

# Validation of the Mobile Fingerprint Workstation under the HIT-NET project

Beata Krzemińska<sup>1</sup>

<sup>1</sup> Central Forensic Laboratory of the Police, [beata.krzeminska@policja.gov.pl](mailto:beata.krzeminska@policja.gov.pl)

## Summary

Mobility<sup>1</sup> is associated with freedom of movement and, in the case of computers, also with wireless connection to the Internet for fast data exchange. Professionals in various industries or formations are increasingly seeking to implement such functionality in the equipment they use. Police use mobile terminals<sup>2</sup>, devices for rapid confirmation of individuals' identities (Kot, Tomaszycski, 2015, pp. 340 and 343), and a mobile police workstation<sup>3</sup>, but are not equipped with a mobile fingerprint workstation. The first prototype workstation of this kind was purchased under the NCBR-funded project no. DOB-BIO9/13/01/2018 (HIT-NET) and validated<sup>4</sup> at the Fingerprint Examination Department of the Central Forensic Laboratory of the Police. The article provides the results of the tests conducted and suggests directions for modernization of such setups.

**Key words:** AFIS, dactyloscopy, validation, Mobile Fingerprint Workstation, HIT-NET

## Introduction

As part of the task no. 3, stage I of the project no. DOB-BIO9/13/01/2018 entitled. "An IT system for supporting the processes of the use and analysis of large amounts of data with the purpose of detection of related evidence for the purposes of ongoing pre-trial proceedings and investigative activities" (HIT-NET<sup>5</sup>), a Mobile Fingerprint Workstation (MFW) was purchased and validated to determine the feasibility of implementing the data it generates in the aforementioned system (Mondzelewski et al., 2020, pp. 29–30). The prototype mobile fingerprint identification and registration workstation, purchased from Identity & Security France, (Krzemińska, 2018a, p. 40) is equipped with the following components:

- LiveScanner for scanning a person's fingerprints,
- a camera to take pictures of fingerprints secured at a crime scene,
- a laptop with standard software and software designed for fingerprint and palmprint image processing (mini-AFIS),

- a battery that supports operation of the above mentioned devices for a minimum of 8 hours,
- a transport case providing mobility of the entire workstation.

Validation did not include testing of the installed biometric data search/comparison algorithms<sup>6</sup> per se. It was aimed at confirming the compliance of the MFW functionalities with the requirements set out by the ordering party (especially in the field) and with the assumptions made for the HIT-NET project. It was investigated whether MFW could be used to conduct elimination activities<sup>7</sup>, detect duplicate data, and make initial identification of individuals<sup>8</sup> directly at the crime scene. The tests performed confirmed the efficient operation of the workstation in terms of acquiring and collecting fingerprint and palmprint images, verifying their quality, as well as automatic and manual encoding of these images, comparing fingerprint data<sup>9</sup> and reporting the compliance results. Data can be transferred into the mini-AFIS directly from LiveScanner or imported from files created in other

<sup>1</sup> <https://s.jp.pwn.pl/szukaj/mobilnosc.html> (access: 6/30/2021).

<sup>2</sup> <https://www.policja.pl/pol/aktualnosci/45124,Terminalne-mobilne.html> (access: 6/11/2021).

<sup>3</sup> <http://www.poznan.policja.gov.pl/w21/prewencja-1/mobilny-komisariat/mobilny-komisariat/112299,mobilny-komisariat.html> (access: 6/11/2021).

<sup>4</sup> Validation – The action of confirming in a documented and compliant manner that an item/device meets user-specified requirements.

<sup>5</sup> An IT system for building interactive graphical networks of links between DNA and dactyloscopic hits in conjunction with personal data and additional criminal information provided by the National Police Information System (KSIP).

<sup>6</sup> Forensic Science Regulator Guidance Validation: Fingerprint Search Algorithm FSR-G-230 Issue 2, [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/914255/230\\_Fingerprint\\_Algorithm\\_Validation.Issue\\_2.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/914255/230_Fingerprint_Algorithm_Validation.Issue_2.pdf) (accessed: 6/30/2021).

<sup>7</sup> Art. 21K (3) (The Police Act of 6 April 1990, consolidated text: Journal of Laws of 2020, item 360, 956).

<sup>8</sup> Art. 21k (1) of the Police Act.

<sup>9</sup> Fingerprint data – for the purposes of this article, it has been assumed that this term will generally refer to fingerprint or palmprint images derived from dactyloscopic cards or from latent.

biometric systems or through various external devices that process fingerprint images. From the mini-AFIS, data can be exported to files and then submitted for registration in AFIS (Automated Fingerprint Identification System). Subsequently, they can be used for searching domestic and foreign databases. The resulting hits can be entered (imported) and processed in the HIT-NET system.

### MFW functional assumptions vs. final solutions

Initially, the HIT-NET project envisioned a prototype mobile fingerprint workstation with the following functionalities:

- rapid identification of individuals using a device that connects directly to the AFIS system;
- authentication (authorization) of individuals using the MFW;
- scanning an individual's fingerprints and palmprints to prepare a digital dactyloscopic card;
- performing quality control of fingerprint images (segmentation<sup>10</sup>) along with the capability of enhancing them using a graphical user interface (GUI);
- taking pictures of fingerprints revealed at the scene of an incident and transferring them to a local database;
- processing dactyloscopic data together with alphanumeric data<sup>11</sup>, i.e. entering, modifying and deleting them by means of specialized mini-AFIS software;
- digital processing of dactyloscopic images<sup>12</sup> at 500 dpi or 1000 dpi resolution (8 bit, 256 shades of gray) – including automatic and manual image encoding;
- performing local comparisons (TP/TP, TP/UL, PP/UP, LT/TP, LP/PP, LT/UL, LP/UP) and verifying the returned results;
- collecting the history of activities (logs) performed by the system and the user;
- exporting/importing data to/from files of various formats (NIST, WSQ, JPEG, TIFF and BMP);
- preparing necessary statistical reports.

The prototype purchased lacked the following features:

- palm scanning capability – no available mobile LiveScanners with a 150 mm × 140 mm (5.9' × 5.51')

<sup>10</sup> Segmentation – selecting flat finger impressions from the control imprints (simultaneous imprint of four fingers of one hand) on the dactyloscopic card and comparing them against the rolled impressions.

<sup>11</sup> The mini-AFIS software allows for a wider range of alphanumeric data to be processed compared to AFIS. This gives users the opportunity to prepare a complete dactyloscopic card.

<sup>12</sup> S. Jaślanek, *Kryminalistyczne znaczenie linii papilarnych w ekspertyzach daktyloskopijnych*, [https://kipdf.com/kryminalistyczne-znaczenie-linii-papilarnych-w-ekspertyzach-daktyloskopijnych\\_5ac710511723dd2bd9589287.html](https://kipdf.com/kryminalistyczne-znaczenie-linii-papilarnych-w-ekspertyzach-daktyloskopijnych_5ac710511723dd2bd9589287.html) (accessed: 3/9/2021).

- scanning area capable of field operation without a permanent power supply;
- a device for rapid identification of individuals – no possibility to reliably test the functionality of such a device – the technologies offered would not communicate with the AFIS system operating in Poland (Krzemińska, 2017, pp. 93–98).

The acquired workstation (see Fig. 1) is equipped with a module for scanning an individual's fingers (LiveScanner MTOP100R) with the associated MESA (Morpho Enrolment Services Application) software, a Nikon D850 digital camera for taking pictures of fingerprints secured at the scene of an incident<sup>13</sup>, a computer (laptop/notebook) Dell Latitude 7424 Rugged Extreme with installed standard and specialized (mini-AFIS) software, an APC SMT1000IC UPS battery with min. 8 hours operating time, and a StormCase PELI transport case for MFW mobility.



Fig. 1. Mobile Fingerprint Workstation (MFW).

The components of the workstation are packed in a convenient transport case in which it can be delivered to the scene of the incident and used to collect and register fingerprint data, perform quality control of the material acquired, improve the legibility of images (especially of traces) and conduct local dactyloscopic searches<sup>14</sup>. Data prepared in this way can be digitally transferred to other external biometric systems for further processing.

<sup>13</sup> A camera can additionally be used to document a visual inspection of the scene.

<sup>14</sup> Searches: tenprint/tenprint, tenprint/latent, latent/tenprint, latent/latent.

### Innovation of MFW

The IT market offers a wide range of mobile biometric stations for registration of finger- and palmprints, facial image, iris, etc., intended for the purposes of:

- verification of a person's identity (comparison with e-documents, with a local or remote database);
- registration and identification of citizens, voters, travelers, emergency responders and patients;
- control of external borders;
- conducting humanitarian aid;
- law enforcement (law enforcement authorities or military agencies) – in particular the interception and transmission of relevant information about suspects, terrorists, or prisoners;
- preparing e-documents such as driver's license, ID card, passport, visa, operator/expert license, patient or welfare card, voter or employee ID with access control to premises, etc.

Examples of mobile biometric kits are shown in Table 1.

An analysis of the technical parameters and available functionalities of the kits listed in Table 1 showed that they are mainly used to verify the identity of individuals with the documents they hold and with a local or central database. Some of them can be used to prepare biometric documents or access cards (PVCs). They primarily process facial images and fingerprint images. They can perform iris scans, collect individuals' signatures on tablets, and occasionally scan the veins of the hand. Certain kits are equipped with an individual battery system connected to a built-in solar panel and they can be used for registration or identification purposes by:

- agencies handling elections;
- citizen registration authorities;
- immigration services;
- border guards and customs authorities;
- law enforcement agencies for the purposes of confirming a person's identity (based on: identity card, driver's license, passport) or checking a person's criminal history (whether they are currently wanted);
- prison service;
- health services for patient registration purposes, as well as to control the administration of medications and the provision of medical services, such as to control vaccinations for COVID-19;
- social services;
- humanitarian aid;
- institutions engaged in the distribution of controlled products, such as the sale of arms and ammunition.

The above mentioned, depending on the implemented components, are used for quick confirmation of persons' identity for both civil and criminal purposes, but they are not capable of processing fingerprints secured at the crime scene. Although the companies offer the possibility of extending the standard versions, they require direct

contact with the buyer and determining the parameters of modification in order to do so. The innovation of MFW lies in the implementation of mechanisms for handling finger and palm latent secured at the crime scene. Its functionalities allow for scanning fingerprints, taking photographs of images of the secured fingerprints and registering these data in a local database. Since elimination procedure can be carried out directly at the crime scene and preliminary identification of perpetrators can be performed, the device can be used for preliminary detection activities<sup>15</sup>. The MFW is self-sufficient<sup>16</sup> and does not work as a remote AFIS workstation (Krzemińska, 2017, pp. 93–98). The implemented module enabling data export/import to file formats commonly used in biometric systems makes mini-AFIS interoperable<sup>17</sup> with these systems.

In April and May 2020, a survey was conducted among EU Member States and it was found that the MFW could be an innovative solution also in European Union. The survey asked police contact experts for the international exchange of fingerprint data under the Prüm Decision<sup>18</sup> whether they use mobile fingerprint workstations similar to the MFW in their countries. They were additionally asked to describe the functionality of these solutions. A total of 11 responses<sup>19</sup> were returned and all of them declared that the experts did not use kits like MFW. Mobile workstations are used in EU Member States, but they are mainly exploited to quickly confirm individuals' identity (in the police, border guard or health care). Other solutions include mobile versions of LiveScanner that communicate directly with AFIS, similar to those used in Poland (Krzemińska, 2018b, p. 154). In certain countries the purchase of workstations like MFW (especially for rapid processing of immigrants) has been considered, but these plans have been hampered by internal laws requiring certification of such kits putting them into service, which significantly increases the cost of acquisition. Therefore, the solutions that connect on line to the main AFIS system are more preferable, especially in border areas. However, insufficient data communications links necessary for secure, high-speed, remote transmission of large data packets are an obstacle. None of the kits described include mechanisms for collecting and processing images of fingerprints secured directly at the crime scene.

<sup>15</sup> Art. 21k (2) of the Police Act.

<sup>16</sup> With the APC SMT1000IC UPS providing a runtime of minimum 8 hours.

<sup>17</sup> [https://www.evidencemagazine.com/index.php?option=com\\_content&task=view&id=89&Itemid=49](https://www.evidencemagazine.com/index.php?option=com_content&task=view&id=89&Itemid=49) (accessed: 6/8/2021).

<sup>18</sup> Council Decision 2008/615/JHA and 2008/616/JHA.

<sup>19</sup> Responses were obtained from: AT, CY, CZ, ES, GR, HU, IT, LT, LV, RO, SE.

**Tab. 1.** Selected mobile biometric stations.

Product name	Photo of the biometric station	Link to the website
<b>Laxton</b> – flagship Biometric Registration Kit		<a href="https://laxtongroup.com/products/">https://laxtongroup.com/products/</a>
The <b>Cross Match Jump Kit</b> Guardian® Jump Kit Multimodal Biometric Jump Kit		<a href="http://mtesolution.com/product-crossmatch-Guardian-jumpkit.php">http://mtesolution.com/product-crossmatch-Guardian-jumpkit.php</a>
<b>HSB</b> – biometric registration solution		<a href="https://www.hsb.nl/our-products/biometric-registration-solution/">https://www.hsb.nl/our-products/biometric-registration-solution/</a>
<b>CardLogix</b> Corporation FbF® BioEnroll – full portable biometric enrollment kit		<a href="https://www.cardlogix.com/product/fbf-bioenroll-portable-biometric-enrollment-kit/">https://www.cardlogix.com/product/fbf-bioenroll-portable-biometric-enrollment-kit/</a>
<b>CardLogix</b> Corvus Government Identity Enrollment and Registry Solution (GIERS)		<a href="https://www.cardlogix.com/product/corvus-government-id-enrollment-registry-solution/">https://www.cardlogix.com/product/corvus-government-id-enrollment-registry-solution/</a>
<b>CardLogix</b> Corvus Micro Booking Station		<a href="https://www.cardlogix.com/product/corvus-micro-booking-station-for-biometric-enrollment/">https://www.cardlogix.com/product/corvus-micro-booking-station-for-biometric-enrollment/</a>
<b>CardLogix</b> Corvus Portable Identity Kit (PIK)		<a href="https://www.cardlogix.com/product/corvus-portable-identity-kit-for-biometric-enrollment/">https://www.cardlogix.com/product/corvus-portable-identity-kit-for-biometric-enrollment/</a>
<b>HYF Shenzhen Herofun Bio-Tech Co BH1164</b> Fingerprint 4-4-2 Biometric Voter kit (BVK)		<a href="https://herofun-bio.manufacturer.globalsources.com/si/6008850883730/pdtl/Industrial-handheld/1178312529/Enrollment-kit-voter-kit-with-4-42.htm">https://herofun-bio.manufacturer.globalsources.com/si/6008850883730/pdtl/Industrial-handheld/1178312529/Enrollment-kit-voter-kit-with-4-42.htm</a>
<b>HYF Shenzhen Herofun Bio-Tech Co HYF-BH1160</b> Fingerprint 4-4-2 Biometric Voter enrollment kit		<a href="https://www.globalsources.com/Biometric-tablet/Biometric-voter-enrollment-kit-for-National-ID-1167780954p.htm#1167780954">https://www.globalsources.com/Biometric-tablet/Biometric-voter-enrollment-kit-for-National-ID-1167780954p.htm#1167780954</a>

Tab. 1. Continue.

Product name	Photo of the biometric station	Link to the website
<p><b>HYF Shenzhen Herofun Bio-Tech Co HYF-BH1165</b> Fingerprint 4-4-2 Biometric Voter kit IRIS</p>		<p><a href="https://www.globalsources.com/Biometric-tablet/Biometric-Vote-Kit-IRIS-Fingerprint-Windows-Laptop-1178212405p.htm#1178212405">https://www.globalsources.com/Biometric-tablet/Biometric-Vote-Kit-IRIS-Fingerprint-Windows-Laptop-1178212405p.htm#1178212405</a></p>
<p><b>Morpho LiveScan Jumpkit</b></p>		<p><a href="https://www.idemia.com/press-release/morpho-and-snap-inc-provide-ruggedized-livescan-jumpkit-us-customs-and-border-patrol-2016-05-18">https://www.idemia.com/press-release/morpho-and-snap-inc-provide-ruggedized-livescan-jumpkit-us-customs-and-border-patrol-2016-05-18</a></p>
<p>Fulcrum Biometrics (USA) <b>FbF ® LiveScan Jumpkit with DactyScan84c</b></p>		<p><a href="https://www.fulcrumbiometrics.com/FbF-LiveScan-Jump-Kit-with-DactyScan84c-p/200311.htm">https://www.fulcrumbiometrics.com/FbF-LiveScan-Jump-Kit-with-DactyScan84c-p/200311.htm</a></p>
<p>Fulcrum Biometrics (USA) <b>FbF bioEnroll Lite</b></p>		<p><a href="https://www.fulcrumbiometrics.com/FbF-bioEnroll-Lite-Portable-Collection-Kit-p/200351-03-ck.htm">https://www.fulcrumbiometrics.com/FbF-bioEnroll-Lite-Portable-Collection-Kit-p/200351-03-ck.htm</a></p>
<p>Fulcrum Biometrics (USA) <b>FbF bioEnroll, standard</b></p>		<p><a href="https://www.fulcrumbiometrics.com/FbF-bioEnroll-Standard-Portable-Collection-Kit-p/200351-02-ck.htm">https://www.fulcrumbiometrics.com/FbF-bioEnroll-Standard-Portable-Collection-Kit-p/200351-02-ck.htm</a></p>
<p>Fulcrum Biometrics (USA) – portable kit <b>FbF bioEnroll</b></p>		<p><a href="https://www.fulcrumbiometrics.com/FbF-bioEnroll-Full-Portable-Collection-Kit-p/200351-01-ck.htm">https://www.fulcrumbiometrics.com/FbF-bioEnroll-Full-Portable-Collection-Kit-p/200351-01-ck.htm</a></p>
<p><b>VISION Dubai</b> Biometric registration kits</p>		<p><a href="https://www.idvisionme.com/biometric-registration-kits/">https://www.idvisionme.com/biometric-registration-kits/</a></p>
<p><b>HID® Jumpkits</b></p>		<p><a href="https://www.hidglobal.com/products/jumpkits/hid/jumpkits">https://www.hidglobal.com/products/jumpkits/hid/jumpkits</a></p>

### MFW validation process

MFW validation was conducted under laboratory conditions at the Fingerprint Examination Department of the Central Forensic Laboratory of the Police according to the validation plan developed earlier along with 10 test scenarios. The results showed that the workstation was equipped with the necessary tools for fingerprint image acquisition, collection, processing and quality control. These tools are also suitable for processing “difficult” latents (e.g. poor-quality or fragmentary images, images of overlapping latents or those collected from curved surfaces). State-of-the-art encoding and matching algorithms allow for efficient searches in the local database.

The tests were carried out in accordance with documentation provided by the contractor and with internal instructions<sup>20</sup> of the Fingerprint Examination Department of the Central Forensic Laboratory of the Police. Each of the prepared scenarios was executed multiple times in the number of repetitions allowing to confirm the correctness of the analysis-database software operation (mini AFIS) in terms of:

- determination of the quality of electronic TenPrints cards prepared with the use of LiveScanner associated with the MFW and the possibility of entering the cards into a local database;
- importing to the local database fingerprint (TP) and palmprint (PP) images from TenPrints as well as finger latents (LT) and palm latents (LP) from other sources saved in different file formats;
- encoding of latent images;
- performing and returning the results of tenprint/tenprint (TP/TP), tenprint/latent (TP/UL, PP/UP), latent/tenprint (LT/TP, LP/PP), latent/latent (LT/UL, LP/UP) searches of the local database for elimination, duplicate detection and pre-identification purposes;
- exporting data from the local database to NIST files and uploading them to AFIS.

The testing material consisted of 130 tenprints and 160 finger or palm latent images. A total of 110 searches of various types were performed.

TP cards were entered into mini-AFIS both from LiveScanner and from files of various formats (see Tab. 2). The choice of file formats was not random. Ink cards (approx. 10% of all cards) are still received by the Fingerprint Examination Department of the Central Forensic Laboratory of the Police (Moszczyński, 1997, pp. 134–142) and scanned before being entered into AFIS. TIF or JPG files are considered the simplest form of electronic carriers for TPs, including the simplicity of preparation and transfer. However, they do not guarantee adequate protection of the data they contain.

For this reason, NIST files (Krzemińska, 2018a, p. 36), considered the most secure file standard for transferring

<sup>20</sup> Instructions: BJ-Z3-In-1, BJ-Z3-In-2, BJ-Z3-In-3 and BJ-Z3-In-4.

**Tab. 2.** File formats used for entering TP into mini-AFIS.

Source of TP data	Number of TP cards
JPG	20
TIF	20
NIST	70
LiveScanner	20

biometric data between systems, are increasingly being used. However, NIST files require content specification due to elaborate internal structure and high openness to personalized records. Practically: only one of two NIST files, seemingly looking the same, can be imported into a particular biometric system. All that is needed in the second file is for one of the fields to be missing an entry, mandatorily required by the specification, or to contain a value different from the specification. In the study conducted, three types of NIST files (the most common ones used in Poland) were used for testing:

- 30 TP cards exported from AFIS in different periods of operation (deaths<sup>21</sup>),
- 10 files from the Prüm test set used to validate the international connection,
- 30 files exported from mini-AFIS.

A standard TP card<sup>22</sup> contains 10 rolled and 4 control fingerprint images (simultaneous imprints of four fingers of the left hand; imprints of the left and right thumbs; and simultaneous imprints of four fingers of the right hand). However, practice shows that the cards do not always contain a complete set of images<sup>23</sup>. Therefore, TP cards with differing image sets were used for testing (see Table 3).

While being entered, the data are subject to automatic quality control, during which the quality of individual images is checked and sequence conformity between the rolled imprints and flat control imprints is verified (Krzemińska, 2018a, s. 36).

In biometric systems, quality thresholds are set and the input information is qualitatively classified<sup>24</sup>. In the application tested, the thresholds were set above those in the AFIS system, which resulted in as many as 95 cards being subjected to quality control, and 5 cards – to segmentation.

<sup>21</sup> Fingerprint data from deceased persons.

<sup>22</sup> Model fingerprint card – Annex 2 to the Regulation of the Minister of Interior and Administration of 21 July 2016 (Journal of Laws of 2016, item 1091).

<sup>23</sup> The person from whom the data is collected may have, for example, a damaged or amputated finger.

<sup>24</sup> Data whose quality has been determined to be below the required threshold are subjected to “Quality Control” performed manually by an expert.

**Tab. 3.** Types of TP entered into mini-AFIS.

TP card content	Number of cards
10 rolled fingerprints	20
10 rolled and 4 control fingerprints	60
10 rolled and 2 control fingerprints (without thumbs)	5
10 rolled and 4 control fingerprints (without fingers 5 and 10)	5
10 rolled and 4 control fingerprints (without fingers 2 and 7)	5
10 rolled and 4 control fingerprints (segmentation required)	5
4 flat control fingerprints	25
4 flat control fingerprints (without fingers 5 and 10)	5

Latent images images can also be provided in different file formats. In this case, an additional difficulty is that a single file (image) can contain several latents. During validation, the ability to retrieve these data from files with different formats was investigated (see Table 4).

These files have been prepared in a number of ways (see Table 5).

Photos were taken with a camera associated with the MFW. Photos and scans included a scaler that allowed the user to control the size and resolution of the image input. This task was made more difficult in the case of screenshots (images captured from the screen), i.e., fingerprint images without a scaler. In these situations, the person entering data had to scale the image independently. It should be emphasized that this activity is very important for the latent entry process. Tenprint images are entered at 1:1 scale with 500 dpi resolution. Thus, for the alignment of latent images to tenprint images to be adequate, it is required that the latents have similar size and resolution. To this end, the latent images are scaled. For the LT latents, two types of ANSI/NIST files were used for the MFW testing: 10 files from the Prüm test set and 10 files exported from mini-AFIS. During data entry, the expert had all the tools necessary to properly process the images registered, particularly the ability to delineate the traces from rounded surfaces (e.g., a bottle or glass) and to delaminate the overlapped latents (Krzemińska, 2018a, p. 37).

The data entered into the local database allowed all types of searches to be performed and the results thereof are shown in Table 6 (Hit result- positive match, NoHit result – no match).

For TP/TP (tenprint / tenprint) searches, 10 tenprint were eliminated and the rest were recognized as duplicates. Sending the tenprints to the latents' database (TP/UL) eliminated 10 latents and identified 10 unsolved

**Tab. 4.** File formats used to enter LT into mini-AFIS.

Source file LT	Number of files	Number of entered latents
JPG	60	85
TIF	25	10
BMP	8	25
NIST	20	40

**Tab. 5.** File formats used to enter LT into mini-AFIS.

Method of securing fingerprints	Number of films	Number of entered latents
Photo of an object	30	65
Photo – overview board	9	10
Photo – transparent gelatin film	9	10
Photo – positive film	4	5
Photo – black gelatin film	4	5
Scan – images from card	5	10
Scan – black gelatin film	5	5
Scan – transparent gelatin film	5	5
Control fingerprint image from the screen	5	5
Single fingerprint image from the screen	7	15
Single fingerprint image	20	25

**Tab. 6.** Types of searches performed in mini-AFIS and the results obtained.

Type of search	Number of searches	Hit result	NoHit result
TP/TP – tenprint/tenprint	30	20	10
TP/UL – tenprint/latent	30	20	10
LT/TP – latent/tenprint	30	20	10
LT/UL – latent/latent	20	10	10

latents located in the local database. Similarly, performing latent searches within a local tenprint database (LT/TP) resulted in partial elimination (10 links to elimination tenprints) and preliminary identification (10 identified Unsolved Latents). Latent/latent (LT/UL) searches revealed 10 matches with Unsolved Latents. All results obtained were as expected.

### MFW validation results

Based on the documented validation results, it was found that for all investigated scenarios the returned results were as expected (100% confirmation of expectations)<sup>25</sup>. This allowed the authors to conclude that the MFW correctly retrieves<sup>26</sup> and collects fingerprint and palmprint images. The workstation can perform quality control of data input, manually encode finger and palm images, perform comparisons of all fingerprint data, and prepare reports of the results. Thus, the MFW can be used for selection and elimination of latents as well as recognition of duplicate tenprints and latents revealed at the crime scene. The system has a data export/import module implemented, which streamlines the transfer of fingerprint data to other biometric systems, but does not perform this automatically. This allows for quick in-field verification of revealed and secured fingerprint material, thus shortening the time for efficient typing of perpetrators. Consequently, it provides a guarantee that no duplicated or eliminable data will be entered into the HIT-NET system.

The identification value of fingerprint data collected in databases is determined by their quality. The mini-AFIS contains the tools necessary to improve the quality of image input<sup>27</sup> and encoding, allowing for efficient processing of secured fingerprint data, whose quality is comparable to that of AFIS data. In addition, the tools available are easy to use and sufficient for conducting initial latent selection.

The mini-AFIS software is capable of communicating with other systems (e.g., national AFIS). It allows for importing images into the local database from the JPG, TIF, BMP and NIST file formats, exported from AFIS. Unfortunately, for NIST files, the reverse operation (i.e., importing files from the MFW into AFIS) cannot be performed. It is anticipated that this type of communication will be possible once the AFIS system is upgraded. Currently, a substitute solution can be used, i.e., saving the images to JPG, TIF, and BMP files and then entering and processing them in AFIS. The downside of this solution is the need to re-encode the image. NIST files offer the possibility of transferring minutiae clouds<sup>28</sup>.

The system logs store information about all mini-AFIS activities performed by the system or the user. Access to

system data is controlled by login (unique and different for each user) and password. The application verifies the user's identity and assigns access to database resources according to the user's privileges. The workstation also implements mechanisms to check the integrity of the data processed. Thus, the history of user or system actions can be reconstructed at any time. This protects the data from uncontrolled corruption.

The MFW equipment is packed into one heavy-duty waterproof and dustproof transport case (StormCase PELI). The entire kit weighs about 40 kg, of which the heaviest component is the UPS battery (18 kg). A user can decide on the components of equipment to be taken to the scene. However, without a backup power supply, the laptop can operate for a maximum of 3 hours under maximum workload. With approximately 0.5 hours needed to set up the workstation, there is little time left for the actual fingerprinting work, which is the reason for equipping the kit a UPS that guarantees 8 hours of work.

A shortcoming of the workstation is that the mini-AFIS restart procedure is complex and requires specialized IT knowledge (virtual machine operation, Linux, Oracle, WEB technologies). If the application is closed incorrectly (e.g. uncontrolled pressing of a key combination) or if the workstation is restarted unexpectedly (e.g. power failure), the database very quickly becomes inoperable (problems with launching key functionalities). Although the data can be recovered, it is substantively beyond the scope of knowledge of the fingerprint expert for whom this workstation is intended. In other words, the unstable operation of the device enforces continuous maintenance of the provider's support.

Another disadvantage of the MFW is its inability to perform palmprint scans<sup>29</sup>. The application itself can process these types of images, but they must be entered into the system by another means, e.g. by file import, which makes it difficult to eliminate such images efficiently. However, such situations are rare because the likelihood of securing a palmprint at the scene is low. In the current AFIS system, unsolved palm latents account for approximately 12% of all unsolved latents entered.

A shortcoming of the MFW is also that it does not include a device for quick confirmation of a person's identity. Any fingerprint images can be exported from the mini-AFIS and submitted for an AFIS search. However, since the MFW does not have the ability to communicate directly with the PSTD network – Police data transmission network, this action must be performed manually, on-site, i.e. at the police unit that has access to the AFIS.

### Conclusions

The purchase of a prototype Mobile Fingerprinting Workstation under Project No. DOB-BIO9/13/01/2018

<sup>25</sup> According to the EN ISO/IEC 17025: 2017 standard – validation is the confirmation by examination and presentation of objective evidence that the requirements for the intended use have been met.

<sup>26</sup> Exception: LiveScanner provided with the MFW used in this study was not suitable for capturing palmprint images.

<sup>27</sup> § 15 and § 23 of the Ordinance No. 28 of 11 August 2020 on fingerprint data sets (Official Journal of the Police Headquarters, 2020.44.).

<sup>28</sup> Minutiae cloud – a set of characteristic features in a fingerprint image determined by a fingerprint expert or biometric system.

<sup>29</sup> LiveScanner with a 3' × 3.2' scanning area.



(HIT-NET) provided a unique opportunity to acquire and test innovative functionalities, especially under field conditions. The validation performed at the Fingerprint Examination Department of the Central Forensic Laboratory of the Police confirmed its proper operation in terms of retrieving, collection, quality control and manual encoding of fingerprint images, comparison of fingerprint data and reporting of compliance results. The device can be used to recognize duplicate tenprints and eliminate latents directly at the scene of an incident. This translates into more reliable verification of data registered, and thus more accurate matching within forensic databases, which is often crucial for law enforcement and the justice system (Jurga et al., 2020, pp. 4–7). The usefulness of the data used in the identification process is increased due to the introduction of latent images into the system that are very likely to originate from crime perpetrators and not from random individuals (Kot, Tomaszycy, 2015, p. 341). As a result, it guarantees the correct matching of perpetrators with crimes in the HIT-NET system containing hit results from DNA and AFIS databases. Networks of connections built on the basis of these data become more reliable and more accurately reproduce the mutual criminal colligations between individuals (Świeżak, 2017, p. 70).

With the data import/export module implemented, the MFW is open to interoperability with other systems, including AFIS (except for full support of NIST files). In addition, the modular design of the workstation opens it to further development, e.g. by adding more devices or implementing new functionalities.

Recent events related to the COVID-19 pandemic have influenced the development of contactless technologies<sup>30</sup>. According to analysts, the future lies in safer and more hygienic solutions<sup>31</sup>. This suggests certain modernization ideas for the MFW equipment. The first suggestion is to replace the current LiveScanner with a contactless version<sup>32</sup> or use applications installed on smartphones<sup>33</sup>. Another is to increase MFW mobility by replacing the UPS with a lighter and more efficient model. Currently, the entire kit including the case weighs about 40 kg, which limits the number of people who can transport it (especially in unpaved terrain). It is also advisable to upgrade the software towards making the mini-AFIS application more end-user friendly, especially in terms of IT support. This applies to both reducing the

time and simplifying the workstation startup procedure, as well as to improving the stability of the database operation. However, all these changes must not be implemented at the expense of reducing the period of failure-free operation.

### Sources of Figures and Tables:

**Fig. 1:** author

**Tab. 1:** summary prepared on the basis of Internet surveys

**Tab. 2–6:** author

### Bibliography

- Jurga, A., Połomska, J., Kot, E. (2020). Zbiory danych DNA i danych daktyloskopijnych – przydatność eliminacyjna. *Horyzonty Kryminalistyki*, 2.
- Kot, E., Tomaszycy, K. (2015). Funkcjonowanie automatycznego systemu identyfikacji daktyloskopijnej AFIS. In: E.W. Pływaczewski, W. Filipowski, Z. Rau (ed.), *Przestępczość w XXI wieku – zapobieganie i zwalczanie. Problemy technologiczno-informatyczne*. Warsaw: Wolters Kluwer Publishing House.
- Krzemińska, B. (2017). Automatyczny System Identyfikacji Daktyloskopijnej w policyjnej „cyberpodprzestrzeni”. In: S. Gwoździwicz, K. Tomaszycy (ed.), *Prawne i społeczne aspekty cyberbezpieczeństwa*. Warsaw: International Institute of Innovation “Science – Education – Development”.
- Krzemińska, B. (2018a). System AFIS w polskiej Policji – wczoraj, dzisiaj, jutro. *Problemy Kryminalistyki*, 300(2).
- Krzemińska, B. (2018b). Współpraca AFIS z systemami wielkoskalowymi. In: E. Gruza, K. Borkowski (ed.), *Horyzonty daktyloskopii*. Warsaw: Publishing House of the Central Forensic Laboratory of the Police.
- Mondzelewski, J., Krzemińska, B., Brągoszewska, A., Wierchowski, P. (2020). HIT-NET – system informatyczny umożliwiający integrację i wizualizację wyników trafień (HIT) w bazach DNA i daktyloskopijnych w powiązaniu z danymi kryminalnymi dotyczącymi przestępstw i ich sprawców. *Problemy Kryminalistyki*, 309(3).
- Moszczyński, J. (1997). *Daktyloskopia – zarys teorii i praktyki*. Warsaw: Publishing House of the Central Forensic Laboratory of the Police.
- Świeżak, R. (2017). Analiza kryminalna w dobie społeczeństwa informacyjnego. *Przegląd Policyjny*, 4(43).

### Legislation and guidelines

- BJ-Z3-In-1*: Instrukcja prowadzenia selekcji, sprawozdania i rejestracji NN śladów w bazach AFIS, wydanie I z dnia 29.07.2016 r.
- BJ-Z3-In-2*: Instrukcja prowadzenia przeszukania w AFIS Karta Daktyloskopijna – Baza NN Śladów (TP/UL), wydanie I z dnia 29.07.2016 r.

<sup>30</sup> <https://www.sourcesecurity.com/insights/covid-19-worries-boost-prospects-touchless-co-11127-ga-sb.1590662579.html> (accessed: 6/11/2021).

<sup>31</sup> <https://filarybiznesu.pl/higieniczne-i-bezpieczne-biometria-bezdotykowa-zanotuje-spektakularne-wzrosty/a9351> (accessed: 6/11/2021).

<sup>32</sup> <https://www.idemia.com/contactless-fingerprint> (accessed: 6/11/2021).

<sup>33</sup> <https://developer.idemia.com/capturesdks/overview> (accessed: 7/7/2021).

3. *BJ-Z3-In-3*: Instrukcja Rejestracji kart daktyloskopijnych w bazach AFIS, wydanie I z dnia 03.12.2018 r.
4. *BJ-Z3-In-4*: Instrukcja rejestracji kart daktyloskopijnych cudzoziemców podlegających procedurom administracyjnym w bazach AFIS oraz JC EURODAC, wydanie I z dnia 03.12.2018 r.
5. Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime (Journal of Laws EU L210/1 of 2008).
6. Council Decision 2008/616/JHA of 23 June 2008 on the implementation of the Council Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime – including an Annex specifying the technical parameters for the exchange of dactyloscopic, DNA and vehicle registration data (Journal of Laws EU L210/12 of 2008).
7. Regulation of the Minister of Internal Affairs and Administration of 21 July 2016 on information processing by the Police (Journal of Laws of 2016, item 1091).
8. Ordinance No. 28 of the Commander-in-Chief of the Police of 11 August 2020 on fingerprint data sets (Official Journal of the Police Headquarters, 2020.44.).
9. The Police Act of 6 April 1990 (consolidated text: Journal of Laws of 2017, item 2067).
- Validation: Fingerprint Search Algorithm FSR-G-230 Issue 2 (accessed: 06/30/2021).
3. <https://www.policja.pl/pol/aktualnosci/45124,Terminale-mobilne.html> – Policja, Terminale mobilne (accessed: 6/11/2021).
4. <http://www.poznan.policja.gov.pl/w21/prewencja-1/mobilny-komisariat/mobilny-komisariat/112299,MOBILNY-KOMISARIAT.html> – strona internetowa KMP w Poznaniu (accessed: 6/11/2021).
5. [https://kipdf.com/kryminalistyczne-znaczenie-linii-papilarnych-w-ekspertyzach-daktyloskopijnych\\_5ac710511723dd2bd9589287.html](https://kipdf.com/kryminalistyczne-znaczenie-linii-papilarnych-w-ekspertyzach-daktyloskopijnych_5ac710511723dd2bd9589287.html) – S. Jaślanek, *Kryminalistyczne znaczenie linii papilarnych w ekspertyzach daktyloskopijnych* (accessed: 3/9/2021).
6. [https://www.evidencemagazine.com/index.php?option=com\\_content&task=view&id=89&Itemid=49](https://www.evidencemagazine.com/index.php?option=com_content&task=view&id=89&Itemid=49) – Kristi Mayo, *Leaders in the field of latent-print identification are starting to look for an “enter once, search many” solution* (accessed: 6/8/2021).
7. <https://www.sourcesecurity.com/insights/covid-19-worries-boost-prospects-touchless-co-11127-ga-sb.1590662579.html> – L. Anderson, *COVID-19 worries boost prospects of touchless biometric systems* (accessed: 6/11/2021).
8. <https://www.idemia.com/contactless-fingerprint> – Idemia, Contactless fingerprint (accessed: 6/11/2021).
9. <https://developer.idemia.com/capturesdks/overview> – Idemia, Capture SDKs (accessed: 7/7/2021).
10. <https://filarybiznesu.pl/higieniczne-i-bezpieczne-biometria-bezdotykowa-zanotuje-spektakularne-wzrosty/a9351> – B. Mróz-Gorgoń, *Higieniczne i bezpieczne. Biometria bezdotykowa zanotuje spektakularne wzrosty* (accessed: 6/11/2021).

#### Websites

1. <https://sjp.pwn.pl/szukaj/mobilność.html> – Internetowy Słownik Języka Polskiego (accessed: 06/30/2021).
2. [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/914255/230\\_Fingerprint\\_Algorith\\_Validation\\_Issue\\_2.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/914255/230_Fingerprint_Algorith_Validation_Issue_2.pdf) – Forensic Science Regulator Guidance

Translation Hanna Wierzchośławska



## REGULAMIN publikowania prac w „Problemach Kryminalistyki”

1. Redakcja „Problemów Kryminalistyki”, zwana dalej Redakcją, przyjmuje do publikacji wyłącznie oryginalne prace teoretyczne i eksperymentalne, syntetyzujące, analityczne i kazuistyczne z zakresu kryminalistyki i dziedzin pokrewnych oraz recenzje monografii naukowych autorstwa jednej lub kilku osób, zwanych dalej Autorem. Złożone teksty nie mogą być opublikowane wcześniej w innych miejscach, ani też w tym samym czasie rozpatrywane pod kątem publikacji w innych czasopiśmiech.
2. Redakcja nie zwraca autorom nadesłanych prac, a także zastrzega sobie prawo skracania i adiustacji tekstów oraz zmiany tytułów i śródtytułów.
3. Redakcja zastrzega sobie możliwość odmowy przyjęcia artykułu bez podania przyczyn.
4. Prace napisane niezgodnie z niniejszym regulaminem nie będą publikowane.
5. Prace należy przysyłać pocztą elektroniczną na adres: [clkpk@policja.gov.pl](mailto:clkpk@policja.gov.pl) bądź dostarczyć do redakcji na nośnikach elektronicznych (CD, DVD, pendrive, które nie podlegają zwrotowi Autorowi).
6. Teksty nie powinny przekraczać 40 000 znaków wraz z rycinami, tabelami, abstraktem i bibliografią, powinny być sporządzone czcionką znormalizowaną (Times New Roman), wielkość czcionki 12, odstępy 1,5 wiersza, z marginesem 2,5 cm z lewej i prawej strony. Zapis powinien być dokonany podstawowym krojem pisma bez wyróżnień.
7. Do każdego tekstu należy dołączyć abstrakt (maksymalnie 150 słów) oraz od 3 do 7 słów kluczowych.
8. Prace mogą być dostarczone w języku polskim lub angielskim.
9. Prac nie należy podpisywać. Przesłane prace nie mogą zawierać danych pozwalających zidentyfikować autora tekstu. W osobnym pliku należy umieścić imię i nazwisko autora (autorów), tytuł publikacji, nazwę instytucji, w której zatrudniony jest autor, zajmowane stanowisko, dane korespondencyjne, numer telefonu, adres e-mail oraz, jeśli wymagane, informacje dotyczące źródeł finansowania dla prowadzonych badań.
10. Nadsyłane prace będą recenzowane przez dwóch recenzentów zgodnie z zasadą *double-blind review*, co oznacza to, że recenzenci nie znają tożsamości autora tekstu, a autor nie wie, kto jest recenzentem. Raz w roku na stronie internetowej wydawnictwa zostają umieszczone nazwiska recenzentów współpracujących z czasopiśmie. Recenzenci wybierani są spoza instytucji, do której afiliowany jest jej autor.
11. W sytuacji gdy ocena jest pozytywna, ale recenzent wskazuje na konieczność zmian i poprawek, Autor jest zobowiązany do ustosunkowania się do uwag i ewentualnego uwzględnienia sugerowanych poprawek.
12. Redakcja przyjęła i stosuje Kodeks Etyki Publikacyjnej. Wydawca, Autorzy i Recenzenci są zobowiązani do przestrzegania zasad etyki, a w szczególności zasady odpowiedzialności, uczciwości, przejrzystości i poufności. Redakcja przypomina, że *ghostwriting* oraz *guest authorship* są przejawem nierzetelności naukowej, a wszelkie wykryte przypadki będą demaskowane i dokumentowane, włącznie z powiadomieniem odpowiednich podmiotów (instytucje zatrudniające autorów, towarzystwa naukowe, stowarzyszenia edytorów naukowych itp.). W celu przeciwdziałania występowaniu tych zjawisk Redakcja wymaga od poszczególnych autorów ujawnienia wkładu w powstanie publikacji.
13. Ryciny i tabele powinny być opatrzone tytułami oraz źródłami, z którego pochodzą (np. adres internetowy z podaniem daty dostępu). Ich liczbę należy ograniczyć do minimum niezbędnego dla zrozumienia tekstu. Podpisy pod rycinami oraz opisy tabel powinny być sporządzone w języku polskim lub angielskim, a numery zapisane cyframi arabskimi. Rozdzielczość zdjęć powinna wynosić 300 dpi. Ryciny i fotografie należy lokalizować w tekście za pomocą podpisów, a wszelkie materiały graficzne załączać osobno (nie w tekście).
14. Autor składając tekst do publikacji oświadcza, że przesłany tekst jest jego autorstwa i przysługują mu w pełni (wyłączne) osobiste i majątkowe prawa autorskie do tekstu. Autor oświadcza również, że ma prawo do dysponowania umieszczonymi przez niego w utworze materiałami takimi, jak np. ryciny, grafiki, wykresy itp., oraz że ich wykorzystanie w dziele nie narusza praw osób trzecich.
15. Odsyłacze do prac przywoływanych w tekście oraz bibliografia powinny zostać sporządzone zgodnie ze standardami systemu APA (American Psychological Association), wersją szóstą:

## REGULAMIN publikowania prac w „Problemach Kryminalistyki”

**a) odsyłacze do przywoływanych prac** – w przypadku powoływania się na prace innych autorów zawsze należy podać nazwisko autora/ autorów oraz rok publikacji.

Przykłady:

– **jeden autor:**

Według Malinowskiego (2015)...

W słowniku języka polskiego (Doroszewski, 1961)...

– **dwóch autorów:**

Według Widackiego i Dukaty (2015)...

W badaniach poligraficznych stwierdza się (Widacki, Dukata, 2015)...

– **od trzech do pięciu autorów** – wszystkie nazwiska podajemy wyłącznie za pierwszym razem powoływania się na daną pracę w tekście, w kolejnych odsyłaczach podajemy wyłącznie nazwisko pierwszego autora oraz skrót „i in.”.

Jak w swoim artykule wykazali Bajerlein, Wojterska, Grewling i Kokociński (2015)...

We wspomnianym wyżej artykule Bajerlein i in. (2015) wykazali....

Jak wykazały badania (Bajerlein i in., 2015)...

– **sześciu autorów i więcej** – należy podać nazwisko tylko pierwszego autora, dodając skrót „i in.” oraz rok (za każdym razem – zarówno dla pierwszego, jak i następnym odsyłaczy).

**b) dosłowne cytowania** – jeśli w pracy pojawia się dosłownie cytowany fragment tekstu, powinien on zaczynać się i kończyć cudzysłowem, a bezpośrednio za cytatem należy podać źródło cytatu z numerami stron:

„.....” (Kowalski, 2016, s. 31)...

**c) bibliografię należy zredagować alfabetycznie w oparciu o podane przykłady:**

Arntzen, F. (1989). *Psychologia zeznań świadków*. Warszawa: Państwowe Wydawnictwo Naukowe.

Buller, D.B., Burgoon, J.K. (1996). Interpersonal Deception Theory. *Communication Theory*, 6(3), 203–242. DOI: 10.1111/j.1468-2885.1996.tb00127.x

Sweetser, E.E. (1987). The definition of lie: An examination of the folks models underlying a semantic prototype. W: D. Holland (red.), *Cultural Models in Language and Thought*. New York: Cambridge University Press.

Widacki, J. (red.). (2012). *Kryminalistyka*. Warszawa: C.H. Beck.

16. Po zakwalifikowaniu pracy do publikacji z Autorem zostaje zawarta umowa o przeniesieniu na Redakcję autorskich praw majątkowych.
17. Za publikację w kwartalniku Autorowi nie przysługuje wynagrodzenie.
18. Wersją pierwotną (referencyjną) czasopisma jest wydanie papierowe. „Problemy Kryminalistyki” są dostępne także na stronie internetowej wydawnictwa.

## TERMS AND CONDITIONS of publishing in “Issues of Forensic Science” /“Problemy Kryminalistyki”/

1. The editorial board of “Issues of Forensic Science”, referred to as “the Editorial board” accepts only original articles of theoretical and experimental content in form of synthetic, analytical and casuistic work that covers forensic science and related areas as well as reviews of scientific monographic works of one or more authors which are later referred to as “the Author”. The submitted works can neither be published in any other form, nor in the reviewing process by other publishers simultaneously.
2. The editorial board does not return the articles to its author. The board reserves the right to shortening and adjusting of the text as well as to modifying its titles and subtitles.
3. The board reserves the right to dismiss the submitted work without detailed reasons.
4. The works written against the present terms and conditions will not be published.
5. The works are to be send to the e-mail address: [clkpk@policja.gov.pl](mailto:clkpk@policja.gov.pl) or provided to the board on a digital data carrier such as CD, DVD or USB drive (the carriers are not to be returned to the author by the board).
6. The number of characters in submitted text should not exceed 40 000 including figures, tables, abstract and bibliography. The text should be formatted in Times New Roman, size 12, spacing of 1,5 lines, margins of 2,5 cm width on both sides of the document. The contents are to be made with the basic formatting, with no highlights.
7. Every submitted article is to be accompanied by an abstract (max. 150 words) and 3 to 7 key words.
8. The submitted article should be written in Polish or English.
9. The submitted article cannot be signed – it cannot bear any signs that may lead to identification of the author of the work. This data (first and last name(s) of the author(s), title of the publication, name of the author’s employing institution, their position, address, phone number, e-mail, and, if required, information regarding the funding of the conducted research) should be enclosed in a separate file.
10. The submitted articles will be subject to review by two reviewers in accordance with double-blind review principle, which entails that both reviewers and author(s) are unaware of each other’s identities. Reviewers are selected from outside the institution to which the author is affiliated (authors are affiliated). Once a year, in the publishing house’s website, the last names of our reviewers will be published.
11. If the article receives positive feedback from the editor, but it is suggested that modifications and corrections be introduced, the author is obliged to answer the comments and consider introducing the suggested modifications.
12. The editorial office has adopted and applies the Code of Publication Ethics. The Publisher, Authors and Reviewers are obliged to comply with the principles of ethics, in particular the principles of responsibility, integrity, transparency and confidentiality. The board recalls that ghostwriting and guest authorship are manifestation of scientific unreliability, therefore all detected incidents will be revealed and documented, including notification of relevant parties (the institutions that employ authors, scientific societies, association of scientific editors etc.). In order to counteract occurrence of such incidents, the Editorial Board requires from all the authors revealing the contributions to creation of their works.
13. Figures and Tables should be provided with titles and information on their sources (e.g. website address with a date of accessing). Their number would be limited to a minimum necessary to understand the text. Captions under Figures and descriptions of Tables should be made in Polish or English language; numbers of Figures and Tables should be expressed in Arabic digits. Photographs ought to have 300 dpi resolution. The location of Figures and Photographs in the text should be marked by the captions and all graphic materials should be delivered in separate appendices (not in the text).
14. Upon submitting a text for publication the Author declares that the text sent is of his/her authorship and he/she possesses full (exclusive) personal and property right to it. The author also declares, that he has the right to dispose of materials placed in the work, such as: Figures, graphics, Tables, etc., and that their use in the work does not infringe the rights of third parties.
15. References to other works in the text and Bibliography should be made according to APA (American Psychological Association) system, version 6:

## TERMS AND CONDITIONS of publishing in “Issues of Forensic Science” /“Problemy Kryminalistyki”/

- a) references to other works** – in case of referring to works of other authors the name of author/authors and year of publishing should always be given.

Examples:

– **one author:**

According to Malinowski (2015)...

In Polish Language Dictionary (Doroszewski, 1961)

– **two authors:**

According to Widacki and Dukata (2015)...

It is stated in Polygraph examinations (Widacki, Dukata, 2015)...

- **three to five authors** – all the names are given only in the first instance of referring to a given work in the text; in subsequent references exclusively the name of first author and an abbreviation “et al.”

As Bajerlein, Wojterska, Grewling and Kokociński (2015) demonstrated in their article...

In the article mentioned above Bajerlein et al. (2015) demonstrated...

As research has shown (Bajerlein et al., 2015)...

- **six and more authors** – the name of the first author followed by the abbreviation “and others” as well as the year should be provided each time for the first and subsequent links.

- b) direct quotations** – if a direct quotation from another work is included in the text, it should start and end with quotation marks and directly after the quotation the source with page numbers should be given:

“.....” (Kowalski, 2016, p. 31)

- c) Bibliography should be made in the alphabetical order basing on the following examples:**

Arntzen, F. (1989). *Psychologia zeznań świadków*. Warsaw: Państwowe Wydawnictwo Naukowe.

Buller, D.B., Burgoon, J.K. (1996). Interpersonal Deception Theory. *Communication Theory*, 6(3), 203–242. DOI: 10.1111/j.1468-2885.1996.tb00127.x

Sweetser, E.E. (1987). The definition of lie: An examination of the folks models underlying a semantic prototype. W: D. Holland (ed.), *Cultural Models in Language and Thought*. New York: Cambridge University Press.

Widacki, J. (ed.). (2012). *Kryminalistyka*. Warszawa: C.H. Beck.

16. Upon approval of the work for publication an Agreement on Transfer of Copyright to the Editor is concluded with the author.
17. The author is not entitled to a remuneration for the publication in the Quarterly.
18. The primary (referential) version of the Quarterly is the hard copy. “Issues of Forensic Science” is also available on the Editorial House’s website.