https://doi.org/10.31410/EMAN.2025.615

The Prosecutor in Digital Forensics Procedure – "Just Look, Don't Touch"

Dragi Rashkovski[1]
Veronika Rashkovska[2]

Received: April 28, 2025
Accepted: December 30, 2025
Published: xxx

Keywords:
Digital forensics;
Prosecutor;
Good practices

Abstract: *The digital forensics (DF) procedure requires full compliance with a procedure that is determined in advance with more or less equal world standards translated into internal rules of the organization that carries out the DF. The procedures and good practices exclude the direct contribution of the public prosecutor in this process, with the aim of objectivity, impartiality and equality of the parties in the criminal procedure. Due to the poor application of such rules, in this paper we indicate the most common misconceptions that some public prosecutors have when it comes to the digital forensic procedure, forgetting that it is a procedure of the procedure, not theirs, and to what extent the public prosecutor is allowed to be an active stakeholder in the DF process.*

1. INTRODUCTION

The digital forensic analysis procedure is aimed at determining the content found in the digital device, usually seized in criminal proceedings, but often also in administrative and civil proceedings submitted by one of the parties. If digital forensics is much "looser" in terms of the rules on how digital evidence should be treated in civil and administrative proceedings, in criminal proceedings, these rules are without exception imperative for the evidence to be allowed in the courtroom.

In civil proceedings, parties are usually legal entities and natural persons, and accordingly their interest is to prove the existence or non-existence of a legal relationship in order to prove whose right is stronger and which of the parties should draw the fruits of that legal relationship, or if the benefit is divided, then it should be determined which of the parties in what proportion will have a share in it. This is a generalization of civil relations, reducing that relation mostly to material or non-material benefits, but in general, it does not affect the most valuable thing, and that is the freedom of the person. The situation is similar in the administrative procedure, where one of the parties is a state authority; however, this is also a dispute in which the amount of benefit or the amount of damage compensation from the established legal relationship should also be derived.

In both cases, if part of the evidentiary procedure is digital evidence, it is "voluntarily" submitted to the court by the parties, considering that in this way they have a greater chance of a greater benefit in the court case.

The situation is not like that when it comes to the criminal procedure because the public prosecutor who initiates the legal case usually appears as a party in the procedure. To be honest, there are also private criminal proceedings, but they are for the so-called lighter crimes, where there

[1] Ss. Cyril and Methodius University, Iustinianus Primus Faculty of Law, bul. Goce Delchev 9b, 1000 Skopje, Republic of North Macedonia
[2] MIT University - Skopje, Faculty of Legal Sciences, International Relations and Diplomacy, bul. Treta Makedonska brigade 66b, 1000 Skopje, Republic of North Macedonia

is no injury to the life and body of individuals or groups and there is no greater social damage. That is the reason why our focus is on criminal cases where the public prosecutor is a party in the proceedings.

In such a case, the digital evidence against the suspect or the defendant is collected against his will, i.e. it is most often done with a court order, where digital devices should also be listed as items that should be seized from the defendant/suspect during a search.

The criminal procedure following a private lawsuit in which there is digital evidence, as well as the preparation of the defense in which the public prosecutor appears as a party, while the defendant is a natural or legal person, requires the fulfillment of legal standards, but is not a condition for exclusion of digital evidence. It is primarily because the ordinary citizen, who can very easily become accused, not only does not have daily contact with digital forensics procedures, but it may also be the first time that he faces such an experience. What's more, digital forensics for evidence collected upon the request of the prosecutor's office, usually with search and seizure, is entrusted to digital forensics scientists, so that there can be no exception to the rules of good forensic practice for these experts.

This should not mean, and it does not mean, that citizens can automatically propose and have their digital evidence approved. Their digital evidence during the procedure for proposing and approving the evidence, and further during the main hearing, can be challenged by the opposite party, both in terms of content, as well as in terms of form and method of their provision, and all this to prove or disprove one of the main properties for digital evidence to be approved by the court, which is to prove its authenticity.

One of the provisions of the rules of the NATO Cooperative Cyber Defense Center of Excellence entitled "Digital Intelligence and Evidence Collection In Special Operations" refers thereto and article 10.4. indicates that:

“Even if the evidence is not collected according to the criminal proceedings law or may have been illegally obtained, it might still not be excluded from criminal proceedings. There is a distinction between a citizen and police or other official investigators. The police, as a state actor, is bound by the criminal proceedings law, which aims to protect citizens against the power of the state. If the police have collected the evidence in violation of the law, this evidence will be excluded. If, on the other hand, the evidence is collected by a citizen who is not restricted by the protection provided by this law, the evidence might be accepted (NATO Cooperative Cyber Defence Centre of Excellence, 2016).

Not only because of this norming by one of the most relevant organizations in the world, such as NATO, but also due to the nature of things, which is the complexity of digital forensics, it is normal to exempt citizens from strict procedures. The forensically correct procedure requires a very detailed knowledge thereof, but also great thoroughness, and additionally, the formal implementation of a criterion for a digital forensic scientist, which is followed by expensive specialized equipment and software; therefore, this attitude is justifiable. However, that does not mean that a "hidden forensic scientist" as a party in one of the civil or administrative procedures, even private criminal ones, shall not abuse this facilitation. Therefore, each item of digital evidence, regardless of the procedure, may be challenged.

However, when it comes to law enforcement and certified digital forensic experts, there's almost no space for error. That error may consist of non-observance of procedure or violation of the

objectivity of the procedure, through interference in the digital forensics procedure by the person who requested the seizure of digital devices.

And now we come to the main thesis of this paper – What is the position of the public prosecutor concerning digital evidence after it is collected and taken to a digital forensic laboratory?

2. FIVE MISCONCEPTIONS ABOUT THE ROLE OF THE PUBLIC PROSECUTOR IN THE DIGITAL FORENSICS PROCESS

By way of negation of where and what the prosecutor must not do in relation to digital forensic procedure, supported affirmatively by referring to the rules of the most renowned international organizations (OLAF, NATO, Council of Europe, US Department of Justice and others), we have grouped into five units the most common procedural errors and misinterpretations of their own powers by prosecutors themselves regarding their role in the digital forensics procedure.

2.1. First Misconception (The Evidence Is Mine)

In criminal proceedings, digital evidence is seized from the suspect after the court issues an order for its seizure, upon the request of the public prosecutor. This is where the first misconception arises that "this evidences is evidence belonging to the prosecution". The impression is wrong because this is evidence that was in the full possession of the defendant until the moment of their seizure. By seizing them with a court order, the prosecutor does not get any privileged status over them as they call them "evidence of the prosecution" in the indictments, but it is "evidence of the procedure". There is no doubt that the prosecution can build its case based on this type of evidence, but not prevent the suspect from using and having access to this evidence in building his defense.

The prosecutor "may but does not have to" be present when the digital evidence is seized. He must in no case be in contact with them, much less perform any examinations or analyses. It is natural that it should be so, and why? Because the parties in the procedure (the prosecutor and the suspect) must be equal. As soon as the digital devices are taken away from the first, they must not be given to the latter, because the principle of equality would be violated. If the suspect is no longer allowed to have access to the digital devices after seizure, then neither is the prosecutor. That is why there are digital forensics experts whose presence is mandatory when digital devices are seized by court order. And it is very common. If, for example, it is necessary to take a blood sample in order to determine the presence of psychotropic substances in the blood of a traffic accident suspect, it is done by medical personnel, not by the prosecutor or police officers. After a blood sample is taken, it is not given to the prosecutor for inspection or to do his own analysis, but it is taken to a laboratory for examination. The prosecutor may, but does not have to be present when the blood sample is taken; he can only observe and do nothing more.

The rules of the INTERPOL Global Guidelines for Digital Forensics Laboratories also refer thereto, stating that digital evidence may be sent after seized to the DFL (Digital Forensics Laboratory). The rule reads:

"When electronic evidence (exhibits) is received, it is important for the exhibit to be sealed before custody can be transferred to the DFL. To eliminate any reasonable doubt about the integrity of the evidence, both the Requester and the Examiner must be able to demonstrate that no-one else has gained access to the evidence during the transfer process from one party to the other. This practice is new and costly for some agencies, the DFL will nevertheless provide constant awareness and provide a firm timeline to start practising this procedure with the agencies." (INTERPOL, n.d.).

2.2. Second Misconception (I Lead the Digital Forensics Procedure)

The second misconception of the digital forensics procedure by the prosecutor is connected to the previous one. The digital forensic scientist is the undisputed leader in the digital forensic procedure, receiving instructions from the prosecutor on what to look for, that is, to analyze, but not how and what with. Just as the prosecutor must not interfere with the laboratory technician when analyzing the blood taken during a traffic accident. He can and should say which parameters should be examined (presence of alcohol or drugs in the blood), but not which scientific methods the laboratory technician should apply, even less mixing reagents or touching the blood with his own hands. In parallel, in digital forensics, the prosecutor should instruct the digital forensic scientist what digital evidence to look for (for example, extract all conversations on all applications between the suspect and the victim, or provide him with all documents between two dates) but not to sit at the computer on which digital forensic analysis is performed and make his own selection and analysis.

This point of view, apart from being supported by general logic, is also supported by the legal acts of numerous organizations that precisely determine the position of the public prosecutor, which is behind the door of the digital laboratory. The public prosecutor can request, as well as the suspect's lawyer, to access the digital forensic laboratory (DFL) if necessary, with special approval from the head or director of the DFL, but it must be all properly recorded with each step taken, with the mandatory presence of the digital forensic scientist, while reviewing the forensic copy and not the original media.

This in itself means that digital evidence from the moment of seizure until the end of the court case, in its original form, can be exclusively in the possession of an authorized digital forensic expert while the investigation is ongoing, and further be kept under judicial supervision, but in no way to be in the possession of the prosecution. The reason behind this, as we mentioned, relates to the point when digital devices are already seized, they are taken from the suspect, but not to be in the possession of the prosecutor, because then, according to common law, the prosecutor receives a higher right than the suspect, bringing himself into privileged position in relation to the suspect, because he can have materials that he would use against the suspect, and the suspect is deprived of that right. He would have to try to remember what was on the device, running the risk of misremembering or completely inventing something, and the prosecutor would have something at his disposal that he could even abuse.

Therefore, the impression that the prosecutor leads the DFA proceedings is wrong. The procedure for DFA is strictly determined by international and internal rules and in none of them it is specified that the prosecutor is the one who dictates segments of the procedure. He "can order", but not interfere in the analysis process.

All jurists must understand that the fact that the DFA procedure resembles a bureaucratic procedure and that it is commonly closer to them than common analyzes does not give them the right to appropriate it.

The prosecution and the defense would violate their equality in criminal proceedings if procedural access to digital devices, digital forensic analysis and digital forensic laboratory were to be privileged. Any privilege casts doubt on influence and manipulation, in conditions that DFA (Digital Forensic Analysis) rules emphasize without exception.

DFL is a place that must be under the full supervision of the one who further guarantees the integrity of the digital evidence, which is the digital forensic scientist, and above him the director.

Access to DFL must be controlled, even for the prosecutor, as stated in the "Guidelines for identification, collection, acquisition and preservation of digital evidence" of OLAF (Office de Lutte Anti-Fraude) in article 2.3, where it reads that:

"2.3. Access to this laboratory is restricted to system administrators and operational staff that have a need to know via electronic access control and logged by badge readers. Entrance to the laboratory is monitored by a video surveillance system" (OLAF – Office de Lutte Anti-Fraude, 2012).

2.3. Third Misconception (I Select the Content of the Evidence)

Digital evidence contains a large amount of data of a different nature, very often private, and may even be intimate. Therefore, by seizing a digital device that the suspect has been using constantly (for example, a mobile phone), data on almost every segment of his life - business, private and intimate - is also seized. So, it is quite debatable to what extent the prosecutor may demand that data from the seized device be provided to him. A crucial task of the prosecutor is to build a good theory of his case, that is, to know exactly what he is accusing the suspect of. Unfortunately, when a device has already been seized (for the purposes of this paper, we will operate with a mobile phone, as the most content-rich device that a suspect can use), there is no one to limit the prosecutor to what extent he can indulge into the privacy of the contents of the mobile phone. That unlimited power should be curbed by the digital forensic scientist. The digital forensic scientist is the one who has to ask the prosecutor exactly what he wants to select in the mobile phone, whereas the scientist can ask if the request for digital forensic analysis directed to the digital forensic laboratory is too general. The prosecutor's request must contain accurate data on what type of digital records are requested (messages, images, videos, etc.), and the prosecutor must briefly or in detail describe the suspicions that the suspect is accused of, with the aim of the digital forensic scientist to get a more detailed idea of what to look for as content. This must in no case be covered with the legal phrase "all records in the form of pictures, word documents, videos and the like", because in that case, the right of the prosecutor to receive part of the evidence is abused. However, unfortunately, legal practice shows that prosecutors often use this way of collecting the entire content from the mobile phone, through which they also get unprincipled means to create an advantage over the suspect.

If we go back to the example of taking a blood sample from a suspect in a traffic accident, this means that the prosecutor can ask the medical laboratory to measure the blood alcohol per mile, as well as the presence of psychotropic substances, but not to measure the cholesterol level or blood sugar, because these parameters are not in reference to the indicators of possible causing a traffic accident. However, if the prosecutor obtains them, it can create an advantage for the prosecutor by familiarizing with private details about the suspect's health that can be misused. This especially applies in circumstances when it is found out through blood analysis that a suspect who has caused a traffic accident is seriously ill, so such data further becomes part of the court case and may violate the objectivity of the trial.

Therefore, it is extremely important to know that the prosecutor is not the one who selects what content from the evidence will be extracted as evidence. He is obliged to make a "good request" which he will support in the background with his theory of the case, and the digital forensic scientist is the one who should and must respond to that request by handing over the entire material that corresponds to the request. This means that, if something exists as material, found by the forensic scientist, and was not handed over to the prosecutor, the responsibility lies with the digital forensic scientist, who, at the very least, if it is proven that he made such an omission intentionally, will be responsible for hiding evidence.

Why is it still important to know that the prosecutor may not select evidence? Because the separation of evidence in an inappropriate way is not only formally legally defective and renders the evidence unusable, but it is also technically ruined digital evidence. Requesting the digital forensic scientist obliges him to protect the integrity of the digital evidence, which is a basic prerequisite for its acceptance in court. Because the digital forensic scientist would do this process in a forensically correct way, by hashing them and by saving the metadata of the digital records, which are technical procedures that technically guarantee the integrity of the data. By referring to such data verification, the process becomes verifiable and repeatable, which is also a prerequisite for the acceptance of digital evidence in court.

In the same way and with the same principles, this issue is regulated in the "Guidelines for identification, collection, acquisition and preservation of digital evidence" of OLAF, where in article 8.4. it is clearly defined that the investigators (those who operationally implement the tasks of the prosecutor) who are part of the prosecutor's team should clearly prepare the task that they will give to the digital forensic scientist.

"8.4 When the forensic work file is available, the investigator shall launch written requests through the CMS Intelligence Request Module to index the forensic work file and as appropriate obtain the assistance of the DES or operational analyst to identify data relevant for the investigation. The latter request should describe the aim of the search and what type of evidence and/or proof the investigator is searching for. In response to the investigator's written request and in conjunction with the investigator the DES shall extract data matching the search criteria from the digital forensic work file for read-only access by the investigator." (OLAF – Office de Lutte Anti-Fraude, 2012).

In addition, this results in an even greater restriction for the prosecution in the selection of materials, which means that such searches are based on a forensic work file (meaning it must not be a search in the original media as it is sometimes done) and that search is only in the form of reading the data and not copying them for the needs of the prosecution. The prosecutor will later receive an official report with everything he requested and indexed from the entire set of information, not by simple copying, but in a forensically correct way - by saving the metadata of the extracted data and hashing the set of extracted data. In other words - the prosecutor "orders", and receives the order "packaged".

2.4. Fourth Misconception (I Present Digital Evidence)

Digital forensics as a process is composed of several stages, each of them a necessary prerequisite for the overall procedure to be valid. The stage that is the most familiar and closest to the public prosecutor, because it is by its nature present in every evidentiary procedure, is the presentation of digital evidence. Although digital evidence in its most visible form is letters, numbers, images and video materials, what "can't be seen with the naked eye" is the metadata thereof, which as "data about the data" should show us and prove the authenticity, immutability and the source of the digital evidence, which as properties of the digital evidence without their verification are ordinary letters, numbers, images and videos. What makes digital evidence alive is the metadata, the presentation of which must be done by a digital forensics expert who should be, at the same time, an authorized forensic expert. If the prosecutor takes upon himself the right to present digital evidence, he will face another technical difficulty or challenge that he will have to explain, but also prove that it is so, and that is the unchanged hash value of the data package. both on the created forensic copy and on the extracted data that are subject of the investigation. The two challenges together, and especially the first one – presentation of the existence of metadata in

case of arbitrary undertaking of the obligation to present will be faced by the prosecutor on at least two occasions. The first is when presenting it to the suspect during an investigation when the suspect will have to explain 3 questions - What did he do, how did he do it and the third most important for this paper - what evidence does the prosecution have for that? Here, the prosecutor assuming the right to present digital evidence will make an irreparable mistake that will destroy his entire case in the part he supports with this digital evidence. Namely, if the prosecutor in the investigative procedure operates with digital evidence that he received from the digital forensic laboratory, he has already violated the integrity of the evidence, and it is further forensically defective and unusable in court. This does not mean that the prosecutor must not have with him a copy of the data extraction that is the subject of interest in the case, but that he should obtain an additional copy for his own needs, and submit the first copy of the extraction, unchanged, with the evidence material. Only then will the process be forensically sound. Compared to the above example of taking blood from a person suspected of causing a traffic accident, it would be for the public prosecutor to take the right to present evidence from biochemical analyses, while explaining to the court biochemical analyzes he has no qualifications for and no educational background. He will be in a situation where he has to present evidence that contains professional terminology and complex processes that he can only present syntactically, but not in correlation with the reasons that led to a criminal legal event.

However, the crucial reason why the prosecutor is not allowed to present digital evidence is that when, according to the criminal procedure laws, the defense wants to refute such evidence through direct or cross-examination, then the person the cross- and direct questions would be directed to would be the prosecutor himself. This leads us to a legal impasse, because the answers to expert questions will have to be given by the prosecutor himself as the only person present in the court-room who has a connection with the evidence. This duplication of functions (prosecutor-forensic expert) means suspending the right to objective and expert knowledge of the material truth, as well as making it impossible to check the (un)observed procedure that preceded the presentation.

In order not to be misunderstood, the public prosecutor is of course allowed and should use the digital evidence in the indictment, thus making an appropriate presentation thereof, but this must in no way interfere with the presentation of the digital evidence during the presentation of evidence. in the criminal proceedings in court. The presentation of the digital evidence by the prosecutor in the indictment, and later in his closing remarks, is an indirect way of his understanding of the content of the digital evidence, and not an immediate experiential transmission of it. He can paraphrase the digital forensic expert in an incorrect way both in the indictment and in the closing words, which will be subject to the judge's free assessment, after hearing the counter arguments of the defense, and in this case, we refer to a contradiction of the procedure, which is a content point of view to the evidence. The content aspect of digital evidence is not and should not be of interest to the digital forensic scientist at all. Suspending him from entering the courtroom, in such a way that the prosecutor steals his role, is a gross violation of the adversarial principle of the criminal procedure, because the adversarial principle requires that you challenge the work of the one who did the action, not the one who presented that to you (don't kill the messenger).

The digital forensic scientist who performed the analysis of the digital devices is not a digital forensic scientist of the public prosecutor's office. He is a digital forensic scientist of the state, of the system, of the citizens. That is why the public prosecutor must not appropriate him, suspend him and treat him as his assistant. He is just as authorized a person as the public prosecutor is and he is the one who reports, and who should answer questions about his work, not anyone else, and even if he wants to and allows it, let alone someone take it from him.

All these claims of ours find support in Interpol's Global Guidelines for Digital Forensics Laboratories, describing not only the role of the digital forensics (examiner) in the presentation of digital evidence, but also general guidance on how to do it.

"The Presentation phase requires putting together findings in a presentable and understandable way for stakeholders. When the analysis phase is completed, the Examiner needs to put the findings and results in a forensic report. The Examiner should illustrate and translate complicated technical contexts into facts that judges, prosecutors and other parties involved can easily understand. They may also be expected to interpret those facts, and to express an opinion on their meaning. In some cases when a large number of exhibits are analysed, it will be difficult for the examiner to present the outcome to the investigation team. It is recommended to adopt an analytic software to facilitate matching digital evidence with other data from the investigations. These kinds of tools can also be used to index and search all the exhibits, providing the investigation team with a global overview of the case.

The same reference is also given in "A basic guide for the management and procedures of a digital forensics laboratory" of the Directorate General of Human Rights and Rule of Law - Council of Europe by clearly stating that the expertise and competence of the forensic analyst or as who is called an examiner there, should lead to professional terms and technical contexts being presented in a way that will be comprehensible to lawyers, so as to understand the factual situation as well as possible.

"After evidence has been found in the analysis stage, the examiner needs to create a report for the trial. The examiner's job is to illustrate and to translate complicated technical contexts into facts that judges, prosecutors and other parties involved can easily understand. They may also be expected to interpret those facts and to express an opinion on their meaning (Council of Europe, Directorate General of Human Rights and Rule of Law, n.d.).

2.5. Fifth Misconception (I Keep the Evidence During the Investigation)

Given the writing above, we already hinted at the fifth wrong impression, meaning that the public prosecutor keeps the digital evidence and devices with him during the investigation. As a reminder and basic support for such a misconception, we will only repeat that the seized digital devices are not evidence of the prosecution, but evidence of the procedure, and both parties can use them in their own defense. That is why it is almost unbelievable when a public prosecutor, during the investigation, will "wave" the seized digital devices at a suspect in his office. All that the public prosecutor is allowed to obtain from the seized digital devices is – EXTRACTION OF INFORMATION FROM THE FORENSIC COPY OF THE DIGITAL DEVICE THAT IS OF INTEREST TO THE INVESTIGATION. And that is it. Under no circumstances should he be allowed to be the custodian of digital devices. And again, the comparison with the blood sample taken from the suspect in a traffic accident – the prosecutor is not given the blood sample, nor is he given a part of the blood sample to keep in his office. He is not given a document that is an analysis of the tests conducted. A blood sample is not given to him only because it is not allowed according to the procedural rules, but also because the public prosecutor does not have reliable conditions to keep the blood tube.

The same applies to digital devices. They must not be given to him at any time, because he is still only a party in the proceedings. If they are given to him, then according to what principle of equality of parties and tools in the criminal procedure are they not given to the suspect? Digital

devices seized during a search have a very clear trajectory of movement – place of seizure – digital forensics lab – courthouse security room. Each of these stages corresponds depending on the stage in which the criminal procedure is located.

This appropriated right of the public prosecutor in digital devices is particularly highlighted, which is probably due to the interesting content that digital devices hide in themselves, they often contain a large part of private life that can hide interesting moments, which can unfortunately be used later even as blackmail by the prosecutor to cover unjustified and unsubstantiated procedural actions, which are often on the line of just committing a crime on his part.

Indisputably, throughout the world there is the rule of "inviolability of the original", it must be kept only by the one who knows how and where.

Otherwise, as firearms are not so attractive as evidence in criminal proceedings, of different sizes and types, by analogy, and applying the legal principle argumentum ad absurdum, an instant comparison would be what will happen to this evidence if the prosecution does the same as with digital devices, so take them with him.

The American practice, which fully corresponds with the European one, is on the same stand, in a legal document entitled "Digital evidence policies and procedures manual" of the U.S. Department of Justice - National institute of justice where the exceptional importance of keeping digital evidence is emphasized, because, as we mentioned above, the original must remain intact.

"Devices must also be processed properly, whether the data they contain are incriminating or exculpatory. It is equally important that these devices are stored in a manner that will preserve the data in their original state for examination by the defense and for the introduction of the original item into court when necessary." (U.S. Department of Justice, National Institute of Justice, n.d.).

As the most recognized certification of processes in the world, this issue is also dealt with by the ISO standardization, which refers precisely to the process of digital forensics. The digital forensic procedure is divided into several phases, the fourth of which is the preservation phase, that is, keeping the evidence. ISO/IEC 27037:2012 certificate emphasizes the importance of preserving evidence in a forensically sound manner.

"Preservation is the process of securely maintaining custody of property without altering or changing the content of data that resides on devices and removable media. The preservation process is critical for potential digital evidence to be useful in the investigation, and should be initiated and maintained throughout the digital evidence handling processes. Potential digital evidence must be preserved to maintain its integrity for its admissibility in a court of law" (International Organization for Standardization, 2012).

3. CONCLUSION

Based on all the above, we can conclude that the prosecutor, when it comes to the digital forensics procedure and collection of digital evidence, which begins after the evidence is seized, is the "user" of the services of the digital forensic laboratory, and not its process manager. The prosecutor has the right and obligation to request that everything found on the digital devices be extracted, but only in the context of the established criminal case. He must not obtain a forensic copy of the entire device, because the devices may contain data of a personal nature that, in a positive or negative

context, may violate the objectivity of the procedure. Additionally, the prosecutor has the full right to use the digital evidence to support his theory of the case, but their probative strength in terms of procedural correctness should be defended by the digital forensic scientist. The prosecutor can present how he understood all and have it incorporated in the indictment, but the forensic process is defended by the forensic scientist himself.

Digital evidence is evidence of the procedure and should be left to the procedure and kept, that is, it should be in the original with a trusted third party (DFL or the court) and not with one of the parties, i.e. the prosecution.

If the parties are equal, then their tools should be equal too.

INSPIRED BY A TRUE STORY.

References

Council of Europe, Directorate General of Human Rights and Rule of Law. (n.d.). *A basic guide for the management and procedures of a digital forensics laboratory.*

International Organization for Standardization. (2012). *ISO/IEC 27037:2012: Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence.*

INTERPOL. (n.d.). *Global guidelines for digital forensics laboratories.*

NATO Cooperative Cyber Defence Centre of Excellence. (2016). *Digital intelligence and evidence collection in special operations.*

OLAF – Office de Lutte Anti-Fraude. (2012). *Guidelines for identification, collection, acquisition and preservation of digital evidence.*

U.S. Department of Justice, National Institute of Justice. (n.d.). *Digital evidence policies and procedures manual.*