 https://doi.org/10.34836/pk.2021.312.4

Analiza strukturalno-spektroskopowa filmów DFO/PVA jako potencjalnych materiałów stosowanych podczas ujawniania śladów linii papilarnych na podłożach niechłonnych

Paulina Zygadło[1], **Aneta Lewkowicz**[1*]

[1] Uniwersytet Gdański

* autor korespondencyjny: aneta.lewkowicz@ug.edu.pl

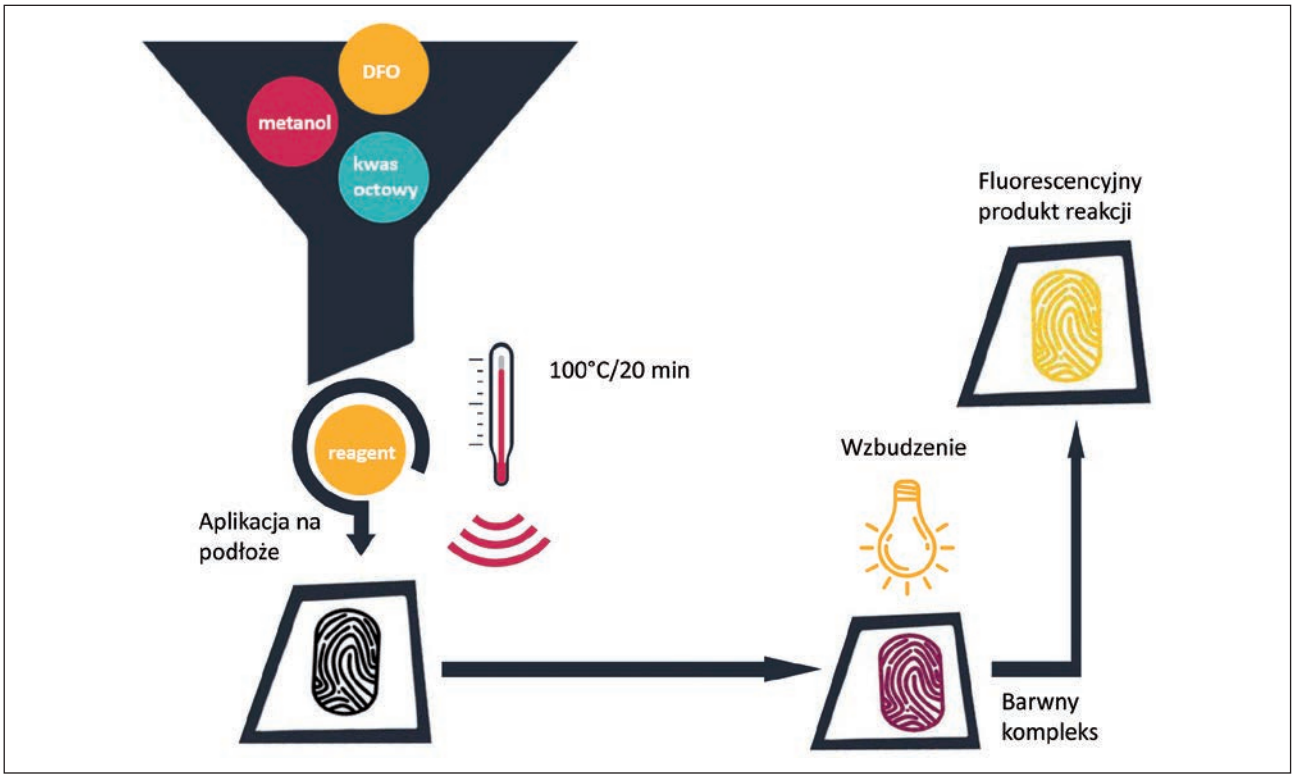
Streszczenie

1,8-diazafluoren-9-on (DFO) to czuła sonda luminescencyjna ukierunkowana na α-aminokwasy. W badaniu wykorzystano jego właściwości fizykochemiczne do utworzenia polimerowych folii DFO/PVA. W rezultacie otrzymano materiały, w których DFO jest stabilny i reaktywny. Analiza spektroskopowa utworzonych filmów wykazała, że folie o najwyższym stężeniu DFO odznaczają się największą reaktywnością. Otrzymano nowoczesne materiały w postaci cienkich filmów DFO/PVA z potencjalnym zastosowaniem do ujawniania śladów linii papilarnych na podłożach niechłonnych.

Słowa kluczowe: folia polimerowa DFO/PVA, fluorescencja, linie papilarne

Wstęp

1,8-diazafluoren-9-on jest aromatycznym związkiem organicznym, który tworzy kompleks z α-aminokwasami, dając fluorescencyjny produkt reakcji (Petrovskaia i in., 2001). Dzięki temu od lat 90. XX wieku używany jest jako reagent do ujawniania śladów linii papilarnych, przeznaczony na podłoża chłonne (D'Elia i in., 2015; Friesen, 2015). Roztwór DFO tworzony jest na bazie metanolu i kwasu octowego, ponieważ wzmacniają one efekt działania 1,8-diazafluoren-9-onu na ślady linii papilarnych (Costa Conn i in., 2001). Do wytworzenia roztworu DFO stosuje się bardzo wysokie stężenia



Ryc. 1. Procedura kryminalistyczna ujawniania śladów linii papilarnych za pomocą DFO.

1,8-diazafluoren-9-onu w ilości ok. 0,25g/L (tj. ok. 10^{-1} [mol/dm^3]) (Bleay i in., 2018). Reagent aplikuje się, spryskując ślad lub zanurzając w nim badane podłoże (Ramotowski, 2013), a następnie ogrzewa w temperaturze ok. 100°C w czasie nieprzekraczającym 20 minut (Browarny, 2014) – rycina 1.

DFO jest cząsteczką o niskiej wydajności kwantowej fluorescencji (Lewkowicz i in., 2019). Jednocześnie molekuła ta jest wysoce reaktywna oraz selektywna dla α-aminokwasów, w rezultacie daje produkt o wysokiej wydajności kwantowej fluorescencji, co jest głównym celem obecnie stosowanej procedury kryminalistycznej służącej do ujawniania śladów linii papilarnych. Używanie bardzo wysokich stężeń głównego reagenta DFO może jednak skutkować obserwacją fluorescencji pochodzącej od asocjatów 1,8-diazafluoren-9-onu, a nie od kompleksu DFO z α-aminokwasami. Zjawisko to obserwowano już wcześniej wśród innych molekuł zdolnych do luminescencji, np. Rodaminy 6G (Lewkowicz i in., 2012; Lewkowicz i in., 2014). W przypadku ketonów aromatycznych wcześniejsze doniesienia literaturowe wskazują również na obecność dimerów tych molekuł, chociażby na skutek cykloaddycji do wiązania C=C w pierścieniu aromatycznym. Zjawisko przedstawiono jako efekt oddziaływania ketonów w stanie trypletowym, przykładowo w procesie dimeryzacji cykloheksanonu uczestniczy cząsteczka w stanie $^3(\pi, \pi^*)$ (Lam, Valentine, Hammond, 1967; Inhülsen, Kopf, Margaretha, 2008; Parthasarathy, Samanta, Ramamurthy, 2013). W niniejszym badaniu umieszczono molekułę DFO w innym nośniku niż obecnie stosowane w daktyloskopii roztwory. Materiałem, który może stanowić obiecującą matrycę dla DFO, jest alkohol poliwinylowy (PVA). PVA jest bezwonnym, bezbarwnym oraz nietoksycznym polimerem. Ma właściwości higroskopijne oraz jest materiałem biokompatybilnym i biodegradowalnym, dzięki czemu jest szeroko stosowany w medycynie (Yang i in., 2021; Liu i in., 2014). Dzięki zdolności do absorbowania wody utworzone z PVA filmy pęcznieją, co umożliwia uwolnienie zawartej w nich molekuły do środowiska (Yang i in., 2021); prawdopodobnie ten sam mechanizm pozwala na pochłonięcie cząsteczek ze środowiska do wewnątrz polimeru.

Cel badań

Celem badań jest otrzymanie materiałów polimerowych o wysokiej trwałości i selektywności względem α-aminokwasów z możliwością potencjalnego zastosowania do podłoży zarówno chłonnych, jak i niechłonnych podczas ujawniania śladów linii papilarnych.

Materiały i metody

Sprzęt, wyposażenie i odczynniki chemiczne

Wszystkie odczynniki chemiczne użyte w badaniu były czystości analitycznej. Czysty spektroskopowo (zawartość barwnika 99%) 1,8-diazafluoren-9-on, alkohol poliwinylowy oraz glicynę zakupiono od Aldrich (Sigma-Aldrich Monachium, Niemcy). Wodę dejonizowaną pozyskano z systemu HydroLab.

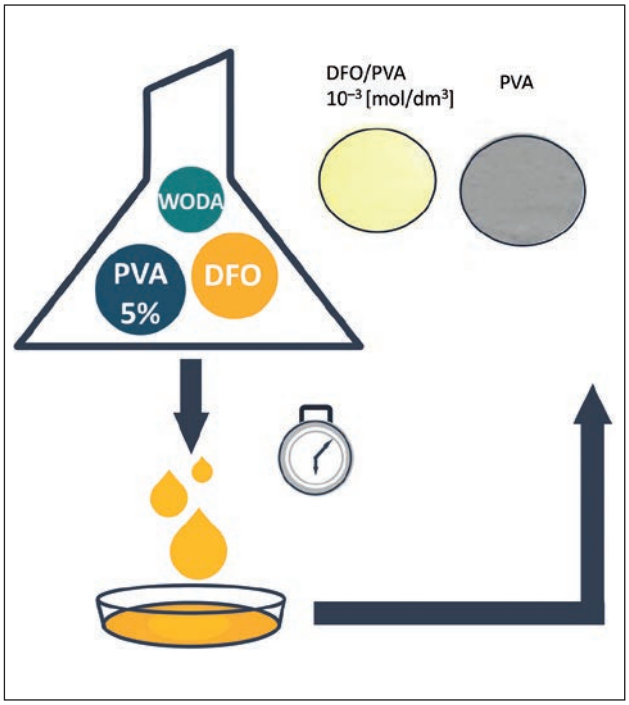
Widma Ramana uzyskano wraz ze zintegrowanym konfokalnym systemem mikro-Raman z LabRam Aramis (Horiba Jobin Yvon) Spektrometr 460 mm. Źródłem wzbudzenia jest laser HeNe półprzewodnikowy pompowany diodą (DPSS), emitujący czerwone światło przy 632 nm z mocą 50 mW. Widma absorpcji mierzono za pomocą spektrofotometru Shimadzu UVmini-1240. Fluorescencję wzbudzano za pomocą lampy UV UVITEC LF-206.LS LAMP 365/254NM 1X6W 230V EU oraz za pomocą oświetlacza, przy długości fali wzbudzenia 465 nm. Widma emisji uzyskano za pomocą spektrofluorymetru Horiba Jobin Yvon, model FluoroMax4TCSPC.

Przygotowanie folii PVA z zainkorporowanym DFO

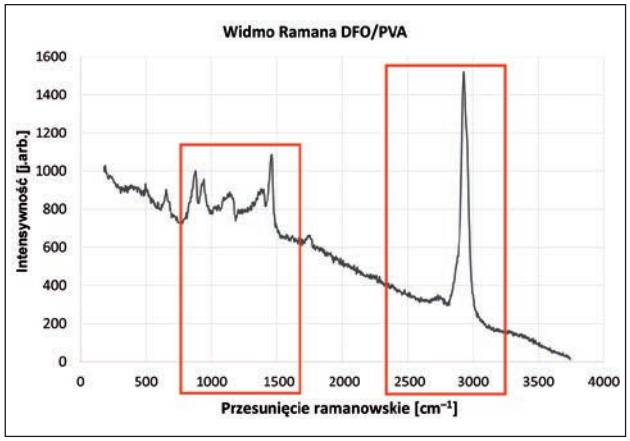
Na rycinie 2 przedstawiono schemat otrzymywania filmów polimerowych DFO/PVA. Filmy te powstały w procesie polimeryzacji w temperaturze pokojowej i ciśnieniu atmosferycznym. PVA i DFO rozpuszczono w wodzie demineralizowanej. Otrzymano następujące stężenia DFO w filmach PVA: 10^{-5}, 10^{-4}, 10^{-3}, $5 \cdot 10^{-3}$ [mol/dm^3].

Analiza strukturalna

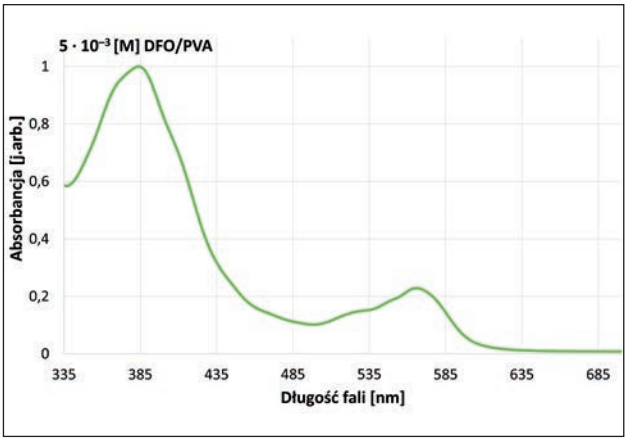
Rycina 3 pokazuje widmo Ramana dla folii PVA. Położenie pików ramanowskich na widmie jest charakterystyczne dla struktury tego polimeru, występują one pomiędzy 750–1500 cm^{-1} oraz 2500–3500 cm^{-1} (Publicspectra.com; Thomas, Stuart, 1997).



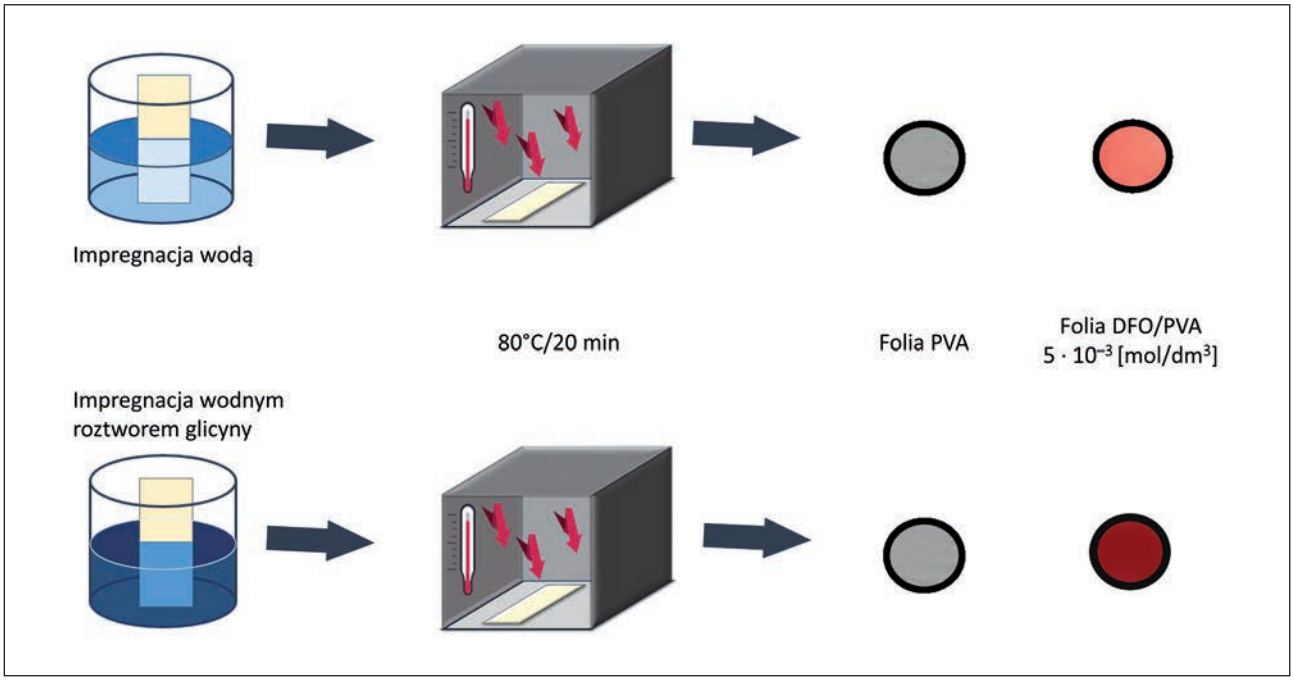
Ryc. 2. Schemat otrzymywania filmów polimerowych DFO/PVA.



Ryc. 3. Widmo Ramana folii DFO/PVA.



Ryc. 4. Widmo absorpcji folii DFO/PVA dla $c_{DFO} = 5 \cdot 10^{-3}$ [mol/dm³].



Ryc. 5. Procedura impregnacji wodnym roztworem glicyny folii polimerowych DFO/PVA.

Pomiaru widm absorpcji folii DFO/PVA dokonano w temperaturze pokojowej i ciśnieniu atmosferycznym. Rycina 4 przedstawia widmo absorpcji dla najwyższego stężenia DFO w folii PVA i stanowi potwierdzenie obecności 1,8-diazafluoren-9-onu w matrycy PVA – charakterystyczne pasmo absorpcji z maksimum przy długości fali 385 nm. W przypadku najwyższych stężeń DFO (10^{-3} oraz $5 \cdot 10^{-3}$ [mol/dm³]) zaobserwowano występowanie drugiego pasma absorpcji z maksimum przy długości fali 570 nm. Pojawienie się dodatkowego pasma potwierdza powstawanie nowych struktur chemicznych, prawdopodobnie są to tzw. agregaty DFO.

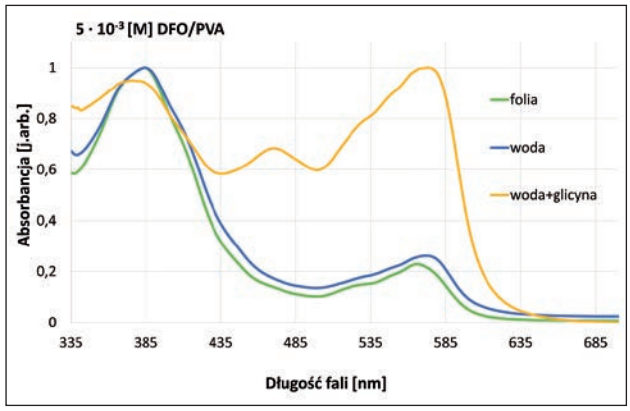
Impregnacja folii DFO/PVA

Folie DFO/PVA impregnowano w dwóch roztworach: woda (ślepa próba) oraz wodny roztwór glicyny 10^{-4} [mol/dm³]. Każdą z próbek zanurzano na 30 sekund w roztworze, a następnie wygrzewano w piecu – rycina 5. Folie DFO/PVA o wysokich stężeniach, tj. 10^{-3} oraz $5 \cdot 10^{-3}$ [mol/dm³], które zostały zaimpregnowane wodnym roztworem glicyny, zmieniły kolor na purpurowy.

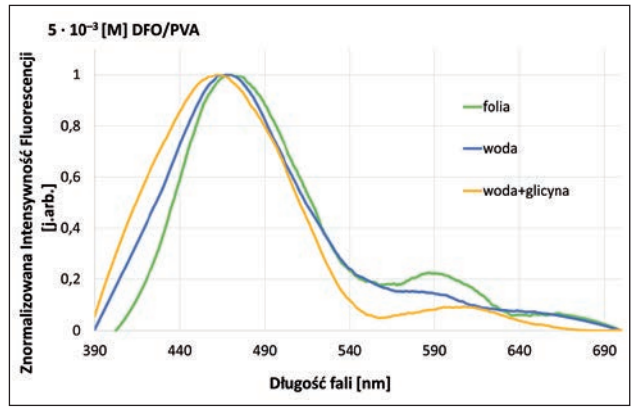
Analiza spektroskopowa

Po impregnacji dokonano pomiaru widm absorpcji folii DFO/PVA w zakresie spektralnym 250–700 nm, a następnie porównania widm absorpcji folii o najwyższym stężeniu $5 \cdot 10^{-3}$ [mol/dm³] impregnowanych w wodzie, w wodnym roztworze glicyny 10^{-4} [mol/dm³], a także niepoddanych impregnacji – rycina 6.

Na widmie absorpcji ponownie widoczne są dwa pasma absorpcji dla próbki niepoddanej impregnacji



Ryc. 6. Widmo absorpcji folii DFO/PVA dla $c_{DFO} = 5 \cdot 10^{-3}$ [mol/dm^3].

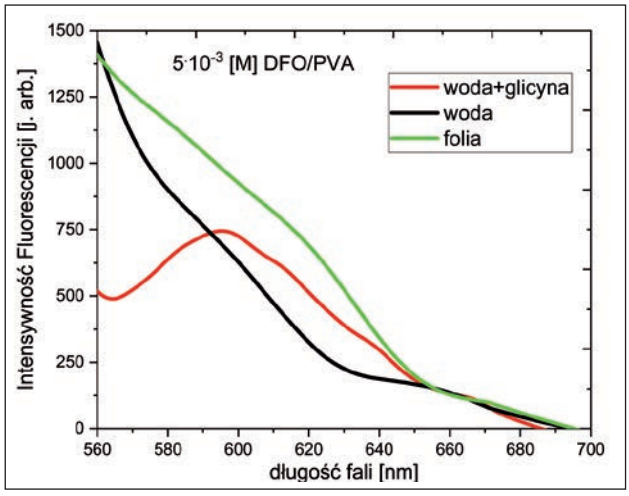


Ryc. 7. Widmo fluorescencji folii DFO/PVA dla najwyższych stężeń $5 \cdot 10^{-3}$ [mol/dm^3] przy wzbudzeniu promieniowaniem o długości fali 380 nm.

oraz impregnowanej wodą. W próbce impregnowanej glicyną widoczne są trzy pasma. Dwa skrajne pasma absorpcji są wspólne dla wszystkich folii: pierwsze z maksimum przy długości fali 385 nm oraz ostatnie z maksimum przy długości fali ok. 570 nm. Środkowe pasmo absorpcji charakterystyczne jest jedynie dla próbki impregnowanej wodnym roztworem glicyny z maksimum przy długości fali 470 nm – specyficzne dla kompleksu DFO z α-aminokwasami.

Próbki otrzymane po impregnacji oświetlono lampą UV: 365 nm oraz oświetlaczem 465 nm. Folie DFO/PVA zaimpregnowane wodnym roztworem glicyny wyświecają dla stężeń 10^{-4}, 10^{-3} oraz $5 \cdot 10^{-3}$ [mol/dm^3]. Fluorescencja była widoczna również dla stężenia $5 \cdot 10^{-3}$ [mol/dm^3] DFO/PVA po zaimpregnowaniu foli wodą.

W foliach DFO/PVA po impregnacji wodnym roztworem glicyny wraz ze wzrostem stężenia rośnie intensywność emisji – tabela 1 i 2. Porównując filmy dla stężenia $5 \cdot 10^{-3}$ [mol/dm^3] DFO/PVA, obserwuje się zbliżoną emisję mimo różnej impregnacji. Cechą nieznacznie różnicującą folie jest barwa emitowanego światła oraz intensywność emisji badanych filmów. W próbkach wzbudzanych przy 365 nm wraz ze wzrostem stężenia pojawia się barwa żółtopomarańczowa. Folia $5 \cdot 10^{-3}$ [mol/dm^3] DFO/PVA impregnowana w wodzie wyświeca na żółto, podczas gdy folia impregnowana w glicynie na pomarańczowo. Natomiast dla próbek o najwyższym stężeniu przy wzbudzeniu promieniowaniem o długości fali 465 nm barwa jest bardziej intensywna niż przy wzbudzeniu promieniowaniem o długości fali 365 nm – pomarańczoworóżowa przy impregnacji wodnym roztworem glicyny.

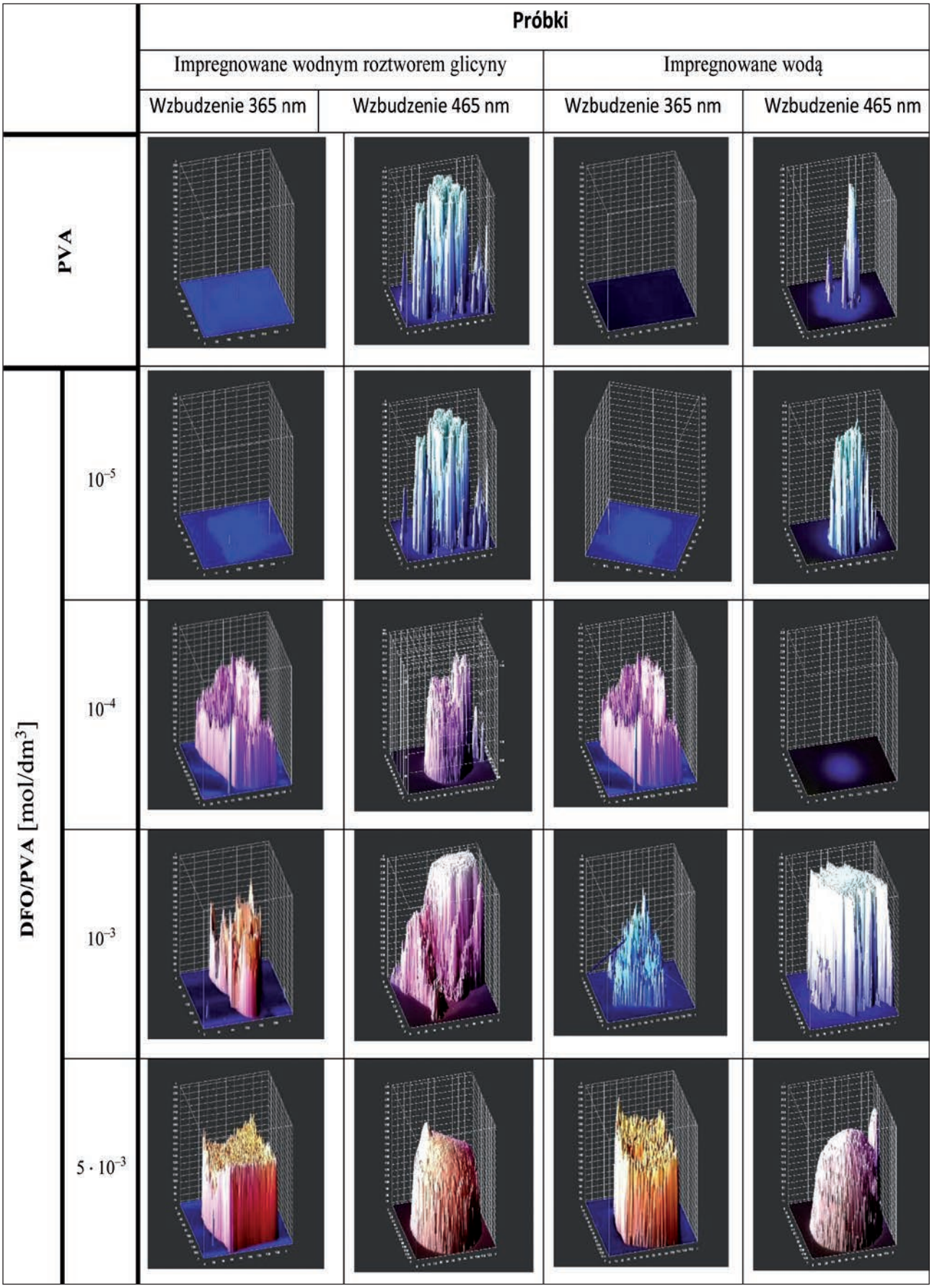


Ryc. 8. Widmo fluorescencji folii DFO/PVA dla najwyższego stężenia $5 \cdot 10^{-3}$ [mol/dm^3] przy wzbudzeniu promieniowaniem o długości fali 470 nm.

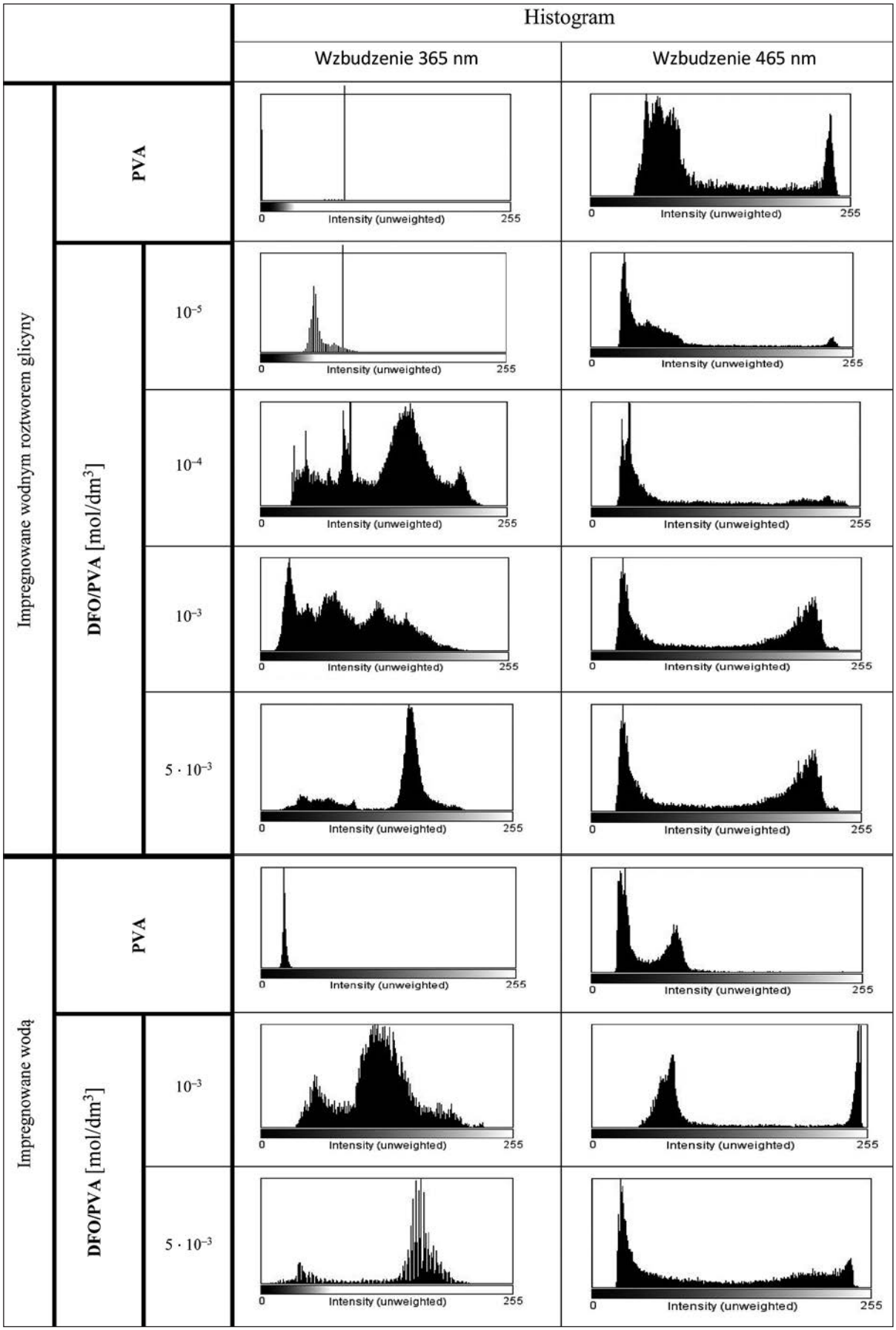
Na rycinie 7 zestawiono widma fluorescencji filmów $5 \cdot 10^{-3}$ [mol/dm^3] DFO/PVA dla poszczególnych impregnacji. Na widmie widoczne są dwa pasma fluorescencji. Maksimum pierwszego pasma fluorescencji znajduje się przy długości fali 460 nm dla impregnacji wodnym roztworem glicyny i przesuwa w stronę długofalową do 470 nm dla pozostałych folii. Nie zaobserwowano istotnych zmian w profilu widmowym fluorescencji dla pierwszego pasma. Drugie pasmo fluorescencji ma maksimum przy długości fali ok. 590–613 nm, najlepiej widoczne jest dla folii DFO/PVA niepoddanej impregnacji.

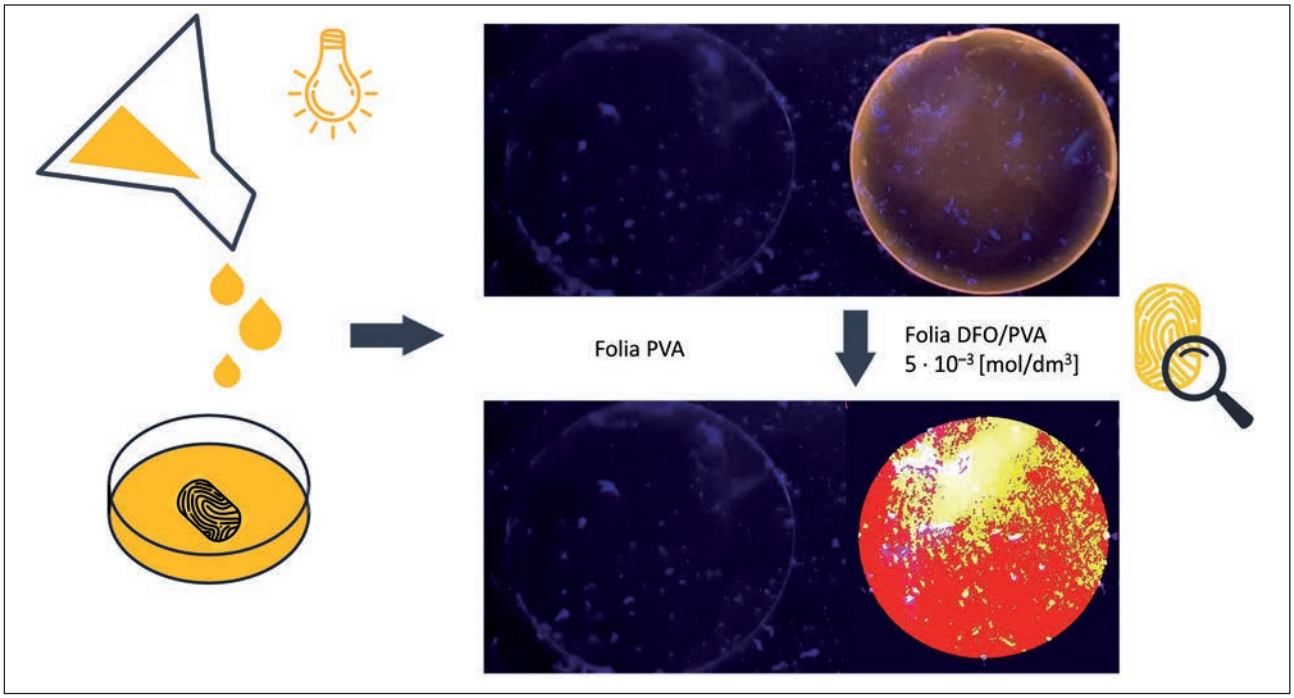
Zgodnie z otrzymanym widmem absorpcji fluorescencję folii zmierzono przy wzbudzeniu promieniowaniem o długości fali 470 nm. Pasmo absorpcji o tym maksimum jest pasmem różnicującym struktury kompleksu DFO z aminokwasem i potencjalnymi agregatami. Na rycinie 8 zestawiono widma fluorescencji dla poszczególnych impregnacji. Na widmie widoczne są trzy pasma fluorescencji, z czego tylko jedno najlepiej wykształcone jest dla folii impregnowanej wodnym roztworem glicyny z maksimum fluorescencji pasma przy długości fali 606 nm. Struktura pozostałych pasm fluorescencji pochodzących od filmów bez impregnacji oraz po impregnacji wodą jest bardzo słabo zarysowana i pochodzi przede wszystkim od DFO z niewielkim wkładem po stronie długofalowej pasma fluorescencji położonego spektralnie w tym samym miejscu co kompleks DFO z glicyną.

Tab. 1. Zestawienie próbek DFO/PVA po impregnacji – wskazanie różnic w emisji przy wzbudzeniu 365 nm i 465 nm.



Tab. 2. Zestawienie histogramów próbek DFO/PVA po impregnacji – wskazanie różnic w emisji przy wzbudzeniu promieniowaniem o długości fali 365 nm i 465 nm.





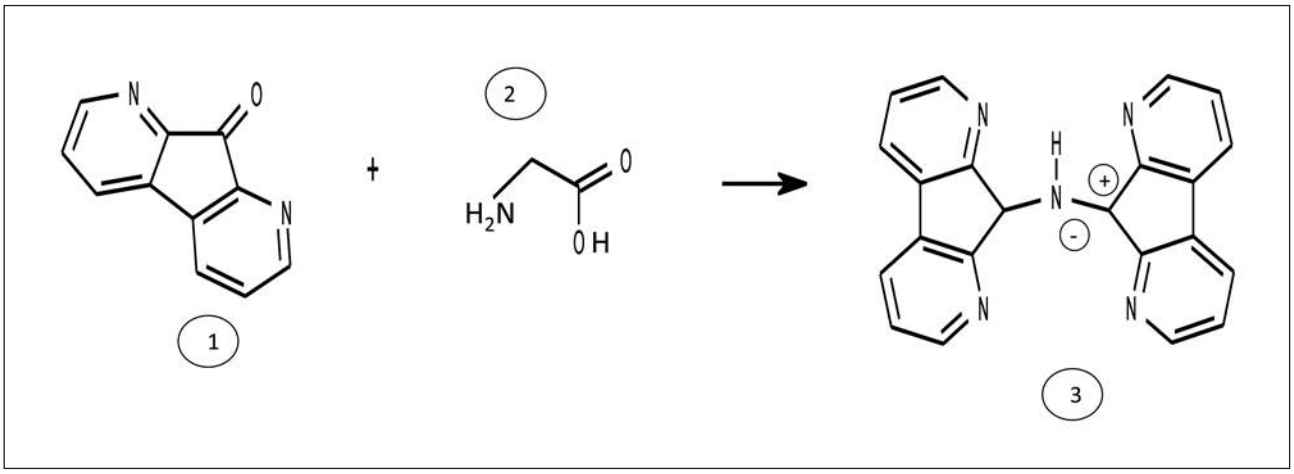
Ryc. 9. Ślady linii papilarnych ujawnione za pomocą folii DFO/PVA, przy wzbudzeniu promieniowaniem o długości fali 365 nm.

Podsumowanie i wnioski

Zmiana barwy oraz fluorescencja folii DFO/PVA po impregnacji wodnym roztworem glicyny wskazuje na utworzenie kompleksu DFO z aminokwasem. Zmiany te nastąpiły jedynie w trzech próbkach, a stężeniem granicznym DFO/PVA, dla którego zachodzi reakcja, jest 10^{-4} [mol/dm^3]. Brak reakcji w próbce o najniższym stężeniu 10^{-5} [mol/dm^3] DFO/PVA. Ma to teoretyczne odwzorowanie w zaleceniach procedury kryminalistycznej, która operuje na wysokich stężeniach 1,8-diazafluoren-9-onu w roztworze. Najwyższe stężenie DFO wykorzystane w badaniu wynosiło 0,09 g/L ($5 \cdot 10^{-3}$ [mol/dm^3] DFO/PVA). Procedury kryminalistyczne podają ilość DFO >0,2 g/L (10^{-1} [mol/dm^3]) jako niezbędną do zajścia reakcji między DFO a aminokwasem. To prawie dwukrotnie większa ilość 1,8-diazafluoren-9-onu niż użyta w niniejszym badaniu. Najniższe stężenie, w którym zaobserwowano fluorescencyjny kompleks, wynosi ok. 0,0018 g/L (10^{-4} [mol/dm^3] DFO/PVA). Oznacza to, że stężenie potrzebne do utworzenia kompleksu z α-aminokwasami jest dużo niższe niż obecnie proponowane.

Podczas przygotowywania folii roztwór DFO/PVA o stężeniu 10^{-3} [mol/dm^3] wylano na ślady linii papilarnych odciśnięte na plastikowej powierzchni szalki Petriego. W procesie polimeryzacji uzyskano film trwale związany z czytelnym luminescencyjnym śladem daktyloskopijnym znajdującym się na niechłonnym podłożu. Folia DFO/PVA (ryc. 9) potwierdza zajście reakcji DFO z α-aminokwasami. Fluorescencję próbek zmierzono przy wzbudzeniu promieniowaniem o długości fali 365 nm oraz 380 nm; te długości fali powinny doprowadzić jedynie do obserwacji fluorescencji DFO. Wedle założeń teoretycznych mają więc wyświecać wszystkie próbki zawierające 1,8-diazafluoren-9-on niezależnie od sposobu impregnacji. Po użyciu oświetlacza 365 nm nie wszystkie folie DFO/PVA wykazały zdolność do luminescencji. Jednak ta długość fali okazała się wystarczająca do zaobserwowania emisji w przypadku próbek zawierających kompleks DFO z α-aminokwasami (tabela 1 i 2; rycina 9) oraz próbek $5 \cdot 10^{-3}$ [mol/dm^3] DFO/PVA impregnowanych wodą. Natomiast po użyciu spektrofluorymetru i przy wzbudzeniu promieniowaniem o długości fali 380 nm zarejestrowano widma fluorescencji dla wszystkich próbek zawierających 1,8-diazafluoren-9-on bez względu na rodzaj impregnacji.

Badane folie różnicuje widmo absorpcji ukazane na rycinie 6, gdzie charakterystyczne pasmo absorpcji z maksimum przy długości fali 470 nm w próbkach impregnowanych wodnym roztworem glicyny wskazuje na utworzenie kompleksu DFO–α-aminokwas, który nie występuje w pozostałych filmach DFO/PVA. Dodatkowo wszystkie folie niezależnie od sposobu impregnacji cechuje zbliżona struktura widm fluorescencji przy wzbudzeniu promieniowaniem o długości fali 380 nm (ryc. 6), natomiast dla wzbudzenia promieniowaniem o długości fali 470 nm zaobserwowano dobrze wykształcone pasmo fluorescencji jedynie w odniesieniu do próbki impregnowanej wodnym roztworem glicyny – rycina 8. Wzbudzenie folii oświetlaczem 465 nm skutkuje emisją dla DFO/PVA od 10^{-4} [mol/dm^3] do $5 \cdot 10^{-3}$ [mol/dm^3] po impregnacji wodnym roztworem



Ryc. 10. Reakcja DFO (1) z α-aminokwasem (2).

glicyny. Fluorescencyjna odpowiedź dla powyższego wzbudzenia widoczna jest również dla $5 \cdot 10^{-3}$ [mol/dm^3] DFO/PVA impregnowanej wodą – tabela 1. Wyświecanie filmów, na których brak jest kompleksu DFO–α-aminokwas, $5 \cdot 10^{-3}$ [mol/dm^3] DFO/PVA impregnowanych wodą przy wzbudzeniu promieniowaniem o długości fali 465 nm (tabela 1 i 2), a także powstawanie dodatkowych pasm przesuniętych w stronę długofalową na widmie absorpcji (rycina 6), sugeruje występowanie asocjatów 1,8-diazafluoren-9-onu w foliach o wysokich stężeniach. Dodatkowo tworzenie się agregatów DFO w matrycy PVA potwierdza intensywna fluorescencja oraz zbliżona barwa emitowanego światła z całej powierzchni próbek o najwyższym stężeniu $5 \cdot 10^{-3}$ [mol/dm^3] DFO/PVA wzbudzanych promieniowaniem o długości fali 365 nm. Zjawisko to potwierdzają również tożsame widma fluorescencji $5 \cdot 10^{-3}$ [mol/dm^3] DFO/PVA przy wzbudzeniu promieniowaniem o długości fali 380 nm bez względu na impregnację.

1,8-diazafluoren-9-on zawarty w matrycach utworzonych z PVA jest stabilny i pełni funkcję sondy luminescencyjnej dla α-aminokwasów. Impregnacja folii DFO/PVA w wodnym roztworze glicyny umożliwia utworzenie kompleksu DFO–glicyna (Lewkowicz i in., 2020; Wilkinson, 2000; Kołek-Kaczanowska, Kreczko, Maćkiewicz, 2014) – rycina 10. Należy jednak podkreślić, że jedynie folie PVA o najwyższych stężeniach DFO wykazują odpowiednio wysoką reaktywność oraz pozwalają zaobserwować okiem nieuzbrojonym utworzenie się kompleksu DFO–α-aminokwas. Otrzymane polimery DFO/PVA są sondami α-aminokwasów, a badania przedstawione w ramach niniejszej pracy mają charakter wstępny z wskazaniem na potencjalne zastosowanie podczas ujawniania śladów linii papilarnych.

Źródło rycin i tabel: autorzy

Bibliografia

1. Bleay, S.M., Croxton, R.S., de Puit, M. (2018). *Fingerprint Development Techniques. Theory and Application*. Hoboken NJ: Wiley.
2. Browarny, K. (2014). Metody i środki wykorzystywane przez specjalistów w praktyce dochodzeniowo-śledczej. W: M. Szostak, I. Dembowska (red.), *Innowacyjne metody wykrywania sprawców przestępstw. Materiały z konferencji*. Wrocław: Prawnicza i Ekonomiczna Biblioteka Cyfrowa, Wydział Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego
3. Costa Conn, C., Ramsay, G., Roux, C., Lennard, C. (2001). The effect of metal salt treatment on the photoluminescence of DFO-treated fingerprints. *Forensic Science International*, *116*.
4. D'Elia, V., Materazzi, S., Iuliano, G., Niola, L. (2015). Evaluation and comparison of 1,2-indanedione and 1,8-diazafluoren-9-one solutions for the enhancement of latent fingerprints on porous surfaces. *Forensic Science International*, *254*.
5. Friesen, J.B. (2015). Forensic chemistry: The revelation of latent fingerprints. *Journal of Chemical Education*, *92.*
6. Inhülsen, I., Kopf, J., Margaretha, P. (2008). Photocycloaddition reactions of 5,5-Dimethyl-3-(3--methylbut-3-en-1-ynyl)cyclohex-2-en-1-one. *Helvetica Chimica Acta*, *91*.
7. Kołek-Kaczanowska, E.K., Kreczko, J., Maćkiewicz, Z. (2014). Metody wykorzystywane do wizualizacji śladów linii papilarnych. *Wiadomości Chemiczne*, *68.*
8. Lam, E., Valentine, D., Hammond, G. (1967). Mechanisms of photochemical reactions in solution. XLIV. Photodimerization of cyclohexenone. *Journal of the American Chemical Society*, *89*.
9. Lewkowicz, A. i in. (2012). Concentration-dependent fluorescence properties of Rhodamine 6G in titanium dioxide and silicon dioxide nanolayers. *The Journal of Physical Chemistry C*, *116.*

10. Lewkowicz, A. i in. (2014). Aggregation of Rhodamine 6G in titanium dioxide nanolayers and bulk xerogels. *Optical Materials*, *36*(10).
11. Lewkowicz, A., Baranowska, K., Bojarski, P., Józefowicz, M. (2019). Solvent dependent spectroscopic properties of fingerprint reagent – 1,8-diazafluoren-9-one. *Journal of Molecular Liquids*, *285*.
12. Lewkowicz, A. i in. (2020). The luminescence of 1,8-diazafluoren-9-one/titanium dioxide composite thin films for optical application. *Materials*, *13.*
13. Liu, P., Chen, W., Liu, Y., Bai, S., Wang, Q. (2014). Thermal melt processing to prepare halogen-free flame retardant poly(vinyl alcohol). *Polymer Degradation and Stability*, *109*.
14. Parthasarathy, A., Samanta, S., Ramamurthy, V. (2013). Photodimerization of hydrophobic guests within a water-soluble nanocapsule. *Research on Chemical Intermediates*, *39.*
15. Petrovskaia, O. i in. (2001). Investigations of the reaction mechanisms of 1,2-indanediones with amino acids. *The Journal of Organic Chemistry*, *66.*
16. Ramotowski, R. (red.). (2013). *Lee and Gaensslen's Advances in Fingerprint Technology*, wyd. 3. Boca Raton FL: CRC Press.
17. Thomas, P.S., Stuart, B.H. (1997). A Fourier transform Raman spectroscopy study of water sorption by poly (vinyl alcohol). *Spectrochimica Acta Part A*, *53*.
18. Wilkinson, D. (2000). Study of the reaction mechanism of 1,8-diazafluoren-9-one with the amino acid, L-alanine. *Forensic Science International*, *109*.
19. Yang, W. i in. (2021). Highly transparent PVA/nanolignin composite films with excellent UV shielding, antibacterial and antioxidant performance. *Reactive and Functional Polymers*, *162*.
20. https://publicspectra.com/Raman/Polyvinyl%20alcohol (dostęp: 22.06.2021).

Biometric methods and their application in the Police investigation work

Edyta Kot[1*], Anna Jurga[1], Ewa Kartasińska[1], Ewa Lewandowska[1], Sławomir Paśko[2]

[1] Central Forensic Laboratory of the Police
[2] Warsaw University of Technology
* Corresponding author: edyta.kot@policja.gov.pl

Summary

Biometrics is one of the basic detection techniques used in law enforcement activities on a daily basis. Like other techniques, it is constantly changing. This article aims to provide an overview of what was in the past, what is now, and what will be in the near future. It presents the selected methods of collecting some of the data, as well as the systems used to process them. In addition, practical guidance is provided on how individual biometric data should be collected and, for specific cases, it explains why the data collection procedure is carried out in one way and not another, and what it means for its subsequent processing. As problems sometimes arise during recovery of the material they have been presented together with an overview of the reasons for that. In addition to information on the technical aspects, the article also includes references to legal acts regulating issues related to biometrics.

Key words: biometry, dactyloscopic data, DNA, facial image, RapidHIT, Live Scanner

Introduction

Everybody strongly associates biometrics in its scientific aspect with an image, because the image of a person's face is in fact their "calling card". Face appearance allows recognition of people on a daily basis, identification of their emotions, assessment of their character, age and even health.

There is no definition of a facial image in any of the laws. The colloquial meaning of this word is defined by the PWN Polish Language Dictionary. It says that a personal image is "a picture of someone in a drawing, painting, photo, etc., but also the way in which that person or thing is perceived and represented." In other words, it can be said that an image is that of a human being, and it is not important how it was created, but it is important that the person can be recognised in it. The identification of perpetrators of crimes for search purposes was known in the ancient. That was discovered by R. Heind, examining the Egyptian papyri on which wanted notices were written. As an example, he cited a wanted notice of 145 BCE, issued in Alexandria, Egypt: "A young slave Aristogenes, Sr. Giuzupus, fled from Alexandria. His name is Herman, he is also called Nejlesen, he is Syrian by birth, 18 years old, of medium height, without facial hair. He has straight legs, a dimple in his chin, and a lentil-shaped wart on the left side of his nose. There is a scar above the left corner of his mouth. He has a slave sign tattooed on his right wrist. He was dressed in a chlamys and a leather apron" (Kozieł, Dębiński, 1992).

In addition to the description, criminals were also identified by mutilations and branding. For example, the Hammurabi Code provided for a manus law (cutting off a hand for theft). The first attempts to mark people for the purpose of identifying them were already used in the Roman empire – slaves were marked by mutilations (cutting the skin, branding) in order to prevent them from escaping. In France, in the fourteenth and eighteenth centuries, and in Russia until the nineteenth century, criminals were stigmatised by burning marks on their bodies. In France, a thief was marked with the letter "V", and reoffender: "VV". In Russia, in 1637, the principle of branding criminals for evidence purposes was introduced. Marks of the stigma were generated on the face. The letter "B" identified a thief (Russian "vor"). The above-described mutilations and stigmatisation made it possible to recognise and even identify a person by special signs added to their outer appearance. Alphonse Bertillon, a famous French forensic examiner and scientist, became interested in this problem. He initiated the systematising of external appearance characteristics and thus founded the scientific field, which he called anthropometry (Kozieł, Dębiński, 1992).

With the advancement of civilisation and technology, new methods of recognising and identifying crime perpetrators were emerging. Initially, the state law and order services used methods such as a "parade of detainees". The creator of this method was Eugène-François Vidocq. In this procedure, a group of prisoners formed a circle and walked around police agents who were looking at them and memorising their appearances. In the light of the development in natural and technical sciences the identification using the "parade of detainees", which was an excellent method

at the beginning of the century became obsolete and ineffective. A certain method of identification was needed that would not have been based only on the unreliable memories of a handful of detectives, and therefore it had to employ scientific techniques (Kędzierska, 2007). The discoveries of biologists, chemists and physicists proved useful in the work of law enforcement agencies. This is how the area of forensics developed the origins of which date back to the second half of the 19th century, when fingerprints were used for the first time to identify suspects, forensic photography was launched and traces left at crime scenes were focused on and used in the process of investigating crimes.

A significant step in forensics came thanks to Alphonse Bertillon, who developed and implemented anthropometry as a technique that helps in identifying a person. The scientific idea was based on the assumption that some dimensions of the human body (height, head circumference, arm length) are unchanged from the moment of reaching maturity. The same scientist also developed a method of photographing people, introducing numerous technical innovations, including the camera itself, the distance between the camera and the subject, the photographed person's position – front view (en face) and side view (profile), type of lighting, etc. It is still used today.

Currently, in addition to the image of the face, an invaluable role in identifying people is played by fingerprints known for over a hundred years and the DNA profile, sometimes called the DNA fingerprint. In 1987, the UK police used DNA profiling for the first time to find the perpetrator of two murders and rapes. Since then, this method has been widely used by law enforcement and judicial authorities and is one of the fastest-growing in terms of technology. Fingerprints and DNA are referred to as biometric data, which have been classified as a special category of personal data by the EU GDPR regulations since May 25, 2018. The definition of biometric data is included in Article 4 point 14 the GDPR Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. According to the above regulation, biometric data mean "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person." These include features such as facial image, DNA, the iris of the eye, the arrangement of blood vessels, voice, shape of the auricle, or fingerprint data.

Facial image

Signalment photography is the method and principles of photographing criminals and suspects for reconnaissance purposes. The shots include the right-profile and front-profile, as well as right and left half-profiles. If a photographed person or an unknown corpse has visible distinctive signs on their body, such as tattoos, scars, birthmarks, deformities, missing fingers, they are recorded on separate photos. To take pictures of the face, a signalment pictures cabin is used, and in its absence, a special swivel chair.

A photograph preserves the image of a person and constitutes comparative material in anthroposcopic

Fig. 1. The room adapted for taking photographs in the seat of the Paris Police.

research. The methodology of performing these examinations is related to anthropometry, which initiated the identification of people and corpses based on the appearance of the body and skeleton by their measurements. The emergence of this science has led to initiating the field of anthroposcopic examinations.

In the course of anthroposcopic identification individual, basic elements of the external constitution of a person – mainly the face – and the presence of individual characteristics of the external appearance are analysed. The result of the study and conclusions, which summarise these studies, expressed in taking a position on the resolution of the issue posed by the procedural authority, are influenced by the presence of a feature that in some respect distinguishes the tested object from other objects. The properties of this feature are important so that it can be used to make such determinations that will relate to the final result in the form of group or individual identification. These properties include:

1) the abundance of identification features, which should be understood as the study of many features, which results in the need for particularly in-depth research and determination of as many features that characterise the identified object as possible. The more features will be determined, the higher the degree of likelihood of the positive identification test result;
2) quality of identification features – by itself, even a very large number of low-quality features will not allow for effective identification of the tested object determined by such features. A very important element here is the high quality of identification features. This quality may be determined by many factors, e.g. the clarity of the feature, stability durability of the feature and its measurability;
3) specificity of identification features – that is, the significance or the factor distinguishing one, and at most a few individual elements of a given system. Due to such selectivity or reference selectivity, this factor gains its significance.

The presented three properties of features should appear jointly in relation to each feature of the object undergoing identification (Pikulski, Kaliszczak, 1998).

Quality of identification features found not only on within the face but also in the entire body is the most widely used in anthroposcopic examinations. It should be noted that in these studies, there is no required number of features, allowing identification of a person. In some cases, one feature may be sufficient. Such characteristic features include, for example, scars, slashes, moles, skin discoloration, thickening of the epidermis, tattoos, etc. Their individual properties will be the shape, size, colour, convexity and place of occurrence (or arrangement in relation to each other). That is why it is so important to store photos of people in a 3D face/head model or a large number of photos in 2D format to enable the comparison of two photos of the same face/head alignment.

A forensic opinion in the field of anthroposcopy is difficult to elaborate in a case of incorrectly recovered evidence or poorly collected comparative material. Technical and visual quality of material determines both the possibility of performing examinations and the degree of categorising its final effect. Technical quality depends mainly on recording parameters, i.e. image or video resolution, file type and size as well as compression used during recording or archiving, as well as the type of recording device. Visual quality includes visibility of the features of compared elements, which is influenced by: external conditions such as lighting, weather conditions, as well as facial expressions, obscuring, distance from the recording device, size, scale and elements of appearance (glasses, facial hair, makeup).

In the present time, there is no separate registration of facial images in a 3D image in a specially designed database. Data containing images, in the form of mug shots, general photographs, images from industrial cameras and photos from private collections (e.g. of missing persons), are stored in the National Police Information System (KSIP). Ultimately the images ought to be stored in an electronic form (a set of facial images, personal data, characteristic features and additional data enabling the identification of the case/type of investigation) with just a limited number of hard copies (a set of documentation containing: decision to enter the material in the database, documents related to acquiring images, personal data and facial images, related correspondence with relevant authorities). A 3D image of the face is extremely useful for forensic identification.

The development of visual techniques and the introduction of street security cameras recordings for evidential and preventive purposes confirm the importance of the essence of a person's appearance for recognition or identification. In Poland, the first street security cameras were used in 1997 to reduce the crime rate. After two years, the effects were surprising as the statistics in this regard dropped by 60%. Therefore monitoring has become ubiquitous. In view of the large amount of secured data algorithms for persons identification began to be developed.

Currently, there are many methods of identification based on biometrics. However, they mostly are based on traces the occurrence of which is not as common as facial images from recordings in the present times of large-scale use of security camera systems (banks, offices, public transport, city cameras). Biometric systems for people identification are mainly based on the external appearance of the face. The face has been accepted as the primary information about a person included in biometric documents. Technologies using facial recognition are non-invasive, non-contact and the most natural, not restricting the movements of a person

in any way. Thus not only single images are used more and more, but also video recordings. Anthroposcopic examinations are based on the analysis of both photographs and video recordings, the specificity of which enables the identification of a person on the basis of material obtained in a non-invasive and universal way, so they are increasingly used in forensics. Face verification is the most natural and at the same time the most complicated way. Although work on this method of identification has been going on for 50 years it is still in the experimental phase. The face identification process usually includes three stages:

– location of a face in an image/video recording,
– isolation of characteristic features,
– identification.

The oldest face identification technique is the eigenfaces method, developed by M. Turk and A. Pentland in 1991. It is based on a large number of facial images contained in the identification system database. The first step is to divide the stored images into subgroups that are characterised by the highest degree of similarity, the second step is to create a "face" on the basis of a separate group. This "own face" is a graphic representation of the most and least similar features in a given group. "Own faces" are treated as creations composed of many different components, from which, by combination the system is able to create the face of any person, and then compare it with an image stored in its database. The greater the number of "own faces", the better the system's efficiency, although correct identification can be obtained on the basis of "only" approximately 100 "own faces". The disadvantage of this technique is that correct identification depends on a similar (in relation to the image in the database) lighting, pose or facial expression of the identified person. A smile is enough for the identification system to reject the image (Gutowska, Stolc, 2004).

Despite the imperfections of the algorithms we still hear about systems for identifying a person based on various features – the same ones that are also examined by forensic practitioners. Is the result of the operation of a specific system an identification or only verification of the entered stimulus with the one stored in its database? Identification and recognition are words that describe completely different processes and bring about varying consequences. Identification of a person is a very extensive issue requiring in specific cases the use of achievements of science and technology from many fields. The activities performed as part of forensic identification, which usually requires interdisciplinary cooperation of experts and the use of various research methods depending on the condition of the research material, in order to obtain the result of confirming the identity of a person, have only a slightly narrower scope. Recognition, on the other hand, does not require the use of analytical methods and is not as categorical as identification.

In practical applications biometric techniques deal primarily with the verification of persons (they compare the obtained features with a previously saved sample, i.e. one chooses one out of many and verifies it), and to a lesser extent with their recognition, when the features obtained from the measurement should be compared with every sample recorded in the database. The obtained result is not always sufficiently reliable, because apart from other factors that affect, e.g. an image recorded at the scene, it should be remembered that the characteristics in question change throughout life. While in many applications this is not a problem, a forensic identification performed mainly for evidential purposes must not allow even 1% uncertainty.

Fingerprint data

A great step in biometrics was made thanks to dactyloscopy. Skin ridges pattern is a unique feature that remains unchanged throughout human life. This feature in combination with their uniqueness is used to identify persons. The interest in biometric data, such as fingerprints date back to ancient Babylon, but it was probably not known then that their fingerprints could be used to identify a person. It was only at the turn of the 19th and 20th centuries that fingerprint identification became an effective method of fighting crime (Moszczyński, 1997). After regaining the independence by Poland, in 1919, the State Police began to use fingerprint examination more and more frequently in the investigative work (Buras, 2009). The 1920s marked the beginning of the State Police collecting tenprint cards of persons suspected of committing crimes. Initially, fingerprint cards were submitted to the central file kept by the Central Investigation Service, and for many years the collection file operated only in paper form (Buras, 2009). That changed in 2000 and since then the Central Fingerprint Register has been kept both in both paper and in electronic form. In the same year, the first professional Sagem Automated Fingerprint Identification System (AFIS) was purchased and launched in the Polish Police. Ten years later, this system was upgraded to the newer version no. 4.0. Currently, works on the upgrade (modernization) of AFIS to the MBIS version are in progress. By the end of 2020, 4,117,382 tenprint cards and 111,224 images of unknown latents from crime scenes had been collected in AFIS. In 2020, 49,313 tenrpint cards, 40,284 palm prints and 3,017 unsolved latents images were introduced. There had been 20,428 hits, including 18,603 tenprint card/tenprint card, 53 tenprint card/fingermark, 1,772 fingermark/tenprint card. With the help of devices for rapid identification of people based on fingerprints, 20,403 verifications of identity had been performed with 6,418 recorded hits.

The Fingerprint Data Collection is maintained in accordance with the principles set out in art. 21h–21n of the Police Act (The Act of April 6, 1990 on the Police). The tenprint cards of the persons subject to registration

are made by the ink method or electronically. Ink pads, a roller and a tenprint card are used to perform ink fingerprinting and palmprinting. Fingerprints of the right hand are taken first, then the fingers of the left hand. Fingerprinting starts with the thumb and ends with the little finger. Fingers of the right hand are first rolled on the fingerprint pad, then clockwise on the card, and the fingers of the left hand in the opposite direction. After rolling the individual fingertips, control prints are made of four fingers, from the index to the little one, by simultaneously pressing them in the appropriate place on the tenprint card. The control prints of the thumbs are made by simultaneously rolling them from the phalanx fold towards the fingertips. Palm prints are collected using a special roller, on which a sheet of paper or a cheiloscopic card is placed, and then the hand is rolled from the wrist towards the fingers.

All over the world, making tenprint cards with the ink method posed many problems for the persons responsible for fingerprinting, therefore, in the late 1980s, work began on developing a new, better method of collecting prints. The effort resulted in the development of devices for electronic fingerprint collection. They are Live Scanners, which have one thing in common: they do not use ink. Finger and palm images are collected electronically and transferred "live" to the database. Live Scanner with a camera built into the cabin with a swivel chair are part of the full-function electronic registration station. Currently, there are 385 such stations in the Polish Police.

The collection of fingerprint and palm print data at the fully-functional electronic registration station of persons' identification data is preceded by the registration of the fact of fingerprinting a specific person in a specific case. This is done by means of the National Police Information System (KSIP). After entering personal data into the KSIP, a policeman generates a file containing information on the person and the crime, and then sends it to the application installed at the station for registering the identification data of persons. Upon starting the application, the fingerprinting officer selects the registration mode (criminal, administrative, interview), and when the Live Scanner has been confirmed ready the fingerprinting process begins. It always starts with scanning the left and right hands, then simultaneously scanning four fingerprints of the left hand, the so-called control prints or "flats" and, further on, the right hand and control prints of both thumbs. The control prints of the right and left hand collected in this way are used in the fingerprinting process to verify the order of scanning the prints of the shifted fingers (from the big to the little finger). A very important functionality of the application is the quality control of scanned images and information about the error in case of failure to reach the assumed quality threshold. All the data sent from fully functional workstations to the central FingerPrint receiving system, located at the Central Fingerprint Registry at the Central Forensic Laboratory of the Police, is authorised with an electronic signature. A special key, called a token, is used to generate a signature every time.

In addition to criminal cases, the Police and Border Guard conduct administrative proceedings in which fingerprint cards of foreign citizens are drawn up. These activities are also carried out on the fully functional stations for registering the identification data of persons or on Live Scanners (in the Border Guard). Fingerprinting of a foreigner does not differ from the analogous procedure under criminal registration, with the exception of taking fingerprints of hands, which are not collected in those cases.

In the case of this technique, unfortunately it has not been possible to eliminate all the undesirable phenomena accompanying fingerprinting. The factors affecting the quality of fingerprint prints include:
– cleanness and dryness of skin,
– even pressure to the prism,
– steadiness of rolling,
– correct positioning of fingers and hands on the scanner window,
– epidermis injuries,
– hand and finger contracture,
– scars and deformations.

Regardless of the method of performing fingerprinting (either ink or electronic) officers make similar mistakes. The most common mistakes made during fingerprinting with Live Scanners are listed in Table 1.

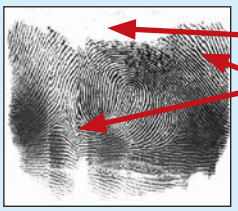
The method of collecting and obtaining information by the Police in the form of fingerprints and the method of preparing tenprint cards are regulated by the Regulation of the Minister of the Interior and Administration of January 28, 2020 on tenprint cards (Journal of Laws of 2020, item 173), Regulation of the Minister of Internal Affairs and Administration of 24 July 2020 on taking fingerprints and cheek mucosa swabs from police officers and employees (Journal of Laws of 2020, item 1347) and order No. 28 of the Police Commander in Chief of August 11, 2020 on fingerprint data collections (Official Journal 2020.44).

Due to the very good opinion that Live Scanner enjoys in the Police, it was decided that it would become an integral part of the station for comprehensive biometric data collection, built under the project "Development of a technologically advanced information system enabling automated processing of information collected in forensic biometric databases in order to combat crime or identify persons" No. DOB-BIO10/09/01/2019 "BIOMETRIA".

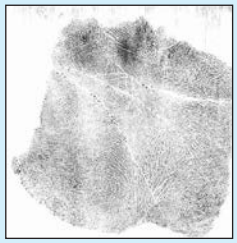
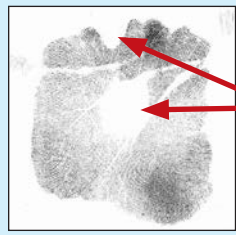
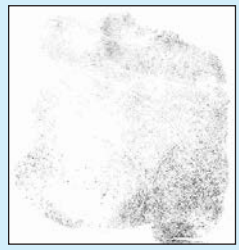
DNA data

DNA analysis has been used in examinations of case materials collected by investigators For several dozen years, i.e. it was relatively recently introduced. Deoxyribonucleic acid (DNA) occupies a unique

Tab. 1. List of the most common mistakes made when fingerprinting people with Live Scanners.

Correctly taken fingerprint	Description	Incorrectly collected fingerprints	Explanation of causes of incorrect collection of fingerprints and palm prints
	1. Good quality of collected fingerprint. 2. Visible pattern of skin ridges. 3. Finger has been rolled. 4. Visible intraphalange crease.		1. Missing upper portion of fingertip. 2. Too large area under the intraphalange crease.
			1. Missing visible part of print in the area of intraphalange crease (incorrectly rolled finger – uneven pressure).
			1. Cut-off part of fingerprint on the left.
			1. Missing top portion of fingertip. 2. Apparent lateral and axial slips and distortions in the print.
			1. Soiled, greasy or very sweaty finger. 2. Too small area of rolling – the finger was pressed on but not rolled. 3. Intraphalange crease not visible. 4. Too strong pressure of the finger on the prism.
			1. Finger was to dry; application of moisturising hand cream needed. 2. Too small area of rolling. 3. Too small pressure of finger on the prism.

Tab. 1. Continue.

Correctly taken fingerprint	Description	Incorrectly collected fingerprints	Explanation of causes of incorrect collection of fingerprints and palm prints
			1. Soiled, greasy or very sweaty finger. 2. Too strong pressure of the finger on the prism. 3. No distinct interphalange crease.
	1. Visible complete palm print. 2. Even pressure of all the areas of the palm. 3. Clean palm of appropriate moisture level.		1. Uneven pressure of individual areas of the palm. 2. Missing central part and upper of palm.
			1. Too weak pressure of all palm areas. 2. Very dry hand that has not been greased. 3. Illegible mark.
			1. Partly cut-off left and bottom part of the print. 2. Too strong palm pressure in one spot. 3. Clean hand of appropriate moisture level.

position among the chemical molecules that make up living matter. In the form of a linear sequence of bases, DNA stores information about the structure of protein and RNA (ribonucleic acid) molecules, which in turn determine the complete structure and all vital functions of cells and entire living organisms. The special structure of the DNA molecule has one important feature – it enables the precise duplication of genetic information. Without this process in would not be impossible to reproduce organisms and inherit features, and therefore the process of evolution on Earth (Węgleński, 1995). DNA is found in every human body, and the human body is made up of different types of tissue, which in turn are made up of cells. It is estimated that there are approximately 1,000 trillion of cells (1015) containing "the same" DNA molecule. Every living cell, except for mature erythrocytes – red blood cells – constitutes its source (Branicki et al., 2008).

DNA is a special molecule that has, inter alia, fingerprint-like features that made it so popular in forensics; namely: uniqueness, indelibility and immutability. The uniqueness (individuality) of DNA in the non-coding regions (Butler, 2005) makes it possible to distinguish individuals from one another, with the exception of monozygotic twins, which have the same profiles. The permanence (indelibility) of DNA is expressed in the fact that this molecule is located in the cell nucleus and protected by its wall. Additionally, a DNA molecule itself is quite stable and resistant to environmental factors. On the basis of a profile obtained e.g. from bone, it is even possible to identify a specific person long after death (Rothe et al., 2015). Another proof for the durability of the DNA molecule is the fact that DNA profiling is performed even after several dozen years, to investigate cases discontinued due to the failure to identify the perpetrator.

DNA profiling is most often used in forensics is based on the polymorphism of STR loci of short tandem repeats (STR). It is a very good source of information enabling the identification of suspects, persons with undetermined identity or hiding their identity, unknown human corpses, as well as allowing for establishing kinship. The most common biological materials analysed for the forensic DNA examination purposes include: blood, saliva, semen, hair, fragments of soft tissues, bone material and the so-called contact traces.

Although DNA analysis is a method that gives a high degree of certainty as to the correctness of identification, currently no biometric devices that use DNA as an identifier are offered by the private sector (Tomaszewska-Michalak, 2015). This may be due to the fact that the modern world it is usually required to confirm a person's identity in real time, e.g. when crossing the border, making banking or online commercial transactions. On the other hand, a standard analysis of DNA profiles is laborious and time-consuming and takes about 7–8 hours (Thong et al., 2015). Moreover, it requires laboratory conditions and is a multi-stage process consisting of DNA extraction, measurement of its quantity, amplification of specific STR regions during PCR reaction, separation of PCR reaction products during capillary electrophoresis and, finally, their detection and analysis of DNA profiles (Butler et al., 2004).

Currently, DNA analysis is routinely used for law enforcement and the judiciary activities. In cases where the DNA profiles of unknown offenders' traces obtained by forensic experts remain unidentified, they are registered the national DNA database. This collection is kept in accordance with the principles set out in Art. 21a–21e of the Police Act (Act of April 6, 1990 on the Police, 1990).

The information, including personal data, depending on the category, is entered into the DNA data collection upon an order by the authority conducting the preparatory proceedings, by the court, order or request of the locally competent Police authority. The DNA data that are processed include information about the non-coding part of DNA only. This collection is a source of non-procedural information and is an invaluable tool supporting the work of both the police and other law enforcement agencies (Ćwik, 2017). The DNA profiles entered in the Database are compared by means of CODIS (Combined DNA Index System) software with the already stored profiles. The software allows entry of a large number of profiles at the same time and their immediate comparison with the entire collection. Automated searches may lead to finding consistence between DNA profiles, the so-called match or hit. In case a match is found, such as: crime scene stain/ person, stain/stain, unknown body/unknown person/ person, unknown body/unknown person, relatives of the missing individual and relevant authorities are notified about this fact, i.e. authorities conducting criminal proceedings, proceedings in juvenile-related cases or detection/ identification activities (Article 21c of the Police Act). A lot of the matches found constitute the, so-called, cold hits, i.e. hits in which the selected people were not among suspects.

Obtaining matches is correlated with the number of registered profiles, so it is important that data are added to the database in a continuous and steady manner, i.e. not only unknown crime scene stains profiles should be entered, but also reference (comparative) profiles (Jurga, Mondzelewski, 2017).

By mid-2017, for the purposes of the DNA database, comparative (reference) profiles obtained from samples collected from persons specified in Art. 74 of the Code of Criminal Proceedings (Act of 6 June 1997 – Code of Criminal Proceedings) had been elaborated only by the Central Forensic Laboratory of the Police (CFLP). A buccal swab was taken with use of a forensic kit, labelled with an individual barcode, and then together with the biological sample registration card and the order referred to in Art. 21b of the Police Act, submitted to the CFLP. The amendment of legal regulations and the entry into force of Order No. 26 of the Chief Commander of the Police of 10 July 2017 on the performance by the Police of tasks related to the processing of information on the results of deoxyribonucleic acid (DNA) analysis and the maintenance of a DNA database made it possible to register DNA profiles of persons listed in art. 74 of the Code of Criminal Procedure obtained on the basis of an expert opinion from every forensic laboratory accredited in accordance with ISO 17025, which contributed to the increase in the registration of reference DNA profiles from the above-mentioned individuals.

On December 31, 2020, the data collection of the National DNA Database contained 129,895 DNA profiles, including 17,483 unknown stains profiles, 107,466 DNA profiles of suspects, 1,466 DNA profiles of unknown bodies, 37 DNA profiles of unknown persons, 570 DNA profiles of missing persons 2,809 DNA profiles of missing persons relatives and 64 profiles of police officers and employees of the Police. At the end of April this year, Order No. 13 of the Police Commander in Chief of April 12, 2021 on the DNA data collection entered into force, which upheld the existing rules for registering DNA profiles of persons listed in Art. 74 of the Code of Criminal Proceedings.

The automation of work and analysis of the obtained results contributed to greater throughput in forensic laboratories, and thus made it possible to test a large number of samples at the same time. It should be noted, however, that so far DNA profiling could only have been performed in a laboratory space, which is not always the best solution. Therefore, for many years, work has been underway on solutions allowing to obtain DNA profiles directly from the scene of a criminal event, mass disaster or from Identified persons, e.g. those arrested for a crime. New technologies are being regularly

implemented and validated in order to expand the capabilities of laboratories dealing with the detection of DNA and they have demonstrated improved sensitivity and informativeness (Butler, 2015).

One of the cutting-edge technologies in the field of forensic DNA analysis that uses the automation process is rapid DNA testing. It enables a quick analysis of the DNA profile using the STR loci polymorphism. Currently three devices of this type are available on the market: RapidHIT™ ID and RapidHIT™ 200 by Thermo Fisher Scientific, and ANDE from ANDE Corporation. Rapid DNA testing technology has been assessed, among others in cases of sexual abuse in Nepal and Costa Rica. The tests included the evaluation of reference samples from victims and evidential samples, including cigarette butts, water bottles, glasses and condoms. DNA profiles were obtained from all buccal swabs and 71% of evidence samples (Palmbach et al., 2014). It is worth mentioning that the rapid DNA testing technology is also introduced at scenes of mass disasters, e.g. in November 2018, after a fire of 60,000 hectares of land in Butte County, California (Gin et al., 2020) or after a helicopter crash, in 2019, in the Hawaiian Islands region in the range of cliffs on the northwest side of Kaua'i (Thermo Fisher Scientific, 2020).

Due to the importance of DNA analysis in biometrics, it was decided that an individual identification analyser should be incorporated in the station constructed under the already mentioned DOB-BIO10/09/01/2019 project. In order to make sure that the rapid DNA testing technology was in line with the project's expectations, validation tests were carried out on the Thermo Fisher Scientific RapidHIT™ ID device.

The device is an automated mobile platform for rapid individual identification based on DNA analysis (STR loci polymorphism) from biological material. It has been developed with a prospect of using it not only in laboratory conditions, but above all at the scene of crime or on the site of a mass disaster to identify victims or perpetrators of terrorist attacks. RapidHIT™ ID enables DNA processing (extraction, amplification and electrophoretic separation, as well as analysis in the form of a genotype) in about 90 minutes, practically without human interference. All that has to be done is to place a buccal swab in a disposable cartridge for comparative material analysis (ACE Sample Cartridge) and start the analysis. Due to the fact that the system is automated, it can also be operated by persons who are not specialists in the area of forensic DNA analysis, that is by employees of law enforcement and judicial authorities, employees of entities responsible for state security at airports, border crossings or in police units (Thermo Fisher Scientific, 2020).

The RapidHIT™ ID device has small dimensions, i.e. 28 cm width × 53 cm depth × 47 cm hight, and its weight amounts to only 28.4 kg. It is connected to a computer

Fig. 2. RapidHIT™ ID with connected to the computer with installed software and disposable cartridges (ACE Sample Cartridge).

(Figure 2) with the RapidLINK™ software installed and Genemarker® HID STR Human Identity Software, which enable an automatic analysis.

Results of such DNA analysis can be sent directly to CODIS or analysed locally (it is possible to save a large number of DNA profiles on the device and they can be compared with subsequent results). RapidLink™ (RapidLink™ Software V1.0 User Guide) has a module for analysis of kinship and a module that allows detecting DNA contamination. Kinship analysis is carried out using the RapidLINK™ Kinship module. The RapidLINK™ Staff Elimination module is designed to process and collect DNA profiles of persons who might possibly be the source of contamination of analysed samples, e.g. maintaining the device, performing the analysis, collecting the samples. The module allows automatic detection of the said contamination (Kartasińska, Jurga, 2020).

As part of the implemented project the RapidHIT™ ID device was validated and the process involved an evaluation of the parameters characterising its operation during execution of the method of determining the DNA profiles from the biological material in the form of saliva (buccal swabs). The assessed parameters included: sensitivity, balance, stochastic thresholds, reproducibility, cross-contamination test, stutter peaks heights, compliance and quality of DNA profiles, versatility of the method, determination of the components of DNA mixtures, resistance to environmental factors and inhibitors, specificity of the method. The above parameters were determined according to the recommendation of the European Network of Forensic Science Institutes DNA Working Group (ENFSI, 2010), guidelines by Scientific Working Group on DNA Analysis Methods (SWGDAM, 2016) and DAB-10 document (Polish Center for Accreditation, 2016). The validation has shown that profiles obtained by means of RapidHIT™ ID present sufficient good quality to allow analysing material collected onto a swab from internal cheek mucosa (reference material) and use the profiles to search the DNA database collections. The results are reproducible and reliable, and genotypes are compatible. The data generated by the traditional method of extraction, quantification and amplification followed by the electrophoretic separation are fully compatible with those generated by the RapidHIT™ ID system. The device can be operated by users who are not experts, because the procedure is simple and does not require specialist knowledge. However, a training in the operation of the device ought to be provided. The analysis of DNA profiles is carried out automatically by GeneMarker® HID STR Human Identity Software. Specialist knowledge is necessary for precise operation of that tool. When the DNA profile provided by RapidHIT™ ID is not sufficient to be entered to the DNA data collection, RapidLINK™ software signals it requires checking by a qualified analytics possessing specialist knowledge to decide whether the profile should be analysed.

Small dimensions and weight of RapidHIT™ ID device allow its transporting and use outside the laboratory, e.g. directly at the scene of the incident. It is also worth emphasising that cartridges in which biological material from buccal swabs samples are placed may be stored at room temperature, i.e. 15–25°C for up to two months. This allows them to be used, for example, at the police station or transport to a place of a criminal event without the need of procuring a refrigerator. A longer storage (up to six months), if necessary, requires a temperature of 4–10°C. An unquestionable advantage of RapidHIT™ ID is a short time of obtaining a DNA profile, i.e. 90 minutes, despite the fact that during this time you can get a profile from just one person. Until now, this long waiting time was an obstacle that hampered or even prevented the use of DNA analysis results as biometric data. The use of rapid DNA testing as part of the designed station for downloading biometric data will allow shortening the time lost, as compared with obtaining biometric data in the form of fingerprints or facial image, due to the necessity not only to transport a biological sample to the laboratory, but also to submit it for processing and analyses that lasted additionally approximately 7–8 hours. Thanks to speeding up the process by using the RapidHIT™ ID device it is possible to enter the obtained DNA profile to CODIS and search the DNA database sooner and, and thus – the verification of the person in question is achieved in a shorter time. In addition to that setting up of the above mentioned device, for example, at the police station, will facilitate the acceleration of activities undertaken in relation to a person detained for 48 hours, due to a legitimate suspicion that he/she has committed a crime (e.g. a crime defined in art. 248 § 1 of the Criminal Code).

Summary

Biometric systems are a proven method of fighting crime. Until recently, every collection of data or sample download was executed independently. That situation has, however, been changing for some time, an example of which is the tendency to combine recording the facial image with fingerprinting, referred to in the article. As part of the project: „Opracowanie zaawansowanego technologicznie systemu informatycznego umożliwiającego zautomatyzowane przetwarzanie informacji zgromadzonych w kryminalistycznych biometrycznych bazach danych w celu zwalczania przestępstw lub identyfikacji osób" (Developing the technologically advanced IT system enabling automated processing of information collected in the forensic biometric databases for the purpose of combating crimes or identification of persons) No. DOB-BIO10/09/01/2019 "BIOMETRIA" integration of biometric systems enters a new level and besides the mentioned systems the station will incorporate also a device for rapid DNA testing. Additionally, instead of a typical facial image

registration device an automated 3D scanner collecting information around person's head will be used. The use of 3D scanning will contribute to increasing the available visual information about individuals' appearance, which, when appropriately made use of, shall undoubtedly result in a higher crime detection rate. At the same time, gathering all devices in one place will shorten the data collection process and a special IT system will make this process more reliable.

ACKNOWLEDGEMENTS

The Authors wish to thank for the financial support received from NCBIR for the project „Opracowanie zaawansowanego technologicznie systemu informatycznego umożliwiającego zautomatyzowane przetwarzanie informacji zgromadzonych w kryminalistycznych biometrycznych bazach danych w celu zwalczania przestępstw lub identyfikacji osób" (Developing a technologically advanced IT system enabling automated processing of information collected in the forensic biometric databases for the purpose of combating crimes or identification of persons) No. DOB-BIO10/09/01/2019.

Sources of Figures and Tables:
Fig. 1: U.S. National Library of Medicine, 2006
Fig. 2: A. Jurga
Table 1: Authors

Bibliography

1. Branicki, W., Kupiec, T., Wolańska-Nowak, P. (2008). *Badania DNA dla celów sądowych*. Cracow: Institute of Forensic Research Publishing House.
2. Buras, D. (2009). Daktyloskopia na ziemiach polskich i w Polsce w latach 1909–1939. In: P. Rybicki, T. Tomaszewski (ed.), *Daktyloskopia. 100 lat na ziemiach polskich*. Warsaw: Association of Warsaw University Faculty of Law and Administration Graduates.
3. Butler, J.M. (2005). *Forensic DNA Typing: Biology, Technology, and Genetics of STR Markers*, 2nd ed. London: Academic Press Inc.
4. Butler, J.M. (2015). The future of forensic DNA analysis. *Philosophical Transactions of the Royal Society B: Biological Sciences*, *370*(1674), 20140252, https://doi.org/10.1098/rstb.2014.0252.
5. Butler, J.M., Buel, E., Crivellente, F., McCord, B.R. (2004). Forensic DNA typing by capillary electrophoresis using the ABI Prism 310 and 3100 genetic analyzers for STR analysis. *Electrophoresis*, *25*(1011), https://doi.org/10.1002/elps.200305822.
6. Ćwik, K. (2017). Elimination DNA database – an opportunity or a threat? A review of the functioning of elimination databases in selected countries. *Issues of Forensic Science, 295*(1).
7. ENFSI (2010). *Recommended Minimum Criteria for the Validation of Various Aspects of the DNA Profiling Process*, http://enfsi.eu/wp- content/uploads/2016/09/minimum_validation_guidelines_in_dna_profiling_-_v2010_0.pdf.
8. Gin, K., Tovar, J., Bartelink, E.J., Kendell, A., Milligan, C., Willey, P., Wood, J., Tan, E., Turingan, R.S., Selden, R.F. (2020). The 2018 California wildfires: Integration of Rapid DNA to dramatically accelerate victim identification. *Journal of Forensic Sciences*, *65*(3), https://doi.org/10.1111/1556-4029.14284.
9. Gutowska, D., Stolc, L. (2004). Techniki identyfikacji osób z wykorzystaniem indywidualnych cech biometrycznych. *Zeszyty Naukowe Wydziału Elektrotechniki i Automatyki Politechniki Gdańskiej*, *20*.
10. Jurga, A., Mondzelewski, J. (2017). Functioning of the DNA Database in Poland. *Issues of Forensic Science*, *297*(1).
11. Kartasińska, E., Jurga, A. (2020). *Rapid DNA* – a technology for rapid automated DNA profile analysis based on STR *loci* polymorphism. *Issues of Forensic Science*, *309*(3).
12. Kędzierska, G. (2007). In: W. Kędzierski (red.), *Technika kryminalistyczna*. Szczytno: Police Academy Publishing House.
13. Kozieł, T., Dębiński, Z. (1992). Image portrait in identification and search of persons. *Issues of Forensic Science*, *197–198*.
14. Moszczyński, J. (1997). *Daktyloskopia. Zarys teorii i praktyki*. Warsaw: Central Forensic Laboratory of the Police Publishing House.
15. Palmbach, T., Blom, J., Hoynes, E., Primorac, D., Gaboury, M. (2014). Utilizing DNA analysis to combat the world wide plague of present day slavery – trafficking in persons. *Croatian Medical Journal*, *55*(1), https://doi.org/10.3325/cmj.2014.55.3.
16. Pikulski, S., Kaliszczak, M. (1998). *Nowa metoda kryminalistycznej identyfikacji zwłok ludzkich*. Szczytno: Police Academy Publishing House.
17. Polish Centre for Accreditation (2016). Akredytacja laboratoriów badawczych – dostawców usług kryminalistycznych wykonujących czynności laboratoryjne (DAB-10 2nd edition of 2020-12-15), https://www.pca.gov.pl/download/data/rep-files/userfiles/_public/dokumenty_pca/dokumenty_ogolne/dab-10_2.pdf.
18. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.05.2016.
19. Rothe, J., Melisch, C., Powers, N., Geppert, M., Zander, J., Purps, J., Spors, B., Nagy, M. (2015). Genetic research at a fivefold children's burial from medieval Berlin. *Forensic Science International: Genetics*, *15*, https://doi.org/10.1016/j.fsigen.2014.10.022.
20. SWGDAM (2016). *Validation Guidelines for DNA Analysis Methods*.

21. Thermo Fisher Scientific (2020). The Kaua'i Police Department uses rapid DNA technology to save time and cost in disaster victim identification, http://assets.thermofisher.com/TFS-Assets/GSD/Reference-Materials/Kauai-police-dna-technology-disaster-victim-identification.pdf.
22. Thong, Z., Phua, Y.H., Loo, E.S., Goh, S.K., Ang, J., Looi, W.F., Syn, C.K.C. (2015). Evaluation of the RapidHIT™ 200 System: A comparative study of its performance with Maxwell® DNA IQ™/Identifiler® Plus/ABI 3500xL workflow. *Forensic Science International: Genetics*, *19*, https://doi.org/10.1016/j.fsigen.2015.05.006.
23. Tomaszewska-Michalak, M. (2015). *Prawne i kryminalistyczne aspekty wykorzystania technologii biometrycznej w Polsce*. Warsaw: Difin Publishing House Ltd.
24. U.S. National Library of Medicine (2006). *Visible Proofs: Forensic Views of the Body: Galleries: Technologies: The Bertillon System*. 2006-02-16.
25. Act of 6 June, 1997 – Code of Criminal Proceedings, Journal of Laws of 1997 No. 89, item 555, as amended.
26. Act of 6 April, 1990 on the Police, Journal of Laws of 1990 (consolidated text Journal of Laws 2020.0.360).
27. Węgleński, P. (ed.). (1995). *Genetyka molekularna*. Warsaw: Scientific Publisher PWN.
28. Order No. 13 of the Police Commander in Chief of April 12, 2021 on the DNA data collection, Official Journal 2021.27.
29. Order No. 28 of the Police Commander in Chief of August 11, 2020 on fingerprint data collections, Official Journal 2020.44.

Translation Ewa Nogacka

Digital forensics in the context of cloud computing data storage services

Paweł Olber[1]

[1] The Police Academy in Szczytno, p.olber@wspol.edu.pl

Summary

The role and capabilities of digital forensics in the cloud computing environment still remain an unsolved and insufficiently explored scientific area. The growing popularity of cloud-based data storage services makes recovery of evidence on the Internet a major challenge for forensic IT exminers. Existing legal barriers in most cases prevent direct access to cloud stored resources for the purpose of recovering data. In many situations, assistance from foreign law enforcement and judicial authorities is required. Findings made during forensic IT analysis that allow reconstructing user's activities and indicate the act of taking advantage of cloud computing data storage is a justification for undertaking international cooperation. Therefore, it is important to know potential sources of information that enable the reconstruction of the activity of the user in cloud computing services, as well as the awareness of the current state of knowledge and scientific research in this field.

Key words: computing cloud, file hosting service, digital forensics, IT examinations

Introduction

Cloud computing technology provides an unlimited access to computing resources such as servers and storage that are delivered with a minimal interaction with the service provider. Undoubtedly, one of the main advantages of cloud solutions is easy and quick access to resources that may be available on demand from anywhere in the world (Mell & Grance, 2011).

The growing popularity of cloud computing data storage services and the possibility of using these solutions for criminal purposes call for efforts on the part of scientists and practitioners in the field of forensic IT (Sharma, Arora, Sakthivel, 2018). One of the reasons for this situation is that cloud computing specifics exacerbate the difficulties in recovering and analysing digital evidence (Samy et al., 2018). A detailed review of the existing challenges and problems of digital forensics in the aspect of obtaining and examining data from cloud computing has been documented in the Report of the American National Institute of Standards and Technology: NIST (Herman et al., 2014). A large number of open challenges presented in the aforementioned document confirms that the role and possibilities of digital forensic in the cloud computing environment remain an unsolved and insufficiently explored area of scientific research (Martini, Choo, 2014). In order to overcome the persisting problems some scientists point to artifacts remaining in the memory of the data carriers recovered for the purpose of forensic examination as they may be important in the context of resources stored in the cloud computing environment.

The aim of the article is to present and summarise the current state of knowledge on the traces of cloud storage services users activities remaining in the memory of digital data carriers.

In view of the purpose of the article, the following research question was defined: what kind of traces of user activity of cloud computing data storage services stay in the memory of digital data carriers?

In connection with the posed research question a hypothesis was adopted according to which information on the activity of a user of Internet cloud remote file hosting service are stored in the memory of digital data carriers. That information can help to determine the content of resources in the cloud computing environment.

The research hypothesis had determined the structure of this publication. The results of previous research on forensic computing and cloud storage services were presented in separate parts of the article. Then, the existing possibilities of identifying traces of user activity in Dropbox and Google Drive were described in detail.

The research was carried out using the monographic method with critical literature analysis. In addition to that an empirical method was also applied to verify published results of Dropbox and Google Drive services research. Finally, the conclusions were formulated.

Literature review

Cloud computing services in the context of digital forensics are the subject of many scientific research undertakings. However, few scientists have studied the possibility of revealing traces of activity of users of cloud data storage services in the memory of local devices.

Dehghantanha and Dargahi (2017) endeavoured analyses of two services: CloudMe and Qihoo 360

Yunpan. CloudMe is a European file storage service established in 2012, owned by CloudMe AB. It offers secure cloud storage, file synchronization and remote data management client software. Qihoo 360 Yunpan, on the other hand, is a Chinese file storage service distinguished by the largest free online drive in the world. In the course of research, the authors used various operating systems: Windows 8.1, Android KitKat 4.4.2 and Apple iOS 8.0. As a result, they found that the analysis of the disk content, RAM memory, internal memory of mobile devices and secured network traffic allowed for the reading of authentication data, names of devices, as well as files stored on the on-line drives. These studies show that the use of cloud computing services leaves many traces in the memory of digital data carriers. They also demonstrate that the traces are formed as a result of performing various operations on files located in the cloud, but also during the installation / uninstallation of the client application. The researchers also highlighted the issue of data encryption in each of these services. They found that in the case of the Qihoo 360 Yunpan service, data security during the transfer was very low. The authors easily gathered and analysed network traffic data to recover required evidence. CloudMe protect users' privacy much better. Uninstalling the CloudMe client application, although it retained the configuration files, did not change the registry keys and uses data encryption during the transfer.

Mohtasebi et al. (2017) conducted studies of three more services: SpiderOak, JustCloud and pCloud. The researchers located and described various forensic artefacts connected to the use of these services by three web browsers: Internet Explorer, Mozilla Firefox and Google Chrome, as well as client applications installed on Windows 8.1 and an iPhone 5S with iOS 8.1.1. The data revealed and retrieved during the study included e-mail addresses, the ID and name of the created account, as well as the names of uploaded and downloaded files.

Teing, Dehghantanha, and Choo (2018) investigated the possibility of revealing traces of CloudMe online disk user activity. Their analyses covered various operating systems: Windows 8.1 Professional, Linux (Ubuntu 14.04.1 LTS distribution), Apple Mac OS X Mavericks 10.9.5, as well as mobile devices: iPhone 4 with iOS 7.1.2 and HTC One with Android KitKat 4.4.4. The research included the installation / uninstallation of CloudMe client applications, as well as uploading, downloading, browsing, deleting, synchronizing and sharing resources. Those authors emphasise that during examinations of the CloudMe service, attention should be paid to the database files: Cache.db, db.sdb and logs, application configuration files, as well as the web browser cache. The analysis of web browsing history allowed them to identify unique web addresses that helped to determine the activities performed by the CloudMe user, such as logging in / logging out, accessing files / folders and data downloading. Even though the connection to CloudMe via the web browser was encrypted, the researchers recovered the contents of the application's root directory from the browser cache. The application directory included user files, metadata, and OpenSearch description files containing timestamp information and passwords for shared resources.

Ahmad et al. (2020) who illustrated the existing trace identification capabilities in Windows 7 Ultimate described the existing possibilities of revealing the traces of pCloud service users' activities in volatile RAM. The scientists verified the possibility of revealing information on user interaction with the online drive based on various scenarios including data transfer with opening and viewing of its contents. In the study, the content of the volatile RAM memory as well as the cache of the Google Chrome web browser were analysed. Consequently, in the case of the pCloud service, it was possible to read all credentials and all information about files stored on the file hosting service. The study in question confirms the results of the previous experiments (Dargahi, Dehghantanha, Conti, 2017), whose authors focused on the pCloud service and presented the possibility of detecting many traces in the following operating systems: Microsoft Windows, Android, iOS and Linux. They showed that it was possible to read the credentials of pCloud users and information about files stored on the disk.

According to the above literature review the analysis of the content of digital data carriers allows (in principle) the disclosure of information indicating the use of cloud computing data storage services by the user of the device / system and additional information, such as: the content of virtual resources, user identification data and credentials. The research projects focus on several different services, including: CloudMe, Qihoo 360 Yunpan, SpiderOak, JustCloud, pCloud, which do not exhaust the catalogue of existing remote data storage solutions. This list may be extended, for example, by two popular services: Dropbox and Google Drive, which were the subject of Horsman's research (2020). Due to the widespread popularity of these services and the timeliness of the study the results will be presented and verified later in the article.

Methodology

In order to make a preliminary assessment of the possibility of detecting traces of the Dropbox and Google Drive users activities, an analysis of the results of the above-mentioned studies was carried out. Horsman's experiments (2020) used the Microsoft Windows 10 operating system and the Google Chrome web browser (version 67.0.3396.99). The web browser cache was read with Nirsoft's ChromeCacheView v1.77. In the course of repeating the examination procedure of Horsman (2020), a newer version of the Google Chrome web browser (version 89.0.4389.90) and current Nirsoft programs: ChromeCacheView v2.25, ChromeHistoryView v1.42 were used.

Dropbox service

The research conducted by Horsman (2020) shows that in case of using the Dropbox service via the Google Chrome web browser a file called www.dropbox.com.html is saved in the web browser's cache. This file does not open in the web browser window. Source code analysis is required. That procedure allows reading basic information about the service user and identification of the contents of the virtual disk. The information stored in the www.dropbox.com.html file comprises the following data:

- User name (tag: „display_name":),
- Account identifier (tag: „id":),
- User's email address (tag: „email"),
- URL address of user's profile picture (tag: „photo_circle_url":).

A fragment of the code recorded in www.dropbox.com.html file is presented in Figure 1.

Main window of the program

The www.dropbox.com.html file contains additional records that reflect user's activity on the Dropbox homepage. By default, on the homepage of the drive there is a list the last actions taken by the user. Each entry in the list of recent activities is incorporated in the structure of the www.dropbox.com.html file. The list of recent activities is saved under the "recent_activities" tags. The tags contain the interaction time (e.g. opening a folder / file), which is saved in UNIX format. If the user unfolds the last event that contains one or more files (usually graphic ones), a preview of the image is displayed for each file. That results in saving files with very specific names in the memory of the web browser, for example: size = 100x100size_mode = 4.jfif. In the event of finding files with similar names in the browser cache it should be concluded they indicate the above form of activity have taken place on the Dropbox drive.

Preview of drive contents

In the event that the Dropbox user displays all the files saved on the disk, the URL address is saved in the history of the web browser: https://www.dropbox.com/home. Additional information is saved in the www.dropbox.com.html file. In order to determine the entire contents of the user's virtual disk, read the information marked with "event_type": tags.

Preview of file contents

Horsman's research (2020) shows that when the graphic file content is displayed on the online drive it is cached by the web browser (stays in the cache) similarly to the situation when a file is previewed in the main window. The name of the file is very distinctive because it contains information about its size: size = 32x32size_mode = 5.jfif. The original file name is saved in the URL address and can be read from the browser's history: www.dropbox.com/home?preview=FILENAME.png. Additional information about viewed image files is saved in a text file named: is_xhr = trueactivity_context = 3activity_context_data =% 2FFILENAME.txt.


```
\{\"LOCALE\": \"GB\", \"prompt_ha_hiding\": true, \"_viewer_properties\":
{\"display_name\": \"GREY JOY\",
\"can_moderate_comments\": false,
\"deprecated_first_user_in_the_cookie_id\": 77837232,
\"is_reseller_session\": false,
\"is_team_assume_user_session\": false,
\"is_assume_user_session\": false,
\"_user_data\": [\{"initials_url\":\"https://ac.dropboxstatic.com/account_photo/get_initials?initials=GJ
\"user_root_permissions\":
\"edit\", \"has_never_set_password\": false,
\"id\": 77837232, \"sso_required\": false,
\"display_name\": \"Grey Joy\",
\"_authed\": true, \"home_ns_id\": 126648836,
\"lname\": \"JOY\", \"role\": \"personal\",
\"is_email_verified\": true,
\"fname\": \"GREY\",
\"cdm_path\": \"\",
\"email\": \"grey.joy@gooqlemail.com\",
\"is_paper_disabled\": false,
\"account_id\": \"dbid:AAAAz7mAv7FTO-BYzKWNpC1uj3FaJ1wVfBA\",
\"is_cdm_member\": false, \"nid\": \"01529833775757704936\",
\"is_dropbox_admin\": false,
\"paid\": 0,
\"root_ns_id\": 126648836,
\"photo_url\": null,
\"is_team_admin\": false,
\"familiar_name\": \"GREY\",
\"is_team\": false,
\"photo_circle_url\":"https://dl-web.dropbox.com/account_photo/get/dbaphid\%3AAACJ-_rJyCoDzFXXbB8MDaBqtS
\"DEFAULT_ROOT_NAME\": \"Dropbox\",
\"PERSONAL_ROLE_STRING\": \"Personal\"}
\}
```


Fig. 1. Fragment of www.dropbox.com.html file code.

Users' comments

A Dropbox user has an option of adding comments to files stored on the drive. Comments can also be added by other users who have access to the specific resource. Making a comment causes saving additional information, marked with the "comment": tag, in the text file is_xhr = trueactivity_context = 3activity_context_data =% 2FFILENAME.txt. If a third party responds to the comment, the account name of that third party will be saved in the following tags: display_name, lname and fname. However, the metadata does not include the e-mail address and account ID of the person responding to the comment, so it does not seem possible to identify the actual third party account.

File sharing and deletion

When a user goes to the tab containing the resources shared with other users it is reflected in the browsing history of websites: https://www.dropbox.com/share. Viewing a list of shared resources does not cache any additional information in the web browser. The same is true for deleted files. The Dropbox service stores deleted files for 30 days, and during that period the user can restore and view them. However, there will be no records in the web browser's cache that can be assigned to the data wipe action.

Results of author's own research

Upon repeating the research procedure of Horsman (2020) the author obtained different results. Namely, it has been found that when the contents of the Dropbox virtual drive are displayed https://www.dropbox.com/.html file is cached by Google Chrome and its name is encoded. This file is highlighted in Figure 2.

It has been determined that https://www.dropbox.com/.html does not contain any data identifying a Dropbox user. The examinations confirmed that the activity of the service user has its reflection in the website browsing history. If the Dropbox user views the entire disk content, the URL: https://www.dropbox.com/home is saved in the history of the web browser (according to Horsman's findings). Similarly, the web browser history stores web addresses that indicate other user activities, such as: viewing shared resources, opening a list of file requests, and opening a list of deleted files.

The author's examinations confirmed that displaying the content of the graphic file in the Dropbox service results in saving it in the cache of the web browser in JFIF format. In the example under discussion, the graphic file was saved under the name: fv_content = true & size_mode = 5.jfif.

The original name of the file was incorporated in the URL address and it can be read in the web browsing history. In the discussed example it is the file named: *1.JPG.*

The conducted study did not confirm the findings of Horsman (2020), according to which viewing the content of an image file and adding a comment in the Dropbox service causes saving additional information in text files.

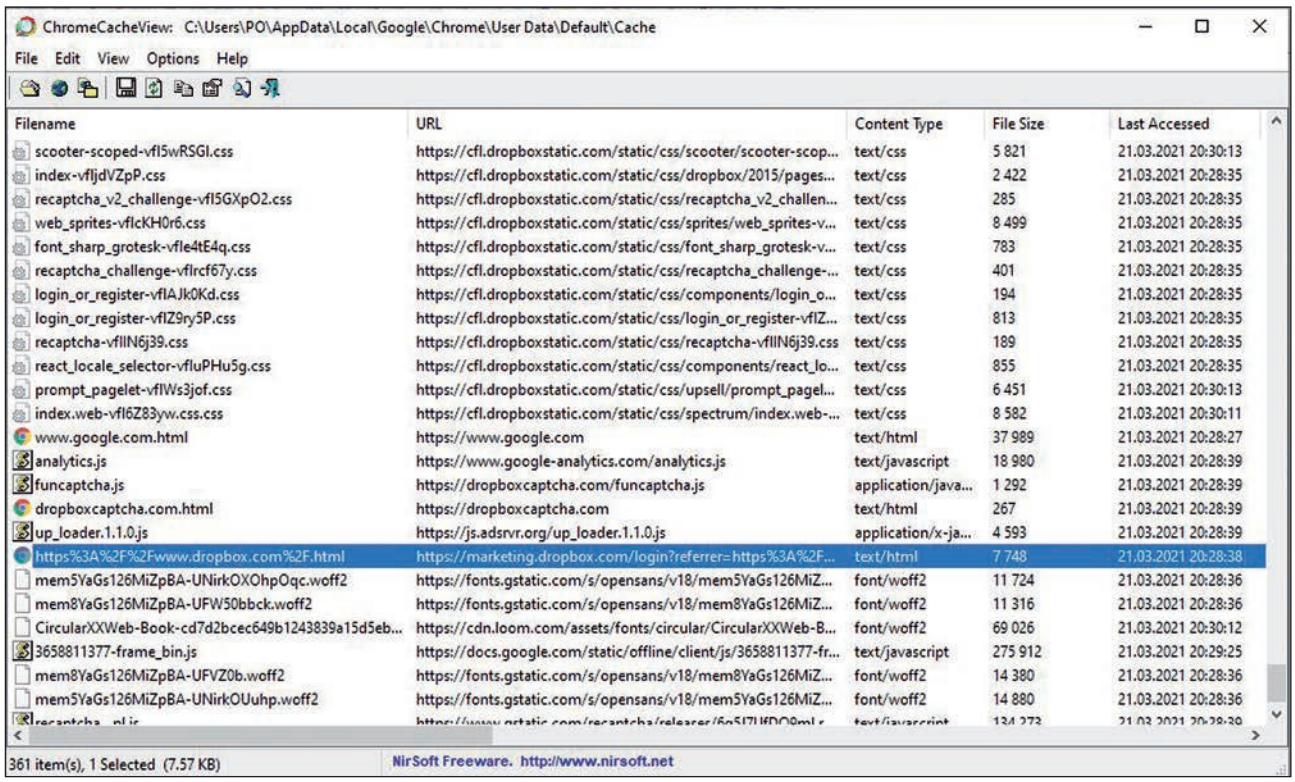


Fig. 2. ChromeCacheView window with the contents of the browser cache.

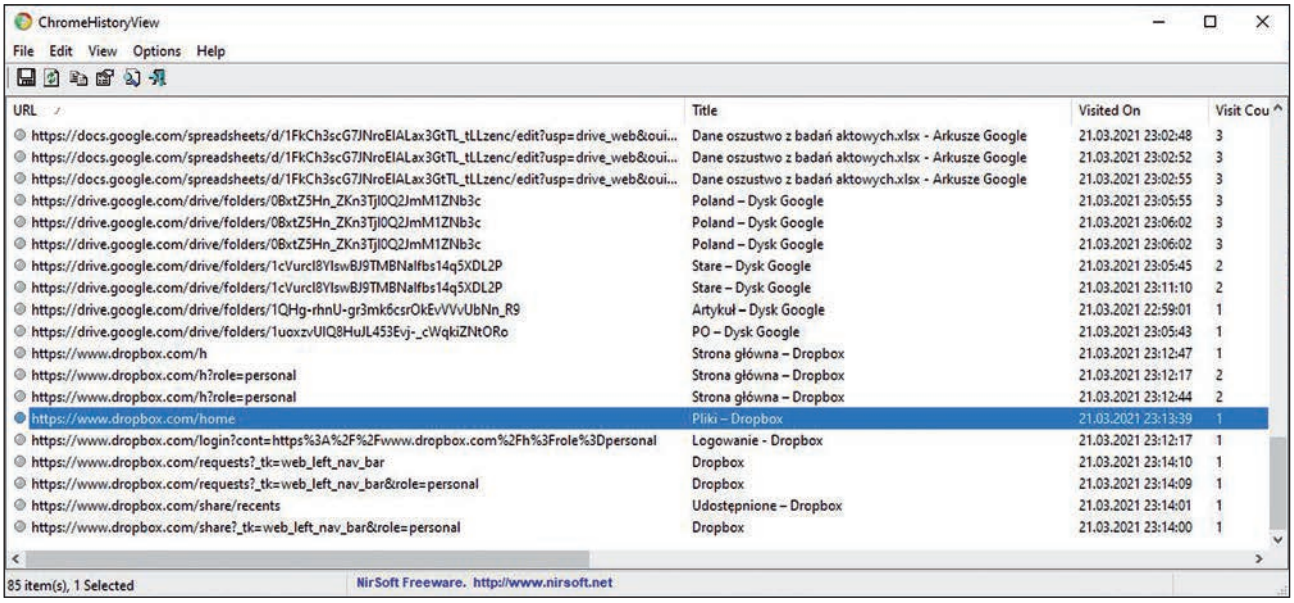


Fig. 3. Web browsing history.

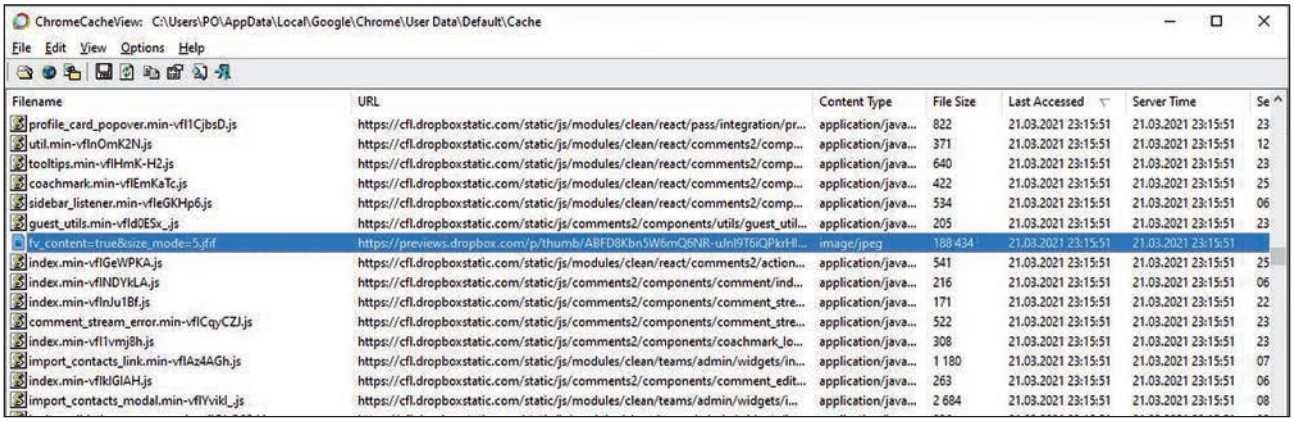


Fig. 4. Indication of fv_content=true&size_mode=5.jfif file.

Google Drive service

In the cache of the Google Chrome web browser limited information is available regarding the user's interaction with the Google Drive service. Research by Horsman (2020) shows that Google Chrome web browser cache does not contain files revealing the identity of the user or describing the contents of the virtual Google Drive. This means the information about the Google Drive service is not cached, unlike the Dropbox service. Only graphic files viewed from the Google Drive level are saved in the browser memory. The browsed files are saved under a specific name, for example: W1366-H662. This property does not apply to text documents, spreadsheets and multimedia presentations viewed at the disk level.

According to Horsman (2020) web addresses stored in the history of browsing websites and related to the user's activity contain limited information. For example, previewing the contents of an image file on a virtual drive does not change the URL: https://drive.google.com/drive/my-drive. On the other hand, displaying the contents of a specific folder alters the web address in a way that does not allow the resource name to be determined: https://drive.google.com/drive/folders/0By-CihkhmywOek1Gak4ySlhnQkk.

Results of author's own research

As a result of his own research the author found that Horsman's (2020) conclusions regarding the Google Drive service need to be complemented in terms of the possibility of identifying the names of folders stored on a virtual drive. Each time the contents of a directory are displayed, the URL changes, which does not allow the resource name to be determined. However, displaying web browsing history through ChromeHistoryView v1.42 allows to determine the names of Google Drive directories that have been opened by the user. Directories' names are included in the website titles, as shown in Figure 6.

The conducted research confirmed that the preview of the content of the graphic file on the Google Drive

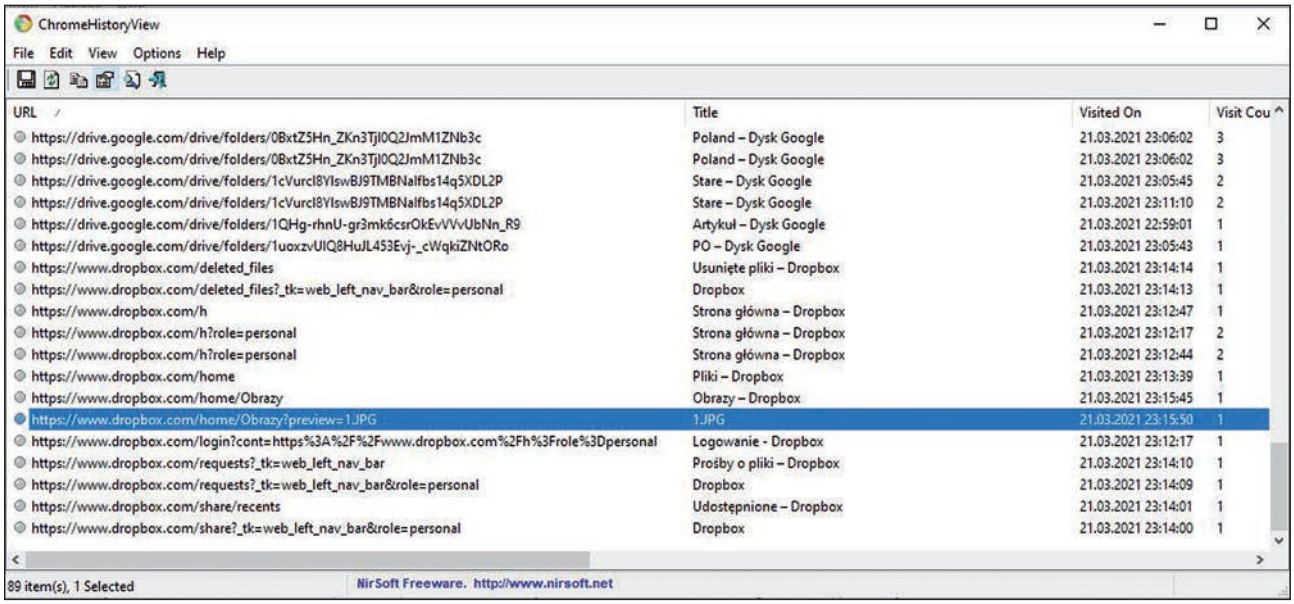


Fig. 5. Indication of 1.JPG file.

causes that it is cached and saved in the cache of the Google Chrome web browser. Figure 7 shows the graphic file w1280-h881-ft.jfif, the content of which has been displayed on the disk.

Displaying the content of text documents, spreadsheets and multimedia presentations saved on a virtual Google Drive does not result in saving additional information in the browser cache. However, it is possible to define the names of files opened by the user. Such information is available in the ChromeHistoryView program window, as shown in Figure 8.

Results and discussion

The analysis of published studies and the repeated procedure show that user interactions with Dropbox and Google Drive services result in saving information in the memories of local devices. Most information is saved when the Dropbox service is used. In this case, however, author's own research led to obtaining results different from the results of Horsman (2020). These differences are most likely due to the use of different versions of Google Chrome browser and free programs: ChromeHistoryView v1.42 and ChromeCacheView v2.25. The possibility of determining the content of the Google Drive based on the titles of the websites displayed via the above-mentioned applications, which was not described in the Horsman study (2020) should also be mentioned.

Summary

It can be assumed that the popularity of cloud computing storage services will continue to grow, which is due to the many advantages of these solutions. Therefore, there is a growing probability that a lot of data significant for criminal proceedings will be located in cloud storage including the virtual drives. However, in most cases the existing legal barriers make it impossible to gain direct access to this type of resources. In these circumstances it is necessary to use the assistance of foreign law enforcement and judicial authorities. The justification for applications addressed to foreign entities may be the findings made by experts in digital forensics. Those analyses may confirm the use of cloud-based data storage services, as well as help in determining credentials and the content of resources, which may be of importance for criminal proceedings.

Although the presented publication has mainly a character of an informative review it does contain

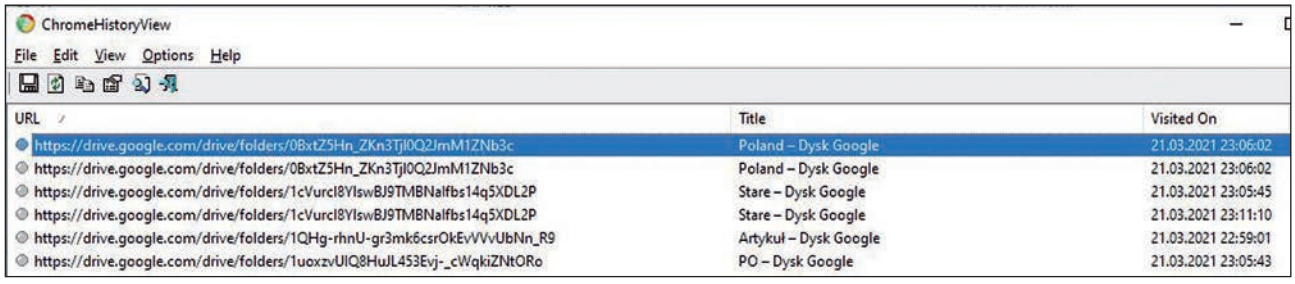


Fig. 6. Virtual disk folder names in web page titles.

Fig. 7. W1280-h881-ft.jfif graphic file saved in the browser cache.

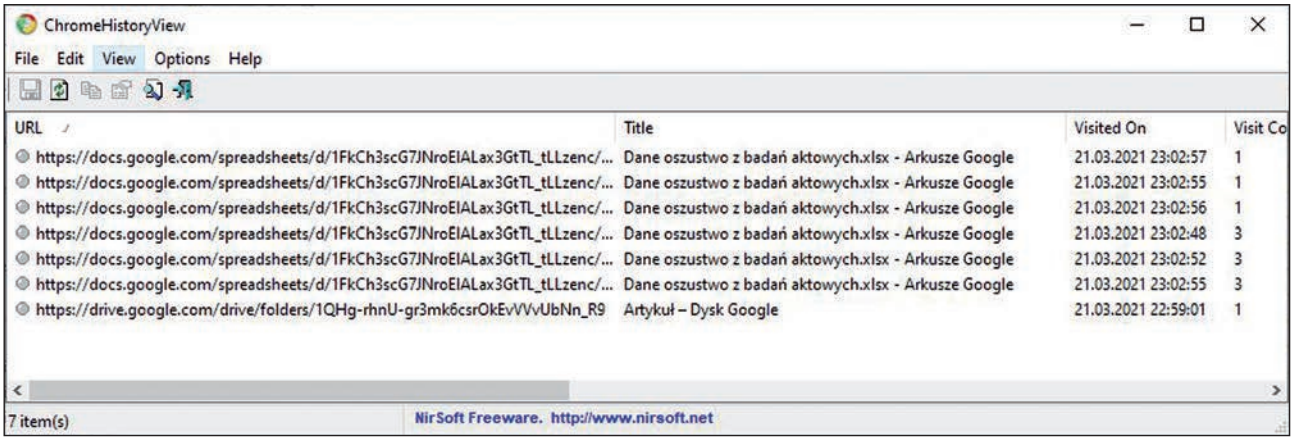


Fig. 8. Names of files opened by a Google Drive user.

a description and the results of author's own research confirming the adopted hypothesis. The own research was carried out using the latest versions of the application, which explains the differences in the obtained results. This example also confirms that each IT examination is of unique kind.

In future scientific research on the issue of detecting traces of user's activity in cloud computing services, one ought to pursue applying more advanced programms designed for forensic IT examinations, such as: X-Ways Forensics, NetAnalysis and HstEx.

Sources of figures:
Fig. 1: elaborated by author basing on: Horsman, 2020
Figs. 2–8: author

Bibliography

1. Ahmad, N.H., Hamid, A.S.S.A., Shahidan, N.S.S., Ariffin, K.A.Z. (2020). Cloud forensic analysis on pCloud: From volatile memory perspectives. In: M.H. Miraz, P. Excell, A. Ware, S. Soomro, M. Ali (ed.), *Emerging Technologies in Computing, Third EAI International Conference, iCETiC 2020*. Cham: Springer.
2. Dargahi, T., Dehghantanha, A., Conti, M. (2017). Investigating storage as a service cloud platform: pCloud as a case study. In: A. Dehghantanha, K.-K.R. Choo (ed.), *Contemporary Digital Forensic Investigations of Cloud and Mobile Applications*. Amsterdam–Boston et al.: Elsevier, https://doi.org/10.1016/B978-0-12-805303-4.00012-5.
3. Dehghantanha, A., Dargahi, T. (2017). Residual cloud forensics. In: A. Dehghantanha, K.-K.R. Choo (red.), *Contemporary Digital Forensic Investigations of Cloud and Mobile Applications*. Amsterdam–Boston et al..: Elsevier, https://doi.org/10.1016/B978-0-12-805303-4.00014-9.
4. Herman, M., Iorga, M., Salim, A.M., Jackson, R.H., Hurst, M.R., Leo, R., … Sardinas, R. (2014). *NIST Cloud Computing Forensic Science Challenges*. Gaithersburg: National Institute of Standards and Technology.
5. Horsman, G. (2020). What's in the cloud? – An examination of the impact of cloud storage usage on the browser cache. *Journal of Digital Forensics, Security and Law*, *15*(1).
6. Martini, B., Choo, K.-K.R. (2014). Cloud forensic technical challenges and solutions: A snapshot. *IEEE Cloud Computing*, *1*(4), https://doi.org/10.1109/MCC.2014.69.
7. Mell, P.M., Grance, T. (2011). *The NIST Definition of Cloud Computing*. Gaithersburg: National Institute of Standards and Technology.

8. Mohtasebi, S.H., Dehghantanha, A., Choo, K.-K.R. (2017). Cloud storage forensics. In: A. Dehghantanha, K.-K.R. Choo (ed.), *Contemporary Digital Forensic Investigations of Cloud and Mobile Applications* (s. 205–246). Amsterdam–Boston et al.: Elsevier, https://doi.org/10.1016/B978-0-12-805303-4.00013-7.
9. Samy, G.N., Shanmugam, B., Maarop, N., Magalingam, P., Perumal, S., Albakri, S.H. (2018). Digital forensic challenges in the cloud computing environment. In: F. Saeed, N. Gazem, S. Patnaik, A.S. Saed Balaid, F. Mohammed (red.), *Recent Trends in Information and Communication Technology*. Cham: Springer, https://doi.org/10.1007/978-3-319-59427-9_69.
10. Sharma, P., Arora, D., Sakthivel, T. (2018). Mobile cloud forensic: Legal implications and counter measures. W: S.C. Satapathy, A. Joshi (red.), *International Conference on Information and Communication Technology for Intelligent Systems*. Cham: Springer, https://doi.org/10.1007/978-3-319-63673-3_64.
11. Teing, Y.-Y., Dehghantanha, A., Choo, K.-K.R. (2018). CloudMe forensics: A case of big data forensic investigation. *Concurrency and Computation: Practice and Experience*, *30*(5), https://doi.org/10.1002/cpe.4277.

Translation Ewa Nogacka