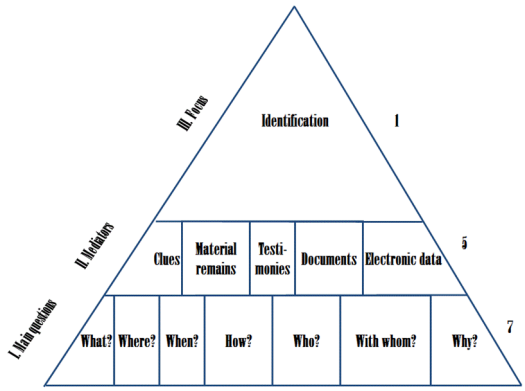
**CSABA FENYVESI – JÓZSEF ORBÁN**

# The electronic data as the constituent of the 751 pyramid model of criminalistics

## The Pyramid Model of Criminalistics

In the first part of our paper, we will outline a model of the central questions, methodology, system of mediators, and the ultimate goal of criminalistics, by now a sophisticated, meticulous and diversified empirical science of facts. It is hoped that the model is presented in a simple form which is clear to everybody and can be used in theory, in everyday practice as well as in education.

For purposes of diagrammatic representation, the shape of a pyramid, composed of 7-5-1 building blocks from bottom up, seems most appropriate. The pyramid model can be called the 7-5-1, or simply 751- model. Consider the diagram below.



### *Level I: PRINCIPAL QUESTIONS IN CRIMINALISTICS.*

At the bottom of the pyramid, as in the physical world, we find the most solid basic building blocks—the seven basic questions, already consolidated in the technical literature: WHAT? WHERE? WHEN? HOW? WHO? WITH WHOM? and WHY? (I/1-2-3-4-5-6-7). (Sieben Golden Fragen, 7 Main Questions, 7 W Questions)

Some theoreticians in forensic science have expanded these questions up to twelve, adding, for example, To whose gravamen? With what means? For what reason or purpose? Causing what damage? etc. It may be noted that question no. 6, With whom?, need not be asked, as if more than one person was involved, then, according to the rules of English grammar, the answer to question no. 5, Who?, will contain the names of accomplices too. Nevertheless, the "7 WH-questions" formula, adopted here, has become a conventionally and internationally accepted concept in forensic science (as well as the practice of criminalistics).[1]

It is no coincidence that the first among the seven short questions is "WHAT?", as the answer to the essential question "What happened?" not only gives the impetus but also decides whether the authorities need to start a criminal investigation at all or instead proceed to take public administration, labour, etc. measures, to mention only a few of countless alternative possibilities and areas. If the answer to that question is "a criminal act", that will immediately decide about the personnel to be deployed, the expertise required, methods and devices to be employed, and some further basic questions will immediately become sharper. The word "immediately" receives special emphasis here, as the question of time becomes important

[1]MALEVSKY, H.-JOUDKAITÉ-GRANSKIENÉ, G. (eds.): Criminalistics and Forensic Examination: sciences, studies, practice. Mykolas Romeris University, Vilnius, 2013.; METENKO, J.: Kriminalisticka taktika. Akadémia Policajného Zboru v Bratislave, Bratislava, 2012; HAUTZINGER, Z.: Gondolatok a kriminalisztika elméleti rendszeréről. [Thoughts about Theoretical System of Criminalistics.] Jura 2019/1. 86.

instantly not only because of the need for a speedy investigation and the rapid uncovering of the facts but also because the "WHEN?" question comes to the foreground. The triplet of questions, WHERE-WHEN-HOW, begin to compete for priority as soon as the "WHAT?" question is answered. They arise almost simultaneously and urgently, demanding accurate answers in the shortest possible time, because without them the rest of the questions (WHO, WITH WHOM?) cannot be explored.

Now it seems appropriate to skip the boxes on the second level of the pyramid and move directly to the single block at the top, on level III.

### *Level III—THE FOCUS OF CRIMINALISTICS*

This represents the point of focus, the goal of the entire struggle to learn about the past, the target of all the basic questions every time and in every detail, namely IDENTIFICATION.

This goal, printed in huge letters in red above the chalk board on a wall in the "forensic laboratory" in Pécs (Hungary), used to remind everybody of what constantly guides (and needs to guide) criminalists in each move in their search for noise-free answers to the seven questions.

We identify the type of act—whether it was a criminal act, or perhaps an accident, a natural disaster or self-violence.

If (and only if) we are dealing with a criminal act, we may move on from the primary question to the rest of the questions, that is, we need to identify the scene or scenes, we need to identify the time and manner of the commission of the act, its motive (and sometimes also the aggrieved party), and finally (all of) the perpetrator(s).

How do we get from the basic questions at the bottom to the top of the pyramid? In other words, what are the methods and instruments of identification? The answers can be worked out from the three blocks on Level II, the intermediate level of the pyramid.

### *Level II—CRIMINALISTICAL INSTRUMENTS (WAYS and PATHS)*

The terms "ways" and "paths" suggest that it is through or along them that we work our way from clarifying and ascertaining data relevant to the main questions at the bottom through identification, that is, giving straight answers to them at the top. We can call them the media or "mediators", which deliver all the necessary information provided that you know how to "talk to them" or understand them. The set of all possible paths, instruments and media can be divided into three main groups—CLUES, MATERIAL REMAINS, TESTIMONIES, DOCUMENTS, ELECTRONIC DATA (II/1-2-3-4-5).

An overview of our demonstration system, the kinds of evidence specified in criminal procedure law (demonstration procedures), makes it apparent that the means of demonstration worked out in theory or employed in practice (instruments of demonstration) fall into one of the three categories. Witness testimonies, accused testimonies, hearings at the scene, facial recognition tests, testimonies at confrontations[2] and polygraph tests[3] all fall within the category of testimonies, which may also include experts' opinions as well as their (parallel) hearings. The list is not exhaustive. We must add that expert opinions overlap with traces and material remains, as the former chiefly testify about results from studying and identifying the latter, which they may find identical or otherwise.

Physical evidence emerging from surveys is, in reality, traces and material remains or their causers or carriers. (Consider, for example, the means of perpetration, the thing(s) affected by the criminal act or things that come to exist as a consequence of a criminal act.)

---

[2] ANTAL, D. (2011): Confrontation as a Special Criminalistic Method. In: Jozef Metenko, Sona Masnicová and Magdaléna Krajníková (eds.), *Pokroky v Kriminalistike 2011 EU SEC II/B*. Akadémia Policajného zboru v Bratislave, Slovakia. 68-83

[3] BUDAHÁZI, Á.: Poligráf a büntetőeljárásban [The polygraph in the criminal procedure.] Belügyi Szemle 2011/12. 104-117

Documentary evidence, too, is a carrier of traces or material remains, and frequently appears in the form of expert opinions. In addition, it also "testifies", as it presents the statements it contains.[4]

Evidence obtained in a secret manner can also be classified into the three categories,[5] as

a) it contains statements, assertions, communications, such as, for example, intercepted conversations, correspondence, computer data, which, although appear in documentary format in the circle of evidence in accordance with procedural rules, may be considered testimonies or traces from a forensic perspective;
b) it delivers physical evidence, traces or material remains (any drug is material remains in a forensic sense), for example, in the course of secret searches or pseudo-purchases.

The order of boxes on level II is not arbitrary. Traces (clues) and material remains are intentionally mentioned first and second, respectively, preceding testimonies. This is for the theoretical and practical reason that traces and material remains are "incorruptible witnesses", that is, according to modern theories of evidence and criminalistics, their validity surpasses that of personal testimonies (compare the level of validity of dactyloscopy or individual identification by DNA samples), which are often distorted, especially in the circle of witnesses and suspects. The idea accords well with tendencies in criminalistics in the 21st century, one of which happens to assert precisely the primacy of forensic techniques over forensic tactics. The desire is to raise forensic techniques to the level of scientific

[4] TÓTH, Cs.-MÉSZÁROS, B.-FENYVESI, Cs. :, Examinarea documentelor suspecte [Questioned Document Examination] Revista De Criminologie, De Criminalistica Si De Penologie, Societatea Romana De Criminologie Si Se Criminalistica. Cluj Napoca, (Roumania) 3/2010. 152-160

[5] MÉSZÁROS, B (2019): Fedett nyomozó alkalmazása a bűnüldözésben. [Covered Agent int he Criminal Investigation.] Dialóg Campus Kiadó, Budapest.

knowledge, characterized by outstanding validity, as opposed to the, albeit non-malevolent, inaccuracy and unpredictability of testimonies.

## The electronic data

Based on the latest Hungarian Criminal Procedure Law Act (year 2017. number XC.) paragraph 165, wich declares: evidence are: a) the witness statement, b.) the statement of the suspect/accused, c.) expert opinion, d.) opinion of the parole officer, e.) factual/material evidence including documents and records, and f.) electronic/digital data.")

### *Interpreting electronic data*

The real question is whether the digital data formerly detailed in our essays and theses[6] is different or similar to the electronic data mentioned in the legal texts. We might as well ask the following chain of questions: In the case that one is part of the other, what is their relation to each other and what is the content and core feature of the electronic data?

This bundle of questions is even more relevant since in the last few years the attribute "digital" has arisen in connection with electronic information in essays and in professional circles. According to the Criminal Procedure Law (Act XC. of 2017 which is also the IV. Criminal Procedure Law) subsection (1) of section 205,

*"Electronic data is every aspect of facts, information or concepts that is suitable to be processed by an information system, including the program which ensures the execution of a function by the information system."* The lawmaker's choice of words seems appropriate when using the term electronic and not digital data.

[6] Further on this topic: FENYVESI, Cs. (2016): The importance of line-up and digital data in the case of pornographic crime. Belügyi Szemle 2016/9. 119-129; The importance of digital data in criminalistics. JURA 2016/2. 50-59; ORBÁN, J (2018): Bayes-webs in criminal cases, PhD thesis PTE ÁJK Pécs.; DOMOKOS, A. – ORBÁN, J.: The past and future of identification. Miskolci Jogi Szemle 2017/2. 5-18

In our opinion the information system in relation with the criminal procedure law has a narrowing meaning.

According to our choice of words the electronic data is a component - containing information - produced, processed, forwarded or recovered in an electronic system. Including the case when one of the elements of the aforementioned chain is realised due to light, sound, or radiofrequency. The electronic data incorporates the information both in analog and digital form. A purely analog signal can be the sound of an old vinyl record or a purely digital information can be the green or red signal of the traffic light. By digital data we mean binary numbers in other words the binary system consisting of ones and zeros which has seemed sufficient so far. The traffic light signals at least three but more likely four state. Stating this seemed important because the electronic miniaturization will soon reach physical boundaries and then one of the ways of increasing information density is the sign of many phases which might mean the return to the analog electronic information-carrier.

Based on subsection (1) of Paragraph 204 of the Criminal Procedure Law Act it can be summarized that the electronic evidence is factual evidence based on electronic data (also information), which possesses relevant data in relation to the crime. And so for instance it carries the clues of the committing of the crime or in relation to that of the perpetrator which exist due to the committal of the crime or was used as instrument or the crime was committed to gain it.

Part of the electronic data is volatile[7] thanks to its physical characteristic and after removing the pressure from the system in question the data irreversibly perishes[8]. Other electronic data can be destroyed by mechanic

[7] The evidence detected in the electromagnetic fields can be seen as volatile unless an act prescribes its enforceable recording.

[8] Such is the group of data stored in the computer's operative memory. Furthermore the data can be saved in the case of a computer in stand-by mode and thus the information before hibernation can be saved.

force (too), but it must be added that the data can only be electronically altered.[9]

In our opinion the electronic evidence includes both the electronic analog and the electronic digital evidence. The investigative and verifying work in connection with the electronic evidence might need the cooperation of multiple authorities[10]. The examination in connection with the transmitted radiofrequency signals usually managed by authorities[11] monitoring newscast activity. The transmitted information is a digital bundle of signals[12] embedded in analog radiofrequency waves. The message recovered from the bundles of information is the actual content.

Communication in the case of IT devices is based on the concept by Shannon[13]. Based on the content it means:

1) The source produces the message (or a chain of messages) and wants to forward it to the receiver. The message can be a sound, text, picture, etc.
2) On the side of the source the message must be converted into signals in a way that it could be transmitted by the communication channel (coding).
3) In most cases the message/statement becomes damaged due to it being added to the information. (Eg.: the scratching noise on the

[9]When destroying confidential data found on electronic data storage devices, the one responsible for handling data orders the physical demolition of the data storage device. Especially since some data deleting methods only change the way of visibility of the information, but depending on the method the original condition can be restored. In conclusion the physically intact but seemingly deleted data storage device can always hide the necessary electronic evidence.

[10] In our essay we do not deal with the national security and military adaptation.

[11] In Hungary the National Media and Newscasting authority.

[12] Since digital broadcasting gained popularity analogue broadcasting is less common nowadays. Permanent exception from this rule is the analogue sound based communication between the pilot of an aircraft and a moderator in an air traffic control center.

[13] SHANNON, C. E-WEAVER, W. (1998): The Mathematical Theory of Communication. University of Illinois Press. Urbana and Chicago. 34

radio, hardly understandable phone call, flickering screen). The message reaches the receiver via a communication channel.
4) On the side of the receiver the signals must be restored (decoding).
5) And thus the restored information arrives at its destination. The statement/announcement is the information transmitted by the channel, or in other words the content.

In a communication channel there are three ways to commit a crime:

a) transmitting radio frequency signals without permission
b) disturb one's permitted and legal transmission
c) illegal content during a permitted transmission. In this latter category belong the hate speech[14] transmitted via a radio or TV broadcast, furthermore any record containing child pornography that is shared or acquired on internet based sites, furthermore that is stored in any kind of electronic format or that is forwarded.

Broadcasting radio frequency signals without permission can cause the economic[15] or physical discontent[16] of others as well.

[14] ORTIGOSA, A-INGLEZAKIS, I. (2017): D4.1b: FAQ on Responding to online hate speech Monitoring and Detecting Online Hate Speech.
Source: http://mandola-project.eu/m/filer_public/3e/32/3e32fcaa-e420-4868-b3e2-070e2a7983cb/d41b_faq_final.pdf.
Accessed: 26.08.2018.
[15] Here can be mentioned the devices that make it impossible to use cell phone or GPS to determine location.
[16] Due to its cost and size the experimental usage of radiofrequency weapons causing pain and personal harm is only common in the military. But since technology develops at an alarmingly rapid rate it might be possible that wealthy criminals gain access to these devices. Crimes committed using these devices would be impossible to prove with traditional methods. At the same time certain devices can be manufactured at home. Such a thing can cause the death of a person who is relying on a pacemaker and there would be no outer traces that would determine the cause of death.

Due to the above mentioned points it is palpable that the electronic evidence consists of a much larger area than just the digital evidence or the data that can be acquired in connection with computer related crime.

### *The classification and sources of electronic data*

The classification holds significance not only for the theoretic criminalist. Classification might help manage the data correctly, and extract and interpret the immanent information.

As Flórián Tremmel has said: "it can be traced back to important theoretical and pragmatic aspects, and thus they are worth our attention."[17]

Keeping Tremmel's subdivision[18] but taking into consideration the specialities of electronic evidence further aspects of subdivision can be introduced. In our opinion this subdivision might be significant in a pragmatic viewpoint.[19]

Various aspects (1-9.) can determine the classification.

I. The "classic" approach states that the basis shall be the analog and digital classification.
II. The way of feasibility determines three possible groups:

   a) Instantly feasible (audio, video, documentum)
   b) Can be used after processing
   c) Evidence with mixed ingredients

[17] Tremmel, F. (2006): Bizonyítékok a büntetőeljárásban [Evidence in the criminal procedure.]. Dialóg Campus Kiadó. Budapest-Pécs. 82

[18] Tremmel referencing the technical literature differentiates organic and derivative evidence; personal and factual evidence; inculpatory and saving evidence; and finally direct and indirect evidence. Tremmel, ibid 82.

[19] This is especially true in the case of the operative measures or the creation of a program that helps computer investigation.

The first or group „A" requires no further explanation. The evidence requiring processing cannot be interpreted in their acquired state. They do not have probative value on their own. It is especially easy to realise in the case of coded information that it needs decryption. To be translated or interpreted requires the special knowledge and tools of an expert. It is called mixed, because not only the audio and visual data must be transmitted but the so called metadata that is connected to the call as well.

III. The method of perpetration (modus operandi) based classification includes the evidences of crimes that were supported by using radiofrequency weapons, computers or communication devices.[20]

IV. Based on where the crime was committed and whether there is evidence to be found there are physical and cyber crimes. Cloud based services gained popularity in cyberspace. Its undeniable benefit is a fatal vulnerability at the same time. The rightful user can access the content but the perpetrator can commit the crime far from the victim.

Traces of crimes committed in real or physical space can be recorded via electronic signals that is why the electronic trace recording belongs here. (for instance: digital photo, digital site plan.)[21]

[20] It must be added that the military usage incorporates the guided energy microwave weapons, which forces the victim to do or not to do something by heating up the human tissue, paralyzing the sensory organs and the nervous system. The weapon requires no ammunition or bullet. Due to the rapid development of technology the microwave weapons will be available in the near future for the masses as well.

[21] The FORLAB (Forensic Laboratory for in-situ evidence Analysis in a post blast scenario) task force of the European Commission summarises in its report the problems of trace recording in a blasting scene and lists possible solutions as well. The laser 3D recording enables the reconstruction of traces and material remains. The non-GPS based system works at a 10 cm accuracy both outside and inside. Amongst the used technologies LIF (Laser Induced Fluorescence) is mentioned which is laser sweeping recording sensing the polymer and plastic debris. LIBS (Laser Induced Breakdown Spectroscopy which with the help of a laser beam heats up materials of picogram amount to plasma state and then estimates the ingredients) and the Raman analysing system used in chemical industry which enables the remnants of the explosive material to be separated from the non-significant debris. Amongst the recommended tools there is NLJD (Non-Linear Junction Detector)

V. Based on source the evidence can be wired or wireless and also a source classification can be created and reached via an electronic information holding device.

VI. Based on durability volatile and durable data are differentiated.

As an explanation it must be added that evidence (its formation, acquisition, preservation, introduction) is handled differently based on what type it is. It is especially true in the case of the lifecycle of the electronic evidence. In certain cases the only option is to acquire it at the time of formation. Storing itself is the cause in some cases of the decaying of the quality of the evidence. An example for this is the radiocommunication between perpetrators, or the group of data that is stored in the cloud or in the memory of the computer. Many theses[22] and monographies[23] focuse on the problem of the forensic preservation of the latter one. The data on cell phone usage is kept on the devices of the service provider and so for this amount of time they are obtainable.

device, which shows the electronic devices on the scene, regardless whether they are on or off.
It is important that due to the evidence being forwarded at once to the headquarters that coordinates the investigation, the scene can be reconstructed from a distant location, the following of a lead without any technical delay, the identification and catching up to the perpetrator. A further advantage is that the scene before the crime can be reconstructed as well.
Source: https://cordis.europa.eu/result/rcn/191750_fr.html.
Accessed: 05.08.2018.

[22] PURNAYE, P. - JYOTINAGAR, V. : Cloud forensics: Volatile data preservation. International Journal of Computer Science Engineering Vol. 4 No.02. March 2015

[23] TERMANINI, R. (2016): The Cognitive Early Warning Predicting System Using the Smart Vaccine. The New Digital Immunity Paradigm for Smart Cities and Critical Infrastructure. CRC Press Taylor & Francis Group, Boca Raton.

VII. Based on types of communication crimes committed or supported by wired devices, cell phone or radiotransmitter24 can be differentiated.

VIII. Sources can be classified *based on content*.

a) data
b) metadata
c) direct
d) to be interpreted content.

The class of data includes the direct data.

Metadata is embedded deeper into the electronic data and thus usually stays hidden from the user. Such as: the circumstances of the creation of the data, information referring to the creator, and any further fact that the creator of the structure deemed remarkable. Here can be mentioned the digital photos containing the date of production, manufacturer and type of the device, resolution, color depth, exposure time, and in the case of more recent devices - whether GPS is allowed to be used on the device - the precise coordinates of the place of production. In the case of forwarding text messages - besides its content - the time of forwarding and reading can both be extracted from the system. When talking on a mobile phone the number of the parties[25] and the length of the phone call can be obtained from the devices. Information such as the speaker's geographic coordinates, the vector of their movement, and further confidential, hidden data can be obtained only from the service providers. Based on vectoral data the means of transportation can be determined.

[24] Out of the three instrument groups the latter one needs to be further clarified. Using legally owned transceiver during the perpetration of a crime. It is illegal to broadcast if the one with the permit oversteps the boundaries set down in the permit or in other restrictive documents or broadcasts content that violates law.

[25] In the case of a conference call more than two parties can take part in the discussion.

The subdivision of direct content means the evidence that can be acquired via perceiving textual, audio, visual, video content.

The subdivision of to be interpreted content is de facto coded, or classified information, furthermore it includes the facts that hold a special meaning in a certain age and in society.[26]

IX. Based on appearance electronic data (evidence) can be categorised as follows:

1) electronic audio evidence
    a) analog audio record
    b) digitalised or digitally recorded audio
2) visual evidence
    a) still information (face, iris, retina, etc.)
    b) fixed directed source with motion picture[27]
    c) infra camera (in case of a poorly lit surroundings)
    d) visual evidence obtained via manual tracking system
    e) motion picture visual tracking system controlled by artificial intelligence
3) imaging systems through which evidence can be obtained:
    a) medical imaging systems (DRTG, CT, MRI, FMRI, etc.)[28]
    b) criminal personal body screening systems (devices with THz frequency)
    c) infracamera to make body heat map[29]

[26] Hate speech and slang changing with every generation might be good examples for the latter one.

[27] The subject of collecting evidence is the monitored area.

[28] The evidential significance of dental X-rays has been common knowledge for a long time. Modern devices not only make identification possible but due to the time stamp the alibi of the person in question can be justified or refuted.

[29] By studying body heat maps one can deduce the bigger objects hidden underneath the clothing or recognise the state of excitement due to the increased body temperature.

   d) X-ray baggage screening devices with reduced energy[30]
   e) underground imaging systems (eg.: ground radar)
   f) surface imaging systems (vehicle screening system)
   g) atmospheric imaging systems (the location and tracking of not monitored devices moving in the atmosphere for criminal purpose)[31]
4) electronically sensed scent information[32]
5) radiofrequency evidence
   a) passive radiofrequency tracking information
   b) radiofrequency semi-active[33] evidence (RFID[34])
   c) active radiofrequency evidence
6) evidence existing in a limited information technology environment[35]

[30]High energy industrial X-ray machines are used during the study of matter for measuring. Searching baggage is conducted by lower energy X-ray radiation. The imaging system artificially colours the objects inside the baggage based on spectral attributes.

[31] The non-monitored air space is a concept of air traffic control. In this part of air space the organisation responsible for air traffic control only gives information. The exploration of air space is either not guaranteed or with certain limits.

[32] There are such entry systems already in use where the examined person goes through a small so called floodgate channel and the exhaled breath is examined by sensory detectors and presume the lack of drugs and explosives. See: HORVÁTH, O.: A kriminalisztikai szagazonosítás jelene és jövője [Criminalistical Scent Identification's Present and Future.]. Belügyi Szemle 2013/2. 88-101

[33] A semi-active device can only be used in a radiofrequency environment, it is not suitable to identify the evidence in a still state. In a suitable radiofrequency environment it absorbs energy. From the energy it radiates its characteristic data with radiofrequency transmission. In certain cases for example in controlled species the absence of mandatory implants is the basis of suspicion. (Fraud, smuggling, theft.)

[34] RFID (Radio Frequency IDentification) is a device implanted into modules, goods, or living creatures which contains the information specific to that object or creature or the information of the owner. Such devices are product protection devices or the chips used for identification of animals.

[35] In the case of limited IT environment it is simpler to acquire evidence. In the case of their destruction there is a specific group of individuals who are the perpetrators. At the same time the crime-like nature of external "black hat" intrusions - except the so called "white hat" intrusions serving as legal methods to inspect the safety of the system - is the basis of malicious intent.

   a) in IT data storage devices and components (CD, DVD, pendrive, hard drive etc.)
   b) in intelligent mobile communicational and informatics related devices (smartphone, tablet, e-book, notebook, laptop etc.)
   c) in off grid computer systems[36]
   d) in smaller networks including WIFI
   e) in IT systems protected by medium level firewalls
   f) in IT systems protected by high level firewalls and VPN[37]
7) evidence existing in cyber space
   a) data on the open internet (Facebook, LinkedIn, Twitter, Videa, etc.)
   b) data forwarded and stored on illegal networks[38]
8) evidence reconstructed by IT tools
9) evidence of the systems following and reconstructing the activity
10) evidence revealed via electronic investigation that cannot be listed elsewhere

## Summary

In our opinion by the effective exploration of the electronic data (including digital data) that belongs to the group of so called "second generation" evidence (relevant to criminal law) by secret or well-known criminalistical methods and also the safekeeping and using can significantly help the crime-fighters (the digit-commandos) with answering in the most precise

[36] The main characteristic of off grid is that neither the wired nor the wireless devices are in connection with any other device outside of the network. The criminal data found in the system is in direct or indirect connection with the users of the network. Illegal IT intrusion requires physical presence.
[37] VPN: Virtual Private Network
[38] Individuals and organisations operating such networks serve criminal organisations dealing with drugs and arms trafficking. Furthermore establishers and maintainers of sites containing childpornography, sadistic content for entertainment purposes, or showing ordered homicidal actions.

way the seven basic questions at the base of the criminal pyramid, with the identification process of a person, object or action. It also enables the crime-fighters to look into the past with sharp eyes, to see a clear image in the mirror, and at last to be able to reveal the facts as they are.