number of cybercrime criminal offenses has increased in recent years. Among the major issues that have been researched and highlighted in this paper are:

The experiences of law enforcement and judicial authorities combating cybercrime are now yielding positive results in illuminating major events reported in the press. As a result, when a cybercrime is reported, digital evidence may be lost or destroyed due to a lack of knowledge about the crime by law enforcement personnel who arrive on the scene to deal with IT equipment breaches. Digital evidence, on the other hand, can be obtained safely in the presence of technical experts who can assist in the collection of digital evidence.

Competent institutions that are unaware of the unique need for proactive cybercrime proceedings and criminal prosecution will miss opportunities to develop contacts with other actors, which may be critical to the prevention of future criminal offenses, improving crime reporting, and when a cybercrime is reported, expert cybersecurity computer experts should come to the scene to prove these allegations and obtain digital evidence.

All issues concerning the investigation of the crime scene of criminal offenses, particularly computer criminality. So, the significance of the crime scene investigation in the criminalistic and legal senses, as well as the significance of this investigative action in the overall process of investigating the case.

In computer crime cases, the use of cutting-edge methods for searching, locating, sketching, photographing, and documenting the crime scene. Because the presence of traces and material evidence at a crime scene cannot be denied, the examination of traces and material evidence has also been analysed and studied in this paper. In order for this investigative process to progress properly as an object of study in this research, we also obtained documentation of the crime scene, presenting the benefits that such an action has in fulfilling all of the investigative group's objectives in the process of inspection and investigation of the crime scene. Another issue raised in this paper is the process of managing investigations at the crime scene in cases of cybercrime, which includes elaborating on all of the challenges the investigation faces as well as the processing of evidence at the scene of such offenses. The management of cases of cybercrime criminal offenses is a challenging process that necessitates a well-prepared staff, both in terms of general and specific knowledge, because to investigate such a case, a well-trained staff with the skill and dexterity to perform these important tasks is required.

5. Discussions

Despite numerous attempts by various authors to define cybercrime, there is no universally accepted

definition as of yet. This type of criminality, unlike others, does not yet represent a phenomenological summary category, but rather a broader range, making precise definition impossible. The difficulty in defining cybercrime stems from the variety of forms it takes and the speed with which it spreads.[34]
In a report prepared for the Bureau of Statistics of the United States Department of Justice, SRI, computer criminality is defined as "any crime for which the perpetrator requires technical knowledge of computers in order to intervene in them" (Parker, 1981). According to the prosecutor's manual, cybercrime is defined as "any illegal act for which prosecution is successful as well as the necessary knowledge of computer technology." (Parker, 1989).

In a narrow sense, cybercrime will be defined as any behaviour carried out through electronic actions. Its goal is to secure digital data processed by information systems. (Swanson, Chamelin, Territo, & Taylor, 2000).

On the other hand, cybercrime will be defined in a broader sense as any illegal behaviour committed in the form, method, or through a computer or computer system, including crimes such as illegal processing, provision, or distribution of information by a computer or network, to abuse and attract attention in forms such as those for supporting terrorist groups, neo-Nazis, pornography, and paedophilia. (Wall D. S., 2007). This will also include types of fraud crimes, such as illegal gambling, pyramid schemes, credit card fraud, and other types of illegal activities that breach network security. According to some authors, cybercrime is only defined as criminal offenses that cannot be committed without special knowledge or offenses that cannot be committed without the assistance of a computer.

In this regard, there is a definition according to which: "cybercrime contains all those offenses committed with the help of special knowledge on the professional use of computer technology". In this regard, author Taber states that "the computer tort must contain high professional operations on computers, under conditions when the violation cannot be put in any other way." (Korajlic, 2008).

The author, Urlich Sieber's definition of computer criminality is as follows: "cybercrime includes illegal violations of property, in which electronically processed data is knowingly changed (computer manipulation), destroyed (computer sabotage), or used in an unauthorized way (computer espionage)." (Korajlic, 2008).

Also, Don Parker, a world-renowned expert in the field of cybercrime, was focused on the scientific treatment of this problem when it came to understanding cybercrime. According to the author, computer criminality is defined as "any action related to the use of computer technology in which the victim suffers or may suffer loss, while the perpetrator acts to benefit himself/herself." (Parker, 1981).

By studying opinions of different authors from available literature related to the meaning and definition of cybercrime, author V. Vula concluded that "cybercrime is a special form of criminality, in which a computer is presented as a tool for committing illegal actions or as an object of attack, directed by persons who possess special knowledge and inclinations for computer systems, in order to bring benefits themselves or others" (Vula, 2009). According to criminalist Latifi, cybercrimes are:

> *"The main objective of crimes committed through information systems is to harm the victims' reputations, earn money from the victims, and inflict material and moral harm on the victims." (Latifi, 2009)*[35].

There are many ways and types of cybercrime and that is why this type of crime is very hard to fight. Systems where digital devices (including smart phones, information systems, printers, computers, tablets, etc.) are connected to the internet are increasing day by day.

[34] *https://en.oxforddictionaries.com/definition/cybercrime, 2020*

[35] *Latifi, Vesel,Kriminalistika: Zbulimi dhe të provuarit e krimit (Eng. Criminology: Detecting and Proving Crime),2009.*

> *So, in theory, criminals can wreak havoc and block all our access to the world via the Internet, and the because of this great peril that is presented all over the world, governments are beginning to take cybercrime and the fight against it very seriously (Zittrain, 2008). There are several ways and types of cybercrime and they are: Cyberbullying, Spam Emails, Phishing, Identity Theft, prohibited offensive content, child sexual abuse materials, fraud and online sales, etc.*

Given that cybercrime is complex, failure to have it analysed by experts may result in victimization of those who are harmed by the crime. Even if offenders who violate the law do not have a criminal record, they can use computer access as a powerful new tool to achieve their criminal goals. (Bequai, 1983).

In terms of evidence, they are the notifications on the facts and circumstances related to the criminal offense that are obtained from the sources specified in the criminal procedural law, in accordance with the rules established by it, and which serve to prove whether or not the criminal offense was committed, its consequences, the defendant's guilt or innocence, and the degree of his/her responsibility. (Koçollari, 2010)[36].

If facts and circumstances related to the criminal offense are presented, or sources provided by the procedural law prove that a certain criminal offense has been committed or not, and all of these are provided in a legal manner, they constitute evidence (Police Academy, 2002).

By evidence, we mean the factual data contained in the law according to the sources foreseen on the evidence or their carriers (persons, animals, plants, objects, traces) on the basis of which the competent body ascertains the presence or absence of the criminal offense, the form of guilt of the particular person, and other important circumstances for issuing a meritorious decision in the procedure regulated by the positive laws.[37]

In the broadest sense, evidence in the broadest sense, can also be defined as an ascertained fact that serves to define other facts. As facts, evidence must be objectively related to the object of argumentation. The information that a fact presents, which allows the conclusion about a criminal offence, and its author can be considered as evidence. The evidence must be relevant and objective. (Hysi, 2010).

Evidence is always in a secondary relationship to the criminal offense and to the perpetrator as the author and primary element. Here we are talking about the difference between contested facts (themaprobandi) and evidence (Koçollari, 2010).

> *We believe that cybercrimes are all crimes committed through networks and devices that have their own special programs. The human factor, as well as any illegal communication or processing via computers and other technological devices associated with cybernetics, are presented as evidence in this regard. As a result, prepared staff and relevant institutions to combat this phenomenon are critical, as is supplementing or amending the norms in the framework of the laws in force, given the nature of cybercrime.*

6. Conclusions

Pursuing and proving criminal offenses involving electronic communications networks and services, as well as forensic analysis of electronic evidence, require specialized knowledge. In this regard, criminal justice authorities should rely on the establishment and strengthening of elements such as: Special cybercrime units within the structure of police forces or high technical units; increasing the level of specialized knowledge within the judicial system; collaboration among agencies, etc.

It is more than necessary to establish a team of initiators and prosecutors with sole responsibility over cybercrimes, with other investigative and prosecution responsibilities limited.

[36] *Koçollari, Irakli, Tribunë Juridike (Eng. Legal Tribune),Tirana,2010.*

[37] *https://www.i-sight.com/resources/15-types-of-evidence-and-how-to-use-them-in-investigation/,2022*

Cybersecurity professionals trained in the collection and analysis of digital evidence can help with the technical aspects of computer crime investigation and prosecution. Training of expert technical personnel is one of the responsibilities of judicial authorities and judicial law enforcement units.

More frequent training for specialists in this field. Much newer and more diverse types of crime emerge as information and computer technologies evolve and change. As a result, adjudicating units and law enforcement officers should receive ongoing training in cyber security and obtaining digital evidence.

Many other crimes fall under the jurisdiction of computer crimes. Authorities in charge of investigations and prosecutions should keep a close eye on technological advancements. However, very few judges and prosecutors are well-versed in this area. As a result, investigating and prosecuting them may necessitate a collaborative approach or the establishment of a separate specialized court.

The purpose of crime scene investigation is to help uncover the nature of the cyber-attack (reconstruct the crime scene) and identify the perpetrators. This is demonstrated by meticulously documenting the conditions at a crime scene and identifying all relevant physical and electronic evidence.

Investigating a digital crime scene is difficult and time-consuming. Examination and research based on a specific procedure makes it easier to obtain digital evidence. Based on the limited information available, the cyber security expert should not jump to conclusions about who the perpetrator is, but rather generate several different theories about the crime, keeping those that are not eliminated with the information available at the crime scene. Reasonable assumptions about the alleged incident in the past, as well as digital evidence obtained and witness statements, will guide the incident's clarification.

If the location of the alleged cyber incident is documented and marked, the temperature, humidity, and magnetic field of the crime scene, if not carried out under appropriate conditions, may damage or corrupt or destroy the digital evidence.

The main challenge for any team conducting a crime scene investigation is dealing with events that they have never seen before and that necessitate a high level of professionalism and work. All of this because, while the offense may appear to be the same at first glance, the manner in which it is carried out differs greatly. The proper application of scientific and technological tools reveals facts that, while the type of offense is the same, the manner in which it is committed differs.

References

Ademaj, X. (2010). Ekspertiza Kriminalistike (Eng. Criminal Expertise). Prishtina.

Akademia Policore. (2002). Këqyrja e vendit të ngjarjes, doracak për studentë, Kursi bazik i forenzikës (Eng. Crime scene inspection. Manual for students: Basic forensic course). Vushtrri, Kosovo.

Arkin, S. S. (1988). Prevention and Prosecution of Computer and High Technology Crime. Matthew Bender and Co.

Begeja, S. (2011). Kriminalistika (Eng. Criminology) (Vol. 2). Tirana.

Bequai, A. (1983). How to prevent computer crime: A guide for managers. John Wiley & Sons.

Bequai, A. (1987). Technocrimes - Why the cops can't cope? Law Enforcement Technology, 28.

Bergman, R. A. (1988). Impact of Technological Advancement on Forensic Science Practice. Canadian Society of Forensic Science Journal, 21(4), 169-175.

Conser, J. A., Carsone, L. P., & Snyder, R. (1988). Investigating Computer-Related Crimes Involving Small Computer Systems. In M. Palmiotto, Critical issues in criminal investigation. Anderson Publishing Co.

Ealy, K. (2003). A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention. SANS Institute. Retrieved from www.gi.

Eren, M. A., Morina, M., & Papajorgji, E. (2021). Digital Evidence and Prohibitions of Evidence Evaluation. Journal of Educational and Social Research, 11(5), 67-76. doi:https://doi.org/10.36941/jesr-2021-0106

Finn, P., McGillis, D., & Sinnot, R. (1988). State Law Enforcement: A Survey of Major Services. Cambridge: Abt Associates.

Fisher, W. W. (2007). Promises to keep: Technology, Law and the Future of Entertainment. Stanford: Stanford University Press.

Geberth, V. J. (2015). Practical Homicide Investigation: Tactics, Procedures, and Forensic Techniques (Practical Aspects of Criminal and Forensic Investigations) 5th Edition. Boca Ration: Taylor & Francis Group.

Holland, J. F. (2014, December 18). FCW. Retrieved from Managing a cyber crime scene: https://fcw.com/security/2014/12/managing-a-cyber-crime-scene/254880/

Hysi, V. (2010). Kriminologjia (Eng. Criminology). Tirana.

Icove, D., Seger, K., & VonStorch, W. (1995). Computer crime: A crimefighter's handbook. Sebastopol: O'Reilly & Associates, .

Inman, K., & Rudin, N. (2001). Principles and Practice of Criminalistics: The Profession of Forensic Science. CRC Press.

Koçollari, I. (2010). Tribunë Juridike (Eng. Legal Tribune). Tirana.

Korajlic, N. (2008). Kriminalisticka Metodika. Sarajevo.

Kovacich, G., & Boni, W. C. (2006). High-Technology Crime Investigator's Handbook. Butterworth-Heinemann.

Latifi, V. (2009). Kriminalistika: Zbulimi dhe të provuarit e krimit (Eng. Criminology: Detecting and Proving Crime). Prishtina.

Lee, H. C. (1998). Materijalni Tragovi. Zagreb: Birotisak d.o.o.

McEwen, J. T., & Nugent, H. (1988). Results of the National Assessment Survey: Police and Sheriffs. Washington D.C.: National Institute of Justice.

Morina, M., Papajorgji, E., & Eren, M. A. (2021). Collecting Evidence in Forensic Events and Comparison of the Digital Evidence Practices of Kosovo and Turkey. Academic Journal of Interdisciplinary Studies, 10(5), 45-56. doi:https://doi.org/10.36941/ajis-2021-0122

Parker, D. B. (1981). How much computer abuse is there? Menlo Park: SRI International.

Parker, D. B. (1989). Computer crime: criminal justice resource manual. University of Michigan Library.

Purdy, S. R. (1988). Computer Crime Investigations. Federal Computer Investigations Committee.

Purdy, S. R. (1988). Computer Crime Investigations: Draft Monograph. Federal Computer Investigations Committee.

Reimer, D. M. (1986). Judicial and Legislative Responses to Computer Crimes. Insurance Counsel Journal, 406-430.

(2006). Report. U.S. Department of the Treasury.

Sanger, D. E. (1984, April 4). S.E.C's Computer Revolution. The New York Times.

Soma, J. T., Smith, P. J., & Sprague, R. D. (1985). LEGAL ANALYSIS OF ELECTRONIC BULLETING BOARD ACTIVITIES. Western New England Law Review, 7, 571-626.

Somers, L. E. (1984). Economic Crimes: Investigative Principles and Techniques. Clark Boardman Callaghan.

Southard, D. K. (1986). To Catch a Thief: Criminal Law is Catching Up with High Tech's Information Thieves.

Swanson, C., Chamelin, N., Territo, L., & Taylor, R. W. (2000). Criminal Invesigation (7th ed.). Boston, Mass.; McGraw-Hill, c2000.

Procedure Code of Turkish Republic https://www.mevzuat.gov.tr/mevzuatmetin/1.5.5271.pdf

Turkish Republic Code of Criminal Procedure https://cigm.adalet.gov.tr/Resimler/SayfaDokuman/23202011159Adli%20Kolluk%20Yönetmeliği.pdf

Thackeray, G. (1985). Problems of Computer Evidence. The Practical Prosecutor, 2, 10-11.

The New York Times. (1987, September 16). German computer hobbyist rifle NASA's file: Serge Schmemann. 7(1), 102. The New York Times. doi:10.1016/0167-4048(88)90521-4

Trew, A. (1986). Does Technology Outstrip Enforcement. Computer Law and Practice, 178-181.

Vula, V. G. (2009). Kriminaliteti Kompjuterik (Eng. Cybercrime). Prishtina.

Wall, D. (. (2001). Crime and the Internet. Routledge.

Wall, D. S. (2007). Cybercrime: The transformation of crime in the information age.

Webster, W. H. (1985). Technology Transfer, Industrial Espionage, and Computer Crime: The FBI's Activities. Computer Security Journal, 3(2), 7-12.

Why is Evidence Placed in a Paper Bag. (2022, March 6). Retrieved from www.realonomics.net: https://realonomics.net/why-is-evidence-placed-in-a-paper-bag/

Zittrain, J. L. (2008). The Future of the Internet. Yale Unviersity Press & Penguing UK.